CDM
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

2014

The big bang of mobile malware

DECEMBER 2013

CONTENTS

CYBER WARNINGS

Published monthly by Cyber Defense Magazine and distributed electronically via opt-in Email, HTML, PDF and Online Flipbook formats.

EDITOR

PierLuigi Paganini, CEH
Pierluigi.paganini@cyberdefensemagazine.com

ADVERTISING

Jessica Quinn
jessicaq@cyberdefensemagazine.com

CDTL - LAB REVIEWS

Stevin Victor
stevinv@cyberdefensemagazine.com

KEY WRITERS AND CONTRIBUTORS

Pierluigi Paganini
Dan Dagnall
Dave Porcello
Phillip Hallam-Baker
Christian Mairoll
Keith Ross
Dan Ross
Edward A. Adams
Peter Jenney
Paul Paget
David Rosen
James Valdez
Evan H. Lesser
Mike Danseglio
David Strom
Jeff Bardin
Jake Sailana
Marcela De Vivo
and many more…

Interested in writing for us:
writers@cyberdefensemagazine.com

CONTACT US:

Cyber Defense Magazine

Toll Free: +1-800-518-5248
Fax: +1-702-703-5505
SKYPE: cyber.defense
Magazine: http://www.cyberdefensemagazine.com

Executive Producer: Gary S. Miliefsky, CISSP®

Prediction: 2014 – The Big Bang Year of Mobile Malware

Yes, 2014 is litterly around the corner and the tail end of 2013 has been abuzz with they typical Brick and Mortar and eCommerce retailer hacking and thefts such as the recent breach at Target in the US. You can keep up with these breaches at http://www.privacyrights.org.

However, quietly lurking as a strong under current, and many of you have seen my recent articles and blog posts on this subject is the nearly explosive growth of Mobile Malware.

I fear that 2014 will be the year of Mobile Malware exploding onto the scene in full force. Recently, when the FTC.gov discovered that an Android Flashlight app was behaving maliciously (such as eavesdropping on user location, contact list and much more), the US Government stepped in and fined the company, threatening to shut them down if they don't fix the behavior and provide better disclosure information to their 50,000,000 (yes, 50m) end-user community.

This is just the beginning. Just checkout Dat Dealer and try their game if you want to see how much information is readily available and how valuable it is at https://datadealer.com/ (by way of full disclosure, our Executive Producer invested in this project).

I predict much more – first it's adware then spyware then real 'spook' spyware where governments spying on each other and their citizens, then it's the monetization of criminal malware where more and more citizens lose their personally identifyable information (PII) possibly followed by hidden bitcoin p2p malware used for mining –imagine your favorite app like Angry Birds or Candy Crush, running on over 100m smartphone devices becomes a network of 100m bitcoin computations.

So, as we round a corner, we can all agree that 'big data' is 'the big target' and now stealing it through access to smartphones and tablets will be the new wave – mobile malware is about to hit…and hit us very hard in 2014. This means it's time to consider not only the bring your own device dilemma (BYOD) as a big theme for 2014 but also the core concept of mobile encryption, data protection, system hardening and counterveillance for 2014.

To our faithful readers, Enjoy,

Pierluigi Paganini

Pierluigi Paganini, Editor-in-Chief, Pierluigi.Paganini@cyberdefensemagazine.com

P.S. Congrats Rose Midavaine (Belgium) – this month's contest winner!

RSA® CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share. Learn. Secure.

Capitalizing on
Collective Intelligence

Save $400 on Your Full Conference Pass | **Discount Ends Jan 24th**

2 Expos | 350+ Exhibitors | 21 Tracks
300+ Sessions | 17 Keynotes

Closing Keynote Speaker

STEPHEN COLBERT
Award-winning host and executive producer of *"The Colbert Report"* and *New York Times* best selling author

Experience new ways of learning with these exciting opportunities:

- > **NEW – The Sandbox** featuring *Innovation Sandbox* and *The Most Innovative Company*
- > **Flash Talks** Powered by PechaKucha
- > Two Day Immersive **SANS Tutorials**
- > (ISC)² Half Day **CBK Training Previews**

FOLLOW US ON: #RSAC

Register Now! www.rsaconference.com/cyberdefense

Global Diamond Sponsors: Juniper Networks, Microsoft, RSA

Global Platinum Sponsors: Cisco, FireEye

Global Gold Sponsors: Akamai, ixia, splunk>

Platinum Sponsors: HP, McAfee, Qualys, Symantec

Gold Sponsors: HOB, SOPHOS, TeleTrusT, Trend Micro, websense

Simplifying and Ensuring Data Security Across the WAN

By Keith Ross

A number of forces drive the need for increased data security, including protecting corporate information and trade secrets, government regulation, trade partner privacy agreements, and customer expectations.

For example, in banking and finance, the payment card industry has very strict digital security standards to prevent credit card information from being stolen from the network. The healthcare industry has regulations, including HIPAA and HITECH, to insure that sensitive personal health information is secure.

Current solution: the VPN tunnel

Many organizations don't encrypt their data over the WAN because it's traveling on a "safe" multiprotocol label switching (MPLS) network. Although MPLS networks provide more reliable connections than the Internet and aren't as public, they cannot be counted upon to be private—they're still vulnerable to attack.

It is important to understand that VPNs and technologies such as MPLS are not encrypted by default, and so require additional security measures to protect data. Even if the network is "private" or "virtually private," it is still subject to attacks. Data sent on MPLS networks is kept separate from other traffic, but it is not encrypted. What's more interesting is that over the past few years, many MPLS carriers have merged their private WANs and Internet backbones, further reducing security in the process.

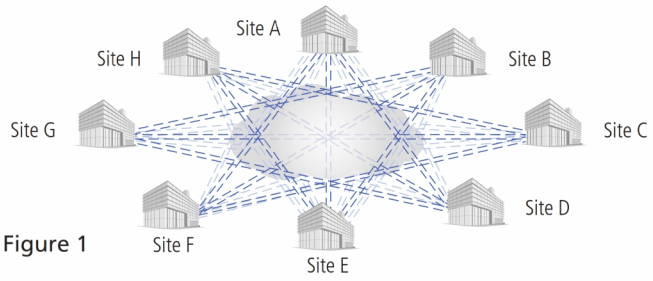


Figure 1

Breaking out of the tunnel

IPsec VPN tunnels are fairly simple to set up between only two points. However, when remote sites multiply, the number of tunnels increases exponentially. A tunnel is needed between each pair of sites **(Fig. 1)**, leading to administrative hassles every time a remote site is added. EncrypTight™ eliminates the need to establish point-to-point tunnels between each pair of remote sites, freeing network administrators for other tasks. With EncrypTight, every site on your WAN can establish an instant encrypted connection to every other site equipped with an EncrypTight appliance.

How is EncrypTight different than a VPN?

The EncrypTight solution is based on group encryption in which the encryption keys are centrally generated and securely sent to the EncrypTight appliances. This enables you to manage policy and key distribution centrally instead of on a time-consuming, site-by-site basis, as is the case with VPNs. EncrypTight enables you to secure "data in motion" in a way that is transparent to network architectures and protocols. And, if you decide to migrate to the Internet from MPLS networks using EncrypTight, you don't experience any service interruptions.

Layer 4 encryption

In addition to Layer 2 Ethernet frame encryption and Layer 3 IP packet encryption, EncrypTight offers a Layer 4 payload-only encryption option. Layer 4 encryption offers many advantages, including:

- Ability to pass encrypted data through NAT devices. VPN tunnels, which encapsulate the Layer 3 address, often don't work with NAT.
- Compatibility with policy-based routing and load balancing that require Layer 3 addresses to be intact.
- Layer 4 encryption leaves Layer 3 headers intact, making it possible to troubleshoot a network without turning off encryption.
- Because headers are intact, data looks unencrypted, making it possible to use within countries that restrict encrypted data.

Faster, safer, cheaper

If you want to lower costs and increase throughput, consider EncrypTight. It will enable you to quickly and easily set up a fully encrypted "mesh" that provides high-speed, secure, any-to-any connectivity over any public (or private) network. You can switch from expensive, private WAN links to inexpensive, public Internet connections with much greater bandwidth (**Fig. 2**). Plus, you'll get a fully compliant solution that offers security via encryption and ongoing authentication.

Cost and Throughput Comparison: Going from 10 Mbps to 100 Mbps

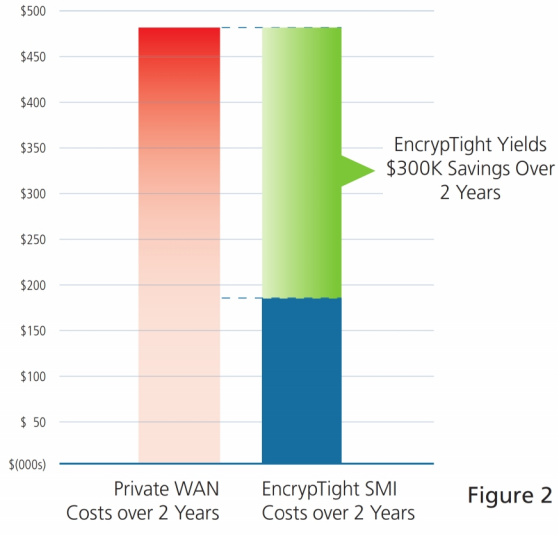


Figure 2

For more information, including a free whitepaper titled *Group Encryption: The key to protecting data in motion*, please visit **blackbox.com/go/EncrypTight**

Keith Ross is the Director of Product Management for networking products at Black Box (www.blackbox.com), a leading supplier of IT infrastructure and networking solutions.

Bitcoin case - How cybercriminals exploit typosquatting

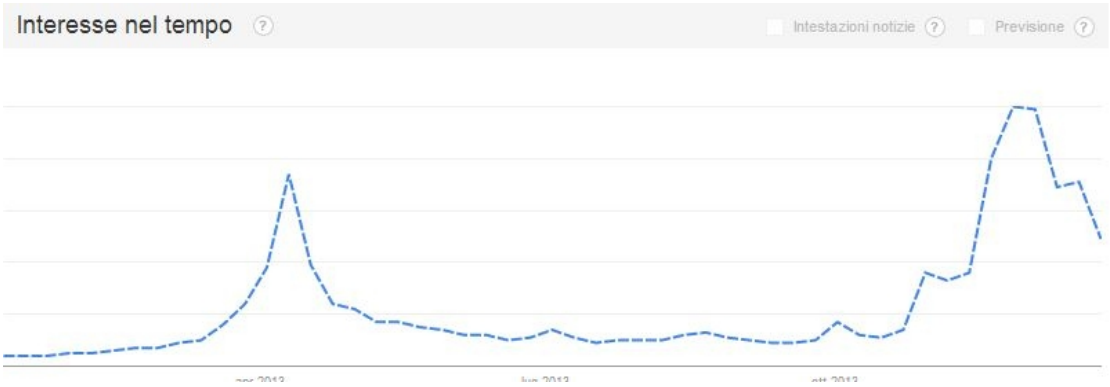
How cyber criminals could exploit typosquatting? The case of MtGox proposed by MalwareBytes, a fake domain used to serve malicious codes.

Typosquatting, also called URL hijacking, is a common form of hacking which relies on mistakes such as typographical errors made by Internet users when typing the website address into the address bar of their browser. Should a user accidentally enter an incorrect website address, they may be led to URLs related to websites managed by cybercriminals.

Criminals could operate substantially with two different techniques to exploit typosquating:

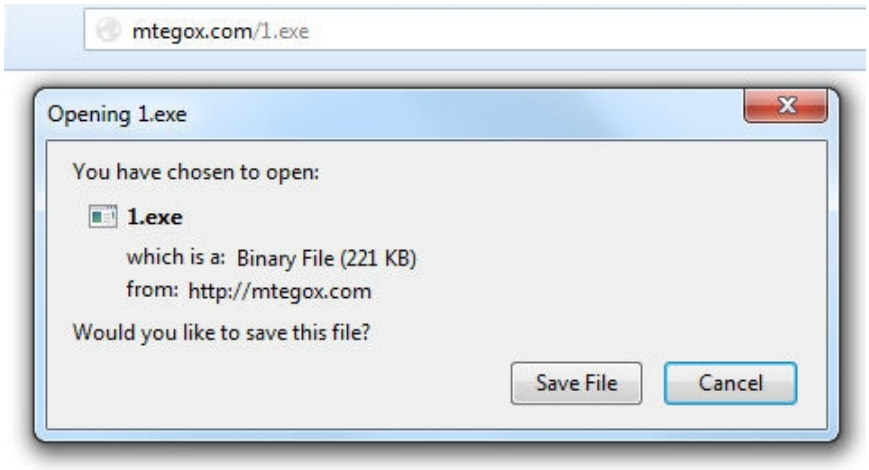
- register domains having URLs similar to legitimate websites belonging to popular brands.
- analyze the topic of interest in a particular period registering domain with URL similar to legitimate website reporting the information of interest.

Let's wear the clothes of the cyber criminal and try to take advantage of the second scenario, the first topic I have in mind is Bitcoin so let's verify if it could be a good idea to exploit typosquatting on URL related to websites that propose information on the popular virtual currency. Google Trends is a mine of information and looking at the below graph it is possible to note an increasing interest on the topic confirmed by the number of research on it. This means that a huge quantity of Internet users searches for Bitcoin information and navigate on Bitcon website.



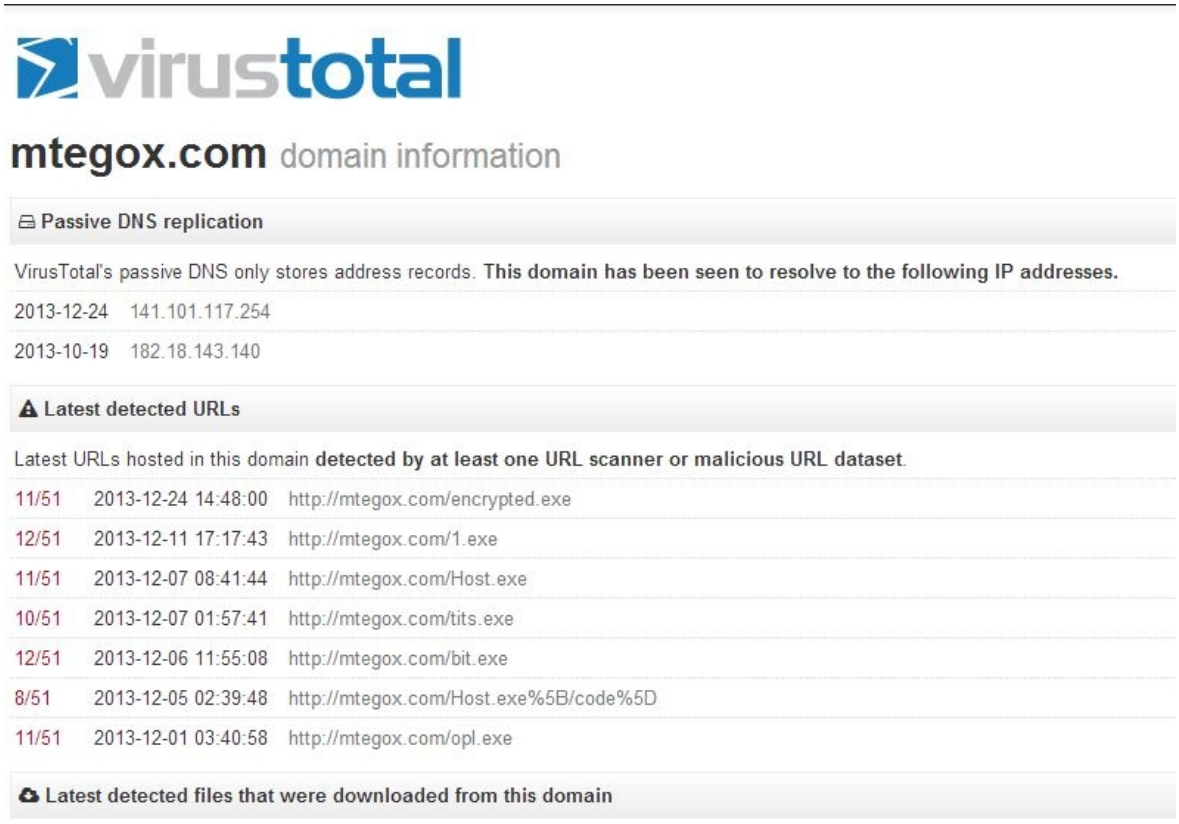
Malwarebytes security firm published an interesting post titled "Typo Trouble in Bitcoin Land" to show how much dangerous could be a typosquatting on the World's Largest Bitcoin exchange Mt. Gox.

Looking at the image below it is possible to not that cybercriminals exploited the error made by users typing "mtegox(.)com" instead "mtgox.com".



The site is managed by cybercriminals, currently it is down, and was a repository of malicious files served to users under the pretense of *"This file is needed to do x with your Bitcoins"*.

VirusTotal provided a detailed analysis of the malicious domain demonstrating that typosquatting method was used in the specific case by the attackers.



The experts at MalwareBytes discovered that running the malicious file the executable deletes the original file, placing additional hidden folders and files on the infected machine.

"That particular foldername shows up in a couple of sandbox reports and other pieces of analysis, including Malwr, a Joe Sandbox report and Lavasoft with the last two referencing a dayzstreaming website offering up yet more files."

Malwarebytes Anti-Malware detects the above as Spyware.Zbot.ED, and it is currently pegged at 39/49 on VirusTotal.

The malicious domain is full of other malicious elements a good reason to consider typosquatting a serious menace. A good practice is to be sure to double-check any and all “gox” themed URLs sent your way.

Typosquatting could be effective to arrange phishing campaigns or to serve malicious code such as spyware and Bitcoin miner, good advice is to double check URLs before submit them.

Source: Pierluigi Paganini, Editor-in-Chief, CDM

As XP's Term Ends, Don't Get Stuck with Lame Duck Security

Microsoft's end of support for Windows XP provides a prime opportunity to revisit the direction of security and compliance

By Joe Sturonas, CTO, PKWARE

In politics, a lame duck candidate is one who's reached the end of their term, typically with diminishing clout and support. When software vendors end support for products, business users are left with a lame duck of their own – expiring products that may often threaten the security of sensitive data they left behind.

Could this changing of the guard with your software and systems provide an opportunity to turn security and compliance into a source of incumbent strength?

Such is the case with Microsoft's Windows XP operating system. Microsoft will step away from support for XP in April 2014 after a dozen years and nearly a decade as the most prevalent operating system in the world, especially with SMBs and in the government sector. According to estimates earlier this year from Gartner and British IT representative group BCS, XP Windows' popularity carries a potential security and compliance time bomb: there are hundreds of millions of PC installations and users still on XP.

As summarized by Tim Rains, director of product management for Microsoft's Trustworthy Computing Group, in one of Microsoft's many posts on the end of support for XP: "*[I]nevitably there is a tipping point where dated software and hardware can no longer defend against modern day threats and increasingly sophisticated cybercriminals."*

Facing four months of active support and untold security threats, the expiration of XP makes room for not only a new choice with desktop operating systems, but also for the security and compliance regulations that keep them protected. As XP finishes out its "lame duck term," we want to offer suggestions for keeping on top of your operating systems' security and make sure you've truly got your compliance demands covered.

Three-Step Campaign for Compliant Security after Support Ends

Just like you'll be updating your operating system from XP, it's time to update your business philosophy around securing sensitive documents. Data is transmitted from one place to another more now than ever before. When XP came out, data largely just resided locally on the desktop/laptop. Today, data moves frequently and rapidly between desktop/laptop, mobile and the cloud. If your focus does is not on protecting

the data, volumes of unprotected data will find itself on mobile devices or in the cloud, where the device or storage isn't protected. Here, we're sharing three principles to keep data protected that we share in discussions with businesses as they deal with end-of-support of software and systems.

1. Run Supported Systems and Software. It bears repeating this straight-forward advice. XP has already run past the typical 10-year Microsoft support cycle and they have already posted warnings of the potential multiplication of "zero day" attacks on the system after the April 8 support deadline. In part, that's because after the April deadline, there will be no more updates or security guarantees from Microsoft. So, it just makes good security sense to get off XP and onto a supported operating system for your business and personal use. This also opens the conversation around security with all of the software and applications connected to XP. Are these up-to-date? Beyond that, do they match today's threats and your own risk appetite?

2. For Enterprise Security, Start with the Data. The shift in operating systems provides a chance to swap your security focus to the data itself, then the device. Data-centric encryption, for instance, guards against attacks from hackers. This keeps encryption both ahead of most threats and outpaces the slower rate of change found with operating systems. Focusing on this type of data-centric protection boils down to implementing controlled encryption, with policies in place that include a contingency key with every encryption operation so that the organization never loses access to the data, even as employees come and go.

3. Are You Really in Compliance? Put a different way, don't make compliance initiatives on security merely a checkmark in your strategy. Miss out on the details of compliance as it relates to your security plan and you fail to protect yourself from the bad guys and the auditor. For example, the Federal Information Processing Standards, or FIPS 140-2, covers varying levels of encryption. What government agencies need is a review of encryption products to ensure they are all FIPS 140-2 compliant. From what we've seen in the past, this hasn't stopped some software from being passed off as "compliant" – and business users being okay with that. For example, one government customer discovered that the product they were using was incapable of providing any policy based contingency keys or private key escrow, in addition to not being FIPS 140-2 compliant. They were left with gigabytes of encrypted, inaccessible, useless data. If they had only implemented a FIPS 140-2 compliant, policy based encryption solution with master key capabilities, all of their data would have been protected

and accessible. (It's worth noting that to satisfy FIPS 140-2, you also need to run on a supported operating system.)

The thing about lame duck candidates is that they're replaced with a new one – and with a new leader comes the potential for fresh approaches to existing challenges. The end of support for XP opens the door to a parallel conversation on security that truly covers the compliance. Election year or not, no one can afford to get stuck with lame duck security.

About the author

Joe Sturonas is the Chief Technology Officer at PKWARE, inventors of the ZIP file standard with data performance and security solutions in use by more than 30,000 global customers every day. Sturonas has been developing commercial software for nearly three decades and as CTO at PKWARE he is responsible for enterprise product development. He holds a BS degree from Miami University and an MS degree in Computer Science from DePaul University.

OPSEC novice ... here the manual for perfect cyber criminals

Cyber security expert Dancho Danchev profiled a new OPSEC training services in the underground, a new trend that is converging to standardization of knowledge sharing in the cybercrime ecosystem.

Speaking of cybercrime, with the term OPSEC are usually referred the basic operational security activities conducted by cyber criminals to avoid being tracked and monetize their cyber crimes (e.g. Frauds, scams, hacking campaigns and much more).

Cybercrime business will never stop to surprise us, every day new products and model of sale are proposed by gangs of criminals with a primary purpose to make their services user-friendly and available for a wide audience.

The cybercrime has its rules, operations, its patterns and monetization processes that are increasing in sophistication, an attractive underground in which the principal actors have started to think to earn also sharing their experience and expertise.

The cybercrime expert Dancho Danchev has recently profiled a product/training service launched around the middle of this year 2013, it is a course that caters novice cyber criminals offering them tools, manuals and precious suggestions to successfully undertake their career in illegality.

The course is complete and according Danchev covers the most interesting topics of OPSEC

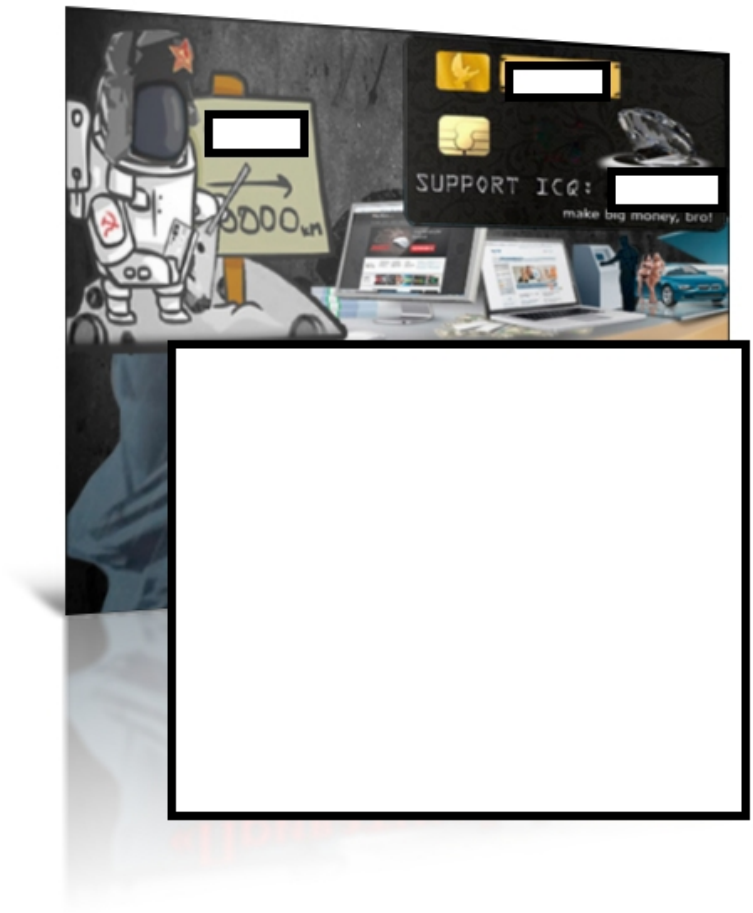
- *Basic host security*
- *Setting up Virtual Machines*
- *Setting up encrypted backups*
- *Setting up and securely using email clients*
- *Setting up a firewall*
- *Basics of OpenVPN and i2p*
- *Basics of Bitcoin use*
- *How to configure popular browsers for maximum security and anonymity*
- *How to use Socks4/Socks5 servers (malware infected hosts)*
- *How to anonymously use the most popular Web payment processes such as WebMoney, Yandex etc.*
- *How to securely communicate online using free/public/community tools*

Giving a look to the topics it is easy to recognize the knowledge of all the principal phases of a malicious criminal activity from the setup of a malicious architecture to the monetization phases and payment processes.

I consider the coverage of these topics fundamental also for any professionals that desires proof its knowledge of cybercrime and its OPSEC. The training in Operational

Security (OPSEC) is very interesting, it also includes access to a private forum set up for customers only in which the apprentices could exchange experiences and ask the support to skilled cyber criminals in an anonymous way.

The cost of the training package is very cheap, just $40 for the manual inclusing the access to the forum, dont' forget the discount of further 10$ in case the customer provides relevant feedback about course.



"The standardized OPSEC offering is targeting novice cybercriminals, and also has an interesting discount based system, offering $10 discounts for every feedback from those who've already taken the course." states the blog post published by Danchev.

As highlighted by Danchev we will assist in the future in the a standardization process of the OPSEC knowledge, through localization (translating the original documents) and training courses to instruct novice criminals. Online courses for novice cyber criminals are increasing and their quality is improving also thanks to the direct contribution of criminals that daily improve their methods and strategies on the field responding to the increasing pressure from law enforcement.

Probably elsewhere someones already arranging the next cyber criminal boot camp ... are you ready for the training on the job?

Source: Pierluigi Paganini, Editor-in-Chief, CDM

Fixing the Broken Internet

Applying NTRU Public Key Cryptography

Public key cryptography is the basis of security on the internet. SSL and TLS, which provide the foundation for secure communications are both based on public key, and they're in danger. The recent "Snowden" events have brought to light the fact that what was considered our strongest public key option, ECC [Elliptic Curve Cryptography], might have been tinkered with by the NSA, which makes it a non-viable implementation. RSA, the other major public key system is nearly broken and its performance is too poor for today's rapid transaction systems such as NASDAQ OMX which executes one million messages per second at sub 40 microsecond speeds. With the primary public key systems compromised, we find ourselves needing an alternative that is a) secure, b) fast, c) open, and d) not riddled with back doors and other holes that could be exploited by crooks. A perfect solution would also be future proof and be useful far down the road, after the time when quantum computers, a cryptographers nightmare, will be commonplace.

Enter NTRU; a fresh, lattice based public key cryptography system that's small, fast, strong, open source and will resist attacks by quantum computers . Implementing NTRU as an alternative to ECC and RSA is surely a daunting task and will need to be spread out over several years, but the result could be a completely secure and future proof Internet. The performance gains alone make NTRU the logical choice for carrying on the Internet public key activities.

Some may say that the key size in lattice based systems like NTRU are prohibitive. That may have been the case 10 or 20 years ago when systems relied on compact data to enable security, but todays systems are well capable of working with kilobyte long keys without breathing hard. Looking at the performance numbers in table 1 we can see that NTRU is 5000 times faster than RSA and roughly 43 times faster than ECC at the same bit strength and load. The significance of speed is realized in the time consuming handshaking activities when setting up a SSL/TLS connection where potentially thousands of transactions take place every second. Imagine the speed gains on an ecommerce site serving millions of people and the reduced load on the servers; a 5000x gain in performance allows quicker connects and more connects and improves both the user experience and machine efficiency.

Performance is key, but speed without strength makes no sense. An attack against RSA and ECC is multi year, multi computer affair however, advances in math have brought new algorithms to bear that are threatening RSA, and whatever NSA has done with ECC makes a math attack irrelevant. NTRU is based on lattice math which can be thought of as a "needle in a haystack" problem. The math allows NTRU to hide information in a huge matrix and quickly find

it again using its keys. This approach makes it nearly impossible to crack, by normal computers and quantum computers as well. For RSA and ECC, a quantum computer attack, without diving into Shor's Algorithm , basically does very rapid factorization and a machine with an appropriate number of Qubits should be able to crack any key in a matter of seconds. NTRU math makes this kind of attack impossible and reduces the attacker to a brute force approach where the system not only has to find all the "needles" in the haystack, but put them together in a cogent fashion; replicating the private key. In order to do this every possible combination of "needles" needs to be tried. It's estimated that NTRU's strength will be reduced by 50% under a brute force attack by a sufficiently large Quantum computer; far better than the 100% effectiveness against the factor based systems. Building cryptographic strength like this into todays applications means that they will be secure and remain secure far into the future.

Performance and strength are key to success in a public key system, but its just as important that the algorithms be open and available for scrutiny to eliminate the possibility of hidden back doors or other security holes. Security Innovation, the owner of NTRU, recently open sourced the patents and reference code with the goal of driving its adoption and helping to lock down the Internet as soon as possible. They've put together an Open Source licensing model that includes GPL 2 and higher , a FOSS exception and include statements that its an irrevocable grant by Security Innovation and/or any future owners of the patented NTRU algorithms. They've also provided a commercial license for non-open source applications, so there are no barriers to adoption due to licensing issues—the bugaboo of open source projects.

All this strength, performance and openness is great, but the real problem with introducing a new algorithm is the adoption curve. There needs to be an ever increasing number of system that have implemented a system before it can be used effectively—the old chicken and egg problem. Implementation of NTRU is no different and requires adoption of the algorithm generally and at both ends of the connection to work. It's risky as there's no guarantee that it will be implemented everywhere, hence it makes sense to not do a complete replacement but to implement it side by side with one or more of the major public key systems. William Whyte, Security Innovation's Chief Scientist, suggests that well built systems would use both ECC and NTRU encryption keys and use the ECC and NTRU signing mechanisms to transport the appropriate digital certificates. He goes further to say that there should be a well defined process for integrating other algorithms as they become available. Using this side by side approach reduces risk by providing options for future strength and backwards compatibility, smoothing the NTRU adoption curve.

NTRU, which was developed in 1996, has been peer reviewed and adopted as a standard by two standards bodies so far, IEEE 1363 and the Financial Services Industry's Accredited Standards Committee X9. The system has also been reviewed by NIST who state "Of the various lattice based cryptographic schemes that have been developed, the NTRU family of cryptographic algorithms appears to be the most practical...smallest key size...highest

performance." Currently, Security Innovation is betting that rapid adoption and implementation of the system will help push NTRU through the FIPS 140 certification process so it can be adopted by the US Government and DoD. There's a boatload of information on their website (https://www.securityinnovation.com/security-lab/crypto.html) detailing the state and status of the system, its definitely worth a look at.

Wrapping up, our global public key cryptography infrastructure is badly broken, one major public key system is near its end of life and the other has been compromised and no longer a trustworthy. NTRU is a new public key system that brings strength, speed, longevity and trustworthiness to the table. The advent of true quantum computing is near and that will break most every type of cryptography known, but NTRU will resist an attack, giving up a little strength but not falling over like the rest. Much is known about NTRU; its been positively reviewed in the international government, commercial, and education sectors and now that its been open sourced, its ready to begin replacing our broken public key infrastructure!

Anonymous Author

Sources:

http://www.nasdaqomx.com/technology/marketplacesolutions/trading

http://en.wikipedia.org/wiki/Quantum_computer

http://en.wikipedia.org/wiki/Shor's_algorithm

http://en.wikipedia.org/wiki/Qubit

https://github.com/NTRUOpenSourceProject/ntru-crypto

http://en.wikipedia.org/wiki/GPL

http://en.wikipedia.org/wiki/FOSS

http://blog.securityinnovation.com/blog/2013/08/crypto-algorithm-agility-solving-our-single-point-of-failure-problem.html

Pwnie Express

Pwn Plug R2

Introducing the Pwn Plug R2: a tightly-integrated penetration testing platform in a portable, shippable, plug-and-pwn form factor.

With onboard high-gain wireless and dual-Ethernet, external high-gain Bluetooth, 4G/GSM cellular, more storage, and many software improvements, the Pwn Plug R2 is the enterprise pentester's dream tool.

HARDWARE SPECS:

- *Processor / RAM: 1.2GHz Armada-370 CPU / 1GB DDR3*
- *Disk storage: 32GB microSDHC*
- *Onboard wireless: High-gain 802.11b/g/n, packet injection & monitor mode, 8" antenna*
- *Onboard I/O: 2x Gigabit Ethernet, 2x USB 3.0, serial console, microSD slot*
- *External high-gain Bluetooth adapter (up to 1000' range) supporting packet injection & monitor mode*
- *Optional support for Zigbee/Zwave, RFID, and Software-Defined Radios (SDR)*
- *Voltage: 110-240v*
- *Power draw: 5 watts idle, 15 watts max*
- *Dimensions: 5.2" x 3.7" x 0.8"*

pwnieexpress.com
sales@pwnieexpress.com
855.793.1337
@pwnieexpress

Core Features

- Onboard high-gain 802.11b/g/n wireless
- Onboard dual Gigabit Ethernet
- External high-gain Bluetooth adapter (up to 1000')
- External unlocked 4G/GSM cellular adapter (SIM card not included)
- 32GB microSDHC disk storage
- Automated NAC/802.1x/RADIUS bypass
- Simple web-based administration with "Pwnix UI"
- One-click Evil AP, stealth mode, & passive recon
- Out-of-band SSH access over 4G/GSM cell networks
- Maintains persistent, covert, encrypted SSH access to your target network
- Tunnels through application-aware firewalls & IPS
- Supports HTTP proxies, SSH-VPN, & OpenVPN
- Runs Pwnix, a custom Debian distro using the Kali Linux (kali.org) repositories
- OSS-based pentesting toolkit includes Metasploit, SET, Kismet, Aircrack-NG, SSLstrip, nmap, Hydra, w3af, Scapy, Ettercap, Bluetooth/VoIP/IPv6 tools, & many more!
- Unpingable and no listening ports in stealth mode

Cybercriminal threatens to sell 3.7M Customers data Israeli Banks

A group of hackers has threatened Israeli banks to disclose stolen data belonging 3.7 million customers unless the organizations pay up.

The Israel Hayom news revealed that at least three Israeli banks report extortion attempt by hacker demanding payoff in Bitcoin, the criminal threatens the financial institutions to reveal sensitive information of banking customers.

The cyber criminals claim to have stolen the details of 3.7 million customers and they threaten to sell the data on the underground market unless the organizations pay up.

The hacker involved in one of the biggest botnet in the Israel has threatened the 3 major Israeli banks, Israel Discount Bank, Bank Yahav and the First International Bank of Israel.

The banks immediately reported the threat to the Israel Police and Bank of Israel, they received an e-mail message threatening that unless they handed over a certain sum in Bitcoin currency by the end of next week, *"a list of customers' details would be given to hostile elements."*

In time I'm writing there is news regarding a possible data breach occurred to the banks, but the hacker claimed to have gathered the precious information through a powerful financial trojan botnet across Israel composed of millions of systems. According the

hacker the botnet collected a massive dump of stolen personal information, credentials, banking information and credit card numbers of 3.7 Million users.

Banks declined to comment the event but security experts don't believe realistic the threat, but we must consider that banking is even more target of cyber attacks. Cybercrime is adopting sophisticated techniques and advaced malware to avoid detection and monetize its effort, we have read of a new generation of malware that is able to operate with resilient infrastructure based on P2P protocol and hosted on Tor Network like the last varial of Zeur designed for 64 bit systesm.

The number of security incidents that involve wide audience is increasing, last in order of time is the data breach that suffered the US retailer Target.

Another concerning trend in the cyber criminal ecosystem is the cyber extortion, an illegal practice that is diffusing, malware authors that request the payment of a fee to unlock files encrypted by ransomware (e.g. cryptolocker) or gangs of cybercriminals that threaten private companies, including banks, with cyber attacks like DDoS and requesting the payment of a fee to stop the offensive.

Source: Pierluigi Paganini, Editor-in-Chief, CDM

File Transfers Don't Have to Be Risky Business

Simplify • Automate • Encrypt

GoAnywhere™ is a managed file transfer solution that improves workflow efficiency, tightens data security, and increases administrative control across diverse platforms and various databases, with support for all popular protocols (SFTP, FTPS, HTTP/S, AS2, etc.) and encryption standards.

With robust audit logs and error reporting, GoAnywhere manages file transfer projects through a browser-based dashboard. Optional features include Secure Mail for ad-hoc file transfers and NIST-certified FIPS 140-2 encryption. **Visit GoAnywhere.com for a free trial.**

See for Yourself

Find out why this bank depends on GoAnywhere to automate daily file exchanges with vendors.

GO ANYWHERE™

a managed file transfer solution by LINOMA SOFTWARE

GoAnywhere.com 800.949.4696

Kaspersky Labs Special Report: Mobile Malware

The explosive growth in mobile malware that began in 2011 has continued this year. There are now more than 148,427 mobile malware modifications in 777 families. The vast majority of it, as in recent years, is focused on Android – 98.05% of mobile malware found this year targets this platform. This is no surprise. This platform ticks all the boxes for cybercriminals: it's widely-used, it's easy to develop for and people using Android devices are able to download programs (including malware) from wherever they choose. This last factor is important: cybercriminals are able to exploit the fact that people download apps from Google Play, from other marketplaces, or from other web sites. It's also what makes it possible for cybercriminals to create their own fake web sites that masquerade as legitimate stores. For this reason, there is unlikely to be any slowdown in development of malicious apps for Android.

The malware targeting mobile devices mirrors the malware commonly found on infected desktops and laptops – backdoors, Trojans and Trojan-Spies. The one exception is SMS-Trojan programs – a category exclusive to smartphones. The threat isn't just growing in volume. We're seeing increased complexity too. In June we analyzed the most sophisticated mobile malware Trojan we've seen to-date, a Trojan named Obad. This threat is multi-functional: it sends messages to premium rate numbers, downloads and installs other malware, uses Bluetooth to send itself to other devices and remotely performs commands at the console. This Trojan is also very complex. The code is heavily obfuscated and it exploits three previously unpublished vulnerabilities. Not least among these is one that enables the Trojan to gain extended Device Administrator privileges – but without it being listed on the device as one of the programs that has these rights. This makes it impossible for the victim to simply remove the malware from the device. It also allows the Trojan to block the screen. It does this for no more than 10 seconds, but that's enough for the Trojan to send itself (and other malware) to nearby devices – a trick designed to prevent the victim from seeing the Trojan's activities.

Obad also uses multiple methods to spread. We've already mentioned the use of Bluetooth. In addition, it spreads through a fake Google Play store, by means of spam text messages and through redirection from cracked sites. On top of this, it's also dropped by another mobile Trojan – Opfake. The cybercriminals behind Obad are able to control the Trojan using pre-defined strings in text messages. The Trojan can perform several actions. including sending text messages, pinging a specified resource, operating as a proxy server, connecting to a specified address, downloading and installing a specified file, sending a list of apps installed on the device, sending information on a specific app, sending the victim's contacts to the server and performing commands specified by the server.

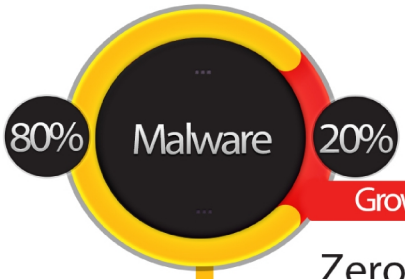
The Trojan harvests data from the device and sends it to the command-and-control server – including the MAC address of the device, the operating name, the IMEI number, the account balance, local time and whether or not the Trojan has been able to successfully obtain Device Administrator rights. All of this data is uploaded to the Obad control-and-command server: the Trojan first tries to use the active Internet connection and, if no connection is available, searches for a nearby Wi-Fi connection that doesn't require authentication.

SnoopWall

RECLAIM YOUR PRIVACY ™

TRADITIONAL MALWARE

Virus
Blended-Threat
Botnet
Zombie
Worm
Spyware
Trojan



MODERN MALWARE

Growing by 30,000 New Samples Daily

Zero Day
Advanced Persistent Threats
Command & Control Channels
Eavesdropping
Remote Control Threats on Smartphones, Tablets, iPhones & iPads

Anti-Virus programs can detect and protect you from **Traditional Malware** and only a small fraction of **Modern Malware**

SnoopWall protects you from **Modern Malware** - puts you in control

Get SnoopWall for

Windows (COMING SOON!)

iPhone (COMING SOON!)

Android

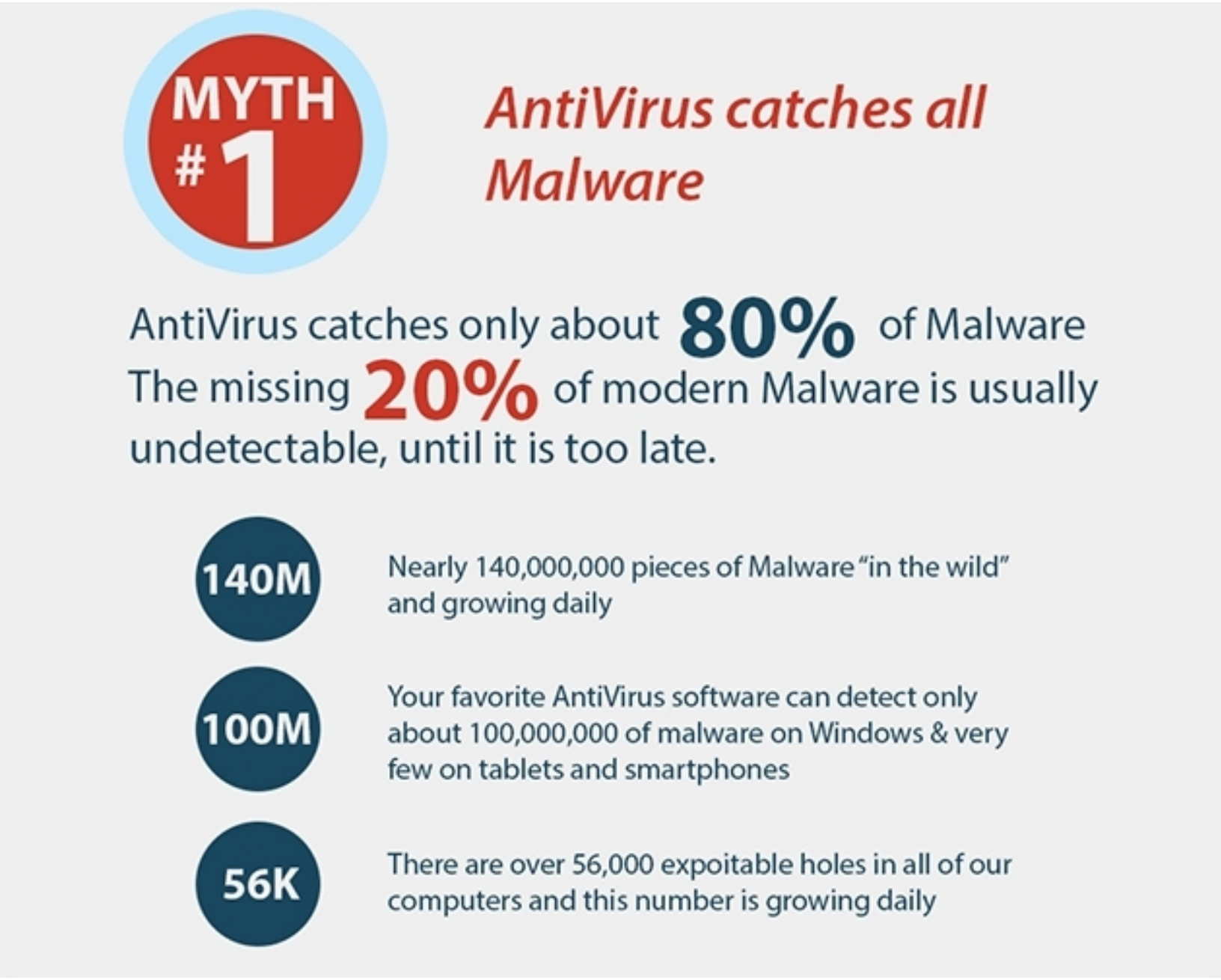
DID YOU KNOW ?

Less spying means longer battery life for your devices!

RECLAIM YOUR PRIVACY ™

Top 3 Myths About Antivirus Software

by AntivirusTruth.org

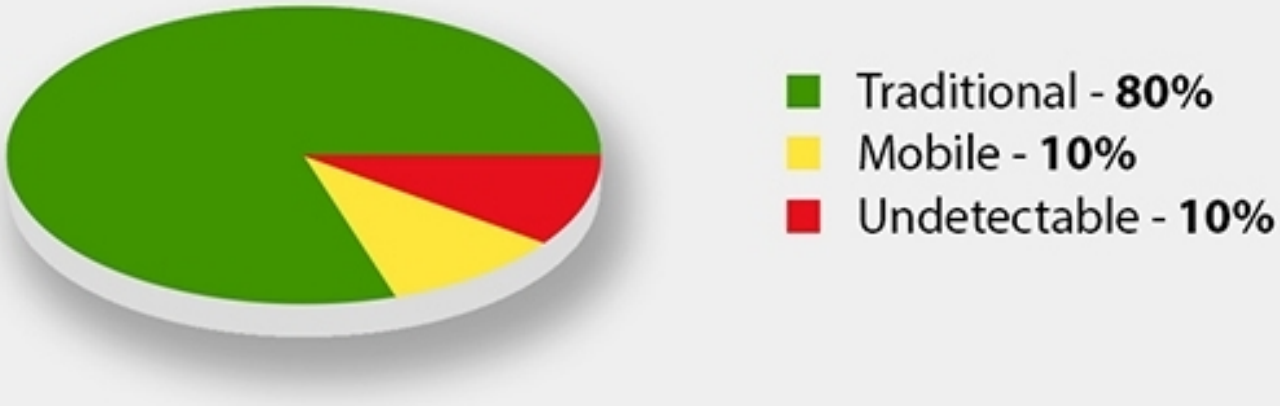


AntiVirus is proactive

AntiVirus is a **reactive** technology

not proactive.

It cleans up only the malware it recognizes and usually after the infection



Modern malware is going mobile and cannot always be detected. Undetectable malware is also called Zero-Day Malware (0day) and Advanced Persistent Threats (APTs) with Remote Control and Data Theft Through Command and Control (C&C) Channels over the Internet.

(Source: www.AntiVirusTruth.org, www.privacyrights.org, and nvd.nist.gov)

What the Average Joe should know about NSA

The National Security Agency has attracted the ire of the public recently. The actions of the organization have been justified time and again by officials, but the dust has hardly settled. Now civil libertarians and tech firms have started taking a stand against the organization and have asked the government for tighter rules and regulations. But what of the common man? Prof. Tung Yin, in a recent interview, highlighted many aspects that every American should keep in mind about the NSA.

The Patriot Act

A lot of ambiguity exists on where to draw the line with the Patriot Act. Many times a lot of what people feel relates to the act has nothing to do with it at all. As a piece of legislation, the Patriot Act needs some reformation, but its removal is not warranted. In the context of the NSA, Yin believes that "there are parts of the Patriot Act that made it easier for the government to get and to share what we call foreign intelligence information and this is a lot of what the NSA is going after. But you can see the issue here is that the police or the government has to have a probable cause to believe that the person has already committed a crime. And the NSA is not going to be in that position. They are in the position of trying to figure out, if we think this is what they are doing, who may be planning terrorist attacks or whatever. And they're doing a big dragnet of everybody, trying to figure out among everybody 'who should we be spending more time on'. So they can't possibly meet that probable cause standard."

LOVEINT: what you should know

When news broke that NSA employees had been tracking their exes and significant others through the database, it surprised no one. It is enough to make anyone paranoid, but there isn't much you can do about it. Yin highlights that one wouldn't know that the NSA had any data on them unless they were being dragged out into a criminal court case. And in that case anyone would have bigger problems to deal with than whether or not their lovelorn communication had been seen by government. But by some fluke if

someone is able to find out that they are being spied on then they can follow through with a civil rights lawsuits for the violation of their privacy rights.

Facebook vs NSA

The amount of data being gathered by the NSA is nothing compared to what firms such as Google or Facebook have collected over the years. A debate in favour of the NSA has often revolved around the fact that people are so wired in these days. They put a lot of information on social media sites and blogs etc without a thought for security or privacy but argue heavily against the NSA when they list information. However, there is a key difference. Yin says, “Facebook is entirely voluntary. I know a few people who refused to join Facebook and if they refuse to join Facebook, then Facebook does nothing about that. So, you can opt out from Facebook, but you can’t really opt out from the NSA.”

The problem lies in the fact that the NSA cannot and will not exclude people from its monitoring lists. People can try to be as private as possible but they can’t tell the NSA to stay out of their data.

Personal Privacy vs National Security

There are double standards at play. President Obama, when he was just a candidate for presidency, he was almost always talking the same language as civil libertarians. Such is not the case right now. The reality is that real threats do exist. Yin adds, “It’d be easy to be extremely critical of the NSA. I’m not saying that I would fully defend what it’s doing, but I guess I would say that if we saw more of what it is that the NSA is coming across, we might have a slightly different view of what’s going on.”

The government makes a valid point when it says that it could prevent 9/11 attacks if it had the proper intel at that time. “If you compare the two like that, the tangible and immediate [security concerns] tend to win out. But it will always win out if that’s the way you look at it. Then civil liberties will invariably be compromised,” says Yin.

You're on the list

In the aftermath of the revelations that the NSA has been extracting data many found their own unique ways of voicing their displeasure. Several people began posting dangerous words from the NSA's checklist in their emails and online posts etc. The idea was to detract the NSA from whatever aims they're trying to achieve. To some this may sound like a funny revenge to take against the government. But Yin warns that it isn't so simple. "I think messing with the NSA is a high-risk proposition… if your idea is 'I don't like the NSA and I'd do what I can to make its job more difficult and so I'm going to start making myself look like a bad guy', that's what I mean by high-risk strategy, maybe you can get away with it for a while, and maybe the risk isn't so much that you'll be hauled off for some political prosecution. Rather, the problem is that the government zeroes in on somebody who's doing that and they can find something else wrong that the person has done breaking the law. In the United States, there are over three thousand federal crimes." It won't be fun and games when the NSA zeros in on other aspects of your life just to get you into the trouble that you started as a joke.

At the end of the day what most people should know about the NSA is that it is here to stay. People could do *'The New York Times* test' on their own posts online i.e., would you be okay with the data or information showing up on the front page of *The New York Times*? If not then don't post it. This is easier said than done though. The NSA has a function to perform and it's not going to stop performing said function. What people can do is to try and use PGP (pretty good privacy) programs and other such tools to keep their data out of the NSA's hands.

Author Bio: Jessica has been writing about security and privacy issues for the last couple of years. She writes regularly for the Mobistealth blog and tweets @Jcarol429

NSA Spying Concerns? Learn Counterveillance

Free Online Course Replay at www.snoopwall.com/free

"NSA Spying Concerns? Learn Counterveillance" is a 60-minute recorded online instructor-led course for beginners who will learn how easily we are all being spied upon - not just by the NSA but by cyber criminals, malicious insiders and even online predators who watch our children; then you will learn the basics in the art of Counterveillance and how you can use new tools and techniques to defend against this next generation threat of data theft and data leakage.

The course has been developed for IT and IT security professionals including Network Administrators, Data Security Analysts, System and Network Security Administrators, Network Security Engineers and Security Professionals.

After you take the class, you'll have newfound knowledge and understanding of:

1. How you are being Spied upon.
2. Why Counterveillance is so important.
3. What You can do to protect private information.

Course Overview:

How long has the NSA been spying on you?
What tools and techniques have they been using?
Who else has been spying on you?
What tools and techniques they have been using?
What is Counterveillance?
Why is Counterveillance the most important missing piece of your security posture?
How hard is Counterveillance?
What are the best tools and techniques for Counterveillance?

Your Enrollment includes :

1. A certificate for one free personal usage copy of the Preview Release of SnoopWall for Android
2. A worksheet listing the best open and commercial tools for Counterveillance
3. Email access to the industry leading Counterveillance expert, Gary S. Miliefsky, our educator.
4. A certificate of achievement for passing the Concise-Courses Counterveillance 101 course.

Visit this course online, sponsored by Concise-Courses.com and SnoopWall.com at http://www.snoopwall.com/free

trueventus

BLUESPACE

18 - 20 FEBRUARY 2014 | KUALA LUMPUR, MALAYSIA

Exclusive 20% discount for ISACA – Malaysia Chapter members.
For more information, kindly visit the event website www.trueventus.com
To receive updated brochure and registration details, kindly contact Sandy at sandyb@trueventus.com or +603 2781 1510

Endorser

ISACA®
Trust in, and value from, information systems
Malaysia Chapter

Supporting Organisations

CyberSecurity MALAYSIA
An agency under MOSTI

ispa.my
Information Security Professionals Association of Malaysia

The Information Security Professional Association of Malaysia (ISPA) is the only association in Malaysia that supports the development of Information Security.

Media Partner

CDM
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR I.T. SECURITY INFORMATION

Top Twenty INFOSEC Open Sources

Our Editor Picks His Favorite Open Sources You Can Put to Work Today

There are so many projects at sourceforge it's hard to keep up with them. However, that's not where we are going to find our growing list of the top twenty infosec open sources. Some of them have been around for a long time and continue to evolve, others are fairly new. These are the Editor favorites that you can use at work and some at home to increase your security posture, reduce your risk and harden your systems. While there are many great free tools out there, these are open sources which means they comply with a GPL license of some sort that you should read and feel comfortable with before deploying. For example, typically, if you improve the code in any of these open sources, you are required to share your tweaks with the entire community – nothing proprietary here.

Here they are:

1. TrueCrypt.org – The Best Open Encryption Suite Available
2. OpenSSL.org – The Industry Standard for Web Encryption
3. OpenVAS.org – The Most Advance Open Source Vulnerability Scanner
4. NMAP.org – The World's Most Powerful Network Fingerprint Engine
5. WireShark.org – The World's Foremost Network Protocol Analyser
6. Metasploit.org – The Best Suite for Penetration Testing and Exploitation
7. OpenCA.org – The Leading Open Source Certificate and PKI Management
8. Stunnel.org – The First Open Source SSL VPN Tunneling Project
9. NetFilter.org – The First Open Source Firewall Based Upon IPTables
10. ClamAV – The Industry Standard Open Source Antivirus Scanner
11. PFSense.org – The Very Powerful Open Source Firewall and Router
12. OSSIM – Open Source Security Information Event Management (SIEM)
13. OpenSwan.org – The Open Source IPSEC VPN for Linux
14. DansGuardian.org – The Award Winning Open Source Content Filter
15. OSSTMM.org – Open Source Security Test Methodology
16. CVE.MITRE.org – The World's Most Open Vulnerability Definitions
17. OVAL.MITRE.org – The World's Standard for Host-based Vulnerabilities
18. WiKiD Community Edition – The Best Open Two Factor Authentication
19. Suricata – Next Generation Open Source IDS/IPS Technology
20. CryptoCat – The Open Source Encrypted Instant Messaging Platform

Please do enjoy and share your comments with us – if you know of others you think should make our list of the Top Twenty Open Sources for Information Security, do let us know at marketing@cyberdefensemagazine.com.

(Source: CDM)

National Information Security Group Offers FREE Techtips

Have a tough INFOSEC Question – Ask for an answer and 'YE Shall Receive

Here's a wonderful non-profit organization. You can join for free, start your own local chapter and so much more.

The best service of NAISG are their free Techtips. It works like this, you join the Techtips mailing list.

Then of course you'll start to see a stream of emails with questions and ideas about any area of INFOSEC. Let's say you just bought an application layer firewall and can't figure out a best-practices model for 'firewall log storage', you could ask thousands of INFOSEC experts in a single email by posting your question to the Techtips newsgroup.

Next thing you know, a discussion ensues and you'll have more than one great answer. It's the NAISG.org's best kept secret.

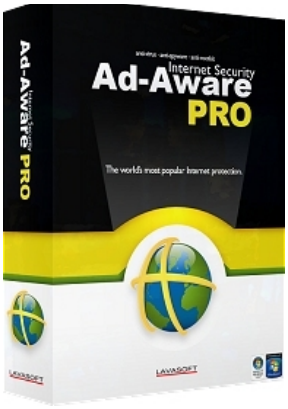
So use it by going here:

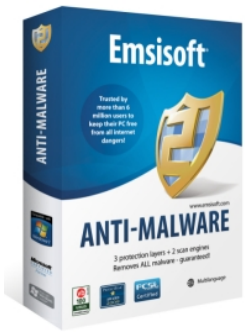
http://www.naisg.org/techtips.asp

SOURCES: CDM and NAISG.ORG

SIDENOTE: Don't forget to tell your friends to register for Cyber Defense Magazine at:

http://register.cyberdefensemagazine.com





where they (like you) will be entered into a monthly drawing for the Award winning Lavasoft Ad-Aware Pro, Emsisoft Anti-malware and our new favorite system 'cleaner' from East-Tec called Eraser 2013.

Job Opportunities

Send us your list and we'll post it in the magazine for free, subject to editorial approval and layout. Email us at marketing@cyberdefensemagazine.com

Free Monthly Cyber Warnings Via Email

Enjoy our monthly electronic editions of our Magazines for FREE.

This magazine is by and for ethical information security professionals with a twist on innovative consumer products and privacy issues on top of best practices for IT security and Regulatory Compliance. Our mission is to share cutting edge knowledge, real world stories and independent lab reviews on the best ideas, products and services in the information technology industry. Our monthly Cyber Warnings e-Magazines will also keep you up to speed on what's happening in the cyber crime and cyber warfare arena plus we'll inform you as next generation and innovative technology vendors have news worthy of sharing with you – so enjoy.

You get all of this for FREE, always, for our electronic editions.

Click here to signup today and within moments, you'll receive your first email from us with an archive of our newsletters along with this month's newsletter.

By signing up, you'll always be in the loop with CDM.

CDM

CYBER DEFENSE MAGAZINE™

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Cyber Warnings E-Magazine December 2013

Sample Sponsors:

To learn more about us, visit us online at http://www.cyberdefensemagazine.com/

Cyber Warnings Newsflash for December 2013

Highlights of CYBER CRIME and CYBER WARFARE Global News Clippings

Get ready to read on and click the titles below to read the full stories – this has been one of the busiest months in Cyber Crime and Cyber Warfare that we've tracked so far. Even though these titles are in **BLACK**, they are active hyperlinks to the stories, so find those of interest to you and read on through your favorite web browser…

The NSA Intercepts Laptops Purchased Online to Install Malware

12/29/2013 14:47 (Yahoo! News)

The NSA Intercepts Laptops Purchased Online to Install **Malware** According to a new report from Der Spiegel on the National Security Agency's top...

Mobile gadgets security called biggest challenge for business: Report [Asian News International]

12/29/2013 06:17 (Technology News)

...said the mobile endpoints used in their organizations had been hit by **malware**. Some 40 percent also said these endpoints were the entry point...

The Color of Money: Take action after Target breach

12/29/2013 05:34 (The Columbus Dispatch)

...a fraud victim. So if you shopped at Target during the period its **system** was **compromised**, you need to take steps to protect yourself. If you...

BBB warns job seekers of LinkedIn scams

12/28/2013 08:20 (Daily Journal Online)

...that information to steal your identity, access bank accounts or install **malware** on your computer. "Legitimate recruiters will never ask you for...

Cyber spying? China points finger at US

12/28/2013 06:00 (The Hill - Blog)

Rep. Dutch Ruppersberger (Md.), which would allow the federal **government** to share classified information to help private U.S. companies protect...

Shane Harris: Electric grid open to attack

12/28/2013 00:34 (MontereyHerald.com)

...facilities these days, the first thing that comes to mind is probably a computer **hacker** trying to shut off the lights in a city with **malware**. When U.S.

Target Confirms Encrypted PINs Stolen

12/27/2013 17:00 (GovInfoSecurity)

...during this incident," Target states. On Dec. 23, Target confirmed **malware** was to blame for an infection of its point-of-sale system that likely...

Australia : Bitcoin-mining Malware is rising in APAC region [TendersInfo (India)]

12/27/2013 15:45 (Technology News)

Australia : Bitcoin-mining **Malware** is rising in APAC region [TendersInfo (India)] (TendersInfo (India) Via Acquire Media NewsEdge) Bitcoin has...

Cyber security to become a major concern for 2014

12/27/2013 15:16 (Thestar.com)

New Pentagon blueprint sees bigger role for robot warfare

12/27/2013 12:41 (Yahoo! News)

...used robots to dismantle roadside bombs in America s wars, and the **DOD** is developing pack robots like BigDog designed by Boston Dynamics, a firm...

Heads-Up: Your Malware Protection Could Be Out-Dated And Ineffective

12/27/2013 12:06 (Forbes)

Heads-Up: Your **Malware** Protection Could Be Out-Dated And Ineffective It s pretty much tradition now for me. It s pretty much tradition now for...

NSA Scandal May Help Build Cyber-Barriers

12/27/2013 09:03 (Bloomberg)

in order to do so, it hopes to free itself from the German **government** s 32 percent ownership in the company. It has also expressed a desire to...

Bank robberies decrease as criminals switch to cyber-crime

12/26/2013 19:54 (Technology News)

...cyber-criminals, officials warn. "Instead of guns and masks, they used laptops and **malware**," says Loretta E. Lynch, U.S. attorney for the Eastern District...

Samsung Galaxy S4 Vulnerable to Malware

12/26/2013 15:57 (CIO Today)

Samsung Galaxy S4 Vulnerable to **Malware** A Ph.D student in Israel says adding an innocuous app to the non-secure area of Samsung's Knox architecture...

Cyber Scam Predictions for 2014

12/27/2013 07:33 (AARP Blog)

...app promising more Likes for users Instagram postings. More mobile **malware**. Cybercrooks used to focus their attacks mainly on desktop computers.

Your Facebook account worth more than your credit card

12/27/2013 03:55 (News 4 San Antonio)

...it was worth anything," Robertson says. According to an international **cyber security** firm, there's a black market where social media pages are...

Security breach brings suits

12/27/2013 03:00 (The Journal Gazette)

...chain, faces almost two dozen lawsuits filed by customers after a **computer security** breach exposed data on 40 million debit and credit cards.

How to be a hacker

12/27/2013 02:55 (The Guardian)

...enough: keep your computer up to date try not to fall prey to **phishing** attempts and don t run programmes from untrusted sources When it comes to drive-by...

Camp Shelby looks to future in cyberspace, drones

12/27/2013 02:17 (Mississippi Business Journal)

...getting under way that will bring together the Army, Navy, **Air Force** and Department of Homeland Security to figure out the most efficient use...

Analog security in a digital age

12/27/2013 00:06 (PilotOnline.com)

Analog **security** in a **digital** age We use plastic to pay for everything from packs of gum to parking meters to big screen televisions. We use plastic...

Metadata Not Anonymous at All, Stanford Researchers Show

12/26/2013 21:39 (Yahoo! News)

...Google+. Follow us @tomsguide, on Facebook and on Google+. 7 **Computer**-**Security** Fixes to Make Right Now How to Protect Yourself from Data Breaches 2014...

Costco Customers Targeted In Phishing Scam

12/26/2013 20:08 (KOLO)

Costco Customers Targeted In **Phishing** Scam Marianne Bartley is used to seeing on line scams. Marianne Bartley is used to seeing on line scams.

Hole found in Samsung's Knox security feature

12/26/2013 15:56 (SiliconBeat)

...left untouched, said Mordechai Guri, a Ph.D. student in the **Cyber Security** Labs at Israel s Ben-Gurion University of the Negev, who discovered...

Windows XP End of Life is only 4 months away! What does that mean for those still running it on their computers?

12/26/2013 15:04 (West Cobb Patch)

...most times does have vulnerabilities in it that can allow hackers, **malware** and such to gain access to the information on our computers and even...

US Sen. Menendez wants Federal Trade Commission to hold companies accountable for hacks

12/26/2013 14:13 (Pendleton Times-Post)

...States Congress (1246) United States government (2738) Subjects: **Computer** and data **security** (15) Consumer protection and advocacy (21) Consumer...

How have surveillance practices impacted cyber security agenda, private sector?

12/26/2013 13:26 (NewsNetNebraska)

How have surveillance practices impacted **cyber security** agenda, private sector? To review what we've learned about the National Security Agency's...

Christmas Warning: Kaspersky Lab Finds Gamers Attacked 11.7 Million Times In 2013 [Mid-East.Info]

12/26/2013 05:55 (Technology News)

...2013. Currently Kaspersky Lab knows 4.6 million pieces of gaming focused **malware**, with the total number of attacks facing gamers hitting 11.7 million...

Cyber attack on Target puts spotlight on card security

12/26/2013 04:30 (The Killeen Daily Herald)

Cyber attack on Target puts spotlight on card **security** The **cyber** thieves who broke into the computer systems of giant merchant Target Corp. timed...

What can we expect next year?

12/26/2013 03:44 (Help Net Security)

...research team, the list includes expected advances in ransomware, **hacking** of IoT (Internet of Things) devices, **critical infrastructure** exploits...

The latest on the Target credit card hack

12/25/2013 20:43 (MyFOX8.com)

...two weeks to Dec. 15. Here s what we know: The breach: **Malware** on store point-of-sale systems was involved in the security breach. The company...

Target Denies That Customer PIN Data Stolen During Huge Security Breach

12/25/2013 14:38 (Yahoo! News)

...of the theft is still under investigation, some experts say **malware** infected the swipe machines at store registers and likely traveled into Target's...

Why small businesses must tackle cybersecurity

12/25/2013 12:34 (Daily Record (AP))

...Communications Commission (FCC) created a tailored small business **Cyber Security** Planning guide that allows a user to customize the security...

Experts to discuss digital security issues [TradeArabia]

12/25/2013 10:25 (Technology News)

Experts to discuss **digital security** issues [TradeArabia] (TradeArabia Via Acquire Media NewsEdge) Leading global experts will be in Doha for...

Slovenian hacker gets jail for writing malware behind global botnet

12/24/2013 15:57 (Technology News)

Slovenian hacker gets jail for writing **malware** behind global botnet (UPI Science News Via Acquire Media NewsEdge) A Slovenian hacker accused...

40% of the Android users use no security on their devices [Mid-East.Info]

12/24/2013 04:40 (Technology News)

...been the most popular platform for ordinary users and the cybercriminals who use **malware** to steal from them. Only 58% of smartphone and 57% of...

Cyber criminals offer malware for Nginx, Apache Web servers

12/24/2013 04:18 (Computerworld)

Cyber criminals offer **malware** for Nginx, Apache Web servers Effusion **malware** available on cybercrime forums can infect Web servers and inject...

Sophisticated and targeted attacks on the horizon

12/24/2013 01:17 (Help Net Security)

...undermine two-factor authentication based on SMS. A move towards TOR used in **malware** With the continued use of TOR (The Onion Router), we will see...

Target: Breach Caused by Malware - BankInfoSecurity

12/23/2013 20:30 (Bankinfosecurity)

Target: Breach Caused by **Malware** - BankInfoSecurity Retailer Confirms Attack **Infected** POS **System** Target CEO Gregg Steinhafel Target Corp. has...

New York Scam Alert: Last Minute Gift Dash? Scam Artists are Banking on it

12/23/2013 18:44 (Yahoo! News)

...information, passwords and other sensitive data when you click on links infected with **malware**. Also, beware of what's known as cybersquatting, where crooks...

WebRTC Represents A New Era For Video Calls

12/23/2013 15:45 (Forbes)

...consider are security, to make sure WebRTC communications don t give **hackers** a **backdoor** into others systems, as well as ensuring the bandwidth...

Target hackers try new ways to use stolen card data

12/23/2013 15:41 (ComputerworldUK.com)

...wireless network can be exploited to gain access to a payment **network**. Massive data **compromises** at Heartland Payment Systems and Hannaford Brothers...

Target's Hacking Mess Nearly Ruining Christmas

12/23/2013 15:32 (Yahoo! News)

...cards over the first three weeks of the holiday season. Using **malware** to lift shoppers' personal information through the company's network of...

Pentagon’s cyber arm poised to expand role

12/23/2013 15:30 (Politico)

Pentagon s **cyber** arm poised to expand role The U.S. military s **Cyber** Command is about to receive the digital equivalent of faster ships and stronger...

Our nation's growing cyber crisis

12/23/2013 15:00 (The Hill - Blog)

...credit card fraud, Trojans, zero-day attacks, worms, viruses, **malware**, and an assortment of other online threats. Such a growing list of unseen...

Is DHS growing into cyber mission?

12/23/2013 13:08 (Federal Times)

Is DHS growing into **cyber** mission? From the beginning of the Homeland Security Department, there has been vigorous debate about its cybersecurity...

Could a $150,000 enforced bug bounty put zero-day exploit brokers out of business?

12/23/2013 12:40 (Computerworld Blogs)

...by exploit vendors to governments and are also available in the **cybercrime** underground. A half dozen exploit brokers have the capacity to offer...

After Takeover, Botnet Abandoned

12/23/2013 10:43 (Isssource.com)

...their investigation. Those who fear their computers have ZeroAccess **malware** should review the instructions provided by Microsoft on how to clean...

The top 10 tech stories of 2013

12/23/2013 09:48 (IT Manager Daily)

...top 10 in our year in review. 10. 3 ways **malware** is bypassing companies antivirus software Most companies are using antivirus software, firewalls...

Lessons learned in password security 2013

12/23/2013 03:15 (Help Net Security)

...accounts on those sites were compromised. And the most likely culprit is **malware** on a victim s system. By using two-factor authentication, sites...

WatchGuard Technologies Releases Top 8 Security Predictions for 2014 [Professional Services Close - Up]

12/23/2013 02:24 (Technology News)

...research team, the list includes expected advances in ransomware, **hacking** of IoT (Internet of Things) devices, **critical infrastructure** exploits...

The Year Ahead In Cyber Security: What You Need To Know

12/22/2013 10:00 (Forbes)

The Year Ahead In **Cyber Security**: What You Need To Know 2013 was a watershed year for **cyber security** and digital secret-keeping. 2013 was a watershed...

Taylor Made Issue Seasonal Malware Warnings and Recommend Online Backup

12/22/2013 03:33 (Technology News)

Taylor Made Issue Seasonal **Malware** Warnings and Recommend Online Backup (PR Web Via Acquire Media NewsEdge) (PRWEB UK) 22 December 2013 The Christmas...

BBB Tip of the Week: Holiday scams, frauds

12/22/2013 03:00 (The Spokesman-Review)

...Business Bureau is warning about these common holiday scams and frauds: **Malware** e-cards: Viruses and **malware** often travel in email attachments...

'Internet Privacy' Set to be Key IT Security Topic of 2014 Reveals ESET 'Trends for 2014' Report [Mid-East.Info]

12/22/2013 02:50 (Technology News)

...of the NSA revelations, cybercrime particularly relating to increasing **malware** on the Android mobile platform and the emergence of threats on...

eWave: Hackers ride the Internet for illicit gains

12/21/2013 22:15 (The Providence Journal (AP))

...click. And that, he said, may clandestinely introduce malicious software **malware** into the company s computer network. Now the perpetrator is in.

Target offers 10% discount after credit card hack

12/21/2013 16:16 (KAIT ABC-8)

...retailer's point-of-sale system. That means they either slipped **malware** into the terminals where customers swipe their credit cards, or they collected...

Why Target Customers Shouldn't Panic After Data Breach

12/20/2013 17:30 (Forbes)

...that the criminals were able to steal this information by installing **malware** into a company machine, or persuaded an unsuspecting employee to...

Webcams Can Watch Without User Knowing

12/20/2013 17:25 (Isssource.com)

...that runs on the iSight, enables a virtual machine escape whereby **malware** running inside a virtual machine reprograms the camera to act as a...

Pulling RSA Keys by Listening

12/20/2013 17:03 (Isssource.com)

...sound generated by computers. That comes on top of a **malware** prototype introduced earlier this month that uses inaudible audio signals to communicate...

Colorado casinos affected by data breach

12/20/2013 16:19 (9News.com)

...and debit card information. Affinity Gaming said Friday that its **system** was **infected** with **malware** that compromised card data from customers at...

Fake Adobe "licence key delivery" emails carry malware

12/20/2013 05:19 (Help Net Security)

Fake Adobe "licence key delivery" emails carry **malware** A clever **malware** distribution campaign is currently hitting inboxes, taking the form of...

Whitepaper: The modern malware review

12/20/2013 03:13 (Help Net Security)

Whitepaper: The modern **malware** review This review provides the first analysis of **malware** behavior that include not only analysis of how **malware**...

Information security and compliance trends for the new year

12/20/2013 02:44 (Help Net Security)

updates and system changes. 4. There will be a significant increase in **malware** for Android phones, and **malware** will begin to affect iPhones, too.

Better Business Bureau Offers Suggestions to Target Customers Following Data Breach

12/20/2013 01:33 (Technology News)

...ask you to click on a link or open an attachment, which can download **malware** designed to steal your identity. * Don't click on any email links...

'Businesses need to tighten cyber security' [Arab News (Saudi Arabia)]

12/20/2013 01:28 (Technology News)

Sullivan, who is here to address 200 various Saudi companies and **government** agencies on the gravity and rapid increase of cyber attacks and the...

Older Mac webcams can spy without activating warning light, researchers find

12/19/2013 21:54 (Computerworld Malaysia)

...indicates when they're active, but it's possible for **malware** to disable this important privacy feature on older Mac computers, according to research...

Target data theft fuels new worries on cybersecurity

12/19/2013 21:13 (Los Angeles Times)

...database, security experts said. Another theory is that they sent **malware**-laden email to Target employees that spread through the retailer's...

Computer Sounds Give Up Secret Information

12/19/2013 20:09 (Yahoo! News)

...is not directly related to a possible newly discovered piece of **malware** that may send messages among infected machines using high-pitched sound.

DDoS Botnet via Poland

12/19/2013 18:00 (Isssource.com)

...CERT Poland. What s interesting about it is the attackers developed **malware** to infect Windows and Linux machines. The botnet is only for DDoS...

Breach could prove very costly for Target

12/19/2013 14:11 (ComputerworldUK.com)

...either hackers penetrated company's Point of Sale (POS) network or **malware** was somehow inserted into card swipe devices used by customers. "It is...

Unique malware evades sandboxes

12/19/2013 12:45 (Computerworld Malaysia)

Unique **malware** evades sandboxes **Malware** used in attack on PHP last month dubbed DGA.Changer, **Malware** utilized in the attack last month on the...

The rise of hobbyist programmers

12/19/2013 11:02 (Computerworld)

...could turn their talents to nefarious activities, such as writing **malware**, or leave the countries altogether for work opportunities. By Joab...

iSeeYou: Apple webcam bug allows creepy peeps to peep in on you

12/19/2013 06:06 (Computerworld Blogs)

...your night. Apple (NASDAQ:AAPL) webcams are vulnerable to silent **malware** attack. It's long been believed that nobody can turn on your iSight...

ISACA Recommends Five Resolutions to Prepare IT Professionals for 2014 Trends

12/19/2013 04:38 (Technology News)

...some elements of IT security operational responsibility (including **malware** detection, event analysis and control operation) increasingly being...

Five resolutions to help IT pros get ready for 2014

12/19/2013 02:45 (Help Net Security)

...some elements of IT security operational responsibility (including **malware** detection, event analysis and control operation) increasingly being...

Commentary: If 'password' is your password, you're toast

12/19/2013 02:21 (The Daily Record)

Of course, password vigilance will not save you from a malevolent **keylogger**, the keystroke-tracking program that enabled the recent thefts. But...

Surveillance review board recommends U.S. shift to cyber defense

12/19/2013 00:52 (Yahoo! News)

...in encryption systems that "guard global commerce." Instead, the **government** should work to promote strong encryption, and its use "should be...

Criminal gangs offer large scale Malware-as-a-Service: Websense

12/18/2013 22:08 (Computer World Singapore)

Criminal gangs offer large scale **Malware**-as-a-Service: Websense The arrest of masterhacker 'Paunch' has led to cybercriminals to revert to less...

Cybercrims will use ransomware to target businesses: McAfee

12/18/2013 22:01 (Computerworld Malaysia)

...target businesses: McAfee Cybercriminals will increasingly use ransomware, **malware** and hacktivism over the next year to move further into the...

New DDoS malware targets Linux and Windows systems

12/18/2013 21:56 (Computerworld Malaysia)

New DDoS **malware** targets Linux and Windows systems Attackers are compromising Linux and Windows systems to install a new **malware** program designed...

2014 is the tipping point year of mobile malware: RSA chief Art Coviello

12/18/2013 21:40 (Computerworld Malaysia)

2014 is the tipping point year of mobile **malware**: RSA chief Art Coviello Says the next hacking target is not mobile, but the Internet of Things.

Microsoft's cybercrime unit files 1st case

12/18/2013 15:48 (The Register-Guard)

...bring together different units that work on fighting everything from **malware** to intellectual-property theft. When Microsoft opened its sleek...

5 Things You Probably Didn't Know About Identity Theft

12/18/2013 15:11 (Yahoo! Canada Finance)

Mozilla Blocks Botnet Add-on

12/18/2013 14:55 (Isssource.com)

...downloading and using the rogue add-on. It s possible the **malware** came bundled with other downloaded software, or users ended up tricked into...

Attackers Exploit ColdFusion Bug

12/18/2013 14:25 (Isssource.com)

...vulnerability in Adobe s ColdFusion, attackers are installing data stealing **malware** in Microsoft s Internet Information Services (IIS) Web server...

Death by 1,000 Security Alerts?

12/18/2013 14:13 (National Mortgage News Blogs)

Death by 1,000 Security Alerts? WE RE HEARING as **malware** and virus detection gets more advanced, financial firms may find their IT departments...

11 Tips for Keeping Your Mobile Phone Secure

12/18/2013 13:18 (Yahoo! News)

...how to stay safe, mobile crime is on the rise - with **malware** or malicious software increasing by 58 percent this year. **Malware** can steal personal...

Perspective: Throw Windows XP a lifeline, Microsoft

12/18/2013 10:02 (Computerworld)

...year. Absent security updates, Windows XP will be substantially more vulnerable to **malware** attacks, perhaps -- if Microsoft's own estimate is on...

What's the greatest security risk?

12/18/2013 03:02 (Help Net Security)

Additionally, 68 percent say their mobile devices have been targeted by **malware** in the last 12 months, yet 46 percent of respondents say they...

Battelle helps bank in fighting cybercrime

12/18/2013 02:27 (The Columbus Dispatch)

Battelle helps bank in fighting **cybercrime** Banks increasingly have been the targets of criminals whose faces don t show up on security cameras.

Counterfeit tech gifts come with dangers

12/18/2013 02:22 (The Columbus Dispatch)

...from a reputable app store. But even in those locations, some hidden **malware** programs intended to do harm can sneak in. In such cases, a common...

Drugmakers urge FDA security audit after cyber breach

12/18/2013 01:07 (Yahoo! News)

which was published in pharmaceutical trade publications, referred to the **compromised system** as an "online submission system" at the Center for...

Advanced persistent threats now hitting mobile devices

12/17/2013 21:32 (Computer World Singapore)

Smartphones, tablets and other mobile devices have become the target of **malware** and are even getting hit by highly targeted attacks known as "advanced...

Android botnet stole SMSes from South Korea, emailed them to China

12/17/2013 21:30 (Computer World Singapore)

...messages may be one of the largest and most advanced mobile **malware** operations discovered, according to security vendor FireEye. An Android botnet...

Mobile Botnet a Busy Application

12/17/2013 18:21 (Isssource.com)

...has been in at least 64 spyware campaigns, researchers said. The MisoSMS **malware** (Android.Spyware.MisoSMS) that powers the botnet is able to...

Bad VPN Website Issues Malware

12/17/2013 18:06 (Isssource.com)

Bad VPN Website Issues **Malware** Virtual Private Networks (VPNs) can protect data, and more and more people want to use the service to ensure a...

Practical SCADA Security

12/17/2013 17:50 (Isssource.com)

...systems the biggest challenge. 4. Protect the manufacturing systems from **malware** attacks from PCs by: a. Removing PCs from the manufacturing...

AIG Says Companies 'Massively Under-Insured' Against Cyber Risk

12/17/2013 15:45 (Washington Post - Bloomberg)

...carried out by the Syrian Electronic Army, a group that supports the **government** of President Bashar al-Assad. Businesses contend with a variety of...

IE flaw targeted in Aurora attacks still actively exploited

12/17/2013 12:37 (Help Net Security)

...the best things you can do to keep your computer safe against **malware** infection. Regular software patching is often touted as one of the best...

How effective are Android AV solutions?

12/17/2013 10:49 (Help Net Security)

...effective are Android AV solutions? As the onslaught of Android **malware** continues, the recently released testing results by independent IT-security...

Prison Time for Hacker

12/17/2013 10:46 (Isssource.com)

...Computerworld. Miller, previously convicted in 2004 of involvement in writing **malware**, pled guilty to conspiracy and computer fraud on August 26,

Patched Hole could be a Perfect Cyber Crime

12/17/2013 09:44 (Isssource.com)

...be the perfect cyber crime. The attack doesn t involve any **malware** payload security professionals can reverse engineer, no file hash to trace,

Mozilla blocks rogue add-on that made computers scan sites for flaws

12/17/2013 08:53 (Help Net Security)

...use the rogue add-on. It's possible that the **malware** came bundled with other downloaded software, or that users were tricked into downloading...

Report: FEC system hacked during shutdown

12/17/2013 08:16 (The Hill - Blog)

...an independent audit last year that warned of a **vulnerable** information technology **system**. Without adopting and implementing National Institute...

How human behaviour affects malware and defense measures

12/17/2013 05:25 (Help Net Security)

How human behaviour affects **malware** and defense measures Installing computer security software, updating applications regularly and making sure...

Attackers exploited ColdFusion vulnerability to install Microsoft IIS malware

12/17/2013 03:55 (ComputerworldUK.com)

Attackers exploited ColdFusion vulnerability to install Microsoft IIS **malware** The **malware** works as an IIS module and can capture data entered...

Boot up: Firefox botnet, Mavericks.1, Nokia dumps Android, and more

12/17/2013 02:56 (Technology News)

...clear yet how the initial infection is being spread, but the **malware** enslaves PCs in a botnet that conducts SQL injection attacks on virtually...

Cybercriminals clone pirate versions of top Android and iOS apps

12/16/2013 21:43 (Computerworld Malaysia)

...unprotected apps are vulnerable to tampering: either through installed **malware** or through decompiling and reverse engineering - enabling hackers to...

Savvy computer users pose security risk: study

12/16/2013 20:01 (Montreal Gazette)

Tool to Register Tumblr Accounts

12/16/2013 18:23 (Isssource.com)

...to redirect victims to a fake Facebook login page, and ultimately to a **malware**-serving website. Next to its multi-threaded nature, the tool basically...

Lockheed sees strong cyber demand despite NSA scandal -CEO

12/16/2013 17:28 (Reuters US News)

Lockheed sees strong **cyber** demand despite NSA scandal -CEO WASHINGTON Dec 16 (Reuters) - **Lockheed Martin** Corp, the Pentagon's No. 1 supplier...

Imitation Ransomware Discovered

12/16/2013 16:50 (Isssource.com)

...by receiving and opening executables disguised as mp3 files. Once the **malware** is on the target computer, it proceeds to encrypt files one by...

DHS cyber effort shifts to insider threats

12/16/2013 16:15 (Federal Times)

...Washington. DHS has yet to release details to industry about what the **government** will buy during phase two of the continuous monitoring program. But Streufert...

Resurgence of malware signed with stolen certificates

12/16/2013 13:20 (Help Net Security)

Resurgence of **malware** signed with stolen certificates Since 2009, variants of the Winwebsec rogue AV family have been trying to trick users into...

Listen Here: Malware Can Be Transmitted Through Audio

12/16/2013 12:38 (Reviewed.com)

Listen Here: **Malware** Can Be Transmitted Through Audio Researchers have shown how computers can be hacked even without being connected to a network.

Addressing advanced malware in 2014

12/16/2013 11:21 (Enterprise Strategy Group Blogs)

Addressing advanced **malware** in 2014 Endpoint security, security analytics, and process automation top the to-do list In the cybersecurity annals...

Hackers may be invading your privacy more than you think

12/16/2013 10:12 (KDBC)

Shady Android AV pushed onto unsuspecting users

12/16/2013 09:55 (Help Net Security)

...which ones, but says that they aren t ones they would expect to see **malware** on - and the warning is clear: an Android virus has been detected.

WhatsApp-themed spam campaign delivers malware

12/16/2013 08:54 (Help Net Security)

WhatsApp-themed spam campaign delivers **malware** A new WhatsApp-themed spam campaign has been spotted targeting users of the popular IM service.

Bogus antivirus program uses a dozen stolen signing certificates

12/16/2013 06:04 (Computerworld Malaysia)

...samples of Antivirus Security Pro using it, indicating "that the **malware**'s distributors are regularly stealing new certificates, rather than using...

Gamers attacked 11.7 million times in 2013

12/16/2013 04:49 (Help Net Security)

...2013. Currently Kaspersky Lab knows 4.6 million pieces of gaming focused **malware**, with the total number of attacks facing gamers hitting 11.7 million...

Week in review: Cryptolocker copycat, CyanogenMod's built-in SMS encryption, NSA uses Google cookies to track suspects

12/16/2013 00:31 (Help Net Security)

...layered defense in-depth versus single defender. FBI used spying **malware** to track down terror suspect Court documents related to a recent FBI...

Online behaviors that increase the risk of identity theft

12/16/2013 00:31 (Help Net Security)

Watch out for malware on Android

12/16/2013 00:01 (The Buffalo News)

Watch out for **malware** on Android Do you need to run antivirus software on a smartphone? Do you need to run antivirus software on a smartphone?

Hackers like Playstation 4 and Xbox One too

12/15/2013 21:33 (ConsumerAffairs.com)

...it currently known of about 4.6 million pieces of gaming focused **malware** that are directed against the game systems. It's measure of European...

Marketers excited about Gmail image display changes

12/15/2013 21:22 (Computerworld Malaysia)

...announced Thursday. This allows Google to check the images for viruses and **malware** before an image is showed in Gmail. This extra step means that...

BLOG: Strong opportunities and some challenges for big data security analytics in 2014

12/15/2013 21:15 (Computer World Singapore)

...response. Existing monolithic security analytics tools are no match for advanced **malware**, stealthy attack techniques, and the growing army of well-organized...

Some Foreign Nations Have Cyberwar Capability To Destroy Our Financial System, NSA Admits

12/15/2013 21:00 (Forbes)

...hear, Plunkett basically made it appear that the nation s cyber-defense **system** was very **vulnerable**, which should send the fear of God into Wall Street,

Bitcoin market price app, 'Bitcoin Alarm,' is carefully cloaked malware

12/15/2013 11:52 (Computer World Singapore)

Bitcoin market price app, 'Bitcoin Alarm,' is carefully cloaked **malware** If you get a spam message advertising an application called "Bitcoin Alarm,"

3 Steps To Protect Yourself From Malicious QR Codes

12/15/2013 10:33 (QR Code Press)

...options, app download authentication, and, of course, QR **malware** protection for your mobile device. You can prevent identity theft with other...

Humans Now Account for Less Than 40% of Web Traffic

12/14/2013 20:45 (Yahoo! News)

...of top-tier hackers who are proficient enough to create their own **malware** has risen, though. These impersonators are usually custom-made for...

Zeus banking malware resurfaces in 64-bit version

12/14/2013 11:32 (TechHive)

Zeus banking **malware** resurfaces in 64-bit version A 64-bit version of the notorious Zeus family of banking **malware** has been found, an indication...

Water and wastewater industry cyberattacks increasing [InTech]

12/14/2013 11:17 (Technology News)

...decade, but has come under increased scrutiny following the discovery of the **Stuxnet** virus in 2010, the Duqu virus in 2011, and the Shamoon virus...

5 Holiday Cyberscams to Watch Out For

12/14/2013 08:49 (Yahoo! News Canada)

'Locker' malware demands ransom to restore infected files [Asian News International]

12/14/2013 00:49 (Technology News)

'Locker' **malware** demands ransom to restore infected files [Asian News International] (Asian News International Via Acquire Media NewsEdge) London,

Booz Allen Finds that Cyber Attacks Are the 'New Normal' for Financial Services Industry [Manufacturing Close - Up]

12/13/2013 20:55 (Technology News)

...Trojan - a crimeware kit -- and other cross- platform **malware** have identified large gaps in mobile device security. These threats take advantage...

Mobile Advertising SDK Brings Attacks

12/13/2013 17:35 (Isssource.com)

...the Android marketplace. One of the issues behind Widdit is the **malware** requests a large number of permissions. The SDK integrated into Android...

What Is Digital Forensics?

12/13/2013 13:33 (U Publish Articles)

Kaspersky Lab detects 315,000 new malicious files every day

12/13/2013 05:35 (Technology News)

...the main target, attracting a massive 98.05 per cent of known **malware**. Christian Funk, Senior Virus Analyst at Kaspersky Lab, comments, 'There...

Top 100 Android apps hacked in 2013

12/13/2013 05:17 (Help Net Security)

...apps are vulnerable to tampering: either through installed **malware** or through decompiling and reverse engineering enabling hackers to analyze...

Top security trend predictions for 2014

12/13/2013 02:44 (Help Net Security)

...out-of-sight and out-of-mind. Every day, **critical infrastructure** and organization entities face state-sponsored cyber attacks. Far less common is...

Guest View: Cybersecurity in 2014

12/12/2013 22:57 (Computer World Singapore)

...begun to target mobile devices, which are ripe targets for new **malware** and a logical place for new threat vectors. We have witnessed attacks...

Microsoft bets on Windows XP disaster

12/12/2013 21:54 (Computer World Singapore)

...eight-item prognostication from several security professionals on its anti-**malware** and Trustworthy Computing teams, Microsoft forecast an increase in...

Hacker sentenced to 18 months for peddling computer access to US national security lab

12/12/2013 21:43 (Computerworld Malaysia)

including targeting specific authorized network users and infecting their computers with **malware**, which allowed him to steal their log-in information.

Banks shouldn't rely on mobile SMS passcodes, security firm says

12/12/2013 21:31 (Computerworld Malaysia)

...a person's login credentials. But there are now multiple mobile **malware** suites that work in tandem with desktop **malware** to defeat one-time passcodes,

Malware at Record Levels in '13

12/12/2013 19:04 (Isssource.com)

Malware at Record Levels in 13 Almost 10 million new **malware** strains have hit the world so far this year, researchers said. Almost 10 million...

16.6 Million People Experienced Identity Theft In 2012

12/12/2013 17:25 (Dallas Morning News - Mediawebsite.net)

AutoCAD Malware Lurking

12/12/2013 17:02 (Isssource.com)

AutoCAD **Malware** Lurking There is a piece of **malware** out there masquerading as an AutoCAD component with the goal of making systems vulnerable...

Despite Arrest, RAT Usage Grows

12/12/2013 16:57 (Isssource.com)

Attackers use Cool to distribute W32.Shadesrat and other pieces of **malware**. This happened until recently when Russian police said they arrested the...

"Mission Accomplished" on identity theft? Not so fast.

12/12/2013 10:00 (The Hill - Blog)

64-bit Zeus Trojan version found and analyzed

12/12/2013 07:28 (Help Net Security)

Kaspersky Lab researchers have shared. The 64-bit agent is contained in the **malware**'s 32-bit version, and has been since June 2013 at least,

Yes, e-receipts can be convenient – but don't let them compromise your personal info

12/12/2013 03:37 (FortWayne.com)

...emails requesting your personal information; they could be scams that download **malware** on your computer. Ask if you can opt-out of receiving...

Zeus malware gets 64-bit makeover

12/12/2013 03:25 (ComputerworldUK.com)

Zeus **malware** gets 64-bit makeover Kaspersky Lab finds new version of infamous banking **malware** making the rounds A 64-bit version of the notorious...

Young professionals exposing workplaces to cyber attack

12/12/2013 02:52 (Help Net Security)

...they have connected, their own devices, potentially infected with malicious **malware**, to their company s network. Forty-seven percent also use...

How cyber squatters and phishers target antivirus vendors

12/12/2013 02:52 (Help Net Security)

...pornographic or underground pharmaceutical websites, or even to infect with **malware** user machines who accidentally made a typo in the URL or...

BLOG: CyberArk makes 10 security predictions for 2014

12/12/2013 01:32 (Computer World Singapore)

...powers of rogue nations and state-sponsored terrorist groups. As with **Stuxnet**, these attacks are dismantled and re-purposed - the attacks become...

Growth of BYOD Calls for Stronger Network Security

12/12/2013 00:43 (Hospitality Technology)

...information. Older firewalls cannot adequately protect an organization from the **malware** and viruses that criminals inflict today and even the most sophisticated...

Security tactics might have helped in foreign ministry hacks

12/11/2013 21:54 (Computerworld Malaysia)

...attackers. The campaign, named Ke3chang after a reference found in the **malware** code, demonstrates that the probability of an attacker breaking into a...

Outlook 2014 II: Bad Guys Getting Better

12/11/2013 17:18 (Isssource.com)

...threat report highlights new security concerns ranging from stealthy **malware** tools that offer dynamic camouflage and provide attackers with long-term...

Malware can Make Phone Calls

12/11/2013 16:46 (Isssource.com)

Malware can Make Phone Calls Mobile devices continue to be the low hanging fruit for attackers as a new version of **malware** is now able to make...

Data Stealing Malware Almost Undetectable

12/11/2013 16:16 (Isssource.com)

Data Stealing **Malware** Almost Undetectable There is new **malware** out there that collects data entered into Web-based forms, pretending to be a...

United States : Kaspersky Lab Survey Finds Average Consumer Loses $418 in Media Files on Devices [TendersInfo (India)]

12/11/2013 15:08 (Technology News)

...lost, stolen or broken and 27 percent have encountered a **malware** incident. Protecting your valuable data Cybercriminals understand that consumers...

Outlook 2014: Mobile Attacks will Intensify

12/11/2013 14:26 (Isssource.com)

...predictions from IT security firm Trend Micro. The report focuses on mobile **malware**, targeted campaigns, attack vectors, data breaches, Java 6 and...

Imaging on mobile devices [Applied Radiology]

12/11/2013 14:13 (Technology News)

...concerns. Multiuser support, verification, device encryption, and **malware**-prevention improvements have to be made more robust inherently at the...

Patch Tuesday Fixes One Zero-Day, Leaves Another Open

12/11/2013 13:14 (CIO Today)

...not safe. Trustwave s SpiderLabs on Tuesday discovered a piece of **malware** that collects data, masking itself as a module for Microsoft s Internet...

Apple and Google app stores vulnerable to hacking, warns security company

12/11/2013 11:12 (The Guardian)

...September. But even Google's official Play store can be a source of **malware** and hacked apps. In September BlackBerry had to halt the rollout of its BBM...

Banks shouldn't rely on mobile SMS passcodes, security firm says

12/11/2013 10:37 (Computer World Australia)

...a person's login credentials. But there are now multiple mobile **malware** suites that work in tandem with desktop **malware** to defeat one-time passcodes,

RAT-wielding attacker compromises poker player's laptop

12/11/2013 09:50 (Help Net Security)

...high-profile Finnish poker player has been found to contain spying **malware** after the device was stolen from and then returned to his room in...

Smarter cyber crime forces industry to change

12/11/2013 03:44 (Help Net Security)

...threat report highlights new security concerns ranging from stealthy **malware** tools that offer dynamic camouflage and provide attackers with long-term...

Chinese hackers snooped on five EU ministries, says US security firm [Asian News International]

12/11/2013 02:22 (Technology News)

...(ANI): Chinese hackers reportedly snooped on five European foreign ministries with **malware**-infected emails over the summer, new research from US security...

Update vulnerability in third-party SDK exposes some Android apps to attacks

12/10/2013 21:25 (Computer World Singapore)

...the application's request as it travels over an insecure wireless **network** or a **compromised network** gateway and serve back a malicious JAR file,

Old was new again in security in 2013: Blue Coat

12/10/2013 21:04 (Computer World Singapore)

...sophisticated in 2014, particularly with the upsurge of ransomware, a type of **malware** holds a company's IT and corporate data hostage. Andresen has seen...

Firms Average 9 Targeted Attacks a Year

12/10/2013 19:34 (Isssource.com)

...report said. Cyberespionage actors are getting stealthier, encrypting their **malware** to evade detection, for example, said George Tubin, senior...

Botnet Steals 2 Million Logins

12/10/2013 19:03 (Isssource.com)

...and secure shell account details. It wasn t clear what kind of **malware** infected victims computers and sent the information to the command-and-control...

Smarter, shadier and stealthier cyber crime forces industry to dramatic change

12/10/2013 18:31 (Computer World Australia)

...threat report highlights new security concerns ranging from stealthy **malware** tools that offer dynamic camouflage and provide attackers with long-term...

EU Cyber Group Guide to Mitigate Attacks

12/10/2013 18:25 (Isssource.com)

...distribution, water treatment, transportation, as well as chemical, **government**, defense and food processes. Oftentimes, ICS are easy targets...

Ransomware Survives Takedown

12/10/2013 17:30 (Isssource.com)

...to take down command and control nodes associated with the CryptoLocker **malware** was unsuccessful. An attempt to take down command and control...

FDA Breach Raises Lawmakers' Hackles

12/10/2013 15:16 (GovInfoSecurity)

...the letter. "The security breach of FDA's gateway **system** not only **compromised** the security of personal identifiable information, but also compromised...

Data-stealing malware pretends to be Microsoft IIS server module

12/10/2013 12:14 (Computer World Singapore)

Data-stealing **malware** pretends to be Microsoft IIS server module Trustwave's SpiderLabs researchers have found a piece of **malware** that collects...

Visualizing the year's top cyber attacks

12/10/2013 11:59 (Help Net Security)

...discovered by Kaspersky Labs was responsible for targeting select enterprises. **Malware** was used to phone home to command and control servers and...

Microsoft Patch Tuesday reinforces the value of software upgrades

12/10/2013 05:49 (Computer World Australia)

addressed in MS13-098, allows attackers to add their own **malware** to software being installed on a computer over a network using the Authenticode...

Banks, regulators moving to thwart cyberattacks

12/09/2013 21:10 (USA Today)

...large-bank websites last year but much work remains. The **government** is sharing intelligence with financial institutions and the industry is spending...

Global Effort to Bring Botnet Down

12/09/2013 19:33 (Isssource.com)

...also seen use in hijacking compromised devices for Bitcoin mining. The **malware** is one of the most robust and durable botnets in operation. Its...

Website Tells You If Your Password's Been Leaked

12/09/2013 17:13 (Yahoo! News)

...appealing in order to trick you into clicking a bad link or downloading a **malware**-infested attachment. The data breaches at Adobe, Gawker, Yahoo,

Cybercrime ignorance is a serious risk

12/09/2013 05:56 (Help Net Security)

...Simon Bain, founder of Simplexo. A recent report from the UK **Government** and Home Office has revealed that the UK s top companies are not accounting...

13 Anonymous hackers plead guilty to PayPal DDoS attack

12/09/2013 03:59 (Help Net Security)

...in San Jose on Friday to charges related to their involvement in the **cyber**-**attack** of PayPal s website as part of the group Anonymous. Thirteen...

ENISA issues recommendations on SCADA patching

12/09/2013 03:52 (Help Net Security)

...issues recommendations on SCADA patching "How long can we afford having **critical infrastructures** that use unpatched SCADA systems?" "How long can...

Cloud Backup Safeguards Against Dangerous Ransomware

12/09/2013 03:42 (Technology News)

...experts at Taylor Made Computer Solutions (TMCS). The Cryptolocker **virus** is attacking **computer** systems globally. It infected 12,000 US computers...

Week in review: Air gap-hopping malware, first PoS botnet, and the new issue of (IN)SECURE Magazine

12/09/2013 00:18 (Help Net Security)

Week in review: Air gap-hopping **malware**, first PoS botnet, and the new issue of (IN)SECURE Magazine Here's an overview of some of last week's...

Natwest website targeted in DDOS cyber attack

12/08/2013 19:53 (Computer World Singapore)

Natwest website targeted in DDOS **cyber attack** Natwest has been targeted in a **cyber attack** which prevented customers from accessing its website.

HP, VMware, Google cashing in on end of support for Windows XP

12/08/2013 19:09 (Computer World Singapore)

...machines running the OS and how unpatched browser bugs are often used by **malware** to infect such PCs. Were extending support for Chrome on Windows XP,

JP Morgan suffers cyber attack, 465,000 card customer details stolen

12/08/2013 11:52 (Computerworld Malaysia)

...are used by US companies to pay employees, and by **government** agencies to pay benefits such as unemployment compensation. A bank spokesperson...

BBB Tip of the Week: Beware the digital hijacker

12/08/2013 03:02 (The Spokesman-Review)

a digital hijacker, is targeting businesses. Once installed, this **malware**, also called ransomware, encrypts files and networked volumes. Next,

Airlines fight cyberattacks

12/08/2013 01:59 (The Free Lance-Star)

...every other sector, said Paul Kurtz, chief strategy officer for **computer security** firm CyberPoint International. It s just a matter of time before...

Singapore banks told to boost security after StanChart data theft [Times of Oman]

12/08/2013 01:22 (Technology News)

...websites of Lee and President Tony Tan as well as pro-**government** media. Some of the attackers denounced new rules requiring news websites in...

Microsoft disrupts fake-click malware ZeroAccess

12/07/2013 14:47 (Alaska Dispatch)

Microsoft disrupts fake-click **malware** ZeroAccess Microsoft, the FBI, and the European CyberCrime Center (EC3) claim to have disrupted computer...

The state of targeted attacks

12/06/2013 05:31 (Help Net Security)

...threats 87% said company execs were not aware of APT threats 93% said **malware** was the source of an APT attack 68% said zero day attacks are their...

New ICS cyber security cert

12/06/2013 05:31 (Help Net Security)

New ICS **cyber security** cert Global Information Assurance Certification (GIAC), a leading provider of **cyber security** certifications and an affiliate...

Microsoft and law enforcement disrupt ZeroAccess botnet

12/06/2013 04:47 (Help Net Security)

...Intelligence Program (C-TIP). ZeroAccess is very sophisticated **malware**, blocking attempts to remove it, and Microsoft therefore recommends that...

Point-of-sale malware infections on the rise

12/06/2013 03:20 (ComputerworldUK.com)

Point-of-sale **malware** infections on the rise Researchers from Arbor Networks and IntelCrawler identify new attacks using **malware** designed for...

'ZeroAccess' click-fraud botnet disrupted, but not dead yet

12/06/2013 02:43 (ComputerworldUK.com)

...has published general instructions for how people can keep their computer free of **malware**. Send news tips and comments to jeremy_kirk@idg.com.

Microsoft leads disruption of largest infected global PC network

12/06/2013 01:37 (Yahoo! News)

Microsoft Corp said on Thursday it had disrupted the largest **network** of **compromised** personal computers, involving some 2 million machines around...

Passwords reset after 'Pony' botnet stole 2 million credentials

12/06/2013 00:47 (Computer World Singapore)

...passwords of 2,400 clients but did not believe its internal **network** was **compromised**. Facebook, LinkedIn and Twitter have also reset some user...

New Industrial Control Systems Cyber Security Certification Exam is Now Available

12/05/2013 18:14 (Yahoo! News)

New Industrial Control Systems **Cyber Security** Certification Exam is Now Available Global Information Assurance Certification Offers the Only...

News Summary: Venezuela in cyber crackdown

12/05/2013 18:07 (Yahoo! News)

...accuses the sites of fueling an "economic war" against his **government**. **Government** opponents say the controls are designed to obscure reporting of...

Recent Hack Discovery Underscores Need For Better Security And Stronger Passwords

12/05/2013 17:42 (Forbes)

...LinkedIn have been comprised. The security researchers found that a **keylogger** tool associated with the Pony botnet enabled thieves to harvest the...

Microsoft lines up critical Windows, Office and IE fixes for next week

12/05/2013 16:20 (ComputerworldUK.com)

...are not deployed, criminals may be able to infect PCs with **malware**, steal information, acquire additional privileges that would let them run...

Microsoft joins move to encrypt Web traffic

12/05/2013 14:42 (Yahoo! News)

...potentially now constitutes an 'advanced persistent threat,' alongside sophisticated **malware** and cyber attacks." Smith said Microsoft said decided to "take...

Cyber Attacks Up 15 Percent Since 2010, According to Emerson, Ponemon Institute Study

12/05/2013 13:24 (Technology News)

Cyber Attacks Up 15 Percent Since 2010, According to Emerson, Ponemon Institute Study COLUMBUS, Ohio --(Business Wire)-- With both **cyber** attacks...

JP Morgan suffers cyber attack, 465,000 card customer details stolen

12/05/2013 11:30 (ComputerworldUK.com)

...are used by US companies to pay employees, and by **government** agencies to pay benefits such as unemployment compensation. A bank spokesperson...

Researchers uncover Point-of-Sale botnet

12/05/2013 08:55 (Help Net Security)

...spotted an active Point of Sale (PoS) compromise campaign using the Dexter **malware** or variants of it, aimed at stealing credit and debit card data.

2 million stolen passwords for Facebook, Twitter, Google, Yahoo and others leaked online

12/05/2013 07:30 (WRCBtv.com)

...during its latest Internet sweep for the Pony botnet controller, a **malware**-spreading set of programs which the researchers say they're increasingly...

Browser hygiene tips for making online shopping safer

12/05/2013 04:47 (Help Net Security)

...their holiday shopping online may be more susceptible to falling into **malware** traps that attempt to steal credit card info or banking passwords.

Hackers steal 2 million Facebook, Google, Twitter, Yahoo passwords

12/05/2013 04:15 (Yahoo! News)

...number of computers. Facebook users have been the biggest victims of the **malware** so far, as an estimated 318,000 Facebook accounts have been...

BLOG: APT: The security attack everyone loves to hate

12/05/2013 01:35 (Computer World Singapore)

...world, and so has a tremendous amount of data in terms of **malware**, endpoint protection and security analysis and intelligence. Michael Sutton uses...

Cyber threat spurs new drive to step up online security [Gulf Daily News (Bahrain)]

12/05/2013 01:34 (Technology News)

Via Acquire Media NewsEdge) BANKS, retail outlets and major **government** bodies in Bahrain are set to tighten up their online security following...

Two charged with hacking computers to generate bitcoins

12/05/2013 01:05 (Computerworld)

Two charged with hacking computers to generate bitcoins The suspects used **malware** to build a botnet, German police said IDG News Service - German...

Britain to give all-clear to Huawei security centre

12/04/2013 17:48 (CNBC)

More technology equals more risk in 2014: IDC) Australia's **government** upheld a ban in October on Huawei bidding for work on its National Broadband...

Majority of users could not fully restore data damaged by malware [Kuwait Times]

12/04/2013 17:19 (Technology News)

Majority of users could not fully restore data damaged by **malware** [Kuwait Times] (Kuwait Times Via Acquire Media NewsEdge) Kaspersky booth at...

The Bitcoin Bubble

12/04/2013 15:22 (Forbes)

...is not as safe as it once was. Cyber gangs are developing **malware** to steal individuals bitcoin purses on line. Those values are only going higher.

Kaspersky Lab Names This Year's Top Cyber Security Threats

12/04/2013 14:01 (Forbes)

Kaspersky Lab Names This Year's Top **Cyber Security** Threats Russian **cyber security** company Kaspersky Lab listed their take on the year s top security...

Financial services cyber security trends for 2014

12/04/2013 12:39 (Help Net Security)

...Perkele Trojan - a crimeware kit - and other cross-platform **malware** have identified large gaps in mobile device security. These threats take...

Kaspersky, six others top malware removal tests

12/04/2013 11:35 (Computerworld Malaysia)

Kaspersky, six others top **malware** removal tests A-V Comparative finds that seven antimalware packages are the best at removing -- not finding...

Spoofed MasterCard warning delivers malware

12/04/2013 10:42 (Help Net Security)

Spoofed MasterCard warning delivers **malware** A worrisome email notifying users that their MasterCard debit card has been blocked just when most...

Air Gaps Not Even Secure

12/04/2013 10:31 (Isssource.com)

...could end up being a moot point as there is a **malware** prototype that uses inaudible audio signals to communicate and covertly transmit sensitive...

ENISA provides new guide for mitigating ICS attacks

12/04/2013 06:20 (Help Net Security)

ENISA provides new guide for mitigating ICS attacks The EU s **cyber security** agency ENISA has provided a new manual for better mitigating attacks...

Lost forever - 60% of users in the UAE could not fully restore data damaged by malware [Mid-East.Info]

12/04/2013 05:52 (Technology News)

Lost forever - 60% of users in the UAE could not fully restore data damaged by **malware** [Mid-East.Info] (Mid-East. (Mid-East.Info Via Acquire...

Over 80% of employees use unauthorized apps at work

12/04/2013 05:49 (Help Net Security)

...also encrypt sensitive information, prevent data loss, protect against **malware**, and enable IT to enforce acceptable usage policies. The survey...

Fake Amazon “Order Status” emails deliver malware

12/04/2013 05:48 (Help Net Security)

Fake Amazon Order Status emails deliver **malware** It comes as no surprise that as holiday shoppers begin to flood the internet looking for deals,

Researchers create malware that transmits data seamlessly via sound waves [Asian News International]

12/04/2013 05:17 (Technology News)

Researchers create **malware** that transmits data seamlessly via sound waves [Asian News International] (Asian News International Via Acquire Media...

URM fixes malware problem plaguing credit card system

12/03/2013 22:19 (KXLY.com)

URM fixes **malware** problem plaguing credit card system You can swipe your plastic again at dozens of local grocery stores as URM says the problem...

Experimental malware uses inaudible sound to defeat network air gaps

12/03/2013 21:41 (Computer World Singapore)

Experimental **malware** uses inaudible sound to defeat network air gaps In a development likely to concern those who believe that a system that's...

SMBs in A/NZ are continually vulnerable to cyber attacks: Check Point

12/03/2013 21:41 (Computer World Singapore)

...limited. "This provides a perfect platform for criminals to target these organisations with **malware**, C&C and data loss attacks," he said. The next...

Eight tips for more secure mobile shopping

12/03/2013 21:22 (Computer World Singapore)

That way, a malicious app on the phone won't have the opportunity to **compromise** the corporate **network**. "It's not likely (to happen), but there...

Worm may create an Internet of Harmful Things, says Symantec (Take note, Amazon)

12/03/2013 21:11 (Computerworld Malaysia)

...will increase, by multitudes, the number of things that can be **hacked** and attacked. Security firm Symantec says it has found a Linux **worm** aimed...

A taste of the horrible things to come for Windows XP

12/03/2013 19:33 (Yahoo! News)

...even warned users of the imminent tsunami of viruses and other **malware** that will inevitably wash over XP stragglers once it stops issuing updates...

JPEGs on the Attack

12/03/2013 17:55 (Isssource.com)

...itself. These files also contain details about hostnames in the **compromised network** and the process names of several antivirus products. Some...

Ransomware Uses Webcam in Scam

12/03/2013 17:38 (Isssource.com)

...people by secretly taking their picture with their webcam. The **malware** disables your computer then claims to have detected viruses and demands...

Cyber-security puzzle: Who is sending Internet traffic on long, strange trips?

12/03/2013 13:20 (Yahoo! News)

In each case, the intentional diversion sent the company or **government** data stream cascading overseas to a distant location then quickly on to...

Software vulnerabilities are the top cause of internal data security issues for business

12/03/2013 09:31 (Technology News)

...technologies, which offer top-of-the-line protection against **malware** and other cyber threats, are built into Kaspersky Endpoint Security for Business,

Experts offer cyber security forecast for the year ahead

12/03/2013 09:23 (Help Net Security)

Experts offer **cyber security** forecast for the year ahead Kroll released its third annual **Cyber Security** Forecast, a prediction of the most significant...

New Stuxnet under development, says Iranian news agency [ITP.net (United Arab Emirates)]

12/03/2013 08:27 (Technology News)

New **Stuxnet** under development, says Iranian news agency [ITP.net (United Arab Emirates)] (ITP.net (United Arab Emirates) Via Acquire Media NewsEdge)

Whistlehackers in the age of surveillance

12/03/2013 02:49 (Yahoo! News)

...learned, for instance, that the U.S. government NSA **malware** reportedly infects more than 50,000 computers worldwide operates an aggressive system...

RBS' services back online after outage on Cyber Monday

12/02/2013 21:17 (CNBC)

...what to expect) RBS, which is 82 percent owned bythe UK **government**, faced a probe by the Financial Conduct Authority in April when technology...

Hacker of Koch Industries website sentenced in Kansas

12/02/2013 20:50 (Yahoo! Canada Finance)

Wisconsin trucker sentenced in Koch cyberattack

12/02/2013 19:24 (Yahoo! News)

was sentenced in U.S. District Court for taking part in the **cyber**-**attack** on Koch Industries. He pleaded guilty earlier to a misdemeanor count...

International Agents Shut Down Counterfeit Sites in Flashy Sting

12/02/2013 19:15 (Yahoo! News)

...market-price item for cheap, and hackers prey on giddy shoppers by **phishing** for personal and financial information. This is just another reminder that...

Linux Worm Targets ICS

12/02/2013 16:35 (Isssource.com)

set-top boxes, and security cameras could also fall victim. The **malware** spreads by exploiting a PHP vulnerability patched back in May 2012, said...

90,000 patients' info exposed in hospital malware attack

12/02/2013 14:12 (Help Net Security)

90,000 patients info exposed in hospital **malware** attack Personal information of some 90,000 patients of two Seattle hospitals has been compromised...

Online banking malware volume increases: Trend Micro report [India Business] [Times of India]

12/02/2013 13:19 (Technology News)

Online banking **malware** volume increases: Trend Micro report [India Business] [Times of India] (Times of India Via Acquire Media NewsEdge) BANGALORE:

Spam emails and phishing bankers' primary IT concern [Northwestern Financial Review]

12/02/2013 13:18 (Technology News)

...said they had been spammed via instant messaging. Only 36 percent reported they had sustained a **malware** attack. (c) 2013 NFR Communications Inc

Free shopping voucher offer leads to phishing

12/02/2013 13:04 (Help Net Security)

...part with their personal and financial information, or to install **malware**. Cybercriminals have been ramping up their efforts as the year draws...

Is your computer secretly mining Bitcoin?

12/02/2013 12:58 (Yahoo! News)

...less-than-honest companies looking to hijack as many processors as possible via **malware** or Potentially Unwanted programs (PUPs) such as this app. And...

Legitimate apps bundled up with secret Bitcoin miner

12/02/2013 11:57 (Help Net Security)

...them. This latter option is usually performed illegally, by installing **malware** on the victims machines without their approval and knowledge, but...

City of London Police to take over Action Fraud cyber crime reporting centre

12/02/2013 09:38 (ComputerworldUK.com)

City of London Police to take over Action Fraud **cyber crime** reporting centre National Fraud Authority is being shut down The City of London Police...

Shopping convenience overrides security concerns

12/02/2013 09:10 (Help Net Security)

...Q3 2012. Yet, during the same time period, mobile **malware** threats also increased 26 percent, making consumers more vulnerable to mobile attacks...

Week in review: Cyber Monday dangers, Twitter adds Forward Secrecy, and a Linux worm that targets the Internet of Things

12/02/2013 04:54 (Help Net Security)

...surrounding secure email provider Lavabit and its legal fight against the US **government** continues with a reply brief filed last Friday by the former,

OS X hardening tips

12/02/2013 03:29 (Help Net Security)

...improving with each OS release but the days of "Macs don't get **malware**" are gone. OS X security is evolving: defenses are improving with each...

Microsoft to Protect Its Customers From Cyber Crimes.

12/02/2013 02:21 (Technology News)

...Technology, emphasized the need to fight cyber crimes since the **government** wants to embrace technology fully given that ICT has been recognized...

Second-hand memory cards pose identity theft risk, warn experts [Asian News International]

12/02/2013 02:21 (Technology News)

...proper deletion of previous data may lead to identity theft, **security** experts have warned. **Computer** scientists from Edith Cowan University in...

Recent cyber attacks reveal bank vulnerabilities, says Bank of England

12/01/2013 23:02 (Computer World Singapore)

...institutions could result in "significant" costs for the sector. "**Cyber attack** has continued to threaten to disrupt the financial system. In the...

Bitcoin mining malware could be hidden in app, security researchers warn

12/01/2013 22:37 (The Guardian)

Bitcoin mining **malware** could be hidden in app, security researchers warn 'If Bitcoin, or a currency working in a similar way to it, got a stable...

It is Happening Again! Microsoft Warns Windows XP Users from Cyber Attacks

12/01/2013 14:04 (Headlines & Global News)

...security company that offers automated threat forensics and dynamic **malware** defense against sophisticated cyber threats. The security company...

Defense Department tackles mobile device authentication through several pilots

12/01/2013 10:11 (Pendleton Times-Post)

...(206) United States government (2738) Subjects: Military technology (9) **Computer** and data **security** (We also have more stories about: (click the...

Don't be caught off guard on Cyber Monday

12/01/2013 02:34 (Press-Republican (AP))

...use officially authorized applications. With the increases in mobile **malware** and viruses, ensure that application publishers are authorized by...

Google Wants To Make Your Passwords Obsolete

11/30/2013 11:24 (Forbes)

...convenience, however, the U2F standard offers robust protection against **malware** that records your keystrokes, since there s no password to type.

Beware: 'Tis the Season for Cyberscams

11/30/2013 11:11 (CIO Today)

...engineering and greed," says Sorin Mustaca, security analyst at anti-**malware** firm Avira. The bad guys count on one in 10 recipients of holiday-themed...

Symantec: Gobal training programme in cyber security to be piloted in New Zealand and Australia

11/29/2013 12:00 (ComputerWorld)

...when it comes to the digital revolution. In New Zealand, the **government** is expected to table a draft of new privacy legislation very soon. This...

Cyber Defense Magazine
848 N. Rainbow Blvd. #4496, Las Vegas, NV 89107.
EIN: 454-18-8465, DUNS# 078358935.
All rights reserved worldwide.
marketing@cyberdefensemagazine.com
www.cyberdefensemagazine.com

Cyber Defense Magazine - Cyber Warnings rev. date: 12/30/2013

RSA® CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share. Learn. Secure.

Capitalizing on
Collective Intelligence

Save $400 on Your Full Conference Pass | **Discount Ends Jan 24th**

2 Expos | 350+ Exhibitors | 21 Tracks
300+ Sessions | 17 Keynotes

Closing Keynote Speaker

STEPHEN COLBERT
Award-winning host and executive producer of *"The Colbert Report"* and *New York Times* best selling author

Experience new ways of learning with these exciting opportunities:

- > **NEW – The Sandbox** featuring *Innovation Sandbox* and *The Most Innovative Company*
- > **Flash Talks** Powered by PechaKucha
- > Two Day Immersive **SANS Tutorials**
- > (ISC)² Half Day **CBK Training Previews**

FOLLOW US ON: #RSAC

Register Now! www.rsaconference.com/cyberdefense

Global Diamond Sponsors: Juniper Networks, Microsoft, RSA

Global Platinum Sponsors: Cisco, FireEye

Global Gold Sponsors: Akamai, ixia, splunk>

Platinum Sponsors: HP, McAfee, Qualys, Symantec

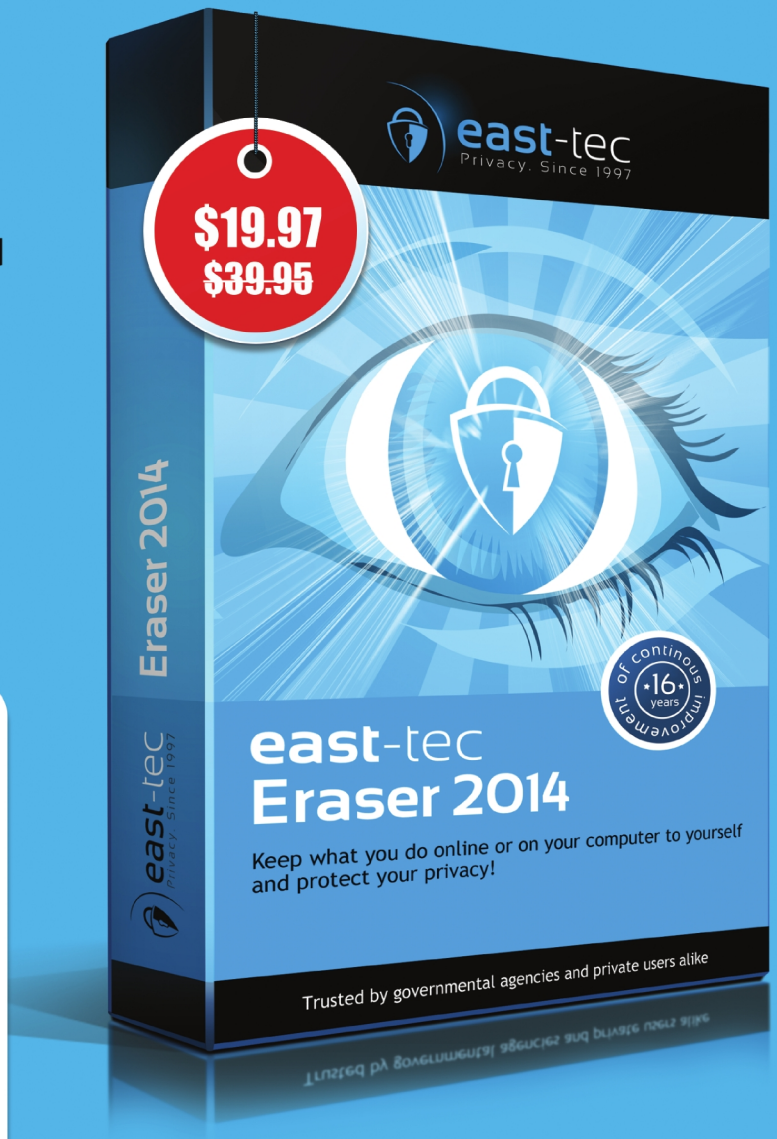
Gold Sponsors: HOB, Sophos, TeleTrusT, TREND MICRO, websense

east-tec
Privacy. Since 1997

www.east-tec.com

east-tec Eraser 2014

Protect your data and privacy by removing all evidence of your online and offline activity with **East**-Tec **Eraser 2014**.
Securely erase your Internet and computer activities and traces, improve your PC performance, keep it clean and secure!



Exclusive offer for
Cyber Defense magazine
readers

Save 50%

on ALL East-Tec products
www.east-tec.com

Coupon Code:

CYBERMAG2014

private evidence protection traces from 250 + apps history
pages online privacy secure search pictures
cookies
security emails