CDM
CYBER DEFENSE MAGAZINE
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

JANUARY 2013

WHAT IS NEXT?

Find out in Cyber Defense Magazine.

CONTENTS

CYBER WARNINGS

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

EDITOR

Gary S. Miliefsky, CISSP®, FMDHS
garym@cyberdefensemagazine.com

ADVERTISING

Jessica Quinn
jessicaq@cyberdefensemagazine.com

CDTL - LAB REVIEWS

Stevin Victor
stevinv@cyberdefensemagazine.com

KEY WRITERS AND CONTRIBUTORS

Pierluigi Paganini
Dave Porcello
Phillip Hallam-Baker
Christian Mairoll
Tim Pierson
Edward A. Adams
Peter Jenney
Paul Paget
David Rosen
Allan Cowen
David Melnichuck
Mike Danseglio
David Strom
Jeff Bardin
Merchant Bhaumik
Clement Dupuis
Robert A Martin

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

Welcome to 2013. We have a lot of updates coming…

Refreshing our website content and gearing up for RSA Conference 2013…

Happy to see you are still with us. Those darn Myans fooled us again! I bought the emergency food kit, a bunker, an emergency ticket to the international space station. No refund policy. Oh well.

The good news is we are all still here – we'll most of us. From Ravi Shankar to Dick Clark, we lost some global icons and for those of us interested in space travel, we lost science fiction icon Ray Bradbury. To top that off Neil Armstrong, the first man on the moon has passed while Sally Ride, the first Woman in space also passed on. As we move forward in our lives, it's good to reflect on the past as a marker and to help guide us on where we are going.

Where are we going anyway? We'll, Cyber Defense Magazine is going to the RSA Conference 2013. As we move past the bittersweet memories of those who are no longer with us, and cherish what they gave to make the world a better place, the future of information security looks brighter and brighter.

The RSA Conference 2013 shall be a marker for all of us in the industry. After this conference we shall look back and say it was an amazingly positive way to kickoff the new year. At this event, we shall each attendee learn something new. There will be innovative ideas on how to secure your USB stick, your Hard Drive,

your Computer, your Email, your Web and Cloud applications, your Network, your Identity, your Organization and your new smart phone and tablet devices.

Our website shall be going through some content upgrades and we're launching a contest for both paid and free subscribers – it will be your chance to win prizes just for being one of our readers. The first round of prizes will be licenses to the Editor's Choice for Anti-malware – Emsisoft's product suite. More on this soon on our website so please bookmark our home page and pay us a visit in a week or so. By the way, to start off the new year on a good note, I gave my best ideas on Bulletproof IT Security out on a very cool educational blog site called Concise-Courses.com. You can watch it at: http://www.concise-courses.com/infosec/20130115/#. I also recommend, like the NAISG.org free techtips or the CCCure.org free quiz, you join this site – it's free and the mini-courses are very educational and some ☺ are a little entertaining as well. Nothing stopping us from securing cyberspace and enjoying it in the process, right?

As it's a brave new world and an exciting new year, let's take the best we've learned in 2012 and start out 2013 on a most positive note. Let's be as proactive as we can be in our field and get one step ahead of the well organized cyber criminals and their new and innovative forms of zero-day malware such as Red October (or was that a Cyber Weapon launched as part of Cyber Warfare and Cyber Espionage?) Remember - vigilance is key. *Hold the ethical course and stay vigilant! By the way, we're growing thanks to you; I'll be moving to the Executive Producer role bringing in an amazing new Editor and Chief whom many of you already know for his amazing INFOSEC articles and work. Exciting times…*

Peace and Prosperity, Gary S. Miliefsky, Editor 

Bouncer, new phishing variant from RSA

by Pierluigi Paganini, Special Contributor to Cyber Defense Magazine.

Despite simplicity of the schema phishing attacks have increased exponentially in the last years targeting every sector,both public and private. RSA's October Online Fraud Report 2012 revealed a worrying scenario, phishing attacks increased up 19% over the second half of 2011, the total loss for various organizations has been estimated to $2.1 billion over the last 18 months.

> *"As we close out 2012, it's safe to say that phishing has had yet another record year in attack volumes. The total number of phishing attacks launched in 2012 was 59% higher than the total calculated for 2011, up from 279,580 attacks to 445,004, costing the global economy over $1.5 billion dollars in fraud damages. According to RSA research, this amount is 22% higher than the losses recorded in 2011, part of the growing worldwide monetary losses associated with phishing attacks." "Beyond rising attack numbers and the money they harvest, phishing kits are increasingly advancing on the technical level, written by malware authors and black hats. 2012 saw the popular use of kit plugins doing real-time credential validation; or reporting via web analytics tools the success of attack campaigns."*

Phishing attacks are exploiting new channels, such as social media and mobile, due the large diffusion of these platforms and the leak of proper security countermeasures. Security firm RSA has recently published a post in which cybercrime specialist Limor Kessem reveals a new scheme for phishing attack, dubbed Bouncer Phishing. The post reported that cyber criminals identify in unique way the targets, they assign to each victim an ID that is used during the

scam campaigns, for each attack is composed a list of victims and only the IDs presents in the list are hit by the attack. The unique ID is automatically generated for each victim and for it is composed an unique web address to click on.

> *"the kit immediately generates an attack page, creating it on the very same hijacked website. The kit's code is programmed to copy pertinent files into a temporary new folder and send victims to that page in order to steal their credentials."*

When the ID of a victims is not include in the list of targets the link created will simply be presented with an harmless error page showing 404 error message. The expert Kessem said:

> *"And now we're seeing the more unusual breeds: bouncer list phishing. It holds this moniker because much like many high-profile nighttime hotspots – if your name is not on the list, you're staying out! After the kit collects victim credentials it sends them to yet another hijacked website (taken over using the exact same method of vulnerability exploit and web-shell), where the password-protected attack page lies in wait to steal user credentials."*

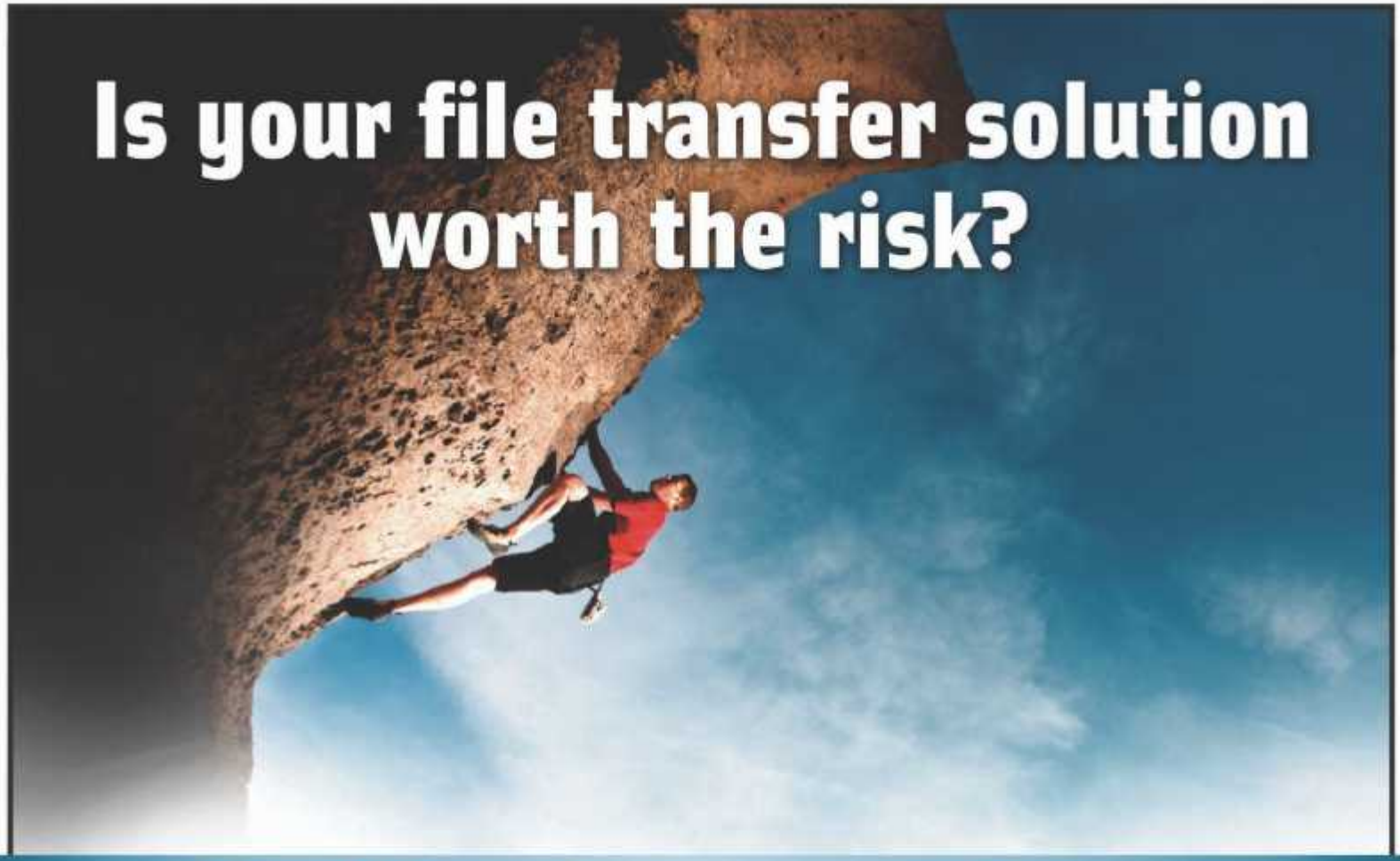
The approach could have serious consequence on the "detection procedure" implemented by the principal security firms, but which is the advantage of the techniques? The methods allow to the attackers to collect data only related to a specific groups of users, of course the techniques in less noisily respect classic phishing schema. The techniques is very efficient, let's imagine an attack on a geographic region where a local shop propose exceptional discounts or where is arranged a specific event, in that cases it is possible to address the victims selecting only ID of the users that live or work in the area, the most interested to information

provided and so more exposed to social engineering attacks. Only most pertinent credentials from a restricted audience are collected by the attacks differently by traditional massive phishing campaign. RSA expert explained that each campaign targeted an average number of 3,000 recipients from a list containing a mix of users profiles (e.g. corporate addresses, bank employees) obtained with as aggregation of spam lists or data breach collections. Phishing techniques are evolving and they are showing increasing complexity and bouncer phishing is just the last innovation in this sense. The post of RSA also introduces a couple techniques to compromise website to use in the phishing attacks to host malicious code:

- Preying on WordPress plugin zero-day vulnerabilities to compromise and hijack websites
- Uploading a web-shell to hijacked sites, taking over and exploiting them as resources

You can bet that in the future new techniques will be studied and implemented by cyber criminals … and then security companies will try to remedy, as in a continuous play cops and robbers. In the meantime let's do awareness … the only way to avoid the cyber threats is know them.

(Source: Pierluigi Paganini, CDM)



Simplify • Automate • Encrypt

GoAnywhere™ protects data in motion with an enterprise managed file transfer solution. It supports popular protocols such as SFTP, FTPS, and HTTPS, as well as Open PGP, GPG, AS2 and AES encryption standards.

With robust audit logs and error reporting, GoAnywhere manages file transfer projects through a browser-based dashboard. Features include Secure Mail for ad-hoc file transfers, high availability clustering and load balancing, and NIST-certified FIPS 140-2 encryption.

Don't risk having your sensitive data compromised. **Download a free full-version trial of GoAnywhere or request a demo today!**

See for yourself
Watch these video success stories from GoAnywhere customers.

GO ANYWHERE™

GoAnywhere.com 800.949.4696

a managed file transfer solution by

LINOMA SOFTWARE

Checkout Concise-Courses Free Hacker Hotshots

http://www.concise-courses.com/upcoming/

We are a team of IT security trainers and educators who are passionate about using the Internet to deliver highly specialized and convenient instructor-led information security education. We offer boot camps for the following security pathways:

7 Week Online Training - **ISC2 CISSP: Certified Information Systems Security Professional**
4 or 6 Day Online Training Boot Camp - **CompTIA Security+**
4 Day Online Training Boot Camp - **EC Council Certified Ethical Hacker (CEHv7)**
4 Day Online Training Boot Camp - **Mile2 CPTE**

We also host a live weekly InfoSec web show called "Hacker Hotshots!"

What Makes Us Special?

1. Convenient Class Schedules

Our live instructor led classes do not require time off work. Classes are offered in the evening and/ or the weekends.

2. Cost-Effective Enrollment Fees

The truth is, the only real costs in offering live instructor led online education is the cost of the instructor. Our enrollment fee structure passes these saving on to you, while always offering the best instructors in the industry.

Why Should I Care?

1. No time off work.

2. Guaranteed lowest enrollment fees for live online instruction.

3. No risk. 100% money back guarantee.

Thanks for the props. See you at RSA Booth #2747

Cyber Defense Magazine has named Pwnie Express "Best of Class for Penetration Testing 2013." We're dedicated to bringing the best pentesting equipment to light in 2013.

PWNIE EXPRESS

PwnieExpress.com | 802-227-2PWN

- Pwn Plug
- Power Pwn
- Pwn Phone
- EPA

Chinese Hackers Exploit Internet Explorer Zero Day for Cyber Espionage

CFR – Council on Foreign Relations Website Becomes Malware Magnet

According to Fireeye, the web site for the Council on Foreign Relations was compromised and recently hit by a drive-by attack that was detected this month. The exploiters are suspected to be from mainland China. They exploited a zero day vulnerability in Internet Explorer at the most elite foreign policy group in America – the CFR.

According to Fireeye researchers, malicious content on the website was hosted by hackers whch is used as a 'drive by' that is exploiting the fully patched and allegedly secure (yea, right) Internet Explorer version 8.0 to take advantage of visitors to the CFR website. Fireeye has provided the information to Microsoft and has not released additional details hoping that Microsoft will be able to develop a patch to this issue for Internet Explorer 8.0 users.

(Source: Fireeye)

Romanian National Sentenced to 21 Months in Prison for Role in Multimillion-Dollar Scheme to Remotely Hack into and Steal Payment Card Data from Hundreds of U.S. Merchants' Computers

A Romanian national was sentenced this month to serve 21 months in prison for his role in an international, multimillion-dollar scheme to remotely hack into and steal payment card data from hundreds of U.S. merchants' computers, announced Assistant Attorney General Lanny A. Breuer of the Justice Department's Criminal Division; U.S. Attorney for the District of New Hampshire John P. Kacavas; and Holly Fraumeni, Resident Agent in Charge of the U.S. Secret Service (USSS), Manchester, N.H., Resident Office.

Cezar Butu, 27, of Ploiesti, Romania, was sentenced by Judge Steven J. McAuliffe in U.S. District Court in New Hampshire. On Sept. 17, 2012, Butu pleaded guilty to one count of conspiracy to commit access device fraud. In his guilty plea, Butu admitted that, from approximately 2009-2011, he participated in a Romanian-based conspiracy to hack into hundreds of U.S.-based computers to steal credit, debit and payment account numbers and associated data (collectively "payment card data") that belonged to U.S. cardholders.

According to court documents, Butu and his co-conspirators used the stolen payment card data to make unauthorized charges on, and/or transfers of funds from, cardholders' accounts (or alternatively to transfer the stolen payment card data to other co-conspirators who would do the same). Butu admitted that he repeatedly asked an alleged co-conspirator to provide him with

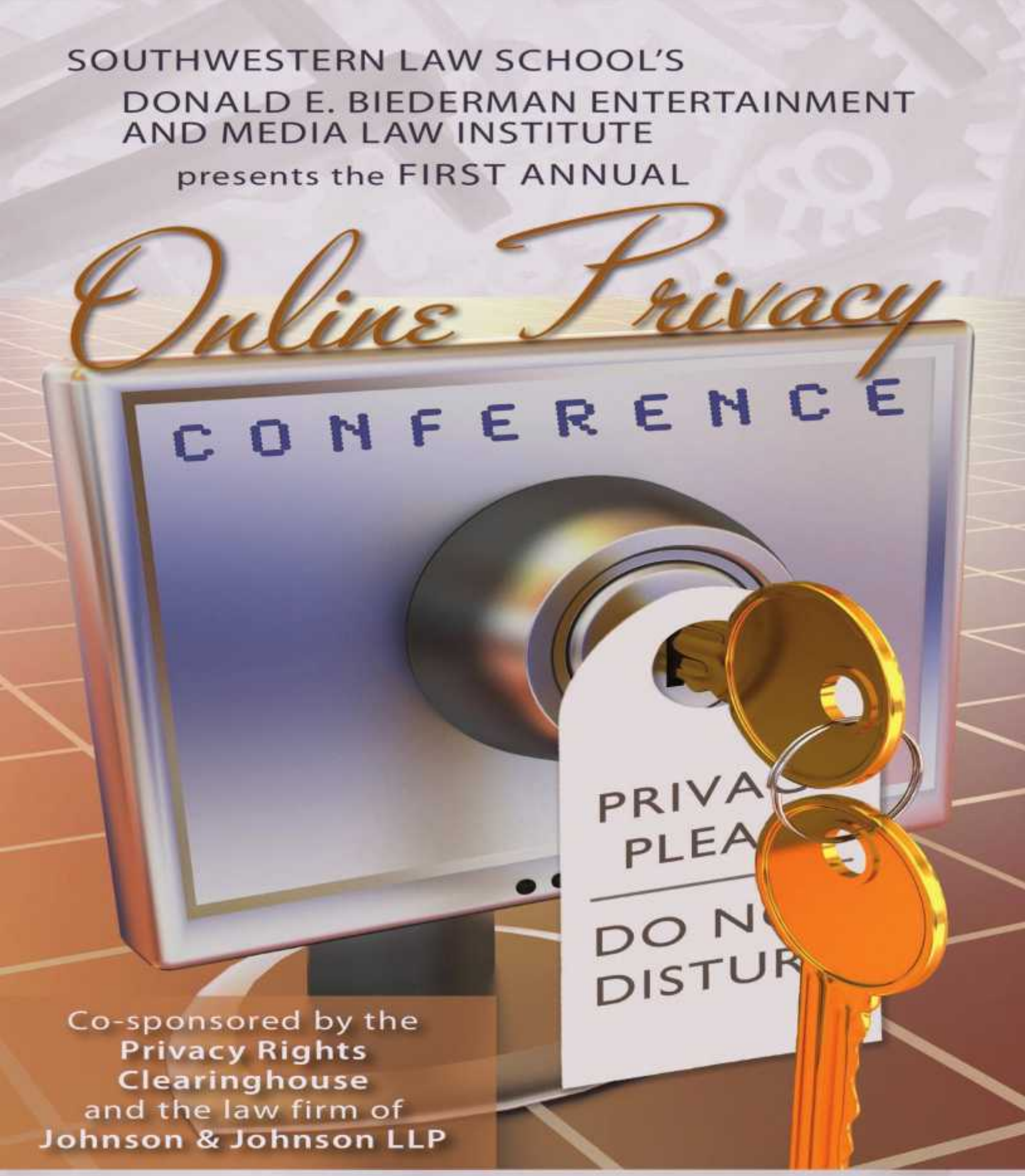
stolen payment card data and that the alleged co-conspirator provided him with instructions for how to access a website where a portion of the stolen payment card data was stored. Butu later attempted to use the stolen payment card data to make unauthorized charges on, or transfers of funds from, the accounts. According to Butu's plea agreement, he also attempted to sell, or otherwise transfer, the stolen payment card data to other co-conspirators for them to use in a similar manner. Butu admitted to acquiring stolen payment card data belonging to approximately 140 cardholders during the course of the scheme.

In his plea agreement, Butu agreed to be sentenced to 21 months in prison. Butu's co-conspirator Iulian Dolan pleaded guilty to one count of conspiracy to commit computer fraud and two counts of conspiracy to commit access device fraud, and has agreed to be sentenced to seven years in prison. Dolan's sentencing hearing is scheduled for April 4, 2013. Alleged co-conspirator Adrian-Tiberiu Oprea is scheduled for trial on Feb. 20, 2013, in U.S. District Court in New Hampshire. The case was investigated by the USSS, with the assistance of the New Hampshire State Police and the Romanian Directorate of Investigation of Organized Crime and Terrorism. The case is being prosecuted by Trial Attorney Mona Sedky in the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorney Arnold H. Huftalen from the District of New Hampshire.

(Sources: USDOJ.gov, CyberCrime.gov)

SOUTHWESTERN LAW SCHOOL'S
DONALD E. BIEDERMAN ENTERTAINMENT AND MEDIA LAW INSTITUTE
presents the FIRST ANNUAL

Online Privacy CONFERENCE



Co-sponsored by the
Privacy Rights Clearinghouse
and the law firm of
Johnson & Johnson LLP

FRIDAY, FEBRUARY 22, 2013

SOUTHWESTERN LAW SCHOOL – LOS ANGELES, CA

Cyber Newsflash for January 2013

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

Oil firms face soaring security bill after attacks

01/25/2013 04:18 (Reuters Top News)

(Repeats Thursday report with no changes) * Cyber, militant attacks overshadow Davos oil gathering * North Africa likely to suffer oil investment slowdown By Dmitry Zhdannikov DAVOS, Jan 24 (Reuters) - Oil executives are resigned to a rise in security costs which will be steep even for an indust

Create a secure browsing session on any Windows computer

01/25/2013 02:28 (Help Net Security)

Making online purchases and secure internet browsing is safer and easier than ever with the launch of Kanguru's new Defender DualTrust, a new secure online access and encrypted USB storage device developed jointly by Kanguru and Deepnet Security.

Facebook's Graph Search worries security experts

01/25/2013 02:17 (Computerworld Malaysia)

Post highlighting embarrassing things raises questions of user privacy with Graph Search, which Facebook users cannot opt out of Facebook's new Graph Search has security experts warning people who use the social network to raise their privacy settings in order to avoid embarrassment or becoming vic

Cyber security funding welcomed by industry

01/25/2013 01:23 (Computerworld Malaysia)

ACS calls for registration of ICT professionals and more research and development funding. The federal government's $1.46 billion funding in improvements to cyber security networks and establishment of an Australian Cyber Security Centre has received a largely positive response from information sec

Security intelligence solutions for mobile technology providers

01/25/2013 00:25 (Help Net Security)

Webroot announced the availability of a portfolio of internet security solutions that give mobile technology providers – from carriers to device manufacturers to mobile device management (MDM) companies – easily deployable and cost-effective services to make security an integral part of their own of

Cybercrime takedown: Is it game over for Gozi trojan that stole millions?

01/24/2013 20:31 (Yahoo! News Canada)

Cyber Newsflash for January 2013 (cont')

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

Will smartphones soon replace wallets?

01/24/2013 20:04 (Yahoo! News)

If there are two things that most of us carry with us every waking moment of the day, it's our phones and wallets. So, in the name of convenience, some of the biggest technology companies are hard at work to combine the two.

In wake of Manti Te'o affair, a warning about 'catfishing' on dating sites

01/24/2013 19:24 (Taunton Daily Gazette (AP))

Similar to popular email phishing scams, 'catfishing" scams occur when a scammer assumes a persona on a social networking site and then creates an entire false identity using the pictures, hobbies, interests and even friends of someone else.

Cyber Report: Attack Intensity on Rise

01/24/2013 18:35 (Isssource.com)

Server-based botnets and encrypted layer attacks are new attack tools challenging organizations during distributed denial of service (DDoS) attacks, according to a new report.

OVERNIGHT DEFENSE: DOD officially ends women in combat ban

01/24/2013 18:29 (The Hill - Blog)

The Topline: The Pentagon on laid out a three-year plan for integrating women into most combat positions on Thursday as the Pentagon's leaders officially ended the ban on women in combat.

U.S. homeland chief: cyber 9/11 could happen "imminently"

01/24/2013 18:22 (Yahoo! News Canada)

Obama's Executive Order on Cybersecurity Fighting Words to GOP

01/24/2013 17:13 (ComputerWorld)

A prominent GOP lawmaker urges President Obama to not issue an executive order mandating new cybersecurity provisions

UCI develops app that stores DNA info on smartphones

01/24/2013 14:57 (The Daily Pilot)

Computer scientists at UC Irvine have developed an app that stores encrypted segments of DNA information on smartphones, giving way to countless possible medical and social uses, according to KTLA.

Cyber Newsflash for January 2013 (cont')

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

Senate Introduces Cybersecurity Bill that Prioritizes Information Sharing

01/24/2013 14:36 (Threat Post)

The United States Senate says it will prioritize the passage of a comprehensive cybersecurity bill designed to fortify the nation's public and private IT systems in this session of Congress.

Users targeted with phishing scam via Facebook messages

01/24/2013 07:49 (Help Net Security)

Facebook users are advised to be on the lookout for bogus personal messages supposedly sent by the Facebook Security Team. The message claims that the users' account has been reported for violating "policies that are considered annoying or insulting Facebook users," and that they have to "reconfirm"

Sony fined in UK over PlayStation cyberattack

01/24/2013 07:40 (Bradenton Herald)

LONDON — British regulators fined Sony 250,000 pounds ($396,100) on Thursday for having insufficient security measures to prevent a cyberattack on its PlayStation Network.

Android Malware, The Biggest Threat to Our Information in 2013?

01/24/2013 05:52 (Android News)

All of this said their are ways to protect your Android device and they should be implemented as quickly as possible, even if it is just for peace of mind.

IT challenges with managing increasing amounts of data

01/24/2013 04:18 (Help Net Security)

Half of all organizations EVault surveyed in the USA, UK, France, Germany, and the Netherlands say they are managing more data now than they were a year ago, and 70 percent of those same organizations expect that the volumes of data they manage will only continue to climb.

Governments fishing for more user data from Google : Technology

01/24/2013 01:43 (WCFCourier.com)

Google is being pulled into an increasing number of police and government investigations around the world as authorities seek to learn more about the people who use its Internet search engine, email and other services.

Cyber Newsflash for January 2013 (cont')

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

Study: Digital information can be stored in DNA : Technology

01/24/2013 01:43 (WCFCourier.com)

It can store the information from a million CDs in a space no bigger than your little finger, and could keep it safe for centuries. Is this some new electronic gadget? Nope.

3 in U.S. charged over widespread Gozi computer virus

01/23/2013 23:02 (Metro)

Australian Cyber Security Centre deemed new government hub

01/23/2013 21:46 (Computer World Australia)

Based in Canberra, industry, state and territory partners will collaborate with government agencies.

U.S. arrests three in cyber crime case involving millions of dollars

01/23/2013 19:10 (The Globe and Mail)

DARPA Seeking Help With Targeted Attack Analysis

01/23/2013 09:35 (Threat Post)

The networks of government agencies and the military are under constant attack from a variety of sources, and the U.S., like most other countries, relies on those networks to not just run daily operations, but to support missions around the world.

Hackers out-Smart power utilities

01/23/2013 07:40 (Power Engineering International)

A rush towards â€˜Smartâ€™ technology, without an associated hike in security, is laying the power sector open to devastating cyber attacks, warns the head of a UK-based security specialist.

Microsoft identifies 13 Shanghai PC resellers involved in Windows piracy

01/23/2013 04:42 (Computerworld)

Microsoft could take legal action against the resellers if settlement isn't reached

Fraud alert: Bold new ATM schemes prompt warnings [Star Tribune (Minneapolis)]

01/23/2013 04:33 (Equities.com)

By Jennifer Bjorhus, Star Tribune (Minneapolis) McClatchy-Tribune Information Services Jan. 23--ATM swindles have moved beyond mere skimming -- planting tiny cameras on gas pumps, for instance, to spy on your swipe and steal your cash.

Cyber Newsflash for January 2013 (cont')

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

Reporters Without Borders website abused in malware campaign

01/23/2013 02:48 (ComputerWorld Singapore)

The website for Reporters Without Borders was booby-trapped to deliver malicious software using the latest Java and Internet Explorer vulnerabilities, security vendor Avast said on Tuesday.

Spam hits five-year low while phishing scams target Facebook

01/23/2013 01:13 (Geektown Blog)

Android malware potentially stole up to 450,000 pieces of personal data: Symantec

01/22/2013 23:21 (Computer World Australia)

More than 3000 visits were made to fake app store, Android Express Play

Ask the Mompreneur: No business too small to get hacked

01/22/2013 22:52 (Macon.com)

You've heard of Tupperware parties and maybe even Botox parties, but have you ever heard of an Internet safety party? Theresa Payton, former White House chief information officer and co-author of "Protecting Your Internet Identity: Are You Naked Online?" is offering to host a customized version of

U.S. Attorney announces new initiative to combat child porn

01/22/2013 22:30 (Indianapolis Star)

At first glance, the five men bear little resemblance to each other. One is a 23-year-old from New Palestine. Another, a 42-year-old from Noblesville.

Cyber Command looks to hire 1,000

01/22/2013 22:15 (My San Antonio (AP))

Crippling uncertainty continues, with March 1 now the deadline for deep cuts in military and federal domestic spending that would last a decade. But for one portion of San Antonio's military community, the outlook for growth remains positive.

CyberPatriot Announces Teams Advancing to the National Finals Competition

01/22/2013 21:32 (News 10 ABC- WTEN)

/PRNewswire-USNewswire/ -- After three impressive preliminary rounds, 28 teams of high school students have advanced to the National Finals Competition of the nation's largest and fastest growing high school cyber defense competition – CyberPatriot V! CyberPatriot-The National High School Cyber Def

Cyber Newsflash for January 2013 (cont')

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

Gillard puts nation on cyber-attack alert

01/22/2013 19:06 (The Guardian)

Prime Minister Julia Gillard has warned that Australia is a prime target for malicious cyber attack by hackers and nations. Launching the nation's first national security strategy today in Canberra, Ms Gillard announced the establishment of a new Australian Cyber Security Centre.

Virut Botnet Goes Down

01/22/2013 16:15 (Isssource.com)

In a coordinated takedown effort, an organization dedicated to fighting spam took over the 300,000-strong Virut botnet late last week. The Virut malware spreads by inserting malicious code into clean executable files and by copying itself to fixed, attached and shared network drives, said officials

As BlackBerry 10 phones near, hopes send RIM stock rising

01/22/2013 13:58 (ComputerWorld)

Speculation, rumors, and hopes about the upcoming BlackBerry 10 launch next week have sent Research in Motion's (RIMM - Nasdaq) stock price soaring.

Skype becomes a malware minefield

01/22/2013 12:36 (Help Net Security)

Skype users should be careful when using the service these days. First CSIS researchers unearthed a campaign misusing Skype to replicate and spread the Shylock banking Trojan with a plugin called msg.

Infected Site Spreading SMS Android Malware

01/22/2013 12:23 (Threat Post)

The website of a popular watch retailer is reportedly redirecting users that visit the site on Android-based devices to a number of malicious domains serving up premium rate SMS malware.

Avoid the Landmine That is Hacking Back

01/22/2013 11:45 (Threat Post)

Rarely a day goes by without mention of a targeted attack against some government-related website, massive disruptions in online banking services, or critical vulnerabilities in specialized software running our power plants and water supplies.

Cyber Newsflash for January 2013 (cont')

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

How to encrypt almost anything [Computer News Middle East]

01/22/2013 10:07 (Equities.com)

IDG Reporter Al Bawaba Ltd. It's all too easy to neglect data security, especially for a small business. While bigger organisations have IT departments, service contracts, and enterprise hardware, smaller companies frequently rely on consumer software, which lacks the same sort of always-on security.

News: DC National Guard executes cyberspace mission in support of 57th Presidential Inauguration

01/22/2013 00:05 (DVIDS)

By: Senior Airman Jennifer Hotte and Senior Airman Ian Caple WASHINGTON - In support of the 57th Presidential Inauguration, National Guard computer network defense teams from seven states conducted defensive cyber operations in Washington, DC.

Cyber attacks remain security threats in 2013 – Verizon study

01/21/2013 22:18 (ComputerWorld Singapore)

Cyber attacks of all forms will continue to pose a threat to organisations this year. According to a recent data breach report by Verizon, authentication attacks and "hacktivism" are some of the top threats that organisations should be prepared for.

College Student Expelled After Bringing Web Vulnerability to School's Attention

01/21/2013 22:01 (Threat Post)

A Canadian college student was expelled after reporting a vulnerability in the school's Web site that potentially exposed private data on more than 250,000 students.

Security researchers cripple Virut botnet

01/21/2013 20:21 (Computerworld Malaysia)

Attackers still control some domains used by the botnet, the researchers say. Many of the domain names used by a cybercriminal gang to control computers infected with the Virut malware were disabled last week in a coordinated takedown effort, Spamhaus, an organization dedicated to fighting spam, an

How The 'Computer Wizard' Who Created The First Internet Virus Got Off Without A Day Of Jail

01/21/2013 18:40 (Yahoo! Canada Finance) \

Understanding the new security in Java 7 Update 11

01/21/2013 18:08 (Computerworld Blogs)

The recently released Java 7 Update 11 changed security rules that had just been introduced with Update 10. The ink was barely dry, so to speak. Here I hope to explain the rules for running Java programs embedded in web pages.

Cyber Newsflash for January 2013 (cont')

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

In Google's Future, You May Log in with Your Ring

01/21/2013 17:05 (CIO Today)

A smartphone or "smartcard-embedded finger ring," wrote the Google authors, could "authorize a new computer via a tap on the computer, even in situations in which your phone might be without cellular connectivity." The Google authors call for the "primary authenticator" to be a piece of hardware, bu

Malware Spreads through Skype

01/21/2013 16:30 (Isssource.com)

There is a new version of the Shylock malware spreading through Skype and is playing off the fact Microsoft is about to kill its Messenger application in favor of Skype.

Exprespam Android Malware Steals Upwards to 75,000 Bits of Information

01/21/2013 15:29 (Threat Post)

Early research from Symantec estimates that spammers behind a new type of Android malware may have already stolen "between 75,000 and 450,000 pieces of personal information" from Japanese users.

Web Site Security Holes

01/21/2013 15:14 (Isssource.com)

There were vulnerabilities in the websites of Microsoft and Twilio and flaws in the ProActive content management system (CMS), a researcher said. Twilio rushed to address the Cross-site request forgery (CSRF) vulnerability identified by researcher Rafay Baloch.

Commerce considering managed service to fix cyber weakness

01/21/2013 14:58 (FederalNewsRadio.com)

The Commerce Department wants to fix a glaring cyber weakness. It lacks full centralized enterprisewide cybersecurity reporting capabilities across its 90,000 computers.

Microsoft Security Essential Fails Security Certification Test Again

01/21/2013 14:18 (Mobile & Apps)

Microsoft's free anti-virus product Security Essentials, for the second time in a row, failed to win quality certification by AV-Test Institute. AV-Test is a Germany-based test firm that evaluates both free and paid anti-virus tools and issues certifications for the most reliable anti-virus software.

Cyber Newsflash for January 2013 (cont')

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

Proposed EU cyber security law will require proactive network security

01/21/2013 11:36 (Help Net Security)

Last week, the European Commission proposed new legislation to require major tech firms like Google and Facebook to report any security breaches to local cyber crime authorities or risk sanctions like fines.

Google Deems Pirate Bay As 'Malware Distributor' - Chrome & Firefox Give Warnings

01/21/2013 10:38 (Mobile & Apps)

Chrome and Firefox browser users may have some difficulty accessing The Pirate Bay, as Google has now deemed the site as a malware distributor. In fact, any other site that uses bayimg, the image hosting service The Pirate Bay (TPB) founded back in 2007, is in the same situation.

Polish CERT hits Virut botnet

01/21/2013 07:56 (Help Net Security)

The Polish Research and Academic Computer Network (NASK), the national registry of the .pl domain and founder of CERT Polska, has announced on Friday that they took over 23 domains that served as C&C servers for the Virut botnet.

Bracing for furloughs: DoD, others begin detailed sequester planning

01/21/2013 07:03 (Federal Times)

Federal agencies are girding for mass furloughs and other cutbacks as across-the-board budget reductions loom in barely a month. "Hundreds of thousands" of employees face unpaid time off if those cuts take effect, Jeff Zients, acting chief of the Office of Management and Budget, wrote in a Jan.

Cyber-crime expert's advice is to trust no one [The New Hampshire Union Leader, Manchester]

01/20/2013 08:35 (Equities.com)

By Dave Solomon, The New Hampshire Union Leader, Manchester McClatchy-Tribune Information Services Jan. 20--NASHUA -- If you still think of the typical computer hacker as a nerdy teenager working from his mother's basement to engage in online vandalism, think again.

Researchers find another Java security flaw [Computer News Middle East]

01/20/2013 03:46 (Equities.com)

IDG Reporter Al Bawaba Ltd. Researchers from a Poland-based vulnerability research firm on Friday announced that they had found vulnerabilities in Java 7 Update 11 that can be exploited to bypass the software's security sandbox and execute arbitrary code on computers.

Cyber Newsflash for January 2013 (cont')

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

Tech Tips: Is your cellphone safe from 'Smishing?'

01/20/2013 00:00 (Carroll County Times)

Many technology experts are declaring that a top security threats for 2013 will be cyber-attacks on mobile devices. In fact, smishing, a form of hacking information from cell phones (derived from SMS, or Small Message Service), is already running rampant for both consumers and business owners alike.

Malaysia's cyber security agency has new head

01/19/2013 20:36 (ComputerWorld Singapore)

CyberSecurity Malaysia's CEO comes from Ministry of Science Technology and Innovation. Photo - Dr Amirudin bin Abdul Wahab, CEO, CyberSecurity Malaysia National cyber security agency CyberSecurity Malaysia has appointed Dr Amirudin bin Abdul Wahab as its new chief executive officer with effect fro

Belt-tightening begins at Air Force Academy

01/19/2013 16:59 (Colorado Springs Gazette)

Lt. Gen. Mike Gould planned to meet with the president of Brigham Young University on Thursday. The leader of another university took his place. Gould, the Air Force Academy's superintendent, also had plans to fly into Dallas this week and present former academy football star Chad Hennings with the

Fighting a ghost: What DDoS means to SMEs

01/19/2013 13:54 (Business Review Europe)

Tim Pat-Dufficy, managing director of hosting experts ServerSpace, explains why business owners need to be aware of the risks of insufficient security measures

Google Pushing To Make Passwords A Thing Of The Past

01/19/2013 12:08 (Android in Canada Blog)

Hacktivism: Civil Disobedience or Cyber Crime?

01/19/2013 12:05 (Herald De Paris)

by Christie Thompson When Reddit co-founder and internet freedom activist Aaron Swartz committed suicide last Friday, he was facing up to 13 felony counts, 50 years in prison, and millions of dollars in fines.

Democrat warns revamp of hacking law could take 'a very long time'

01/19/2013 09:15 (The Hill - Blog)

Rep. Zoe Lofgren (D-Calif.) wants to overhaul a computer hacking law in the wake of the suicide of Internet activist Aaron Swartz, but she warns it will not be an easy task.

Cyber Newsflash for January 2013 (cont')

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

Bank online or by smartphone? Consider these safeguards

01/19/2013 09:00 (OregonLive.com)

, updated January 19, 2013 at 7:13 AM View/Post Comments U.S. Bank this month announced Portland is one of two cities where it's testing an iPhone case that enables customers to wave their phone at store checkouts to pay.

Plug-in device unplugs viruses

01/19/2013 05:44 (Boston.com)

V3 Click anti-malware device by AhnLab Inc. $39.95 at Amazon.com Millions of us are too lazy to install software that can protect our computers from viruses and other malware.

Government works to build up its IT knowledge

01/19/2013 03:05 (The StarPhoenix)

Air Force Duo Design Smart Phone Application For Inauguration Day

01/19/2013 01:39 (Equities.com)

Targeted News Service WASHINGTON, Jan. 18 -- The U.S. Air Force issued the following story: Two Airmen with the Joint Task Force - National Capital Region Public Affairs created a free, public cellphone application that allows users to stay informed about the 57th Presidential Inauguration.

Malware masquerades as patch for Java

01/18/2013 01:46 (Computerworld Malaysia)

The malware, ironically, does not actually exploit the Java vulnerabilities, according to Trend Micro. Trend Micro has spotted a piece of malicious software that masquerades as the latest patch for Java, a typically opportunistic move by hackers.

'Madware' and virtualisation key areas to watch in 2013: Symantec

01/18/2013 01:27 (Computerworld Malaysia)

Businesses need to be aware of, and prepared for, mobile adware, or "madware", in 2013, according to Symantec Pacific region specialist solutions director, Sean Kopelke, who includes social media, mobile and Cloud threats in his warning.

The six most common identity theft risks at tax time

01/18/2013 00:01 (The Powdersville Post)

(BPT) - Tax time is always tough. Whether you will owe or anticipate a refund, plan to do your own taxes or pay a professional to do them for you, preparing and filing your taxes can be a tedious task.

Cyber Newsflash for January 2013 (cont')

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

Iran strengthened cyber capabilities after Stuxnet: U.S. general

01/17/2013 23:18 (Yahoo! News)

WASHINGTON (Reuters) - Iran responded to a 2010 cyber attack on its nuclear facilities by beefing up its own cyber capabilities, and will be a "force to be reckoned with" in the future, a senior U.

Shylock banking malware updated to spread via Skype, researchers say

01/17/2013 22:51 (Computerworld Malaysia)

The Shylock home banking malware has been updated with new functionality that allows it to spread automatically using the popular Skype Voice-over-IP (VoIP) and instant messaging client.

Phishing sites use whitelisting to keep out unwanted victims

01/17/2013 22:22 (ComputerWorld Singapore)

Businesses increasingly use whitelisting to keep the bad guys out but now it turns out that criminals are employing the same tactics to target favoured victims, security firm RSA has reported.

Expected EU data breach rules draw fire before their release

01/17/2013 22:21 (ComputerWorld Singapore)

European Commission proposals for a strategy on cybercrime have come under fire before they have even been released. The Commission is due to present its plan for a European Strategy for Internet Security on Wednesday, but Digital Agenda Commissioner Neelie Kroes has already said that under the pro

Security vendors failing to tackle mobile malware, say CISOs

01/17/2013 20:47 (Computerworld Malaysia)

Malware is still the biggest threat to mobile security, but most mobile device management (MDM) strategies tend to focus on securing the physical device in case of loss of theft, according to Peter Gibbons, head of Information Security at Network Rail.

Iran's Cyber Threat Potential Great, U.S. General Says

01/17/2013 19:06 (Bloomberg)

Iran's developing ability to launch cyber attacks will make it "a force to be reckoned with," the head of the U.S. Air Force Space Command said. General William Shelton said the Iranians are responding to an attack on the computer operating system that runs the uranium enrichment facilities….

Cyber Newsflash for January 2013 (cont')

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

White House cyber chief: Information sharing a 'key ingredient' in cyber efforts

01/17/2013 18:24 (FederalNewsRadio.com)

In the minds of many, information security and information sharing would seem to be polar opposites. But in the White House's new national strategy on information sharing released last month, the two concepts are paired together.

Big Data, Cloud Security Tops the List of IBM Patents in 2012

01/17/2013 16:47 (CloudTimes)

The number of patents registered in the U.S. hit a record last year, with the giant blue once again at the forefront of technological giants, who maintain a war on intellectual property.

Bouncer Phishing Kit Limits Users

01/17/2013 16:46 (Isssource.com)

There is a new type of phishing kit that allows cybercriminals to ensure only certain users can access their phishing websites. Because only users that are on "the list" can access the site, the crime kit's name: "Bouncer.

Large-scale DDoS attacks getting larger

01/17/2013 16:01 (IT Business)

Inside the 1,000 Red October Cyberespionage Malware Modules

01/17/2013 14:20 (Threat Post)

The Red October espionage malware campaign is providing security researchers with a deep dive into the complexity of targeted attacks, which in this case made use of more than 1,000 malware modules for everything from reconnaissance on targets to exfiltration of data to command and control servers.

Large-Scale DDoS Attacks Grow Bigger and More Diversified: According to Prolexic's Latest Report - Seven 50+ Gbps Attacks Mitigated against Financial, SaaS and e-Commerce Firms

01/17/2013 05:43 (Fox 19)

This article was originally distributed via PRWeb. PRWeb, WorldNow and this Site make no warranties or representations in connection therewith. SOURCE: Prolexic Technologies Prolexic Technologies, the global leader in Distributed Denial of Service (DDoS) protection services, today announced that t

ThreatTrack 2.0 plugs malware holes in real-time

01/17/2013 05:31 (Help Net Security)

GFI Software launched GFI ThreatTrack 2.0, the latest version of the security intelligence solution that provides users with visibility into the threat landscape.

Cyber Newsflash for January 2013 (cont')

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

SC's cost for cyber-security fixes could be known about May 1

01/17/2013 04:00 (TheState.com)

COLUMBIA, SC — South Carolina should know by May 1 how to tackle some of its most severe cybersecurity shortcomings and how much the fix might cost, state officials told lawmakers Wednesday.

New Java flaw found in days, sells on black web [Computer News Middle East]

01/17/2013 03:48 (Equities.com)

IDG Reporter Al Bawaba Ltd. Oracle's bad Java week got worse on Wednesday, after it was announced that a previously unknown flaw in the programming language still threatens the security of millions of PCs.

Microsoft vows to improve security suite after failed evaluation

01/17/2013 01:21 (ComputerWorld Singapore)

Microsoft vowed on Wednesday to improve two of its security products after both failed to pass an evaluation by a Germany security software testing organization.

Panetta: fiscal crisis poses biggest immediate threat to DoD

01/17/2013 01:13 (Fort hood sentinel)

WASHINGTON - The "perfect storm of budget uncertainty" howling around his department is the biggest immediate threat facing the U.S. military, Defense Secretary Leon Panetta told reporters here Jan.

Banks request U.S. help with Web attacks

01/17/2013 00:36 (Pittsburgh Post-Gazette)

Several big U.S. banks, including Pittsburgh-based PNC Financial Services Group, have asked the federal government to take action to stop cyber attacks against their websites, according to a story Wednesday in the Wall Street Journal.

How to keep yourself from getting cyber-stalked

01/16/2013 23:09 (The Norman Transcript)

Sooner or later, we all get that email that we don't want, or receive something posted on our social network page that we wish we never got, and whether the message is from a company, an overzealous salesperson or from a personal acquaintance, they can be annoying and even upsetting at times.

Patent Issued for Methods and Systems for Detecting Rootkits

01/16/2013 22:31 (Equities.com)

Symantec Corporation NewsRx.com By a News Reporter-Staff News Editor at Electronics Newsweekly -- A patent by the inventors McCorkendale, Bruce (Manhattan Beach, CA); Satish, Sourabh (Fremont, CA); Sobel, William E.

Cyber Newsflash for January 2013 (cont')

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

Utah health department reports another data breach, says contractor lost personal information

01/16/2013 19:17 (Pendleton Times-Post)

We also have more stories about: (click the phrases to see a list) Subjects: Data privacy (9) Computer and data security (16) Technology issues (82) Government pensions and social security (96) Computing and information technology (153) Government-funded health insurance (322) Government programs

Kaspersky Lab's "Red October" cyber-espionage saga leaves lots of questions unanswered

01/16/2013 19:16 (ComputerWorld)

Moscow-based anti-malware firm Kaspersky Lab says it's uncovered a years-long cyber-espionage campaign using phishing to target individuals in business, research and government offices mainly in Russia and Eastern Europe to steal sensitive data. This cyber-spy operation is also suspected to be run b

Air Force cuts imminent

01/16/2013 18:00 (Oxford Press)

A "definitive plan" is expected by late this week or early next week

Firewall Passes Tough Testing

01/16/2013 17:32 (Isssource.com)

When the SCADA Security Scientific Symposium (S4) convenes in Miami every year, the security world expects to hear about how various systems, products or devices have huge gaping holes.

Cyber security on a tight budget

01/16/2013 14:56 (WBTV 3 News)

CHARLOTTE, NC (WBTV) - The "bad guys" go where the action is. Your press release of a recent achievement, award, or expanding business catches their eye.

Log audit reveals developer outsourced his job to China

01/16/2013 05:52 (Help Net Security)

Log analysis can reveal a lot of security mistakes and fails, but a lot of security sins, too. Take for example the incident recently shared by Verizon's Risk Team: called in by a critical infrastructure company to investigate what seemed to be a breach of its networks by the hands of Chinese-based…

Cyber Newsflash for January 2013 (cont')

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

'Convincing' scam circulates IU email accounts

01/16/2013 00:54 (Indiana Daily Student)

Phishers are targeting IU students, staff and faculty in what University Information Security officials called a "convincing-looking" email scam. The message, which uses the IU logo and correctly cites the name of University Information Technology Services, prompts recipients to follow a link to a

Zaxby's Warns of Credit/Debit Card Security Breach

01/15/2013 22:51 (WNCT)

GREENVILLE, N.C. (WNCT) - A fast food chain is dealing with a major security breach, and they're warning you to keep an eye on your bank statement. Zaxby's says if you've used a debit or credit card at some of its stores, hackers might have had access to your information.

Hackers target netizens using Java Script

01/15/2013 21:54 (LocalNews8.com)

POCATELLO, Idaho - The United States Department of Homeland Security is urging people to be careful if they have they are running the computer programming script commonly known as Java.

Twitter urged to sign up to cyber-bullying guidelines

01/15/2013 21:41 (The Guardian)

Prime Minister Julia Gillard has called on social media giant Twitter to sign up to new guidelines for dealing with complaints on social networking sites.

Mobile devices, social networks to remain security targets in 2013: Sourcefire

01/15/2013 21:41 (ComputerWorld Singapore)

The greatest challenge for today's security infrastructure and methods of protection is advanced malware attacks. When having discussions with customers in 2012, Sourcefire A/NZ regional director, Chris Wood, said they were struggling to find effective protection against these threats "without over

Troll alert: 600,000 kids to learn about cyber safety

01/15/2013 20:40 (The Guardian)

A new cyber safety program will teach Australian middle-school students about cyberbullying, keeping passwords private and the dangers of posting embarrassing photos and videos online.

Cyber Newsflash for January 2013 (cont')

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

N.J. businesses should brace for higher cyber security costs, complexity, experts warn

01/15/2013 20:13 (NJ.com)

Cyber security will become an increasingly complex and costly part of doing business, but caution and preparedness is a better alternative than getting hacked or duped by cyber thieves, security experts said today at a conference on the problem.

General News - Anti-hacking law questioned after death of Internet activist

01/15/2013 18:10 (PhillyBurbs.com)

By Aaron Pressman BOSTON, Jan 15 (Reuters) - Lie about your identity on Facebook or delete files from your work laptop before you quit and you could run afoul of a 29-year-old U.

Facebook takes on Google with new search engine that can scan a BILLION profiles to find everything

01/15/2013 18:01 (GA Daily News)

How you search Facebook is about to change. In fact, just the act of searching Facebook is probably about to start. Facebook is trying to give Google a run for its money, with a new product called "Graph Search.

Oracle says Java is fixed; feds maintain warning

01/15/2013 17:46 (Daily Journal Online)

Oracle Corp. said Monday it has released a fix for the flaw in its Java software that raised an alarm from the U.S. Department of Homeland Security last week.

Malware infects US power facilities through USB drives

01/15/2013 16:38 (Computerworld)

ICS-CERT recommends power plants adopt new USB practices

Cyberstalking is a Real Crime: One in Five Americans Affected by Unwanted Contact

01/15/2013 16:18 (TulsaCW.com)

/PRNewswire-USNewswire/ -- The National Cyber Security Alliance (NCSA) and McAfee today released survey data in light of Annual Stalking Awareness Month indicating that 20 percent of Americans have been affected by cyberstalking, persistent emails, and other unwanted contact.

Android Botnet Infects 1M+ Phones in China

01/15/2013 13:03 (Threat Post)

Up to a million Android users in China could be part of a large mobile botnet according to research unveiled by Kingsoft Security, a Hong Kong-based security company, this week.

Cyber Newsflash for January 2013 (cont')

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

Java still risky, even after security update: US [TradeArabia]

01/15/2013 05:31 (Equities.com)

Washington Al Bawaba Ltd. The US Department of Homeland Security warned that a security update of Oracle Corp's Java software for Web browsers does not do enough to protect computers from attack, sticking to its previous advice that the program be disabled.

Oracle says Java is fixed; feds maintain warning

01/15/2013 05:10 (Daily Record (AP))

LOS ANGELES (AP) - Oracle Corp. said Monday it has released a fix for the flaw in its Java software that raised an alarm from the U.S. Department of Homeland Security last week.

Compliance auditing: The first step to cyber security

01/15/2013 04:17 (Help Net Security)

Assuring that your company complies with industry standards is imperative. Being compliant not only heightens your reputation and allows you to trade in some industries, it also gives your clients confidence in your ability to secure their data.

Firm alleges cyberspy network

01/15/2013 02:55 (The Boston Globe)

Effort infiltrates geopolitical sites mainly inRussia

Malware Infects Two Power Plants Lacking Basic Security Controls

01/14/2013 21:22 (Threat Post)

During the past three months, unnamed malware infected two power plants' control systems using unprotected USB drives as an attack vector. At both companies, a lack of basic security controls made it much easier for the malicous code to reach critical networks.

Web Activist's Suicide Highlights Tech Law

01/14/2013 19:34 (The Wall Street Journal)

The suicide of Internet activist Aaron Swartz has set off a round of questions about whether federal prosecutors are too aggressive in pursuing cases of computer crimes committed for idealistic reasons.

DHS: Infrastructure Attacks on Rise

01/14/2013 16:56 (Isssource.com)

Power, water, and nuclear systems in the U.S. are increasingly under attack by cybercriminals seeking to gain access to critical infrastructure. The number of attacks reported to the U.

Cyber Newsflash for January 2013 (cont')

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

US has 'responsibility' to support French offensive in Mali, says Panetta

01/14/2013 16:56 (The Hill - Blog)

The White House and Pentagon have a "responsibility" to provide support to French forces looking to push out al Qaeda-linked militants out of northern Mali and ensure the terror group does not gain a foothold in western Africa, Defense Secretary Leon Panetta said Monday.

Fake MSN/Hotmail email alert phishes for user info

01/14/2013 11:07 (Help Net Security)

Despite the fact that spam levels decreased by 53% in 2012 as compared to 2011, targeted spam and phishing attacks via e-mail are on the rise. Some of these campaigns consist of emails that are so effectively crafted that they could fool even some of the more advance users, while others look so obv

Looking back at a year of Microsoft patches

01/14/2013 09:34 (Help Net Security)

Last year Microsoft's Patch Tuesdays featured a total of 83 bulletins, which is a decline from previous years. Since their security efforts impact countless security professionals, we wanted to see what IT security leaders, and Microsoft, think about the patches released in 2012.

Nearly Half Of Mobile Apps Contain Pop-Up Ad Malware

01/14/2013 09:33 (Yahoo! Canada Finance)

Kaspersky Lab Once Again a 'Leader' in Magic Quadrant for Endpoint Protection Platforms

01/14/2013 09:01 (Equities.com)

M2 Communications ENP Newswire - 14 January 2013 Release date- 10012013 - Abingdon, UK - Kaspersky Lab, a leading developer of secure content and threat management solutions, has been named a 'Leader' in the Gartner Magic Quadrant for Endpoint Protection Platforms* for the second year in a row.

Oracle updates Java; experts say bugs remain [TradeArabia]

01/14/2013 05:31 (Equities.com)

Boston Al Bawaba Ltd. Oracle Corp released an emergency update to its Java software for surfing the Web on Sunday, but security experts said the update fails to protect PCs from attack by hackers intent on committing cyber crimes.

Cyber Newsflash for January 2013 (cont')

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

DDoS bank attacks signal new era of cyberwarfare [Computer News Middle East]

01/14/2013 03:47 (Equities.com)

IDG Reporter Al Bawaba Ltd. Cyberattacks on U.S. banks over the last several months reflect a frightening new era in cyberwarfare, according to security expert Darren Hayes, who says that corporations are unprepared to battle such attacks because of a shortage of experts skilled in building effecti

Air Force's sequestration hit would mean less of everything

01/14/2013 03:45 (FederalNewsRadio.com)

The Air Force is mapping out ways to cut out everything but the basics as it draws up plans for how it would handle sequestration. The across-the-board cuts now are scheduled to take place on March 1 after Congress instituted a two-month delay earlier this month as part of the partial agreement on

Bogus Chrome update offers shadow real updates

01/14/2013 03:43 (ComputerWorld Singapore)

Google's recent upgrade of Chrome has sparked a new round of bogus updates of the Web browser from cybercriminals hoping to steal online banking credentials and perform other mayhem.

Increase in targeted spam and phishing attacks via e-mail

01/14/2013 01:55 (Help Net Security)

The threat level in the field of e-mail security increased in 2012 and will continue to do so in 2013 – despite the fact that spam levels decreased by 53% in 2012 as compared to 2011.

Oracle fixes Java flaw after Homeland Security warning

01/14/2013 00:39 (The Boston Globe)

NEW YORK — Oracle fixed a security flaw in its Java software Sunday after the Department of Homeland Security warned computer users to disable the software completely, citing a loophole that allows hackers to take control of their machines.

Better Business Bureau lists top 10 scams of 2012

01/13/2013 22:33 (CJOnline.com)

Each year the Better Business Bureau reports on the previous year's most damaging and prevalent scams so consumers can better recognize the tactics of fraudulent schemers.

Cyber Newsflash for January 2013 (cont')

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

Linkedin.com: Cybersecurity holes in Social Media

01/13/2013 14:19 (Examiner.com - Pennsylvania)

New threats to security are being introduced in cyberspace. The super highway has personal information copied from one network to another and data (and the threat of comprised data) is being exposed.

Government warns on Java as security concerns escalate

01/11/2013 12:07 (Reuters Canada)

Experts: Text message scams trend with consumer spending

01/11/2013 10:54 (WIS News 10)

COLUMBIA, SC (WIS) - By now, you or someone you know has probably received a text message congratulating you on winning a gift card to a major retailer.

Attackers Using Fake Chrome Updates to Lure Victims

01/11/2013 10:07 (Threat Post)

Google patched nearly two dozen security vulnerabilities in Chrome on Thursday and a day later attackers have begun circulating fake Google Chrome updates that actually are part of a scam related to the Zeus botnet and is designed to stael online banking credentials, among other things.

Fake LinkedIn notifications lead to phishing and malware

01/11/2013 09:38 (Help Net Security)

LinkedIn users are once again targeted with a massive and widespread spam campaign that takes the form of a notification about a supposedly received message from a potential new connection: Unfortunately, the offered links - although legitimate-looking - take users to compromised sites that either

Bogus U.S. Airways registration confirmation leads to info-stealing malware

01/10/2013 05:46 (Help Net Security)

A new email spam campaign impersonating U.S. Airways is hitting inboxes, warns Webroot, and the airline's customers would do well to be on the lookout for the following "booking confirmation" email (click on the screenshot to enlarge it): There are obvious spelling mistakes that should alert users

Botnets for hire likely used in US cyber attacks, Iran denies involvement [Computer News Middle East]

01/10/2013 03:44 (Equities.com)

IDG Reporter Al Bawaba Ltd. Evidence collected from a website that was recently used to flood U.S. banks with junk traffic suggests that the people behind the ongoing DDoS attack campaign against U.

Cyber Newsflash for January 2013 (cont')

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

Businesses overconfident about cyber security

01/10/2013 03:01 (Help Net Security)

Recent research from Deloitte has highlighted that firms in technology, media and telecommunications are confident that they are safe from cyber attacks and data security breaches.

Technology can't save businesses from the threat of cyber criminals

01/10/2013 02:43 (Equities.com)

TOM BURTON City AM BRITAIN's national security is in peril. According to a report released yesterday by the House of Commons Defence Select Committee, the threat to British IT systems from cyber attack is both rapidly evolving and increasingly significant.

Banks crack down on cyber-based account takeovers

01/10/2013 01:48 (ComputerWorld Singapore)

U.S. banks and their customers are doing a better job of protecting themselves against cyberattacks that result in thieves taking over commercial accounts, according to a survey released by the Financial Services-Information Sharing and Analysis Center.

The six most common identity theft risks at tax time

01/10/2013 01:29 (Ashton Gazette)

(BPT) - Tax time is always tough. Whether you will owe or anticipate a refund, plan to do your own taxes or pay a professional to do them for you, preparing and filing your taxes can be a tedious task.

President signs $633 billion National Defense Authorization Act into law

01/10/2013 01:01 (Fort hood sentinel)

WASHINGTON - President Barack Obama signed the $633 billion fiscal 2013 National Defense Authorization Act into law Jan. 2. The legislation, which cleared Congress last month, authorizes the department to act in any number of instances.

How vulnerable is US to cyberattack in 2013?

01/09/2013 23:39 (Alaska Dispatch)

The phalanx of cyberthreats aimed squarely at Americans' livelihood became startlingly clear in 2012 – and appears poised to proliferate in 2013 and beyond as government officials, corporate leaders, security experts, and ordinary citizens scramble to devise protections from attackers in cyberspace.

Cyber Newsflash for January 2013 (cont')

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

Cyberattack could leave UK 'fatally compromised', MPs warn

01/09/2013 22:27 (ComputerWorld Singapore)

A major cyber-attack on the UK could leave the UK's armed forces "fatally compromised" without a viable 'plan b' a committee of MPs has warned the Government.

Drive-by attacks, Trojans and code injection the biggest threats, says ENISA

01/09/2013 22:27 (ComputerWorld Singapore)

Cybercriminals will are turning their attention to mobile platforms, cloud computing, social media, critical and trust infrastructure and even big data, according to European Security Agency ENISA's annual and now rather depressing summary of security industry opinion.

Japanese Police 'Collar' Cat Carrying Malware Code

01/09/2013 22:15 (Threat Post)

A hacker, or possibly group, that's issued terrorists threats using remotely controlled computers in Japan remains at large despite a rare 3 million yen bounty and continuous games with media and police.

Researchers Bypass Microsoft IE Fix

01/09/2013 17:56 (Isssource.com)

Microsoft is facing a Zero Day with Internet Explorer and while they work to patch the issue, they developed a workaround. The problem is there is a workaround around the workaround.

Cyber War Stakes Rising

01/09/2013 14:52 (Isssource.com)

By Richard Sale U.S. intelligence officials today warned as nation-sponsored cyber warfare goes mainstream this year, attacks on U.S. installations and institutions could result not just in damage and theft but in fatalities.

Yahoo now offers SSL

01/09/2013 14:18 (IT World Canada)

Military IT dependence could result in fatal cyber attacks

01/09/2013 05:49 (Help Net Security)

This week, MPs on the Defence Select Committee have produced a report stating that the UK's armed forces are now so dependent on IT that they could be 'fatally compromised' by cyber attacks.

Cyber Newsflash for January 2013 (cont')

Highlights of CYBER CRIME and CYBER WARFARE Newsclippings from All over the Globe

Congress revises DoD's sequestration starting point

01/09/2013 03:44 (FederalNewsRadio.com)

Having been granted a brief reprieve from automatic budget cuts, Pentagon planners are crunching a new set of numbers. The deal Congress and the White House struck last week created a two month delay in the cuts that were due to take place on Jan.

U.S. Army, U.S. Air Force and DISA Ink Agreement with Microsoft [Travel & Leisure Close - Up]

01/09/2013 02:13 (Equities.com)

ProQuest Information & Learning Microsoft announced that the U.S. Army, U.S. Air Force and Defense Information Systems Agency (DISA) are expanding access to Microsoft solutions by entering into a transformative three-year Joint Enterprise Licensing Agreement for enterprise licenses and software ass

Bank Hacks Were Work of Iranians, Officials Say

01/09/2013 01:53 (CNBC)

The attackers hit one American bank after the next. As in so many previous attacks, dozens of online banking sites slowed, hiccuped or ground to a halt before recovering several minutes later.

Firefox 18 delivers a jolt of speed to Web apps and games

01/09/2013 01:47 (ComputerWorld Singapore)

We've known for some time now that Firefox 18 would bring some significant speed improvements to Mozilla's popular browser, and the final version-released today-made good on that promise officially.

U.S. Agency Dismantles Massive International Cyber Theft Conspiracy

01/09/2013 01:27 (Claims Journal)

A Chinese national pleaded guilty Monday to conspiracy to commit criminal copyright infringement and wire fraud. The individual operated a website used to distribute more than $100 million worth of pirated software around the world, making it one of the most significant cases of copyright infringeme

Tech pioneer John McAfee uses low-tech social engineering to spy on Belize heavyweights

01/08/2013 23:07 (ComputerWorld)

Antivirus pioneer John McAfee spins tales of a Hezbollah plot to smuggle toxic powder into the U.S. that he uncovered when he spied on Belize officials in hopes of getting dirt on them in retaliation for their raiding his island home there, shooting his dog and stealing his stuff.

THE BEST DEFENSE IS OUR DEFENSE

With AppRiver, you can build layers of protection against hackers, spammers, scammers and online crooks. AppRiver's services are easy, effective and affordable. Plus, all of them come with a 30-day free trial and 24/ US-based Phenomenal Care.

Spam & Virus Protection • Web Security • Email Encryption • Secure Exchange Hosting

appriver®
Email & Web Security Experts™

www.appriver.com
sales@appriver.com
(866) 223-4645

Certification Training

CCCure.org Leads the Pack for CISSP® and CEH® Training Support

We're really pleased to be working with CCCure.org. Did you know that more than 150,000 people have used the CCCure's resources over the past 12 years to reach their certification and career goals. CCURE.org offers some of the most complete and relevant quizzes for the CISSP® and the CEH® certifications.

CCCure.org also has over 1600 questions for the CISSP® and many hundreds of questions for the CEH®. You can track your progress and they also offer the ability to review questions you have missed. You can compare your score with others taking tests. They also have thorough explanations with each question. You can also drill down on your weak topics and identify what you don't know.

The CCURE.org quizzes are constantly being updated, revised, with new content added almost daily. Like CCCURE.org, we at CDM do not believe in static quizzes that are updated only once every few years. This makes them one of ourstanding picks for the month. Being online you can access with the platform of your choice and you are not restricted to only one operating system. All you need is a browser to access. So what are you waiting for and go check 'em out…Click here.

NOTE: Send an email to clement.dupuis@gmail.com mentioning you saw CCCURE.org in CDM's Cyber Warnings newsletter and Clement will send you a copy of his Scenario Based questions practice test for FREE. This is a value of $59.99 The real exam contains many scenario based question, get ready for this special format, CCCURE.org is the only vendor providing such type of quizzes.

(Sources: CDM and CCCure.org)

RSA® Conference 2013

Register Today!

RSA® Conference is helping drive the information security agenda worldwide with annual industry events in the U.S., Europe and Asia. Throughout its history, RSA Conference has consistently attracted the world's best and brightest in the field, creating opportunities for conference attendees to learn about IT security's most important issues through first-hand interactions with peers, luminaries and emerging and established companies.

Join us at RSA Conference 2013 Feb 25 – Mar 1 in San Francisco and access over 275 sessions across 22 tracks, including 7 new ones like CISO Viewpoint, Security Mashup and Human Element. Hear lively Debates and attend special government sessions like The FBI and the Private Sector: Safeguarding our Cyber Security. Register today and see why others in the infosec community continue to attend year-after-year.

Register Now >>

(Sources: CDM and RSA Conference)

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:

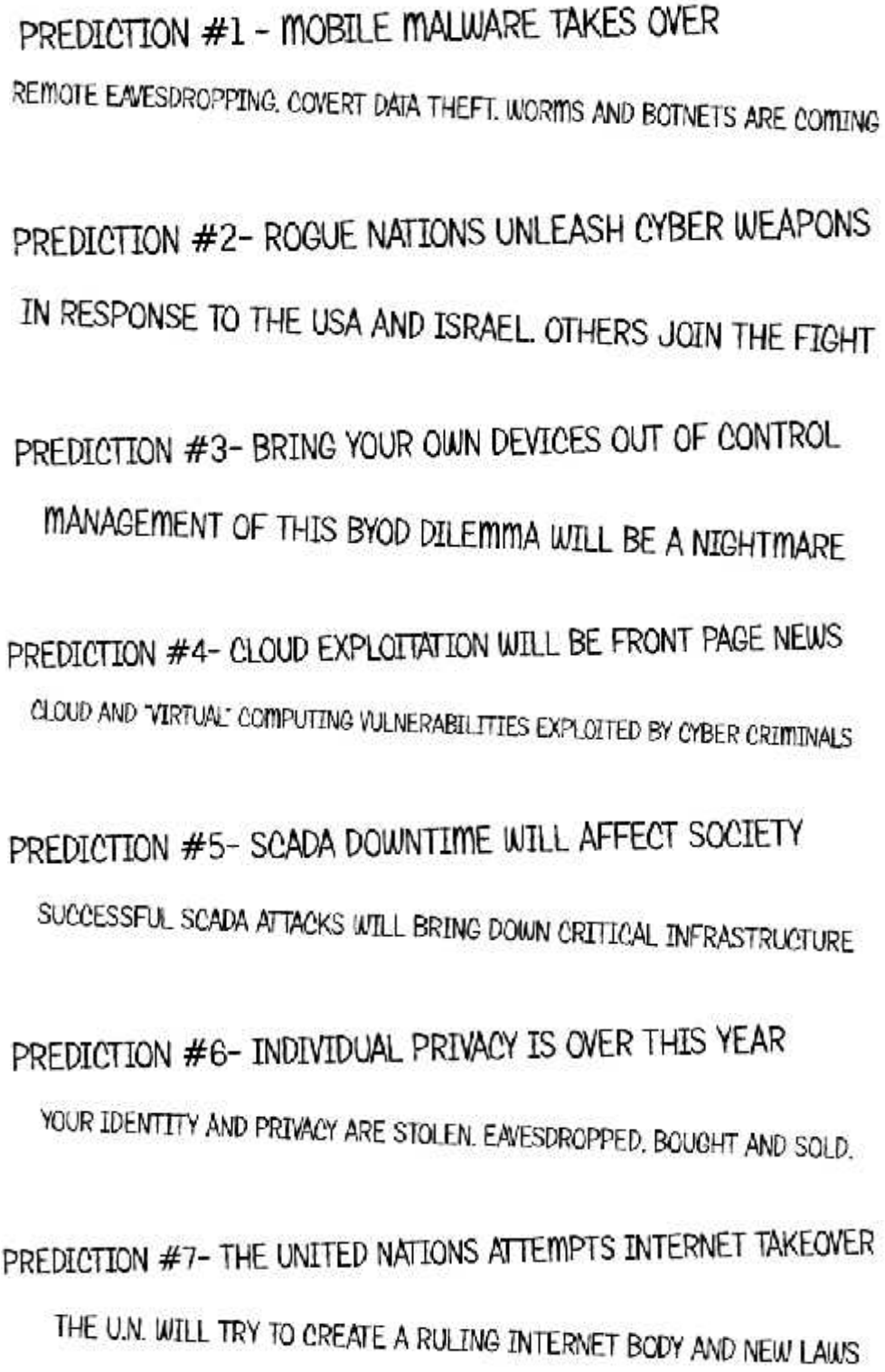
1. TrueCrypt.org – The Best Open Encryption Suite Available
2. OpenSSL.org – The Industry Standard for Web Encryption
3. OpenVAS.org – The Most Advance Open Source Vulnerability Scanner
4. NMAP.org – The World's Most Powerful Network Fingerprint Engine
5. WireShark.org – The World's Foremost Network 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)

Cyber Crime and Cyber War Predictions for 2013



By Gary S. Miliefsky & Pierluigi Paganini. Read the full article in Cyber Defense Magazine during RSA Conference 2013.

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

Cyber Defense Test Labs Review: Emsisoft Anti-Malware 7.0

Introduction

Cyber Defense Magazine (CDM) launched the Cyber Defense Test Labs (CDTL) to test and highlight some of the lesser known anti-virus players and next generation anti-malware solutions on the market. While some are much less significant in size, like Emsisoft, who prides themselves on being one of the leading 'virtual' companies in INFOSEC, with engineers spread throughout the globe, they remain lesser known brands like Symantec and McAfee, yet their products outperform and outshine these bigger brands. What we like most about Emsisoft is how easy the product installs, how quickly it runs and how little 'footprint' it takes during scanning and malware blocking operations. Please read on and learn more about Emsisoft in their award winning product review.

Company Snapshot

Emsisoft was founded in 2003 with lots of anti-trojan, anti-keylogger and firewalling experience including the acquisition of the Online Armor firewall. The company has been growing slowly and organically through revenues only, with no sources of outside funding. This is our Editor's favorite model – sweat equity and gaining happy customers who then spread the news via word of mouth. Same model we are using to build Cyber Defense Magazine. This is only one of the many reasons this product suite has been selected as Editor's Choice. The company is registered in Salzburg, Austria, however, leveraging the 'virtual office' model and telecommuting so popular in Europe, Emsisoft employees are spread around the world. With full-timers, freelancers, part-timers and contractors, Emsisoft has 22 team members. With slow and steady growth, Emsisoft has millions of downloads of their software in 2012. While they are still one of the smallest vendors and the underdog, they have done things that companies with thousands of employees in the INFOSEC space have been unable to accomplish.

Customer Service

They offer customer service in 11 different languages (English, German, Russian, Spanish, French, Italian, Portuguese, Greek, Dutch, Polish and Romanian) via email, but also via phone and remote connection on demand. They guarantee within 24 hours response time and their customer satisfaction level is very high. When it comes to "EMERGENCY" malware infection removal, they do a wonderful job – they passionately enjoy helping folks get rid of infections (and learning how to improve their product in the process), so Emsisoft also offers a free of charge service on our support forum to help getting rid of any infection. Emsisoft actually believes that it is wrong to charge people in such high stress

level situations. If they are convinced by the capabilities of the support team and the malware removal products and services, Emsisoft believes good potential customers will purchase a license afterwards anyway – this is also another reason why they have made Editor's Choice this year. What a wonderful philosophy they've put into action. Talk about a 'positive' charma approach to cleaning up malware. As a result, they have very passionate customer reviews and testimonials throughout the web. If you just search 'Emsisoft positive reviews' you'll see many.

Customer References

While they won't name any customers, they are mostly focused on the CONSUMER and are just now expanding into the small to medium size (SMB) market with the beta version of their centralized command center, called the Emsisoft Enterprise Console. Many of their consumers who have experienced an infection found that they did not have to wipe the hard-drive to remove the malware using Emsisoft and throughout the web you will find very positive reviews, comments and feedback.

Malware Database, Updates, Scanning and Blocking

Emsisoft Anti-Malware uses two scanner engines. One is licensed from Bitdefender and the other is now officially their own scanner engine that specializes in detecting the harder malware traces to find and remove while the Bitdefender engine does a great job finding and catching the more popular malware infections. On top of Bitdefender's MD5 hashed malware signature database, Emsisoft has over 10 million additional unique malware patterns – this is one of the reasons they run so efficiently. They use patterns to detect malware so if you have one of the 100,000 possible derivatives of W32 for example, they only

need a few pattern samples to detect all of these variants. On top of that, Emsisoft updates their database every hour, if there are any changes or improvements, you'll have them very quickly.

Zero-day Malware Detection and Blocking – Strong Multi-scanner Protection

Emsisoft offers frequent, on-demand cloud-based updates, on an hourly schedule. They make claims that this solution can stop all malware including zero-day and it turns out that if you use their product as documented, they may actually be able to hold up to this claim. One of the challenges they face in their attempt to reach this goal is the 'noisiness' of their product in the sense that it can operate in a nearly-paranoid mode, warning you about all malicious behavior including that which we all find acceptable today – such as SKYPE opening ports and operating like covert-channel malware, which technically is mal-behavior. On the bright side, they blocked all the malware we threw at them including many nasty zero-day variants.

Dealing with False Positives – Might Keep You A Bit Busy

You really need to deal with what some might call "paranoid" popups but by doing so, your system remains secure and if you are a geek who enjoys knowing exactly what is happening with your system, Emsisoft knows and tells you, every time. On the scanner and cleanup side you have to be careful quarantining or removing components of trusted applications that trigger alarms with Emsisoft, based on mal behavior. You may trust the program but it may hook the keyboard or install a wierd driver or like SKYPE, open ports without your permission. If a piece of the program ends up in the quarantine, it won't work anymore. You can remove it from the quarantine and you can submit the file directly to Emsisoft so they will review it and decide if they feel that it is a false positive and in one of their

frequent updates they will let you know that they agree with you and will offer to unquarantine the file or files. Because they have millions of users, this happens frequently so you'll get some files optionally unquarantined even if you weren't the one to submit them to Emsisoft for review.

Innovation, Uniqueness and Next Generation

We think Emsisoft has a cutting-edge anti-malware solution. Add the Emsisoft Online Armor firewall to the mix and you have a very "BlackICE" like HIPS engine. Now here's where it can get noisy but it's always to your benefit – it monitors all system areas that might be subject for attacks. If something is changed by unknown software, users will see an alert and can decide how to proceed and store a rule for that decision. However it must be clearly said that HIPS technology is ideal for advanced users by design. The best alert system doesn't help if a novice user just clicks "allow" on each of those 'nasty' alert boxes. As a result, Emsisoft focused on development of a behavior blocking technology, very early in the game. Emsisoft was one of the first vendors that offered a 'working' behavior blocker in Emsisoft Anti-Malware back in 2005 and they also offer a pure behavior blocker product called "Mamutu Behavior Blocker" in parallel. The idea is simple: Each malware behaves in a malicious way, no matter how it does that in technical aspects. A Trojan always sends data, a keylogger always logs keyboard input, a backdoor always open a back door. Their software watches all running programs for such activities in realtime and alerts if something suspicious is done. However the biggest challenge was to reduce the number of wrong alerts caused by good programs that behave very similar to malware to an absolute minimum. After many years of fine tuning Emsisoft claims to have actually cracked the problem and

today they have earned other lab test awards with their behavior blocker when classic signature based detection reaches its limit on zero-day malware attacks.

Free Trials, Platforms, Pricing and Availability

We love free tools, although the hyperlink is subject to change, here is where you will find Emsisoft's trials and free tools:

http://www.emsisoft.com/en/software/download/

Their solutions run on most Windows-only platforms and their pricing is set at market rates. What more could you ask for in malware cleanup for FREE – kudos to Emsisoft for putting together a powerful detection and cleanup suite so we can avoid the all too frequent disk wipe and re-image.

Summary

By living up to their promise of blocking all malware, both known and unknown, combining two best-of-breed multiple anti-malware scanner engines with the constantly updated Online Armor firewall, with a complex graphical user interface (GUI), exposing lots of features and functions, they receive our Editor's Choice Anti-virus Solution Award for 2013.

(Sources: CDM and Emsisoft)

Cyber Defense Test Labs

Next Generation Security Switch Spotlight

Security teams usually use internal Security Information Event Management (SIEMs) to be their watchdog for alarming them about threats and risks behind their firewall. Many have started to deploy complex Network Access Control (NAC) solutions and enhanced Endpoint Security software to detect, alert and block high risk internal network access.

However, most of these alerts happen a little too late. At CDM, we've only seen a few proactive security solutions focused on the actual physical port that the user plugs their Desktops or Laptops into to gain Local Area Network (LAN) access. The HanDreamnet SG2024 is one of the first line-speed, security centric managed switches we've seen on the market. Yes, we actually had to spin the globe and reach far into Asia – South Korea to be exact, to find these innovative switches.

They are now just coming to market in the US and Canada – in fact, Solantus, Inc. – whom you may already know as one of the very few bold and innovative infosec distributors has picked up this product line. Some of the key reasons that we also like this switch fabric is as follows:

1. Lower total cost of ownership (TCO) than Cisco, Juniper or Extreme, among others.
2. No agent-based software to install so you transparently deploy them or replace aging switches.
3. No affect on the network and in fact, these switches are performing at speeds we didn't expect to see, while security functions are all enabled, by default.

4. Real-time detection and blocking of high risk security events at the physical port level.

How beneficial is an internal threat and ddos protecting switch? Here are some real-world examples of deployments in Asia by end-customers of HanDreamnet:

Electronic Semiconductor Manufacturer – Experienced a flooding attack, which occurred internally. Whole manufacturing lines were stopped. All of production material and goods were scrapped. After deploying SG2024 managed switches, the problem was solved and hasn't happened again…one infected system goes instantly offline at the physical switch port level when this kind of problem flares up again. They re-image the system and try to 're-educate' the employee about mal-behavior leading to installation of malware.

Very Large Corporation – Experienced a spreading worm by mobile user's laptop which caused a huge amount of internal traffic flooding. They had difficulty tracking it down to the source and lost an entire day at corporate headquarters because of this fast and wide spreading worm. After deploying SG2024 managed switches, future worm outbreaks were instantly mitigated at the specific ports where they began, before causing peers on the VLANs to become infected or go offline.

Large University – One of the student labs caused a Distributed Denial of Service attack which caused the firewall to lock-up from bulk traffic sessions and they lost internet access for an entire day and evening. Once they replaced their 'big brand name' switches with the SG2024 series they have not encountered any downtime, since, while experiencing frequent 'troublesome' student traffic. This 'troublesome' traffic gets blocked nearly immediately at the physical switch port, protecting the rest of the network.

To learn more about these intelligent managed security switches, please visit http://www.solantus.com.

(Sources: CDM and Solantus)

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 newsletter 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.

Cyber Warnings

Published by Cyber Defense Magazine, a division of STEVEN G. SAMUELS LLC.

Cyber Defense Magazine

848 N. Rainbow Blvd. #4496, Las Vegas, NV 89107.

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

marketing@cyberdefensemagazine.com

www.cyberdefensemagazine.com

Cyber Defense Magazine - Cyber Warnings rev. date: 01/23/2013

CDM

CYBER DEFENSE MAGAZINE

THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Cyber Warnings E-Magazine January 2013

KEY SPONSORS INCLUDE:

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

SecureTheCure.org

IT Security Professionals
Tax-Exempt Non-Profit, helping fund the search for the cure for Cancer and help those in need.

Donate

Tel: 1-210-639-8652
Twitter: @securethecure
Web: www.securethecure.org

SECURETHECURE.ORG IS DEDICATED TO HELPING FIND THE CURE FOR CANCER