CDM
CYBER DEFENSE MAGAZINE™
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

CYBER WARNINGS

MARCH 2013

BEST PRACTICES

FOR INFOSEC

RSA CONFERENCE 2013 TRIP REPORT

MONTHLY CYBER WARNINGS NEWS

NEW WRITERS
MORE TIPS AND TRICKS
OF THE INFOSEC EXPERTS

Contents

CYBER WARNINGS

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

EXECUTIVE PRODUCER

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

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

Credited With Each Article

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

My Second Month as Editor-in-Chief: Overwhelming Cybernews!

From our LinkedIn, Facebook and Twitter messages this month, you've probably noticed we've broken many stories. Meanwhile, our Executive Producer has returned from his annual trek to the greatest INFOSEC show on Earth – The RSA Conference 2013. I don't want to spoil the story for him but I can tell you we're looking at a world record – over 24,000 attendees this year. They had so many vendors that they had to create an extra 'overflow' Expo floor called "Gateway Expo", where many of you were able to pickup copies of our magazine, on the way in to see some of the hot new vendors and winners of the Innovators contest that RSA holds every year. We are thrilled to have tremendous growing hits to our stories on our website and growing subscribers at a fantastic rate. Tell your friends and don't forget, we have lots of giveaways. You or your friends could win some fantastic security products just for signing up – no strings attached. As you may already know, governments are at a not-so-secret war with each other, using the internet as a vehicle to launch their cyberwarfare and cyberespionage initiatives – but who are the actual victims? It seems to me that now is the most important time for each of us to do the following – work together to share best practices and improve our state of personal, business and government security, while also trying to wake up our politicians to the risks and damages of 'going to war' without 'declaring war'. On the internet, a 12 year old can now launch a 'cyberweapon' – with many freely available tools. Just think of the brainpower behind the cyberwarring teams – whether it's the Chinese, the Russians, the US or the Iranians or North Koreans – they have all placed immeasurable resources at these initiatives but what is to keep them in check from harming the citizens – whether it's taking out a power grid or zeroing out bank accounts? It's time we help each other and wake up our public servants and remind them who they work for and what kind of rules were put in place during the Geneva Convention. Enjoy this edition as we focus on BEST PRACTICES across various areas of INFOSEC so you can be one step ahead of a cyber threat – be it from a criminal or a government. *Read, learn, spread the word and enjoy!*

Pierluigi Paganini

Pierluigi Paganini, Editor-in-Chief

Network Analysis Best Practices

Protecting against GIGO, Insuring Compliance, Managing Change

The term GIGO was introduced in the early days of computing meaning Garbage In, Garbage Out. The term originally referred to programming code fed into a mainframe. However, it is just as appropriate in today's networked world. Analysis is only as good as the data being fed into the tool. So, any discussion of network analysis must start with the foundational question; "How to access the network data so that the analysis appliance sees 100% pure and relevant data?" In today's compliance era, this takes on added significance as IT Managers struggle to keep up with reporting and security regulations while managing an increasingly diverse IT infrastructure.

SPAN

There are two primary methods of providing data to an analysis appliance, Switch Port Analyzer ports (SPAN) and Taps. SPAN ports replicate or mirror packets in the switch and direct them to a monitor port where the analysis appliance is connected. SPAN is seen as a simple way to send packets for analysis without disrupting any network link. SPAN access can work well in low bandwidth applications where throughput is well below switch capacity. However, because the SPAN session copies full duplex traffic, a fully loaded 1Gbps link actually can produce 2Gbps of traffic to the monitor port oversubscribing the capability of the port. Note also, that SPAN traffic is the lowest priority traffic in the switch. This will cause all output traffic beyond 1Gbps to be dropped. Because there is no provision for intelligent filtering or load balancing, the packets will be randomly dropped causing unreliable traffic information being passed to the analysis appliance.

The top priority for a switch, of course, is to direct network traffic. Therefore, as the switch reaches capacity, packets to the SPAN port will be dropped. This problem is critical because, just as a need for switch traffic analysis presents itself (packets overrunning switch capacity), so does the condition when the SPAN port will not provide accurate switch traffic information. This is a commonly seen example of Garbage In, Garbage Out.

Even in low utilization environments, there are certain packets such as undersized or error packets that can be filtered on the switch and never make it to the SPAN port. If the analysis requires 100% of packets be submitted to the appliance, SPAN cannot guarantee such accuracy. In this era of required legal compliance in many industries, it is important to be able to document 100% capture with no packet manipulation.

Historically, analysis was primarily a troubleshooting tool. In today's high speed, networked environment, analysis can take on many new functions such as policy management, security, legal compliance, quality of service, customer experience management, policy enforcement and more. As a result of this broad spectrum of analytical applications, there are many specialized appliances that require access to the same data. This often requires more physical connections than SPAN can deliver. This brings us to the second link access technology, Taps.

TAPS

Taps can offer virtually an unlimited number of physical ports for access to network links passing data to analysis, compliance, security and other appliances. The Tap connects two network end points and provides a mirror copy of the traffic passing through the Tap. (See Figure 1 for connection example.) It is important to note that Taps do not analyze packets, change packet timing, alter or otherwise interfere with network traffic. To the network, a Tap looks like a piece of wire. If a Tap loses power, a fail-safe relay will maintain traffic flow.

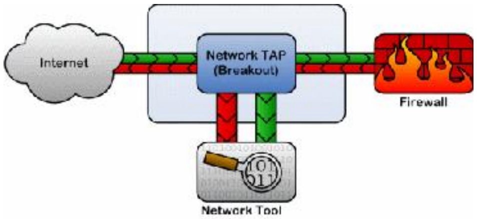


Figure 1

Taps are independent of the network end points making up a link. There are many different points in the network where taps can be inserted offering access to a variety of analysis, compliance and security tools. Some typical tapping points for analysis applications include:

- Between router and firewall for protocol analysis, bandwidth monitoring, traffic trending and packet analysis
- Inside the firewall for LAN analysis, session monitoring and Intrusion Prevention
- Between LAN switches for subnet monitoring or departmental monitoring
- Between LAN switches and access points for user access control, VoIP monitoring or workstation monitoring

Taps also provide flexibility in how they pass traffic to the monitor port. There are four different modes of operation:

- Breakout – A breakout tap operates like the diagram in Figure 1 above. The directional traffic is broken out between two output (monitor) ports. This allows each direction of traffic to be sent to a discreet monitor port at full wire speed. For example, if each direction is operating at a full 1Gbps, the total duplex traffic is 2Gbps. So, not to oversubscribe the monitor port, this method uses two 1Gbps output ports to connect to the analysis appliance eliminating any chance of dropped packets.
- Aggregation – Providing access for applications with lower throughput, Taps can aggregate both directions of the traffic and send the frames to a single monitor

port. This mode can reduce port costs on probes and other analysis appliances by making efficient utilization of expensive analyzer ports.

- Regeneration – As mentioned above, there are often requirements for specialized analysis using a variety of appliances. Regeneration mode allows the same data stream to be sent to two or more monitor ports.
- In-Line or Virtual-In-Line (V-Line) – This is sometimes called By-Pass tapping. In this mode the live network traffic passes through the analysis device real time then back to the Tap. This is used primarily in security analysis appliances such as IPS and DLP. This allows the appliance to see and act on live data as it passes through the network. In this mode, the Tap continuously monitors the analysis appliance for heartbeat and bypasses the appliance if the appliance goes down. This By-Pass feature allows these in-line appliances to be connected without the risk of taking down the network as a result of a software glitch or power loss to the appliance.

Because of a Tap's independence from the network end points, they can mirror 100% of the data to the monitor port. Physical layer errors, error packets, short frames and other packets that might be filtered out on a SPAN session are all passed through Taps to the monitor port(s). This provides the IT Manager with a legally defensible, pure data stream for analysis and reporting. No GIGO. Taps guarantee access to all the data all the time.

Some of the industry trends that are leading IT Managers toward Taps include the massive increase in network bandwidth and throughput with 10Gbps links becoming very common in the data center. In addition to increasing speeds, analysis must often hold up to audits in this era of legal compliance. Recent legislation includes the EU's Data Protection Acts, global banking's Basel iii requirements and the raft of recently introduced US legislation including; the Affordable Care Act (ACA) in healthcare, Dodd Franks in financial services and the yet to be named Cyber Security Bill.

Some current innovations in this technology include drag and drop User Interfaces for ease of configuration and management. Taps are also being combined with port aggregation devices providing efficient port utilization of expensive analytic tools. Taps and port aggregators are also providing advanced filtering and load balancing options that allow optimization of tool performance and improved management of network resources.

IT Managers are increasingly turning to Taps as the preferred method for providing network access to tools. Taps provide access to all the data to ensure accurate analysis. They provide fail-safe operation avoiding risk of network disruption as a result of power interruption or failure of an appliance. Taps can provide simultaneous access to many tools for a wide variety of analytic, security and compliance analysis.

Author: Daniel O'Donnell, Vice President, Business Development, Network Critical

Is your file transfer solution worth the risk?

Best Practices for Secure and Anonymous Browsing

Editor's note: Article written by Dan Gurghian, ibVPN CTO. With more than 10 years of experience in developing online privacy solutions ibVPN is one of the most trustworthy providers on the VPN market.

Everybody knows that the Internet is not the safe and friendly place it should be. Whether you are in a strictly monitored computer network or in a completely free and open one, you need to keep your communications secure and away from prying eyes.

Secure and anonymous browsing is not for everyone and it is not suitable in any situation. However, it is mandatory when you are travelling or accessing the Internet from public locations.

In order to achieve secure and anonymous browsing you need to consider two factors that should work together: *your device* (computer, laptop, smartphone and other device that can connect to the Internet) and *the Internet connection*.

You may secure your device by using firewalls, antivirus/antimalware solution and browsers configurations. The options are quite standard and it is not the goal of this article to get into more details.

Securing the Internet connection may sound complicated, but it is not. Let's start by presenting the most common technical solutions that may be used for your online safety.

	Proxies	**TOR Project**	**VPN service**
How it works	Proxies offer anonymity by acting as an intermediary between your computer and the requested destination (website).	When you use Tor, your Internet traffic travels through several randomly selected nodes from Tor network (run by volunteers), before exiting and arriving at the desired destination.	Encrypts the entire traffic to a server that acts as your personal internet gateway. Basically, it is a proxy with an extra layer of encryption.
Strong points	Easy to use and fair anonymity.	High anonymity.	Strong encryption and high anonymity.
Weaknesses	Encryption is an option, not a standard.	Complicated architecture. Slows down your connection. Suitable for advanced computer users.	May slow down the Internet connection depending on the encryption level.
Supported Operating Systems	Windows, Mac OS, Linux, Android, iOS	Windows, Mac OS, Linux, Android	Windows, Mac OS, Linux, Android, iOS

Proxies

Proxies are used for secure and anonymous browsing for more than 15 years. Basically a proxy acts as an intermediary between your device and the site you are trying to access. A proxy keeps you safe by hiding your real IP address that it actually your online identity.

Proxies may be public or private and come in many flavors. The most common are HTTP proxies, for general purpose browsing, HTTPS for web sites that requires authentication and SOCKS. SOCKS proxies are a versatile solution for anonymous browsing and for anonymous application usage. Many applications can be forced to use SOCKS proxies even if they are designed to connect to the Internet directly.

TOR Project

The usage of **TOR project** is still pretty popular and it is a free solution for secure and anonymous web surfing. Tor can be used for securing the browsing (HTTP and HTTPS traffic) and, with the help of 3rd party applications (most of them open source), for **securing the application usage** like **torrent clients**. The main disadvantage of TOR is that, due to its quite complicated architecture, it significantly slows down your Internet connection.

VPN Services

The usage of VPN is a newer technique and by far is the easiest way to gain access to secure and anonymous browsing. The setup is straightforward even for dummy users and most VPN providers offer one-click applications to easily connect and disconnect to/from the VPN servers.

The VPN is able to encrypt and route all the traffic (generated by browsing or application usage) to a server that will work as your personal gateway to the Internet. The most common VPN protocols (PPTP - *Point-to-Point Tunneling Protocol*, L2TP - *Layer 2 Tunneling Protocol*, SSTP – *Secure Socket Tunneling Protocol* and OpenVPN) are supported by a wide range of devices that can connect to the Internet. The encryption may vary from 128 to 4096 bits and using VPN is the most secure option.

How to secure your Internet connection like a Pro

If you are serious about protecting your online privacy and you want to securely browse the Internet, then **VPN is the answer**. Here are some more tips that you should consider:

- **Do NOT use free proxies**. There is no security behind open proxies and even if they are free there is no guarantee that your traffic is not logged by the 3rd party operating the proxy. There are several companies that offer secure proxies at reasonable prices. You may consider them as an option for lightweight browsing with no or light encryption.
- **TOR is not suitable for extensive usage.** Do not think that the TOR network can be used for high speed Internet browsing, media streaming, online games and other activities that requires large bandwidth. Using the TOR network is free but it is operated by volunteers so there are no guarantees regarding the speed or the reliability.

Disregarding the discussions related to TOR's military background, we are talking about a high secure online privacy network that can be used by anyone.

- **Choose your VPN provider carefully**. There are many providers on the market that offer different packages of services. We recommend testing the trial versions and see if how it works for you and for your devices. Most of the VPN users have more than one device capable of using protocols, like: Windows/MAC/Linux desktops and laptops, iOS/Android devices, gaming consoles, media players and routers. Reading the terms of use and privacy policies is highly recommended in order to know what you can while you are using a VPN server.

Based on your device we recommend the following protocols for best results (high security and good speed):

Operating system	**Recommended Protocol(s)**	**Reason why**
Windows	OpenVPN, SSTP	SSTP is a great option for Windows users as it is very secure. Unfortunately not many VPN providers offer SSTP servers.
Mac OS	L2TP, OpenVPN	L2TP is easy to configure. For OpenVPN protocol one may use Tunnelblick.
Linux	OpenVPN	Easy to install from the command prompt.
iOS	L2TP	L2TP is more secure than PPTP. OpenVPN is not yet a viable option for iOS.
Android	OpenVPN	It is more secure than PPTP and L2TP and there are plenty of Android apps that offer this service.

Don't forget about a **secure browser** with incognito / invisible browsing features. This will disable the cookies used for tracking your online activity.

Consider the tips regarding **secure and anonymous browsing** while:

- *You are using a public (worst case open) Wi-Fi connection from coffee shops, shopping malls, airport or hotels.*
- *You are travelling. There are many geo restricted web sites that will no longer work and the search engines will provide you different search results due to your new location*
- *You do a research project that requires that your identity to be protected*
- *You post / discuss your political, religious or sexual opinions on forums or blogs*

Why it is important to encrypt your Internet connection while you are using a public Wi-Fi connection

If you are regular Internet user, you probably check your emails on public Wi-Fi and when you do that you are tempting fate. With no encryption all your traffic may be intercepted and seen by hackers.

Basically, you should avoid connecting to a public hotspot unless you need it. But if you do, you should ALWAYS use a VPN to protect your data. Also, consider accessing only HTTPS-enabled sites and turning off sharing.

Doing these things will keep most of your data secure when you are just popping in to quickly check your email.

Why it is important to have a VPN connection while you are traveling

When you are traveling the same rules apply as you were connecting from a public Wi-Fi. You may never know who is scanning or intercepting your data traffic, so you need to be a little bit paranoid and encrypt your connection.

Also, if you are traveling abroad, you may need to use the VPN or proxy to watch your favorite show that is only available in your country. Many video streaming sites use the so called *"geo-restriction"* to allow only certain users to access their programs. Take Hulu for example that is only available in United States. A VPN service is able to unblock such geo-restricted websites.

There are also many countries that simply restrict the access to sites like *Facebook, Youtube* or *Twitter*. Even if you are connecting to the Internet from a hotel you won't be able to access such site unless you are you using VPN or other similar solution.

Conclusions

1. These are just a few tips that may bring you important benefits regarding your online security.

2. Some of these methods are more intrusive than others, but the important thing is that they all give *you* control over how you experience the web.

3. With a little effort and the right tools, you can be protected while surfing the Internet. Additional benefits, like bypassing restricted websites, are highly appreciated by a lot of users around the World.

Best Practices for Secure Email and Secure File Transfer

By Dr. Guy Bunker, SVP Products, Clearswift Ltd.

Email continues to be the lifeblood of organizations today. With changes to legislation and the increased attention on data breaches now is the time to revisit your email solution and policies to improve the security of the information that flows through it – both inbound and outbound.

While it has been commonplace to have anti-virus scanning and anti-spam on the incoming email stream for many years, we are only just beginning to see improved security around outbound email, through the Increased use of encryption and deployment of data loss prevention (DLP) solutions. The reason for this is two-fold; the first is understanding the benefits and differences of the myriad of options available. The second is around the cost and ease of use for the solutions. In the past, both encryption and DLP solutions have been notoriously difficult to configure and maintain, making them only options for larger organizations with specialist IT skills.

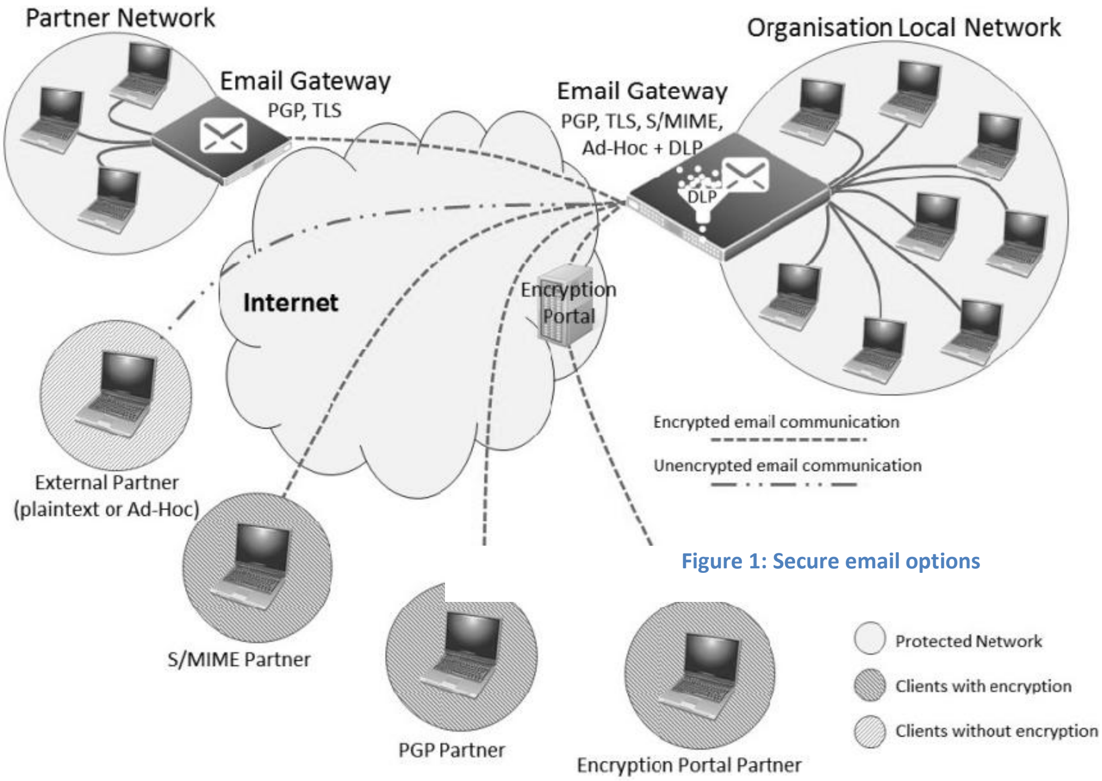


Figure 1: Secure email options

Today's solutions to make email secure have become increasingly sophisticated, but hide the complexity and driving down the management costs, see Figure 1. And yet, there is no silver bullet. Choices have to be made. The real answer is that different solutions are needed at different times and the decision as to which is needed needs to be made automatically - based on the recipient and the information being communicated.

Encryption

Let us start with encryption. Encryption is used to ensure that the contents of an email are not intercepted and read, particularly when it travels outside the organization. Therefore, the ideal place for encryption to occur is on the egress point, as the email enters or leaves the organization. Today's email gateways which protect against inbound threats can also provide automatic encryption of outbound email. There are several different encryption options available, see Table 1 and further explanation on the different types is given below.

	Encrypted Site-to-Site	Encrypted Site-to-Recipient	Encrypted Desktop-to-Desktop	Standards Based	Crypto Strength	Key Exchange or Password	Recipient Transparency
TLS	Yes	No	No	Yes	Medium	No	Yes
S/MIME, PGP	Yes	Yes	Yes	Yes	High	Yes	Site to Site - Yes Encrypted to Recipient may require key and client plugin
Password (Windows)	No	Yes	No	Yes	Medium	Yes	Yes
Password (AES)	No	Yes	No	Yes	High	Yes	Requires Zip package that supports AES256
Portal	No	Yes	No	Yes	High	No	May require plugin for "push" messages

Table 1: Options for Email Encryption

Transport Layer Security (TLS)

For users who simply require encryption on messages between themselves and other organisations, a TLS capability can be used. TLS connections can be 'opportunistic', allowing encrypted messages sent in this mode to automatically seek out and favour a connection using TLS. Alternatively, connections between organisations can be mandated and have pre-specified encryption strengths.

Message Encryption (S/MIME, PGP and Password protected zips)

Good encryption solutions support international standards for OpenPGP and S/MIME message formats, enabling communications between recipients who use standard email clients such as Outlook, Outlook Express and Notes.

Sophisticated email gateways can also use S/MIME and OpenPGP to create policy based secure connections between Gateways or from Gateways to Recipients. With integrated encryption, email gateways can decrypt messages and then use the other tools such as anti-spam, anti-virus and content filtering engines to ensure that communications adhere fully to corporate email policy.

Ad-Hoc Encryption

For recipients who use neither PGP nor S/MIME, the new generation of email gateways can still send messages in a secure format using password protected zips, aka ad-hoc encryption. Even here there are options on whether to use Windows compatible or AES encrypted zip formats.

Windows compatible zip formats can be opened without the need for any additional software. However, for organisations requiring stronger encryption algorithms, for example AES256, there is a need for the recipients to have one of the many Zip clients capable of processing this format.

Passwords created during the ad-hoc encryption process can be dynamically created for individual users or message-specific. In many cases it is then the responsibility of the sender to inform the recipient of the password, but some systems enable a delayed email to be sent automatically to the recipient.

Web Portal based encryption (Pull, Push)
Finally, given that the technological savvy of your intended recipient can often dictate which method of encryption you use and portal based encryption is an easy-to-use method requiring no knowledge of encryption. Encrypted email messages are sent using an encryption portal which can then be opened on all types of devices, from PCs to phones and tablets using a web browser. When this method is invoked the user receives an email to say that they have received an encrypted message through the portal.

Data Loss Prevention

For some information, even email encryption is not sufficient – this information needs to be kept within the organization at all times. For this, data loss prevention (DLP) technologies need to be used to watch for restricted information crossing the egress points and automatically blocking it. A DLP solution enables an organisation to inspect the content of an email and its attachments looking for specific information and then carrying out an action on the email should the information be found.

One simple use-case is to block any email leaving the organization which contains profanity, while other more sophisticated policies may look for credit card or bank information and prevent that from leaving the organization. As with email encryption solutions, the simplest place to implement DLP is at the egress point, on the email gateway. By putting the solution on the gateway, rather than every computer, all devices which are connected to the corporate network are protected.

Web Based Email

For many organizations, when it comes to information security, there is now a need to consider web based email as well as corporate email. Most organizations now require that employees use their work email for work, and work alone – the result is that employees frequently maintain a personal email address for use with friends and for other social reasons. However, the rise of personal email has also resulted in a rise in corporate information risk, with employees sending critical information to their home email accounts (more often than not so they can work on the document at home). When looking at securing corporate information, this communication channel needs to be considered.

A gateway solution which intercepts all web based traffic (as well as traditional corporate email) is an excellent way of ensuring that corporate information remains inside the corporation. The same DLP policies which are used for corporate email can also be used for web based email (and for other web based activities, such as social networking). Having consistent information security policies and technology to enforce them, makes it easier for the IT department and the CIO or CISO who is ultimately responsible for corporate information to define common policies and view any violations.

Secure File Transfer

When it comes to very large files, typically those over 1GB, email is not an option for effective transfer and an alternative needs to be sort. While this size issue has not been an issue for most organisations, the advent of video and rich media means that it is increasingly becoming an issue. Several mechanisms can be used to transfer the file with FTP (File Transfer Protocol) probably the most common as it is easy to use. FTP transfers the file from source to destination – but without any forms of security check. Whereas information sent through email can be scanned for viruses and other malware inbound and have data loss policies applied when outbound - this does not occur with standard FTP. Enter the secure file gateway which enables secure file transfer. In essence this inserts the policies and technology used in email to protect the content into file transfer mechanisms such as FTP. The processing can be completely transparent, automated by the file gateway with the user being unaware of the content inspection being carried out.

Secure file gateways have been used for several years within the defence sector, where information needs to be transferred from one network with one security clearance to another with a different clearance level. However, they are now being increasingly used in the commercial sector, enabling secure transfer of files between partners and increasingly inside organisations which want to segregate information internally. Guaranteeing that only information which complies with policy is shared with other parts of the organisation.

Summary

Email continues to be a critical business tool for organizations big and small. Almost all an organisations intellectual property and company confidential information will travel through email at some point in its lifecycle. This coupled with increased needs for collaboration, imposed legislation and cyber-attacks on corporate information means that organisations need to revisit their email security polices and solutions to protect their critical information. An increased emphasis on Information Governance, the understanding and protection of information, especially that which flows in and out of an organization, is driving even the smallest organization to look to new technologies for securing email.

In the past secure email technology required specialist skills to administer, but today even the smallest of organisations can readily encrypt their email and apply DLP policies without increasing management costs. The same security policies which are applied to corporate email can also be applied to web based email by using combined web and email gateways, giving organisations the assurance they need that their information is secured no matter which communication channel is used.

Furthermore, the advent of web based collaboration tools and very large files means that organisations need to look at secure file transfer technologies to enable the same policies that are applied to email to also be applied to files as they are moved between organizations or even departments.

The offer of Russian Underground for Phishing Campaigns

By Pierluigi Paganini, Editor-in-Chief

Security experts consider the analysis and study of underground crucial to better understand the way cybercrime use to operate and which are the most prolific monetization processes.

The knowledge of underground black markets gives to security researchers precious information on the business model adopted by cyber criminals and on the evolution of principal cyber threats.

Russian underground is considered one of the most interesting and prolific black market, cyber criminals provide a wide range of illegal services to organize sophisticated scams and provide all necessary tools to arrange a cyber attack.

In the underground it is possible to acquire a malicious agent, rent hosting services to deploy compromised web site or to outsourcing a DDoS attack.

In the last months Trend Micro published an excellent study in Russian Black market demonstrating that it is possible to acquire every kind of tools and services to realize cyber criminal activities and frauds.

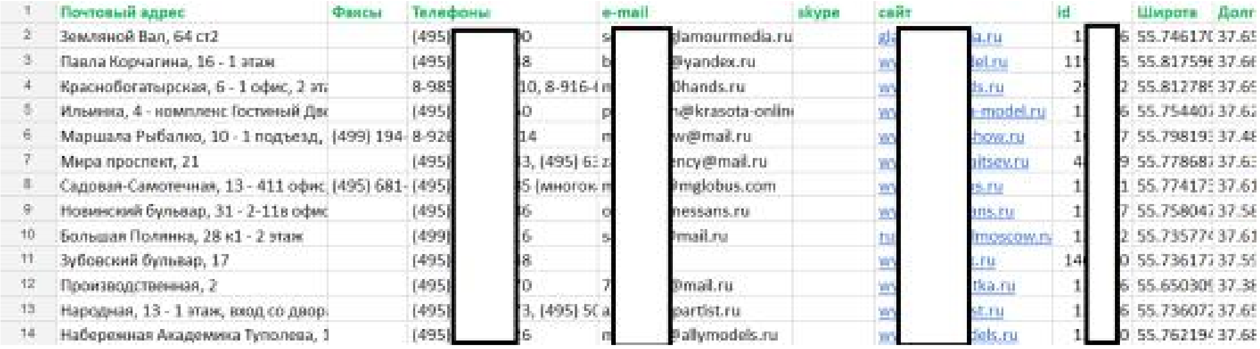
The top 10 activities included software designing, spam and flooding services, hacking, server sales and hosting, denial-of-service attacks, pay-per-install services for downloads and traffic, file encryption, malware, and exploit writing.

1. Programming services and software sales
2. Hacking services
3. Dedicated server sales and bulletproof-hosting services
4. Spam and flooding services, including call and SMS flooding services
5. Download sales

6. DDoS services
7. Traffic sales
8. File encryption services
9. Trojan sales
10. Exploit writing services and sales

Recently I read many posts of famous security researcher Dancho Danchev, a great experts of cybercrime that in various articles revealed the mechanism behind the process to arrange a spear phishing attack among Russian cybercrime.

Recently Danchev wrote on an underground market advertisement that offers access to data to sensibly increase click-through rate for a spear phishing campaign as illustrated in the following picture:



1	Почтовый адрес	Факсы	Телефоны	e-mail	skype	сайт	id	Широта	Долг
2	Земляной Вал, 64 ст2		(495)[redacted]0	s[redacted]glamourmedia.ru		gla[redacted]a.ru	1[redacted]6	55.74617	37.65
3	Павла Корчагина, 16 - 1 этаж		(495)[redacted]8	b[redacted]@yandex.ru		ww[redacted]del.ru	11[redacted]5	55.81759	37.66
4	Краснобогатырская, 6 - 1 офис, 2 эт		8-985[redacted]10, 8-916-	m[redacted]0hands.ru		ww[redacted]ds.ru	2[redacted]2	55.81278	37.65
5	Ильинка, 4 - комплекс Гостиный Дв		(495)[redacted]0	p[redacted]n@krasota-onlin		ww[redacted]-model.ru	1[redacted]6	55.75440	37.62
6	Маршала Рыбалко, 10 - 1 подъезд,	(499) 194-	8-926[redacted]14	m[redacted]w@mail.ru		ww[redacted]how.ru	1[redacted]7	55.79819	37.48
7	Мира проспект, 21		(495)[redacted]3, (495) 6	z[redacted]ency@mail.ru		ww[redacted]aitsev.ru	4[redacted]9	55.77868	37.63
8	Садовая-Самотечная, 13 - 411 офис,	(495) 681-	(495)[redacted]5 (многок	m[redacted]@mglobus.com		ww[redacted]es.ru	1[redacted]1	55.77417	37.61
9	Новинский бульвар, 31 - 2-11в офис		(495)[redacted]6	o[redacted]nessans.ru		ww[redacted]ans.ru	1[redacted]7	55.75804	37.58
10	Большая Полянка, 28 к1 - 2 этаж		(499)[redacted]6	s[redacted]@mail.ru		ru[redacted]lmoscow.ru	1[redacted]2	55.73577	37.61
11	Зубовский бульвар, 17		(495)[redacted]8	[redacted]		ww[redacted]s.ru	14[redacted]0	55.73617	37.59
12	Производственная, 2		(495)[redacted]0	7[redacted]@mail.ru		ww[redacted]tka.ru	1[redacted]6	55.65030	37.38
13	Народная, 13 - 1 этаж, вход со двор		(495)[redacted]3, (495) 5	a[redacted]partist.ru		ww[redacted]st.ru	1[redacted]6	55.73607	37.65
14	Набережная Академика Туполева, 1		(495)[redacted]6	m[redacted]@allymodels.ru		ww[redacted]dels.ru	1[redacted]0	55.76219	37.68

Very interesting is sales model implemented by cybercriminals and the way they composed the offer trying to respond to the “customer’s need”, the “spam leads” included in fact precious information such geographic data, market segment and company information, all the necessary to customize the attacks.

Security community is aware that crime is evaluating the possibility to provide data and tools to do illegal activities instead directly them, a change respect the past when cyber criminals directly used the information for personal instead to sell it.

Millions of harvested emails are offered for sale on the black market, what is concerning is that within the huge quantity of information it could be possible to find data related to government and intelligence agencies, military representatives an government contractors.

Professional hackers could benefit of the offer of entire database containing harvested/compromised data, the information are easily accessible and allow hackers to sensible reduce the phase of information gathering on the targets.

A dangerous phenomenon that is consolidating is the attitude to emerging DIY (do it yourself) trend within underground, novice cybercriminals try to make business with illegal activities outsourcing services (e.g. malware hosting) and acquiring tools and data. The number of this individuals is rapidly exploded and the motivation are various from cybercrime to hacktivism.

Cyber criminals have various options to collect data to resell later, let's think to fraudulent offers that target receive to improve their visibility on line or within a specific business sector. Adopting this tactics criminals are able to build huge collection of data also indexable on various axis of analysis. Cyber criminals, but also state sponsored hackers, could targets specific sectors or individuals using this technique acquiring information to use for large-scale spear-phishing campaigns.

Of course cybercrime has a wide range of weapons in its arsenal to get the information for resale, among them the use of malware is certainly the most invasive and dangerous. It's very easy to infect huge quantity of machines with malicious code able to steal any kind of information from victims. In the underground many serviced provide all necessary to spread malware to wide audience with very cheap costs.

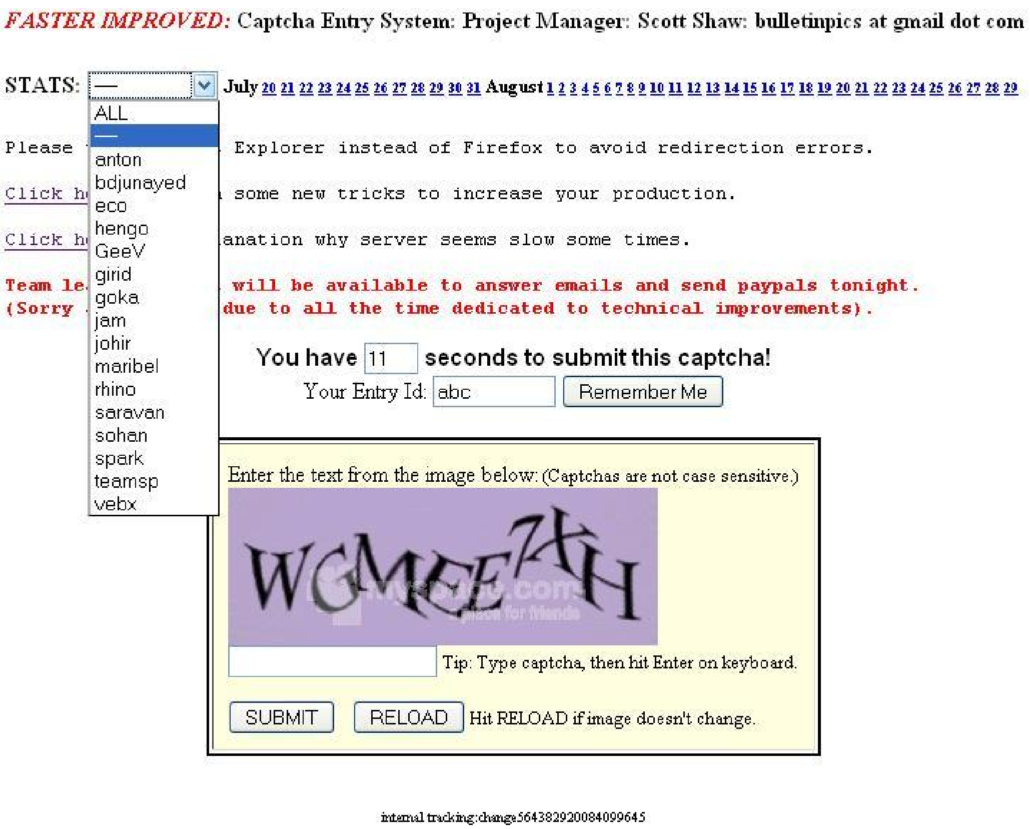
Recently the activities of C2C (cybercrime to cybercrime)

Recent investigation demonstrated a mutual aid/commerce between groups of cyber criminals, in this way organized crime, but also novice ill-intentioned, could speed up the arrangement of illegal activities in which factor "time" is crucial. Thanks to C2C (cybercrime to cybercrime) services is very easy to rent a botnet or lease hosting services to spread malware.

Typically cyber criminals operate in the long term collecting huge quantity of data and addressing their research against specific sector of interests, most valuable information of course are related to Military and Government.

Cyber criminals Hacked databases – in terms of quality data nothing compares to the "value" of a hacked database. Users entrust sensitive and personal details to the service maintaining it, and it is therefore a gold mine for potential spear phishing campaigns if compromised.

Another method cited by Danchev is the "Harvest publicly obtainable data by outsourcing the CAPTCHA-solving process", the expert already provided evidences that humans are recruited for solving security challenge-response test, an army of low-waged solvers earning a mere $2 for solving a thousand CAPTCHA's.


FASTER IMPROVED: Captcha Entry System: Project Manager: Scott Shaw: bulletinpics at gmail dot com

STATS: — July 20 21 22 23 24 25 26 27 28 29 30 31 August 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29

Please … Explorer instead of Firefox to avoid redirection errors.

Click h… some new tricks to increase your production.

Click h… anation why server seems slow some times.

Team le… will be available to answer emails and send paypals tonight.
(Sorry … due to all the time dedicated to technical improvements).

You have 11 seconds to submit this captcha!

Your Entry Id: abc

Enter the text from the image below: (Captchas are not case sensitive.)

Tip: Type captcha, then hit Enter on keyboard.

Hit RELOAD if image doesn't change.

internal tracking:change564382920084099645

“Keeping this in mind, it shouldn’t be surprising that money mule recruiters actively harvest data from job/career web sites; and other cybercriminals are doing exactly the same while targeting legitimate Web properties that exclusively rely on CAPTCHA to prevent such types of automatic abuse.”

The cyber criminals as well as to sell the information obtained can use it to conduct further attacks and expand the collection of data to offer.

To avoid to be victims of phishing campaign be aware of risks related to trust emails from unknown recipients or emails that appear to have a legitimate origin but that offer you "something" not requested and demanding info on you.

SPEAKERS
4.16–4.17

SOURCE Conference

Boston, MA Marriott Tremont April 16-17

Scott Chasin

Scott Chasin is widely recognized as a leading visionary in the cloud security sector, having pioneered the development and marketing of several SaaS-based messaging, collaboration and security-focused technologies. We look forward to his presentation at SOURCE Boston.

Jonathan Cran

Jonathan Cran, CTO for Pwnie Express, presents Practical MitM Pentesting on Thursday, April 17th at the Source Conference in Boston. A key advisor for the well-respected SOURCE Boston Conference, Jonathan looks forward to presenting at this year's conference.

Thinking BYOD? Enterprise Mobility Steps for Success

By JP Halebeed, Development and Product Management, Airwatch

To BYOD, or not to BYOD: that is the question facing business leaders, as the bring-your-own-device (BYOD) movement gains traction in companies across the globe. Organizations that are able to provide access to their networks and welcome employee-owned devices are reporting an increase in employee job satisfaction, improved work-life balance, and an upswing in efficiency and productivity. From a corporate perspective, simplified infrastructure, a reduction in help desk-related headaches, and an improved bottom line as workers contribute to the cost of devices, are reasons enough to seriously consider a BYOD management platform.

Inviting employee-owned laptops, mobile phones, and tablets into the workplace does, however, introduce a new set of security-related hurdles: How do you prevent corporate data from falling into the wrong hands? How much control does a company have on employee-owned devices? What happens if a device is lost or broken?

Set the Stage

The key to fully embracing BYOD and reaping the benefits for both the enterprise and the employee hinges on the delicate balance of security and flexibility, which should be established in a **BYOD policy.** A well-defined user policy sets expectations and lays all the cards on the table, making employees aware of their rights and responsibilities from the beginning. By providing transparency on legal and privacy issues, outlining terms for content and app management, and differentiating between personal and corporate data, workers can make an informed decision and know exactly what they are signing themselves (and their devices) up for. Transparency between employer and employee will also help drive BYOD adoption by shifting the tone of the conversation from one of corporate management to employee empowerment – “I wonder what the catch is?” versus “I know what I’m responsible for and what my employer will cover.”

Play by the Rules

Another tenet of any successful BYOD program is keeping a finger on the pulse of the complex and often fluid data privacy legislation, which varies not only by country, but by sector. Depending on a company’s location and industry, where and when employees can access e-mail, the distinction between public and private data and the ability to track devices is governed not only by a corporate BYOD policy, but by law.

Healthcare professionals appreciate the convenience of using mobile devices in the workplace, but in order to keep patient data safe and comply with HIPAA regulations, they must among other provisions: **encrypt all corporate email, data, and documents (**in transit and at rest) on all devices, monitor device integrity to ensure proper PHI transmission, and block access to certain data or applications. In classrooms across the globe, iPads and tablets are changing the face of education, making learning a fun, interactive experience for students of all ages, and expanding classroom hours. Schools that integrate e-learning into their curriculum must abide by the Children’s Internet Protection Act (CIPA), which requires education institutions and libraries to enforce a written internet safety policy and restrict access to certain types of websites deemed harmful to minors. Across the globe in Switzerland, employees in the banking industry had best think twice about tossing a mobile phone or tablet into a suitcase when traveling abroad - devices with access to private client information are not allowed to leave the country.

To avoid legal headaches and potential fines, all companies considering a BYOD program must be aware of the regulations applicable to their country and industry. Since IT managers are generally not expected to stay up to speed with legislation on mobility matters, it pays to seek council from mobile security experts, legal teams, and human resources departments.

Pick the Right Partners

The old adage “choose your friends wisely” applies not only to one’s social life, but to the successful implementation of BYOD programs too. Picking the right technology partners is instrumental in forging a mutually beneficially collaboration, as well as a smooth transition into the world of BYOD.

When evaluating a potential technology partner, businesses should carefully consider the compatibility of a provider, including whether they offer additional layers of security, such as a NAC, and their ability to integrate with the business’s existing hardware and software investments. Joining forces with an Enterprise Mobility Management (EMM) provider offers a streamlined approach to mitigating business risks, while still giving employees a variety of device options and maintaining their privacy.

Armed with the facts, businesses leaders can weigh the pros and cons and decide whether a BYOD program makes sense for their organization. For thousands of businesses, the answer is a resounding “yes” – the benefits to both the enterprise and employees outweigh the potential risks, which can be alleviated by proper planning and strategic partnerships.

Best Practices for Encrypted Email and File Transfer

By Bob Janacek, CTO and Co Founder of DataMotion

Data leaks are on the rise. Many breaches are the result of employees accidentally, or in some cases maliciously, sharing information that should be kept private through email or file transfers.

In most situations, a person authorized to have access to customer records containing personally identifiable information (PII), protected health information (PHI) or confidential business information sends some of this detail in an email message or file over the public Internet in an unencrypted state.

In some cases, hackers intent on identity theft or fraud will gain access to a compromised system and send this same type of information out of the company walls through email or file transfers.

Unfortunately, rules and regulations governing the protection of such information are also on the rise. Beyond the well-known privacy and data protection regulations such as those included in HIPAA, PCI DSS, and GLBA, more states and industries now have their own data privacy and breach notification laws.

With today's great concern about privacy and data theft, the cost of a breach is high. One industry survey pegged the average cost of a breach at $5.5 million and the cost per record being $194. The costs can include penalties and fines from regulatory bodies, and there are added expenses associated with customer notification and credit card monitoring services. To put these costs into perspective, consider that there have been several cases in the last few years where companies have had to pay roughly $100 per year for two years for credit card monitoring services for every customer whose data was exposed in a data breach. If even a modest 5,000 customers are involved, that would amount to $1 million just for monitoring services.

Complicating matters for companies that want to prevent such breaches is the fact that today's workforce is more mobile and uses a variety of devices to conduct business.

Given these challenges, here are some best practices to help reduce the chance of protected data being exposed through email or file transfers.

Keep it Simple: Employees must be able to conduct business without having to navigate obstructive technology or they'll turn to less-than-secure methods. Similarly, communications and information sharing between employees, business partners and customers must proceed without placing any burdens on the parties involved.

Use Policy-based Gateway Filtering: Since email and file attachments are a prime source for data leaks, deploy gateway technology that can filter messages and the wide variety of file format attachments used in business today. To avoid false positives, and an ensuing drain on IT hours and resources, use technology that combines pattern and exact matching to specific data lists when scanning for data that cannot leave the company in an unencrypted state.

Look for Exceptional Handling of File Attachments: When workers need to send a large file to a business partner or to a home computer to work on after hours, they often use unauthorized file sharing services. Most of these services do not encrypt the data, thus exposing the company to risk. A better approach is to use a solution that lets users easily send large files as email attachments without IT intervention, while still maintaining compliance and control.

Make Use of Extensive Logging and Reporting: Gauging the effectiveness of an effort to prevent protected data from leaving the company unencrypted requires detailed information. Look for a solution that provides extensive logging and reporting to help manage operations, as well as providing details for audits and proof of compliance.

Require Seamless Mobile Integration: With today's more mobile workforce, employees conduct a great deal of business outside of the office. Look for a data protection solution that works with your existing email client on mobile devices so no separate app is needed.

Address Protection of Incoming Data: Communications is a two-way street. Most email data protection solutions focus on outbound traffic. A robust solution would provide a way for customers or business partners to start a secure email exchange without the need to install or use complicated encryption software of their own. Look for a solution that allows the establishment of a secure portal through which outsiders can initiate secure inbound messaging.

Maintain Normal Business Processes: The best security solutions work in the background and do not obstruct work from being done. To reduce complications and prevent business disruptions, a secure email and file transfer solution should tightly integrate with your internal and external workflows to automate business processes and improve efficiency.

Following these best practices will help ensure that your company can continue to conduct business in a normal manner, while reducing data exposure risks that can arise with email and file transfers.

Bob Janacek is the CTO and co founder of DataMotion, an established cloud-based secure data delivery provider. Millions of users worldwide rely on DataMotion to transparently improve business processes and reduce costs, while mitigating security and compliance risk.

Best Practices For Endpoint Security

In this article Håkan Saxmo, CTO at Cryptzone, looks at the evolving IT security challenges facing IT professionals and explores best practices for endpoint security to protect your data.

Industry today faces an increased level of security threats and vulnerabilities: Zero day attacks, hacktivism, APTs, social media and last but not least, technically savvy employees. The use of email, mobile devices, USB sticks, Cloud services, such as Skype, DropBox, Skydrive mean that information gets spread ever more widely without sufficient data protection or corporate control. It has become almost impossible for organizations to track where information is or has been.

Protecting ’big infrastructure’, with all their systems and applications is no longer effective. It has become vital to move the protection closer to or even within the information itself.

Without adaptive and invisible security solutions, companies lock their infrastructure down so hard that it seriously impacts efficiency and business. What’s required is precise access control that is easy to manage down to a very granular level of access and rights. Organizations have a need to be able to administer access rights and authentication globally and locally.

Protecting your internal storage

Whether you use file shares, SharePoint®, network or Cloud storage, it is important to start securing sensitive data even inside your firewalls. Auditors are becoming increasingly aware of the danger within. Far too often it is nosey techies who get hold of salary files, leaking the board of director's information or regulated sensitive content. Consider patient information at a healthcare provider or the lawyer's client information. Used irresponsibly, even without intent, this can cause severe damage.

To protect the data itself with strict authorization and access controls prevents this kind of behavior, even if systems are hacked or access is accidently obtained.

The explosion of BYOD

More and more employees are choosing to bring their own phones or tablets into the office or to remotely access company resources from home or on the move. As information now can be consumed where and when needed, this trend has the potential to dramatically increase efficiency and reduce cost, but equally it represents additional risk to corporate digital assets. The threat landscape is made worse as there is a lack of control over such devices, the applications, data and access protection. This quickly becomes the weakest link in protecting company IP and confidential information.

Organizations must decide if they are going to enforce stricter policies on non-corporate devices in the workplace, strong password authentication and encryption (i.e. extend the network based controls they use today) or whether they are going to control what can be accessed , seen and stored on a device.

With increased contextual awareness capabilities built in to some access control technologies, allowing access to highly confidential data becomes less risky. Delivering truly granular access for users and systems to a single server, application or even document, greatly reduces the security risks. Combined with strong access control, such as two-factor authentication, central auditing, encrypted storage and wiping all traces after use, this is powerful technology.

Adoption of Private Cloud

Communicating to employees the need to secure information stored on a private Cloud, such as DropBox and SkyDrive is vital, but ineffective if you don't also provide simple tools for them to do so with minimal effort and little technical know-how. If your organization bans the use of such storage, I can almost guarantee that more than one person in your organization will still do it. The convenience factor is just too appealing. So administrators need the ability to centrally audit access to content both before and after it leaves the premise through such channels.

Making sure people understand the definition of valuable, confidential and sensitive information as it applies to your organization is also helpful. Don't assume they just know! Create awareness of the consequences of non-compliance for them personally and the wider organization.

Increasing Audit Burden

To reduce the time and costs associated with auditing IT for compliance, make sure that event information is centrally stored and available without a lot of additional work. Automated compliance reporting and pinpoint compliance checks must be managed centrally and easy to apply in order to discover who has used data, where and when.

Make sure you know what is happening to your sensitive data once stored on the network, SharePoint or portable device. Implement technology which prevents the wrong person opening it. Additional measures may need to be taken to ensure highly confidential documents are secured (encrypted), tracked and audited.

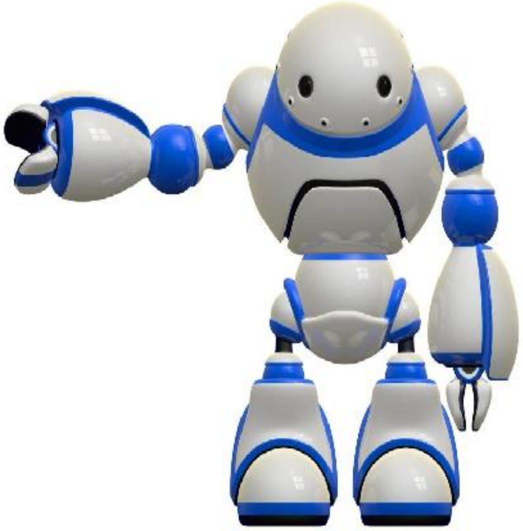
More intricate supply chains

Supply chains are becoming increasingly complex, as organizations around the globe collaborate together. The need to share more and more information with third parties inevitably puts data at increased risk of compromise. Often these third parties do not have very sophisticated IT infrastructures, so you have to take the responsibility to ensure your data is protected. Ultimately you remain liable for any IT security breach. Like researching your family tree make sure you understand the web of relationships that support your contracts. It is not uncommon for your suppliers to sub-contract work, which in turn may be sub-contracted yet again. Stipulate in contracts IT security measures that you expect to be upheld down the supply chain. One way to ensure these are realistic expectations and you keep more control is to provide your suppliers with some shared tools for securely accessing or exchanging information.

In Summary

Organizations should be moving their thinking away from having the network protection as the main form of defense towards a model where centralized control over access to systems, applications and data becomes the primary defense.

Cyber Defense Best Practices



by John Landwehr, Vice President, Adobe Systems

There can be very little disagreement that cyber security is getting more wide-spread public attention today than it ever has in the relative short history of digital networks and information. What's missing from this discussion, however, are not the efforts that government agencies and businesses are taking to secure their firewalls and network perimeters. It's how to continue to secure information after it reaches the first authorized recipient, and may accidentally or intentionally be forwarded elsewhere.

Merely protecting an envelope that temporarily contains the information in storage or transport, while an essential component of any cyber best practices playbook, isn't enough anymore to provide the kind of security that organizations need. Whether covered by International Traffic in Arms (ITAR) requirements, Export Administration Regulations- Commerce Control List (EAR) restrictions, banking regulations, health care legislation or privacy laws, there can be severe consequences and penalties for losing control over sensitive information. An envelope around the data cannot be the end of the solution. The content itself must also have persistently strong protection.

In today's data-driven world, content-centric rights management is being extended to all types of electronic information, with three primary functions in mind:

1) Authentication. Making sure that the recipient who obtained the information is still a person authorized to open and view it, based on their login credentials (including, multi-factor schemes);

2) Authorization. What exactly can the person do with the information once they have opened it? For example, can they copy it, modify it, or print it? Authorization also can set limits on how long they have access, with these permissions being revoked if, say, that person leaves the agency or attempts to go beyond what they are authorized to do.

3) Audit. With the appropriate types of rights management attached to the document itself, that audit trial continues to follow the content, independent of any subsequent transport or storage. It can continuously monitor both success and failure when individuals interact with protected content.

A rights management approach to protecting content also needs to be dynamic. People change roles in organizations and content may become more or less protected throughout it's lifecycle. Therefore, the permissions applied to content should not be burned into the content itself, but managed by a central policy control resource to make changes without the need to republish any content.

This type of security approach can provide great flexibility for employees who need access to sensitive information while traveling beyond the confines of their office desktops. This includes support for smartphones and tablets where the same content-centric security applies in those environments, as well. For example, if someone starts to extract protected documents from a lost or stolen device, those documents are persistently protected to prevent viewing. Plus the audit log alerts administrators that attempts have been made to open the protected content.

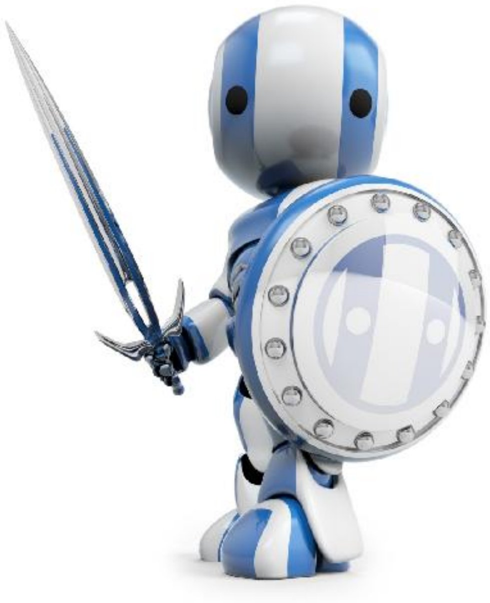
Best practices, then, for document-centered rights management requires:

1) That the recipient authenticate himself every times he accesses the document;
2) That the document always remain encrypted when distributed, even after the recipient opens it;
3) That it be integrated with the desktop applications so that it can be viewed regardless of file format;
4) That the permissions restrict printing, modifying, or copying to the clipboard; and
5) That permissions can expire, be revoked, and be watermarked.

Rights managed document security can also provide a another level of security based on real-time analytics of document use. For example, the number of times a particular document is accessed can be monitored as well as the viewing time of each. This can be used either to set a baseline or to best manage which types of documents require larger distribution. The geographic location of each open can also be monitored and any anomaly can be flagged. Officials can be instantly alerted at the first sign of any unusual activity.

Any agency IT team moving to incorporate a document-based rights management approach to its security program should consider the following requirements:

- Strong encryption meeting FIPS140 standards must be included;
- It should work on multiple operating systems and formats to meet user needs;
- It should allow for dynamic policies to be applied, so that permissions can be revoked as needed;
- It should have advanced analytics for continuous monitoring; and,
- It should have strong authentication sources to assure that it reaches only the intended recipient.



Including document-level security into an agency’s overall security program can mitigate the fears that viewable data can fall into the wrong hands regardless of perimeter protections.

Cyber Attacks – The New Normal

It's time to elevate the importance of cybersecurity

By Bud Michael, President & CEO eSoft

While high-profile cyberattacks against governments, large banks and businesses have made headlines in recent months, small and medium size businesses are now also attractive targets of cyber thieves. The frequency and sophistication of online attacks against business continues to increase. More attacks are surgically concise and invisible, ever-changing and pervasive. They're very hard to detect, and even when detected, they're hard to contain.

The Deloitte 2012 Global Financial Services Industry Security Study points out that even as cybersecurity practices mature and advance, nearly 25% of business respondents indicated they experienced security breaches in the past 12 months. More than 50% of bank respondents consider security breaches involving third-party organizations as a high threat.

Not only can an information security breach cost your company money, in many industries such as financial, healthcare and education, breaches must be made public under state and federal compliance regulations. Consequences of cyber crime include customer notification and remediation costs, increased cybersecurity protection costs, lost revenues, possible litigation, impact on shareholder value, and damage to reputation. Businesses of all sizes are at risk, but small and medium businesses in particular are low hanging fruit for digital thieves and the attacks are growing daily. To make it even easier for cyber thieves, the SMB user community will often click on any link, access any site, or install any application that suits them in disregard or ignorance of the very real dangers.

From a network security perspective, SMBs typically lack the time, expertise and money required to properly strengthen their defenses. In addition, a small business owner or CEO might say, "Why should I spend money on security? Why would hackers attack me? I'm just a small supply company with 40 PCs and one server."

Traditionally, cybersecurity has been thought of as an IT issue and is most often included as part of operational risk management. The mistaken assumption that "the IT guys can handle the problem" leads to the dangerous situation where most employees don't feel that they need to be responsible for the security of their own data. A corporation's finance, human resources, sales, legal, and other departments all own critical data; and just one employee can inadvertently open a portal to attack. Nonetheless, the tendency is to believe that the responsibility for securing data rests down the hall with the IT department. Too often, the IT manager must try to balance the risk against the resistance he or she meets from the reception desk all the way to the corner office.

This mindset needs to change.

The potential negative consequences of cyber attacks on a business are so significant that it is time for cybersecurity and information risk management to be elevated to its own INFOSEC category reporting to the Chief Executives. Boards of directors, general counsels, chief information security officers, and chief risk officers need to understand and monitor their organization's level of planning and preparedness to address cyber risks.

A recent study by Corporate Board Member/FTI Consulting Inc. found that one-third of the general counsel surveyed believe that their board is not effective at managing cyber risk. Only 42 percent of directors in that study said that their company has a formal, written crisis management plan for dealing with a cyber attack, and yet 77 percent of directors and general counsel believe that their company is prepared to detect a cyber breach, statistics that reveal a "disconnect between having written plans and the perception of preparedness." Indeed, a 2012 governance survey by Carnegie Mellon CyLab concluded that "boards are not actively addressing cyber risk management."

Only 25 percent of the study's respondents (drawn from Forbes Global 2000 companies) review and approve top level policies on privacy and information technology risks on a regular basis, while 41 percent rarely or never do so. These figures indicate a need for boards to be more proactive when it comes to overseeing cybersecurity risk management.

The Internet Security Alliance (ISA) recommends the establishment of a Cybersecurity Operation Center to monitor traffic and data and actively respond to attempted intrusions and breaches. A cyber risk analysis should be an integral part of your risk management plan. If you are a smaller business who outsources security through an IT services firm, you should receive regular threat monitor reports for analysis as well as support of compliance requirements for cybersecurity.

Businesses with the lowest relative cybercrime costs tend to have a dynamic cybersecurity plan and utilize a network security system and event management tool, according to the Ponemon study. Businesses that employed security intelligence tools lowered their cybercrime costs by an average of $1.6 million per year, in part by being able to spot and respond to breaches more quickly.

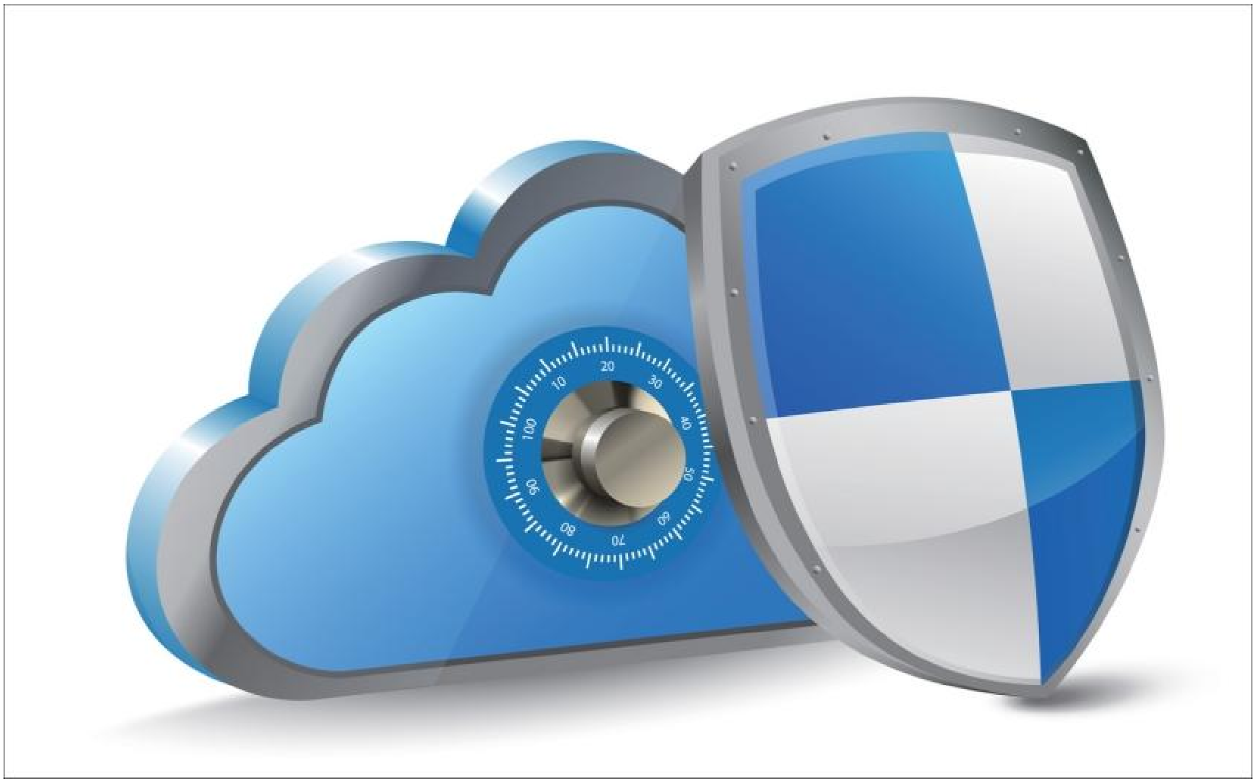
The consequences of cyber crime can ripple through every department of every business with substantial and devastating effects. Every IT manager, regardless of business size, should be viewed as the director of cybersecurity risk management. A cross-functional approach should involve all departments in your company and increase the awareness of and responsibility for cybersecurity by every employee from the C-suite down.

About the Author

*Bud Michael is President & CEO of **eSoft**. eSoft is a leading provider of integrated network security solutions offering small and medium businesses (SMB) protection from dynamic Internet-based threats. eSoft's award winning InstaGate and ThreatWall platforms offer high-performance Deep Packet Inspection security services including firewall, UTM, complete email security, and web filtering and security with an easy to configure and manage user interface. eSoft's solutions provide IT managers with simplicity and flexibility when deploying and managing network security. Visit www.esoft.com to learn more. Bud welcomes your emails at bmichael@esoft.com*

Best Practice for Cloud Computing

By Bill Strain, Chief Technology Officer, iomart Group plc, www.iomart.com



Mention Cloud Computing in business circles and the first question to be fired back at you tends to be, “How secure is it?” The safety and security of mission-critical data in the Cloud is still a major concern for those who haven’t yet adopted Cloud services which, according to various global analysts is anything from 25 to 50 per cent of all enterprises. It’s also vital for those who have already gone down the Cloud road.

The commonly held view is that Cloud Computing is a cost effective way of purchasing computing resources such as web space, storage and back up without the need to own or manage the hardware that they operate on and that you have no control over the management or location of your data. However this is a misconception and applies in the main to the public cloud model offered by companies such as Amazon Web Services, Google and others.

As a major UK vendor of Cloud services we specialize in the provision of private and hybrid Cloud infrastructure solutions as few enterprise level organizations are hugely confident about relying solely on the public Cloud to store their business critical information with its potential, and relatively higher, risk of failure. With private Cloud you might still be sharing some resources (servers) but in a closed space i.e. a designated data center. It's like being a member of an exclusive club with your own personal chair that only you can sit on. Either way, whatever type of Cloud you are considering, there are a number of factors that you should take into consideration when looking at best practice.

1. The vendor

Research the vendor you are potentially going to use thoroughly. Do they own their own data centers or do they lease space in third party data centers? If you're planning to outsource your IT infrastructure to the Cloud then you're already giving up some technical control to a third party – do you want to discover down the line that they too have handed responsibility to yet another party who you have only an indirect relationship with? As a major UK vendor of Cloud services we have asked the security question of ourselves on behalf of our customers. Our answer is straight forward. We own and manage our infrastructure – seven data centers and a super-fast fiber network that connects them. This will help organizations avoid the situation that customers of the now bankrupt 2e2 hosting provider recently discovered; significant quantities of their data was held in non 2e2 data centers without their knowledge. Ensuring the veracity of the data center assets your vendor has at their disposal is vital to successful and secure Cloud adoption. For additional peace of mind, organizations should ensure that the data center environment is ISO accredited (e.g. ISO9001 Quality Management System and ISO27001 Information Security Management System) and complies with all regulatory and legal requirements.

2. SLAs

The Service Level Agreement you have with your Cloud provider is the glue between the two parties. Does the SLA offered by your provider meet the needs and expectations of your business? What guarantees do they give around uptime? What SLAs do they have with their own technology and network partners in terms of hardware failure, software performance and network issues that they don't have full control over? An SLA should not be glossed over or rushed into. Take time to read it, digest it and make sure you understand all the terminology and what happens in the event of an outage or a degradation of service due to a Denial of Service (DoS) for example and check if there is an exit clause.

3. Technical Support

The internet never sleeps and neither should your Cloud provider. While you are self-provisioning your Cloud resources you need to be sure that you can contact someone in the event that you need technical help on site. This should not be help from someone who is asleep in their bed and who then takes two hours to get to respond. Technical support should be available to you 24/7, 365 days of the year.

4. Access

While the above best practices relate to the provider of the data center space you are using, it is important that you do not put all the responsibilities onto them. The internal policy of your organization must match up to the strict standards you expect from your Cloud provider. The key question to ask internally is, “Who has authorized access to your Cloud controls?” Decide what authentication processes are required to ensure security for all server management and Cloud service deployment.

5. Redundancy

It is essential to know what level of redundancy is operated by your Cloud provider. What happens in the event that there is a power outage or a failure of the hardware? What backup is provided automatically to protect your data and IT resources? Redundancy and resilience is what ensures peace of mind. How does your provider match up?

6. Compliance

Outsourcing sensitive and critical data to the Cloud is also changing the dynamics of compliance. Security controls such as endpoint protection, application firewalling, identity management and patch management are all aspects that need to be considered by you and your Cloud provider. Negative publicity or legal and regulatory non-compliance can be costly for any organization. Knowing that your data is secure within known boundaries and locations and complies with the legislation of the country in which it is held, provides reassurance at the highest level.

7. Software as a Service

While all the above points relate to your relationship with a data center operator supplying you with Cloud infrastructure, you need to factor in further checks and balances if you are buying Cloud software services. SaaS adds another link into the supply chain, and means your tick list needs to be longer.

In the past 12 months two significant vendors of email security software announced changes to their Cloud e-mail services. Webroot announced it was killing off its e-mail security service and then Google told 26 million users of Postini, its e-mail security and archiving product, that it was shutting it down. Both sets of users and resellers have been forced to make a choice about changing their services and undertaking migrations they were not expecting. In the UK it has been clear that users have been affected by a lack of appetite to service the geographical market here. So my point about best practice for SaaS would be to check your SaaS vendor's commitment to the local market.

Summary

In the end users of Cloud services need to remember that while it can provide significant benefits, including relief from the cost and responsibilities of IT infrastructure management, it also means a loss of direct control. So factoring in the above checks and balances can help to ensure that responsibility for the Cloud is maintained within a trusted partnership with the vendor that you eventually choose.

Security Issues Unique to Cloud Computing

By David Amsler, President and CIO of Foreground Security

Chances are good that your organization is hosting at least some services through a cloud provider. And if you're not yet, you're thinking about it. These environments introduce some new security issues that you need to incorporate into your security plans.

The virtualization technologies used by cloud computing hosting providers mean that as well as managing your own (virtual) servers and your own staff, you need to make sure the hosting provider's policies for managing their physical servers and staff are acceptable. Security issues to keep in mind include:

Privileged User Access

When data is stored in your own, on-premises data center, you can literally put it behind lock and key--and you control the key. But when you outsource to a cloud provider, you're bypassing all of your physical, logical and personnel controls and handing your data over to a remote entity you've probably never met or spoken to. When put that way, it certainly sounds scary. It should. Consider Dropbox's repeated breaches and the recent Evernote breach.

Not all cloud providers are created equal. Do some due diligence to verify a prospective cloud provider will be a good caretaker for your sensitive data. This can be hard to do when the whole point of cloud services is that there's no physical presence, but the most important thing you can do is carefully review their terms of service. If the provider doesn't include their full terms of service on their website, contact them and ask for a copy. Don't wait until it's time to put pen to paper and sign a contract to review them. If there is anything that is vague or doesn't comply with your own security policy, contact the provider and ask for clarification. As the Dropbox incident makes clear, cloud service providers are realizing they need to be more transparent and specific about their internal security policies and practices. If you don't get the answer(s) you seek, move on to the next cloud provider.

Regulatory Compliance

Your enterprise remains responsible for compliance requirements regardless of whether you're the one hosting the data. Sarbanes-Oxley, HIPAA, and other laws hold many organizations responsible for an exacting level of data monitoring and archiving. Be aware of the regulatory responsibilities that affect your organization and your data, confirm that any potential cloud provider can comply with them, and have a way of auditing that compliance. For example, ask your provider how they prove that deleted data is truly unrecoverable. If they have data centers in multiple countries, cloud providers should not be afraid to submit to audits and security certifications to ensure they're able to hold up their end of the bargain. Amazon Web Services (AWS), for example, has an extensive list of certifications and third-party attestations.

Data Location and Segregation

Any cloud provider worth its salted hash will have multiple data centers for redundancy. Some large providers have data centers in multiple countries. If regulations or your own security policy prohibits offshoring data, make sure your chosen cloud provider has a way to keep your data within U.S. borders.

Most cloud providers use virtualization technologies that will likely store your sensitive data on a physical server or storage device along with data from multiple other customers. Although there have been no documented instances of someone with access to one virtual server being able to "escape" to the hypervisor and then access other virtual servers, the risk remains. One way to eliminate this threat is to encrypt your data before it leaves your organization. There are a number of options for simple file encryption but as Gartner explains in a June 2008 report, "Encryption accidents can make data totally unusable, and even normal encryption can complicate availability."

Monitoring and Investigative Support

Intrusion detection systems (IDS), firewalls, proxies and packet capture devices all work on physical networks. Moving to a cloud hosting provider may mean you're unable to monitor and restrict network traffic. This can make identifying and investigating security incidents difficult if not impossible- especially if the Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) providers are different entities, as is sometimes the case.

Although there are a few security products that support virtual networking, it is still a relatively new segment of the security market. Because these virtual appliances are so new, not all cloud providers have implemented them. Gartner suggests that "If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then your only safe assumption is that investigation and discovery requests will be impossible."

There's another aspect of monitoring and investigative support unique to cloud computing: Under current U.S. law, law enforcement agencies often don't need a warrant to monitor or search any data given to a third party. Your cloud service provider may not inform you if a law enforcement agency requests access to your data stored on their servers. And if your virtual server happens to reside on the same physical server as some other customer that's operating an illegitimate business, there are no guarantees that your virtual server won't be accidentally taken by a law enforcement agency when seizing the other customer's server. This has happened multiple times already.

In light of these significant security factors, it is imperative for prospective cloud users to thoroughly gather their business or mission requirements - particularly for national defense enterprises with unique security constraints. Even cloud providers meeting basic eligibility criteria to support government agencies may vary in capabilities and experience supporting different types of demanding organizations. Because most cloud infrastructures are fundamentally about economies of scale and availability, customers need to drive the security discussion and team with capable providers in a shared approach to protection.

Mobile Botnets: are all around us!

By Meisam Eslahi

Anticipations on mobile botnets' existence have been ended by the Damballa Research Laboratory official reports which discovered 40,000 infected mobile devices that have communicated through cybercriminal C&C servers for the first six months of 2011. Moreover, the McAfee research lab early prediction on advent of widely-distributed and more resilient mobile botnets come closer to reality as the Zeus botnet migrated from computers to mobile devices and targeted mobile banking. Recently nearby a million mobile devices has been infected by botnets in china via 7000 Trojanized applications.

"Security researchers say they have discovered a huge botnet running on the smartphones of more than a million unsuspecting mobile users in China. The botnet can allow the smartphones to be hijacked remotely and potentially used for fraudulent purposes. (BBC)"

The early generations of botnets (e.g. IRC, HTTP, P2P) have been operating on computer and computer networks with their most common targets being less-monitored computers, computers with high-bandwidth connections, university and company servers and home computers. Recently, mobile devices are well integrated with advanced capabilities and technologies which provides efficient environment to attract bot masters. In addition, soaring use of smartphones and Internet along with their convenience and mobility has motivated bot masters to migrate to mobile infrastructures.

Examples of Real Mobile Botnets

Name	Propagation Method	Attack(s)	Mobile OS
Zeus (Zitmo)	• Social Engineering • Infected SMS Messages	• Mobile Banking Attacks • TAC Thefts • Illegal Transactions	• Symbian • Win Mobile • BlackBerry

			• Android
DroidDream	• Exploit Techniques • Trojanized Applications	• Theft of Private Data • Download Malicious Applications	• Android
Android.Bmaster (SmartRoot)	• Exploit Techniques • Trojanized Applications	• Revenue Generation • Theft of Private Data	• Android
AnserverBot	• Social Engineering • Trojanized Applications	• Theft of Private Data	• Android
Ikee.B	• Self-Propagation	• Revenue Generation • Theft of Private Data	• iPhone
TigerBot	• Trojanized Applications	• Theft of Private Data • Change Device Settings	• Android

- **Zeus**

The Zeus in the Mobile or Zitmo infects variety of mobile operating systems, such as Symbian, Windows Mobile, BlackBerry, and Android mainly by social engineering approaches. It sends an infected SMS to victims contain a fake URL to dupe users to download a security certificate which is, in fact, the Zitmo bot. It also intercepts messages which are sent by banks to customers and authenticates illegal transactions by stealing mobile Transaction Authentication Numbers (TAC).

- **DroidDream**

Back in 2007, David Barroso termed botnets *"the silent threat"* as they try to control the infected devices without the knowledge of owners. They do not make any unusual or suspicious use of the CPU, memory, or other resources, which may uncover their activities. DroidDream was one of a good example of these silent patterns, since it is activated silently and at night (11pm to 8 am) when the mobile's users are asleep. It was designed to gain root privileges on infected mobiles and install second application to steal sensitive information and protect itself from removal.

- **Android.Bmaster**

The Android.Bmaster has infected high number of mobile devices by using Trojan applications and exploited techniques. The Symantec named Bmaster as *"A Million-Dollar Mobile Botnet"* since it has gained millions of dollars through premium SMS, telephony or video services. However, recently a new mobile botnet called MDK has overtaken the Bmaster by infecting nearby 7000 applications and having one million mobile devices under the control of its botmaster.

- **Ikee.B**

Although the Ikee.B is a simple botnet in nature, it can be named as one of the early generations of mobile botnets that operates on jailbreak iPhones with almost the same functionality as computer-based botnets. Scanning the IP range of iPhone networks, looking for other vulnerable iPhones in global scale and self-propagation are the main activities of this malware.

- **AnserverBot**

Amongst different types of mobile botnets the AnserverBot can be considered as one of the most sophisticated malwares. Its command and control is designed based on a complex two-layer mechanism and implemented over public blog. In addition to detect and disable the security solution in infected device, the AnserverBot periodically checks its signature to verify its integrity in order to protect itself from any type of changes.

- **TigerBot**

TigerBot is fully controlled by SMS instead of the Internet and web technologies. However, it detects the C&C messages and makes them invisible to the mobile device owners. In addition to collecting private data like SMS messages, it has sophisticated capabilities to record voice call conversations and even surrounding sounds.

The aforementioned botnets are only a few examples of current mobile botnets to emphasize their existence and their negative impacts on mobile network environments. Although the mobile botnets are newly developed, they are growing extremely fast specially in popular platform such as Android.

“Since July 2012, more than 100 million Android phones have found their way to new owners, which represents slightly more than half of the market in smartphones (sorry, iPhones). Fake apps and bad SMS messaging is the entire rave with the malware writers these days, and as the new year unwinds, we have already seen report after report of this rising tide of “new” target exploits. (Drew Williams, President, Condition Zebra)”

On the other hand, mobile environments are less protected compare to computers and computer networks and their specific characteristics bring notable challenges to mobile botnet and malware detection.

Challenges in mobile botnet detection can be reviewed from two different perspectives as follows:

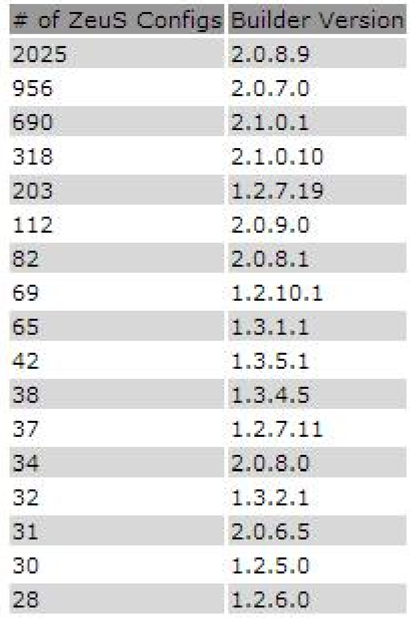
1) Inherent Challenges of Botnets:

Regardless of their operational environments, botnets have several characteristics that make them difficult to detect. They are distributed very fast and the bot masters are always trying different techniques to protect their bots from existing detection solutions.

- ***Developed by Skilful Developers:*** Botnet developers have higher technical capabilities than any other online attackers. Unlike other types of Cyber threats, botnets are designed and developed for long-term goals, therefore, various strategies are employed by bot masters to keep the bots safe and uncovered, as long as possible.

Name	Self-Protection Technique(s)
Zeus (Zitmo)	• Automatic repacking of binaries • Polymorphic encryption
DroidDream	• Midnight's Activities to Avoid Users' Attention
AnserverBot	• Detect and disable the security solution in infected device
TigerBot	• Detects its C&C SMSs and delete them • Using popular application names and icons like Google's search application

- ***Having Dynamic and Flexible Nature:*** Bot and botnets are continuously being updated and their codes change from day to day. The McAfee Research Lab reported that "*every success in Botnet detection is only temporary* "as the bot masters frequently change their strategies, and design new methods to recover and restore their detected bots, within a short time. For instance, based on the Zeus Tracker statistics, there are 17 different versions for Zeus botnets alone.



# of ZeuS Configs	Builder Version
2025	2.0.8.9
956	2.0.7.0
690	2.1.0.1
318	2.1.0.10
203	1.2.7.19
112	2.0.9.0
82	2.0.8.1
69	1.2.10.1
65	1.3.1.1
42	1.3.5.1
38	1.3.4.5
37	1.2.7.11
34	2.0.8.0
32	1.3.2.1
31	2.0.6.5
30	1.2.5.0
28	1.2.6.0

- ***Using Standard Protocols:*** Some botnets are using standard protocols to establish their communication infrastructure. For instance, one of the latest generations of botnet, called HTTP-based, uses the standard HTTP protocol to impersonate normal web traffic and bypass the current network security systems (e.g. firewalls and signature based Antiviruses). The ***AnserverBot*** discussed above is another example in which a public blog is used to implement command and control mechanism.

  "Based on the evaluation with four representative mobile security software, our experiments in November, 2011 show that the best case detects 79.6% of them while the worst case detects only 20.2% in our dataset. These results clearly call for the need to better develop next-generation anti-mobile-malware solutions. (Android Malware Genome Project)"

- ***Working in Silent Mode:*** Without doubts bot masters take a good lesson from what Ram Dass said before! "*The quieter you become, the more you can hear".* The bots on infected targets try to avoid any unusual or suspicious use of the CPU, memory, or other computer resources, which may uncover their presence.

2) Mobile Environments' Point of View:

In addition to the aforementioned general challenges there are some mobile based characteristics that bring more difficulties in mobile botnet detection.

- ***Lack of Protection and Users' Awareness:*** Mobile devices are not properly protected compared to computer and computer networks, and their users pay less attention to the security updates

- ***Resource Limitations:*** Mobile device resources, such as CPU, memory, and battery life, are limited. Therefore, it is difficult to deploy existing botnet detection solutions for mobile botnets.

- ***Mobile-Specific Characteristics:*** There are some mobile-specific characteristics that have differentiated mobile security management from that of computers such as mobility, strict personalization, and different types of connectivity, technology convergence, and variety of capabilities.

- ***Diversity in Infection:*** Unlike computer-based botnets, the MoBots can use different mediums (e.g. SMS/MMS/Bluetooth) along with the Internet to spread. Moreover, this diversity makes it default to detect infection processes using current security systems.

- ***Lack of Central Security Management:*** Among all of the aforementioned issues, the main challenge with mobile security is the lack of central security management, as it can track and monitor security threats and update the security policies on mobile devices accordingly.

.

These sophisticated characteristics show that mobile botnet detection is a notable challenge in mobile security management. There are several methods and techniques that have been used to track botnet activities and detect them in computer networks such as *Honeypots and Honeynets*, *attack's behavior analysis*, *monitoring and analyzing the DNS*, *signature-based botnet detection* and *behavioral analysis techniques.* Regardless of the efficiency and accuracy of these techniques, they are mostly designed based on computer and computer network behaviors and characteristics and may not be directly applicable for mobile devices. Therefore, creative solutions are needed to address the challenges discussed in this article.

Meisam Eslahi *is an information security researcher and digital forensic investigator, received his Masters' of Computer Science in Network Security filed from University of Malaya, Malaysia. He is working toward the Ph.D. degree in Computer Engineering and his domain of interests includes Cyber security Threats Detection, Mitigation and Response (Mobile Botnets in Particular), Behavioral Analysis, Cyber safety and Digital Awareness. He has over 11 years of experience in the field of Information Technology with 5 being focused on Cyber Security related domains and holds multiple certifications such as CEH (Certified Ethical Hacking), CHFI (Computer Hacking Forensic Investigator), and IBM certified Solution Advisor for Cloud Computing.*

Cyber Warnings Newsflash for March 2013

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

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…

Strategies of a world-class computer security incident response team

03/21/2013 05:46 (Help Net Security)

Today's Computer Security Incident Response Team (CSIRT) should have everything they need to mount a competent defense of the ever-changing IT enterprise: a vast array of sophisticated detection and prevention technologies, a virtual sea of cyber intelligence reporting, and access to an exploding wo

North Korea suspected in cyberattack despite China link

03/21/2013 05:18 (Stars and Stripes)

SEOUL, South Korea -- Investigators have traced a coordinated cyberattack that paralyzed tens of thousands of computers at six South Korean banks and media companies to a Chinese Internet Protocol address, but it was not yet clear who orchestrated the attack, authorities in Seoul said Thursday.

Cybersecurity Lobby Surges as Congress Considers New Laws

03/21/2013 00:47 (Bloomberg)

The determination by Congress and President Barack Obama's administration to protect networks of critical U.S. industries from hackers and cyberspies is creating an explosive growth opportunity -- for lobbyists.

Experts: Iran and North Korea are looming cyberthreats to U.S.

03/20/2013 23:48 (Computer World Singapore)

The two countries may lack some capabilities, but they have strong intentions to do harm, experts say Cyberattacks supposedly originating from China have raised alarms in recent weeks, but U.

Botnet simulated humans to siphon millions in click-fraud scam

03/20/2013 23:48 (Computer World Singapore)

A recently discovered click-fraud botnet was costing advertisers more than $6 million per month by simulating human activity in targeting display ads on a couple of hundred websites.

S. Korea Says Chinese Code Used in Computer Attack on Banks

03/20/2013 22:56 (Washington Post - Bloomberg)

(Updates with broadcasters' comments in 15th paragraph.) March 21 (Bloomberg) -- The biggest cyberattack on South Korean computers in two years used malware code from China, according to an initial investigation that is focusing on possible links to North Korea.

Next-wave malware aims for mayhem, not money

03/20/2013 22:30 (Computerworld Malaysia)

Phil Gardner talks about why the recent Shamoon malware attack is a predictor of more targeted, geopolitical cyberattacks to come To most of our CISO clients, malware is a cost of doing business.

Top 5 causes of a slow computer

03/20/2013 18:48 (FOX 19)

A slow-running computer can really torpedo your work day - or any time, for that matter. But experts say there are easy ways to get your PC back up to speed without spending lots of money.

The Awl Network Is Under Attack!

03/20/2013 17:55 (Yahoo! News)

Some hackers are attacking the Awl network of websites -- so The Awl, The Hairpin, Splitsider, The Billfold and The Wirecutter -- and the whole group are now blocked by Google's big, red malware warnings.

Chinese Premier Pressed on Cyber Spying

03/20/2013 17:14 (CNBC)

The newly appointed U.S. Treasury secretary "pressed hard" in meetings with Chinese leaders over alleged Chinese cyber attacks aimed at stealing commercial secrets from American companies, according to U.

Tensions Continue on Korean Peninsula

03/20/2013 15:41 (Yahoo! News)

Cyber Attack on S. Korean Businesses Latest Provocation

Montreal police confirm no sensitive information was leaked in apparent cyberattack

03/20/2013 15:00 (Global Montreal)

When It Comes To Cyberwarfare, North Korea Is No Newbie

03/20/2013 14:42 (GPB)

Who or what caused a takedown of computer systems at banks and broadcasters in South Korea on Wednesday is still a matter of speculation, but suspicion immediately and unsurprisingly fell on Seoul's archenemy to the north.

Why Watering Hole Attacks Work

03/20/2013 13:47 (Threat Post)

Information security is littered with bad analogies. And none sounds sillier than a watering hole attack, which plays off the tactic that dominant animals use when stalking food by loitering at a watering hole.

Lew Tells China Cyber Attacks 'Very Serious Threat To Our Economic Interests'

03/20/2013 13:05 (CBS DC)

BEIJING (AP) — U.S. Treasury Secretary Jacob Lew pressed Chinese leaders over computer hacking and for help with North Korea during two days of talks that ended Wednesday.

Researchers Uncover 'TeamSpy' Attack Campaign Targeting Government, Research Targets

03/20/2013 11:59 (Threat Post)

Researchers have uncovered a long-term cyber-espionage campaign that used a combination of legitimate software packages and commodity malware tools to target a variety of heavy industry, government intelligence agencies and political activists.

Korean Bids Signal Stock Rebound as Cyber Attack Probed

03/20/2013 11:36 (Bloomberg)

South Korean stocks are set to rebound after a computer network shutdown triggered by a cyberattack sent the Kospi Index (KOSPI) to its biggest drop in two months in the final minutes of trading, bids and offers submitted to Korea Exchange show.

What is a secure password?

03/20/2013 10:43 (ChicagoNow)

What is a secure password? The fact is that best password is one that even you can't remember. Of course that doesn't work particularly well if you ever want to access your account again.

Major computer crash in SKorea; hackers suspected

03/20/2013 06:08 (Tulsa World (AP))

Last Modified: 3/20/2013 5:00 AM SEOUL, South Korea — Computer networks at major South Korean banks and top TV broadcasters crashed en masse Wednesday, paralyzing bank machines across the country and prompting speculation of a cyberattack by North Korea.

Why cyber crime remains a growing business

03/20/2013 05:54 (Computerworld Malaysia)

And how to put a dent in it Cyber crime is big business. And it is growing in scope and impact. But what may not be obvious to the casual observer is that cyber crime is growing in its magnitude and sophistication because of two key factors: the consumerisation of crimeware, and the adoption of ti

Cyberattacks: The new normal

03/20/2013 05:29 (ColoradoBIZ Magazine)

It’s time to elevate the importance of cybersecurity

AIG Among Insurers Seeking More Sales as Small Firms Get Hacked

03/20/2013 00:59 (Bloomberg)

Jim Throneburg invented Thorlos socks in 1980 and set out to build a brand worthy of the slogan, “caretakers of the world’s feet.” His company, Thorlo Inc.

Rising cyber-nationalism leads to amplified cyber-mistrust

03/20/2013 00:29 (Computer World Singapore)

Recent news stories about Chinese cyberattacks on the networks and reporters at The New York Times, the Washington Post and The Wall Street Journal -- all of which recently made startling admissions about them -- have put the topic in the public limelight in a way not seen since Google’s claims two

SC Senate committee advances cyber-security bill

03/19/2013 21:43 (ABC News 4)

COLUMBIA, S.C. (AP) - A South Carolina Senate committee has advanced a measure that creates more oversight of public agency computer systems following the massive breach of the state’s tax collection agency.

Sandia’s Cyber Lab Opens

03/19/2013 18:21 (Isssource.com)

With a warning of “malicious cyber activity” hitting the industry, Sandia National Laboratory’s Cyber Engineering Research Laboratory (CERL) formally opened last month.

Pope-Themed Emails Lead Readers to Malware

03/19/2013 17:44 (Yahoo! News Canada)

A new age of piracy: Sailing the cyber seas

03/19/2013 17:31 (The Charlatan)

SC hacking bill heads to Senate floor

03/19/2013 16:54 (TheState.com)

A bill that could give victims of the nation’s largest-ever hacking of a state agency 10 years of free credit monitoring is heading to the S.C. Senate floor.

Data breach affects 25K at Mass. university

03/19/2013 15:41 (SecurityInfoWatch.com)

March 16--SALEM -- The personal information of 25,000 Salem State University employees may be at risk after one of the college’s computer servers was infected with a virus.

Attacks on SCADA, ICS Honeypots Modified Critical Operations

03/19/2013 15:04 (Threat Post)

With antiquated gear running the country’s industrial control systems that oversee critical infrastructure, it’s no shock attackers targeting SCADA networks do their fair share of reconnaissance looking for weak spots in that equipment.

Mandiant: Chinese hacker unit attempted to clean up online presence

03/19/2013 14:33 (The Hill - Blog)

An elite unit of Chinese hackers that allegedly waged a massive cyber-espionage campaign against U.S. companies has attempted to clean up their online presence after being identified in a public report by information security firm Mandiant.

DOE reveals data disclosure involving 12,000 workers

03/19/2013 13:44 (The Augusta Chronicle)

Federal authorities are investigating a security breach in which personal information from at least 12,000 Savannah River Site workers was compromised last month.

Malware pushers poison MSN Messenger search results

03/19/2013 13:26 (Help Net Security)

As the date when the MSN Messenger is scheduled to be phased out speedily approaches, it is getting harder to find an installer for it online, so malware peddlers gave rushed in to fill the vacuum, warns Kaspersky Lab's Fabio Assolini.

Keeping the Lights On: Cyber Terrorism and the Power Grid

03/19/2013 10:36 (Lexington Institute)

Homeland Security Today The clear and present danger of cyber threats to our critical infrastructure, such as the national power grid, can no longer be ignored.

Hacking as an act of war

03/19/2013 10:21 (Help Net Security)

Once the exclusive domain of a small number of geniuses, hacking has gone mainstream as an element of national defense. The United States has established a four-star Cyber Command to provide coordinated military digital response after suffering massive data breaches.

Cybersecurity Standards Dodged by U.S. FCC Panel

03/19/2013 08:55 (Bloomberg)

A U.S. advisory panel failed to reach consensus on recommendations to telecommunications companies and Internet providers on how to bolster their computer systems against cyber attack.

South Korea's 'Top Gun' cyber warriors

03/19/2013 05:23 (Computer World Singapore)

Cheon Joon-Sahng may not look like an elite warrior, but the shy, South Korean high school student has been fully trained for a frontline role in any future cyber battle with North Korea.

Credit report breach has link to Zeus banking malware

03/19/2013 04:45 (Computerworld Malaysia)

A website that leaked credit reports of celebrities and government officials last week appears to have a curious link to the malicious banking software known as "Zeus.

Chesapeake warns of cyber attack risks

03/19/2013 03:30 (Tulsa World (AP))

Last Modified: 3/19/2013 2:30 AM OKLAHOMA CITY - Chesapeake Energy Corp. warned investors Monday about potential cyber attacks. Included in a 14-page section on potential risks affecting Chesapeake and its debt offerings, the Oklahoma City-based energy natural gas company said it has been "the sub

U.S. telecoms prevail in arguing against cybersecurity recommendations

03/19/2013 00:15 (The Guardian)

WASHINGTON (Reuters) - Large telecommunications companies and Internet providers succeeded in convincing an advisory panel that the U.S. government should not pursue enforcement of security measures meant to bolster their defences against the growing threat of cyber attacks, according to a report re

Google Chrome: Best security tips for safer browsing

03/18/2013 22:16 (Computerworld Malaysia)

There's a lot to like about Google Chrome's built-in security features. But like all browsers, Chrome is imperfect, and there are steps you can take to protect it from attack.

7NEWS is granted first access to Boulder computer crime lab where digital evidence is uncovered

03/18/2013 21:40 (TheDenverChannel)

How Boulder team is uncovering digital evidence

New China leader Xi to meet U.S.'s Lew to discuss cyber row, trade

03/18/2013 20:29 (Reuters.co.uk)

BEIJING (Reuters) - U.S. Treasury Secretary Jack Lew will meet new Chinese President Xi Jinping on Tuesday at a critical time in relations between the world's two largest economies, with cyber hacking, the Chinese currency and market access high on the agenda for talks.

Fighting the global cybersecurity crisis locally

03/18/2013 19:02 (Times Union)

Cyber Teaching Hospital trains tech students to detect, prevent attacks

Honeypots Show ICS' Under Attack

03/18/2013 18:22 (Isssource.com)

To show just how vulnerable SCADA systems are, it took just 18 hours for attacks to occur on series of honeypot SCADA systems set up by Trend Micro. On top of that over a 28-day period, these honeypots suffered an attack 39 times from 11 different countries.

AT&T 'hacker' Andrew 'Weev' Auernheimer goes to jail: An explainer

03/18/2013 17:53 (Yahoo! News)

A master troll will serve 41 months in prison for what many argue is not even a cybercrime The internet is going nuts over the 41-month sentence handed down to Andrew 'Weev' Auernheimer, the so-called AT&T hacker who collected and publicly released over 100,000 user email addresses back in 2010.

US Cyber Command to Take Offensive

03/18/2013 15:14 (Hawaii Reporter)

By Matthew Hilburn - The U.S. Department of Defense has made a rare acknowledgement that it is developing offensive cyber capabilities. In testimony before the Senate Armed Services Committee this past week, Gen.

Cyberattack In South Florida Is First Known Hack On Election Data: Report

03/18/2013 15:10 (International Business Times)

The first known case of a cyberattack against online election data has occurred in South Florida, where more than 2,500 “phantom requests” for absentee ballots were reportedly recorded last summer.

Is a "Cyber Pearl Harbor" Looming?

03/18/2013 12:48 (Yahoo! Canada Finance)

Who is attacking industrial control systems?

03/18/2013 10:40 (Help Net Security)

Since the discovery of Stuxnet, industrial control systems (ICS) and supervisory control and data acquisition (SCADA) networks have received a fair share of attention from researchers and attackers alike.

Florida Cyberattack On Absentee Ballot Site Is First Known Case Of Online Election Tampering: Report

03/18/2013 03:38 (The Huffington Post)

A Florida website became the first known target of an election-focused cyberattack last year, when more than 2,500 "phantom requests" for absentee ballots were made from international locations, NBC News reported Monday.

Android malware analysis tool

03/18/2013 03:45 (Help Net Security)

Bluebox Labs announced Dexter, a free tool to help researchers and enterprise security teams analyze applications for malware and vulnerabilities. The Dexter platform provides software architecture information presented through a web-based user interface.

Virtual classroom for incident response

03/18/2013 02:43 (Help Net Security)

To provide digital investigators and other incident responders the tools and skills to detect and respond to targeted attacks, HBGary announced a series of new live online training courses.

Man faces sentencing in iPad data breach case

03/18/2013 01:20 (The Providence Journal (AP))

NEWARK, N.J. (AP) — A man convicted in connection with the theft of more than 100,000 email addresses of Apple iPad users faces sentencing. Andrew Auernheimer is scheduled to appear in federal court in Newark Monday.

Air Force looks to reboot civilian cyber workforce

03/18/2013 01:11 (FederalNewsRadio.com)

The Air Force believes it's done a good job developing a coherent workforce strategy for its uniformed cadre of cyber workers. But it's less satisfied with how it's done so far at managing the career fields of their civilian counterparts.

Cyberattacks sound alarms, spark DC scramble to bolster defenses

03/18/2013 01:00 (The Hill - Blog)

Fears the United States could fall victim to a catastrophic cyberattack have reached a new high in the capitals of business and politics. With just a few strikes on a keyboard, officials warn, hackers could knock out the electric grid of a major city, leaving millions without power or heat.

Fears over cyber-threat control increase

03/18/2013 00:00 (The Province)

Vulnerability database hack highlights need to bolster cybersecurity

03/17/2013 23:49 (Computer World Singapore)

The recent hack of the National Vulnerability Database (NVD) is one more example of the need for a stronger U.S. cybersecurity strategy. President Barack Obama pressed for such an initiative in meetings Wednesday and Thursday with corporate leaders, Bloomberg News reports.

Cyberthreats getting worse, House intelligence officials warn

03/17/2013 22:30 (KDBC)

Ashley Killough, CNN CNN — The highest-ranking officials on the House intelligence committee continued to warn Sunday of the increasing cybersecurity threat to the U.

Finance sector under threat from sophisticated malware threat

03/17/2013 22:18 (Computer World Singapore)

The financial sector is under threat from increasingly sophisticated malware attacks a Symantec report has claimed, with many security solutions ineffective against modern Trojans.

HCSO Operation Cyber Storm Results In Multiple Child Pornography Arrests

03/17/2013 18:56 (Osprey Observer)

By tamas mondovics The Hillsborough County Sheriff's Office Internet Predator Unit (IPU), led by Detective Phil Dubord, conducted an initiative last month to identify and arrest individuals who are engaged in the illegal receipt, possession, production and distribution of child pornographic materia

Washington Police Dept. investigates with new computer crime lab

03/17/2013 17:54 (CINewsNow)

Updated Mar 17, 2013 at 4:42 PM CDT WASHINGTON, Ill -- Detective Commander Jeff Stevens is working with the Washington Police Department's newest resource, a 16-gigabyte computer called a Forensic Recovery of Evidence Device, or F.

Utilities warned about threat of cyberattacks

03/17/2013 03:13 (Daily Republic)

SAN JOSE — California utility officials are warning that hackers increasingly target utilities with cyberattacks that could leave millions of people without electricity, water and other vital services.

An internet without privacy

03/17/2013 02:34 (KDBC)

(CNN) — (CNN) -- I'm going to start with three data points. One: Some of the Chinese military hackers who were implicated in a broad set of attacks against the U.

China, U.S. should stop war of words on hacking, says new Chinese premier

03/17/2013 02:19 (Orlando Sentinel)

BEIJING (Reuters) - China and the United States should avoid "groundless accusations" against each other about cyber-security and hacking into each other's computer systems, newly installed Premier Li Keqiang said on Sunday.

Experts warn utilities increasingly vulnerable to cyberattacks that threaten power, water

03/16/2013 05:08 (Daily Journal)

SAN JOSE, California — California utility officials are warning that hackers increasingly target utilities with cyberattacks that could leave millions of people without electricity, water and other vital services.

25,000 could be affected by data breach at SSU

03/16/2013 04:07 (NewburyportNews.com)

SALEM — The personal information of 25,000 Salem State University employees may be at risk after one of the college's computer servers was infected with a virus.

Social media editor at Reuters Matthew Keys charged in hacking of L.A. Times story

03/15/2013 06:04 (ABC Action News)

SAN FRANCISCO - A journalist has vowed that Friday would be "business as usual" despite charges of conspiring with the notorious hacking group "Anonymous" to deface an online story of the Los Angeles Times.

Is All The Talk About Cyberwarfare Just Hype?

03/15/2013 05:56 (GPB)

U.S. government pronouncements about the danger of a major cyberattack can be confusing. The director of national intelligence, James Clapper, and the head of the U.

Patching for industrial cyber security is a broken model

03/15/2013 01:41 (Help Net Security)

New research from Belden shows that patching is often ineffective in providing protection from the multitude of vulnerability disclosures and malware targeting critical infrastructure systems today.

White House employs cross-agency goals to broaden oversight of cyber

03/15/2013 01:26 (FederalNewsRadio.com)

The White House is re-energizing two long-standing cybersecurity initiatives by getting more than just the chief information officer involved. The administration recently updated all 14 cross-agency priority goals on the Performance.

US NIST’s vulnerability database hacked

03/14/2013 22:25 (Computer World Singapore)

A U.S. government computer vulnerability database and several other websites at the National Institute of Standards and Technology have been down for nearly a week after workers there found malware on two Web servers.

Obama, China’s Xi Discuss Cyber Security Dispute in Phone Call

03/14/2013 18:36 (Albuquerque Express)

WASHINGTON President Barack Obama took mounting U.S. concerns about computer hacking straight to China's president on Thursday in a sign of how seriously the United States takes the threat of cyber attacks emanating from China.

Cyber Attack Teams Forming

03/14/2013 18:25 (Isssource.com)

In a move to protect the U.S. against major computer attacks from abroad, the Pentagon's Cyber Command will create 13 offensive teams by the fall of 2015, National Security Agency (NSA) Director Gen.

Hackers hit Obamas, how to protect yourself

03/14/2013 18:14 (9News.com)

KUSA - President Barack Obama met with CEOs Wednesday to discuss cyber security legislation. It's an issue that hits home in the White House after hackers posted what appears to be First Lady Michelle Obama's personal financial information.

Private, Public Sector Share Data

03/14/2013 18:05 (Isssource.com)

Government has been talking about working and sharing security information with the private sector for quite some time and it seems it is now coming to fruition under the Enhanced Cybersecurity Services (ECS) program.

Report: Facebook No Longer Supporting CISPA

03/14/2013 17:03 (Game Politics)

Facebook is no longer listed as a supporter of the Cyber Intelligence Sharing and Protection Act (CISPA), according to this CNET report. Facebook and its CEO were singled out by activist group Demand Progress, who sent an avalanche of emails to CEO Mark Zuckerberg with the message: "You're encourag

US Cyber command creates 40 new teams for protection and attacks

03/14/2013 14:21 (Digital Journal)

Companies buying cyber insurance increased 33% in 2012, says Marsh

03/14/2013 13:34 (Canadian Underwriter)

Encrypting Trojan targets users, demands $5,000

03/14/2013 12:54 (Help Net Security)

Russian anti-virus company Doctor Web is warning users of an active ransomware campaign executed through brute force attack via the RDP protocol on target machines.

DHS cybersecurity chief to head to The Chertoff Group

03/14/2013 12:20 (The Hill - Blog)

Mark Weatherford, deputy under secretary for cybersecurity at the Department of Homeland Security (DHS), is leaving the department after a little over a year to serve as a principal at The Chertoff Group.

New Attacks Leverage Adobe Sandbox Bypass Against Uyghur Activists

03/14/2013 12:06 (Threat Post)

Attackers with a control infrastructure based in China are leveraging the same vulnerability exploited by Miniduke to attack Uyghur and Tibetan activists with new exploits.

Formula One team under cyberattack in Cyber Security Challenge UK

03/14/2013 11:05 (MyFoxHouston)

In a face-to-face final cyberbattle, one unlikely Brit proved the ultimate weapon against an attack on a Formula One Team. The Cyber Security Challenge UK -- essentially the Olympics of cybergames -- aims to locate the next generation of tech whiz kids.

CID warns of email scam, criminals posing as police

03/14/2013 10:01 (Fort Drum)

WASHINGTON – The U.S. Army Criminal Investigation Command, commonly referred to as CID, is warning both the Army community and the public about a new Internet phishing scam where criminals are attempting to pose as Army CID officials.

TexMessage: Cybersecurity experts urge Congress for stronger public-private partnership

03/14/2013 09:53 (San Antonio Express-News - Blogs)

CommentsComments(1)Comments() | E-mail | Print TexMessage Thursday, March 14 Good morning, TexMessagers! Is Congress doing enough to keep our electronic infrastructure secure? TEXclusive A Department of Homeland Security deputy secretary and cybersecurity chiefs from companies like Houston'

China hacker opens window into cyber-espionage

03/14/2013 15:01 (HeraldNet.com)

BEIJING -- For a 25-year-old computer whiz enlisted in a People's Liberation Army hacking unit, life was all about low pay, drudgery and social isolation.

ICS Patching Ineffective

03/14/2013 08:03 (Isssource.com)

By Gregory Hale Patching is often ineffective in providing protection from the multitude of vulnerability disclosures and malware targeting critical infrastructure systems today, new research shows.

DoD puts 1 million users in its cloud email system

03/14/2013 06:01 (FederalNewsRadio.com)

The Defense Department migrated its one millionth user into its enterprise email system this week. The Army expects to almost completely transition its unclassified accounts into the cloud service within the next month, meanwhile, the Navy and Air Force are kicking the tires on the system.

Java's security problems unlikely to be resolved soon, researchers say

03/14/2013 04:00 (Computer World Singapore)

Since the start of the year, hackers have been exploiting vulnerabilities in Java to carry out a string of attacks against companies including Microsoft, Apple, Facebook and Twitter, as well as home users.

Researchers find German-made spyware across globe

03/14/2013 02:42 (News Tribune)

LONDON (AP) — The discovery of a group of servers linked to an elusive espionage campaign is providing new details about a high-tech piece of spy software that some fear may be targeting dissidents living under oppressive regimes.

Obama pushes cybersecurity legislation

03/14/2013 02:15 (Saukvalley.com)

Obama talks with CEOs about cybersecurity bill

For China, New Era Brings New Set of Problems

03/14/2013 02:05 (CNBC)

Senior Writer Getty Images China's newly-elected President Xi Jinping (R) talks with former President Hu Jintao (L) during the fourth plenary meeting of the National People's Congress at the Great Hall of the People on Thursday in Beijing.

Not ready for cyberwar

03/14/2013 01:00 (HeraldTribune.com)

A recent report by a task force of the Defense Science Board on cyber-conflict makes clear that all is not well in preparing for this new domain of warfare.

New Google site aimed at helping webmasters of hacked sites

03/14/2013 00:08 (Computerworld Malaysia)

Google wants to aid webmasters in identifying site hacks and recovering from them. Google has launched a site for webmasters whose sites have been hacked, something that the company says happens thousands of times every day.

China, in fact, does not hack the most

03/13/2013 23:57 (Alaska Dispatch)

Email Print Text Size -A +A Where do most hackers call home? Russia, in fact. Next up is Taiwan, followed by Germany, Ukraine, Hungary, and -- surprise -- America, according to monitoring done by Deutsche Telekom's Sicherheitstacho project cited by Bloomberg's Businessweek.

America's 3 Biggest Cybersecurity Vulnerabilities

03/13/2013 21:12 (Yahoo! News)

When James Clapper, the country's top intelligence official, visited Capitol Hill this week to discuss the major threats facing America, he put cyberattacks at the top of the list.

AFP takes cyber safety to the people

03/13/2013 20:36 (Computer World Australia)

Commander Glen McEwen says education and partnerships are helping to raise cyber safety awareness

US Intelligence officials outline cyber threat

03/13/2013 17:56 (TG Daily)

US intelligence officials have ranked the specter of cyber-attacks as a major threat on par with concerns over terrorism and North Korea. Indeed, James Clapper, the Obama administration's national security director, said he hasn't seen as more diverse array of threats and challenges for US national

Cyber threats against U.S. 'ramping up,' Obama says

03/13/2013 17:55 (Yahoo! News Canada)

Gone Phishing in Dallas

03/13/2013 16:03 (Isssource.com)

Phishing attacks are gaining in popularity across the globe because they are very effective and work well, and in the U.S., it appears Dallas, TX, is the home of the most carriers for these types of cyber assaults, a new study said.

Microsoft Security Patches Rolling Hard and Fast in 2013

03/13/2013 15:32 (CIO Today)

"We can only hope that this increase is due to a combination of new platforms and better discovery of vulnerabilities, rather than actual ongoing security problems at Microsoft," said security analyst Paul Henry. In 2013, Microsoft is averaging close to nine security patches monthly, including four

The older population is at higher risk of becoming a victim of fraud

03/13/2013 12:46 (KLEW TV)

MOSCOW, ID - Senior citizen fraud has been a hot topic on the Palouse as of late, but there are solutions to the problem. "Identity theft has become, or is becoming a more serious problem," said My Own Home Executive Director Tom La Pointe.

Cell Phone Viruses--The New Threat

03/13/2013 12:43 (The Cutting Edge)

The Digital Edge

U.S. officials say North Korea poses serious threat

03/13/2013 15:01 (HeraldNet.com)

WASHINGTON -- An unpredictable North Korea, with its nuclear weapons and missile programs, stands as a serious threat to the United States and East Asia nations, the director of National Intelligence warned Tuesday in a sober assessment of worldwide threats.

Cyber attack stops access to JPMorgan Chase site

03/13/2013 13:36 (Chicago Tribune)

The consumer banking website of JPMorgan Chase & Co was unavailable to some users on Tuesday as the company tried to deal with a denial-of-service cyber attack that slowed access for some customers.

Cyber attacks rated higher than terrorism as security risks, U.S. intel experts say

03/13/2013 12:12 (Pittsburgh Post-Gazette)

WASHINGTON -- Cyber attacks and cyber espionage pose a greater potential danger to U.S. national security than al-Qaida and other militants who have dominated America's global focus since Sept.

DoD constructing offensive, defensive cyber teams

03/13/2013 06:13 (FederalNewsRadio.com)

The Defense Department is creating dozens of teams to protect its computer networks and go after bad guys. But like so many initiatives, the cuts from sequestration threaten these teams in multiple ways.

Obama to meet corporate leaders to discuss ways to strengthen cyber security

03/13/2013 05:31 (Albuquerque Express)

President Barack Obama will be meeting corporate leaders to discuss efforts to improve cyber security in private industries amid rising concern about hacking attacks from China.

Lawmakers: Cyber defenses are evolving slowly

03/13/2013 04:41 (Politico)

There remains significant trepidation on Capitol Hill that the Pentagon's hub for cybersecurity defenses is maturing slowly, even as the Obama administration emphasizes in its clearest terms to date that hackers and spies are one of the country's most serious threats.

New cyber medal production stopped, being reviewed

03/13/2013 04:16 (News Tribune)

WASHINGTON (AP) — The military has stopped production of a new medal for remote warfare troops — drone operators and cyber warfighters — as it considers complaints from veterans and lawmakers over the award, which was ranked higher than traditional combat medals like the Purple Heart and Bronze Star.

Not ready for cyberwar

03/13/2013 02:56 (Daily Herald (AP))

The following editorial appeared in Tuesday's Washington Post: A recent report by a task force of the Defense Science Board on cyber-conflict makes clear that all is not well in preparing for this new domain of warfare.

Hackers Attack Bank Minutes After NSA Chief Warns Senate About Hackers Attacking Banks

03/13/2013 00:06 (Yahoo! News)

Gen. Keith Alexander, director of the National Security Agency, took the stand in front of the Senate Armed Services Committee on Tuesday and an ambitious expansion of the Pentagon's Cyber Command.

Obama to meet CEOs on cyber security

03/12/2013 23:58 (Yahoo! News)

By Steve Holland WASHINGTON (Reuters) - President Barack Obama will sit down on Wednesday with corporate leaders to discuss efforts to improve cyber security in private industries amid rising concern about hacking attacks emanating from China.

Microsoft's latest patches squash potential USB hijack

03/12/2013 22:24 (Computer World Singapore)

As part of its monthly issue of software patches, Microsoft has fixed a Windows vulnerability that would have allowed someone to subvert a computer's security using only a USB thumb drive and some attack code.

Obama Security Adviser Rebukes China on Cyberattacks

03/12/2013 19:08 (CIO Today)

"Its important for people to understand that attackers in China don’t have to launch their attacks from China," said security researcher Tom Cross. "They can break into computers anywhere in the world and launch their attacks from any geographic location." National Security Adviser Tom Donilon has c

Life of a Botnet: Growth in Spurts

03/12/2013 18:03 (Isssource.com)

Botnets come and botnets go and some just chug along on their merry way delivering spam and malicious emails to the masses on a daily basis. But the good news is McAfee’s latest threat report found there is a continuing decline in global messaging botnet infections.

Pentagon Forming Cyber Teams To Combat Electronic Attacks

03/12/2013 17:36 (CBS DC)

WASHINGTON (AP) — The Defense Department is establishing a series of cyber teams charged with carrying out offensive operations to combat the threat of an electronic assault on the United States that could cause major damage and disruption to the country’s vital infrastructure, a senior military off

Three things you should do if you get hacked

03/12/2013 17:34 (News 10)

Federal authorities are investigating a website that leaked personal information on government officials including FBI Director Robert Mueller and celebrities including Jay-Z and Kim Kardashian.

US seeks ’serious’ action by China on cyber theft

03/12/2013 15:01 (HeraldNet.com)

WASHINGTON -- The White House is calling for "serious steps" by China to stop cyber theft that is intolerable to the international community. National Security adviser Tom Donilon’s comments Monday reflect growing concern in Washington over the security risk posed by cyber intrusions and the econom

Raytheon, Lockheed get U.S. secrets as cybersecurity go-betweens

03/12/2013 15:01 (HeraldNet.com)

WASHINGTON -- Lockheed Martin and Raytheon are vying with telecommunications companies to defend banks and power grids from computer attacks, in a program that gives them access to classified U.

Consumers 'prime targets' for ID theft

03/12/2013 14:13 (Standard-Examiner)

For the fifth consecutive year, identity theft is at the top of the Federal Trade Commission's list of consumer complaints. With more than 2 million complaints lodged nationwide in 2012, including 369,132 related to identity theft, national and local agencies are encouraging the public to take ever

Donilon issues stern cyber warning to China

03/12/2013 12:50 (DoD Buzz)

U.S. National Security Adviser Tom Donilon stopped speaking in vagaries on Monday and called China out by name for the high number of cyber attacks coming from China that target U.

Hackers attack website of Czech UniCredit Bank

03/12/2013 10:57 (Yahoo! News)

PRAGUE (Reuters) - Hackers attacked the website of UniCredit Bank's Czech unit late on Monday, causing a five-minute outage, but no customer data was compromised, a spokesman said.

China says willing to discuss cyber security with the U.S.

03/12/2013 10:17 (Yahoo! News)

By Terril Yue Jones BEIJING (Reuters) - China offered on Tuesday to talk with the United States about cyber security amid an escalating war of words between the two sides on computer hacking, but suspicion is as deep in Beijing as it is in Washington about the accusations and counter-accusations.

White House calls on China to put a stop to hacking

03/12/2013 08:42 (TG Daily)

A senior White House official has demanded that China stop hacking US computer systems and agree to a set of international rules on behavior in cyberspace.

Identity Theft By the Numbers – Facts and Trivia

03/12/2013 07:22 (Cash Money Life)

Sometimes people don't think about an adverse situation until they see the actual statistics. Cold. Hard. Facts. Identity theft and other forms of theft are uncomfortable to think about, but they are real.

How to Detect and Avoid IRS Tax Scams and Identity Theft

03/12/2013 07:22 (Cash Money Life)

There is a phishing scam going around purporting to be from the IRS. In this e-mail, they inform the recipient they are entitled to refunds of $92.35 or some other amount due to a calculation error on a past tax return.

Tax Fraud – Signs You May be a Victim of a Fradulent Tax Return

03/12/2013 07:22 (Cash Money Life)

Identity theft is a big enough disaster all by itself, but when it brings us into closer contact with the Internal Revenue Service, that adds a whole other dimension to the picture.

US calls on Chinese government to crack down on hacking

03/12/2013 07:00 (The Guardian)

Obama’s national security adviser urges China to recognise risk cyber-attacks pose to international relations

Local teens warn of the dangers of unprotected Wi-Fi connection

03/12/2013 05:47 (WCFCourier.com)

CEDAR FALLS, Iowa --- Nearly a month ago a small group of Cedar Falls teenagers piled into a car to spend an afternoon driving through the city. They meticulously worked their way through mostly residential areas bordered by the University of Northern Iowa, Fourth Street, Hudson Road and Main Stree

Cyber Attackers’ Tactics Outpace Companies’ Responses

03/12/2013 04:00 (Bloomberg)

The tactics of hackers, cyber- criminals and state-sponsored spies are evolving so quickly that attackers often can re-enter a company’s networks after being detected and banned, according to a U.

In cyberwarfare, rules of engagement still hard to define

03/12/2013 03:17 (The Oakland Press)

When Gen. Keith Alexander, the head of the Pentagon’s Cyber Command, comes to Capitol Hill on Tuesday, he will probably be asked to describe his plans for building a military force to defend the nation against cyberattacks.

Hackers target grocery store card readers

03/12/2013 02:52 (KVOA.com)

by Lupita Murillo SIERRA VISTA - Residents in Southeastern Arizona are trying to recover after becoming victims of identity theft involving one of Arizona’s grocery chains.

Reporters Without Borders slams five nations for spying on media, activists

03/12/2013 00:21 (Computerworld)

The press freedom advocate called for more harmonized controls over the export of spying technology

US tells China to halt cyberattacks, and in a first, lays out demands

03/11/2013 23:53 (Yahoo! News)

Obama’s national security adviser, Thomas Donilon, spelled out a more aggressive US stance on the cyberattacks, saying China must recognize the problem, investigate it, and join in a dialogue.

15 percent of companies have no BYOD policy

03/11/2013 23:28 (Help Net Security)

ThreatMetrix announced results of a study that surveyed U.S. business managers and IT executives within retail and financial services organizations on their level of cybersecurity planning and fraud prevention solutions.

Week in review: Evernote breached, Java woes and cloud security

03/11/2013 23:25 (Help Net Security)

Here’s an overview of some of last week’s most interesting news, videos, reviews and articles: Evernote breached, forces service-wide password reset The investigation has shown that the attackers were able to gain access to user information, which includes usernames, email addresses associated with

Raytheon, Lockheed to Get U.S. Secrets for Cybersecurity

03/11/2013 04:01 (Bloomberg)

Lockheed Martin Corp. (LMT) and Raytheon Co. (RTN) are vying with telecommunications companies to defend banks and power grids from computer attacks, in a program that gives them access to classified U.

The Android malware problem is not hyped, researchers say

03/11/2013 02:26 (Computer World Singapore)

Recent reports from antivirus companies seem to suggest that the number of Android malware threats is growing. However, there are still many skeptics who think that the extent of the problem is exaggerated.

Framing itself as a Victim, China Calls for a Global Crackdown on Hackers

03/11/2013 02:11 (Yahoo! News)

In between swipes at the United States, China's foreign minister Yang Jiechi called for new "rules and cooperation" against cyber attacks at the annual session of the National People's Congress this weekend.

UPDATE 1-Australia central bank says no information lost in cyber attacks

03/11/2013 01:31 (Reuters.co.uk)

SYDNEY, March 11 (Reuters) - Australia's central bank confirmed on Monday it had been targeted by cyber attacks and that no data had been lost or systems compromised, but would not comment on a media report that a malware virus used in one attack was Chinese in origin.

What's next for cybersecurity after White House order?

03/11/2013 00:31 (Computerworld Malaysia)

Senators renew work on cybersecurity legislation in wake of Obama's executive order. Department of Homeland Secretary reiterates administration's position that a comprehensive bill is needed to expand White House directive.

Hotspot 2.0 will power the mobile Internet

03/10/2013 23:23 (Computer World Singapore)

With an estimated 800 million new Wi-Fi-enabled devices entering the mobile market each year, new Wi-Fi networks are emerging to connect businesses and users inside public venues ranging from malls and airports to hotels, schools and universities.

How I ditched the security risks and lived without Java, Reader, and Flash

03/10/2013 23:12 (Computer World Singapore)

Adobe Flash, Adobe Reader, and Oracle's Java. All three are virtually ubiquitous on modern-day PCs, and all three provide handy-dandy functionality--functionality that, in the case of Flash and Java, can't be directly reproduced by a third-party solution.

The 4 security controls your business should take now

03/10/2013 23:12 (Computer World Singapore)

There never will be a perfect computer or network defense. Computer security is a constantly elevating game of cat-and-mouse. As quickly as you address the latest threat, attackers have already developed a new technique to access your network and compromise your PCs.

FTC crackdown on text spammers highlights business threat

03/10/2013 21:47 (Computer World Singapore)

The Federal Trade Commission's recent crackdown on organizations suspected of sending millions of spam text messages puts a dent in an illicit activity that threatens businesses and consumers.

Guarding your personal information

03/10/2013 21:25 (9News.com)

DENVER - Colorado is among the states with the highest number identity theft cases, which is why you can never be too careful about your personal information - even in places or circumstances that may not be top of mind.

Cybersecurity challenges in 2013

03/10/2013 21:24 (Computer World Singapore)

The security issues affecting businesses are similar around the world. Most involve employees innocently bringing an infected personal mobile device into the corporate network, or clicking on a social media link that looks harmless but hides a Trojan or worm that will secretly steal data and money a

Obama rejected tough options for countering Chinese cyber attacks two years ago

03/10/2013 20:41 (The Washington Times)

President Obama two years ago rejected a series of tough actions against China, including counter-cyber attacks and economic sanctions, for Beijing's aggressive campaign of cyber espionage against the U.

<u>On Computers: After 30 years, rebooting your computer still important</u>

03/10/2013 13:00 (CantonRep.com)

"Last night, I heard my computer rebooting. Is this a virus or something?" Not to worry. A spontaneous reboot most often is caused by Windows Update, the option that checks for updates and installs them.

<u>Use the Internet Safely with a VPN</u>

03/10/2013 12:33 (U Publish Articles)

<u>Cyber security requires public, private cooperation</u>

03/10/2013 12:01 (Springfield News-Sun)

President Barack Obama's executive order calling for increased information sharing between the federal government and private companies to protect the nation's critical infrastructure against cyber-attacks is a good first step, despite concerns about government regulation and data privacy, experts s

<u>Beware of attempts to get sensitive information</u>

03/10/2013 06:54 (HometownLife.com)

Identity theft is a year-round problem, but income-tax season is an especially busy time for people who try to scam the government while posing as someone else, according to police and the Internal Revenue Service.

<u>Almost all mobile malware now targets Android</u>

03/08/2013 08:50 (TG Daily)

As Apple likes to keep reminding us, Android is the biggest target for mobile malware - and, according to F-Secure, it's getting more so all the time. In a new report, the security firm says

Android accounted for 79 percent of mobile malware last year - a whacking 96 percent in the last quarter.

Czech finance sector hit by cyber attacks

03/08/2013 05:39 (ComputerWorld)

The Czech financial sector was targeted in cyber attacks on Wednesday, with the national bank and stock exchange websites disrupted by dedicated denial of service (DDOS) attacks.

Cyber Espionage, National Security … Murder? Computer Forensics May Offer the Best Chance to Find the Truth

03/08/2013 05:16 (Digital Journal)

Bogus alert from Microsoft Digital Crimes Unit carries malware

03/08/2013 03:50 (Help Net Security)

Malware peddlers are impersonating Microsoft’s Digital Crimes Unit to convince users to download a malicious attachment and run it on their computers, warns Sophos.

Cybersecurity program trains students for future

03/08/2013 02:57 (Daily Trojan)

An innovative cybersecurity program established in fall 2003 has grown exponentially. The Viterbi School of Engineering’s master’s degree program for computer science with a specialization in computer security, which was established to help combat the growing threat of cyber attacks, is one of the

Senate hearing spotlights ongoing discord over cybersecurity bill

03/07/2013 23:21 (TVTV - Tanana Valley Portal)

By Alina Selyukh and Deborah Charles WASHINGTON (Reuters) - As the White House and congressional lawmakers resume talks on legislation to improve defenses against cyber-attacks, Homeland Security Secretary Janet Napolitano on Thursday signaled that disagreements remain over a House cybersecurity bi

Cuts Hit Cyber Drills, Security Programs, Napolitano Says

03/07/2013 22:59 (Bloomberg)

The Department of Homeland Security will delay an intrusion detection program to protect U.S. government computers from cyber-attacks and has canceled cybersecurity exercises, Secretary Janet Napolitano said today.

White House puts report on cybersecurity on hold

03/07/2013 22:45 (The Washington Times)

The Obama administration is sitting on a report about the security of federal government computer networks because it is embarrassing, a senior Republican senator said Thursday.

Kaspersky Internet Security 2013 bug can lead to system freeze

03/07/2013 22:38 (Computer World Singapore)

Kaspersky Lab's Internet Security 2013 product contains a bug that can be exploited remotely, especially on local networks, to completely freeze the OS on computers running the software.

Asia Pacific to spend US$39 billion combating malware in 2013

03/07/2013 20:59 (Computer World Singapore)

Fighting cyber crime is expensive and the cost of dealing with the impact of malware-induced cyber attacks for enterprises in Asia Pacific will reach US$39 billion in 2013.

Are Apple's Macs becoming more vulnerable to malware?

03/07/2013 18:40 (Inside Bay Area)

The biggest vulnerability to Macintosh computers is the belief among their devoted users that Apple's (AAPL) superior operating system makes them immune to malware, experts say.

CSA Report: Top Nine Cloud Security Threats in 2013

03/07/2013 18:22 (CloudTimes)

Cloud Security Alliance (CSA), a non-profit industry organization that promotes the protection techniques in the cloud, has recently updated its list of the top threats of cloud in the report entitled “The Notorious Nine Cloud Computing Top Threats in 2013”.

Senate looks to pass cybersecurity legislation this year, but divisions remain

03/07/2013 18:18 (The Hill - Blog)

Despite its failure to pass a bill last year, the Senate is resolved to get back to work on legislation targeted at securing the country against cyberattacks.

Companies want US lawsuit shield for sharing cyber threat data

03/07/2013 17:20 (Telegram.com)

A month after President Barack Obama issued an executive order on strengthening U.S. cybersecurity, companies want Congress to provide incentives for joining the federal push for sturdier computer defenses.

Army CID warns of email phishing scam

03/07/2013 13:23 (Army Times)

If you get an email that appears to come from “US-Army-Criminal-Investigation-Command@usa.com,” it’s a phishing scam. The real Army Criminal Investigation Command, also known as CID, is warning the public that criminals are posing as Army law enforcement officials in an email that is making the rou

Report finds global patchwork of laws could hinder growth of cloud businesses

03/07/2013 11:08 (The Hill - Blog)

A patchwork of international laws governing cloud computing services could hinder the expansion and growth of the technology, according to a report released Thursday by BSA | The Software Alliance.

Ex-Gov. Ridge becomes cybersleuth; Time Warner spinning off Time magazines; more

03/07/2013 12:01 (Tribune-Review (AP))

Updated 15 minutes ago Ex-Gov. Ridge becomes cybersleuth in new firm Former Pennsylvania Gov. Tom Ridge and Howard Schmidt, a senior cybersecurity adviser to the George W.

Malaysian organisations must 'beef up' against DDoS assaults

03/07/2013 08:57 (Computer World Singapore)

Fortinet cites the clash between Malaysian and Filipino hackers over the intrusion in Lahad Datu, Sabah, as well as a recent Stratecast study that shows DDoS attacks are increasing by 20 to 45% every year.

Demand for IT security experts outstrips supply

03/07/2013 06:03 (Computerworld)

Employers will pay more for certified -- and experienced -- IT security pros, studies find

Former e-envoy launches new public sector cybersecurity forum

03/07/2013 05:32 (ComputerWorld)

Former local government e-envoy John Thornton has partnered with McAfee to launch the Digital Government Security Forum (DGSF), a new organisation designed to share cybersecurity best practice and thinking between public sector policy makers.

Companies Want Lawsuit Shield to Share Cyber Threat Data

03/07/2013 05:01 (Bloomberg)

A month after President Barack Obama issued an executive order on strengthening U.S. cybersecurity, companies want Congress to provide incentives for joining the federal push for sturdier computer defenses.

Abrupt drop in Symbian malware

03/07/2013 04:17 (Help Net Security)

In what may be the only good news for Symbian, F-Secure's latest Mobile Threat Report shows a drop in malware targeting the declining platform to just four percent of all mobile threats detected in the fourth quarter of 2012, down from an average of 26 percent in the first three quarters.

Top 10 ways to manage cyber risk

03/07/2013 02:16 (ColoradoBIZ Magazine)

The rise of the Internet has its downside

Cloud forensics: In a lawsuit, can your cloud provider get key evidence you need?

03/06/2013 23:28 (Computer World Singapore)

Any business that anticipates using cloud-based services should be asking the question: What can my cloud provider do for me in terms of providing digital forensics data in the event of any legal dispute, civil or criminal case, cyberattack or data breach? It’s going to be different for every provi

Pentagon Warns Of Terrifying ’Existential Cyber Attack’

03/06/2013 22:46 (Yahoo! Canada Finance)

U.S. military networks not prepared for cyber threats, report warns

03/06/2013 21:30 (Computer World Singapore)

The U.S. is dangerously unprepared to face a full-scale cyber conflict launched by a peer adversary, a report by the military’s Defense Science Board (DSB) warns.

Chinese hackers seen as increasingly professional

03/06/2013 20:33 (The Alaska Journal of Commerce)

BEIJING (AP) — Beijing hotly denies accusations of official involvement in massive cyberattacks against foreign targets, insinuating such activity is the work of rogues.

Feds not entitled to all cyber intelligence

03/06/2013 20:19 (SeminoleChronicle.com)

With all the attention and excitement focused on sequestration, Congress has taken the opportunity to introduce, once again, the Cyber Intelligence Sharing and Protection Act that failed to pass the Senate last spring.

DHEC Requests $1.5 Million for Cyber Security

03/06/2013 17:07 (Wltx.com)

Columbia, SC (WLTX) -- The state Department of Health and Environmental Control is looking to keep sensitive information at the agency safe. Director Catherine Templeton told a senate finance committee the department need $1.

Groundbreaking Cyber Fast Track Research Program Ending

03/06/2013 16:32 (Threat Post)

VANCOUVER--When Peiter Zatko, the security researcher and pioneering hacker known as Mudge, joined the federal government several years ago to help run a DARPA research program, some in the security industry wondered what effect someone with his background could have in an organization as famously c

Fake Google Play Accounts Peddling Banking Malware

03/06/2013 16:01 (Threat Post)

On the one year anniversary of Google Play comes news that a new botkit is making the rounds that leverages actual verified accounts from that marketplace to trick users into downloading phony banking applications.

4 Issues to Resolve Before Jumping on the BYOD Bandwagon

03/06/2013 15:16 (Intuit Small Business Blog)

The BYOD trend is here to stay. New research cited by PC World shows that 30 percent of businesses now embrace letting employees bring their own mobile computing devices to work — without restrictions — and that this figure will double to 60 percent by 2016.

65% of firms in U.K. fear a cyber attack in 2013: survey

03/06/2013 14:34 (Canadian Underwriter)

Sen. Whitehouse plans future cyber hearing on combating trade secret theft

03/06/2013 13:33 (The Hill - Blog)

Sen. Sheldon Whitehouse (D-R.I.) on Wednesday said he plans to hold a future hearing on the resources the Justice Department has in place to prosecute the cyber theft of American intellectual property and take action against botnets.

Scammers use fake chat boxes to steal bank info

03/06/2013 12:29 (WDAM - Channel 7)

Rex Hockemeyer with Union First Market Bank says crooks are using fake pop-up chat boxes to collect your personal information. He says, "It is difficult to track and these people are computer programmers, so they are pretty savvy.

Pentagon cyberdefenses are weak, report warns

03/06/2013 12:01 (Pittsburgh Post-Gazette)

WASHINGTON -- A new report for the Pentagon concludes that the nation’s military is unprepared for a full-scale cyber-conflict with a top-tier adversary and must ramp up its offensive prowess.

Cyber Attacks On The Rise

03/06/2013 11:14 (The 9-5-0)

Several Sites Breached in Recent Months

APT1-Themed Spear Phishing Campaign Linked to China

03/06/2013 10:49 (Threat Post)

Researchers at Seculert have discovered a link between spear phishing campaigns targeting Japanese and Chinese journalists, post-Mandiant’s APT1 report, and domains connected to the Aurora attacks on Google and the Shady RAT campaign.

Task force recommends U.S. keep nuclear option as response for massive computer attack

03/05/2013 12:01 (Tribune-Review (AP))

Updated 12 minutes ago The United States should be prepared to use every military option, including nuclear retaliation, in response to a huge computer attack, an independent Department of Defense task force said.

VASCO launches new card reader for transaction signing and PKI applications

03/05/2013 05:55 (Help Net Security)

VASCO launched DIGIPASS 870, a USB connectable card reader which can be used in both connected and unconnected mode. In connected mode DIGIPASS 870 can be used for a number of PKI-based, e-banking or e-wallet applications making use of the 'what you see is what you sign' functionality.

Transparency around cyberattacks increases

03/05/2013 05:37 (The Oakland Press)

At least 19 financial institutions have disclosed to investors in recent weeks that their computers were targets of malicious cyber attacks last year, a sign of growing openness among corporations about the breadth of cybersecurity incidents plaguing the private sector.

Auditing of Web apps with analytics dashboard for compliance

03/05/2013 05:35 (Help Net Security)

SaaSID has launched Cloud Application Manager 2.0 (CAM), the latest version of its browser-based authentication, management and auditing solution. CAM 2.

Nuke option necessary in case of massive cyberwar, report concludes

03/05/2013 05:35 (Stars and Stripes)

The United States should be prepared to use every military option, including nuclear retaliation, in response to a huge computer attack, an independent Department of Defense task force said.

Google Exception in Obama's Cyber Order Questioned as Unwise Gap

03/05/2013 05:01 (Bloomberg)

Telecommunications companies want President Barack Obama's administration to rethink a decision that may exempt Google Inc. (GOOG)'s Gmail, Apple Inc. (AAPL)'s iPhone software and Microsoft Corp.

One-Day Training Event Will Teach Social Media Skills to Law Enforcement

03/05/2013 04:24 (WY Daily)

WYDaily.com is your source for free news and information in Williamsburg, James City & York Counties. If a convicted felon on probation decides to cross state lines while in possession of a firearm, it's not a good idea for them to take a picture of it and post it on Facebook.

Street Lights, Security Systems And Sewers? They're Hackable, Too

03/04/2013 23:27 (Minnesota Public Radio)

Allegations that the Chinese military has been hacking U.S. corporations are raising tensions. But in the case of a full-fledged cyberwar, things would look very different.

Oracle releases emergency fix for Java zero-day exploit

03/04/2013 23:14 (Computerworld Malaysia)

Oracle released emergency patches for Java on Monday to address two critical vulnerabilities, one of which is actively being exploited by hackers in targeted attacks.

Bruning warns about scams aimed at Nebraskans

03/04/2013 23:04 (Yahoo! News)

Nebraska Attorney General Bruning says financial scams are becoming more sophisticated

NCSU: Google's new mobile app verification service misses most malware

03/04/2013 19:03 (WRAL Tech Wire)

Published: 2012-12-10 10:59:00 Updated: 2012-12-10 11:10:06 Post a comment Print this blog postE-mail blog post Share Beware that app! (A screen shot from NCSU report on Google apps screening.

Napolitano: Immigration priority tops cyber

03/04/2013 18:59 (Politico)

Homeland Security Secretary Janet Napolitano reasserted Monday that cybersecurity reform remains a "high priority" for the administration on Capitol Hill — but she emphasized immigration right now tops the list.

IT experts trying to combine innovation with security in tech

03/04/2013 17:59 (Digital Journal)

A Different Way to Fight Malware

03/04/2013 16:24 (Enterprise Efficiency)

One of the top malware security researchers in the world has said that we've been fighting malware the wrong way. Mikko Hypponen, chief research officer of Finnish anti-malware company F-Secure, said that we've focused too much on preventing malware and not enough on recovering from malware infectio

Cyberattacks becoming the new norm in computer industry

03/04/2013 15:58 (Digital Journal)

Phishing Scams And How To Avoid Them

03/04/2013 14:26 (CBS Boston)

BOSTON (CBS) – This is National Consumers Protection Week. This is a national campaign to help consumers avoid being scammed. Billions of dollars are lost each year to scammers.

Blackhole outfitted with exploit for recently patched Java flaw

03/04/2013 13:54 (Help Net Security)

The exploit for the recently patched CVE-2013-0431 Java vulnerability has been added to the Blackhole exploit kit, Trend Micro researchers report. The fact was discovered through the analysis of the latest PayPal-themed spam run that leads to a page hosting the exploit kit.

Kaspersky PURE 3.0 Total Security released

03/04/2013 12:08 (Help Net Security)

Kaspersky Lab released Kaspersky PURE 3.0 Total Security, which offers protection for users to secure their online activities and digital assets across their home network of PCs.

Securing the network beyond passwords

03/04/2013 03:26 (Computerworld Malaysia)

Passwords have been a weakness of network security since the development of computer networks. Through guessing weak passwords, exploiting weak passwords, acquiring passwords through social engineering, or more recently using malicious software like Advanced Persistent Threats (APT), attackers have

China, India top malware ‘victims’ in Asia Pacific

03/04/2013 03:17 (ComputerWorld Singapore)

China and India were the top two "victim" countries in the Asia Pacific, according to a recent Web threat report. Conducted by Web and mobile security firm Websense, the 2013 Threat Report also ranked Taiwan, Philippines, South Korea, Australia, Hong Kong, Vietnam, Singapore, and Malaysia as comple

Chinese hacking motives remain a riddle

03/04/2013 03:00 (The Sacramento Bee)

SAN FRANCISCO – When Telvent, a company that monitors utilities, water treatment plants and more than half the oil and gas pipelines in North America, discovered last September that the Chinese had hacked into its computer systems, it immediately shut down remote access to its clients’ systems to as

Why mobile security is a systemic problem

03/04/2013 00:31 (ComputerWorld Singapore)

There has been considerable hype around each mobile threat vector that has emerged in the last year, but what's often overlooked is how mobile security is currently approached.

Return of CISPA: Cybersecurity boon or privacy threat?

03/03/2013 23:33 (ComputerWorld Singapore)

SAN FRANCISCO -- Rights advocacy groups and security practitioners remain on opposite ends of the spectrum on the merits of sharing information as a means to improve cyber security.

Prices fall, services rise in malware-as-a-service market

03/03/2013 23:33 (Computerworld Malaysia)

Webroot has seen prices starting for a U.S. botnet fall from $200 to $120, thanks to competition, the company says Prices are falling and the number of services is increasing as developers in the online underground compete fiercely for criminals looking to purchase botnets and other tools to mount

Week in review: New Java 0-day, Stuxnet's earliest known version analyzed, and old school malware used for spying on European govts

03/03/2013 23:31 (Help Net Security)

Here's an overview of some of last week's most interesting news, videos, interviews and articles: HTC agrees to fix vulnerabilities found in millions of its devices HTC America has agreed to settle Federal Trade Commission charges that the company failed to take reasonable steps to secure the softw

Hackers use corporate attacks as staging grounds for other cyber assaults

03/03/2013 23:27 (Computerworld Malaysia)

Fighting a corporate cyber intrusion is fraught with legal, insurance considerations, panelists at RSA Conference say. "There may be law enforcement watching it," said Charles Shugg, retired Brigadier General of the Air Force who once headed the U.

How to use the rogue cloud to innovate the right cloud

03/03/2013 23:26 (Computerworld Malaysia)

Employees keep turning to rogue cloud services, storing and sharing highly sensitive information in the public cloud despite IT’s warnings about the dangers, and despite story after story that validates those warnings.

Government calls for guidance on cyber security standards

03/03/2013 22:36 (ComputerWorld Singapore)

The government is calling on industry to provide evidence on what it thinks is the best ’organisational standard’ for effective cyber risk management, which it will then endorse as the preferred approach.

To beat a hacker, you’d better share knowledge

03/03/2013 21:22 (Delawareonline.com)

SEATTLE — There is a silver lining to the rash of revelations about cyberintruders cracking into the networks of marquee U.S. corporations. Microsoft this week admitted to a major network breach, following in the footsteps of Apple, Facebook, Twitter, The New York Times, The Wall Street Journal and

Java breaches and other security news

03/03/2013 18:15 (The Seattle Times)

It’s time to disable or even remove Java from your Mac, and use a virtual private network for Wi-Fi.

Anti-Virus: How Did I Get Infected?

03/03/2013 17:27 (Examiner.com - Delaware)

So you installed the anti-virus software of your choice onto your computer or laptop. One day you realize that you have a virus; a bad one. You may be asking yourself "How did I become infected"? When your computer gets a virus, it brings on many emotions and questions; what, when, how and why to m

Budget cuts bite into cybersecurity

03/03/2013 13:18 (Federal Times)

Anticipated sharp budget cuts will undermine agencies' efforts to guard against cyber attacks, federal and industry officials say. There is a "resource crunch we're all facing today, whether that's sequestration or whether that's just the fact that IT budgets are getting rounded down," said Jeff Ei

Cybersecurity: Your Employees Put You at Risk

03/03/2013 11:28 (Yahoo! Canada Finance)

Private U.S. firms help battle cyberattacks

03/03/2013 01:00 (THonline.com)

Contractors often can act more quickly than the government and without as much red tape.

The Most Secure VPN to the Cloud

03/02/2013 21:44 (CloudTimes)

Most corporations subscribe and work through computer networks in order for their day-to-day operations to be accomplished. It is also a fact that the internet is widely patronized for research and even communications.

Hack Attacks Give Insurance Business a Boost

03/02/2013 19:50 (Yahoo! Canada Finance)

Cyber wars: America's infrastructure faces increased threats

03/02/2013 13:06 (Times-Standard Online)

March 3, 2013 10:7 AM GMTUpdated: 03/03/2013 02:06:06 AM PST In the not so distant future ... . Residents in L.A. County face a world with no electricity.

Jason Offutt: Harmful hackers hamper happiness

03/02/2013 01:13 (The Examiner)

Maryville, MO — The email message from my friend Chris was only slightly ominous: “Dude, I think you’ve been hacked.” Just a few decades ago, “hacked” was innocently simple.

SC panel tweaks bill on improving cyber-security

03/01/2013 03:47 (ABC News 4)

COLUMBIA, S.C. (AP) - A Senate panel has decided not to create a whole new agency for the state’s cyber-security officer. The subcommittee amended Thursday a bill meant to centralize oversight of state computer systems and prevent another massive breach of taxpayers’ information.

Identity theft complaints up 46% in Wisconsin

03/01/2013 03:09 (Examiner.com - Wisconsin)

Identity theft topped the list of fraud complaints nationwide and in Wisconsin for the 13th consecutive year according to a Federal Trade Commission (FTC) report.

China’s universities linked to cyber-spying

03/01/2013 02:15 (The Argus Leader (AP))

A burgeoning Chinese effort to build academic and civilian expertise in computer espionage has ties to the nation’s military, a science journal reports Thursday.

FBI director: Forget firewalls, Sabu proves attribution wins domestic cyber war

03/01/2013 01:52 (Computerworld Malaysia)

Defence is good, but old school surveillance is better. In a call to arms aimed at the private sector, the FBI’s director of 11 years Robert S. Mueller has declared that war on the new ’terror’, cyber, will be won not by improved defence but by attribution.

Cyber hacking threat puts sequester in perspective

03/01/2013 00:07 (Pocono Record (AP))

WASHINGTON — In the midst of all this worry about cutting defense spending, President Obama signed an executive order to boost U.S. defenses against cyber hacking.

College IT Guys Admit Embezzlement, Forgery, Identity Theft

02/28/2013 23:58 (Belmont Patch)

Bradley John Witham, 43, pleaded guilty to embezzlement and forgery and Mark Anthony Bustos, 42, pleaded guilty to identity theft.

Cadets combat hackers on digital battlefield

02/28/2013 23:20 (Camarillo Acorn)

Ventura County teens took part in nationwide competition to prevent cyber attacks

Use trade policy to put an end to China's hacking

02/28/2013 21:55 (Politico)

Last week, Virginia-based Mandiant Corp. released a report accusing a wing of the Chinese military of waging a campaign of cyberattacks against the United States.

Sourcefire defends against network malware

02/28/2013 21:46 (ComputerWorld Singapore)

Sourcefire is allowing users to defend against sophisticated network malware with the release of an Advanced Malware Protection (AMP) appliance. Built on the FirePOWER platform, the AMP appliance provides increased deployment flexibility for organisations that need immediate protection against adva

Applying big data approaches to information security a challenge

02/28/2013 21:46 (ComputerWorld Singapore)

SAN FRANCISCO - Applying big data approaches to information security can help enterprises build better situational awareness capabilities, but implementation could prove to be a major challenge, security experts said at the RSA Conference 2013 being held here this week.

Cyber illiteracy puts internauts at risk

02/28/2013 18:42 (Tech & Gadget - MSN CA)

FBI Director: Private sector help ’essential’ to combating cyberattacks

02/28/2013 18:25 (The Hill - Blog)

SAN FRANCISCO — FBI Director Robert Mueller on Thursday said the U.S. government and private industry need to forge a collaborative working relationship to successfully combat the growing number of cyber threats facing the country.

MiniDuke Hackers Hit Governments with PDF Exploit

02/28/2013 17:23 (CIO Today)

The MiniDuke attackers are still active and have created malware as recently as Feb. 20, according to Kaspersky. To compromise victims, the attackers used social engineering techniques, which involved sending malicious PDF documents to their targets. The PDFs were highly relevant to their victims, a

NVIDIA Tool Becomes Accomplice

02/28/2013 17:05 (Isssource.com)

A specially crafted RTF document was leveraging a vulnerability in Word to execute a tool from NVIDIA’s graphics card drivers on victims’ computers. The executable file, called nv.

White House debating actions to retaliate against foreign cyberattacks

02/28/2013 17:01 (The Hill - Blog)

SAN FRANCISCO—The White House is debating what actions will be taken to retaliate against individuals and countries that launch cyber attacks against the United States.

Online Security Career Portal

02/28/2013 15:50 (Isssource.com)

There is a new online career-simulation platform that lets students and jobseekers check out careers in cyber security and gain exposure to the skills they'll need.

Senate plans joint hearing on Obama's cybersecurity order

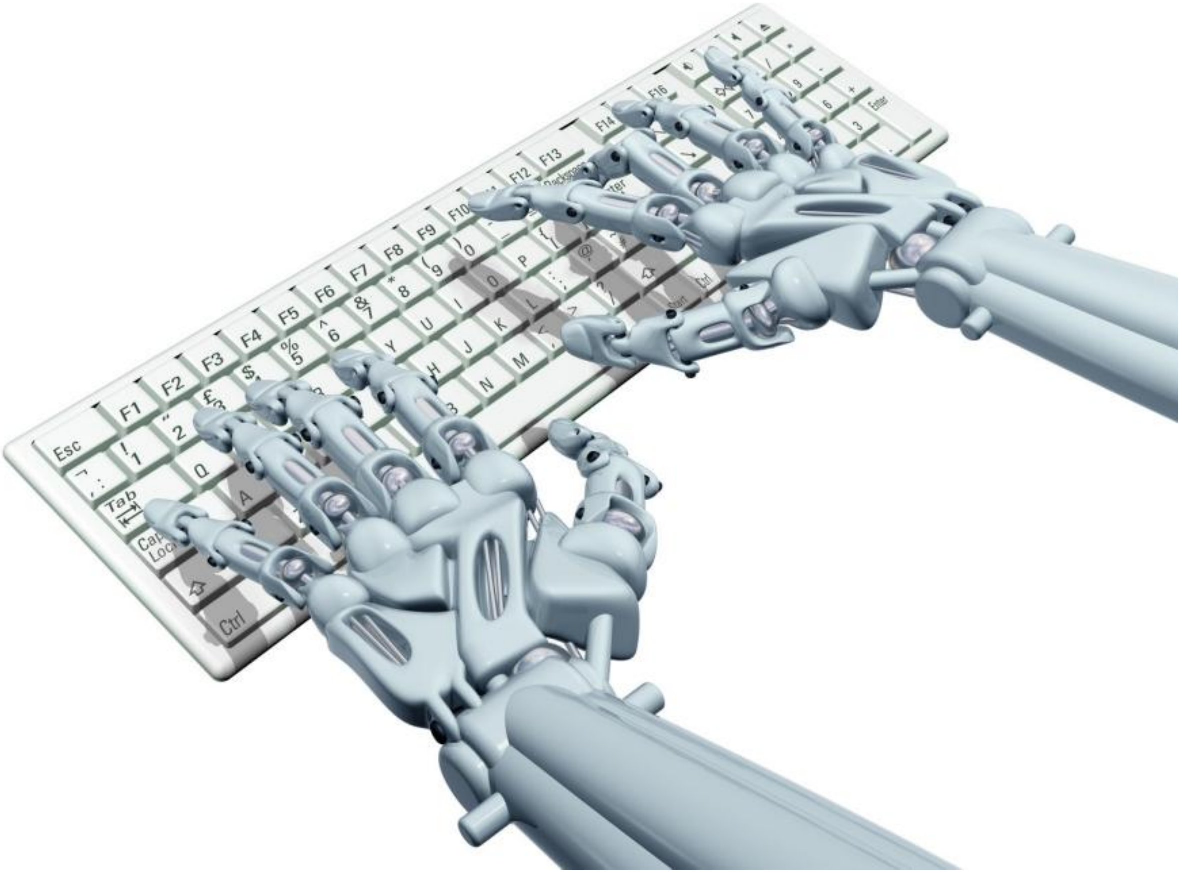
02/28/2013 14:26 (The Hill - Blog)

The chairmen of the Senate Commerce and Homeland Security Committees announced Thursday that they will hold a joint hearing next week on cybersecurity.

ID thieves targeting children

02/28/2013 13:34 (KGUN9)

9OYS Crime Watch



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 – The Greatest InfoSec Show on Earth

I'm finding it really hard to write about this event for a few reasons. First, it was incredible and overwhelming at the same time. I've been going to RSA for many years but something was very different this year. In spite of a worldwide global economic mess, folks from every corner of the globe came to this event – many taking booths to show off their latest and greatest products, technology and services. There was an entire Canadian pavilion. The Chinese pavilion was closely located to the NSA and to Mandiant….how ironic. Germany, South Korea and so much more. Beyond the growth in multi-country vendors on the expo floor, the expo floor itself was wall to wall. In fact, as Pierluigi alluded, we had our magazine placed outside of a second expo hall – called Gateway Expo.

This is a first in RSA history. So many vendors so little time. You really have to spend a few hours culling through the RSA Conference website and look at the list of Expo vendors and visit their websites. There were too many for me to even point out in a single article this year. One of my funny experiences was seeing the Federal Reserve having a booth. I asked them "what are you up to – banking security?" and their answer was "no, we took a booth because we are hiring…" so they leveraged the Expo floor because of the talent roaming the conference. This is actually becoming a global epidemic – not the fact that malware is spreading like wildfire but that there are NOT ENOUGH INFOSEC PROFESSIONALS to fill all the job opportunities – from Governments to Fortune 1000 to the Federal Reserve. When an employee of the Federal Reserve looked at a copy of our Magazine, I said "hey, what do you think about CDM?" and their response was "we'd love to advertise in here….but we have no money!" I could not stop laughing. This individual informed me that the Federal Reserve is a 'non-profit' and the fact that they print money by the trillions doesn't mean they have any to spend. How ironic.

So many great speakers, so many new InfoSec products, so little time. I still feel like I was cheated because the entire week went by so quickly. What I am seeing happening is something very similar to other industries – the growth of new technologies that slice a smaller and smaller piece of a bigger and bigger picture. For example, one vendor invented a 'truly random' seed generator which could help in the creation of tokens for token vendors like RSA, Vasco and Entrust. Imagine, your entire business model is to generate truly random numbers. Yet, this is so important for true security because, if you can find the seed, you can crack the encryption. There were dozens of vendors claiming to secure different aspects of virtualization and cloud computing. There were yet dozens more vendors claiming to have the be-all-end-all answer to the BYOD and MDM dillema.

The list goes on and on and on. That's why I strongly recommend you visit this page and spend a few hours perusing the players:

http://www.rsaconference.com/events/2013/usa/expo-and-sponsors/exhibitor-list.htm and just in case they take the page down, here they all are:

Company	Booth #	Level
3M	532	Exhibitor
6WIND	854	Exhibitor
Accellion, Inc.	340	Exhibitor
AccelOps	136	Exhibitor
Accolade Technology	126	Exhibitor
Accuvant	353	Exhibitor
Advantech	751	Exhibitor
Afore	135	Partner Pavilion
Agency for Science, Technology and Research (A*STAR)	3024	Exhibitor
Agiliance	317	Exhibitor
AhnLab	951	Exhibitor
AirWatch	2153	Exhibitor
Akamai Technologies, Inc.	1630	Global Platinum Sponsor
Alert Logic	2417	Exhibitor
AlgoSec	433	Exhibitor
AlienVault	2317	Exhibitor
Allegro Software Development Corporation	239	Exhibitor
Alta Associates Inc.	551	Exhibitor
AMAX Information Technologies	2351	Exhibitor
American National Standards Institute (ANSI)	127	Exhibitor
American Portwell Technology, Inc.	438	Exhibitor
Antiy Labs	2125	Partner Pavilion
APCON, Inc.	2451	Exhibitor
Application Security, Inc.	732	Exhibitor
AppRiver	1459	Exhibitor
Appthority	245	Exhibitor
Arbor Networks	1453	Exhibitor
Armorize Technologies Inc.	628	Exhibitor
Arxan Technologies	324	Exhibitor
AT&T	723	Exhibitor
Attachmate	2626	Exhibitor
AUCONET, Inc.	1332	Partner Pavilion
Authentex	839	Partner Pavilion
AuthentiDate International AG	1332	Partner Pavilion
Authentify, Inc.	629	Exhibitor
Authernative, Inc.	651	Exhibitor
Aveksa	347	Exhibitor
Axiomtek	2723	Exhibitor
Axway	728	Exhibitor

Barracuda Networks	1147	Exhibitor
Bear Data Solutions	234	Exhibitor
BeCrypt	442	Exhibitor
Behaviosec	2455	Exhibitor
Beijing Heshengda Information Security Technology Co., Ltd.	2133	Partner Pavilion
Beijing Leadsec Technology Co.,Ltd.	2033	Partner Pavilion
Beijing QIHU Technology Co., Ltd.	2033	Partner Pavilion
Beijing Topsec Science & Technology Co., Ltd	2133	Partner Pavilion
Beijing VenustechCybervision Co., Ltd	2033	Partner Pavilion
Beijing Zhongguancun Overseas Science Park (#1)	2033	Exhibitor
Beijing Zhongguancun Overseas Science Park (#2)	2133	Exhibitor
Beijing Zhongguancun Overseas Science Park (#3)	2125	Exhibitor
BeyondTrust Software	1045	Exhibitor
Bit9, Inc.	545	Exhibitor
Bitdefender	756	Exhibitor
BlackBerry	632	Exhibitor
Blue Coat Systems	2017	Silver Sponsor
Bradford Networks	119	Exhibitor
Brinqa	221	Exhibitor
Broadweb	2125	Partner Pavilion
CA Technologies	1447	Gold Sponsor
CCSO.com	357	Exhibitor
Celestix Networks	2551	Exhibitor
CenterTools Software GmbH	1332	Partner Pavilion
Centrify Corporation	233	Exhibitor
Check Point Software Technologies	1925	Silver Sponsor
Checkmarx	657	Exhibitor
CHERRY	2633	Exhibitor
Cigital	132	Exhibitor
CipherCloud	556	Exhibitor
Cisco	1316	Platinum Sponsor
Clearswift Corporation	120	Exhibitor
Click Security	655	Exhibitor
Cloud Security Alliance	3020	Exhibitor
CloudLock	2635	Exhibitor
Collective Software, LLC	351	Exhibitor
Commtouch	553	Exhibitor
Comodo Group Inc.	2734	Exhibitor
Core Security Technologies	2445	Exhibitor
CORISECIO GmbH	1332	Partner Pavilion
COSEINC	3009	Exhibitor
CounterTack	2533	Exhibitor
Coverity, Inc.	1759	Exhibitor
Covisint, a Compuware Company	654	Exhibitor
Critical Watch	650	Exhibitor
Cryptography Research, Inc.	2225	Exhibitor
Cryptomathic, Inc.	2358	Exhibitor
cv cryptovision gmbH	1332	Partner Pavilion
Cybera	338	Exhibitor

Cyber-Ark Software, Inc.	1947	Exhibitor
CyberMaryland	216	Exhibitor
CYBEROAM	2433	Exhibitor
Cybertap LLC	112	Exhibitor
Cypherbridge Systems LLC	3001	Exhibitor
Damballa	2233	Exhibitor
DaoliCloud Information Technology (Beijing) Co., LTD.	2133	Partner Pavilion
DATAGUISE, Inc.	559	Exhibitor
DB Networks	3220	Exhibitor
DBAPP Security Ltd.	253	Exhibitor
Dell Quest Software	2053	Exhibitor
DELL SecureWorks	1933	Silver Sponsor
Device Lock	745	Exhibitor
DHS/Office of Cybersecurity and Communications	945	Exhibitor
Diebold, Inc.	2628	Exhibitor
Digital Defense, Inc.	2637	Exhibitor
DocuSign	225	Exhibitor
DriveSavers Data Recovery	451	Exhibitor
Easy Solutions, Inc	2258	Exhibitor
eco e.V. Verband der deutschen Internetwirtschaft	1332	Partner Pavilion
eleven GmbH	1332	Partner Pavilion
Elliptic	135	Partner Pavilion
Endgame	144	Exhibitor
Enforcive	217	Exhibitor
Enterprise Ireland	3206	Exhibitor
ENTERSEKT (Pty) Ltd.	2753	Exhibitor
Entrust	1139	Silver Sponsor
Equifax	1659	Exhibitor
Esentire	135	Partner Pavilion
ESET, LLC	1638	Silver Sponsor
F5 Networks	1354	Exhibitor
Fasoo.com	2241	Exhibitor
Federal Bureau of Investigation	3216	Exhibitor
Federal Reserve Bank of San Francisco	3005	Exhibitor
Federal Times & C4ISR Journal	2720	Exhibitor
Feitian	839	Partner Pavilion
FEITIAN Technologies Co., Ltd.	2125	Partner Pavilion
FireEye, Inc.	1646	Global Gold Sponsor
FireHost Inc.	959	Exhibitor
FireMon	645	Exhibitor
Fixmo	135	Partner Pavilion
ForeScout Technologies, Inc.	831	Exhibitor
Fortinet	2025	Exhibitor
Fox Technologies, Inc.	850	Exhibitor
Freescale Semiconductor Inc.	3002	Exhibitor
Garner Products	432	Exhibitor
GFI Software	2141	Exhibitor
Gigamon LLC	1753	Exhibitor
Glimmerglass Optical Cyber Solutions	2058	Exhibitor

Global Knowledge Training	2722	Exhibitor
GlobalSCAPE	2259	Exhibitor
GlobalSign	329	Exhibitor
Good Technology	226	Exhibitor
GreenSQL Ltd.	3107	Exhibitor
Guardian Analytics	733	Exhibitor
Guidance Software, Inc.	222	Exhibitor
Gurucul Solutions	229	Exhibitor
GWAVA Technologies	3100	Exhibitor
HBGary, Inc.	2650	Exhibitor
HID Global	2517	Exhibitor
Hitachi ID Systems, Inc	450	Exhibitor
HOB GmbH Co	851	Exhibitor
HP	1717	Platinum Sponsor
Huawei Technologies Co.,Ltd.	2651	Exhibitor
HyTrust	1853	Exhibitor
I Think Security	141	Partner Pavilion
IBM Corporation	241	Exhibitor
iBoss Security	3200	Exhibitor
Identity Finder, LLC	350	Exhibitor
iDrive.com	359	Exhibitor
IEEE Computer Society	2529	Exhibitor
Imperva Inc.	417	Exhibitor
Infineon Technologies AG	1332	Partner Pavilion
Infoblox	122	Exhibitor
InfoExpress, Inc.	2623	Exhibitor
InfoGard	554	Exhibitor
Information Networking Institute - Carnegie Mellon	240	Exhibitor
Information Systems Security Association (ISSA)	152	Exhibitor
Infosecurity Magazine	223	Exhibitor
Intel	1439	Exhibitor
Interface Masters Technologies	117	Exhibitor
International Association of Privacy Professionals (IAPP)	154	Exhibitor
Ipswitch File Transfer	752	Exhibitor
IronKey by Imation	2425	Exhibitor
ISACA	150	Exhibitor
ISC^2	146	Exhibitor
ITAC	2459	Exhibitor
it-sa – The IT-Security Expo	1332	Partner Pavilion
itWatch GmbH	1332	Partner Pavilion
IXIA	2217	Exhibitor
Jiransoft Inc.	1859	Exhibitor
Juniper Networks	1031/2645	Silver Sponsor
Kaspersky Lab	2117	Exhibitor
Key Source International	2355	Exhibitor
Keypasco AB	452	Exhibitor
Kingsoft	2125	Partner Pavilion
Klocwork	2732	Exhibitor
Lancope	1653	Exhibitor

Lanner Electronics Inc	316	Exhibitor
Lieberman Software Corporation	633	Exhibitor
Linoma Software	242	Exhibitor
Lionic Inc.	257	Exhibitor
LJ Kushner & Associates, LLC	446	Exhibitor
Lockheed Martin	341	Exhibitor
LogRhythm	823	Exhibitor
Lumension	1959	Exhibitor
Lynux Works	2450	Exhibitor
Manage Engine	2641	Exhibitor
MANDIANT	2439	Exhibitor
MAD Security, LLC	3111	Exhibitor
MBX Systems	528	Exhibitor
McAfee an Intel Company	1117	Platinum Sponsor
Messageware, Inc.	2550	Exhibitor
Metaforic	3026	Exhibitor
MetricStream	3003	Exhibitor
Microsoft Corporation	1616	Global Diamond Sponsor
MirageWorks Inc.	2619	Exhibitor
MITRE	2617	Exhibitor
MobileIron, Inc.	354	Exhibitor
Mocana Corporation	2454	Exhibitor
Modulo	523	Exhibitor
Motorola Solutions	114	Exhibitor
Myricom, Inc.	3207	Exhibitor
NagraID Security	1039	Exhibitor
Napatech	2545	Exhibitor
Narus, Inc.	1841	Silver Sponsor
National Institute of Standards and Technology	250	Exhibitor
nCircle	1023	Gold Sponsor
NEI	617	Exhibitor
Net IQ	828	Exhibitor
Net Optics, Inc.	1051	Exhibitor
NETGEAR, Inc.	428	Exhibitor
Netronome	2339	Exhibitor
NetScout	2735	Exhibitor
Neusoft Corporation	2033	Partner Pavilion
New Horizons Computer Learning Centers	320	Exhibitor
Nexcom	859	Exhibitor
Nexus Technology	839	Partner Pavilion
Niometrics	3000	Exhibitor
NopSec, Inc.	3105	Exhibitor
Npulse Technologies, Inc.	557	Exhibitor
Norman ASA	2047	Exhibitor
NPCore	2639	Exhibitor
NSA	845	Exhibitor
NSFOCUS	529	Exhibitor
NSS Labs, Inc.	729	Exhibitor
Ntrepid Corporation	153	Exhibitor

NuCaptcha	2749	Exhibitor
NXP Semiconductors	1657	Exhibitor
OASIS Interoperability Standards Showcase	3012	Exhibitor
OATH	839	Exhibitor
Oberthur Technologies	423	Exhibitor
Okta, Inc.	352	Exhibitor
Onapsis Inc.	456	Exhibitor
OneLogin, Inc.	2359	Exhibitor
Ontario Canada Delegation	135	Exhibitor
Ontario Canada Delegation (2)	141	Exhibitor
OPSWAT, Inc.	429	Exhibitor
Oracle	1941	Exhibitor
Palo Alto Networks	931	Exhibitor
Patriot Technologies	656	Exhibitor
PerspecSys Inc.	251	Exhibitor
PhishMe, Inc.	2727	Exhibitor
Phishnix	3106	Exhibitor
PhoneFactor, a Microsoft Company	717	Exhibitor
Pindrop Security	259	Exhibitor
Ping Identity Corporation	2158	Exhibitor
PistolStar, Inc.	248	Exhibitor
PointSharp AB	2755	Exhibitor
Portcullis Inc.	3007	Exhibitor
Premio, Inc.	140	Exhibitor
PrimeKey Solutions AB	459	Exhibitor
PrivateCore Inc	3102	Exhibitor
Prolexic Technologies	2539	Exhibitor
Proofpoint, Inc.	739	Exhibitor
Protected-Networks.com GmbH	2658	Exhibitor
Pwnie Express	2747	Exhibitor
QGroup GmbH	1332	Partner Pavilion
Qosmos	1059	Exhibitor
Qualys, Inc.	1431	Global Platinum Sponsor
QuintessenceLabs	128	Exhibitor
Radiant Logic, Inc.	129	Exhibitor
Radware, Inc.	453	Exhibitor
Rapid7	2247	Exhibitor
RedSeal Networks, Inc	1157	Silver Sponsor
Rohde & Schwarz SIT GmbH	1332	Partner Pavilion
RSA, The Security Division of EMC	1727	Global Diamond Sponsor
RSAM	623	Exhibitor
SafeNet, Inc.	1825	Global Gold Sponsor
SAIC	2041	Exhibitor
SANS/GIAC/STI	2716	Exhibitor
Seagate Technology LLC	555	Exhibitor
SECnology, Inc.	236	Exhibitor
secunet Security Networks AG	1332	Partner Pavilion
Secunia	817	Silver Sponsor
Secure Commerce Systems, Inc	3104	Exhibitor

SecureAuth Corporation	123	Exhibitor
Security Mentor	750	Exhibitor
Securonix LLC	3103	Exhibitor
SecuTech Solutions PTY LTD	3109	Exhibitor
SenSage Inc.	939	Exhibitor
Sentry	141	Partner Pavilion
Shenzhen NORCO Intelligent Technology Co., Ltd.	118	Exhibitor
SilverSky	149	Exhibitor
Sims Recycling Solutions	246	Exhibitor
Sirrix AG security technologies	1332	Partner Pavilion
Skybox Security, Inc.	323	Exhibitor
Skyhigh Networks, Inc.	147	Exhibitor
Smarsh	457	Exhibitor
SmartDisplayer Technology	2624	Exhibitor
Software Engineering Institute	2059	Exhibitor
Solarflare	3214	Exhibitor
Solera Networks	2345	Exhibitor
Solutionary, Inc.	344	Exhibitor
SonicWALL, Inc.	1348	Exhibitor
Sophos	1817	Gold Sponsor
Sourcefire, Inc.	2552	Exhibitor
SparkWeave, LLC.	138	Exhibitor
Spirent Communications	2525	Exhibitor
Splunk Inc.	1917	Global Gold Sponsor
SPYRUS, Inc	2333	Exhibitor
SSH Communications Security	333	Exhibitor
Stealthbits Technologies, Inc.	2555	Exhibitor
Stonesoft Inc.	1953	Exhibitor
StrikeForce Technologies, Inc.	539	Exhibitor
StrongAuth, Inc.	330	Exhibitor
Syferlock	839	Partner Pavilion
Symantec Corporation	1417	Global Diamond Sponsor
Symplified	255	Exhibitor
SynerComm Inc	3108	Exhibitor
Sypris	2726	Exhibitor
SYSMATE	757	Exhibitor
TechGuard Security	2717	Exhibitor
TeleSign Corporation	533	Exhibitor
TeleTrusT - IT Security Association Germany	1332	Gold Sponsor
Tenable Network Security, Inc.	856	Exhibitor
Thales e-Security	517	Exhibitor
ThreatMetrix, Inc.	3203	Exhibitor
Thycotic Software Ltd.	2644	Exhibitor
TIBCO Software	2325	Exhibitor
Tilera Corporation	2751	Exhibitor
TITUS	1017	Silver Sponsor
TraceSecurity, Inc.	3101	Exhibitor
Trend Micro Incorporated	1833	Silver Sponsor
Tripwire, Inc.	923	Silver Sponsor

Trustwave	1324	Platinum Sponsor
Tufin Technologies	439	Exhibitor
TÜV Informationstechnik GmbH	1332	Partner Pavilion
Unisys	3028	Exhibitor
University of Denver	328	Exhibitor
University of Maryland University College	3204	Exhibitor
VASCO Data Security	332	Exhibitor
Venafi, Inc.	1655	Silver Sponsor
Veracode, Inc.	1342	Silver Sponsor
Verdasys, Inc.	2738	Exhibitor
Verizon	917	Silver Sponsor
Viewfinity	3212	Exhibitor
Vineyard Networks	2739	Exhibitor
Visible Statement	339	Exhibitor
V-Key Corp.	3006	Exhibitor
VMware	2253	Exhibitor
VoIP Shield	141	Partner Pavilion
Voltage Security	2627	Exhibitor
Vormetric, Inc.	445	Exhibitor
VSS Monitoring, Inc.	2147	Exhibitor
WatchGuard Technologies, Inc.	1153	Exhibitor
Watsec	141	Partner Pavilion
Wave Systems Corp.	1847	Exhibitor
Webroot, Inc.	832	Exhibitor
Websense Inc.	1129	Gold Sponsor
Wombat Security Technologies, Inc.	3201	Exhibitor
WWPass Corporation	3209	Exhibitor
yaSSL.com	755	Exhibitor
Yubico	839	Partner Pavilion
Zenprise – Now Part of Citrix	3022	Exhibitor
Zix Corporation	550	Exhibitor
Zscaler, Inc.	639	Exhibitor

You might think I pasted this list in to increase the word count in my article and pickup some kudos from our new (and amazing) Editor – but think again! Seriously, as you can see from this list, this is truly the Greatest InfoSec Show on Earth. It's a must attend and my lesson for 2014 is to bring lots of Red Bull, start real early, end real late and spend the following week recovering on a beach somewhere far away from bluetooth, wifi, byod, mdm, tcp/ip stacks and ssl encryption.

Take it from me, with nations using the Internet as a 'theatre' of operation, with cybercriminals making billions from online identity theft, do not expect this conference to be any smaller next year. We're in an explosive industry with limitless possibilities and tremendous opportunities.

Source: Gary S. Miliefsky, CISSP®

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

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.

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

Because of the dynamic nature of the Internet, any Web addresses or links contained in this newsletter may have changed since publication and may no longer be valid. The views expressed in this work are solely those of the author and do not necessarily reflect the views of the publisher, and the publisher hereby disclaims any responsibility for them.

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: 03/25/2013

CDM
CYBER DEFENSE MAGAZINE™
THE PREMIER SOURCE FOR IT SECURITY INFORMATION

Cyber Warnings E-Magazine March 2013

ADDITIONAL SPONSORS INCLUDE:

0000 0000 0000 0000
06 08
06 04
CUSTOMER NAME