



**MANAGING THE SECURITY OF APPLICATIONS IN
PRIVATE AND HYBRID CLOUD INFRASTRUCTURES**

THE FIVE STAGES OF SECURITY GRIEF

**7 DESTINY VIDEO GAME
TACTICS THAT TRANSLATE
TO CYBER SECURITY**



**Prioritizing
penetration
testing**

INFOSEC INDUSTRY: TIME TO PUT UP OR SHUT UP



People spend
over 700 billion
minutes per month
on Facebook.

Research by Facebook



*The Internet is full of temptations.
Can your users resist them?*

The Internet is one of the most useful resources in the office – but only if you can manage the potential issues:

- » Productivity losses due to employees spending time on sites with little work-related content
- » Security risks: from unsecure sites and from legitimate sites that have been compromised
- » Bandwidth losses from people downloading large files or watching streaming media.

Run the 30-day trial of GFI WebMonitor to find out exactly how your Internet connection and remote machines are being used and what security risks you are exposed to.

Quality web filter

Comprehensive web security

Highly competitive pricing

Thousands of customers

Download your free trial from <http://www.gfi.com/webmon>



GFI WebMonitorTM

Web security, monitoring and Internet access control

TABLE OF CONTENTS

Page 05 - **Security world**

Page 10 - The five stages of security grief

Page 13 - Infosec industry: Time to put up or shut up

Page 16 - Review: Secure file storage and sharing
with nCrypted Cloud

Page 21 - Prioritizing penetration testing

Page 24 - **Malware world**

Page 29 - Report: McAfee FOCUS 14

Page 35 - Managing the security of applications in private
and hybrid cloud infrastructures

Page 38 - Vigilance and the Enterprise of Things

Page 42 - Seven Destiny video game tactics that translate
to cyber security

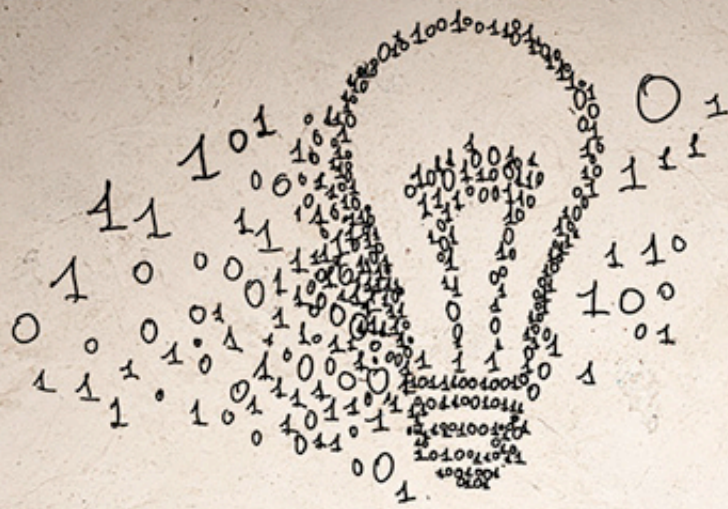
Page 45 - Review: ESET Smart Security 8

Page 48 - **Events around the world**

Page 50 - Maltego transforms for pcap analysis

Page 53 - All your info are belong to us: The biggest phishing
scams of 2014

Page 56 - Why fraudsters love the sharing economy this
holiday season



(IN)SECURE Magazine 44 contributors list

- **Andreas Baumhof**, CTO at ThreatMetrix.
- **Brian Honan**, CEO of BH Consulting, Founder and Head of IRISSCERT.
- **Adam Maxwell**, Security Researcher.
- **Dwayne Melancon**, CTO at Tripwire.
- **Corey Nachreiner**, Director of Security Strategy and Research at WatchGuard Technologies.
- **Gavin Millard**, EMEA Technical Director at Tenable Network Security.
- **Greg Anderson**, Senior Cyber Security Engineer.
- **Jovi Umawing**, Malware Intelligence Analyst at Malwarebytes Lab.
- **Prakash Sinha**, Vice President of Application Delivery Solutions at Radware.

Visit the magazine website at www.insecuremag.com

(IN)SECURE Magazine contacts

Feedback and contributions: **Mirko Zorz**, Editor in Chief - mzorz@net-security.org

News: **Zeljka Zorz**, Managing Editor - zzorz@net-security.org

Marketing: **Berislav Kucan**, Director of Operations - bkucan@net-security.org

Distribution

(IN)SECURE Magazine can be freely distributed in the form of the original, non-modified PDF document. Distribution of modified versions of (IN)SECURE Magazine content is prohibited without the explicit permission from the editor.

Security world



Financial services cyber trends for 2015



If 2014 was the “year of the breach,” what cybersecurity threats await us in 2015? Here is the list according to Booz Allen:

1. There will be a shift towards active cyber risk mitigation and monitoring with third parties, versus the current “self-certification” process that is proving less reliable.
2. The rise of the “fusion center.” Firms are building cyber “fusion centers” that better integrate the many different teams to boost intelligence, speed response, reduce costs and leverage scarce talent.
3. Information protected at the database and data element level. The use of tokenization, chip cards and other solutions will increasingly render stolen data useless to hackers.
4. Rise in alternative payment systems creates exposure. Use of underlying technologies like Bluetooth or NFC creates opportunities for cyber attacks and breaches.
5. Cyber crime analysis evolves away from brute force to big data.
6. Hacktivism spreads to the Middle East. Regional threat actors have adopted local grievances and formed hacktivist collectives similar to or associated with Anonymous.
7. “Western” cyber problems are coming to a developing nation near you. Economic prosperity and light-speed growth in mobile banking in some countries have bypassed regional and local financial organizations’ ability to manage threats.
8. Wargaming drives incident response preparation.
9. Everything firms know about privacy has changed. The next generation of privacy is focused on the halo of information around individuals – the transactional, behavioral and navigation information generated as individuals move and interact through the online and physical world.
10. Cyber insurance usage grows while coverage and ability to successfully make claims shrinks. The insurance industry is in a race to actuarially quantify new cyber risks and to carve out coverage of large, uncertain future risks.

Hackers hit execs for insider info to gain stock market advantage

FireEye's researchers have identified yet another hacking group. Dubbed FIN4, the hacking crew seems to be comprised of native English speakers with "deep familiarity with business deals and corporate communications, and their effects on financial markets."

Their targets are top executives, legal counsel, outside consultants, regulatory, risk, and compliance personnel, advisors and researchers who are believed to have inside knowledge about potential mergers and acquisitions, deals and new research results.

Operational since at least mid-2013, the group has targeted these individuals in over 100 publicly traded companies and advisory firms, the majority of which are in the healthcare and pharmaceutical industries.

Their weapons of choice are extremely well crafted and personalized spear-phishing

emails that are meant to lead recipients to phishing pages impersonating the Outlook Web App login page and trick them into sharing their Microsoft Outlook login credentials.

"FIN4 uses their knowledge to craft convincing phishing lures, most often sent from other victims' email accounts and through hijacked email threads. These lures appeal to common investor and shareholder concerns, enticing the intended victims into opening the weaponized document and entering their email credentials," the researchers shared.

The researchers say that the attackers' goal seems obvious: gain insider knowledge about things that affect the companies' stock price or future revenue, and act upon that information in a way that would earn them money. As the attacks are still ongoing, the researchers advise organizations' network defenders to disable VBA macros in Microsoft Office by default (if possible), block a number of C&C domains currently in use, and enable two-factor authentication for OWA and any other remote access mechanisms.

Most IT pros prefer open source to proprietary software



According to a Ponemon Institute study, more than 70 percent of IT professionals in the US agree that commercial open source software provides more control and ensures better business

continuity than proprietary software.

Cost savings are no longer the hallmark of open source in the minds of IT professionals, with the ability to lower costs ranking below quality in importance. This viewpoint is echoed by 67 percent of IT and IT security practitioners in EMEA.

EMEA organizations are more concerned with the privacy consequences of messaging and collaboration; US organizations focus more on security.

"One of the most interesting survey results was the slow adoption of open source messaging and collaboration software, despite IT professionals' resounding trust in open source software," said Dr. Larry Ponemon, chairman of the Ponemon Institute. "With the majority of deployments being proprietary solutions and the sentiment largely negative, I would expect to see increased interest in new solutions that are based on commercial open source."

Also, 89 percent of employees do not follow company policy on sharing confidential documents, and 74 percent of employees use unauthorized messaging and collaboration applications. For 65 percent of IT professionals in the US, ease of use is the most important factor for selecting a messaging and collaboration solution. 55 percent of them plan to replace their messaging and collaboration solutions within two years, which is a significant opportunity for open source to play a central role in the future of security and privacy across the US and EMEA.

New non-profit CA aims to make HTTPS use universal

To become ubiquitous, encryption must be easy to set up and easy to use, and that's why the Electronic Frontier Foundation (EFF), Mozilla, Cisco, Akamai, IdenTrust, and researchers at the University of Michigan are working on setting up a new certificate authority.

"With a launch scheduled for summer 2015, the Let's Encrypt CA will automatically issue and manage free certificates for any website that needs them. Switching a webserver from HTTP to HTTPS with this CA will be as easy as issuing one command, or clicking one button," explained Peter Eckersley, technology projects director for the EFF.

"The biggest obstacle to HTTPS deployment has been the complexity, bureaucracy, and cost of the certificates that HTTPS requires," he pointed out, adding that this is what stopped many site administrators from switching to HTTPS. Let's Encrypt's goal is to make the process last less than half a minute.

"Let's Encrypt will employ a number of new technologies to manage secure automated verification of domains and issuance of certificates," says Eckersley.

"We will use a protocol we're developing called ACME between web servers and the CA, which includes support for new and stronger forms of domain validation. We will also employ Internet-wide datasets of certificates, such as EFF's own Decentralized SSL Observatory, the University of Michigan's scans.io, and Google's Certificate Transparency logs, to make higher-security decisions about when a certificate is safe to issue," he added.

The CA will also provide public records about all the certificates it will issue and revoke. Renewal of the certificates is automated.

The official overseer of the project is the Internet Security Research Group which will, along with the rest of the project's co-founders, be actively working on setting up the needed architecture in time for the scheduled launch.

Open Whisper Systems helps WhatsApp achieve end-to-end encryption



The immensely popular WhatsApp instant messenger has the potential to become an even more attractive option for users, as the company has partnered with Open Whisper Systems to implement the

latter's TextSecure protocol into their clients. Apparently, the two teams have been working on this implementation for the last six months.

So far, the end-to-end encryption provided by the protocol is only available in the most recent WhatsApp Android client, and only for text messages, but support for encrypted messaging for group chat or media messages is coming soon.

"WhatsApp runs on an incredible number of mobile platforms, so full deployment will be an

incremental process as we add TextSecure protocol support into each WhatsApp client platform," the Open Whisper Systems team shared in the announcement. "We have a ways to go until all mobile platforms are fully supported, but we are moving quickly towards a world where all WhatsApp users will get end-to-end encryption by default."

"We'll also be surfacing options for key verification in clients as the protocol integrations are completed," they added.

Also, this doesn't mean that OWS is abandoning the development of its TextSecure app, which was recently audited by a group of German researchers.

"We're excited to incorporate what we've learned from this integration into our future design decisions, and to bring this experience to bear on integrations that we do with other companies and products in the future," they noted.

China is building a quantum encryption network between Beijing and Shanghai

The race for setting up a secure long-distance communication network based on quantum encryption is on, and China is currently in the lead.

"Since most of the products we buy come from foreign companies, we wanted to accelerate our own programme," said Professor Pan Jianwei, a quantum physicist at the University of Science and Technology of China (USTC) in Hefei. "This is very urgent because classical encryption was not invented in China, so we want to develop our own technology."

The project about which he's talking about and leading is aimed at setting up a fiber-optic cable between Beijing and Shanghai, which will transmit quantum encryption keys.

The main advantage of quantum encryption over regular encryption is that the encryption keys are encoded into photons, which are impossible for third parties to eavesdrop on without measuring them, and by doing this,

introducing anomalies that will indicate that a third party tried to gain knowledge of the key. The disadvantage of a quantum encryption-based system is that photons can't travel far, meaning that this system that will connect two cities distant over 663 miles (a little over a thousand kilometers) will have to include at least 20 nodes - and they will be vulnerable to attackers.

Nevertheless, this is the future of encryption, and the Chinese government has decided to invest in this cable. If this proves to be a successful experiment, eventually all communications in China will likely include quantum encryption.

The professor and others working on this project are aware that while, in theory, quantum communication provides complete security, in practice that might not be true. So, they have invited the finest Chinese hackers to test it and share the knowledge once they do. The project is set to be finished in two years, and China stands to gain a system that will allow the government, the military, and financial institutions to exchange information in a way that will prevent snooping from any third party, including foreign governments.

Darkhotel espionage campaign targets corporate executives traveling abroad



Kaspersky Lab researched the Darkhotel espionage campaign, which has lurked in the shadows for at least four years while stealing sensitive data from selected

corporate executives traveling abroad.

Darkhotel hits targets while they are staying in luxury hotels. The most recent traveling targets include top executives from the USA and Asia doing business and investing in the APAC region. The Darkhotel actor maintains an effective intrusion method set on hotel networks, providing ample access over the years to systems that were believed to be private and secure. They wait until after

check-in when the victim connects to the hotel Wi-Fi network, submitting his room number and surname to login.

The attackers see the victim on the compromised network and trick the person into downloading and installing a backdoor that pretends to be an update for legitimate software, such as Google Toolbar, Adobe Flash or Windows Messenger. The unsuspecting executive downloads this hotel "welcome package," only to infect his machine with a backdoor for the Darkhotel spying software.

Once on a system, the backdoor has been and may be used to further download more advanced stealing tools. Victims lose sensitive information likely to be the intellectual property of the business entities they represent. After the operation, the attackers carefully delete their tools from the hotel network and go back into hiding.

Cisco open sources Big Data security analytics framework

"Technically advanced attackers often leave behind clue-based evidence of their activities, but uncovering them usually involves filtering through mountains of logs and telemetry. The application of big data analytics to this problem has become a necessity," Cisco Security Solutions manager Pablo Salazar pointed out before announcing that the company is open sourcing its OpenSOC Big Data security analytics framework.

"The OpenSOC framework helps organizations make big data part of their technical security strategy by providing a platform for the application of anomaly

detection and incident forensics to the data loss problem," he explained.

OpenSOC integrates elements of the Hadoop ecosystem such as Storm, Kafka, and Elasticsearch, and offers the following capabilities: full-packet capture indexing, storage, data enrichment, stream processing, batch processing, real-time search, and telemetry aggregation.

The fact that all this data is provided through a centralized platform allows security analysts to detect the problems and react swiftly. The emphasis is on data delivery being executed "quickly" - in real-time, in fact - and all in one place so that analysts don't need to check out numerous reports and sources and waste valuable time going through unstructured data.

How to detect fraudulent activity in a cloud without invading users' privacy



The great thing about the cloud is that companies and users can use as much compute power or storage as needed at a specific moment and pay

only for what was used. However, fraudulent, illegal or undesired activities such as using a cloud infrastructure to launch DDoS attacks or cryptocurrency mining can ruin the experience for those who use the cloud for private and corporate purposes, as undesired activities can continuously suck up too much bandwidth and reduce the lifespan of the hardware.

The problem for cloud providers is the following: how to detect such activity on their infrastructure without performing network packet inspection, i.e. invading a paying user's privacy?

"A way of doing this would be to use data aggregates, which do not give a lot of detail, such as CPU usage or the number of outgoing packets in a closed interval, to perform a first classification," researchers Marc Solanasa, Julio Hernandez-Castrob, and Debojyoti Dutta

explained in a paper. "In case a fraudulent activity is suspected, then a more in-depth method can be used. This way allows users who run regular workloads to keep their privacy while detecting suspicious activity."

The samples of data were collected from an OpenStack cluster, featuring regular workloads and fraudulent ones. By testing different classification algorithms, the researchers attempted to classify 5 types of jobs: regular workload (Hadoop workload or highly CPU-intensive job), internal DDoS attack, cryptocurrency mining, and physical network failure.

Of all the OpenStack components, Ceilometer - the Telemetry Service that provides all the usage metrics cloud providers need to establish customer billing - proved to be the most useful. By using five seconds data aggregates of several common metrics (CPU, disk and network) during various activities, and comparing the various patterns, they managed to determine - with relatively high accuracy and in a relatively short time - what type of activity customers are engaged in without discovering detailed information about what they are actually doing. Their privacy is thus preserved, and illegal or undesired activities can be made to stop.



When discussing information security with organizations, I often find many are at different stages of dealing with the problem. I see some ignoring the issue hoping it will go away, others fruitlessly spending money on technology with the expectation that the next investment will finally reduce the probability of a breach, and the remaining few that have accepted the issue and have a strategic plan to deal with it.

To help aid in establishing where different people are in the process, I've noticed parallels to the famous Kübler-Ross model of grief introduced by Elisabeth Kübler-Ross in 1969. The model shows that when people deal with death, they move through a series of emotions, starting with denial and progressing through anger, bargaining, depression and acceptance. The model is used to understand how people deal with a significant negative life event, but it can also be applied to the grief and anxiety of not knowing what to do in order to protect an organization from highly motivated threat actors.

Denial is the first and most common stage of security grief. You can easily identify individuals or organizations at this stage from their

apparent apathy towards the issue. Comments such as "Why would somebody hack us?" or "There are better targets than us" are common at this stage. This disconnect from the reality and enormity of the situation can have huge repercussions.

Unfortunately for the folks in the first stage, security is often a misunderstood issue. The assumption that hackers specifically target large organizations, ignoring everyone else, is flawed.

Whilst big retailers and banking institutions are definitely juicy targets, we must remember that attackers with low motivation and low skills will always be looking for an easy target.

Individuals who are happy to click on a link emailed to them are low hanging fruit for hackers looking to gain a foothold in a network. And so are unpatched systems with easily exploitable vulnerabilities that are being picked up via automated scans that constantly sweep over large chunks of the Internet.

The only way to guide people through the first stage of security grief is education. Helping them grasp that the threat landscape has dramatically changed is critical to making them understand that anyone can be a victim.

Once the magnitude of the issues surrounding IT security has sunk in, they move to the second stage of security grief: anger. This is identified by statements such as “I have a special set of skills and I will hunt these hackers

down” or “Why us? We’re only trying to provide a service to our customers.”

Anger is good because it helps transform apathy into action. But if the emotion isn’t focused on fixing the problems faced, it can be wasted. There is little point in trying to track down the attackers to unleash vengeance upon them when the reality is that the people you want to make pay are in another country behind multiple proxies, and the chances of accurate attribution and extradition for a minor crime is incredibly low. Rather, the energy generated by anger should be focused on trying to proactively reduce the probability of a breach and decrease the time taken to detect and remediate after any issues come up. Until this happens, you can’t move on.

SECURITY ISN’T ABOUT SPENDING A PORTION OF THE ANNUAL BUDGET ON TOOLS, IT’S ABOUT DOING THE RIGHT THING TO REDUCE RISK.

The third stage of security grief is bargaining, and involves the false hope that issues can be undone or avoided by turning to a higher power, the almighty security vendors. With the slick marketing we see today for security solutions, it’s often assumed that spending money with a particular vendor will magically reduce the risk of security issues arising.

Unfortunately, this is rarely the case. Security isn’t about spending a portion of the annual budget on tools, it’s about doing the right thing to reduce risk.

I see many organizations making investments in technology to aid in security, but never implementing the solutions to their full potential. When you don’t operationalize the controls that were deployed, breaches are bound to occur and opportunities to identify the intrusion will be lost. If we look at the Target breach as an example, a significant investment was made in anti-malware technology but the alarms were ignored both when the attackers installed the credit card stealing malware and when it was upgraded to exfiltrate further details. Investing in security solutions is often futile if the effort to operationalize and measure the effectiveness of the controls isn’t undertaken.

User education is also an important factor that is often ignored when investing in security. Raising awareness about the issues and helping users understand why certain activities introduce the risk of a breach can often reap better rewards than buying a piece of tin.

Measuring the effectiveness of your chosen security controls is a great way to ensure they are implemented and functioning as expected. Using metrics to identify how well each part of the business is functioning enables you to identify issues and grasp the enormity of the problem faced because if you don’t measure it, you can’t improve it.

As better situational awareness is gained, it can lead to the fourth stage of security grief: depression.

The reality of the threats we face today are truly depressing, as we are always only one mistake away from attackers stealing our data. At this stage, we want to avoid statements like “Why bother? There is nothing we can do to defend against this” or “I don’t know where to start, so let’s not do anything” as they can lead back to that old enemy of security: apathy.

Fear, uncertainty and doubt surrounding security is a huge issue for many organizations, and the assumption that good security is only achievable by the best of the best can be depressing. Not knowing where to start or the best place to invest in risk reduction can prevent even the most motivated of organizations from taking action, but there are many options to take when building an effective security program.

I always advise organizations to turn to the SANS Top Twenty Critical Security Controls as a starting point. Their advice and approach are solid and, embedded within the controls, examples of great metrics that can be utilized to ensure they are functioning as deployed and expected.

Understanding what needs to be done and having a roadmap to achieve it can swiftly aid in moving through the maudlin phase to the final stage of security grief, the one we need to encourage all organizations and individuals towards: acceptance.

Once an organization or individual has accepted the fact that chances of a breach are high but that something can be done about it, they can begin to deal with the problem. Education, effort, patience, and a roadmap to a secure future are needed to guide organizations through the process of longing for the good old days when the only security threat was somebody defacing their websites, to accepting the fact that we are in a new world of cyber threats that can have a material impact on the business.

Gavin Millard is the EMEA Technical Director at Tenable Network Security (www.tenable.com).



Infosec industry: Time to put up or shut up

by Brian Honan



The information security industry is one of the most exciting industries to be involved in. It offers many opportunities to exercise one's passion and curiosity about technology and address the challenges of keeping that technology secure.

The endless technological innovations and the rapid adoption of technology by businesses, consumers, and society makes our daily lives increasingly dependent on technology. This means that we, as an industry, need to rapidly address the challenges this technology revolution brings, and make sure that these new solutions are as secure as possible.

To some this an opportunity to reach out to those outside of information security to help them understand how these technologies should be adapted in a secure manner. We see a number of people engaging with mainstream media or speaking at various conferences to try and help those outside the field to understand the issues. We see initiatives such as OWASP, and more recently I Am The Calvary, trying to engage people within and outside the IT industry.

This often involves speaking in terms and phrases that non-technical and non-expert

people can grasp and understand. It requires a lot of time and effort to get the attention of those outside our industry. And once that participation has been achieved, it requires simplifying complex concepts and topics into terminology that non-technical people and society in general can absorb.

Unfortunately, instead of embracing these challenges, what I mostly see in the industry is an attitude of skepticism and in some cases even hostility to these initiatives.

The accusations laid against those trying to engage the public is that they are either doing it to raise their own individual profiles, or are looking to raise the profile of their company or movement in order to attract investors. Also, that their efforts undermine and undervalue the "purity" of the technicalities and science that information security professionals engage in every day.

These skeptics are very often the same people that regularly lament the lack of engagement by senior management or by government agencies, and their unwillingness to invest time, money and resources for securing systems and data.

These purists also despise the term “cyber security” and complain how the term “hacker” has been devalued by media associating it with criminal activity. However, we need to accept that this is how mainstream society views and understands these concepts.

Our systems, networks, and data are under constant attack and threat. We are not going

to be able to defend them solely by using technology, especially if those who control the budgets and purse strings do not understand or appreciate the problem.

We need to engage with other sectors of the business and society in general so that people are better educated and aware of the scale of the threats and challenges we face. So instead of shouting in an attempt to drown out the voices of those looking to create this engagement we should be shouting words of encouragement and try to find ways to amplify their message. If we cannot do this, then we should simply stay silent so as not to distract from or derail the message.

Brian Honan (www.bhconsulting.ie) is an independent security consultant based in Dublin, Ireland, and is the founder and head of IRISCERT, Ireland's first CERT. He is a Special Advisor to the Europol Cybercrime Centre, an adjunct lecturer on Information Security in University College Dublin, and he sits on the Technical Advisory Board for several information security companies. He has addressed a number of major conferences, wrote ISO 27001 in a Windows Environment, and co-authored The Cloud Security Rules.

FRESH SECURITY NEWS

www.twitter.com/helpnetsecurity





Fostering Innovation for Global Security Challenges

14 - 16 APRIL 2015

Sands Expo & Convention Centre
Singapore

www.interpol-world.com

BORDER MANAGEMENT

CYBERSECURITY

SUPPLY CHAIN SECURITY

SAFE CITIES

- **Source** from over 250 international solution providers
- **Connect** and cultivate business relations through networking events
- Get updated on **innovative** solutions and technologies
- **Exchange ideas** at INTERPOL World Congress

Your business and networking engine!

Register online at www.interpol-world.com now

Event Owner



Supported By



Supporting
Knowledge Partner

FROST & SULLIVAN

Held In



Managed By





nCrypted Cloud is an interesting offering that tackles threats by adding a strong security layer to the data used and shared via popular cloud-based data storage providers.

Patent pending key managing system

If you are planning to use a product of this kind to protect your private or corporate data, you should be interested in its inner workings.

An nCrypted Cloud account is created by submitting an email address and a password. Besides being used for authentication purposes, this information will also be run through the Password Based Key Derivation Function 2 (PBKDF2) in order to generate your User Personal Key. This private key will be stored on your computer, not on nCrypted Cloud's servers.

The patent pending system uses AES-256 bit encryption for protecting the data. When each of your files gets encrypted, a unique per-file password will be derived from your personal key and the additional entropy.

The result will be a password-protected zip archive containing the original file together with some other data that I'll mention later. Zip containers were chosen because the system creators wanted to use something that isn't proprietary.

From the security perspective, it is important to stress out that the encryption and decryption of data are always performed on the client.



secret.pdf.zip

Uploaded today by bk [redacted]m · 659.7 KB

Support for popular cloud storage providers

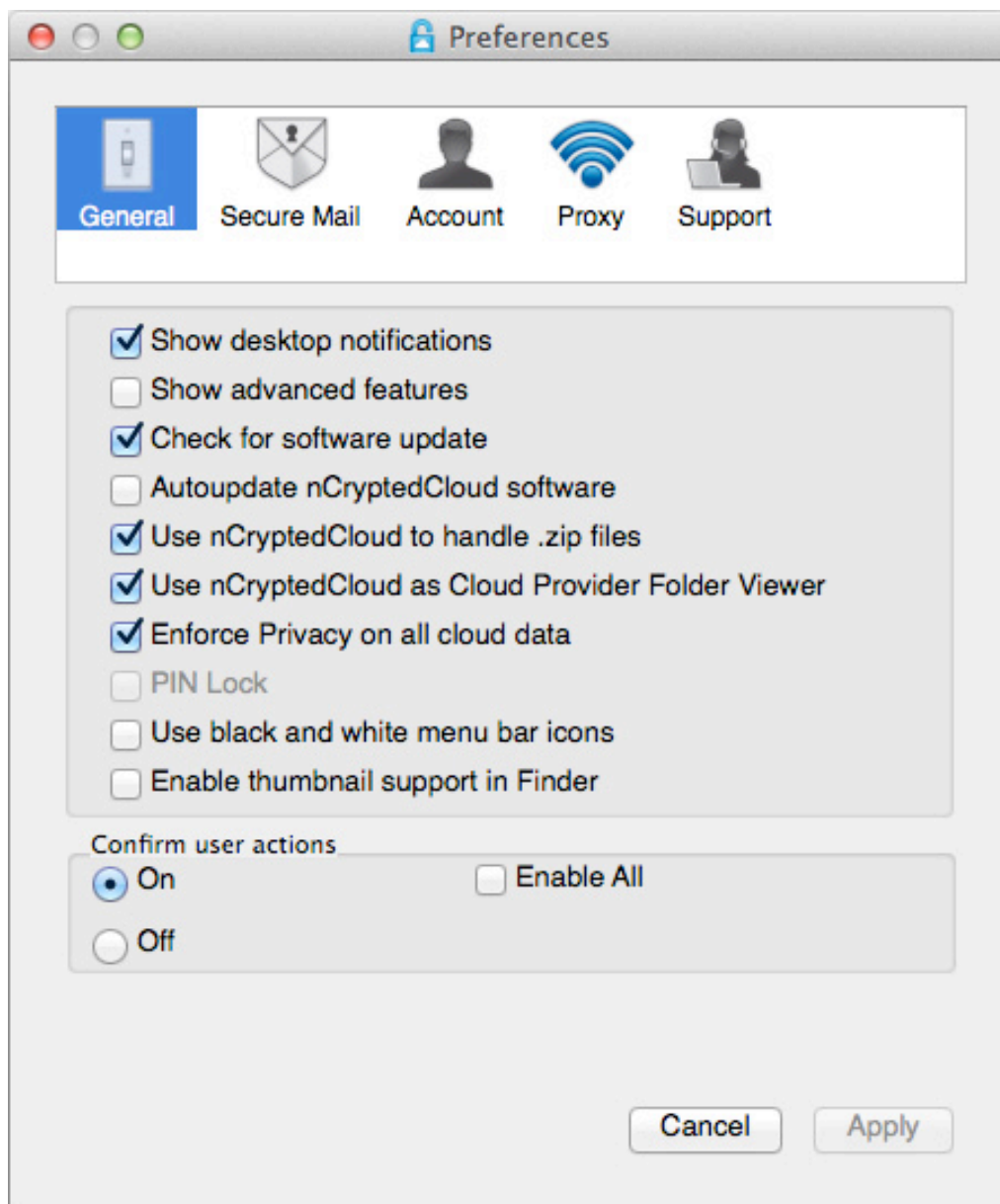
nCrypted Cloud consists of a web interface and client software that can be installed on Windows, OS X, iOS and Android devices. Your first interaction with the service will be through the web interface and you'll need to setup access to the cloud storage services you are using. nCrypted Cloud currently supports Dropbox, Google Drive, OneDrive, Box and Egnyte.

When you successfully link your account(s), you will be able to browse through the stored files via the nCrypted Cloud web interface. The interface is smooth but the files are arranged only by name and you cannot rearrange the listing according to size or date.

The next step is to download and setup the client software on the systems you'll use. The process is rather straightforward and as soon as you activate your account, you will be ready to go. While you will be using the newly created shared folder for syncing your stuff, have in mind that you first need to install sync software from your cloud storage provider.

A new shared folder named nCryptedCloud will appear and by default it will analyze your system and create specific folders for every storage provider that is setup on your system.

As nCryptedCloud is just a secure wrapper service around your storage provider, locally encrypted files will be uploaded to the cloud service of your choosing after you sync them.



Trusted sharing and collaboration platform

A survey released several weeks ago by secure file sharing provider Soonr shows that the majority of full-time employees access files remotely and three out of four share the files via email.


nCrypted Cloud makes it easy to share any file or folder with a click of button. This can be done both from the web interface, and from your local shared drive. The only difference is that when sharing the file via web, you can enable a watermark option which isn't supported in the nCrypted Cloud software application (at least in the OS X one). The watermark is placed over a document identifying the original recipient of the shared file.

Other options include:

- Viewing rights: Will the recipient be able to just view the file or will the download option be provided as well?
- Access rights: Does the recipient need to be an nCrypted Cloud user or not? Will an additional access code be needed to open the file?
- Expiration settings: When will the shared link expire - never, immediately after the first access, or after a specific time period (minutes, hours, days, months)?

From a technical standpoint, trusted sharing via nCrypted Cloud uses a unique symmetric key for every file or folder you share. When you share something with co-workers inside your organization, the symmetric key will be added to their key storage. As soon as sharing rights are revoked, the key gets deleted and further access is denied.

Trusted share

 **ncrypted.pdf**
/ncrypted.pdf

berislav.kucan@net-security.org

nCrypted Cloud

Apply saved settings

☒ View ☐ Download ☐ Upload ☒ Watermark ?

☐ Require login

☐ Require access code

☒ Expire share after...

First access One day One week Other...

[Save current settings...](#)

Hide settings

Cancel

Share

Enterprise management and compliance

In combination with a selected file storage provider, nCrypted Cloud is a powerful enterprise data storage and sharing solution. It provides detailed management of data sharing inside the organization and can be used to manage users and their devices.

Auditing mechanisms can be used to track all company data and its behavior inside the corporate infrastructure. Per user and per organization tracking is available, so one can see who has been accessing and sharing what data, and who are the recipients.

Auditing

History

Search






From

Select date

To

Select date

Q

Name	Action	Date	User	Device
 nrypted.pdf	FileDownload	11/18/2014 11:50	berislav.kucan@	CWP Collaborations
 nrypted.pdf	FileOpen	11/18/2014 11:50	berislav.kucan@	CWP Collaborations
 nrypted.pdf	TrustedSharing	11/18/2014 11:48	Berislav Kucan (Personal)	CWP Berislav Kucan
 nrypted.pdf	FileUpload	11/18/2014 11:45	Berislav Kucan (Personal)	CWP Berislav Kucan
 bug-pouch.pdf	FileOpen	11/18/2014 11:39	Berislav Kucan (Personal)	CWP Berislav Kucan

The service enables its users to have multiple identities, which comes in handy when you need to separate your personal and corporate identity. This is a nice touch and broadens the appeal of nCrypted Cloud. If an employee leaves the company his corporate key will be revoked, but he will still have access to the files encrypted by using his personal identity. Similarly, the company cannot access its employees' personal files.

Depending on the number of deployed users (see the pricing section), you will be able to use some advanced functions such as SAML 2.0 for deploying single sign on (SSO) capabilities, Active Directory integration, DLP integration with reverse proxy, MDM controls, etc.

The service enables covered entities and business associates to maintain HIPAA/HITECH regulatory compliance related to cloud based storage and sharing when delivering health care services. It can also aid in addressing data security elements of various families of controls developed by NIST for FISMA compliance.

Restoring data

nCrypted Cloud never stores your private keys, but there is a smart failsafe mechanism that uses another set of generated keys.

Besides the User Personal Key, the system will also create you a Public/Private key set dubbed User Recovery Key.

This key is stored locally on the client's computer but you can store an encrypted variant of it on nCircle Cloud servers as well. When you encrypt a file, its unique password gets encrypted as well by using the User Recovery Key. This value is then stored in the comments file of the resulting zip archive. This allows users to recover an encrypted file if they still have the recovery key.

Running an encrypted zip file through zipinfo will show the encrypted password in the comments section (parts of the output redacted).

```

Downloads — bash — 85x35
berislav@imac:Downloads$ zipinfo -z secret.pdf.zip
Archive: secret.pdf.zip 675506 bytes 3 files
<zipcipher ver="1">
<![CDATA[
Created by nCryptedCloud Version 1.1.0.5 (Mac OSX)
Copyright (C) nCrypted Cloud. All rights reserved.
]]>
<rc rcid="{647[REDACTED]4928D452E}">
<r>
<rk>{3[REDACTED]2}</rk>
<rb>
<![CDATA[vDcDyyS3T1ehdW0701HEZVinnayvV01Kn913bAG5I.v0K4Woh8B+dv80rI+NL5hdj0=0z
e7ECx3HZnZVlCvrE6poTXJ3[REDACTED]MK5Sswiz6Vw7
Qm0SB0=13EZyohF1R28c0b0w/v0iz56=MtToDhyTPEFz8/W4Wyhx3jaUK+8TpeXVue5zg7UHgz8Ncbt5KhKr
ZV[REDACTED]fCVd4xaavRc0PNycuoQD0R+6Z8EIGbcIzeKfQG40A
MC0Kw4Am4VPxEbPFGWQ==]]>
</rb>
</r>
</rc>
<ar>
<fid>{28D[REDACTED]-FD633128D185}</fid>
<fv>0114[REDACTED]55552</fv>
<o>
<id>254[REDACTED]2753</id>
<iid>{05C0F5B1-6[REDACTED]C1}</iid>
<fn>Berislav Kucan</fn>
</o>
</ar>
</zipcipher>
-rw---- 0.0 fat 185 t- defN 18-Nov-14 12:08 readme.txt
-rw---- 0.0 fat 197 Tx u099 18-Nov-14 12:08 manifest
-rw---- 0.0 fat 697323 Bx u099 18-Nov-14 12:08 secret.pdf
3 files, 697705 bytes uncompressed, 674183 bytes compressed: 3.4%
berislav@imac:Downloads$

```

Pricing

nCrypted Cloud costs \$10 per user on a monthly basis. Depending on the size of the company (25+, 250+ and 2500+ users), every tier has its own set of extra features.

The pricing is for US based companies, for customized or international pricing you'll need to contact their sales team. Consumers (one user, unlimited devices) can use the service for free.

Berislav Kucan is the Director of Operations for (IN)SECURE Magazine and Help Net Security (www.net-security.org).



Prioritizing penetration testing

by Greg Anderson



We all know that information security is focused on the protection of confidentiality, integrity, and availability of information and information systems. What we tend to forget, however, is that these tenets, especially the confidentiality and integrity ones, have existed long before the ubiquitous adoption of information technologies.

The Defense Secrets Act of 1911 was one of the first US laws that criminalized the disclosure of government secrets. To combat threats to the disclosure of this sensitive information, strategic plans were implemented that governed data classification, need-to-know, handling and distribution, etc. While I am sure there was some level of testing performed to validate certain security controls, greater emphasis was placed on governance rather than testing.

Today, however, it is common to observe speakers and attendees of security conferences emphasizing penetration testing rather than the strategic elements of information security. Given the present day trend of data breaches being announced on an almost weekly basis, is this paradigm shift and increased focus on penetration testing really ful-

filling the intended mission of information security? To be clear, I am not saying that we should stop doing penetration testing. Penetration testing can be extremely valuable when used appropriately. What I am saying is that we need to take a step back and reconsider why we are performing penetration testing, when it is and when it's not appropriate and, in the latter case, what else should we be doing instead?

Why?

The purpose of a penetration test is to validate the effectiveness of an organization's security controls - technical, operational, and management controls - against a cyber-attack by simulating the objectives and actions of an attacker.

The results of a penetration test should detail the effectiveness of the organization's security posture, relevant findings, recommendations, and a strategic plan for remediation. Ultimately, penetration tests are performed to identify gaps in an organization's established and implemented security program and to provide a direction for remediation that results in added business value.

As technologists, we sometimes lose sight of business value and focus our attention on technology. Business decision makers, however, don't hire expensive consultants simply for the sake of presenting them with a technical challenge; they expect to receive a certain amount of value for their investment. For this reason, it is important to understand when a penetration test will and will not provide the

most business value and advise business stakeholders accordingly.

When?

Within the Critical Controls for Effective Cyber Defense, penetration testing is addressed in Critical Control 20, meaning it is the last thing that should be considered to support an effective security posture. This approach may not be appropriate for every business, but it does provide a level of guidance on how to prioritize penetration testing with regard to other aspects of an organization's security program.

For example, during pre-engagement meetings, an experienced penetration tester may begin to become aware of what security controls an organization is lacking or where weaknesses in existing controls may exist.

The results of a penetration test should detail the effectiveness of the organization's security posture, relevant findings, recommendations, and a strategic plan for remediation.

When significant gaps in an organization's security posture come to light, such as the lack of automated patch management, does it really make sense (i.e. provide the most value) to proceed with a penetration test? One could easily argue that in this scenario, the organization should scrap the penetration test and invest in an automated patch management solution, since the penetration test will likely uncover that this is a critical weakness anyways.

The point here is that penetration tests should be used to measure the effectiveness of a well thought-out and established security program. In other words, the organization is following a standard, security framework, or relevant industry guidance (e.g. Critical Security Controls, NIST 800-53, ISO 27000, etc.); they are aware of and have documented what security controls they have in place, where they have taken exception, and where they still have gaps.

A penetration test should then focus on validating the effectiveness of the implemented security controls and provide prioritized guid-

ance on remediating gaps. Using penetration tests in this manner ensures that the results of a penetration test do not just mirror information from well-known guidance, but instead provide tailored feedback on how the organization can tune their existing defense to be more effective.

What else?

When choosing what activities to prioritize over penetration testing there are a number of things to consider, primarily based on our perspective or role within the organization. The most important thing to keep in mind is that we want to focus on security as a whole rather than the security silos that we tend to act within.

As a member of the information security department you should develop a prioritized roadmap for improving the security of your systems. Integrate security standards and established industry best practices into your plans. Include penetration testing-like steps in the roadmap to validate the effectiveness of specific security controls.

Have this plan approved by management and use it as leverage to push back on vendors, service providers, and management when funding, products, and solutions do not align with the roadmap.

As a business stakeholder, you should listen to your security department on where funding is needed and support those initiatives. Only hire consultants to perform penetration testing when your security posture is mature enough to benefit from it. Approve security roadmaps and defend them to other members of management.

As a consultant, you should provide more valuable upfront consultations with your clients. Review their security program or solicit information on their security posture.

Make recommendations on prioritizing and addressing the low hanging fruit that can be integrated into their security roadmaps; when those items are addressed, perform the penetration test to identify less obvious gaps. Perform more limited scope penetration testing on the specific controls implemented through their security roadmaps.

Greg Anderson is a Senior Cyber Security Engineer with experience in Information Technology and Information Security engineering, auditing, and consulting. Greg's passion is in Information/Cyber Security governance and ensuring that security objectives align with business missions and the overarching spirit of the security discipline. Find out more at www.sechammer.com or www.linkedin.com/in/end6ame.

Want to reach a large audience of security pros by writing for (IN)SECURE?



Send your idea to mzorcz@net-security.org



Detekt government surveillance spyware on your computer

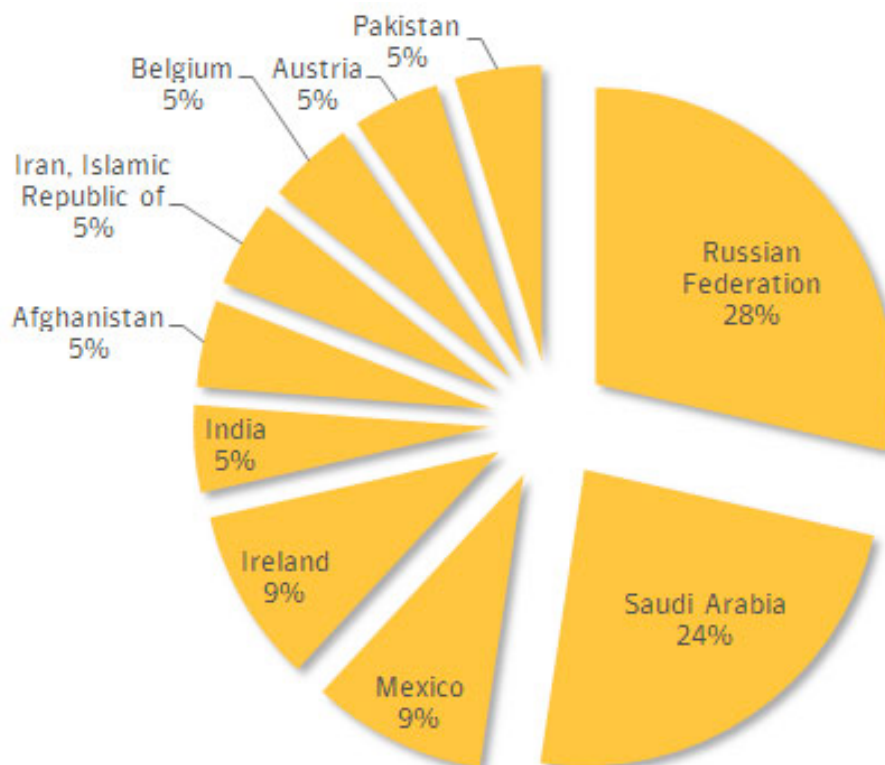
Amnesty International, Digitale Gesellschaft, the Electronic Frontier Foundation and Privacy International have partnered to create and release a free and open source tool for detecting traces of known surveillance spyware on Windows computers.

The tool - dubbed Detekt - is written in Python and relies on Yara, Volatility and Winpmem to scan the memory of a running Windows system, and is currently able to spot pre-defined patterns that point towards the following malware running on the computer: DarkComet RAT, XtremeRAT, BlackShades RAT, njRAT, FinFisher FinSpy, HackingTeam RCS, ShadowTech RAT, and Gh0st RAT.

At the moment it can be used on all Windows version from Windows XP to Windows 8 (32 and 64 bit) and Windows 8.1 (32bit).

As noted above, Detekt is able to identify the presence of some spyware, but not all. So even if it doesn't find anything, this doesn't mean that there is no spyware on the machine. Also, the tool only detects the malware - it can't remove it. If it finds something, it will generate a log file with additional details that will allow technical experts to investigate the matter. In any case, that computer - and the files, emails, and other things on it - should be considered compromised.

Detekt was developed by security researcher Claudio Guarnieri with the help of people from the aforementioned organizations and others. The tool is available in several languages.



Regin backdoor: Sophisticated, stealthy, state-sponsored?

Symantec researchers are warning about a new, complex cyber espionage tool that has been around for years and has likely been created and is wielded by a nation state.

Dubbed Regin, the malware has been used since at least 2008 to mount spying operations against government organizations, infrastructure operators, private sector businesses, but also researchers and private individuals.

In fact, almost 50 percent of all the identified targets are either private individuals and small businesses, followed by telecoms (28 percent), companies in the hospitality and energy business, airlines, and research organizations. Another thing that comes as a bit of a surprise is the fact that the malware was aimed mainly at individuals and organizations in the Russian Federation, Saudi Arabia, Ireland, and Mexico.

Regin has been compared to Stuxnet, Flame, Duqu and Turla (Snake) - all highly complex malware used in sophisticated attacks that are believed to be state-sponsored.

"Backdoor.Regin is a multi-staged threat and each stage is hidden and encrypted, with the exception of the first stage. Executing the first stage starts a domino chain of decryption and loading of each subsequent stage for a total of five stages," Symantec researchers explained. "Each individual stage provides little information on the complete package. Only by acquiring all five stages is it possible to analyze and understand the threat."

The malware is modular, therefore customizable.

Even though the researchers got their hands on two different variants of the backdoor - one that was used between 2008 and 2011, and another from 2013 onwards - they still don't know what infection vectors have been used. It's likely that the malware was delivered via spoofed versions of well-known websites or by exploiting vulnerabilities in apps. "On one computer, log files showed that Regin originated from Yahoo! Instant Messenger through an unconfirmed exploit," they pointed out.

Regin is believed to be wielded by the UK spy agency GCHQ and/or the US NSA, and it has been confirmed that it has been used in the attack against Belgacom, Belgium's primarily state owned telecom, and its subsidiary BICS.

New Citadel variant is after your master password

According to IBM Trusteer researchers, the newest Citadel variants have been instructed to start capturing user keystrokes when the user starts open-source password management solutions Password Safe or KeePass, or the neXus Personal Security Client, an authentication solution for securely effecting financial or e-commerce transactions.

The researchers found this new Citadel configuration file on a user machine protected by a company's solution, but it's impossible to tell if the machine belongs to a private user, an enterprise employee or a contractor.

"The machine was already infected by Citadel when IBM Trusteer Apex was installed on it. Therefore, it is unknown exactly how it became infected," noted Dana Tamir, Director of Enterprise Security at IBM Trusteer. "An

analysis of the configuration file shows that the attackers were using a legitimate Web server as the C&C. However, by the time the IBM Trusteer research lab received the configuration file, the C&C files were already removed from the server, so researchers were not able to identify who is behind this configuration."

It could be a simple opportunistic attack, but it's also possible that it's a more targeted one. Citadel began its existence as generic financial information-stealing malware, but has recently been turned into an APT tool. The Citadel Trojan is capable of bypassing most threat detection security systems and laying low until it's instructed to spring into action.

Using password managers and authentication software is always a good idea, but users must be aware that they also need to keep their computers free of malware that can compromise the master password and, consequently, all other passwords stored in the software.

Tens of thousands web servers backdoored via pirated CMS themes and plug-ins

Over 23,000 websites set up with the help of Joomla, WordPress and Drupal content management systems have been compromised and used for illegal search engine optimization by an attacker who managed to social-engineer site administrators to install a backdoor on their servers.

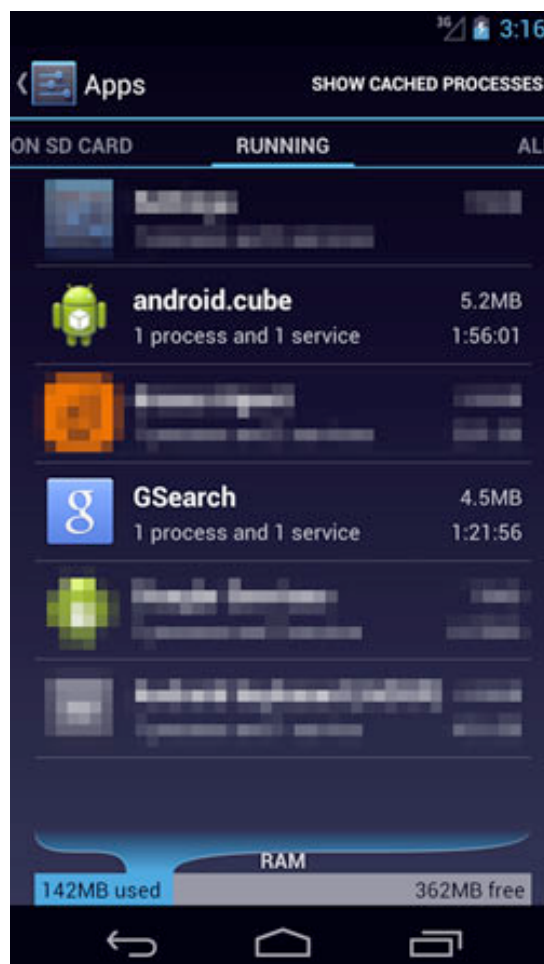
Dubbed CryptoPHP, the backdoor has been included in pirated themes and plug-ins for the aforementioned CMSes, and linked for download on some two dozen specially crafted sites that openly offer pirated software and "nulled" scripts. Once a plugin or theme is installed by a site administrator, the backdoor is also embedded, and adds an extra administrator account that allows the attackers to access to the website even if the backdoor is found and removed. CryptoPHP is capable of updating itself, contact an extensive infrastructure of C&C domains and communicate in encrypted form, and can be

controlled via email or manually in case the C&C servers are taken down.

"With the help of the NCSC, Abuse.ch, Shadowserver and Spamhaus we have been able to gather data about the scale of the operation ran by the CryptoPHP authors. Most C&C domains that were active at the time of publishing have been either sinkholed or taken down. From the sinkholed domains we've been able to gather statistics," Fox IT researchers shared.

"In total 23.693 unique IP addresses connected to the sinkholes. We are already seeing a decline in sinkhole connections, on the 22nd 20.305 connections were made, on the 23rd 18.994 and on the 24th it was already down to 16.786. These numbers are however not a clear indication, mostly because the servers connecting to our sinkholes were shared hosting with at least 1 or multiple backdoored websites. This means the actual affected websites will be higher."

The researchers have provided two Python scripts to help administrators detect CryptoPHP.



Trojanized Android firmware found on inexpensive handhelds

It's unfortunate, but true: we live in a world where even if we buy a brand new mobile phone, it's no guarantee that it's malware-free.

Researchers from Russian AV company Dr. Web have unearthed a Trojan embedded directly in the firmware of numerous Android handhelds.

Becu, as they dubbed the malware, can download, install and remove software from the handheld with the user being none the wiser. It is triggered into life either by turning on the affected device or via a specially crafted SMS.

The malware is modular in nature. Also, being firmware-embedded, the program is very hard to remove by conventional methods.

The main module downloads the rest of them, which make it possible for a remote attacker to install and deinstall additional malware or software on the device, and to intercept

inbound SMS messages from specified numbers.

The researchers discovered the malicious code on a number of common inexpensive Android devices: UBTEL U8, H9001, World Phone 4, X3s, M900, Star N8000, and ALPS H9500.

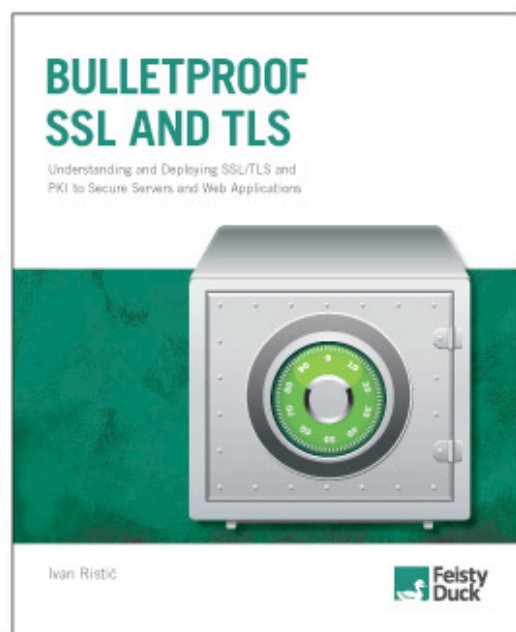
"The firmware infected with Android.Becu.1.origin is either downloaded by users themselves or installed by unscrupulous smartphone and tablet suppliers participating in a criminal scheme," they say.

The Trojan can be removed by disabling its main file (com.cube.activity) on the list of installed programs (the package), then manually removing the other components (com.system.outapi and com.zgs.ga.pack).

"Removing the principal malware component manually on a device with an enabled root account and reflashing the handheld with malware-free firmware (the latter of which will result in the loss of all the stored information) are more radical approaches to neutralizing Android.Becu.1.origin," they noted.

BULLETPROOF SSL AND TLS

Understanding and deploying SSL/TLS and PKI
to secure your servers and web applications



For system administrators, developers, and IT security professionals, this book provides a comprehensive coverage of the ever-changing field of SSL/TLS and Internet PKI. Written by **Ivan Ristić**, a security researcher and author of **SSL Labs**, this book will teach you everything you need to know to protect your systems from eavesdropping and impersonation attacks.

"The most comprehensive book about deploying TLS in the real world!"

Nasko Oskov, Chrome Security developer and former SChannel developer

"Meticulously researched."

Eric Lawrence, Fiddler author and former Internet Explorer Program Manager

"The most to the point and up to date book about SSL/TLS I've read."

Jakob Schlyter, IT security advisor and DANE co-author

For 20% off use code (IN)SECURE
www.feistyduck.com



Report: McAfee FOCUS 14 by Mirko Zorz

In late October, security professionals from all over the globe flew to Las Vegas for McAfee's annual FOCUS conference.

This year's all-star keynote lineup was comprised by Renée J. James President, Intel Corporation; Chris Young, SVP and GM, Intel Security; Condoleezza Rice, Former US Secretary of State; and Mike Fey, CTO & GM of Corporate Products, Intel Security.

Given a complex threat landscape, most IT security professionals need to have a wide area of interest. McAfee FOCUS 14 featured more than 75 breakout sessions, which made it easy to find stimulating presentations.

At the same time, several attendees told me their biggest problem was deciding what talks to attend, since so many were about compelling topics. No wonder, since you could learn seemingly everything about next-generation firewalls, virtualization, hacking wireless networks, intrusion detection, DDoS attacks, and much more.

All these great presentations aside, the biggest value of McAfee FOCUS 14 was the networking opportunities. Visitors had a chance to rub shoulders with experienced

CISOs, and grab a coffee with security pros running immensely complicated networks, all under one roof in a relaxed atmosphere.

The sponsor expo was open daily, enabling attendees to view demos and explore the technology offered by some of the key players in the industry. Especially interesting were the 20-minute, informal poster board sessions called Turbo Talks. After seeing the complete schedule, I wished I had much more time to spend on them.

All in all, McAfee FOCUS was truly a remarkable event where I got the privilege of interacting with some of the brightest people in our industry, and I can't wait to go back next year.

Organizations choose network performance over advanced security features

McAfee, part of Intel Security, published a new report exploring the challenges organizations face in deploying security protections while still maintaining an optimally performing network infrastructure.

Issued at McAfee's FOCUS 14 conference, the report uncovered that an alarming number of organizations are now disabling advanced firewall features in order to avoid significant network performance degradation.

As part of the report, 504 IT professionals were surveyed, with 60 percent stating that the design of their company's network was driven by security. However, more than one-third of respondents admitted to turning off firewall features or declining to enable certain security functions in an effort to increase the performance of their networks.

"It is unfortunate that turning off important firewall features because of network performance concerns has started to become common practice," said Pat Calhoun, General Manager of Network Security at McAfee, part of Intel Security. "At McAfee we believe this is unacceptable. Companies simply should not have to make that kind of trade-off."



Chris Young and Renée J. James

According to the report, the most common features disabled by network administrators include deep packet inspection (DPI), anti-spam, anti-virus, and VPN access. DPI, the feature most frequently disabled, detects malicious activity within regular network traffic and prevents intrusions by blocking offending traffic automatically before any damage occurs. It is essential for robust threat defenses, and is a key component of next generation firewalls,

which now represent 70 percent of all new firewall purchases.

“When I hear about people turning off security they paid for because of performance decreases - this upsets me so much,” said Ray Maurer, CTO at Perket Technologies. “I get a bad feeling knowing I had to remove security in the name of performance. I have a hard time sleeping because it is not a matter of if a network will be compromised, but when.”



Many organizations choose to turn-off DPI because of the high demands it places on network resources, yielding upwards of a 40 percent degradation of throughput, according to third-party research firm, Miercom. McAfee Next Generation Firewall, however, with DPI enabled sustained one of the highest firewall throughputs in Miercom's testing. Overall, McAfee Next Generation Firewall sustained much higher throughput performance with security features enabled when compared to other products in this class. Competing prod-

ucts tested exhibited an average of 75 percent or more performance degradation for DPI, anti-virus and application control when enabled.

According to Calhoun, “With the number of confirmed data breaches climbing more than 200 percent in 2014 over the previous year, it has never been more critical for organizations to embrace the advanced protections available to them with next generation firewalls.”



Chris Young

McAfee outlines channel initiatives

During this year's event, McAfee unveiled several key channel initiatives to help nearly 700 channel partners from around the globe build sustainable security practices.

The purchase behaviors and buying centers for security technology have changed drastically in the last couple of years. As a result, McAfee announced a new, more flexible partner program framework that allows partners to evolve their business models and adapt to the changing customer landscape.

Highlights of the new partner program include:

1. **New name:** As part of continued integration with Intel, effective January 1, McAfee is changing the name of its SecurityAlliance Program to the Intel Security Partner Program.
2. **Simplified solution competencies:** In an effort to reduce program complexity, McAfee will consolidate from five product competencies to three solution competencies:

Endpoint Security, Network Security and Security Management.

3. **Removing baseline certifications and expanding continuing training:** Continuously streamlining training requirements is a critical element to success for any partner program. McAfee is removing the need for partners to complete Baseline Certifications and is expanding Continuing Education to give all partners the flexibility to earn credits for training that is most relevant to their business. This change results in an approximate 30 percent reduction in overall training requirements for McAfee Elite Partners.
4. **Programs to specializations:** Security is a rapidly changing market, requiring a flexible channel program that can quickly and easily integrate programs as well as add new or acquired technologies.

In 2014 McAfee identified enablement as an area of focus and tripled its investment and drove a 40+ percent increase in Continuing Education participation.

The next phase of enablement enhancements are:

CloudRunner Platform: The new CloudRunner Platform is a free, simple, on-demand platform that enables partners to access McAfee's product portfolio via the cloud. The platform makes it easier and faster to deliver product demonstrations to customers, which can accelerate sales cycles and help to increase profitability by lowering the cost of sales.

With CloudRunner, partners can build a demo environment in an average of five minutes without the need to have an appliance, box or virtual machine set up in a customer's environment. CloudRunner will be available in early November and will include, McAfee Next Generation Firewall (NGFW), McAfee Endpoint, and McAfee Network Security Platform (NSP) environments.

Post-Sales Services Enablement: IDC is projecting in 2015 the total addressable market for Security System Integration Services will be more than \$12 billion¹. To help strengthen a partner's implementation serv-

ices, we are introducing post-sales services training and certifications.

There are eight, four-day, instructor led Post-Sales Services Enablement, including NGFW, McAfee Security Information Event Management, McAfee e-Policy Orchestrator, NSP, McAfee Host Intrusion Prevention, McAfee Advanced Threat Defense, McAfee Drive Encryption, McAfee Application Control and McAfee Change Control. Upon passing the associated exam, course participants are recognized as a Certified McAfee Security Specialist (CMSS), validating their installation, configuration, management and basic architecture knowledge.

Creating a Service Delivery Specialization: This will be the first Specialization built under the new partner program framework. It will also be the first McAfee Specialization that uses the CMSS certification as a core requirement. This specialization, available in the second half of 2015, will enable partners to more effectively deliver implementation services which are instrumental in driving partner profitability and customer satisfaction.



McAfee also made two key channel partner experience announcements:

Partner 360 Dashboard: The Partner 360 Dashboard provides partners with a detailed analysis of their performance and profitability, allowing them to make better business decisions. It provides a detailed view into approximately 10 different business indicators, including sales performance, rebate and marketing development funds. The platform will be piloted with a select group of North America

partners in Q4 2014 with a broader roll out aimed for the first half of 2015.

SMARTmarketing Platform: McAfee is committed to helping channel partners make money and more easily turn prospects into leads. To help drive this effort, McAfee has made an investment in a new marketing platform as part of the McAfee SMARTmarketing initiative to give partners the tools needed to run their own marketing activities including syndicated web content, email marketing, social media syndication and website analytics.



Managing the security of applications in private and hybrid cloud infrastructures

by Prakash Sinha



Despite security concerns, organizations are moving to the cloud due to its benefits and cost-effectiveness. By doing this, they are required to deploy business critical applications in the public, private and/or hybrid cloud infrastructure. But this transition presents challenges that need to be addressed.

While this article primarily touches on those related to security and preventing cyber-attacks, there are other aspects you'll need to take into consideration, such as IT equipment failure and its consequences to business continuity, application availability, application performance optimization, visibility and monitoring, and guaranteeing service level agreements (SLA) for tenants.

As we consolidate data centers and make applications web-enabled and delivered through either cloud or hybrid environments, we can assume that cyber-attacks will remain prevalent for a variety of reasons. As application services are accessed via the web and frequently consumed via Application Programming Interfaces (APIs), they are susceptible to denial of service attacks or increasingly application-specific ones. Securing these applications is a complex and resource intensive task, both in terms of provisioning and main-

tenance, and in terms of allocating adequate computing resources. Compromising on either one of them may result in security breaches to the application and/or a significant performance hit to the application, especially when under attack and protection is needed the most.

You'll need to address security at each point of the network - from user identity for administration and access, password policies, auditing and logging across the board, to securing the communication protocol, assessing vulnerability in your applications, detecting and preventing malicious attacks, securing data when at rest or in transit, and addressing any point of possible information leakage due to social engineering. Add to this correlated visibility and forensics covering all of these parts so you can get promptly alerted in the event of a breach and can take remedial action in case of an incident.

Suffice it to say, the more security measures you add, the more impact they will have on performance and latency. Adequate resources need to be allocated - especially for securing business critical data - so that user experience is not hampered.

Preventing Denial of Service

There are some who believe DDoS attacks are isolated events and you need to just weather a storm that will eventually pass. But we've witnessed an increase of DNS-based volumetric floods, which are difficult to detect, require very few resources and can easily maintain anonymity, and DDoS mitigation solutions need to offer a wide attack coverage that can detect not just one attack vector, but a multi-vector attack that hits different layers of the infrastructure.

The first line of defense is edge security. Edge protection typically involves DDoS detection and mitigation services that shield network and application server resources.

Once a DDoS attack is detected, a DDoS protection device or cloud service can divert malicious traffic coming into the customers' network to a Scrubbing Center (SC).

The SC will forward only the legitimate traffic back to the customer, thus eliminating all threats from attacking any part of the customers' network. DDoS mitigation can be further improved by using Intrusion Prevention Services (IPS) and firewalls.

As you move your applications or services to the cloud, you'll need DDoS prevention and mitigation, IPS, and firewall services in your cloud environment to cost-effectively protect your applications.

If you were responsible for securing your application in your own data center, you know how difficult, detail-oriented and time consuming that task is. Just because you're moving those applications into the cloud doesn't mean that this will change.

Protecting applications

If you were responsible for securing your application in your own data center, you know how difficult, detail-oriented and time consuming that task is. Just because you're moving those applications into the cloud doesn't mean that this will change.

At the application and data level, it's now almost commonplace to use transport level security (TLS/SSL) for protecting communications. Additional protection may be provided by Web Application Firewalls (WAFs), which usually focus on the application and data layer and offer protection for application-level attacks such as cookie poisoning, scripting attacks, request forgery, injection attacks (for example SQL or LDAP), and so on – all executed with the intent of stealing or hijacking user data.

Make sure you routinely run vulnerability assessment tools and scan your source code regardless whether it's on-premises or in the cloud.

Make sure to deploy a WAF for the applications that remain vulnerable either because there is currently no patch for a specific vulnerability, or because you can't currently implement it.

Sometimes Denial of Service attacks may be cloaked with SSL. In such cases, once SSL session information is decrypted, the information on the attacks should be detected and relayed to the edge protection to prevent these attacks at the perimeter, or to route these malicious attacks to the SC or cloud-based scrubbing service.

While a service outage is obviously undesirable for customer experience, there are compliance and financial issues to consider as well as you move applications into the private and hybrid cloud environments.

Providing segregation and isolation to guarantee SLA

In a multi-tenant deployment, if the individual environments are not segregated, tenants may start competing for shared server and network resources during peak resource utilization.

It has been documented in the past that 87 percent of security industry professionals stated that they experience service level issues – 60 percent encountered service degradation, while 27 percent experienced outage.

While a service outage is obviously undesirable for customer experience, there are compliance and financial issues to consider as well as you move applications into the private and hybrid cloud environments. The isolation of resources is especially critical in situations where financial and user data are involved.

There are many compliance requirements (PCI, HIPAA, GLBA, and so on) that may further mandate isolation of various environments.

Additionally, in cloud environments where all tenants share the same network and security resources, a potential spike in resource consumption or a wrong configuration change of a single tenant may impact all other tenants, severely impacting an application's quality of service or its availability.

Look for tenant and resource isolation as a key tenet for your architecture: it provides privacy, isolates fault to tenant instances, guarantees performance for tenant instances and

eases capacity planning and resource management, especially for different roles that may be managing different aspects of deployment.

Gaining visibility into the network and application environment

When it comes to security, one of the important areas is correlated view and monitoring of real time transactions, events, notifications and alerts. Security Information Event Management (SIEM) tools, available as a cloud service or as virtualized or physical devices, collect information from network and security devices, identity and access management systems, vulnerability management and policy compliance tools and various applications, and correlate that information with application logs.

These tools are especially useful as a malicious user may try a variety of ways to access a particular system. During an incident, you may want all available tools to do a forensic analysis.

Conclusion

Even if your applications are now fully developed or deployed in the cloud, you will still need to apply the same rigour that you applied to securing your on-premises applications.

Your practices should address communication security, DDoS prevention and mitigation, application security including encrypting data as needed, access enforcement, correlated visibility, auditing and logging. Have the right tools at your disposal for forensics should an incident occur.

Prakash Sinha is the Vice President of Application Delivery Solutions at Radware (www.radware.com), a provider of application delivery and security solutions that assures the availability, performance, and resilience of business-critical applications for over 10,000 enterprises and carriers worldwide.



Most enterprises allow BYOD in their environment, with varying levels of supervision. Typically, these are tablets and smartphones but the number of other Internet of Things devices being brought into the enterprise is on the rise. I like to refer to this as the Enterprise of Things.

Where do you stand?

proval is desired; and how will you be able to detect rogue devices if they show up on your network? Policies describe your expectations, so make sure you are clear about what you expect.

To create an environment of accountability, make sure you have mechanisms to tell if someone has violated your policy. If you can't identify and contain policy violations, you will need to either implement additional controls in your environment or remove that section of the policy until you can detect violations. After all, if you don't have the means to enforce violations, the policy is not a policy, just a hope.

Do your users know about your policies?

Once the policies are clearly documented and you know how you'll enforce them, communication to your user community is vital. I once worked with the CISO of a huge corporation and he asked me to review his security policies to make sure they were sufficient. He handed me a couple of large binders and I asked him, "How many of your users are aware of these policies?"

In his case, the only people who were aware were his system administrators, his security team, and his direct staff. The rest of the

company didn't have any idea these policies existed. I deferred reviewing his policies until he'd communicated them to the company (about a year later). My assertion: if nobody knows about the policies it doesn't really matter whether the policies in the binders are any good.

By the way, I have found it more effective for organizations to not only communicate the policy details, but also to document the goal of the policies along with the "thou shalt" language. In other words, explain the "why" and the desired outcome of each policy. In these cases, you can often get users to buy into the goal even if they don't like the specifics of what you're asking them to do.

In fact, one of the organizations I work with was able to greatly improve compliance by taking suggestions from its user community. A number of creative users who understood the objectives of the rules were able to come up with lower-friction ways to achieve the objectives.

ONCE THE POLICIES ARE CLEARLY DOCUMENTED AND YOU KNOW HOW YOU'LL ENFORCE THEM, COMMUNICATION TO YOUR USER COMMUNITY IS VITAL

Continuous situational assessment

Now that you've decided what you want, you have the policies and controls to make sure your expectations are being met, and people know what's expected of them, your work is only just beginning.

The threat landscape in the Enterprise of Things is constantly changing so constant vigilance is required. That means establishing a strategy that enables continuous discovery and awareness of what's on your network so you don't suddenly become vulnerable without realizing it.

A key part of this strategy is to go beyond discovery into actively profiling, probing, and risk-scoring the devices that show up on our net-

work, whether they are connected directly (plugged into your network or connecting directly to your wireless access points), or indirectly (part of your employees' or partners' network and mingling with your core network via remote connectivity). I describe this as "measuring your attack surface" so you can objectively determine how your risk and exposure is changing over time, and it should be automated as much as possible.

A significant increase in either targetable systems or known vulnerabilities on those systems can cause a spike in your attack surface, which should not only be noticed but should trigger a proportional response from your security team. After all, the more you know, the better equipped you are to do something about the situation.

IF YOU RELY SOLELY ON TECHNICAL CONTEXT, YOU'RE NOT DOING YOUR BUSINESS ANY FAVORS

Business context can trump technical context

Many organizations rely mainly on technical context like CVSS scores, patch levels, etc. to drive their actions. That can work, but I find it more effective if you also integrate business context into your assessment criteria.

Business context includes things like location, business purpose, whether the asset houses or handles sensitive information, whether it is subject to specific SLA's or regulatory requirements, etc.

Integrating business and technical context allows you to make reasoned, business-oriented decisions about how to respond to changes in your attack surface. For example, the potential business impact of a medium-severity security exposure on a highly critical server involved in order processing can be


much more important to resolve than a higher-severity security issue on an internal media server. If you rely solely on technical context, you're not doing your business any favors and you may not be applying your precious resources where they'll get the biggest return.

The Enterprise of Things never sleeps

I'm only scratching the surface here, but the key thing to remember is that we now live in a world in which the "things" we don't control can suddenly threaten the assets and data we're responsible for protecting.

Developing an automated, scalable strategy that allows you to quickly identify potential security threats, prioritize them based on business risk, and take deliberate action based on what you see is crucial in protecting your business in the Enterprise of Things.

Dwayne Melancon is the CTO at Tripwire (www.tripwire.com). When he's not busy fighting cybercrime, he meets with as many customers as he can to foster a deep understanding of their problems, and collaborate with them on practical, real world solutions.



> Visit www.insecuremag.com
> SUBSCRIBE TO (IN)SECURE MAGAZINE



INFOSEC WORLD 2015

Conference & Expo

March 23-25, 2015 | Disney's Contemporary Resort | Orlando, FL | Bonus Workshops March 21-22, 25-27


Earn Up to
55
CPEs!

Top-notch training. Compelling speakers.
Meaningful interactions.

(IN)SECURE Magazine readers save 10%!

Register with discount code OS15/INS and save 10% off the main conference pass.
Call MISTI Customer Service today to secure your spot 508-879-7999 ext. 501

WWW.MISTI.COM/INFOSECWORLD



Seven Destiny video game tactics that translate to cyber security

by Corey Nachreiner

Why learn by grinding through dry security best practices when you can make education unique by mixing in a little geeky fun? In this article I share what Destiny – Bungie’s popular new MMOFPS video game – can teach you about network and information security. Learn how to become an Internet Guardian and fight the encroaching cyber Darkness with these seven tips.

1. Different enemies require different tactics – In Destiny, you fight four rival races, each with various classes of enemies. As with any video game, each enemy requires different tactics to take them down quickly. For instance, on Mars you’ll meet the Cabal’s Legionary enemy, who you can actually take head-on; literally running straight at them and shooting them in the head. Meanwhile, tackling the shield-wielding Phalanx requires different tactics. Firing straight into their shields is about as effective as mowing your lawn by hand, one blade of grass at a time. Instead, you must flank these characters or lob grenades behind them. The point is, every enemy in Destiny has their own specific weakness. You’ll only do well in the game by finding those weaknesses and exploiting them.

There are different enemies in information security as well, each with their own tactics and weaknesses. You have “skript kiddies” who hack for the “lulz” and notoriety, hackers who hack for a cause, petty criminals who

hack for small scores, organized cyber criminals who hack for big money, and nation-states who hack for politics and espionage. Each of these threat actors has different motivations, and thus uses different tools and tactics.

As security “Guardians,” we need to know which threat actors affect our organizations the most in order to combat them efficiently. For instance, if you work for a logging company, hackers might target you, so you probably want to be sure you can withstand big DDoS attacks. Understanding the threat actors helps you implement the right defenses for each actor’s particular brand of attack.

2. Use the right tool for the job – Just as Destiny’s enemies require different tactics to be defeated, they are also vulnerable to different weapons. Even if you haven’t played Destiny, you’ve surely seen this with other games (water defeats fire, fire defeats earth, earth defeats water, etc.).

For instance, in Destiny, you'll more easily handle powerful slow enemies (Ogres & Colossus) by sniping them from afar with a long-range rifle. You'll take down fast, weak enemies (Thrall) more quickly with close-range melee attacks. If an enemy has an obvious weak point (the Legionary's small head), precision aiming with the scout rifle works well.

Along the same lines, enemies with blue shields are more susceptible to "Arc" weapons, while orange shields break down quicker from "Solar" weapons, and so forth. In a nutshell, you'll win more Destiny matches by knowing the right tool for each specific job. This is true for your infosec toolsets as well. Do you know the right security tools to defend against various types of attack? A stateful firewall is great for keeping adversaries from directly attacking certain network resources, but it doesn't protect your users from visiting malicious web sites. For those attacks, you need application-layer or next-generation firewalls that scan web sites for exploits and malware, using IPS, gateway antivirus, and reputation services.

Meanwhile, these web security controls might protect your users from drive-by downloads, but what about your public web server? Firewalls (next generation or otherwise) only offer limited web server protections. You need to switch to WAF to provide more specialized web app protection. Furthermore, none of those controls can really protect you from the high bandwidth DDoS attacks being launched today. For those, you need yet another specific tool. As you can see, like Destiny, each attack requires different tools to defeat. You need to master a full arsenal of defensive weapons to combat today's threats.

3. You won't win the war without layered defense – The previous toolset discussion is a great segue for layered defense. In Destiny, as in infosec, there's no single tactic or weapon that always guarantees a win. Crucible's online player-vs-player (PvP) matches are a great example of this. For instance, in one type of Crucible match called "Control," one team of six defends a certain area from another team of six. There are a number of tactics you might employ to control each area. You can have your team camp directly on the control point, taking on any aggressors; you

can monitor all the "ingress" points to the area to catch enemies before they arrive; or you can station long-range snipers to pick off targets from afar.

All these ideas have merit, but would fail if used individually. If your whole team camps on one spot, the enemy can snipe them from afar or lob a grenade into your group. If you only snipe from afar, the enemy might flood your control area at once, making it near impossible to shoot everyone.

So what's the answer? You should use a combination of all these tactics at once. By divvying up the tactics to different team members, you cover all your bases, ensuring you're poised to react to any enemy countermeasure. Military strategists call this defense in depth or layered security, and the strategy works just as well for information security as it does for Destiny's Crucible matches. There is no one tool or tactic in your arsenal that prevents every attack, so you need to implement many at once to defend your network.

4. Fix bugs or they'll get exploited – If you're a Destiny geek like me, you've probably heard of "loot caves." Essentially, there are areas in the game where enemies respawn very quickly after dying, which basically provides you with an infinite stream of enemies to kill.

Since killing enemies is tied to random loot drops, players camp near these loot caves to kill hundreds of enemies in minutes rather than hours. This increases their chance of finding rare loot. This probably isn't what Bungie intended when they made Destiny; rather it's a bug. As with all bugs, opportunistic "hackers" will exploit them for fun and profit, which became apparent in Destiny by the number of players you could find sitting for hours shooting into a cave.

Infosec professionals probably see a clear analogy here to the bugs and exploits found in business software. Hackers can't magically take over your computer without your interaction, unless there is some sort of vulnerability in your software. However, when there are such bugs in critical software, attackers will find them and exploit them to infect our computers or steal data.

The only way to prevent this is to fix the bugs. Bungie recently released a patch that closes the loot cave issue. Though Destiny is just a game, this loot cave incident shows how a small software bug might translate into a large unintended consequence. Hopefully, it reminds you of the importance of applying critical security patches quickly. Case in point: have you installed the Bash updates yet? If not, this might be a good time to do so.

5. You need to grind a bit to win – If you've played any role-playing game or video game with leveling, you're probably familiar with the concept of grinding. There's often a point in the game where the only way to get your character strong enough to take on the next challenge is to grind through repetitive tasks that give the character the experience needed to level up. This is true with Destiny. Later in the game, you get to a point where the only way to level up is to attain rare (legendary and exotic) armor and weapons. There are many avenues to do this, but all of them pretty much entail grinding through tasks you've done before. Go back and replay patrol missions you've done; keep playing multiplayer matches; repeat your strike missions again and again. In short, you just have to keep doing the same work to eventually get the experience to move to the next level.

Many of your daily security tasks probably feel like a grind. Checking your logs and visibility tools every day might get boring over time. Patching your Microsoft stuff the second Tuesday of every month probably starts to wear thin when you realize you'll have to do it again next month. Cleaning up malware infections on a telecommuter's laptop probably gets irritating after the tenth time you've done it—especially when it's for the same telecommuter. However, as repetitive as these types of tasks seem, they make up the core responsibilities of a good first-level infosec engineer. When you are suffering through this grind, just remember that these little tasks are slowly improving the security of your organization, and giving you the experience needed to become an even better security professional.

6. When you lose, dust off and fight again – So let's make this tip simple. If you're like me

and don't have much time for gaming, you'll die in Destiny's player-vs-player (PvP) matches... a lot! When you ultimately fail, you have two choices; get mad at yourself and others and rage quit, or calm down and try again. Only one of those choices makes you a better player.

In infosec, we talk so much about attack prevention that you probably think the best measure of a security professional is a network that never gets breached. Guess what? That network doesn't exist. Things happen, people make mistakes, and one day your organization will get breached. The best measure of a good security professional is how he reacts to the breach or vulnerability when it does happen. If you stay calm and learn from the experience, you'll ultimately learn to become a better infosec guardian. So next time you're hit with a network disaster, dust yourself off, reevaluate your defenses, and fight another day.

7. Security is a constant arms race – When you play Destiny one thing becomes clear very quickly: there is always someone better than you, with stronger gear and weapons. Every time I get that one new gun that suddenly makes me feel über powerful, a new enemy appears that takes four times the firepower. As soon as I start racking up multi-kills in PvP, some new guy logs on and totally smokes me. Destiny, like many video games, is a constant arms race where you must continually improve your skills, tactics, and weapons.

If there is one thing you can definitely learn about infosec from Destiny, it's that security is never static. As new technologies emerge giving us better defenses, attackers evolve and target new vectors with novel techniques. Everyone wants that fictional silver-bullet defense, but it doesn't exist. You need to stay alert during this arms race, and continue to update your tools and tactics to adjust to the latest threats.

Like the Guardians from Destiny, infosec professionals must stay constantly vigilant to protect their networks and organizations from The Darkness threatening our online galaxy.



Review: ESET Smart Security 8

by Berislav Kucan

Well-known IT security company ESET recently announced major updates to its flagship products - NOD 32 Antivirus and ESET Smart Security.

The most typical modern antivirus solutions nowadays provide much more than just anti-malware functionality, but integrated solutions, such as their Smart Security offering, provide a much better level of security against ever-evolving threats.

Aiming to be a complete security solution for desktop PCs and notebooks, ESET Smart Security surely packs a punch, as it contains practically everything home and small office users need to secure their system. Built-in protection mechanisms include: malware scanning, firewall, antispam, antitheft, end-point protection, parental control and a host-based intrusion prevention system.

ESET's scanning engine is fast and robust. Besides the usual "click and don't ask any

questions" scanning option titled Smart Scan, you can also setup a custom scan by selecting detailed targets including local and network partitions, operating memory, boot sector and removable media. Detailed logs are generated for all of these scans.

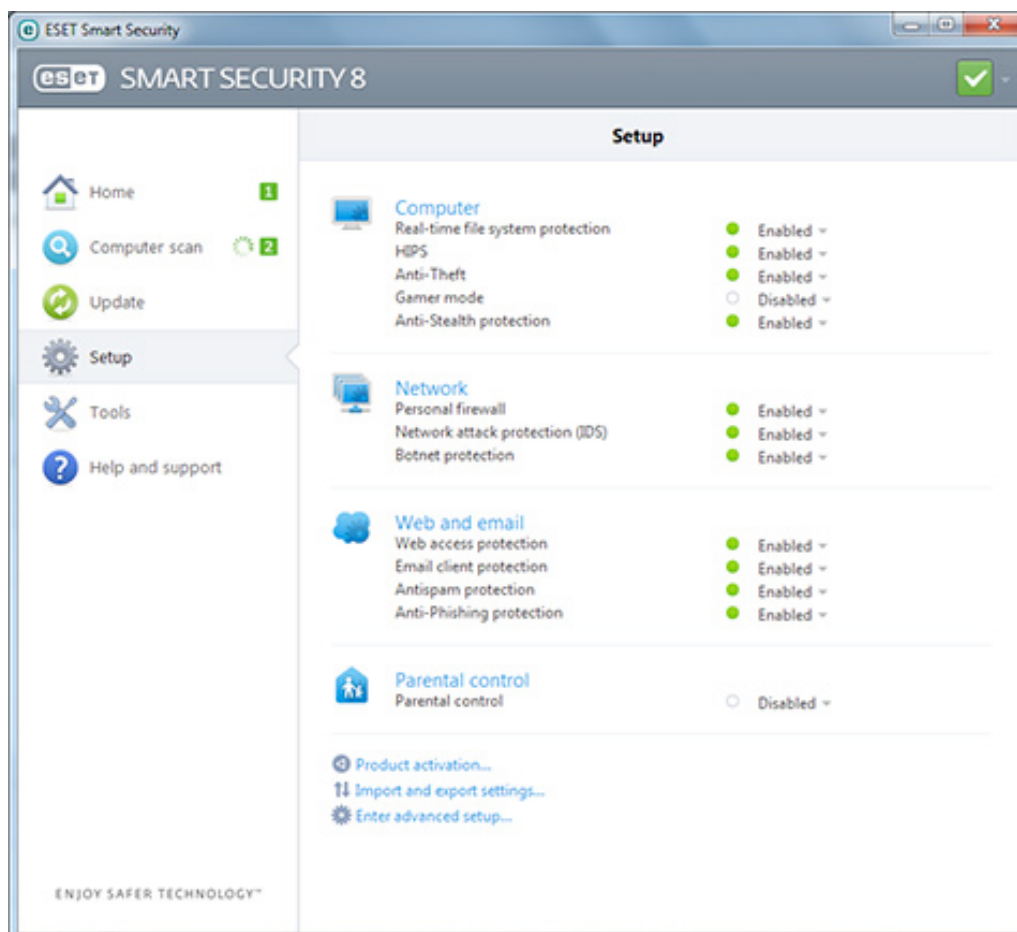
ESET Live Grid module uses the data from the company's global early warning system. Upon installation, you can choose whether you want to participate in this global effort by sending anonymous information of newly discovered potential threats. If you decide to participate, besides helping the Internet be a safer place for fellow ESET users, you will be automatically alerted to breaking news about new types of threats even before your virus definitions get updated.

Images from this device

[Show All](#)[Show Important](#)[Show WebCams](#)[Show Screenshots](#)

Screenshots





With all the stories of lost or stolen notebooks, adding an anti-theft module to this type of a security solution is a good decision. ESET Anti-Theft is a built-in module that works in conjunction with a web application that makes it possible for the user to interact with his or her missing device.

To use this, you'll just need to create your new (free) online account at ESET and your computer will automatically get "paired" with the remote system.

Through a simple and easy to use web interface, you'll first need to setup a dummy account on your computer (can be done from the web app) and from there you'll be able to track the status and the location of your missing

computer. Of course, this all depends on whether the attacker is lazy enough not to format the computer before using it. In the concurrent tests of this service, it proved to be quite good - the legitimate owner can get screenshots, web camera images, GPS coordinates, IP address and a Google Map locating the device.

When you mark the device as missing, the access to all the user accounts except the dummy one will be blocked, effectively protecting your private data. Device monitoring will be started in regular intervals (minimum 10 minutes) and desktop screenshots and camera images from the device will be remotely uploaded and will be made available to you.



Hi! Sorry, this page was blocked.

This site poses a risk to you.
You may have arrived here by mistake – you can go back.
[Show Details](#)

← Go back

In case you've never used your web camera on the missing device, there might be some issues with capturing the person sitting in front of the computer (ecapture.exe constantly tried to open a Windows dialog box asking for further configuration).

There were some slight delays in the communication between the lost computer and the web based "mothership", but everything worked as expected.

The antispam module can be integrated with a number (Microsoft) email clients/services including Microsoft Outlook, Outlook Express, Windows Mail and Windows Live Mail. It provides control of email communications received through POP3 and IMAP protocols.

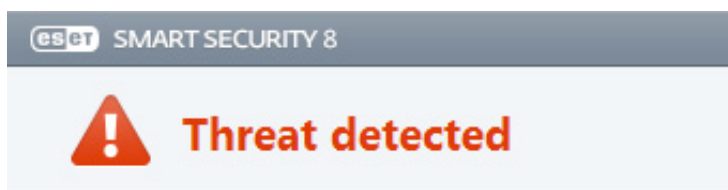
Parental control is turned off by default, but it can be targeted toward a specific user with a list of predefined categories or custom blocked and allowed web pages. With all the problems stemming from injected code in

compromised web sites, it's nice to have the web access protection module. Added by default to your favorite Internet browser, it will automatically block any malware or phishing sites you visit.

The personal firewall inside ESET Smart Security controls all network traffic coming to and from the system.

Based on the specific filtering rules, you can choose one of the four modes:

- Automatic (enabled by default, allows all outbound traffic and blocks all new connections initiated from inside the network)
- Interactive (you tell the firewall what traffic is good or bad)
- Policy-based (uses custom created policy)
- Learning (most insecure mode as nothing is filtered - this should be used just for creating a set of rules that you can later modify to suit your needs).



Access to the web page was blocked. [Show URL](#)

Threat: **HTML/Agent.V trojan**

One of the new additions to version 8 of ESET Smart Security is botnet protection. By analyzing network communication protocols and combining this data with ThreatSense technology detection methods, as well as ESET Live Grid feeds, the software will prevent your system from becoming part of a botnet.

With its powerful set of features and the possibility of customizing everything into details, ESET Smart Security version 8 is a tough de-

fense mechanism against a variety of different threat vectors.

ESET Smart Security version 8 runs on the following Microsoft Windows operating systems: 8.1, 8, 7, Vista, XP, Home Server 2003 and Home Server 2011.

Pricing is different depending on the country where you live in. It is also made available by online retailers like Amazon.

Berislav Kucan is the Director of Operations for (IN)SECURE Magazine and Help Net Security (www.net-security.org).



Events around the world

InfoSec World Conference & Expo 2015

www.misti.com/infosecworld

Disney's Contemporary Resort, Orlando, USA / 20 March - 25 March 2015

InfoSec World 2015 will have a lineup of conference sessions, workshops and summits that address the most pressing matters in information security today. With a selection of top-rated speakers, you'll find content that is compelling, actionable and applicable to the current challenges you face at your job.

INTERPOL World 2015

www.interpol-world.com

Sands Expo & Convention Centre, Singapore / 14 April - 16 April 2015

INTERPOL World is a new biennial international security trade event which will bring police and other law enforcement agencies together with security solution providers and security professionals from around the world to identify future challenges and propose and build innovative solutions.

RSA Conference USA 2015

www.rsaconference.com

Moscone Center, San Francisco, USA / 20 April - 24 April 2015

RSA Conferences are the pulse point of the security industry where leading practitioners connect to protect. Here you'll meet with top industry leaders and fellow security specialists to discover how the latest advances in technology can help you meet those challenges.

THE CYNJA[®]

**TROJANS, WORMS & ZOMBIES
ALL CONTROLLED BY THE EVIL BOTMASTER.
A NEW GENERATION OF NINJAS IS WIELDING
HEX GRENADES & OPTIC PULSE SWORDS.**

WHO WILL WIN?

**A COMIC BOOK SERIES INTRODUCING KIDS TO
THE AWESOME WORLD OF CYBERSECURITY!**



WWW.THECYNJA.COM



Maltego transforms for pcap analysis

by Adam Maxwell

I have a confession to make. I'm a Packet Addict - I've spent the last two years slicing apart network packet files for fun.

Pulling apart the raw network traffic that flows around our digitally connected world is a great way to learn how things work, and how to break them. Like many other people's, my tool of choice was initially Wireshark (www.wireshark.org), but then I learned that I could pull the pcap files apart by using two of my other favorite things: Python and Scapy (www.secdev.org/projects/scapy/).

After a while, regardless of how you analyze pcap files, you will eventually reach a point where you get "packet blind". Whether you sift through them by looking at the code or via Wireshark, you will at some point get "lost in the packets," especially if you are looking for indications of malicious events within legitimate network traffic.

Towards the end of 2012, the Cyber Security Challenge (cybersecuritychallenge.org.uk) released a cipher-related challenge. The goal was to find the artifacts within a single pcap file containing 34,695 packets. This challenge

involved finding the relevant conversations and then carving artifacts out of the pcap file.

Around the same time I had started using the Canari Framework (www.canariproject.com) and decided to write a set of Maltego transforms to analyze pcap files. I hoped that it would allow me to visualize the packets easier than just using Wireshark or looking through snippets of code, while also allowing me to still follow the "flow" of the packets.

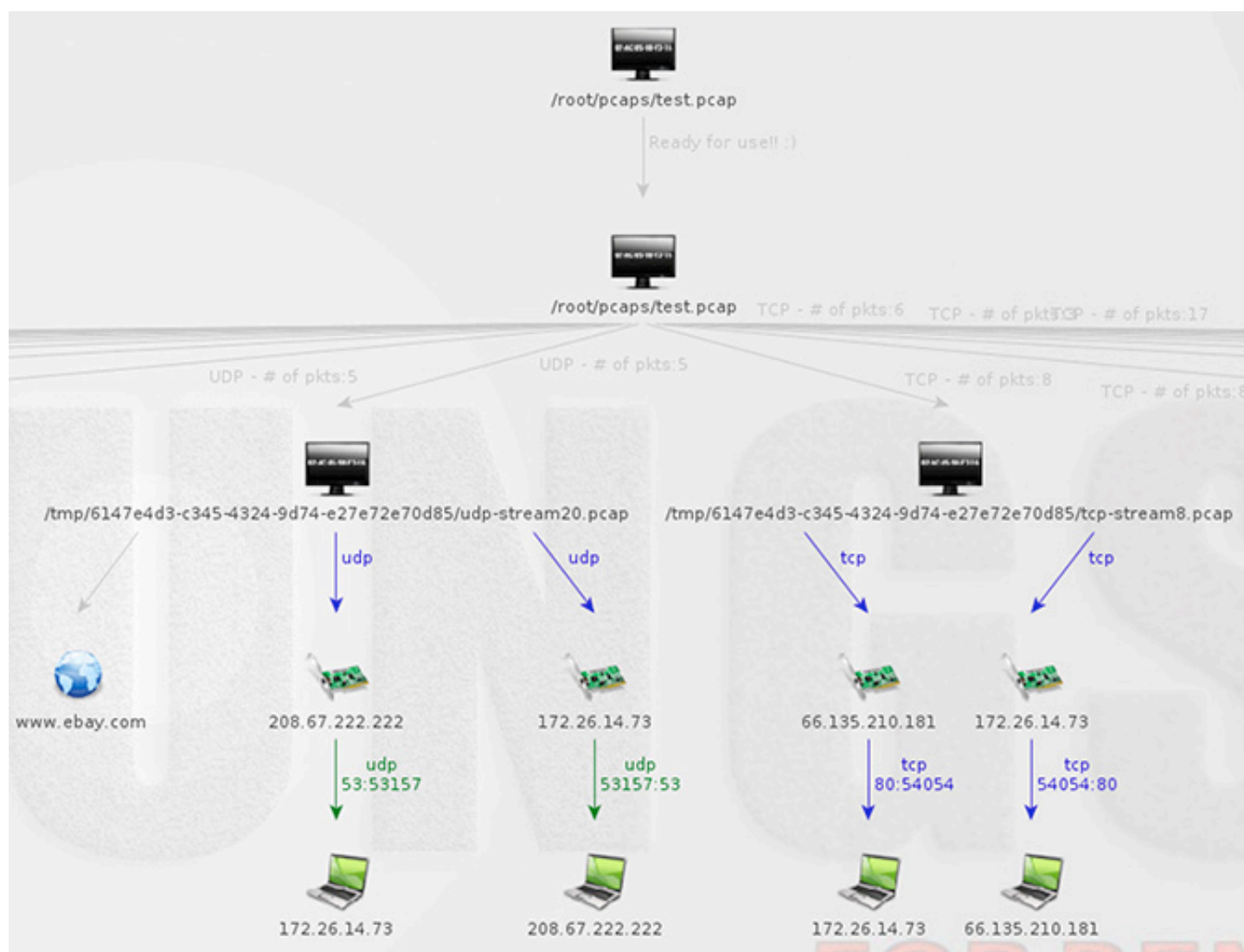
In April 2013 the first beta release of sniffMy-Packets (SmP) was released. Initially the functionality was limited, and I rewrote most of that beta over the coming year to improve it and improve its integration into Maltego (to make use of the existing transforms). 90 percent of the heavy lifting in the background is Scapy-based, while the remaining 10 percent of functionality was achieved with tools like TShark (part of Wireshark), Snort (www.snort.org) and p0f (en.wikipedia.org/wiki/P0f).

The current version of sniffMyPackets consists of 65 Maltego transforms and can, among other things:

- Extract files from pcap
- Send them to Snort for analysis
- Perform geo IP lookup
- Extract TCP and UDP streams
- Do simple packet search
- Perform packet capture (with optional BPF filter).
- Perform MD5 and SHA1 hashing of pcap files
- Find DNS requests
- Export to pcap file
- Extract email addresses from pcap.

sniffMyPackets works like this: you add a pcap file into Maltego, then run a “Prepare pcap for use” transform that ensures the pcap file is in the correct format. It creates a folder to store artifacts and extracted pcap files in, and then hashes the original pcap file for your records (all this information available in the Maltego entity properties).

From here on the choice is yours: you can work on the base pcap file or, as I tend to do, break each base pcap file into its separate TCP and UDP streams as it's easier to handle small chunks at a time. This method also gives you a good idea of who is talking to whom. Below is a screenshot of a basic pcap analysis.



If you judge by the screenshot, your initial impression might be that it's a bit messy, but if you look at the information shown, you will see the value that sniffMyPackets can bring to pcap analysis. The pcap file (/root/pcaps/test.pcap) is first split into individual TCP and UDP streams, each stored in a

separate pcap file, all of which are then stored in a generated folder.

From here you can pull out the IP addresses (as IPv4 Maltego entities), then you can extract the port information and the destination IP address.

Depending on the size of the pcap file, you can quickly – often in less than 5 minutes - see the conversations between IP addresses, the protocol (TCP or UDP) and the ports involved. This will allow you to focus on an IP address or IP addresses that you may have an interest in. From here (as shown in the screenshot) you can pull out such information as DNS requests, look for email addresses, or search for HTTP content.

One of the other “cool” features of sniffMyPackets is the ability to extract files from a pcap file. This will allow you to see any potential malicious files transmitted in it.

The Linux command “file” is run against each file that is extracted, in order to try and determine its content. In the screenshot above you can see that a lot of them have been flagged as HTML content. Each file is hashed (via SHA1) and the file extensions are removed to stop you clicking on things when you shouldn’t.

The current version of sniffMyPackets is now over a year old and the new version (2.0) is in development. I’m planning on adding a lot more functionality to the next release and will be refactoring a lot of the existing code to cut down on the number of Python libraries required (plus, I’ve got better at writing in Py-

thon). In terms of new features and functionality, the next version will include the following two major enhancements:

Database support - Either locally or remotely installed to allow central storage of pcap files. By using the Gobbler library, which I also created, I can extract all the layers out of a packet and store them in a variety of database types.

Web interface - Analysing pcap files can be a team sport, but the nature of the transforms in sniffMyPackets means that the transforms are installed locally on each user’s machine. The web interface, which will tie into the database, will allow you to share with others key information extracted from the pcap files.

I want to make using sniffMyPackets a more collaborative process. One analyst can upload a pcap file either into Maltego or directly into the database and then another analyst can view this in a web browser or pull the information back into Maltego on a totally different machine (or country).

If you want to learn more about sniffMyPackets, visit sniffmypackets.net. It has a link to the GitHub repository as well as some Youtube videos that will show you more of the features available.

Adam Maxwell (www.itgeekchronicles.co.uk) is addicted to Python, pcap and Maltego. He builds infrastructure by day and writes code by night.





All your info are belong to us: The biggest phishing scams of 2014 by Jovi Umawing

We're close to welcoming 2015 and saying our goodbyes to 2014, but most of us can already conclude that majority (if not all) of the high-alert, noteworthy security issues we have faced this year involve a phishing campaign.

This article presents an overview of the top phishing scams of 2014, and as we look back, we also look ahead in expectation that although the events we're about to recall may not be the first time we've encountered them, this will certainly not be the last time we'll be talking about them.

Scammers take advantage of popular leaking incident to steal credentials

In the wake of Celebgate, the leaking of intimate celebrity pictures and videos that were supposedly retrieved via phishing and brute-force guessing of passwords to specific iCloud accounts, Apple began sending emails to clients when their iCloud accounts were accessed over the Web. It didn't take long for scammers to take advantage of this to trick users into giving away their Apple account credentials. A spam campaign with the subject "Your Apple ID was used to sign in to iCloud on an iPhone 5S" was found in the wild in late August, asking users to confirm their details

and update their passwords if they weren't the ones who did that.

Anyone with one or more Apple devices, regardless of whether they have their iCloud accounts enabled or not, was targeted with this campaign.

The hackers apparently plan on releasing their huge stash publicly one batch at a time.

Other backed up data like SMS messages, address books, calendars, notes and GPS coordinates are also believed to have been accessed and stolen.

A Dropbox phish that quickly drops dead

And this all thanks to said cloud company's swift response to reports of a convincing phish found to be hosted somewhere in its own backyard, on dl.dropboxusercontent.com, a legitimate and official domain used to host shared photos and files for its 200 million users.

The email claimed that the recipient needs to view an important file that is unfortunately too big to be attached, so they are sent a link to it instead.

The objective of the phish was not only to let users willingly hand over their credentials for Dropbox but also for their Web-based email providers, as it indicated that they can access the said file only by entering their email credentials as well.

The phishers have refrained from using compromised domains with “Dropbox” in the URL, but they definitely counted on spam recipients trusting the legitimacy of the page. What the victims didn’t realize until the last minute is that although the domain is trustworthy and uses a secure communication protocol, it’s not the right place to enter user credentials.

Phishers home in on Luis Suárez supporters

The controversial biting incident between Luis Suárez and Giorgio Chiellini during the Uruguay vs. Italy World Cup match did not only get the attention of the former heavyweight boxer Mike Tyson but of scammers as well.

In this FIFA 2014-themed phishing campaign, phishers have been inspired to create a petition in support of Suárez. The fake page, which was made to look like the official FIFA World Cup website, asked for sensitive information like email address and mobile number as part of the petition signing. Petitioners were then encouraged to share the link to the fake petition page with their friends via a handy Facebook widget. Reports say that the phishing link spread widely in a matter of days.

Google account owners preyed on by Docs and Drive phishers

A Google Docs and Drive-themed phishing campaign that was spotted in March this year appears to share a number of similarities with the Dropbox campaign we mentioned earlier. The criminals behind both housed their phish pages in legitimate servers of Dropbox and Google, and both heavily relied on users’ trust of the domains. In this case, the scammers used googledrive.com.

In a similar campaign that we found some time in April, the phishers were not only asking for Google account credentials but also credentials from other Web-based email services like Yahoo!, Windows Live, and AOL. In addition, users were prompted with a fake notice to update their browser plug-in. The served update was, of course, malware.

Google credentials are prized data. Anyone who has them can access other Google applications online, like YouTube and Gmail, and this access can be misused by miscreants for their malicious purposes (mostly spamming and new phishing campaigns).

Fortune 500 bank clients chased by smash-and-grab fraudsters

In August, JPMorgan Chase (JPMC) clients were targeted with a legitimate-looking spear phishing, smash-and-grab campaign in the form of a spoofed email with the subject “Daily Report – August 19, 2014.” It contained an HTML attachment, message_zdm.html, that supposedly held the actual message from JPMC. The attachment was actually the phishing page, which phoned back to a server in Russia to get the RIG exploit kit. Systems found to have weaknesses in IE, Adobe Flash, Silverlight, and Java were then infected with the Dyre banking Trojan.

The criminals behind this scheme have actually made an effort to cover all their bases: whether the victims filled in their details or not, they got infected. This is an example of a multi-pronged attack.

This JPMC phishing attack was likely a part of a bigger campaign that targeted other clients of organizations like Companies House and ADP.

Fake Netflix page + fake Microsoft Tech Support = One dangerous phish

We have seen a number of Netflix-themed phishing attacks this year, but this is perhaps the most sophisticated and unique. This campaign may have started off via two mediums: a spam email, which is typical, and a pop-up window, which isn’t. Clicking the link from either lead to a fake site Netflix site.

Submitting login credentials into the site lead to an error page informing users that their account has been suspended and offering up a Member's Service telephone number, which eventually lead to a bogus Microsoft Technical Support scam.

The fake MS certified technician, based in India, then advised users to download a file called "NetFlix Support Software," which is actually TeamViewer, a well-known remote login program. He/She then used it to look for and upload files of interest from the victim's machine to theirs. It is assumed that the scammers will use the retrieved information for future scam attempts.

Phishing for love and money

A massive spear phishing attack was mounted in mid-2014 against clients of popular online dating sites, most notably Chemistry.com, Christian Mingle, eHarmony, Lavalife, Match.com, Plenty of Fish (PoF), SeniorPeopleMeet, and Zoosk. The attack used a phishing kit with hundreds of PHP scripts designed to steal data.

Dating sites normally require payment upon signing up to make full use of the dating service. Gaining access to accounts of legitimate users does not only let the actual scammers get away with not paying, but also to seamlessly impersonate the user and carry out dating fraud against those who are honestly looking to build a relationship with someone.

Phishing involving dating sites—a two billion dollar industry and growing—is not new; however, it presents another option for fraudsters to target and cash in on millions of potential targets.

Protect your information: Choose not to be a victim of phishing

Phishing is a pervasive threat. People continue to fall for it, despite warnings and advances in tools blocking spam and URLs, because at its core, phishing is really about exploiting the human. Computing devices are just some of the other tools scammers use to extract information from their targets. We can

never stress enough the importance of vigilance and the need to continuously catch up with the latest scamming tactics. Protecting your info—effectively, yourself—should be part of everyone's online lifestyle. Here are some tips to start you off:

1. Never click links in message bodies or open attachments from emails purporting to originate from legitimate brands. This not only dramatically lowers the risk of phishing, but also saves you from other online threats such as malware.

2. Familiarize yourself with the login domains you use on a daily basis. With regard to the phishing campaigns targeting Dropbox and Google Docs/Drive users, it pays to know specific URLs where you normally submit your credentials. The login URL for Dropbox is dropbox.com, while the login URL for Google accounts is accounts.google.com. Doing so will allow you to spot bogus pages.

3. Be wary of links shared on social sites. Phishing links, such as the fake FIFA petition referenced above, has been shared in Facebook, forums, and other public domains where users can easily create accounts and post immediately. Unfortunately, the same convenience these sites offer to their user base is also offered to scammers and phishers. It's best to treat posted URLs with healthy suspicion.

4. Refuse to provide personal information over the phone unless you're absolutely sure that the person on the other line is who they claim to be. Scammers are not limited to just sending out spam emails and making fake Web pages. They can use the phone to contact their targets or get in touch with someone who is close to their targets to get information about him/her. Indeed, phishing is as much a danger offline as it is online.

5. Make it a habit to check your online bank accounts every now and then for possible fraudulent or questionable transactions. This way, you can quickly flag any anomalies so banks can address them.

Why fraudsters love the sharing economy this holiday season

by Andreas Baumhof



From peer-to-peer rentals like Airbnb to transportation resources like Lyft and Uber to online marketplaces like Etsy and eBay, the sharing economy has gained traction in the US and around the world. Designed to facilitate connections between consumers and individual providers, this business model makes it possible for anyone to share their skills, products or services with others—for a price.

The sharing economy appeals to consumers because it offers convenience and cost savings. However, consumers aren't the only ones who are benefiting from the sharing economy. Fraudsters are also cashing in on this new way of doing business and unfortunately, many companies in the sharing economy simply aren't prepared to handle the wave of fraud that is set to be unleashed this holiday season.

The global sharing economy

In the sharing economy, the “anytime, anywhere” nature of mobile and social technologies makes it easy and cost effective for consumers to connect with individual providers for products and services, regardless of their geographic location.

Although there is a sense of collaboration between providers and consumers, the sharing economy is big business—and it's getting big-

ger by the day. The global peer-to-peer rental market alone is estimated to be worth more than \$26 billion, and market leaders in the sharing economy enjoy valuations of \$10 billion or more.

- **Peer-to-peer home rental:** Launched in 2008, Airbnb allows individuals to rent their homes or rooms in their homes for short periods of time. To date, the company has facilitated more than 15 million guest stays in over 190 countries.
- **Transportation:** When it comes to auto travel, market leaders include Uber and Lyft—ride-sharing services that use technology to connect passengers with drivers of vehicles for hire. Founded in 2009, Uber is the larger of the two companies. The company is valued at more than \$15 billion and its services are available in 45 countries and more than 100 cities around the globe.

- E-commerce: Etsy and eBay dominate the sharing economy, providing opportunities for individuals to sell merchandise and handmade goods directly to consumers across the globe. Consumers are choosing to purchase “one-of-a-kind” goods via online e-commerce marketplaces more frequently than ever before, and are likely to opt to do so this holiday season.

Ironically, many of the technologies that have made the sharing economy possible also make it a prime target for cyber fraud. Online purchasing, the use of mobile devices and other behaviors increase cybersecurity risks for both businesses and consumers.

Holiday cyber threats for sharing economy businesses

The holidays are a busy time of year in the sharing economy. In addition to holiday retail opportunities on eBay, Etsy and other e-commerce sites, consumers’ holiday travel plans may include peer-to-peer home rentals. Local ridesharing also increases during the holidays due to parties and seasonal events, as well as a cost-friendly mode of transportation to and from airports.

Heading into the 2014 holiday season, fraudsters are increasingly targeting sharing economy businesses. Why? Because the volume of transactions in the sharing economy is significant and most transactions are completed online—not in person. Additionally, many businesses in the sharing economy aren’t adequately prepared to address cybersecurity threats, making them easy targets for fraud.

Some of the most serious cybersecurity threats that sharing economy firms can expect to face this holiday season include:

Payment fraud – All online purchases, including purchases in the sharing economy, are targets for payment fraud. Cybercriminals are becoming increasingly sophisticated in their ability to exploit Card Not Present (CNP) purchases, electronic payment processes (e.g. EFT, electronic wallets) and other online transactions.

Following the holiday season, as US retailers and banks move closer to the looming Octo-

ber 2015 deadline for making the switch to Europay-MasterCard-Visa chip and signature credit card technology to make in-store purchases more secure, cybercriminals will move their efforts to target online payments systems even more aggressively.

As many businesses in the sharing economy employ the use of online payments systems, they must be prepared to be targeted by fraudsters more frequently.

Fraudulent account registrations – During the holidays, sharing economy businesses need to be diligent about identifying fraudsters who use spoofed identities to test stolen credit cards. Red flags include users hiding behind proxies or disguising their true location, a single device creating many different accounts, and attempted registrations from known malicious devices.

Following high profile data breaches such as those that hit Target and Home Depot, as well as recent news about a Russian cyber crime ring gaining access to 1.2 billion usernames and password combinations, sharing economy businesses must make security a priority to assure stolen credentials from these breaches are not fraudulently used during the busy holiday season.

Account takeovers – Another way that criminals exploit businesses and consumers in the sharing economy is through account takeovers. In these types of attacks, criminals obtain user credentials through data breaches, phishing attacks, bad devices, malicious personas, shared passwords, keyword loggers or other strategies.

Cybercriminals ramp up their efforts with sophisticated variants of advanced malware, allowing them to seamlessly intercept customer data online – a huge problem for sharing economy businesses with online and mobile payments systems.

Although these threats are year-round concerns for sharing economy consumers and businesses, the risk of cyber crime increases during the holidays due to higher transaction volumes and increased opportunities for fraud.

Like brands in the traditional economy, brands across the sharing economy are vulnerable to the effects of cyber crime—a single security breach can negatively impact the brand's reputation with consumers.

To mitigate risk, sharing economy executives need to proactively implement solutions and strategies to prevent cyber fraud before it occurs.

Key holiday security strategies for businesses across the sharing economy include:

1. Frictionless context-based authentication

Sharing economy security strategies have to be transparent to users, allowing consumers to enjoy truly seamless transactions and purchase experiences. Many users choose sharing economy businesses based merely on their simplistic interfaces and experience, so those businesses cannot afford to make the process more difficult for the end user.

Frictionless context-based authentication protects against online fraud by establishing trust with account logins via multiple, contextual factors including device usage, geolocation and customer behavior. The result is a more robust transaction environment that doesn't require brands to sacrifice the customer experience for security.

2. Shared global intelligence network

Cybercriminals are sophisticated, well funded and able to launch advanced online attacks from anywhere in the world. A shared global intelligence network combines device identification, threat assessments, identity and be-

havioral intelligence to create holistic online personas. By analyzing access requests, logins and payments against these personas, businesses in the sharing economy can evaluate data related to users and their associated devices across all channels.

Through a shared network, businesses can securely share information about devices and personas connecting to their sites, without sharing any personally identifiable information about customers or visitors with competitors. In essence, shared global intelligence gives organizations effective, real-time risk assessments leveraging information from a global user base.

3. Enhanced mobile identification

Mobile security plays an important role in the sharing economy, since transactions for transportation, e-commerce and even peer-to-peer rentals are often performed on mobile devices.

Cybercriminals typically jailbreak mobile devices to gain full access to the original owners' personal information and complete transactions through their accounts. Enhanced mobile identification technology can detect jailbroken devices, provide location-based authentication and identify transactions originating from devices with compromised security.

It's important to understand that no single security strategy can successfully protect sharing economy businesses from today's cyber threats. However, by targeting a combination of strategies, businesses can begin to implement solutions that significantly improve security and create a safer environment both for consumers and providers.

Andreas Baumhof is CTO of ThreatMetrix (www.threatmetrix.com) and is an expert on cybersecurity with experience in the encryption, PKI, malware and phishing markets. Prior to ThreatMetrix, Baumhof was co-founder of TrustDefender, a provider of security and fraud detection technologies, and Microdasys, a provider of deep-content security solutions. He developed the first SSL proxy with patents pending in Europe and the U.S.

SECURITY NEWS & INDUSTRY INSIGHT. WWW.NET-SECURITY.ORG

SECURITY AWARENESS FOR THE 21st CENTURY

- Go beyond compliance and focus on changing behaviors.

- Create your own program by choosing from 30 different training modules.

- Meets requirements of the Data Protection Act and PCI DSS.

- Training is mapped against the 20 Critical Control framework.

- For more information visit us at www.securingthehuman.eu



www.securingthehuman.eu