October 2015

CYREN

CYBERTHREAT Report

CYBER AWARENESS

An in-depth look at the level of industry awareness in the areas of threats, trends, and technology

CYBER SECURITY AWARENESS

Lior Kohavi
Chief Technical Officer, CYREN, Inc.

At the time of writing this introduction, we're recognizing Cybersecurity Awareness Month (October). Out of curiosity, I looked online to see what sort of information was available on the topic. I wasn't surprised by the results; there were thousands of links, including newspaper articles, infographics, and general awareness notices, with sources that included the U.S. Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), major news publications, expert blogs, and notices from scientific and educational institutions. The overwhelming majority of these links contained meaningful, useful, and valuable recommendations for both businesses and individuals on how to avoid becoming victims of cyberattacks.

With so much quality information readily available, why then are so many companies, large and small, still regularly caught in the agonizing maelstrom of a cyber breach? The answer is straightforward; businesses aren't keeping up in terms of understanding the threats that they face, or investing in the technology necessary to mitigate those threats, as we learned from our recent study, conducted jointly with Network World in July and August of 2015.

In this study (more on p. 4), we sought to understand the challenges associated with delivering web security, as well as to gauge receptivity to cloud-based web security solutions. Most participants worked for companies ranging in size from 1,000 to 5,000 employees and held functional-level, non-CIO or -CTO titles. The responses weren't entirely surprising; while the vast majority of respondents considered their firms to be mid- to high-level risk targets, many indicated that they lacked resources to implement new security solutions, had difficulty assessing their organizations' level of risk, or had no clear or uniform strategy for incidents. And, almost half said the increasing proliferation of mobile devices (laptops, tablets, and smartphones) created complexity and difficulty in managing web security.

This lack of understanding and investment was displayed again recently, as we learned that over 15 million T-Mobile customers lost social security numbers, birthdates, and home addresses in an attack on the servers of the credit-reporting agency Experian. The stolen information is already for sale on the dark web. Worst still, security bloggers are hinting that employees and contractors had voiced their fears to leadership on the possibility of an attack, yet their concerns were ignored.

When reading about the lack of understanding among security professionals or the latest major corporate cyber breach, it is easy to become jaded on the topic of cyber security awareness. We tend to ask ourselves, "How is it possible, with the information and technology currently available, that many businesses still lag behind when it comes to upgrading and investing in trustworthy cyber security solutions?"

It is for just this reason that more than ever businesses and cyber security professionals need to embrace awareness. They need to arm themselves with the facts about the available technology and the true costs and implications of a cyber breach. Business leadership needs to listen to all levels of security staff, from management to engineers and analysts. And most importantly, cyber security professionals need to realize that cyber security technology is changing rapidly. Deciding to take a "wait and see" approach to a new cyber security solution likely means that you will experience a significant breach sooner rather than later.

With the ability to analyze 17 billion internet transactions daily from more than 600 million users in almost 200 countries, (more than any other cyber security organization), CYREN is committed to empowering the cyber security community with awareness and the best, most technically advanced solutions available today.

Perceptions of

Web Security in the Modern Workplace

Multiple devices creating numerous "entry points" is the greatest challenge to web security.

In a Network World/CYREN study, IT professionals confess that they're arming themselves with **10- to 15-year old technology** to prevent and detect cyberattacks. CYREN wanted to know more.

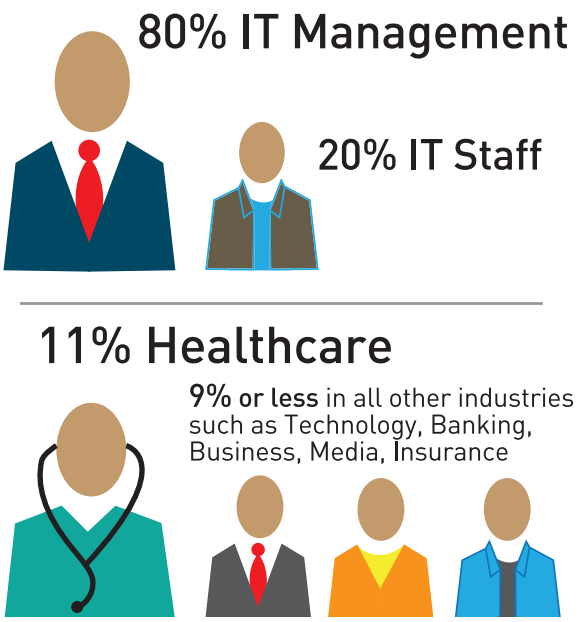
In July and August of 2015, CYREN teamed with computing publication, Network World to conduct the first ever study into the challenges associated with web security, including delivery, awareness, perceptions, and receptivity.

The results are somewhat surprising with IT experts readily admitting that they continue to rely on 10- to 15-year old appliance-centric security technologies and strategies in an attempt to maintain an effective level of protection for their companies. They also confess that they're struggling to prevent and detect attacks. These security professionals admit that they know that the risk of malware infection is high and that their own efforts to control threats and breaches are falling short, yet one-third of the respondents also acknowledge that they haven't adopted modern advanced cloud-based security technology to help protect sensitive information and had no plans to do so.

Network World and CYREN initiated the study with an email to Network World readers inviting them to contribute their opinions and experiences; included in the email was a link to the online survey. IDG Research Services developed the survey questions in conjunction with CYREN and Network World. Final study participants were identified based on organization size (no less than 500 employees and no more than 9,999); job title (IT titles only, with CIO and CTO titles excluded to better focus on the "implementer" role); and level of involvement in web security (must implement and/or maintain web security solutions)

Top Challenges to Web Security

Study Respondents



Respondents generally came from diverse industries, with the largest percentage (11%) coming from the health care industry, and other large segments coming from technology, financial, business/professional services, entertainment/media, and insurance. Notably, almost three-quarters of the respondents worked in the private sector; only a quarter worked in government or for a non-profit. Organization size also varied, with the most (38%) working for companies that ranged in size from 1,000 to 2,499; although slightly more than 20% of the respondents worked for relatively small organizations with only 500 to 999 employees. The vast majority (80%) identified themselves as working in IT management; the remaining 20% identified as technical staff.

While only a quarter of the respondents actually approved or authorized security purchases, the vast majority self-identified as significant contributors to security decisions, including determining requirements and the need for solutions, evaluating solutions, and recommending/selecting vendors.

In analyzing the data, we learned that security professionals recognize that technology has changed dramatically in the last decade. Respondents believe that these fast-paced technological changes have created a number of challenges that make implementing cloud security difficult, including multiple system entry points—in the form of smart phones, tablets, and laptops—along with a lack of continuous visibility to detect advanced attacks. In addition, almost half of the respondents indicated that even if they wanted to implement new security, they lacked the resources to do so. Other high response rates on the topic of web security challenges included "Difficulty in assessing the level of risk/threat profile" (39%); "No clear or uniform strategy for incident response (response is ad-hoc/reactive) (39%); and the belief that "Existing blocking and prevention solutions are insufficient to protect against advance attackers" (38%).

Interestingly, while a full **75 percent of the respondents readily admitted that their firms were likely mid- to high-level risk targets for cyber attacks, only an average of 39 percent of this same group said their current cybersecurity solutions were "extremely" to "very effective"**; in fact, the remaining 61 percent categorized their security solutions as only "somewhat" to "not at all" effective.

The level of current or anticipated cloud security use was relatively high among respondents, with 67 percent saying they already use, or would consider using, a cloud-based solution for web security. However, almost one-third indicated that they did not use and had no plans to use web security. Among these respondents, 61 percent stated that "lack of trust in cloud-based security" was the top obstacle to implementing an advanced cloud-based security solution. Yet only 39 percent of this same group said their current solution was providing the protection they needed.

All Protection Isn't Created Equal: Cloud-based Security IS Faster and Better

The results of the survey provide solid evidence that cloud-based security really does provide an advantage over traditional appliance-centric security technologies and strategies. Respondents who indicate that their organization is currently using a cloud-based web security solution are significantly more likely to assign high effectiveness ratings in the area of protection speed. This response illustrates that the speed at which threats are identified is critical and that this "time advantage" is essential for effective protection in today's battleground of new and emerging threats. This requirement is often referred to as "zero-hour protection," and real-time cloud-based security enjoys a massive advantage in this area because it can defend against new malware, viruses, and other types of malicious code during the first minutes and hours after these threats are released. Signature-based solutions are virtually powerless against such zero-hour threats, since it can take days or even weeks for updates to take place. By contrast, cloud-based solutions are updated instantaneously, the moment that a new threat is identified, providing almost immediate protection.

Conclusions

In response to this study, it is relatively simple (and true) to conclude that IT professionals using advanced cloud solutions enjoy better security. Clearly these individuals already understand that guarding sensitive data in an era of mobile phones, tablets, and cloud services means using a solution that is designed to provide zero-hour, always-available protection in the cloud in a model that follows the user and the devices they use. The bigger and more profound conclusion comes with the realization that fully one-third of the respondents don't trust advanced cybersecurity technology, yet also rate their current legacy solutions as ineffective. These individuals readily admit that they're stitching together an assortment of 10- to 15-year old security point products in an attempt to protect their company and clients from today's sophisticated cybercrime. And, it is fairly safe to assume that if these companies haven't already become victims of a cyberbreach, they soon will be. Convincing these IT professionals to switch their security approach from securing fixed computing assets to protecting users on whatever device they use, is clearly the immediate "awareness" challenge.

Trust in the Cloud

In the recent Network World/CYREN Web Security study, almost one-third (32%) of the respondents indicated that they were not using a cloud-based solution to provide cybersecurity. Of these, the vast majority (more than 60%) said the reason was lack of "trust in cloud-based security solutions."

The benefits of the cloud-based security models are well known and include always having up-to-the-moment security intelligence, reduced cost of ownership, flexibility of deployment model, device independence, scalability, rapid deployment, and little or no capital investment. These benefits notwithstanding, cloud security is the best way to protect companies from threats and breaches due to the increased numbers of employees using their own devices that may not have corporate security software installed, or using corporate devices from unsecure locations, such as home networks, airports, and coffee shops.

"Employees logging into corporate systems using their personal smart phones or tablets, are putting corporations at significantly increased risk of a data breach," says CYREN Vice President, Amit Monovich.

"If a company has 5,000 employees, then they have 10,000 – 15,000 different potential Internet access points for a cybercriminal, since each employee likely uses a laptop, smart phone, or tablet. Multiple those numbers even further if the employee is logging in from locations outside the corporate security perimeter. You can have all the security you want on your own servers, but if your employees are accessing your systems from unsecured networks, such as their home, the airport, or coffee shops, then your perimeter-based security will fail. On the other hand, if your users log into your network from a remote location and they're required to funnel their activities through a cloud-based security service such as CYREN WebSecurity, then the risk of the employee downloading and installing malware on a corporate system diminishes."

In addition, cloud-based security operates in near-real time, so companies can quickly define and apply continuous, consistent, and accurate web-use policy, regardless of the end-user device type and location. Corporations can also use cloud-based security to gain detailed visibility into web use across all types of devices, and they can simplify their network infrastructure by allowing remote users to connect directly to the Internet through a highly secure global platform, reducing the need to backhaul traffic through multiple security appliances.

CLOUD SECURITY - THE MATH

5000 Employees

x

2 or 3 Devices
(smart phones,laptops, tablets)

=

10,000 to 15,000 Internet access points

x

Multiple Locations
(Coffee Shops, Airports, Hotels, Home)

=

Increased Chance of significant threat or breach

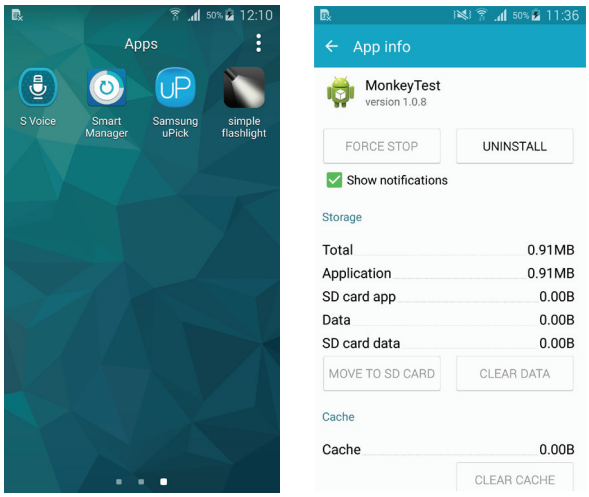
Hidden Malware and the Ghosts of Mobile Technology

Halloween ghosts and ghouls are out in full force in 3rd quarter malware.

Android Malware: Ghost Push

Already discovered packaged into 39 different Android apps, "Ghost Push" (sometimes also called "Rootnik") malware turns an infected device into a platform for the installation of adware, unwanted homescreen links, and further malware. Victims have found the malware to be deeply entrenched and difficult to remove.

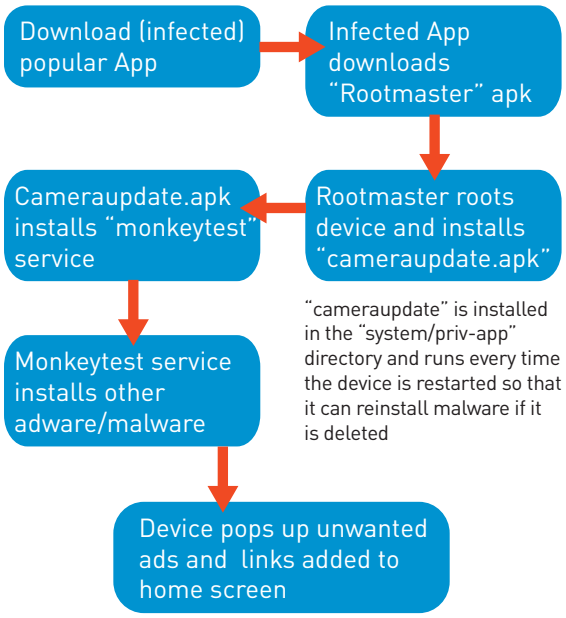
The malicious code is initially installed when the Android user downloads an infected version of popular application, such as a flashlight app or a popular game from a 3rd party app store.



GhostPush app image upon launch and MonkeyTest malware service

While the infected app is functional, it also gathers information about the host device and sends it to a command and control (C&C) server. The server then replies by sending an Android Application Package (.apk) file tailored to root the specific device type. After rooting the device, the malware replaces and modifies system files and installs a malicious service called cameraupdate.apk into the root system folder ("system/priv-app"). Installation files present in the "priv-app" directory are run every time the device starts. In this way, the malware can reinstall itself if removed, ultimately making it very hard to uninstall.

Cameraupdate.apk then installs a service called "MonkeyTest" (other names, such as TimeService, might also be used). MonkeyTest is able to install unknown applications (primarily adware-related) without the user's knowledge, turn off WIFI, and use the mobile data to download other malicious applications, potentially costing the victim excessive amounts in data charges. The malware also drains the battery and slows the device. MonkeyTest gathers device information, such as the International Mobile Station Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI), and app packages installed.



Based on the code and app signatures, CYREN believes the source of the malware to be China. GhostPush is detected by CYREN as AndroidOS/Rootnik.A.gen!Eldorado. As the malware originates from non-GooglePlay store sources, we once again caution users about downloading apps that require enabling the "Unknown Sources" check box.

Top 10 Q3 Android Malware

1. AndroidOS/AirPush.A.gen!Eldorado
2. AndroidOS/Wooboo.A.gen!Eldorado
3. AndroidOS/Revmob.A
4. AndroidOS/Inoco.A.gen!Eldorado
5. AndroidOS/Frupi.C
6. AndroidOS/Agent.LD
7. AndroidOS/FakeInst.FD
8. AndroidOS/Kuguo.B.gen!Eldorado
9. AndroidOS/Addisplay.A
10. AndroidOS/SMSPay.A

Web Malware

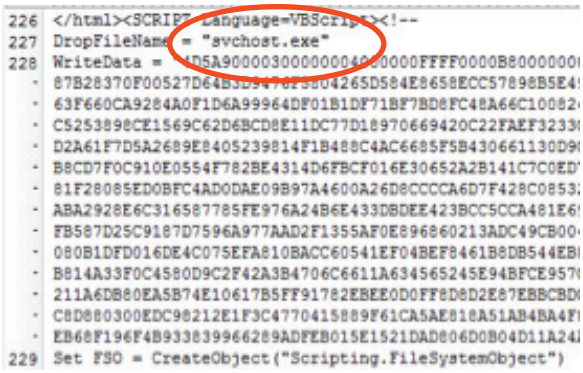
SEOHide and Faceliker

The top Web malware identified by CYREN analysts in the 2015 Q1 report returned in Q3, with the top three being JS/SEOHide.A, JS/Faceliker.A!Eldorado, JS/Faceliker.a.

As reported in CYREN's Q1 CyberThreat Report, SEOHide and FaceLiker are designed to generate revenue by hijacking the resources and activities of unsuspecting site owners and visitors. The JavaScript-based Trojan, FaceLiker hijacks mouse clicks to force users to "like" a particular Facebook page. Achieving a "like" is often the first-step in spreading 'malvertising' scams on Facebook. Another JavaScript Trojan, SEOHide, injects code into compromised websites to boost page rankings by hiding hyperlinks to them throughout the infected sites. Cybercriminals use SEOHide to give a short- term "Black Hat SEO" boost to a site that they are targeting for monetary purposes; for example, they may receive a commission on any business transacted through the site, or they are using the site to deliver malware to unsuspecting visitors.

VBS/DropDownld.B and JS/IFrame.VJ.gen

VBS/DropDownld.B and JS/IFrame.VJ.gen rounded out the top five malware for the third quarter. VBS/DropDownld.B is malicious script found on infected websites. When a user visits the site, the script automatically stores a hex-encoded string on the victim's computer. The script then decodes the string into a file called svchost.exe, saves it in the temp directory, and then executes the file. The malware is then executed in the background without user intervention, and typically without user knowledge.



Svchost.exe" is Created from the Hex "Writedata"

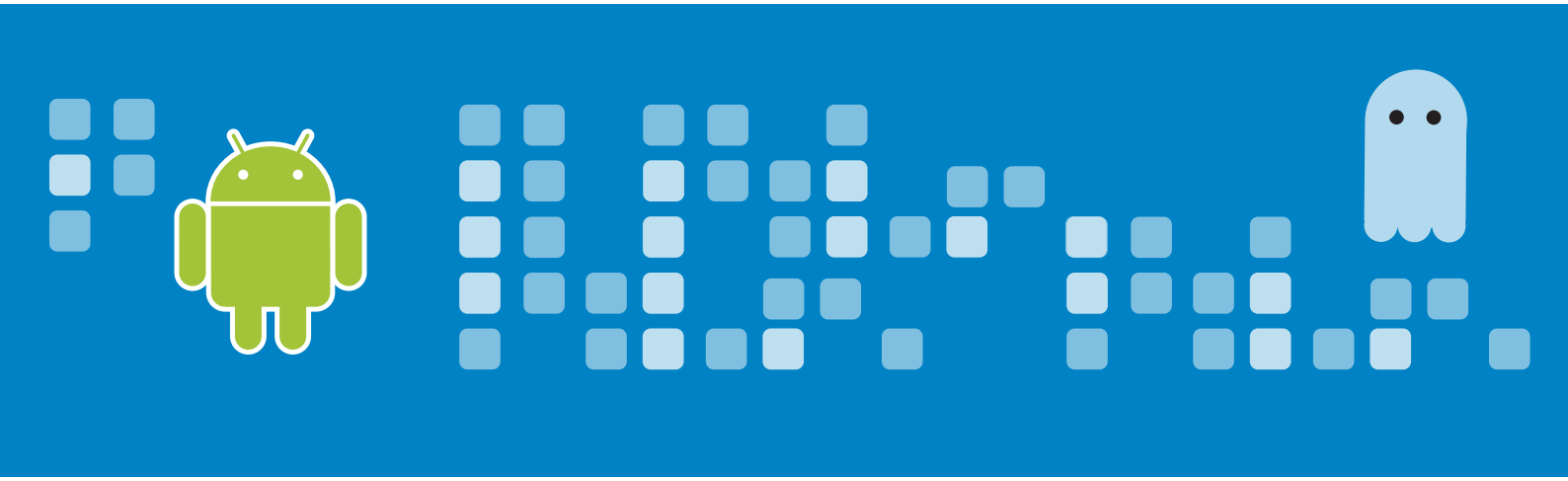
The dropped file, svchost.exe, is a variant of the infamous worm/infector malware family of Ramnit detected by CYREN as W32/Ramnit.X. Like Ramnit, VBS/DropDownld.B disables Windows security features, such as Windows Defender, Windows Firewall, and User Account Control), as well as preventing Windows Update from operating correctly. VBS/DropDownld.B

also stops the system from installing antivirus software. Once installed, the malware proceeds to collect online services account information—financial, banking, social, and professional—by creating fake copies of legitimate websites. The cybercriminals then gain access to these accounts. VBS is only supported by Internet Explorer and users of more modern browsers are therefore not at risk.

JS/IFrame.VJ.gen is a form of spyware launched in August 2015. It is found on compromised WordPress, Drupal, and Joomla pages containing injected JavaScript. The infection starts when a user visits a compromised site. The simplified JavaScript code contains an iframe that redirects to a malicious server location. Additional JavaScript is loaded, which then gathers information such as the operating system, timestamp, timezone, and existence of certain legitimate applications like Adobe Flash Player. The collected information is sent back to the original server and a series of redirects to fake sites follow, that look identical to or closely resemble Flash upgrade sites, Google Chrome plugins, or other fake application sites. Once on these fake sites, the victim is encouraged to download spyware or potentially unwanted applications (PUA) that pretend to be real applications.

Top 10 Q3 Web Malware

1. JS/SEOHide.A
2. JS/Faceliker.A!Eldorado
3. JS/Faceliker.a
4. VBS/DropDownld.B
5. JS/IFrame.VJ.gen
6. IFrame.gen
7. JS/Faceliker.B!Eldorado
8. JS/Redir.XG
9. JS/IFrame.RS.gen
10. JS/Faceliker.C.gen



Can you spot the scam?

Cybercriminals use a variety of sophisticated techniques to take advantage of unsuspecting Internet users. Here is a sample of two different scams **#DetectedbyCYREN** during this quarter.

CYREN Identifies Over 100,000 Ashley Madison Extortion Emails

In July 2015, the Ashley Madison scandal broke with the announcement that cybercriminals had stolen all of the company's customer data, including names, email addresses, home addresses, credit card information, and other types of highly "personal" information. The criminals threatened to release all this sensitive information if this website (and other related sites owned by parent company Avid Life Media) were not shut down.

The morally questionable nature of the Ashley Madison site notwithstanding, it is well-known that there were individuals who had Ashley Madison accounts set up against their will, as a joke, or because of a mistyped email address. These individuals also lost their data to the world of cybercrime, along with every bona fide Ashley Madison user, in spite of many of them having previously paid a fee to Ashley Madison to have their names removed from the system.

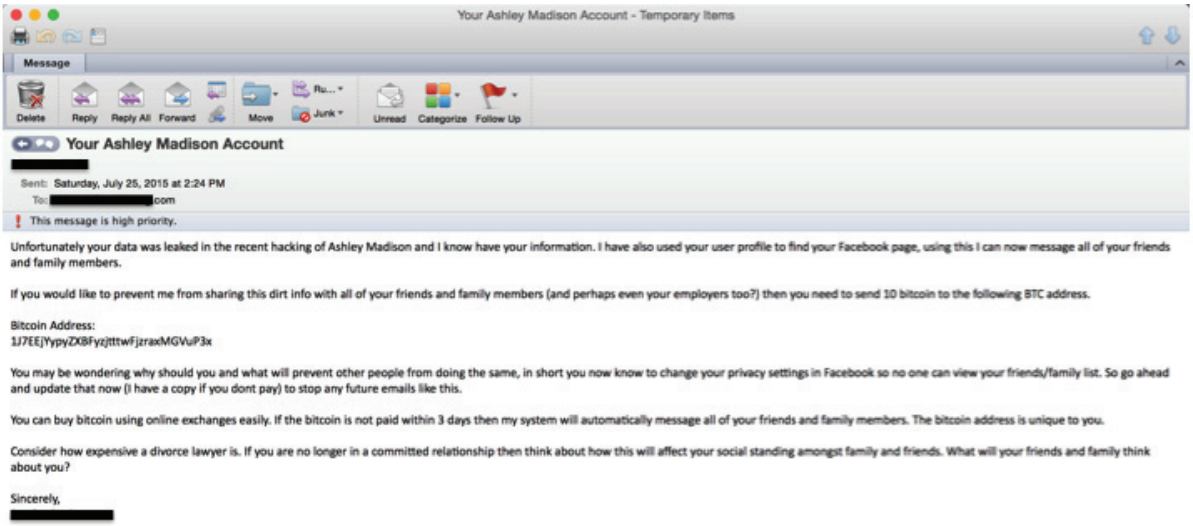
In the initial phase of the attack, criminals released the database of Ashley Madison details. It didn't take long, however, for other cybercriminals to capture the list of email addresses and send out extortion emails. Late in the third quarter, CYREN began to see **hundreds of thousands** of these "ransom emails" in bulk distributions.

Every email stated the following:

"Unfortunately your data was leaked in the recent hacking of Ashley Madison and I know [sic] have your information. I have also used your user profile to find your Facebook page, using this I can now message all of your friends and family members.

If you would like to prevent me from sharing this dirt info with all of your friends and family members (and perhaps even your employers too?) then you need to send 10 bitcoin to the following BTC address.

Bitcoin Address: 1J7EEjYypyZXBFyzjtttwFjzraxMGVuP3x



You may be wondering why should you and what will prevent other people from doing the same, in short you now know to change your privacy settings in Facebook so no one can view your friends/family list. So go ahead and update that now (I have a copy if you dont pay) to stop any future emails like this.

You can buy bitcoin using online exchanges easily. If the bitcoin is not paid within 3 days then my system will automatically message all of your friends and family members. The bitcoin address is unique to you.

Consider how expensive a divorce lawyer is. If you are no longer in a committed relationship then think about how this will affect your social standing amongst family and friends. What will your friends and family think about you?"

The value of 10 bitcoins is approximately $2,600, not a cheap undertaking for those willing to cough up the money. However, there is little sense in paying this ransom, since the personal data is already publicly available and paying one extortionist would probably not stop a different extortionist from exposing the same information. Further, it is also highly unlikely that these criminals have access to Facebook account information.

Unfortunately, it is likely that extortion attempts like these will continue to increase in scope and scale. For example, using email addresses obtained from Ashley Madison, cybercriminals could begin to deliver malware and 'ransomware', locking down the victims' computer files unless a ransom is paid to obtain a decryption key. Government organizations could also be at risk; over 15,000 registered Ashley Madison members used their U.S. government workplace email addresses, including those that worked for the Army, Navy, Department of Justice, Homeland Security, and the IRS.

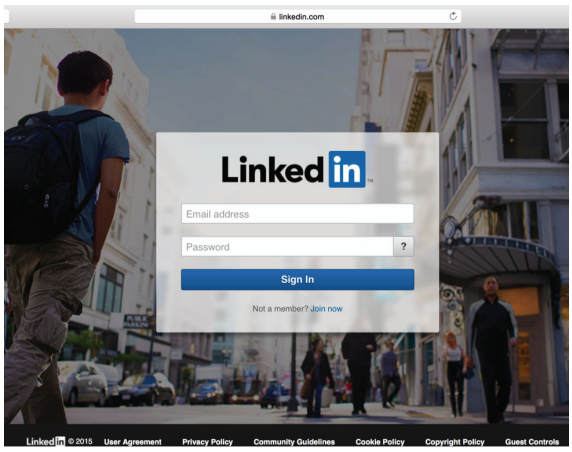
Sophisticated Phishing Emails #DetectedbyCYREN

CYREN identified a major phishing scam targeting corporate and government email credentials.

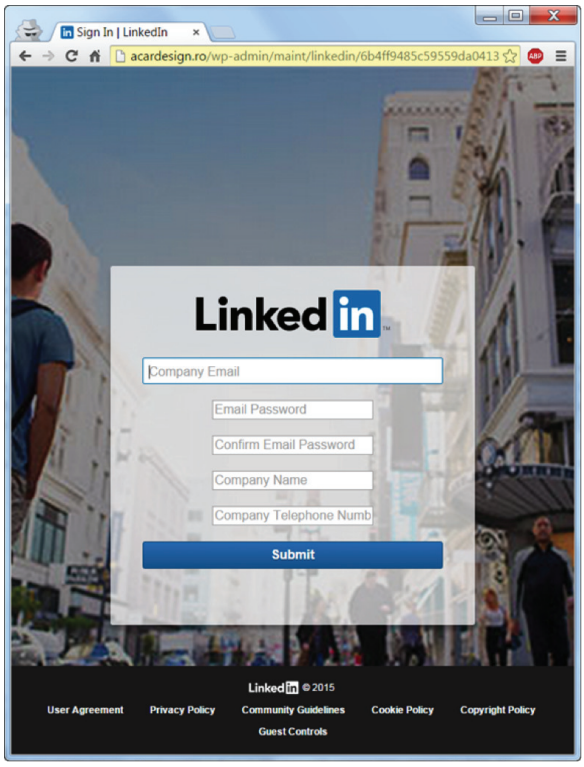
The frustrating part about cybercrime is that it is getting harder and harder for the average computer user to detect a threat. Cybercriminals are becoming sophisticated and savvy, as we see in this series of phishing emails that popped up this quarter.

What is particularly interesting about this scam is that the criminals attempted to gain the victims' corporate names, email addresses, passwords, and phone numbers, using spoofed images from well known and reputable cloud service companies, such as LinkedIn, Apple, and Amazon. CYREN analysts believe this may be part of a long-term threat process in which criminals are trying to amass corporate login data to eventually be sold and/or used in corporate breaches. The attacks may also be intended to target well known webmail services that can now be used to access corporate content, such as Gmail credentials used for Google apps access.

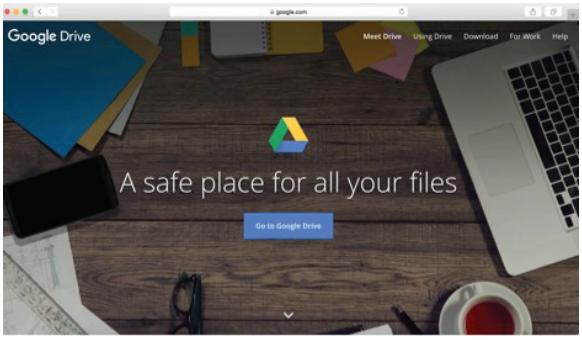
The faked websites used to entice victims included the United Kingdom's government revenue and customs website, Apple, Bank of



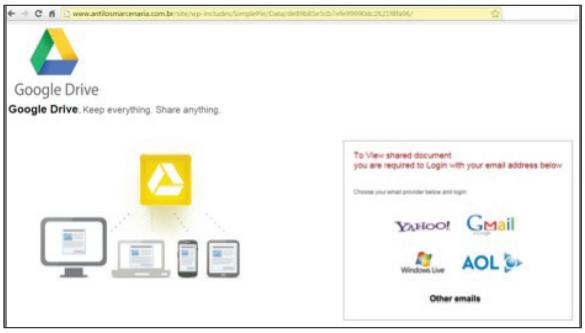
Legitimate LinkedIn Site Login Page



Fake LinkedIn Phishing Site Login Page



Legitimate GoogleDrive Site



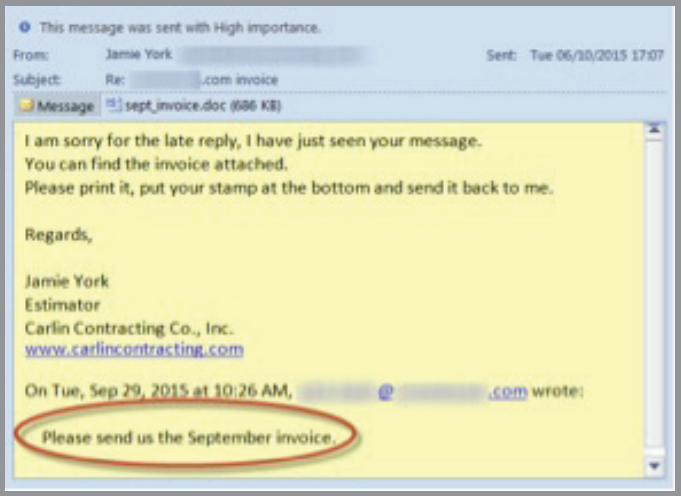
Fake GoogleDrive Site

America, DHL, Dropbox, Facebook, Alibaba, Google Docs, Paypal, and Amazon. Even smaller regional corporations, such as the U.S.-based government financial institution, Navy Federal Credit Union, and the U.S. cable company Comcast were targeted.

Fortunately, these emails never made it into the inbox of their intended victims, thanks to CYREN. But email users that are not protected by CYREN security services may well receive such an email and respond by typing in their user name and password, as well as their company name and password, which could once again result in the announcement of a massive data breach, such as those with Experian and the U.S. Office of Personnel Management.

Social Engineering— Be Aware of New Tricks!

The email shown here includes a .doc malware attachment. What is unusual is the use of the recipient name inside the email "requesting" the invoice. This makes the email seem more legitimate and increases the chances that the recipient will open it.



CYREN
Threat Intelligence Powering Trend Awareness

CYREN

CYBERTHREAT Report

CYREN cyber intelligence powers the security solutions of over 200 of the largest IT and security technology providers in the world. Every day, CYREN collects and analyzes 17 billion pieces of threat data, through 500,000 global points of presence, distributed across 200 countries, ultimately protecting 600 million global users.

200 COUNTRIES

500K GLOBAL POINTS OF PRESENCE

600M GLOBAL USERS

17B PIECES OF THREAT DATA

Q3 2015

Android Malware

6.25%
of all Android apps installed are malicious

655,000
new Android malware variants found in Q3 — **24% less than in Q2**

24%

7
of the top 10 types of Android malware are adware related; the remaining 3 are SMS Trojans

Phishing Trends

4.3 million
phishing URLs tracked by CYREN
— **down 19% from July**

19%

CYREN analysts believe that the decrease could be a normalizing trend from the significant increase in Q2 (38%)

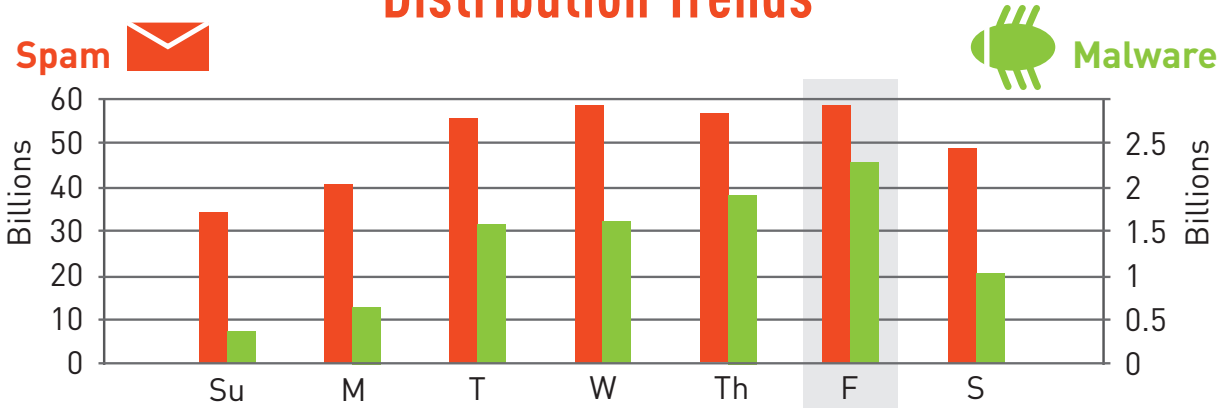
Spam Trends

52 billion
average Spam Per Day in Q3
— **down 5.4% from 55 billion in Q2**

5.4%

The September 2015 spam level was the lowest in six years, at 47.4 billlion per day

Distribution Trends



Fridays are the peak distribution days for both Malware and Spam.

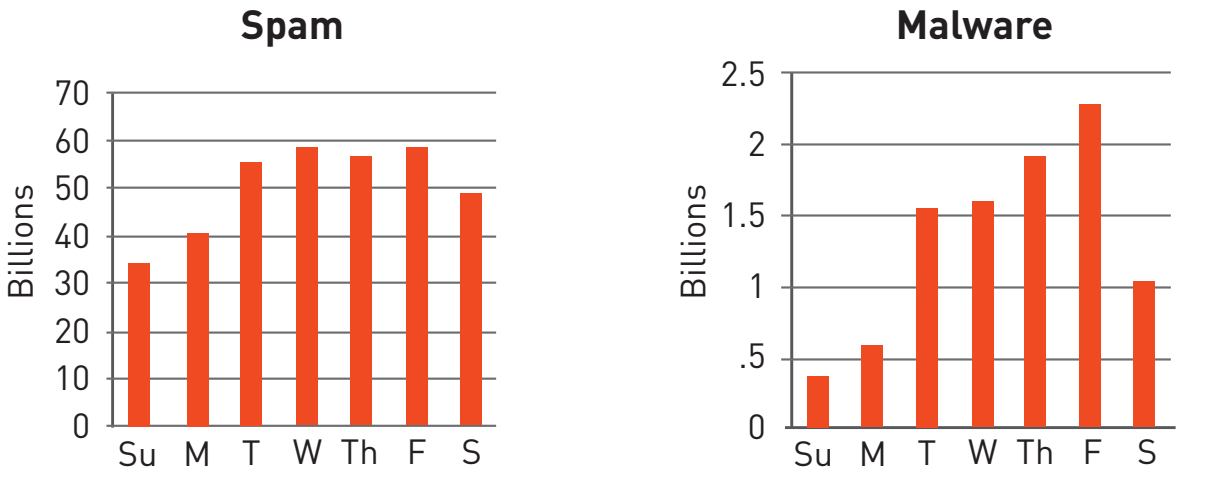
2.25 billion
average Malware attachments on Fridays in Q3

And Finally...Friday Malware Peak Gives Cybersecurity Professionals a "Case of the Mondays"

There has always been anecdotal evidence from colleagues and clients that Mondays are the worst day for cleaning up threats and breaches. As we discussed in an August blog entry, cybersecurity professionals report that as employees return to the office on Monday and login to corporate networks, security alerts begin popping up. These professionals speculate that when employees take their laptops home over the weekend, they connect to the Internet through public or unsecured WiFi, and proceed to surf the web and download content. Because employees are no longer behind perimeter Web firewalls, they may connect with sites that contain unsafe or inappropriate content that would otherwise be blocked while surfing in a secure office environment. Additionally, users may also click on links or download content that comes through in email.

CYREN analysts were curious if there was any truth behind the stories. To test the hypothesis that Monday mornings are the worst time for threats and breaches to appear on corporate networks, we decided to look at the daily malware distribution trend during the third quarter. It turns out that Fridays are the peak distribution days for malware and spam, lending some credence to the theory that employees are downloading unsafe content on Saturdays and Sundays when using their laptops on unsecured networks.

The solution? Cybersecurity, in the form of web or cloud-based security, must follow the user and the device at all times, but particularly when users are connecting to the Internet from outside of the office. Without web security, IT professionals are very likely to end up with a bad "case of the Mondays."



Friday Peak in the Billions of Spam and Malware Attachments Distributed Per Day

CYREN

Applied Cyber Intelligence

U.S. HEADQUARTERS
7925 Jones Branch Drive,
Suite 5200
McLean, VA 22102
Tel:703-760-3320
Fax:703-760-3321
www.CYREN.com

USA
1731 Embarcadero Road, Suite 230
Palo Alto, CA 94303
Sales:650-864-2114
General:650-864-2000
Fax:650-864-2002

ISREAL
1 Sapir St., 5th Floor, Beit Ampa
P.O. Box 4014
Herzliya, 46140
Tel:+972-9-8636 888
Fax:+972-9-8948214

GERMANY
Hardenbergplatz 2
10623 Berlin
Tel:+49 (0)30/52 00 56 – 0
Fax:+49 (0)30/52 00 56 – 299

ICELAND
Thverholti 18
IS-105, Reykjavik
Tel:+354-540-7400
Fax:+354-540-7401