THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

6 November 2014

Purpose
Educate recipients of cyber events to aid in protecting electronically stored DoD, corporate proprietary, and/or Personally Identifiable Information from theft, compromise, espionage

Source
This publication incorporates open source news articles educate readers on security matters in compliance with USC Title 17, section 107, Para a. All articles are truncated to avoid the appearance of copyright infringement

Publisher
* SA Jeanette Greene
Albuquerque FBI

Editor
* CI SA Scott Daughtry
DTRA Counterintelligence

Subscription
To receive this newsletter please send an email to scott.daughtry@dtra.mil

Disclaimer
Viewpoints, company names, or products within this document are not necessarily the opinion of, or an endorsement by, the FBI or any member of the New Mexico Counterintelligence Working Group (NMCIWG)

NMCIWG Members
Our membership includes representatives from these agencies: 902nd MI, AFOSI, AUSA, DCIS, DOE, DSS, DTRA, FBI, HSI, Los Alamos Labs, NAG, NCIS, NGA, NRO, and Sandia National Labs

Distribution
This product may NOT be forwarded to personal email accounts (e.g. AOL, Gmail, Hotmail, Yahoo). Further dissemination of this product is allowed to U.S. person co-workers or other U.S. agency / U.S. company email accounts providing this newsletter's content is NOT copied / pasted into another document, database or email Altered in any way, to include the removal of NMCIWG logos and / or caveat markings. Credit is given to the NMCIWG for the compilation of this open source data

This is the most advanced iPhone malware yet, and it should terrify you

BGR, 6 Nov 2014: Apple used its iOS anti-malware security many times to bash Android's malware problem — which is an issue that affects plenty of Android users — but it looks like the company might have a serious iOS and OS X security issue on its hands, The New York Times reports. While malware attacks have been possible against jailbroken iOS devices for some time, a new piece of malware has been discovered that can infect even iPhones that have not been jailbroken. Researchers at the Palo Alto Networks discovered the program, called WireLurker, which can be used for many purposes including spying silently on users. It seems to already have affected hundreds of thousands of users in Asia. The point of entry seems to be OS X computers, with researchers having found 467 malware OS X applications in the unofficial Maiyadi App Store in China that were downloaded more than 356,000 times in the past six months in the region. Once on a Mac, WireLurker can infect any iPhone that's connected via USB to the computer, and install malicious applications. "WireLurker exhibits complex code structure, multiple component versions, file hiding, code obfuscation and customized encryption to thwart anti-reversing," the researchers wrote. "WireLurker is capable of stealing a variety of information from the mobile devices it infects and regularly requests updates from the attacker's command and control server. This malware is under active development and its creator's ultimate goal is not yet clear," he said. "They are still preparing for an eventual attack," Palo Alto Networks director of threat intelligent Ryan Olson told the Times. "Even though this is the first time this is happening, it demonstrates to a lot of attackers that this is a method that can be used to crack through the hard shell that Apple has built around its iOS devices." This isn't the first time Apple has had security problems in China, with the company having fought a complex iCloud phishing attack only a few weeks ago. To read more click **HERE**

New technique makes phishing sites easier to create, more difficult to spot

Heise Security, 5 Nov 2014: Researchers have spotted a new technique used by phishers which could trick even more users into believing they are entering their information in a legitimate web form. Instead of replicating as faithfully as possible a legitimate website - for example an e-commerce site - the attackers need only to set up a phishing page with a proxy program which will act as a relay to the legitimate site, and create a few fake pages for when users need to enter their personal and financial information. "So long as the would-be-victim is just browsing around the site, they see the same content as they would on the original site. It is only when any payment information is entered that modified pages are displayed to the user," Trend Micro Senior Threat Researcher Noriaki Hayashi explains. "It does not matter what device (PC/laptop/smartphone/tablet) or browser is used, as the attacker proxies all parts of the victim's HTTP request and all parts of the legitimate server's response." In the spotted attack, users are directed to the malicious site by clicking on a search result they got by entering a product's name. The attackers used a number of blackhat SEO techniques to make the URL appear in the results. But spam emails and messages can also be used to lure potential victims to the malicious site. The actual attack begins when the user clicks on the "Add to Basket" button on the legitimate site - the attacker has re-written the function so that the user is redirected to a spoofed e-cart page that leads to more fake pages simulating the checkout process. The first page asks the victims to enter their personal information (name, address, phone number) as well as their email address and password. The second one requests the entry of credit card information (including the card's security code). The third one asks for additional information that is sometimes required to authorize a transaction. Once the victims have submitted all this information, they will receive a fake confirmation email for the purchase to the email address submitted - and the illusion is complete. "So far, we have only identified this attack targeting one

specific online store in Japan. However, if this attack becomes more prominent, it could become a very worrying development: this makes phishing harder to detect by end users, as the phishing sites will be nearly identical to the original sites," Hayashi noted. This approach makes phishing websites much easier to set up, and very difficult for the owners of the legitimate websites to detect. To read more click **HERE**

Inside corporate privacy programs at Fortune 1000 companies

Heise Security, 6 Nov 2014: The International Association of Privacy Professionals (IAPP) released a survey of corporate privacy programs at Fortune 1000 companies. The survey found that while corporate investment in privacy is likely to increase, many privacy leaders feel their programs are relatively nascent and want greater influence over corporate decision-making. Driven by exponential growth in cloud, mobility and big data analysis in the digital age, privacy has become an important issue companies must address as a core part of doing business. When faced with increasing levels of regulatory scrutiny on corporate privacy practices and growing consumer concern for protecting their personal information, companies find themselves grappling with managing a complex set of privacy requirements and expectations. "Understanding how several of the world's largest companies are managing their privacy programs can help professionals across the board more effectively develop programs and advocate for the budget, tools and organizational influence they need to be successful," said J. Trevor Hughes, CIPP, president and CEO of the IAPP. "The study showed that managing privacy in the ever-changing technological landscape with seemingly endless layers of regulation to comply with, cultural sentiments to accommodate and consumer expectations to satisfy requires strong privacy programs and leadership."

Privacy budgets in the millions:

- Surveyed organizations had an annual privacy budget of $2.4 million, which equates to an average of $204 per $1 million in revenue. Privacy falls far short of the average security budget of $4.1 million in 2014 according to PwC's Global State of Information Security Survey.
- Thirty-eight percent of respondents said they would likely increase their privacy budget an average of 34 percent with only 10 percent likely to experience budget contraction.
- Based on current spending levels and projected spending from respondents, privacy spending for the Fortune 1000 is expected to approach $3 billion in 2015.
- This projected increase in budget could be due in part to many programs being relatively nascent with only 26 percent of companies characterizing their programs as mature.

Privacy is a growing and lucrative profession at Fortune 1000:

- Privacy is a relatively lucrative profession with more than half of employees making more than $200,000 in base salary. Further, the profession is nearly equally split between women (48 percent) and men (52 percent), a ratio more rare in comparable technical fields.
- Many of the Fortune 1000 are looking to increase the number of employees focused on privacy issues. One third (33 percent) of organizations plan to increase fully dedicated privacy headcount or create positions with privacy as part of its responsibility in the next year.
- Extrapolating the average headcounts to the full Fortune 1000, then multiplying by the expected average increases, translates to a projected increase of 950 full-time privacy professionals with another 2,200 professionals with privacy as part of their responsibilities over the next year.
- Steep growth in the IAPP's membership numbers – from 10,000 members in 2012 to a projected 20,000 at the end of 2014 – further shows this trend extends outside the Fortune 1000.

Increased CPO influence and integration with IT and security:

- There is a clear trend of privacy responsibilities being increasingly linked to security at companies.

- CPOs surveyed recognized the importance of integrating privacy with security. Ninety-three percent of respondents indicated having a close working relationship with information security colleagues and 79 percent report working with the broader IT organization.
- This close working relationship translates to significant influence over security and IT decision-making. A majority of respondents report satisfaction with their influence over IT (64 percent) and information security (61 percent) operations.

To read more click **here**.

What attackers do after bypassing perimeter defenses

Heise Security, 6 Nov 2014: Vectra Networks collected data over five months from more than 100,000 hosts within sample organizations to gain a deeper understanding of breaches that inevitably bypass perimeter defenses, and what attackers do once inside networks. They found that more than 11,000 hosts experienced one or multiple cyber-attacks that made it through perimeter defenses. Of these attacked hosts, 10 percent had detections for two or more attack phases – such as botnet monetization, command and control, reconnaissance, lateral movement and exfiltration. Overall, 15 percent of hosts in the participating organizations experienced a targeted attack. Once the attackers established a stronghold, they performed reconnaissance via internal port scans, lateral movement using brute force attacks, remote control of the attack with command and control communication, and exfiltration through hidden tunnels. Oliver Tavakoli, CTO of Vectra Networks, said: "Cyber attacks are increasingly sophisticated, highly organized, and successful despite $60 billion invested in cyber security annually worldwide. All of the attack phases detected in this report are ones that evaded organizations' perimeter and endpoint security systems." Additional key findings of the study include:

- Eighty-five percent of attacks experienced by the sample organizations were opportunistic attacks. Two percent of the hosts experiencing an opportunistic attack were being used to spread botnet malware to other computers within the organization.
- Fifteen percent of attacks experienced by the sample organizations were targeted attacks. Two percent of these hosts under targeted attack were breached to the exfiltration stage, where the attacker was preparing to steal data.
- Seven percent of hosts had both botnet and exfiltration detections, which indicates possible theft of credentials for use in a subsequent targeted attack against the sample organization or other organizations.

To read more click **HERE**

Linksys SOHO router owners urged to patch multiple vulnerabilities

Heise Security, 5 Nov 2014: Owners of a number of Linksys small office/home office routers have been urged last week to update their device's firmware in order patch two vulnerabilities, one of which could allow a remote, unauthenticated attacker to read or modify sensitive information on the router, and the other could allow a local attacker to read the device's password file. Unfortunately, owners of Linksys router models EA2700 and EA3500 can't do it, as a security update has not yet been made available. The latter ones are in greater danger, as according to Threatpost, PoC exploits for the vulnerabilities in the EA3500 and EA6500 models have been made available on a Turkish hacker site in September. "It should also be noted that the router exposes multiple ports to the WAN by default. Port 10080 and 52000 both expose the administrative web interface to WAN users. Depending on the model, additional ports may be exposed by default as well," CERT's advisory pointed out. Both vulnerabilities were discovered by researcher Kyle Lovett, who responsibly disclosed them to Linksys in July. Since Linksys provides the option for firmware updates to be delivered and implemented automatically on these devices, users are advised to go for it. To read more click **HERE**

Mobile security breaches impacted 68% of organizations

Heise Security, 5 Nov 2014: Mobile security breaches have affected 68 percent of organizations in the last 12 months, according to a new global study from BT. Despite this, organizations are still not taking sufficient security measures to protect themselves against mobile threats, such as lost or stolen devices and malware infections. Around half of respondents' organizations who had suffered a mobile security breach, experienced more than four incidents in the last year. The research explores the attitudes of IT decision makers towards security within their organizations. It shows that uptake of BYOD (Bring Your Own Device) and COPE (Corporately Owned Personally-Enabled) devices is very high, with 93 percent of organizations allowing employees to use these devices for work purposes. However, only four in 10 organizations surveyed actively have a BYOD policy. In this environment, device security is falling by the wayside: only a quarter of respondents felt that their company had sufficient resources in place to prevent a mobile security breach. Surprisingly, three in 10 (29 percent) do not have password protection, and less than half (45 percent) report that their organization has IT security training for all. The report highlights that while 33 percent of personal or corporate owned mobile devices have full access to the internal networks or contain sensitive client information, a third of organizations do not have any kind of enforceable mobile security policy. For those that do, the average length of time between reviewing mobile security measures is nine months. The infrequency of this is cause for concern, as many IT decision makers believe that the rate of malware infections will be on the rise in the next three to five years. Security breaches, such as lost or stolen devices, malware infections such as viruses, spyware, and Trojan Horses, or the loss or theft of company or customer data, have had a major impact on business processes, including taking up valuable help desk time and other IT resources. They have reduced employee productivity, day to day activity and even customer experience, as well as causing reputational damage. Some have even resulted in hefty fines. Mark Hughes, president of BT Security, said: "Today's threat landscape shifts very quickly so it is important for organizations to start with security in mind, rather than add it as an afterthought. This will ensure that security processes develop with them, and not after them. This makes the task of being security-led much more straightforward." Staff attitudes remain the biggest threat to data security. The report reveals that 74 percent are not taking the security of devices seriously. However, delving further into this, it becomes clear that this attitude trickles down from the top: sixty-nine percent of IT decision makers do not believe their CEO takes security very seriously. This is concerning, as security programs need to have complete top down buy-in in order to be successful, with everyone from the CEO right throughout the organization taking part. Mark Hughes said: "If CEOs are passionate about making security practices work, then these will inevitably become an intrinsic part of people's lives. Problems usually arise when people don't understand the risks and the impact that neglecting security could cause for the business, as well as for them personally. A security breach could cause a share price drop and reputational brand damage. This means that security is everyone's job." To read more click **HERE**

Contractors face greater risk as accountability measures grow

Washington 5 Technology, 5 Nov 2014: From personnel-related executive orders to emerging proposals that would hold prime contractors entirely accountable for information security practices throughout their entire supply chain, we are seeing today a renewed government trend toward shifting greater responsibility (and thus, risk) to contractors for the behavior and performance of others, including those over which they have no real control. As is so often the case, taken alone, it is difficult to argue with the government's intentions. Everyone can agree that government contracts should not be awarded to companies that routinely and intentionally (emphasis on the latter) violate federal labor statutes. And everyone can agree that government contractors have to assume reasonable responsibility for protecting information in their possession or ensuring the authenticity of the parts they use. That's the easy part. But what we are seeing today has less to do with the term "reasonable" and more to do with pure risk shifting. On the information security front, what we call "supply chain accountability" is one of the most significant, but under-discussed, trends in government contracting. Here, policies are quickly evolving that will place all responsibility for protecting information and for cybersecurity at every level of the supply chain on the

prime contractor. This includes holding the prime contractor liable for information breaches at lower-tier subcontractors, an area into which the prime often has no visibility or even privity of contract. To be sure, the government has reason to be concerned. We see almost daily news about hacks at banks, retail outlets, government agencies, universities, and companies. And many argue that information security has only recently begun to attract the level and degree of attention it deserves in both the public and private sectors. But is the answer really as simple as slapping total accountability on a prime contractor? Some make the case that, by virtue of being a prime, a company is willingly accepting a wide array of responsibility for ultimate performance on a contract or program, so why is information protection and security any different? However, the reality is that while prime contractors can and should be held accountable, that liability can only reasonably be extended to areas and elements over which the contractor, within reasonable and practical parameters, actually has visibility and control. Breaches and other problems will inevitably happen, but if reasonable steps were taken to protect against them, can we really expect that much more from any institution? This issue was at the heart of the debate over the government's acquisition of counter-terrorism capabilities in the immediate post-9/11 environment and that experience offers a possible option here. Absent liability limits, bidding companies faced effectively "betting the farm" on every contract since a failure to stop a terrorist attack could result in a near endless series of lawsuits and liability. In that case, the SAFETY Act was born. Under it, contractor liability is limited, provided they have met all reasonable performance requirements. Given the rise of well-placed concern over information and cybersecurity, it is time to extend SAFETY Act-like protections into the cyber realm. We have already recommended to Congress just such an action. However, a similar answer does not exist for the most recent workforce executive order, "Fair Pay and Safe Workplaces." That order, a reprise of the Clinton era "blacklisting rule," is so broadly and vaguely written that a practical middle ground will likely prove elusive, absent significant changes to the order or to the soon-to-be-issued implementing regulation. Indeed, while we all agree that companies that routinely violate labor laws should generally not be given government contracts, this order raises serious questions about fairness, due process, timeliness, objectivity, and scope. But as different as supply chain accountability and the "Fair Pay" executive order might be, they have two, critical, common components: significant additional compliance costs and the shifting to the prime contractor of virtually all risk, even for matters over which they have no real control. And that should be a concern for both government and industry. Some experts estimate that compliance with government unique rules today costs about 25 cents for every contract dollar. The added supply chain requirements and, to the extent compliance is even possible, the new labor executive order, are likely to jack that cost up to well over 30 cents of every contract dollar. Seem like a lot? It is. In fact, almost across the board, the government-unique compliance regime, as its associated costs and risks, is growing. To read more click **HERE**

NIST outlines steps for coordinated cyber incident response

Fierce Government IT, 5 Nov 2014: Improved information sharing and coordinated incident response can help agencies bolster defenses against cyber threats, says draft guidance from NIST that aims to help agencies establish, participate in, and maintain information-sharing relationships throughout the incident response life cycle. In order to be effective, incident response activities must employ safe information sharing practices and leverage standard data formats and transport protocols, says a draft special publication (**pdf**) from NIST, which was issued for public comment Oct. 28. The guidance also explores the planning, implementation and maintenance of information sharing programs. According to NIST, there are several things organizations should do to facilitate a cybersecurity strategy that harnesses "the collective wisdom of peer organizations." Agencies should take inventory of the information they currently possesses, the information they can produce and under what circumstances that information should be shared. The draft SP also advises agencies to exchange threat intelligence, tools and techniques with partners, as well as employ open, standard data formats and transport protocols to facilitate information exchange. Publication authors say agencies should augment local data collection, analysis and management functions with third-party information in order to enhance their security posture. They should also define an adaptive cybersecurity approach for the entire cyber-attack lifecycle, and identify

resources needed for ongoing participation in a sharing environment. NIST says organizations should have constant awareness of information security, vulnerabilities and threats to their assets. The draft is open for comment until Nov. 28. Download SP 800-150 (draft) **here**. To read more click **HERE**