THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

30 October 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

Scary new malware uses a Gmail trick to steal your data

Yahoo, 29 Oct 2014: Scary new malware uses a Gmail trick to steal your data.A new piece of malware that can spy on a user's computer has been discovered, Wired reports, with researchers also having found a clever way for the program to communicate with its creators: Google's popular Gmail email service. Security startup Shape Security says it found a new strain of malware that's able to read instructions from Gmail drafts and respond to the hacker's commands without the user actually noticing anything happening on the computer. "What we're seeing here is command and control that's using a fully allowed service, and that makes it superstealthy and very hard to identify," Shape security researcher Wade Williamson said. "It's stealthily passing messages back and forth without even having to press send. You never see the bullet fired." For everything to work, hackers first set up an anonymous Gmail account, and then infect a target computer with the malware. After gaining control of the computer, the hacker will remotely open an invisible instance of Internet Explorer in which the Gmail account is loaded. Once that's done, information can be passed back and forth using the drafts folder. The malware uses a Python script to retrieve commands and code entered into the draft field, and then it can respond in Gmail drafts and can include the data it wants to steal. The malware is apparently a variant of an existing Trojan called Icoscript first found by security firm G-Data in August. Icoscript has been infecting computers since 2012, using Yahoo Mail to hide its command and control, before switching to Gmail drafts recently. It's not clear how many machines have been infected by this malware strain, and there's no way of easily detecting it, Shape says. To read more click **HERE**

October 28, KATV 7 Little Rock – (Arkansas) **ASU-Beebe still investigating possible data breach.** Arkansas State University-Beebe informed an unknown number of students and staff of a possible data breach at multiple locations after learning October 21 that its servers may have been compromised. The university is investigating and officials announced that the school's servers were taken offline after getting the report. Source: http://www.katv.com/story/27147008/asu-beebe-still-investigating-possible-data-breach

October 29, Securityweek – (International) **Vulnerability found in firmware update process of ASUS routers.** A researcher identified and reported a vulnerability in ASUS RT-series routers that could have allowed attackers to use a man-in-the-middle (MitM) attack to trick users into downloading older, vulnerable firmware versions or potentially malicious code due to the firmware request being sent in HTTP instead of HTTPS. ASUS closed the vulnerability in its 3.0.0.4.367.1123 update. Source: http://www.securityweek.com/vulnerability-found-firmware-update-process-asus-routers

NIST Guide to Cyber Threat Information Sharing open for comments

Heise Security, 30 Oct 2014: NIST has announced the public comment release of Draft Special Publication (SP) 800-150, Guide to Cyber Threat Information Sharing (**link**). The purpose of this publication is to assist organizations in establishing, participating in, and maintaining information sharing relationships throughout the incident response life cycle. The publication explores the benefits and challenges of coordination and sharing, presents the strengths and weaknesses of various

information sharing architectures, clarifies the importance of trust, and introduces specific data handling considerations. The goal of the publication is to provide guidance that improves the efficiency and effectiveness of defensive cyber operations and incident response activities, by introducing safe and effective information sharing practices, examining the value of standard data formats and transport protocols to foster greater interoperability, and providing guidance on the planning, implementation, and maintenance of information sharing programs. NIST is asking the public to comment on the draft by November 28, 2014. They are to be sent to sp800-150comments(at)nist.gov. To read more click **HERE**

Over a third of orgs have no real-time insight on cyber risks

Heise Security, 30 Oct 2014: Most organizations (67%) are facing rising threats in their information security risk environment, but over a third (37%) have no real-time insight on cyber risks necessary to combat these threats. This is one of the topline findings of EY's annual Global Information Security survey, Get Ahead of Cybercrime, which this year surveys 1,825 organizations in 60 countries - mostly chief information officers, chief information security officers, chief executive officers and other information security executives. Companies are lacking the agility, the budget and the skills to mitigate known vulnerabilities and successfully prepare for and address cybersecurity. Forty-three percent of respondents say that their organization's total information security budget will stay approximately the same in the coming 12 months despite increasing threats, which is only a marginal improvement to 2013 when 46% said budgets would not change. Over half (53%) say that a lack of skilled resources is one of the main obstacles challenging their information security program and only 5% of responding companies have a threat intelligence team with dedicated analysts. These figures also represent no material difference to 2013, when 50% highlighted a lack of skilled resources and 4% said they had a threat intelligence team with dedicated analysts. "Careless or unaware employees" is revealed as the number one vulnerability companies face, with 38% of respondents saying it is their first priority, and "outdated information security controls or architecture" and "cloud computing use" are second and third respectively (35% and 17%). "Stealing financial information," "disrupting or defacing the organization" and "stealing intellectual property or data" are the top three threats (28%, 25% and 20% respectively say it is their first priority). This year's survey finds that organizations need to do a better job of anticipating attacks in an environment where it is no longer possible to prevent all cyber breaches, and where threats come from ever more resourceful and well-funded sources. The report encourages organizations to embrace cybersecurity as a core competitive capability. This requires keeping the organization in a constant state of readiness, anticipating where new threats may arise and shedding the "victim" mindset of operating in a perpetual state of anxiety. To read more click **HERE**

White House network breach was likely nation-sponsored

Heise Security, 29 Oct 2014: The White House has confirmed that the unclassified Executive Office of the President network has been breached by unknown hackers. People in the know speculate that the attackers are working for the Russian government. This would not be the first time that a Russian cyber group has targeted US' government and military networks, and the recently discovered cyber espionage efforts aimed at NATO, the European Union, Ukrainian and Polish government organizations by the hands of the pro-Russian SandWorm Team points towards a concentrated effort to spy on states deemed to work against Russian interests. Naturally, it will be hard - if not impossible - to prove the origin of the attack and pin it to a specific group or state. Another thing that is yet unknown is what the attackers were after and what information they managed to access. The compromise apparently happened two or three weeks ago. US officials didn't notice it themselves, but received a tip from an allied country. The FBI, Secret Service and National Security Agency have been called in to investigate the intrusion, and the White House "took immediate measures to evaluate and mitigate the activity." White House workers were asked to change their passwords and remote access to the network via VPN was made temporarily impossible. The email system was slower that usual, but kept working. An anonymous White House official shared with the Washington Post that, so far, it appears that the classified network wasn't breached, and that the attackers didn't do any internal damage on the unclassified one. "The reconnaissance attack on the White

House is a dramatic reminder of a general truth: whenever we look for any kind of attack, we find that yes, indeed, it is happening. Anyone assuming they are not under attack because nothing has gone wrong so far is suffering the 'Christmas Turkey fallacy' - all the days the turkey spends seem to be pretty good, except for that last one," commented Dr. Mike Lloyd, CTO at RedSeal. "Attacks are very often not destructive at all – modern malware is frequently designed to do as little as possible, so as to avoid detection. Adversaries understand the value of good information – of maps, and the relationship of assets. Such information can be extracted with a minimum of fuss, unless the person being scanned is very diligent and observant." "Government networks the world over are on the front lines of a digital conflict, so it's no surprise the White House has been targeted as it presents a very rich target," says Chris Boyd, Malware Intelligence Analyst at Malwarebytes. "Whilst political tensions are often played out in public, it seems that highly specialist cyber-incursions have become a popular and lower profile offensive tactic. Whilst this particular breach doesn't seem to have compromised any sensitive information, it is still a sign of how geopolitical tensions are expressed in the modern world." "As details on the actual breach are still thin on the ground, it's difficult to comment on the technical aspects, but it does underline the growing success of advanced attacks. Traditional security solutions are continually being left wanting as advanced exploits, social engineering and other complex attacks develop too fast. Large organizations, particularly those in sensitive areas, need to combine advanced countermeasures with frequent staff training to ensure the best possible defence against this relentless progression in attacks." To read more click **HERE**

US-CERT Alerts of Ongoing Phishing Campaign Delivering Dyre Banking Trojan

SoftPedia, 28 Oct 2014: An alert from US-CERT (Computer Emergency Readiness Team) on Monday warns of a malicious email campaign spreading the Dyre banking Trojan, also known as Dyreza. The wave of messages started to appear since the middle of the month, US-CERT claims, and the actors behind them do not discriminate as far as recipients are concerned. It appears that the campaign has several variations with regards to the sender address, theme of the email and the exploits used. However, the ultimate goal is to lure the recipient to open a malicious attached file, which, according to CERT, purports to be an invoice in PDF format. The document (Invoice621785.pdf) is weaponized and carries exploits for old vulnerabilities in Adobe Reader. As such, the cybercriminals target users with old unpatched versions of the document reader. One of the vulnerabilities leveraged is CVE-2013-2729, which allows execution of arbitrary code in Adobe Reader and Acrobat versions earlier than 9.5.5, 10.1.7 and 11.0.03. The Dyre banking Trojan is not a new malware family as it was spotted for the first time in June this year. Since then, the malicious tool was identified in multiple cyber incidents, one of the most prominent being against customers of Salesforce in September. Users are advised to exercise caution when receiving unsolicited emails and pay particular attention to the spelling in the body and the subject of the message as this is an indicator of fraud. Also, the presence of Google Update Service could be a sign of infection. Cybercriminals have been testing user vigilance all summer The Trojan is designed to steal log-in information, banking details in particular, and send it to its operator. However, the piece was adapted for other types of credentials and in a recent incident it has been observed to include bitcoin websites on the list of targets in the configuration file. Email campaigns having the delivery of Dyre as the ultimate goal have been carried out all summer, as this seems to be the preferred method of the cybercriminals behind it. It has been seen in phishing emails purporting to come from the JP Morgan financial institution, as well as in messages claiming to be notifications for new voice messages. The malware has been improved in the months following its release in the wild, up to the point that it used its own SSL certificate to secure communication with the command and control server and to hide malicious traffic. To read more click **HERE**

Microsoft Account Termination Email Is a Scam

SoftPedia, 29 Oct 2014: Email messages claiming to be from Microsoft and informing about account termination have been spreading lately in an attempt to dupe unsuspecting users into providing credentials for the email service. Plenty of users still fall for this type of tricks, where a situation requiring urgent action is presented in order to lower the chances of signs of deceit to be spotted. In this

campaign, the potential victim receives the message as a result of an alleged submitted request to close the Microsoft account. A period of three days is given to cancel the procedure, which is designed to prompt an urgent action from the victim. As is usually the case, a link for stopping the account termination process is offered, which points to a fraudulent page that requires logging in. All the information submitted via the fields available is sent straight to the crooks. A Microsoft account is used for multiple services from the company, including access to the OneDrive cloud storage, where multimedia files and documents can be saved, as well as to the web-based email service. Moreover, these credentials can be synonymous with the username and password used for logging into the latest versions of Windows. As such, guarding this information should be paramount for users and a moment should be taken to think whether the message is genuine or not. In any case, it is advisable not to use the URL provided in a suspicious message to log in, but type the address manually in the web browser in order to access the service. To read more click **HERE**

Free Pizza Hut Coupon Hooks Asprox Trojan into System

Softpedia, 29 Oct 2014: Cybercriminals operating the Asprox/Kuluz botnet try to replenish the number of infected computers by baiting potential victims with the promise of a free coupon that can be used in any Pizza Hut restaurant to get a free meal. Many would think that they would not fall for the "free coupon" lure, but in this campaign the email looks genuine and could fool even the more suspicious users. Researchers at Cloudmark identified the new campaign on Tuesday and after analyzing the payload, they determined that it was an effort to expand the Asprox botnet, also known as Kuluoz. The offer of the free Pizza Hut coupon comes as a promotion from the restaurant celebrating its 55th anniversary; but as Cloudmark noticed, the restaurant was founded in 1956, making it 58 years old, a fact that is not known or verified by the potential victims. This is actually one of the few clues that indicate that the offer in the email is not to be trusted, because all other elements of the message do not betray the deceit; there is even a deadline for claiming the voucher, set for November 5. After clicking on the provided link, "you do not get a coupon for free pizza – you get a .zip file containing a Windows executable which will make you part of a malicious botnet called Asprox or Kuluoz," Andrew Conway from Cloudmark writes in a blog post. The botnet has been around since 2008, constantly modifying its size. It is used for all types of nefarious activities, from distributing spam to spreading Trojans and carrying out click-fraud activities. It is also leveraged to scan the Internet for web servers vulnerable to SQL injection attacks. These, in turn, are used to infect other workstations, ensuring the Asprox operators a vast network of computers at their disposal. "Everybody wants to believe in free pizza. We are seeing an unusually high number of people taking this email out of their spam folders. Users are more than four times more likely to take this out of their spam folder than the largest recent malware spam campaign which claimed to be a notice to appear in court," Conway writes. However, users should be more suspicious of unsolicited emails, especially if they promise free stuff. A simple way to make sure they land on the right web page is to check the web address, which, in the case of Pizza Hut, should be http://pizzahut.com/, the researcher advises. To read more click **HERE**

167 Data Breach Incidents Expose 18.5 Million Records of California Residents

SoftPedia, 29 Oct 2014: An annual report on cyber incidents affecting the residents of California has been compiled by the Office of the Attorney General for 2013, revealing a more than 600% increase in the number of exposed records; the raw data translates into 167 data loss events and about 18.5 million records at risk. The document takes into consideration all the events that resulted in the loss or exposure of personal information of more than 500 Californians and does not discriminate between business sectors. Responsible for the spike in the amount of victims are two incidents that occurred in 2013, namely the intrusion at LivingSocial, which, overall, leaked details of 50 million individuals, and the attack on Target announced in December, which lost card data info on about 40 million customers. Together, these two impacted about 15 million Californians, according to the report from the Attorney General's Office. By comparison, the number of breaches reported in 2012 was 28% lower, amounting to 131 incidents, and the total of records potentially fallen into the hands of unauthorized persons was 2.6

million. More than half of customer data loss incidents in California in 2013 were on account of malware infections or hacking, theft of physical devices (computer systems, storage units) containing personal client records coming in second with 26%, while errors and misuse of technology accounted for the least amount of incidents, 18% and 4%, respectively. According to the report, although 53% of the incidents were due to infiltration of malicious software and hacking of the computer system infrastructure, these incidents accounted for the largest amount (93%) of the compromised personal records. In these cases, it is safe to assume that at least some of this information was sold on underground forums and that it was used for malicious activities leading to financial losses for the victims. As far as the data type exposed is concerned, social security numbers were at the top followed closely by payment card details. These are the most valuable to cybercriminals, who can use them for identity theft and subsequently obtaining financial gains. As it was to be expected, the retail sector was the most affected by data breach incidents, as crooks tried to exfiltrate card information from payment processing systems. Bill to make entities pay for exposing sensitive customer details Lately, such incidents have become common, Kmart, Dairy Queen, Supervalu and Home Depot being the most prominent victims this year, hundreds of stores and tens of millions of customers being affected across the US. California Attorney General Kamala Harris says that an assembly bill (AB 1710) has been enacted, requiring that the source of a breach involving customer personal information to provide complimentary identity theft and mitigation services to the affected individuals for a period of at least one year; affected individuals should also be informed of the incident within 15 days of the discovery. The bill is set to take effect in California starting January 2015. Recommendations from the Attorney General for retailers to prevent such events include using strong encryption (very useful in other sectors, too) for the stored data, as well as switching to chip-enabled payment processing systems. To read more click **HERE**

BlackEnergy Malware Hits Industrial Control Systems in the US

SoftPedia, 29 Oct 2014: An ongoing malicious campaign has compromised multiple industrial control systems (ICS) in the US by using a version of BlackEnergy toolkit on Internet-facing human-machine interfaces (HMI) from different vendors. The activity is believed to have started at least three years ago, in 2011, the malware being identified by multiple companies on the control solutions they use. According to the US ICS-CERT (Industrial Control Systems Cyber Emergency Response Team), the threat actors behind this BlackEnergy campaign targeted the HMI products of GE Cimplicity, Advantech/Broadwin WebAccess, and Siemens WinCC. Other solutions may also be affected, although at the moment there are no details about which ones. The malware is modular in architecture, which allows its operators to implement new modules that would cover additional functions. Despite its multiple capabilities, at the moment, only modules designed for lateral movement on the network have been observed, searching for shared locations and removable media. However, this type of activity has not been noted and the malware remained on the compromised HMIs. ICS-CERT found no evidence that BlackEnergy tried to influence in any way the control processes on the victimized systems. The findings of the investigation revealed that on GE Cimplicity, the threat actors leveraged a vulnerability (CVE-2014-0751) that allowed remote execution of arbitrary code through a specially crafted message to TCP port 10212. The security glitch was publicly disclosed at the beginning of 2014, while instructions for mitigating the risk had been published by GE in December 2013, but ICS-CERT says that the operators have been exploiting it since at least January 2012. According to the analysis of the attack on Cimplicity products, BlackEnergy executes a self-delete routine following its installation on the target machine. "Analysis suggests that the actors likely used automated tools to discover and compromise vulnerable systems. ICS-CERT is concerned that any companies that have been running Cimplicity since 2012 with their HMI directly connected to the Internet could be infected with BlackEnergy malware," the advisory says. Attack vectors for the other HMI products have not been determined yet, but files associated with the BlackEnergy campaign have been discovered on machines running WinCC and Advantech/Broadwin WebAccess control software. A strong recommendation has been issued for companies operating industrial control systems to check their assets for signs of intrusion. ICS-CERT created a Yara signature to help identify the BlackEnergy compromise. "This signature is provided 'as is' and has not been fully tested for all variations or environments. Any

positive or suspected findings should be immediately reported to ICS-CERT for further analysis and correlation," the group of experts warn. BlackEnergy is a toolkit that has been employed by multiple criminal groups over the years. In a recent incident discovered by Finnish security researchers at F-Secure, samples of the malware were seen collecting intelligence from Ukranian government entities. The custom versions were attributed to the Quedagh group, known for aiming at political organizations. To read more click **HERE**

Overdue Invoices Hide Pony Info-Stealing Trojan

Softpedia, 28 Oct 2014: A new email campaign has been detected to deliver Pony stealer disguised as a PDF file purporting to contain details about an overdue invoice. The document has a double extension and is, in fact, a COM executable file that includes commands for downloading the malware from a compromised website, after running a few unpackaging procedures. The newest variants of Pony feature capabilities for stealing crypto-currency wallets available on the infected computers but can also exfiltrate sensitive information as well as download other malware families. Security researchers from Avast analyzed the hacked website used by cybercriminals to host the malware and found that other threat samples were being hosted. This can be done because of a backdoor specifically created for this purpose, allowing complete access. Apart from this, the researchers noticed that the site was used to place several Pony stealer administration panels on it, along with the original installation package. Users are advised to exercise caution when receiving unsolicited emails that try to convince them to open documents claiming to offer information about a payment. As noted by researchers at Damballa, among other capabilities present in Pony stealer, there is decoding of passwords saved by a significant number of programs, from digital currency clients and FTP managers to web browsers and email clients. To read more click **HERE**