



The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals
22 April 2014

Purpose

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

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, Sandia 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 open source data

April 20, CNN – (National) **Heartbleed causes HealthCare.gov to change users' passwords.** Registered users of the U.S. national health insurance exchange Web site had their account passwords reset and were prompted to change their passwords as a precaution due to the Heartbleed vulnerability in OpenSSL. There was no indication that users' personal information was at risk or any indication that the vulnerability had been used against the Web site. Source: <http://politicalticker.blogs.cnn.com/2014/04/19/heartbleed-causes-healthcare-gov-to-change-users-passwords/>

April 21, Dark Reading – (International) **Heartbleed attack targeted enterprise VPN.** Researchers at Mandiant identified a successful attack campaign that utilized the Heartbleed vulnerability in OpenSSL to target an undisclosed organization's virtual private network (VPN) and obtain VPN session tokens. The attack began April 8, hijacked several active user sessions, and allowed the attackers to attempt to escalate their privileges within the organization. Source: <http://www.darkreading.com/attacks-breaches/heartbleed-attack-targeted-enterprise-vpn-/d/d-id/1204592>

April 18, Threatpost – (International) **ICS-CERT warns of Heartbleed vulnerabilities in Siemens gear.** The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) issued an advisory warning that the Innominate mGuard firmware and several Siemens industrial control systems are vulnerable to the Heartbleed vulnerability in OpenSSL. Innominate issued a patch for the vulnerable firmware, while Siemens identified affected systems. Source: <http://threatpost.com/ics-cert-warns-of-heartbleed-vulnerabilities-in-siemens-gear/105554>

April 19, Softpedia – (International) **Sophos names spam-relaying "dirty dozen" countries for Q1 2014.** Sophos released its list of top spam-relaying countries for the first quarter of 2014, with the U.S. accounting for the most spam by volume at 16 percent of all spam, followed by Spain and Russia. Source: <http://news.softpedia.com/news/Sophos-Names-Spam-Relaying-Dirty-Dozen-Countries-for-Q1-2014-438517.shtml>

April 18, The Register – (International) **Reddit users discover iOS malware threat.** Reddit users identified a piece of malware for iOS devices known as Unflod Baby Panda which can target jailbroken iOS devices. Researchers at SektionEins found that the malware listens to SSL traffic and searches for Apple ID information to steal. Source: http://www.theregister.co.uk/2014/04/18/reddit_users_discover_ios_malware_threat/

April 18, CSO – (International) **Major security flaws threaten satellite communications.** Researchers at IOActive released a paper outlining critical vulnerabilities in satellite communication gear from several major manufacturers that could allow attackers to disrupt or eavesdrop on communications systems used in the maritime, energy, aeronautics, and media industries as well as those used by government and emergency services. Affected manufacturers were notified and details will not be publicly released



The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals
22 April 2014

until the second half of 2014 to allow manufacturers to close the vulnerabilities. Source:
<http://www.networkworld.com/news/2014/041814-major-security-flaws-threaten-satellite-280848.html>

Microsoft Fixes Security Essentials Bug on Windows XP

SoftPedia, 22 Apr 2014: An update released by Microsoft for its own Security Essentials anti-virus and other anti-malware solutions caused a number of Windows XP computers to freeze after boot, with some reports pointing to thousands of machines that got affected by the issue. Redmond has however shipped another update that comes to address all these problems, so consumers who were experiencing problems on Windows XP, Windows Server 2003, and other platforms after deploying anti-malware signature updates should get the new one as soon as possible. Antimalware Engine 1.1.10502.0 was shipped to computers running Microsoft Security Essentials, Forefront Client Security, Forefront Endpoint Protection, Windows Intune Endpoint Protection, and System Center Endpoint Protection customers and contains signature package 1.173.0.0 that fixes the aforementioned bug. "This is due to an update that was shipped on April 15, 2014 that may have caused interrupted service for some customers using Microsoft security products. This was corrected via signature update, which automatically resolved the issue, and customers who have deployed the most recent signatures do not need to take any action," Microsoft says. The company also noted that while the problems were initially experienced on Windows XP and Windows Server 2003, some other platforms might have been impacted as well. Customers who disabled Behavior Monitoring or applied other workarounds are recommended to revert the changes as soon as possible and deploy this new update. To read more click [HERE](#)

NullCrew Hackers Target UVa, the State of Indiana, National Credit Union and Others

SoftPedia, 22 Apr 2014: On Easter Sunday, hackers of the NullCrew collective announced breaching the systems of nine organizations. The list of targets is comprised of the University of Virginia, Spokeo, Telco Systems, National Credit Union, the Science and Technology Center of Ukraine (STCU), the International Civil Aviation Organization, the State of Indiana and ArmA2. Earlier this month, the hackers also attacked Klas Telecom, a government contractor which admitted that its legacy helpdesk system was breached and that NullCrew gained access to some old customer data. "[FTS] is generally aimed at the government, or anything that is corrupt; and that is the reason for these attacks. Ranging from government contractors, to universities, to telecommunications companies, to information databases, and other things," the hackers wrote next to the leaked data. "They are all part of the system; and have failed examinations the first time around; some of the attack methods may have been simple, or the data not too complex," they added. "But, it can still lead to things that they do not want; and it also costs them, therefore we have committed actual damage to this certain aspect of the system. In a way, we achieve our goal." From each of the penetrated systems, the hackers have leaked various types of data, including administrator credentials, email addresses, usernames, password hashes and server information. As far as the University of Virginia is concerned, this isn't the first time its systems are breached. However, it appears that the organization still hasn't managed to properly secure its networks. The university hasn't said anything regarding the incident, but DataBreaches.net has learned that they're investigating. Spokeo representatives have confirmed for ZDNet that their systems have been hacked. The company said that the attack took place in mid-January. They claim that NullCrew has only breached the Spokeo blog and that no customer information has been compromised. The hackers said they had "backdoored" Spokeo over 6 times in a 72-hour period. None of the other targeted organizations have mentioned anything about the incident, but the hackers have provided some details about their operation. For instance, they claim to have harvested emails from STCU's mail server for more than one year. Risk Based Security and Data Breaches have analyzed the leaked data. RBS notes that while the hackers haven't leaked any sensitive data belonging to the customers of the National Credit Union, they have leaked credentials for forms, CMSs and WordPress Installations affiliated with the organization. In the case of the State of Indiana, NullCrew pulled off the attack by exploiting a local file inclusion vulnerability. To read more click [HERE](#)



The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals
22 April 2014

Cybercriminals Use “Unflod” Malware to Steal Apple Passwords from iPhones and iPads

SoftPedia, 22 Apr 2014: A piece of malware dubbed “Unflod.dylib” or “framework.dylib” has been attempting to steal the Apple ID credentials of iPad and iPhone owners. The campaign has been named the “Unflod Baby Panda” and it’s believed to have been launched by Chinese actors. This is another example that Apple devices, particularly jailbroken ones, are not 100% secure. Reddit users first revealed seeing the malware around 4 days ago when their Apple devices started crashing. German security researcher Stefan Esser explains that the threat is distributed as a library called Unflod.dylib or framework.dylib. When it’s installed on an iPhone or an iPad, it hooks into all processes in an effort to listen to outgoing SSL connections. It appears that the attackers are targeting Apple usernames and passwords, which are sent back to some remote servers. The servers in question are owned by US hosting firms, but they’ve been rented by Chinese customers. The language used in the malicious code indicates that Unflod has been developed by Chinese programmers. It’s believed that the threat is being distributed via Chinese piracy repositories, but this hasn’t been confirmed yet. It’s worth noting that the malware only affects jailbroken devices. Furthermore, Esser has told Ars Technica that only phones and tablets running the 32-bit version of iOS are impacted. The Trojan should not work on iPhone 5s, iPad mini 2G or iPad Air. After analyzing the malicious library, Esser has determined that the malware is signed with a developer certificate issued by Apple for an individual named Wang Xin. “This person might be a fake persona, the victim of certificate theft or really involved. It is impossible for us to know, but Apple should be able to investigate from this information and terminate that developer account,” Esser noted in a blog post. “Furthermore the signature date is the 14th of February of this year, which hints at this threat being around for a short while now without being discovered.” Russian security company Dr. Web was the first to detect the threat (iPhoneOS.PWS.Stealer.1). Around 14 hours ago, at the time of the last VirusTotal report, 15 of 50 antivirus engines detected the Trojan, including AVG, Bitdefender, ESET, Emsisoft, F-Secure, Sophos, Trend Micro and GData. This means that if you have an antivirus solution installed, it might be able to detect the threat. While some experts have determined that the malware can be removed by deleting the Unflod.dylib (framework.dylib) binary, Esser believes that this isn’t guaranteed to work. That’s because it’s still uncertain how the malware ends up on Apple devices and it could be bundled with additional threats. The best way to ensure that the threat is removed is to fully restore the infected devices, but this means the jailbreak is lost. To read more click [HERE](#)

Microsoft Provides Fix for Errors 800f0092 and 80073712 on Windows 8.1 Update

SoftPedia, 22 Apr 2014: A number of users are still struggling to deploy Windows 8.1 Update even though the OS update was launched nearly 2 weeks ago to everyone running Windows 8.1. Time is running out, however, as Microsoft has made Windows 8.1 Update mandatory for Windows 8.1 users, so it’s pretty clear that those struggling to install it are really having a hard time doing it right now. Basically, users are provided with two or three different error codes when attempting to install Windows 8.1 Update via Windows Update, no matter if they run 32- or 64-bit hardware configuration. Some of those affected by the bug explained that Windows 8.1 Update installation worked smoothly on a number of computers, but it failed with errors 800f0092 and 80073712 on others, which could be an indication that hardware incompatibility is the root cause of these problems. “I have the same problem with the error code 80070005 when I’m trying to install Windows 8.1 x64 Update KB2919355 (the big one of aprox. 900 MBytes) only for 1 PC. As yourself, I tried a lot of tricks but none of them worked,” one user wrote on Microsoft’s Community forums. Basically, it appears that the initial Windows 8.1 Update installation fails to complete and does not remove some of the files it deployed, so relaunching the setup or performing the whole process manually is basically impossible without first deleting the leftovers. A Microsoft support engineer posted on the company’s forums a workaround very similar to the one we’ve already told you about, so follow these steps to make sure that you manage to install Windows 8.1 Update success. Microsoft’s tutorial is available in the box after the jump, so just click the “Press Release” button and read all the instructions to make sure that you’re on the safe side. As far as the Windows 8.1 Update is concerned, Microsoft says that everyone needs to install it by May 13 in order to receive other patches and security fixes released by the company as part of the Patch Tuesday rollouts. Redmond says that this is absolutely needed because all future updates



The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals
22 April 2014

will actually be based on this new OS version, so those who won't install it won't be able to implement the new features. Windows 8.1 Update is currently being offered to users via Windows Update, but it's also available as a manual download in case you do not have an Internet connection or you're experiencing issues during the installation process. To read more click [HERE](#)

Verizon Publishes 2014 Data Breach Investigations Report

Softpedia, 22 Apr 2014: Verizon has published the 2014 Data Breach Investigations Report (DBIR), one of the industry's most important and most referenced information security studies. The latest report focuses on several issues, including cyber espionage, attacks against point-of-sale (POS) systems, denial-of-service, physical theft and loss, insider threats, crimeware and web application attacks. The report shows that a total of 198 POS intrusions were reported last year, the accommodation and food services, and retail industries being the most targeted. Despite some significant attacks being disclosed over the past period, Verizon says that the number of POS intrusions has decreased over the last several years. "That's mainly because we've seen comparatively fewer attack sprees involving numerous small franchises. Brute forcing remote access connections to POS still leads as the primary intrusion vector. A resurgence of RAM scraping malware is the most prominent tactical development in 2013," the report reveals. When it comes to web app attacks, a total of 3,937 incidents were reported last year, 490 of which with confirmed data disclosure. Experts say that web applications can be hacked in two ways: either by exploiting vulnerabilities, or by using stolen credentials. Most of the attacks analyzed by Verizon have targeted popular content management systems like WordPress, Drupal and Joomla and abused them for distributed denial-of-service (DDOS) campaigns. The study also focuses on incidents involving insiders or privilege misuse. "Most crimes by trusted parties are perpetrated for financial or personal gain. The most noticeable shifts in the 2013 dataset, however, were an increase in insider espionage targeting internal data and trade secrets, and a broader range of tactics," the report reads. Of the over 9,000 physical theft and loss incidents, most have impacted the healthcare, public and mining industries. Interestingly, loss is reported more often than theft. When it comes to theft, corporate offices are more often targeted than residences or personal vehicles. The security attributes of an information asset can become compromised and it doesn't necessarily involve losing a device. Instead, it can be a result of unintentional actions. Verizon has placed these types of incidents in a category called "miscellaneous errors." More than 16,000 such incidents were reported last year. When it comes to cyber espionage, a total of 511 incidents have been reported, 306 of which with confirmed data disclosure. The professional, transportation, manufacturing, mining and public sectors are the most targeted. "Most surprising to us is the consistent, significant growth of incidents in the dataset. We knew it was pervasive, but it's a little disconcerting when it triples last year's already much-increased number," Verizon noted in its report. The complete 2014 Data Breach Investigations Report is available on Verizon's website ([link](#)). To read more click [HERE](#)