Counterintelligence NEW MEXICO Working Group

NMCIWG Purple Arrow Established 2001

THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

15 July 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

July 14, The Register – (International) **FBI: We found US MILITARY AIRCRAFT INTEL during raid on alleged Chinese hacker.** A Chinese man was arrested by Canadian authorities at the request of the FBI for working with two other uncharged suspects and allegedly hacking into several defense contractors' networks in the U.S. and Europe in order to steal information on 32 U.S. projects, including the U.S. Lockheed F-22 and F-35 aircraft and Boeing's C-17 cargo plane. Authorities alleged the suspects were able to extract several thousand digital files and attempted to sell the information off to State-owned companies in China. Source: http://www.theregister.co.uk/2014/07/14/us_military_aircraft_intel_captured_in_alleged_chinese_hacker_raid/

July 14, Securityweek – (International) **Kronos: New financial malware sold on Russian underground forum.** Researchers with Trusteer reported July 11 that a new piece of banking malware known as Kronos has recently been advertised on a Russian underweb forum in a pre-release sale. The malware contains HTML injection and form-grabbing capabilities, allegedly works with modern and older Web browsers, and is compatible with the Zeus trojan. Source: http://www.securityweek.com/kronos-new-financial-malware-sold-russian-underground-forum

July 11, Dark Reading – (International) **International hacker pleads guilty to 2011 global cyberattack.** A member of an international cybercrime organization pleaded guilty July 11 for working with co-conspirators to hack into the payment card processor for the American Red Cross in 2011 and stealing payment card data that was then used to make $14 million in fraudulent ATM withdrawals around the world. Source: http://www.darkreading.com/international-hacker-pleads-guilty-to-2011-global-cyberattack/d/d-id/1297241

July 14, Help Net Security – (International) **Critical vulnerabilities in web-based password managers found.** Researchers at the University of California identified and reported various vulnerabilities in five Web-based password managers that could allow attackers to obtain a user's credentials. LastPass, My1Login, RoboForm, and PasswordBox reported that they closed the vulnerabilities after they were reported, while the researchers did not receive word on the issues from NeedMyPassword. Source: http://www.net-security.org/secworld.php?id=17111

July 14, Help Net Security – (International) **Keyloggers found at hotel business centers, US Secret Service warns.** U.S. officials issued an advisory to hospitality industry companies encouraging them to secure their public computers and limit guest accounts to non-administrator accounts following the arrest of a group of individuals that are suspected of compromising computers in Texas hotel business centers. The suspects allegedly used stolen credit cards to register as hotel guests and used the hotel's business center to download and execute key logging software, which was used to capture the information of other guests. Source: http://www.net-security.org/secworld.php?id=17110

July 11, Securityweek – (International) **Attackers use keyloggers, email to steal data in "NightHunter" attacks.** Cyphort researchers reported identifying a cybercriminal operation known as "NightHunter" that has been active since 2009 and uses various pieces of malware and keyloggers to target organizations in the energy, education, health, insurance, and charity industries. The campaign distributes the malware through phishing emails that are usually sent to finance, human resources, and sales departments. Source: http://www.securityweek.com/attackers-use-keyloggers-email-steal-data-nighthunter-attacks

July 14, Softpedia – (International) **Cisco patches four-year-old Apache Struts 2 issue.** Cisco patched a vulnerability in Apache Struts 2 that was reported in 2010 which could allow an attacker to use a malicious Object-Graph Navigation Language (OGNL) expression to compromise vulnerable systems. Source: http://news.softpedia.com/news/Cisco-Patches-Four-Year-Old-Apache-Struts-2-Issue-450663.shtml

Kronos Malware Available with a $7,000 (€5,140) Price Tag

Softpedia, 15 Jul 2014: A post on a Russian underground forum offered a new financial malware named Kronos for a full price of $7,000 / €5,140, with a one-week trial period available for $1,000 / €734. The price alone suggests that this is aimed to be a premium piece of malware, and the initial list of features seems to confirm it. Kronos malware is touted to include regular infostealing capabilities, such as form grabbing and HTML injection for Google Chrome, Mozilla Firefox and Internet Explorer. The post announcing the availability of the new malware family has been found by the security researchers at IBM's Trusteer, who did not get their hands on a sample for deeper analysis. It is also advertised as being able to bypass antivirus protection, as well as sandbox environments used by security researchers to analyze the samples. The crooks implemented a rootkit component (for both 32-bit and 64-bit systems) that can protect itself from other Trojans. "The Trojan uses an undetected injection method to work in a secure process and bypass proactive anti-virus protections," says the Trusteer translation of the forum post. Furthermore, "the Trojan is able to bypass any hook in usermode functions which bypasses rootkits or sandboxes which use these hooks." As it was to be expected, the communication between the infected machine and the command and control server is encrypted. It appears that the forum post already delivered plenty of information, as they said that "the HTML injection mechanism is compatible with Zeus," and pointed out that this was most likely because most of the cybercriminals it addresses either used or are still using variants of the Zeus malware. As such, the developers of Kronos made sure that they wouldn't have a tough time implementing the web inject component. Although the price asked may seem high, previous premium malware were sold for as much as $15,000 / €11,000 if delivered with all the modules. However, the Kronos malware writers promised to add new modules to the piece in order to expand its functionality, each of them being charged separately. Just like regular developers, they are willing to provide bug fixes with each update, which will not be charged. During the one-week trial, testers will have access to a server hosted specifically for them, with full control of the panel and no imposed limitations. It is too early to say if Kronos will be indeed the father of Zeus, but the good thing is that security experts and law enforcement now have a name to pin to the Kronos sample when they catch it. To read more click HERE

Internet Explorer Patch Breaks Down InstallShield on Windows PCs

Softpedia, 15 Jul 2014: Microsoft rolled out six different security bulletins on Patch Tuesday to address a total of 29 vulnerabilities in its software, including some critical glitches in Internet Explorer, the company's in-house browser which is said to be used by more than 58 percent of the desktop computers worldwide. It turns out that one of the patches released during this last rollout actually breaks down InstallShield 2011 through 2014 software, with Flexera, the company behind this app, confirming the issue in a public statement. Microsoft hasn't yet provided a fix on this, but users who posted on the Community forums explained that KB2962872 appeared to be at fault for startup crashes and a significant slowdown of InstallShield. InfoWorld says that the problem could be caused by a bug in handling .HTM files, so uninstalling the update rolled out by Microsoft could indeed fix the problems. "Moving the.htm files to a backup folder has been shown to reduce the impact of the issue for some InstallShield customers. Please note, that by taking these steps, the InstallShield Start Page and inline help will be limited and navigating to some views may still trigger a crash. Those using this method should save their projects frequently," Flexera said in a statement. According to Microsoft information, this particular security bulletin is supposed to fix flaws in all Internet Explorer versions, starting with 6 and ending with 11. The company says that one publicly disclosed vulnerable and 23 privately reported flaws in the browser are expected to be fixed by this patch, but no specifics have been provided on any compatibility issues that might occur following the installation of this bulletin. "The most severe of these vulnerabilities could allow remote code execution if a user views a specially crafted webpage using Internet Explorer. An attacker who successfully exploited these vulnerabilities could gain the same user rights as the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights," Microsoft said. At this point, no fully working fix is available, so everybody is still waiting for Microsoft to release a patch that would allow them to deploy it without risking any software crash. We've also reached out to Microsoft for more information on this, so we'll update the article when we receive an answer, hopefully with a working fix or timing details for a new patch. To read more click HERE

CNET Hacked, Perps Ask One Bitcoin for Details of 1 Million Users

Softpedia, 15 Jul 2014: Recently, a hacker group from Russia informed over Twitter that they managed to hack the systems of CNET and collect a database with login credentials of more than one million users of the website. The data stolen from CNET's servers is said to contain usernames, emails and encrypted passwords, and the group, communicating under the alias "w0rm," tweeted that they were willing to sell the information for as little as one Bitcoin (roughly $620/€455). Perpetrators said they asked for such a low price because they wanted to gain notoriety. The security hole exploited is in the Symphony PHP framework, which allows web developers to build more sophisticated websites. A representative from CBS Interactive, which owns the CNET publication, admitted the servers had been accessed by an attacker over the weekend and said that the issue had been identified and eliminated, but they would keep their eyes on the matter. W0rm did not provide the full path to the exploit, and it appears that the motivation behind the attack was to raise security awareness, a high-profile website being the best way to achieve this goal. https//w0rm.in/cnet.com.tar.gz cnet hacked, here is src of www. pic.twitter.com/ggkaNF3VfE — w0rm (@rev_priv8) July 12, 2014 Although the passwords retrieved by the hackers are encrypted, there is no information on the algorithm used to protect them or if they were salted and hashed. As a precaution, it would be wise for those with login credentials for CNET website to change their passcodes for the service, even if decrypting the details may not lead to accessing them in plain text. It is worth noting that the same security awareness motivation was behind the recent distributed denial-of-service attacks carried out last week against multiple financial institutions in Norway. The attacker sent the media publications an email claiming he was part of Anonymous Norway and said that "the motivation behind the current attacks and the next attacks in the future is to get the community to wake up. The number of major IT security attacks is increasing and there is nothing being done to prevent such events." A few days later he was identified as a 17-year-old and the authorities arrested him under the initial charge of gross vandalism, which carries in Norway a maximum prison penalty of six years. The teen was revealed to be a script kiddie who leveraged a known vulnerability in WordPress. However, in this case, it appears that the hackers know what they are doing and are not expected to be careless about their identity. To read more click HERE

UK Beefs Up Cyber Defenses

Softpedia, 15 Jul 2014: British Prime Minister David Cameron announced an investment of £1.1/$1,885/€1,387 billion in the Armed Forces, most of them being assigned to intelligence and surveillance equipment relating to cyber-defense technology. Cameron wrote in The Telgraph that the threats have changed radically since the Cold War 30 years ago, and that today, the enemy may be seen and unseen, with plots being hatched miles away from the intended victim. He said that "the plain fact is that in the 21st century, you cannot defend the realm from the white cliffs of Dover." £800 million of the financial injection (approximately $1,370 / €1 billion) is to be allotted to improving the cyber defense technology and surveillance aircraft used by the Armed Forces, so that flights can be conducted over areas like the Horn of Africa in order to identify threats against the UK and the allies. Security against cyber attacks and for the protection of the energy sector is also to benefit from the investment. Despite the lack of richer information regarding the strengthening of cyber-defenses, the fact that this sector has been recognized as in need of increased attention should be applauded and followed as a good example of keeping up with the various threats that can target a nation via computer systems. To read more click HERE

Most Critical Infrastructure Companies Struggle with Security

Softpedia, 15 Jul 2014: A survey on a sample of 599 employees responsible with the IT security measures in critical infrastructure companies revealed that most of these entities have not fully deployed their IT security programs. The study was conducted independently between April and May this year by the Ponemon Institute and was sponsored by Pennsylvania-based global IT company Unisys. It included IT security executives in 13 countries, all of them familiar with security regulations regarding the protection of information assets and critical infrastructures. According to the report, only 17% of the surveyed companies have initiated measures to mitigate the risk of cyber-attacks, although 57% believe "cyber-threats are putting industrial control systems and SCADA at greater risk." 67% of the respondents acknowledge that their companies have been affected by at least one security compromise in the past year, which led to loss of sensitive information or disruption of operations. In some cases (24%), the incidents occurred because of an insider attack or the carelessness of IT users with increased privileges. The figures in the survey show that most of the respondents are aware of the high risks the industrial control systems (ICS) are facing when there is no improvement as far as the security posture is concerned. "Security maturity levels are mostly at the early or middle stage," reads the report, which also says that "the majority of companies say important security governance activities are only partially or not implemented at all." "Specifically, 58 percent of the respondents say their organizations are only partially or not vetting contractors, vendors and other third parties to make sure they have high security standards. Similarly, compliance with security requirements are only partially or not strictly enforced." It is also highlighted that there is no proactive attitude for mitigating future security risks, but rather a concern on immediate incidents. This is because minimization of downtime is considered more important than adopting security measures for preventing cyber-attacks. Furthermore, only 32% of the respondents recognize the importance of enhancing the security posture as a top objective and even less (6%) offer cyber-security training programs for their employees. More than half (55%) of the surveyed entities said they had only one person responsible for the security of the ICS/SCADA systems. More worryingly, a quarter of the respondents said they had no one to fulfil this duty and 5% did not know. Databases, computer systems (desktops, laptops, smartphones and tablets), cloud-based systems, servers and ICS, were among the most attacked devices, while the most vulnerable to attacks were applications, databases, mobile devices, routers/switches, and servers. The survey included utility, oil and gas, energy and manufacturing companies, and Ponemon admits that the results rely on the responses provided by the subjects and that there is the possibility that not all of them were accurate. To read more click HERE

LinkedIn Credentials Targeted by Phishing Campaign

SoftPedia, 15 Jul 2014: Even if Facebook is the preferred social network targeted by scammers, similar services from other companies are not overlooked. A recent campaign seeks to steal the credentials of LinkedIn users. Because LinkedIn is a social network for professionals, the credentials for these accounts are more valuable than those for Facebook users. The recent phishing campaign sends the potential victim an email informing that the account had been blocked because it was not accessed for a long period of time. To keep the LinkedIn service active, the victim has to access a link and verify the email address by providing the username and password. Obviously, the provided link leads to a phishing site that impersonates the LinkedIn log-in page and all the information entered in the available fields is automatically sent to the cybercriminals. To make sure they get the right information, the crooks ask for the primary address, in case multiple ones are available for the LinkedIn account. With the victim's credentials in their hands, the bad actors can easily launch other spam campaigns in the name of the victim, with an increased rate of success because the targets receive the lure from someone they know. One way to spot the fake message is to take a look at the link and check if it leads to a valid LinkedIn domain. Also, logging into the account of this service is done in a secure manner, so if the HTTPS connection is missing, you can be sure that it is a scam. To read more click HERE

100+ Security Fixes Announced for the Oracle Critical Patch Update

SoftPedia, 15 Jul 2014: On Tuesday, July 15, Oracle will push the quarterly critical patch update, which addresses a hefty set of 113 vulnerabilities in multiple products from the company. More than half of the fixes (70) aim to eliminate remotely exploitable risks that could be leveraged by an attacker without the need of authentication for the following products:

- Oracle Database Server (1)
- Oracle Fusion Middleware (27)
- Oracle Hyperion (2)
- Oracle E-Business Suite (2)
- Oracle Supply Chain Products Suite (1)
- Oracle PeopleSoft Products (1)
- Oracle Siebel CRM (4)
- Oracle Communications Applications (1)
- Oracle Retail Applications (3)
- Oracle Java SE (20)
- Oracle Virtualization (8)

Other vulnerabilities, affecting Oracle MySQL, Oracle and Sun Systems Products Suite and Oracle Enterprise Manager Grid Control, are to be delivered tomorrow, but these cannot be exploited without a username and password. Notable is the fact that users running Windows XP will also receive security updates for Java 7, despite the operating system becoming obsolete in April, this year. However, users will no longer receive official support from Oracle. Henrik Stahl of Oracle made this issue clear in a blog post last week, informing that the company announcement saying that official support for Windows XP had been interrupted was mis-interpreted. By removing official support for the obsolete platform the company is no longer required (and may not be able) to issue a patch or a workaround for an issue encountered by a customer on Windows XP, and they will have to reproduce it on a newer platform, starting with Windows Vista. Java 8 does not include support for XP, and Oracle knows that there are problems with the installer. Nevertheless, Stahl says that the company is "looking at possible ways to address this issue but may decide not to - if you are on Windows XP it's not clear that it's worth updating to Java 8 without also updating the OS." The vulnerabilities listed in the pre-release announcement for this quarterly patch update are not necessarily identical with the ones actually delivered by the developer. Inconsistencies may occur due to changes caused by new information. The total number of products that are targeted with this set of fixes amounts to hundreds, since many of the listed entries are actually suites containing multiple applications. Oracle strongly recommends customers to apply these updates due to the serious risks that a successful attack may pose. Based on this pre-release announcement, customers can prepare their machines in advance for receiving the updates in order to avoid unnecessary trouble. The previous quarterly update was released in April and contained a total of 104 fixes.To read more click HERE

Massive Malware Campaign Steals Everybody's Passwords

Tom's Guide, 15 Jul 2014: Who, or what, is NightHunter? And what do they — or it — want? Security researchers discovered last week that for the past five years, a mysterious group has been stealing user credentials from Facebook, Dropbox, Skype, Amazon, LinkedIn, Google, Yahoo, Hotmail, the Indian Web portal Rediff and several banks. Dubbed NightHunter, the campaign appears to have amassed an enormous database of stolen information. The goals of the attacks remain unclear. NightHunter appears untargeted, simply interested in collecting as many user credentials as possible, according to Santa Clara, California-based security company Cyphort, which discovered and named NightHunter. The NightHunter campaign involves several different types of keyloggers, including Predator Pain, Limitless and Spyrex. What sets NightHunter apart — and has made it so difficult to trace — is the fact that the keylogging malware relays its captured data back to the criminals in an unusual way: by emailing it. Most malware communicates with its operators using Web protocols such as HTTP or Internet Relay Chat. But the NightHunter malware uses the email protocol SMTP, which has been around since 1982. NightHunter's preferred method of infecting target computers appears to be via phishing emails, Navaraj says. These emails are sent to personnel in the finance, sales or HR departments of all sorts of large companies and organizations, and bear .doc, .zip or .rar attachments, sometimes with fake IDM or 7zip installers bundled in. Some of the phishing emails are crafted to appear to be from goods-resale agents. In addition to logging user keystrokes, the NightHunter malware also gathers and relays information about the Web browsers, instant-messaging and email clients, password managers, Bitcoin wallets or video games present on an infected computer. Since 2009, NightHunter has amassed such an enormous database of stolen credentials from the abovementioned online services that, according to Cyphort, whoever is behind the campaign is in a position to do some serious damage. "The potential for analyzing and correlating the stolen data to mount highly targeted, damaging attacks is high," Navaraj wrote in the blog post. "The actors behind NightHunter can use the trove of stolen credentials to leverage big-data analytics and enable new cyberthreats, for purposes of extortion, credit card or bank fraud, stealing state secrets or corporate espionage." To read more click HERE