THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

2 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

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

June 30, KENS 5 San Antonio – (Texas) **Metro Health reports immunization records theft.** The San Antonio Metropolitan Health District notified about 300 patients June 30 that their immunization records and personal information were stolen May 30 when a City of San Antonio-owned laptop was reported missing. Authorities are investigating the incident and do not believe the data was a target for the theft. Source: http://www.kens5.com/news/Metro-HEalth-reports--265272641.html

July 1, Help Net Security – (International) **Microsoft disrupts malware networks and APT operations.** Microsoft's Digital Crimes Unit seized 22 free domain names operated by No-IP.com due to the domain names allegedly being used by the NJrat and NJw0rm families of malware. No-IP stated that the Microsoft takeover and rerouting of traffic through sinkholes has also disrupted legitimate customers' service. Source: http://www.net-security.org/secworld.php?id=17071

July 1, Computerworld – (International) **Apple patches iOS, OSX and Safari on mega Monday.** Apple released updates June 30 for its iOS mobile operating system, OSX operating system, and Safari Web browser, closing 44 vulnerabilities in iOS, 19 in OSX, and 12 in Safari. Source: http://www.computerworld.com/s/article/9249480/Apple_patches_iOS_OS_X_and_Safari_on_Mega_Monday

June 30, Softpedia – (International) **A lighter ZeuS is discovered.** Researchers with Fortinet identified a new variant of the Zeus trojan named Zeus Lite that has fewer functions than previous versions but contains improved encryption and the ability to control infected systems. Source: http://news.softpedia.com/news/A-Lighter-ZeuS-Is-Discovered-448940.shtml

July 1, Softpedia – (International) **Houston Astros' systems breached, trade talks revealed.** An unauthorized individual accessed confidential information, including content related to internal trades, stored on an online database created by the Houston Astros baseball team as a means of confidential communication. Team officials are working with the FBI to investigate the incident, but believe the intrusion may be due to a weak password. Source: http://news.softpedia.com/news/Houston-Astros-Systems-Breached-Trade-Talks-Revealed-449040.shtml

Microsoft is testing a fix for Windows 8.1 upgrade woes
EnGadget, 1 Jul 2014: There are many Windows 8 and RT users who want to upgrade to Windows 8.1 and RT 8.1, but can't; a glitch has kept a seemingly random batch of PCs from installing this latest revision through the Windows Store. Thankfully, relief is in sight. Microsoft tells SuperSite for Windows that it's testing a patch which automatically upgrades these stubborn computers to their respective 8.1 releases. If you're eligible, you only need to check Windows Update (not the Store) to get the ball rolling. Microsoft isn't saying if and when the fix will spread worldwide, but it likely can't come soon enough if you're stuck with outdated software. To read more click **HERE**

Self-Spreading Cridex Variant Detected

Softpedia, 2 Jul 2014: Security researchers have discovered a new version of the Cridex malware that includes a self-replicating component and sends phishing emails based on a database of 50,000 stolen SMTP credentials. Dubbed Geodo, the Cridex variant is as bad as the original when it comes to stealing information from an infected computer, and it exfiltrates sensitive data such as email credentials and banking details. A blog post from Seculert CTO, Aviv Raff, says that the new strain basically turns "each bot in the botnet into a vehicle for infecting new targets." A sample was analyzed, and the researchers concluded that once Geodo infects a computer, it downloads another malicious file that communicates with the command and control server (C&C), which sends it a database with about "50,000 stolen SMTP account credentials including the related SMTP servers to connect to." The addresses are spammed with 20 legitimate-looking emails at a time, and the C&C provides a unique sender address, subject line and body text for each batch. This makes it possible for the cybercriminals to launch different phishing campaigns, which adds to a higher rate of success. According to Seculert, the country of origin for the stolen SMTP credentials is Germany (46%). Additional evidence sustaining that the German citizens are targeted by the threat actors behind Geodo is the fact that the emails are written in German. They contain a link that leads to downloading a ZIP archive with an executable masquerading as a PDF file; opening it installs Geodo on the computer and the perpetuating cycle is initiated. Given that the threat is capable of stealing email credentials, the number of SMTP credentials can increase with new entries added from the botnet itself. "There is no definitive information on where the 50,000 stolen credentials came from, but Cridex is the suspected culprit. And as a data stealer, Geodo can compromise the intellectual property of a corporation, putting its business and reputation at risk. This new email worm capability displayed by Geodo serves to further emphasize the growing threat of advanced malware to today's enterprises." Cridex, also known under the names of Feodo and Bugat, has been designed to steal sensitive information, including personal details, online banking credentials, as well as login credentials for social networking websites. It includes the capability to update itself and some samples rely on Domain Generation Algorithm (DGA) to constantly change the command and control addresses it connects to. To read more click **HERE**

HotelHippo Website Down for Security Reasons

Softpedia, 2 Jul 2014: Recently, the website for the HotelHippo hotel booking service has been taken offline to remedy some security risks that caused leaking of customer information. Security consultant Scott Helme found a myriad of security flaws when trying to book a hotel room through HotelHippo.com, owned by HotelStayUK. The flaws he observed would allow a cybercriminal to extract customer data regarding the hotels booked by a potential victim, the duration of the stay, the rooms reserved, and the number of persons they would be traveling with. All this information could be obtained despite the secure connection it was provided through. The flaw consisted in the fact that the secure URL address contained the booking reference number, which was created sequentially. Loading the page with a changed number offered access to the aforementioned booking details of other customers. It appears that the reference number was also present in the link with payment details, which provided the name of the customer, along with the billing address. The security flaws go even further, as Helme discovered that the booking information sent in the confirmation link is received via an insecure connection. The details available included the hotel booked, the cost of the rooms, the number of rooms and customers, as well as check-in and check-out dates. However, the worst of all was the fact that the booking reference number was also present in the link, which allowed pulling out all this information from other customers, too. With all these details at their disposal, cybercriminals can run phishing attacks on the victim in order to get credit card information, or they can plot a burglary, since they know the exact address and the time interval the owners are gone. Helme also checked if the website administrators had enforced protection against crawling agents that index information, such as the one from Google. It turns out that the robots.txt file did not impose any restriction, and crawlers could move freely on any area of the website, indexing even information that was supposed to be private. The security consultant ran a Google search, which revealed a link to payment details containing a booking reference number. Scott Helme contacted HotelHippo via

phone and email on June 25, as soon as he found the security flaws, but the company representatives did not reply. The website was taken offline only after the company was contacted by the BBC about the security measures. "Whilst I have to applaud them for taking the affected areas of the site offline at that time, it shouldn't have to get so far before companies start taking responsible disclosures seriously," said Helme. To read more click **HERE**

Russians Get Closer to Forcing Foreign Internet Companies to Store Locals' Data in the Country

Softpedia, 2 Jul 2014: A massive wave of blocked sites is on its way in Russia, as the government is moving one step closer to banning all online services that don't store content within its borders. This isn't exactly a surprise considering that there have already been warnings about Russia taking steps in this particular direction, especially following the NSA revelations, which they use as an excuse to copy off China's book of rules. The first bill requiring that personal data of Russians be stored inside the country passed the Russian State Duma yesterday. If it manages to get all the stamps of approval, all non-Russian companies will be forced to find a way to store local data in the country. This means that Facebook, Google, Yahoo and any other service, including apps, that doesn't come from Mother Russia, but is used by locals, will need to put physical servers inside the country. What's more, all these companies wouldn't even be allowed to send data outside the country unless they can guarantee for the data stored in Russia. The bill states that when personal data is collected, the operator is required to provide a guarantee that the collection, storage, updating and retrieval of personal data on citizens of the Russian Federation is held in data centers on the territory. Unless companies comply, access to these services will be restricted. The new law is said to take effect in September 2016 if it passes all political hurdles, which means that all these companies would have plenty of time to build data centers within the country. The changes would not only represent a big inconvenience to tech companies around the world, but there would also be huge costs. While this isn't the first time the idea of storing a country's data locally has been thrown around, it has, in the past, been deemed unrealistic because of the huge costs of implementing it. Russians peg national security as one of the reasons for desiring to close off Internet access to some of the biggest companies in the world unless they comply with the new rules, but in recent months, the country's government has given signs of moving more towards controlling Internet access as a whole rather than just to foreign sites. To read more click **HERE**

Sony Recalling VAIO Flip Laptops Due to Fire and Burn Safety Risks

Softpedia, 2 Jul 2014: Now here's an awkward situation. Remember that back in April Sony made an announcement saying an estimated 26,000 units of its VAIO Fit 11A laptops could be affected by battery problems, and it advised owners to stop using the products asap. However, the majority of the products being targeted by the announcement was owned by customers located in the Asia-Pacific region and Japan. Even as Sony has sold off the VAIO branch to a Japanese company, it still has to take care of the products its launched under the banner. With this in mind, the US Consumer Product Safety Commission has issued a warning to customers who have acquired the Sony VAIO Flip PC with model / product number SVF11N13CXS. Owners are urged to stop using the device immediately, shut it down, and contact Sony in order to receive a full refund or just get the machine fixed. Like in yesterday's story with the Dell Inspiron laptop which blew up, the VAIO Flip's battery can overheat, resulting in fire and burn hazards. The notice reads: "Sony is aware of four incidents, which occurred in Asia, of computers overheating, resulting in units smoking, catching on fire and melting. No injuries have been reported." The affected laptops were sold in the US between the months of February and April 2014 for $800 / €585 a pop. The products were sold in three color models, including silver, black and pink and took advantage of a Panasonic-made lithium-ion battery. The Flips also had a folding 11.6-inch touchscreen, backlit keyboard, and it offers Intel Core i5 and i7 Haswell processor options. To determine whether your VAIO Flip is among the affected units, owners should check the black label with white lettering on the underside of the screen. There you should find the model and serial numbers. To find the label, you'll have to open the computer, move the switch from the lock and flip the display. Customers with a faulty VAIO Flip can go ahead and contact Sony over the phone or online. It appears around 680 models have been affected in

the US. As you might be well aware, Sony has sold off the VAIO line to a Japanese company, and as we told you yesterday, the two first models arriving without the Sony banner have already been launched in Japan. Sadly, the new products are all-too reminiscent of what Sony had to offer. To read more click **HERE**

EMET Protection Disabled by Publicly Available Exploit

Softpedia, 2 Jul 2014: The latest stable version of Microsoft's Enhanced Mitigation Experience Toolkit (EMET) has been found to be susceptible to public exploits, which can completely disarm its protection. Researchers at Offensive Security selected an older exploit that leveraged a weakness in the way Internet Explorer 8 handled the objects in memory in order to bypass ASLR (address space layout randomization) and DEP (data execution prevention) security features, and they altered it to disable the protection offered by EMET. Using the original exploit, the researchers hit a couple of dead ends because EMET thwarted their attempts to run arbitrary code through HeapSpray and StackPivot mitigation techniques. Since bypassing the protections one by one did not seem like a valid approach, they started to think of a way to disable all of them at once, by disarming EMET. They found a global variable in the ".data" section in "EMET.dll" that can turn on or off all ROP (return-oriented programming) protections at runtime. Eliminating it completely would cause all ROP mitigations implemented by EMET to be disabled. "This requires an attacker to build a ROP chain that will dynamically retrieve the base address of EMET.dll and overwrite the global variable with a zero," the Offensive Security post says. The method worked in the debugging environment and the command-line became available, but running the exploit outside the debugger caused EAF (export address filtering) to kick in. However, since there are various methods to disarm EAF, the researchers continued the experiment and managed to get shell access outside the debugger. The entire exploit code for disarming EMET 4.1.x is publicly available. The exploit affects Internet Explorer 8 and has been tested on Windows 7, which appears to be the prevalent combination among computer users. According to statistics provided by NetMarketShare, Internet Explorer 8 accounts for 21.25%, the largest chunk of the total browser market, followed at a safe distance by IE 11. They also put Windows 7 in the lead as far user preference of the operating system is concerned, with a market share of 50.55%. Although Offensive Security has not encountered such an exploitation method for disabling EMET in the public database, they do believe that Microsoft is well aware of the possibility because they plugged the holes in the upcoming version of the security kit. They label EMET as a good tool that can challenge exploit developers, but it should not be regarded as a full solution. "What this shows is that while EMET is definitely a good utility and raises the bar for exploit developers, it is not a silver bullet in stopping these types of attacks," they say. To read more click **HERE**

Hackers Change Physical Education Records, Get Prosecuted

Softpedia, 2 Jul 2014: Two students at a university in Shanghai were charged with damaging a computer network after breaching the computer systems of the educational institution in order to modify information regarding the physical education course. With entrepreneurship running through their veins, the duo, studying at the Lixin University of Commerce in Shanghai, found a simple way to make some easy money, about $4,000/€2,900 (25,000 yuan). One of the requirements of the university is for male students to complete twenty 1,500-meter-long runs per semester, while females have to complete 18 runs. The data is recorded in the database by swiping a card upon starting and completing the run. Not completing the number of runs leads to failing the physical education course. Students Zhou and Cao started to put together a business that would earn them constant revenue from customers that needed their run records altered. Zhou feared that he would fail the course, and to avoid it, he accessed the database without authorization and modified the records. Some colleagues found out and offered him money to do the same for them. Cao learned about the business and offered to help Zhou by gathering customers for a cut, leaving him more time for the hacking. The lucrative activity lasted for four months and each hack was charged about $3/€2 (20 yuan). The university finally caught wind of the deed and reported the two students to the police. In their defense, they said that they knew it was wrong, but they never imagined the act was a crime. To read more click **HERE**

Cyber-Attacks On the Rise in Iraq

Softpedia, 2 Jul 2014: Malicious cyber-incidents started to record an upward trend, with activity concentrating in Baghdad, Erbil, Basra, and Mosul. Los Angeles-based cyber-threat intelligence firm IntelCrawler reports that the malicious activities within the Iraqi ISP sector have intensified in the last two months and that multiple new botnets have emerged. Attackers rely on dynamic DNS services to communicate with the infected machines. Based on the recent geo-political conflicts in the area, the company speculates that these computers could have been used in cyber-espionage campaigns and targeted multi-stage attacks. IntelCrawler says that many of the malicious domain names used as command and control servers were registered with free public DNS providers. "The resolved IP addresses were related to subnets of various regional ISPs in Iraq, such as GORANNET, IQ-EARTHLINK, IQNETWORKS, IQ-NEWROZ and IQ-TARINNET," says the company in a blog post. A chart showing the malicious activity recorded per ISP puts GORANNET ahead of others. The strongest malicious activity has been recorded in Baghdad, with more than 50%, followed at a safe distance by Erbil, Basra, and Mosul. As far as the threats used for malicious purposes are concerned, the security firm notes numerous remote administration toolkits "using Secure Sockets (SOCKS) and FTP/HTTP BackConnect with embedded file system browser for infected victims remote monitoring masked under Google Chrome and publicly available software." It seems that Microsoft's recent seizure of 23 No-IP domain names has contributed to decreasing the malicious activity in the area because the cyber-attacks were conducted using NJrat as well. NJrat is part of the Bladabindi malware family, which has been under close monitoring from Micrososft since December 2012. Recently, the Redmond company served a federal court order to No-IP that allowed it to route traffic through its own infrastructure in order to identify bad traffic and sinkhole it to interrupt communication between the infected machine and the command and control server. This particular type of threat has been observed during the Syrian conflict, employed against the Syrian opposition groups. Small Office/Home Office (SOHO) routers in the IPv4 range of Iraq have been compromised by exploiting flaws in UPnP and through brute-forcing techniques. The attacks were targeted and a potential risk is mass network traffic surveillance. "The share of Iraqi-based bad actors involved into various illegal activities in cyberspace acting as mercenaries seems to have significantly increased. Most appear united with Egypt, Lybian, Lebanese, Iranian, Syrian and various distributed Islamic groups performing targeted attacks because of religious and political motivation supported by state parties," reads the report. To read more click **HERE**

Europe and the U.S. Targeted by Jenxcus and Bladabindi Malware

SoftPedia, 2 Jul 2014: Believed to be created by two Kuwaiti and Algerian nationals, the Jenxcus (NJw0rm) and Bladabindi (NJrat) malware families focused mostly on users in Europe in the past 12 months, but they affected the United States, too. At the moment, an accurate number of infected machines is not available, but Microsoft's antivirus products detected different variants of the malicious items on at least 7,486,833 computers. Microsoft made available a map with the global impact of the two threats, and users in Europe are the most affected. It appears that the most detections have been recorded in France, the United Kingdom, Germany, Italy, Netherlands, Belgium and Austria. As far as the risks of an infection with Jenxcus and Bladabindi are concerned, sensitive information would be extracted from the victim's computer and sent to remote machines under the control of cybercriminals. The data collected consists not just of credentials for web services, as Bladabindi includes logging components and it can also control the built-in webcam to take snapshots and record without user permission. Furthermore, some variants come with remote-control capability. They can increase in functionality and conduct more complex illegal activities by downloading other malware components from the command and control center. The attack vectors employed by the cybercriminals are diverse and range from social engineering techniques to bundling the malicious component into programs and video files in torrent downloads. Most of the times, cybercriminals try to lure the victim to a malicious address via email messages or posts on social networks. In some cases, the malware is purported as a Flash update that needs to be installed. The two malware families are not new on the computer security scene, as their activity has been observed by researchers since 2012, Bladabindi making an appearance in July and

Jenxcus stepping in in December. However, they managed to evade takedown action until Monday, June 30, when Microsoft seized a total of 23 No-IP domain names involved in facilitating communication between the infected machines and the command and control server of the malware. As a result, Microsoft can identify the bad traffic and direct it to a sinkhole in order to disrupt the malicious activity. According to a post from Microsoft, there is plenty of information online that can be used by anyone to create their variant of the threat. "This makes Bladabindi and Jenxcus a bit different from the previous botnets we have seen. A traditional botnet usually has one command-and-control (CNC) server to control all infected machines. In the case of Bladabinda and Jenxcus there can be a syndicate of botnets and thousands of botnet herders," says the post. To read more click **HERE**