Counterintelligence Working Group NEW MEXICO

NMCIWG Purple Arrow

The Cyber Shield

Cyber News for Counterintelligence / Information Technology / Security Professionals

4 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 1, Reuters – (International) **Two U.S. hackers admit to international cyber crime in N.J. court.** Two New York men pleaded guilty April 1 in federal court in New Jersey to their roles in an international cybercrime and bank fraud ring that hacked into several financial services businesses and institutions and attempted to steal around $15 million by diverting funds to accounts and payment cards that they controlled. The alleged leaders of the ring are Ukrainian citizens and remain at large. Source: http://www.reuters.com/article/2014/04/01/usa-crime-cybercrime-idUSL1N0MT23O20140401

April 3, Threatpost – (International) **Yahoo encrypts data center links, boosts other services.** Yahoo announced April 2 that it has begun encrypting all traffic moving between its data centers, turned encryption on between its email servers and others who support the SMTPLS standard, and turned on encryption on its home page, searches, and other properties to enhance user privacy and security. Source: http://threatpost.com/yahoo-encrypts-data-center-links-boosts-other-services/105228

April 3, Softpedia – (International) **Cybercriminals add new component to Sality to hijack the DNS addresses of routers.** Researchers at ESET analyzed a new component of the Sality malware that was recently added and allows the malware to hijack the primary DNS address of routers. The analysis showed that the malware targets specific router models and attempts to use a brute force attack to gain administrator access, and then changes the router's DNS server address in order to direct users to fake installation sites. Source: http://news.softpedia.com/news/Cybercriminals-Add-New-Component-to-Sality-to-Hijack-the-DNS-Addresses-of-Routers-435654.shtml

April 3, Softpedia – (International) **ISPs exposed to DNS DDoS attacks due to millions of vulnerable home routers.** Researchers at Nominum reported finding over 5.3 million routers have open DNS proxies, which can put Internet service providers at risk of DNS amplification distributed denial of service (DDoS) attacks. Source: http://news.softpedia.com/news/ISPs-Exposed-to-DNS-DDOS-Attacks-Due-to-Millions-of-Vulnerable-Home-Routers-435608.shtml

ACLU Creates Database of Leaked NSA Files
SoftPedia, 4 Apr 2014: The American Civil Liberties Union (ACLU) wants to make sure that nothing is forgotten about what the NSA is doing, so the Snowden documents that have been reported on thus far have been gathered in a database. The NSA Documents Database is a searchable and categorized database that contains over 200 previously classified documents and which includes files from Edward Snowden and other newly declassified files from the intelligence agency. "The ACLU and others have long suspected that the National Security Agency has gone far beyond its mandate of gathering information for counterterrorism and foreign intelligence purposes, implementing a massive spying system to conduct bulk surveillance of hundreds of millions of innocent Americans," the ACLU writes. The organization mentions that all of its suspicions were confirmed on June 5, 2013, when the first series of documents from the Snowden stash made their way online thanks to the Guardian. "Together,

they have triggered a remarkable and long-overdue public debate about the legality and propriety of the government's surveillance practices," the ACLU writes. You can search by keywords and pick the type of legal authority mentioned in the file, such as the FISA Amendment Act or Section 215. The type of file can also be chosen through a series of checkboxes. From here, you can pick to look for internal NSA documents alone, for compliance reports, FISA court filings or reports to Congress, to name just a few. The type of record collection discussed in the file can be picked out as well. For instance, you can choose to look for telephony or Internet metadata, financial records, telephone content and more. The leaked files from Edward Snowden have revealed a lot of questionable practices from the NSA, including the collection of phone call metadata. While one could say that this doesn't give out much information about a person since the content of the conversations isn't (theoretically) included, there are a lot of details that can be discovered by analyzing metadata, including the location, the numbers and identities of your family members, friends and acquaintances, or even your religion and sexual orientation. Other files have revealed that the NSA spies on hundreds of world leaders, as well as organizations such as the United Nation and UNICEF. More concerning files have indicated that the NSA has put in a lot of effort to make sure that the encryption standards are weakened so that it can easily crack open conversations that users thought were protected. To read more click **HERE**

INFOSEC REMINDER: Classified information posted on public facing web sites is STILL considered as classified material by the U.S. government. The introduction of classified material onto unclassified Automated Information Systems (AIS) constitutes an information spill, which requires sanitization processes to be documented/executed by the AIS owner. In most instances, the offending web site should be blocked at the proxy server to prevent employees from creating an information spill – legitimate, multi-purpose web sites like the ACLU that choose to make (potentially) classified information available to the public create additional INFOSEC/leadership challenges to prevent information spills from occurring.

Victims of Experian Data Breach Not Notified Because the Company Can't Identity Them

SoftPedia, 4 Apr 2014: Last year, investigative journalist Brian Krebs revealed that a Vietnamese man running an online identity theft service managed to gain access to the details of hundreds of millions of Americans through an Experian subsidiary. US authorities are said to be investigating the data breach. 24-year-old Hieu Minh Ngo – who has already been arrested and pleaded guilty – had fueled his criminal service with data from US Info Search. This company had an arrangement with Court Ventures according to which they could access each other's data. The Vietnamese man made a contract with Court Ventures, but the company was acquired by Experian in March 2012. Experian failed to notice that anything was amiss for several months after the acquisition. Now, Reuters reports that a number of US states are investigating the incident. Experian representatives have told the media giant that Ngo's access to the data was cut off when the Court Ventures portal was shut down in early December 2012. US authorities haven't revealed if they know how many individuals are impacted by the breach, and no specific cases of data from Court Ventures being used for identity theft have been identified. Experian says that it's working on determining what records are impacted, but so far, neither Experian nor US Info Search has notified customers because they haven't been able to identify those affected by the breach. Ngo was arrested in February 2013 after being lured to the United States by the Secret Service. The operator of the identity theft service was expecting to close a business deal in the US. Last month, the suspect pleaded guilty to wire fraud, access device fraud, and identity theft. He was charged in October 2013. Authorities said he had over 1,300 customers who had paid him around $1.9 million (€1.25 million) between 2007 and the time of his arrest. In the 18-month period before he was arrested, Ngo's customers made around 3.1 million queries on his website. The service offered social security numbers, dates of birth, addresses, phone numbers, email addresses and other data. At his trial, Ngo told the judge that he had some medical problems, namely that he kekepteps hearing voices in his head.

His lawyer said he didn't know anything about his client's issues until that point. Ngo will be sentenced on June 16 and he faces up to 46 years in jail for his crimes. To read more click **HERE**

Windows XP Still Number One in China
SoftPedia, 4 Apr 2014: It's no secret that Windows XP support is coming to an end in just a few days, but it appears that users do not really care about it, as statistics provided by third-party research companies across the world show that many XP users have no intention to upgrade. China, which continues to be one of the largest markets for Microsoft, is still pretty much addicted to Windows XP, which means that Redmond's warnings to upgrade to a newer OS are more or less just a waste of time, at least in this particular market. StatCounter data for the month of March 2014 shows that Windows XP continues to hold the leading spot in China with a market share of 47.13 percent, while Windows 7 comes second with 44.79 percent. This means that these two operating systems are powering no less than 91.92 percent of the desktop computers in the country, even though Microsoft has already launched one new operating system – Windows 8 – and two important updates – Windows 8.1 and Windows 8.1 Update 1. China was one of the countries where Microsoft was rumored to be offering extended support due to the big number of computers still running Windows XP in the country. The company, however, has explained that it applies the same decision to all markets, so Windows XP will be discontinued on April 8 all over the world, unless extended support is purchased. "Microsoft China has taken special actions to closely work with leading Chinese internet security and anti-virus companies including Tencent for them to provide security protection for Chinese Windows XP users before they upgrade to modern operating system," a statement released by Microsoft in early March explained. Microsoft has recently signed a deal with the United Kingdom to provide support for Windows XP for another 12 months, but such an agreement is pretty expensive. The UK, for example, will pay Microsoft £5.5 million ($9.1 million / €6.6 million) in exchange for critical and important security updates for Windows XP, Office 2003 and Exchange 2003. Worldwide, Windows XP is still installed on 28 percent of desktop computers and since end of support is just around the corner, there's no doubt that many PCs will continue to run this OS version beyond April 8. Microsoft warns that everyone still running Windows XP will become vulnerable overnight if an unpatched flaw is found, despite the plethora of security products that will still work on this OS version after retirement. To read more click **HERE**

Windows XP to Get the Final Update on Tuesday
SoftPedia, 4 Apr 2014: Windows XP will be retired on Tuesday and during the same day, it'll also receive the final update that's supposed to correct all issues found in the operating system and thus try to keep users on the safe side as much as possible. The 13-year-old platform is one of the operating systems that are going to receive a critical update on Patch Tuesday, as Microsoft has discovered that Internet Explorer 6, 7, and 8 are all vulnerable to attacks. An important update is also being prepared for Windows XP, but no other specifics have been provided, as Microsoft tries to keep users safe and disclose full details after the release of the updates. Windows XP will be officially discontinued on April 8, so after this date, no other updates and security patches will be released, which means that those who will still be running this particular OS version could become vulnerable to attacks overnight if hackers find unpatched flaws. Microsoft warns that without security updates and fixes, Windows XP computers will be easy to hack, especially because cybercriminals are expected to focus all their efforts on this particular operating system. "Microsoft has provided support for Windows XP for the past 12 years. But now the time has come for us, along with our hardware and software partners, to invest our resources toward supporting more recent technologies so that we can continue to deliver great new experiences," the company said. According to third-party statistics, Windows XP is still installed on nearly 28 percent of computers worldwide, so it's pretty obvious that the transition to another operating system won't be entirely made before April 8, so lots of devices could become vulnerable if unpatched flaws are found. "If you continue to use Windows XP after support ends, your computer will still work but it might become more vulnerable to security risks and viruses. Also, as more software and hardware manufacturers continue to optimize for more recent versions of Windows, you can expect to encounter greater numbers of apps and devices that do not work with Windows XP," the software

giant pointed out. On April 8, Microsoft will also remove download links for Security Essentials with Windows XP support, but existing installations will continue to work just fine and receive updates for at least one more year. Windows XP will also be supported by plenty of third-party security vendors out there, so it shouldn't be that hard to find an anti-virus app that works on your system. To read more click **HERE**

Microsoft Announces Critical Windows, Office Updates
SoftPedia, 4 Apr 2014: Microsoft is getting ready for another Patch Tuesday rollout, this time planning to fix vulnerabilities found in the Windows operating system and the Office productivity suite. A total of four security bulletins will be released on Tuesday, two rated as critical and two considered to be important. As usual, Microsoft hasn't provided any specifics on the vulnerabilities that are going to be fixed by these new patches, but it did mention that both Windows and Office will receive one critical update. All but one version of Internet Explorer will be fixed on Patch Tuesday, as the software giant found a bug that needs to be addressed as soon as possible. Internet Explorer 10 is the only version that's not vulnerable, the company said. As far as Office is concerned, the critical security glitch has been found in all versions of the productivity suite, hence the critical rating offered by the parent company. Just like it happens every month, the security updates will be delivered to computers via Windows Update, so no user input would be required if the computer is connected to the Internet. At this point, it's not yet clear whether Microsoft is also planning to address a recently-found bug in Word that would allow attackers to remotely execute code using a malicious RTF document. The company has already issued a Fix It solution to help users configure their computers to remain protected until it manages to resolve the glitch, so a full-time workaround is expected to be released this Patch Tuesday. Limited attacks have already been confirmed, so it's critical for both users and Microsoft to see the patch getting shipped to computers running MS Word as soon as possible. "At this time, we are aware of limited, targeted attacks directed at Microsoft Word 2010. The vulnerability could allow remote code execution if a user opens a specially crafted RTF file using an affected version of Microsoft Word, or previews or opens a specially crafted RTF email message in Microsoft Outlook while using Microsoft Word as the email viewer," Microsoft recently said in a security advisory. Users are thus recommended to avoid opening suspicious files coming from unknown sources, at least until the full patch is delivered. All versions of Microsoft Word currently supported by the company are affected by this new vulnerability, including Microsoft Word 2003 Service Pack 3, Microsoft Word 2010 Service Pack 1 and 2, and Microsoft Word 2013 in 32-bit, 64-bit, and ARM flavors. To read more click **HERE**

Microsoft Announces Updated Internet Explorer 11 for Windows 7, Windows 8.1
SoftPedia, 4 Apr 2014: Microsoft has completed development of another Internet Explorer update, so everyone should be getting it in the coming days on Windows 8.1 and Windows 7. The same version will also be part of Windows Phone 8.1 when it debuts later this year, the company said. Installed by default on Windows 8.1 Update, the new IE version will come to provide a seamless experience across all devices, comprising WebGL improvements, new enhancements to the F12 developer tools, and a brand new Enterprise Mode aimed at organizations. First of all, the new Internet Explorer 11 version will offer support for both smaller and larger devices, while also working flawlessly in either landscape or portrait modes. "The Web is still front-and-center but new design enhancements make your browsing experience feel like it was made just for your device – like the number of tabs on-screen and the size of the fonts and menus. You can also now control when the browser remains on-screen or hides away for full-screen browsing depending on the type of device you use," Microsoft points out. As far as the developer tools are concerned, the new IE11 version comes with improved UI and Memory tools, while also offering new shortcuts to quickly control specific options from the keyboard. The new Enterprise Mode, which has been spotted in some leaked builds of Windows 8.1 Update that reached the web in the past few months, enables organization to offer backwards compatibility for websites that were designed to work on Internet Explorer 8 or below. This is particularly important for businesses because many are still struggling to upgrade their in-house applications. This fresh build of Internet Explorer 11 for Windows 8.1 and Windows 7 is already up for grabs from MSDN and TechNet, but as you can easily guess, a subscription is needed in order to get

them. Those without a subscription will have to wait until April 8, when Microsoft will deliver the updated browser via Windows Update for all users. April 8 is the day when Microsoft will also start shipping Windows 8.1 Update to users across the world, but also Patch Tuesday fixes supposed to address the vulnerabilities found in the company's software solutions lately. Last but not least, Windows XP is projected to reach end of support on April 8, so the operating system launched 13 years ago will no longer receive updates and security patches as of this date. To read more click **HERE**

Cybercriminals Add New Component to Sality to Hijack the DNS Addresses of Routers

SoftPedia, 3 Apr 2014: The notorious piece of malware known as Sality has been around since at least 2003. However, over the past months, its developers have started adding new functionality, namely a component that's designed to hijack the primary DNS address of routers. Security researchers from ESET have been analyzing this new component, which was first seen at the end of October 2013. The threat, dubbed Win32/RBrute, was first spotted by experts from Russian security company Dr. Web. In the first part of an attack, a component detected by ESET as Win32/RBrute.A scans the Web for various router models. The list includes D-Link, Cisco, Huawei, ZTE and TP-Link routers. Most targeted models are from TP-Link. When one of these routers is identified, the malware downloads a list of IP addresses from the command and control server, and tries to perform a brute-force attack on the device's administration panel.   The C&C server sends the bot a list of around a couple of dozen common or default passwords to try and access the administration page. The list includes "password," "qwerty," "root," "trustno1," "admin," "12345," "123456," "abc123" and "administrator." Once access is obtained, the router's primary DNS server address is changed. By changing the server's address, cybercriminals can redirect users to arbitrary web pages.   ESET experts have found that users whose computers are infected will be redirected to a fake Google Chrome installation site whenever domains containing the words "google" or "facebook" are requested. The fake Chrome pages are set up to distribute Sality. This way, other users that might be relying on the infected router can get infected. "The IP address used as the primary DNS on a compromised router is part of the Win32/Sality network. In fact, another malware, detected by ESET as Win32/RBrute.B, is installed by Win32/Sality on compromised computers and can act either as a DNS or a HTTP proxy server to deliver the fake Google Chrome installer," ESET's Benjamin Vanheuverzwijn explained. Based on their analysis, researchers have determined that the same group of developers is behind both the main file infector and the new components. Experts say that this operation is similar to the one that relied on the notorious DNSChanger, which infected millions of computers worldwide and redirected their owners to arbitrary domains. The number of Sality infections has steadily decreased since 2012. However, around December 2013, a small increase was recorded. This increase coincided with the malware being released in the wild. For additional technical details on this new Sality component, check out ESET's We Live Security blog (**LINK**). To read more click **HERE**