THE CYBER SHIELD

Cyber News for Counterintelligence / Information Technology / Security Professionals

6 June 2014

June 5, Help Net Security – (California) **American Express credit card data exposed.** American Express announced June 2 that over 76,000 cardholders in California may have had their payment card information disclosed in a batch of payment card information exposed by a hacktivist group in March. Many of the cards in the larger March breach appeared to come from older leaks and not from a new breach. Source: http://www.net-security.org/article.php?id=2034

June 5, Nextgov – (National) **Flaw lets hackers control electronic highway billboards.** The U.S. Department of Homeland Security advised transportation operators June 4 of a hard-coded password vulnerability discovered in Daktronics Vanguard highway notification sign configuration software which could allow hackers to gain unauthorized access to the highway signs. The vendor was notified and is working to fix the issue. Source: http://www.nextgov.com/cybersecurity/2014/06/flaw-lets-hackers-control-electronic-highway-billboards/85849/

June 5, Threatpost – (International) **New OpenSSL MitM flaw affects all clients, some server versions.** A security researcher identified a remotely exploitable vulnerability in all versions of OpenSSL that could be used in a man-in-the-middle (MitM) attack to decrypt traffic between vulnerable clients and servers. The researcher reported that the vulnerability appears to have existed in OpenSSL's code since 1998 Source: http://threatpost.com/new-openssl-mitm-flaw-affects-all-clients-some-server-versions

June 5, Softpedia – (International) **Skype users face security risk due to unencrypted data.** Solutionary researchers reported in the company's May Threat Report that Skype users' personal information and chat transcripts could be vulnerable to attackers due to the data being kept in an unencrypted file on the local system in Windows and Linux. The files are hidden by default but could easily be found by an attacker. Source: http://news.softpedia.com/news/Skype-Users-Face-Security-Risk-Due-to-Unencrypted-Data-445414.shtml

BullGuard Warns: Phishing Attacks Spread After Cryptolocker Disruption

SoftPedia, 6 Jun 2014: Earlier this week, the US and European authorities told Internet users that they had managed to crack the malware known as Gameover Zeus that had been used to divert millions to the bank accounts of criminals, as well as Cryptolocker, a viral scam that was used by hackers to obtain control over people's computers and ransomed the data. People were told that they had two weeks to protect themselves against these threats after authorities disrupted the system used by criminals. "Whether you find online security complicated or confusing, or simply haven't thought about keeping your personal or office computers safe for a while, now is the time to take action. Our message is simple: update your operating system and make this a regular occurrence, update your security software and use it and, think twice before clicking on links or attachments in unsolicited emails," said Andy Archibald, deputy director of the national cyber crime unit at the National Crime Agency in the UK. Bullguard, a global software company that provides Internet security and antivirus protection, has detected a wave of malware-ridden spam that pretends to be a CryptoLocker file decrypter, and it advises people not to waste time before installing a security solution. While these viruses can no longer be used to steal information and encrypt files as long as the communication with the command and control servers is cut, other malware

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 writers are currently taking advantage of the frenzy. Massive phishing campaigns have been spotted and viruses are already being distributed as attachments to spam emails. Some of these are delivered under the false pretense that they are a Cryptolocker file decryption tool. Since Cryptolocker has used a strong encryption method that cannot be cracked, it means that there is no such tool out there. Those who do receive such emails should be aware that they are certainly spam and that they really shouldn't click on the links or download the files. The so-called file decrypter is in fact malware. The tool pretends to be a registry cleaner that will automatically detect severe issues even if there is none there. The trick is to get the victim to buy the software. Doing so won't just leave your wallet a lot lighter, but it will also put your personal information and banking details in danger. "People should not be tricked: if they pay for this software, the only outcome is that they will help Cryptolocker and GameOver Zeus indirectly cause more financial damage. And the situation will certainly escalate and more dangerous viruses will be marketed as Cryptolocker file decrypters. The only viable solution is to have a powerful security suite installed, which both detects and prevents such malware, and also to regularly backup your files," writes BullGuard. To read more click HERE

Microsoft Announces Windows and IE Security Updates, Windows XP Left Out Again

SoftPedia, 6 Jun 2014: Microsoft will launch a set of seven different security updates next week, as part of its monthly Patch Tuesday rollout, with Windows XP again to be left out and thus not getting any improvements that could block potential exploits. In the advance notification for this month's Patch Tuesday updates, Microsoft said that two of the vulnerabilities it found are critical and affect Internet Explorer, Windows, and Office. The first bulletin is supposed to address a critical security flaw in all versions of Internet Explorer, including the very latest Internet Explorer 11 on Windows 8.1. No other details have been provided right now, as Microsoft still wants to keep users protected until it officially rolls out the patches. A second bulletin is supposed to repair a critical hole in Windows and Office. The remote code execution vulnerability exists in the majority of versions, with the exception of Office 2013. The remaining five bulletins are considered to be of a critical severity rating and are supposed to address flaws in Office and Windows, the company revealed. As you can see, Windows XP is again left out of Patch Tuesday, after the software giant pulled the plug on it on April 8. XP computers won't be getting any other updates, which makes users still running it even more vulnerable because some of the vulnerabilities found in the other Windows versions could also exist on Windows XP. The difference is that all the other Windows builds will actually get patches, while XP systems are left vulnerable to attacks. Microsoft has been telling the same thing for months, warning that once support comes to an end, Windows XP computers are very likely to become hackers' preferred target due to the large market share this operating system still owns. "For starters, it'll become five times more vulnerable to security risks and viruses, which means you could get hacked and have your personal information stolen," Microsoft said. "While it's true that you can keep using your PC with Windows XP after support ends, we don't recommend it." And still, that doesn't necessarily mean that users are ready to give up on Windows XP. Stats released earlier this month indicate that more than 25 percent of the desktop computers worldwide are still running it right now, despite the many warnings released by Microsoft in the last couple of years. Windows XP's market share, however, is expected to drop significantly in the coming months, especially because many large companies with thousands of computers are projected to complete the transition to a newer operating system by the end of the year. To read more click HERE

UK government proposes life sentences for hackers

Heise Security, 6 Jun 2014: Hackers in the UK could be in for a world of problems, as the UK government is looking to hand out life-long prison sentences to those who are found guilty of organizing and executing devastating cyber attacks, reported The Guardian. In Wednesday's speech from the throne, the British Queen talked about a number of issues that will be on the UK government's agenda for the coming parliamentary session, and among them were changes to the Serious Crime Bill. Among other things, the new bill would "create a new offense of possessing 'pedophilic manuals'" (with a maximum three year sentence), and "amend the Computer Misuse Act 1990 to ensure sentences for attacks on computer systems fully reflect the damage they cause." Hackers who perform "cyber-attacks which result in loss of life, serious illness or injury or serious damage to national security, or a significant risk thereof" could be facing a lifetime in prison under the new bill. Harsher sentences have also been proposed for those found guilty of cyber espionage, especially when it comes to industrial espionage, and for those whose attacks create "a significant risk of severe economic or environmental damage or social disruption." For the latter offense the current maximum sentence is 10 years, and the government is looking to make it 14. To read more click HERE

Estimating the cost of a cloud data breach

Heise Security, 5 Jun 2014: IT and security professionals expect cloud services to multiply the likelihood and economic impact of data breaches as they pervade the enterprise. They also reveal that the scope of usage and responsibility for securing cloud services remains largely unknown among IT, according to Netskope. The report draws upon Ponemon Institute's May 2014 Cost of a Data Breach study that established a cost of $201.18 per lost or stolen customer record. For a data breach involving 100,000 or more customer records the cost would come to just over $20 million. Survey respondents were asked to estimate the current probability of a data breach of that magnitude and then how increasing the use of cloud services would change that probability. The report states that this multiplies the probability of a data breach by as much as 3x. "With a $201 price tag for every record lost, the cost of a data breach of just 100,000 records is $20 million. Imagine then if the probability of that data breach were to triple simply because you increased your use of the cloud. That's what enterprise IT folks are coming to grips with and they've started to recognize the need to align their security programs to account for it," said Sanjay Beri, CEO and founder of Netskope. "We've been tracking the cost of a data breach for years but have never had the opportunity to look at the potential risks and economic impact that might come from cloud in particular," said Dr. Larry Ponemon, Chairman and Founder of Ponemon Institute. "It's fascinating that the perceived risk and economic impact is so high when it comes to cloud app usage." Across the board, respondents believe that their high-value IP and customer data are less secure when the use of cloud services increases. Respondents said they believe there is a lack of due diligence in the implementation and monitoring of security programs within companies and have uncertainty about cloud service provider security practices, while recognizing that there are unknown cloud services in a network. This all leads to the general perception that the probability of a data breach is increasing in today's IT environment.

- Respondents estimate that every 1 percent increase in the use of cloud services will result in a 3 percent higher probability of a data breach. This means that an organization using 100 cloud services would only need to add 25 more to increase the likelihood of a data breach by 75 percent.
- More than two-thirds (69 percent) of respondents believe that their organization is not proactive in assessing information that is too sensitive to be stored in the cloud.
- 62 percent of respondents believe the cloud services in use by their organization are not thoroughly vetted for security before deployment.
- Almost three-quarters (72 percent) of respondents believe their cloud service provider would not notify them immediately if they had a data breach involving the loss or theft of their intellectual property or business confidential information, and 71 percent believe they would not receive immediate notification following a breach involving the loss or theft of customer data.
- Respondents believe 45 percent of all software applications used by organizations are in the cloud, but exactly half (22.5 percent) of these applications are not visible to IT.
- Respondents estimate that 36 percent of business critical apps are based in the cloud, yet IT lacks visibility into nearly half of them.
- Ponemon Institute surveyed 613 IT and security practitioners in the U.S. who are familiar with their company's usage of cloud services. The web-based survey was fielded in March of 2014.

To read more click HERE

Hagel pushes open dialogue with China on cybersecurity Fierce Government

IT, 4 Jun 2014: Although China has stopped participating in the U.S.-China Cyber Working Group, U.S. officials would still like to pursue an open discussion on core issues that will benefit both parties, said Defense Secretary Chuck Hagel. China opted out of participation in the working group when the Justice Department brought cyber espionage charges against members of the People's Liberation Army May 19. The working group was a collaborative effort to strengthen cybersecurity. Knowing which programs your agency should support doesn't have to be a guessing game. Learn how you can align projects with strategic goals, balance spending and assess risk with Oracle's Primavera Portfolio Management's enterprise approach to governance. Download Now. In a May 31 speech delivered at the IISS Shangri-La Dialogue in Singapore, Hagel emphasized the importance of maintaining an open dialogue with Chinese officials that would focus on "getting at the real issues and delivering more results." Hagel said relations with the Chinese are part of a larger, U.S. strategy to foster economic stability and security as well as continue the legacy of "Asia-Pacific's rules-based order" in the region. He expressed the need to establish a "regional security architecture" that can grow and adapt as technology progresses. To read more click HERE

Agencies fail to consistently apply cyber response practices

Fierce Government IT, 2 Jun 2014: Across the board, major federal agencies are not consistently responding to cyber incidents, such as computer network breaches. About 65 percent of the time agencies aren't completely documenting actions taken in response to detected incidents, concludes the Government Accountability Office with 95 percent confidence. The findings come as part of a report released publicly May 30. Only sometimes do agencies identify the scope of the incident, most frequently they won't determine the impact of an incident and they often fail to demonstrate post-incident actions to prevent recurrence, find auditors. In a recent survey on Federal IT Reform, Senior government IT executives laid out their vision for the coming year, detailing challenges and identifying priorities. After a closer review of just six selected agencies, GAO determined that cyber incident response policies, plans and procedures were only partially developed and didn't fully comply with federal requirements. For more, download the report, GAO-14-354 (.pdf). To read more click HERE

Security controls lacking across VA networks, finds IG

Fierce Government IT, 1 Jun 2014: A material weakness still exists in the Veterans Affairs Department's information security program, concludes the department's inspector general in its annual Federal Information Security Management Act audit. VA has not fully implemented security control standards on all of its servers and network devices, leading to weaknesses in access and configuration management controls. The department also has no process to review and remediate its system security vulnerabilities, finds a May 29 VA office of inspector general report. "VA has not remediated approximately 6,000 outstanding system security risks in its corresponding Plans of Action and Milestones to improve its overall security posture," write auditors. Knowing which programs your agency should support doesn't have to be a guessing game. Learn how you can align projects with strategic goals, balance spending and assess risk with Oracle's Primavera Portfolio Management's enterprise approach to governance. Download Now. The report makes a total of 35 recommendations for helping achieve better FISMA outcomes – five of which are carry-overs from previous years' audits. Authors say FISMA is a challenge for the department due to the nature and maturity of its IT systems. The effect of these open recommendations should be considered in next year's assessment of VA's security posture, say report authors. "We remain concerned that continuing delays in implementing effective corrective actions to address these open recommendations can potentially contribute to reporting an IT material weakness from this year's audit of VA's Consolidated Financial Statements," write auditors. For more: - download the report, 13-01391-72 (.pdf). To read more click HERE

Obama administration satisfied with cybersecurity regulations

Fierce Government IT, 27 May 2014: The Obama administration doesn't need to develop new cybersecurity regulations, a review by the administration has concluded. That conclusion doesn't apply to independent regulators, such as the Federal Energy Regulatory Commission, which are responsible for much of the nation's critical infrastructure. The review stemmed from an executive order, which can only apply to agencies under the purview of the White House. The departments of Health and Human Services and Homeland Security, as well as the Environmental Protection Agency, were subject to the order. All three agencies concluded that voluntary implementation of the cybersecurity framework that the National Institute of Standards and Technology released in February would suffice for now. "At this time...existing regulatory requirements, when complemented with strong voluntary partnerships, are capable of mitigating cyber risks to our critical systems and information," said Michael Daniel, the White House cybersecurity coordinator, in a May 22 blog post. Daniel did note though that going forward, the administration may try to improve the clarity of existing cybersecurity regulations and coordination among agencies. For more:

- read the White House blog post
- read the HHS report
- visit the download page for the three DHS reports
- download the EPA report (pdf)

To read more click **HERE**