[redacted] Cyber-Threat Newsletter – 04 Jan 16

(b)(3) 10 USC § 424

Patches & Updates of the Week:

(U) Microsoft issues patches for Flash in Explorer and Microsoft Edge
(U) Following Adobe's patch for 19 vulnerabilities in Flash this week - including a critical zero-day that could be exploited by attackers to take control of the affected computer - Microsoft issued its own patch to address Flash vulnerabilities that affect Internet Explorer and Microsoft Edge. The affected software includes Flash Player in Internet Explorer in Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10, and Windows 10 version 1511. Microsoft noted in its updated security advisory that the KB3132372 patch updates "Adobe Flash libraries contained within Internet Explorer 10, Internet Explorer 11, and Microsoft Edge." Earlier this month, Adobe issued 78 patches for its several Adobe products including Flash. The company's patch this week was ahead of schedule. Adobe was not scheduled to issue an update until January 16. (scmagazine.com, 31Dec15)

(U) IBM patches vulnerability in SPSS Statistics software
(U) An IBM SPSS Statistics scripts permissions error can allow local users to gain elevated privileges, the company is reporting. IBM's bulletin reported the vulnerability (CVE-2015-7489) on December 29. The report said the issue impacts IBM SPSS Statistics versions 22.0.0.2 and 23.0.0.2, which use a python scripts that have write permissions to Everyone. This would allow a local user to add malicious OS commands to the python code. "These command will later be executed in case another user (for example an administrator) opens SPSS and uses that module," IBM said in the bulletin. IBM has issued interim fixes, 22.0.0.2-10 and 23.0.0.2-7 23.0.0.2-7, for both versions of the affected software. IBM SPSS Statistics is a family of analytical products to include planning, data collection and analysis. (scmagazine.com, 31Dec15)

Threats & Vulnerabilities of the Week:

(U) ProxieBack sneakily uses the victim's server to bypass its own security
(U) Palo Alto Networks has come across a new family of proxy-creating malware, called ProxyBack, that the company said it believes has been in the wild since 2014 and may have more than 20 versions now running. Unlike other proxy-generating malware, ProxieBack does something unusual, and particularly dangerous for security personnel, Palo Alto researcher Jeff White wrote in a blog. It creates a reverse tunnel over TCP from the target server to a server controlled by the attacker. "To establish this tunnel, ProxyBack will initially make a connection to a web server hosting a PHP file that simply contains a URL to another PHP file on the same server. This subsequent PHP file will be used by the malware to send commands to the initial web server and fetch information used to setup its proxy connection," White wrote. Much of the traffic being routed through infected servers was seen coming from a system creating fake accounts and soliciting people on various dating sites, White noted. (scmagazine.com, 30Dec15)

(U) AVG's Chrome extension exposes personal data of 9 million users
(U) Google Project Zero researcher Tavis Ormandy discovered a vulnerability, since fixed, in AVG Web TuneUp, a Chrome extension that forcibly installs when users install the AVG antivirus software. The extension, which has over 9 million active users, contains a serious flaw that exposes users' browsing history, cookies, and personal data to attackers. "This extension adds numerous JavaScript API's to chrome, apparently so that they can hijack search settings and the new tab page," wrote Ormandy in the bug report. "The installation process is quite complicated so that they can bypass the chrome malware checks, which specifically tries to stop abuse of the extension API." Ormandy was involved in the discovery of vulnerabilities in Kaspersky's anti-virus product in September and a critical vulnerability in FireEye network security devices earlier this month. Ormandy wrote in a follow-up response to the bug report Monday, "I believe this issue is resolved now, but inline installations are disabled while the CWS team investigate possible policy violations." SCMagazine.com obtained an email response from AVG. "We thank the Google Security Research Team for making us aware of the vulnerability with the Web TuneUp optional Chrome extension," wrote AVG. "The vulnerability has been fixed; the fixed version has been published and automatically updated to users." (scmagazine.com, 29Dec15)

Incidents of Interest:

(U) UConn website hacked and used to spread malware
(U) The University of Connecticut (UConn) became the most recent institution of higher learning to be hit with a cyberattack when it was hacked on Dec. 27 and used to distribute malware. The hackers were able to take control the DNS records associated with the university's primary URL, uconn.edu, and point visitors to a server where a pop-up ad appeared that stated the visitor's Flash Player plugin is outdated and needed to be upgraded, according to the Daily Campus. Those clicking the link were were hit with the malware.
The cyberattackers also spoofed the school's mail exchange (MX) records, which slowed down the school's response when it attempted correct the DNS records to have them once again point back to the proper URL, the Daily Campus reported. The problem has been rectified and the university said it is investigating the incident. (scmagazine.com, 30Dec15)

(U) Quincy Credit Union hit by ATM skimming scam

(U) The Quincy Credit Union (QCU) may have had up to 700 customers victimized by an ATM skimming scam that took place earlier this month. Stewart Steele, CEO of the Qunicy, Mass. credit union, estimates that 670 accounts were compromised when someone attached a skimming device to one of the company's ATMs, the Boston Globe reported. The branch where the skimmer was placed was not revealed. Steele believes the incidents took place in early December, but it just came to light over the holiday weekend when the credit union's customers began to report unauthorized activity on their ATM cards. The QCU shut down its ATM and debit activity on Sunday in light of the activity, the Globe said. QCU is asking all its customers to check their card usage and said any losses will be reinstated into customer's accounts. (scmagazine.com, 29Dec15)

(U) Who Left a Gigantic US Voter Database Sitting Naked on the Internet?

(U) An unsecured database containing information on more than 190 million U.S. voters has been floating around the Internet, and nobody seems to know how it got there. That's a troubling sign as political campaigns become increasingly dependent on collecting, analyzing, and utilizing personal voter information. Internet researcher Chris Vickery found the database on Dec. 20; it has since been taken down. The database contained information that citizens provided to states when they registered to vote: names, addresses, phone numbers, and potentially demographic info and voting history. The information would be time consuming to aggregate (it can be purchased from state governments) but it is only truly useful to campaigns when combined with other data sets obtained from media companies, pollsters, and direct voter contact. Vickery, recognizing the voter file information that is used by campaigns to plot outreach and strategy, began contacting political data vendors to figure out where it came from, and found telltale data labels used by a company called Nation Builder. "While the database is not ours, it is possible that some of the information it contains may have come from data we make available for free to campaigns," Nation Builder CEO Jim Gilliam wrote on his company's website. "From what we've seen, the voter information included is already publicly available from each state government so no new or private information was released in this database." According to campaign spending data, Nation Builder's biggest clients in the current election cycle are the Massachusetts Republican Party, West Virginia congressman David McKinley, and the Lyndon Larouche Political Action Committee—associated with the controversial conspiracy theorist and perennial presidential candidate. There are a patchwork of state laws that limit using the data for commercial or non-political use, and the unsecured data is worrying to security professionals and privacy advocates. But it's important to recognize that all of this information is available to the public. Ultimately, this is appears to be a much less worrying incident than the data breaches that have plagued major retailers and the U.S. government. (nextgov.com, 29Dec15)

(U) Donald Trump receives a Christmas gift from a California hacker

(U) Republican presidential candidate Donald Trump received some support from hackers who took over an electronic highway sign in California on Christmas night to post "Merry Xmas - Vote Donald Trump. The display was located on interstate 15 in Corona, Calif., according to the Daily Mail. The reprogrammed sign was spotted by local resident Nikki Worden, who recorded the message and posted it on her Facebook account. It has since received more than 500,000 views, she told KABC-TV Channel 7. A California Transportation Department (CalTrans) spokesperson said the complete message stated "Inland Empire supports Donald Trump. Merry Xmas. Vote Donald Trump" adding that the transportation department had nothing to do with the message. Security has since been increased on the mobile sign, but KABC-TV said it sent a team to check the sign. They found the box, through which it is programmed, was unlocked and accessible. However, a password is needed to make any changes to the sign, which CalTrans believe was obtained by someone hacking their computer system. (scmagazine.com, 29Dec15)

OGA

Items of Interest

(U) There Were So Many Data Breaches in 2015. Did We Learn Anything From Them?

(U) 2015 has proven to be one of the most challenging in terms of the scope and severity of security breaches. The biggest and most interesting known breaches this year affected over 150 million people, putting billions of dollars at risk and costing businesses millions of dollars. As reported in October by Nextgov's Caitlin Fairchild, "The Biggest Cyber Breaches of 2015," some of those include:

- (U) Premera Blue Cross Blue Shield – Over 11 million subscribers' information was stolen.
- (U) Anthem – 80 million patients' and employees' information was stolen.
- (U) Bank heist – Cyber-crime ring Carbanak infiltrated over 100 banks worldwide to gain access credentials and to hijack ATMs to steal more than $1 billion.
- (U) Office of Personnel Management 1 & 2 – Over 4 million personnel files including security clearance information were stolen; an additional breach affected over 21 million federal employees and contractors. Information stolen included not just SSNs, but fingerprints and personal details that could leave federal personnel vulnerable to blackmail.
- (U) Internal Revenue Service – Online transcripts of over 100,000 taxpayers were accessed as a result of access to previously stolen identity information. Significant personal information was stolen costing taxpayers $50 million.
- (U) Ashley Madison (notorious "cheating" website) – 37 million customers' information was stolen, likely for shame and blackmail rather than credit card numbers.
- (U) Central Intelligence Agency Director John Brennan – Security clearance files from Brennan's hacked AOL account were posted on WikiLeaks.

(U) These breaches demonstrate the broad and deep spectrum of the security challenges and impact across the both the public and private sectors. Specifically, the breaches at OPM have taken a significant toll on the level of trust between the federal government and the public. In short, the exposure and problem is real, the impact is significant, and reputations are severely damaged. Cybersecurity/information security governance must be strengthened significantly to provide the needed direction and oversight to ensure the enterprise information assets and data are secure. Management must take advantage of all of the resources available and take ownership and responsibility for enterprise cybersecurity. (nextgov.com, 29Dec15)

(U) Firefox users should eliminate Mint Cast, Shell&Services: Report

(U) Firefox browser users might want to heed the call to remove the latest potentially unwanted programs (PUPs) from adware application Mint Cast and its variant Shell&Services. Pieter Arntz reported last week in a Malwarebytes blog, that the Mintcast PUP triggers unrequested changes to your system. An earlier report by malwaretips.com provided tips on how to remove the adware's unwanted popups. "Mintcast and its variants are adware applications that install two services on your system and one driver. The driver called WinDivert is a legitimate one that is also used by other applications as a network packet capture and (re)injection driver," Arntz wrote. When installed, the Mint Cast Network browser extension will display advertising banners, pop-up advertisements and in-text ads, sometimes promising "a premium offer." (scmagazine.com, 28Dec15)

(b)(3) 10 USC ⊥ 424

Note: This is not original product but is consolidated from various sources.

(b)(3) 10 USC ⊥ 424