

May 13, 2016

North Dakota State and Local Intelligence Center

Bi-Weekly Cyber Rollup



Included in this week's summary:

Click on the Section Header to go directly to that location in the Summary

[NORTH DAKOTA & REGIONAL](#)

(U) Cloquet school district in Minnesota recovering from Ransomware

(U) Woman loses \$1,825 to mystery shopping scam posing as BestMark, Inc., (BestMark is based in Mankato MN)

[NATIONAL](#)

(U) Pentagon working to 'take out' Islamic State's internet.

(U) San Bernardino iPhone Hack Tool Cost FBI 'Under \$1 Million'

(U) Google suffers minor data breach via third-party benefits vendor

(U) Over two dozen flaws found in Aruba products.

[INTERNATIONAL](#)

(U) German nuclear plant infected with computer viruses, operator says

(U) Lithuania government websites hit by cyberattacks for 3rd time

(U) MosQUito exploit stealing legitimate traffic from WordPress and Joomla Websites.

(U) New security flaw found in Lenovo Solution Center software.

NORTH DAKOTA & REGIONAL

(U) Cloquet school district in Minnesota suffers Ransomware attack

(U) The Cloquet school district recently suffered from a Ransomware attack. The attack resulted in the equivalent of a lock on much of its information and a \$6,000 ransom demand to have it released.

During a Cloquet School Board meeting, Superintendent Ken Scarbrough brought the board up to date on the attack on district computers and network servers that closed school for a day. The ransom was not paid instead Cloquet opted to restore and reimage computers. Sensitive student and staff data was not breached. That information is stored externally.

Of the district's eight servers, Scarbrough said six were infected by the malware. The two other servers were shut down so they wouldn't be infected. The attack affected the district's food service accounting system, bells, intercoms, email, heating and ventilation control, the library and more.

The Cloquet Police Department was notified and it contacted the local FBI office, which brought in its cybercrimes division, said Cloquet commander Derek Randall.

<http://www.grandforksherald.com/news/crime-and-courts/4002425-minnesota-school-continues-recovery-after-malicious-computer-attack>

(U) Woman loses \$1,825 to mystery shopping scam posing as BestMark, Inc.

(U) A woman in Houston, Texas is out \$1,825 after scammers targeted her using the name of a legitimate company that specializes in mystery shopping.

Based in Minnetonka, MN, BestMark provides mystery shopping services to organizations across the country. A Google search of the company's name will be all most people need to believe what they see in their mailbox – a check for nearly \$2,000.

Along with the check, the package also contained instructions. Follow-up communications from the scammers, via email and text message, encouraged the victim to follow the instructions and collect her commission. The email the victim received is worded with broken English, but simple enough to follow.

<http://www.csoonline.com/article/3054996/security/woman-loses-1-825-to-mystery-shopping-scam-posing-as-bestmark-inc.html>

NATIONAL

(U) Pentagon working to 'take out' Islamic State's internet.

(U) Pentagon officials reported April 28 that the U.S. military's Cyber Command (CYBERCOM) was working to destroy the Islamic State's Internet connection and leave the terrorist group in virtual isolation by interrupting the Islamic State's command and control (C&C), interrupting the group's ability to move funds, and interrupting the group's ability to recruit externally, among other actions. The task will be the command's first major combat operation in relation to the Islamic State threat.

<http://www.securityweek.com/pentagon-working-take-out-islamic-states-internet>

(U) San Bernardino iPhone Hack Tool Cost FBI 'Under \$1 Million'

(U) Agency now owns mechanism that can exploit unknown Apple security flaws. The FBI paid under \$1 million to the contractor who cracked the iPhone owned by the San Bernardino shooter, according to US government sources who spoke to Reuters.

This is a different figure than the \$1.3 million figure FBI director James Comey had suggested last week. When asked how much the third party was paid for the hacking tool, Comey had replied that it was more than what he would make during the rest of his tenure, which is seven years and four months.

[http://www.darkreading.com/mobile/san-bernardino-iphone-hack-tool-cost-fbi-under-\\$1-million/d/d-id/1325320](http://www.darkreading.com/mobile/san-bernardino-iphone-hack-tool-cost-fbi-under-$1-million/d/d-id/1325320)

(U) Google suffers minor data breach via third-party benefits vendor

(U) Google notified an unknown number of employees following a data breach that occurred when a manager of a third-party benefits vendor sent a file containing the names and Social Security numbers of an undisclosed number of Google employees to the wrong person. The individual who received the data deleted it from his computer and notified Google's vendor of the incident.

Google will start sending notification letters to all affected employees starting today, May 9, 2016. A copy of the notification letter is available via the Office of Attorney General for the State of California.

<http://news.softpedia.com/news/google-suffers-minor-data-breach-via-third-party-benefits-vendor-503839.shtml>

(U) Over two dozen flaws found in Aruba products.

(U) Aruba Networks patched some of the 26 security flaws discovered by a Google security engineer, and is working to patch the remaining vulnerabilities which impact all versions of ArubaOS, AirWave Management Platform 8.x versions prior to 8.2, and Aruba Instant access points (IAP) prior to 4.1.3.0 and 4.2.3.1.

Some of the vulnerabilities discovered include the transmission of login credentials via Hypertext Transfer Protocol (HTTP), default accounts, remote code execution flaws, firmware-related weaknesses, information disclosure issues, and Protocol Application Programming Interface (PAPI)-related security bugs.

<http://www.securityweek.com/over-two-dozen-flaws-found-aruba-products>

INTERNATIONAL

(U) German nuclear plant infected with computer viruses, operator says

(U) a nuclear power plant in Germany has been found to be infected with computer viruses, but they appear not to have posed a threat to the facility's operations because it is isolated from the Internet, the station's operator said on Tuesday. The Gundremmingen plant, located about 120 km (75 miles) northwest of Munich, is run by the German utility RWE (RWE.G.DE).

The viruses, which include "W32.Ramnit" and "Conficker", were discovered at Gundremmingen's B unit in a computer system retrofitted in 2008 with data visualization software associated with equipment for moving nuclear fuel rods, RWE said. Malware was also found on 18 removable data drives, mainly USB sticks, in office

computers maintained separately from the plant's operating systems. RWE said it had increased cyber-security measures as a result.

<http://www.reuters.com/article/us-nuclearpower-cyber-germany-idUSKCN0XN2OS>

(U) Lithuania government websites hit by cyberattacks for 3rd time

(U) Lithuanian officials say government websites have been hit by cyberattacks for the third time this month. The latest so-called denial-of-service attacks disrupted the websites of Parliament and the ministries of finance, defense, agriculture and others for about 30 minutes on Thursday.

Police launched an investigation but couldn't immediately say who was behind the Thursday attacks and those earlier this month. The most intense attacks happened on April 11 during a meeting of Crimean Tartars in Lithuania.

Arvydas Zvirblis, head of the Infobalt cybersecurity committee, said "these coordinated attacks are unpredictable and can cause serious damage." He said Lithuania needs to upgrade its cyber defense capabilities.

<http://www.crookstontimes.com/news/20160422/lithuania-govt-websites-hit-by-cyberattacks-for-3rd-time>

(U) MosQUito exploit stealing legitimate traffic from WordPress and Joomla Websites. (U) eZanga.com, Inc., published a list that revealed 9,285 Web sites were affected by a malicious campaign dubbed, MosQUito after discovering that hackers were searching for Web sites where the jQuery JavaScript library was loaded and replaced with a malicious PHP file, jQuery.min.php, to steal paid traffic from legitimate businesses and to redirect victims to another Web site controlled by the attacker.

<http://news.softpedia.com/news/mosquito-exploit-stealing-legitimate-traffic-from-wordpress-and-joomla-websites-503647.shtml>

(U) New security flaw found in Lenovo Solution Center software.

(U) Trustwave SpiderLabs reported a new vulnerability in Lenovo's Solution Center software which is tied to the software's backend and can allow an attacker with local network access to a PC to execute arbitrary code and elevate privileges. The company updated a previous security advisory disclosing the additional vulnerability and released a fix addressing the vulnerability.

<https://threatpost.com/new-security-flaw-found-in-lenovo-solution-center-software/117896/>

The Bi-Weekly Cyber Roll up is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material. If you have any items that you would like to see added to the Bi-Weekly Cyber Roll up, please forward it to the NDSLIC (ndslic@nd.gov).