October 28, 2016

North Dakota State and Local Intelligence Center

Bi-Weekly Cybersecurity 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) Phish Looking to Hook NDSU Community
(U) Task force close to finalizing cybersecurity recommendations

NATIONAL
(U) Locky ransomware accounted for 97 percent of all malicious email attachments
(U) Weebly breach affects over 43 million users
(U) U.S. calls on automakers to make cyber security a priority

INTERNATIONAL
(U) Magneto malware hides stolen card data in image files
(U) WordPress sites under attack via security flaw in unmaintained plugin
(U) Windows zero-day exploited by "FruityArmor" APT group
(U) Linux kernel zero-day CVE-2016-5195 patched after being deployed in live attacks
(U) Dyn DDoS attack: The aftermath
(U) LinkedIn to get Banned in Russia for not Complying with Data Localization Law

NORTH DAKOTA & REGIONAL

(U) Phish Looking to Hook NDSU Community

(U) Over 280 North Dakota State email accounts had been compromised by phishing attackers since Tuesday. Students, staff and faculty are mainly being targeted through malicious phishing emails through their NDSU accounts. Examples include false emails saying users may upgrade their email storage space through Help Desk, someone's cousin needs money or individuals in Africa need money.

Source: (U) http://ndsuspectrum.com/phish-looking-to-hook-ndsu-community/

(U) Task force close to finalizing cybersecurity recommendations

(U) A state cybersecurity task force is preparing for one last discussion early next month before they sign off on their recommendations in a final report to the governor. Dan Sipes, deputy chief information officer for the North Dakota Information Technology Department, said the meeting will be held Nov. 2 in the Rough Rider Room at the state Capitol.

Source: (U) http://bismarcktribune.com/news/columnists/nick-smith/task-force-close-to-finalizing-cybersecurity-recommendations/article_9943b7ec-add4-5741-bfbc-89468b547689.html

NATIONAL

(U) Locky ransomware accounted for 97 percent of all malicious email attachments

(U) Locky ransomware accounted for 97 percent of all malicious email attachments. Proofpoint released its Quarterly Threat Summary for quarter 3 (Q3) 2016, which reported that the Locky ransomware was found in 96.8 percent of all malicious spam email attachments and typically manifests itself as a ZIP file with a JavaScript file inside, Microsoft Office documents with malicious macro scripts, Hypertext Markup Language Application (HTA) files, or Microsoft Windows Script Files (WSF). The report also stated that banking trojans continue to be a pervasive threat, while exploit kit (EK) activity has decreased 65 percent since Q2.

Source: (U) http://news.softpedia.com/news/locky-ransomware-accounted-for-97-percentof-all-malicious-email-attachments-509335.shtml

(U) Weebly breach affects over 43 million users

(U) Weebly, a San Francisco-based Web hosting service, confirmed that hackers stole the account information of over 43 million users, including usernames, Internet Protocol (IP) addresses, and password hashes after breaching the company's systems in February 2016. The company advised its user to reset their passwords and the cause of the breach remains under investigation.

Source: (U) http://www.securityweek.com/weebly-breach-affects-over-43-million-users

(U) U.S. calls on automakers to make cyber security a priority

(U) Automakers should make shielding the electronic and computer systems of vehicles from hackers a priority, developing layers of protection that can secure a vehicle throughout its life, U.S. regulators said on Monday

Source: (U) http://mobile.reuters.com/article/idUSKCN12O2JG

INTERNATIONAL

(U) Magneto malware hides stolen card data in image files

(U) Sucuri researchers discovered malicious actors were using real image files related to an online store's products to plant payment card-swiping malware on Websites running the Magneto ecommerce platform in order to exfiltrate stolen card data via email or by including it in a file that the attacker later retrieves. Sucuri advised online stores to keep all their software updated in order to protect their Websites from the malware.

Source: (U) http://www.securityweek.com/magento-malware-hides-stolen-card-data-image

(U) WordPress sites under attack via security flaw in unmaintained plugin

(U) Security researchers from White Fir Design discovered the WordPress Marketplace plugin was plagued with an arbitrary file upload vulnerability that could allow an attacker to upload arbitrary files on Websites with the plugin installed and potentially take over a site's underlying server. The researchers discovered the flaw after detecting scans for the plugin's Cascading Style Sheets (CSS) file on multiple Websites.

Source: (U) http://news.softpedia.com/news/wordpress-sites-under-attack-via-securityflaw-in-unmaintained-plugin-509387.shtml

(U) Windows zero-day exploited by "FruityArmor" APT group

(U) Security researchers from Kaspersky Lab discovered that a zero-day remote code execution vulnerability patched by Microsoft in its October 2016 security bulletin was being leveraged in attacks carried out by an advanced persistent threat (APT) group, dubbed "FruityArmor" for privilege escalation on an affected system. Researchers found that the FruityArmor APT's attack platform is built around Microsoft PowerShell and abuses Windows Management Instrumentation (WMI) for persistence in order to make it difficult to detect on a system.

Source: (U) http://www.securityweek.com/windows-zero-day-used-fruityarmor-aptprivilege-escalation

(U) Linux kernel zero-day CVE-2016-5195 patched after being deployed in live attacks

(U) The Linux kernel team patched a zero-day security flaw named Dirty COW, as it is caused by a race condition in the way Linux kernel's memory handles copy-on-write (COW) breakage of read-only memory mappings, which could allow an attacker to escalate their privileges, potentially to root level, on a targeted system. A security researcher notified Red Hat of attackers deploying an exploit that leverages this vulnerability in the wild.

Source: (U) http://news.softpedia.com/news/linux-kernel-zero-day-cve-2016-5195-patchedafter-being-deployed-in-live-attacks-509494.shtml

(U) Dyn DDoS attack: The aftermath

(U) New Hampshire-based Dyn DNS Company suffered 3 distributed denial-of-service (DDoS) attacks involving millions of Internet Protocol (IP) addresses that targeted the company's managed Domain Name Server (DNS) infrastructure and rendered many Websites and online services such as Twitter, PayPal, and Etsy, among others inaccessible for several hours October 21. Security researchers from Flashpoint and Akamai confirmed that one source of the attacks' traffic were Internet of Things (IoT) devices infected by the Mirai botnet.

Source: (U) https://www.helpnetsecurity.com/2016/10/24/dyn-ddos-attack-aftermath/

(U) LinkedIn to get Banned in Russia for not complying with Data Localization Law

(U) The world's largest online professional network LinkedIn could face a bain in Russia after the company has failed to comply with a Russian data localization law that compels companies to keep data on Russian users in their country

Source: (U) http://thehackernews.com/2016/10/russia-linkedin-ban.html

The Bi-Weekly Cybersecurity 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).