

September 30, 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) October is Cybersecurity Awareness Month

[NATIONAL](#)

(U) 500 million Yahoo accounts breached

(U) State Computers Increasingly Under Attack by Cybercriminals

(U) KrebsOnSecurity Hit with Record DDoS

[INTERNATIONAL](#)

(U) Adobe patches 29 vulnerabilities in Flash Player

(U) Microsoft patches browser vulnerability exploited in attacks

(U) Sixth Linux DDoS Trojan discovered in the last 30 days

(U) Apple patches 7 flaws with release of iOS 10

(U) Researchers remotely hack Tesla Model S while it is being driven

NORTH DAKOTA & REGIONAL

(U) October is Cybersecurity Awareness Month

(U) Governor Dalrymple has [proclaimed](#) October as Cyber Security Awareness Month in the State of North Dakota.

Source: (U) <http://governor.nd.gov/media-center/proclamation/cyber-security-awareness-month-4>

Source: (U) <https://staysafeonline.org/ncsam/>

NATIONAL

(U) 500 Million Yahoo Accounts Breached

(U) Information from at least 500 million Yahoo accounts was stolen from the company in 2014, the company said Thursday, indicating it believes a state-sponsored actor was behind the hack.

Source: (U) <http://www.usatoday.com/story/tech/2016/09/22/report-yahoo-may-confirm-massive-data-breach/90824934/>

(U) State Computers Increasingly Under Attack by Cybercriminals

(U) State information technology officials have strengthened their defenses against hackers and cybercriminals who attack their computer networks millions of times a day, but admit they're not fully prepared for increasingly complex threats that could expose the personal information of their residents

Source: (U) <http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2016/09/21/state-computers-increasingly-under-attack-by-cybercriminals>

(U) KrebsOnSecurity Hit With Record DDoS

(U) On Tuesday evening, KrebsOnSecurity.com was the target of an extremely large and unusual distributed denial-of-service (DDoS) attack designed to knock the site offline. The attack did not succeed thanks to the hard work of the engineers at **Akamai**, the company that protects my site from such digital sieges. But according to Akamai, it was nearly double the size of the largest attack they'd seen previously, and was among the biggest assaults the Internet has ever witnessed.

Source: (U) <https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/>

INTERNATIONAL

(U) Adobe patches 29 vulnerabilities in Flash Player

(U) Adobe released updates for Flash Player, Digital Editions, and Adobe Air SDK & Compiler resolving a total of 37 vulnerabilities, including integer overflow, use-after-free, among other memory corruption issues in Flash Player that can be exploited to leverage arbitrary code execution, as well as several memory corruption flaws and a use-after-free issue in Digital Editions 4.5.1 and earlier that can be exploited for arbitrary code execution, among other vulnerabilities.

Source: (U) <http://www.securityweek.com/adobe-patches-29-vulnerabilities-flash-player>

(U) Microsoft patches browser vulnerability exploited in attacks

(U) Microsoft released 13 security bulletins patching nearly 50 vulnerabilities plaguing Windows, Internet Explorer, Edge, Exchange, and Office, including an information disclosure flaw in Internet Explorer and Edge that can be exploited if an attacker convinces a victim to access a compromised Website, as well as a memory corruption issue that can be exploited for remote code execution if the victim accesses a compromised Website, among other vulnerabilities.

Source: (U) <http://www.securityweek.com/microsoft-patches-browser-vulnerabilityexploited-attacks>

(U) Sixth Linux DDoS Trojan discovered in the last 30 days

(U) Dr. Web security researchers discovered a Trojan affecting Linux machines via the Shellshock vulnerability that launches 25 child processes that carry out a distributed denial-of-service (DDoS) attack on a targeted device when the attacker in control of the Trojan botnet issues an attack command. Researchers stated the Trojan can start Transmission Control Protocol (TCP) floods, User Datagram Protocol (UDP) floods, and Hypertext Transfer Protocol (HTTP) floods, as well as update itself, terminate its process, and delete itself, among other capabilities.

Source: (U) <http://news.softpedia.com/news/sixth-linux-ddos-trojan-discovered-in-the-last30-days-508309.shtml>

(U) Apple patches 7 flaws with release of iOS 10

(U) Apple Inc., released version 10 of its operating system (iOS), Xcode version 8, and watchOS version 3 patching a total of seven vulnerabilities, including a flaw in iOS that can be exploited by a man-in-the-middle (MitM) attacker to prevent a device from receiving updates, an information disclosure vulnerability in iOS and watchOS that can be exploited by malicious applications to access an user's location data, and a flaw in Xcode that could allow a local attacker to execute arbitrary code or crash an application, among other flaws.

Source: (U) <http://www.securityweek.com/apple-patches-7-flaws-release-ios-10>

(U) Researchers remotely hack Tesla Model S while it is being driven

(U) Chinese researchers from Keen Security Lab of Tencent [announced](#) that they could chain multiple vulnerabilities together, which allowed them to remotely hack the Tesla Model S P85 and 75D from as far as 12 miles away.

Source: (U) http://www.networkworld.com/article/3121934/security/researchers-remotely-hack-tesla-model-s-while-it-is-being-driven.html?token=%23tk.NWWNLE_nlt_networkworld_after_dark_alert_2016-09-20&idg_eid=94156a9acf672d152d1d4b66367c1bc1&utm_source=Sailthru&utm_medium=email&utm_campaign=NWW%20After%20Dark%20Alert%202016-09-20&utm_term=networkworld_after_dark_alert#tk.NWW_nlt_networkworld_after_dark_alert_2016-09-20

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).