

June 10, 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) Reporter who wrote about Target breach says well-trained staff is best defense against cyberattacks

[NATIONAL](#)

(U) Wendy's Comes clean on data breach

(U) Stolen laptop of Redskins trainer contained player's medical info

(U) Two men plead guilty in U.S. to hacking, spamming scheme.

[INTERNATIONAL](#)

(U) University of Calgary Pays Ransom

(U) Kiddicare Hacked, 794,000 Accounts Leaked

(U) London Clinic fined 180,000 pounds for Leaking HIV Patients Data

(U) Windows zero-day affecting all OS versions on sale for \$90,000.

(U) WordPress sites under attack from new zero-day in WP mobile detector plugin

(U) Uber pays researcher \$10K for login bypass exploit

(U) 32 million Twitter passwords hacked

[NORTH DAKOTA & REGIONAL](#)

(U) Reporter who wrote about Target breach says well-trained staff is best defense against cyberattacks

(U) Brian Krebs, cybercrime journalist who first broke the story of Minnesota based Target Corp.'s 2013 data breach, stressed the importance of security professionals when he delivered the keynote lecture at the Secure360 Twin Cities Conference.

Source: (U) <http://www.startribune.com/reporter-who-wrote-about-target-breach-says-well-trained-staff-is-best-defense-against-cyberattacks/379831601/>

[NATIONAL](#)

(U) Wendy's comes clean on data breach

(U) Wendy's has disclosed it was a victim of a point-of-sale system attack, software installed malware on PoS (Point-of-Sale) computers affecting 300 franchise restaurants. This is released as part of the company's first quarter 2016 SEC filings.

Source: (U) <https://threatpost.com/wendys-comes-clean-on-data-breach/118034/>

(U) Stolen laptop of Redskins trainer contained players' medical info

(U) Laptop containing medical records of thousands of NFL players was stolen from the care of a Washington Redskins trainer last month. According to a letter from the NFLPA (Players' Association) was obtained by Deadspin. The stolen medical records were of every player who went through the NFL scouting combine from 2004 through 2016, plus current Redskins players. The backpack also contained a zip drive and hard copies of the medical records. The laptop was stolen on April 15 in downtown Indianapolis, where a car window was broken.

Source: (U) http://espn.go.com/nfl/story/_/id/15884597/laptop-stolen-washington-redskins-trainer-contained-medical-records-thousands-nfl-players

(U) Two men plead guilty in U.S. to hacking, spamming scheme

(U) Officials reported June 2 that two men pleaded guilty in New Jersey for their involvement in a hacking and spamming scheme that generated more than \$2 million in illegal profits after the duo and a co-conspirator targeted and stole the personal information of 60 million people, hacked into corporate email accounts, seized control of corporate mail servers, and created their own software to exploit vulnerabilities in numerous corporate Web sites via specially crafted code in computer programs, which hid the origin of the spam and bypassed spam filters.

Source: (U) <http://www.reuters.com/article/us-usa-cyber-pleas-idUSKCN0YO2TQ>

INTERNATIONAL

(U) University of Calgary Pays Ransom

(U) University of Calgary pays cyber attackers after systems were infected with ransomware. The University paid \$20,000 Canadian (\$15,700 US) and is now assessing and evaluating the decryption keys. The University started communicating about the attack in late May. Email was restored for faculty and staff on June 6, but warned obtaining the decryption keys did not mean all systems could be restored and data recovered

Source: (U) <http://www.databreachtoday.com/university-calgary-pays-ransom-a-9190>

(U) Kiddicare Hacked, 794,000 Accounts Leaked

(U) Kiddicare admitted that company has suffered a data breach, leading to the theft of 794,000 users' sensitive data, including phone numbers and residential addresses.

Source: (U) <http://thehackernews.com/2016/05/top-data-breach.html>

(U) London Clinic Fined 180,000 pounds for Leaking HIV Patients Data

(U) The Information Commissioner's Office (ICO) has fined a London-based clinic 180,000 pounds (about \$260,000) for leaking data of 781 HIV patients. The clinic mistakenly sent an email containing sensitive medical information relating to 781 HIV patients together rather than individually, leaking their names and email addresses to one another.

Source: (U) <http://thehackernews.com/2016/05/top-data-breach.html>

(U) Windows zero-day affecting all OS versions on sale for \$90,000

(U) A hacker under the name, BuggiCorp was discovered selling a zero-day vulnerability affecting over 1.5 billion users and all versions of Windows operating systems (OS) after security firm Trustwave found the attacker could escalate the privileges of an application in Windows 10 with the May 2016 security patch installed, and bypass all security features including Microsoft's newest version of the Enhanced Mitigation Experience Toolkit (EMET) toolkit.

Source: (U) <http://news.softpedia.com/news/windows-zero-day-affecting-all-os-versions-on-sale-for-90-000-504716.shtml>

(U) WordPress sites under attack from new zero-day in WP mobile detector plugin

(U) Security researchers from Plugin Vulnerabilities discovered that hackers were exploiting an arbitrary file upload vulnerability in WP Mobile Detector plugin, which handles image uploads, to upload Hypertext Preprocessor (PHP)-based backdoors on WordPress Web sites after finding that the plugin lacks basic input filtering, allowing attackers to pass a malicious file to upload it to the plugin's/cache directory.

Source: (U) <http://news.softpedia.com/news/wordpress-sites-under-attack-from-new-zero-day-in-wp-mobile-detector-plugin-504818.shtml>

(U) Uber pays researcher \$10K for login bypass exploit

(U) Uber Technologies Inc., recently patched a flaw in its Web site after a security researcher found a hacker could bypass the OneLogin system used for employee authentication and potentially compromise its internal network hosted on Atlassian's Confluence collaboration software. In addition, the security researcher stated that the flaw could be exploited to compromise a server that uses WordPress plugins.

Source: (U) <https://threatpost.com/uber-pays-researcher-10k-for-login-bypass-exploit/118516/>

(U) 32 million Twitter passwords hacked

(U) Millions of Twitter accounts stolen passwords are floating around the dark side of the Internet. The website LeakedSource said it received a cache of Twitter data that contains 32 million records, including passwords. Twitter states that systems haven't been breached. LeakedSource said the passwords were most likely collected over time by malware-infected browsers.

Source: (U) http://host.madison.com/business/report-twitter-user-data-leaked/article_330c81c9-6208-5816-9c72-916d1511f7b9.html

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).