

**UNCLASSIFIED**

**16 November 2015**



# **NORTH DAKOTA HOMELAND SECURITY Cyber Summary**



The North Dakota Open Source Cyber Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Cyber Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

**UNCLASSIFIED**

**NDSLIC DISCLAIMER**

The Cyber Summary 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.

**TABLE OF CONTENTS**

[Regional](#)..... 3

[National](#)..... 3

[International](#)..... 3

[Banking and Finance Industry](#)..... 4

[Chemical and Hazardous Materials Sector](#)..... 5

[Commercial Facilities](#)..... 5

[Communications Sector](#)..... 5

[Critical Manufacturing](#)..... 6

[Defense/ Industry Base Sector](#)..... 6

[Emergency Services](#)..... 6

[Energy](#)..... 7

[Food and Agriculture](#)..... 7

[Government Sector \(including Schools and Universities\)](#)..... 7

[Information Technology and Telecommunications](#)..... 7

[US-Cert Updates and Vulnerabilities](#)..... 9

[ICS-Cert Alerts & Advisories](#)..... 10

[Public Health](#)..... 10

[Transportation](#)..... 10

[Water and Dams](#)..... 11

[North Dakota Homeland Security Contacts](#)..... 11

**NORTH DAKOTA**

Nothing Significant to Report

**REGIONAL**

Nothing Significant to Report

**NATIONAL**

**(National)** Fake IT admin tricked Cox rep into handing over customer database – cableco fined \$600K. The U.S. Federal Communications Commission fined Cox Communications for \$595,000 November 5 for allegations that the company failed to provide adequate security for its customer database and failed to notify the Federal government after a 2014 security breach in which a Lizard Squad hacker accessed customer records and leaked partial information on 8 customers and changed the passwords of 28 others while disguised as an employee in the Intelligence Technology (IT) department. The hacker had control over customer billing information including names, addresses, payment data, and even partial social security numbers and State identification numbers.

[http://www.theregister.co.uk/2015/11/06/fcc\\_cox\\_data\\_breach/](http://www.theregister.co.uk/2015/11/06/fcc_cox_data_breach/)

**INTERNATIONAL**

**(International)** No surprise here: Adobe's Flash is a hacker's favorite target. Researchers from Recorded Future released a new study November 9 revealing that Adobe Systems' Flash plugin was the highest targeted software program used by cybercriminals to install malware onto computers following research that revealed 8 of the 10 top vulnerabilities were seen targeting Adobe's Flash plugin.

[http://www.computerworld.com/article/3003062/security/no-surprise-here-adobes-flash-is-a-hackers-favorite-target.html#tk.rss\\_security](http://www.computerworld.com/article/3003062/security/no-surprise-here-adobes-flash-is-a-hackers-favorite-target.html#tk.rss_security)

## UNCLASSIFIED

**(International) Security flaws found in Google Chromecast, Home Security Systems, Smart Coffee Makers.** Security researchers from Kaspersky discovered several vulnerabilities in Internet of Things devices (IoT) including a “rickrolling” vulnerability in Google Chromecast devices that enables attackers to hijack smart TV content, a vulnerability in a smart coffee maker device that exposes the user’s Wi-Fi password, allowing attackers to spy on homeowners by connecting to Internet protocol (IP) cameras used in Webcams and baby monitors, as well as infiltrate a home security system by using powerful magnets that allows attackers to gain access to homes without triggering the alarm.

<http://news.softpedia.com/news/security-flaws-found-in-google-chromecast-home-security-systems-smart-coffee-makers-495864.shtml>

## **BANKING AND FINANCE INDUSTRY**

**(Nevada) Six charged in \$2.7 million tax refund fraud scheme.** Federal authorities charged six people November 6 for their roles in a \$2.7 million Internal Revenue Service tax refund scheme where suspects would acquire the personal information of deceased persons from genealogical databases and use it to create fraudulent W-2 forms, driver’s licenses, and Social Security cards to file for tax refunds.

<http://www.news3lv.com/content/news/local/story/tax-refund-fraud-scheme-federal-Bogden/ozlX-4ppL0eIVnvhzVsHuA.cspX>

**(International) U.S. charges Scottish man over fake tweets that hurt stocks.** The U.S. Department of Justice reported November 5 that a Scottish national was charged after he set up Twitter accounts as market research firms Muddy Waters Research and Citron Research and falsely reported that Audience Inc., and Sarepta Therapeutics Inc., were under Federal investigation, sending their stock prices plunging and costing investors \$1.6 million in losses in an effort to profit from illegal trading.

<http://www.reuters.com/article/2015/11/06/us-usa-crime-tweets-idUSKCN0SV07G20151106>

**(International) Charges announced in J.P. Morgan hacking case.** A Federal indictment was unsealed November 10 against three men in connection to an alleged massive cyber-attack against J.P. Morgan Chase & Co., and several other

UNCLASSIFIED

## UNCLASSIFIED

U.S. financial institutions that allowed the suspects to steal the personal information of more than 100 million customers by hacking into the financial institutions' systems and stealing customer information to carry out a stock-manipulation scheme. The defendants would artificially inflate stock prices and send spam emails to customers to trick them into buying stocks.

<http://www.wsj.com/articles/prosecutors-announce-charges-in-connection-with-j-p-morgan-hack-1447169646>

### CHEMICAL AND HAZARDOUS MATERIALS SECTOR

**Nothing Significant to Report**

### COMMERCIAL FACILITIES

**(Michigan) Four Winds warns of credit card breach.** An official from Four Winds Casino Resort reported November 5 that its network system was compromised revealing cardholder names, card numbers, expiration dates, and internal verification codes for an unknown number of customers at its properties in New Buffalo, Hartford, or two facilities in Dowagiac following an investigation that found a program was installed onto the casino's network to search for payment card data from October 2014 – October 2015.

[http://www.heraldpalladium.com/news/local/four-winds-warns-of-credit-card-breach/article\\_62ddc82a-64af-54e1-863c-b4052d000819.html](http://www.heraldpalladium.com/news/local/four-winds-warns-of-credit-card-breach/article_62ddc82a-64af-54e1-863c-b4052d000819.html)

### COMMUNICATIONS SECTOR

**(National) Comcast says it's not to blame after 200,000 user accounts were put up for the sale online.** Comcast announced November 9 that it will reset passwords for roughly 200,000 customers after a package of personal data, including the e-mail addresses and passwords, was listed for sale for \$1,000 on a Dark Web site. The company reported it was not hacked and that its systems and apps were not compromised and held unsuspecting customers responsible for visiting malware-laden sites or fallen victim to other schemes that allowed

UNCLASSIFIED

## UNCLASSIFIED

hackers to obtain their data. <https://www.washingtonpost.com/news/the-switch/wp/2015/11/09/comcast-says-its-not-to-blame-after-200000-accounts-were-illegally-put-up-for-sale/>

**(National) Securus Technologies: A rogue employee, not a hacker, exposed 70 million inmate calls.** Securus Technologies announced November 12 that it is investigating an alleged breach of its systems that provides phone service to incarcerated people around the U.S., and stated that its system was not hacked by an outside, but likely breached by an internal employee. An investigation into the breach, which reportedly includes unauthorized access to over 70 million recorded prison phone conversations, is ongoing.

<http://www.ibtimes.com/securus-technologies-rogue-employee-not-hacker-exposed-70-million-inmate-calls-2181819>

### CRITICAL MANUFACTURING

Nothing Significant to Report

### DEFENSE/ INDUSTRY BASE SECTOR

Nothing Significant to Report

### EMERGENCY SERVICES

**(New Hampshire) Computer virus infects county dispatch center.** The Strafford County chief deputy announced November 12 that computers at the Strafford County Regional Dispatch Center in Dover were infected by the CryptoLocker ransomware which severely limited the amount of data utilized by both dispatchers and emergency personnel on the field. Officials were able to isolate the virus and are working on bringing systems back online.

<http://www.fosters.com/article/20151112/NEWS/151119727>

UNCLASSIFIED

**ENERGY**

Nothing Significant to Report

**FOOD AND AGRICULTURE**

Nothing Significant to Report

**GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)**

Nothing Significant to Report

**INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS**

**(International) Updated Cryptowall encrypts file names, mocks victims.**

Researchers from both Bleeping Computer and an independent researcher discovered that the Cryptowall malware was recently updated to encrypt data on victims' machines and file names, making infected files difficult to recover without paying a ransom. The ransomware infects victims via email attachments, disguised as Microsoft Word documents, through JavaScript executable.

<https://threatpost.com/updated-cryptowall-encrypts-file-names-mocks-victims/115285/>

**(International) Ransomware found targeting Linux servers and coding repositories.**

Researcher from Russian-based antivirus maker Dr. Web discovered a new ransomware that targets Linux Web servers and attacks Web development environments used to host Web sites or code via a downloaded file containing the public RSA key used to store AES keys that add .encrypt extension to each file, as well as a ransom text message where it encrypts data. The ransomware was detected as Linux.Encoder.1 and uses the PolarSSL library.

## UNCLASSIFIED

<http://news.softpedia.com/news/ransomware-found-targetting-linux-servers-and-coding-repositories-495836.shtml>

**(International) Flaw in Linux encryption ransomware exposes decryption key.**

Researchers at Bitdefender discovered a flaw in the Linux.Encoder1 ransomware in its advanced encryption standard (AES) key generation process that revealed the libc rand() function, seeded with the current system timestamp during encryption, allows the retrieval of the AES key without having to decrypt the malware by paying the attackers for a RSA public key. The security firm released a decryption tool that automatically restores encrypted files previously attacked by Linux.Encoder1. <http://www.securityweek.com/flaw-linux-encryption-ransomware-exposes-decryption-key>

**(International) Remote code execution flaw found in Java app servers.**

Researchers from FoxGlove Security released a report addressing deserialization vulnerabilities in Java applications including Oracle WebLogic, IBM - 6 - WebSphere, and Jenkins, among other products that can be remotely exploited for arbitrary code due to poor coding via Java library Apache Commons Collections that is used for more than 1,300 projects. A Java deserialization library and a report were released to secure applications from malicious actors and educate developers on how to avoid such flaws. <http://www.securityweek.com/remote-code-execution-flaw-found-java-app-servers>

**(International) “Cherry Picker” PoS malware cleans up after itself.** Researchers from Trustwave discovered that a point-of-sale (PoS) malware dubbed “Cherry Picker” relies on a new memory scraping algorithm using a file infector for persistence that removes all traces of the infection from the system with updated versions of sr.exe and srf.exe, which has been used to install the malware and inject a data definition language (DLL) into processes. The latest version of the malware relies on an application programming interface (API) called “QueryWorkingSet” to scrape the memory and harvest the data.

<http://www.securityweek.com/cherry-picker-pos-malware-cleans-after-itself>

**(International) Attackers abuse security products to install “Bookworm” trojan.**

Researchers from Palo Alto Networks discovered a new trojan dubbed “Bookworm” which captures keystrokes and steals the content of a clipboard, as

## UNCLASSIFIED

well as load additional modules from its command and control (C&C) server to expand its abilities by using a Smart Installer Maker tool to disguise the malware as a self-extracting RAR archive, or a Flash slideshow/installer, to write a executable data definition language (DDL) file named "Loader.ddl," and a file named "readme.txt," to the victims' system.

<http://www.securityweek.com/attackers-abuse-security-products-install-bookworm-trojan>

### **(National) New PoS malware delivered via malicious docs, exploit kit.**

Researchers from Proofpoint observed the "AbaddonPOS" point-of-sale (PoS) malware and determined that it was being widely distributed with the aid compromised Microsoft Word documents designed to download information-stealing threats. Once the malware infects the system, it targets the memory of all processes in track 1 and track 2 data associated with payment cards.

<http://www.securityweek.com/new-pos-malware-delivered-malicious-docs-exploit-kit>

### **(International) Latest Android phones hijacked with tidy one-stop-Chrome-pop.**

A researcher from Quihoo 360 discovered, and reported during the MobilePwn2Own event at the PacSec security conference, a single clean exploit in Google's Chrome browser for Android via its JavaScript v8 engine that does not require several chained vulnerabilities to gain access and load software without user interaction once a user visits a malicious Web site.

[http://www.theregister.co.uk/2015/11/12/mobile\\_pwn2own/](http://www.theregister.co.uk/2015/11/12/mobile_pwn2own/)

## **US-CERT UPDATES AND VULNERABILITIES**

**Microsoft Releases November 2015 Security Bulletin.** Published Tuesday, November 10, 2015. Microsoft has released 12 updates to address vulnerabilities in Microsoft Windows. Exploitation of some of these vulnerabilities could allow an attacker to take control of an affected system. <https://technet.microsoft.com/en-us/library/security/ms15-nov.aspx>

**Google Releases Security Updates for Chrome and Chrome OS.** Published Wednesday, November 11, 2015. Google has released security updates to

UNCLASSIFIED

## UNCLASSIFIED

address vulnerabilities in Chrome and Chrome OS. Exploitation of one of these vulnerabilities may allow a remote attacker to take control of an affected system.

<https://www.us-cert.gov/ncas/current-activity/2015/11/11/Google-Releases-Security-Updates-Chrome-and-Chrome-OS>

**Apache Commons Collections Java Library Vulnerability.** Published Friday, November 13, 2015. US-CERT is aware of a deserialization vulnerability in the Apache Commons Collections (ACC) Java library. Java applications that either directly use ACC, or contain ACC in their classpath, may be vulnerable to arbitrary code execution. <http://www.kb.cert.org/vuls/id/576313>

### **ICS-CERT ALERTS & ADVISORIES**

ICS-MM201510 : September-October 2015. The NCCIC/ICS-CERT Monitor for September-October 2015 is a summary of ICS-CERT activities for these months.

<https://ics-cert.us-cert.gov/monitors/ICS-MM201510>

ICSA-15-274-02 : Unitronics VisiLogic OPLC IDE Vulnerabilities. This advisory was originally posted to the US-CERT secure Portal library on November 3, 2015, and is being released to the NCCIC/ICS-CERT web site. This advisory provides mitigation details for vulnerabilities in Unitronics VisiLogic OPLC IDE. <https://ics-cert.us-cert.gov/advisories/ICSA-15-274-02>

### **PUBLIC HEALTH**

**Nothing Significant to Report**

### **TRANSPORTATION**

**Nothing Significant to Report**

UNCLASSIFIED

**WATER AND DAMS**

Nothing Significant to Report

**NORTH DAKOTA HOMELAND SECURITY CONTACTS**

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **North Dakota State and Local Intelligence Center:** 866-885-8295(IN ND ONLY); Email: [ndslic@nd.gov](mailto:ndslic@nd.gov); Fax: 701-328-8175 **State Radio:** 800-472-2121; **Bureau of Criminal Investigation (BCI):** 701-328-5500; **North Dakota Highway Patrol:** 701-328-2455; **US Attorney's Office Intel Analyst:** 701-297-7400; **Bismarck FBI:** 701-223-4875; **Fargo FBI:** 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Darin Hanson, ND Division of Homeland Security [dthanson@nd.gov](mailto:dthanson@nd.gov), 701-328-8165