

UNCLASSIFIED

14 December 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](#)..... 6

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

[Defense/ Industry Base Sector](#)..... 7

[Emergency Services](#)..... 7

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

[Food and Agriculture](#)..... 8

[Government Sector \(including Schools and Universities\)](#)..... 8

[Information Technology and Telecommunications](#)..... 8

[US-Cert Updates and Vulnerabilities](#)..... 11

[ICS-Cert Alerts & Advisories](#)..... 11

[Public Health](#)..... 11

[Transportation](#)..... 12

[Water and Dams](#)..... 12

[North Dakota Homeland Security Contacts](#)..... 13

NORTH DAKOTA

Nothing Significant to Report

REGIONAL

Nothing Significant to Report

NATIONAL

(International) **300 American ISIS Supporters Help Islamic State Recruitment, Propaganda On Twitter.** No fewer than 300 American sympathizers are helping the Islamic State terrorist group recruit potential members and spread propaganda via Twitter, according to a new report from George Washington University's Program on Extremism. The report drew on court records, media reports, interviews and other sources to find that U.S. supporters of the group, aka ISIS, "spasmodically create accounts that often get suspended in a never-ending cat-and-mouse game." <http://www.ibtimes.com/300-american-isis-supporters-help-islamic-state-recruitment-propaganda-twitter-2207702>

INTERNATIONAL

(International) **Google brings safe browsing to Chrome for Android.** Google released its Safe Browsing technology in Google Play Services version 8.1, and Chrome for Android version 46 and above versions that will warn users when accessing a flagged Web site, including social engineering, phishing, and other malicious Web sites. <http://www.securityweek.com/google-brings-safe-browsing-chrome-android>

(International) **DNS Root servers hit by DDoS attack.** Researchers from RootOps reported that a large-scale denial-of-service (DDoS) attack on the Internet's Domain Name System (DNS) root servers caused timeouts for the B, C, G, and H

UNCLASSIFIED

node servers after 2 attacks blasted up to 5 million queries per second per DNS root name server. The DDoS attacks did not cause serious damage.

<http://news.softpedia.com/news/dns-root-servers-hit-by-ddos-attack-497363.shtml>

(International) Microsoft warns of imminent end of support for all but the latest Internet Explorer versions. Microsoft reported that the company will no longer provide security updates, non-security updates, online content updates, or technical support for older versions of its web browser, Internet Explorer in an attempt to encourage users to upgrade from Internet Explorer 11 to Microsoft Edge and Windows 10. <http://www.net-security.org/secworld.php?id=19197>

(International) Russian cyberspies use updated arsenal to attack defense contractors. Researchers from Kaspersky Lab reported that Russian-linked cyber espionage group, Pawn Storm, which targets international military, media, defense, and government organizations has updated its data theft tools and is utilizing a new version of the AZZY trojan which is being delivered by another piece of malware instead of a zero-day exploit. The new AZZY backdoor also uses an external library for command and control (C&C) communications. <http://www.securityweek.com/russian-cyberspies-use-updated-arsenal-attack-defense-contractors>

(International) International operation disrupts dorkbot botnet. Global law enforcement agencies have partnered with Microsoft, ESET, and CERT Polska to disrupt the Dorkbot botnet, dubbed Nrgbot, after the malware spread through multiple channels, including Universal Serial Bus (USB) flash drives, instant messaging programs, social network sites, exploit kits (EK), and spam emails, affecting over a million computers in 190 countries. Researchers advised users to keep their antivirus programs updated at all times to ensure proper protection from the malware that steals personal information and credentials and distributes other forms of malware. <http://www.securityweek.com/international-operation-disrupts-dorkbot-botnet>

BANKING AND FINANCE INDUSTRY

UNCLASSIFIED

UNCLASSIFIED

(International) U.S. citizen deported from Uganda to face counterfeiting charges in western Pennsylvania. Officials in Pennsylvania announced December 7 that a U.S. citizen was extradited from the Republic of Uganda and charged with allegedly operating a worldwide cyber counterfeiting scheme that circulated over \$1.4 million in fake U.S. Federal Reserve Notes from December 2013 – December 2014. <https://www.fbi.gov/pittsburgh/press-releases/2015/u.s.-citizen-deported-from-uganda-to-face-counterfeiting-charges-in-western-pennsylvania>

(International) Botnet takes “shotgun” approach to hack PoS systems. Researchers at Trend Micro reported a new campaign dubbed operation Black Atlas that targets point-of-sale (PoS) systems at small and medium sized businesses and healthcare organizations worldwide utilizing various penetration testing tools including brute force, Simple Mail Transfer Protocol (SMTP) scanners, and remote desktop viewers. Black Atlas received its name from the BlackPOS malware, works in stages, and uses variants of other known malware, allowing hackers to potentially steal sensitive information. <http://www.securityweek.com/botnet-takes-shotgun-approach-hack-pos-systems>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

Nothing Significant to Report

COMMERCIAL FACILITIES

(New Jersey) Wyndham settles FTC data breach charges. Wyndham Worldwide Corp. agreed to settle charges December 9 filed by the U.S. Federal Trade Commission to resolve allegations that the company failed to properly safeguard information on 619,000 customers following 3 data breaches in which attackers hacked into the company’s computer system and stole customers’ payment card and personal information, resulting in more than \$10.6 million in fraudulent charges. As part of the settlement, Wyndham is required to comply with a widely used industry standard to protect the safety of payment card information. <http://www.reuters.com/article/us-wyndham-ftc-cybersecurity-idUSKBN0TS24220151209#RHSWcQQVCPUHqTt0.97>

UNCLASSIFIED

(National) Security breach at restaurant chain Elephant Bar may affect customers' cards across 7 states. Dallas-based CM Ebar, LLC reported December 8 that payment processing systems for its Elephant Bar restaurants were compromised and may have exposed an unknown amount of customers' names and payment card information across seven States after a forensic investigation revealed that individuals installed malicious software onto payment systems. Customers who used their debit or credit cards from August 12 – December 4 were affected. <http://www.nbcsandiego.com/news/local/Security-Breach-at-Restaurant-Chain-Elephant-Bar-May-Affect-Customers-Cards-Across-7-States-361080981.html>

COMMUNICATIONS SECTOR

(National) Popular mobile modems plagued by zero-day flaws. Security researchers with Positive Technologies tested mobile broadband modems and routers from Huawei, Gemtek, Quanta, and ZTE and found that the 3G/4G devices were vulnerable to remote code execution, had cross-site scripting (XSS) vulnerabilities, and lacked cross-site request forgery (CSRF) protection, among other issues, leaving the devices open to attackers for exploitation. Huawei was the only vendor that released firmware updates addressing the vulnerabilities, out of the four companies tested. <http://www.securityweek.com/popular-mobile-modems-plagued-zero-day-flaws>

CRITICAL MANUFACTURING

(International) Ship data recorders vulnerable to hacker attacks. A researcher from IOActive released a report addressing serious vulnerabilities in a Furuno voyage data recorder (VRD), used in ships, including weak encryption, insecure authentication, a defective firmware mechanism, services plagued by buffer overflow, and command injection vulnerabilities that can be exploited by an unauthenticated attacker with access to the vessel's network in order to remotely execute arbitrary commands with root privileges, fully compromising the devices. <http://www.securityweek.com/ship-data-recorders-vulnerable-hacker-attacks>

UNCLASSIFIED

(International) Barbeques are now hackable thanks to ever-evolving technology.

Two American security researchers discovered that smart Internet of Things (IoT) devices can be easily abused after discovering ways to infiltrate the BBQ Guru-owned CyberQ Wifi BBQ Control, which comes manufactured with Internet capabilities, via a malicious Uniform Resource Locator (URL) code crafted by attackers intended to deceive a CyberQ owner into opening the link via a simple spear phishing campaign. Once the malicious link is opened, hackers can access the user's privileges and command the barbeque to alter its behavior.

<http://news.softpedia.com/news/barbeques-are-now-hackable-thanks-to-ever-evolving-technology-497418.shtml>

DEFENSE/ INDUSTRY BASE SECTOR

Nothing Significant to Report

EMERGENCY SERVICES

(New Mexico) Computer trouble interferes with Bernalillo County jail, other operations. Crews worked to restore service to the Bernalillo County government's computer systems December 3 following an outage that knocked out the county's Web site and email system. The outage disrupted some operations and held up the release of jail inmates.

<http://www.abqjournal.com/685371/news/abq-news/computer-trouble-interferes-with-bernalillo-county-jail-other-operations.html>

ENERGY

Nothing Significant to Report

UNCLASSIFIED

FOOD AND AGRICULTURE

Nothing Significant to Report

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(Ohio) Ohio man accused of making threats against military members. An Ohio man was charged December 8 for allegedly posting the names and addresses of 100 members of the military on social media and calling for them to be killed. A spokesman from the Cleveland U.S. attorney's office stated that the information was reposted and did not originate from the man.

<http://abcnews.go.com/US/wireStory/ohio-man-accused-making-threats-military-members-35658937>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

(International) Critical flaw found in AVG, McAfee, Kaspersky products.

Researchers from enSilo discovered a serious vulnerability in AVG, McAfee, and Kaspersky security products that allows attackers to bypass Windows protection protocol and exploit vulnerabilities in third-party applications to compromise the underlying system in a multi-stage attack. AVG, McAfee, and Kaspersky patched the flaws in each of their systems. <http://www.securityweek.com/critical-flaw-found-avg-mcafee-kaspersky-products>

(International) Stealthy backdoor compromised global organizations since 2013:

FireEye. Researchers from FireEye reported that the malicious backdoor malware dubbed, LATENTBOT primarily targets the financial services and insurance sectors to steal passwords, record keystrokes, transfer files, and enable attached microphones or webcams by leveraging malicious emails with contaminated Word documents created with Microsoft Word Intruder (MWI) exploit kit (EK) that when opened, executes malicious code and connects to a MWISTAT server and a LuminosityLink, a remote access trojan (RAT).

UNCLASSIFIED

<http://www.securityweek.com/stealthy-backdoor-compromised-global-organizations-2013-fireeye>

(International) WP engine resets password after data breach. Officials from WP Engine reported that users' credentials may have been compromised in a security breach and recommended that users reset passwords associated with WP Engine user portal, the original WP-Admin account, the WordPress database, and Secure File Transfer Protocol (SFTP), among others. The company continues to investigate the breach. <http://www.securityweek.com/wp-engine-resets-passwords-after-data-breach>

(International) Many Cisco products plagued by deserializations flaws. Cisco Systems reported that it is investigating which of its products are affected by the Java deserialization vulnerability that can be exploited for remote code execution (RCE) via the Apache Commons Collections library due to the failure of developers to ensure that untrusted serialized data is not accepted for deserialization. Cisco will release software updates addressing the flaw.

<http://www.securityweek.com/many-cisco-products-plagued-deserialization-flaws>

(International) Microsoft warns of possible attacks after Xbox certificate leaked. Microsoft released an advisory stating that the private keys to the xboxlive.com domain were inadvertently disclosed, allowing attackers to impersonate Xbox users and carry out man-in-the-middle (MitM) attacks, as well as intercept the Web site's secure connection to deceive users in providing their username and passwords to hackers. <http://www.zdnet.com/article/microsoft-warns-attacks-possible-after-xbox-certificate-leaked/>

(International) Malware steals iOS and BlackBerry backups via infected PCs. Palo Alto Networks released a report stating that many mobile backup tools lack secure encryption protocols, which can allow attackers to steal local mobile backup data and sensitive information from infected Apple Mac and Microsoft Windows computers, and discover and extract Apple iOS and Microsoft BlackBerry backup files via 6 trojan families that use the BackStab attack technique. Security researchers advised users to use backup tools that supports encryption, to maintain routine updates to their mobile operation system (OS), and to use an antivirus product, among other recommendations.

UNCLASSIFIED

UNCLASSIFIED

<http://news.softpedia.com/news/malware-steals-ios-and-blackberry-backups-via-infected-pcs-497244.shtml>

(International) Rootnik trojan modifies legitimate root tool to hack Android devices. Researchers at Palo Alto Networks discovered a new trojan, dubbed Rootnik, that uses the Root Assistant utility to gain root access on Android devices, which can allow attackers to download executable files from remote servers for local execution; steal Wi-Fi passwords, keys, Service Set Identifiers (SSID), and Basic Service Set Identifiers (BSSID); and harvest victims' private information. The trojan can infect computers by being embedded on copies of legitimate applications including Wi-Fi Analyzer, Open Camera, Infinite Loop, and HD Camera, among other tools. <http://www.securityweek.com/rootnik-trojan-modifies-legitimate-root-tool-hack-android-devices>

(International) Trifecta of security bugs affecting Dell, Lenovo, and Toshiba products. Security researchers from LizardHQ reported that three major security vulnerabilities were affecting current and older versions of computer products including Dell System Detect, Lenovo's Solution Center, and Toshiba Service Station that allows attackers to abuse an application program interface (API) to bypass the Windows User Account Control limitations on Dell products, run malicious code and escalate privileges to administrative rights on Lenovo products, and allows attackers to read parts of the Windows registry as a SYSTEM-level users in Toshiba products. The companies released recommendations on how to fix the vulnerabilities. <http://news.softpedia.com/news/trifecta-of-security-bugs-affecting-dell-lenovo-and-toshiba-products-497226.shtml>

(International) Serious flaws found in Honeywell gas detectors. Honeywell released firmware updates to its Midas gas detectors after a security researcher discovered that Midas gas detectors running firmware versions 1.13b1 and older, and Midas Black products running firmware versions 2.13b1 and older, were susceptible to a path traversal flaw and a clear text flaw that can be exploited remotely by an attacker with low skill by typing a targeted Uniform Resource Locator (URL) into the device to bypass authentication procedures. <http://www.securityweek.com/serious-flaws-found-honeywell-gas-detectors>

(International) Heartbleed, other flaws found in Advantech ICS Gateways. Researchers from Rapid7 discovered that the newest firmware versions for

UNCLASSIFIED

UNCLASSIFIED

Advantech Modbus gateway products including EKI-136X, EKI-132X, and EKI-122X were susceptible to Heartbleed attacks and Shellshock attacks which can be exploited via the Boa web server by administering any of the shell scripts in /www/sgi-bin. The vulnerabilities were tested with the genuine binaries in an emulator environment with a Metasploit module.

<http://www.securityweek.com/heartbleed-other-flaws-found-advantech-ics-gateways>

US-CERT UPDATES AND VULNERABILITIES

Bulletin (SB15-348) Vulnerability Summary for the Week of December 7, 2015

<https://www.us-cert.gov/ncas/bulletins/SB15-348>

ICS-CERT ALERTS & ADVISORIES

ICSJWG 2016 Spring Meeting - Save the Dates

The Industrial Control Systems Joint Working Group invites you to Scottsdale, AZ from May 3 - 5, 2016. We are excited to announce that the ICSJWG 2016 Spring Meeting will occur May 3 - 5, 2016 in Scottsdale, AZ. Please save the date and watch for the call-for-abstracts and registration links that are coming soon. Let us know if you have any questions, and we look forward to seeing you in Scottsdale! For additional information concerning ICSJWG and the Spring Meeting visit the ICSJWG Web page, or contact us directly at ICSJWG.Communications@hq.dhs.gov

PUBLIC HEALTH

(Connecticut) Middlesex Hospital suffers patient data security breach. Middlesex Hospital in Middletown announced December 8 that it will notify 946 patients of an October phishing scam and data breach that may have compromised patients'

UNCLASSIFIED

personal and medical information. <http://fox61.com/2015/12/08/middlesex-hospital-suffers-patient-data-security-breach/>

TRANSPORTATION

Nothing Significant to Report

WATER AND DAMS

Nothing Significant to Report

UNCLASSIFIED

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; 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, 701-328-8165

UNCLASSIFIED