

UNCLASSIFIED

20 July 2015



NORTH DAKOTA HOMELAND SECURITY Cyber Summary



The North Dakota Open Source Anti-Terrorism 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 Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

NDSLIC DISCLAIMER

The Anti-Terrorism 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

[North Dakota](#) 3

[Regional](#) 3

[National](#) 3

[International](#) 4

[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](#) 8

[Public Health](#) 9

[Transportation](#) 10

[Water and Dams](#) 10

[North Dakota Homeland Security Contacts](#) 11

NORTH DAKOTA

(North Dakota) What to do if your information was compromised in the North Dakota Workforce Safety and Insurance (WSI) hack. It was reported that over 50,000 WSI reports including names, social security numbers, and other sensitive information were breached in the beginning of July. The Village Financial Resource Center Counselor, Alicia Kellebrew, suggest looking at your credit report. WSI has contacted ALL Clear ID for one year to assist with those who are affected. Taking advantage of the All Clear system may help clean up your credit if it is affected.

<http://www.valleynewslive.com/home/headlines/Your-Information-Was-HackedNow-What-315112081.html>

REGIONAL

(Minnesota) Clinic announces inappropriate access of records. The Mayo Clinic Health System announced July 11 that a data breach which was discovered within the past two months after a Red Wing, Minnesota employee inappropriately accessed records for 601 patients. An internal investigation was launched upon discovery of the breach, and all affected patients are being notified.

<http://www.republican-eagle.com/news/3783678-clinic-announces-inappropriate-access-records>

NATIONAL

(National) How prepared is the U.S. against cyber-attacks? On Wednesday this nation faced technical glitches that both grounded hundreds of United Airlines flights and halted the NYSE. It was also revealed that a hack had compromised 21.5 million records belonging to American workers. It is believed that none of the information has been released and no confirmation of a specific attacker has been released.

<http://www.nbcnews.com/meet-the-press/video/how-prepared-is-the-u.s.-against-cyber-attacks--482988611764>

INTERNATIONAL

(International) Darkode computer hacking forum shuts after investigation spanning 20 countries. U.S. authorities filed hacking charges against 12 suspects affiliated with the Darkode hacker Web forum after the FBI and law enforcement organizations from 20 countries shut down the site and arrested or searched 70 Darkode members worldwide. The Web site allowed hackers to share technology and tradecraft used to infect computers and wireless devices of victims.

http://www.networkworld.com/article/2948634/darkode-computer-hacking-forum-shuts-after-investigation-spanning-20-countries.html#tk.rss_all

(International) Chinese APT group uses Hacking Team's Flash Player exploit. Security researchers from Volexity reported that the Wekby advanced persistent threat group (APT), also known as APT 18, Dynamite Panda, and TG-0416, was leveraging an Adobe Flash Player exploit revealed through the July breach of the software company Hacking Team by sending spear-phishing emails purporting to be from Adobe which directed users to download a compromised Flash Player file containing malware.

<http://www.securityweek.com/chinese-apt-group-uses-hacking-team%E2%80%99s-flash-player-exploit>

(International) APT group uses Seaduke trojan to steal data from high-value targets. Security researchers from Symantec released an analysis of the highly-configurable Seaduke trojan used by an advanced persistent threat (APT) group known for cyber-espionage attacks against high-value targets including government organizations. The report revealed that the trojan is installed onto select systems through the CozyDuke trojan, and that it shares similarities with other "Duke" malware.

<http://www.securityweek.com/apt-group-uses-seaduke-trojan-steal-data-high-value-targets>

BANKING AND FINANCE INDUSTRY

(Kansas) ATM skimmer use discovered at 7th Wichita bank. Home Bank & Trust Co., officials reported that an ATM skimming device was used at a Wichita location, bringing the total number of skimmers found in Wichita in July to seven.

UNCLASSIFIED

<http://www.kake.com/home/headlines/Another-ATM-Skimmer-Found-At-Wichita-Bank--315526371.html>

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

Nothing Significant to Report

COMMERCIAL FACILITIES

(National) Data breach at ‘sweetest place on earth’ may have compromised guests’ financial info. Hershey Entertainment & Resorts reported July 10 that its point-of-sale system (PoS) was compromised after a program was installed in its payment system that extracted payment card data from February 14 – June 2. The company is working to resolve the issue and is offering card monitoring to those affected.

<http://www.nbcphiladelphia.com/news/local/Hershey-Entertainmnet-Data-Breach-313430341.html>

(International) N-Able RSMWinService contains hard coded security constants allowing decryption of domain administrator password. A remote attacker with domain user credentials or access to RSM files on an installed system can obtain domain administrator access. It is believed to affect version 9.5.0, as well as version 9.0 through 9.4. The current solution is to apply an update to the software as it is believed that 9.5.1 and above and 10.0 have addressed the issue.

<http://www.kb.cert.org/vuls/id/912036>

COMMUNICATIONS SECTOR

(Michigan) Cable provider WOW says weekend attach on servers left Michigan customers without internet service. Metro Detroit customers of WOW, an Internet, cable and phone service provider, experienced an Internet outage during the weekend of July 11 due to an attack on the Domain Name Server. Crews repaired the issue July 13 and most customers have internet service.

UNCLASSIFIED

UNCLASSIFIED

<http://www.wxyz.com/news/cable-provider-wow-says-attack-has-left-michigan-customers-without-internet-service>

CRITICAL MANUFACTURING

Nothing Significant to Report

DEFENSE/ INDUSTRY BASE SECTOR

(National) Current, former Guard members warned of data breach. An Army National Guard spokesperson announced July 14 a recent security breach affecting over 850,000 current and former Guard members was caused by a mishandled data transfer, not a cyberattack.

<http://www.armytimes.com/story/military/guard-reserve/2015/07/14/national-guard-data-breach-opm-ssn/30150319/>

(International) Java zero-day used in attacks on NATO member, U.S. defense organization. Security researchers at Trend Micro reported that the cyber-espionage group with monikers including Pawn Storm and APT28 was using a Java Oracle SE zero-day remote code execution vulnerability in attacks directed against the armed forces of a NATO member country as well as a U.S. defense organization by sending out emails containing links to malicious domains containing the exploit and a trojan dropper.

<http://www.securityweek.com/java-zero-day-used-attacks-nato-member-us-defense-organization>

EMERGENCY SERVICES

Nothing Significant to Report

UNCLASSIFIED

ENERGY

(National) Eaton's Cooper Power Series Form 6 Control and Idea/IdeaPlus Relays with Ethernet Vulnerability. An attacker could potentially use this TCP/IP stack vulnerability to enable a man-in-the-middle (MitM) attack against products that are Internet facing. A successful MitM attack allow the attacker to cause a crash of the system.

[https://ics-cert.us-cert.gov/advisories/ICSA-15-006-01\](https://ics-cert.us-cert.gov/advisories/ICSA-15-006-01)

(International) Siemens SICAM MIC Authentication Bypass Vulnerability. Attackers with network access to the device's web interface (Port 80/TCP) could possibly circumvent authentication and perform administrative operations. A legitimate user must be logged into the web interface for the attack to be successful.

<https://ics-cert.us-cert.gov/advisories/ICSA-15-195-01>

FOOD AND AGRICULTURE

Nothing Significant to Report

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(National) Not just OPM – agency cybersecurity incidents on the rise. A report released by the Government Accountability Office July 8 showed both cyber and non-cyber security breaches affecting Federal systems have steadily increased from 6,000 in 2006 to 67,000 in 2014. The report advocated risk-based cybersecurity programs and improved responses to security incidents.

<http://www.nextgov.com/cybersecurity/2015/07/agency-security-incidents-rise/117496/>

(National) OPM hack: U.S. has not notified 21.5 million victims of massive data breach. A July 14 report revealed that the U.S. Office of Personnel Management (OPM) has yet to officially notify 21.5 million victims of a cyberattack discovered

UNCLASSIFIED

UNCLASSIFIED

in May which exposed sensitive information disclosed in security clearance investigations. Multiple Federal agencies are working with OPM to develop a central system to inform victims, although officials reported this could be delayed for several weeks due to the complicated nature of the data.

<http://www.ibtimes.com/opm-hack-us-has-not-notified-215-million-victims-massive-data-breach-2008940>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

(International) Security support ends for remaining Windows XP machines.

Microsoft ended security support for Microsoft Security Essentials customers running Windows XP as part of its July Patch Tuesday roll-out, and released security advisories for a patched race condition flaw in the Malicious Software Removal Tool (MSRT) allowing for privilege escalation, as well as an update enhancing use of Data Encryption Standard (DES) encryption keys.

<https://threatpost.com/security-support-ends-for-remaining-windows-xp-machines/113796>

(International) Nearly all Web sites have serious security vulnerabilities.

Acunetix released a report on 15,000 Web site and network scans of 5,500 companies revealing that almost half of Web applications scanned contained high security vulnerabilities, and 4 of 5 were affected by medium security vulnerabilities, plying that most organizations fail to comply with the Payment Card Industry Data Security Standard (PCI DSS), among other findings.

<http://www.net-security.org/secworld.php?id=18637>

(International) Microsoft releases July 2015 Security Bulletin. Microsoft released 14 updates on July 14 to address vulnerabilities including but not limited to remote code execution or elevation of privileges. Details of the vulnerabilities can be found in [Microsoft's July security bulletin](#).

<https://www.us-cert.gov/ncas/current-activity/2015/07/14/Microsoft-Releases-July-2015-Security-Bulletin>

(International) Microsoft releases security update. Microsoft has released a security update to address a critical vulnerability in Windows. Exploitation of this vulnerability may allow a remote attacker to take control of an affected system.

UNCLASSIFIED

To see if your software is affected please see Microsoft Security Bulletin [MS11-078](#).

<https://www.us-cert.gov/ncas/current-activity/2015/07/20/Microsoft-Releases-Security-Update>

(international) Total Commander File Info plugin vulnerable to denial of service via an out-of-bounds read. An attacker that can control the contents of certain file types may be able to cause an out-of-bounds read error in Total Commander File Plugin version 2.21. The solution to this issue is to apply the newest update. Total Commander File Info plugin has released version 2.22, which addresses the issue.

<http://www.kb.cert.org/vuls/id/813631>

(International) Hackers of cheaters' site Ashley Madison threaten to expose user profiles. Millions of users' information is at risk of exposure. A representative of the company has said, "At this time, we have been able to secure our sites, and close the unauthorized access points." The hack is believed to be from the hacking group dubbed The Impact Team.

<http://www.cnet.com/news/hackers-of-cheaters-site-ashley-madison-threaten-to-expose-user-profiles/>

PUBLIC HEALTH

(Pennsylvania) Misdirected email faulted in data breach affecting hundreds of UPMC insurance customers. An email meant for a physician's office in Lawrence County was mistakenly sent to an incorrect address, revealing sensitive personal information for 722 UPMC Health Plan members, the insurance company announced July 15. The breach was discovered June 4, and the Department of Health and Human Services was alerted July 2.

<http://www.post-gazette.com/business/healthcare-business/2015/07/15/Misdirected-email-compromises-hundreds-of-UPMC-insurance-customers/stories/201507150176>

(National) CMS cutting-edge technology identifies and prevents \$820 million in improper Medicare payments in first three years. The U.S. Centers for Medicare and Medicaid Services announced July 14 its Fraud Prevention System had

UNCLASSIFIED

UNCLASSIFIED

identified or blocked \$820 million in inappropriate payments during its first 3 years by using predictive analytics to identify irregular billing patterns.

<http://www.cms.gov/Newsroom/MediaReleaseDatabase/Press-releases/2015-Press-releases-items/2015-07-14.html>

(National) Blue Cross Blue Shield rolls out new identity protections. Blue Cross and Blue Shield health insurers announced July 14 that they would offer free credit monitoring and fraud detection to millions of unaffected customers nationwide by January 1, in addition to those provided to victims of recent data breaches which affected the company early 2015.

<http://www.post-gazette.com/business/healthcare-business/2015/07/15/Blue-Cross-Blue-Shield-rolls-out-new-identity-protections/stories/201507150098>

TRANSPORTATION

(Nevada) DMV camera, scanner systems back up after electrical problem. A Las Vegas Department of Motor Vehicles location was evacuated and camera and scanner systems used for identification cards and driver's licenses were down State-wide July 9 following a transformer blow-out near the East Sahara facility.

<http://www.dailyjournal.net/view/story/2650f6022d794bbbb970a4bff2490fb/NV--DMV-Outage>

WATER AND DAMS

Nothing Significant to Report

NORTH DAKOTA HOMELAND SECURITY CONTACTS

To report a homeland security or cyber 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