NORTH DAKOTA STATE AND LOCAL INTELLIGENCE CENTER

Bi-Weekly Cyber Rollup

April 17th, 2020

Included In This Summary

Click on the *section header* to go directly to that location in the summary.

NORTH DAKOTA AND REGIONAL

(U) Utah CEO from Bismarck pleads guilty for having more than 13,000 files of child porn
(U) A Utah Tech company CEO from Bismarck pleaded guilty to charges related to having more than 13,000 files of child pornography.Utah prosecutors say 40-year-old Douglas Saltsman pleaded guilty on March 19 to three counts of sexual exploitation of a minor.
Source: (U) https://www.kfyrtv.com/content/news/Utah-CEO-from-Bismarck-pleads-guilty-for-having-more-than-13000-files-of-child-porn-569647471.html?fbclid=IwAR2ugB2ne1tYFSfc8rEc2ksIcwURDJAS1JIuVA9zF7tVjSBpdL273eFCD20

(U) Dakota Community Bank & Trust Scam Alert
(U) Dakota Community Bank & Trust observed that customers and non-customers receive text messages from a scammer acting as the bank
Source: (U) https://www.facebook.com/dakotacommunitybank/posts/2932555810123482

(U) North Dakota students receive national awards, compete in online cybersecurity competition
(U) Chief Information Officer Shawn Riley today congratulated ten North Dakota students who received national recognition by the National Center for Women & Information Technology (NCWIT), as well as Valley City State University student Shane Hitch who was a top-five finisher in a Capture the Flag cybersecurity competition hosted by NICERC, the National Integrated Cyber Education Research Center. The CTF was held in conjunction with the first-of-its-kind technology focused, multi-industry career expo, Dakota Strike, scheduled for April 8 at the Fargodome, which was cancelled due to COVID-19.
Source: (U) https://www.nd.gov/itd/news/6753/north-dakota-students-receive-national-awards-compete-online-cybersecurity-competition

(U) Realtors Use Technology to Connect with Clients and COVID-19
(U) FARGO, N.D.- Aspire Realty in Fargo is used to showing 15 to 25 houses a week and selling about 11 houses a month. “Through the month of March, business was really good, but coming into April and now as we’re seeing a massive increase in the numbers of positive cases, we’re starting to slow down tremendously,” says Katherine Kiernan, the owner of Aspire Realty. But, the agency says the show must go on- at least virtually.
Source: (U) https://www.kvrr.com/2020/04/10/realtors-use-technology-to-connect-with-clients-amid-covid-19/

(U) 3D-Fuel encourages customers to print PPE with discounted prices
(U) FARGO, N.D. — Fargo-based buisness 3D Fuel has found a unique way to lend a hand in the fight against COVID-19. “It’s kind of like hand sanitizer,” said the company’s CEO John Schneider. “It may not sound that essential. It’s not really the cool part of virus response, but it is still incredibly important.”
Source: (U) https://www.kvrr.com/2020/04/12/3d-fuel-encourages-customers-to-print-ppe-with-discounted-prices/

(U) Applications open for Al Golden Scholarship program
(U) BISMARCK – The North Dakota Petroleum Council is now accepting applications for its Al Golden Scholarship program for the 2020-2021 school year. The NDPC will award up to nine $2,000 scholarships to students pursuing degrees or training in an energy-related field.
Source: (U) https://www.minotdailynews.com/news/local-news/2020/04/applications-open-for-al-golden-scholarship-program/

(U) SRT annual meeting postponed
(U) SRT Communications has postponed its annual meeting until Oct. 1 at the North Dakota State Fair Center in Minot. The meeting is to elect SRT's Board of Directors, hold a business meeting and review the financial statements of the cooperative. The original date was scheduled for June.
Source: (U) https://www.minotdailynews.com/news/local-news/2020/04/srt-annual-meeting-postponed/

(U) Minot State University presents 'Surveillance: Your Privacy Matters or Not?" Campus and Community Dialogue
(U) On Wednesday, Minot State University will host the Campus and Community Dialogues event "Surveillance: Your Privacy Matters or Not?" from 7-9 p.m. via Facebook Live @MinotStateUniversity and askMSU.com/dialogues.
Source: (U) https://www.minotdailynews.com/news/local-news/2020/04/applications-open-for-al-golden-scholarship-program/

NATIONAL

(U) Travelex Paid $2.3 Million in Bitcoin Following Ransomware Attack
(U) Foreign exchange company Travelex paid hackers $2.3 million in bitcoin to regain access to their network following a ransomware attack. According to a report by the Wall Street Journal, London-based Travelex paid hackers 285 BTC after being advised by experts on how to handle the ransomware attack.
Source: (U) https://www.cryptoglobe.com/latest/2020/04/travelex-paid-2-3-million-in-bitcoin-following-ransomware-attack/

(U) BBB Tip: Thinking of sharing your senior photo on Facebook? Think twice!
(U) Watch out, scammers or hackers who surf through social media sites will see these #ClassOf2020 posts, and will now have the name of your high school and graduation year, which are common online security questions. All it takes is an internet search to reveal more information about you, such as family members, your real name, birthdate or even where you live.
Source: (U) https://www.bbb.org/article/news-releases/22088-bbb-tip-thinking-of-sharing-your-senior-photo-on-facebook-think-twice

(U) Coronavirus Update App Leads to Project Spy Android and iOS Spyware
(U) We discovered a potential cyberespionage campaign, which we have named Project Spy, that infects Android and iOS devices with spyware (detected by Trend Micro as AndroidOS_ProjectSpy.HRX and IOS_ProjectSpy.A, respectively). Project Spy uses the ongoing coronavirus pandemic as a lure, posing as an app called Coronavirus Updates. We also found similarities in two older samples disguised as a Google service and, subsequently, as a music app after further investigation.
Source: (U) https://blog.trendmicro.com/trendlabs-security-intelligence/coronavirus-update-app-leads-to-project-spy-android-and-ios-spyware/?web_view=true

(U) TikTok users beware: Hackers could swap your videos with their own
(U) Mobile app developers Tommy Mysk and Talal Haj Bakry just published a blog article entitled “TikTok vulnerability enables hackers to show users fake videos.” As far as we can see, they’re right.
Source: (U) https://blog.trendmicro.com/trendlabs-security-intelligence/coronavirus-update-app-leads-to-project-spy-android-and-ios-spyware/?web_view=true

(U) Hospitals face a surge of cyberattacks during the novel coronavirus pandemic
(U) Hospitals that are already pushed to their limit dealing with a patient surge from the novel coronavirus pandemic are getting slammed with cyberattacks and digital scams, as well. Among the most damaging are ransomware attacks that aim to shut down entire hospitals until they pay a fee that can cost millions of dollars.
Source: (U) https://www.sfgate.com/news/article/Hospitals-face-a-surge-of-cyberattacks-during-the-15201802.php

(U) FBI says Foreign States hacked into U.S. COVID-19 Research Centers: Report
(U) While most of the COVID-19 threat warnings emerging from the Federal Bureau of Investigations have been regarding scams and fraud, now something a lot more sinister and disturbing has emerged. It has been reported that the FBI has seen evidence of foreign state-sponsored hackers breaking into U.S. COVID-19 research institutions.
Source: (U) https://www.forbes.com/sites/daveywinder/2020/04/17/fbi-says-foreign-states-hacked-into-us-covid-19-research-centers-report/#273637d53c29

(U) Linksys asks users to reset passwords after hacks hijacked home routers last month
(U) Router vendor Linksys has locked user accounts on its Smart WiFi cloud service and is asking users to reset passwords after hackers have been observed hijacking accounts and changing router settings to redirect users to malware sites. Linksys' decision only impacts Smart WiFi accounts. Linksys Smart WiFi is a cloud-based account system that lets device owners connect to Linksys routers (and other equipment) over the internet to manage router settings.
Source: (U) https://www.zdnet.com/article/linksys-asks-users-to-reset-passwords-after-hackers-hijacked-home-routers-last-month/

(U) CISA warns Patched Pulse Secure VPNs could still Expose Organizations to Hackers
(U) The United States Cybersecurity and Infrastructure Security Agency (CISA) yesterday issued a fresh advisory alerting organizations to change all their Active Directory credentials as

a defense against cyberattacks trying to leverage a known remote code execution (RCE) vulnerability in Pulse Secure VPN servers—even if they have already patched it.
Source: (U) https://thehackernews.com/2020/04/pulse-secure-vpn-vulnerability.html

INTERNATIONAL

(U) Leading accounting firm MNP hit with cyberattack
(U) A leading accounting firm in Canada forced a company-wide shutdown of their systems after getting hit with a cyberattack last weekend, BleepingComputer has learned. Canadian accounting firm MNP's systems were impacted last weekend in what BleepingComputer was told was a ransomware attack.
Source: (U) https://www.bleepingcomputer.com/news/security/leading-accounting-firm-mnp-hit-with-cyberattack/

(U) Mastering Communication in Cyber Intelligence Activities: A Concise User Guide
(U) Communication is key in intelligence activities. On the one hand, it is essential to transfer to a number of recipients the knowledge coming from information acquisition and analysis ("intelligence communication"); on the other hand, it is crucial to understand and control the communication connected with the activities carried out ("communication intelligence").
Source: (U) https://securityaffairs.co/wordpress/101760/intelligence/communication-cyber-intelligence-activities.html

(U) Hunting the coronavirus in the dark web
(U) While the COVID19 pandemic was spreading a global scale, specific goods became victims of looting and financial speculation. In my first investigation, I focused my searches on masks to avoid contagion and disinfectant products, because these goods quickly disappeared from the official markets due to the high demand.
Source: (U) https://securityaffairs.co/wordpress/101689/deep-web/darkweb-coronavirus-part-2.html

(U) Shipping giant MSC discloses a malware-based attack
(U) The shipping giant Mediterranean Shipping Company (MSC) discloses a malware-based attack that took place on April 10. The incident affected the company's data center and took down its website, *msc.com*, and its myMSC customer and vendor portal. "*The incident was confined to MSC's headquarters in Geneva only and affected the availability of some of MSC's digital tools and msc.com for a few days during the Easter holiday long weekend. MSC agencies remained fully functional and continued serving customers as usual during this time." reads the advisory published by MSC.*
Source: (U) https://securityaffairs.co/wordpress/101740/cyber-crime/msc-malware-attack.html

(U) Syria-linked APT group SEA targets Android users with COVID-19 lures
(U) Syrian hackers are behind a long-running campaign that has been active since January 2018 and that targets Arabic-speaking Android users. The campaign aimed at users in Syria

and surrounding regions was spotted by experts from mobile security firm Lookout, threat actors employed tens of Android apps, none of which is available in the official Google Play Store.
Source: (U) https://securityaffairs.co/wordpress/101754/malware/sea-targets-android.html

(U) Grandoreiro Malware Now Targeting Banks in Spain
(U) During the past few months, IBM X-Force researchers have noticed a familiar malware threat that typically affects bank customers in Brazil has spread to attack banks in Spain. The rise in campaigns prompted us to look into it further. Grandoreiro, a remote-overlay banking Trojan, has migrated to Spain without significant modification, proving that attackers who know the malware from its Brazilian origins are either collaborating with attackers in Spain or have themselves spread the attacks to the region.
Source: (U) https://securityintelligence.com/posts/grandoreiro-malware-now-targeting-banks-in-spain/

Email: ndslic@nd.gov NDSLIC: 701-328-8172

Sensitivity/ Handling Notice:
Sources may use **TLP:WHITE** when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.