TLP:WHITE

NORTH DAKOTA STATE AND LOCAL INTELLIGENCE CENTER

Bi-Weekly Cyber Rollup

April 3rd, 2020

Included In This Summary

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

TLP:WHITE

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

(U) Coronavirus: Tunisia deploys Police Robot on Lockdown patrol
(U) UK government defends PM's use of Zoom
(U) Coronavirus: Israeli Spyware Firm pitches to be COVID-19 Savior

NORTH DAKOTA AND REGIONAL

(U) Stenehjem: Don't be Fooled by Coronavirus Scam
(U) "Scam artists are using the current pandemic situation to exploit our fears. We can stop them by getting the facts and using a common sense approach when dealing with those offering what seem to be too-good-to-be-true opportunities," said Stenehjem.
Source: (U) https://www.newsdakota.com/2020/04/02/stenehjem-dont-be-fooled-by-a-coronavirus-scam/

(U) North Dakota's Unified approach to Data Protection and Cybersecurity
(U) With incidents of hacking and identity theft on the rise, North Dakota aims to train 700 teachers tocyber-educate every school student in the state.
Source: (U) https://www.newsdakota.com/2020/03/25/north-dakotas-unified-approach-to-data-protection-and-cybersecurity/

(U) FirstLink is there for People feeling isolated during Coronavirus Outbreak
(U) FARGO, N.D. – With an economic and social decline impacting society, FirstLink hopes that more people lean on them for support. The FirstLink call center at 211 is known for its suicide prevention care. They are able to help their callers by connecting them with resources to help them get through their day-to-day lives.
Source: (U) https://www.kvrr.com/2020/04/02/firstlink-is-there-for-people-feeling-isolated-during-coronavirus-outbreak/

(U) Distance Learning in Full Swing for Students across Fargo-Moorhead
(U) When Minnesota and North Dakota officials decided to close schools due to the Coronavirus, educators across the metro scrambled to put together a plan of how to move forward.
Source: (U) https://www.kvrr.com/2020/04/02/distance-learning-in-full-swing-for-students-across-fargo-moorhead/

(U) Fargo Police warn of Grandparent Scams amid COVID-19 Pandemic
(U) The Fargo Police Department is warning people about scams that target grandparents specifically. Police say scammers pose as grandchildren who are supposedly in trouble and need money wired to them immediately.
Source: (U) https://www.kvrr.com/2020/04/03/fargo-police-warn-of-grandparent-scams-amid-covid-19-pandemic/

(U) Use 3D Printer for COVID-19 Relief Efforts
(U) Three-D printers are proving themselves useful in the Coronavirus battle. According to *KFYR*, five Minot local residents are helping hospital workers protect themselves from COVID-19. The people are utilizing 3D printers to make masks for the hospital workers at Trinity Health in Minot. So far, these good Samaritans are have produced 50 masks to donate, with the hopes of donating 400 masks to Trinity.
Source: (U) https://hot975fm.com/use-your-3d-printer-for-covid-19-relief-efforts/

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

(U) Rural Internet's Importance Highlighted by Coronavirus
(U) Getting broadband internet access to rural areas has been a goal for rural advocates and service providers alike for years, but the COVID-19 pandemic has made such access more important than ever.
Source: (U) https://www.farmforum.net/farm_forum/rural-internets-importance-highlighted-by-coronavirus/article_5702c228-02a7-5431-b8f7-981d54c14af9.html

NATIONAL

(U) 'Not Business as Usual' for Government's Tech Workers
(U) The technology officials working in state and local government say that while their core mission remains to support agency operations, they're being confronted with new tasks and challenges they hadn't previously considered.
Source: (U) https://statescoop.com/not-business-as-usual-for-governments-tech-workers/

(U) Hackers target WHO, other Heath Organizations fighting COVID-19
(U) The World Health Organization was the target of an unsuccessful cyberattack earlier this month, with hackers trying to steal passwords from agency staffers. Officials say attack attempts have more than doubled in recent weeks. Hackers have apparently been trying to breach the firewalls of the World Health Organization (WHO), which was the target of an unsuccessful cyberattack earlier this month, according to Reuters.
Source: (U) https://www.govtech.com/security/Hackers-Target-WHO-Other-Health-Organizations-Fighting-COVID-19.html?utm_term=READ%20MORE&utm_campaign=Hackers%20Target%20WHO%2C%20Other%20Health%20Organizations%20Fighting%20COVID-19&utm_content=email&utm_source=Act-On+Software&utm_medium=email

(U) 50 Tips to Improve your Work from Home Life
(U) Remote work in the U.S. increased by 159% from 2005 to 2017, according to data from FlexJobs and Global Workplace Analytics. Before the COVID-19 outbreak, 4.7 million people—about 3.4% of the population—worked from home. In light of social-distancing and shelter-in-place orders, that number has jumped exponentially in the last month and is expected to continue climbing throughout 2020.
Source: (U) https://hot975fm.com/50-tips-to-improve-your-work-from-home-life/

(U) Quarantine together is a Dating app for These Times
(U) If there has ever been a weird time to date, this is it. But even as millions of Americans stay at home due to the coronavirus pandemic, nothing is stopping them from dating online. Daniel Ahmadizadeh and Christopher Smeder designed Quarantine Together, a dating app for exactly this moment.
Source: (U) https://www.cnn.com/2020/03/29/us/dating-app-quarantine-wellness-trnd/index.html

(U) Protecting Yourself from Online Scammers
(U) COVID-19 is an issue that has been on many people's minds during the past few weeks. Unfortunately, scammers and other malicious actors are using people's fears and uncertainties to take advantage of this crisis. Because of this unfortunate reality, I want to point out a few ways to identify potential scam messages for a more general audience.

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

Source: (U) https://contextualsecurity.com/2020/03/protecting-yourself-from-online-scammers/

(U) Zoom's Web Client is Down, Users Report 403 Forbidden Errors
(U) Zoom users are currently reporting that they are unable to use the Zoom web client or start and attend webinars, with reports saying that the web client is throwing '403 Forbidden' errors.
Source: (U) https://www.bleepingcomputer.com/news/technology/zooms-web-client-is-down-users-report-403-forbidden-errors/

(U) Microsoft: Emotet took down a Network by Overheating All Computers
(U) Microsoft says that an Emotet infection was able to take down an organization's entire network by maxing out CPUs on Windows devices and bringing its Internet connection down to a crawl after one employee was tricked to open a phishing email attachment.
Source: (U) https://www.bleepingcomputer.com/news/security/microsoft-emotet-took-down-a-network-by-overheating-all-computers/

(U) New Coronavirus-Themed Malware locks you out of Windows
(U) With school closed due to the Coronavirus pandemic, some kids are creating malware to keep themselves occupied. Such is the case with a variety of new MBRLocker variants being released, including one with a Coronavirus theme. MBRLockers are programs that replace the 'master boot record' of a computer so that it prevents the operating system from starting and displays a ransom note or other message instead.
Source: (U) https://www.bleepingcomputer.com/news/security/new-coronavirus-themed-malware-locks-you-out-of-windows/

(U) Hacker Group backdoors thousands of Microsoft SQL Servers daily
(U) Hackers have been brute-forcing thousands of vulnerable Microsoft SQL (MSSQL) servers daily to install cryptominers and remote access Trojans (RATs) since May 2018 as researchers at Guardicore Labs discovered in December. This attack campaign is still actively infecting between 2,000 and 3,000 MSSQL servers on a daily basis and it was dubbed Vollgar because the cryptomining scripts it deploys on compromised MSSQL will mine for Monero (XMR) and Vollar (VDS) cryptocurrency.
Source: (U) https://www.bleepingcomputer.com/news/security/hacker-group-backdoors-thousands-of-microsoft-sql-servers-daily/

(U) Phishers try 'Text Direction Deception' technique to Bypass Email Filters
(U) Scammers can be pretty innovative when it comes to finding new ways to sneak phishing messages past secure email gateways and other filtering mechanisms. One example is "text direction deception," a tactic where an attacker forces an HTML rendering engine to correctly display text that has been deliberately entered backward in the code — for example, getting text that exists in HTML code as "563 eciffO" to render forward correctly as "Office 365."
Source: (U) https://www.darkreading.com/attacks-breaches/phishers-try-text-direction-deception-technique-to-bypass-email-filters/d/d-id/1337483

(U) New Magecart Skimmer Infects 19 Victim Websites
(U) MakeFrame, named for its ability to make iframes for skimming payment data, is attributed to Magecart Group 7. A new Magecart skimmer, dubbed MakeFrame, has been observed compromising 19 victim websites. The skimmer was named for its ability to make iframes for skimming payment data.

Source: (U) https://www.darkreading.com/vulnerabilities---threats/new-magecart-skimmer-infects-19-victim-websites/d/d-id/1337472

(U) FBI Warns Education & Remote Work Platforms about Cyberattacks
(U) The FBI expects attackers will target virtual environments as more organizations rely on them as a result of the COVID-19 pandemic. The FBI's Internet Crime Complaint Center (IC3) has issued an advisory that warns online education and remote work platforms of an increase in cyberattacks as more public and private organizations rely on virtual tools because of the COVID-19 pandemic.
Source: (U) https://www.darkreading.com/vulnerabilities---threats/fbi-warns-education-and-remote-work-platforms-about-cyberattacks/d/d-id/1337485

INTERNATIONAL

(U) AppTrana offers Protection to Online Businesses during Coronavirus Outbreak
(U) Cybersecurity company Indusface that holds expertise in keeping applications over the internet secure has decided to step up and do our bit to the society. During this unprecedented time, Indusface has announced to support organizations affected by COVID-19 by offering professional cybersecurity protection to their online businesses at free of cost for at least a month.
Source: (U) https://thehackernews.com/2020/03/apptrana-web-app-security.html

(U) Hackers attack around 300,000 devices in South Africa amid COVID-19 Crisis
(U) Based on a research from Kaspersky, businesses in South Africa suffered several network attacks between March 15 to March 21, 2020. It revealed that cybercriminals attacked up to 310,000 devices in one week. With millions of people in the country accessing corporate networks remotely, hackers have increased attacks on IT networks, *MyBroadband* reported.
Source: (U) https://www.cisomag.com/hackers-attack-around-300000-devices-in-south-africa-amid-covid-19-crisis/

(U) Tech against Corona: A Cybersecurity Campaign to Fight COVID-19-related cybercrimes in the Netherlands
(U) A group of organizations in the Netherlands have launched the “Tech against Corona” campaign to help the Dutch government with their technology and security skills, and mitigate COVID-19-related cybercrimes. The companies participating in the campaign will offer their technology, algorithms, and security services to the government entities, aid workers, health care providers and hospitals free of charge, *Public Matters* reported.
Source: (U) https://www.cisomag.com/tech-against-corona-a-cybersecurity-campaign-to-fight-covid-19-related-cybercrimes-in-the-netherlands/

(U) Hackers attack Database of India’s COVID-19 Patients and Potential Suspects
(U) Kerala, one of the worst-hit states in India’s COVID-19 crisis, reported five positive cases from Aythala in Ranni-Pazhavangady panchayat. The database of all the active patients, and those who came in direct contact with them, was maintained on the district administrator’s office computers. The data included information on other people coming into the district from abroad and those kept in self-quarantine, their recent travel history, residential addresses and contact details, etc. District Collector P. B. Nooh admitted that this COVID-19 database has been hacked and has since sought an investigation into the incident.

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

Source: (U) https://www.cisomag.com/hackers-attack-database-of-indias-covid-19-patients-and-potential-suspects/

(U) Researchers Uncover a Nigerian Hacker's Pursuit of his Million Dollar Dream
(U) Social engineering-driven malware threats continue to be a big threat, but new research details how cybercriminals profit off such schemes to launder hundreds of thousands of dollars from stolen credit cards of unsuspecting victims.
Source: (U) https://thehackernews.com/2020/03/nigerian-hacker-million-dollars.html

(U) Coronavirus: Should the UK use drones to disinfect public spaces?
(U) A group of drone experts is calling on the UK government to relax regulations on chemical spraying from the air during the coronavirus pandemic. It wants to train drone pilots from the emergency services to spray public areas with disinfectant.
Source: (U) https://www.bbc.com/news/health-52109824?intlink_from_url=https://www.bbc.com/news/technology&link_location=live-reporting-story

(U) Coronavirus: Tunisia deploys Police Robot on Lockdown patrol
(U) A police robot has been deployed to patrol areas of Tunisia's capital, Tunis, to ensure that people are observing a coronavirus lockdown. If it spies anyone walking in the largely deserted streets, it approaches them and asks why they are out.
Source: (U) https://www.bbc.com/news/world-africa-52148639?intlink_from_url=https://www.bbc.com/news/technology&link_location=live-reporting-story

(U) UK government defends PM's use of Zoom
(U) The UK government has defended using Zoom to hold cabinet video conferences. Questions had been raised about potential security risks after the prime minister tweeted a picture in which a meeting ID was visible.
Source: (U) https://www.bbc.com/news/technology-52126534

(U) Coronavirus: Israeli Spyware Firm pitches to be COVID-19 Savior
(U) A controversial Israeli cyber-security company is marketing software that uses mobile phone data to monitor and predict the spread of the coronavirus. NSO Group says it is in talks with governments around the world, and claims some are already testing it.
Source: (U) https://www.bbc.com/news/health-52134452

TLP:WHITE

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