 Included In This Summary
Click on the section header to go directly to that location in the summary.

NORTH DAKOTA AND REGIONAL
(U) NDIT, NDUS Partner to Strengthen Cybersecurity for Higher Ed Campuses
(U) Schell Selected for Leadership Position in National Tech Professionals Association
(U) CIO, CISO to Participate in Third Annual CyberCon

NATIONAL
(U) U.S. Treasury Sanctions Hacking Group Backed by Iranian Intelligence
(U) U.S. Announces Charges Against 2 Russian and 2 Iranian Hackers
(U) Cryptocurrency Tracer Could Give Cops an Edge on Cybercrime
(U) Massachusetts City Dodges Eastern European Hack Attempt
(U) US Bans WeChat, TikTok from App Stores, Threatens Shutdowns

INTERNATIONAL
(U) Ransomware Attack on Hospital in Dusseldorf Leads to Unexpected Death
(U) Major Instagram App Bug Could've Given Hackers Remote Access to Your Phone
(U) A New Hacking Group Hitting Russian Companies with Ransomware
(U) British Hacker Sentenced to 5 Years for Blackmailing U.S. Companies
(U) Unsecured Microsoft Bing Server Exposed Users' Search Queries and Location
(U) A Bug Could Let Attackers Hijack Firefox for Android via Wi-Fi Network

TLP: WHITE
NORTH DAKOTA AND REGIONAL

(U) NDIT, NDUS Partner to Strengthen Cybersecurity for Higher Ed Campuses
(U) North Dakota Chief Information Security Officer Kevin Ford and NDUS Vice Chancellor of Information Technology Darin King announced today that NDIT Cybersecurity Operations Center (CyOC) and North Dakota University Systems’ technology team Core Technology Services (CTS) are partnering to ensure heightened cybersecurity as universities adapt to changing technology needs and increased virtual learning needs.

(U) Schell Selected for Leadership Position in National Tech Professionals Association
(U) North Dakota Information Technology’s Chief Technology Officer Duane Schell has been selected as the Vice President on the 2021 Executive Board of the National Association of State Technology Directors. This follows Schell’s prior year as Secretary/Treasurer of the organization, which represents information technology professionals from all 50 states.
Source: (U) https://www.nd.gov/itd/news/schell-selected-leadership-position

(U) CIO, CISO to Participate in Third Annual CyberCon
(U) North Dakota Chief Information Officer Shawn Riley and Chief Information Security Officer Kevin Ford will participate in the third annual critical infrastructure and cybersecurity conference scheduled for Oct. 6 – 7, 2020. Hosted by Bismarck State College, this year’s event will be held virtually and features experts including NFL Senior Vice President of Security Cathy Lanier and owner of Black Hills Information Security John Strand. North Dakota CIO Shawn Riley will give opening remarks on day two of the conference followed by a keynote by Ford.
NATIONAL

(U) U.S. Treasury Sanctions Hacking Group Backed by Iranian Intelligence
(U) The U.S. government on September 17th, 2020 imposed sweeping sanctions against an Iranian threat actor backed by the country's Ministry of Intelligence and Security (MOIS) for carrying out malware campaigns targeting Iranian dissidents, journalists, and international companies in the telecom and travel sectors. According to the U.S. Treasury and the Federal Bureau of Investigation (FBI), the sanctions target Rana Intelligence Computing Company (or Rana), which the agencies said operated as a front for the threat group APT39 (aka Chafer or Remix Kitten), Iranian cyber espionage hacking collective active since 2014 known for its attacks on companies in the U.S. and the Middle East with an aim to pilfer personal information and advance Iran's national security objectives. Source: (U) https://thehackernews.com/2020/09/iranian-hackers-sanctioned.html

(U) U.S. Announces Charges Against 2 Russian and 2 Iranian Hackers
(U) Immediately after revealing criminal charges against 5 Chinese and 2 Malaysian hackers, the United States government on September 16th also made two separate announcements charging two Iranian and two Russian hackers and added them to the FBI's most-wanted list. The two Russian nationals—Danil Potekhin and Dmitrii Karasavidi—are accused of stealing $16.8 million worth of cryptocurrencies in a series of phishing attacks throughout 2017 and 2018. Whereas, both two Iranian nationals—Mehdi Farhadi and Hooman Heidarian—are allegedly involved in government-linked hacking operations and have stolen hundreds of terabytes of sensitive data from several targeted organizations. Source: (U) https://thehackernews.com/2020/09/us-announces-charges-against-2-russian.html

(U) Cryptocurrency Tracer Could Give Cops an Edge on Cybercrime
(U) Digital intelligence vendor Cellebrite recently launched its new crypto tracer solution, a tool to help state and local police more effectively investigate cybercrime. The company says its product will give law enforcement agencies the ability to better track illicit cryptocurrency transactions, the kind that are ubiquitous amongst ransomware hackers and other cybercriminals. "The solution empowers teams to lawfully obtain evidence and trace criminals who use bitcoin and other cryptocurrencies for illicit activities, including money laundering, terrorism, drug and human trafficking, weapon sales and ransomware schemes," the company explained in a statement. Source: (U) https://www.govtech.com/security/Cryptocurrency-Tracer-Give-Cops-Edge-on-Cybercrime.html

(U) Massachusetts City Dodges Eastern European Hack Attempt
(U) An attempt over the summer by Eastern European hackers to gain entry into the Methuen's computer system — with its information about taxpayers, employees and much more — was nearly successful, according to city officials, but quick action helped keep the information secure. Mayor Neil Perry said on September 22nd the hacking attempt was one of the reasons city councilors held an executive session July 13, during which they voted to spend $272,000 in emergency funds to buy hardware and software to combat the threat. The funding was also used for a forensic audit of the entire IT system to determine if there were other hidden threats. Source: (U) https://www.govtech.com/security/Massachusetts-City-Dodges-Eastern-European-Hack-Attempt.html

(U) US Bans WeChat, TikTok from App Stores, Threatens Shutdowns
(U) The U.S. Commerce Department recently stated it will ban Chinese-owned TikTok and WeChat from U.S. app stores on Sunday and will bar the apps from accessing essential internet services in the U.S. — a move that could effectively wreck the operation of both Chinese services for U.S. users. The order, which cited national security and data privacy concerns, followed weeks of deal making over the video-sharing service TikTok. Source: (U) https://www.twincities.com/2020/09/18/us-bans-wechat-tiktok-from-app-stores-threatens-shutdowns/
INTERNATIONAL

(U) Ransomware Attack on Hospital in Dusseldorf Leads to Unexpected Death
(U) On Thursday, September 17th, at the Dusseldorf hospital - which is affiliated with the Heinrich Heine University - 30 servers were encrypted. However, the perpetrators wanted to target the university, not the hospital. When authorities communicated to the hackers that lives were in danger, the attackers withdrew their extortion demands and provided a digital ransomware decryption key. In the interim, on account of the cyber disruptions, an ambulance carrying a person in need of emergency services was re-routed to a hospital 20-miles away. This led to a significant delay in treatment, and the individual did not survive.


(U) Major Instagram App Bug Could've Given Hackers Remote Access to Your Phone
(U) Check Point researchers disclosed details about a critical vulnerability in Instagram’s Android app that could have allowed remote attackers to take control over a targeted device just by sending victims a specially crafted image. According to an advisory published by Facebook, the heap overflow security issue (tracked as CVE-2020-1895, CVSS score: 7.8) impacts all versions of the Instagram app prior to 128.0.0.26.128, which was released on February 10 earlier this year.


(U) A New Hacking Group Hitting Russian Companies with Ransomware
(U) The ransomware gang, codenamed "OldGremlin" and believed to be a Russian-speaking threat actor, has been linked to a series of campaigns at least since March, including a successful attack against a clinical diagnostics laboratory that occurred last month on August 11. The group has targeted only Russian companies so far, which was typical for many Russian-speaking adversaries, such as Silence and Cobalt, at the beginning of their criminal path," Singaporean cybersecurity firm Group-IB said in a report.


(U) British Hacker Sentenced to 5 Years for Blackmailing U.S. Companies
(U) A UK man who threatened to publicly release stolen confidential information unless the victims agreed to fulfill his digital extortion demands has finally pleaded guilty on Monday at U.S. federal district court in St. Louis, Missouri. Nathan Francis Wyatt, 39, who is a key member of the infamous international hacking group 'The Dark Overlord,' has been sentenced to five years in prison and ordered to pay $1,467,048 in restitution to his victims.


(U) Unsecured Microsoft Bing Server Exposed Users' Search Queries and Location
(U) A back-end server associated with Microsoft Bing exposed sensitive data of the search engine's mobile application users, including search queries, device details, and GPS coordinates, among others. The logging database, however, doesn't include any personal details such as names or addresses. The data leak, discovered by Ata Hakcil of WizCase on September 12, is a massive 6.5TB cache of log files that was left for anyone to access without any password, potentially allowing cybercriminals to leverage the information for carrying out extortion and phishing scams.

(U) A Bug Could Let Attackers Hijack Firefox for Android via Wi-Fi Network

(U) ESET security researcher Lukas Stefanko on September 18th tweeted an alert demonstrating the exploitation of a recently disclosed high-risk remote command execution vulnerability affecting the Firefox app for Android. Discovered originally by Australian security researcher Chris Moberly, the vulnerability resides in the SSDP engine of the browser that can be exploited by an attacker to target Android smartphones connected to the same Wi-Fi network as the attacker, with Firefox app installed.