COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 22, Number 6. June 09, 2022 Privacy Briefs: June 2022

By Jane Anderson

◆ **A report from the HHS Health Sector Cybersecurity Coordination Center (HC3) found that in early 2022, ransomware groups increasingly turned to legitimate software during intrusions.**[1] Software used included remote access, encryption, file transfer and open-source tools, as well as internal Microsoft utilities. In this approach, threat actors leverage what is already available in the target environment instead of deploying custom tools and malware, HC3 said. Attackers that use legitimate software for malicious actions are less likely to see their activity flagged by antivirus or endpoint detection tools, because malicious actions are more likely to blend in with normal administrative tasks, HC3 said. The agency recommended several mitigation strategies, including using the host firewall to restrict file-sharing communications, deploying network intrusion detection and prevention systems that use network signatures, using multifactor authentication for user and privileged accounts, and configuring access controls and firewalls to limit access to domain controllers and systems used to create and manage accounts.

◆ **An information technology specialist has been indicted on a federal criminal charge for allegedly hacking into the server of an Oak Lawn, Illinois, health care company where he formerly worked as a contractor.**[2] Aaron Lockner of Downers Grove allegedly illegally accessed the server on April 16, 2018, according to an indictment returned May 24 by a U.S. district court in Chicago. This intrusion impaired medical examinations, treatment and care of multiple individuals, the indictment stated. Lockner had previously performed information security and technology work for the health care company and had access to its computer network, the indictment alleged. Two months before the cyberattack, Lockner had sought and was denied an employment position with the health care company. If convicted, Lockner faces up to 10 years in federal prison.

◆ **The HHS Office for Civil Rights (OCR) has opened a probe into the Rhode Island Public Transit Authority (RIPTA) data breach from last August, a RIPTA spokesperson confirmed.**[3] Cristy Raposo Perry told WPRI that OCR was investigating but said it's unclear what information RIPTA has been asked to provide or how long the review would take. OCR does not comment on or confirm investigations. Rhode Island Sen. Lou DiPalma said, "United Healthcare provided to RIPTA access to personal information—potentially health information as well—that was unauthorized for 22,000 people." Conti, a ransomware hacker group with Russian ties, attacked the transit authority in August. RIPTA hired Coveware Inc., "a firm that helps entities recover hacked data, and ended up paying $170,000 to recover its stolen data on Aug. 12," WPRI reported.

◆ **The FBI's Cyber Division has warned that BlackCat/ALPHV ransomware as a service (RaaS) has compromised "at least 60 entities worldwide and is the first ransomware group to do so successfully using RUST**, considered to be a more secure programming language that offers improved performance and reliable concurrent processing. BlackCat-affiliated threat actors typically request ransom payments of several million dollars in Bitcoin and Monero but have accepted ransom payments below the initial ransom demand amount," the FBI said.[4] "Many of the developers and money launderers for BlackCat/ALPHV are linked to Darkside/Blackmatter, indicating they have extensive networks and experience with ransomware operations." The group steals data before the execution of the ransomware, including from cloud storage, and leverages Windows scripting to deploy ransomware and compromise additional hosts, the FBI said, and asked for "any information that can be shared, to include IP logs showing callbacks from foreign IP addresses, Bitcoin or Monero addresses and transaction IDs, communications with the threat actors, the decryptor file, and/or a benign sample of an encrypted file."

◆ **myNurse, a health care startup providing chronic care management and remote patient monitoring services, said it would shut down after reporting a data breach that exposed personal information of its users**, *TechCrunch* reported.[5] According to the report, myNurse filed a notice "with the California attorney general's office that it discovered a breach on March 7 during which an unauthorized individual accessed the company's protected health data. The data breach notice warned that patients' demographic, health and financial information was accessed, including names, phone numbers, dates of birth, but also medical histories, diagnoses, treatments, lab test results, prescriptions, and health insurance information." The notice said that the decision to shutter the business "is unrelated to the data security incident," but the company did not provide a reason for the unexpected shutdown. According to *TechCrunch*, "the company said it began notifying affected patients on April 29, the same day as its breach notification, more than seven weeks after the breach was discovered. myNurse co-founder and chief executive Waleed Mohsen provided *TechCrunch* with a short statement saying the company was considering 'how best to adjust our business model amid a changing healthcare landscape,'" but declined to answer questions about the breach. The company did not say how many patients were affected. California law requires notification if more than 500 people are affected.

◆ **A ransomware attack at the Oklahoma City Indian Clinic in early March has disrupted clinic operations for two months so far**, the clinic confirmed in a notice of data incident.[6] The attack, which occurred on March 10, caused technical issues that left the care team without access to certain computer systems, the clinic said. Due to the attack, the clinic shut down its automated prescription refill line, which required patients to place phone calls to refill their prescriptions. The attack also shuttered mail order prescriptions, the clinic said. Staff members have been re-entering prescription information into clinic systems manually, the clinic said on social media. In late March, a ransomware group called Suncrypt claimed responsibility for the attack.[7]

◆ **Personal information of nearly 2 million Texans was exposed and publicly available for nearly three years, according to a state audit.** According to *The Texas Tribune*, the Texas Department of Insurance (TDI) said "the personal information of 1.8 million workers who have filed compensation claims—including Social Security numbers, addresses, dates of birth, phone numbers and information about workers' injuries—was accessible online to members of the public from March 2019 to January 2022."[8] Department officials said the unauthorized disclosure was discovered during a data management audit and reported. "On March 24, after the state's audit was completed, TDI posted a public notice acknowledging it became aware of the issue in January," the auditor's office said. "The incident occurred because of an issue in the programming code in the department's web application that manages workers' compensation data. The issue in the code allowed members of the public to access a protected part of that online application," the department said. "Texas Department of Insurance spokesperson Ben Gonzalez said the department temporarily disconnected the web application from the internet after identifying the unauthorized disclosure." A forensic investigation did not turn up any evidence of misuse, the spokesperson said.

[1] HHS Health Sector Cybersecurity Coordination Center, "Ransomware Trends in the HPH Sector (Q1 2022)," May 5, 2022, https://bit.ly/3m4aKOn.

[2] Department of Justice, United States Attorney's Office for the Northern District of Illinois, "I.T. Specialist Charged in Cyber Intrusion of Suburban Chicago Health Care Company," news release, May 25, 2022, https://bit.ly/3M80EGE.

[3] Tolly Taylor, "Target 12: Feds open probe into RIPTA data breach," WPRI, May 20, 2022, https://bit.ly/3m2kgBo.

[4] FBI, “BlackCat/ALPHV Ransomware Indicators of Compromise,” FBI Flash, CU-000167-MW, April 19, 2022, https://bit.ly/3x97A2i.

[5] Zack Whittaker, “Health startup myNurse to shut down after data breach exposed health records,” *TechCrunch*, May 2, 2022, https://tcrn.ch/3GTR6hP.

[6] Oklahoma City Indian Clinic, “Notice of Data Incident,” May 9, 2022, https://bit.ly/3PNSIxo.

[7] Austin Breasette, “Ransomware group claims responsibility for cyber-attack on metro healthcare organization,” KFOR, March 28, 2022, https://bit.ly/3anHWh5.

[8] Jason Beeferman, “Personal Information of 1.8 Million Texans with Department of Insurance Claims Was Exposed for Years, Audit Says,” *The Texas Tribune*, May 16, 2022, https://bit.ly/3x7pORx.