HC3: Healthcare Cybersecurity Bulletin

Q3 2021 TLP: White Report: 202110261600

Executive Summary

In the third quarter of 2021, HC3 observed a continuation of ongoing trends with regards to cyber threats to the healthcare and public health community. Ransomware attacks were as prevalent as ever and ransomware operators continued to evolve their techniques for increasing extortion pressure and maximizing their payday. This was reflected in a number of industry reports included in this bulletin, as well as in internal HC3 data. Data breaches continued to plague healthcare, often combined with ransomware attacks. Vulnerabilities in software and hardware platforms, some ubiquitous and some specific to healthcare, continued to keep the attack surface of healthcare organizations wide open.

News and Industry Reports of Interest to the Health Sector for Quarter 3

- The Kaseya cyberattack was one of the biggest managed service provider (MSP) cyberattacks in history. On Friday, July 2, the software company Kaseya became aware of a compromise of their Virtual System Administrator (VSA) platform, which is remote monitoring and endpoint management software they sell to their customer base of managed service providers. Immediately after the attack, they shut down VSA. They estimated that between 50 and 60 of their customers were impacted and those impacted customers – managed service providers – are believed to manage IT services for about 1,500 companies and organizations. The ransomware operators, REvil (AKA Sodinokibi) claimed responsibility. Initially, REvil offered a universal decryptor for $70 million in Bitcoin and reports noted that the demand dropped to $50 million shortly thereafter. CISA and FBI jointly released guidance and a free Kaseya VSA compromise detection tool which looks for indicators of compromise. The White house stated that they did not believe the Russian government was the source of these attacks but instead criminal groups physically located in Russia. Kaseya announced that they obtained a decryptor key (no further details). It is not known if (or how many) healthcare or public health (HPH) organizations were impacted by the Kaseya cyberattack, however HPH is often targeted via MSP compromise and REvil/Sodinokibi is a prolific threat to HPH as well.
- In late July, IBM released their annual Cost of a Data Breach report. In it, they assessed data breaches in 2021 cost a company $4.24 million on average per incident, which is the highest figure in the 17-year history of the report. In the United States, a data breach cost about $9 million on average per incident. The cost of breaches increased about 10% in a year, and IBM largely attributes some of that to the remote workforce which has increasingly been in place since the beginning of the pandemic. IBM also found that the average cost of a breach increased about $1 million when remote work was a factor in the breach. It's worth noting that breaches in the healthcare industry were more expensive than any other industry, and that was the 11th year in a row that that was the case. The average healthcare breach was $9.23 million, which was a dramatic increase, about 30%, from the $7.13 million it was in 2019.
- The company Critical Insight released their Healthcare Breach report for the first half of 2021 in August. The number of breaches in the first half of 2021 are as high as they have been for any six-month period since 2018, excluding the second half of last year, which has a spike due to a single, large breach. According to their report, breaches have been steadily increasing over time and have almost doubled – increased 77% - in the last three years. Critical Insight also found outpatient facilities, especially family medicine and specialty clinics, to be heavily targeted. Outpatient facilities were breached almost as much as hospitals. Finally, they noted that business associates were the cause of 43% of all healthcare breaches, which continues a 3-year increasing trend.
- RiskBased Security released their 2021 Mid-Year Data Breach Report in August. In that research, they identified 1,767 publicly reported breaches in the first six months of 2021. They found that 18.8 billion records were exposed year to date, and of those, the majority – 1201 – were caused by a cyberattack. The healthcare sector remained the most targeted and breached industry accounting for 238 of breaches as of the date of the report.
- In September, the US Treasury Department announced sanctions on ransomware operators and specifically on the ransom payments they receive. Those sanctions will focus on specific targets and not an entire

cryptocurrency infrastructure. This also included the first ever designation of a virtual currency exchange, SEUX OTC, a Russian owned cryptocurrency exchange alleged to have conducted laundering activities associated with ransomware operators.

HC3 Products

In the third quarter of 2021, HC3 released alerts, briefs and other guidance on vulnerabilities, threat groups and technical data of interest to the health sector and public health community. Our products can be found at this link: https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html. The below table highlights those products.

RELEASE DATE	TITLE	SUMMARY
9/30	Conti Ransomware Amplify Alert	Conti is a ransomware group that has aggressively targeted healthcare organizations since it was first observed in 2019. Conti ransomware attacks have targeted healthcare industry, major corporations and government agencies, particularly those in North America. During this type of cyber-attack, the threat actor steals sensitive data from compromised networks, encrypts the targeted organizations' servers and workstations, and threatens to publish the stolen data unless the target pays a ransom.
9/28	Alert: No Fix for Azure Active Directory Password Brute-Forcing Flaw	A newly discovered bug in Microsoft Azure's Active Directory implementation enables a single-factor brute-forcing of an Active Directory instance without authentication. Currently there is no available patch for this vulnerability.
9/23	Analyst Note: BrakTooth Vulnerabilities	The BrakTooth vulnerabilities came on the radar in August 31, 2021, after being discovered by the ASSET (Automated Systems Security) Research Group at the Singapore University of Technology and Design (SUTD). It is described as a new family of security vulnerabilities found in commercial Bluetooth Classic stacks for various System-on-Chips (SoC). BrakTooth uses the Bluetooth Classic (BR/EDR) protocol and affects millions of Bluetooth-enabled devices that are manufactured by Intel, Qualcomm, Texas Instruments, Infineon (Cypress), Zhuhai Jieli Technology, and Silicon Labs.
9/22	Sector Alert: VMware Vulnerabilities	On September 21, 2021, VMware disclosed numerous vulnerabilities affecting their vCenter Server and Cloud Foundation products, some of which could be exploited for the deployment of ransomware or other malicious activity. VMware recommends that customers install available updates, patches, or workarounds immediately to mitigate these vulnerabilities in affected VMware products.
8/27	Sector Alert: Pulse Secure Vulnerabilities	Since April 2021, there have been several vulnerabilities in Pulse Secure VPN technology. These allow for a variety of malicious activity, including authentication bypass, multi-factor authentication bypass, password logging, and persistence through patching, all of which can facilitate further attacks on an information infrastructure. The Department of Homeland Security has observed threat actors creating scheduled tasks and remote access trojans to establish persistence, exfiltrate files, and execute ransomware on the victim's network environment including healthcare organizations.

HC3: Healthcare Cybersecurity Bulletin

Q3 2021 TLP: White Report: 202110261600

8/26	Alert: Indicators of Compromise Associated with Hive Ransomware	The FBI shared indicators of compromise (IOCs) associated with the Hive ransomware, which they believe "likely operates as an affiliate-based ransomware." While Hive uses multiple methods to comprise victims' networks, the FBI highlighted "phishing emails with malicious attachments." Once a victim's network is compromised Hive provides "two to six days" for payment of the ransom by the victim. If the ransom is not paid, Hive leaks their victim's data to their Tor website, HiveLeaks. Because Hive uses legitimate applications to further their compromise of a victim's network, "the FBI recommends removing any application not deemed necessary for day-to-day operations."
8/24	Alert: Indicators of Compromise Associated with OnePercent Group Ransomware	The FBI shared indicators of compromise (IOCs) associated with the ransomware threat actors the OnePercent Group. The OnePercent Group uses IceID-infected phishing email attachments to install ColbaltStrike and other malware on their victims' computers. Because the OnePercent Group uses the rclone program, the FBI recommends "organizations be aware" of the hashes associated with rclone that are included in their alert. "Rclone is a command line program to manage files on cloud storage."
8/19	Sector Alert: FortiWeb Zero-Day Vulnerability.	A zero-day command injection vulnerability has been identified in Fortinet's FortiWeb web application firewall (WAF) and effects versions 6.3.11 and earlier. This OS Command injection vulnerability allows remote, authenticated attackers to execute arbitrary commands on the system through the SAML server configuration page allowing for full compromise of the system and the potential for further compromise of the enterprise network. Fortinet will be releasing a patch that is intended to fix this vulnerability.
8/18	Alert: BadAlloc Vulnerability Affecting BlackBerry QNX RTOS.	BlackBerry identified the following products are affected by an integer overflow vulnerability (CVE-2021-22156) with CVSS Score 9.0: BlackBerry QNX Software Development Platform (SDP) version 6.5.0SP1 and earlier, QNX OS for Medical 1.1 and earlier, and QNX OS for Safety 1.0.1. BlackBerry states there "are no known workarounds for this vulnerability."
8/3	Sector Alert: PwnedPiper Impact on Healthcare	Nine vulnerabilities (dubbed PwnedPiper) were recently discovered in a brand (Swisslog) of pneumatic tubes – the tube systems within many hospitals and other healthcare organizations which transports small items such as lab samples, blood, tissue or medication from one part of the medical facility to another – which can allow a cyberattacker to compromise and/or disrupt the operations of the system. These vulnerabilities are believed to impact over 3,000 hospitals worldwide, including 80% of all hospitals in North America. All healthcare organizations are urged to review this document and apply the appropriate steps outlined in the mitigation section as needed.
7/29	Alert: Top Routinely Exploited Vulnerabilities of 2020 and 2021.	The recently released Joint Cybersecurity Advisory coauthored by CISA, the FBI, the UK National Cyber Security Centre, and the Australian Cyber Security Centre contains information on the top 30 vulnerabilities malicious cyber actors have most often exploited since the beginning of 2020 to July 2021. The advisory contains vulnerability descriptions, IOCs, detection methods, patch availability, mitigation recommendations, and vulnerable technologies and versions.

HC3: Healthcare Cybersecurity Bulletin

Q3 2021 TLP: White Report: 202110261600

7/22	Alert: Exploitation of Pulse Connect Secure Vulnerabilities	Since June 2020, unidentified threat actors have targeted vulnerabilities in certain Ivanti Pulse Connect Secure products. Threat actors gained initial access through the targeting of the following vulnerabilities: CVE-2019-11510, CVE-2020-8260, CVE-2020-8243, and CVE-2021-22893. Upon exploitation, the threat actors "place webshells on the Pulse Connect Secure appliance for further access and persistence." The threat actors' access can allow them to perform: authentication bypass, multi-factor authentication bypass, password logging, and persistence through patching.
7/15	Alert: PrintNightmare, Windows Print Spooler Service Vulnerability (Update 1)	PrintNightmare is the name given to a critical remote code execution vulnerability in the Windows Print spooler service. Attackers can take advantage of this vulnerability to gain control of affected systems. Cybersecurity and Infrastructure Security Agency (CISA) advises all organizations follow Microsoft's guidance for CVE-2021-34527 and also implement Microsoft's best practice from January 11, 2021.
7/9	Sector Alert: Phillips Vue PACS Vulnerabilities. You may distribute through your appropriate channels for the level of information as marked	The Philips Vue PACS (Picture Archiving and Communication System) is an image-management software platform that enables hospitals to archive, distribute, display and retrieve images and data from all hospital modalities and information systems. Vulnerabilities have been identified in Philips Vue PACS products, which include 5 classified as critical that allow for a number of negative impacts including disruption, data theft and total device compromise.
7/8	Analyst Note: Overview of Phobos Ransomware	Phobos ransomware first surfaced in late 2017 with many researchers quickly discovering links between Phobos and the Dharma and CrySiS ransomware variants. The Phobos ransomware operators are known to primarily target small- to medium-sized businesses (including healthcare entities such as hospitals) and typically demand lower ransom amounts compared to other ransomware families. The capabilities of Phobos ransomware continue to evolve, with new variants making the ransomware more difficult to detect, identified as recently as April 2021.
7/6	Vulnerability Bulletin: PrintNightmare, Windows Print Spooler Remote Code Execution Vulnerability	PrintNightmare is the name given to a critical remote code execution vulnerability in the Windows Print spooler service. Attackers can take advantage of this vulnerability to gain control of affected systems. The Cybersecurity and Infrastructure Security Agency (CISA) advises all organizations to follow Microsoft's guidance for CVE-2021-34527 and implementing Microsoft's best practice from January 11, 2021. Additional background information can be found in the document published by the CERT Coordination Center.

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback