Rhysida Ransomware Attack
HHS 405(d)Program SBAR Brief
August 16, 2023

The 405(d) **S**ituation, **B**ackground, **A**ssessment, **R**ecommendation (SBAR) is an HPH focused review of active cyber intelligence and alerts from across federal agencies. Mandated by the Cybersecurity Act of 2015 with the goal of aligning health care industry security approaches, the 405(d) **SBARs**, backed with the knowledge and expertise of HHS and the 405(d) Task Group, provide the HPH sector with a clear HPH focused understanding, assessment, and recommended mitigations that HPH organizations can apply against these active cyber incidents.

A concise statement of the problem

SITUATION: A ransomware-as-a-service group called Rhysida attacked a health care system which operates 16 hospitals and more than 165 clinics and outpatient centers in four states, on Thursday, August 3rd, 2023. According to news reports, the attack resulted in "emergency departments to close, ambulances to be diverted, and other medical services to cease operations" in what appeared to be a ransomware attack. The attack required the hospitals to take their systems offline to protect their patient data and to revert to using paper records. In some states, the health system's blood draw stations and medical imaging locations were also impacted. Areas saw emergency departments, as well as some primary and specialty locations closed until further notice. As a result, impacted entities were contacting patients individually due to the various effects to patient care.

Pertinent and brief information related to the situation

BACKGROUND: As documented by Health Sector Cybersecurity Coordination Center (HC3) Sector Alert, released on Friday, August 4th, 2023, Rhysida was first observed on May 17th, 2023, following the emergence of their victim support chat portal, hosted via TOR (.onion). Rhysida deceitfully describes itself as a "cybersecurity team" that aims to help victims highlight potential security issues and secure their networks. While not much is known about the group's origins or country affiliations, Rhysida ransomware is deployed in multiple ways.

Primary methods include breaching a target's network via social engineering attacks, more specifically phishing. Once an attack is successful, they can penetrate the network and encrypt your data by utilizing a sophisticated encryption protocol known as 4096-bit RSA key with the ChaCha20 Algorithm, which locks your data and denies your ability to access your systems. After encryption details are established, Rhysida then one-by-one locks files and folders by calling PowerShell to delete the binary after encryption is completed, making your files, systems, or connected medical devices no longer available to you.

The encryption phase orchestrated by the Rhysida group leaves a ransomware note in a PDF form with detailed instructions on how to potentially pay to retrieve your stolen data. The threat actors gain initial access to victims' networks in several ways, including targeting public-facing applications with targeted phishing campaigns and then utilize a penetrating testing tool that has been reconfigured to exploit its post-exploitation capabilities.

These types of breaches not only put patient privacy at risk but can also threaten lives when operations are disrupted. For more details regarding the Rhysida cyber group, please review HC3's Sector Alert: Rhysida Alert.

Analysis and considerations of options—what we found and think

ASSESSMENT: Rhysida is an emerging threat group, targeting many critical infrastructure sectors including the Healthcare and Public Health (HPH) sector. Our assessment of this threat causes us to believe that organizations need to act now to mitigate any potential future impacts. The group has already been successful in orchestrating ransomware attacks, resulting in the temporary closure of major hospitals and urgent care facilities. The Rhysida ransomware group is a significant threat to the HPH sector due to their ability to enter your network, lock your files and cause your systems to go offline, potentially impacting patient care and halting business functions, with the threat of public distribution of collected sensitive data.

Recommended/ requested action—what we want you to do

RECOMMENDATION: The Rhysida threat actors target public facing applications that are usually connected to the internet. This is a serious risk for healthcare organizations due to the amount of patient data that is shared over the connected network daily. Recognizing our reliance on the internet and the sensitive nature of healthcare data, it is suggested that you ensure that every level of your organization is cyber aware and knows their role. This should include all staff, c-suite, medical and nursing leadership. It is also recommended that your IT department implement the following best practices found in The Health Industry Cybersecurity Practices Technical Volumes 1&2 and Knowledge on Demand to protect your valuable health information from such threats.

A sample of recommendations from HICP include:

- **Enable multi-factor authentication (MFA) —** Deploy multi-factor authentication (MFA) before enabling access to your email system. MFA can prevent hackers who have obtained a legitimate user's credentials from accessing your system. Make sure that MFA is in place for web access and your local client access. It's popular to want to use IMAP or POP3 protocols, but these might not support MFA and can leave a back door open to your email mailboxes. (1.S.A)
- **Phishing awareness training —** Train your employees how to report suspicious messages. These should be reported to the person responsible for maintaining your IT system. That individual or service provider can then advise the employee regarding disposition of the suspicious message (1.S.A, 1.S.B) For additional practices check out our "How To" covering cyber workforce training.
- **Secure your email system —** Configure your email system to tag messages that are sent from outside of your organization as "EXTERNAL". Consider implementing a tag that advises the user to be cautious when opening such emails, for example, "Stop. Read. Think. This is an External Email." (1.S.A)
- **User management —** It is recommended to have a robust Identity and access management (IAM) program that encompasses the processes, people, technologies, and practices relating to granting, revoking, and managing user access. Given the complexities associated with healthcare environments, IAM models are critical for limiting the security vulnerabilities that can expose organizations. A common phrase used to describe these programs is "enabling the right individuals to access the right resources at the right time." (3.M.A)
- **Ensure your endpoints are patched —** Patching (i.e., regularly updating) systems removes vulnerabilities that can be exploited by attackers. Each patch modifies a software application, mitigating a vulnerability that has been exposed. Configure endpoints to patch automatically and ensure third-party applications are patched as soon as possible. Automatically update and distribute patches to third- party applications that are known to be vulnerable, such as internet browsers (e.g., Adobe Flash, Acrobat Reader, Java). (7.S.A)(2.M.A) For additional practices check out our "How To" on patching for Small & Medium organizations.
- **Restrict inbound Internet access —** Limit the amount of connectivity to only those services needed to be exposed to the Internet, and ensure all remote access systems have MFA enabled such as VPNs, VDI and so forth. Organizations should deploy firewall capabilities in the following areas: on wide area network (WAN) pipes to the internet and perimeter, across data centers, in building distribution switches, in front of partner WAN/VPN connections, and over wireless networks (6.M.A).
- **Establish data back-up —** It is equally important to have a backup strategy in the event of cybersecurity incidents. There will be events that cause an asset, or multiple assets, to be thoroughly compromised. During these events, routine backups can be the only way to ensure proper execution of the recovery phase of your IR process. Fully decommissioning affected assets and restoring them to a time before the compromise occurred is the best method to neutralize the compromise. (4.M.D)
- **Establish an incident response process —** Create a large-scale cybersecurity incident response plan in coordination with your emergency management and business continuity teams. This large-scale response is designed to allow for the continuity of operations of the business during a cyber-attack. (8.M.B)

Legend:

Key: 1-10 = HICP Cybersecurity Practice | S = Small (Tech Vol 1) | M = Medium (Tech Vol 2) | L = Large (Tech Vol 2) | A-Z= Respective Sub-Practice

Example: "1.S.B Education": "1" refers to the cybersecurity Practice "Email Protection System" | "S" refers to Small size organization | "B" refers to the sub practice for small size organization within the Email Protection System – Cybersecurity Practice, which in this case is "Education"

Additional Resources/Reference:

HC3- https://www.hhs.gov/sites/default/files/rhysida-ransomware-sector-alert-tlpclear.pdf
H-ISAC- https://h-isac.org/ransomware-actors-target-healthcare/
CISA: Stop Ransomware Guide: https://www.cisa.gov/stopransomware
NIST National Vulnerability Database: fake URL in address bar via phishing URL link: https://nvd.nist.gov/vuln
Beckers Hospital Review https://www.beckershospitalreview.com/cybersecurity/after-prospect-medical-cyberattack-ransomware-remains-a-big-problem-for-big-health-systems.html