American Hospital Association™
Advancing Health in America

Cybersecurity Advisory

November 15, 2023

New Ransomware Threat: Rhysida Group Targets Hospitals, Puts Patient Safety at Risk

Hospitals among group's "targets of opportunity" for high-impact ransomware attacks, resulting in significant disruption and delay to health care delivery

The FBI, Cybersecurity and Infrastructure Security Agency (CISA), and Multi-State Information Sharing and Analysis Center (MS-ISAC) today issued a warning about Rhysida, a ransomware-as-a-service group that since May has predominantly deployed its ransomware variant against the health care, education, manufacturing, information technology and government sectors. The group targets victims around the world and publishes stolen files online.

Hospitals and health systems are urged to lower their risk by prioritizing remediation of known vulnerabilities, segment their networks and enable multifactor authentication.

"When hospitals are attacked, lives are threatened," said John Riggi, AHA's national advisor for cybersecurity and risk. "Let's be clear: Ransomware attacks against hospitals are not financial crimes; they are acts of cyber terrorism and threat-to-life crimes. We encourage the U.S. government and our allies to continue to use their combined capabilities to respond as such, with offensive cyber operations against these cyber terrorists. We in health care need to do our part to defend against these attacks by following the recommended mitigation strategies and enhancing our resiliency against these attacks. Preparing clinical downtime procedures to sustain a loss of technology and communications for up to 30 days will assist in mitigating the impacts to patient care and safety."

MITIGATION STRATEGIES

Rhysida actors have been observed leveraging external-facing remote services to initially access and persist within a network.

The FBI, CISA and MS-ISAC are providing tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Mitigation steps for hardening defenses against Rhysida ransomware include:

- **Require** phishing-resistant multifactor authentication for all services to the extent possible, particularly for webmail, VPN, and accounts that access critical systems.
- **Disable** command-line and scripting activities and permissions.

- **Implement** verbose and enhanced logging within processes, such as command-line auditing and process tracking.
- **Restrict** the use of PowerShell using Group Policy and only grant access to specific users on a case-by-case basis.
- **Update** Windows PowerShell or PowerShell Core to the latest version; uninstall all earlier PowerShell versions; and enable enhanced PowerShell logging.
- **Restrict** the use of RDP and other remote desktop services to known user accounts and groups.
- **Secure** remote access tools by:
    - Implementing application controls to manage and control execution of software, including allowlisting remote access programs.
    - Apply the recommendations in CISA's Joint Guide to Securing Remote Access Software.

Additional details on mitigation strategy can be found on CISA's #StopRansomware page.

FURTHER QUESTIONS

If you have further questions, please contact John Riggi, AHA's national advisor for cybersecurity and risk, at jriggi@aha.org. For the latest cyber threat intelligence and resources, visit www.aha.org/cybersecurity.