Threat Advisory: Ransomware Targeting the Healthcare Sector

Overview

On October 28, the FBI, DHS, and CISA released a joint alert on ransomware activity targeting hospitals and other healthcare providers. The security advisory highlights information on TrickBot, BazarLoader (aka BazarBackdoor), Ryuk, and Conti, including indicators of compromise (IOCs) and YARA rules for detection.

The targeted threat is multi-stage:

- Cybercriminals disseminate TrickBot and/or BazarLoader via phishing campaigns that trick users to either click links to malicious websites that host the malware or download attachments containing the malware.
- TrickBot uses legitimate applications to evade detection, leveraging the anchor_dns module to hide communication to command and control (C2) servers to prevent being blocked by traditional firewalls and web protection.
- BazarLoader is used to infect victim networks and deploy ransomware, most commonly Ryuk, to execute on target systems.
- Ryuk ransomware often utilizes off-the-shelf tools such as Cobalt Strike or PowerShell Empire to steal credentials, quickly enumerate the network, and ultimately encrypt files.

What We're Hunting For

- Huntress has built-in detections for TrickBot malware, specifically hunting for nefarious services and scheduled tasks. To date, Huntress has discovered and remediated over 8,000 TrickBot infections.
- Huntress detects filenames with the naming conventions used by TrickBot and monitors the targeted directories to find persistent footholds or odd behavior. Our ThreatOps team offers human analysis to have a firm understanding of what context code is running in.
- Huntress automatically gathers a list of scheduled tasks to look for callbacks and persistence mechanisms. The random naming convention validates the detection of TrickBot malware, and upon discovery, Huntress can remediate and remove the malicious service.
- Ryuk ransomware encrypts files and often leaves behind a specific Ryuk ransom note. The change in the file contents will trigger Huntress' Ransomware Canaries, which will then be confirmed by our ThreatOps teams, so you are rapidly notified if a ransomware attack occurs.

For a full analysis and additional mitigation steps, view the joint cybersecurity advisory here.

Mitigation Best Practices

- Establish and maintain patching plans, security policies, user agreements, business continuity plans, and incident response plans.
- Enable anti-spam and anti-phishing protections, and double check that web protection is preventing access to known malicious websites and filtering questionable content.
- Regularly change passwords to network systems and accounts and use multi-factor authentication where possible.
- Disable unused remote access /RDP ports and monitor remote access/RDP logs.
- Maintain off-site or cloud-based copies of backups to assist with recovery after a ransomware attack.