Ransomware: Where We Are

Ransomware isn't going anywhere. The healthcare sector continues to fight the COVID-19 pandemic that has fueled numerous incidents of malicious cyber activity. Ransomware attacks were up over 400% in 2020 and smaller healthcare organizations have become a primary target.

Ransomware adversaries that proliferated in 2020 are as motivated as ever, evidenced by the introduction of increasingly damaging tactics and attacks. There is also evidence that remote working increases the risk of a successful ransomware attack. There are weaker controls on home technology and a higher likelihood of individuals clicking on COVID-19 themed lure emails. Some current ransomware lures include:

- Information about vaccines, masks and critical medical supplies
- Financial scams offering government support and assistance
- Critical updates to collaboration and workforce effectiveness

In 2020 five key ransomware variants affected the healthcare sector: Maze, Conti, Netwalker, REvil and Ryuk. Maze recently disbanded and formed Egregor, which is actively extorting organizations. Threat actors continue to target healthcare with ransomware given their susceptibility and prominence amid the pandemic. Hackers will continue to leak, trade and sell databases containing PHI stolen in these attacks.

Where we are:

- Nearly four out of five interactive intrusions uncovered in 2020 were driven by eCrime actors
- Overall numbers of all types of malware were significantly larger than 2020 over 2019
- Threat tracking groups show that nation-state adversaries (North Korea, China, Russia, Iran) are not letting up and continue to merit strong consideration in 2021
- Healthcare R&D continues to be a high-priority collection requirement for many targeted intrusion adversaries
- The selling of access to healthcare entities has more than doubled in the last year
- Perimeter vulnerabilities were the most common entry point in healthcare related cases. Attackers exploited unpatched vulnerabilities and weak, reused or default passwords used in remote connections
- Healthcare victims face a secondary threat from ransomware operations that exfiltrate data prior to the execution of the ransomware

A new money-making endeavor has sprung up. Hackers called Initial Access Brokers gain access through several means with Remote Desktop Protocol (RDP) as the most common entry point. RDP can be compromised through a mix of open-source tracking of email formats and credential stuffing attacks to find passwords without alerting network administrators. Once an entry is gained, it's then sold online to the highest bidder. Access is most frequently sold to ransomware groups through the dark web and other cybercrime forums.

Education is key to preventing a successful Ransomware attack. Train staff to identify email attachments and links that could contain ransomware, by showing typical attack examples and providing

tips on identifying lures. Perform phishing simulations to train staff to be diligent when examining emails and provide staff a practical guide on what to do if their device is compromised. Also, it is important that staff are comfortable in reporting incidents and allowing the organization to deal with the consequences.

Some practical steps to protect your organization against ransomware include:

- Ransomware can overwrite incremental and other online backups. Take regular full system backups of servers, databases and file stores
- Maintain an additional offline copy of key servers and data sets where a criminal who acquires domain administrator rights can't access the copy
- Patch critical vulnerabilities on a timely and periodic basis
- Configure email phishing controls as tight as you can
- Perform more thorough checking of embedded mail links using Microsoft Advanced Threat Protection
- Encourage a stricter separation between personal and corporate devices and ensure security software is installed on personal devices

Cybersecurity readiness matters more than ever during this time of increased cyber-attacks. Be prepared. A serious ransomware incident can and probably will affect you at some time. Don't assume it won't. Be protected and ready now.