ABA Insurance Services | MEMBER OF GREAT AMERICAN INSURANCE GROUP

SafeAlert™

Be aware of emerging Ransomware ruses hitting the banking industry

Cybersecurity has been a key concern for banks for many years, especially related to ransomware threats and tactics. 85% of community bank executives cited cybersecurity as a top priority according to a 2022 survey conducted by the Risk Management Association.

While losses from ransomware are nothing new, this SafeAlert addresses a few emerging trends that distinguish the current threat landscape from the environment of only a few years ago and offers some best practices that may mitigate your exposure.

Supply Chain Attacks are those where threat actors target critical supply chain vendors, hoping to inflict serious financial and reputational damage to the many companies downstream of that vendor. By increasing their "blast radius" and creating major disruption, criminals seek to maximize ransom amounts and increase their odds of getting paid. For example, a 2021 ransomware attack affected at least 1,500 customers of an IT service provider. Another highly publicized event, the 2020 SolarWinds hack, affected over 18,000 users of their system management software.

Intermittent Encryption is the process of only partially encrypting files. It is designed to increase the speed of a malware attack, thereby increasing the odds the malware will avoid detection by security software.

Double Extortion is a particularly concerning situation where threat actors gain additional leverage over their victims by both encrypting your system and exfiltrating sensitive information such as PPI of your customer base. The hackers then threaten to release the data if they are not paid. The potential reputational damage to your bank has the potential to be a greater threat than your encrypted system. Cybersecurity pundits opine threat actors view extortion of exfiltrated data to be more attractive than mere ransomware.

Ransomware as a Service (RaaS) is an extremely alarming trend where novice threat actors, lacking the sophistication or time to develop their own code, purchase ransomware variants on the Dark Web from proven operators. Think of RaaS as pay-for-use malware. It provides the necessary code and operational infrastructure to launch and maintain a ransomware campaign against your bank.

Steps to Mitigate Ransomware

- ☑ Security Awareness Training. Staff awareness and education are critical as people are the most vulnerable entry point for cyber-attacks. Regular, ongoing training that emphasizes the latest attack vectors is your best protection.
- ☑ Multifactor Authentication. MFA is an authentication method that requires users to provide two or more verification factors to gain system access, going beyond standard username and password log in requirements. MFA is a core component of proper cyber hygiene and should be part of your bank's security protocol.
- ☑ Incident Response Plans. In the event your bank's cybersecurity safeguards fail, it is critical that you have an incident response plan in place. The plan should clearly outline what procedures to enact during a threat. It should include your internal IT resources as well as your insurance provider's breach response services and clearly outline the responsibilities of the various team members. Regular testing and updating of the plan is highly recommended as threats evolve.

Source: techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts

Visit abais.com for more loss control information or to view this SafeAlert® online. To subscribe to SafeAlert, request reprints or if you have questions about this newsletter or articles, contact marketing@abais.com or 800-274-5222.