Ransomware Advisory

09 / 15 / 2019

If you have any questions about this memorandum, please contact your regular Certus Cybersecurity representative.

This memorandum is intended to help companies understand the significant threats posed by ransomware cyberattacks and what they can do to protect against these potentially devastating events.

What is Ransomware?

Ransomware is malicious software (malware) used in a cyberattack to encrypt the victim's data with an encryption key that is known only to the attacker, thereby rendering the data unusable until a ransom payment (usually cryptocurrency, such as Bitcoin) is made by the victim.

Why Should You be Concerned?

If your company is the victim of a ransomware attack, many, if not all, of your key systems will be disabled, which will likely have an immediate and severe impact on your company's ability to operate. If you elect to pay the ransom, the amount paid may have a significant impact on your profitability. In addition, companies that pay the ransom have no guarantee that the attackers will provide the encryption keys necessary to restore normal operation. In short, the impacts can be devastating. Taking action to prevent ransomware attacks should be a top priority for any company.

How does it Work?

Ransomware is most commonly delivered to the victim's systems through exploit kits, waterhole attacks (in which one or more websites that an organization frequently visits is infected with malware), malicious advertising (malvertising), or email phishing campaigns. Attackers will usually gain initial access to targeted systems using one of two methods:

- Social engineering/phishing to get an unsuspecting user to expose their network credentials or install malware.
- Exploiting a vulnerability in a public-facing (internet) application or service.

Once delivered, ransomware typically uses some form of an embedded file extension list to identify user files and data to be encrypted. It is also programmed to avoid interacting with certain system directories (e.g., WINDOWS system directory or certain program files directories) to ensure system stability for delivery of the ransomware after the payload finishes running. Files in specific locations, that match one of the listed file extensions, are then encrypted. Otherwise, the file(s) are left alone. After encrypting the files, the ransomware typically leaves a notification for the user with instructions on how to pay the ransom.

What Can You do to Protect Against Ransomware Attacks?

Fortunately, there are many steps you can take to proactively guard against these insidious attacks. Here are Certus Cybersecurity's top recommendations:

1. Conduct regular security awareness training for your employees. It is especially important to focus training on awareness of social engineering attacks (e.g., phishing, phone scams, and impersonation calls) and the importance of inspecting all emails closely before opening any attachment.

This memorandum was prepared by Certus Cybersecurity for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

Certus Cybersecurity
303 Twin Dolphin Drive
Suite 1100
Redwood City, CA 94065
877.905.0975

2. Create and enforce policies for email hygiene, password sharing (e.g., prohibitions against sharing or revealing user credentials—even with IT and/or security), and strong passwords.
3. Mark all emails from external sources as “Email from external source”.
4. Enable security functionality on email gateways including blocking or removing executables and sandbox detonation for email attachments, sender policy framework (SPF) verification to mitigate email spoofing, and email throttling (or “graylisting”) to rate-limit potential spam emails.
5. Conduct periodic automated port and vulnerability scans to identify and alert on vulnerable software and unauthorized ports, devices, and wireless access points.
6. Implement automated patch management tools to frequently deploy operating system and software patches to ensure the most recent vendor security updates are implemented.
7. Disable unnecessary, vulnerable, or unsupported software, including browsers, email clients, browser plugins, and email client plugins.
8. Implement two-factor authentication (where possible).
9. Centralize security logging on a secure log collector or security incident and event management (SIEM) platform, and frequently review and analyze log information. Ensure logging includes sufficient detail to enable effective diagnosis of potential security issues (e.g., date and time stamp, source and destination addresses, event source). Ensure logs are reviewed regularly to identify potential security issues.
10. Enforce the principle of least privilege and eliminate user “privilege creep” to limit an attacker’s ability to escalate privileges.
11. Identify services that are critical for business survival and ensure they are automatically backed up on a regular basis. Implement and regularly test a disaster recovery program to ensure you can restore critical systems from the backup location. Backups should be encrypted and maintained on a separate backup network.
12. Assess and practice your incident response capabilities, and monitor and measure the overall effectiveness of your security posture on an ongoing and continual basis.

Please contact your Certus Cybersecurity representative if you have any questions on this memorandum or would like our help in implementing any of these important steps to prevent ransomware attacks.