Ransomware

Ransomware is a form of malware that targets both human and technical weaknesses in organizations in an effort to deny the availability of critical data and/or systems. When the victim organization determines they are no longer able to access their data, the cyber actor demands the payment of a ransom, at which time the actor purportedly provides an avenue to the victim to regain access to their data. Recent iterations target enterprise end users, making awareness and training a critical preventative measure.

Infection Vectors

Ransomware is frequently delivered through phishing e-mails to end users. Early ransomware e-mails were often generic in nature, but more recent e-mails are highly targeted to both the organization and individual, making scrutiny of the document and sender important to prevent exploitation. An e-mail compromise occurs in one of two ways:

1. Receipt of an e-mail containing malicious attachments, including: .pdf, .doc, .xls, and .exe file extensions. These attachments are described as something that appears legitimate, such as an invoice or electronic fax, but contain malicious code.

2. Receipt of an e-mail that appears legitimate but contains a link to a website hosting an exploit kit.

When the user opens the malicious file or link in the phishing e-mail, the most frequent end result is the rapid encryption of files and folders containing business-critical information and data. Recent ransomware campaigns have employed robust encryption that prevents most attempts to break the encryption and recover the data.

Another infection method involves adversaries hacking a known website to plant the malware. End users are infected when visiting the compromised website while using outdated browsers, browser plugins, and other software.

After infection, the malware usually calls home to command and control (C2) infrastructure to obtain encryption keys from the adversary. Once keys are obtained, the malware begins rapidly encrypting files and folders on local drives, attached drives, and network shares to which the infected user has access. Organizations are generally not aware that they have been infected until users are no longer able to access data or begin to see messages advising them of the attack and demanding a ransom payment.

While the FBI normally recommends organizations invest in measures to prevent, detect, and remediate cyber exploitation, the key areas to focus on with ransomware are prevention, business continuity, and remediation. It is very difficult to detect a successful ransomware compromise before it is too late. The best approach is to focus on defense in depth, or several layers of security, as there is no single method to prevent a compromise. As ransomware techniques and malware continue to evolve and become more sophisticated, even with the most robust prevention controls in place, there is no guarantee against exploitation. This fact makes contingency and remediation planning crucial to business recovery and continuity, and those plans should be tested regularly to ensure the integrity of sensitive data in the event of a compromise.

Cyber DIVISION
FEDERAL BUREAU OF INVESTIGATION

Prevention Considerations

- Focus on awareness and training. Since end users are targeted, employees should be made aware of the threat of ransomware, how it is delivered, and trained on information security principles and techniques.
- Patch the operating system, software, and firmware on devices. All endpoints should be patched as vulnerabilities are discovered. This can be made easier through a centralized patch management system.
- Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.
- Manage the use of privileged accounts. Implement the principle of least privilege. No users should be assigned administrative access unless absolutely needed. Those with a need for administrator accounts should only use them when necessary; and they should operate with standard user accounts at all other times.
- Implement least privilege for file, directory, and network share permissions. If a user only needs to read specific files, they should not have write access to those files, directories, or shares. Configure access controls with least privilege in mind.
- Disable macro scripts from office files transmitted via e-mail. Consider using Office Viewer software to open Microsoft Office files transmitted via e-mail instead of full office suite applications.
- Implement software restriction policies (SRP) or other controls to prevent the execution of programs in common ransomware locations, such as temporary folders supporting popular Internet browsers, or compression/decompression programs, including those located in the AppData/LocalAppData folder.

Business Continuity Considerations

- Regularly back up data and verify its integrity.
- Secure your backups. Ensure backups are not connected to the computers and networks they are backing up. Examples might be securing backups in the cloud or physically storing them offline. Some instances of ransomware have the capability to lock cloud-based backups when systems continuously back up in real-time, also known as persistent synchronization. Backups are critical in ransomware; if you are infected, backups may be the best way to recover your critical data.

Other Considerations

Some other considerations that can be highly dependent on organizational budget and system configuration include:

- Implement application whitelisting. Only allow systems to execute programs known and permitted by security policy.
- Use virtualized environments to execute operating system environments or specific programs.
- Categorize data based on organizational value, and implement physical/logical separation of networks and data for different organization units. For example, sensitive research or business data should not reside on the same server and/or network segment as an organization's e-mail environment.
- Require user interaction for end user applications communicating with websites uncategorized by the network proxy or firewall. Examples include requiring users to type information or enter a password when their system communicates with a website uncategorized by the proxy or firewall.

The Ransom

The FBI does not advocate paying a ransom to an adversary. Paying a ransom does not guarantee an organization will regain access to their data. In fact, some individuals or organizations were never provided with decryption keys after paying a ransom. Paying a ransom emboldens the adversary to target other organizations for profit and provides a lucrative environment for other criminals to become involved. Finally, by paying a ransom, an organization is funding illicit activity associated with criminal groups, including potential terrorist groups, who likely will continue to target an organization. While the FBI does not advocate paying a ransom, there is an understanding that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers.

In all cases, the FBI encourages organizations to contact their local FBI Cyber Task Force immediately to report a ransomware event and request assistance. The FBI works with federal, state, local, and international partners to pursue cyber actors globally and assist victims of cyber crime. Victims are also encouraged to report cyber incidents to the FBI's Internet Crime Complaint Center (www.ic3.gov).

Contact the **Cyber Task Forces** at www.fbi.gov/contact-us/field
and the **Internet Crime Complaint Center** at www.ic3.gov