October 02, 2019

Alert Number
I-100219-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field-offices

HIGH-IMPACT RANSOMWARE ATTACKS THREATEN U.S. BUSINESSES AND ORGANIZATIONS

This Public Service Announcement (PSA) is an update and companion to Ransomware PSA I-091516-PSA posted on www.ic3.gov. This PSA contains updated information about the ransomware threat.

WHAT IS RANSOMWARE?

Ransomware is a form of malware that encrypts files on a victim's computer or server, making them unusable. Cyber criminals demand a ransom in exchange for providing a key to decrypt the victim's files.

Ransomware attacks are becoming more targeted, sophisticated, and costly, even as the overall frequency of attacks remains consistent. Since early 2018, the incidence of broad, indiscriminant ransomware campaigns has sharply declined, but the losses from ransomware attacks have increased significantly, according to complaints received by IC3 and FBI case information.

Although state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector.

HOW DOES RANSOMWARE INFECT ITS VICTIMS?

Cyber criminals use a variety of techniques to infect victim systems with ransomware. Cyber criminals upgrade and change their techniques to make their attacks more effective and to prevent detection.

The FBI has observed cyber criminals using the following techniques to infect victims with ransomware:

- Email phishing campaigns: The cyber criminal sends an email containing a malicious file or link, which deploys malware when clicked by a recipient. Cyber criminals historically used generic, broad-based spamming strategies to deploy their malware, while recent ransomware campaigns have been more targeted. Criminals may also compromise a victim's email account by using precursor malware, which enables the cyber criminal to use a victim's email account to further spread the infection.
- Remote Desktop Protocol vulnerabilities: RDP is a proprietary network protocol that allows individuals to control the resources and data of a computer over the internet. Cyber criminals have used both brute-force methods, a technique using trial-and-error to obtain user credentials, and credentials purchased on darknet marketplaces to gain unauthorized RDP access to victim systems. Once they have RDP access, criminals can deploy a range of malware—including ransomware—to victim systems.
- Software vulnerabilities: Cyber criminals can take advantage of security weaknesses in widely used software programs to gain control of victim systems and deploy ransomware. For example, cyber criminals recently exploited vulnerabilities in two remote management tools used by managed service providers (MSPs) to deploy ransomware on the networks of customers of at least three MSPs.

IF MY SYSTEM IS INFECTED, SHOULD I PAY THE RANSOM? SHOULD I CONTACT THE FBI?

The FBI does not advocate paying a ransom, in part because it does not guarantee an organization will regain access to its data. In some cases, victims who paid a ransom were never provided with decryption keys. In addition, due to flaws in the encryption algorithms of certain malware variants, victims may not be able to recover some or all of their data even with a valid decryption key.

Paying ransoms emboldens criminals to target other organizations and provides an alluring and lucrative enterprise to other criminals. However, the FBI understands that when businesses are faced with an inability to function, executives will evaluate all options to protect their shareholders, employees, and customers.

Regardless of whether you or your organization have decided to pay the ransom, the FBI urges you to report ransomware incidents to law enforcement. Doing so provides investigators with the critical information they need to track ransomware attackers, hold them accountable under U.S. law, and prevent future attacks.

HOW CAN I PROTECT MYSELF AGAINST RANSOMWARE?

The most important defense for any organization against ransomware is a robust system of backups. Having a recent backup to restore from could prevent a ransomware attack from crippling your organization. The time to invest in backups and other cyber defenses is *before* an attacker strikes, not afterward when it may be too late.

As ransomware techniques and malware continue to evolve and become more sophisticated, even the most robust prevention controls are no guarantee against exploitation. This makes contingency and remediation planning crucial to business recovery and continuity. Those plans should be tested regularly to ensure the integrity of sensitive data in the event of a compromise.

CYBER DEFENSE BEST PRACTICES

- Regularly back up data and verify its integrity. Ensure backups are not connected to the computers and networks they are backing up. For example, physically store them offline. Backups are critical in ransomware; if you are infected, backups may be the best way to recover your critical data.
- Focus on awareness and training. Since end users are targeted, employees should be made aware of the threat of ransomware and 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 that regular scans are conducted.
- Implement the 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 email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Office Suite applications.
- Implement software restriction policies or other controls to prevent the execution of programs in common ransomware locations, such as temporary folders supporting popular internet browsers, and compression/decompression programs, including those located in the AppData/LocalAppData folder.
- Employ best practices for use of RDP, including auditing your network for systems using RDP, closing unused RDP ports, applying two-factor

	authentication wherever possible, and logging RDP login attempts. • 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 and logical separation of networks and data for different organizational units. For example, sensitive research or business data should not reside on the same server and network segment as an organization's email environment. • Require user interaction for end-user applications communicating with websites uncategorized by the network proxy or firewall. For example, require users to type information or enter a password when their system communicates with a website uncategorized by the proxy or firewall.