Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Date: September 15, 2016
Alert Number: I-091516-PSA

RANSOMWARE VICTIMS URGED TO REPORT INCIDENTS TO FEDERAL LAW ENFORCEMENT

The FBI issued a Public Service Announcement on September 15, 2016, urging victims to report ransomware incidents to federal law enforcement to "help us gain a more comprehensive view of the current threat and its impact on U.S. victims." This document presents excerpts from the original PSA, which is available at the link above.

What Is Ransomware?

Ransomware is a type of malware installed on a computer or server that encrypts the files, making them inaccessible until a specified ransom is paid. It is an increasingly popular cybercrime.

Ransomware is typically installed when a user clicks on a malicious link, opens a file in an email that installs the malware, or through drive-by downloads (which do not require user-initiation) from a compromised website. Ransomware can also be delivered through social engineering, with callers posing as Microsoft computer technicians, for example, alerting users to urgent problems with their computers and offering immediate remote access resolution.

Recommended Preventive Measures

The FBI recommends computer users consider the following prevention and continuity measures to lessen the risk of a successful ransomware attack.

1. Regularly back up data and verify the integrity of those backups. Backups are critical in ransomware incidents; if your computer is infected, backups may be the best way to recover your critical data.

2. Patch all endpoint device operating systems, software, and firmware as vulnerabilities are discovered. This precaution can be made easier through a centralized patch management system.
3. Focus on user awareness and training. Because end users are often targeted, employees should be made aware of the threat of ransomware and how it is delivered. They should also be trained on information security principles and techniques.
4. Scrutinize links contained in emails and do not open attachments included in unsolicited emails.
5. Only download software – especially free software – from sites you know and trust. When possible, verify the integrity of the software through a digital signature prior to execution.
6. Ensure that application patches for the operating system, software, and firmware are up to date, including Adobe Flash, Java, Web browsers, etc.
7. Ensure anti-virus and anti-malware solutions are set to automatically update and regular scans are conducted.
8. Implement application whitelisting. Only allow systems to execute programs known and permitted by security policy.
9. Disable macro scripts from files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Office Suite applications.
10. Implement software restrictions 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.
11. Manage the use of privileged accounts by implementing 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; they should operate with standard user accounts at all other times.
12. Configure access controls with least privilege in mind. If a user only needs to read specific files, he or she should not have write access to those files, directories, or shares.
13. Use virtualized environments to execute operating system environments or specific programs.
14. Secure your backups by ensuring they are not connected to the computers and networks they are backing up. Examples might include securing backups in the cloud or physically storing them offline. It should be noted, 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.
15. Categorize data based on organizational value, and implement physical/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/or network segment as an organization's email environment.

16. Require user interaction for end user applications communicating with websites uncategorized by the network proxy or firewall. Examples include requiring users to type in information or enter a password when the system communicates with an uncategorized website.

Why the FBI Needs Your Help

New ransomware variants are emerging regularly. Cyber security companies reported that in the first several months of 2016, global ransomware infections were at an all-time high. Within the first weeks of its release, one particular ransomware variant compromised an estimated 100,000 computers a day.

Ransomware infections impact individual users and businesses regardless of size or industry by causing service disruptions, financial loss, and in some cases, permanent loss of valuable data. While ransomware infection statistics are often highlighted in the media and by computer security companies, it has been challenging for the FBI to ascertain the true number of ransomware victims as many infections go unreported to law enforcement.

Victims may not report to law enforcement for a number of reasons, including concerns over not knowing where and to whom to report; not feeling their loss warrants law enforcement attention; concerns over privacy, business reputation, or regulatory data breach reporting requirements; or embarrassment. Additionally, those who resolve the issue internally either by paying the ransom or by restoring their files from back-ups may not feel a need to contact law enforcement.

The FBI is urging victims to report ransomware incidents regardless of the outcome. Victim reporting provides law enforcement with a greater understanding of the threat, provides justification for ransomware investigations, and contributes relevant information to ongoing ransomware cases. Knowing more about victims and their experiences with ransomware will help the FBI to determine who is behind the attacks and how they are identifying or targeting victims.

New Threats Target Business Servers

All ransomware variants pose a threat to individual users and businesses. Recent variants have targeted and compromised vulnerable business servers (rather than individual users) to identify and target hosts, thereby multiplying the number of potential infected servers and devices on a network.

Cybercriminals engaging in this targeting strategy are also charging ransoms based on the number of host (or servers) infected. Additionally, recent victims who have been infected with these types of ransomware variants have not been provided the decryption keys for all their

files after paying the ransom, and some have been extorted for even more money after payment.

This recent technique of targeting host servers and systems could translate into victims paying more to get their decryption keys, a prolonged recovery time, and the possibility that victims will not obtain full decryption of their files.

The FBI Does Not Support Paying the Ransom

The FBI does not support paying ransom to the cybercriminal for these reasons:

1. Paying a ransom does not guarantee the victim will regain access to their data; in fact, some individuals or organizations are never provided with decryption keys after paying a ransom.
2. Paying a ransom emboldens the adversary to target other victims for profit
3. Paying a ransom could provide incentive for other cybercriminals to engage in similar illicit activities for financial gain.

While the FBI does not support paying a ransom, it recognizes executives, when faced with inoperability issues, will evaluate all options to protect their shareholders, employees, and customers.

What to Report to Law Enforcement

The FBI is requesting victims reach out to their local FBI office and/or file a complaint with the **Internet Crime Complaint Center**, at www.IC3.gov, with the following ransomware infection details (as applicable):

1. Date of Infection
2. Ransomware Variant (identified on the ransom page or by the encrypted file extension)
3. Victim Company Information (industry type, business size, etc.)
4. How the Infection Occurred (link in email, browsing the Internet, etc.)
5. Requested Ransom Amount
6. Actor's Bitcoin Wallet Address (may be listed on the ransom page)
7. Ransom Amount Paid (if any)
8. Overall Losses Associated with a Ransomware Infection (including the ransom amount)
9. Victim Impact Statement

For the original Alert go to: https://www.ic3.gov/media/2016/160915.aspx