Managed Security Pulse eNewsletter

September 2016

SOC Threat Advisory Threat Level – Restricted

Ransomware

This is to reference the [SingCERT] Ransomware
05/06/16

Overview

There has been a noticeable rise in ransomware infections in both Singapore and overseas. This advisory provides information on ransomware and how enterprises can mitigate and prevent this threat.

Currently, recovery of any data infected by ransomware is extremely difficult. Only a handful of decryptors which worked for older versions of ransomware are available. The best way to guard against ransomware is to prevent it from happening.

What is Ransomware?

Ransomware is a type of malware that holds a victim's files, computer system or mobile device ransom, restricting access until a ransom is paid. Operating systems that can be infected include Windows, Mac OS X and Linux. Some ransomware variants are also known to traverse across the network and encrypt all files stored in shared and/or network drives. The more prevalent type of ransomware today encrypts commonly-used files, such as user documents, images, audio, and video files.

Once the files in an infected computer have been encrypted, a ransom note will be displayed on screen to the victim, detailing the steps that need to be taken to decrypt the files.

Ransomware has proven to be effective in extorting money from victims. By holding important data ransom, cyber criminals instill fear and panic into their victims and further pressure them to pay the ransom by threatening destruction of the decryption key.

How is Ransomware Spread?

There are numerous ways in which ransomware is known to spread.

One common way is through phishing emails that contain malicious attachments or links. Unsuspecting users can be infected with ransomware if they open these attachments or links, although these are rarely the ransomware itself. Rather they tend to take the form of an inconspicuous document, which when opened, downloads the ransomware from an external server and executes it.

Secondly, the unsuspecting victim may click on a malicious link and be redirected to a malicious website that contains scripts to automatically download and install the malware without their knowledge.

Thirdly, the infection vector for ransomware may come through malicious advertisements that exploit vulnerabilities in the user's browser to serve and install ransomware (commonly known as drive-by downloads). Such advertisements may be found on malicious websites, and–to a much lesser extent–even legitimate websites, if the advertisement service has been compromised.

Symptoms of Ransomware Infection

A key sign of a ransomware infection is the inability of a victim to access his/her files or computer system. A ransom note will also persistently appear, typically replacing the Desktop's wallpaper, to inform the victim of the ransom and payment instructions.

Some ransomware set deadlines for the victim to pay the ransom. Failing to meet these deadlines may result in the ransom increasing in price, or deletion of the decryption key, which would result in the victim losing his/her files or access to the computer permanently.

Impact of Ransomware

Ransomware is indiscriminate and destructive in nature; it targets both home and business users, and its impact can be disastrous. Personal, sensitive, or propriety information may be lost if there is no backup of this data. Business operations may also be disrupted if employees are unable to work because certain files are encrypted. Furthermore, there may be financial implications to reinstate personal computers or business systems back to their original state.

Solution

The best solution for ransomware is to prevent it from happening. Fujitsu recommends that users take the following preventive measures to better protect themselves against ransomware:

- Follow Internet Browsing Best Practices to Stay Safe Online
  - Users should exercise caution and avoid opening suspicious email attachments; when in doubt, verify with the email sender if they had sent the email.
  - Similarly, do not click on suspicious links to websites that you do not recognise or are sent from people you do not know. These websites may contain malicious codes that infect a visitor's computer with ransomware.
  - More importantly, do not download software from unofficial or disreputable sources.

- Update Software Regularly
  - Some types of ransomware rely on software vulnerabilities to infect a system. Keep your operating system and anti-malware software updated with the latest patches to prevent such exploits.
  - Perform a scan of your entire computer at least once a week, and scan all files you receive or removable storage devices that you connect.

- Perform File Backups Regularly
  - Ransomware leverages on scare tactics by holding your data ransom. Having data backups to circumvent this limits the impact of a ransomware attack, and is pivotal to the recovery process. Formulate a backup and recovery plan for critical data, and perform data backups regularly.

  - As ransomware is able to infect connected storage devices, take additional precaution and ensure that your backups are stored offline or disconnected when not in use.
  - For a full list of recommended best practices to safe Internet browsing, visit https://www.csa.gov.sg/gosafeonline/go-safe-for-me/homeinternetusers/protect-your-computer-from-cyber-threats

Additional Preventive Measures to Consider

While the measures highlighted above are important to keeping your data safe and secure, there are additional preventive measures you should consider to further safeguard against ransomware attacks.

- Encrypt sensitive data

  Some variants of ransomware encrypt only commonly-used file types, such as images and documents. Consider encrypting your data, which will prevent such ransomware from doing so. Sensitive or critical data should, all the more, be encrypted to prevent loss or leakage.

- Enable Microsoft Office macros only when required

  One key delivery mechanism of ransomware is the abuse of Microsoft Office macros to infect a computer with ransomware. Users are advised to be cautious and enable macros only for trusted documents.

- Application Control

  Consider installing application control software that provides application and/or directory whitelisting. Whitelisting allows only approved programs to run while restricting all others, and is one of the best security practices to protect a computer system.

- Restrictive Access

  Strictly limit the number of people and systems with access privileges for shared data.

- Education to Users

  Conduct trainings and workshops for all end users on preventive measures. Educating them on such attacks is particularly important as these techniques play a crucial role in carrying out successful attacks.

How to Remove Ransomware?

In the event that a machine is infected with ransomware, Fujitsu recommends taking the following measures:

1. Disconnect the infected computer immediately from:
   - Any wired or wireless network (e.g. Internet and Intranet) that it is connected to
   - Storage devices such as cloud-based storage, external hard disks, and Network Attached Storage (NAS)
   - Bluetooth devices

Doing so isolates the infected system and prevents further spread of the ransomware.

2. Scan and disinfect the computer with an antivirus or anti-malware application. Most types of ransomware create some form of persistence in the infected computer, and may re-encrypt data subsequently if not properly removed.

3. Perform data restoration from the backup sources. If possible, do on a clean installation to ensure that the system is completely free of malware.

Further Reading:

https://www.us-cert.gov/ncas/alerts/TA16-091A

http://www.bleepingcomputer.com/virus-removal/ransomware

https://threatpost.com/new-server-side-ransomware-hitting-hospitals/117059/

http://www.webroot.com/hk/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering

For more information, please contact:

Fujitsu Managed Security Services

fapl.askMSS@sg.fujitsu.com