Ransomware Protection Guide

1. Prevention Advice - ransomware attack prevention measures

1.1 Precautionary measures – System Protection

(1) Use antivirus software and update the system and applications in a timely manner：Attackers usually use unpatched vulnerabilities to access unauthorized systems and networks to perform subsequent malicious activities.

- Antivirus/antimalware software should be installed and keep updated for the virus and malicious signature code. Perform a scan for the system and network at least once a week, and scan all received documents.
- When a mobile storage device (such as a flash drive) is connected, an antivirus scan should be performed.
- Update the system and application software to the latest version, also download the latest security update file.

(2) Strengthen the security of the server with dispatch ability: Because the antivirus software has central control on AD server, asset management system, etc. it is necessary to pay special attention to security updates and closely watch their group policies for abnormal changes.

(3) Only enable Microsoft Office macros as needed：Ransomware may infect through malicious Microsoft Office files and introduce virus with macros enable when view the file incautiously.

(4) Minimize open port setting：Ransomware may use exposed services and open ports (such as RDP port 3389 and SMB port 445) to spread on the Internet. In addition to confirming the necessity of opening, it should also be confirmed that the users of these services are trusted.

(5) Set up a firewall to block any network connection with known malicious IP and URL, prohibit the use of rules that allow any connection, and only allow connections with external service IP and DN.

(6) Minimum use authority of personnel：In order to reduce the opportunity for attackers to gain administrative rights, we should：

- Control and restrict access rights, and only those who need full access rights to perform work are authorized.
- Provide users other than managers with the minimum authority required for their duty.
- View and manage all the usage of user accounts and disable inactive accounts.
- Implement multi-factor authentication.

(7) Raise cyber security awareness：Employees should be trained regularly to establish good cybersecurity awareness and Internet use behavior, such as identifying suspicious e-mails, do not click links randomly, and do not open e-mail attachments from unknown or untrusted sources. In addition, conduct social engineering drills to improve training effectiveness.

1.2 Precautionary measures – Data Protection

(1) Encrypt important and sensitive information：Important and sensitive data should be encrypted. If the data is stolen, it can increase the difficulty for the attacker. In addition, some ransomware only works on common file types (such as images and documents), and encryption can also prevent them from detecting files.

(2) Maintain updated backup and keep them offline：Performing data backup regularly helps to restore data in the event of a ransomware attack, and the host or device storing the backup data should not be connected to the network to prevent the ransomware from affecting the backup data through the network.

- 3-2-1 Backup principle：3 backups, 2 storage media, and 1 offsite storage location.

(3) Regularly maintain image files of important systems：The image file of a virtual machine or server includes a pre-configured operating system and related application software. When an attack occurs and the system needs to be rebuilt, these image files can be used to achieve rapid deployment and recovery.

1.3 Precautionary measurement for enterprise organizations – Preparation for Incident Handling

(1) Before an incident occurs, it is very important to develop an incident contingency plan and conduct drill to verify whether the plan is feasible. When attacked, it is difficult to judge the correct course of action immediately. The plan and implementation will help employees understand the actions to be taken and determine the priority of restoration of various systems and environments.

(2) Prepare a list of external information security units that can seek assistance when a cyber security incident occurs, and a list of police investigations and contact methods.

2. Ransomware Response - response measurement after being infected by ransomware

2.1 How to identify a ransomware attack?

The initial symptom when attacked by ransomware is large number of files are been encrypting, which cause the hard disk, CPU, and memory run with very high usage. In addition, the affected files are usually modified with extensions.

After the file is encrypted, in most cases, the ransomware will demand a ransom from the victim, so the ransom message will be displayed on the screen of the device, or relevant documents will be posted. They will leave a way on how to contacting so the victim can communicate with the attacker about payment issues.

The attacker may even threaten to publish data online to force the victim to pay the ransom. For example, the attacker of the MAZE ransomware published the medical files of Hammersmith Medicines Research to force them to pay the ransom.

2.2 Contingency measures

(1) Immediately disconnect the infected device from all networks, whether wired, wireless or mobile-based. In very serious cases, consider turning off Wi-Fi, disabling any core network connections (including switches), and disconnecting the internet connection.

(2) Report the case to the Investigation Bureau or Criminal Bureau for assistance.

(3) Report information security incidents through the official website of TWCERT/CC (twcert.org.tw) or Email (twcert@cert.org.tw).

(4) Seek external information security professional units to assist in handling the incident.

(5) Communicate in accordance with internal notification procedures and initiate relevant contingency measures.

(6) Monitor network traffic and perform anti-virus scans to determine if there are still infections.

(7) Take inventory of potentially affected devices and perform antivirus software scans on these devices.

(8) Most of the data encrypted by ransomware are difficult to crack, but you can still try to check the virus type through the ransomware name, extension and other information, look for a decryption tool provided by a trusted information security unit on the website of "no more ransom project"[1].

3. Ransomware Recovery - recovery phase

(1) Reset authorization credentials including passwords.

(2) Confirm that the infected device has been completely cleaned and reinstall the operating system.

(3) Before using the backup to restore, it is necessary to confirm that the backup does not contain any malicious software. If the backup and the equipment connected to it are very clean, the restoration should only be performed from the backup.

(4) Connect the device to a clean network to download, install, and update the operating system and all other software.

(5) Install, update and run antivirus software.

(6) It is recommended to share attack event information through TWCERT/CC (de-identification) to help other domestic and foreign enterprises and organizations prevent related attacks and reduce the impact of ransomware.

(7) Making improvement plan and execute according based on the cause of ransom and hacking.

[1] https://www.nomoreransom.org/zht_Hant/decryption-tools.html

Reference

[1]https://jenner.com/system/assets/assets/11480/original/memo-what-we-urge-you-to-do-to-protect-against-the-threat-of-ransomware.pdf
[2]https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf
[3] https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks