Ransomware Protection Guide

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 have 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 contact 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) Prevent expansion

- 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.
- If system services are interrupted by ransomware, the system mirror server should be started immediately to maintain uninterrupted system services and confirm that the system is not infected.

(2) Report

- Report to your nearest police station with evidence (Take screen shots of online evidence) or contact to the Investigation Bureau or Criminal Bureau for assistance.

- Report information security incidents through the official website of TWCERT/CC (twcert.org.tw) or Email (twcert@cert.org.tw).
- Seek external information security professional units to assist in handling the incident.
- Communicate in accordance with internal notification procedures and initiate relevant contingency measures.

(3) Impact confirmation

- Monitor network traffic and perform anti-virus scans to determine if there are still infections.
- Take inventory of potentially affected devices and perform antivirus software scans on these devices.

(4) Identify viruses and backup encrypted files

- 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, filename 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].
- For files that cannot find the decryption tool, you can back up these files to a safe place first. These archives can be decrypted when decryption tools appear in the future.
- Back up the system log file and send it to the external information security team for analysis. It is possible to understand the cause of the incident and reduce the chance of secondary infection.
- Inventory the scope of affected data, including design and development, testing, finance, customers, suppliers, account passwords and other sensitive data, in order to study the countermeasures for data damage or leakage.

[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