Ransomware Protection Guide

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) Investigate the cause of the incident to ensure that the same incident does not happen again.

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

(9) In addition to encrypting files, ransomware also conducts extortion by exposing data. Investigate whether information has been leaked in places such as Internet and the darknet. Investigate through tools such as haveibeenpwned, Firefox Monitor, OSRFramework, or seek help from outside information security companies.

(10) In the event of a data breach, the severity of Confidentiality, Integrity, and Availability should be assessed, and report to the relevant stakeholders.

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