Date2019/06/03

Cyberattack WarningRecently, PORT 445 is actively used by encryption ransomware, please step up the system/application updates and data backup operations

Subject: Cyberattack WarningRecently, PORT 445 is actively used by encryption ransomware, please step up the system/application updates and data backup operations

- Description:
  - N-ISAC security alert forward: NISAC-ANA-202006-0095
  - Recent ransomware attacks information indicates that this wave of ransomware was carried out by using Microsoft Server Message Block (SMB, PORT 445) protocol. When malware infects your computer, all files (including network drives, shared folder) on your computer will be encrypted and cannot be open or read, in order to blackmail users to pay for their files decryption.
  - It is recommended that all government agencies apart from strengthening the organization’s information security protection, also constantly check the relevant application updates, back up important files regularly, strengthen information security awareness and avoid opening unknown emails or links.
- Impacted platform: ALL
- Recommended practices:
  1. It is recommended that update the operating system as soon as possible, and close PORT 445 service if there is no special need.
  2. Identify important data, conduct regular backup operations with the following reference:
     - Perform important data backups regularly.
     - The backup data should have appropriate physical and environmental protection.
     - To ensure the availability of backup data, it should be tested periodically.
     - The duration of backup data and the requirement of permanent archival preservation should be considered by the data owner.
     - Confidential data backups should be protected by encryption.
  3. Check the user access permissions for network drives and shared folder to avoid unnecessary access.
  4. Check the update status of the operating system, antivirus software, and applications (e.g. Adobe Flash Player, Java), and regularly review system/application update records to prevent hackers from exploiting system/application security vulnerabilities.
  5. If you are using a USB flash drive to transfer data, it should be checked to verify if it infected by viruses or malware.
  6. If suspected infection is found, the following practices can be considered:
     - To prevent the spreading, shut down the computer and disconnect the network immediately.
     - Inform the IT staff or vendor to help salvage files that have not been encrypted.
     - It is recommended to reinstall the operating system and application, confirm the latest patch is installed before restore the backup data.

- Backup data should be checked with anti-virus software to ensure there is no residual malware before it is restored to the computer.

7. Enhance user education and training to pay attention to the relevant emails and the source of the emails, do not open the attached links or files from unknown sources, in case there are implanted in backdoor programs.

Network System Division
Computer and Communication Center