Date2019/05/07

Cyberattack WarningEncryption ransomware is rampant, please step up the system/application updates and data backup operations

Subject: Cyberattack WarningEncryption ransomware is rampant, please step up the system/application updates and data backup operations

- Description:
  - N-ISAC security alert forward: NISAC-ANA-202005-0115
  - Recently, ransomware attacks become more frequent. 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. According to a recent attack activity research report, hackers successfully invaded a target organization by advanced persistence APT (Advanced Persistent Threat). After obtaining the domain administrator authority, the ransomware distributed by group policy and spread out to achieve a maximum range of data encryption purposes. Members are advised to be vigilant and check the routine scheduling and delivery mechanisms regularly. The causes of the incident should be clarified in depth to avoid missing the opportunity for investigation. In addition, traditional ransomware transmits by application vulnerabilities (e.g. Flash Player) and social engineering. It is recommended that all members 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. Check the logs of the system, the scheduling and delivery mechanism of the system regularly. If abnormal connection or new scheduling is detected, the cause should be clarified in depth immediately.
  2. Check the account usage of the system from time to time and change the account password periodically. Ensure the password is accordance with the principle of complexity.
  3. Identify important data, conduct regular backup operations with the following reference:
     1. The backup data should have appropriate physical and environmental protection.Perform important data backups regularly.
     2. To ensure the availability of backup data, it should be tested periodically.
     3. The duration of backup data and the requirement of permanent archival preservation should be considered by the data owner.
     4. Confidential data backups should be protected by encryption.
  4. Check the user access permissions for network drives and shared folder to avoid unnecessary access.

Network System Division
Computer and Communication Center