Date：2019/05/19

【Cyberattack Warning】【Update malware matching information】【Encryption ransomware is rampant, please step up the system/application updates and data backup operations

Subject: 【Cyberattack Warning】【Update malware matching information】【Encryption ransomware is rampant, please step up the system/application updates and data backup operations

- Description:
  - N-ISAC security alert forward: NISAC-ANA-202005-0424
  - 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. Currently known malware information (SHA1) are listed below:
    03589DFFE2AB72A0DE5E9DCE61B07E44A983D857
    0b4b8404e459a4e892ad06e69ac05ec09d40d3a3
    0CB8ED29268EC9848FF1C7F25F28B620271E61C9
    0f63da0ce881fd3979864a0731b14231682e8e5b
    1acb8e1c912c00aa2de6fafedeff1869cfdbb254
    1f2d2b311c0fc6e04b868b8c54f4e2a4312c6ed3
    2051f0a253eced030539a10ebc3e6869b727b8a9
    2367326f995cb911c72baadc33a3155f8f674600
    275473714B3BDDBDE3FF1BDA892E4BD65C383DEB
    29cc0ff619f54068ce0ab34e8ed3919d13fa5ee9
    2ab7cdcae22011ee91823854792ab962611c698b
    2c68fbd1275de9a9ba0f5fbf742c3fffd4177e05
    321901969d7e63d64769236940618aed444f8271
    5B9B7FB59F0613C32650E8A3B91067079BCB2FC2
    5ce619790d42d49453dbb479074d5a5ae294ee0e
    5fc7165336fce9a2113da9ac4d28b56394e63fb1
    63697b356cb278535d847e9b27c49bd989e013a2
    65bc1801aca0af1a323bacc4b0208bc9321c879b
    6aed0e607eab4d4a1e2c038b5790dafa27801b74

71431cbfb8d0090b1ba6877c2774a83f61546035
75e49120a0238749827196cebb7559a37a2422f8
7a1c5e1799bdeebb01527f54a7fd89d0b720dea7
95db7a60f4a9245ffd04c4d9724c2745da55e9fd
9d6feb6e246557f57d17b8df2b6d07194ad66f66
a0402754def2c4055f0ea6f5da2db91de1e271d1
a2046f17ec4f5517636ea331141a4b5423d534f0
AD6783C349E98C2B4A8CE0B5C9207611309ADCA7
b78e56a2e84ae36d5cfadcad09057381f50b97c0
bab4b926042aa271c3fdd8d913bc70539152d04b
de9a0386c9736b60e63defd99eb0eba9930561d2
e7aa8f55148b4548ef1ab9744bc3d0e67588d5b7
ec7a59e79be688928d6c2441ec5c8e95532619cf
ef8cd0f9ef1e20b119f1908978d2e74b587c275e
efa69a6be36d0d4ec787515799c15ad236502be0
f0ebd358ceea9a90090c1cd0e6704965e234396f
f7db1c8e17aae7b5b0a1c3d168a2663cbc541219
f8c4cc8505982994e2855a9eacfd7c73bdc11b4f
f908577ed2eb1e913d93eb6261a4ece692ade364

    - In addition, traditional ransomware transmits by application vulnerabilities (e.g. Flash Player) and social engineering. 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. If a suspicious file is found in the system, it is recommended to perform a SHA1 comparison to confirm if it is malware.
    2. 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.
    3. 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.
    4. 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.
    5. Check the user access permissions for network drives and shared folder to avoid unnecessary access.
    6. 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.
    7. If you are using a USB flash drive to transfer data, it should be checked to verify if it infected by viruses or malware.
    8. 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.

9. 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