Nworm

TrickBot Updates Propagation Module

June 7th, 2020

www.atlas-cybersecurity.com

TrickBot Modules

- TrickBot is modular, which means it utilizes different binaries during infection to perform different functions. In typical cases, the basis for a TrickBot infection is a malicious Windows executable file that is saved to the disk
- This EXE is usually called a "TrickBot Loader" as its main function is to load the TrickBot modules
- The TrickBot modules are dynamic link libraries (DLLs) or EXEs run from system memory
  - On an infected Windows 10 host, TrickBot modules are only found in the system memory, while on an infected Windows 7 host, artifacts related to the modules are stored on the disk; these artifacts are in actuality encrypted binaries
  - During a typical TrickBot infection, these binaries are decrypted and run from system memory
- Three modules that TrickBot uses to spread to a Domain Controller in an Active Directory environment are:
  - mwormDll64 (the "mworm" module; deprecated and upgraded to "nworm")
  - mshareDll64 (the "mshare" module)
  - tabDll64 (the "tab" module)
- These three modules generate distinct activity when propagating to a vulnerable DC.
  - For the mshare and tab modules:
    - An infected Windows client retrieves a new TrickBot EXE using an HTTP URL.
    - The infected Windows client sends this new TrickBot EXE over SMB traffic to the vulnerable DC.
  - For the mworm module:
    - The infected Windows client uses an SMB exploit targeting the vulnerable DC.
    - The vulnerable DC retrieves a new TrickBot EXE using an HTTP URL and infects itself with it.

Upgrading to nworm

- First witnessed in April 2020, while generating a TrickBot infection in a lab environment, the TrickBot malware stopped using the mworm module; in its place, a new module named "nworm" appeared on an infected Windows 7 client
- HTTP traffic for TrickBot executables caused by nworm is noticeably different than traffic caused by mworm. The differences are:
    - mworm: URL for TrickBot EXE ends with /images/redcar.png
    - nworm: URL for TrickBot EXE ends with /ico/VidT6cErs
    - mworm: Follow-up TrickBot EXE is returned unencrypted in the HTTP traffic
    - nworm: Follow-up TrickBot EXE is returned as an encrypted or otherwise encoded binary in the HTTP traffic
- Like mworm, the new nworm module does not appear unless the TrickBot infection happens in an Active Directory environment with a Domain Controller
- The most important change is that when infected with TrickBot through nworm, the malware is run from memory. No artifacts are found on the infected domain controller and TrickBot on the DC does not remain after reboot or shutdown
    - In cases where mshare and tab infect a vulnerable DC with TrickBot, these infections remain persistent on the DC, but TrickBot caused by nworm is not persistent.

Indicators of Comrpomise

- **Recent HTTP URLs for TrickBot binaries for propagation to vulnerable DC**

  (Read: First seen YYYY-MM-DD – module name – URL)

  - 2020-04-20 – nworm – hxxp://107.172.221[.]106/ico/VidT6cErs
  - 2020-04-20 – mshare – hxxp://107.172.221[.]106/images/cursor.png
  - 2020-04-20 – tab – hxxp://107.172.221[.]106/images/imgpaper.png
  - 2020-05-08 – nworm – hxxp://23.95.227[.]159/ico/VidT6cErs
  - 2020-05-08 – mshare – hxxp://23.95.227[.]159/images/cursor.png
  - 2020-05-08 – tab – hxxp://23.95.227[.]159/images/imgpaper.png

Indicators of Compromise cont.

- **SHA256 hash for nwormDll64 artifact (encrypted binary) from an infected Windows 7 client on April 24th 2020:**
  - 900aa025bf7701024283 50e584e8110342a70159ef2f92a9bfd651c5d8e5f76b
- **SHA256 hash for nwormDll64 artifact (encrypted binary) from an infected Windows 7 client on May 8th 2020:**
  - 85d88129eab948d44bb9999774869449ab671b4d1df3c593731102592ce93a70