Pipemon

Modular Backdoor by the Winnti Group

June 6th, 2020

ATLAS CYBERSECURITY

www.atlas-cybersecurity.com

www.atlas-cybersecurity.com

The Attack

- Pipemon's first stage consists of a password protected RARSFX executable embedded in the .rsrc section of its launcher
- To make sure that the malware remains active on the systems, Winnti used Windows print processors that convert spooled data from a print job into a format readable by a print monitor.
- A malicious DLL loader drops where the print processors reside and registered as an alternative print processor. This is done by modifying one of the two registry values
  - DEment.dll
  - EntAppsvc.dll

www.atlas-cybersecurity.com

Maintaining Persistence

- Next, the malware restarts the print service to load the malicious process. Since the service starts every time the computer boots up, persistence is achieved.
  - ESET notes that a similar technique was seen with DePriMon downloader, but the researches believe that the way PipeMon does it is novel and has not been documented before
  - Also according to ESET, PipeMon is a modular backdoor, each component being a DLL with different functionality. They are encrypted on the disk and remain hidden by naming themselves as benign files with such names as
    - banner.bmp
    - certificate.cert
    - license.hwp

www.atlas-cybersecurity.com

The Trojan

- Custom commands can load other modules on demand
- A few of the things PipeMon is capable of are:
  - Send the victim's RDP information to the C&C server
  - Send OS, CPU, PC and time zone information to the C&C server
  - Send network information, disk drive information and running processes information to the C&C server

www.atlas-cybersecurity.com

Indicators of Compromise

- Filenames
  - 100.exe
  - 103.exe
  - Slack.exe
  - setup.exe
  - %SYSTEM32%\spool\prtprocs\x64\DEment.dll
  - %SYSTEM32%\spool\prtprocs\x64\EntAppsvc.dll
  - %SYSTEM32%\spool\prtprocs\x64\Interactive.dll
  - %SYSTEM32%\spool\prtprocs\x64\banner.bmp
  - %SYSTEM32%\spool\prtprocs\x64\certificate.cert
  - %SYSTEM32%\spool\prtprocs\x64\banner.bmp103.exe
  - %SYSTEM32%\spool\prtprocs\x64\License.hwpsetup.exe
  - %SYSTEM32%\spool\prtprocs\x64\D8JNCKSoDJE
  - %SYSTEM32%\spool\prtprocs\x64\BoSDFUWEkNCj.log
  - %SYSTEM32%\spool\prtprocs\x64\K9dsofhNCisdjf
  - %SYSTEM32%\spool\prtprocs\x64\JSONDIU7c9djE
  - %SYSTEM32%\spool\prtprocs\x64\NTFSSSE.log
  - AceHash64.exe
  - mz64x.exe

www.atlas-cybersecurity.com

Indicators of Compromise cont.

- Named Pipes
  - \\.\pipe\ScreenPipeRead%CNC_DEFINED%
  - \\.\pipe\ScreenPipeWrite%CNC_DEFINED%
  - \\.\pipe\RoutePipeWriite%B64_TIMESTAMP%
  - \\.\pipe\MainPipeWrite%B64_TIMESTAMP%
  - \\.\pipe\MainPipeRead%B64_TIMESTAMP%
  - \\.\pipe\MainHeatPipeRead%B64_TIMESTAMP%
  - \\.\pipe\InCmdPipeWrite%B64_TIMESTAMP%
  - \\.\pipe\InCmdPipeRead%B64_TIMESTAMP%
  - \\.\pipe\FilePipeRead%B64_TIMESTAMP%
  - \\.\pipe\FilePipeWrite%B64_TIMESTAMP%
  - \\.\pipe\ComHeatPipeRead%B64_TIMESTAMP%
  - \\.\pipe\CMDPipeRead
  - \\.\pipe\CMDPipeWrite

www.atlas-cybersecurity.com

Indicators of Compromise cont.

- Registry
  - HKLM\SYSTEM\ControlSet001\Control\Print\Environments\Windows x64\Print Processors\PrintFiiterPipelineSvc\Driver = “DEment.dll”
  - HKLM\SYSTEM\CurrentControlSet\Control\Print\Environments\Windows x64\Print Processors\lltdsvc1\Driver = “EntAppsvc.dll”
  - HKLM\SOFTWARE\Microsoft\Print\Components\DC20FD7E-4B1B-4B88-8172-61F0BED7D9E8
  - HKLM\SOFTWARE\Microsoft\Print\Components\A66F35-4164-45FF-9CB4-69ACAA10E52D

www.atlas-cybersecurity.com

Indicators of Compromise cont.

- Pipemon Encrypted Binaries
  - 168101B9B3B512583B3CE6531CFCE6E5FB581409
  - C887B35EA883F8622F7C48EC9D0427AFE833BF46
  - 44D0A2A43ECC8619DE8DB99C1465DB4E3C8FF995
  - E17972F1A3C667EEBB155A228278AA3B5F89F560
  - C03BE8BB8D03BE24A6C5CF2ED14EDFCEFA8E8429
  - 2B0481C61F367A99987B7EC0ADE4B6995425151C

- C&C Domains and IP's
  - n8.ahnlabinc[.]com
  - owa.ahnlabinc[.]com
  - ssl2.ahnlabinc[.]com
  - www2.dyn.tracker[.]com
  - ssl2.dyn-tracker[.]com
  - client.gnisoft[.]com
  - nmn.nhndesk[.]com
  - ssl.lcrest[.]com
  - 154.223.215[.]116
  - 203.86.239[.]113