New SectopRAT - Remote access malware utilizes second desktop to control browsers

By Karsten Hahn

Published: 2019-11-21 · Archived: 2026-04-05 18:50:46 UTC

General appearance and obfuscation

SectopRAT is a .NET based remote access malware. The sample[1] was originally found by MalwareHunterTeam and announced in a tweet on 15. November 2019. It was compiled on 13. November 2019. Using the following Yara rule we were able to obtain a second sample[2] that was compiled on 14. November 2019 and submitted a day later to Virustotal.

```
 rule SectopRat
{
        meta:
                author = "Karsten Hahn at G DATA CyberDefense AG"

        strings:
                $s_1 = "RemoteClient\x00"
                $s_2 = "InitHDesktop\x00"
                $s_3 = "InitBrowser\x00"
                $s_4 = "EnoghtSpace\x00"
                $s_5 = "SPI_SETSCREENSAVEACTIVE\x00"

        condition:
                all of them and
                uint16(0) == 0x5A4D
}
```

The first sample[1] is signed by Sectigo RSA Code Signing CA, uses a Flash icon and has the following Version Information.

language ID: 0x0409
code page: 0x04B0
Comments: Idito PleasweN MinIMus Inc.
CompanyName: Nikler
LegalCopyright: Nikler
ProductName: Idito PleasweN MinIMus Inc.
FileVersion: 3.21.0005
ProductVersion: 3.21.0005

InternalName: Burataslop
OriginalFilename: Burataslop.exe

The second sample[2] is not signed and uses an icon that looks like a red floppy disk. The Version Information looks different too but follows a similar pattern of upper and lower case combinations in a jumble of arbitrary words.

language ID: 0x0409
code page: 0x04B0
Comments: errORs KilEfnos INCreASe MY Wife
CompanyName: LAkoRasen Kuscev MeaninG Jow
LegalCopyright: FAW ISir Polaris ComapNY
LegalTrademarks: investORS Leanda MikiRUck
ProductName: Colleti
FileVersion: 4.01.0009
ProductVersion: 4.01.0009
InternalName: Veerfus413
OriginalFilename: Veerfus413.exe

The first section of both samples has arbitrary characters for its name and has write and execute characteristics. The 5th and last section has no name and contains the entry point. The other sections look rather typical.

The threat actor used ConfuserEx to obfuscate the control flow and add anti-tamper to the .NET assembly. The anti-tamper prevents tools like DnSpy from decompiling the code (see picture below).

Source: https://www.gdatasoftware.com/blog/2019/11/35548-new-sectoprat-remote-access-malware-utilizes-second-desktop-to-control-browsers