

Analysis of strange PS1 file October 25, 2023

SHA1 hash: 7c7275e8f3a431bf408a2676e76cfc4d6aeb4fd4

MD5 hash: 6accb2ec91e6221f4ece6ec618d9b5bc

Malware obtained from Malware Bazaar

First seen: 2023-10-25 12:50:54 UTC

I began the analysis by bringing the PS1 file into Sublime-text. The entire file contained garbled text. No PowerShell commands could be detected within it. Tried to decode this in base64. This did not produce any results I could see. I took a closer look at the file. Noticed the beginning of all the text was two equal signs. Usually in base64 it ends with none, one or two equal signs.


I made a quick Python script to flip the text around, saved the output and then decoded from base64. Checked the results and immediately noticed "MZ" at the beginning of the file and the stub "This program cannot run in DOS mode".


Running the File command showed it was a dll file. Next I ran Strings. There were references to X509Certificate, certificates, FromBase64String, DownloadString. These indicate the file will communicate via SSL to a C2 server and download additional payloads. The payloads most likely will be encoded in base64. Verified it was a dll with the string .NETFramework,Version=4.0.

The other string I noticed was ClientIva21.exe. I suspect this is the exe that will call our malicious dll.

I finished off by running the dll file through VirusTotal. 62 out of 72 saw it as malicious.

← → ↻ <https://www.virustotal.com/gui/file/b99b8c52dd67d2a9d4b8a58664056b7ce64f271e25efe3a3b8adf33c70d3db46/details> ☆

 b99b8c52dd67d2a9d4b8a58664056b7ce64f271e25efe3a3b8adf33c70d3db46 🔍 ⬆️ 📄 🗨️ ⌛ Sigr



🚨 62 security vendors and 3 sandboxes flagged this file as malicious

🔄 Reanalyze ⚙️ Similar ▾ More

b99b8c52dd67d2a9d4b8a58664056b7ce64f271e25efe3a3b8adf33c70d3db46

Client.exe

Size: 47.50 KB | Last Analysis Date: 1 hour ago

👤 EXE

peexe malware assembly detect-debug-environment long-sleeps calls-wmi

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 9

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Basic properties ⓘ

MD5	f7a2deae211b49311fa7f56c1e4566f2			
SHA-1	c68da69262d1e227b9a571365fac2530c19fbef3			
SHA-256	b99b8c52dd67d2a9d4b8a58664056b7ce64f271e25efe3a3b8adf33c70d3db46			
Vhash	24403655511f08d311e105d			
Authentihash	5c1f8f1e7d198c87be53bed24797752393b563934c3a626a0e2cc16a051c3737			
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744			
SSDEEP	768:sq+s3pUtDILNCCA+DIETTpDBWQuiVW8Yb/gevZ1Cc5VVTtjXvEgKJbZVc6KN:sq+AGtQOETTpNWOwzblS1Cc5PxnkJbZI			
TLSH	T19C235D403798C136E2FD4BB8ACF2A2458275D6576A03CA5D7CC811EA1B13FC55A136FD			
File type	Win32 EXE	executable	windows	win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows			
TrID	Generic CIL Executable (.NET, Mono, etc.) (60.4%) Windows screen saver (10.8%) Win64 Executable (generic) (8.7%) Win32 Dynamic Link Library (generic) (5.4%) Win16 NE executable (generic) (4.1%)			
DetectItEasy	PE32	Library: .NET (v4.0.30319)	Compiler: VB.NET	Compiler: VB.NET Library: .NET (v4.0.30319) Linker: Microsoft Linker (8.0)
File size	47.50 KB (48640 bytes)			

Based on some of the signatures in VirusTotal, this file appears to be a remote access trojan.