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

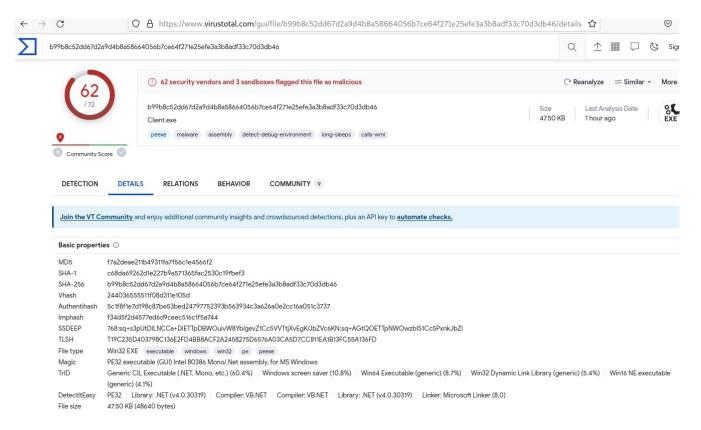
I began the analysis by bringing the PS1 file into Sublime-text. The entire file contained garbled text. No PowerShell commands could be detected within it. Tried to decode this in base64. This did not produce any results I could see. I took a closer look at the file. Noticed the beginning of all the 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.



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