Panda Banker Analysis Part 1

By Crovax

Published: 2021-08-26 · Archived: 2026-04-05 17:47:33 UTC

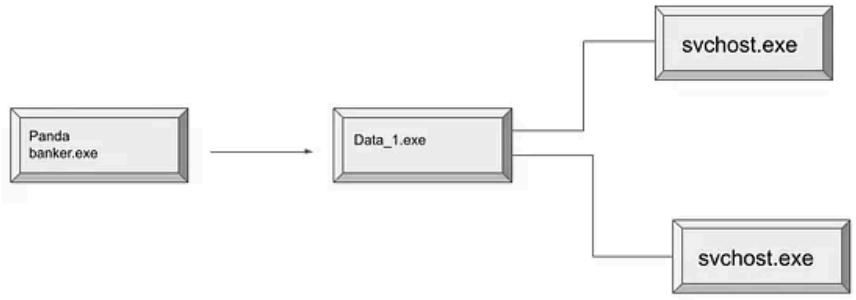
Panda banker is a banking trojan which shares some of its code base with an older malware variant called ‘Zeus.’ It’s known to inject code into the users web browser and attempt to steal banking/credit card credentials.

Panda banker has a series of different anti-analysis and code obfuscation techniques to thwart any attempt in analyzing it. Some of these techniques consist of checking for process monitoring tools and packet analysis tool. The executable, once it has detected one of these tools, it will delete itself from the host system.

Get Crovax’s stories in your inbox

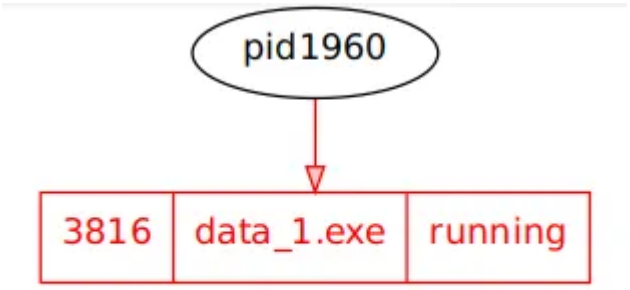
After execution Panda banker would spawn another binary in the AppData directory then execute it. Once running, the original process would then terminate and delete itself. After a while of running, it would spawn two additional processes (svchost.exe) then terminate itself as well.

Press enter or click to view image in full size



Based off the initial analysis I conducted ,you can see an unknown process (pid 1960) spawning another process named ‘data_1.exe’ (pid 3816) then terminating itself. We can see this during the process tree listing in volatility because we don't have the matching parent process in the pslist output. I attached the graph output of the analysis I

did (see below) to get a better visual representation of this activity. The rest of the memory analysis was focused on the data_1.exe activity captured during the time of execution.



To note: During part 2 of this analysis, I'll cover the behavioral and reverse engineering sections of Panda banker. This is where we'll discover additional functionalities not covered in this write up. :)

Link to memory analysis:

https://crovaxthecursed.github.io/malware%20analysis/Panda_Banker/
