Antimeter Tool

written by Mert SARICA | 24 May 2010

Generally I prefer writing my articles in Turkish and I support my articles with proof of concept codes, videos and small tools. In my previous article, I created a small tool called antimeter which scans memory for detecting and also killing Metasploit's meterpreter. I did not expect that much interest from the community therefore I did not implement core features like logging and autokill but suddenly antimeter got nice feedbacks so I have decided to implement these features and more for the community. ~~I will release the second version of antimeter in two days, stay tuned…~~

Here is the antimeter version 2.0 as I promised to the community, click here to download it.

USAGE

——-

Usage: antimeter.exe [arguments]

Optional arguments:
-t [time interval] Scans memory in every specified time interval (Default time interval is one minute)
-a Automatically kills the meterpreter process (Disabled by default)
-d Only detects the meterpreter process (Disabled by default)
-e Adds process to the exclusion list

EXAMPLES

———-

Scans memory in every 5 minutes, kills the meterpreter process automatically, verbose mode is enabled: antimeter.exe -t 5 -a -v

Scans memory in every minute and only detects the meterpreter process: antimeter.exe -n

Scans memory in every minute, explorer and winlogon processes are excluded from scanning: antimeter.exe -e explorer.exe,winlogon.exe

CHANGELOG (v2.0)

————

Added logging feature. (log file is antimeter.txt)
Added auto kill feature. (Kills the meterpreter process automatically after detection, no user interaction)
Added “detection mode only” feature. (Does not kill the meterpreter process, detection only)
Added exclusion support. (Do not scan specified processes. Seperate multiple processes with , (comma))

VIDEO
———