HermeticWiper

Article URL
malware.php?mal_id=44956646227b4ddaa8c16.40440904

Author
SsecurityHome.eu

Published: 08 March 2022

Aliases :

There are no other names known for **HermeticWiper**

.

Explanation :

HermeticWiper is a malware used in the Ukrainian of 2022, and aims to make systems "unbootable" by overriding the boot records and configurations.

The HermeticWiper infections observed thus far appear to follow a familiar path: initial foothold achieved by exploitation of external-facing servers and compromised identities leveraged to move laterally. And, as is so often the case, privileged access appears to play a critical role in these attacks.

Technical Analysis

At first glance, HermeticWiper appears to be a custom-written application with very few standard functions. The malware sample is 114KBs in size and roughly 70% of that is composed of resources. The developers are using a tried and tested technique of wiper malware, abusing a benign partition management driver, in order to carry out the more damaging components of their attacks. HermeticWiper uses a similar technique by abusing a different driver, empntdrv.sys.

The copies of the driver are ms-compressed resources. The malware deploys one of these depending on the OS version, bitness, and SysWow64 redirection.

The benign EaseUS driver is abused to do a fair share of the heavy-lifting when it comes to accessing Physical Drives directly as well as getting partition information. This adds to the difficulty of analyzing HermeticWiper, as a lot of functionality is deferred to DeviceIoControl calls with specific IOCTLs.

MBR and Partition Corruption

HermeticWiper enumerates a range of Physical Drives multiple times, from 0-100. For each Physical Drive, the .EPMNTDRV device is called for a device number.

The malware then focuses on corrupting the first 512 bytes, the Master Boot Record (MBR) for every Physical Drive. While that should be enough for the device not to boot again, HermeticWiper proceeds to enumerate the partitions for all possible drives.

They then differentiate between FAT and NTFS partitions. In the case of a FAT partition, the malware calls the same *bit fiddler*

to corrupt the partition. For NTFS, the HermeticWiper parses the Master File Table before calling this same bit fiddling function again.

Further functionality refers to interesting MFT fields ($bitmap, $logfile) and NTFS streams ($DATA, $I30, $INDEX_ALLOCATION). The malware also enumerates common folders (My Documents, Desktop, AppData), makes references to the registry (ntuser), and Windows Event Logs ("?C:WindowsSystem32winevtLogs"). Our analysis is ongoing to determine how this functionality is being used, but it is clear that having already corrupted the MBR and partitions for all drives, the victim system should be inoperable by this point of the execution.

Along the way, HermeticWiper's more mundane operations provide us with further IOCs to monitor for. These include the momentary creation of the abused driver as well as a system service. It also modifies several registry keys, including setting the *SYSTEMCurrentControlSetControlCrashControl CrashDumpEnabled key*

to 0, effectively disabling crash dumps before the abused driver's execution starts.

Finally, the malware waits on sleeping threads before initiating a system shutdown, finalizing the malware's devastating effect.

Last update 08 March 2022