HermeticWiper, Software S0697 | MITRE ATT&CK®

Archived: 2026-04-05 18:17:50 UTC

Enterprise T1134 Access Token Manipulation

HermeticWiper can use `AdjustTokenPrivileges` to grant itself privileges for debugging with `SeDebugPrivilege`, creating backups with `SeBackupPrivilege`, loading drivers with `SeLoadDriverPrivilege`, and shutting down a local system with `SeShutdownPrivilege`.[5][3]

Enterprise T1059 .003 Command and Scripting Interpreter: Windows Command Shell

HermeticWiper can use `cmd.exe /Q/c move CSIDL_SYSTEM_DRIVE\temp\sys.tmp1 CSIDL_WINDOWS\policydefinitions\postgresql.exe 1> \\127.0.0.1\ADMIN$\_1636727589.6007507 2>&1` to deploy on an infected system.[8]

Enterprise T1543 .003 Create or Modify System Process: Windows Service

HermeticWiper can load drivers by creating a new service using the `CreateServiceW` API.[3]

Enterprise T1485 Data Destruction

HermeticWiper can recursively wipe folders and files in `Windows`, `Program Files`, `Program Files(x86)`, `PerfLogs`, `Boot, System`, `Volume Information`, and `AppData` folders using `FSCTL_MOVE_FILE`. HermeticWiper can also overwrite symbolic links and big files in `My Documents` and on the Desktop with random bytes.[8]

Enterprise T1140 Deobfuscate/Decode Files or Information

HermeticWiper can decompress and copy driver files using `LZCopy`.[3]

Enterprise T1561 .001 Disk Wipe: Disk Content Wipe

HermeticWiper has the ability to corrupt disk partitions and obtain raw disk access to destroy data.[3][1]

.002 Disk Wipe: Disk Structure Wipe

HermeticWiper has the ability to corrupt disk partitions, damage the Master Boot Record (MBR), and overwrite the Master File Table (MFT) of all available physical drives.[1][2][3][5]

Enterprise T1484 .001 Domain or Tenant Policy Modification: Group Policy Modification

HermeticWiper has the ability to deploy through an infected system's default domain policy.[8]

Enterprise T1083 File and Directory Discovery

HermeticWiper can enumerate common folders such as My Documents, Desktop, and AppData.[1][5]

Enterprise T1562 .006 Impair Defenses: Indicator Blocking

HermeticWiper has the ability to set the `HKLM:\SYSTEM\\CurrentControlSet\\Control\\CrashControl\CrashDumpEnabled` Registry key to `0` in order to disable crash dumps.[1][3][5]

Enterprise T1070 Indicator Removal

HermeticWiper can disable pop-up information about folders and desktop items and delete Registry keys to hide malicious services.[3][8]

.001 Clear Windows Event Logs

HermeticWiper can overwrite the `C:\Windows\System32\winevt\Logs` file on a targeted system.[8]

.004 File Deletion

HermeticWiper has the ability to overwrite its own file with random bites.[3][8]

Enterprise T1490 Inhibit System Recovery

HermeticWiper can disable the VSS service on a compromised host using the service control manager.[3][8][5]

Enterprise T1680 Local Storage Discovery

HermeticWiper can enumerate physical drives on a targeted host.[1][3][8][5]

Enterprise T1036 .005 Masquerading: Match Legitimate Resource Name or Location

HermeticWiper has used the name `postgressql.exe` to mask a malicious payload.[8]

Enterprise T1112 Modify Registry

HermeticWiper has the ability to modify Registry keys to disable crash dumps, colors for compressed files, and pop-up information about folders and desktop items.[1][3][5]

Enterprise T1106 Native API

HermeticWiper can call multiple Windows API functions used for privilege escalation, service execution, and to overwrite random bites of data.[1][3][8][5]

Enterprise T1027 .015 Obfuscated Files or Information: Compression

HermeticWiper can compress 32-bit and 64-bit driver files with the Lempel-Ziv algorithm.[2][3][5]

Enterprise T1053 .005 Scheduled Task/Job: Scheduled Task

HermeticWiper has the ability to use scheduled tasks for execution.[2]

Enterprise T1489 Service Stop

HermeticWiper has the ability to stop the Volume Shadow Copy service.[5]

Enterprise T1553 .002 Subvert Trust Controls: Code Signing

The HermeticWiper executable has been signed with a legitimate certificate issued to Hermetica Digital Ltd.[2][3][4][5]

Enterprise T1082 System Information Discovery

HermeticWiper can determine the OS version and bitness on a targeted host.[1][3][8][5]

Enterprise T1569 .002 System Services: Service Execution

HermeticWiper can create system services to aid in executing the payload.[1][3][5]

Enterprise T1529 System Shutdown/Reboot

HermeticWiper can initiate a system shutdown.[1][5]

Enterprise T1497 .003 Virtualization/Sandbox Evasion: Time Based Checks

HermeticWiper has the ability to receive a command parameter to sleep prior to carrying out destructive actions on a targeted host.[3]
