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 regar 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 mis 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 six files for analysis: five 32-bit Dynamic-link Library (DLL) files and one 32-bit executable file. These files have been identified as IsaacWiper a HermeticWizard. During analysis of HermeticWizard, another file was dropped and identified as HermeticWiper. The submitted files are designed to spread latera through a network via Server Message Block (SMB) and Windows Management Instrumentation (WMI). These files attempt to overwrite the first 65536 bytes o data contained on the C:\ drive as well as any attached storage disks in order to render them useless to the victim user. The malware also creates a file and continuously writes to it until the disk runs out of free space and crashes. Upon reboot, the machine is no longer operable.

For a downloadable copy of IOCs, see: MAR-10376640-1.v1.stix.

Submitted Files (6)

13037b749aa4b1eda538fda26d6ac41c8f7b1d02d83f47b0d187dd645154e033 (Cleaner.dll)

2d29f9ca1d9089ba0399661bb34ba2fd8aba117f04678cd71856d5894aa7150b (exec_x32.dll)

5a300f72e221a228e3a36a043bef878b570529a7abc15559513ea07ae280bb48 (romance.dll)

a259e9b0acf375a8bef8dbc27a8a1996ee02a56889cba07ef58c49185ab033ec (Wizard.dll)

abf9adf2c2c21c1e8bd69975dfccb5ca53060d8e1e7271a5e9ef3b56a7e54d9f (Cleaner.dll)

afe1f2768e57573757039a40ac40f3c7471bb084599613b3402b1e9958e0d27a (Cleaner.exe)

Findings

5a300f72e221a228e3a36a043bef878b570529a7abc15559513ea07ae280bb48

Tags

backdoortrojanwiperworm

Details

Name	romance.dll
Size	348424 bytes
Type	PE32 executable (DLL) (console) Intel 80386, for MS Windows
MD5	0959bf541d52b6e2915420442bf44ce8
SHA1	ac5b6f16fc5115f0e2327a589246ba00b41439c2
SHA256	5a300f72e221a228e3a36a043bef878b570529a7abc15559513ea07ae280bb48
SHA512	b08ce87165b82db5a35353f9e42665fa9e736603b8e131e46501c0bbf4c830abbaba7bdbb5513af6201f19ba6741aa86b7cf736a8d92fef2c43a90383bf9ba6
ssdeep	6144:zB0WZ3twfUMDH34YslWeXEuS0dOIB9LcO1bJ/fKtn7eENm2eK7mnoUSgpAY8ODcV:lDRtSUMDH34DlWQEuS0UIzLR1NXKtn7f
Entropy	6.683668

Antivirus

Avira	WORM/Agent.pjgwz
Bitdefender	Trojan.GenericKD.48563945
Cyren	W32/Agent.XHXW-4345
ESET	Win32/Agent.OJC worm
Emsisoft	MalCert-S.OE (A)
IKARUS	Worm.Win32.Agent
K7	Trojan (0058f30e1)
Lavasoft	Trojan.GenericKD.48563945
McAfee	Exploit-DcomRpc.c.gen
Quick Heal	APEXCFC.Backdoor.Gen
Sophos	Mal/BadCert-Gen
Symantec	Trojan.KillDisk
Trend Micro	Worm.Wi.A1D01B0A
Trend Micro HouseCall	Worm.Wi.A1D01B0A
VirusBlokAda	Worm.Hermetic
Zillya!	Worm.Agent.Win32.99417

YARA Rules

- rule CISA_10376640_02 : trojan wiper worm HERMETICWIZARD { meta: Author = "CISA Code & Media Analysis" Incident = "10376640" Date =
  "2022-03-12" Last_Modified = "20220413_1300" Actor = "n/a" Category = "Trojan Wiper Worm" Family = "HERMETICWIZARD" Description = "Dete
  Hermetic Wizard samples" MD5_1 = "0959bf541d52b6e2915420442bf44ce8" SHA256_1 =
  "5a300f72e221a228e3a36a043bef878b570529a7abc15559513ea07ae280bb48" strings: $s0 = { 70 00 69 00 70 00 65 00 5C 00 25 00 73 } $s1 = { 6
  6D 00 61 00 6E 00 73 00 65 00 72 00 76 } $s2 = { 73 61 6D 72 } $s3 = { 62 72 6F 77 73 65 72 } $s4 = { 6E 65 74 6C 6F 67 6F 6E } $s5 = {
  6C 73 61 72 70 63 } $s6 = { 6E 74 73 76 63 73 } $s7 = { 73 76 63 63 74 6C } $s8 = { 73 74 61 72 74 20 63 6D 64 20 2F 63 20 22 70 69 6E
  20 6C 6F 63 61 6C 68 6F 73 74 } $s9 = { 67 00 75 00 65 00 73 00 74 } $s10 = { 74 00 65 00 73 00 74 } $s11 = { 75 00 73 00 65 00 72 } $s
  { 61 00 64 00 6D 00 69 00 6E 00 69 00 73 00 74 00 72 00 61 00 74 00 6F } $s13 = { 51 00 61 00 7A 00 31 00 32 00 33 } $s14 = { 51 00 77
  65 00 72 00 74 00 79 00 31 00 32 } $s15 = { 63 6D 64 20 2F 63 20 73 74 61 72 74 20 72 65 67 } condition: all of them }

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2022-02-22 02:30:07-05:00
Import Hash	0802be27b58612f1b2648b8a57d1acfd

PE Sections

MD5	Name	Raw Size	Entropy
6ca6e4584fdfe512c2567bc3df334540	header	1024	2.665881
023be81d5f495e7428cde5d930ecf8ce	.text	286208	6.662690
5ed93c823af444567d6fac7c5b868db8	.rdata	43008	5.287553
d2ceb15c0042bf0981352c5e7af10677	.data	3584	3.239415
84a3f07cc1f758d0993531a1da9e3f6a	.reloc	10752	6.623638

Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

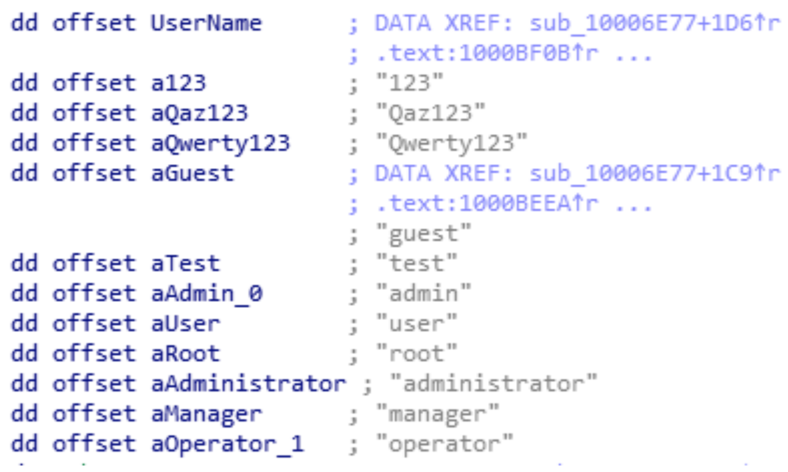
Relationships

5a300f72e2...	Contained_Within	a259e9b0acf375a8bef8dbc27a8a1996ee02a56889cba07ef58c49185ab033ec
5a300f72e2...	Dropped_By	a259e9b0acf375a8bef8dbc27a8a1996ee02a56889cba07ef58c49185ab033ec

Description

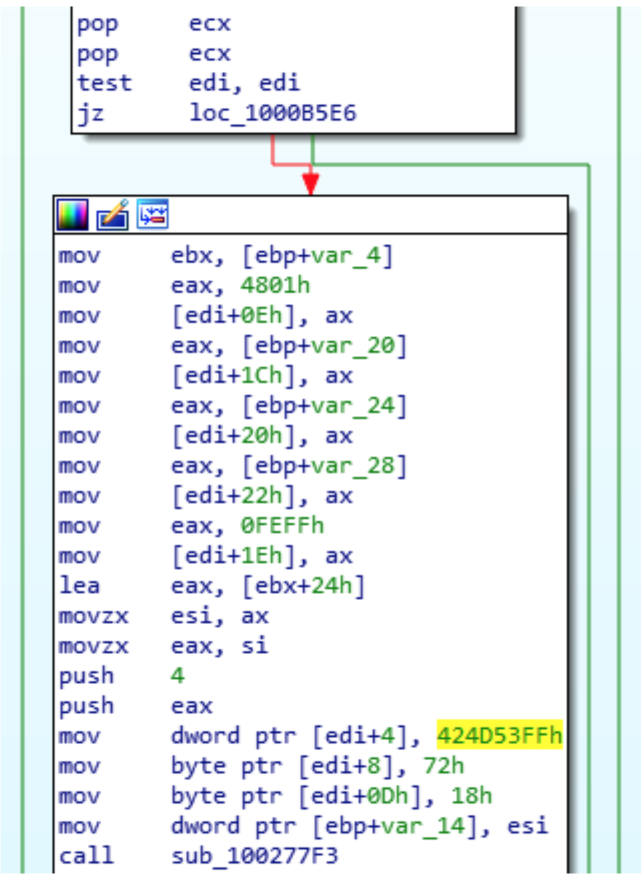
This application is a 32-bit DLL and has been identified as HermeticWizard. A filename is generated for the malware using the string 'c%02X%02X%02X%02X%02X%02X', which will create a random set of 12 characters, 6 hex bytes beginning with 'c'. The purpose of the DLL is to spread t other machines over the SMB protocol to the Admin Share (IPC$). The malware attempts to authenticate through SMB using a set of hard-coded usernames and passwords. --Begin Usernames-- guest test admin user root administrator manager operator --End Usernames-- --Begin Passwords-- 123 Qaz123 Qwerty123 --En Passwords-- The malware is designed to use the command-line parameters below for execution: --Begin command-line-- cmd /c start regsvr32.exe /s /i..\\<malici DLL> & start cmd /c "ping localhost -n 7 & wevtutil cl System --End command-line--

Screenshots



```
dd offset UserName      ; DATA XREF: sub_10006E77+1D6↑r
                        ; .text:1000BF0B↑r ...
dd offset a123          ; "123"
dd offset aQaz123       ; "Qaz123"
dd offset aQwerty123    ; "Qwerty123"
dd offset aGuest        ; DATA XREF: sub_10006E77+1C9↑r
                        ; .text:1000BEEA↑r ...
                        ; "guest"
dd offset aTest         ; "test"
dd offset aAdmin_0      ; "admin"
dd offset aUser         ; "user"
dd offset aRoot         ; "root"
dd offset aAdministrator ; "administrator"
dd offset aManager      ; "manager"
dd offset aOperator_1   ; "operator"
```

Figure 1 - This screenshot shows the hard-coded usernames and passwords used to attempt authentication with the target machine.



```
pop     ecx
pop     ecx
test    edi, edi
jz      loc_1000B5E6
```

```
mov     ebx, [ebp+var_4]
mov     eax, 4801h
mov     [edi+0Eh], ax
mov     eax, [ebp+var_20]
mov     [edi+1Ch], ax
mov     eax, [ebp+var_24]
mov     [edi+20h], ax
mov     eax, [ebp+var_28]
mov     [edi+22h], ax
mov     eax, 0FEFFh
mov     [edi+1Eh], ax
lea     eax, [ebx+24h]
movzx   esi, ax
movzx   eax, si
push    4
push    eax
mov     dword ptr [edi+4], 424D53FFh
mov     byte ptr [edi+8], 72h
mov     byte ptr [edi+0Dh], 18h
mov     dword ptr [ebp+var_14], esi
call    sub_100277F3
```

Figure 2 - This screenshot shows the malware establishing a connection via the SMB protocol.

2d29f9ca1d9089ba0399661bb34ba2fd8aba117f04678cd71856d5894aa7150b

Tags

backdoortrojanwiperworm

Details

Name	exec_x32.dll
Size	122632 bytes
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	58d71fff346017cf8311120c69c9946a
SHA1	6b5958bfabfe7c731193adb96880b225c8505b73
SHA256	2d29f9ca1d9089ba0399661bb34ba2fd8aba117f04678cd71856d5894aa7150b
SHA512	315cc419f6ec600a345447b0f49e3de9f13c1e96d9bbc272f982204b1c7ec71cb3805f5ff7821da3e7944e327c22e5eba6f3c94b08c66b6e241395e1ea133ec
ssdeep	3072:gnu7OIMtlhyAnF1bIoENm2eK7mnoUSgpAY8ODcDcm7cIsF4RO06loHGvJnuqO:g4OlhlzjENm2eK7mnoUSgpAY8ODcDcmT
Entropy	6.646213

Antivirus

AhnLab	Trojan/Win.FoxBlade
Avira	WORM/Agent.juikt
Bitdefender	Trojan.GenericKD.39179683
ESET	Win32/Agent.OJC worm
Emsisoft	MalCert-S.OE (A)
IKARUS	Worm.Win32.Agent
K7	Trojan (00028d131)
Lavasoft	Trojan.GenericKD.39179683
Quick Heal	APEXCFC.Backdoor.Gen
Sophos	Mal/BadCert-Gen
Symantec	Trojan.Gen.2
Trend Micro	Worm.Wi.A1D01B0A
Trend Micro HouseCall	Worm.Wi.A1D01B0A
VirusBlokAda	Trojan.Agent
Zillya!	Worm.Agent.Win32.99414

YARA Rules

- rule CISA_10376640_03 : trojan wiper worm HERMETICWIZARD { meta: Author = "CISA Code & Media Analysis" Incident = "10376640" Date =
  "2022-03-13" Last_Modified = "20220413_1300" Actor = "n/a" Category = "Trojan Wiper Worm" Family = "HERMETICWIZARD" Description = "Dete
  Hermetic Wizard samples" MD5_1 = "58d71fff346017cf8311120c69c9946a" SHA256_1 =
  "2d29f9ca1d9089ba0399661bb34ba2fd8aba117f04678cd71856d5894aa7150b" strings: $s0 = { 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F }
  = { 5C 00 5C 00 25 00 73 00 5C 00 70 00 69 00 70 00 65 00 5C 00 25 00 73 } $s2 = { 64 00 6C 00 6C 00 00 00 2D 00 69 } $s3 = { 2D 00 6
  00 00 00 00 00 2D 00 73 } $s4 = { 2D 00 63 00 00 00 00 00 2D 00 61 } $s5 = { 43 6F 6D 6D 61 6E 64 4C 69 6E 65 54 6F 41 72 67 76 57 }
  condition: all of them }

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2022-02-22 02:23:15-05:00
Import Hash	0efd6cfc0613f20a06fa0746b2d5b8bc

PE Sections

MD5	Name	Raw Size	Entropy
90d5fe0b84e27aef0c20e1f645feb2b0	header	1024	2.713966
6e7013478def0b223ed6acb0a52fad70	.text	81408	6.654914
b63a5c496bdfc65b0a87074ddb5ea3ea	.rdata	29184	5.513656
cd29db9b4e978a706ddf3195b7a6b9b9	.data	2560	2.223270
463a2a119664cff0f6ea5941379a7700	.reloc	4608	6.499252

Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

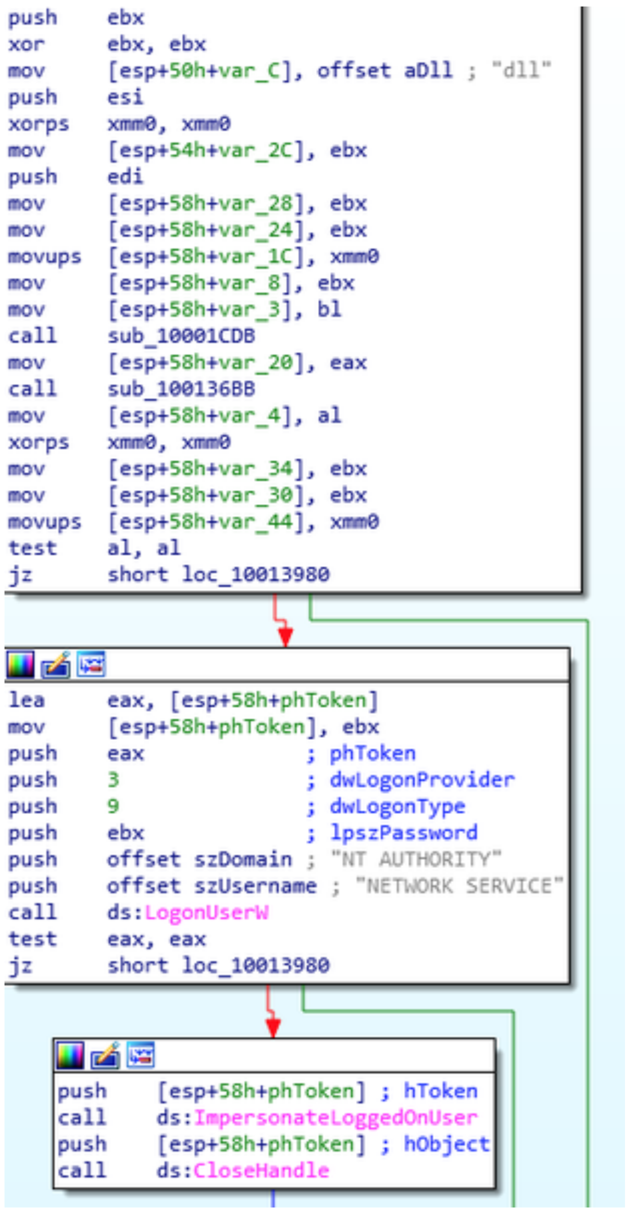
Relationships

2d29f9ca1d...	Contained_Within	a259e9b0acf375a8bef8dbc27a8a1996ee02a56889cba07ef58c49185ab033ec
2d29f9ca1d...	Dropped_By	a259e9b0acf375a8bef8dbc27a8a1996ee02a56889cba07ef58c49185ab033ec

Description

This is a 32-bit DLL file. This DLL spreads laterally through the network via the WMI protocol. The malware copies a file over to the target machine for execu This copied filename is generated using the string 'c%02X%02X%02X%02X%02X%02X' which will create a random set of 12 characters, 6 hex bytes beginnin with 'c'. The copied file has been identified as HermeticWizard. The malware identifies a running process with a desired authority and uses the token for impersonation to create a new process and service to launch the copied file. --Begin command-line-- cmd /c start regsvr32.exe /s /i <malicious DLL path> --End command-line--

Screenshots



```
push    ebx
xor     ebx, ebx
mov     [esp+50h+var_C], offset aDll ; "dll"
push    esi
xorps   xmm0, xmm0
mov     [esp+54h+var_2C], ebx
push    edi
mov     [esp+58h+var_28], ebx
mov     [esp+58h+var_24], ebx
movups  [esp+58h+var_1C], xmm0
mov     [esp+58h+var_8], ebx
mov     [esp+58h+var_3], bl
call    sub_10001CDB
mov     [esp+58h+var_20], eax
call    sub_100136BB
mov     [esp+58h+var_4], al
xorps   xmm0, xmm0
mov     [esp+58h+var_34], ebx
mov     [esp+58h+var_30], ebx
movups  [esp+58h+var_44], xmm0
test    al, al
jz      short loc_10013980
```

```
lea     eax, [esp+58h+phToken]
mov     [esp+58h+phToken], ebx
push    eax             ; phToken
push    3               ; dwLogonProvider
push    9               ; dwLogonType
push    ebx             ; lpszPassword
push    offset szDomain ; "NT AUTHORITY"
push    offset szUsername ; "NETWORK SERVICE"
call    ds:LogonUserW
test    eax, eax
jz      short loc_10013980
```

```
push    [esp+58h+phToken] ; hToken
call    ds:ImpersonateLoggedOnUser
push    [esp+58h+phToken] ; hObject
call    ds:CloseHandle
```

Figure 3 - This screenshot shows the malware authority type and impersonation.

a259e9b0acf375a8bef8dbc27a8a1996ee02a56889cba07ef58c49185ab033ec

Tags

backdoortrojanworm

Details

Name	Wizard.dll
Size	698632 bytes
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	517d2b385b846d6ea13b75b8adceb061
SHA1	3c54c9a49a8ddca02189fe15fea52fe24f41a86f
SHA256	a259e9b0acf375a8bef8dbc27a8a1996ee02a56889cba07ef58c49185ab033ec
SHA512	1de912f50b7f5cc2f4fcea7b6d3c84a39bd15d668122f50a9b11da66447ed99f456e86e006d0dfe7ab0fca7dc8e35efa7ff57959033463d94ef37e570551543
ssdeep	12288:J4WCTqjtByJsZrjIYlkytnSg9hcr1DnDH2iRNL5tj1XUNgASK4CTfVf1WZ62PNTr:HGqRBRtnSEhMhDH2iRNL5tj1XUNgASKw
Entropy	7.451862

Antivirus

AhnLab	Trojan/Win.FoxBlade
Antiy	Trojan/Win32.Agent
Avira	WORM/Agent.sejyu
Bitdefender	Trojan.GenericKD.48550079
ClamAV	Win.Malware.HermeticWizard-9941571-0
ESET	Win32/Agent.OJC worm
Emsisoft	MalCert-S.OE (A)
IKARUS	Worm.Win32.Agent
K7	Trojan (0058f30e1)
Lavasoft	Trojan.GenericKD.48550079
McAfee	Generic trojan.wh
NANOAV	Trojan.Win32.TrjGen.jngwij
Quick Heal	APEXCFC.Backdoor.Gen
Sophos	Mal/BadCert-Gen
Symantec	Trojan.Gen.MBT
TACHYON	Trojan/W32.HermeticWizard.698632
Trend Micro	Worm.Wi.38D94AB0
Trend Micro HouseCall	Worm.Wi.38D94AB0
VirusBlokAda	BScope.Trojan.Agent
Zillya!	Worm.Agent.Win32.99423

YARA Rules

- rule CISA_10376640_05 : trojan wiper worm HERMETICWIZARD { meta: Author = "CISA Code & Media Analysis" Incident = "10376640" Date = "2022-04-14" Last_Modified = "20220414_1037" Actor = "n/a" Category = "Trojan Wiper Worm" Family = "HERMETICWIZARD" Description = "Dete Hermetic Wizard samples" MD5_1 = "517d2b385b846d6ea13b75b8adceb061" SHA256 = "a259e9b0acf375a8bef8dbc27a8a1996ee02a56889cba07ef58c49185ab033ec" strings: $s0 = { 57 69 7A 61 72 64 2E 64 6C 6C } $s1 = { 69 6E 66 6C 74 65 } $s2 = { 4D 61 72 6B 20 41 64 6C 65 72 } condition: all of them and filesize < 2000KB }

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2022-02-22 03:07:17-05:00
Import Hash	e099d3524b6906cf8460b4e6db0b11f2

PE Sections

MD5	Name	Raw Size	Entropy
01185a4f21be653f13b885a655da2239	header	1024	2.945954
d7ed7d880b3eed5eae7787055766502c	.text	312832	6.633510
87728459f7938f00f8d53d0bd6e6a337	.rdata	60416	5.802039
31b2ae0f6a40196c4bce89d36302d545	.data	3584	2.914857
d77cbf49cf473a8235a67912f0edd78f	.rsrc	304128	7.948029
32ec2dc9dc4b9fc8f96ac18835fea101	.reloc	12800	6.692458

Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

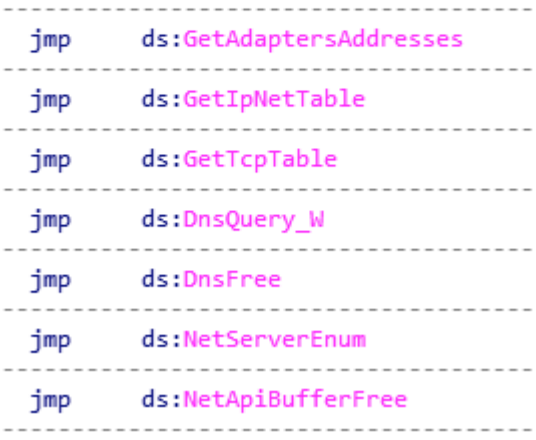
Relationships

a259e9b0ac...	Contains	5a300f72e221a228e3a36a043bef878b570529a7abc15559513ea07ae280bb48
a259e9b0ac...	Contains	2d29f9ca1d9089ba0399661bb34ba2fd8aba117f04678cd71856d5894aa7150b
a259e9b0ac...	Dropped	5a300f72e221a228e3a36a043bef878b570529a7abc15559513ea07ae280bb48
a259e9b0ac...	Dropped	2d29f9ca1d9089ba0399661bb34ba2fd8aba117f04678cd71856d5894aa7150b

Description

This is a 32-bit DLL and has been identified as HermeticWizard. The original filename for the DLL is Wizard.dll. It is designed to use the command-line param
below for execution: --Begin command-line-- regsvr32.exe /s /i <malicious DLL path> --End command-line-- The application contains three 32-bit encrypted bin
that are decrypted and installed into the current directory at runtime. --Begin files-- %current directory%\exec_x32.dll %current directory%\romance.dll %current
directory%\<6 randomly generated alphanumerical characters>.ocx --End files-- At runtime, it attempts to detect all active hosts on the victim's network. It is cap
of moving laterally across the network by actively scanning ranges of reachable IP version 4 addresses and ports. It is designed to create and connect to multipl
name pipes. Displayed below are the list of port numbers it attempts to connect to. --Begin port numbers-- 20 21 22 80 135 137 139 443 445 --End port numbers-- Once an active host (system) is found, it attempts to execute the command-line below to move to the reachable machine: --Begin command-- "C:\Windows\System32\rundll32.exe %current directory%\<6 randomly generated alphanumerical characters>.ocx #1 -s <path to Wizard.dll> — i <reachable system address>" --End command-- It executes the file <6 randomly generated alphanumerical characters>.ocx binary to wipe the drive. This OLE Control Extension (O
file has been identified as HermeticWiper. The SHA256 of the OCX file is 0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da. Note: Analysis of this file is included in MAR-10375867.r1.v1.WHITE.

Screenshots



```
jmp     ds:GetAdaptersAddresses
jmp     ds:GetIpNetTable
jmp     ds:GetTcpTable
jmp     ds:DnsQuery_W
jmp     ds:DnsFree
jmp     ds:NetServerEnum
jmp     ds:NetApiBufferFree
```

Figure 4 - This screenshot shows the functionalities used to perform local network enumeration.

abf9adf2c2c21c1e8bd69975dfccb5ca53060d8e1e7271a5e9ef3b56a7e54d9f

Tags

trojan

Details

Name	Cleaner.dll
Size	11264 bytes
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	aa98b92e3320af7a1639de1bac6c17cc
SHA1	ad602039c6f0237d4a997d5640e92ce5e2b3bba3
SHA256	abf9adf2c2c21c1e8bd69975dfccb5ca53060d8e1e7271a5e9ef3b56a7e54d9f
SHA512	5549bdb658736c187c2d6493c82f46461dda728a0ec365833bf1987e9436a5f9e1a42cab68082af2640b5a10ab92aa9251095d3b453934d3ebeb211bfd42
ssdeep	192:bqSlxiV3BdNHxRvb8WZVPspRgssSt7NCphJHlHMjz5e:dnYx5RvYW3mQphJHVMjc
Entropy	5.648075

Antivirus

ESET	a variant of Win32/KillMBR.NHP trojan
Trend Micro	Trojan.9FABA348
Trend Micro HouseCall	Trojan.9FABA348

YARA Rules

- rule CISA_10376640_01 : trojan wiper ISAACWIPER { meta: Author = "CISA Code & Media Analysis" Incident = "10376640" Date = "2022-03-14" Last_Modified = "20220418_1900" Actor = "n/a" Category = "Trojan Wiper" Family = "ISAACWIPER" Description = "Detects ISACC Wiper samples" MD5_1 = "aa98b92e3320af7a1639de1bac6c17cc" SHA256_1 = "abf9adf2c2c21c1e8bd69975dfccb5ca53060d8e1e7271a5e9ef3b56a7e54d9f" MD5_2 = "8061889aaebd955ba6fb493abe7a4de1" SHA256_2 = "afe1f2768e57573757039a40ac40f3c7471bb084599613b3402b1e9958e0d27a" MD5_3 = "ecce8845921a91854ab34bff2623151e" SHA256_3 = "13037b749aa4b1eda538fda26d6ac41c8f7b1d02d83f47b0d187dd645154e033" strings: $s0 = { 73 74 00 61 00 72 00 74 00 20 00 65 00 72 00 61 00 73 00 69 00 6E 00 67 } $s1 = { 6C 00 6F 00 67 00 69 00 63 00 61 00 6C } $s2 = { 46 00 00 49 00 4C 00 45 00 44 } $s3 = { 5C 00 6C 00 6F 00 67 00 2E 00 74 00 78 00 74 } $s4 = { 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E } $s5 = {53 74 61 72 74 40 34} $s6 = {3B 57 34 74 2D 6A} $s7 = {43 6C 65 61 6E 65 72 2E} condition: all of ($s0,$s1,$s2,$s3,$s4) or all of ($s5,$s6,$s7) }

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2021-10-19 10:17:30-04:00
Import Hash	8156382b4b0f02a7467108b32103b82a

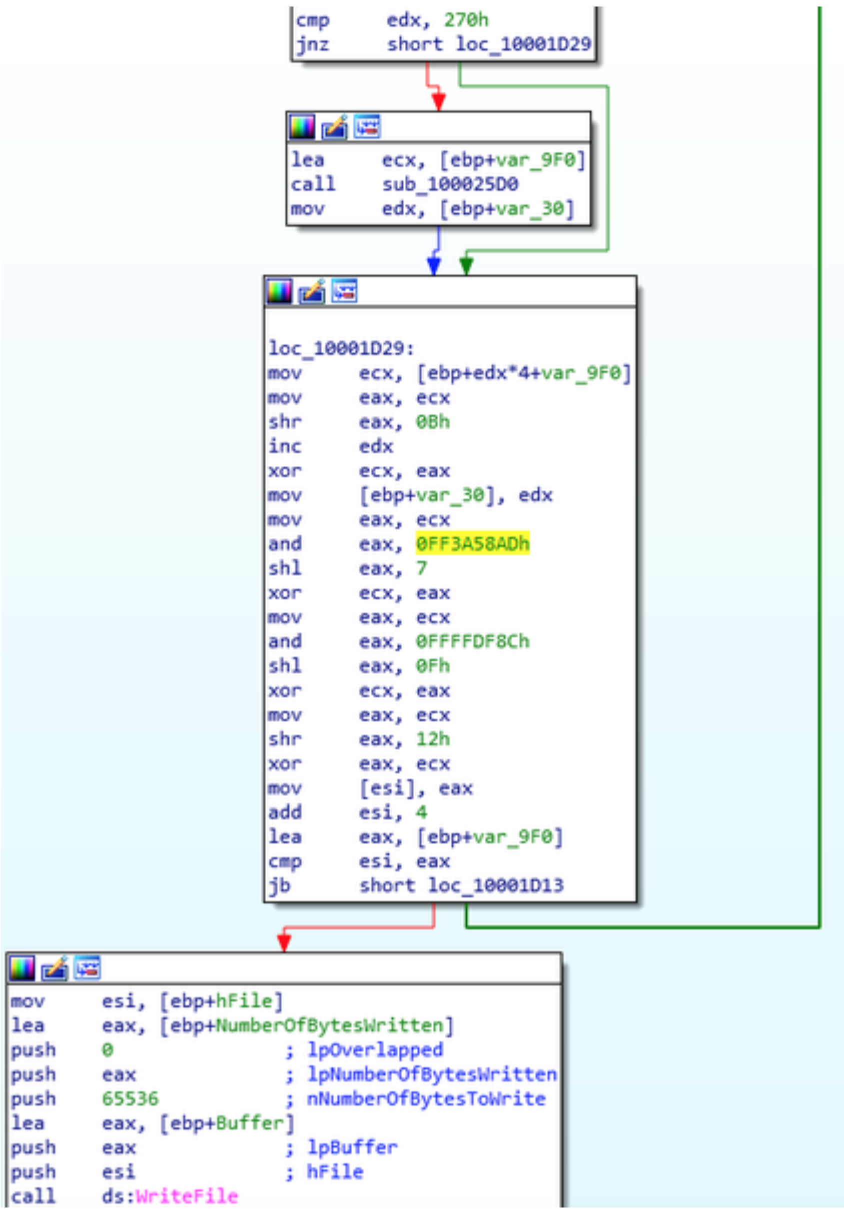
PE Sections

MD5	Name	Raw Size	Entropy
1e9e616d75f50f562b0d56edc472a8ea	header	1024	2.226630
decfc792ded248587084a6329217380e	.text	7680	6.321812
99ec3d78dee2e180fa53da106a9a7540	.rdata	1536	3.859100
9475a59226943a3ad422e18169989f66	.data	512	0.020393
60a3ce8706953c03b2a4f22e43dccb26	.reloc	512	2.886370

Description

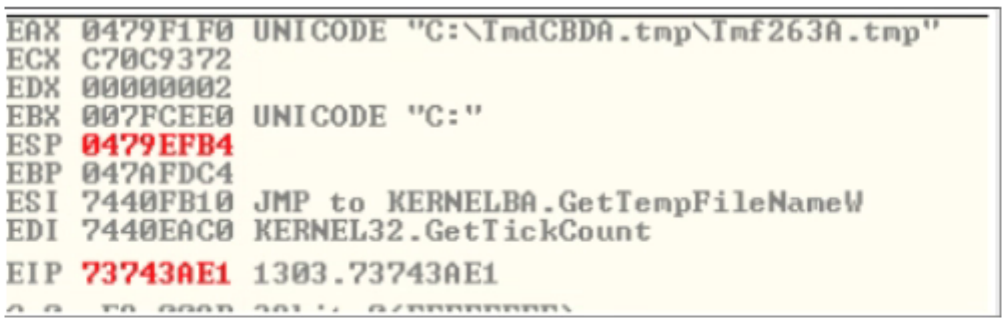
Cleaner.dll is a 32-bit DLL which has been identified as a variant of the IsaacWiper. It attempts to overwrite the first 65536 bytes of data on the C:\ drive and attached storage disks in order to render them useless to the victim user. The malware also overwrites the victim user's files so they cannot be recovered. The da used to overwrite the disk drives and user files is random data that is generated via the Mersenne Twister algorithm. Cleaner.dll also attempts to create a directo the root directory of attached storage disks. The malware will then create a file within this newly created directory and attempt to fill it with random data, gener via the Mersenne Twister algorithm, in an effort to fill the drive up as another destructive method of rendering the storage device unusable to the victim user. Th name of the folder created will begin with the letters "Tmd" and the remaining part of the folder name will be randomly generated alphanumerical characters. Th filename created will begin with the letters "Tmf" and the remaining part of the filename will be randomly generated alphanumerical characters. Displayed below the format of the file installed: --Begin file-- Filename: "C:\Tmd[4 randomly generated characters]\Tmf[4 randomly generated alphanumerical characters].tmp" Sample: "C:\Tmd21D9.tmp\Tmf1E9E.tmp" --End file-- Analysis indicates that the application fails to execute if the above tmp file already exists on the victim's machine.

Screenshots



```
cmp     edx, 270h
jnz     short loc_10001D29

lea     ecx, [ebp+var_9F0]
call    sub_100025D0
mov     edx, [ebp+var_30]

loc_10001D29:
mov     ecx, [ebp+edx*4+var_9F0]
mov     eax, ecx
shr     eax, 0Bh
inc     edx
xor     ecx, eax
mov     [ebp+var_30], edx
mov     eax, ecx
and     eax, 0FF3A58ADh
shl     eax, 7
xor     ecx, eax
mov     eax, ecx
and     eax, 0FFFFDF8Ch
shl     eax, 0Fh
xor     ecx, eax
mov     eax, ecx
shr     eax, 12h
xor     eax, ecx
mov     [esi], eax
add     esi, 4
lea     eax, [ebp+var_9F0]
cmp     esi, eax
jb      short loc_10001D13

mov     esi, [ebp+hFile]
lea     eax, [ebp+NumberOfBytesWritten]
push    0               ; lpOverlapped
push    eax             ; lpNumberOfBytesWritten
push    65536           ; nNumberOfBytesToWrite
lea     eax, [ebp+Buffer]
push    eax             ; lpBuffer
push    esi             ; hFile
call    ds:WriteFile
```

Figure 5 - This screenshot illustrates the malware overwriting the first 65536 bytes of the C:\ drive, or attached storage disk, using random encrypted data gener via the Mersenne Twister algorithm.



```
EAX 0479F1F0 UNICODE "C:\TmdCBDA.tmp\Tmf263A.tmp"
ECX C70C9372
EDX 00000002
EBX 007FCEE0 UNICODE "C:"
ESP 0479EFB4
EBP 047AFDC4
ESI 7440FB10 JMP to KERNELBA.GetTempFileNameW
EDI 7440EAC0 KERNEL32.GetTickCount
EIP 73743AE1 1303.73743AE1
```

Figure 6 - This screenshot illustrates a sample file created by the malware. This malware will write random encrypted data to this file until the C:\ drive and attached storage devices runs out of space. This is just one method the malware utilizes in an attempt to corrupt the victim user's machine.

afe1f2768e57573757039a40ac40f3c7471bb084599613b3402b1e9958e0d27a

Tags

trojan

Details

Name	Cleaner.exe
Size	11264 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	8061889aaebd955ba6fb493abe7a4de1
SHA1	e9b96e9b86fad28d950ca428879168e0894d854f
SHA256	afe1f2768e57573757039a40ac40f3c7471bb084599613b3402b1e9958e0d27a
SHA512	27874dca36c2ebe3ac240c3c6592093ef8cd09611ede1e16de22357bea35dfb70065c2545b6381a19198139b9591e2f4fe0f882483f418a9bd2e0c2f126a0b
ssdeep	192:9ClgiV30I+0Kxn+rgRvb865VPkMsuW089mNCEFlggO4C6z5C:gmYLY5RvY6XW0ZQslggPC6
Entropy	5.628275

Antivirus

Avira	TR/Crypt.XPACK.Gen8
ESET	a variant of Win32/KillMBR.NHP trojan
Trend Micro	Trojan.9FABA348
Trend Micro HouseCall	Trojan.9FABA348

YARA Rules

- rule CISA_10376640_01 : trojan wiper ISAACWIPER { meta: Author = "CISA Code & Media Analysis" Incident = "10376640" Date = "2022-03-14" Last_Modified = "20220418_1900" Actor = "n/a" Category = "Trojan Wiper" Family = "ISAACWIPER" Description = "Detects ISACC Wiper samples" MD5_1 = "aa98b92e3320af7a1639de1bac6c17cc" SHA256_1 = "abf9adf2c2c21c1e8bd69975dfccb5ca53060d8e1e7271a5e9ef3b56a7e54d9f" MD5_2 = "8061889aaebd955ba6fb493abe7a4de1" SHA256_2 = "afe1f2768e57573757039a40ac40f3c7471bb084599613b3402b1e9958e0d27a" MD5_3 = "ecce8845921a91854ab34bff2623151e" SHA256_3 = "13037b749aa4b1eda538fda26d6ac41c8f7b1d02d83f47b0d187dd645154e033" strings: $s0 = { 73 74 00 61 00 72 00 74 00 20 00 65 00 72 00 61 00 73 00 69 00 6E 00 67 } $s1 = { 6C 00 6F 00 67 00 69 00 63 00 61 00 6C } $s2 = { 46 00 00 49 00 4C 00 45 00 44 } $s3 = { 5C 00 6C 00 6F 00 67 00 2E 00 74 00 78 00 74 } $s4 = { 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E } $s5 = {53 74 61 72 74 40 34} $s6 = {3B 57 34 74 2D 6A} $s7 = {43 6C 65 61 6E 65 72 2E} condition: all of ($s0,$s1,$s2,$s3,$s4) or all of ($s5,$s6,$s7) }

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2022-02-24 04:48:46-05:00
Import Hash	fd8214e8ca810e64eb947f522acbead7

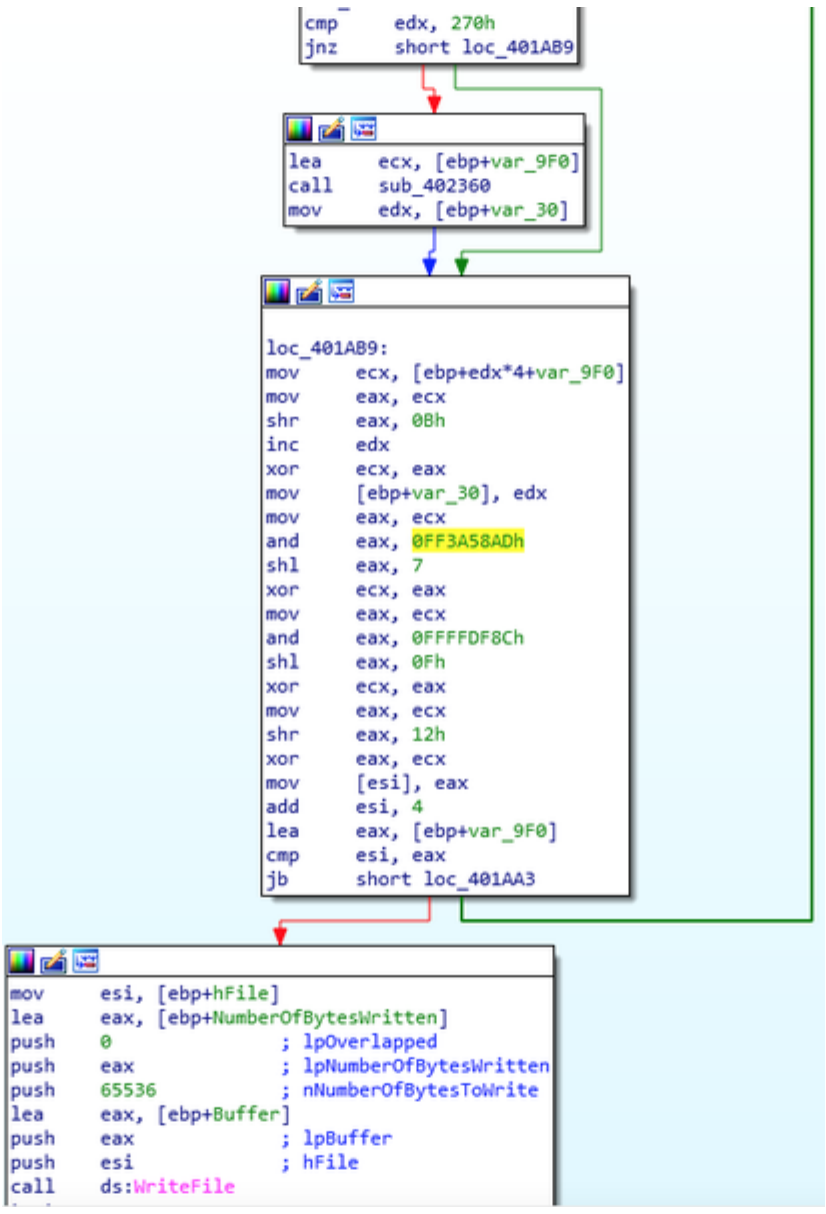
PE Sections

MD5	Name	Raw Size	Entropy
c1ecc108a6c84989eb4102d2d387c3cb	header	1024	2.235812
12bbe2ed84c503c161528eb9c65e06b7	.text	7680	6.297084
a84958d0a1ba6ccf7f68b0f082a1c656	.rdata	1536	3.901725
9475a59226943a3ad422e18169989f66	.data	512	0.020393
4c8100d03804167a977995936cfbf536	.reloc	512	2.937988

Description

Cleaner.exe is a 32-bit executable file (EXE) which has been identified as another variant of the IsaacWiper. It can be executed immediately or has a sleep func for 15 minutes. When executed, it attempts to overwrite the first 65536 bytes of data contained on the C:\ drive and on attached storage disks in order to rende them useless to the victim user. The malware also overwrites the victim user's files so they cannot be recovered. The data used to overwrite the disk drives and files is random data that is generated via the Mersenne Twister algorithm. Cleaner.exe also attempts to create a directory in the root directory of attached storage disks. The malware will then create a file within this newly created directory and attempt to fill it with random data, generated via the Mersenne Twister algorit in an effort to fill the drive up as another destructive method of rendering the storage device unusable to the victim user. The name of the folder created will be with the letters "Tmd" and the remaining part of the folder name will be randomly generated alphanumerical characters. The filename created will begin with the letters "Tmf" and the remaining part of the filename will be randomly generated alphanumerical characters. Displayed below is the format of the file installed: -- Begin file-- Filename: "C:\Tmd[4 randomly generated characters]\Tmf[4 randomly generated alphanumerical characters].tmp" Sample: "C: \Tmd21D9.tmp\Tmf1E9E.tmp" --End file-- Analysis indicates that the application fails to execute if the above tmp file already exists on the victim's machine.

Screenshots



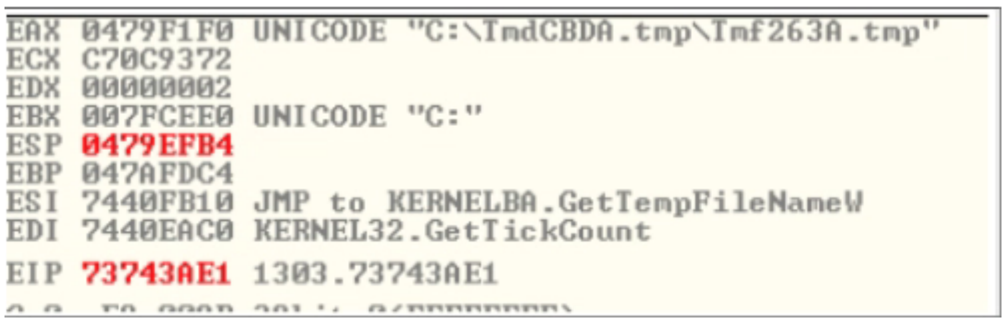
```
cmp     edx, 270h
jnz     short loc_401AB9
```

```
lea     ecx, [ebp+var_9F0]
call    sub_402360
mov     edx, [ebp+var_30]
```

```
loc_401AB9:
mov     ecx, [ebp+edx*4+var_9F0]
mov     eax, ecx
shr     eax, 0Bh
inc     edx
xor     ecx, eax
mov     [ebp+var_30], edx
mov     eax, ecx
and     eax, 0FF3A58ADh
shl     eax, 7
xor     ecx, eax
mov     eax, ecx
and     eax, 0FFFFDF8Ch
shl     eax, 0Fh
xor     ecx, eax
mov     eax, ecx
shr     eax, 12h
xor     eax, ecx
mov     [esi], eax
add     esi, 4
lea     eax, [ebp+var_9F0]
cmp     esi, eax
jb      short loc_401AA3
```

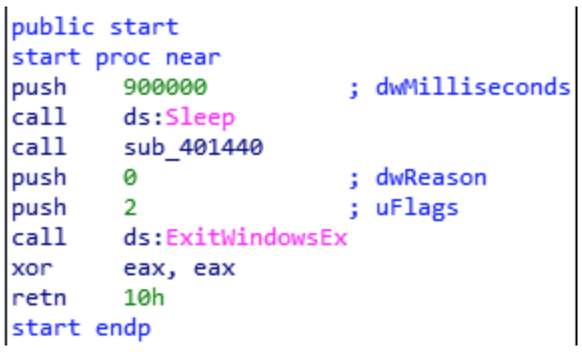
```
mov     esi, [ebp+hFile]
lea     eax, [ebp+NumberOfBytesWritten]
push    0                ; lpOverlapped
push    eax              ; lpNumberOfBytesWritten
push    65536            ; nNumberOfBytesToWrite
lea     eax, [ebp+Buffer]
push    eax              ; lpBuffer
push    esi              ; hFile
call    ds:WriteFile
```

Figure 7 - This screenshot illustrates the malware overwriting the first 65536 bytes of the C:\ drive, or attached storage disk, using random encrypted data gener via the Mersenne Twister algorithm.



```
EAX 0479F1F0 UNICODE "C:\TmdCBDA.tmp\Tmf263A.tmp"
ECX C70C9372
EDX 00000002
EBX 007FCEE0 UNICODE "C:"
ESP 0479EFB4
EBP 047AFDC4
ESI 7440FB10 JMP to KERNELBA.GetTempFileNameW
EDI 7440EAC0 KERNEL32.GetTickCount
EIP 73743AE1 1303.73743AE1
```

Figure 8 - This screenshot illustrates a sample file created by the malware. This malware will write random encrypted data to this file until the C:\ drive and attached storage devices runs out of space. This is just one method the malware utilizes in an attempt to corrupt the victim user's machine.



```
public start
start proc near
push    900000          ; dwMilliseconds
call    ds:Sleep
call    sub_401440
push    0               ; dwReason
push    2               ; uFlags
call    ds:ExitWindowsEx
xor     eax, eax
retn    10h
start endp
```

Figure 9 - This screenshot show the executable's sleep function.

13037b749aa4b1eda538fda26d6ac41c8f7b1d02d83f47b0d187dd645154e033

Tags

backdoortrojanviruswiper

Details

Name	Cleaner.dll
Size	224768 bytes
Type	PE32 executable (DLL) (console) Intel 80386, for MS Windows
MD5	ecce8845921a91854ab34bff2623151e
SHA1	736a4cfad1ed83a6a0b75b0474d5e01a3a36f950
SHA256	13037b749aa4b1eda538fda26d6ac41c8f7b1d02d83f47b0d187dd645154e033
SHA512	36fda34df70629d054a55823a3cc83f9599446b36576fbc86a6aac6564460789e8b141eeb168d3e4578f28182da874dd840e57b642af1a1a315dfe08a17b5
ssdeep	6144:pjU6yx1p7lvER8SPD/xzL0ruSSbAOfyV:Ju1pZvPuDF0ruSSbkV
Entropy	6.612476

Antivirus

AhnLab	Trojan/Win.IsaacWiper
Avira	TR/KillMBR.hlwrn
Bitdefender	Trojan.GenericKD.39120112
ClamAV	Win.Malware.IsaacWiper-9940626-0
Cyren	W32/Killmbr.GBHG-3949
ESET	Win32/KillMBR.NHQ trojan
Emsisoft	Trojan.GenericKD.39120112 (B)
IKARUS	Virus.Wiper.Isaac
K7	Trojan (0058efff1)
Lavasoft	Trojan.GenericKD.39120112
McAfee	RDN/Generic.dx
Quick Heal	APEXCFC.Backdoor.Gen
Sophos	Troj/Wiper-F

Symantec	Trojan.Gen.MBT
Trend Micro	Trojan.6050981D
Trend Micro HouseCall	Trojan.6050981D
VirusBlokAda	Trojan.Agentb
Zillya!	Trojan.KillMBR.Win32.666

YARA Rules

- rule CISA_10376640_01 : trojan wiper ISAACWIPER { meta: Author = "CISA Code & Media Analysis" Incident = "10376640" Date = "2022-03-14" Last_Modified = "20220418_1900" Actor = "n/a" Category = "Trojan Wiper" Family = "ISAACWIPER" Description = "Detects ISACC Wiper samples" MD5_1 = "aa98b92e3320af7a1639de1bac6c17cc" SHA256_1 = "abf9adf2c2c21c1e8bd69975dfccb5ca53060d8e1e7271a5e9ef3b56a7e54d9f" MD5_2 = "8061889aaebd955ba6fb493abe7a4de1" SHA256_2 = "afe1f2768e57573757039a40ac40f3c7471bb084599613b3402b1e9958e0d27a" MD5_3 = "ecce8845921a91854ab34bff2623151e" SHA256_3 = "13037b749aa4b1eda538fda26d6ac41c8f7b1d02d83f47b0d187dd645154e033" strings: $s0 = { 73 74 00 61 00 72 00 74 00 20 00 65 00 72 00 61 00 73 00 69 00 6E 00 67 } $s1 = { 6C 00 6F 00 67 00 69 00 63 00 61 00 6C } $s2 = { 46 00 00 49 00 4C 00 45 00 44 } $s3 = { 5C 00 6C 00 6F 00 67 00 2E 00 74 00 78 00 74 } $s4 = { 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E } $s5 = {53 74 61 72 74 40 34} $s6 = {3B 57 34 74 2D 6A} $s7 = {43 6C 65 61 6E 65 72 2E} condition: all of ($s0,$s1,$s2,$s3,$s4) or all of ($s5,$s6,$s7) }

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2022-02-25 10:48:07-05:00
Import Hash	a4b162717c197e11b76a4d9bc58ea25d

PE Sections

MD5	Name	Raw Size	Entropy
28378e0c1da3cce94aa72585f5559fc6	header	1024	2.656680
06d63fddf89fae3948764028712c36d6	.text	150528	6.676976
48f101db632bb445c21a10fd5501e343	.rdata	60416	5.634639
5efc98798d0979e69e2a667fc20e3f24	.data	4096	3.256171
9676f7c827fb9388358aaba3e4bd0cc6	.reloc	8704	6.433076

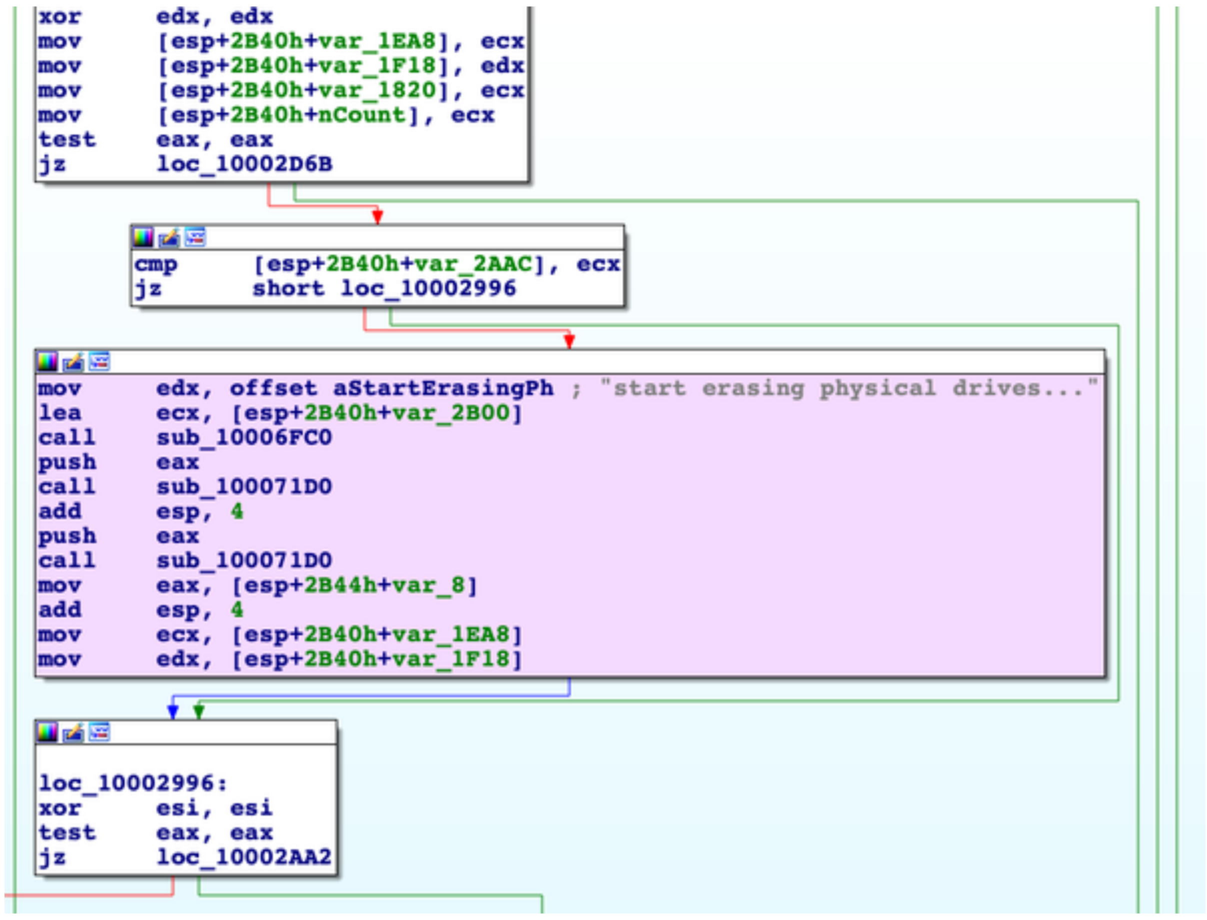
Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

Description

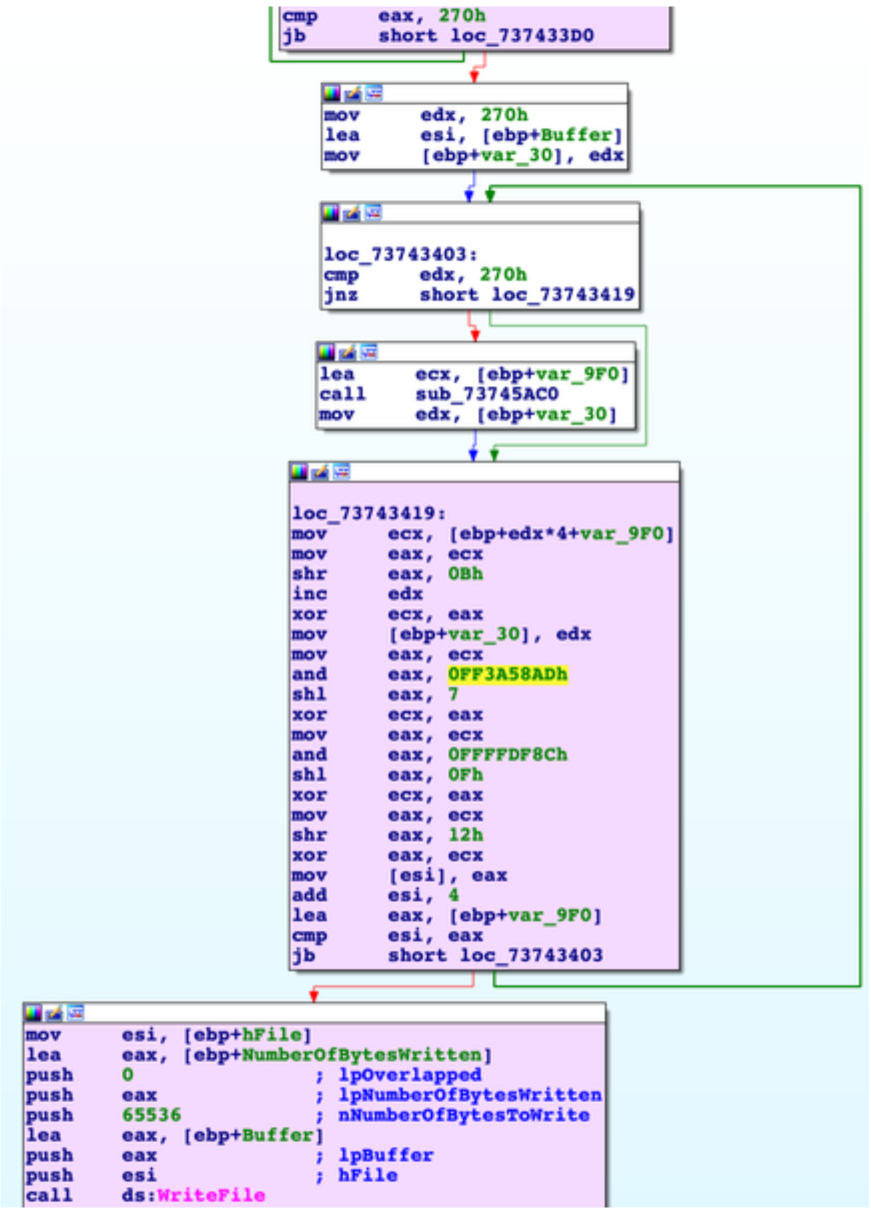
This application is a 32-bit DLL which has been identified as another variant of the IsaacWiper. It attempts to overwrite the first 65536 bytes of data on the C:\ drive and on attached storage disks in order to render them useless to the victim user. The malware also overwrites the victim user's files so they cannot be recovered. The data used to overwrite the disk drives and user files is random encrypted data that is generated via the Mersenne Twister algorithm. The malware also attempts to create a directory in the root directory of attached storage disks. The malware will then create a file within this newly created directory and atte to fill it with random encrypted data, generated via the Mersenne Twister algorithm, in an effort to fill the drive up as another destructive method of rendering th storage device unusable to the victim user. The name of the folder created will begin with the letters "Tmd" and the remaining part of the folder name will be random. The filename created will begin with the letters "Tmf" and the remaining part of the folder name will be random. This malware creates a log file in the location C:\ProgramData\log.txt. This file logs the malware's process of systematically corrupting the victim user storage disks. Illustrated below is sample data th malware recorded to its log file during runtime: --Begin log.txt Data-- getting drives... physical drives: -- system physical drive 0: PhysicalDrive0 logical drives: system logical drive: C: -- logical drive: D: start erasing system physical drive... system physical drive -- FAILED start erasing system logical drive C: --End log Data--

Screenshots



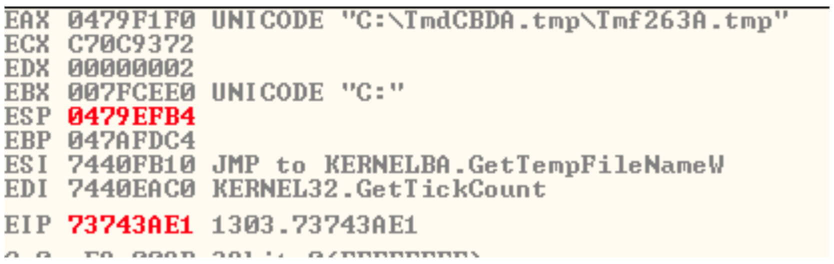
```
xor     edx, edx
mov     [esp+2B40h+var_1EA8], ecx
mov     [esp+2B40h+var_1F18], edx
mov     [esp+2B40h+var_1820], ecx
mov     [esp+2B40h+nCount], ecx
test    eax, eax
jz      loc_10002D6B

cmp     [esp+2B40h+var_2AAC], ecx
jz      short loc_10002996

mov     edx, offset aStartErasingPh ; "start erasing physical drives..."
lea     ecx, [esp+2B40h+var_2B00]
call    sub_10006FC0
push    eax
call    sub_100071D0
add     esp, 4
push    eax
call    sub_100071D0
mov     eax, [esp+2B44h+var_8]
add     esp, 4
mov     ecx, [esp+2B40h+var_1EA8]
mov     edx, [esp+2B40h+var_1F18]

loc_10002996:
xor     esi, esi
test    eax, eax
jz      loc_10002AA2
```

Figure 10 - This screenshot illustrates the malware logging the beginning of its attempt to corrupt the victim user's storage device. This log data will be recorde within the log file named log.txt.



```
cmp     eax, 270h
jb      short loc_737433D0

mov     edx, 270h
lea     esi, [ebp+Buffer]
mov     [ebp+var_30], edx

loc_73743403:
cmp     edx, 270h
jnz     short loc_73743419

lea     ecx, [ebp+var_9F0]
call    sub_73745AC0
mov     edx, [ebp+var_30]

loc_73743419:
mov     ecx, [ebp+edx*4+var_9F0]
mov     eax, ecx
shr     eax, 0Bh
inc     edx
xor     ecx, eax
mov     [ebp+var_30], edx
mov     eax, ecx
and     eax, 0FF3A58ADh
shl     eax, 7
xor     ecx, eax
mov     eax, ecx
and     eax, 0FFFFDF8Ch
shl     eax, 0Fh
xor     ecx, eax
mov     eax, ecx
shr     eax, 12h
xor     eax, ecx
mov     [esi], eax
add     esi, 4
lea     eax, [ebp+var_9F0]
cmp     esi, eax
jb      short loc_73743403

mov     esi, [ebp+hFile]
lea     eax, [ebp+NumberOfBytesWritten]
push    0               ; lpOverlapped
push    eax             ; lpNumberOfBytesWritten
push    65536           ; nNumberOfBytesToWrite
lea     eax, [ebp+Buffer]
push    eax             ; lpBuffer
push    esi             ; hFile
call    ds:WriteFile
```

Figure 11 - This screenshot illustrates the malware overwriting the first 65536 bytes of an attached storage disk using random encrypted data generated via the Mersenne Twister algorithm.



```
EAX 0479F1F0 UNICODE "C:\TmdCBDA.tmp\Tmf263A.tmp"
ECX C70C9372
EDX 00000002
EBX 007FCEE0 UNICODE "C:"
ESP 0479EFB4
EBP 047AFDC4
ESI 7440FB10 JMP to KERNELBA.GetTempFileNameW
EDI 7440EAC0 KERNEL32.GetTickCount

EIP 73743AE1 1303.73743AE1
```

Figure 12 - This screenshot illustrates a sample file created by the malware. This malware will write random encrypted data to this file until the C:\ drive and attached storage devices runs out of space. This is just one method the malware utilizes in an attempt to corrupt the victim user's machine.

Relationship Summary

5a300f72e2...	Contained_Within	a259e9b0acf375a8bef8dbc27a8a1996ee02a56889cba07ef58c49185ab033ec
5a300f72e2...	Dropped_By	a259e9b0acf375a8bef8dbc27a8a1996ee02a56889cba07ef58c49185ab033ec
2d29f9ca1d...	Contained_Within	a259e9b0acf375a8bef8dbc27a8a1996ee02a56889cba07ef58c49185ab033ec
2d29f9ca1d...	Dropped_By	a259e9b0acf375a8bef8dbc27a8a1996ee02a56889cba07ef58c49185ab033ec
a259e9b0ac...	Contains	5a300f72e221a228e3a36a043bef878b570529a7abc15559513ea07ae280bb48
a259e9b0ac...	Contains	2d29f9ca1d9089ba0399661bb34ba2fd8aba117f04678cd71856d5894aa7150b
a259e9b0ac...	Dropped	5a300f72e221a228e3a36a043bef878b570529a7abc15559513ea07ae280bb48
a259e9b0ac...	Dropped	2d29f9ca1d9089ba0399661bb34ba2fd8aba117f04678cd71856d5894aa7150b

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 th 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 scams. Reporting forms can be found on CISA's homepage at www.cisa.gov.

Revisions

April 28, 2022: Initial Version

This product is provided subject to this Notification and this Privacy & Use policy.

Please share your thoughts.

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