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 regarding 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 misuse, 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 one unique file for analysis. This file is a malicious 32-bit Windows Portable Executable (PE). During runtime, this malware attempts to overwrit the victim user's files with null bytes. The malware also attempts to overwrite the Master Boot Record of attached drives with null bytes, thereby corrupting ther and rendering it impossible for the victim to access the victim's stored data.

For a downloadable copy of IOCs, see: MAR-10376640-2.v1.stix.

Submitted Files (1)

a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea (a294620543334a721a2ae8eaaf9680...)

Findings

a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea

Tags

trojanviruswiper

Details

Name	a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea
Size	9216 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	42e52b8daf63e6e26c3aa91e7e971492
SHA1	98b3fb74b3e8b3f9b05a82473551c5a77b576d54
SHA256	a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea
SHA512	b21039ad67e07a77bbcfe73a89afd22c7e1fd782a5293c41edd0ae1dbd75c4fdf6404d8cfe5cf2191ad1822e32877ded1675e48895e8b9898778855d3dd566
ssdeep	192:76f0CW5P2Io4evFrDv2ZRJzCn7URRsjVJaZF:76fPWl24evFrT2ZR5Cn7UR0VJo
Entropy	5.108650

Antivirus

AhnLab	Trojan/Win.Agent
Avira	TR/Crypt.XPACK.Gen
Bitdefender	Gen:Variant.CaddyWiper.2
ClamAV	Win.Malware.CaddyWiper-9941573-1
Cyren	W32/Trojan.WXHP-9071
ESET	Win32/KillDisk.NCX trojan
Emsisoft	Gen:Variant.CaddyWiper.2 (B)
IKARUS	Trojan.Win32.KillDisk

K7	Trojan (0058f88b1)
Lavasoft	Gen:Trojan.Heur.FU.amW@aiAsbgg
McAfee	Trojan-caddywiper.b
NANOAV	Virus.Win32.Gen.ccmw
Quick Heal	SM.mal.generic
Sophos	Troj/KillDisk-G
Symantec	Trojan.Gen.MBT
TACHYON	Trojan/W32.Agent.9216.ABY
Trend Micro	Trojan.F383D2EE
Trend Micro HouseCall	Trojan.F383D2EE
Vir.IT eXplorer	Trojan.Win32.CaddyWiper.DGP
VirusBlokAda	Trojan.DoS.CaddyBlade
Zillya!	Trojan.KillDisk.Win32.311

YARA Rules

- rule CISA_10376640_04 : trojan wiper CADDYWIPER { meta: Author = "CISA Code & Media Analysis" Incident = "10376640" Date = "2022-03-23" Last_Modified = "20220324_1700" Actor = "n/a" Category = "Trojan Wiper" Family = "CADDYWIPER" Description = "Detects Caddy wiper samples" MD5_1 = "42e52b8daf63e6e26c3aa91e7e971492" SHA256_1 = "a294620543334a721a2ae8eaaf9680a0786f4b9a216d75b55cfd28f39e9430ea" strings: $ = { 44 73 52 6F 6C 65 47 65 74 50 72 69 6D 61 72 79 44 6F 6D 61 69 6E } $s1 = { 50 C6 45 A1 00 C6 45 A2 48 C6 45 A3 00 C6 45 A4 59 C6 } $s2 = { C6 45 A6 53 C6 45 A7 00 C6 45 A8 49 C6 } $s3 = { C6 45 B0 44 C6 45 B1 00 C6 45 B2 52 } $s4 = { C6 45 B8 45 C6 45 B9 00 C6 45 BA 39 } $s5 = { C6 45 AC 43 C6 45 AD 3A C6 45 AE 5C C6 45 AF } $s6 = { 55 C6 45 B0 73 C6 45 B1 65 C6 45 B2 72 C6 45 B3 } $ = { C6 45 E0 44 C6 45 E1 3A C6 45 E2 5C C6 45 E3 } $s8 = { 21 54 68 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F } condition: all of them }

ssdeep Matches

No matches found.

PE Metadata

Compile Date 2022-03-14 03:19:36-04:00

Import Hash ea8609d4dad999f73ec4b6f8e7b28e55

PE Sections

MD5	Name	Raw Size	Entropy
6194652d04e28dad063a1b6e60d110ab	header	1024	1.873192
f0d4c11521fc3891965534e6c52e128b	.text	7168	5.644240
d4b14cf770a6e660ba6a6e63f7c22451	.rdata	512	0.988058
0f1286f7c8817e0974ddc3ce1edc1b59	.reloc	512	0.081539

Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

Description

This file is a 32 bit Windows PE that has been identified as a variant of the malware family known as Caddy Wiper. Static analysis of this application indicates primary purpose is to destroy victim user data. First the malware attempts to enumerate all files in the directory "C:\Users". The malware will then attempt to recursively overwrite files that it can access in this directory with null bytes, effectively "zeroing" the files out. The malware will then attempt to access drives attached to the target system, starting with the drive "D:\", and recursively "zero" out all the files it can access on those drives too. Finally, the malware attempt

to use the API DeviceIoControl to directly access the physical memory of attached drives. If it is able to access these drives, the malware will zero out the first 1920 bytes of the physical drives, effectively wiping its Master Boot Record and corrupting the drive.

Screenshots

Figure 1. - This screenshot illustrates the main structure of the malware. As illustrated, the malware's main purpose is to recursively overwrite victim user's files and physical drives with null bytes.

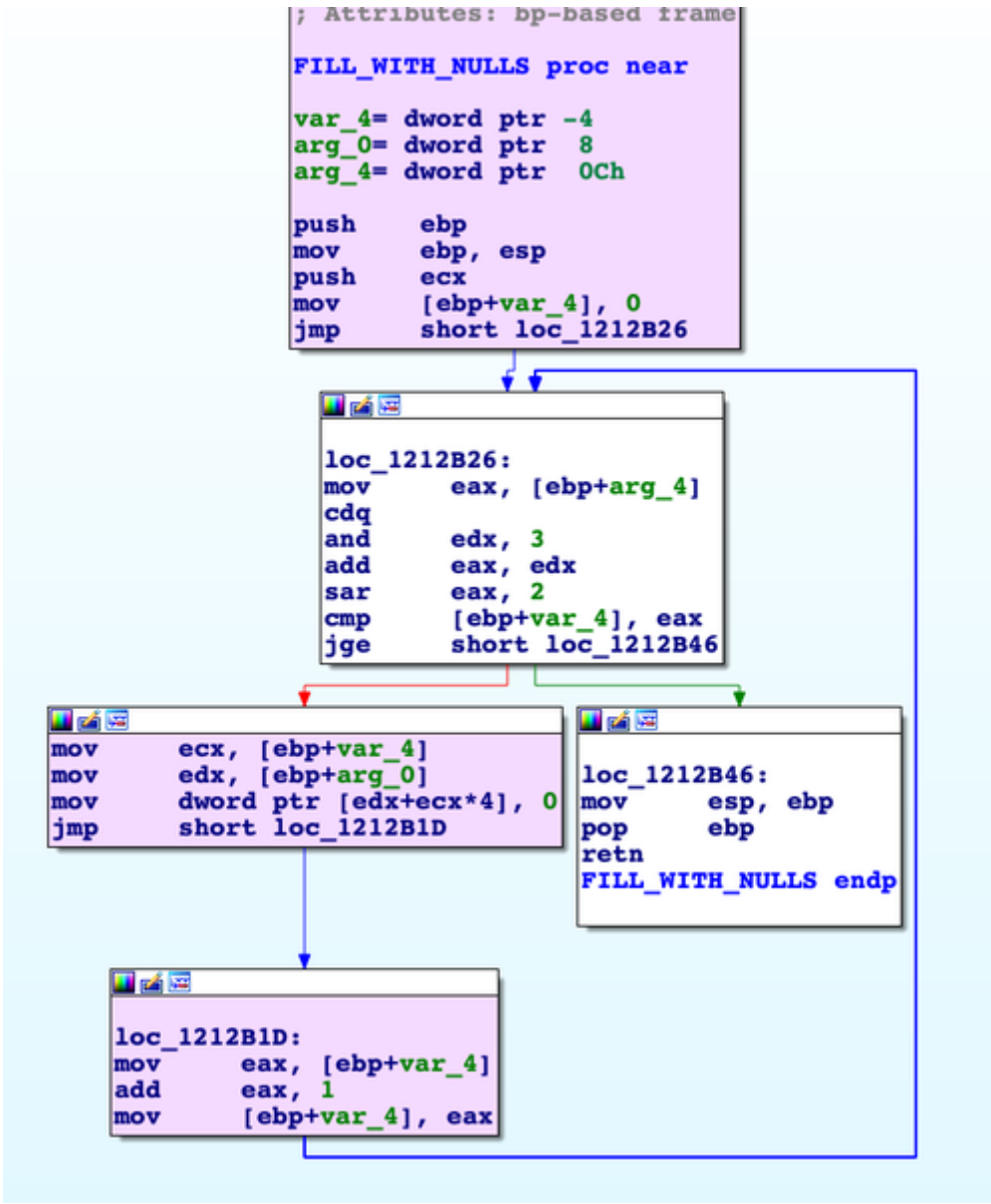

Figure 2. - Structure that malware uses to build null buffer. This buffer is utilized to overwrite the victim user's target files.

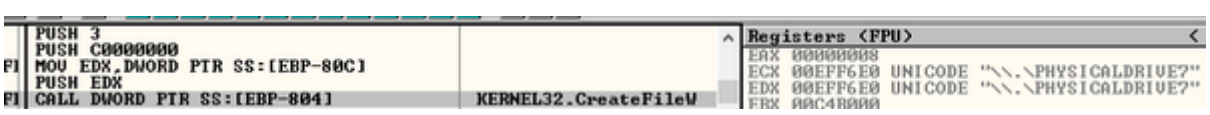

Figure 3. - Malware trying to zero out \\.\PHYSICALDRIVE7

Figure 4. - Malware trying to zero out \\.\PHYSICALDRIVE4

Figure 5. - Malware trying to zero out \\.\PHYSICALDRIVE3

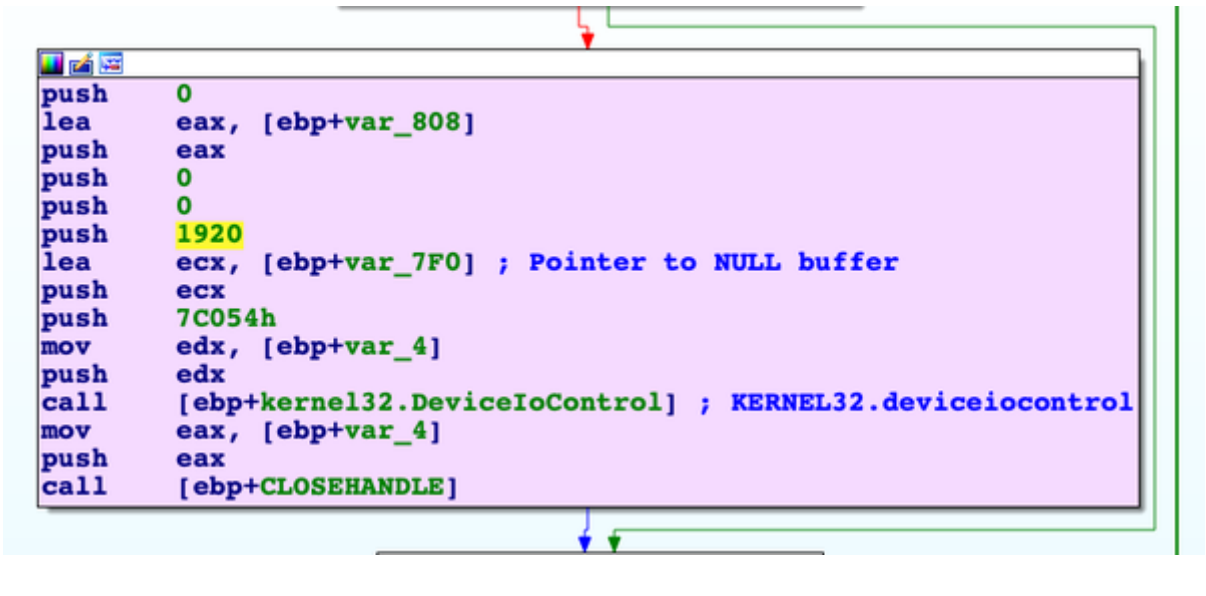

Figure 6. - Malware attempting to zero out first 1920 bytes of a physical drive attached to the target system.

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 URL: 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 the 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

Please share your thoughts.

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