ANALYSIS REPORT

10365227.r2.v1 NUMBER

Malware Analysis Report

2022-09-21 DATE

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:CLEAR–Disclosure is not limited. Sources may use TLP:CLEAR 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:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol (TLP), see http://www.cisa.gov/tlp.

Summary

Description

This Malware Analysis Report (MAR) is the result of analytic efforts by the Cybersecurity and Infrastructure Security Agency (CISA) to provide detailed analysis of files associated with HyperBro, a Remote Access Trojan (RAT). CISA obtained HyperBro malware samples during an on-site incident response engagement at a Defense Industrial Base (DIB) Sector organization compromised by advanced persistent threat (APT) actors.

CISA analyzed 4 files associated with HyperBro malware. The files creates a backdoor program that is capable of uploading and downloading files to and from the system. The RAT is also capable of logging keystrokes and executing commands on the system.

For more information on the confirmed compromise, see Joint CSA: Impacket and Exfiltration Tool Used to Steal Sensitive Information from Defense Industrial Base Organization.

Submitted Files (4)

52072a8f99dacd5c293fccd051eab95516d8b880cd2bc5a7e0f4a30d008e22a7 (vftrace.dll)

df847abbfac55fb23715cde02ab52cbe59f14076f9e4bd15edbe28dcecb2a348 (msmpeng.exe)

f1a2791eebaea183f399110c9e8ae11c67f5bebf93a5573d1ac3c56fc71b2230 (config.ini)

f2ba8b8aabf73020febd3a925276d52ce88f295537fe57723df714c13f5a8780 (thumb.dat)

IPs (1)

104.168.236.46

Findings

df847abbfac55fb23715cde02ab52cbe59f14076f9e4bd15edbe28dcecb2a348

Tags

loader

Details

Name	msmpeng.exe
Size	351240 bytes
Type	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	4109ac08bdc8591c7b46348eb1bca85d

SHA1	6423d1c324522bfd2b65108b554847ac4ab02479
SHA256	df847abbfac55fb23715cde02ab52cbe59f14076f9e4bd15edbe28dcecb2a348
SHA512	0605362190a9cb04a7392c7eae3ef79964a76ea68dc03dfabe6ec8f445f1c355772f2ca8166cbee73188e57bff06b74fb2cfa59869cb4461fffe1c3589856554
ssdeep	6144:BTMoU0+zvvLIpa8bo5GOc1G41vupWn2rwRGekPHZLZKA1UnmOlm:XUDvvsc80AOc1GYvAW2EGtH5ZKAKmOQ
Entropy	6.471736

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2016-01-05 08:22:40-05:00
Import Hash	b66afb12e84aa5ce621a6635837cadba
Company Name	CyberArk Software Ltd.
File Description	CyberArk Viewfinity
Internal Name	vf_host.exe
Legal Copyright	Copyright © 1999-2016 CyberArk Software Ltd. All Rights Reserved.
Original Filename	vf_host.exe
Product Name	CyberArk Viewfinity
Product Version	5.5.10.101

PE Sections

MD5	Name	Raw Size	Entropy
3822119e846581669481aba79308c57c	header	1024	2.580725
98ccfff2af4ccaa3335f63592a1fba02	.text	270848	6.543317
9dcc89a0d16e36145bb07924ca260dfe	.rdata	50688	5.132125
14d493033fc147f67601753310725b2b	.data	5632	3.711689
615729d1383743a91b8baf309f1a8232	.rsrc	16896	4.839559

Packers/Compilers/Cryptors

Microsoft Visual C++ ?.?

Relationships

df847abbfa...	Used	52072a8f99dacd5c293fccd051eab95516d8b880cd2bc5a7e0f4a30d008e22a7

Description

This artifact is a version of vf_host.exe from Viewfinity. The file is used to side-load the malicious dynamic-link library (DLL), vftrace.dll.

The program is also capable of bypassing User Account Controls (UAC) on the system by disabling Admin Approval Mode in User Account Controls Group Policy in HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System. This can allow the malware to run with Admin privileges, or allow remote logon (RDP) with full Admin privileges.

52072a8f99dacd5c293fccd051eab95516d8b880cd2bc5a7e0f4a30d008e22a7

Tags

trojan

Details

Name	vftrace.dll
Size	73728 bytes
Type	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	7655ff65f74f08ee2c54f44e5ef8f098
SHA1	3c7beb8978feac9ba8f5bab0656242232471bf7d
SHA256	52072a8f99dacd5c293fccd051eab95516d8b880cd2bc5a7e0f4a30d008e22a7
SHA512	efea9b8a7b6b7cfa31814af4ffe45fab68d159a6239271b632166b2f6b44af8a4e1cc559fa56537ec4142e0484031a9b79034d4e5a8cbbf1d5250b86370cdfcf
ssdeep	1536:d0X1BkgxVXJyBaUihWutqQQ4znsWgcdqydbPX:07XMBOs41znqypP
Entropy	6.334911

Antivirus

Adaware	Gen:Variant.Bulz.429221
AhnLab	Trojan/Win.HYPERBRO
Avira	TR/Injector.nmrbf
Bitdefender	Gen:Variant.Bulz.429221
Comodo	Malware
Cyren	W32/Agent.GCPS-3922
ESET	a variant of Win32/LuckyMouse.BR trojan
IKARUS	Trojan.Win32.LuckyMouse
K7	Riskware (0040eff71)
NANOAV	Trojan.Win32.LuckyMouse.iwacwz
Sophos	Troj/Agent-BGVD
Trend Micro	Trojan.780F7AE8
Trend Micro HouseCall	Trojan.780F7AE8
VirusBlokAda	TScope.Malware-Cryptor.SB
Zillya!	Trojan.LuckyMouse.Win32.24

YARA Rules

No matches found.

ssdeep Matches

No matches found.

PE Metadata

Compile Date	2021-03-02 02:18:56-05:00
Import Hash	182f35372e9fd050b6e0610238bcd9fd

PE Sections

MD5	Name	Raw Size	Entropy
a89421fb59d33658892123b94906aa72	header	1024	2.836214
624b09cd367db7ebfc510aab51f95791	.text	42496	6.692212
8885c137e1772d11b48e71da92aa3d3c	.rdata	23552	4.949495
2304803a4ce5a785e19eb0b45efb7065	.data	2048	2.051382
2139727f6ccf1b15d0f96e805001b2fc	.gfids	512	1.386027
a4fc8d9199bcb8669008e62d5dc7d675	.rsrc	512	4.712298
73a0737f1475d88793ad42fc04bef1ab	.reloc	3584	6.466489

Packers/Compilers/Cryptors

Borland Delphi 3.0 (???)

Relationships

52072a8f99...	Connected_To	104.168.236.46
52072a8f99...	Used_By	df847abbfac55fb23715cde02ab52cbe59f1407 6f9e4bd15edbe28dcecb2a348
52072a8f99...	Created	f1a2791eebaea183f399110c9e8ae11c67f5be bf93a5573d1ac3c56fc71b2230
52072a8f99...	Created	f2ba8b8aabf73020febd3a925276d52ce88f29 5537fe57723df714c13f5a8780

Description

This DLL is side-loaded by df847abbfac55fb23715cde02ab52cbe59f14076f9e4bd15edbe28dcecb2a348 detailed in this report.

When the DLL is executed it will create a Globally Unique Identifier (GUID) to identify the system to the command and control (C2) during communication. The GUID is written to a file called 'Config.ini' and placed in the current directory.

The program will decrypt and read a configuration file called 'thumb.dat' that instructs it to spawn a new instance of the Service Host Process (svchost.exe) and inject itself into the new instance. Svchost.exe is run with the -k netsvcs parameter to allow the malware to connect to its C2. The malware collects the following information to send to the C2 via POST when establishing a connection.

—Begin Collected Information—
Computer Name
IP Address
Path to the malware location
Process name that it is running in (svchost.exe)
Mode
Name of the malware
GUID
—End Collected Information—

During analysis, the malware attempted to connect to the Uniform Resource Identifier (URI), hxxps[:]//104.168.236.46/api/v2/ajax using the fixed User-Agent string Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.116 Safari/537.36.

To achieve persistence on the system, the program creates a service in the registry called 'Windows Defenders Service' that starts automatically when the user logs on.

—Begin Registry Settings—
HKLM\System\CurrentControlSet\services\windefenders\Type. Data: 272
HKLM\System\CurrentControlSet\services\windefenders\Start. Data: 2
HKLM\System\CurrentControlSet\services\windefenders\ErrorControl. Data: 1
HKLM\System\CurrentControlSet\services\windefenders\ImagePath Data: "C:\Program Files (x86)\Common Files\windefenders \msmpenge.exe"
HKLM\System\CurrentControlSet\services\windefenders\DisplayName Data: Windows Defenders
HKLM\System\CurrentControlSet\services\windefenders\WOW64. Data: 1
HKLM\System\CurrentControlSet\services\windefenders\ObjectName. Data: LocalSystem
HKLM\System\CurrentControlSet\services\windefende37337060\DeleteFlag. Data: 1
HKLM\System\CurrentControlSet\services\windefende37337060\Start. Data: 4
HKLM\System\CurrentControlSet\services\windefenders\Description Data: Windows Defenders Service
—End Registry Settings—

It may also create an autorun entry in the registry at HKLM\Software\Microsoft\Windows\Current Version\Run.

The malware creates a hidden folder called 'windefenders' in the path C:\Program Files (x86)\Common Files\ where it will copy the PE file 'msmpeng.exe' along with the GUID file, 'config.ini', the malicious library 'vftrace.dll', and the encrypted configuration file 'thumb.dat'. A second hidden folder called 'windefenders' is also created in the path C:\ProgramData\. This folder holds another instance of the PE file.

The program is capable of logging keystrokes, uploading and downloading files, and will also invoke RpcServerListen to wait for incoming Remote Procedure Call (RPC) connections. It will also open a pipe called '\Device\NamedPipe\testpipe' that it uses to pass commands from its daemon to any worker processes it may set up.

104.168.236.46

Tags

command-and-control

URLs

- hxxps[:]//104.168.236.46/api/v2/ajax

Ports

- 443 TCP

Whois

Domain Name: HOSTWINDSDNS.COM
Registry Domain ID: 1655837964_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2021-06-25T06:27:14Z
Creation Date: 2011-05-12T23:01:53Z
Registry Expiry Date: 2029-05-12T23:01:53Z
Registrar: NameCheap, Inc.
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.6613102107
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: DNS1.HOSTWINDSDNS.COM
Name Server: DNS2.HOSTWINDSDNS.COM
Name Server: DNS3.HOSTWINDSDNS.COM
Name Server: DNS4.HOSTWINDSDNS.COM
DNSSEC: unsigned

Domain name: hostwindsdns.com
Registry Domain ID: 1655837964_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2020-04-27T12:40:10.00Z
Creation Date: 2011-05-12T23:01:53.00Z
Registrar Registration Expiration Date: 2029-05-12T23:01:53.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.9854014545
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Redacted for Privacy Purposes
Registrant Name: Redacted for Privacy Purposes
Registrant Organization: Redacted for Privacy Purposes
Registrant Street: Redacted for Privacy Purposes
Registrant City: Redacted for Privacy Purposes
Registrant State/Province: WA
Registrant Postal Code: Redacted for Privacy Purposes
Registrant Country: US
Registrant Phone: Redacted for Privacy Purposes
Registrant Phone Ext: Redacted for Privacy Purposes
Registrant Fax: Redacted for Privacy Purposes
Registrant Fax Ext: Redacted for Privacy Purposes
Registrant Email: Select Contact Domain Holder link at https://www.namecheap.com/domains/whois/result?domain=hostwindsdns.com
Registry Admin ID: Redacted for Privacy Purposes
Admin Name: Redacted for Privacy Purposes
Admin Organization: Redacted for Privacy Purposes
Admin Street: Redacted for Privacy Purposes
Admin City: Redacted for Privacy Purposes
Admin State/Province: Redacted for Privacy Purposes
Admin Postal Code: Redacted for Privacy Purposes
Admin Country: Redacted for Privacy Purposes

Admin Phone: Redacted for Privacy Purposes
Admin Phone Ext: Redacted for Privacy Purposes
Admin Fax: Redacted for Privacy Purposes
Admin Fax Ext: Redacted for Privacy Purposes
Admin Email: Select Contact Domain Holder link at https://www.namecheap.com/domains/whois/result?domain=hostwindsdns.com
Registry Tech ID: Redacted for Privacy Purposes
Tech Name: Redacted for Privacy Purposes
Tech Organization: Redacted for Privacy Purposes
Tech Street: Redacted for Privacy Purposes
Tech City: Redacted for Privacy Purposes
Tech State/Province: Redacted for Privacy Purposes
Tech Postal Code: Redacted for Privacy Purposes
Tech Country: Redacted for Privacy Purposes
Tech Phone: Redacted for Privacy Purposes
Tech Phone Ext: Redacted for Privacy Purposes
Tech Fax: Redacted for Privacy Purposes
Tech Fax Ext: Redacted for Privacy Purposes
Tech Email: Select Contact Domain Holder link at https://www.namecheap.com/domains/whois/result?domain=hostwindsdns.com
Name Server: dns1.hostwindsdns.com
Name Server: dns2.hostwindsdns.com
Name Server: dns3.hostwindsdns.com
Name Server: dns4.hostwindsdns.com
DNSSEC: unsigned

Relationships

104.168.236.46	Connected_From	52072a8f99dacd5c293fccd051eab95516d8b880cd2bc5a7e0f4a30d008e22a7

Description

During analysis, the file vftrace.dll attempted to connect to this domain.

---

f1a2791eebaea183f399110c9e8ae11c67f5bebf93a5573d1ac3c56fc71b2230

Details

Name	config.ini
Size	49 bytes
Type	ASCII text, with CRLF line terminators
MD5	9d8d7d7bb357ee37a6ae71c5140f28b9
SHA1	40fc8b1a691339b9fa1526970ff2a2e1d3f899d7
SHA256	f1a2791eebaea183f399110c9e8ae11c67f5bebf93a5573d1ac3c56fc71b2230
SHA512	1d30fb579e0dba09b24669a5a981652f1f6404d2f536e8e640c48585b3035d0826fed15279568400418c19849e17489baccd18e35b53f8cdbc196a0dd5abd496
ssdeep	3:pSMk0eR2Hxm+yn:pSMFeR2Vy
Entropy	4.546046

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

f1a2791eeb...	Created_By	52072a8f99dacd5c293fccd051eab95516d8b880cd2bc5a7e0f4a30d008e22a7

Description

This artifact contains a GUID that is generated by the malware to uniquely identify the system during communication with the C2.

f2ba8b8aabf73020febd3a925276d52ce88f295537fe57723df714c13f5a8780

Tags

backdoor keylogger

Details

Name	thumb.dat
Size	58274 bytes
Type	data
MD5	84f09d192ec90542ede22c370836ffa6
SHA1	7fb23c6b4db90b55694bdd1cc5c1b4c706a4e181
SHA256	f2ba8b8aabf73020febd3a925276d52ce88f295537fe57723df714c13f5a8780
SHA512	56474f45eed25ab86ac9d17b6afb69e0dee07fe507fc5ac4e22ebae0d124700c533dc2adaaaf4be096a5dab27f7f88c21b290cca600576dbf8f10482f2f62d8b
ssdeep	1536:xy98XehX2k0xfXGxGKt5mzvOOIE3CYzahbdoZJI7Vq:xRX0X90KNtevUXYzahbdfq
Entropy	7.301514

Antivirus

No matches found.

YARA Rules

No matches found.

ssdeep Matches

No matches found.

Relationships

f2ba8b8aab...	Created_By	52072a8f99dacd5c293fccd051eab95516d8b880cd2bc5a7e0f4a30d008e22a7

Description

This artifact is the encrypted configuration data that is read by 52072a8f99dacd5c293fccd051eab95516d8b880cd2bc5a7e0f4a30d008e22a7 detailed in this report. The decrypted strings in the configuration are listed below:

—Begin Decrypted Strings—
system -k networkservice
svchost.exe
localservice -k localservice
networkservice
clip.log
rb %04/%02d%02d:%02d:%02d
ab+
SOFTWARE\Microsoft
config_ :\ \ %d %d %d %d
config.ini
Guid
Config %08X%04X%04X%02X%02X%02X%02X%02X%02X%02X%02X%02X
RtlGetVersion
ntdll.dll
Vista
Win2008
Win7
Win2008(R2)
Win8
Win2012
Win8.1

Win2012(R2)
WinXp
Win2003
Win10
Win2016
IsWow64Process
kernel32
open
%d/%d/%d %d:%d
key.log
explorer.exe
/api/v2/ajax
POST
https://%s:%d/api/v2/ajax
\pipe\testpipe
\HKEY_CURRENT_USER\
\HKEY_LOCAL_MACHINE\
config.ini
SOFTWARE\Microsoft\Windows\CurrentVersion\Run
log.log
%s\%d
exe
wb
Kernel32.dll
msiexec.exe
\cmd.exe
ntdll
SeDebugPrivilege
runas
taskmgr
exe
ccc
bbb
aaa
windefende%d
80A85553-1E05-4323-B4F9-43A4396A4507
Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/34.0.1847.116 Safari/537.36

—End Decrypted Strings—

This configuration allows the malware to connect to its C2, create persistence on the system, log keystrokes and telemetry data, and execute commands from the command line.

Relationship Summary

df847abbfa...	Used	52072a8f99dacd5c293fccd051eab95516d8b880cd2bc5a7e0f4a30d008e22a7
52072a8f99...	Connected_To	104.168.236.46
52072a8f99...	Used_By	df847abbfac55fb23715cde02ab52cbe59f14076f9e4bd15edbe28dcecb2a348
52072a8f99...	Created	f1a2791eebaea183f399110c9e8ae11c67f5bebf93a5573d1ac3c56fc71b2230
52072a8f99...	Created	f2ba8b8aabf73020febd3a925276d52ce88f295537fe57723df714c13f5a8780
104.168.236.46	Connected_From	52072a8f99dacd5c293fccd051eab95516d8b880cd2bc5a7e0f4a30d008e22a7
f1a2791eeb...	Created_By	52072a8f99dacd5c293fccd051eab95516d8b880cd2bc5a7e0f4a30d008e22a7
f2ba8b8aab...	Created_By	52072a8f99dacd5c293fccd051eab95516d8b880cd2bc5a7e0f4a30d008e22a7

Conclusion

The following MITRE ATT&CK tactics and techniques were observed during analysis of these samples.

T1543.003 Persistence: Create or Modify System Process. Adversaries may create or modify Windows services to repeatedly execute malicious payloads as part of persistence. When Windows boots up, it starts programs or applications called services that perform background system functions. Windows service configuration information, including the file path to the service's executable or recovery programs/commands, is stored in the Windows Registry. Service configurations can be modified using utilities such as sc.exe and Reg.

T1574.002 Hijack Execution Flow: DLL Side-Loading. Adversaries may execute their own malicious payloads by side-loading DLLs. Side-loading involves hijacking which DLL a program loads. But rather than just planting the DLL within the search order of a program then waiting for the victim application to be invoked, adversaries may directly side-load their payloads by planting then invoking a legitimate application that executes their payload(s).

T1567.000 Exfiltration: Exfiltration Over Web Service. Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel. Popular Web services acting as an exfiltration mechanism may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to compromise. Firewall rules may also already exist to permit traffic to these services.

T1560.000 Collection: Archive Collected Data. An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network. Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender.

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 (UNCLASS)
- CISA SIPR (SIPRNET)
- CISA IC (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 this 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 the CISA at 1-888-282-0870 or CISA Service Desk.

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
- 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.

TLP: CLEAR