Overview

We analysed Trickbot during a forensics case and extracted a dropper executable on to a laptop in our malware lab for secondary dynamic analysis, monitoring it in the controlled environment. Trickbot, classified as a Trojan, has risen in prominence in recent years and our analysis enabled us to capture system changes and network communications during infection. The analysis allows us to share some of the indicators of Trickbot on infected systems. Notes for defensive hardening against this Trojan are included in the conclusion.

Trickbot is a dominant trojan malware continuously being updated with new capabilities, features and distribution vectors. The researcher Vitali Kremez classifies it as an infection framework to sell to criminal customers for exploitation [1]. Trickbot is a flexible malware with secondary malware module delivery, shown in section 5 below, that can be distributed as part of multi-purpose campaigns. For this reason, it has been employed to do different tasks by different groups, the highest profile of which is the delivery of RYUK ransomware against state departments and hospitals in the United States. State departments including Florida City in June 2019 [2], Louisiana in Nov 2019 [3] and owner of 17 hospitals Hackensack Meridian Health in December 2019 [4] suffered widespread ransomware attacks, where forensic investigation revealed Trickbot having dropped RYUK ransomware on the most important target machines. We continue to see instances of Trickbot and RYUK across the academic sector with no sign of activity decreasing. We would advise that security teams look to have the capability of capturing or alerting on these types of advanced polymorphic malware, when implementing detection solutions.

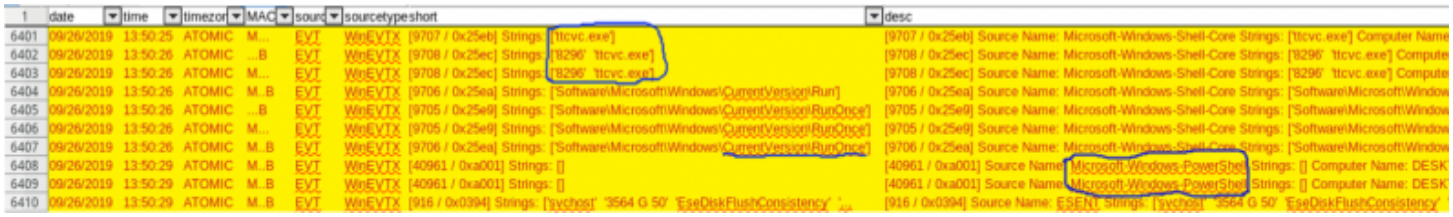
The file analysed: ttcvc.exe
SHA256 signature:
c1d5b3f7632669153420db62e9ab24616ddcaa85751d0114c7b7d04be12edb04

Delivery

Trickbot malware is commonly delivered either by malattachments over email or via a pre-loaded Emotet backdoor infection that is already present [12]. CSIRT have been contacting organisations that have been seen with matching callouts to Emotet C2 domains and IPs for this reason. An example of direct Trickbot delivery via spam mail used is malicious email attachments, and in 2018/2019 the Microsoft Office vulnerability CVE-2017-0199 was a knowr vector for delivery of Trickbot as confirmed by Microsoft Intelligence [5]. This method performs a download and execution of Visual Basic script containing PowerShell commands, occurring when a user opens a document containing RTF formatting. It evades detection by calling out for its second stage over PowerShell, which is very commonly not logged by endpoints. The Trickbot authors are looking to exploit holes in mail security and attachment security to deliver their payload.

Powershell download, evasion

As we had a pre-delivered sample from the wild, this was loaded onto an isolated malware lab machine. The endpoint in the malware lab was infected with the extracted executable on 26th June and was left and kept monitored during a long dwell time. As the machine had PowerShell Module and ScriptBlock logging enabled (detailed in Appendix), we were able to capture the PowerShell events on the machine. The device was left in situ and the below timeline captured from the device, shows the malicious ttcvc.exe running, followed by PowerShell command events.



1	date	time	timezor	MAC	sourc	sourcetype	short	desc
6401	09/26/2019	13:50:25	ATOMIC	M...	EVT	WinEVTX	[9707 / 0x25eb] Strings: ['ttcvc.exe']	[9707 / 0x25eb] Source Name: Microsoft-Windows-Shell-Core Strings: ['ttcvc.exe'] Computer Name
6402	09/26/2019	13:50:26	ATOMIC	...B	EVT	WinEVTX	[9708 / 0x25ec] Strings: ['8296' 'ttcvc.exe']	[9708 / 0x25ec] Source Name: Microsoft-Windows-Shell-Core Strings: ['8296' 'ttcvc.exe'] Compute
6403	09/26/2019	13:50:26	ATOMIC	M...	EVT	WinEVTX	[9708 / 0x25ec] Strings: ['8296' 'ttcvc.exe']	[9708 / 0x25ec] Source Name: Microsoft-Windows-Shell-Core Strings: ['8296' 'ttcvc.exe'] Compute
6404	09/26/2019	13:50:26	ATOMIC	M..B	EVT	WinEVTX	[9706 / 0x25ea] Strings: ['Software\Microsoft\Windows\CurrentVersion\Run']	[9706 / 0x25ea] Source Name: Microsoft-Windows-Shell-Core Strings: ['Software\Microsoft\Window
6405	09/26/2019	13:50:26	ATOMIC	...B	EVT	WinEVTX	[9705 / 0x25e9] Strings: ['Software\Microsoft\Windows\CurrentVersion\RunOnce']	[9705 / 0x25e9] Source Name: Microsoft-Windows-Shell-Core Strings: ['Software\Microsoft\Window
6406	09/26/2019	13:50:26	ATOMIC	M...	EVT	WinEVTX	[9705 / 0x25e9] Strings: ['Software\Microsoft\Windows\CurrentVersion\RunOnce']	[9705 / 0x25e9] Source Name: Microsoft-Windows-Shell-Core Strings: ['Software\Microsoft\Window
6407	09/26/2019	13:50:26	ATOMIC	M..B	EVT	WinEVTX	[9706 / 0x25ea] Strings: ['Software\Microsoft\Windows\CurrentVersion\RunOnce']	[9706 / 0x25ea] Source Name: Microsoft-Windows-Shell-Core Strings: ['Software\Microsoft\Window
6408	09/26/2019	13:50:29	ATOMIC	M..B	EVT	WinEVTX	[40961 / 0xa001] Strings: []	[40961 / 0xa001] Source Name: Microsoft-Windows-PowerShell Strings: [] Computer Name: DESK
6409	09/26/2019	13:50:29	ATOMIC	M..B	EVT	WinEVTX	[40961 / 0xa001] Strings: []	[40961 / 0xa001] Source Name: Microsoft-Windows-PowerShell Strings: [] Computer Name: DESK
6410	09/26/2019	13:50:29	ATOMIC	M..B	EVT	WinEVTX	[916 / 0x0394] Strings: ['svchost' '3564 G 50' 'EseDiskFlushConsistency' '...	[916 / 0x0394] Source Name: ESENT Strings: ['svchost' '3564 G 50' 'EseDiskFlushConsistency' '

[i] The controlled laptop malware infection timeline with malicious exe running, followed by PowerShell events and matching parent process:8296 of process:8432 svchost.exe start time in UTC, shown on screenshot viii.

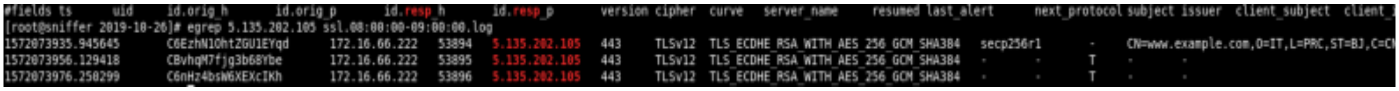
The recorded Powershell script showed the common Trickbot action of disabling Windows Threat Defender:

PowerShell_transcript.DESKTOP-KLN3EO8._NcmK7Q4.20190926145031.txt
RunAs User: DESKTOP-KLN3EO8\XZ123
Configuration Name:
Machine: DESKTOP-KLN3EO8 (Microsoft Windows NT 10.0.17134.0)
Host Application: Powershell Set-MpPreference -DisableRealtimeMonitoring $true

Persistence and network events

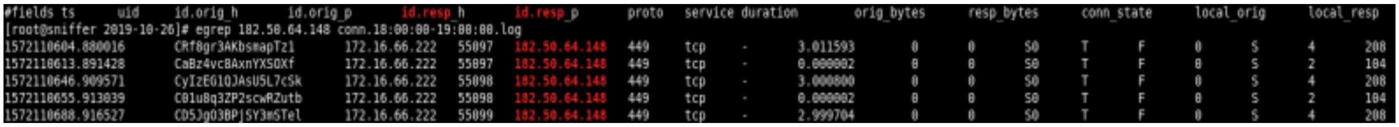
Under dynamic analysis, network traffic was captured using Bro/Zeek NSM logging. Through understanding of Trickbot behaviour and identifying the malicious C2 IPs involved, we were able to capture malicious traffic events. These are 'heartbeat' like callouts from Trickbot over port 449 which we observed in a contained malware network. Traffic over ports 443 and 449 to the IPs in the IOC section are an atomic indication of Trickbot [6], worthy of tracking and identifying hosts for investigation.

Below are captured examples of Trickbot traffic



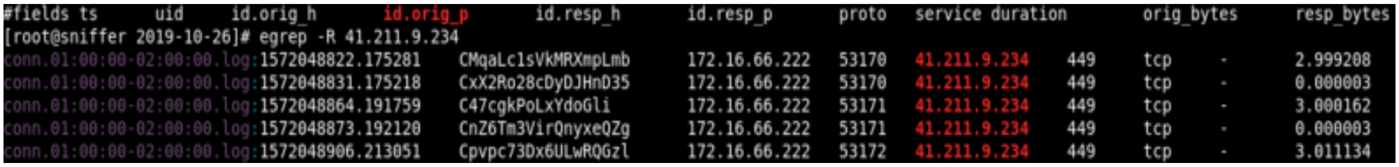
```
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       version cipher  curve   server_name     resumed last_alert      next_protocol subject issuer  client_subject  client_
[root@sniffer 2019-10-26]# egrep 5.135.202.105 ssl.08:00:00-09:00:00.log
1572073935.945645       C6EzhN1OhtZGU1EYqd      172.16.66.222   53894   5.135.202.105   443     TLSv12  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384   secp256r1       -       CN=www.example.com,O=IT,L=PRC,ST=BJ,C=CN
1572073956.129418       CBvhqM7fjg3b68Ybe       172.16.66.222   53895   5.135.202.105   443     TLSv12  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384   -       -       T       -       -
1572073976.250299       C6nHz4bsW6XEXcIKh       172.16.66.222   53896   5.135.202.105   443     TLSv12  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384   -       -       T       -       -
```

[ii] Remote host: *5.135.202.105:443 (captured SSL traffic to malware C2 note SSL example subject and self-signed issuer China)*



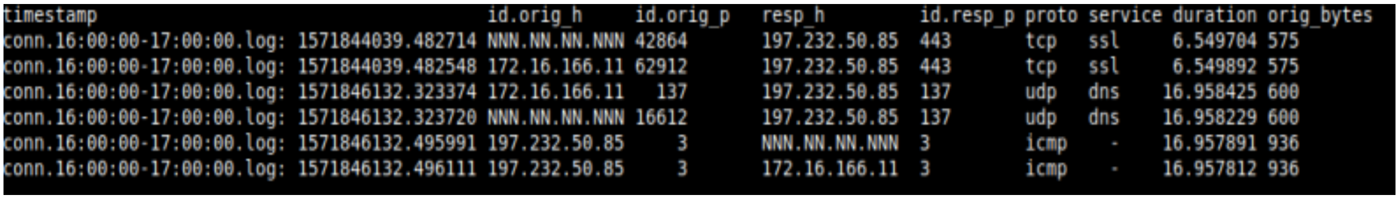
```
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   service duration        orig_bytes      resp_bytes      conn_state      local_orig      local_resp
[root@sniffer 2019-10-26]# egrep 182.50.64.148 conn.18:00:00-19:00:00.log
1572110604.880016       CRf8gr3AKbsmapTz1       172.16.66.222   55097   182.50.64.148   449     tcp     -       3.011593        0       0       S0      T       F       0       S       4       208
1572110613.891428       CaBz4vc8AxnYXSOXf       172.16.66.222   55097   182.50.64.148   449     tcp     -       0.000002        0       0       S0      T       F       0       S       2       104
1572110646.909571       CyIzEG1QJAsU5L7cSk      172.16.66.222   55098   182.50.64.148   449     tcp     -       3.000800        0       0       S0      T       F       0       S       4       208
1572110655.913039       C01u8q3ZP2scwRZutb      172.16.66.222   55098   182.50.64.148   449     tcp     -       0.000002        0       0       S0      T       F       0       S       2       104
1572110688.916527       CD5Jg03BPjSY3mSTel      172.16.66.222   55099   182.50.64.148   449     tcp     -       2.999704        0       0       S0      T       F       0       S       4       208
```

[iii] Remote host *182.50.64.148:449 (Trickbot C2* https://otx.alienvault.com/indicator/ip/182.50.64.148*)*



```
#fields ts      uid     id.orig_h       id.orig_p       id.resp_h       id.resp_p       proto   service duration        orig_bytes      resp_bytes
[root@sniffer 2019-10-26]# egrep -R 41.211.9.234
conn.01:00:00-02:00:00.log:1572048822.175281    CMqaLc1sVkMRXmpLmb      172.16.66.222   53170   41.211.9.234    449     tcp     -       2.999208
conn.01:00:00-02:00:00.log:1572048831.175218    CxX2Ro28cDyDJHnD35      172.16.66.222   53170   41.211.9.234    449     tcp     -       0.000003
conn.01:00:00-02:00:00.log:1572048864.191759    C47cgkPoLxYdoGli        172.16.66.222   53171   41.211.9.234    449     tcp     -       3.000162
conn.01:00:00-02:00:00.log:1572048873.192120    CnZ6Tm3VirQnyxeQZg      172.16.66.222   53171   41.211.9.234    449     tcp     -       0.000003
conn.01:00:00-02:00:00.log:1572048906.213051    Cpvpc73Dx6ULwRQGzl      172.16.66.222   53172   41.211.9.234    449     tcp     -       3.011134
```

[iv] Remote host: 41.211.9.234:449 (Trickbot C2 as confirmed in Microsoft advisory [7])



```
timestamp                                       id.orig_h       id.orig_p       resp_h          id.resp_p proto service duration orig_bytes
conn.16:00:00-17:00:00.log: 1571844039.482714 NNN.NN.NN.NNN 42864      197.232.50.85  443       tcp   ssl      6.549704 575
conn.16:00:00-17:00:00.log: 1571844039.482548 172.16.166.11 62912      197.232.50.85  443       tcp   ssl      6.549892 575
conn.16:00:00-17:00:00.log: 1571846132.323374 172.16.166.11   137      197.232.50.85  137       udp   dns     16.958425 600
conn.16:00:00-17:00:00.log: 1571846132.323720 NNN.NN.NN.NNN 16612      197.232.50.85  137       udp   dns     16.958229 600
conn.16:00:00-17:00:00.log: 1571846132.495991 197.232.50.85     3      NNN.NN.NN.NNN  3         icmp  -       16.957891 936
conn.16:00:00-17:00:00.log: 1571846132.496111 197.232.50.85     3      172.16.166.11  3         icmp  -       16.957812 936
```

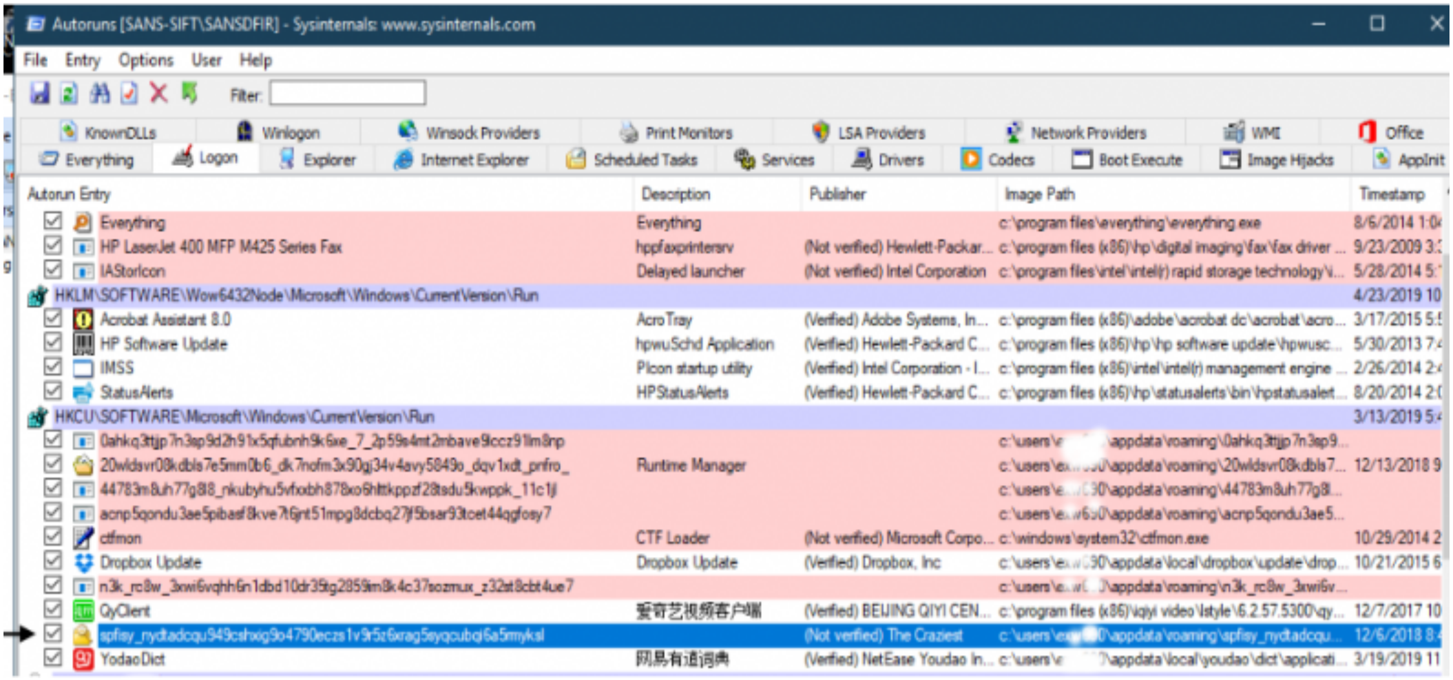
[v] Remote host: 197.232.50.85 SSL, ICMP, NetBIOS (showing as dns port 137) traffic (Trickbot https://otx.alienvault.com/indicator/ip/197.232.50.85)

Researchers at the Centre for Internet Security [8] noted that a variant Trickbot sample was observed performing callouts to 'whats-my-ip' style services to feed back to the infection command and control. Examples include:

api.ipify.org
ipecho.net/plain
ipinfo.io/ip

This checking of NATed IP activity wasn't captured however during our analysis of the Trickbot sample. Trickbot persistence comes from auto-start services being added to systems. Autoruns.exe is a Windows program that is part of their SysInternals Utilities, a suite of system tools. It shows which services or executables have been set to run on system start-up. This is a nice, fast way to identify if processes are present that should not be.

As highlighted in the Autoruns output below, spfisy…exe is a malicious amendment to the HKEY_Current_User registry SOFTWARE\Microsoft\Windows\CurrentVersion\Run policy that refers to the location of the executable. This technique is used by malware to ensure the service is still running after system reboot. Note that it is enabling persistence to these same malicious files store in the Username\AppData\Roaming folder.



Autorun Entry	Description	Publisher	Image Path	Timestamp
☑ Everything	Everything		c:\program files\everything\everything.exe	8/6/2014 1:0
☑ HP LaserJet 400 MFP M425 Series Fax	hppfaxprintersrv	(Not verified) Hewlett-Packar...	c:\program files (x86)\hp\digital imaging\fax\fax driver ...	9/23/2009 3:3
☑ IAStorIcon	Delayed launcher	(Not verified) Intel Corporation	c:\program files\intel\intel(r) rapid storage technology\i...	5/28/2014 5:1
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				4/23/2019 10
☑ Acrobat Assistant 8.0	AcroTray	(Verified) Adobe Systems, In...	c:\program files (x86)\adobe\acrobat dc\acrobat\acro...	3/17/2015 5:5
☑ HP Software Update	hpwuSchd Application	(Verified) Hewlett-Packard C...	c:\program files (x86)\hp\hp software update\hpwusc...	5/30/2013 7:4
☑ IMSS	PIcon startup utility	(Verified) Intel Corporation - I...	c:\program files (x86)\intel\intel(r) management engine ...	2/26/2014 2:4
☑ StatusAlerts	HPStatusAlerts	(Verified) Hewlett-Packard C...	c:\program files (x86)\hp\statusalerts\bin\hpstatusalert...	8/20/2014 2:0
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				3/13/2019 5:4
☑ 0ahkq3ttjp7n3ep9d2h91x5qfubnh9k6xe_7_2p59s4mt2mbave9lccz91lm8np			c:\users\[redacted]\appdata\roaming\0ahkq3ttjp7n3ep9...	
☑ 20wldsvr08kdbls7e5mm0b6_dk7nofm3x90gj34v4avy5849o_dqv1xdt_pnfro_	Runtime Manager		c:\users\[redacted]\appdata\roaming\20wldsvr08kdbls7...	12/13/2018 9
☑ 44783m8uh77g8l8_nkubyhu5vfxxbh878xo6hltkppzf28sdu5kwppk_11c1jl			c:\users\[redacted]\appdata\roaming\44783m8uh77g8l...	
☑ acnp5qondu3ae5pibasf8kve7t6jnt51mpg8dcbq27jf5bsar93tcet44qgfosy7			c:\users\[redacted]\appdata\roaming\acnp5qondu3ae5...	
☑ ctfmon	CTF Loader	(Not verified) Microsoft Corpo...	c:\windows\system32\ctfmon.exe	10/29/2014 2
☑ Dropbox Update	Dropbox Update	(Verified) Dropbox, Inc	c:\users\[redacted]\appdata\local\dropbox\update\drop...	10/21/2015 6
☑ n3k_rc8w_3xwi6vqhh6n1dbd10dr35tg2859im8k4c37sozmux_z32st8cbt4ue7			c:\users\[redacted]\appdata\roaming\n3k_rc8w_3xwi6v...	
☑ QyClient	爱奇艺视频客户端	(Verified) BEIJING QIYI CEN...	c:\program files (x86)\iqiyi video\lstyle\6.2.57.5300\qy...	12/7/2017 10
☑ spfisy_nydtadcqu949cshxig9o4790eczs1v9r5z6xrag5eyqcubqi6a5myksl		(Not verified) The Craziest	c:\users\[redacted]\appdata\roaming\spfisy_nydtadcqu...	12/6/2018 8:4
☑ YodaoDict	网易有道词典	(Verified) NetEase Youdao In...	c:\users\[redacted]\appdata\local\youdao\dict\applicati...	3/19/2019 11

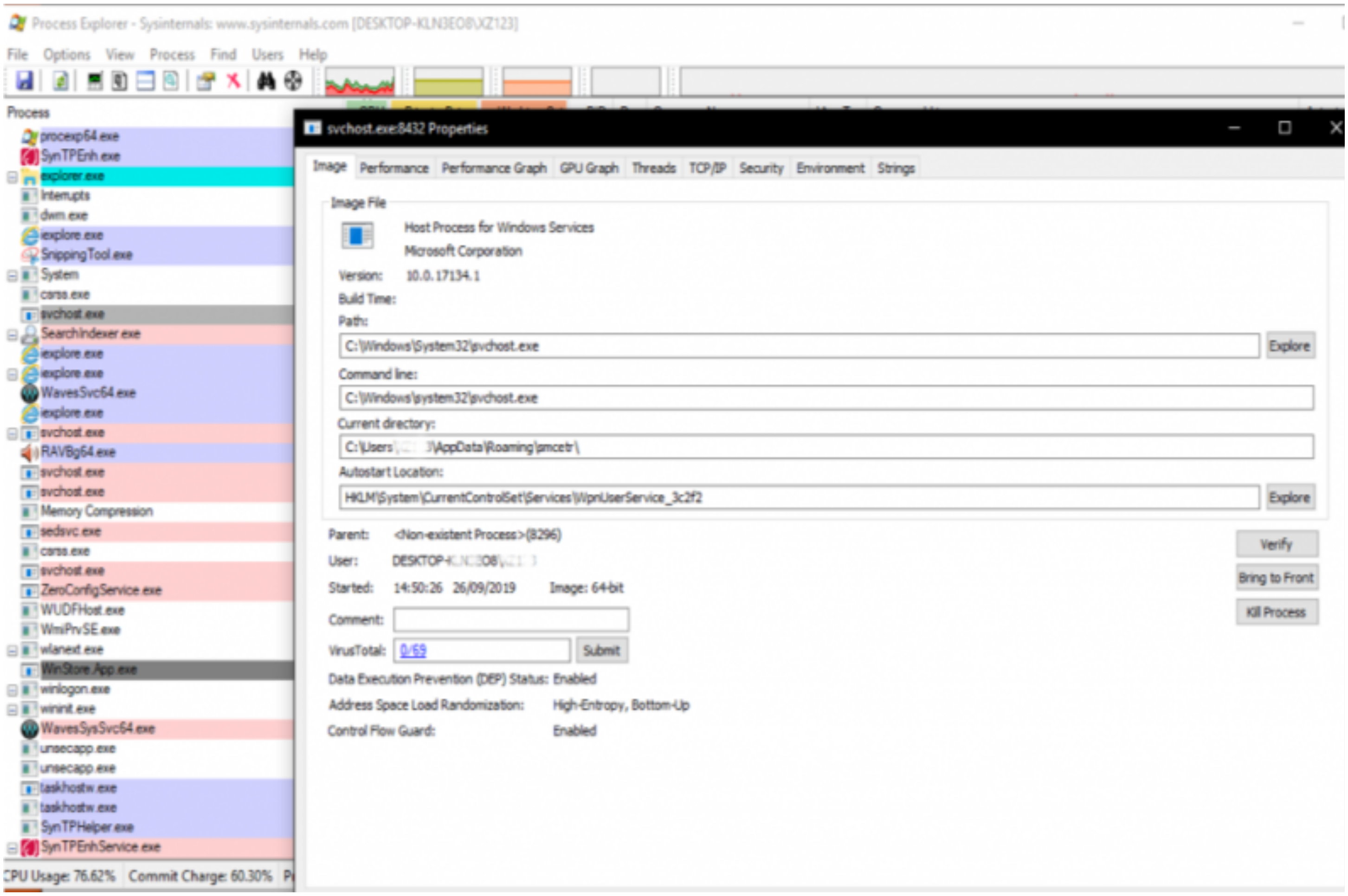
[vi] Autoruns output on forensics case. This executable was dropped by Trickbot, to ensure the stcvc.exe was in place.

Trickbot operation and exploitation modules

Once a Trickbot infection is live, the 'heartbeats' are calling over ports 449 or 443. Code from the Trickbot infection is typically injected into the svchost.exe process, noted as T1055 in the Trickbot software entry within the MITRE ATT&CK framework [9]. We captured this process injection occurring - see screenshot [viii] and note the directory of svchost.exe is the users' AppData directory mentioned previously.

This svchost.exe injection activity is somewhat indicative of 'Man in the Browser' technique to steal online banking credentials [12], while our host was also calling out to the IPs given on the Microsoft advisory that backs this up [7]. It was suspicious advertising in an open browser that gave some indication the host was infected. If a raw memory capture was taken (it wasn't obtained in the raw format at the time) and analysed with Volatility, this would have offered further investigation opportunity to prove that the legitimate process svchost.exe was started, suspended then replaced with malicious binary stcvc.exe and restarted.

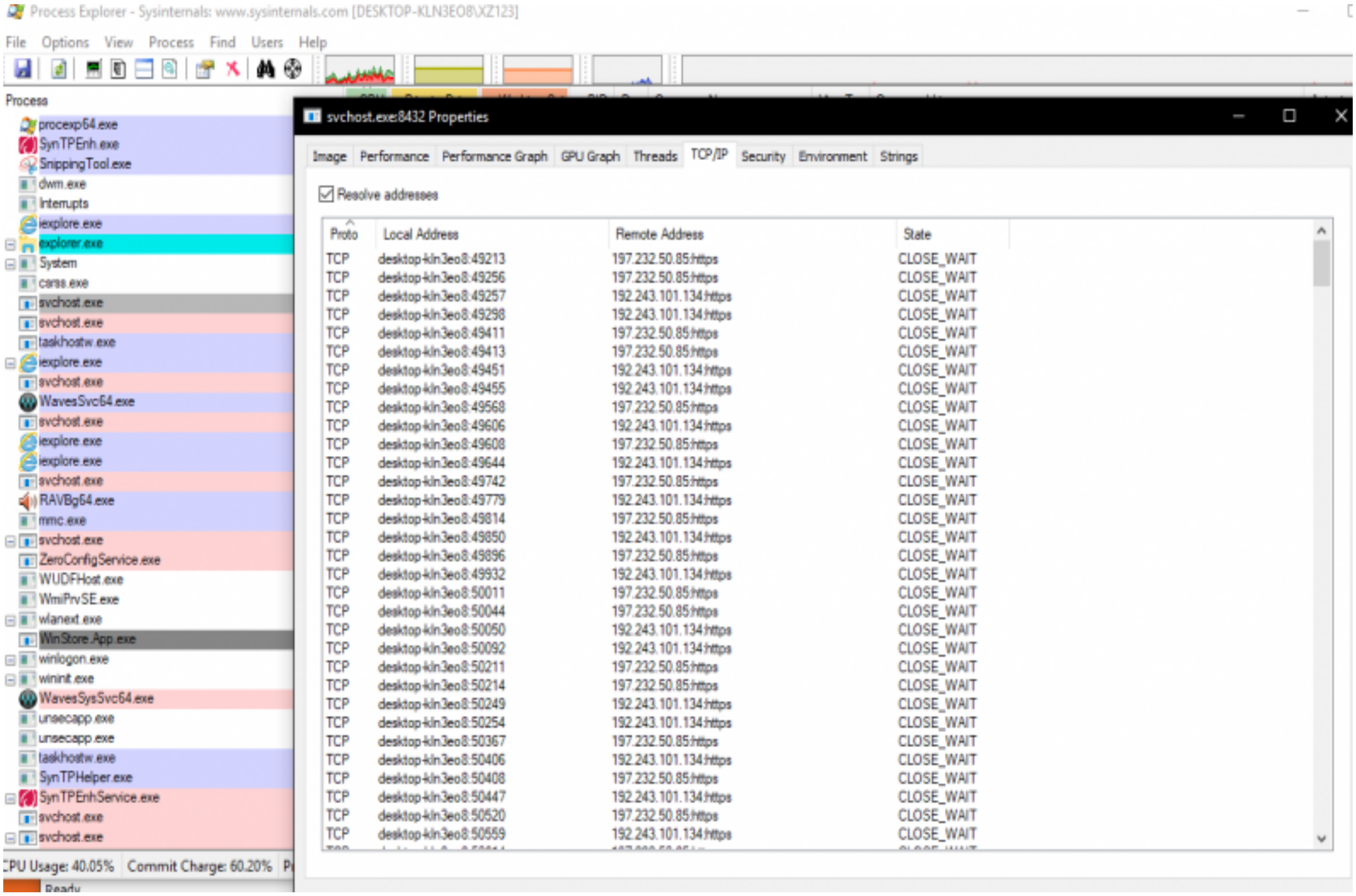
Despite this, it was rewarding to catch an injected Trickbot svchost.exe process live with IP connections [ix]. Sysinternals' Process Explorer proved very useful in analysing the running malicious process and identifying its TCP/IP communications to IPs identified as Trickbot C2s.



```
procexp64.exe
SynTPEnh.exe
explorer.exe
Interrupts
dwm.exe
iexplore.exe
SnippingTool.exe
System
csrss.exe
svchost.exe
SearchIndexer.exe
iexplore.exe
iexplore.exe
WavesSvc64.exe
iexplore.exe
svchost.exe
RAVBg64.exe
svchost.exe
svchost.exe
Memory Compression
sedsvc.exe
csrss.exe
svchost.exe
ZeroConfigService.exe
WUDFHost.exe
WmiPrvSE.exe
wlanext.exe
WinStore.App.exe
winlogon.exe
wininit.exe
WavesSysSvc64.exe
unsecapp.exe
unsecapp.exe
taskhostw.exe
taskhostw.exe
SynTPHelper.exe
SynTPEnhService.exe
CPU Usage: 76.62%   Commit Charge: 60.30%
```

Host Process for Windows Services
Microsoft Corporation
Version: 10.0.17134.1
Build Time:
Path: C:\Windows\System32\svchost.exe
Command line: C:\Windows\system32\svchost.exe
Current directory: C:\Users\[redacted]\AppData\Roaming\smcetr\
Autostart Location: HKLM\System\CurrentControlSet\Services\WpnUserService_3c2f2
Parent: <Non-existent Process>(8296)
User: DESKTOP-[redacted]
Started: 14:50:26 26/09/2019 Image: 64-bit
Comment:
VirusTotal: 0/69
Data Execution Prevention (DEP) Status: Enabled
Address Space Load Randomization: High-Entropy, Bottom-Up
Control Flow Guard: Enabled

[viii] Showing 'smcetr' directory of Trickbot infection at 14:50:26 GMT matching timeline event from [i]


Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-KLN3EO8\XZ123]
File Options View Process Find Users Help
svchost.exe:8432 Properties
Image Performance Performance Graph GPU Graph Threads TCP/IP Security Environment Strings
Ready

```
Process
procexp64.exe
SynTPEnh.exe
SnippingTool.exe
dwm.exe
Interrupts
iexplore.exe
explorer.exe
System
csrss.exe
svchost.exe
svchost.exe
taskhostw.exe
iexplore.exe
svchost.exe
WavesSvc64.exe
svchost.exe
iexplore.exe
iexplore.exe
svchost.exe
RAVBg64.exe
mmc.exe
svchost.exe
ZeroConfigService.exe
WUDFHost.exe
WmiPrvSE.exe
wlanext.exe
WinStore.App.exe
winlogon.exe
wininit.exe
WavesSysSvc64.exe
unsecapp.exe
unsecapp.exe
taskhostw.exe
SynTPHelper.exe
SynTPEnhService.exe
svchost.exe
svchost.exe
CPU Usage: 40.05%   Commit Charge: 60.20%
```

☑ Resolve addresses

Proto	Local Address	Remote Address	State
TCP	desktop-kln3eo8:49213	197.232.50.85:https	CLOSE_WAIT
TCP	desktop-kln3eo8:49256	197.232.50.85:https	CLOSE_WAIT
TCP	desktop-kln3eo8:49257	192.243.101.134:https	CLOSE_WAIT
TCP	desktop-kln3eo8:49298	192.243.101.134:https	CLOSE_WAIT
TCP	desktop-kln3eo8:49411	197.232.50.85:https	CLOSE_WAIT
TCP	desktop-kln3eo8:49413	197.232.50.85:https	CLOSE_WAIT
TCP	desktop-kln3eo8:49451	192.243.101.134:https	CLOSE_WAIT
TCP	desktop-kln3eo8:49455	192.243.101.134:https	CLOSE_WAIT
TCP	desktop-kln3eo8:49568	197.232.50.85:https	CLOSE_WAIT
TCP	desktop-kln3eo8:49606	192.243.101.134:https	CLOSE_WAIT
TCP	desktop-kln3eo8:49608	197.232.50.85:https	CLOSE_WAIT
TCP	desktop-kln3eo8:49644	192.243.101.134:https	CLOSE_WAIT
TCP	desktop-kln3eo8:49742	197.232.50.85:https	CLOSE_WAIT
TCP	desktop-kln3eo8:49779	192.243.101.134:https	CLOSE_WAIT
TCP	desktop-kln3eo8:49814	197.232.50.85:https	CLOSE_WAIT
TCP	desktop-kln3eo8:49850	192.243.101.134:https	CLOSE_WAIT
TCP	desktop-kln3eo8:49896	197.232.50.85:https	CLOSE_WAIT
TCP	desktop-kln3eo8:49932	192.243.101.134:https	CLOSE_WAIT
TCP	desktop-kln3eo8:50011	197.232.50.85:https	CLOSE_WAIT
TCP	desktop-kln3eo8:50044	197.232.50.85:https	CLOSE_WAIT
TCP	desktop-kln3eo8:50050	192.243.101.134:https	CLOSE_WAIT
TCP	desktop-kln3eo8:50092	192.243.101.134:https	CLOSE_WAIT
TCP	desktop-kln3eo8:50211	197.232.50.85:https	CLOSE_WAIT
TCP	desktop-kln3eo8:50214	197.232.50.85:https	CLOSE_WAIT
TCP	desktop-kln3eo8:50249	192.243.101.134:https	CLOSE_WAIT
TCP	desktop-kln3eo8:50254	192.243.101.134:https	CLOSE_WAIT
TCP	desktop-kln3eo8:50367	197.232.50.85:https	CLOSE_WAIT
TCP	desktop-kln3eo8:50406	192.243.101.134:https	CLOSE_WAIT
TCP	desktop-kln3eo8:50408	197.232.50.85:https	CLOSE_WAIT
TCP	desktop-kln3eo8:50447	192.243.101.134:https	CLOSE_WAIT
TCP	desktop-kln3eo8:50520	197.232.50.85:https	CLOSE_WAIT
TCP	desktop-kln3eo8:50559	192.243.101.134:https	CLOSE_WAIT

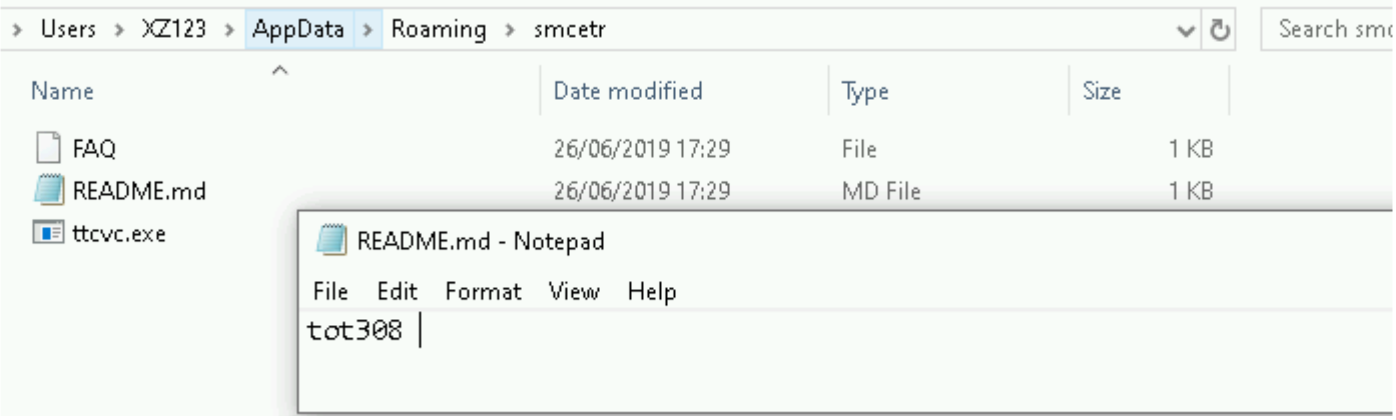
[ix] Process injection of communications channel into svchost.exe seen on same Process ID 8432, using TCP port 443. Note the IP 197.232.50.85 as shown in the Bro logs [v] and classec as an atomic indicator of Trickbot.

Analysis in windows executable static analysis tool Dependency Walker of the loaded DLLs by stcvc.exe also confirmed the behaviour of this Trickbot infection. This tool shows not only the loaded DLLs, but also the imported functions which indicates what the malware does [10]. Analysis performed on this tool revealed that the following items were loaded:

Kernel32.dll – core functionality, access and manipulation of memory, files, and hardware – Called the function CreateProcessA, a strong indicator the program will create another process, a malicious process.

Ws2_32.dll - networking DLL used by a program for connections to a network or performs network-related tasks, indicating network traffic will occur from the malicious process.

Once a host is infected a group tag is assigned to identify it to the trickbot infrastructure. Our system was given the below group tag on system infection. FireEye have listed examples of captured group tags [11], and their list includes the same totxxx format. For us this is another indicator of a live infection, but in wider terms it does imply they are managing large amounts of infected devices and allocating tags simplifies the management of infected devices for post-exploitation activity.

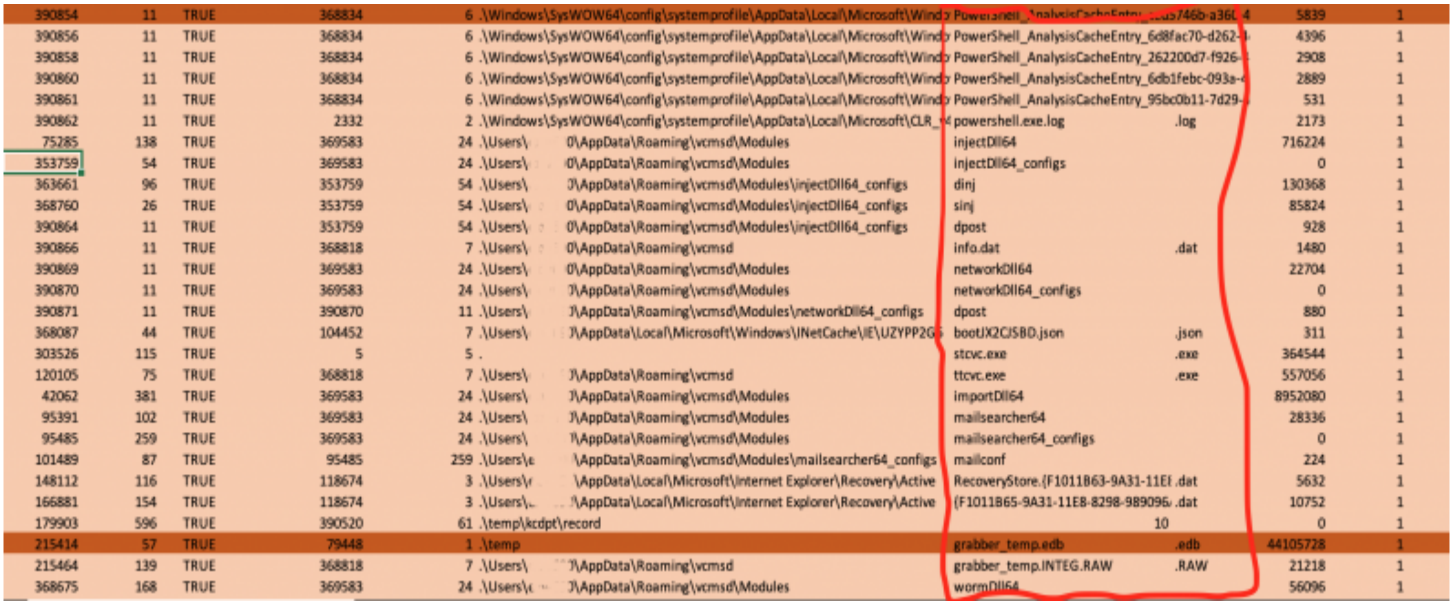

› Users › XZ123 › AppData › Roaming › smcetr
Search smc
README.md - Notepad
File Edit Format View Help

Name	Date modified	Type	Size
FAQ	26/06/2019 17:29	File	1 KB
README.md	26/06/2019 17:29	MD File	1 KB
ttcvc.exe			

```
tot308
```

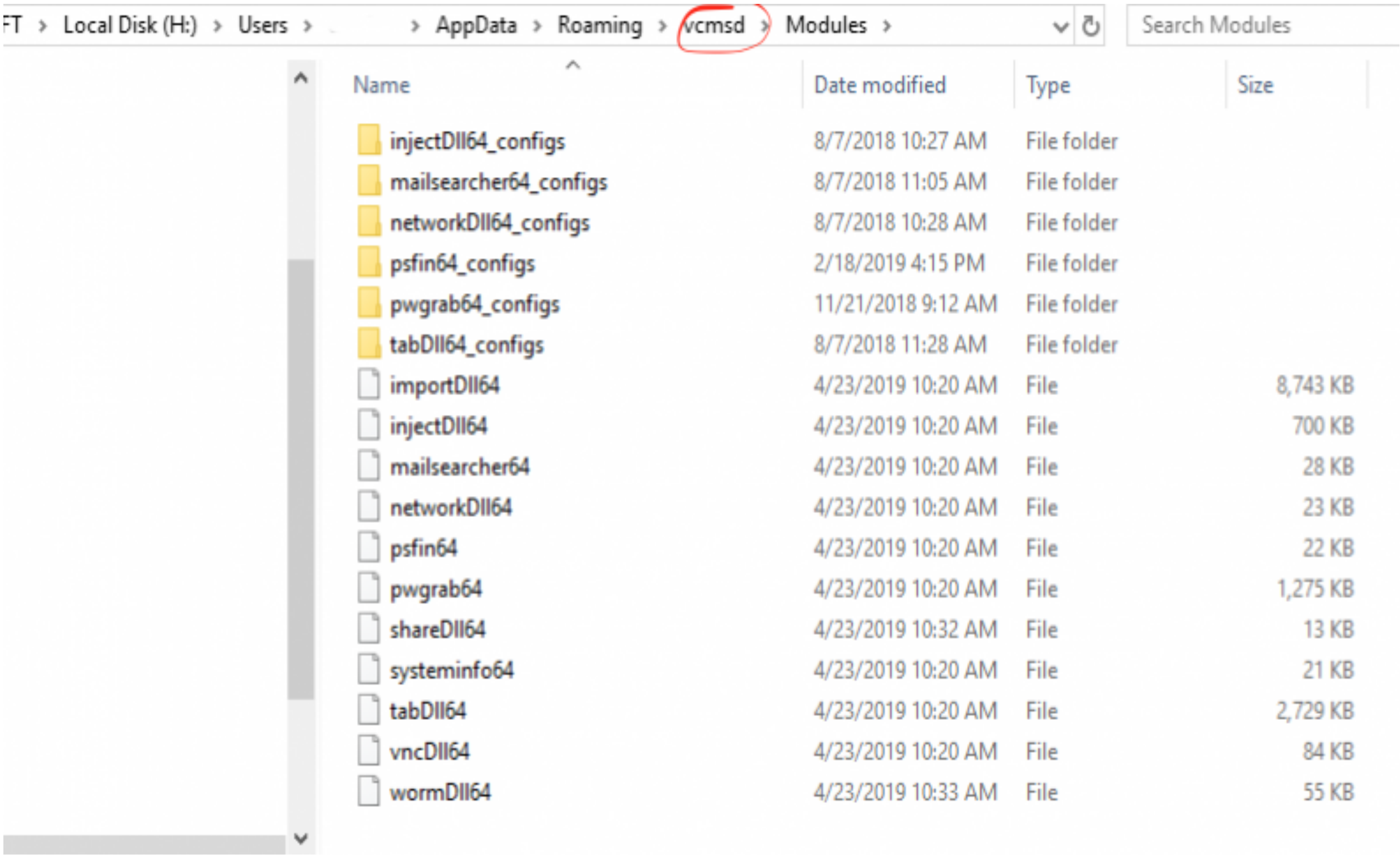
[vii] Screenshot of 'gtag' used to label systems, taken from the malware network laptop alongside the infection exe. CIS have listed this same gtag behaviour in Trickbot [8]

Once Trickbot has a foothold on a system and after a short dwell period, further exploitation modules will be dropped. Below are captures from the forensic case disk examination, where the top of screenshot [x] demonstrates PowerShell usage to download Trickbot modules to the infection vcmsd folder, giving clear evidence of PowerShell's continued use in the exploitation of Trickbot. On this system the threat actor was utilising mail searcher, SMB worm and password grabber modules to perform their actions, evident from the file changes on the timeline. On the second screenshot [xi] we see there is actually a 'module' folder with named Trickbot module DLLs.



390854	11	TRUE	368834	6	.\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windo	PowerShell_AnalysisCacheEntry_[illegible]5746b-a36(4		5839	1
390856	11	TRUE	368834	6	.\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windo	PowerShell_AnalysisCacheEntry_6d8fac70-d262-4		4396	1
390858	11	TRUE	368834	6	.\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windo	PowerShell_AnalysisCacheEntry_262200d7-f926-		2908	1
390860	11	TRUE	368834	6	.\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windo	PowerShell_AnalysisCacheEntry_6db1febc-093a-4		2889	1
390861	11	TRUE	368834	6	.\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\Windo	PowerShell_AnalysisCacheEntry_95bc0b11-7d29-		531	1
390862	11	TRUE	2332	2	.\Windows\SysWOW64\config\systemprofile\AppData\Local\Microsoft\CLR_v4	powershell.exe.log	.log	2173	1
75285	138	TRUE	369583	24	.\Users\ 0\AppData\Roaming\vcmsd\Modules	injectDll64		716224	1
353759	54	TRUE	369583	24	.\Users\ 0\AppData\Roaming\vcmsd\Modules	injectDll64_configs		0	1
363661	96	TRUE	353759	54	.\Users\ 0\AppData\Roaming\vcmsd\Modules\injectDll64_configs	dinj		130368	1
368760	26	TRUE	353759	54	.\Users\ 0\AppData\Roaming\vcmsd\Modules\injectDll64_configs	sinj		85824	1
390864	11	TRUE	353759	54	.\Users\ 0\AppData\Roaming\vcmsd\Modules\injectDll64_configs	dpost		928	1
390866	11	TRUE	368818	7	.\Users\ 0\AppData\Roaming\vcmsd	info.dat	.dat	1480	1
390869	11	TRUE	369583	24	.\Users\ 0\AppData\Roaming\vcmsd\Modules	networkDll64		22704	1
390870	11	TRUE	369583	24	.\Users\ )\AppData\Roaming\vcmsd\Modules	networkDll64_configs		0	1
390871	11	TRUE	390870	11	.\Users\ )\AppData\Roaming\vcmsd\Modules\networkDll64_configs	dpost		880	1
368087	44	TRUE	104452	7	.\Users\ )\AppData\Local\Microsoft\Windows\INetCache\IE\UZYPP2G5	bootJX2CJSBD.json	.json	311	1
303526	115	TRUE	5	5	.	stcvc.exe	.exe	364544	1
120105	75	TRUE	368818	7	.\Users\ )\AppData\Roaming\vcmsd	ttcvc.exe	.exe	557056	1
42062	381	TRUE	369583	24	.\Users\ )\AppData\Roaming\vcmsd\Modules	importDll64		8952080	1
95391	102	TRUE	369583	24	.\Users\ )\AppData\Roaming\vcmsd\Modules	mailsearcher64		28336	1
95485	259	TRUE	369583	24	.\Users\ )\AppData\Roaming\vcmsd\Modules	mailsearcher64_configs		0	1
101489	87	TRUE	95485	259	.\Users\ \AppData\Roaming\vcmsd\Modules\mailsearcher64_configs	mailconf		224	1
148112	116	TRUE	118674	3	.\Users\ \AppData\Local\Microsoft\Internet Explorer\Recovery\Active	RecoveryStore.{F1011B63-9A31-11E	.dat	5632	1
166881	154	TRUE	118674	3	.\Users\ \AppData\Local\Microsoft\Internet Explorer\Recovery\Active	{F1011B65-9A31-11E8-8298-989096	.dat	10752	1
179903	596	TRUE	390520	61	.\temp\kcdpt\record	10		0	1
215414	57	TRUE	79448	1	.\temp	grabber_temp.edb	.edb	44105728	1
215464	139	TRUE	368818	7	.\Users\ )\AppData\Roaming\vcmsd	grabber_temp.INTEG.RAW	.RAW	21218	1
368675	168	TRUE	369583	24	.\Users\ )\AppData\Roaming\vcmsd\Modules	wormDll64		56096	1

[x]Timeline excerpt from full forensic investigation of supplied disk, showing modules and module configs. These are commonly named sinj, dinj, dpost [8]



FT > Local Disk (H:) > Users > > AppData > Roaming > vcmsd > Modules >

Name	Date modified	Type	Size
injectDll64_configs	8/7/2018 10:27 AM	File folder	
mailsearcher64_configs	8/7/2018 11:05 AM	File folder	
networkDll64_configs	8/7/2018 10:28 AM	File folder	
psfin64_configs	2/18/2019 4:15 PM	File folder	
pwgrab64_configs	11/21/2018 9:12 AM	File folder	
tabDll64_configs	8/7/2018 11:28 AM	File folder	
importDll64	4/23/2019 10:20 AM	File	8,743 KB
injectDll64	4/23/2019 10:20 AM	File	700 KB
mailsearcher64	4/23/2019 10:20 AM	File	28 KB
networkDll64	4/23/2019 10:20 AM	File	23 KB
psfin64	4/23/2019 10:20 AM	File	22 KB
pwgrab64	4/23/2019 10:20 AM	File	1,275 KB
shareDll64	4/23/2019 10:32 AM	File	13 KB
systeminfo64	4/23/2019 10:20 AM	File	21 KB
tabDll64	4/23/2019 10:20 AM	File	2,729 KB
vncDll64	4/23/2019 10:20 AM	File	84 KB
wormDll64	4/23/2019 10:33 AM	File	55 KB

[xi] Modules seen on forensic case, these load via DLL side injection/process injection when needed by the threat actor.

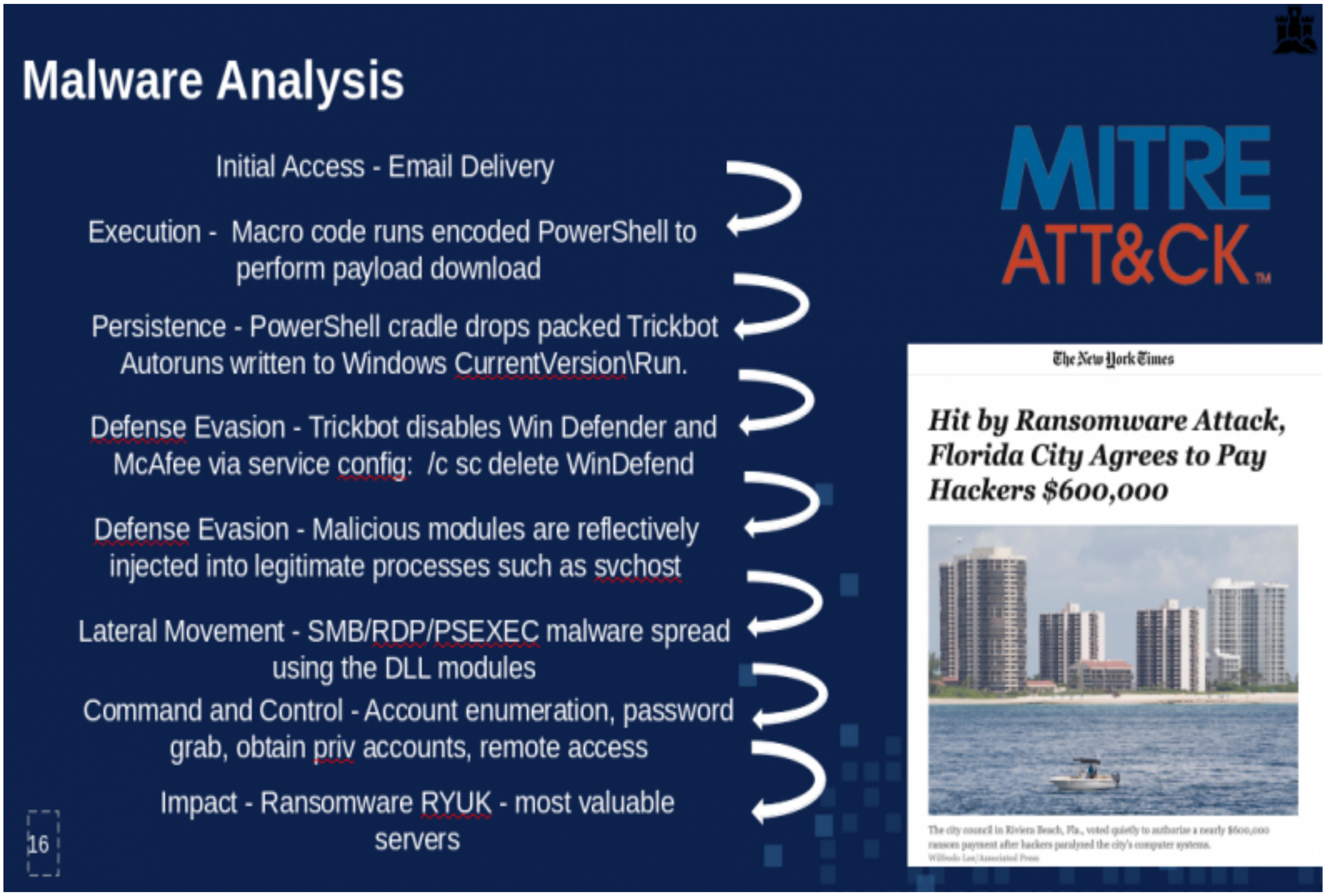
As modular malware, infected hosts can be exploited using modules for different purposes. From the forensics case of a long dwell time Trickbot infection, shown in screenshot [xi], there were multiple module DLLs ready to be loaded for use. Using reference from an excellent Cybereason article that covers the modules [12], I list below the purposes of some of these to demonstrate the capabilities of this malware family:

VncDll64 - Allows an attacker to remotely view and control a victim's desktop without the victim noticing, VNC like module.
pwgrab64 - harvests saved user credentials from browsers, registry keys, and other programs such as Outlook.
mailsearcher64 - searches all files on disk and compares their extensions to a predefined list.
wormDll64 - used for propagation of the malware, to self-replicate and spread on the network using the SMB vulnerability.

The bad news for this forensic case was that the various modules had been downloaded and used by the threat actor, meaning several different malicious events had occurred.

Conclusion, Mitigation and IOCs

Understanding of the full expanse of Trickbot has taken quite some time both for the team and in the wider community. The use of PowerShell to evade detection is a technique used by APTs and is known to be difficult to monitor without the right security controls. However, while stealthily dropped as polymorphic packed executables, the artefacts, behaviour and network callouts themselves do give indication of the infection. With the use of MITRE Attack analysis to map the Trickbot malware stages, it is demonstrated where monitoring and protection can be enhanced at each level to pick up on Trickbot events in security hardening, a SIEM or logging centre.



Malware Analysis

Initial Access - Email Delivery

Execution - Macro code runs encoded PowerShell to perform payload download

Persistence - PowerShell cradle drops packed Trickbot Autoruns written to Windows CurrentVersion\Run.

Defense Evasion - Trickbot disables Win Defender and McAfee via service config: /c sc delete WinDefend

Defense Evasion - Malicious modules are reflectively injected into legitimate processes such as svchost

Lateral Movement - SMB/RDP/PSEXEC malware spread using the DLL modules

Command and Control - Account enumeration, password grab, obtain priv accounts, remote access

Impact - Ransomware RYUK - most valuable servers

16

The New York Times

Hit by Ransomware Attack, Florida City Agrees to Pay Hackers $600,000

The city council in Riviera Beach, Fla., voted quietly to authorize a nearly $600,000 ransom payment after hackers paralyzed the city's computer systems.
Wilfredo Lee/Associated Press

[xii] The Trickbot stages mapped to MITRE Attack framework stages i.e. persistence. Slide from Jisc 2019 Security Conference presentation, including the reference to U.S. federal depts affected by Trickbot and RYUK ransomware.

One of the chief concerns involved is the RYUK ransomware exploit being dropped by Trickbot a very damaging strain of ransomware and we are aware of cases where this occurred. The following defensive options can be deployed to detect and mitigate Trickbot malware attacks:

> Trickbot is spread through malicious attachments, if policy is set to disable macros across the environment [9], this can help to prevent the initial delivery of this and other malware.

> Monitoring and logging PowerShell events on Windows is good practice and works best with endpoints having PowerShell 5.0 installed. Both Script Blocks logging and Module logging are the auditing options to set. See PowerShell Auditing in the appendix. Event ID 4104 will be your best bet to catch malicious activity in PowerShell 5 or use Event ID 500 and 800 in PowerShell 4 and lower and Event ID 4688 New Process Creation with Process Command Line enabled in all versions of Windows. Sending/Forwarding these to central logging would be best too, especially for servers.

Install Next Gen Behavioural based AV or additional AV capabilities not based on signatures but files and processes themselves. Because malware such as this is polymorphic, with different file signatures on each download, also running AV shutdown from PowerShell and performing stealth process injection it is evasive. Modern AV solutions use behavioural analytics, looking for suspicious behaviours such as rogue svchost.exe creation. They can stop this process injection and flag it.

IDS solutions, with network signatures. While it's difficult for AV to trace polymorphic packec malware, IDS solutions such as Bro/Zeek now include integration with JA3 for SSL string hashes to match Trickbot traffic **https://github.com/salesforce/ja3**.

Preventing lateral movement with network segmentation, restrictions per segment on port 445 and avoiding PSExec rights on machines. Disable old protocol SMBv1 from any usage.

Trickbot Investigation IOCs

BRO IPs with ports as listed above:
197.232.50.85:443
41.211.9.234:449
5.135.202.105:443
182.50.64.148:449
192.243.101.134:443

Trickbot sends HTTP requests to the following websites to determine the infected host's public IF address [4]:
hxxp://myexternalip.com/raw
hxxp://api.ipify.org
hxxp://icanhazip.com
hxxp://bot.whatismyipaddress.com
hxxp://ip.anysrc.net/plain/clientip
hxxp://ipecho.net/plain
hxxp://ipinfo.io/ip
Ja3 SSL Bro fingerprint match: 6734f37431670b3ab4292b8f60f29984
This is a new field but security teams using Bro can enable Ja3 SSL hash strings, to identify when matching Trickbot SSL communications are occurring.
Svchost.exe processes running from unexpected folder locations indicate process injection into run malicious code and processes.

Folder names of Trickbot infection:

Username\Appdata\Roaming\smectr

Username\Appdata\Roaming\vcmsd

Username\Appdata\Roaming\stsvc

Please refer back and credit the article in any use externally.

References:

[1] https://labs.sentinelone.com/the-deadly-planeswalker-how-the-trickbot-group-united-high-tech-crimeware-apt/ Vitali Kremez classifies Trickbot as a framework

[2] https://www.nytimes.com/2019/07/07/us/florida-ransom-hack.html News article

[3] https://arstechnica.com/information-technology/2019/11/hackers-paradise-louisianas-ransomware-disaster-far-from-over/ News article

[4] https://www.app.com/story/news/health/2019/12/13/hackensack-meridian-ransom-hackers-cyber-attack-hospitals/2638701001/ News article

[5] https://twitter.com/MsftSecIntel/status/984601317669715968?s=20 Microsoft intelligence on CVE-2017-0199 threat

[6] https://unit42.paloaltonetworks.com/wireshark-tutorial-examining-trickbot-infections/ Wireshark traffic port 449 shown

[7] https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Trojan:Win32/Trickbot&threatId=-2147244282 Windows advisory Trojan:Win32/Trickbot

[8] https://www.cisecurity.org/white-papers/security-primer-trickbot/ **Full DLL breakdown and behaviour**

[9] https://attack.mitre.org/software/S0266/ MITRE ATTACK Trickbot

[10] Practical Malware Analysis, Michael Sikorski and Andrew Honig p.17

[11] https://www.fireeye.com/blog/threat-research/2019/01/a-nasty-trick-from-credential-theft-malware-to-business-disruption.html **Group Tags**

[12] https://www.cybereason.com/blog/triple-threat-emotet-deploys-trickbot-to-steal-data-spread-ryuk-ransomware Full Triple Threat article with DLLs listed.

Appendix

PowerShell Auditing from Microsoft guidelines and FireEye

https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt...

Enable module logging.

Enable script block logging.

Windows Full Audit logging**. You must have Audit Process Creation auditing enabled to see event ID 4688 which is PowerShell Process creation.**

To enable the Audit Process Creation policy, edit the following group policy:

Policy location: Computer Configuration > Policies > Windows Settings > Security Settings > Advanced Audit Configuration > Detailed Tracking

Policy Name: Audit Process Creation

Emotet: A quick explanation of Emotet – it too arrives via email malspam infected attachments and malicious URLs and injects malicious code into explorer.exe and other running processes. Emotet artefacts are typically found in arbitrary paths located off of the Username\AppData\Local and Username\AppData\Roaming directories and mimicking names c known executables. Persistence is typically maintained through scheduled tasks or via registry keys.

Further Reading

https://www.fortinet.com/blog/threat-research/deep-analysis-of-the-online-banking-botnet-trickbot.html

Contains decrypted parameters Trickbot collects through forms and server responses.

https://www.malware-traffic-analysis.net/2018/08/07/index2.html

Trickbot Jumping laterally to a Domain Controller.

https://posts.specterops.io/offensive-lateral-movement-1744ae62b14f?gi=73b8345024a7

Offensive PowerShell, WMI, PSExec lateral movement and Cobalt Strike

*/

#CSIRT #SECURITY #INFOSEC