Malware Analysis Report

SOC ACADEMY

Prepared by GROUP 4

Group Members

1. Adebisi Mololuwa
2. Aderinola Kehinde
3. Oghenetejiri Brume
4. Comfort Ukangwobia
5. Nwobodo Chigozie
6. Moses Aleka
7. Gyekye Ampofo
8. Odunayo Balogun
9. Victoria Simon

Executive Summary

A suspicious file was identified on a company workstation, triggering a malware analysis to assess its behavior and potential impact. Through static analysis, the file was found to display multiple indicators of malicious activity, including abnormal file properties, unexpected library dependencies, and hidden or irregular data structures. These initial red flags were validated by dynamic analysis, which revealed that the file engages in harmful operations such as creating or modifying files, altering system registry keys, and attempting to connect with external servers. It also initiates additional processes and incorporates persistence techniques to maintain its presence on the system. Collectively, these behaviors confirm the file as malware, posing a serious threat to system security and data confidentiality.

Static Analysis

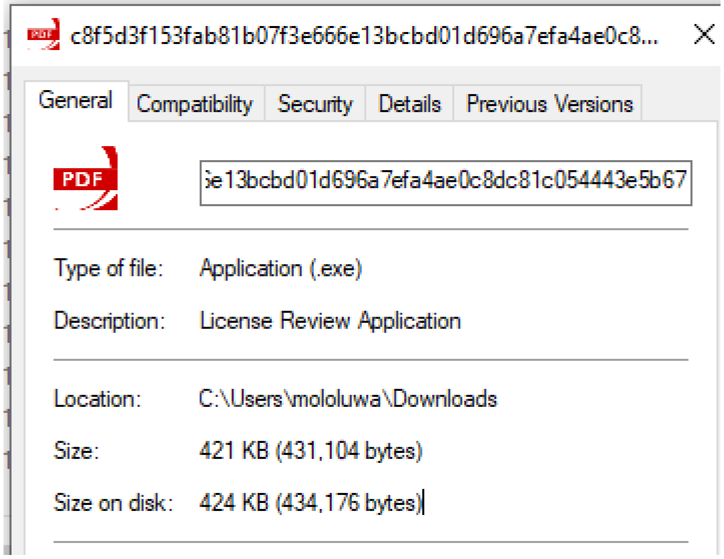
Static analysis is the process of analyzing a file, program, or code without running it to detect signs of malicious behavior, suspicious structures, or potential vulnerabilities. It involves inspecting elements like file metadata, strings, libraries, and code logic to assess risk before execution, and single out indicators of Compromise (Iocs)

Initial Examination

Starting off with metadata analysis by simply inspecting the properties of the file we can see that the file type is an application file with the .exe extension making it an executable application file

And in the description it says that it is a license review application

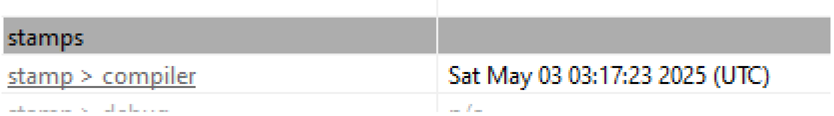
The size of the file is 421kb(431,104 bytes)but the size on disk is 424kb (434,176 bytes)
This doesn’t indicate much as the slight difference in size is probably due to how disk storage is allocated



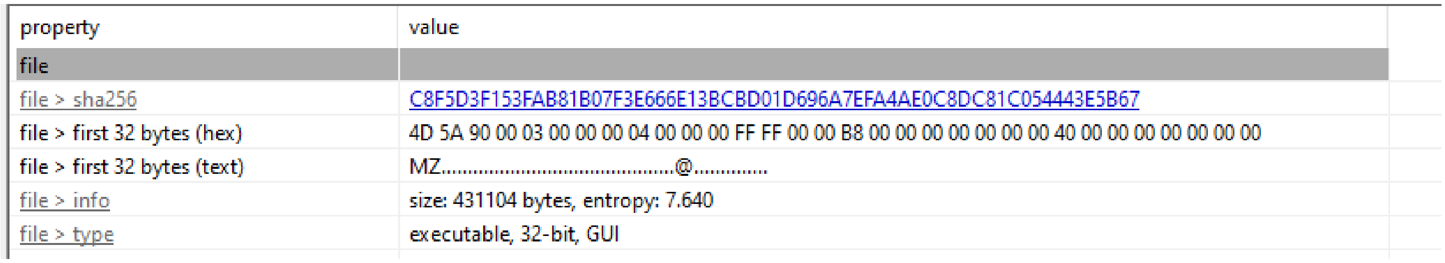
ͻe13bcbd01d696a7efa4ae0c8dc81c054443e5b67

Type of file:	Application (.exe)
Description:	License Review Application
Location:	C:\Users\mololuwa\Downloads
Size:	421 KB (431,104 bytes)
Size on disk:	424 KB (434,176 bytes)

Also using pestudio I was able to find the compilation date of the file to be may 03 2025 Also it showed a high entropy of 7.640 which indicates that the file is probably obfuscated also more information about the file type was uncovered with pe studio here we can see that it is a 32 bit executable file with a gui



stamps	
stamp > compiler	Sat May 03 03:17:23 2025 (UTC)

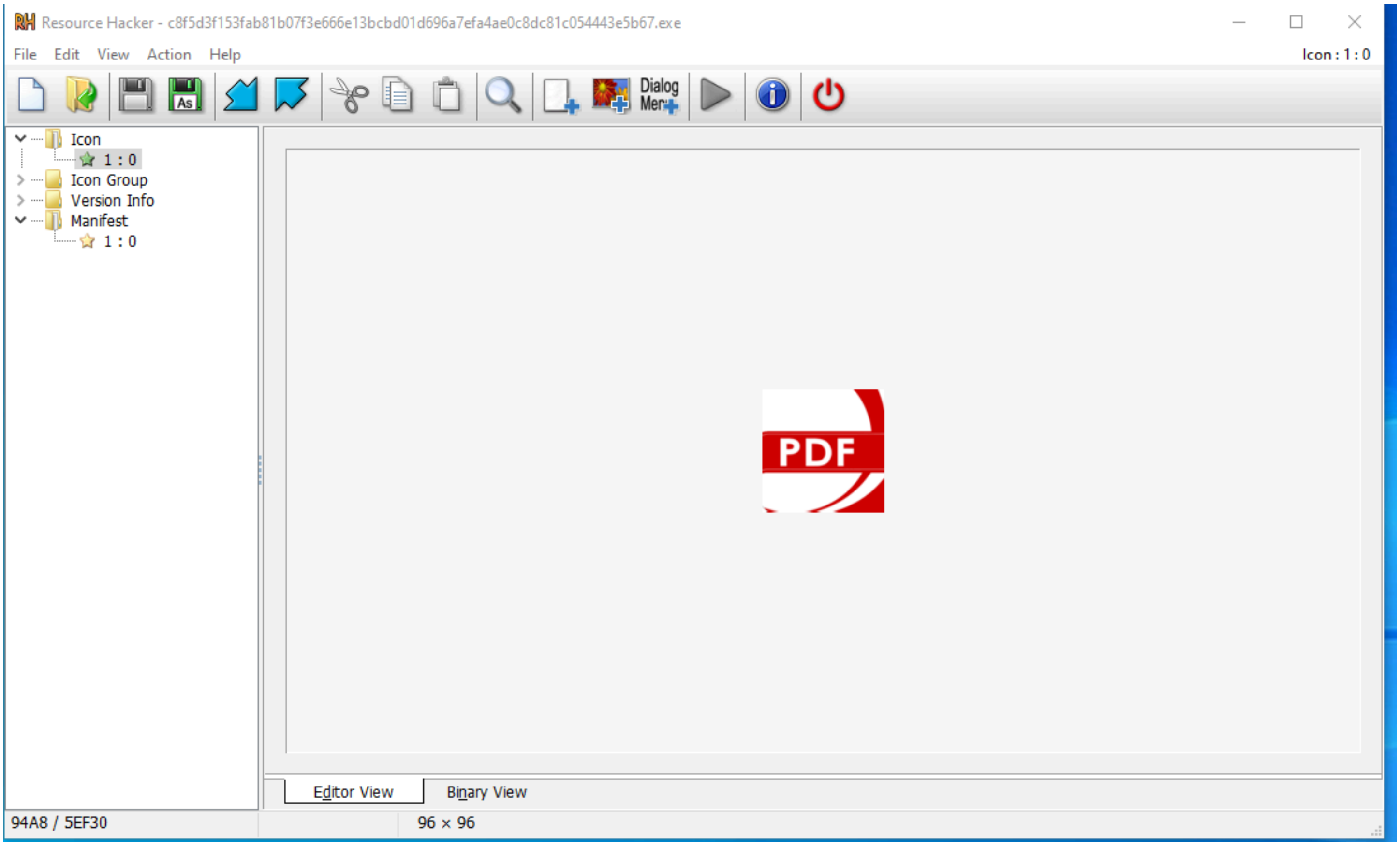


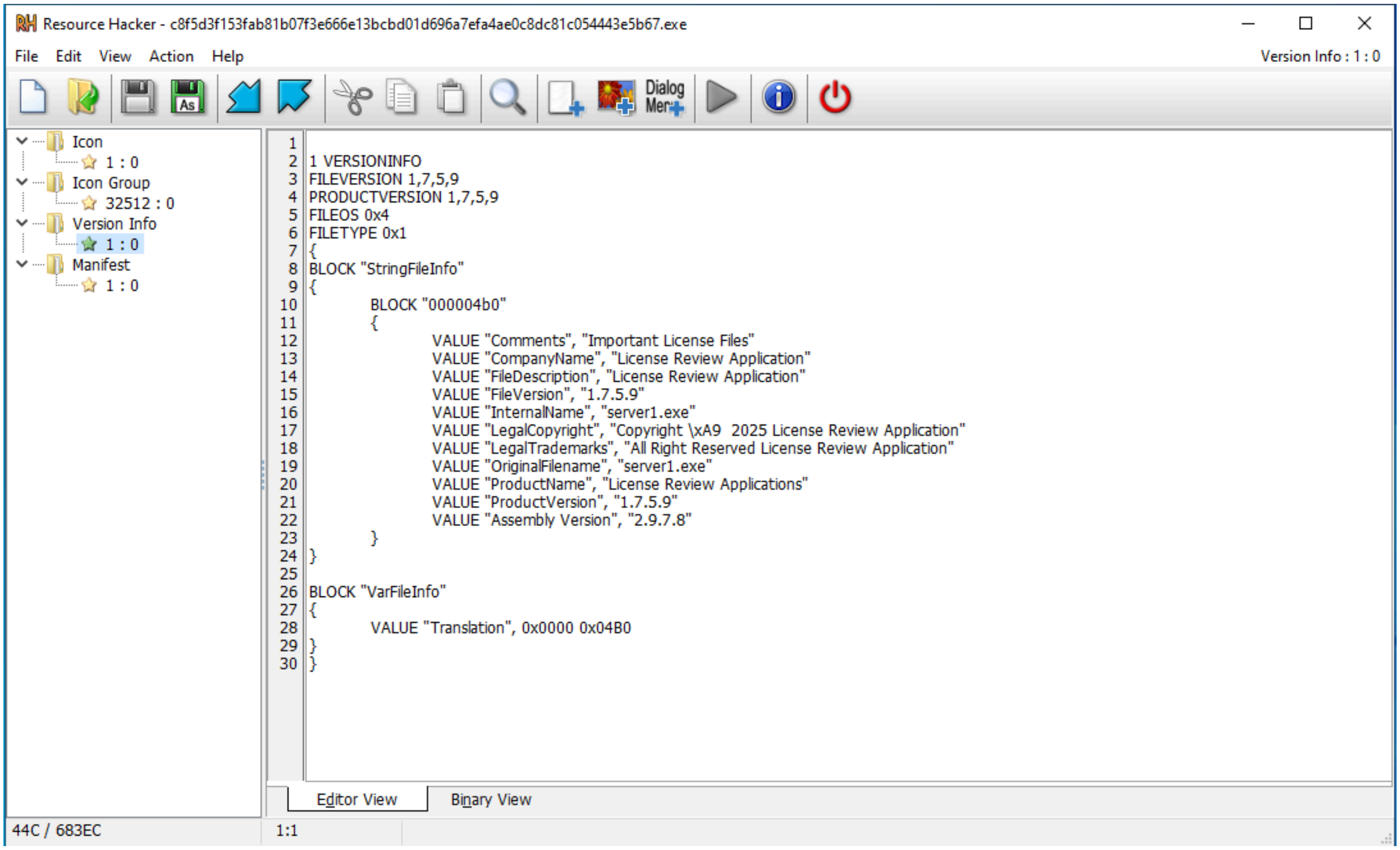
property	value
file	
file > sha256	C8F5D3F153FAB81B07F3E666E13BCBD01D696A7EFA4AE0C8DC81C054443E5B67
file > first 32 bytes (hex)	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
file > first 32 bytes (text)	MZ..@..............
file > info	size: 431104 bytes, entropy: 7.640
file > type	executable, 32-bit, GUI

Resource Hacker was utilized to explore the file's internal components, including icons, version details, and any embedded data. The analysis uncovered several suspicious elements, such as

- A deceptive PDF-style icon embedded in the executable — a classic social engineering technique used to trick users into believing the file is a legitimate document.

- An unusual icon and version information labeling the file as a “License Review Application,” with server1.exe listed as both the original and internal filename.





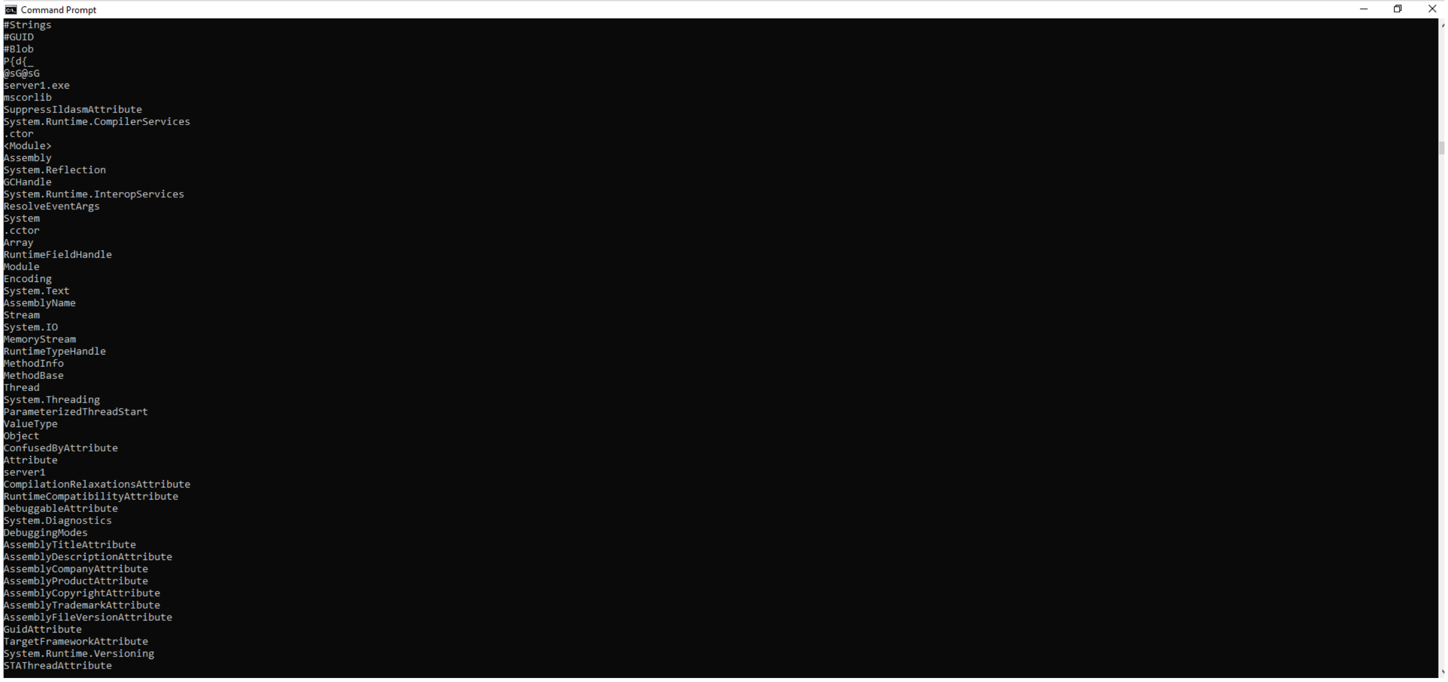
```

1 VERSIONINFO
FILEVERSION 1,7,5,9
PRODUCTVERSION 1,7,5,9
FILEOS 0x4
FILETYPE 0x1
{
BLOCK "StringFileInfo"
{
	BLOCK "000004b0"
	{
		VALUE "Comments", "Important License Files"
		VALUE "CompanyName", "License Review Application"
		VALUE "FileDescription", "License Review Application"
		VALUE "FileVersion", "1.7.5.9"
		VALUE "InternalName", "server1.exe"
		VALUE "LegalCopyright", "Copyright \xA9  2025 License Review Application"
		VALUE "LegalTrademarks", "All Right Reserved License Review Application"
		VALUE "OriginalFilename", "server1.exe"
		VALUE "ProductName", "License Review Applications"
		VALUE "ProductVersion", "1.7.5.9"
		VALUE "Assembly Version", "2.9.7.8"
	}
}

BLOCK "VarFileInfo"
{
	VALUE "Translation", 0x0000 0x04B0
}
}
```

Strings Analysis

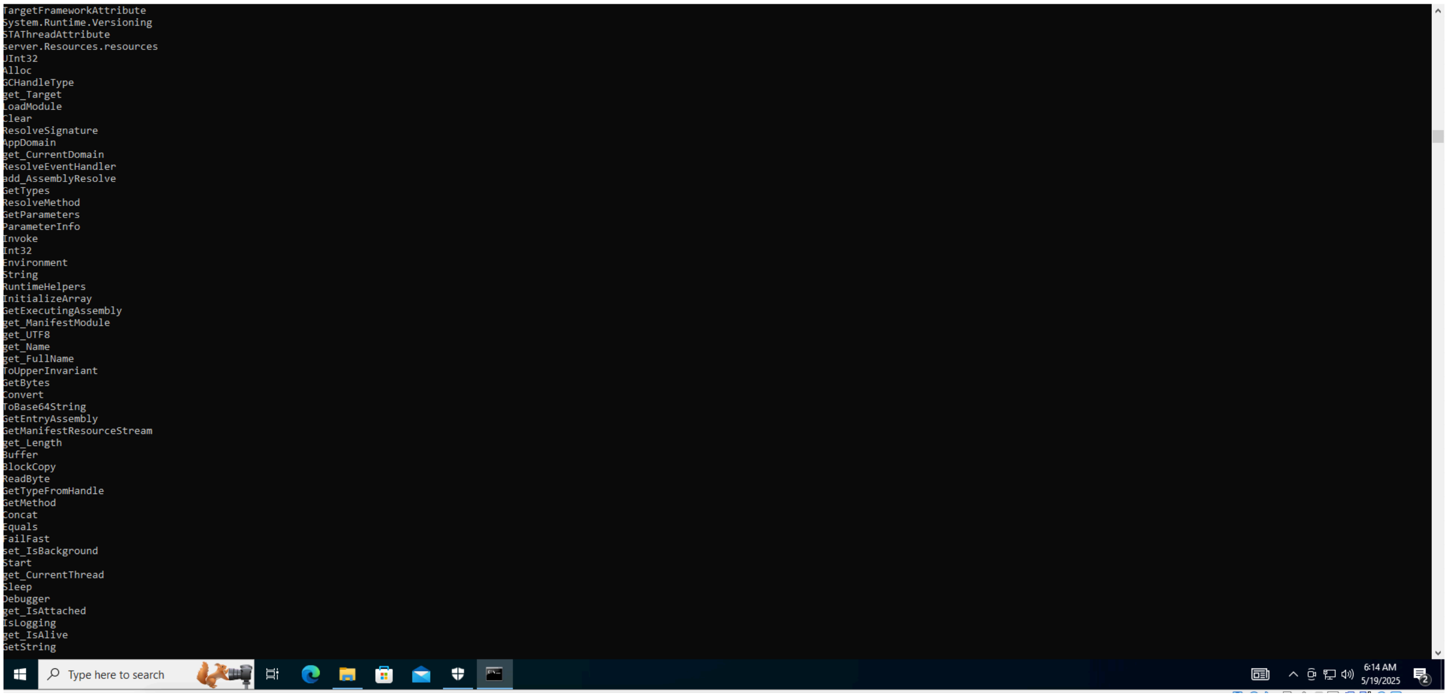
Running the strings tool on the malware sample revealed several indicators of potentially malicious behavior. The file is an executable, and the extracted strings suggest the use of obfuscation and reflection techniques. Key indicators include:

- **Base64String** : Shows the malware uses Base64 encoding to hide data or code from easy detection.
- **AppDomain:** A .NET feature that lets malware load and run code separately to stay hidden.
- **AssemblyResolve**: Used to load hidden code or modules during runtime, making detection harder.
- **FailFast:** Makes the program crash immediately to avoid being analyzed or debugged.
- **GCHandle:** Helps the malware keep code in memory to run it without leaving traces on disk.

These indicators reflect common malware tactics like code obfuscation, dynamic loading, and anti-analysis measures designed to avoid detection and maintain persistence.



```
#Strings
#GUID
#Blob
P{d{_
@sG@sG
server1.exe
mscorlib
SuppressIldasmAttribute
System.Runtime.CompilerServices
.ctor
<Module>
Assembly
System.Reflection
GCHandle
System.Runtime.InteropServices
ResolveEventArgs
System
.cctor
Array
RuntimeFieldHandle
Module
Encoding
System.Text
AssemblyName
Stream
System.IO
MemoryStream
RuntimeTypeHandle
MethodInfo
MethodBase
Thread
System.Threading
ParameterizedThreadStart
ValueType
Object
ConfusedByAttribute
Attribute
server1
CompilationRelaxationsAttribute
RuntimeCompatibilityAttribute
DebuggableAttribute
System.Diagnostics
DebuggingModes
AssemblyTitleAttribute
AssemblyDescriptionAttribute
AssemblyCompanyAttribute
AssemblyProductAttribute
AssemblyCopyrightAttribute
AssemblyTrademarkAttribute
AssemblyFileVersionAttribute
GuidAttribute
TargetFrameworkAttribute
System.Runtime.Versioning
STAThreadAttribute
```

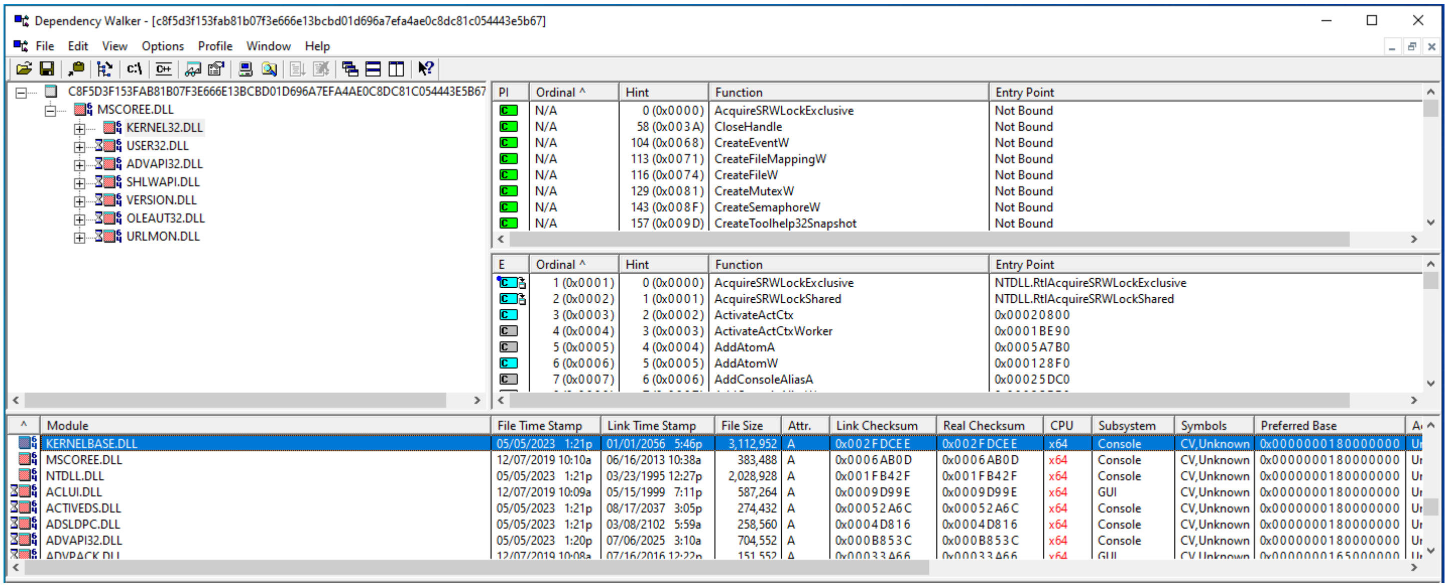


```
TargetFrameworkAttribute
System.Runtime.Versioning
STAThreadAttribute
server.Resources.resources
UInt32
Alloc
GCHandleType
get_Target
LoadModule
Clear
ResolveSignature
AppDomain
get_CurrentDomain
ResolveEventHandler
add_AssemblyResolve
GetTypes
ResolveMethod
GetParameters
ParameterInfo
Invoke
Int32
Environment
String
RuntimeHelpers
InitializeArray
GetExecutingAssembly
get_ManifestModule
get_UTF8
get_Name
get_FullName
ToUpperInvariant
GetBytes
Convert
ToBase64String
GetEntryAssembly
GetManifestResourceStream
get_Length
Buffer
BlockCopy
ReadByte
GetTypeFromHandle
GetMethod
Concat
Equals
FailFast
set_IsBackground
Start
get_CurrentThread
Sleep
Debugger
get_IsAttached
IsLogging
get_IsAlive
GetString
```

Dependencies Analysis

Dependency Walker was used to examine the libraries required by the malware "c8f5d3f153fab81b07f3e666e13bcbd01d696a7efa4ae0c8dc81c054443e5b67.exe"The analysis revealed the following dependencies:

- **ADVAPI32.DLL:** Used to access the registry and manage system services — common for persistence and privilege abuse.
- **KERNEL32.DLL:** Enables the malware to perform core system actions like file creation, memory management, and process execution.
- **URLMON.DLL:** Handles URL and file downloads, often used to fetch payloads or communicate with C2 servers.
- **MSCOREE.DLL**: Loads .NET assemblies, indicating the malware is a .NET executable with potential for obfuscation and dynamic code execution.



Dependency Walker - [c8f5d3f153fab81b07f3e666e13bcbd01d696a7efa4ae0c8dc81c054443e5b67]

```
C8F5D3F153FAB81B07F3E666E13BCBD01D696A7EFA4AE0C8DC81C054443E5B67
    MSCOREE.DLL
        KERNEL32.DLL
        USER32.DLL
        ADVAPI32.DLL
        SHLWAPI.DLL
        VERSION.DLL
        OLEAUT32.DLL
        URLMON.DLL
```

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	0 (0x0000)	AcquireSRWLockExclusive	Not Bound
C	N/A	58 (0x003A)	CloseHandle	Not Bound
C	N/A	104 (0x0068)	CreateEventW	Not Bound
C	N/A	113 (0x0071)	CreateFileMappingW	Not Bound
C	N/A	116 (0x0074)	CreateFileW	Not Bound
C	N/A	129 (0x0081)	CreateMutexW	Not Bound
C	N/A	143 (0x008F)	CreateSemaphoreW	Not Bound
C	N/A	157 (0x009D)	CreateToolhelp32Snapshot	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
C	1 (0x0001)	0 (0x0000)	AcquireSRWLockExclusive	NTDLL.RtlAcquireSRWLockExclusive
C	2 (0x0002)	1 (0x0001)	AcquireSRWLockShared	NTDLL.RtlAcquireSRWLockShared
C	3 (0x0003)	2 (0x0002)	ActivateActCtx	0x00020800
C	4 (0x0004)	3 (0x0003)	ActivateActCtxWorker	0x0001BE90
C	5 (0x0005)	4 (0x0004)	AddAtomA	0x0005A7B0
C	6 (0x0006)	5 (0x0005)	AddAtomW	0x000128F0
C	7 (0x0007)	6 (0x0006)	AddConsoleAliasA	0x00025DC0

^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	A
	KERNELBASE.DLL	05/05/2023 1:21p	01/01/2056 5:46p	3,112,952	A	0x002FDCEE	0x002FDCEE	x64	Console	CV,Unknown	0x0000000180000000	U
	MSCOREE.DLL	12/07/2019 10:10a	06/16/2013 10:38a	383,488	A	0x0006AB0D	0x0006AB0D	x64	Console	CV,Unknown	0x0000000180000000	U
	NTDLL.DLL	05/05/2023 1:21p	03/23/1995 12:27p	2,028,928	A	0x001FB42F	0x001FB42F	x64	Console	CV,Unknown	0x0000000180000000	U
	ACLUI.DLL	12/07/2019 10:09a	05/15/1999 7:11p	587,264	A	0x0009D99E	0x0009D99E	x64	GUI	CV,Unknown	0x0000000180000000	U
	ACTIVEDS.DLL	05/05/2023 1:21p	08/17/2037 3:05p	274,432	A	0x00052A6C	0x00052A6C	x64	Console	CV,Unknown	0x0000000180000000	U
	ADSLDPC.DLL	05/05/2023 1:21p	03/08/2102 5:59a	258,560	A	0x0004D816	0x0004D816	x64	Console	CV,Unknown	0x0000000180000000	U
	ADVAPI32.DLL	05/05/2023 1:20p	07/06/2025 3:10a	704,552	A	0x000B853C	0x000B853C	x64	Console	CV,Unknown	0x0000000180000000	U
	ADVPACK.DLL	12/07/2019 10:08a	07/16/2016 12:22p	151,552	A	0x00033A66	0x00033A66	x64	GUI	CV,Unknown	0x0000000165000000	U

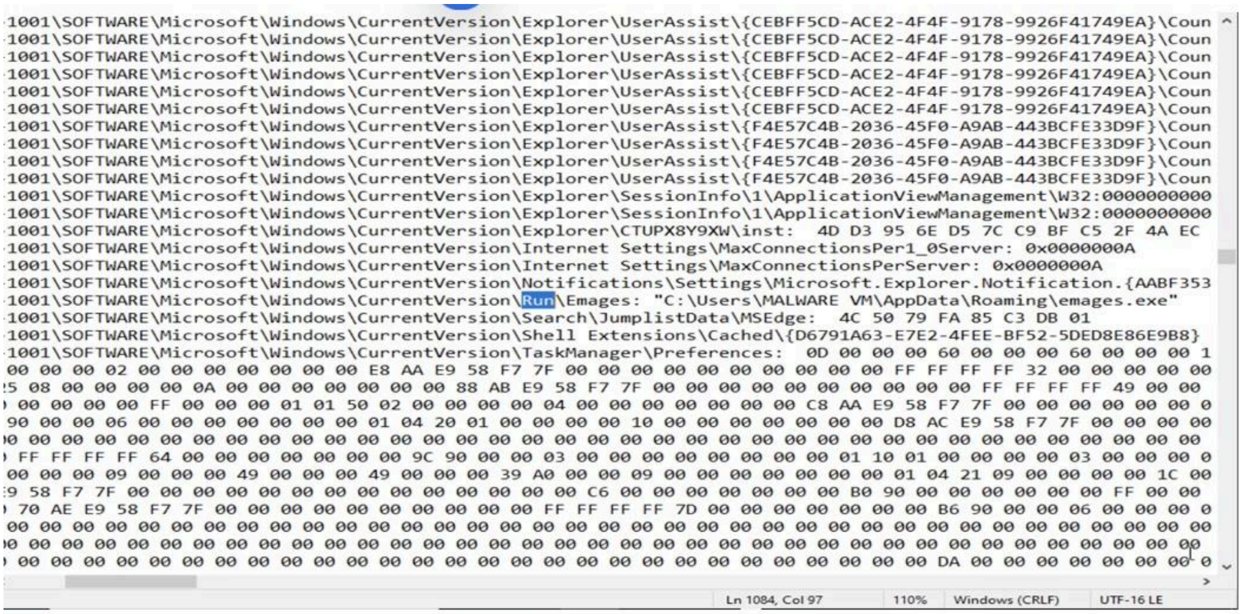
Dynamic Analysis

Dynamic analysis was performed by running the suspicious file in a secure, isolated environment to monitor its behavior and system interactions. This method reveals real-time actions the file attempts during execution, offering valuable insights into its malicious intent. The tools listed below were used to analyze the behavior of the malware. “c8f5d3f153fab81b07f3e666e13bcbd01d696a7efa4ae0c8dc81c054443e5b67.exe”:

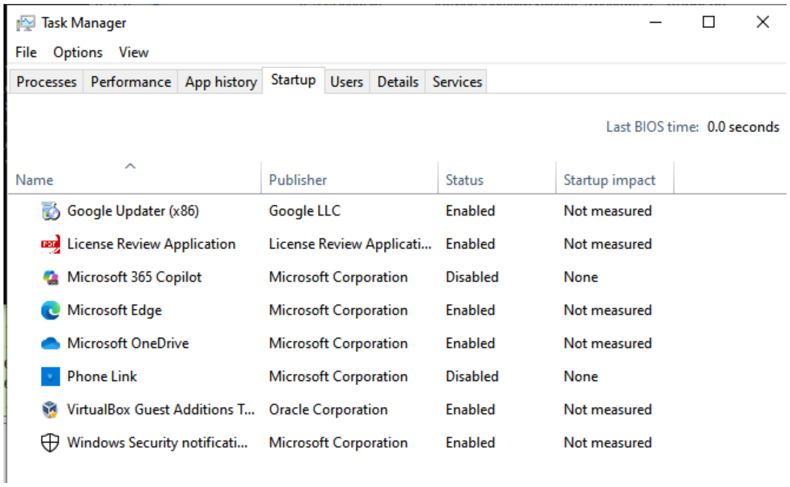
- ProcMon (Process Monitor)
- Regshot
- Wireshark
- FakeNet-NG

Behavioral Analysis

- **Registry Activity:** Regshot was utilized to take system registry snapshots before and after executing the malicious file,Comparing these snapshots revealed key changes, suggesting that the executable is attempting to establish persistence on the system.



```
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Coun
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Coun
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Coun
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Coun
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Coun
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Coun
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Coun
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Coun
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Coun
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}\Coun
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:0000000000
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\CTUPX8Y9XW\inst:  4D D3 95 6E D5 7C C9 BF C5 2F 4A EC
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\MaxConnectionsPer1_0Server: 0x0000000A
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\MaxConnectionsPerServer: 0x0000000A
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Notifications\Settings\Microsoft.Explorer.Notification.{AABF353
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Emages: "C:\Users\MALWARE VM\AppData\Roaming\emages.exe"
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\JumplistData\MSEdge:  4C 50 79 FA 85 C3 DB 01
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Shell Extensions\Cached\{D6791A63-E7E2-4FEE-BF52-5DED8E86E9B8}
1001\SOFTWARE\Microsoft\Windows\CurrentVersion\TaskManager\Preferences:  0D 00 00 00 60 00 00 00 60 00 00 00 1
00 00 00 02 00 00 00 00 00 00 00 E8 AA E9 58 F7 7F 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 32 00 00 00 00 00
5 08 00 00 00 00 0A 00 00 00 00 00 00 00 88 AB E9 58 F7 7F 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 49 00 00
 00 00 00 00 FF 00 00 00 01 01 50 02 00 00 00 00 04 00 00 00 00 00 00 00 C8 AA E9 58 F7 7F 00 00 00 00 00 00 0
90 00 00 06 00 00 00 00 00 00 00 01 04 20 01 00 00 00 00 10 00 00 00 00 00 00 00 D8 AC E9 58 F7 7F 00 00 00 00
0 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
 FF FF FF FF 64 00 00 00 00 00 00 00 9C 90 00 00 03 00 00 00 00 00 00 00 01 10 01 00 00 00 00 03 00 00 00 0
00 00 00 09 00 00 00 49 00 00 00 49 00 00 00 39 A0 00 00 09 00 00 00 00 00 00 00 01 04 21 09 00 00 00 00 1C 00
9 58 F7 7F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 C6 00 00 00 00 00 00 00 B0 90 00 00 00 00 00 00 FF 00 00
 70 AE E9 58 F7 7F 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 7D 00 00 00 00 00 00 00 B6 90 00 00 06 00 00 00 0
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
0 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 00 00 00 00 00 00 00 00 00 00 DA 00 00 00 00 00 00 00 00 0
```


Task Manager
File Options View
Processes Performance App history Startup Users Details Services

Last BIOS time: 0.0 seconds

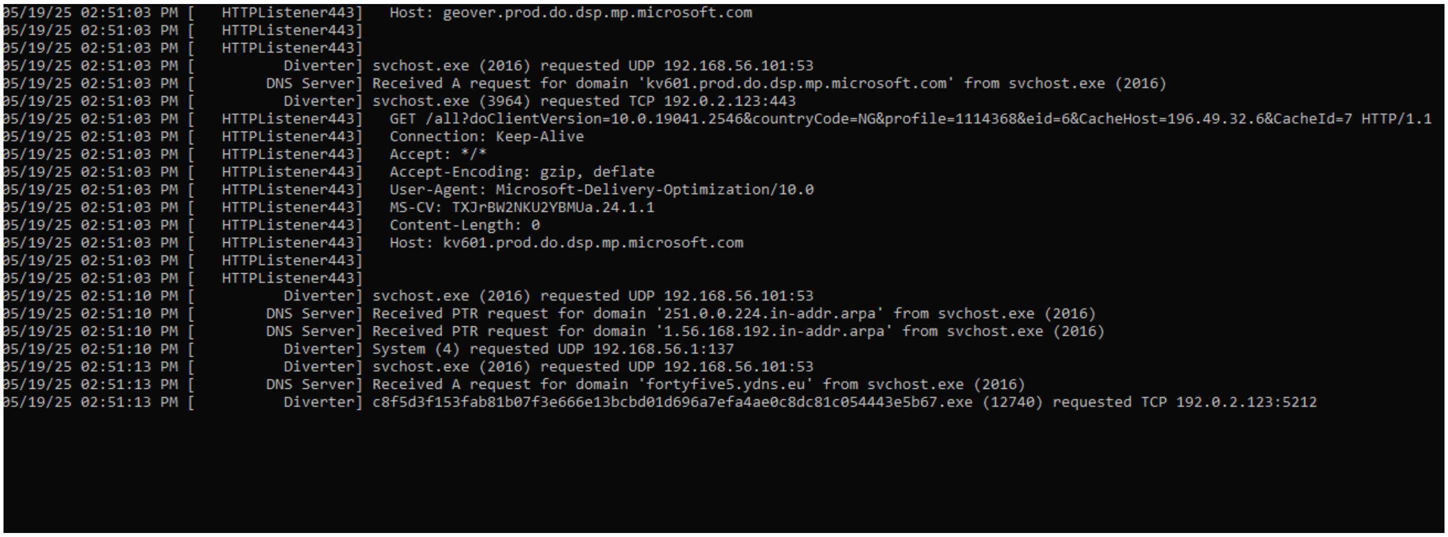
Name	Publisher	Status	Startup impact
Google Updater (x86)	Google LLC	Enabled	Not measured
License Review Application	License Review Applicati...	Enabled	Not measured
Microsoft 365 Copilot	Microsoft Corporation	Disabled	None
Microsoft Edge	Microsoft Corporation	Enabled	Not measured
Microsoft OneDrive	Microsoft Corporation	Enabled	Not measured
Phone Link	Microsoft Corporation	Disabled	None
VirtualBox Guest Additions T...	Oracle Corporation	Enabled	Not measured
Windows Security notificati...	Microsoft Corporation	Enabled	Not measured

The Startup tab in Task Manager shows that the suspicious "License Review Application" which is the malware is enabled, suggesting it is configured to launch at system boot, so as to achieve persistence

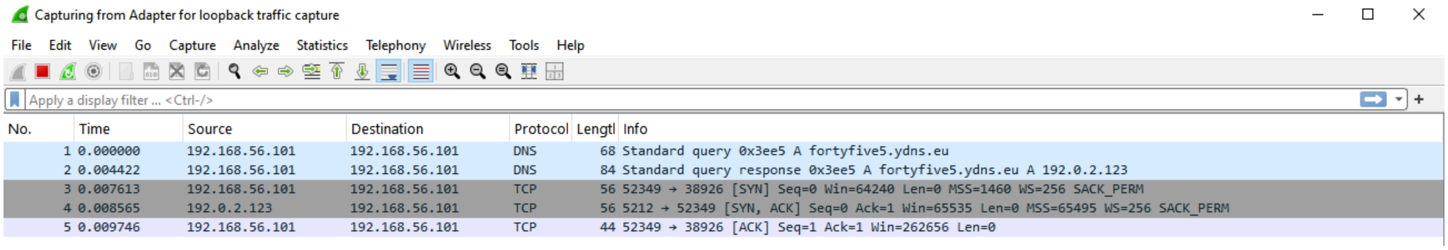
Network Analysis

Wireshark and fakenet ng was used to monitor network activity after successfully executing the malware, Wireshark was used to monitor network activity for any suspicious activity while fakenet was used to simulate a network environment and intercept network requests initiated by the malware "c8f5d3f153fab81b07f3e666e13bcbd01d696a7efa4ae0c8dc81c054443e5b67.exe"

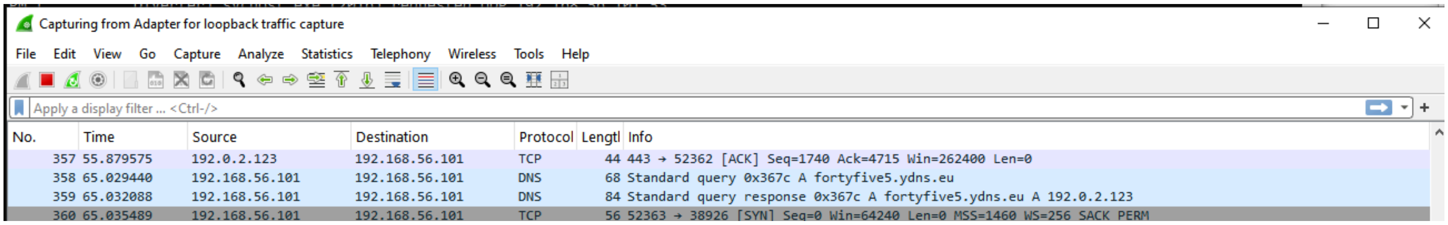
Through the combination of both we were able to identify multiple suspicious dns requests to the domain "fiftyfive5.ydns.eu."



```
05/19/25 02:51:03 PM [   HTTPListener443]   Host: geover.prod.do.dsp.mp.microsoft.com
05/19/25 02:51:03 PM [   HTTPListener443]
05/19/25 02:51:03 PM [   HTTPListener443]
05/19/25 02:51:03 PM [          Diverter] svchost.exe (2016) requested UDP 192.168.56.101:53
05/19/25 02:51:03 PM [        DNS Server] Received A request for domain 'kv601.prod.do.dsp.mp.microsoft.com' from svchost.exe (2016)
05/19/25 02:51:03 PM [          Diverter] svchost.exe (3964) requested TCP 192.0.2.123:443
05/19/25 02:51:03 PM [   HTTPListener443]   GET /all?doClientVersion=10.0.19041.2546&countryCode=NG&profile=1114368&eid=6&CacheHost=196.49.32.6&CacheId=7 HTTP/1.1
05/19/25 02:51:03 PM [   HTTPListener443]   Connection: Keep-Alive
05/19/25 02:51:03 PM [   HTTPListener443]   Accept: */*
05/19/25 02:51:03 PM [   HTTPListener443]   Accept-Encoding: gzip, deflate
05/19/25 02:51:03 PM [   HTTPListener443]   User-Agent: Microsoft-Delivery-Optimization/10.0
05/19/25 02:51:03 PM [   HTTPListener443]   MS-CV: TXJrBW2NKU2YBMUa.24.1.1
05/19/25 02:51:03 PM [   HTTPListener443]   Content-Length: 0
05/19/25 02:51:03 PM [   HTTPListener443]   Host: kv601.prod.do.dsp.mp.microsoft.com
05/19/25 02:51:03 PM [   HTTPListener443]
05/19/25 02:51:03 PM [   HTTPListener443]
05/19/25 02:51:10 PM [          Diverter] svchost.exe (2016) requested UDP 192.168.56.101:53
05/19/25 02:51:10 PM [        DNS Server] Received PTR request for domain '251.0.0.224.in-addr.arpa' from svchost.exe (2016)
05/19/25 02:51:10 PM [        DNS Server] Received PTR request for domain '1.56.168.192.in-addr.arpa' from svchost.exe (2016)
05/19/25 02:51:10 PM [          Diverter] System (4) requested UDP 192.168.56.1:137
05/19/25 02:51:13 PM [          Diverter] svchost.exe (2016) requested UDP 192.168.56.101:53
05/19/25 02:51:13 PM [        DNS Server] Received A request for domain 'fortyfive5.ydns.eu' from svchost.exe (2016)
05/19/25 02:51:13 PM [          Diverter] c8f5d3f153fab81b07f3e666e13bcbd01d696a7efa4ae0c8dc81c054443e5b67.exe (12740) requested TCP 192.0.2.123:5212
```


Capturing from Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Lengtl	Info
1	0.000000	192.168.56.101	192.168.56.101	DNS	68	Standard query 0x3ee5 A fortyfive5.ydns.eu
2	0.004422	192.168.56.101	192.168.56.101	DNS	84	Standard query response 0x3ee5 A fortyfive5.ydns.eu A 192.0.2.123
3	0.007613	192.168.56.101	192.168.56.101	TCP	56	52349 → 38926 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
4	0.008565	192.0.2.123	192.168.56.101	TCP	56	5212 → 52349 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM
5	0.009746	192.168.56.101	192.168.56.101	TCP	44	52349 → 38926 [ACK] Seq=1 Ack=1 Win=262656 Len=0


Capturing from Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

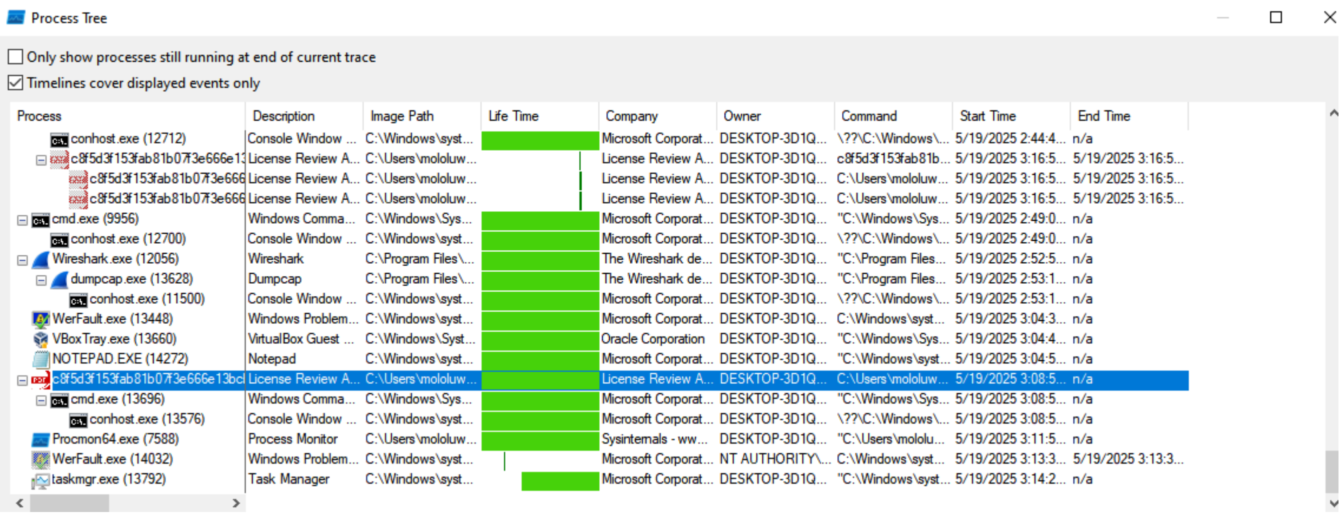
No.	Time	Source	Destination	Protocol	Lengtl	Info
357	55.879575	192.0.2.123	192.168.56.101	TCP	44	443 → 52362 [ACK] Seq=1740 Ack=4715 Win=262400 Len=0
358	65.029440	192.168.56.101	192.168.56.101	DNS	68	Standard query 0x367c A fortyfive5.ydns.eu
359	65.032088	192.168.56.101	192.168.56.101	DNS	84	Standard query response 0x367c A fortyfive5.ydns.eu A 192.0.2.123
360	65.035489	192.168.56.101	192.168.56.101	TCP	56	52363 → 38926 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK PERM

1. Captured DNS traffic shows repeated requests to the suspicious domain fiftyfive5.ydns.eu, with responses resolving to 192.0.2.123, a non-routable address used by FakeNet-NG for redirection. This behavior suggests the malware is attempting to simulate or initiate command and control (C2) communication.
2. This activity indicates that the malware is trying to initiate command and control (C2) communication with a remote host with domain “fiftyfive5.ydns.eu”

System Activity Analysis

Using Procmon we monitored the process list after executing the malware and we noticed a couple of indicators which revealed that

- New processes were spawned
- The process tree highlights multiple instances or the malware c8f5d3f153fab81b07f3e666e13bcbd01d696a7efa4ae0c8dc81c054443e5b67.exe repeatedly relaunching itself which in its own might suggest persistence

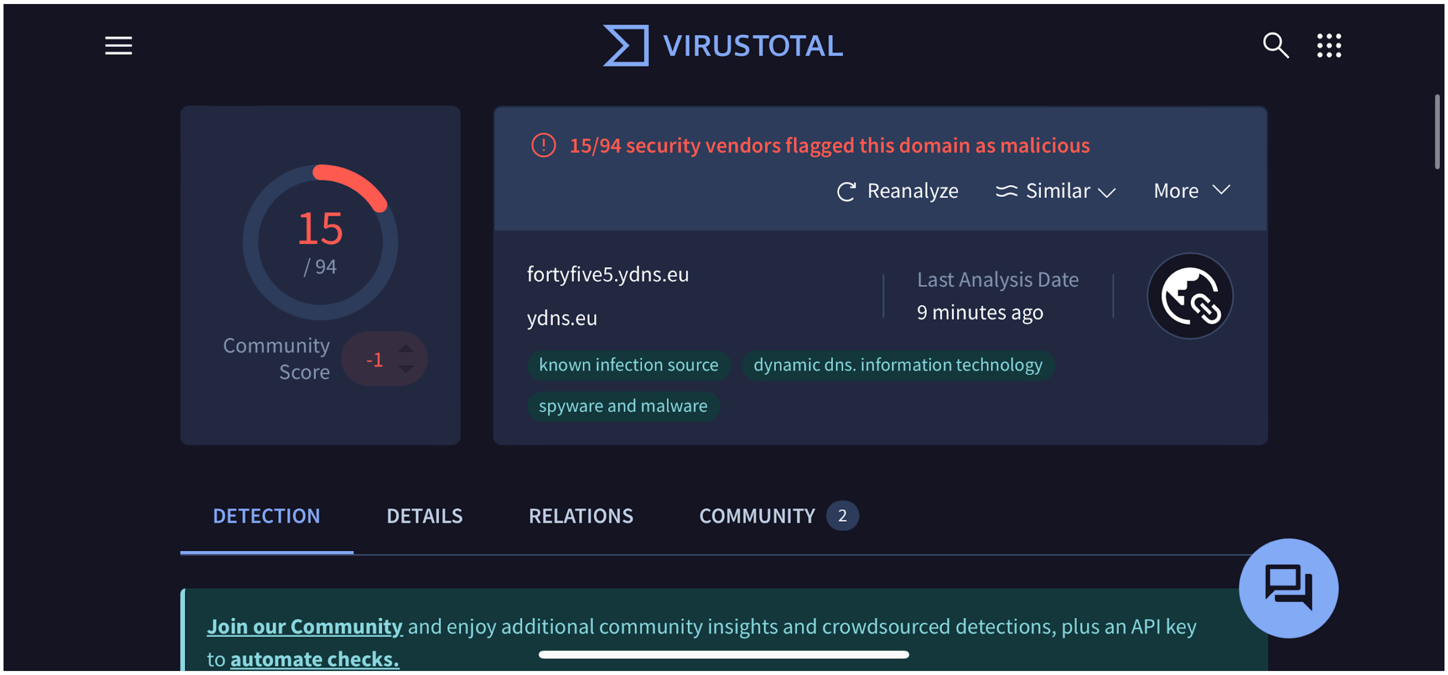


□ Only show processes still running at end of current trace

☑ Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company	Owner	Command	Start Time	End Time
conhost.exe (12712)	Console Window ...	C:\Windows\syst...	🟩	Microsoft Corporat...	DESKTOP-3D1Q...	\??\C:\Windows\...	5/19/2025 2:44:4...	n/a
c8f5d3f153fab81b07f3e666e13	License Review A...	C:\Users\mololuw...		License Review A...	DESKTOP-3D1Q...	c8f5d3f153fab81b...	5/19/2025 3:16:5...	5/19/2025 3:16:5...
c8f5d3f153fab81b07f3e666	License Review A...	C:\Users\mololuw...		License Review A...	DESKTOP-3D1Q...	C:\Users\mololuw...	5/19/2025 3:16:5...	5/19/2025 3:16:5...
c8f5d3f153fab81b07f3e666	License Review A...	C:\Users\mololuw...		License Review A...	DESKTOP-3D1Q...	C:\Users\mololuw...	5/19/2025 3:16:5...	5/19/2025 3:16:5...
cmd.exe (9956)	Windows Comma...	C:\Windows\Sys...	🟩	Microsoft Corporat...	DESKTOP-3D1Q...	"C:\Windows\Sys...	5/19/2025 2:49:0...	n/a
conhost.exe (12700)	Console Window ...	C:\Windows\syst...	🟩	Microsoft Corporat...	DESKTOP-3D1Q...	\??\C:\Windows\...	5/19/2025 2:49:0...	n/a
Wireshark.exe (12056)	Wireshark	C:\Program Files\...	🟩	The Wireshark de...	DESKTOP-3D1Q...	"C:\Program Files...	5/19/2025 2:52:5...	n/a
dumpcap.exe (13628)	Dumpcap	C:\Program Files\...	🟩	The Wireshark de...	DESKTOP-3D1Q...	"C:\Program Files...	5/19/2025 2:53:1...	n/a
conhost.exe (11500)	Console Window ...	C:\Windows\syst...	🟩	Microsoft Corporat...	DESKTOP-3D1Q...	\??\C:\Windows\...	5/19/2025 2:53:1...	n/a
WerFault.exe (13448)	Windows Problem...	C:\Windows\syst...	🟩	Microsoft Corporat...	DESKTOP-3D1Q...	C:\Windows\syst...	5/19/2025 3:04:3...	n/a
VBoxTray.exe (13660)	VirtualBox Guest ...	C:\Windows\Syst...	🟩	Oracle Corporation	DESKTOP-3D1Q...	"C:\Windows\Sys...	5/19/2025 3:04:4...	n/a
NOTEPAD.EXE (14272)	Notepad	C:\Windows\syst...	🟩	Microsoft Corporat...	DESKTOP-3D1Q...	"C:\Windows\syst...	5/19/2025 3:04:5...	n/a
c8f5d3f153fab81b07f3e666e13bc	License Review A...	C:\Users\mololuw...	🟩	License Review A...	DESKTOP-3D1Q...	C:\Users\mololuw...	5/19/2025 3:08:5...	n/a
cmd.exe (13696)	Windows Comma...	C:\Windows\Sys...	🟩	Microsoft Corporat...	DESKTOP-3D1Q...	"C:\Windows\Sys...	5/19/2025 3:08:5...	n/a
conhost.exe (13576)	Console Window ...	C:\Windows\syst...	🟩	Microsoft Corporat...	DESKTOP-3D1Q...	\??\C:\Windows\...	5/19/2025 3:08:5...	n/a
Procmon64.exe (7588)	Process Monitor	C:\Users\mololuw...	🟩	Sysinternals - ww...	DESKTOP-3D1Q...	"C:\Users\mololu...	5/19/2025 3:11:5...	n/a
WerFault.exe (14032)	Windows Problem...	C:\Windows\syst...		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\syst...	5/19/2025 3:13:3...	5/19/2025 3:13:3...
taskmgr.exe (13792)	Task Manager	C:\Windows\syst...	🟩	Microsoft Corporat...	DESKTOP-3D1Q...	"C:\Windows\syst...	5/19/2025 3:14:2...	n/a

The domain fortyfive5.ydns.eu was flagged as malicious by 15 security vendors VirusTotal



15
/ 94

Community Score -1

15/94 security vendors flagged this domain as malicious

fortyfive5.ydns.eu

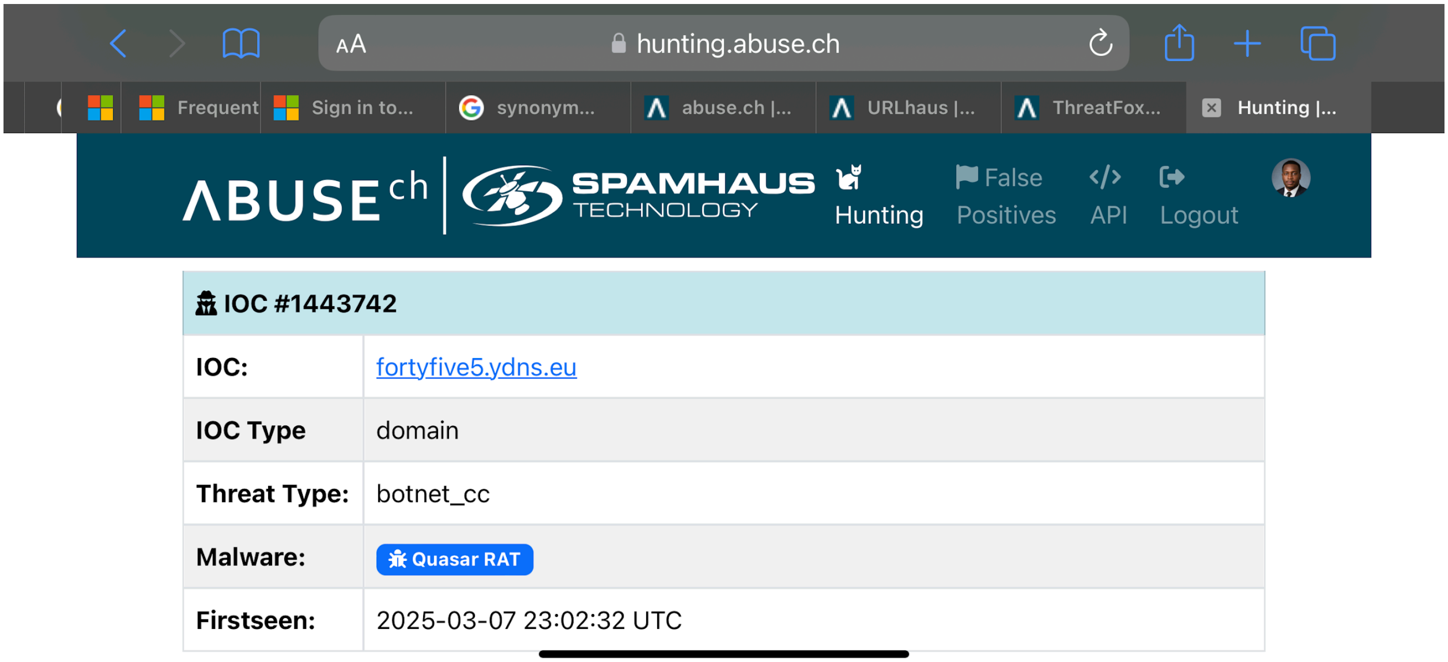
ydns.eu

Last Analysis Date
9 minutes ago

known infection source | dynamic dns. information technology | spyware and malware

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

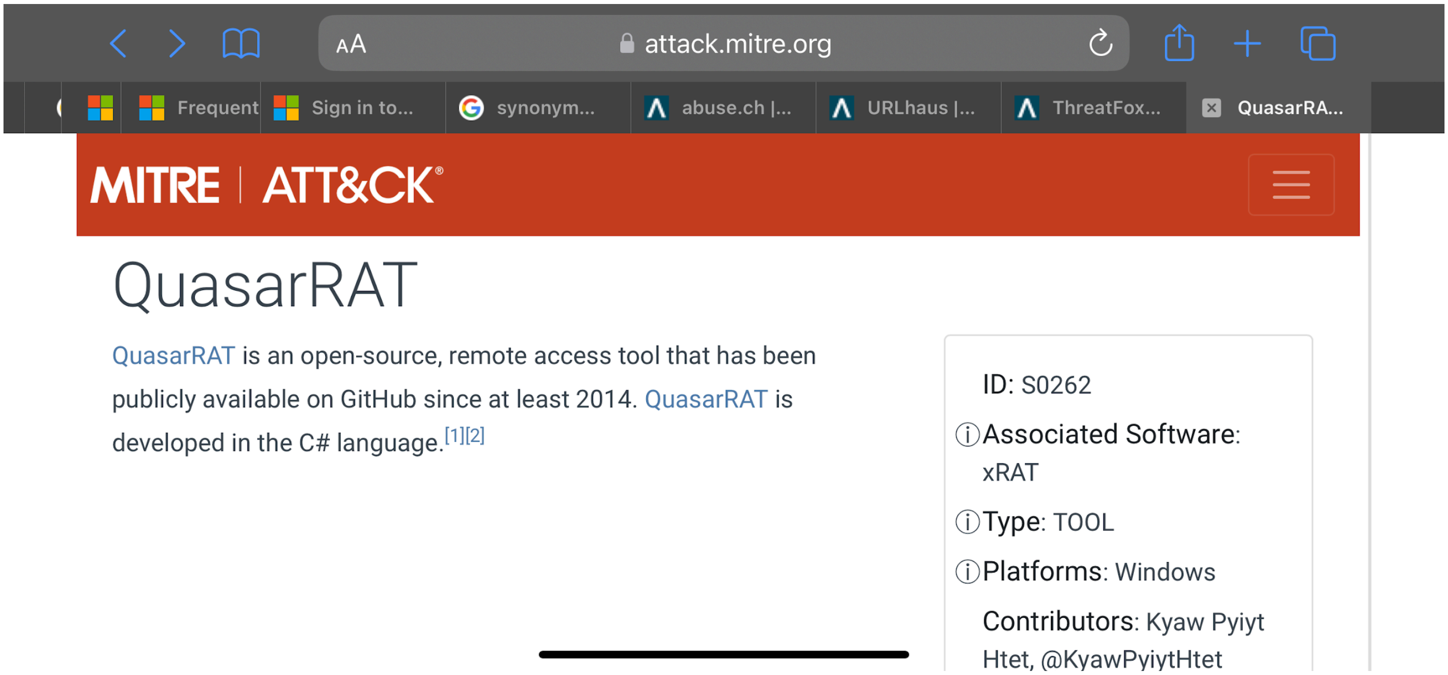
A lookup on fortyfive5.ydns.eu via Abuse.ch ThreatFox confirms its association with Quasar RAT and identifies it as an active botnet C2 server. Its classification under malware infrastructure validates the suspicious external network activity observed during local analysis.



IOC #1443742

IOC:	fortyfive5.ydns.eu
IOC Type	domain
Threat Type:	botnet_cc
Malware:	Quasar RAT
Firstseen:	2025-03-07 23:02:32 UTC

A MITRE ATT&CK screenshot highlights that QuasarRAT is a widely used, open-source remote access tool (ID: S0262) developed in C#. It has been employed by several known threat groups, including Patchwork (G0040), LazyScripter (G0140), Gorgon Group (G0078), Kimsuky (G0094), menuPass (G0045), and BackdoorDiplomacy (G0135), underscoring its prevalence in real-world cyberattacks.



QuasarRAT

QuasarRAT is an open-source, remote access tool that has been publicly available on GitHub since at least 2014. QuasarRAT is developed in the C# language.[1][2]

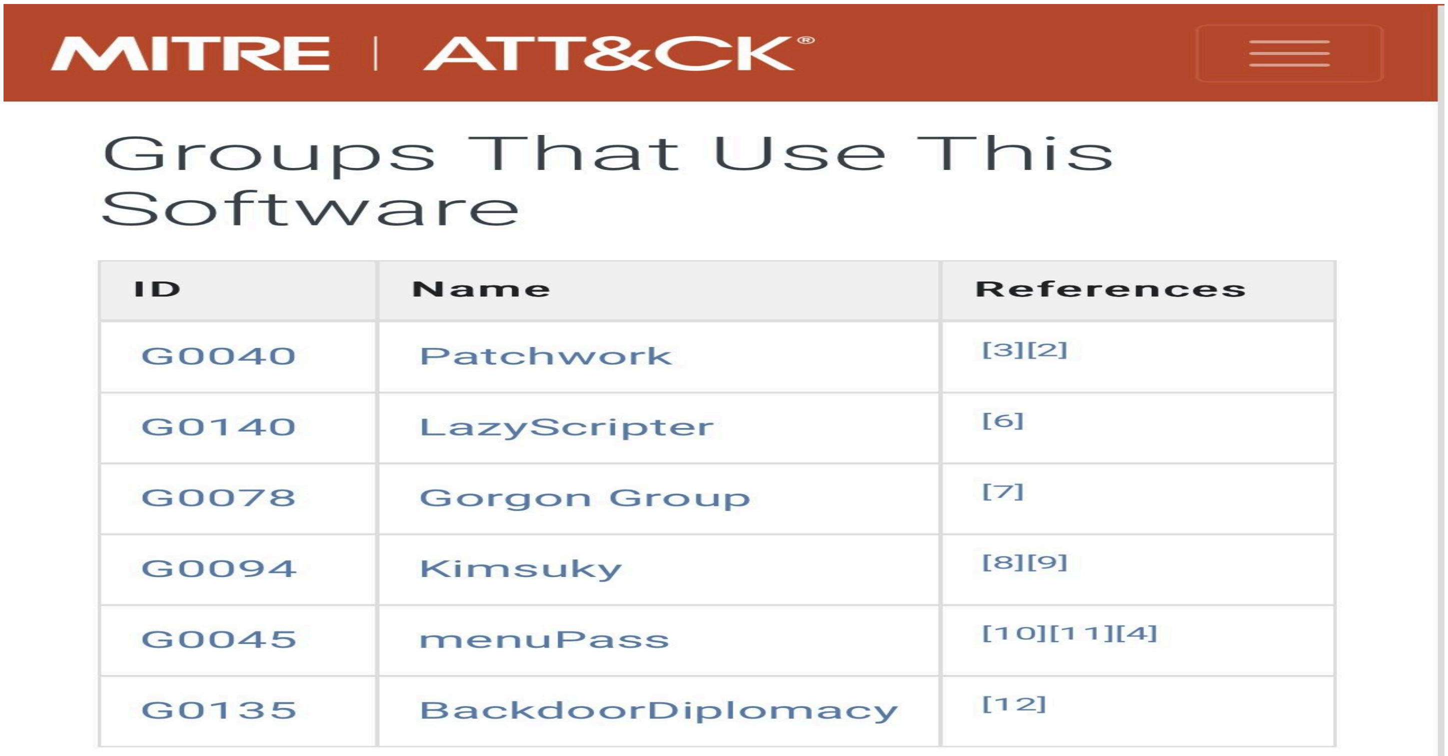
ID: S0262

ⓘAssociated Software: xRAT

ⓘType: TOOL

ⓘPlatforms: Windows

Contributors: Kyaw Pyiyt Htet, @KyawPyiytHtet



Groups That Use This Software

ID	Name	References
G0040	Patchwork	[3][2]
G0140	LazyScripter	[6]
G0078	Gorgon Group	[7]
G0094	Kimsuky	[8][9]
G0045	menuPass	[10][11][4]
G0135	BackdoorDiplomacy	[12]

Recommended Mitigation

- **Quarantine all affected systems:** Immediately disconnect the compromised workstation from the network to halt any ongoing malicious activity and prevent lateral movement.

- **Securely eliminate the malicious file**: Locate and permanently delete the file c8f5d3f153fab81b07f3e666e13bcbd01d696a7efa4ae0c8dc81c054443e5b67.exe, using secure deletion tools to ensure it cannot be recovered.

- **Conduct a comprehensive malware scan**: Run a full system scan using a trusted antivirus or EDR solution to uncover and remove any additional malicious components or artifacts.

- **Monitor and restrict network traffic:** Enable continuous network traffic analysis and apply firewall rules or DNS filtering to block connections to the identified C2 domain fiftyfive5.ydns.eu.

- **Apply critical system updates:** Ensure the operating system, software, and security tools are fully patched to mitigate known vulnerabilities and reduce the attack surface.

- **Initiate user awareness programs:** Provide regular training to employees on identifying phishing attempts, malicious attachments, and unsafe downloads.

- **Audit system and user activity logs:** Review Windows Event Logs and endpoint activity to identify any unusual behavior that may indicate further compromise.

- **Deploy endpoint detection and response (EDR):** Consider deploying EDR solutions for real-time threat detection, automated response, and deeper visibility into endpoint activities.