

## Summary:

While studying malware analysis, I came across an interesting malware sample. The story behind this malware is captivating, as it represents a real-world threat that was sent to a company.

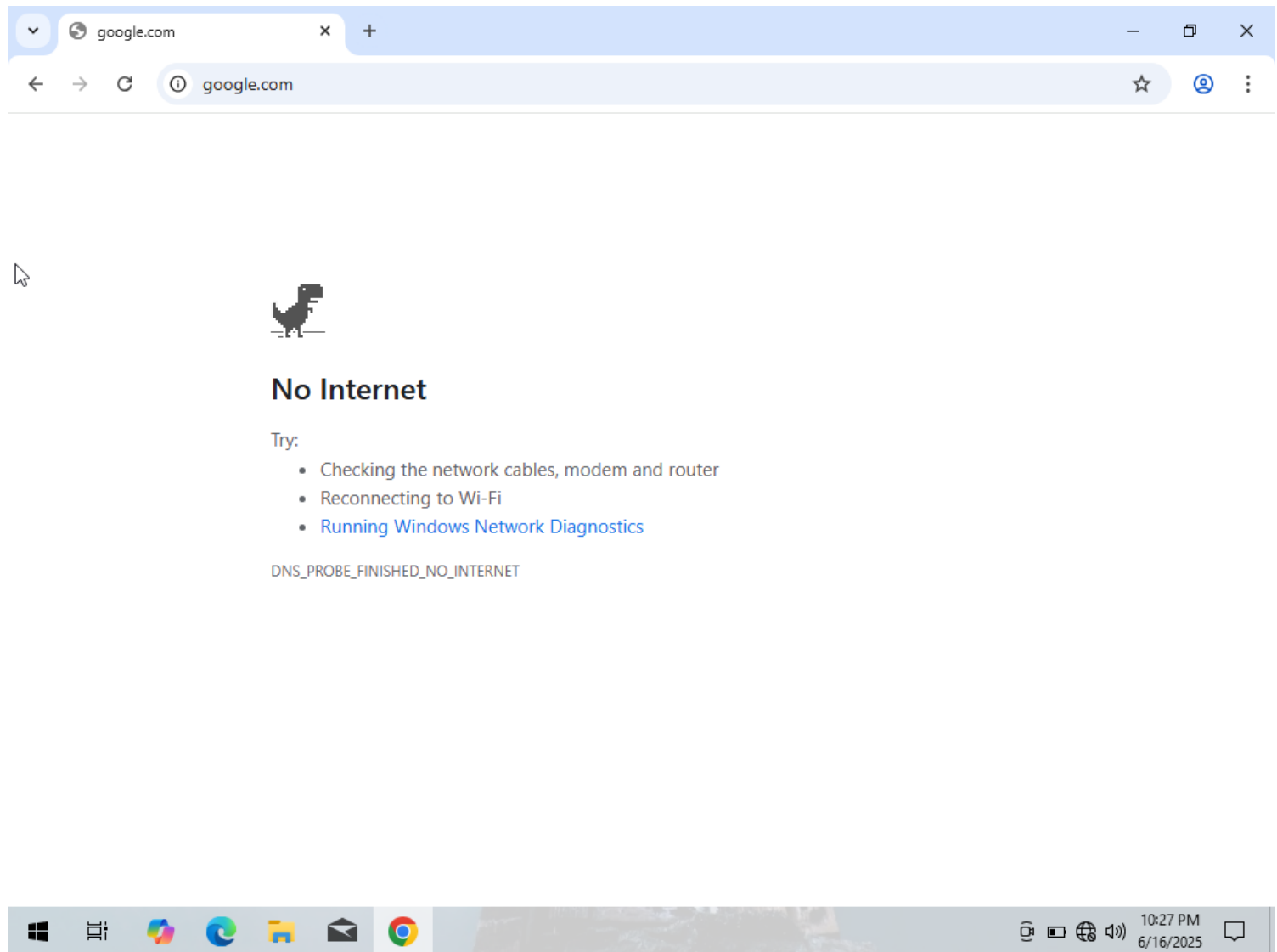
I will perform both static and dynamic analysis on this file to understand how it modifies the system, whether it contacts any external addresses, and how the malware can be detected on the system.

Before proceeding, here are a few things to keep in mind:

- 1- Download and install updates to ensure the system doesn't consume unnecessary resources during the analysis.
- 2-Download, install, and verify that the analysis tools are functioning properly.
- 3-In the network settings, ensure the **host-only network** option is selected.
- 4-Disable **Windows Defender** (or any other antivirus software) and **firewalls**.
- 5-Take a **snapshot** once everything is initialized.

Virustotal Link: <https://www.virustotal.com/gui/file/15cc3cad7aec406a9ec93554c9eaf0bfbcc740bef9d52dbc32bf5559e90f53fee>

Ensure that the virtual machine does not have any contact with network services.



Disable antivirus protection to ensure a clean analysis without interruptions.

Windows Security

←

≡

🏠

🛡️

👤

🗨️

📁

📅

🔒

👥

⚙️

## ⚙️ Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

### Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

❌ Real-time protection is off, leaving your device vulnerable.

☐ Off

### Cloud-delivered protection

Provides increased and faster protection with access to the latest protection data in the cloud. Works best with Automatic sample submission turned on.

⚠️ Cloud-delivered protection is off. Your device may be [Dismiss](#) vulnerable.

☐ Off

### Automatic sample submission

Send sample files to Microsoft to help protect you and others from potential threats. We'll prompt you if the file we need is likely to contain personal information.

Have a question?  
[Get help](#)

Help improve Windows Security  
[Give us feedback](#)

Change your privacy settings  
View and change privacy settings for your Windows 10 device.  
[Privacy settings](#)  
[Privacy dashboard](#)  
[Privacy Statement](#)

🏠

📁

📅

🔒

👥

⚙️

🔌

📶

🌐

🔊

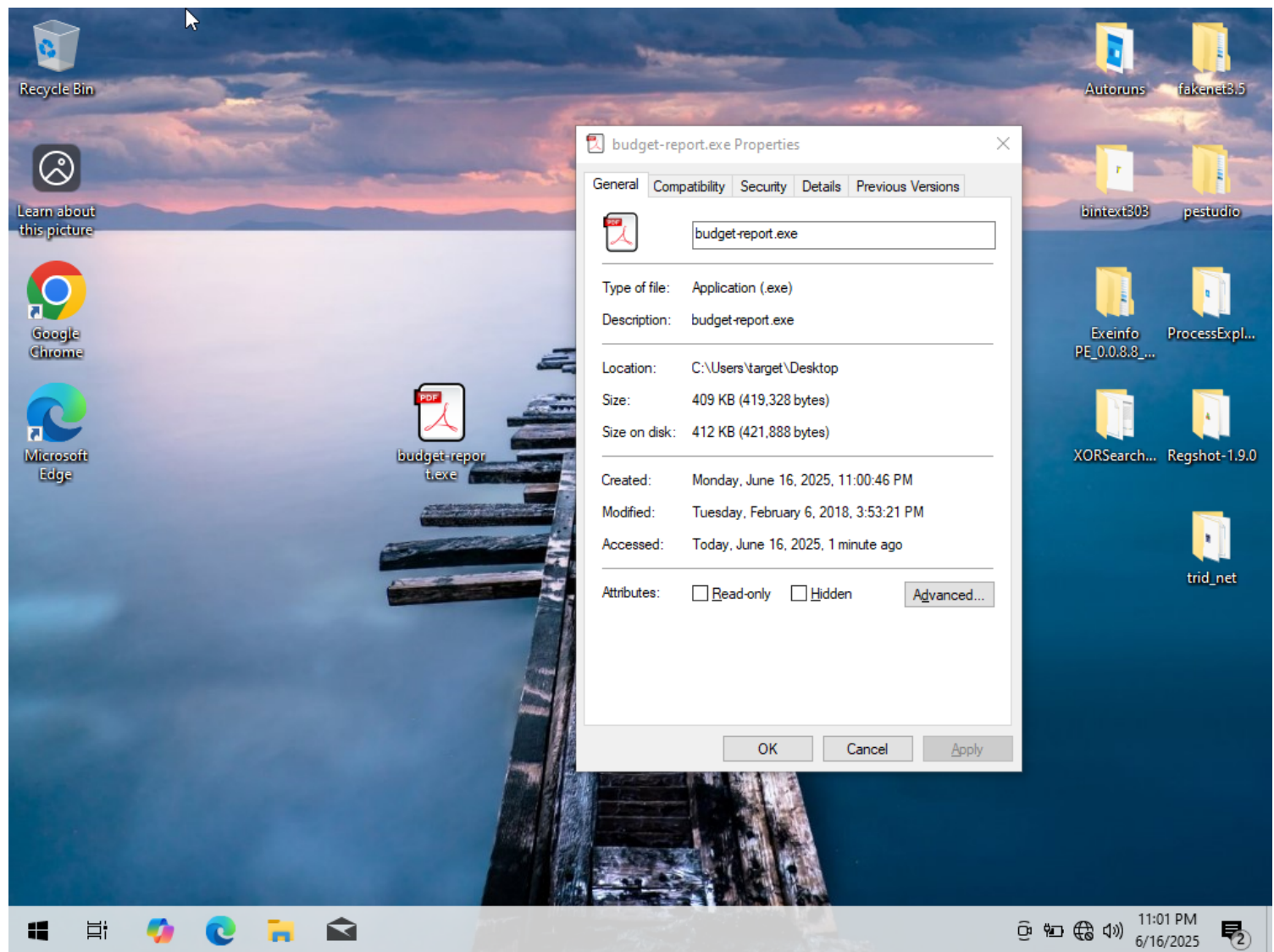
10:28 PM

6/16/2025

🗨️ 1

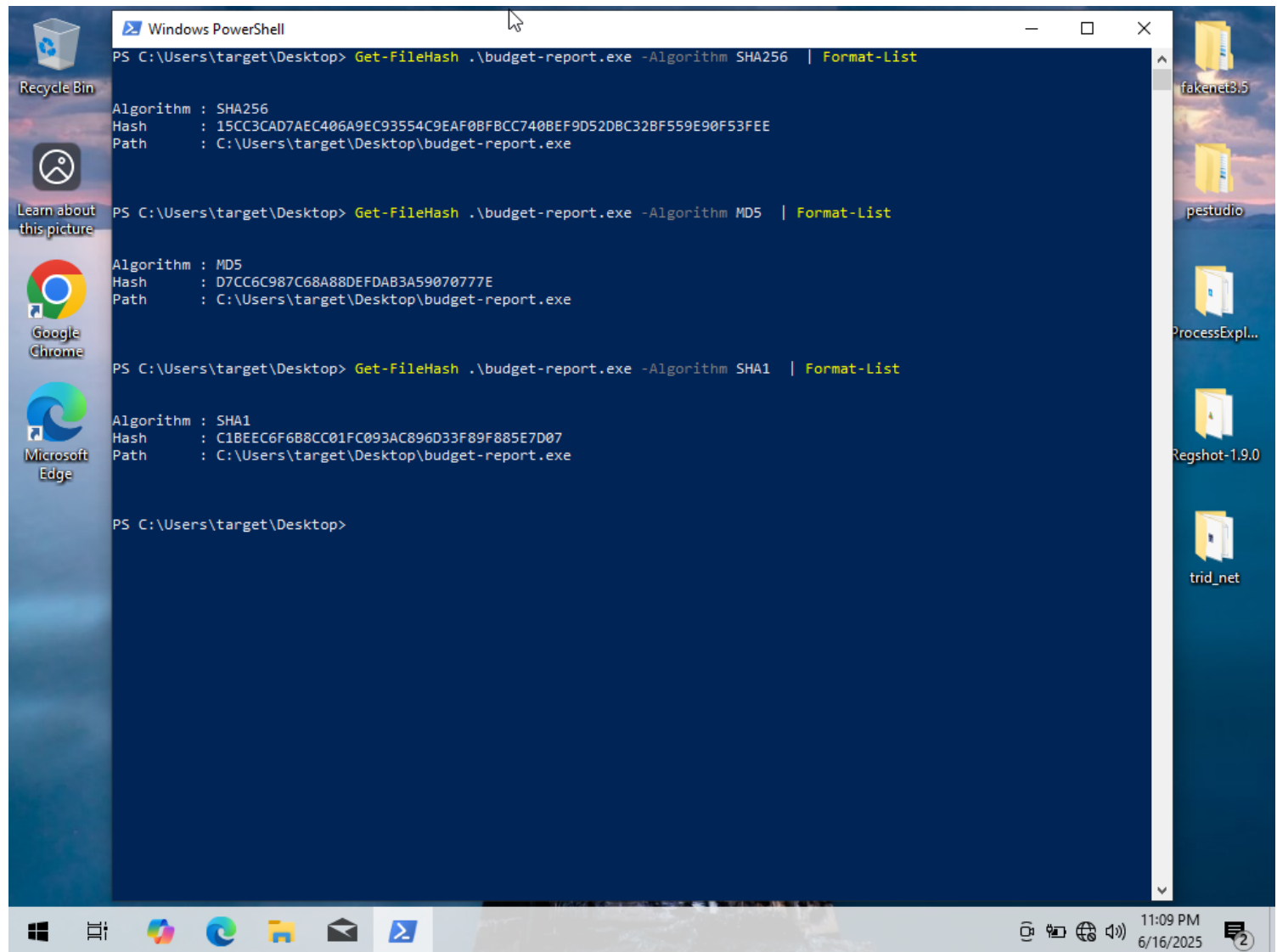
3/30

# budget-report.exe (Static Analysis)



The malware looks convincing enough to fool people into thinking it's a PDF file. Many systems don't display file extensions, which can lead an amateur user to believe it's an actual PDF file, causing them to open it. Now, we can collect the hash value of the file. The reason we're obtaining the hash value is to identify this malware, as the filename can be changed, but the file hash remains unchanged.

## Hash Analysis:



The screenshot shows a Windows PowerShell window titled "Windows PowerShell" with the following commands and output:

```
PS C:\Users\target\Desktop> Get-FileHash .\budget-report.exe -Algorithm SHA256 | Format-List
Algorithm : SHA256
Hash      : 15CC3CAD7AEC406A9EC93554C9EAF0BFBC740BEF9D52DBC32BF559E90F53FEE
Path      : C:\Users\target\Desktop\budget-report.exe

PS C:\Users\target\Desktop> Get-FileHash .\budget-report.exe -Algorithm MD5 | Format-List
Algorithm : MD5
Hash      : D7CC6C987C68A88DEFDAB3A59070777E
Path      : C:\Users\target\Desktop\budget-report.exe

PS C:\Users\target\Desktop> Get-FileHash .\budget-report.exe -Algorithm SHA1 | Format-List
Algorithm : SHA1
Hash      : C1BEEC6F6B8CC01FC093AC896D33F89F885E7D07
Path      : C:\Users\target\Desktop\budget-report.exe

PS C:\Users\target\Desktop>
```

The desktop background is a blue gradient with icons for Recycle Bin, Learn about this picture, Google Chrome, and Microsoft Edge on the left, and folders for fakenet3.5, pestudio, ProcessExpl..., Regshot-1.9.0, and trid\_net on the right. The taskbar at the bottom shows the Start button, task view, and several application icons, along with the system clock showing 11:09 PM on 6/16/2025.

We got the 3 popular hash value for this following file, SHA-256 hash is highly reliable compared to the other two because it doesn't cause collision while calculating the hash value for a file.

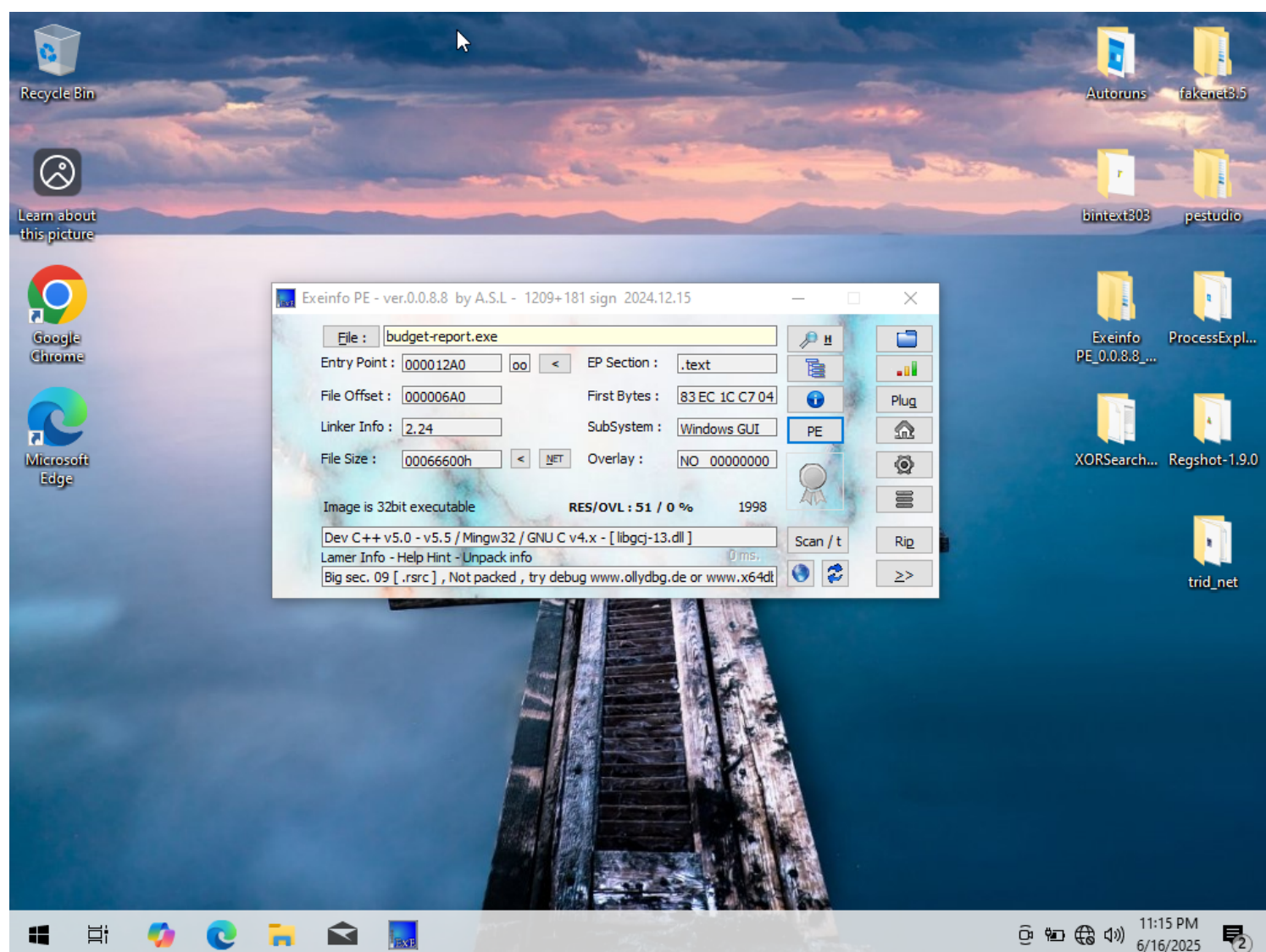
SHA256 : **15CC3CAD7AEC406A9EC93554C9EAF0BFBC740BEF9D52DBC32BF559E90F53FEE**

SHA-1 : **C1BEEC6F6B8CC01FC093AC896D33F89F885E7D07**

MD5 : **D7CC6C987C68A88DEFDAB3A59070777E**

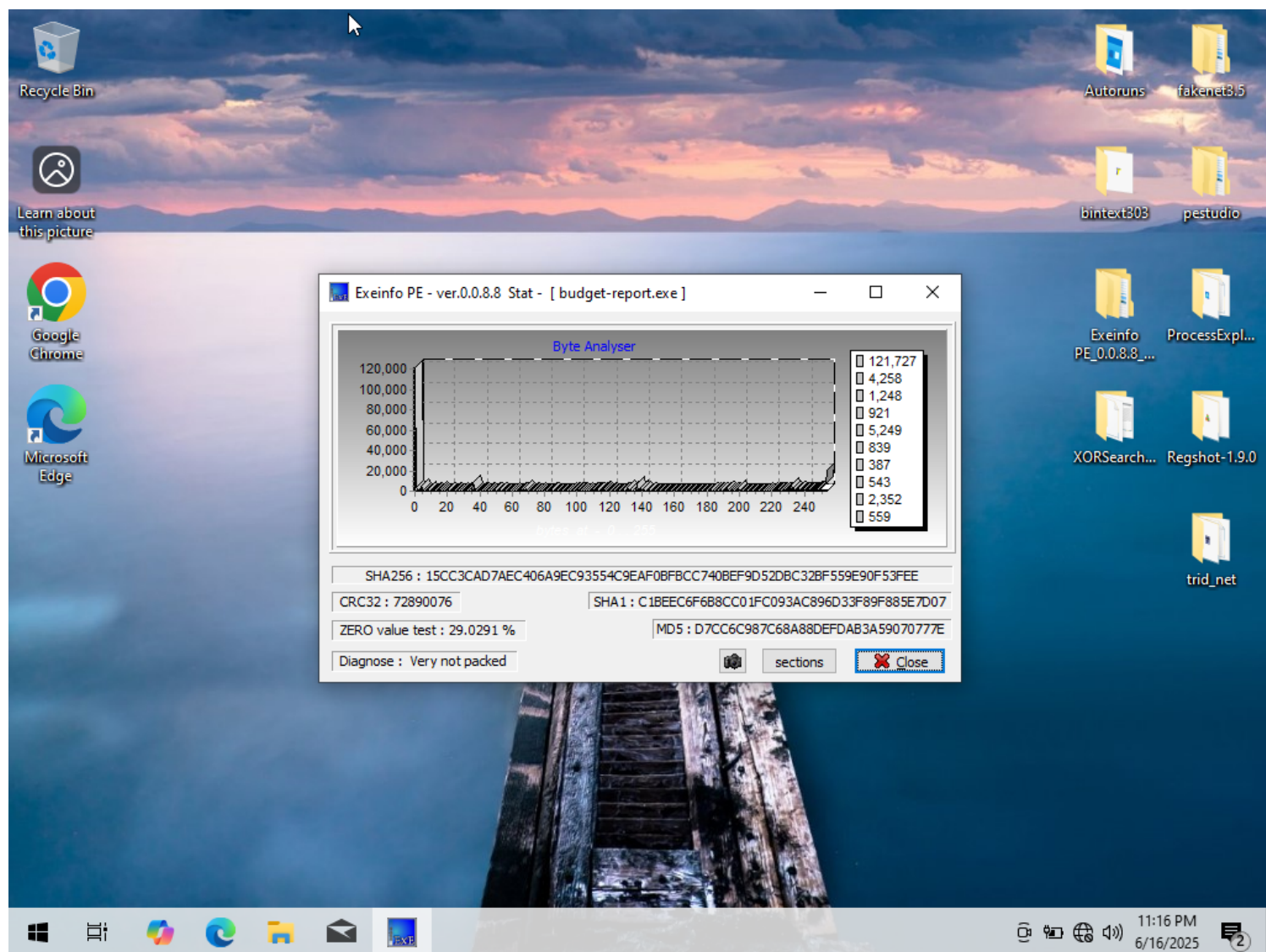
## File Analysis:

Now, let's focus on identifying the file further using the Exeinfo PE tool.

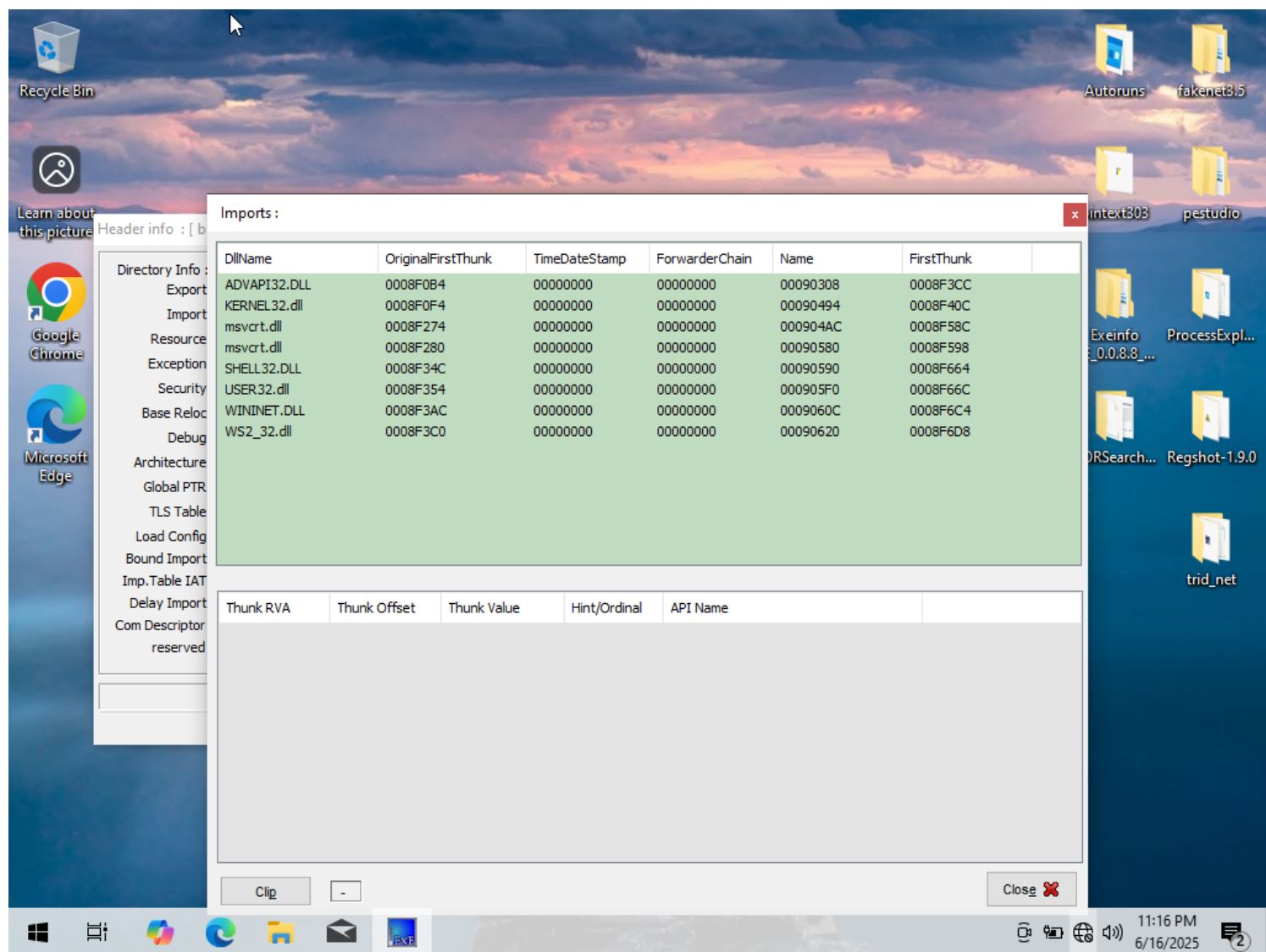


When we use **Exeinfo PE** to identify information about the file, we discover that there are no packers used, and the file was created using Dev C++, MinGW32, or GNU C.





We can also cross-verify the hash value of the file using this tool, and it matches.



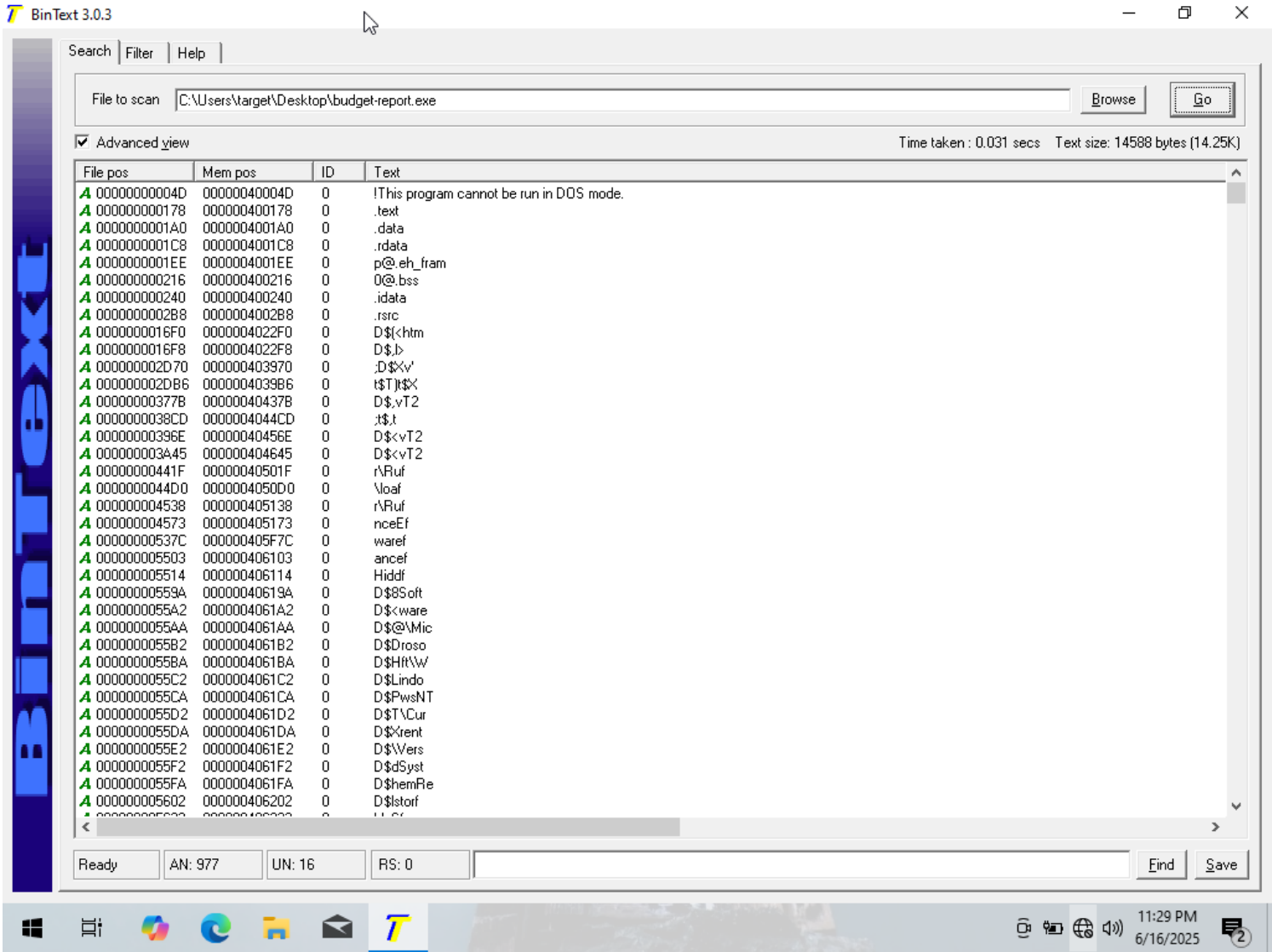
These are the following dll's which were used by the program during execution.

- 1- **advapi32.dll**: Provides advanced Windows API services, including security, user authentication, registry management, and event logging.
- 2- **kernel32.dll**: Handles memory management, input/output operations, process control, and basic system services for Windows programs.
- 3- **msvcrt.dll**: Contains Microsoft C Runtime Library functions for memory management, string manipulation, input/output operations, and more.
- 4- **shell32.dll**: Manages Windows shell functionality, including file management, dialogs, and user interface elements like icons and menus.
- 5- **user32.dll**: Provides user interface functions for managing windows, controls, and messages in a graphical environment on Windows.
- 6- **wininet.dll**: Manages Internet connectivity, including functions for HTTP, FTP, and other network protocols for web browsing.
- 7- **ws2\_32.dll**: Provides Windows Sockets API for network communication, handling TCP/IP protocols, and managing socket-based connections.



**String Analysis:**

Let's find out the embedded characters in this file, as there could be some useful information that may assist in our analysis. I am using a tool called **BinText**, which reads the strings of the program and outputs them based on our filter. I set the minimum string length to 5 characters, so if the tool finds a string with at least 5 characters, it will be displayed.



We can see that the tool has provided the available strings from the file.

Search Filter Help

File to scan C:\Users\target\Desktop\budget-report.exe

Browse

Go

☒ Advanced view

Time taken : 0.031 secs Text size: 14588 bytes (14.25K)

File pos	Mem pos	ID	Text
A 00000002BDF8	00000042E1F8	0	%s%s.exe
A 00000002BE02	00000042E202	0	Mozilla/4.0 (compatible)
A 00000002BE24	00000042E224	0	PROGRAMDATA
A 00000002BE30	00000042E230	0	RPSessionInterval
A 00000002BE42	00000042E242	0	RPGlobalInterval
A 00000002BE53	00000042E253	0	RPLifeInterval
A 00000002BE62	00000042E262	0	TimerInterval
A 00000002BE70	00000042E270	0	SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List
A 00000002BEE5	00000042E2E5	0	%s:*Enabled:%s
A 00000002BEF8	00000042E2F8	0	SYSTEM\CurrentControlSet\Services\Disk\Enum
A 00000002BF2B	00000042E32B	0	%s\%i.bat
A 00000002BF39	00000042E339	0	%s\U%i.bat
A 00000002BFE8	00000042E3E8	0	Shell_TrayWnd
A 00000002BFF6	00000042E3F6	0	regedit.exe
A 00000002C002	00000042E402	0	taskmgr.exe
A 00000002C00E	00000042E40E	0	cmd.exe
A 00000002C016	00000042E416	0	msconfig.exe
A 00000002C023	00000042E423	0	autoruns.exe
A 00000002C030	00000042E430	0	%s:%i
A 00000002C038	00000042E438	0	Software\Skype\Phone
A 00000002C04D	00000042E44D	0	SkypePath
A 00000002C057	00000042E457	0	SkypeControlAPIDiscover
A 00000002C06F	00000042E46F	0	SkypeControlAPIAttach
A 00000002C088	00000042E488	0	%s(%s)
A 00000002C08F	00000042E48F	0	LOCALAPPDATA
A 00000002C09C	00000042E49C	0	%s\Google\Chrome\Application\chrome.exe
A 00000002C0C4	00000042E4C4	0	%s\Internet Explorer\iexplore.exe
A 00000002C0E6	00000042E4E6	0	%s\Opera\opera.exe
A 00000002C0FC	00000042E4FC	0	%s\Mozilla Firefox\firefox.exe
A 00000002C11B	00000042E51B	0	%s\Maxthon3\Bin\Maxthon.exe
A 00000002C138	00000042E538	0	Google Chrome
A 00000002C146	00000042E546	0	Opera
A 00000002C14C	00000042E54C	0	Firefox
A 00000002C154	00000042E554	0	Internet Explorer
A 00000002C166	00000042E566	0	Maxthon
A 00000002C16E	00000042E56E	0	"unknown"

Ready

AN: 977

UN: 16

RS: 0

Find

Save

11:33 PM  
6/16/2025

Search | Filter | Help

File to scan: C:\Users\target\Desktop\budget-report.exe Browse Go

☒ Advanced view Time taken : 0.031 secs Text size: 14588 bytes (14.25K)

File pos	Mem pos	ID	Text
00000002C178	00000042E578	0	%s:%i
00000002C17E	00000042E57E	0	chrome.exe
00000002C189	00000042E589	0	opera.exe
00000002C193	00000042E593	0	firefox.exe
00000002C19F	00000042E59F	0	ieexplore.exe
00000002C1AC	00000042E5AC	0	Maxthon.exe
00000002C1B8	00000042E5B8	0	ltype:on_exec{luid:%spriv:%slarch:w%slgend:%scores:%ilos:%sver:%slnet:%slnew:
00000002C208	00000042E608	0	http://
00000002C210	00000042E610	0	https://
00000002C220	00000042E620	0	ltype:repeat{luid:%sram:%ldbk_killed:%ilbk_files:%ilbk_keys:%ilbusy:%s}
00000002C278	00000042E678	0	gethostbyname
00000002C28D	00000042E68D	0	%s:%s
00000002C293	00000042E693	0	interval
00000002C29C	00000042E69C	0	taskid
00000002C2A3	00000042E6A3	0	command
00000002C2A8	00000042E6A8	0	ERROR_NOT_IN_DB
00000002C2B8	00000042E6B8	0	200 OK
00000002C2C4	00000042E6C4	0	Content-Length: 0
00000002C2D6	00000042E6D6	0	Location:
00000002C2E0	00000042E6E0	0	ltype:response{luid:%staskid:%lreturn:%sbusy:%s}
00000002C356	00000042E756	0	IsWow64Process
00000002C380	00000042E780	0	ConvertStringSecurityDescriptorToSecurityDescriptorW
00000002C388	00000042E788	0	ConvertSecurityDescriptorToSecurityDescriptorStringW
00000002C3ED	00000042E7ED	0	GetCurrentHwProfileA
00000002C414	00000042E814	0	IcmpCreateFile
00000002C423	00000042E823	0	IcmpCloseHandle
00000002C433	00000042E833	0	IcmpParseReplies
00000002C45A	00000042E85A	0	ObtainUserAgentString
00000002C486	00000042E886	0	WSAStartup
00000002C491	00000042E891	0	gethostbyname
00000002C49F	00000042E89F	0	htons
00000002C4A5	00000042E8A5	0	socket
00000002C4AC	00000042E8AC	0	ioctlsocket
00000002C4B8	00000042E8B8	0	connect
00000002C4C0	00000042E8C0	0	closesocket
00000002C4D6	00000042E8D6	0	sendto

Ready AN: 977 UN: 16 RS: 0 Find Save

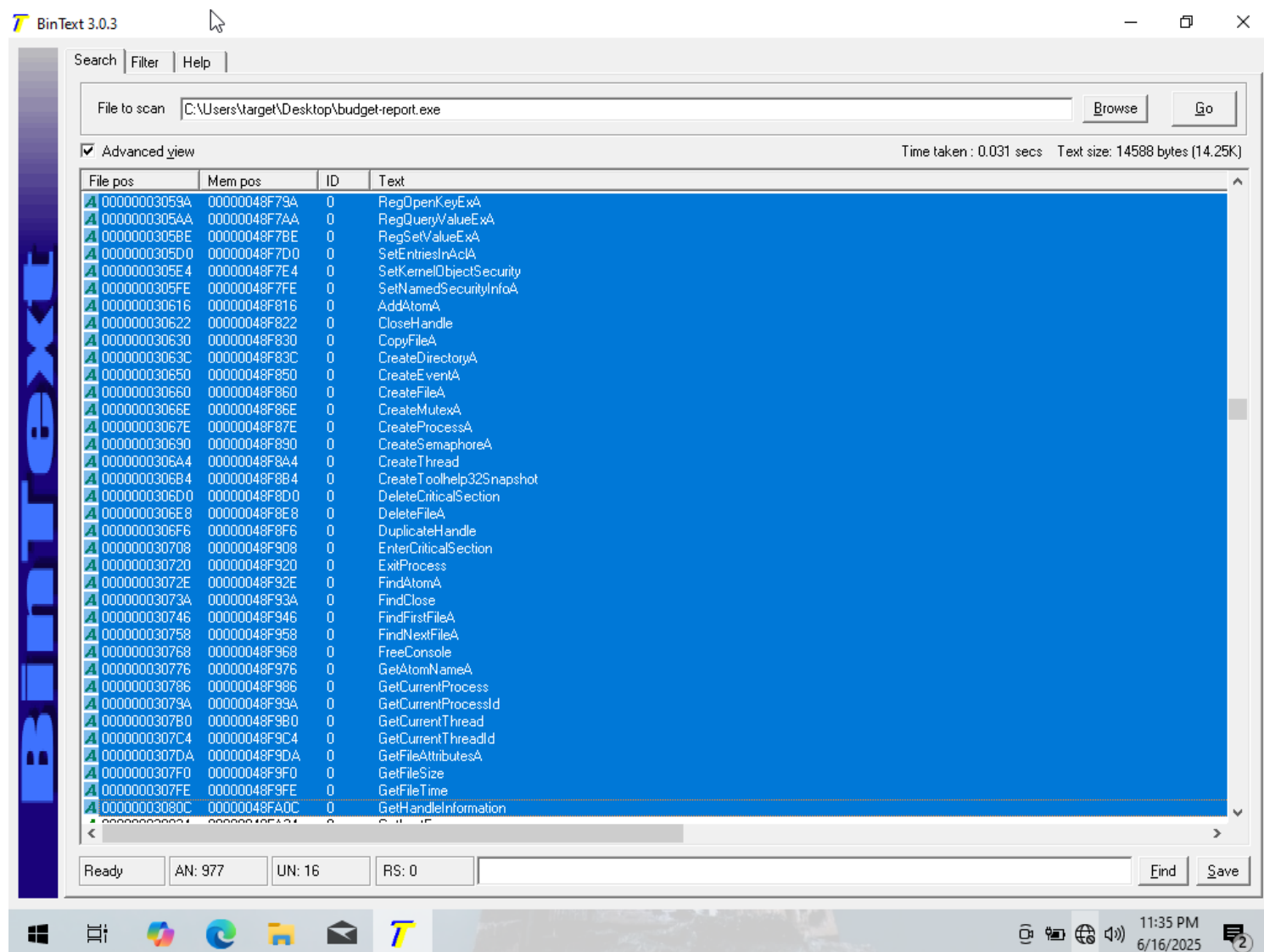
Search | Filter | Help

File to scan: C:\Users\target\Desktop\budget-report.exe Browse Go

☒ Advanced view Time taken : 0.031 secs Text size: 14588 bytes (14.25K)

File pos	Mem pos	ID	Text
A 00000002C876	00000042EC76	0	uninstall
A 00000002C880	00000042EC80	0	%lh %lm %ls
A 00000002C890	00000042EC90	0	%s\System32\drivers\etc\protocol
A 00000002C8C8	00000042ECC8	0	%s\Microsoft.NET\Framework\
A 00000002C8E7	00000042ECE7	0	v4.0.30319
A 00000002C8F2	00000042ECF2	0	v2.0.50727
A 00000002C930	00000042ED30	0	%s-%s
A 00000002C937	00000042ED37	0	CURRENT_USER
A 00000002C944	00000042ED44	0	%s:%i
A 00000002C950	00000042ED50	0	text/html, application/xml;q=0.9, application/xhtml+xml, image/png, image/webp, image/jpeg, image/gif, image/x-bitmap, */*;q=0.1
A 00000002C9D4	00000042EDD4	0	image/jpeg, application/x-ms-application, image/gif, application/xaml+xml, image/pipe, application/x-ms-xbap, application/x-shockwave-flash, ap
A 00000002CA7C	00000042EE7C	0	application/xml,application/xhtml+xml,text/html;q=0.9, text/plain;q=0.8,image/png,*/*;q=0.5
A 00000002CAD8	00000042EED8	0	Connection:
A 00000002CAE5	00000042EEE5	0	ERR_FAILED_TO_RESOLVE_HOST
A 00000002CB00	00000042EF00	0	http://
A 00000002CB08	00000042EF08	0	https://
A 00000002CB17	00000042EF17	0	HTTP/1.
A 00000002CB20	00000042EF20	0	dnsapi.dll
A 00000002CB28	00000042EF28	0	DnsFlushResolverCache
A 00000002CB41	00000042EF41	0	%s@%s:%i
A 00000002CB4A	00000042EF4A	0	%s & %s
A 00000002CB52	00000042EF52	0	WINDIR
A 00000002CB59	00000042EF59	0	APPDATA
A 00000002CB66	00000042EF66	0	USERPROFILE
A 00000002CB72	00000042EF72	0	ALLUSERSPROFILE
A 00000002CB82	00000042EF82	0	PROGRAMFILES
A 00000002CB8F	00000042EF8F	0	PROGRAMDATA
A 00000002CB9B	00000042EF9B	0	%s%s%s%s%i%s%s
A 00000002CBAC	00000042EFAC	0	ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789
A 00000002CBEB	00000042EFEB	0	MAIN_%li
A 00000002CBF4	00000042EFF4	0	BACKUP_%li
A 00000002CBFF	00000042EFFF	0	UNINSTALL_%li
A 00000002CC0D	00000042F00D	0	%i.%i.%i
A 00000002CC1E	00000042F01E	0	NOERRSUC
A 00000002CC27	00000042F027	0	ERROPFA
A 00000002CC34	00000042F034	0	SeDebugPrivilege
A 00000002CC4F	00000042F04F	0	%s %s

Ready AN: 977 UN: 16 RS: 0 Find Save



From the following images, we can observe some strings related to the file's activities. Notable strings include **cmd.exe**, **socket**, **connect**, **Skype**, and other **registry-related activity strings** present in the file. These may indicate that the file likely uses these services or activities to perform various actions on the executed target system.

We have gathered a significant amount of information so far, allowing us to form an understanding of the activities the file is likely to perform upon execution.

## PE Header Analysis:

Using the PE Studio tool, I analyzed the malware and discovered some interesting information in the Resources tab. The icon resource's language is set to **English-US**, which suggests that the developer may have used a U.S. English configured personal computer. However, this cannot be considered definitive proof, as the developer could have manipulated this information.

pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\target\desktop\budget-report.exe (read-only)

file settings about

c:\users\target\desktop\budget-report.exe

- indicators (imports > flag)
- footprints (type > sha256)
- virustotal (offline)
- dos-header (size > 64 bytes)
- dos-stub (size > 64 bytes)
- rich-header (n/a)
- file-header (executable > 32-bit)
- optional-header (subsystem > GUI)
- directories (count > 4)
- sections (characteristics > virtual)
- libraries (flag > 2)
- imports (flag > 56)
- exports (n/a)
- thread-local-storage (callback > 3)
- .NET (n/a)
- resources (count > 19)
- strings (count > 4622)
- debug (n/a)
- manifest (n/a)
- version (n/a)
- certificate (n/a)
- overlay (n/a)

name (19)	signature	location (from-to)	size (21463...	footprint (sha256)	entropy	language (1)	resou
icon		0x00031DE4 - 0x0...	0x00000668...	1B410C84E8A57B06...	3.099	English-US (0x00000409)	28 00
icon		0x000383A4 - 0x0...	0x00010828...	08189CB079D7C469...	3.430	English-US (0x00000409)	28 00
icon		0x00048BCC - 0x0...	0x000094A...	6F7ABC15C946ECB...	3.910	English-US (0x00000409)	28 00
icon		0x00052074 - 0x0...	0x000067E8...	FF6EC6856140C423...	3.949	English-US (0x00000409)	28 00
icon		0x0005885C - 0x0...	0x00005488...	C559469B11D8ECE8...	3.844	English-US (0x00000409)	28 00
icon		0x0005DCE4 - 0x0...	0x00004228...	23B22DE90190612A...	3.780	English-US (0x00000409)	28 00
icon		0x00061F0C - 0x0...	0x000025A...	B913A26A5D72266A...	4.182	English-US (0x00000409)	28 00
icon		0x000644B4 - 0x0...	0x000010A...	0F858E021225F489F...	4.354	English-US (0x00000409)	28 00
icon		0x0006555C - 0x0...	0x00000988...	630F7C7E1B5C67B5...	4.556	English-US (0x00000409)	28 00
icon		0x00065EE4 - 0x0...	0x00000468...	75D5D72F1E1307E6...	4.794	English-US (0x00000409)	28 00
icon		0x0003244C - 0x0...	0x000002E8...	C07D11E7FDFE291B...	3.600	English-US (0x00000409)	28 00
icon		0x00032734 - 0x0...	0x000001E8...	8199C15876E9C64C...	3.145	English-US (0x00000409)	28 00
icon		0x0003291C - 0x0...	0x00000128...	96E75DE3B28B4D02...	3.091	English-US (0x00000409)	28 00
icon		0x00032A44 - 0x0...	0x000035E0...	28B90965D78CBC85...	7.947	English-US (0x00000409)	89 50
icon		0x00036024 - 0x0...	0x00000EA...	74293B021844D2A6...	4.870	English-US (0x00000409)	28 00
icon		0x00036ECC - 0x0...	0x000008A...	25C550C6DABB52A...	4.820	English-US (0x00000409)	28 00
icon		0x00037774 - 0x0...	0x000006C...	AEBB3208E432AED...	4.292	English-US (0x00000409)	28 00
icon		0x00037E3C - 0x0...	0x00000568...	79DB354661760421...	3.020	English-US (0x00000409)	28 00
ON icon-group		0x0006634C - 0x0...	0x00000102...	wait...	3.297	English-US (0x00000409)	00 00

sha256 > 15CC3CAD7AEC406A9EC93554C9EAF0BFBC740BEF9D52DBC32BF559E90F53FEE    cpu > 32-bit    file > type > executable    subsystem > GUI

11:53 PM 6/16/2025



pestudio 9.61 - Malware Initial Assessment - www.winitor.com | c:\users\target\desktop\budget-report.exe (read-only)

file settings about

c:\users\target\desktop\budget-report.exe

- indicators (imports > flag)
- footprints (type > sha256)
- virustotal (offline)
- dos-header (size > 64 bytes)
- dos-stub (size > 64 bytes)
- rich-header (n/a)
- file-header (executable > 32-bit)
- optional-header (subsystem > GUI)
- directories (count > 4)
- sections (characteristics > virtual)
- libraries (flag > 2)
- imports (flag > 56)**
- exports (n/a)
- thread-local-storage (callback > 3)
- .NET (n/a)
- resources (count > 19)
- strings (count > 4622)
- debug (n/a)
- manifest (n/a)
- version (n/a)
- certificate (n/a)
- overlay (n/a)

imports (190)	flag (56)	type	ordinal	first-thunk (IAT)	first-thunk-original
<a href="#">AdjustTokenPrivileges</a>	x	implicit	-	0x0008F6E4	0x0008F6E4
<a href="#">BuildExplicitAccessWithName</a>	x	implicit	-	0x0008F6FC	0x0008F6FC
<a href="#">LookupPrivilegeValueA</a>	x	implicit	-	0x0008F71C	0x0008F71C
<a href="#">OpenProcessToken</a>	x	implicit	-	0x0008F734	0x0008F734
<a href="#">RegCreateKeyExA</a>	x	implicit	-	0x0008F756	0x0008F756
<a href="#">RegDeleteValueA</a>	x	implicit	-	0x0008F768	0x0008F768
<a href="#">RegFlushKey</a>	x	implicit	-	0x0008F78A	0x0008F78A
<a href="#">RegSetValueExA</a>	x	implicit	-	0x0008F7BC	0x0008F7BC
<a href="#">SetEntriesInAclA</a>	x	implicit	-	0x0008F7CE	0x0008F7CE
<a href="#">SetKernelObjectSecurity</a>	x	implicit	-	0x0008F7E2	0x0008F7E2
<a href="#">SetNamedSecurityInfoA</a>	x	implicit	-	0x0008F7FC	0x0008F7FC
<a href="#">AddAtomA</a>	x	implicit	-	0x0008F814	0x0008F814
<a href="#">CopyFileA</a>	x	implicit	-	0x0008F82E	0x0008F82E
<a href="#">CreateDirectoryA</a>	x	implicit	-	0x0008F83A	0x0008F83A
<a href="#">CreateProcessA</a>	x	implicit	-	0x0008F87C	0x0008F87C
<a href="#">CreateToolhelp32Snapshot</a>	x	implicit	-	0x0008F8B2	0x0008F8B2
<a href="#">DeleteFileA</a>	x	implicit	-	0x0008F8E6	0x0008F8E6
<a href="#">FindAtomA</a>	x	implicit	-	0x0008F92C	0x0008F92C
<a href="#">FindFirstFileA</a>	x	implicit	-	0x0008F944	0x0008F944
<a href="#">FindNextFileA</a>	x	implicit	-	0x0008F956	0x0008F956
<a href="#">GetAtomNameA</a>	x	implicit	-	0x0008F974	0x0008F974
<a href="#">GetCurrentProcess</a>	x	implicit	-	0x0008F984	0x0008F984
<a href="#">GetCurrentProcessId</a>	x	implicit	-	0x0008F998	0x0008F998
<a href="#">GetCurrentThread</a>	x	implicit	-	0x0008F9AE	0x0008F9AE
<a href="#">GetCurrentThreadId</a>	x	implicit	-	0x0008F9C2	0x0008F9C2
<a href="#">GetThreadContext</a>	x	implicit	-	0x0008FAE8	0x0008FAE8
<a href="#">GetThreadPriority</a>	x	implicit	-	0x0008FAFC	0x0008FAFC
<a href="#">GlobalMemoryStatus</a>	x	implicit	-	0x0008FB5A	0x0008FB5A
<a href="#">Module32First</a>	x	implicit	-	0x0008FC58	0x0008FC58
<a href="#">Module32Next</a>	x	implicit	-	0x0008FC68	0x0008FC68
<a href="#">MoveFileExA</a>	x	implicit	-	0x0008FC78	0x0008FC78

sha256 > 15CC3CAD7AEC406A9EC93554C9EAF0BFBC740BEF9D52DBC32BF559E90F53FEE | cpu > 32-bit | file > type > executable | subsystem > GUI

11:53 PM 6/16/2025

While reviewing the information about the imported Windows API functions, we can identify many that are flagged as potentially dangerous. However, these functions are not always malicious, as they are also used in legitimate programs. Each Windows API function can perform a variety of activities, and it's important to note that they may also be utilized by malware.

## **budget-report.exe (Dynamic Analysis)**

Run **FakeNet** to monitor incoming and outgoing network traffic in real-time, and also to ensure the malware believes we are connected to the internet (since some malware only activates when the target system is online).

```

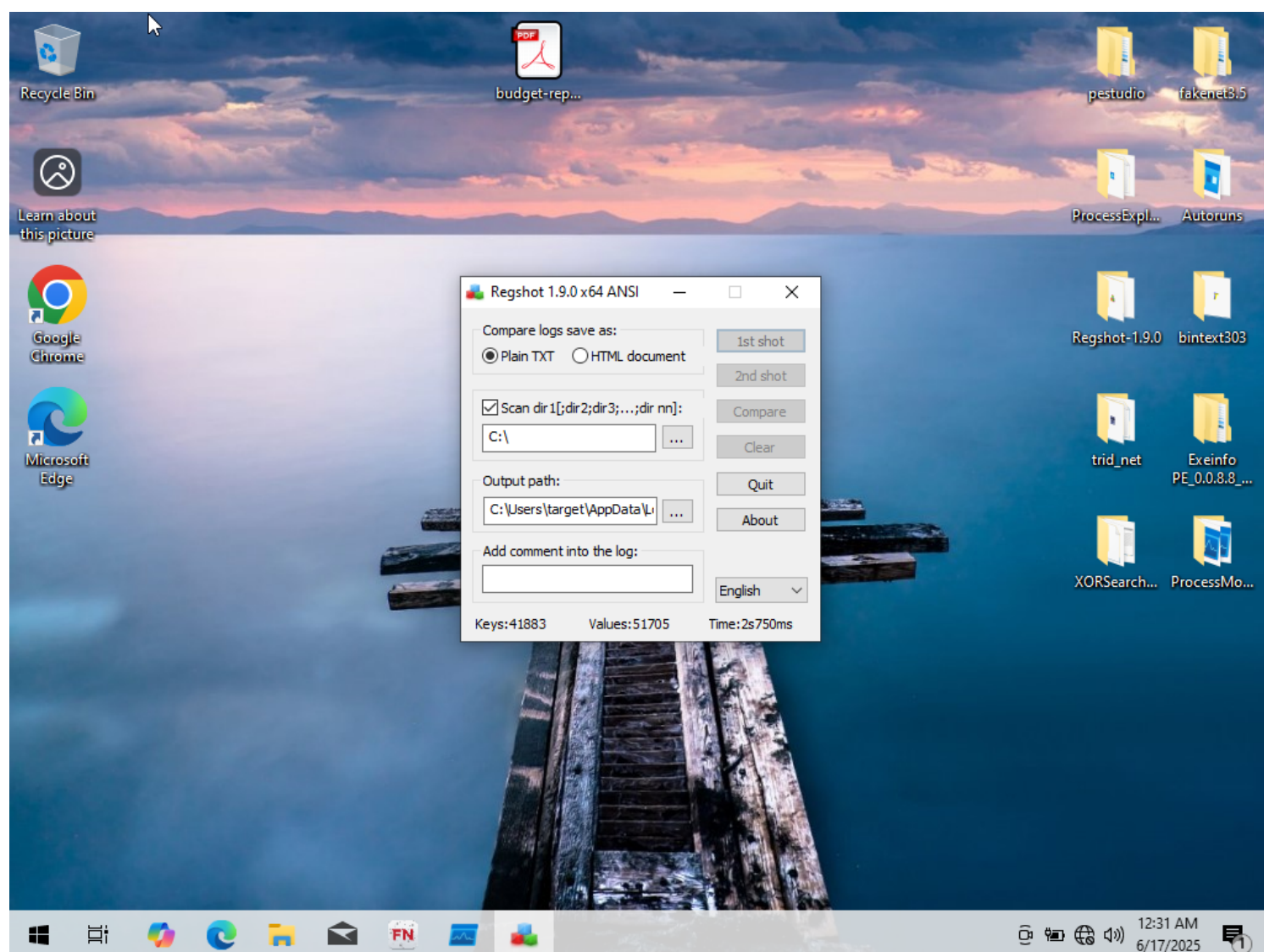
C:\Users\target\Desktop\fake\enet3.5\fakeenet.exe
06/17/25 12:28:02 AM [ FakeNet] Loaded configuration file: C:\Users\target\Desktop\fake\enet3.5\fakeenet3.5\configs\de
fault.ini
06/17/25 12:28:06 AM [ Diverter] Capturing traffic to packets_20250617_002806.pcap
06/17/25 12:28:06 AM [ Diverter] WARNING: No gateways configured!
06/17/25 12:28:16 AM [ Diverter] Setting gateway 169.254.246.1 on interface Ethernet
06/17/25 12:28:16 AM [ Diverter] WARNING: No DNS servers configured!
06/17/25 12:28:17 AM [ Diverter] Setting DNS 169.254.246.91 on interface Ethernet
06/17/25 12:28:17 AM [ Diverter] Failed calling GetBestInterface
Root "Trusted Root Certification Authorities"
Signature matches Public Key
Certificate "fakenet.flare" added to store.
CertUtil: -addstore command completed successfully.
06/17/25 12:28:20 AM [ DNS Server] Hiding logs from blacklisted processes
Root "Trusted Root Certification Authorities"
Signature matches Public Key
Related Certificates:

Exact match:
Element 3:
Serial Number: 01903a
Issuer: CN=fakenet.flare, C=US
NotBefore: 6/17/2025 12:28 AM
NotAfter: 4/13/2026 12:57 AM
Subject: CN=fakenet.flare, C=US
Signature matches Public Key
Root Certificate: Subject matches Issuer
Cert Hash(sha1): 961c427e966451d79d7f62ce4ed4ecc7580b1b9f

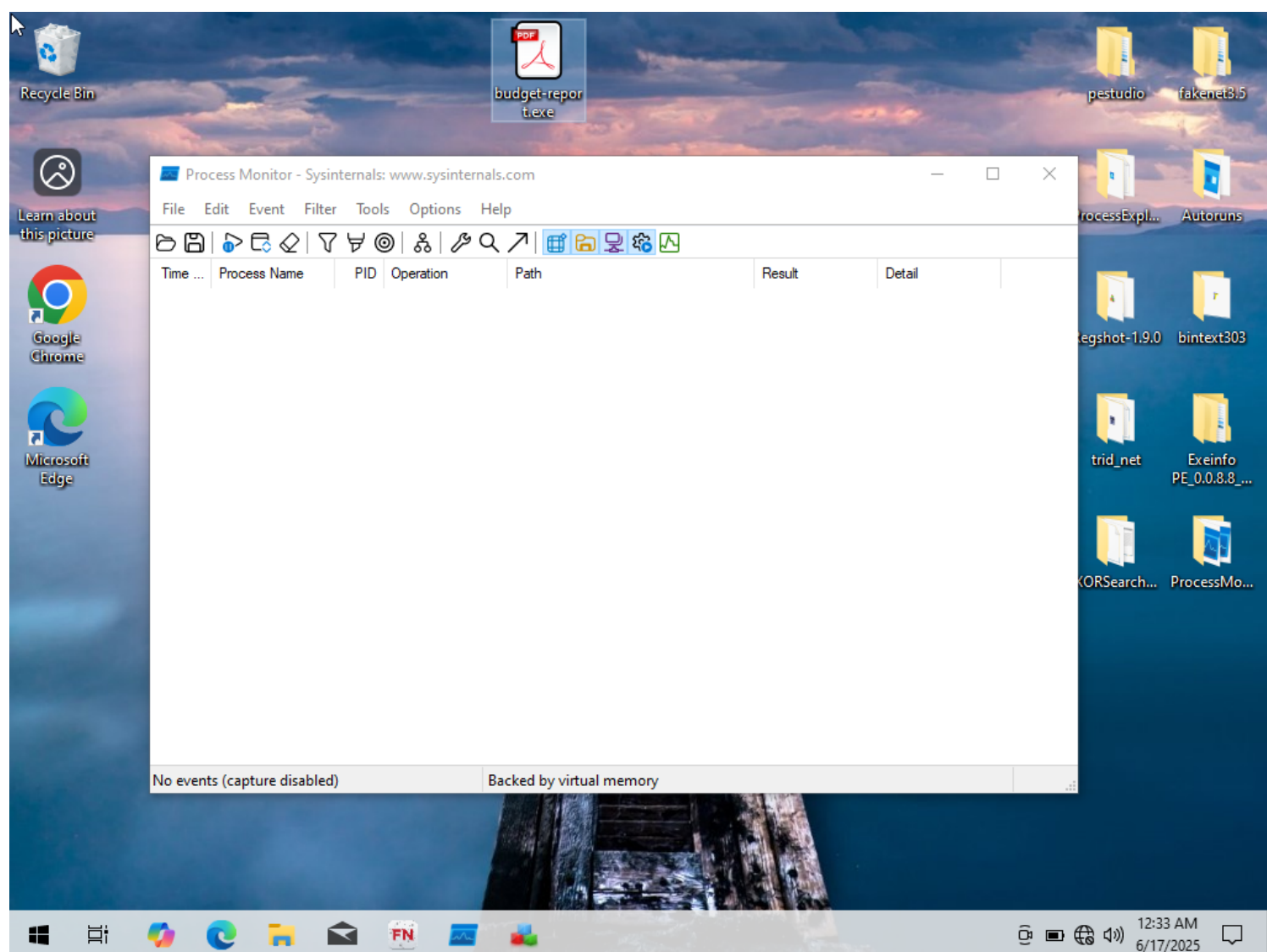
Certificate "fakenet.flare" already in store.
CertUtil: -addstore command completed successfully.
06/17/25 12:28:22 AM [ FTP] concurrency model: multi-thread
06/17/25 12:28:22 AM [ FTP] masquerade (NAT) address: None
06/17/25 12:28:22 AM [ FTP] passive ports: 60000->60010
06/17/25 12:28:22 AM [ Diverter] Set DNS server 169.254.246.91 on the adapter: Ethernet
06/17/25 12:28:22 AM [ Diverter] OpenService failed for Dnscache
06/17/25 12:28:23 AM [ Diverter] svchost.exe (2096) requested UDP 169.254.246.91:53
06/17/25 12:28:23 AM [ DNS Server] Received A request for domain 'licensing.mp.microsoft.com' from svchost.exe (2096)
06/17/25 12:28:23 AM [ DNS Server] Received A request for domain 'www.msftconnecttest.com' from svchost.exe (2096)
06/17/25 12:28:24 AM [ Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:28:25 AM [ DNS Server] Received A request for domain 'api.msn.com' from svchost.exe (2096)
06/17/25 12:28:27 AM [ Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:28:30 AM [ Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:28:40 AM [ Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91

```

Open **Regshot** and take the first shot, saving it as a plain text log. Make sure to select the **Scan Directory** option and choose the top-level directory path (this is the best option for detecting any changes made on the storage disk). The process may take some time, so please be patient until it's complete.

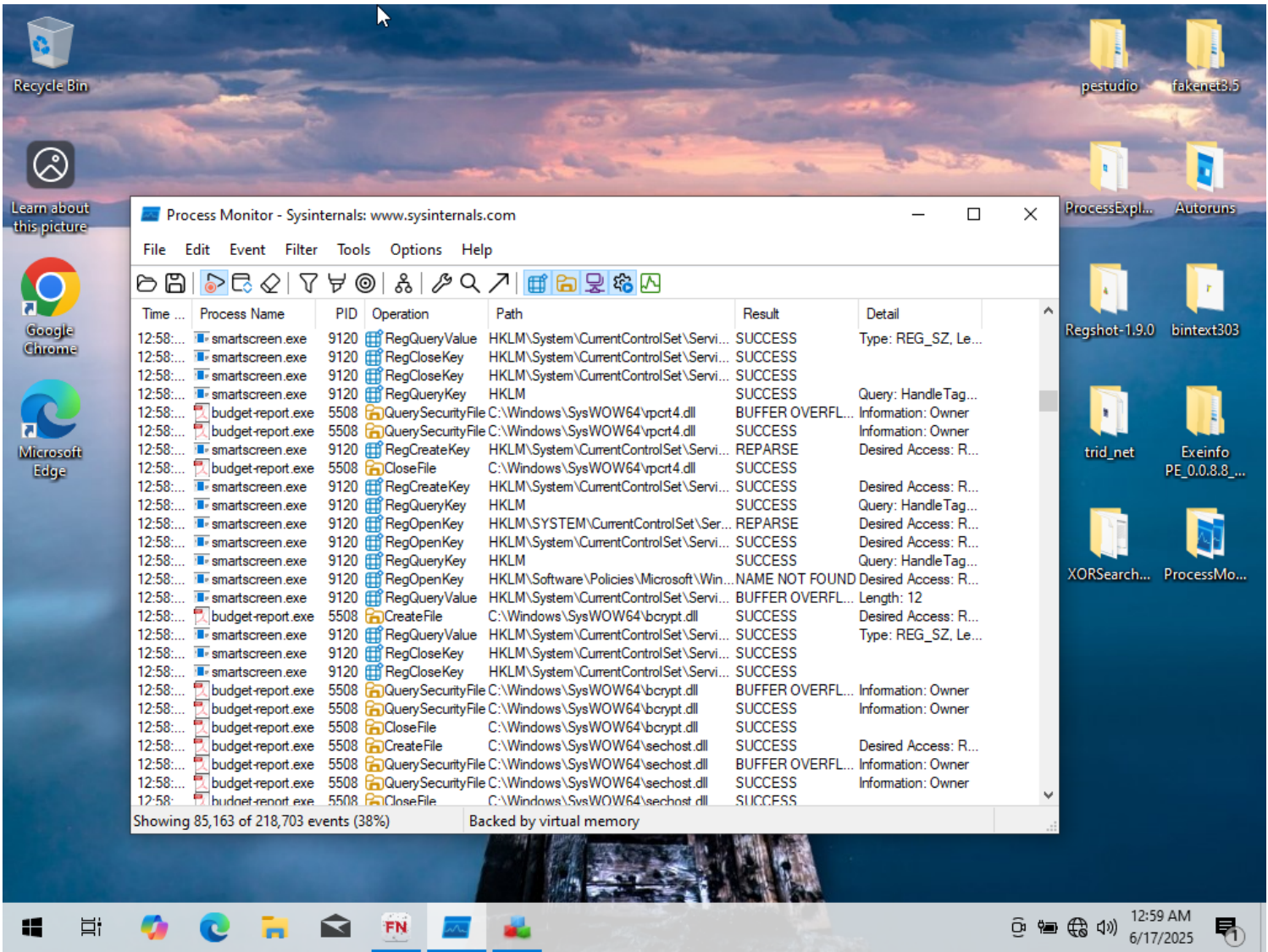


Once you've successfully taken the snapshot with Regshot, open **Process Monitor**. It will begin recording system events automatically. Pause the recording and clear the current logs before proceeding. Once the logs are cleared and you're ready to execute the malware, execute the malware.





The tool will begin recording all system events. Wait for a while until it captures a sufficient number of events occurring on the system.



Make sure to monitor the network activities as well. If you observe any suspicious or unfamiliar network connections, be sure to document them in your notes.

We observed a network request sent and received from **msedge.exe** to **Skype**. During the string analysis, we also identified the presence of the "Skype" string within the malware, which could indicate that the malware is attempting to use Skype's services.

```
Select C:\Users\target\Desktop\fakeNet3.5\fakeNet3.5\fakeNet.exe
06/17/25 12:55:07 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:55:11 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:55:15 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:55:21 AM [DNS Server] Received A request for domain 'cp601.prod.do.dsp.mp.microsoft.com' from svchost.exe (2096)
06/17/25 12:55:23 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:55:27 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:55:31 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:55:37 AM [DNS Server] Received A request for domain 'cp601.prod.do.dsp.mp.microsoft.com' from svchost.exe (2096)
06/17/25 12:55:39 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:55:43 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:55:47 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:55:55 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:57:50 AM [DNS Server] Received A request for domain 'storecatalogrevocation.storequality.microsoft.com' from svchost.exe (2096)
06/17/25 12:57:51 AM [DNS Server] Received A request for domain 'time.windows.com' from svchost.exe (2096)
06/17/25 12:57:52 AM [DNS Server] Received A request for domain 'time.windows.com' from svchost.exe (2096)
06/17/25 12:57:53 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:57:53 AM [DNS Server] Received A request for domain 'settings-win.data.microsoft.com' from svchost.exe (2096)
06/17/25 12:57:56 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:57:59 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:58:03 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:58:08 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:58:11 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:58:40 AM [DNS Server] Received A request for domain 'checkappexec.microsoft.com' from svchost.exe (2096)
06/17/25 12:58:42 AM [DNS Server] Received A request for domain 'update.microsoft.com' from svchost.exe (2096)
06/17/25 12:58:43 AM [DNS Server] Received A request for domain 'mbaquyahcn.biz' from svchost.exe (2096)
06/17/25 12:58:43 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:58:46 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:58:50 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:58:53 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:58:56 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:59:00 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:59:08 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:59:38 AM [Diverter] msedge.exe (5184) requested UDP 169.254.246.91:53
06/17/25 12:59:38 AM [DNS Server] Received A request for domain 'config.edge.skype.com' from msedge.exe (5184)
06/17/25 12:59:38 AM [DNS Server] Received HTTPS request for domain 'config.edge.skype.com' from msedge.exe (5184)
06/17/25 12:59:40 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:59:43 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:59:47 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
06/17/25 12:59:55 AM [Diverter] ICMP type 3 code 1 169.254.246.91->169.254.246.91
```



After a while, I stopped the Process Monitor and applied filters to display only the relevant malware related events. As seen below, there are still numerous events to review, fortunately with the help of effective filtering, I was able to narrow it down to the essential information.

Process Monitor - Sysinternals

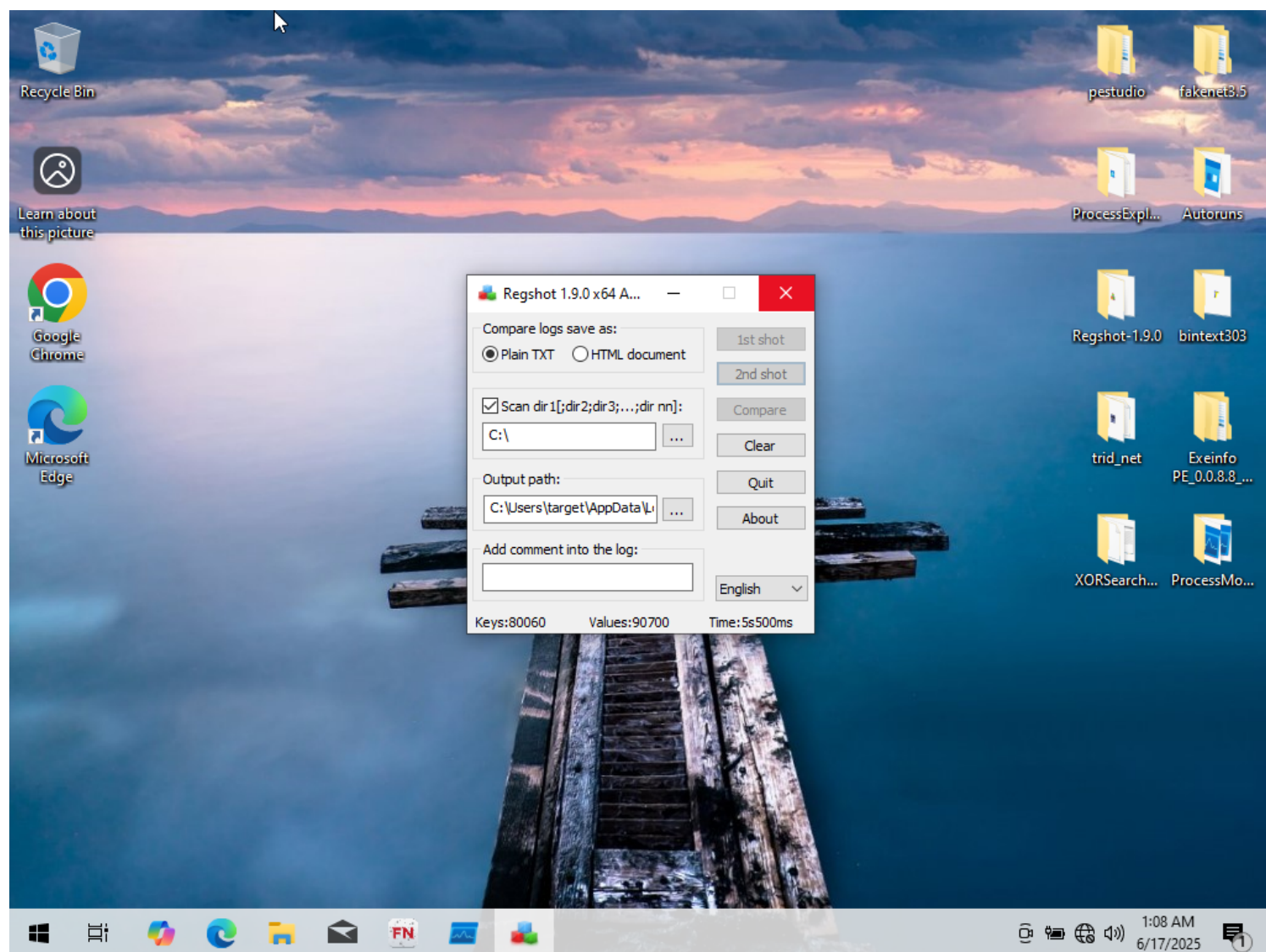
File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
12:58:...	budget-report.exe	5508	Process Start		SUCCESS	Parent PID: 4980, Comman...
12:58:...	budget-report.exe	5508	Thread Create		SUCCESS	Thread ID: 6964
12:58:...	budget-report.exe	5508	Load Image	C:\Users\target\Desktop\budget-report.exe	SUCCESS	Image Base: 0x400000, Ima...
12:58:...	budget-report.exe	5508	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7fd8c75000...
12:58:...	budget-report.exe	5508	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77a80000, I...
12:58:...	budget-report.exe	5508	CreateFile	C:\Windows\Prefetch\BUDGET-REPORT.EXE-A58A523E.pf	NAME NOT F...	Desired Access: Generic R...
12:58:...	budget-report.exe	5508	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value
12:58:...	budget-report.exe	5508	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value
12:58:...	budget-report.exe	5508	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibleDeadlock	NAME NOT F...	Length: 80
12:58:...	budget-report.exe	5508	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
12:58:...	budget-report.exe	5508	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap	REPARSE	Desired Access: Query Value
12:58:...	budget-report.exe	5508	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap	NAME NOT F...	Desired Access: Query Value
12:58:...	budget-report.exe	5508	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Valu...
12:58:...	budget-report.exe	5508	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Valu...
12:58:...	budget-report.exe	5508	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT F...	Length: 24
12:58:...	budget-report.exe	5508	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
12:58:...	budget-report.exe	5508	CreateFile	C:\Windows	SUCCESS	Desired Access: Execute/T...
12:58:...	budget-report.exe	5508	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x7fd8b14000...
12:58:...	budget-report.exe	5508	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x7fd8b57000...
12:58:...	budget-report.exe	5508	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT F...	Desired Access: Read Attrib...
12:58:...	budget-report.exe	5508	CreateFile	C:\Windows	SUCCESS	Desired Access: Read Attrib...
12:58:...	budget-report.exe	5508	QueryNameInfo...	C:\Windows	SUCCESS	Name: \Windows
12:58:...	budget-report.exe	5508	CloseFile	C:\Windows	SUCCESS	
12:58:...	budget-report.exe	5508	RegOpenKey	HKLM\Software\Microsoft\Wow64\wow64	SUCCESS	Desired Access: Read
12:58:...	budget-report.exe	5508	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\wow64\budget-report.exe	NAME NOT F...	Length: 520
12:58:...	budget-report.exe	5508	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\wow64(Default)	SUCCESS	Type: REG_SZ, Length: 26...
12:58:...	budget-report.exe	5508	RegCloseKey	HKLM\SOFTWARE\Microsoft\Wow64\wow64	SUCCESS	
12:58:...	budget-report.exe	5508	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x77a70000, I...
12:58:...	budget-report.exe	5508	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value
12:58:...	budget-report.exe	5508	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value
12:58:...	budget-report.exe	5508	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	KeySetInformationClass: Ke...
12:58:...	budget-report.exe	5508	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibleDeadlock	NAME NOT F...	Length: 80
12:58:...	budget-report.exe	5508	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
12:58:...	budget-report.exe	5508	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap	REPARSE	Desired Access: Query Value
12:58:...	budget-report.exe	5508	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap	NAME NOT F...	Desired Access: Query Value
12:58:...	budget-report.exe	5508	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Valu...
12:58:...	budget-report.exe	5508	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Valu...
12:58:...	budget-report.exe	5508	RegSetInfoKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	KeySetInformationClass: Ke...
12:58:...	budget-report.exe	5508	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT F...	Length: 24

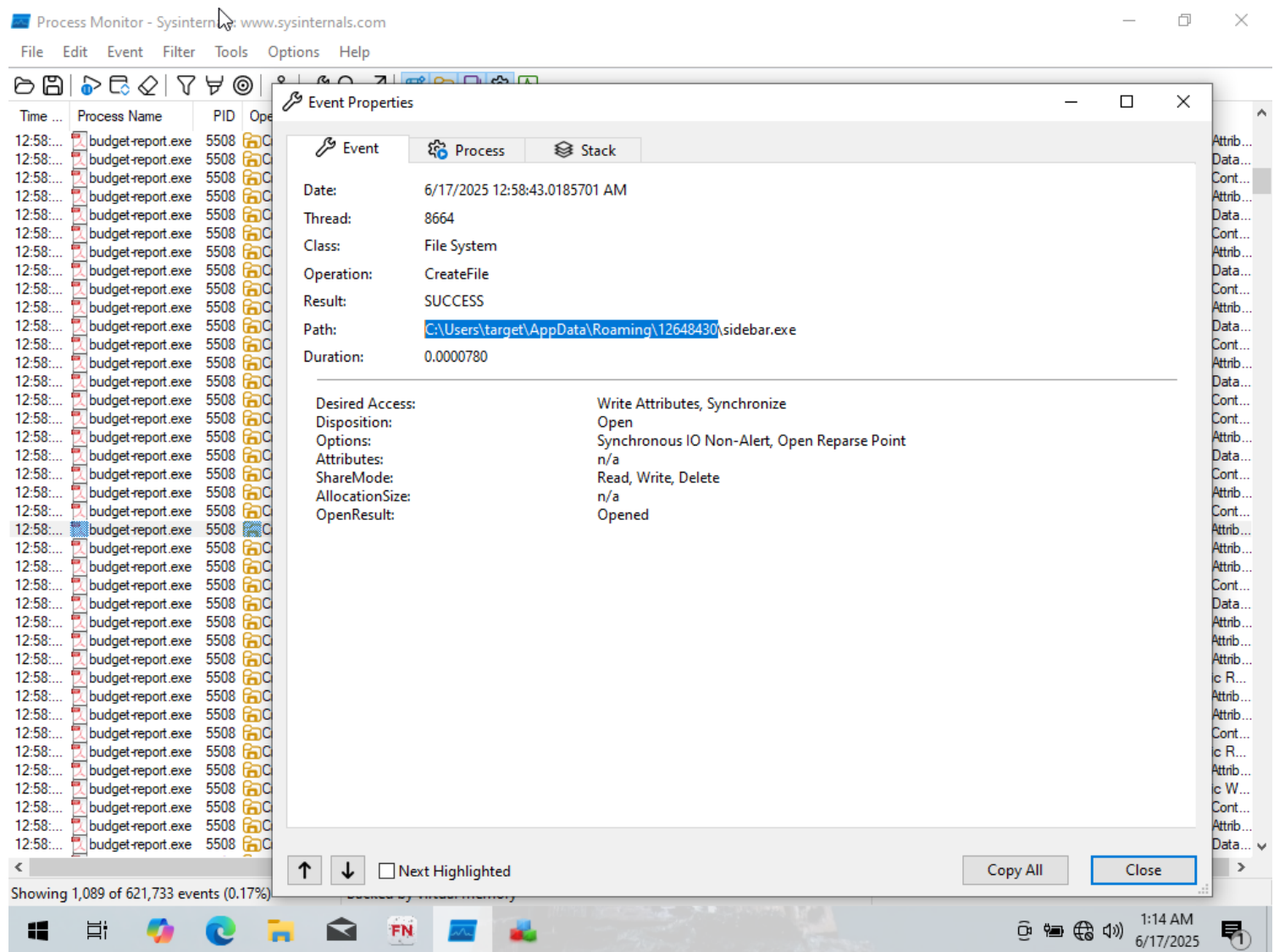
Showing 97,003 of 621,733 events (15%) Backed by virtual memory

1:07 AM 6/17/2025

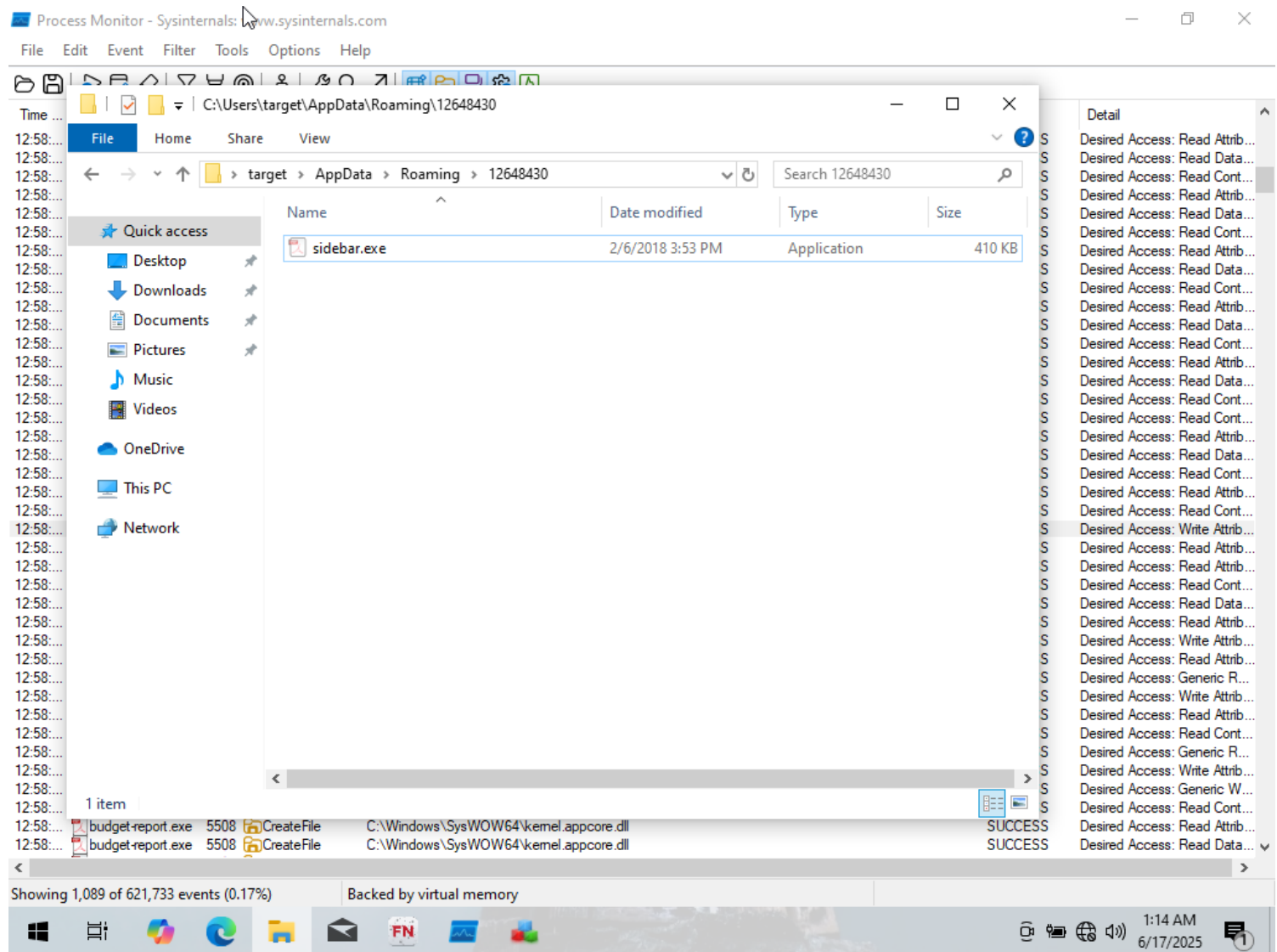
Now, let's take the second shot using the Regshot tool to analyze the changes made by the system during this period. The process may take some time, so let's go back to process monitor while it is running.



While analyzing the malware events using Process Monitor, we discovered a new file named **sidebar.exe** in the AppData folder.



We can verify the existence of this file by navigating to the following folder in File Explorer.

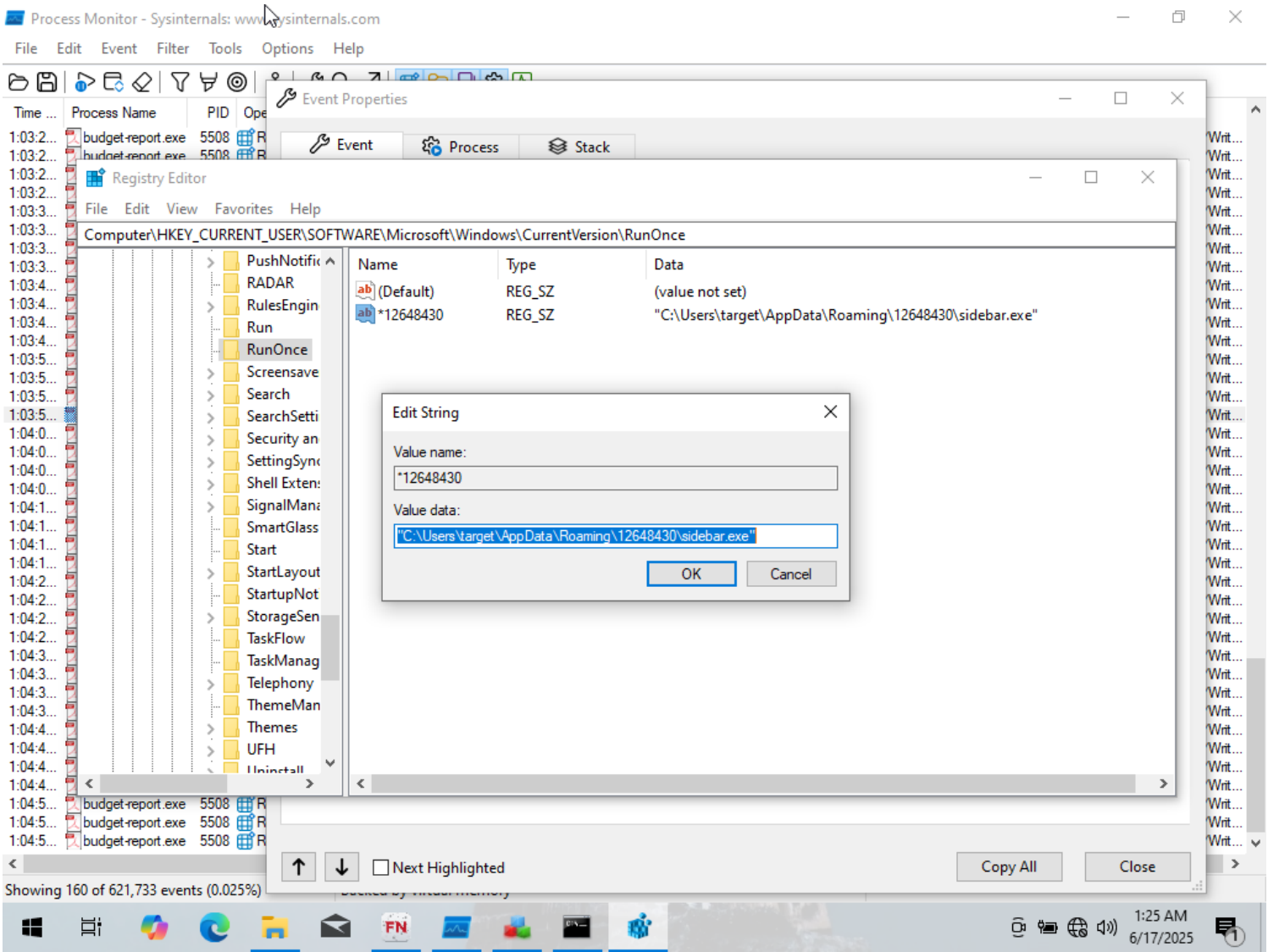




While analyzing the changes made to the registry, we observed that the file created a new entry in **HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce**. This registry key is commonly used to ensure the persistence of a file on the system, allowing it to run once at the next system startup.

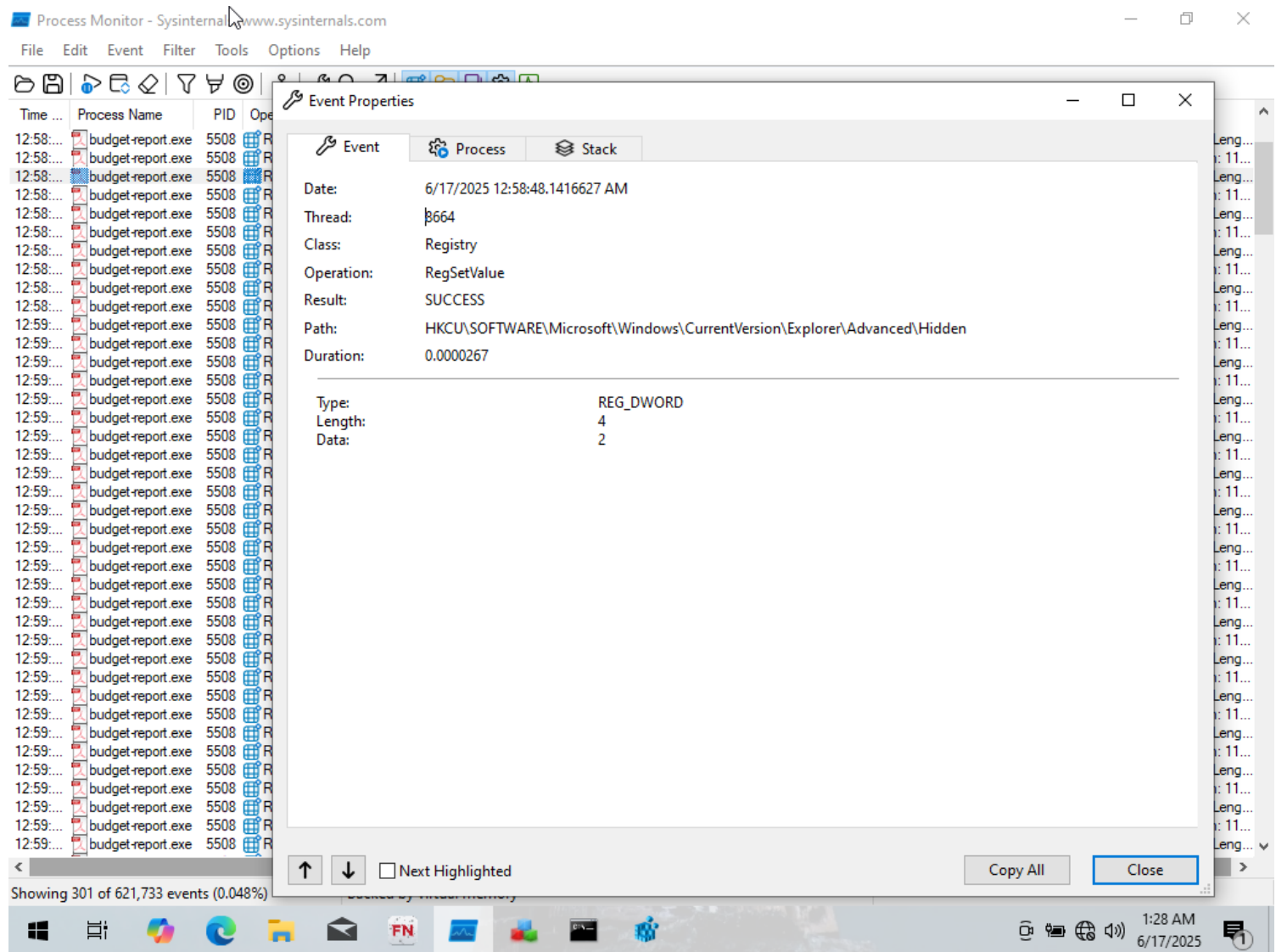
[illegible]

In the Registry Editor, when we navigate to the following path, we find an entry named **\*12648430**, which holds a value pointing to the file created by the malware.





We also found another intriguing registry change made by the malware in **HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden**, where its value was set to **2**.



By modifying this value, we can control the visibility of hidden files and folders in File Explorer.

1. **Value 0:** Hides protected operating system files and makes hidden files and folders invisible.
2. **Value 1:** Displays hidden files and folders, but still hides protected operating system files.
3. **Value 2:** Shows both hidden files, folders, and protected operating system files.



Time ...	Process Name	PID	Operation	Path	Result	Detail
12:58:...	budget-report.exe	5508	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\AutoDetect	SUCCESS	Type: REG_DWORD, Leng...
12:58:...	budget-report.exe	5508	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\*12648430	SUCCESS	Type: REG_SZ, Length: 11...
12:58:...	budget-report.exe	5508	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden	SUCCESS	Type: REG_DWORD, Leng...
12:58:...	budget-report.exe	5508	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\*12648430	SUCCESS	Type: REG_SZ, Length: 11...
12:58:...	budget-report.exe	5508	RegSetValue	HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Hidden	SUCCESS	Type: REG_DWORD, Leng...
12:58:...	Registry Editor					
12:58:...	File Edit View Favorites Help					
12:58:...	Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced					
12:59:...			Name	Type	Data	
12:59:...			(Default)	REG_SZ	(value not set)	
12:59:...			AutoCheckSelect	REG_DWORD	0x00000000 (0)	
12:59:...			DontPrettyPath	REG_DWORD	0x00000000 (0)	
12:59:...			Filter	REG_DWORD	0x00000000 (0)	
12:59:...			Hidden	REG_DWORD	0x00000002 (2)	
12:59:...			HideFileExt	REG_DWORD	0x00000000 (0)	
12:59:...			Hidelcons	REG_DWORD	0x00000000 (0)	
12:59:...			IconsOnly	REG_DWORD	0x00000000 (0)	
12:59:...			ListviewAlphaSe...	REG_DWORD	0x00000001 (1)	
12:59:...			ListviewShadow	REG_DWORD	0x00000001 (1)	
12:59:...			MapNetDrvBtn	REG_DWORD	0x00000000 (0)	
12:59:...			OnboardUnpinC...	REG_DWORD	0x00000001 (1)	
12:59:...			ReindexedProfile	REG_DWORD	0x00000001 (1)	
12:59:...			SeparateProcess	REG_DWORD	0x00000000 (0)	
12:59:...			ServerAdminUI	REG_DWORD	0x00000000 (0)	
12:59:...			ShowCompColor	REG_DWORD	0x00000001 (1)	
12:59:...			ShowCortanaBu...	REG_DWORD	0x00000000 (0)	
12:59:...			ShowInfoTip	REG_DWORD	0x00000001 (1)	
12:59:...			ShowStatusBar	REG_DWORD	0x00000001 (1)	
12:59:...			ShowSuperHidd...	REG_DWORD	0x00000001 (1)	
12:59:...			ShowTypeOverlay	REG_DWORD	0x00000001 (1)	

Edit DWORD (32-bit) Value

Value name:  
Hidden

Value data:  
2

Base  
☒ Hexadecimal  
☐ Decimal

OK Cancel

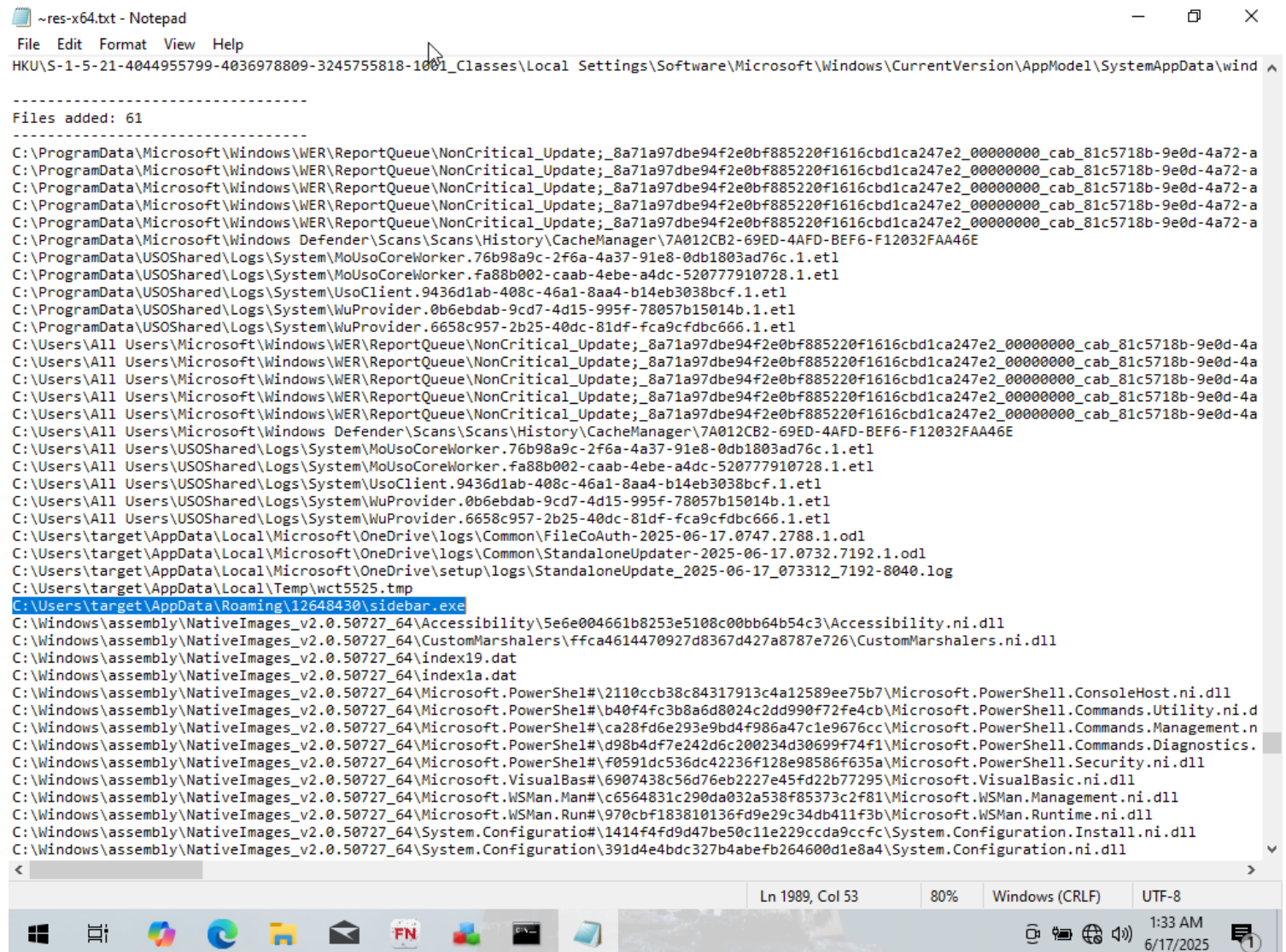
Showing 301 of 621,733 events (0.048%)

Backed by virtual memory



When we compare the shots taken by Regshot, we can observe information that aligns with what we already learned from the Process Monitor tool. There will likely be numerous activities recorded, but not all of them may be caused by the malware itself. Regshot is useful for identifying changes made to the system over a specific period of time.

In the image below, we can see that the **sidebar.exe** file has been created.



```
~res-x64.txt - Notepad
File Edit Format View Help
HKU\S-1-5-21-4044955799-4036978809-3245755818-1001_Classes\Local Settings\Software\Microsoft\Windows\CurrentVersion\AppModel\SystemAppData\wind
-----
Files added: 61
-----
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\NonCritical_Update;_8a71a97dbe94f2e0bf885220f1616cbd1ca247e2_00000000_cab_81c5718b-9e0d-4a72-a
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\NonCritical_Update;_8a71a97dbe94f2e0bf885220f1616cbd1ca247e2_00000000_cab_81c5718b-9e0d-4a72-a
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\NonCritical_Update;_8a71a97dbe94f2e0bf885220f1616cbd1ca247e2_00000000_cab_81c5718b-9e0d-4a72-a
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\NonCritical_Update;_8a71a97dbe94f2e0bf885220f1616cbd1ca247e2_00000000_cab_81c5718b-9e0d-4a72-a
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\NonCritical_Update;_8a71a97dbe94f2e0bf885220f1616cbd1ca247e2_00000000_cab_81c5718b-9e0d-4a72-a
C:\ProgramData\Microsoft\Windows Defender\Scans\Scans\History\CacheManager\7A012CB2-69ED-4AFD-BEF6-F12032FAA46E
C:\ProgramData\USOShared\Logs\System\MoUsoCoreWorker.76b98a9c-2f6a-4a37-91e8-0db1803ad76c.1.etl
C:\ProgramData\USOShared\Logs\System\MoUsoCoreWorker.fa88b002-caab-4ebe-a4dc-520777910728.1.etl
C:\ProgramData\USOShared\Logs\System\Usoclient.9436d1ab-408c-46a1-8aa4-b14eb3038bcf.1.etl
C:\ProgramData\USOShared\Logs\System\WuProvider.0b6ebdab-9cd7-4d15-995f-78057b15014b.1.etl
C:\ProgramData\USOShared\Logs\System\WuProvider.6658c957-2b25-40dc-81df-fca9cfdbc666.1.etl
C:\Users\All Users\Microsoft\Windows\WER\ReportQueue\NonCritical_Update;_8a71a97dbe94f2e0bf885220f1616cbd1ca247e2_00000000_cab_81c5718b-9e0d-4a
C:\Users\All Users\Microsoft\Windows\WER\ReportQueue\NonCritical_Update;_8a71a97dbe94f2e0bf885220f1616cbd1ca247e2_00000000_cab_81c5718b-9e0d-4a
C:\Users\All Users\Microsoft\Windows\WER\ReportQueue\NonCritical_Update;_8a71a97dbe94f2e0bf885220f1616cbd1ca247e2_00000000_cab_81c5718b-9e0d-4a
C:\Users\All Users\Microsoft\Windows\WER\ReportQueue\NonCritical_Update;_8a71a97dbe94f2e0bf885220f1616cbd1ca247e2_00000000_cab_81c5718b-9e0d-4a
C:\Users\All Users\Microsoft\Windows\WER\ReportQueue\NonCritical_Update;_8a71a97dbe94f2e0bf885220f1616cbd1ca247e2_00000000_cab_81c5718b-9e0d-4a
C:\Users\All Users\Microsoft\Windows Defender\Scans\Scans\History\CacheManager\7A012CB2-69ED-4AFD-BEF6-F12032FAA46E
C:\Users\All Users\USOShared\Logs\System\MoUsoCoreWorker.76b98a9c-2f6a-4a37-91e8-0db1803ad76c.1.etl
C:\Users\All Users\USOShared\Logs\System\MoUsoCoreWorker.fa88b002-caab-4ebe-a4dc-520777910728.1.etl
C:\Users\All Users\USOShared\Logs\System\Usoclient.9436d1ab-408c-46a1-8aa4-b14eb3038bcf.1.etl
C:\Users\All Users\USOShared\Logs\System\WuProvider.0b6ebdab-9cd7-4d15-995f-78057b15014b.1.etl
C:\Users\All Users\USOShared\Logs\System\WuProvider.6658c957-2b25-40dc-81df-fca9cfdbc666.1.etl
C:\Users\target\AppData\Local\Microsoft\OneDrive\logs\Common\FileCoAuth-2025-06-17.0747.2788.1.odl
C:\Users\target\AppData\Local\Microsoft\OneDrive\logs\StandaloneUpdater-2025-06-17.0732.7192.1.odl
C:\Users\target\AppData\Local\Microsoft\OneDrive\logs\StandaloneUpdate_2025-06-17_073312_7192-8040.log
C:\Users\target\AppData\Local\Temp\wct5525.tmp
C:\Users\target\AppData\Roaming\12648430\sidebar.exe
C:\Windows\assembly\NativeImages_v2.0.50727_64\Accessibility\5e6e004661b8253e5108c00bb64b54c3\Accessibility.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\CustomMarshalers\ffca4614470927d8367d427a8787e726\CustomMarshalers.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\index19.dat
C:\Windows\assembly\NativeImages_v2.0.50727_64\index1a.dat
C:\Windows\assembly\NativeImages_v2.0.50727_64\Microsoft.PowerShell#2110ccb38c84317913c4a12589ee75b7\Microsoft.PowerShell.ConsoleHost.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\Microsoft.PowerShell#b40f4fc3b8a6d80242dd990f72fe4cb\Microsoft.PowerShell.Commands.Utility.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\Microsoft.PowerShell#ca28fd6e293e9bd4f986a47c1e9676cc\Microsoft.PowerShell.Commands.Management.n
C:\Windows\assembly\NativeImages_v2.0.50727_64\Microsoft.PowerShell#d98b4df7e242d6c200234d30699f74f1\Microsoft.PowerShell.Commands.Diagnostics.
C:\Windows\assembly\NativeImages_v2.0.50727_64\Microsoft.PowerShell#f0591dc536dc42236f128e98586f635a\Microsoft.PowerShell.Security.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\Microsoft.VisualBasic#6907438c56d76eb2227e45fd22b77295\Microsoft.VisualBasic.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\Microsoft.WSMan.Man#1c6564831c290da032a538f85373c2f81\Microsoft.WSMan.Management.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\Microsoft.WSMan.Run#970cbf183810136fd9e29c34db411f3b\Microsoft.WSMan.Runtime.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Configuration#1414f4fd9d47be50c11e229ccda9ccfc\System.Configuration.Install.ni.dll
C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Configuration\391d4e4bdc327b4abefb264600d1e8a4\System.Configuration.ni.dll
```

Scrolling down, we can see the files that were deleted by the malware after execution. This confirms that the malware deletes itself to prevent detection and analysis.

```
~res-x64.txt - Notepad
File Edit Format View Help

-----
Files deleted: 18
-----
C:\ProgramData\Microsoft\Windows Defender\Scans\History\Store\27C40AED31E6A3C361488CEC2D6A78E8
C:\ProgramData\Microsoft\Windows Defender\Scans\History\Store\2BEF88BEF2BE4B114417B3A79A03113D
C:\ProgramData\Microsoft\Windows Defender\Scans\History\Store\7762991023F75C8B49E772012D60BDF2
C:\ProgramData\Microsoft\Windows Defender\Scans\History\Store\BC7C903D8DCF8425829F238594EA7282
C:\ProgramData\Microsoft\Windows Defender\Scans\History\Store\D0849D9157D1F87E14CAF8027154F0A1
C:\ProgramData\Microsoft\Windows Defender\Scans\History\Store\DD1FD9AD19791C0B4D8F8BF6583B4492
C:\Users\All Users\Microsoft\Windows Defender\Scans\History\Store\27C40AED31E6A3C361488CEC2D6A78E8
C:\Users\All Users\Microsoft\Windows Defender\Scans\History\Store\2BEF88BEF2BE4B114417B3A79A03113D
C:\Users\All Users\Microsoft\Windows Defender\Scans\History\Store\7762991023F75C8B49E772012D60BDF2
C:\Users\All Users\Microsoft\Windows Defender\Scans\History\Store\BC7C903D8DCF8425829F238594EA7282
C:\Users\All Users\Microsoft\Windows Defender\Scans\History\Store\D0849D9157D1F87E14CAF8027154F0A1
C:\Users\All Users\Microsoft\Windows Defender\Scans\History\Store\DD1FD9AD19791C0B4D8F8BF6583B4492
C:\Users\target\Desktop\budget-report.exe
C:\Windows\assembly\NativeImages_v2.0.50727_64\indexc.dat
C:\Windows\assembly\NativeImages_v2.0.50727_64\indexd.dat
C:\Windows\SoftwareDistribution\DataStore\Logs\tmp.edb
C:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\InstallService\{76C4EC8A-41CC-4648-8CD2-A52739D81FEC}.checkpoint
C:\Windows\System32\Tasks\Microsoft\Windows\Setup\SetupCleanupTask

-----
Files [attributes?] modified: 159
-----
C:\Program Files (x86)\Google\GoogleUpdater\138.0.7194.0\Crashpad\settings.dat
C:\Program Files (x86)\Google\GoogleUpdater\prefs.json
C:\Program Files (x86)\Google\GoogleUpdater\updater.log
C:\Program Files (x86)\Microsoft\EdgeUpdate\Download\{F3017226-FE2A-4295-8BDF-00C3A9A7E4C5}\137.0.3296.83\MicrosoftEdge_X64_137.0.3296.83.exe
C:\ProgramData\Microsoft\Diagnosis\EventStore.db-wal
C:\ProgramData\Microsoft\EdgeUpdate\Log\MicrosoftEdgeUpdate.log
C:\ProgramData\Microsoft\Network\Downloader\edb.chk
C:\ProgramData\Microsoft\Network\Downloader\edb.log
C:\ProgramData\Microsoft\Network\Downloader\qmgr.db
C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm
C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Deployment.srd
C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Deployment.srd-shm
C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Deployment.srd-wal
C:\ProgramData\Microsoft\Windows\AppRepository\StateRepository-Machine.srd-wal
C:\ProgramData\Microsoft\Windows\WER\ReportQueue\NonCritical_Acquisition;9N8M_fd67a1d70e0ce932ff56f2c3e22d64ca550_00000000_cab_523c8a8b-76b5-40
C:\ProgramData\Microsoft\Windows Defender\Support\MPDetection-20250614-224915.log
C:\ProgramData\Microsoft\Windows Defender\Support\MPDeviceControl-20250615-084151.log
C:\ProgramData\Microsoft\Windows Defender\Support\MPLog-20250614-224915.log
C:\ProgramData\Microsoft\Windows Defender\Support\MPScanSkip-20250615-084151.log
C:\ProgramData\Microsoft\Windows Defender\Support\MpiWppCoreTracing-20250617-000835-00000003-100000000.bin
```