Malware Analysis Report:

[37cqsj.exe]

By: Liad Bahari.

Analysis Date: 27/11/2025.

Enjoy Reading 😊

General Information

- **Original File Name: 37cqsj.exe**
- **MD5: 64bdd94921a2d2daa4ccd8cfe2ce74ef**
- **SHA1: 14bc94f5ee27621af1c4ca02064fe0a63a698634**
- IMPHASH: 099c0646ea7282d232219f8807883be0
- **File Size: 1'584'368 bytes = 1.584368 MB**
- **First Seen: 2025-11-24**
- **Number Of Downloads (Until the date above) : 107**
- **Origin Country: 🇮🇱 IL**
- **File Type: Adware (Adware.PushWare)**
- **The file also known as:**

"ba9b47b7c3d69397cf50583df171b5ca71a5726e2a24e0f788dbef2319b8672e .exe"

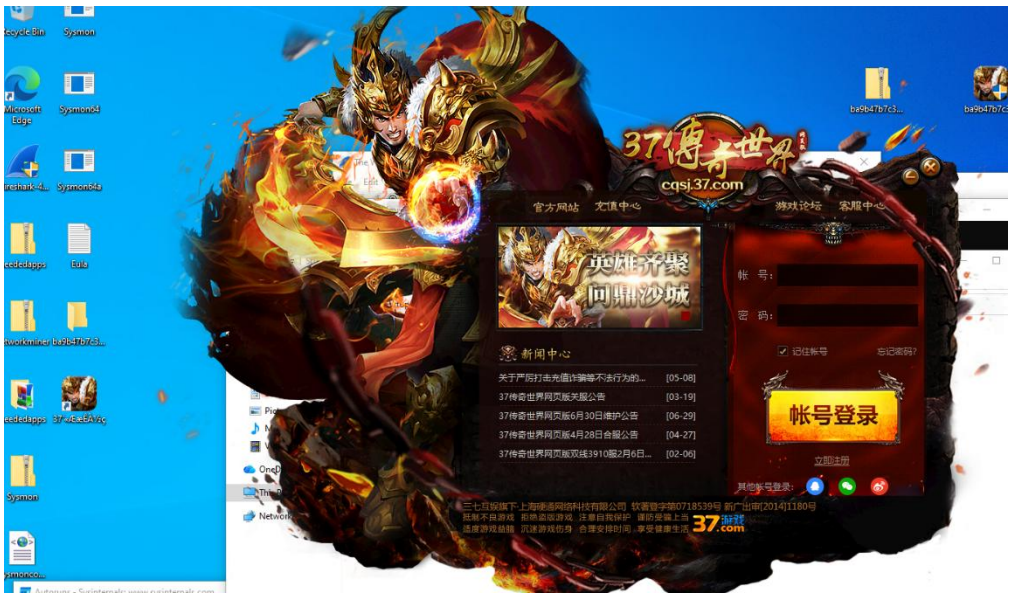
A little about the file

37cqsj.exe is a Unwanted software (PUP) that forcefully displays intrusive advertisements, often by tracking your online activity and pushing pop-up .

Analysis Overview:

32cqsj.exe being identified as Adware that pops up on the screen when executed - looks like a "computer game". The file downloads some pictures for its visualization HTTP GET request (JPG, PNG, etc.). Surprisingly, the file does not maintain a Persistence via REGISTRY paths = It does not come up when the system is restarted (startup). Also it starts On-Execution Only.

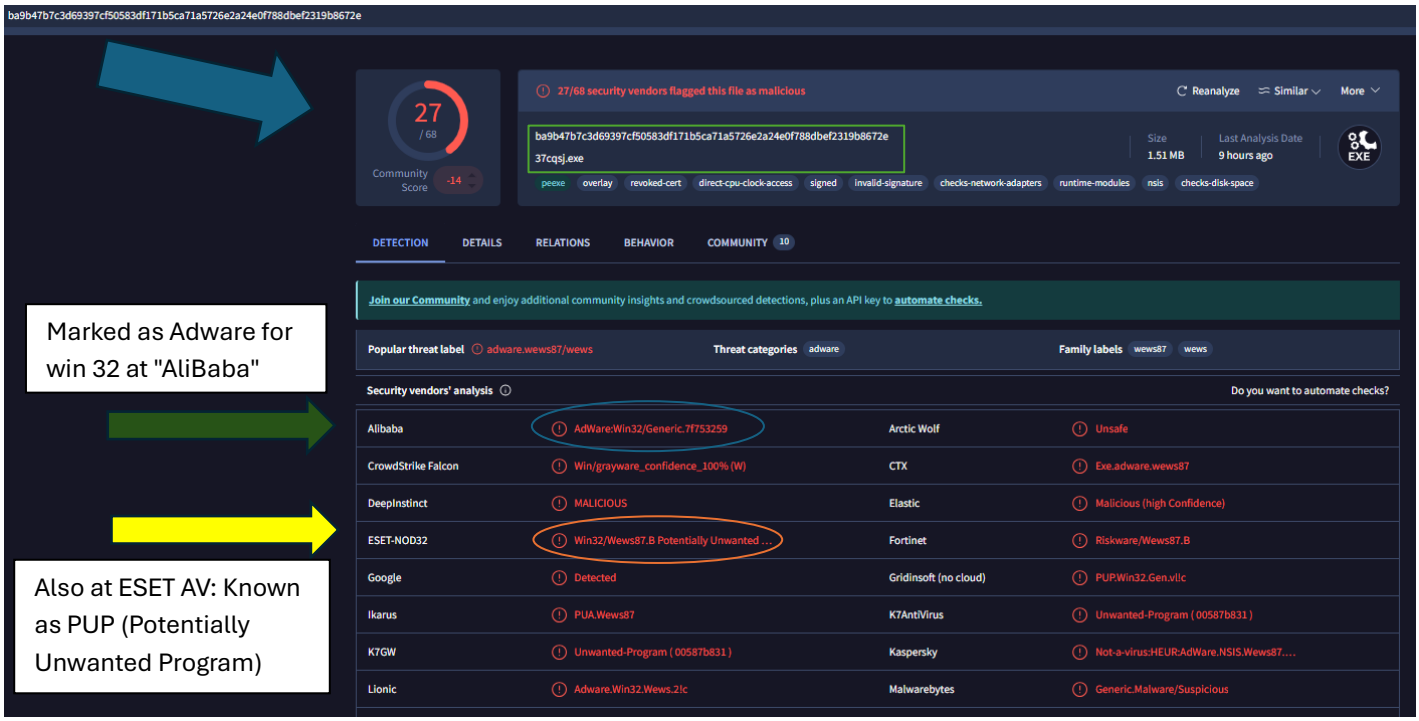
Table of Contents



(picture of 37cqsj.exe.)

Static Analysis:

First Static Analysis on Virus Total



Marked as Adware for win 32 at "AliBaba"

Also at ESET AV: Known as PUP (Potentially Unwanted Program)

From this we understand that the malware is marked as suspicious by many tests and companies.

Exiftool using:

```
└─$ exiftool 562582ffed521b0144b0120cc7dfd5fb50c38e94d6c10a86f9ef800ff0cf7bd1.exe
ExifTool Version Number         : 13.25
File Name                       : 562582ffed521b0144b0120cc7dfd5fb50c38e94d6c10a86f9ef800ff0cf7bd1.exe
Directory                       : .
File Size                       : 2.8 MB
File Modification Date/Time     : 2025:11:23 16:35:50-05:00
File Access Date/Time           : 2025:11:23 11:37:13-05:00
File Inode Change Date/Time     : 2025:11:23 11:36:14-05:00
File Permissions                : -rw-r--r--
File Type                       : Win64 EXE
File Type Extension             : exe
MIME Type                       : application/octet-stream
Machine Type                    : AMD AMD64
Time Stamp                      : 0000:00:00 00:00:00
Image File Characteristics      : Executable, Large address aware
PE Type                         : PE32+
Linker Version                  : 3.0
Code Size                       : 1000448
Initialized Data Size           : 48128
Uninitialized Data Size         : 0
Entry Point                     : 0×695a0
OS Version                      : 6.1
Image Version                   : 1.0
Subsystem Version               : 6.1
Subsystem                       : Windows GUI
```

Volatility tool:

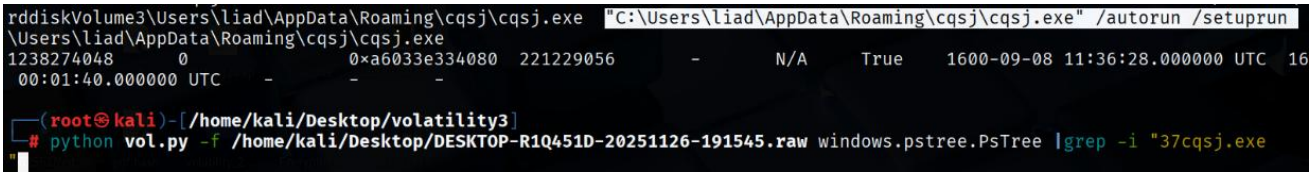
Trying to check for persistence.

Taking the ".raw" file of the memory dump while executing the ADWARE.

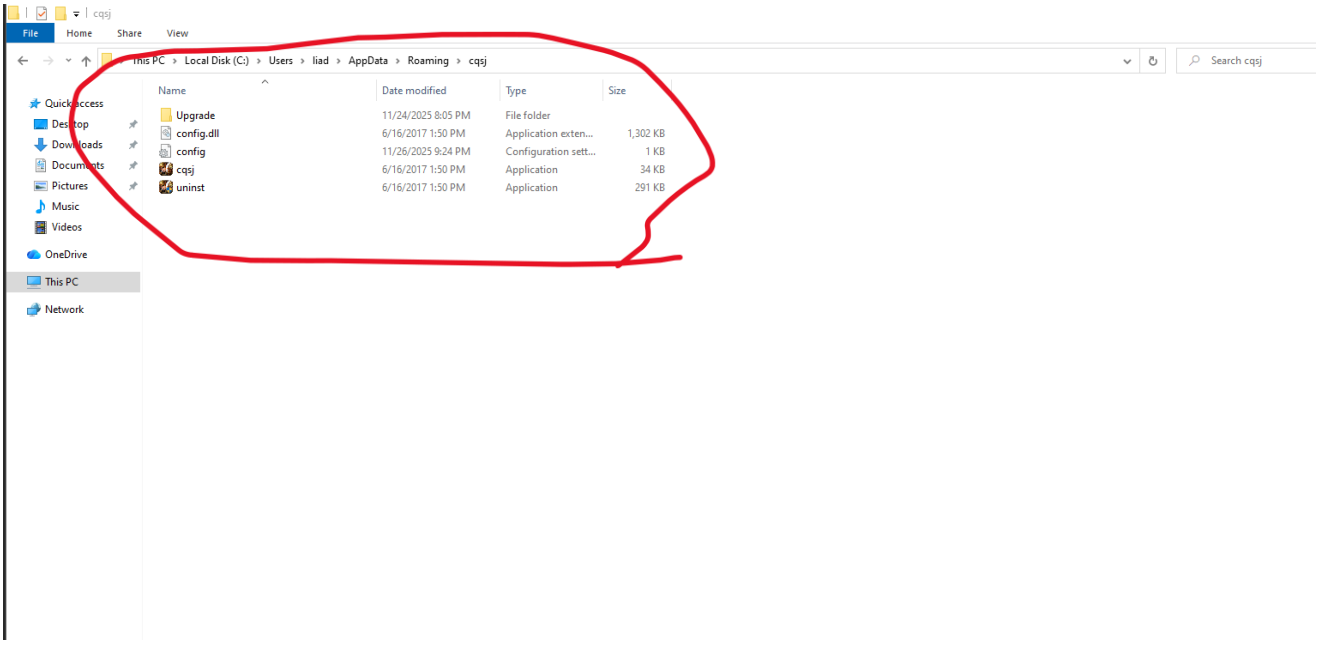
With the VOL3 command and its plugin "windows.pstree", we found that

there is Created storage of the file and its configuration extensions in the folder: "C:\Users\liad\AppData\Roaming\cqsj\cqsj.exe".

The software has set itself to load automatically every time the computer is turned on. It "hooks" into the system to ensure that the advertisements (like the one you saw in the first image) continue to appear.



And when we get into this specific path We can see this visually.



STRINGS tool:

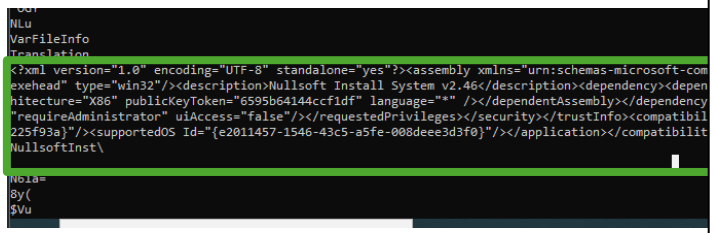
According to STRINGS, you can see that the file knows how to:

- **Read/write/delete files (CreateFileA, ReadFile, WriteFile, DeleteFileA, CopyFileA, MoveFileA, CreateDirectoryA, RemoveDirectoryA, GetTempPathA, GetTempFileNameA).**
- **Work with Registry (RegCreateKeyExA, RegSetValueExA, RegDeleteKeyA, RegEnumKeyA, RegEnumValueA), i.e. add/delete/modify keys – whether for legitimate installation or Persistence.**
- **Display GUI and manage windows and dialog boxes (MessageBoxIndirectA, CreateDialogParamA, DialogBoxParamA, ShowWindow, SetWindowTextA, TrackPopupMenu, etc.) – classic installation interface.**
- **Perform shell operations such as ShellExecuteA, SHFileOperationA, SHBrowseForFolderA, SHGetSpecialFolderLocation, SHGetFolderPathA – open files/folders, shortcut, select folder.**
- **Work with advanced privileges (OpenProcessToken, AdjustTokenPrivileges, LookupPrivilegeValueA, SeShutdownPrivilege) – for example, allow startup/shutdown after installation or delete locked files.**

All things relevant to the INSTALLER of a particular application.

In addition, the file uses a lot of DLLs that were captured during the STRINGS command.

Using the STRINGS command we can see legitimate DLL's unlike the dynamic analysis within the PROCESS MONITOR below.



This is an XML format text that tells the system what type of OS the endpoint is, what configurations it works with, whether it requires ADMIN permissions, etc. In addition, it means that an NSIS Installer file:

Not a "pure" EXE file, but an installer with a payload inside.

It allows hiding internal files.

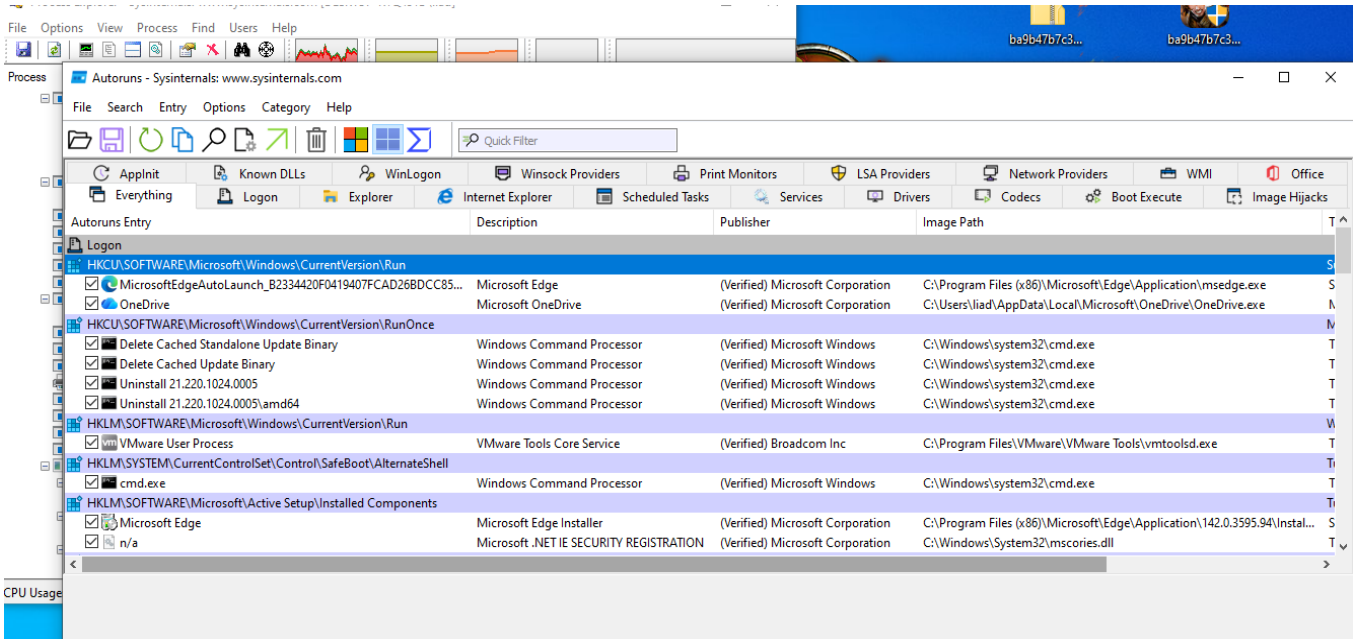
Allows unzip of payload at runtime.

Allows scripts (.nsi files).

Dynamic Analysis:

Persistence via Registry Changes (with "Autorun"):

With a short Investigation on AUTORUN by "sysinternals" we understand that there is no Registry change for persistence purposes.



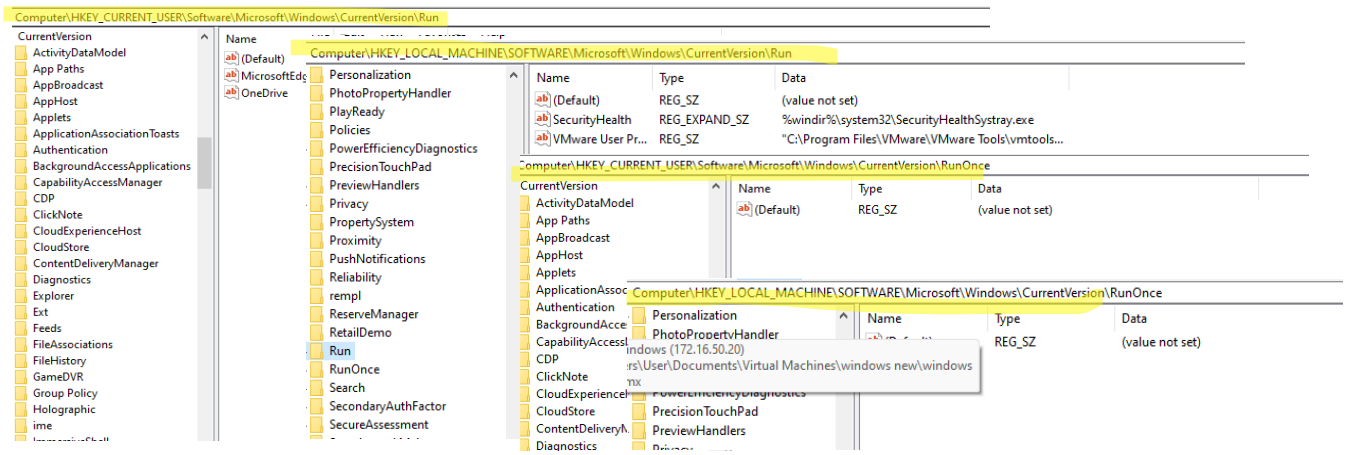
In addition, no changes were found in the REGISTRY paths themselves within the "Regedit" software. - The reg - keys checked:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

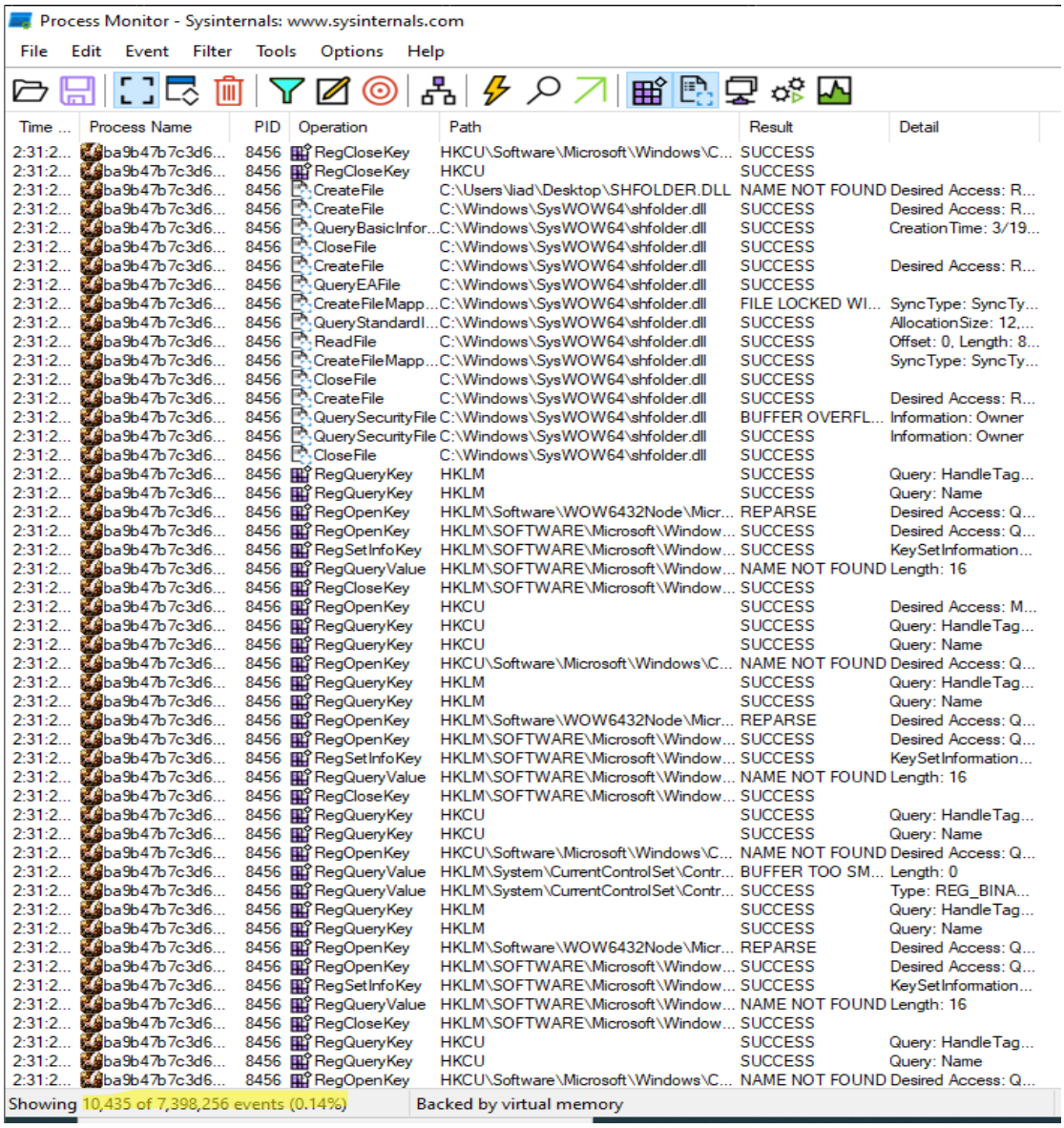
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run



Investigation at ProcessMonitor:

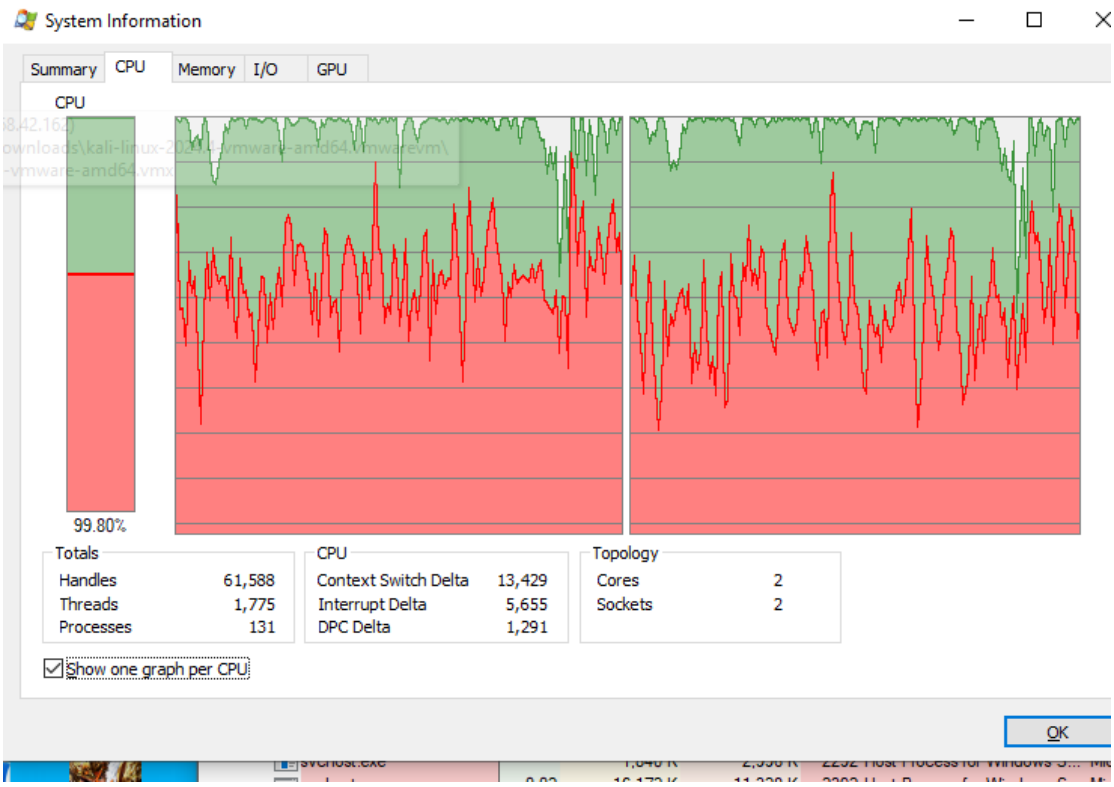
The adware creates registry keys to temporarily activate functions or run code that it executes in real time, and not with the intention of maintaining persistence over time. This could be, for example, temporary values for tracking or payload delivery. (NO PERSISTENCE !)

The adware is trying to modify lots of registry paths to perform an action such as loading a DLL, connecting to a network, or changing settings, and then closes them when the action is complete so that no visible traces are left or the system retains them.



We can see a huge number of events shown at The Adware's execution and until its exit and close itself. (taked at ProcessMonitor)

As we said earlier, because of the many processes it creates, it uses the computer's resources (CPU) in an increased and disproportionate way.



(at process explorer)

Wireshark:

Using wireshark network packets analyzer, We can see quite a few different network packets.

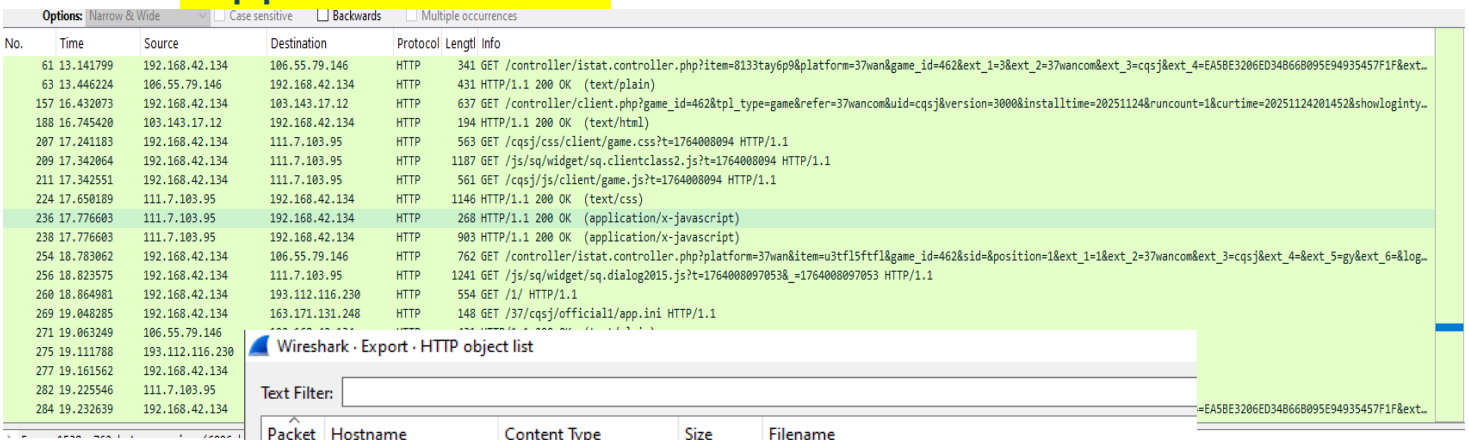
The packets I focused on mostly belong to the DNS and HTTP protocols.

According to the HTTP requests I investigated, we can see many requests mainly to sites with the ".com" extension in China, such as "https://my.37.com" , "http://d.wanyouxi7.com/37/cqsj/official1/app.ini" and more.

Our ADWARE also uses HTTP GET requests that it sends from the browser on owr end-device where it is located. Most of the HTTP requests included downloads of settings and applications in JAVASCRIPT and CSS code, apparently to be used for visualization of the ADWARE file.

From this we understand that the application gains access to free communication with our network while executed – we don't want it !.

Http packets in wireshark



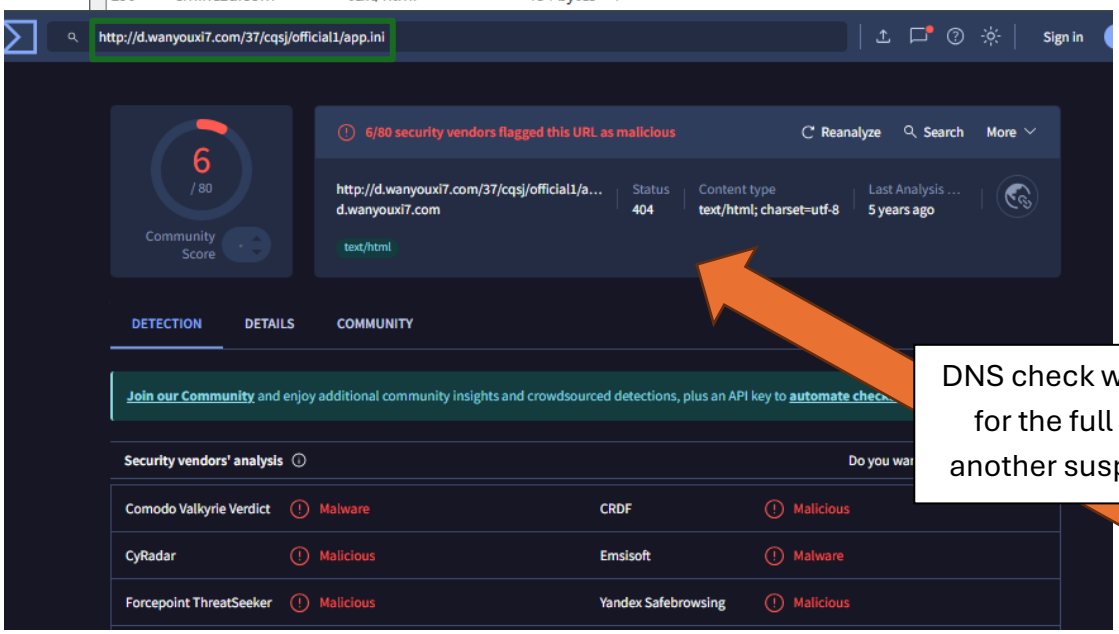
No.	Time	Source	Destination	Protocol	Length	Info
61	13.141799	192.168.42.134	106.55.79.146	HTTP	341	GET /controller/istat.controller.php?item=8133tay6p9&platform=37wan&game_id=462&ext_1=3&ext_2=37wancom&ext_3=cqsj&ext_4=EA5BE3206ED34B66B095E94935457F1F&ext…
63	13.446224	106.55.79.146	192.168.42.134	HTTP	431	HTTP/1.1 200 OK (text/plain)
157	16.432073	192.168.42.134	103.143.17.12	HTTP	637	GET /controller/client.php?game_id=462&tpl_type=game&refer=37wancom&uid=cqsj&version=3000&installtime=20251124&runcount=1&curtime=20251124201452&showloginty…
188	16.745420	103.143.17.12	192.168.42.134	HTTP	194	HTTP/1.1 200 OK (text/html)
207	17.241183	192.168.42.134	111.7.103.95	HTTP	563	GET /cqsj/css/client/game.css?t=1764008094 HTTP/1.1
209	17.342064	192.168.42.134	111.7.103.95	HTTP	1187	GET /js/sq/widget/sq.clientclass2.js?t=1764008094 HTTP/1.1
211	17.342551	192.168.42.134	111.7.103.95	HTTP	561	GET /cqsj/js/client/game.js?t=1764008094 HTTP/1.1
224	17.650189	111.7.103.95	192.168.42.134	HTTP	1146	HTTP/1.1 200 OK (text/css)
236	17.776603	111.7.103.95	192.168.42.134	HTTP	268	HTTP/1.1 200 OK (application/x-javascript)
238	17.776603	111.7.103.95	192.168.42.134	HTTP	903	HTTP/1.1 200 OK (application/x-javascript)
254	18.783062	192.168.42.134	106.55.79.146	HTTP	762	GET /controller/istat.controller.php?platform=37wan&item=u3tfl5ftfl&game_id=462&sid=&position=1&ext_1=1&ext_2=37wancom&ext_3=cqsj&ext_4=&ext_5=gy&ext_6=&log…
256	18.823575	192.168.42.134	111.7.103.95	HTTP	1241	GET /js/sq/widget/sq.dialog2015.js?t=17640080970538_=1764008097053 HTTP/1.1
260	18.864981	192.168.42.134	193.112.116.230	HTTP	554	GET /1/ HTTP/1.1
269	19.048285	192.168.42.134	163.171.131.248	HTTP	148	GET /37/cqsj/official1/app.ini HTTP/1.1
271	19.063249	106.55.79.146				
275	19.111788	193.112.116.230				
277	19.161562	192.168.42.134				
282	19.225546	111.7.103.95				
284	19.232639	192.168.42.134				

Wireshark · Export · HTTP object list

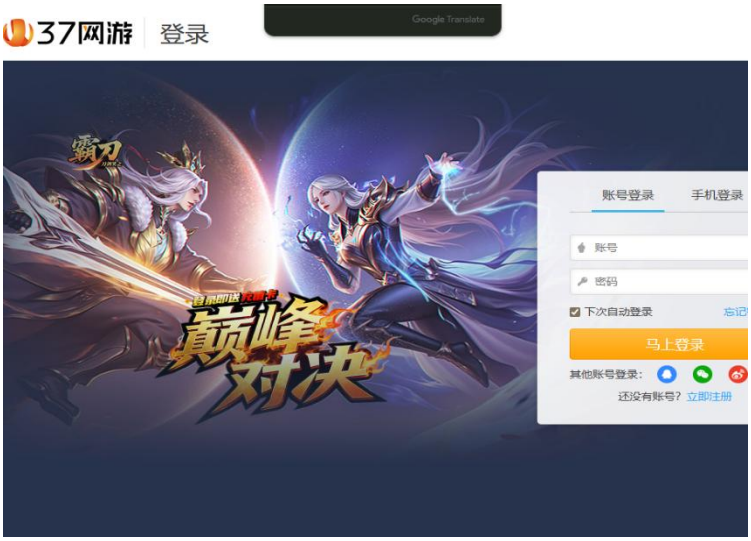
Text Filter:

Packet	Hostname	Content Type	Size	Filename
	a.clickdata.37wan.com	text/plain	38 bytes	istat.controller.php?item=8133tay6p9&platform=37wan&g
	gameapp.37.com	text/html	9728 bytes	client.php?game_id=462&tpl_type=game&refer=37wancor
	img1.37wanimg.com	application/x-javascript	3813 bytes	game.js?t=1764250086
	ptres.37.com	application/x-javascript	45 kB	sq.clientclass2.js?t=1764250086
	img1.37wanimg.com	text/css	12 kB	game.css?t=1764250086
	d.wanyouxi7.com	text/html	168 bytes	app.ini
286	a.clickdata.37wan.com	text/plain	38 bytes	istat.controller.php?platform=37wan&item=u3tfl5ftfl&gam
290	cm.he2d.com	text/html	154 bytes	1

It downloads app.ini – configuration file



DNS check with virus total for the full URL brings to another suspicious pages

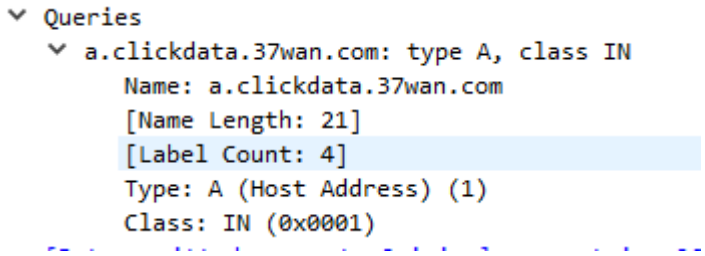


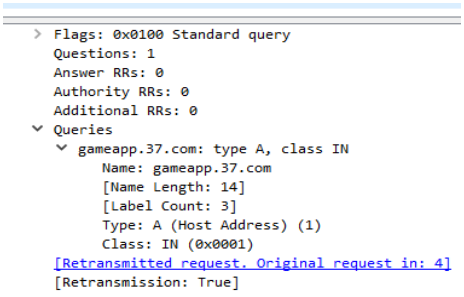
"https://my.37.com"

The site that **was Found at the DNS communications - between (my) client browser (by '37cqsj.exe') and the internet.**

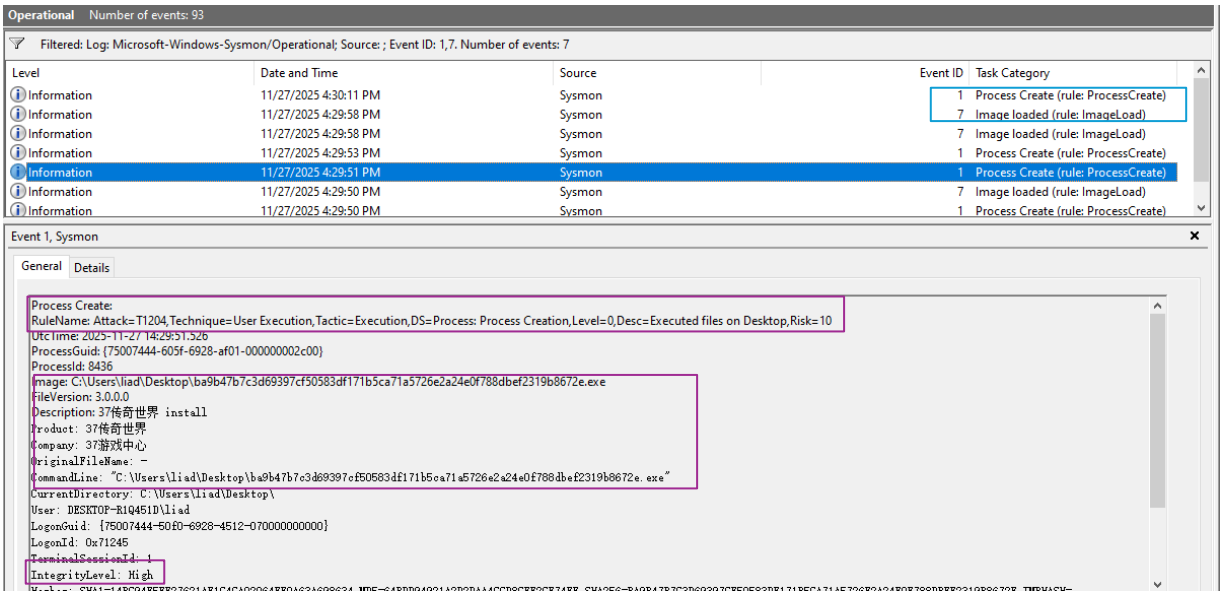
Dns Queries found at Wireshark:

From the network traffic captured in Wireshark, multiple DNS queries can be observed that are repeatedly requesting hostnames under the domains 37.com and 37wan.com, such as gameapp.37.com and a.clickdata.37wan.com, which are associated with the 37Games online gaming platform and its advertising/tracking infrastructure.





Sysmon



You can explicitly see by filtering in EVENT VIEWER under PROCESS CREATE RULE and IMAGE LOADED RULE: the name of our file, along with comments in Chinese under DESCRIPTION.

I found that there is also an entire field that describes an execution technique (T1204) from MITRE ATT&ACK - with a RISK of 10.

Summary:

37cqsj.exe is a software that freely communicates with the Internet browser and creates requests and DLLs easily. Adware (Including MALWARES) can be terribly dangerous, and will probably not end with the download of a code OR a legitimate application as in our case, but could lead to much more serious things.

We discovered that the file is very quiet, and runs as a computer game to disguise the actions it creates in the background - behind the scenes.

Surprisingly, it does not keep a hold on the REGISTRY - probably to keep quiet, but instead it makes some conf files copy of itself on to the APPDATA path in Windows, a path that is hardly accessed.

37cqsj.exe does change a lot of keys and values in the Registry (temporarily), thus essentially creating environmental conditions that allow it to operate indirectly and transparently to the user, without leaving clear traces of traditional Persistence. In addition, its manipulations in the registry help to hide its activity, run components in the background and maintain stability of operation even without direct registration in automatic startup.

Recommendations:

First of all, you should remove the software immediately.

Isolate the end-point device.

kill the sessions and Block the communication.

Clean the browsers: Remove strange extensions, reset homepage/search engine, and reset browser settings to default if needed.

Block the suspicious Domains on your FW / proxy and add the Unknown IP's to a black-list.

Run a full security scan: Use your antivirus/EDR and, if possible, an extra adware/PUA removal tool and delete everything it flags.

To continue:

It is recommended to investigate further about its communications, processes and the DLL's it maked.