

# The Russian SpyAgent – a Decade Later and RAT Tools Remain at Risk

deepinstinct.com/blog/the-russian-spyagent-a-decade-later-and-rat-tools-remain-at-risk

October 11, 2022



[Learn more](#)

OCTOBER 11, 2022

[Deep Instinct Threat Lab](#)

Deep Instinct Threat Lab researchers have observed changes in the distribution scheme of SpyAgent (A.K.A. TeamSpy/TVRat/TeamBot/Sheldor), a malware that likely originated over a decade ago based on the historical timeline below.

SpyAgent is a malware that abuses legitimate, well-known remote access tools (RAT). The recent changes observed by our team allow the malware to stay stealthy while bypassing and evading many security products.

Attackers evading existing security controls is a trend we see increasing. This is a problem for the industry as most security solutions that were developed with an “assume breach” mindset will miss these stealthy attacks until it is far too late to stop the damage.

## Historical Background on SpyAgent:

- In a report from [2011](#), a malware named “Sheldor” used DLL search order hijacking to abuse TeamViewer 5.0 for malicious activities.
- In a report from [2013](#), a malware named “TeamSpy” used DLL search order hijacking to abuse TeamViewer 6.0 for malicious activities. The report also shows a relationship between “Sheldor” and “TeamSpy.”
- In a report from [2016](#), a malware named “Spy-Agent” used DLL search order hijacking to abuse TeamViewer 6.0 for malicious activities. The report contains unique URI patterns that the malware uses to communicate with the C&C server.
- SpyAgent’s main capabilities are leveraged to enhance the usage of TeamViewer by hooking some of the functions used by legitimate applications.
- The most important thing that SpyAgent does is obtain the client’s unique ID, which is required to connect to a computer using TeamViewer.
- Other hooks disable logging and hide the GUI of the application to make it stealthy and avoid detection.

## 10 years later:

- A report published in [2021](#) showed that the “Spy-Agent” malware has been observed shifting from hijacking TeamViewer to hijacking “Safib Assistant,” a Russian replica of TeamViewer.
- The report demonstrates the distribution scheme of the malware, using fake crypto applications as a theme.
- The fake applications are actually downloaders of multiple malware families, which include different RATs and stealers, such as RedLine. “SpyAgent” is one of the downloaded malware families.

## Recent Changes

In May 2022, a small change was observed in the fake crypto campaign first seen in 2021. Instead of using NSIS or Inno Setup droppers, executable files over 700MB were used to evade detection. This is because many security products limit the size of scanned files to compensate for performance issues. This is similar to the way the "Quartz.dll" SpyAgent files are inflated to 1GB+, as noted in the 2021 report. This is done by simply appending a large overlay of zeros to the file, and this technique allows the file to be compressed to the actual size without the overlay.

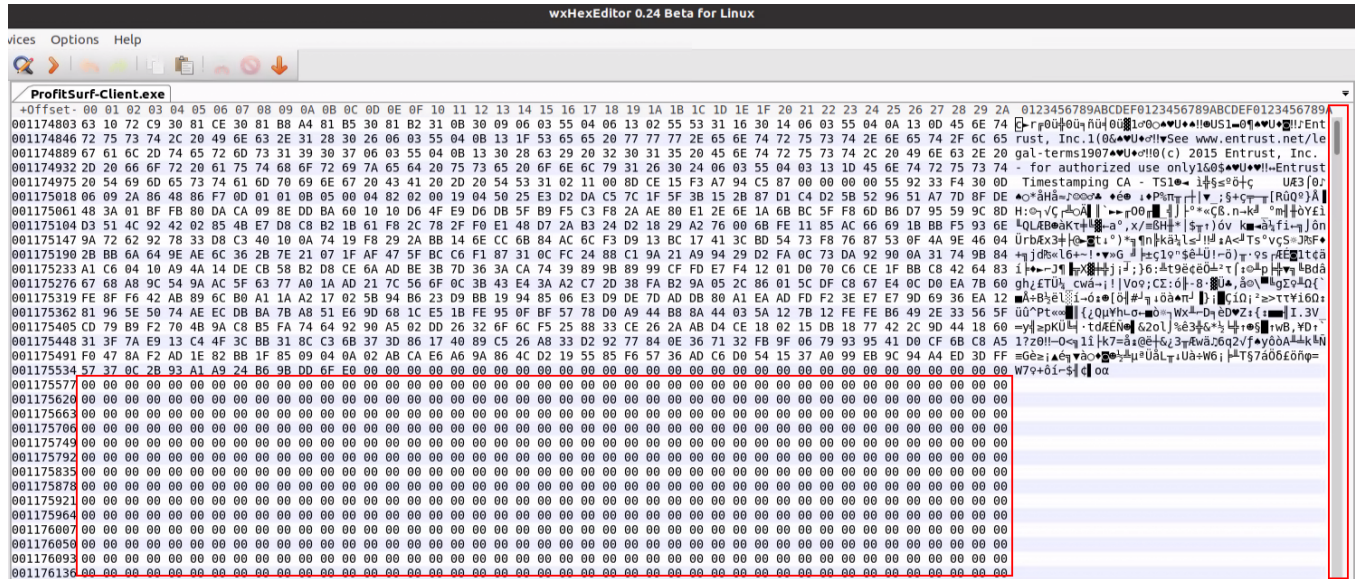


Figure 1: Overlay of zeros appended at the end of the file to inflate its size to avoid detection

Due to their large size, the files are not stored in public malware repositories or sandboxes.

The large overlaid executables are droppers which use Microsoft's .NET ClickOnce launch utility "AppLaunch.exe" to download and execute malware files from the web.

More malicious files related to this change can be found by [searching](#) the included txt file inside the zip:

1. Запускаем клиент в архиве
2. Вводим свои кошельки для выплат
3. Радуемся доходу каждый день!

Figure 2: Contents of the text file included in the zip archive

Compressed Parents (12) ⓘ

Scanned	Detections	Type	Name
2022-05-02	8 / 61	ZIP	ProfitSurf.zip
2022-05-02	7 / 59	ZIP	ProfitSurf.zip
2022-05-03	7 / 59	ZIP	C:\Users\Paul\Downloads\ProfSurf.zip
2022-05-04	13 / 59	ZIP	ClickProfit.zip
2022-05-18	21 / 60	ZIP	C:\Users\Loja\Downloads\ClickProfitClient.zip
2022-05-09	17 / 60	ZIP	TRXWallet.zip
2022-05-11	20 / 61	ZIP	SeedParser.zip
2022-05-11	10 / 61	ZIP	c4be526c9a0c33a392e63c524fb16f442886cdf830f3903b1f38c552d68879
2022-09-15	28 / 60	ZIP	/var/www/clean-mx/virusesevidence/output.197211358.txt
2022-05-31	25 / 61	ZIP	C:\Users\2022\Downloads\TRXWallet-qt.zip
2022-05-18	17 / 61	ZIP	C:\Users\MR Ahmed\Downloads\hostero.zip
2022-06-02	23 / 60	ZIP	OriBux.zip

Figure 3: More

archives containing the same text file

The text translates from Russian into:

1. We execute the client inside the archive
2. We enter our wallets to receive payments
3. We are happy everyday because of the profit!

In June 2022, additional changes were observed.

The SpyAgent theme is no longer related to crypto applications.

The dropper files are once again Inno Setup files, however, they no longer download any additional malware except “SpyAgent” bundled with “Safib Assistant.”

Since “Safib Assistant” is a legitimate tool, similar to TeamViwer, just less known, this change lowers the detection rate for the campaign as the only real malware is “SpyAgent.”

However, as previously was reported, the “SpyAgent” DLL files are very large.

T1027.001 is a known MITRE technique that adversaries use to “decrease the effectiveness of certain tools and detection capabilities that are not designed or configured to scan large files. This may also reduce the likelihood of being collected for analysis. Public file scanning services, such as VirusTotal, limits the maximum size of an uploaded file to be analyzed.”

Example file

1565d137d235b65af1d1e4963ebc02eaf36cc81f870534674983bc6f67e5e274 is an Inno Setup file that during the writing of this article was detected by four security vendors:

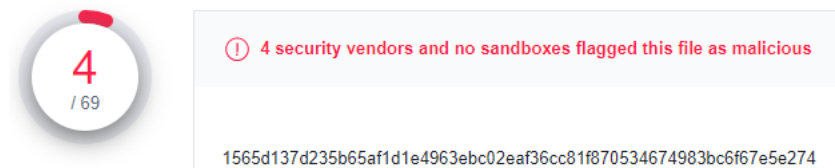


Figure 4: Detection rate at first submission (2022-07-

18 06:04:01 UTC)

This file is inside three different zip files, which are not related to a crypto theme.

The dropper silently installs “Safib Assistant,” the software’s main executable hash is b8dde42c70d8c4a3511d5edffbc9f7f0c03dbda980e29693e71344f76da6bb0f and it is detected by only two security vendors, although it is not malicious without the SpyAgent DLL:

b8dde42c70d8c4a3511d5edffbc9f7f0c03dbda980e29693e71344f76da6bb0f

**Signature Info** ⓘ

**Signature Verification**

✔ Signed file, valid signature

**File Version Information**

Copyright	ООО «САФИБ»
Product	Ассистент
Description	Ассистент 4
Original Name	Assistant.exe
File Version	4.5.2109.1401
Date signed	2021-09-14 09:26:00 UTC

**Signers**

- + SAFIB
- + Sectigo RSA Code Signing CA
- + USERTrust RSA Certification Authority
- + Sectigo (AAA)

Figure 5: Metadata of the “Safib Assistant” main executable

The SpyAgent C&C server is thief[.]lol which resolved during the analysis to the IP address 185.125.206[.]172.

During our investigation, the C&C was still working, allowing us to confirm that the malware bundled with “Safib Assistant” is indeed “SpyAgent.”



Figure 6: SpyAgent C2 panel

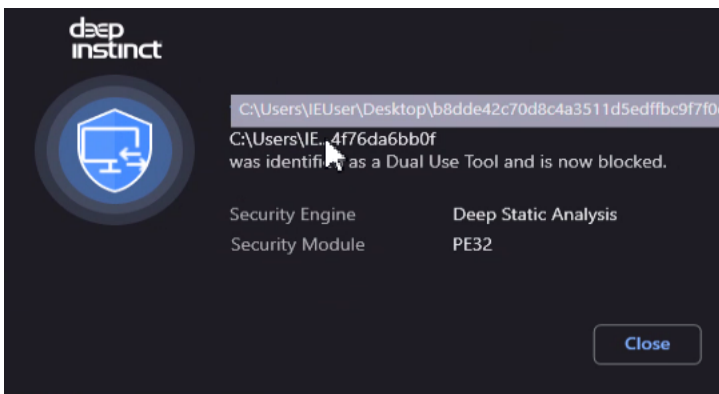
## Conclusion

Both TeamViewer and “Safib Assistant” are legitimate remote admin tools, however, without the spy-agent malware DLL which adds stealth they are less useful for cybercriminal operations.

On the other hand, there are several other legitimate remote admin tools that don't require any additional malicious DLL files to be stealthy which are used as-is by cybercriminals.

Deep Instinct classifies such tools as dual-use because they are 3rd-party software that is not necessarily allowed to be used in a corporate network as it can be used maliciously.

Deep Instinct blocks the Safib Assistant application.



## MITRE ATT&CK:

Tactic	Technique	Description	Obse
Discovery	T1082 System Information Discovery	<p>SpyAgent computes environment hash as an MD5 of the string created by concatenating the following:</p> <p>Value 1 = to_uppercase(crc32(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuid))</p> <p>Value 2 = to_uppercase(crc32(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName))</p> <p>Value 3 = to_uppercase(crc32(user name))</p> <p>Value 4 = to_uppercase(crc32(computer name))</p>	<C&C <9dig hash>

Tactic	Technique	Description	Obse
Defense Evasion	T1027.001 Obfuscated Files or Information: Binary Padding	SpyAgent's quartz.dll was artificially inflated to the size of 1GB	e2ee - 7z f bundl
		SpyAgent's dropper executable was artificially inflated to the size of 700MB	c727 - zip
	T1574.002 Hijack Execution Flow: DLL Side-Loading	SpyAgent hooks and patches various API functions called by the original DLLs used by TeamViewer and Safib Assistant	tv.dll msim avica quartz
	T1140 Deobfuscate/Decode Files or Information	SpyAgent comes with a config file (.cfg) that contains an encrypted configuration. The bitmap file (.bmp) is used for deriving the key to decrypt the config file	8089 - bmp 6f496 - cfg
Command and Control	T1219 Remote Access Software	SpyAgent's quartz.dll uses the "Safib Assistant"	8002 - Assi
		SpyAgent's avicap32.dll uses TeamViewer	28c4 - Tear
	T1071.001 Web Protocols	SpyAgent uses HTTP for command and control	<C&C <9dig hash>

## IOC

1565d137d235b65af1d1e4963ebc02eaf36cc81f870534674983bc6f67e5e274

Active Spy Agent C2:

23.19.227[.]217

45.66.151[.]237

108.62.118[.]48

jmai[.]ink

[Back To Blog](#)