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

: 10/11/2022

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 is it far too late to stop the damage.

Historical Background on SpyAgent:

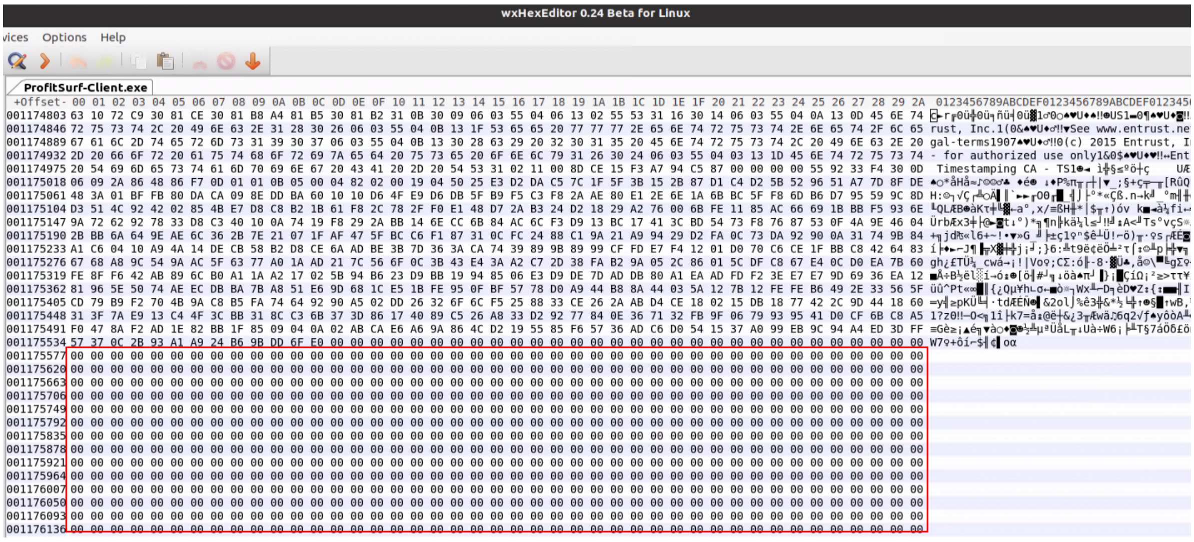
- In a report from 2011, a malware named “Sheldor” used DLL search order hijacking to abuse TeamViewer 5.0 for malicious activities.
- In a report from 2013, a malware named “TeamSpy” used DLL search order hijacking to abuse TeamViewer 6.0 for malicious activities. The report also shows a relationship 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.



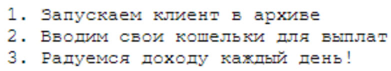
```
 +Offset- 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F 20 21 22 23 24 25 26 27 28 29 2A  0123456789ABCDEF0123456789ABCDEF012345
001174803 63 10 72 C9 30 81 CE 30 81 B8 A4 81 B5 30 81 B2 31 0B 30 09 06 03 55 04 06 13 02 55 53 31 16 30 14 06 03 55 04 0A 13 0D 45 6E 74 c├r╓0ü╫0ü╕ñü╡0ü▓1♂0○♠♥U♦♠‼☻US1▬0¶♠♥U♦◙‼
001174846 72 75 73 74 2C 20 49 6E 63 2E 31 28 30 26 06 03 55 04 0B 13 1F 53 65 65 20 77 77 77 2E 65 6E 74 72 75 73 74 2E 6E 65 74 2F 6C 65 rust, Inc.1(0&♠♥U♦♂‼▼See www.entrust.ne
001174889 67 61 6C 2D 74 65 72 6D 73 31 39 30 37 06 03 55 04 0B 13 30 28 63 29 20 32 30 31 35 20 45 6E 74 72 75 73 74 2C 20 49 6E 63 2E 20 gal-terms1907♠♥U♦♂‼0(c) 2015 Entrust, I
001174932 2D 20 66 6F 72 20 61 75 74 68 6F 72 69 7A 65 64 20 75 73 65 20 6F 6E 6C 79 31 26 30 24 06 03 55 04 03 13 1D 45 6E 74 72 75 73 74 - for authorized use only1&0$♠♥U♦♥‼↔Ent
001174975 20 54 69 6D 65 73 74 61 6D 70 69 6E 67 20 43 41 20 2D 20 54 53 31 02 11 00 8D CE 15 F3 A7 94 C5 87 00 00 00 00 55 92 33 F4 30 0D  Timestamping CA - TS1☻◄ ì╬§≤ºö┼ç    UÆ
001175018 06 09 2A 86 48 86 F7 0D 01 01 0B 05 00 04 82 02 00 19 04 50 25 E3 D2 DA C5 7C 1F 5F 3B 15 2B 87 D1 C4 D2 5B 52 96 51 A7 7D 8F DE ♠○*åHå≈♪☺☺♂♣ ♦é☻ ↓♦P%π╥┌┼|▼_;§+ç╤─╥[RûQ
001175061 48 3A 01 BF FB 80 DA CA 09 8E DD BA 60 10 10 D6 4F E9 D6 DB 5F B9 F5 C3 F8 2A AE 80 E1 2E 6E 1A 6B BC 5F F8 6D B6 D7 95 59 9C 8D H:☺┐√Ç┌╩○Ä▌║`►►╓OΘ╓█_╣⌡├°*«Çß.n→k╝_°m╢╫
001175104 D3 51 4C 92 42 02 85 4B E7 D8 C8 B2 1B 61 F8 2C 78 2F F0 E1 48 D7 2A B3 24 D2 18 29 A2 76 00 6B FE 11 85 AC 66 69 1B BB F5 93 6E ╙QLÆB☻àKτ╪╚▓←a°,x/≡ßH╫*│$╥↑)óv k■◄à¼fi←
001175147 9A 72 62 92 78 33 D8 C3 40 10 0A 74 19 F8 29 2A BB 14 6E CC 6B 84 AC 6C F3 D9 13 BC 17 41 3C BD 54 73 F8 76 87 53 0F 4A 9E 46 04 ÜrbÆx3╪├@►◙t↓°)*╗¶n╠kä¼l≤┘‼╝↨A<╜Ts°vçS☼
001175190 2B BB 6A 64 9E AE 6C 36 2B 7E 21 07 1F AF 47 5F BC C6 F1 87 31 0C FC 24 88 C1 9A 21 A9 94 29 D2 FA 0C 73 DA 92 90 0A 31 74 9B 84 +╗jd₧«l6+~!•▼»G_╝╞±ç1♀ⁿ$ê┴Ü!⌐ö)╥·♀s┌ÆÉ◙
001175233 A1 C6 04 10 A9 4A 14 DE CB 58 B2 D8 CE 6A AD BE 3B 7D 36 3A CA 74 39 89 9B 89 99 CF FD E7 F4 12 01 D0 70 C6 CE 1F BB C8 42 64 83 í╞♦►⌐J¶▐╦X▓╪╬j¡╛;}6:╩t9ë¢ëÖ╧²τ⌠↕☺╨p╞╬▼╗
001175276 67 68 A8 9C 54 9A AC 5F 63 77 A0 1A AD 21 7C 56 6F 0C 3B 43 E4 3A A2 C7 2D 38 FA B2 9A 05 2C 86 01 5C DF C8 67 E4 0C D0 EA 7B 60 gh¿£TÜ¼_cwá→¡!|Vo♀;CΣ:ó╟-8·▓Ü♣,å☺\▀╚gΣ♀╨
001175319 FE 8F F6 42 AB 89 6C B0 A1 1A A2 17 02 5B 94 B6 23 D9 BB 19 94 85 06 E3 D9 DE 7D AD DB 80 A1 EA AD FD F2 3E E7 E7 9D 69 36 EA 12 ■Å÷B½ël░í→ó↨☻[ö╢#┘╗↓öà♠π┘▐}¡█ÇíΩ¡²≥>ττ¥i6Ω↕
001175362 81 96 5E 50 74 AE EC DB BA 7B A8 51 E6 9D 68 1C E5 1B FE 95 0F BF 57 78 D0 A9 44 B8 8A 44 03 5A 12 7B 12 FE FE B6 49 2E 33 56 5F üû^Pt«∞█║{¿Qµ¥h∟σ←■ò☼┐Wx╨⌐D╕èD♥Z↕{↕■■╢I.3V_
001175405 CD 79 B9 F2 70 4B 9A C8 B5 FA 74 64 92 90 A5 02 DD 26 32 6F 6C F5 25 88 33 CE 26 2A AB D4 CE 18 02 15 DB 18 77 42 2C 9D 44 18 60 ═y╣≥pKÜ╚╡·tdÆÉÑ☻▌&2ol⌡%ê3╬&*½╘╬↑☻§█↑wB,¥D↑`
001175448 31 3F 7A E9 13 C4 4F 3C BB 31 8C C3 6B 37 3D 86 17 40 89 C5 26 A8 33 D2 92 77 84 0E 36 71 32 FB 9F 06 79 93 95 41 D0 CF 6B C8 A5 1?zΘ‼─O<╗1î├k7=å↨@ë┼&¿3╥Æwä♫6q2√ƒ♠yôòA╨╧k╚Ñ
001175491 F0 47 8A F2 AD 1E 82 BB 1F 85 09 04 0A 02 AB CA E6 A6 9A 86 4C D2 19 55 85 F6 57 36 AD C6 D0 54 15 37 A0 99 EB 9C 94 A4 ED 3D FF ≡Gè≥¡▲é╗▼à○♦◙☻½╩µªÜåL╥↓Uà÷W6¡╞╨T§7áÖδ£öñφ=
001175534 57 37 0C 2B 93 A1 A9 24 B6 9B DD 6F E0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 W7♀+ôí⌐$╢¢▌oα
001175577 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
001175620 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
001175663 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
001175706 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
001175749 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
001175792 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
001175835 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
001175878 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
001175921 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
001175964 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
001176007 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
001176050 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
001176093 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
001176136 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
```

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.

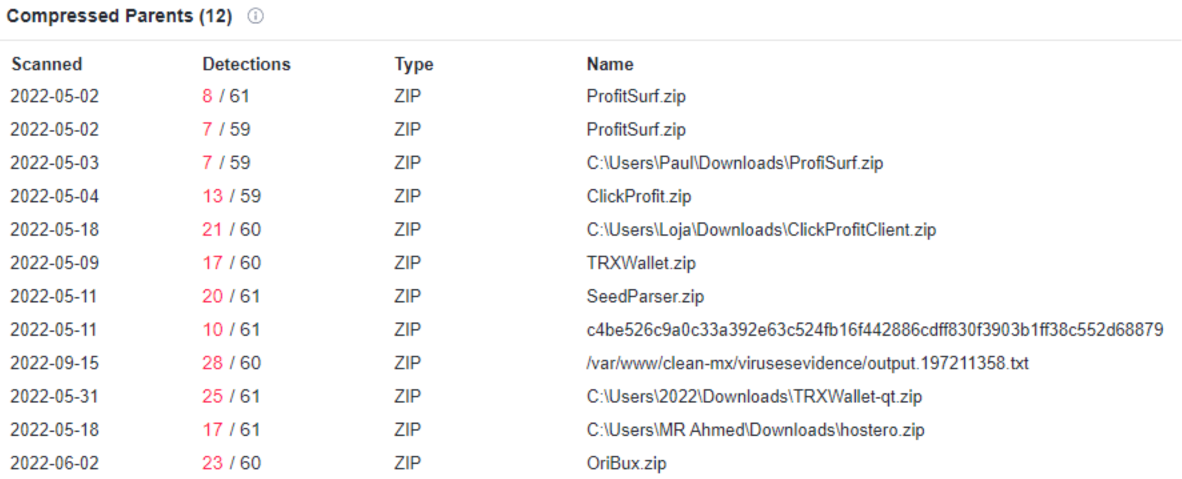
The large overlayed executables are droppers which use Microsoft's .NET ClickOnce launch utility "AppLaunch.exe" to download and execute malware files from the web.

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\ProfiSurf.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	c4be526c9a0c33a392e63c524fb16f442886cdff830f3903b1ff38c552d68879
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.

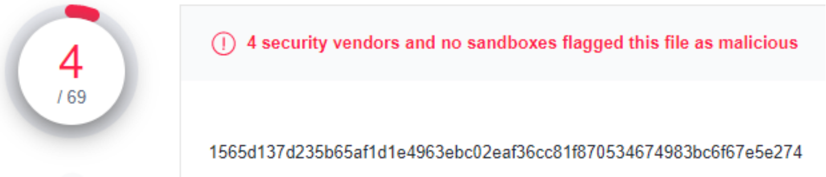
The dropper files are once again Inno Setup files, however, they no longer download any additional malware except "SpyAgent" bundled with "Safib Assistant."

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:



4
/ 69

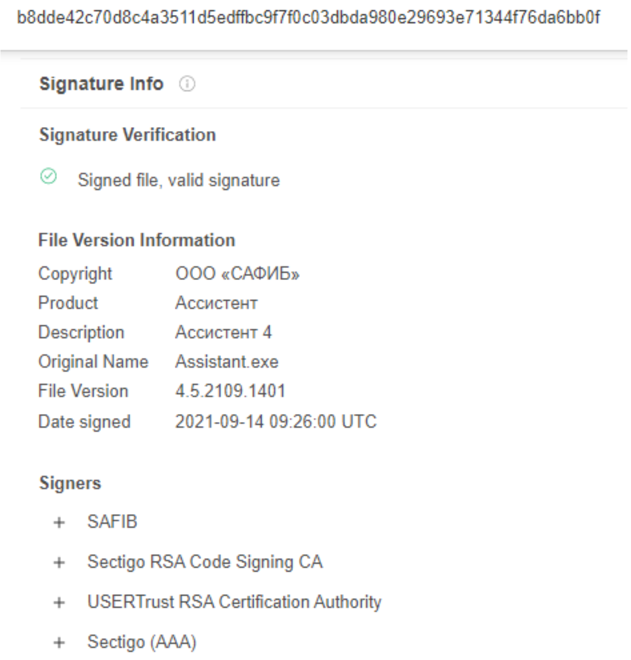
4 security vendors and no sandboxes flagged this file as malicious

1565d137d235b65af1d1e4963ebc02eaf36cc81f870534674983bc6f67e5e274

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:”

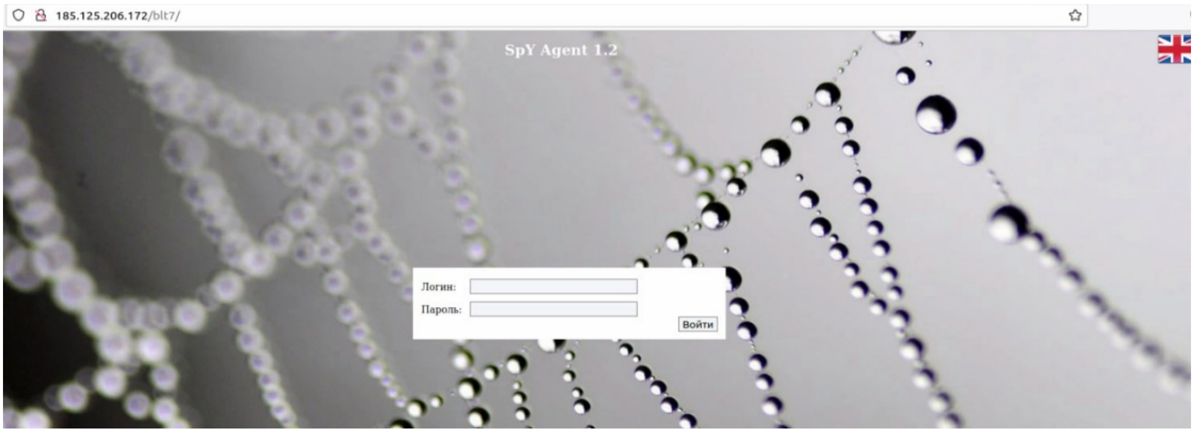


Figure 6: SpyAgent C2 panel

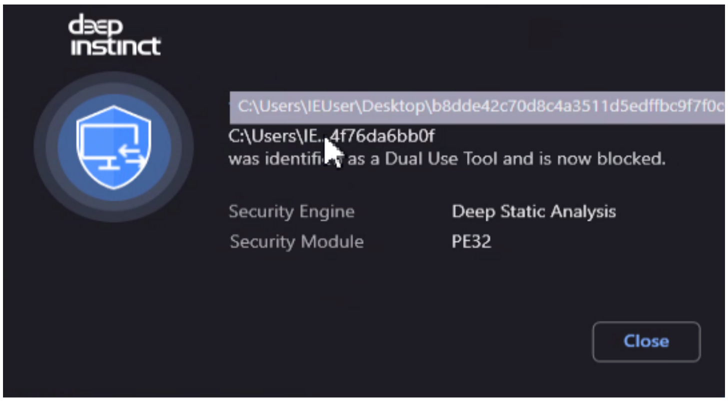
Conclusion

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.



C:\Users\IEUser\Desktop\b8dde42c70d8c4a3511d5edffbc9f7f0c

C:\Users\IE. 4f76da6bb0f
was identifi as a Dual Use Tool and is now blocked.

Security Engine Deep Static Analysis
Security Module PE32

MITRE ATT&CK:

Tactic	Technique	Description
Discovery	T1082 System Information Discovery	SpyAgent computes environment hash as an MD5 of the string created by concatenating the following: Value 1 = to_uppercase(crc32(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MachineGuic Value 2 = to_uppercase(crc32(HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName)) Value 3 = to_uppercase(crc32(user name)) Value 4 = to_uppercase(crc32(computer name))
Defense Evasion	T1027.001 Obfuscated Files or Information: Binary Padding	SpyAgent’s quartz.dll was artificially inflated to the size of 1GB
		SpyAgent’s dropper executable was artificially inflated to the size of 700MB
	T1574.002 Hijack Execution Flow: DLL Side-Loading	SpyAgent hooks and patches various API functions called by the original DLLs used by TeamView and Safib Assistant
	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
Command and Control	T1219 Remote Access Software	SpyAgent’s quartz.dll uses the “Safib Assistant”
		SpyAgent’s avicap32.dll uses TeamViewer
	T1071.001 Web Protocols	SpyAgent uses HTTP for command and control

IOC

1565d137d235b65af1d1e4963ebc02eaf36cc81f870534674983bc6f67e5e274

Active Spy Agent C2:
23.19.227[.]217
45.66.151[.]237
108.62.118[.]48
jmai[.]ink