SparkRAT Being Distributed Within a Korean VPN Installer

asec.ahnlab.com/en/52899/

By Sanseo May 18, 2023

AhnLab Security Emergency response Center (ASEC) has recently discovered SparkRAT being distributed within the installer of a certain VPN program. SparkRAT is a Remote Administration Tool (RAT) developed with GoLang. When installed on a user's system, it can perform a variety of malicious behaviors, such as executing commands remotely, controlling files and processes, downloading additional payloads, and collecting information from the infected system like by taking screenshots.

1. Case of Distribution

The VPN provider, whose installer contained SparkRAT appears to have been in operation since the past, as seen in the signed certificates of the files and notices on their official website. Therefore, it is clear that the current website was not created specifically for distributing malware as the distribution of an installer with malware inside of it was discovered recently.

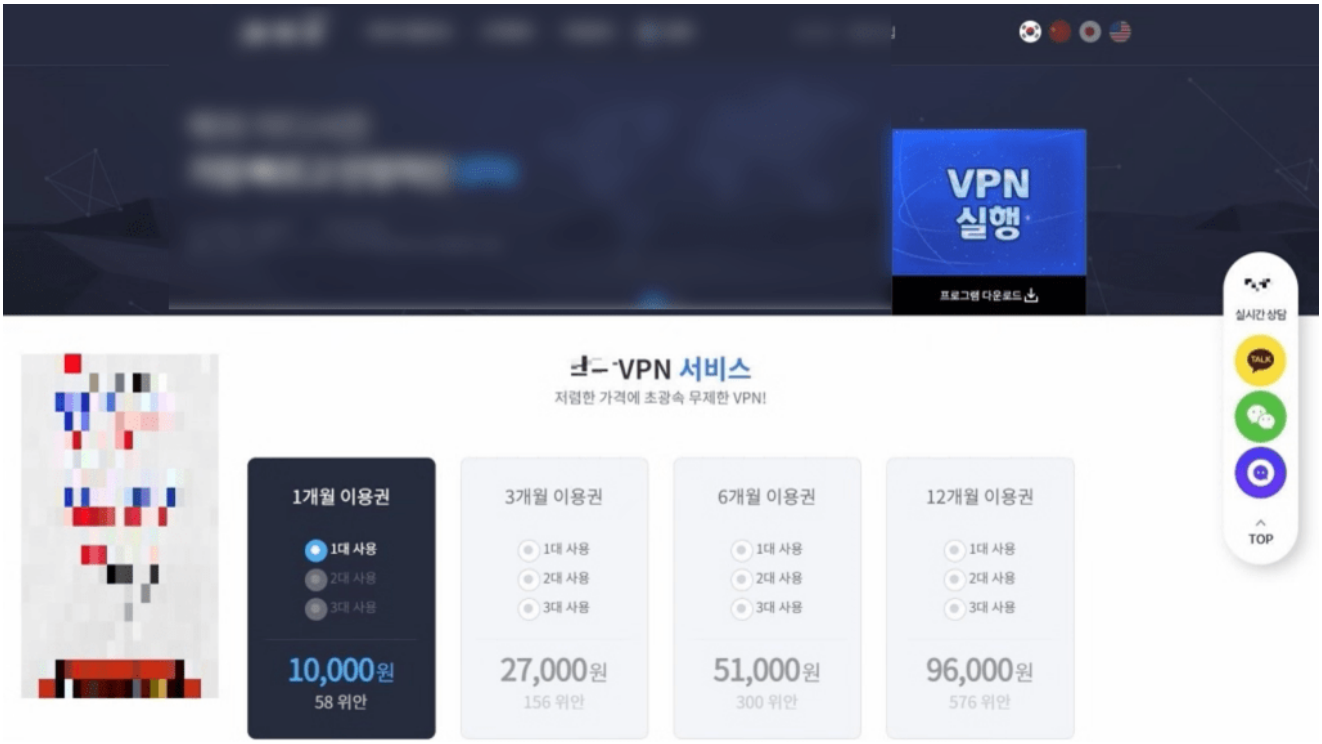

Figure 1. Official website of the VPN containing SparkRAT

The installer is only available in Korean, but the official website of the VPN supports English, Chinese, and Japanese. According to their notice, it can be assumed that many people in China install the program to ensure smooth Internet access. In fact, even in our own AhnLab Smart Defense (ASD) logs, we have observed a higher number of installations from users in China compared to Korea.

Figure 2. Process tree

The file downloaded from the official website is not the previously confirmed installer, but rather a dropper created using .NET. The dropper has the original VPN installer and the malware stored in its resources. When executed, it generates the malware in the path %LOCALAPPDATA%\Syservices\svchost.exe before launching it.

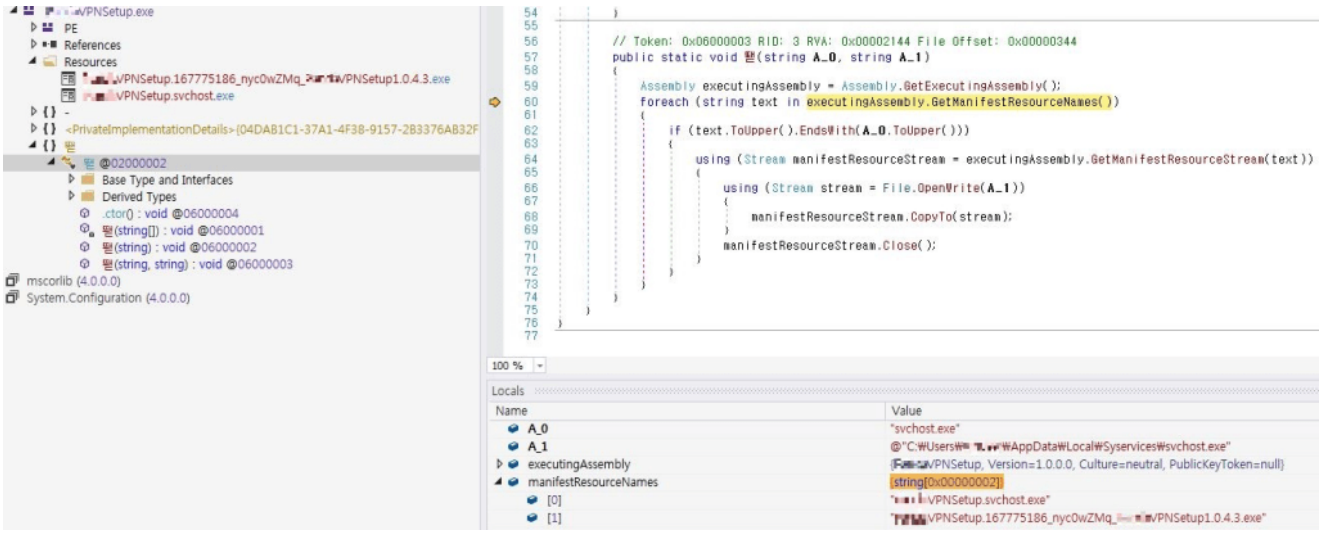

Figure 3. Malware and installer saved in resources

In addition, since the original VPN installer is created and launched along with the malware, it is difficult for users to recognize that malware had been installed, and are led to believe that the VPN installer was executed without issue. Furthermore, the malware is registered in the task scheduler to ensure it will be executed even after system reboots.

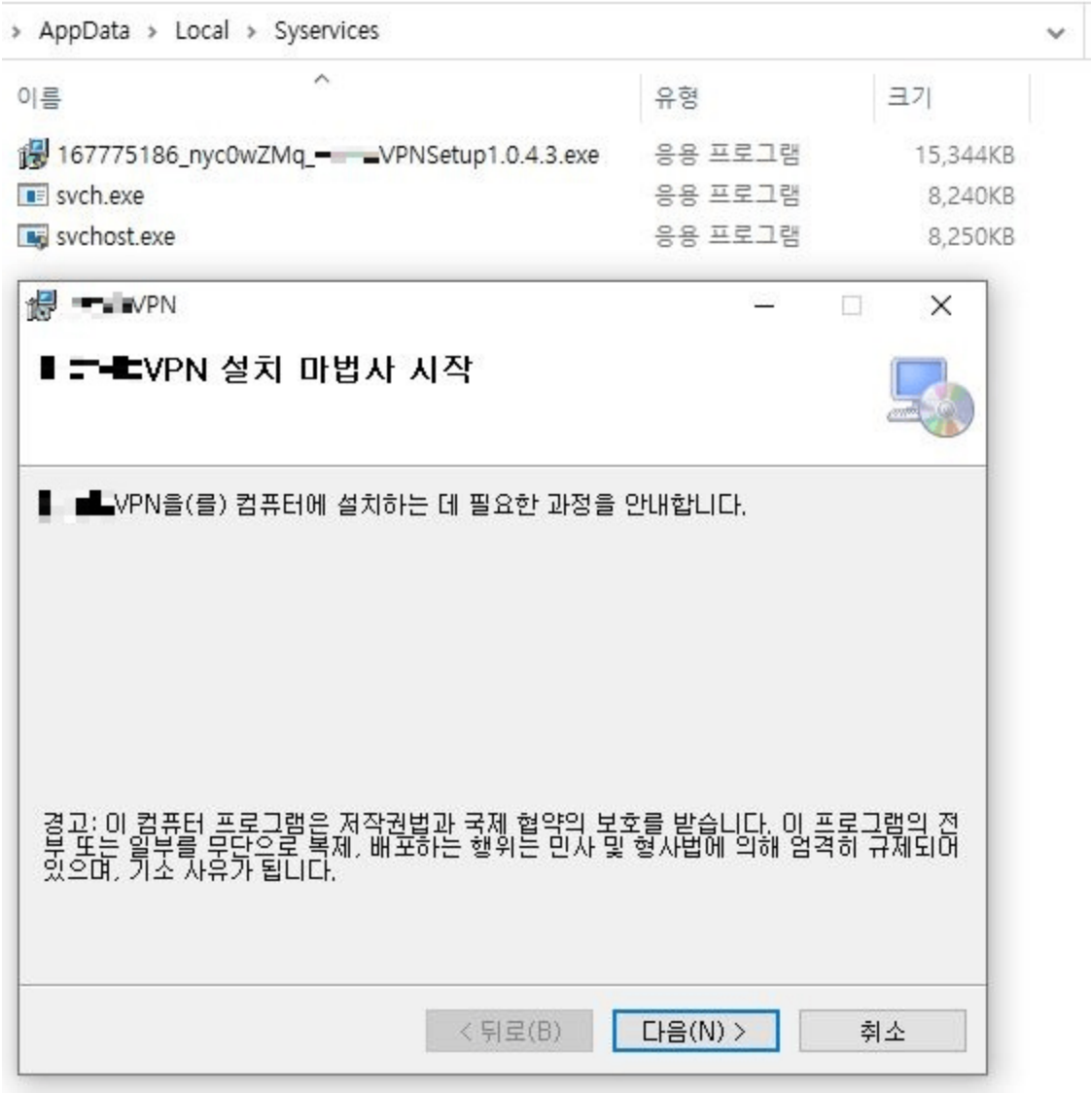

Figure 4.

Generated files and the executed VPN installer

The malware created under the name “svchost.exe” is also a dropper. It bears similarities to the aforementioned dropper in that it contains SparkRAT within its resources. Its function is to generate the malware as “svch.exe” in the same directory and execute it.

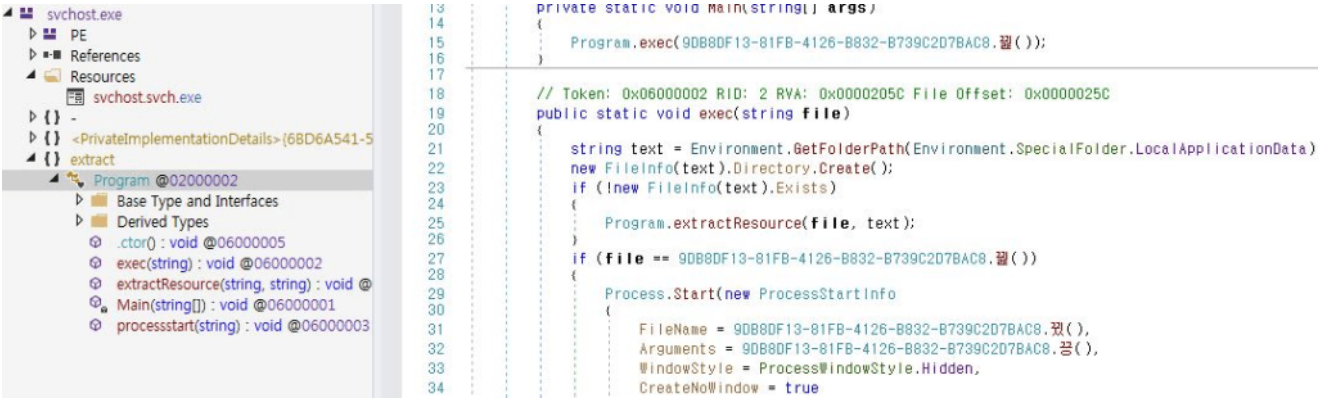

Figure 5. Similarly structured dropper that creates SparkRAT

2. SparkRAT

SparkRAT is an open-source RAT malware that is publicly available on GitHub. Notable for being developed with GoLang, SparkRAT provides basic features commonly found in RAT malware, such as executing commands, stealing information, and controlling processes and files.

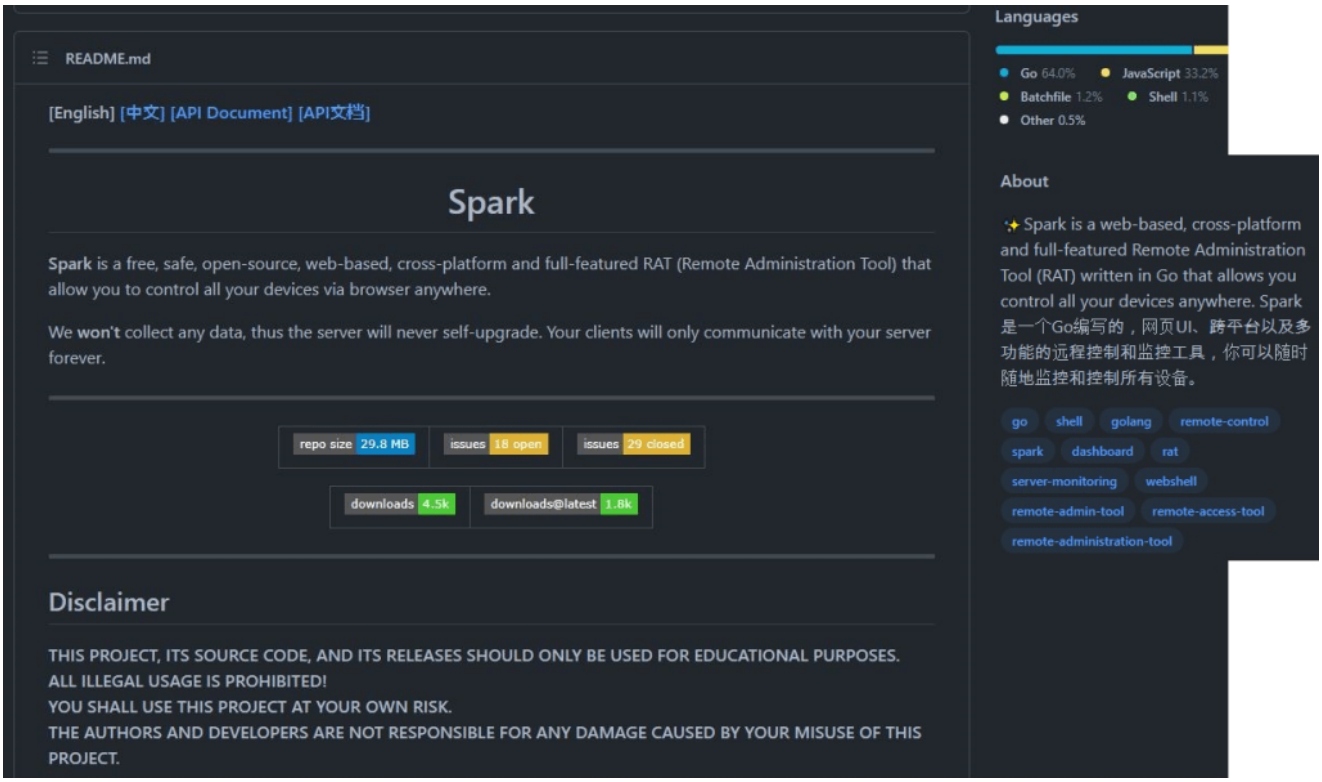

Figure 6. SparkRAT source code publicly available on GitHub

Due to its support for various platforms, the GoLang is commonly used to develop malware that targets not only Windows but also Linux and MacOS. Similarly, SparkRAT supports all three operating systems and provides categorized features based on each platform, as shown in the following table.

Features

Feature/OS	Windows	Linux	MacOS
Process manager	✓	✓	✓
Kill process	✓	✓	✓
Network traffic	✓	✓	✓
File explorer	✓	✓	✓
File transfer	✓	✓	✓
File editor	✓	✓	✓
Delete file	✓	✓	✓
Code highlight	✓	✓	✓
Desktop monitor	✓	✓	✓
Screenshot	✓	✓	✓
OS info	✓	✓	✓
Terminal	✓	✓	✓
* Shutdown	✓	✓	✓
* Reboot	✓	✓	✓
* Log off	✓	✗	✓
* Sleep	✓	✗	✓
* Hibernate	✓	✗	✗
* Lock screen	✓	✗	✗

Figure 7. Features offered for each platform

As shown in the above GitHub page, another notable feature of SparkRAT is its support for the Chinese language. The developer is also known for their ability to use Chinese. **[1]** In the past, SentinelOne had covered the DragonSpark attack campaign that used SparkRAT and made the assumption that the threat actors were fluent in Chinese. While it is not possible to identify the specific threat actor, it is worth noting that the VPN used in the current attack is also a program commonly used in China.

The SparkRAT used in the attacks was not obfuscated, making it easy to distinguish based on the used function names. SparkRAT decrypts the configuration data and retrieves information such as the C&C address and port number from the initialization function, main.init().

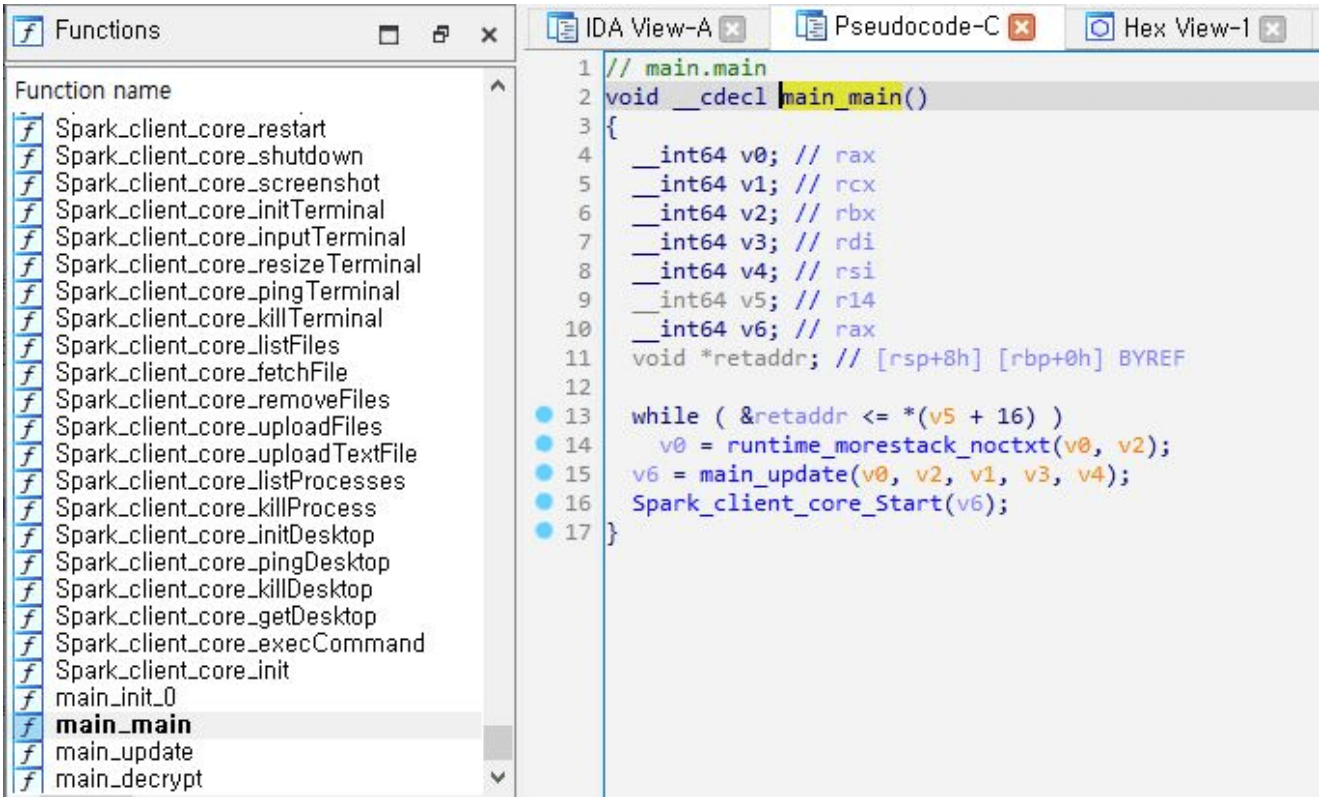

Figure 8. SparkRAT that has not been obfuscated

```
0000000000827D51   83E2 10          and edx,10
0000000000827D54   48:01C2          add rdx,rax
0000000000827D57   48:89C7          mov rdi,rax
0000000000827D5A   BE 10000000      mov esi,10
0000000000827D5F   49:89C8          mov r8,rcx
0000000000827D62   48:89D0          mov rax,rdx
0000000000827D65   4C:89C9          mov rcx,r9
0000000000827D68   E8 53030000      call <svch.main.decrypt>
0000000000827D6D   48:85FF          test rdi,rdi
0000000000827D70   0F85 B4000000    jne svch.827E2A

<svch.main.decrypt>

.text:0000000000827D68 svch.exe:$377D68 #377368

Dump 1  Dump 2  Dump 3  Dump 4  Dump 5  Watch 1  [x=] Locals  Struct

Address          Hex                                              ASCII
000000C000128180 7B 22 73 65 63 75 72 65 22 3A 74 72 75 65 2C 22  {"secure":true,"
000000C000128190 68 6F 73 74 22 3A 22 67 77 65 6B 65 6B 63 63 65  host":"gwekekcce
000000C0001281A0 66 2E 77 65 62 75 6C 6C 2E 64 61 79 22 2C 22 70  f.webull.day","p
000000C0001281B0 6F 72 74 22 3A 34 34 33 2C 22 70 61 74 68 22 3A  ort":443,"path":
000000C0001281C0 22 2F 22 2C 22 75 75 69 64 22 3A 22 39 35 38 30  "/","uuid":"9580
000000C0001281D0 37 33 38 38 65 61 32 35 30 34 34 30 35 34 38 31  7388ea2504405481
000000C0001281E0 66 36 62 31 61 31 36 64 61 63 34 36 22 2C 22 6B  f6b1a16dac46","k
000000C0001281F0 65 79 22 3A 22 64 62 34 32 32 32 65 31 30 36 36  ey":"db4222e1066
000000C000128200 62 30 61 38 30 30 38 34 31 32 32 61 36 38 30 36  b0a80084122a6806
000000C000128210 30 61 64 31 61 30 36 32 65 39 65 65 65 66 30 64  0ad1a062e9eeef0d
000000C000128220 33 64 33 33 32 35 30 64 31 34 37 65 65 63 37 62  3d33250d147eec7b
000000C000128230 61 66 39 32 66 22 7D 00 00 00 00 00 00 00 00 00  af92f"}.........
000000C000128240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Figure 9. Decrypted configuration data of SparkRAT

Additionally, while checking related files through the company's ASD logs, ASEC discovered additional malware through the installer malware believed to be this VPN. These malware samples are suspected to have been distributed around the same time and are notable for their use of SparkRAT based on x86 architecture.

```
007919E0    83E3 10       AND EBX,00000010
007919E3    01D3          ADD EBX,EDX
007919E5    891C24        MOV DWORD PTR SS:[ESP],EBX
007919E8    83C1 F0       ADD ECX,-10
007919EB    894C24 04     MOV DWORD PTR SS:[ESP+4],ECX
007919EF    896C24 08     MOV DWORD PTR SS:[ESP+8],EBP
007919F3    895424 0C     MOV DWORD PTR SS:[ESP+0C],EDX
007919F7    C74424 10 10( MOV DWORD PTR SS:[ESP+10],10
007919FF    894424 14     MOV DWORD PTR SS:[ESP+14],EAX
00791A03    E8 68030000   CALL main.decrypt()
00791A08    8B4424 18     MOV EAX,DWORD PTR SS:[ESP+18]                ASCII
00791A0C    8B4C24 1C     MOV ECX,DWORD PTR SS:[ESP+1C]
00791A10    8B5424 20     MOV EDX,DWORD PTR SS:[ESP+20]
00791A14    8B5C24 24     MOV EBX,DWORD PTR SS:[ESP+24]
Dest=00791D70 (svh.main.decrypt())
```

Figure 10.

```
Address   Hex dump                                          ASCII
0A4CC0C0  7B 22 73 65 63 75 72 65 22 3A 66 61 6C 73 65 2C  {"secure":false,
0A4CC0D0  22 68 6F 73 74 22 3A 22 35 39 2E 32 32 2E 31 36  "host":"59.22.16
0A4CC0E0  37 2E 32 31 37 22 2C 22 70 6F 72 74 22 3A 33 34  7.217","port":34
0A4CC0F0  36 34 36 2C 22 70 61 74 68 22 3A 22 2F 22 2C 22  646,"path":"/","
0A4CC100  75 75 69 64 22 3A 22 37 30 32 35 31 61 30 36 65  uuid":"70251a06e
0A4CC110  31 65 33 64 62 33 64 39 32 62 35 62 33 63 61 65  1e3db3d92b5b3cae
0A4CC120  32 38 30 32 63 35 39 22 2C 22 6B 65 79 22 3A 22  2802c59","key":"
0A4CC130  39 34 35 63 32 30 32 33 65 32 36 38 32 66 64 39  945c2023e2682fd9
0A4CC140  33 39 65 30 39 39 35 66 34 34 37 34 35 34 65 31  39e0995f447454e1
0A4CC150  65 35 37 32 66 30 32 30 37 30 64 63 31 61 35 33  e572f02070dc1a53
0A4CC160  30 37 37 62 64 31 34 64 37 34 66 33 32 62 33 62  077bd14d74f32b3b
0A4CC170  22 7D 00 00 00 00 00 00 00 00 00 00 00 00 00 00  "}
0A4CC180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Configuration data of x86 SparkRAT

In addition, while the x64 version of SparkRAT used the https protocol, the x86 version used http, which allows the following unencrypted packets to be observed.

```
GET /ws HTTP/1.1
Host: 59.22.167.217:34646
User-Agent: Go-http-client/1.1
Connection: Upgrade
Key: 945c2023e2682fd939e0995f447454e1e572f02070dc1a53077bd14d74f32b3b
Sec-WebSocket-Key: wx0MVnjBwSsAvS4Q0yy6iA==
Sec-WebSocket-Version: 13
UUID: 70251a06e1e3db3d92b5b3cae2802c59
Upgrade: websocket

HTTP/1.1 101 Switching Protocols
Upgrade: websocket
Connection: Upgrade
Sec-WebSocket-Accept: 7sIElAvy7vOriXD4VaWMmGbbbUA=
Secret: 1ab5291bcf578a99b165823467ad9108622982ee95755398760deb261392b946

.~...U5.R.<@.{$...&.S[%.F....8.^7.R....`.o..r...>6....N...G.....=MQ.W.
%..z.rKDza%...7f*.Og.y        {....g.......Ca......
```

Figure 11. Packet communication of x86 SparkRAT

3. Conclusion

ASEC has recently confirmed cases where SparkRAT was distributed within VPN installers. It is suspected that the threat actor hacked a legitimate VPN service to distribute their malware. When users download and install the malicious installer from the official website, the installer not only installs SparkRAT but also the original VPN installer, rendering it difficult for users to notice that they have been infected by malware. Users must practice caution by updating V3 to the latest version to block malware infection in advance.

File Detection
– Dropper/Win.Agent.C5421402 (2023.05.03.00)
– Trojan/Win.Malware-gen.R557808 (2023.02.11.01)
– Dropper/Win.Agent.C5421380 (2023.05.03.00)
– Trojan/Win.Generic.C5228761 (2022.08.28.00)
– Dropper/Win.SparkRAT.C5421465 (2023.05.03.01)
– Backdoor/Win.SparkRAT.C5421466 (2023.05.03.01)

IOC
MD5
– 2e3ce7d90d988e1b0bb7ffce1731b04b: Malicious installer downloaded from the official website (167775071_dJABfPme_[…..]VPNSetup1.0.4.3.exe)
– b571d849c0cb3c7af1cee6990654972b: Dropper generated by the malicious installer (svchost.exe)
– 5b78c44262ebcb4ce52e75c331683b5b: SparkRAT x64 (svch.exe)
– a5950704dfa60ba5362ec4a8845c25b2: Malicious installer (167780244_4sfjr6so_[…..]vpnsetup1.0.4.3.exe)
– 7923f9e0e28ceecdb34e924f2c04cda0: Malicious installer – SparkRAT x86 (167775071_gbyri71h_167775186_nyc0wzmq_[…..]vpnsetup1.0.4.3.exe)
– e4805cbd59fe793c48f6341f3d1e5466: SparkRAT x86 (svh.exe)
– 54dd763bca743cbdbdfe709d9ab1d0db: SparkRAT x86 (svh.exe)

C&C
– gwekekccef.webull[.]day:443: SparkRAT x64
– 59.22.167[.]217:34646: SparkRAT x86

Subscribe to AhnLab's next-generation threat intelligence platform 'AhnLab TIP' to check related IOC and detailed analysis information.

Categories:Malware Information

Tagged as:SparkRAT,vpn