Operation Red Signature Targets South Korean Companies

trendmicro.com/en_my/research/18/h/supply-chain-attack-operation-red-signature-targets-south-korean-organizations.html

21 August 2018

APT & Targeted Attacks

We uncovered Operation Red Signature, an information theft-driven supply chain attack targeting organizations in South Korea. We discovered the attacks around the end of July, while the media reported the attack in South Korea on August 6.

By: Jaromir Horejsi, Joseph C Chen, Kawabata Kohei, Kenney Lu August 21, 2018 Read time: (words)

Together with our colleagues at IssueMakersLab, we uncovered Operation Red Signature, an information theft-driven supply chain attack targeting organisations in South Korea. We discovered the attacks around the end of July, while the media reported the attack in South Korea on August 6.

The threat actors compromised the update server of a remote support solutions provider to deliver a remote access tool called 9002 RAT to their targets of interest through the update process. They carried this out by first stealing the company's certificate then using it to sign the malware. They also configured the update server to only deliver malicious files if the client is located in the range of IP addresses of their target organisations.

9002 RAT also installed additional malicious tools: an exploit tool for Internet Information Services (IIS) 6 WebDav (exploiting CVE-2017-7269) and an SQL database password dumper. These tools hint at how the attackers are also after data stored in their target's web server and database.

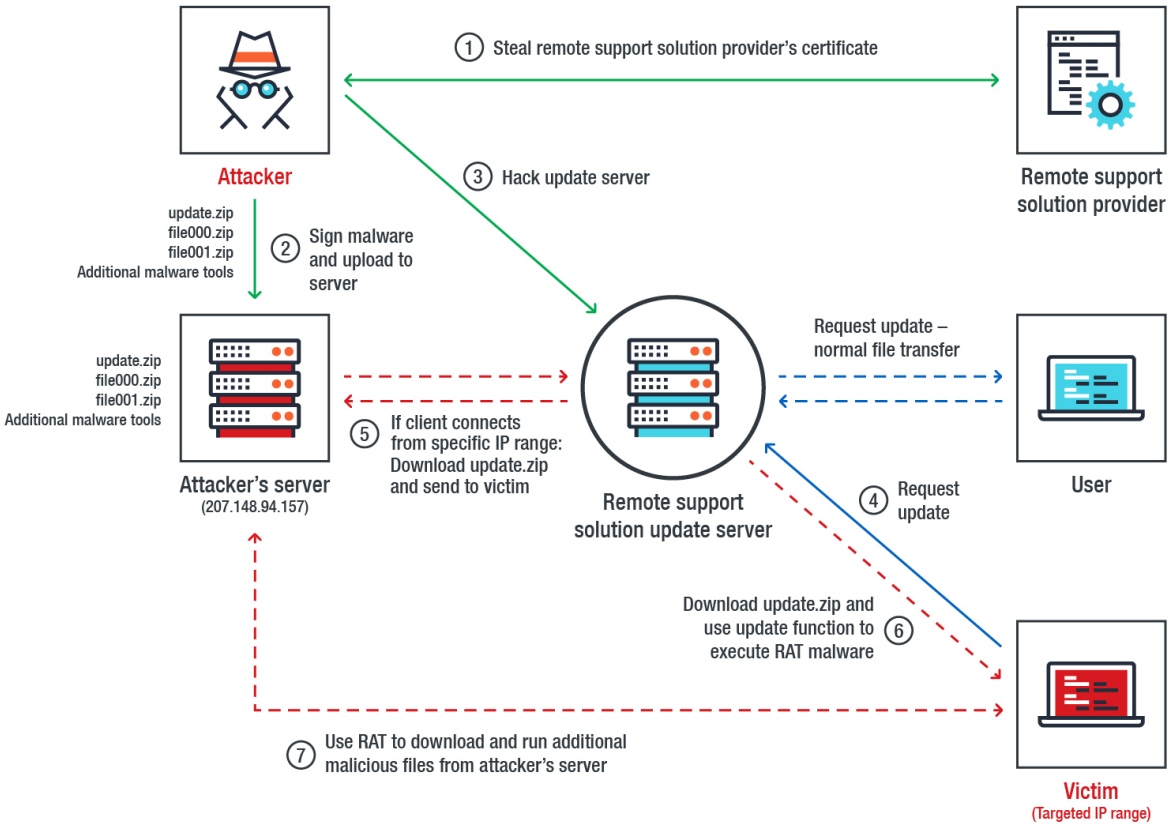


Figure 1. Operation Red Signature's attack chain

Here's how Operation Red Signature works:

1. The code-signing certificate from the remote support solutions provider is stolen. It's possible that the certificate was stolen as early as April 2018, as we found a ShiftDoor malware (4ae4aed210f2b4f75bdb855f6a5c11e625d56de2) on April 8 that was signed with the stolen certificate.
2. Malicious update files are prepared, signed with the stolen certificate, and uploaded to the attacker's server (207[.]148[.]94[.]157).
3. The update server of the company is hacked.
4. The update server is configured to receive an *update.zip* file from the attackers' server if a client is connecting from a specific range of IP addresses belonging to their targeted organisations.
5. The malicious *update.zip* file is sent to the client when the remote support programme is executed.
6. The remote support programme recognises the update files as normal and executes the 9002 RAT malware inside it.
7. 9002 RAT downloads and executes additional malicious files from the attackers' server.

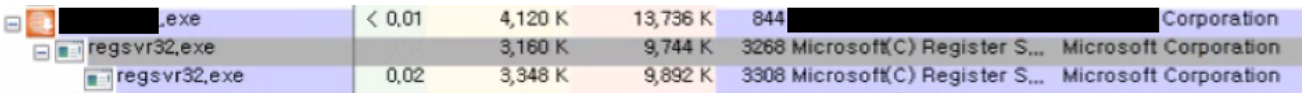
Technical analysis

The *update.zip* file contains an *update.ini* file, which has the malicious update configuration that specifies the remote support solution programme to download *file000.zip* and *file001.zip* and extract them as *rcview40u.dll* and *rcview.log* to the installation folder.

The programme will then execute *rcview40u.dll*, signed with the stolen certificate, with Microsoft register server (*regsvr32.exe*). This dynamic-link library (DLL) is responsible for decrypting the encrypted *rcview.log* file and executing it in memory. 9002 RAT is the decrypted *rcview.log* payload, which connects to the command-and-control (C&C) server at 66[.]42[.]37[.]101.

```
[Files]
FILE0=1000
FILE1=1001
[BeforeUpdate]
Before1=Before_KillFile
[Before_KillFile]
File1=c:\Windows\System32\regsvr32.exe
File2=C:\Windows\SysWOW64\regsvr32.exe
[AfterUpdate]
After1=After_RunFile
[After_RunFile]
File1=0"regsvr32" "%InstallDir%\rcview40u.dll"
[1000]
RealFileName=rcview40u.dll
FileDirectory=%InstallDir%
RealFileSize=64008
DownFileName=file000.zip
DownFileSize=34555
[1001]
RealFileName=rcview.log
FileDirectory=%InstallDir%
RealFileSize=31581
DownFileName=file001.zip
DownFileSize=31725
```

Figure 2. Contents of the malicious update configuration



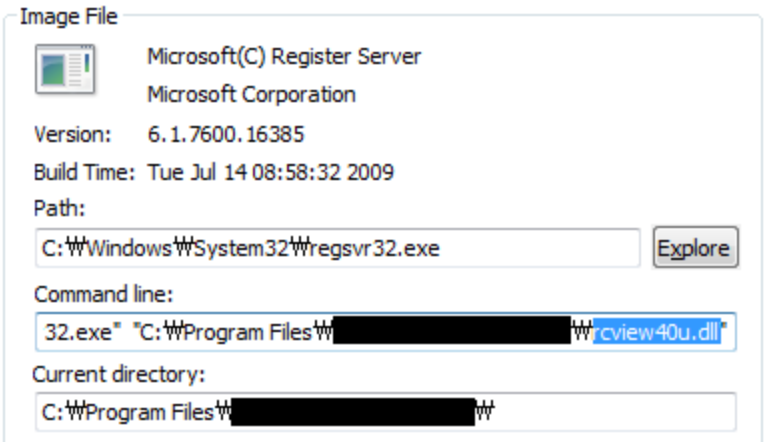


Figure 3. How the compromised update process launches the 9002 RAT malware

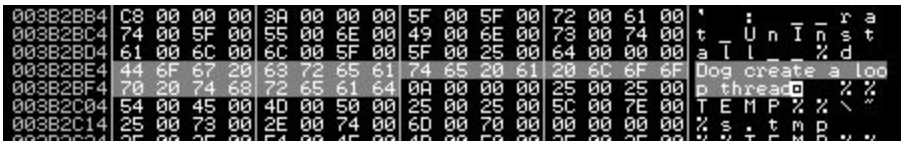


Figure 4. Known 9002 RAT string pattern inside the decrypted payload of the rcview.log file

Correlating 9002 RAT

Delving into 9002 RAT, we found that it was compiled on July 17, 2018, and that the configuration files inside *update.zip* were created on July 18. Our analysis of an update log file we found reveals the remote support programme's update process started around 13:35 on July 18, with the 9002 RAT being downloaded and launched. We also saw the RAT file used for this specific attack was set to be inactive in August, so we can construe that the RAT's activity was rather short-lived (from July 18 to July 31).

```
00004DEE                call    sub_D751
00004DF3                add     esp, 0Ch
00004DF6                cmp     [ebp+var_C], 20180717h
00004DFD                jnz     loc_5081
```

이름	크기	압축된 크기	수정한 날짜
rsup.key	1 156	1 156	2018-07-18 02:49
update.ini	532	258	2018-07-18 02:48

```
07/18/18, 13:35:27 -> Update.zip File Download Success
07/18/18, 13:35:27 -> Update File Count : 2
07/18/18, 13:35:27 -> file000.zip File Downloaded [rcview40u.dll]
07/18/18, 13:35:27 -> file001.zip File Downloaded [rcview.log]
07/18/18, 13:35:28 -> [rcview40u.dll] File Copy
07/18/18, 13:35:28 -> [rcview.log] File Copy
```

Figure 5. Compilation timestamp on 9002 RAT sample (top), timestamp of the malicious configuration (centre), and snapshot of the programme's update log (bottom)

```
if ( ++dword_1000FB34 != 1 )
  goto LABEL_22;
GetSystemTime(&SystemTime);
if ( SystemTime.wYear >= 2018u && SystemTime.wMonth >= 8u )
  goto LABEL_22;                                    // 2018년 8월부터 무한 Sleep(동작안함)
Sleep(1000u);
v0 = GetModuleHandleA("rcview40u.dll");
```

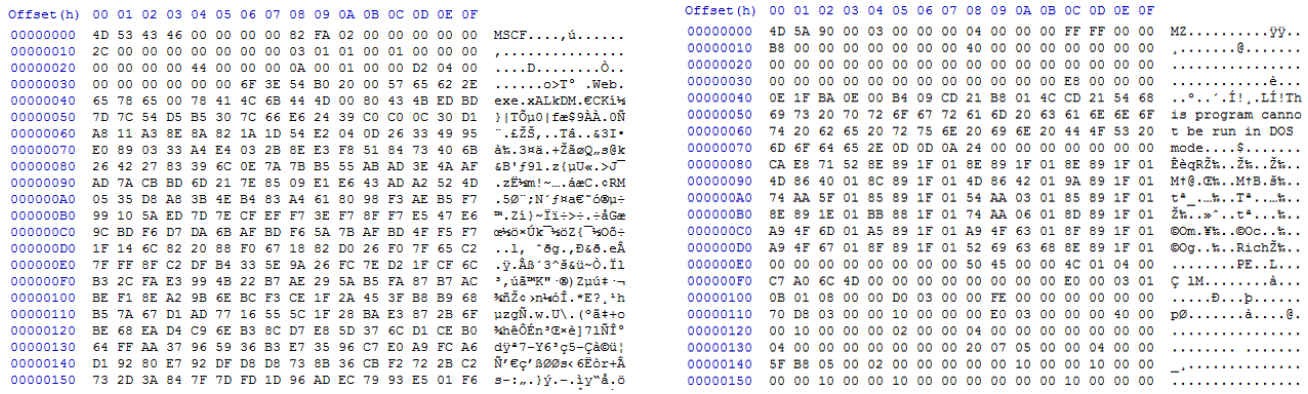
Figure 6. Code snippet showing 9002 RAT checking the system time and setting itself to sleep in August 2018

Additional malware tools

The 9002 RAT also serves as a springboard for delivering additional malware. Most of these are downloaded as files compressed with the Microsoft cabinet format (.cab). This is most likely done to avoid detection by antivirus (AV) solutions.

Here's a list of files that 9002 RAT retrieves and delivers to the affected system:

Filename	Tool	Purpose
dsget.exe	DsGet	View active directory objects
dsquery.exe	DsQuery	Search for active directory objects
sharphound.exe	SharpHound	Collect active directory information
aio.exe	All In One (AIO)	Publicly available hack tool
ssms.exe	SQL Password dumper	Dump password from SQL database
printdat.dll	RAT (PlugX variant)	Remote access tool
w.exe	IIS 6 WebDav Exploit Tool	Exploit tool for CVE-2017-7269 (IIS 6)
Web.exe	WebBrowserPassView	Recover password stored by browser
smb.exe	Scanner	Scans the system's Windows version and computer name
m.exe	Custom Mimikatz (including 32bit / 64bit file)	Verify computer password and active directory credentials



```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000   4D 53 43 46 00 00 00 00 82 FA 02 00 00 00 00 00  MSCF....‚ú......
00000010   2C 00 00 00 00 00 00 00 03 01 01 00 01 00 00 00  ,...............
00000020   00 00 00 00 44 00 00 00 0A 00 01 00 00 D2 04 00  ....D........Ò..
00000030   00 00 00 00 00 00 6F 3E 54 B0 20 00 57 65 62 2E  ......o>T° .Web.
00000040   65 78 65 00 78 41 4C 6B 44 4D 00 80 43 4B ED BD  exe.xALkDM.€CKí½
00000050   7D 7C 54 D5 B5 30 7C 66 E6 24 39 C0 C0 0C 30 D1  }|TÕµ0|fæ$9ÀÀ.0Ñ
00000060   A8 11 A3 8E 8A 82 1A 1D 54 E2 04 0D 26 33 49 95  ¨.£ŽŠ‚..Tâ..&3I•
00000070   E0 89 03 33 A4 E4 03 2B 8E E3 F8 51 84 73 40 6B  à‰.3¤ä.+Žãø Q„s@k
00000080   26 42 27 83 39 6C 0E 7A 7B B5 55 AB AD 3E 4A AF  &B'ƒ9l.z{µU«.>J¯
00000090   AD 7A CB BD 6D 21 7E 85 09 E1 E6 43 AD A2 52 4D  .zË½m!~….áæC.¢RM
000000A0   05 35 D8 A8 3B 4E B4 83 A4 61 80 98 F3 AE B5 F7  .5Ø¨;N´ƒ¤a€˜ó®µ÷
000000B0   99 10 5A ED 7D 7E CF EF F7 3E F7 8F F7 E5 47 E6  ™.Zí}~Ïï÷>÷.÷åGæ
000000C0   9C BD F6 D7 DA 6B AF BD F6 5A 7B AF BD 4F F5 F7  œ½ö×Úk¯½öZ{¯½Oõ÷
000000D0   1F 14 6C 82 20 88 F0 67 18 82 D0 26 F0 7F 65 C2  ..l‚ ˆðg.‚Ð&ð.eÂ
000000E0   7F FF 8F C2 DF B4 33 5E 9A 26 FC 7E D2 1F CF 6C  .ÿ.Âß´3^š&ü~Ò.Ïl
000000F0   B3 2C FA E3 99 4B 22 B7 AE 29 5A B5 FA 87 B7 AC  ³,úã™K"·®)Zµú‡·¬
00000100   BE F1 8E A2 9B 6E BC F3 CE 1F 2A 45 3F B8 B9 68  ¾ñŽ¢›n¼óÎ.*E?¸¹h
00000110   B5 7A 67 D1 AD 77 16 55 5C 1F 28 BA E3 87 2B 6F  µzgÑ.w.U\.(ºã‡+o
00000120   BE 68 EA D4 C9 6E B3 8C D7 E8 5D 37 6C D1 CE B0  ¾hêÔÉn³Œ×è]7lÑΰ
00000130   64 FF AA 37 96 59 36 B3 E7 35 96 C7 E0 A9 FC A6  dÿª7–Y6³ç5–Çà©ü¦
00000140   D1 92 80 E7 92 DF D8 D8 73 8B 36 CB F2 72 2B C2  Ñ'€ç'ßØØs‹6Ëòr+Â
00000150   73 2D 3A 84 7F 7D FD 1D 96 AD EC 79 93 E5 01 F6  s-:„.}ý.–.ìy“å.ö

Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000   4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ.........ÿÿ..
00000010   B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
00000020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030   00 00 00 00 00 00 00 00 00 00 00 00 E8 00 00 00  ............è...
00000040   0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
00000050   69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
00000060   74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS
00000070   6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
00000080   CA E8 71 52 8E 89 1F 01 8E 89 1F 01 8E 89 1F 01  Êèq RŽ‰..Ž‰..Ž‰..
00000090   4D 86 40 01 8C 89 1F 01 4D 86 42 01 9A 89 1F 01  M†@.Œ‰..M†B.š‰..
000000A0   74 AA 5F 01 85 89 1F 01 54 AA 03 01 85 89 1F 01  tª_.…‰..Tª...…‰..
000000B0   8E 89 1E 01 BB 88 1F 01 74 AA 06 01 8D 89 1F 01  Ž‰..»ˆ..tª...‰..
000000C0   A9 4F 6D 01 A5 89 1F 01 A9 4F 63 01 8F 89 1F 01  ©Om.¥‰..©Oc..‰..
000000D0   A9 4F 67 01 8F 89 1F 01 52 69 63 68 8E 89 1F 01  ©Og..‰..RichŽ‰..
000000E0   00 00 00 00 00 00 00 00 50 45 00 00 4C 01 04 00  ........PE..L...
000000F0   C7 A0 6C 4D 00 00 00 00 00 00 00 00 E0 00 03 01  Ç lM........à...
00000100   0B 01 08 00 00 D0 03 00 00 FE 00 00 00 00 00 00  .....Ð...þ......
00000110   70 D8 03 00 00 10 00 00 00 E0 03 00 00 00 40 00  pØ.......à....@.
00000120   00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00  ................
00000130   04 00 00 00 00 00 00 00 20 07 05 00 00 04 00 00  ........ .......
00000140   5F B8 05 00 02 00 00 00 00 00 10 00 00 10 00 00  _¸..............
00000150   00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00  ................
```

Figure 7. Downloaded Web.ex_ cabinet file (left) and decompressed Web.exe file (right)

One of the downloaded files *printdat.dll*, which is another RAT. It is a variant of PlugX malware, and connects to the same C&C server (66[.]42[.]37[.]101).

```
.text:1000E0A7    push    esi
.text:1000E0A8    mov     eax, edi
.text:1000E0AA    mov     dword ptr [esi], 20120712h
.text:1000E0B0    mov     dword ptr [esi+4], 4000h
.text:1000E0B7    mov     dword ptr [esi+8], 4
.text:1000E0BE    mov     dword ptr [esi+0Ch], 0
.text:1000E0C5    call    sub_1000FB30
```

Figure 8. Internal PlugX date dword value inside the printdat.dll file

Mitigating supply chain attacks

Supply chain attacks don't just affect users and businesses — they exploit the trust between vendors and its clients or customers. By trojanizing software/applications or manipulating the infrastructures or platforms that run them, supply chain attacks affects the integrity and security of the goods and services that organisations provide. In healthcare, for instance, where the industry heavily relies on third-party and cloud-based services, supply chain attacks can risk the privacy of personally identifiable data and intellectual property, disrupt hospital operations, and even endanger patient health. And when stacked up with regulations such as the EU General Data Protection and Regulation (GDPR), the impact can be exacerbated.

Here are some best practices:

- Oversee third-party products and services; apart from ensuring the security of the organisation's own online premises (e.g., patching, authentication mechanisms), security controls must also be in place in third-party applications being used.
- Develop a proactive incident response strategy: Supply chain attacks are often targeted; organisations must be able to fully understand, manage, and monitor the risks involved in third-party vendors.
- Proactively monitor the network for anomalous activities; firewalls and intrusion detection and prevention systems help mitigate network-based threats.

- Enforce the principle of least privilege: Network segmentation, data categorisation, restriction of system administration tools, and application control help deter lateral movement and minimise data being exposed.

Trend Micro Solutions

The Trend Micro™ Deep Discovery™ solution provides detection, in-depth analysis, and proactive response to today's stealthy malware and targeted attacks in real time. It provides a comprehensive defence tailored to protect organisations against targeted attacks and advanced threats through specialised engines, custom sandboxing, and seamless correlation across the entire attack life cycle, allowing it to detect threats even without any engine or pattern update. Trend Micro endpoint solutions such as the Smart Protection Suites and Worry-Free Business Security solutions can protect users and businesses from threats by detecting malicious files and blocking all related malicious URLs.

Indicators of Compromise (IoCs):

Related hashes (SHA-256):

- 0703a917aaa0630ae1860fb5fb1f64f3cfb4ea8c57eac71c2b0a407b738c4e19 (ShiftDoor) — detected by Trend Micro as BKDR_SETHC.D
- c14ea9b81f782ba36ae3ea450c2850642983814a0f4dc0ea4888038466839c1e (aio.exe) — HKTL_DELOG
- a3a1b1cf29a8f38d05b4292524c3496cb28f78d995dfb0a9aef7b2f949ac278b (m.exe) — HKTL_MIMIKATZ
- 9415ca80c51b2409a88e26a9eb3464db636c2e27f9c61e247d15254e6fbb31eb (printdat.dll) — TSPY_KORPLUG.AN
- 52374f68d1e43f1ca6cd04e5816999ba45c4e42eb0641874be25808c9fae15005 (rcview.log) — TROJ_SIDELOADR.ENC
- bcfacc1ad5686aee3a9d8940e46d32af62f8e1cd1631653795778736b67b6d6e (rcview40u.dll) — TROJ_SIDELOADR.A
- 279cf1773903b7a5de63897d55268aa967a87f915a07924c574e42c9ed12de30 (sharphound.exe) — HKTL_BLOODHOUND
- e5029808f78aec4a079e889e5823ee298edab34013e50a47c279b6dc4d57b1ffc (ssms.exe) — HKTL_PASSDUMP
- e530e16d5756cdc2862b4c9411ac3bb3b113bc87344139b4bfa2c35cd816e518 (w.exe) — TROJ_CVE20177269.MOX
- 28c5a6aefcc57e2862ea16f5f2ecb1e7df84b68e98e5814533262595b237917d (Web.exe) — HKTL_BROWSERPASSVIEW.GA

URLs related to the malicious update file:

- hxxp://207[.]148[.]94[.]157/update/rcv50/update.zip
- hxxp://207[.]148[.]94[.]157/update/rcv50/file000.zip

- hxxp://207[.]148[.]94[.]157/update/rcv50/file001.zip

URLs related to additionally downloaded malicious files:

- hxxp://207[.]148[.]94[.]157/aio.exe
- hxxp://207[.]148[.]94[.]157/smb.exe
- hxxp://207[.]148[.]94[.]157/m.ex_
- hxxp://207[.]148[.]94[.]157/w
- hxxp://207[.]148[.]94[.]157/Web.ex_

Related C&C server (9002 RAT and PlugX variant):

66[.]42[.]37[.]101