Supply Chain Attack Operation Red Signature Targets South Korean Organizations

Posted on: August 21, 2018 at 6:04 am **Posted in:** Malware, Targeted Attacks
Author: Trend Micro Cyber Safety Solutions Team

by Jaromir Horejsi, Joseph C. Chen, Kawabata Kohei, and Kenney Lu

Together with our colleagues at IssueMakersLab, 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.

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 organizations.

9002 RAT also installed additional malicious tools: an exploit tool for Internet Information Services

Featured Stories

systemd Vulnerability Leads to Denial of Service on Linux

qkG Filecoder: Self-Replicating, Document-Encrypting Ransomware

Mitigating CVE-2017-5689, an Intel Management Engine Vulnerability

A Closer Look at North Korea's Internet

From Cybercrime to Cyberpropaganda

Security Predictions for 2018

Attackers are banking on network vulnerabilities and inherent weaknesses to facilitate massive malware attacks,

(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.

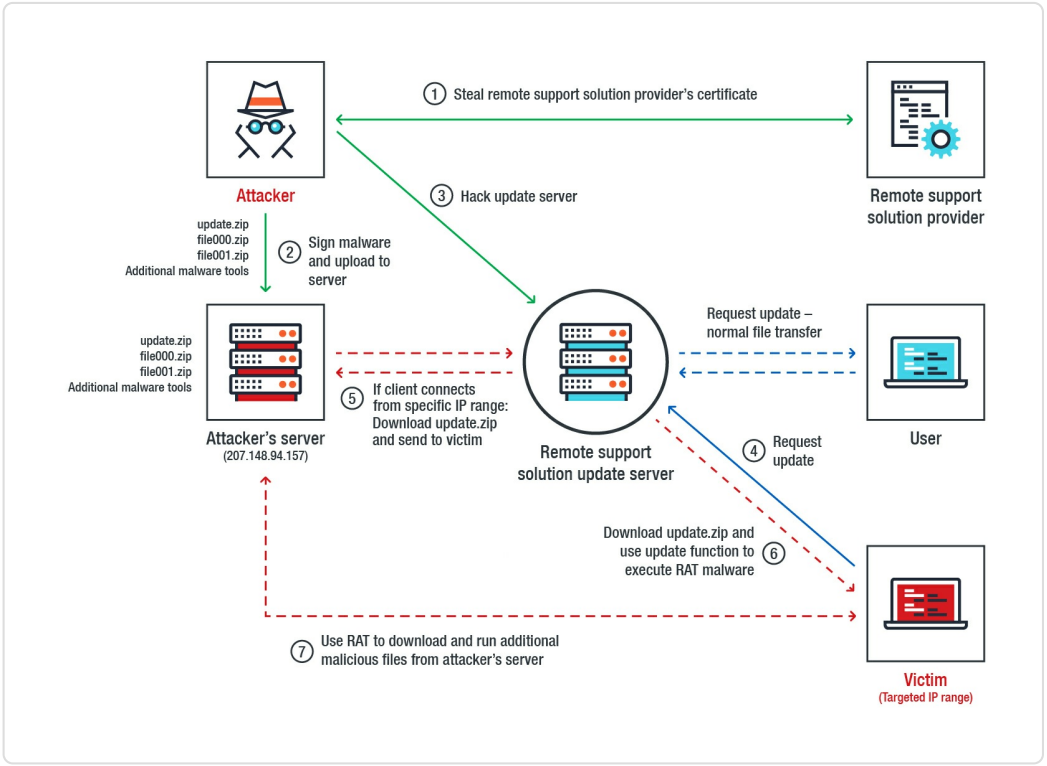


Figure 1. Operation Red Signature's attack chain

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 organizations.

IoT hacks, and operational disruptions. The ever-shifting threats and increasingly expanding attack surface will challenge users and enterprises to catch up with their security.
Read our security predictions for 2018.

Business Process Compromise

Attackers are starting to invest in long-term operations that target specific processes enterprises rely on. They scout for vulnerable practices, susceptible systems and operational loopholes that they can leverage or abuse. To learn more, read our Security 101: Business Process Compromise.

Recent Posts

Supply Chain Attack Operation Red Signature Targets South Korean Organizations

Use-after-free (UAF) Vulnerability CVE-2018-8373 in VBScript Engine Affects Internet Explorer to Run Shellcode

August Patch Tuesday: A Tale of Two Zero-Days

Ransomware as a Service Princess Evolution Looking for Affiliates

How Machine Learning Can Help Identify Web Defacement Campaigns

5. The malicious *update.zip* file is sent to the client when the remote support program is executed.
6. The remote support program recognizes 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 program to download *file000.zip* and *file001.zip* and extract them as *rcview40u.dll* and *rcview.log* to the installation folder.

The program 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.

Popular Posts

The Need for Managed Detection and Response: Persistent and Prevalent Threats in North America's Security Landscape

New Underminer Exploit Kit Delivers Bootkit and Cryptocurrency-mining Malware with Encrypted TCP Tunnel

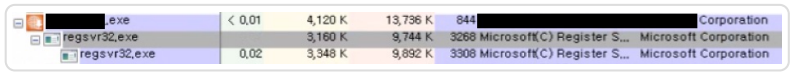
How Machine Learning Can Help Identify Web Defacement Campaigns

Malware Targeting Bitcoin ATMs Pops Up in the Underground

Ransomware as a Service Princess Evolution Looking for Affiliates

```
[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



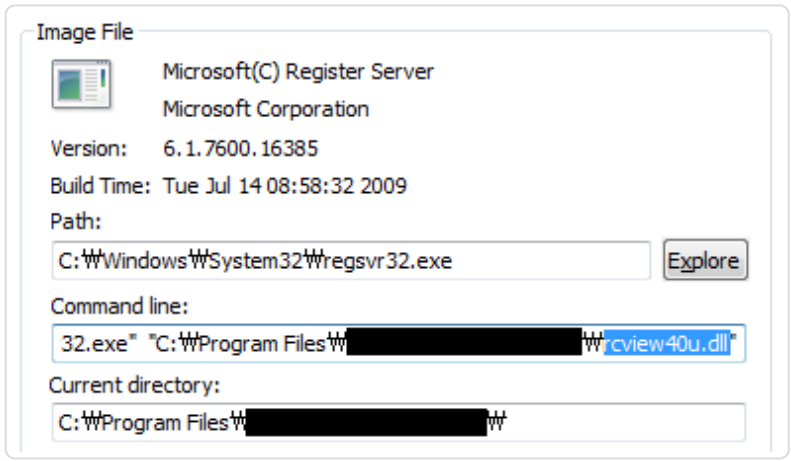


Figure 3. How the compromised update process launches the 9002 RAT malware

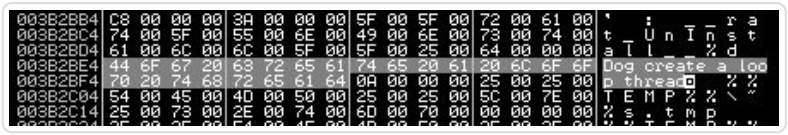


Figure 4. Known 9002 RAT string pattern inside the decrypted payload of the rcview.log file

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 program'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 (center), and snapshot of the program'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

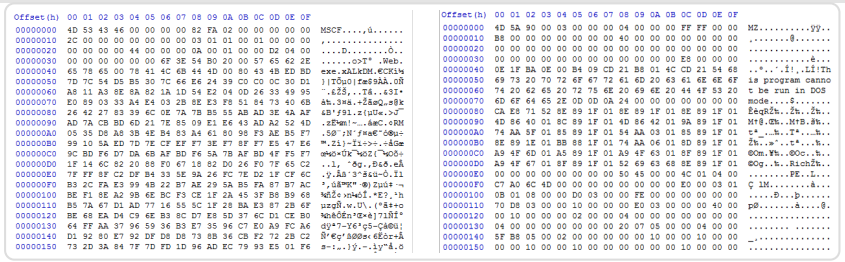


Figure 7. Downloaded Web.ex_ cabinet file (left) and decompressed Web.exe file (right)

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 organizations 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 organization'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; organizations 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 categorization, restriction of system administration tools, and application control help deter lateral movement and minimize 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 defense tailored to protect organizations against targeted attacks and advanced threats through specialized 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
- 52374f68d1e43f1ca6cd04e5816999ba45c4e42eb0641874be25808c9fe15005 (rcview.log) — TROJ_SIDELOADR.ENC
- bcfacc1ad5686aee3a9d8940e46d32af62f8e1cd1631653795778736b67b6d6e (rcview40u.dll) — TROJ_SIDELOADR.A
- 279cf1773903b7a5de63897d55268aa967a87f915a07924c574e42c9ed12de30 (sharphound.exe) — HKTL_BLOODHOUND
- e5029808f78ec4a079e889e5823ee298edab34013e50a47c279b6dc4d57b1ffc (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

Related Posts:

- **From Cybercrime to Cyberpropaganda**

- **REDBALDKNIGHT/BRONZE BUTLER's Daserf Backdoor Now Using Steganography**
- **Lazarus Campaign Targeting Cryptocurrencies Reveals Remote Controller Tool, an Evolved RATANKBA, and More**
- **Tropic Trooper's New Strategy**

Tags: Operation Red Signature | South Korea | supply chain