Operation Red Signature Targets South Korean Companies

By Jaromir Horejsi, Joseph C Chen, Kawabata Kohei, Kenney Lu (words)

Published: 2018-08-21 · Archived: 2026-04-05 23:12:09 UTC

Together with our colleagues at IssueMakersLabopen on a new tab, 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 (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.


intel*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.
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.

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).

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

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).

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 healthcarenews article, for instance, where the industry heavily relies on third-party and cloud-based servicesnews article, 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:

- Overseenews- cybercrime-and-digital-threats 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; firewallsnews article and intrusion detection and prevention systemsproducts help mitigate network-based threats.

- Enforce the principle of least privilegenews- cybercrime-and-digital-threats: Network segmentationnews article, data categorizationnews article, restrictionnews- cybercrime-and-digital-threats of system administration toolsnews article, and application control help deter lateral movement and minimize data being exposed.

Trend Micro Solutions

The Trend Micro™ Deep Discoveryproducts™ 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 sandboxingnews article, 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 Suitesproducts 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

Source: https://blog.trendmicro.com/trendlabs-security-intelligence/supply-chain-attack-operation-red-signature-targets-south-korean-organizations/