Kimsuky disguised as a Korean company signed with a valid certificate to distribute Troll Stealer (English ver.)

medium.com/s2wblog/kimsuky-disguised-as-a-korean-company-signed-with-a-valid-certificate-to-distribute-troll-stealer-cfa5d54314e2

S2W

February 8, 2024

--

Author: Jiho Kim & Sebin Lee | BLKSMTH

> *: Feb 7, 2024*

Photo by on

Executive Summary

S2W threat research and intelligence center has hunted for and analyzed a sample of what is believed to be a new malware from the Kimsuky group on VirusTotal.

— The malware was found to be distributed from a page that redirects users to a specific site located in South Korea to download a security program.

— Unlike typical supply chain attacks, only 2 of the 5 installers distributed by the site were modified to include the malware.

- The hunted malware is an Info-stealer malware written in Go language that steals information from the infected system, which is dropped and executed from a Dropper disguised as a security program installation file (TrustPKI, NX_PRNMAN) from SGA Solutions.
- The dropper runs as a legitimate installer alongside the malware, and both the dropper and malware are signed with , suggesting that the company's certificate was actually stolen.
- S2W Talon has named the malware "" because it contains the pathname "D:/~/repo/golang/src/root.go/s//agent" within the malware.
- Troll Stealer can steal information from the infected system like SSH, FileZilla, C drive files/directories, browser, system information, screen captures and send it to the C&C server.
- Based on the Kimsuky group's recent active use of Go-based malware, and the fact that Troll Stealer contains a lot of code similar to the AppleSeed and AlphaSeed malware associated with the Kimsuky group, we speculate that the Kimsuky group is behind the distribution of this malware.

— However, there is also a possibility that another group closely associated with the Kimsuky group is behind the malware, as we have identified some differences in the TTPs from those previously observed from the Kimsuky group.

Troll Stealer includes the ability to steal the GPKI folder on infected systems, which suggests that the campaign may have been targeting devices within administrative and public organizations in South Korea.

— However, there are some differences in the TTP from the Kimsuky group's previous TTPs, suggesting that another group closely associated with the Kimsuky group may be behind this campaign.

In addition to Troll Stealer, , so malware signed with that certificate may be distributed in the future.

Introduction

On January 10, 2024, a Go language-based information-stealing malware was discovered and we conducted a detailed analysis. The malware was distributed from a security program download page that was redirected when accessing a specific website in Korea and disguised as a security program installation file (TrustPKI, NX_PRNMAN) of SGA Solutions.

Figure 1. Example of a security program download page when accessing a specific website in South Korea

The malware was identified as a dropper type that drops and executes both a legitimate installer and malware when executed, and both the dropper and internal malware were signed with a valid "**D2innovation Co.,LTD**" certificate instead of the original certificate "SGA Solutions".

Figure 2. Valid D2innovation Co.,LTD certificate identified by the Dropper malware.

The DLL file dropped from the dropper file is a Go language-based information-stealing malware packed with VMProtect and contains the path "D:/~/repo/golang/src/root.go/s/**troll**/agent" inside. It collects certain files and system information on the infected system and leaks the collected information to the C&C server. Our analysis revealed that it borrows some code from open-source stealers.

Figure 3. Paths present in the Troll Stealer.

Talon, S2W's threat research and intelligence center, believes that the Kimsuky group is behind the malware because it has similarities to existing malware from the Kimsuky group, such as nearly identical commands for collecting system information in the AppleSeed malware and the same RC4 + RSA combination for file encryption used by the AlphaSeed malware.

Talon has named the malware "**Troll Stealer**" because it uses the pathname "D:/~/repo/golang/src/root.go/s/**troll**/agent".

Detailed Analysis

Sample Information

- MD5: 7b6d02a459fdaa4caa1a5bf741c4bd42
- SHA256: f8ab78e1db3a3cc3793f7680a90dc1d8ce087226ef59950b7acd6bb1beffd6e3

The malware is disguised as the TrustPKI installer for the SGA solution, and when executed, it steals information from the infected system and sends it to the C&C server.

1. Dropper drops a malicious DLL file and loads the file via Rundll32.exe
2. It executes the NXTPKIENTS.exe file, which is a legitimate installer
3. Troll Stealer steals information from the infected system through malicious behavior
4. Then, it sends stolen data to the C&C server
5. Also, it performs self-deletion via Powershell

Figure 4. Malware execution flow

Stage1. Dropper

1. Mutex & Self-deletion

When executed, it creates a mutex to prevent duplicate execution and subsequently creates and executes a BAT script file in the %Temp% subpath for self-deletion.

Mutex name: windows update {2024–1020–02A}

- : %Temp%\\[A-Z0–9]{4}.tmp.bat
-

```
:goto_redelrd /s /q [File path]del [File path]if exist [File path] goto goto_redeldel %Temp%\\[A-Z0-9]{4}.tmp.bat
```

2. Execute Normal Installer (NXTPKIENTS.exe)

Then drop and run a legitimate installation file from SGA Solutions in the Desktop path. The installation file is verified to be a legitimate file signed with the "SGA Solutions Co.,Ltd". certificate.

: %USERPROFILE%\Desktop\NXTPKIENTS.exe

Figure 5. Legitimate SGA Solutions installation file executed by the Dropper malware.

3. Drop & Load Malicious DLL

In addition to the normal installation files, it also drops Troll Stealer and a file for checking for infection, and the paths to each of these files are shown below. The folder and file names generated by different Dropper malware samples vary, but the following paths and names were found in the samples we analyzed.

Table 2. Paths where information-stealing malware is dropped and filenames for infection history checks

Troll Stealer is then executed via the rundll32.exe process, which calls the same Export function as the filename used for the infection check. The malware was packed with VMProtect to prevent analysis.

: C:\Windows\system32\rundll32.exe %AppData%\[DLL Path] [Export]

Stage2. Troll Stealer

- : C:\Users\admin\AppData\Roaming\Hancom\hc-[a-z0–9]{8}.png
- : 88f183304b99c897aacfa321d58e1840
- : 61b8fbea8c0dfa337eb7ff978124ddf496d0c5f29bcb5672f3bd3d6bf832ac92
- : DLL

1. Initial behavior

During its initial execution, it deletes the “ChromeUpdateTaskMachineUAC” scheduler. However, given that Troll Stealer and its parent Dropper do not have the feature to register a scheduler with the above name, it is likely that it did not accidentally remove a feature that was used in the past.

: schtasks /delete /f /tn “ChromeUpdateTaskMachineUAC”

The malware then checks for the existence of the file to check the infection dropped by the dropper malware to determine if it was executed via a dropper. It performs malicious behavior only if the file exists.

: %ProgramData%\limsjo.a

Stealer itself registers mutexes to prevent malware duplicate execution.

: chrome development kit 1.0

2. Set configuration data

It collects the MAC address and directory path of the infected system and creates a temporary file with configured data for later malicious behavior. Configuration contains information such as C&C server addresses.

- : %UserProfile%\.tmp\{Random Number}.org
- : hxxp[:]//qi.limsjo.p-e[.]kr/index.php
- : hxxp[:]//ai.limsjo.p-e[.]kr/index.php

Table 2. Data in configuration

Examples of configuration data

```
{ "ServerID": 0, "ObjectID": 0, "GtType": 2111, "GtID": [sha1_hash(little_endian(mac_addr[:8]))], "GtVer": "gt@2.0", "Interval": 0,
"LocalPath": "%AppData%\\local\\", "MacAddr": [MacAddr], "ProxyNum": 5, "ProxyUrl": [  "",  "",  "",  "http://qi.limsjo.p-
e.kr/index.php",  "http://ai.limsjo.p-e.kr/index.php" ]}
```

The Config file is then encrypted, sent to the C&C server, and deleted.

%AppData%\local\gcfg@{YYMMDD}(HH.MM.SS-000).gte1

3. Data collection

Troll Stealer steals various information from the infected system, encrypts it, and sends it to the C&C server. The malware steals the following information

Table 3. Target data and encrypted filename

3.1. SSH

It exfiltrates the infected system's SSH information. It compresses the system's *.ssh* directory and creates a file. Afterward, it encrypts the compressed file, creates a file in a different path, and sends it to the C&C server.

- : %USERPROFILE%\.ssh
- : %AppData%\local\tsd@{YYMMDD}(HH.MM.SS-000).gte1

3.2. FileZilla

It exfiltrates information from FileZilla software present on the infected system. It compresses the *filezilla* directory and creates a file. The compressed file is then encrypted and created as a file in a different path and sent to the C&C server.

- : %AppData%\filezilla
- : %AppData%\local\tfd@{YYMMDD}(HH.MM.SS-000).gte1

3.3. Microsoft Sticky Note

It exfiltrates information from Microsoft Sticky Note present on the infected system. It compresses the *localstate* directory and creates a file. The compressed file is then encrypted and created as a file in a different path and sent to the C&C server.

- : %USERPROFILE%\AppData\Local\packages\microsoft.microsoftstickynotes_8wekyb3d8bbwe\localstate
- : %AppData%\local\tnd@{YYMMDD}(HH.MM.SS-000).gte1

3.4. "GPKI" directory in C Drive

Troll Stealer steals data from a specific folder on the C drive of an infected system. The attacker collects the names of files and folders on the C drive and appends additional strings to create a new string, as shown below. It then generates a SHA512 hash of that string, and if it is the same as the hardcoded SHA512 hash in the malware, it encrypts the file and sends it to the C&C server. Analyzing the hardcoded SHA512 hash revealed that the attacker attempted to steal the **GPKI** folder on the C drive.

: "aaxxyyzz" + {File name} + "zzyyxxaa"

==> Target string: aaxxyyzz**gpki**zzyyxxaa

- : 17ccb0832c3382b5f9e86236e035d899a351c98f3871080c138d4494218cbbc2b6f9dc43705ed97e8b0b09f25752302094e0d297151f67b2232
- : %AppData%\local\tcd@{YYMMDD}(HH.MM.SS-000).gte1

GPKI, also known as an administrative electronic signature certificate, is an authorized certificate used to verify the authenticity of administrative electronic signatures, which is used by governments such as administrative and public institutions in South Korea. In other words, it is not used on ordinary computers but is usually installed on computers used for public affairs. In this regard, it is believed that this campaign is aimed at targeting PCs installed in public.

3.5. Browser Information

It steals browser information from the infected system. The malware is believed to have utilized HackBrowserData, an open-source program written in Go language, to steal browser information. It targets Chromium-based browsers and Firefox browsers on infected systems and steals various information such as cookies, history, downloads, and extensions and saves them as JSON files in the browser directory. After compressing the browser directory, it performs encryption and sends it to the C&C server.

- : %AppData%\local\browser
- : %AppData%\local\tbd@{YYMMDD}(HH.MM.SS-000).gte1

3.6. System Information

It steals system information from an infected system. It collects infected system information through CMD commands, encrypts it, and creates a file. The encrypted file is sent to the C&C server.

: %AppData%\local\ccmd@{YYMMDD}(HH.MM.SS-000).gte1

Table 4. List of system information collected

```
systeminfo & net user & query user & powershell Get-CimInstance -Namespace root/SecurityCenter2 -Classname AntivirusProduct & wmic
qfe & wmic startup get & wmic logicaldisk get & ipconfig /all & arp -a & route print & tasklist & wmic process get Caption,
Commandline & dir "%programfiles%" & dir "%programfiles% (x86)" & dir "%programdata%\Microsoft\Windows\Start Menu\Programs" & dir
"%appdata%\Microsoft\Windows\Recent" & dir /s "%userprofile%\desktop" & dir /s "%userprofile%\downloads" & dir /s
"%userprofile%\documents"
```

3.7. Screen Capture

Capture the current desktop screen of the infected machine and save it to a file. Use the screenshot package of "kbinani" published on Github to capture the desktop screen. Encrypt the captured file and create a file, then send the encrypted file to the C&C server.

: %AppData%\local\ssht@{YYMMDD}(HH.MM.SS-000).gte1

4. File Encryption

Before sending the stolen data to the C&C server, it encrypts the data using a combination of RC4 and RSA-4096 algorithms. The malware parses the RSA public key from the hardcoded DER of PKCS#1. It then randomly generates an RC4 key value and uses it to encrypt the stolen data. The RC4 encryption key is encrypted with the RSA public key.

Figure 6. Encryption flow before file transfer

```
3082020a0282020100c3fc0e50f4dcafec48ee42362d70c8f6b3153e91566b15a9540d0ca9f3e81846093d8752940b414043c0eaa752dd29b3aa7132bc3a1c9d8c8e
```

5. C&C Communication

The malware creates a 60-byte structure and organizes 12 fields to exfiltrate the Config data and data stolen from the victim system. The value of each field is set differently depending on the purpose of the communication and the type of data to be transmitted, and the payload is located after the size_payload field. The configured data is XORed and Base64 encoded and sent to the C&C server through the HTTP protocol. The common structure for communication is shown in *Figure 7*, and the meaning of each field is described in *Table 5*.

Figure 7. The communication data structures used by Troll Stealer.

Table 5. Fields in a data structure

After organizing the data to be sent into a structure, it performs an XOR operation followed by Base64 encoding using a hardcoded 4-byte key in the binary. The encoded result is sent to the C&C server in the format "**a=[Encoded_Data]**".

: DD 33 99 CC

Figure 8. Data computation process

The final stolen data is sent as follows:

Steal data => Encrypt file(RC4+RSA) => Encode structure used for communication(XOR+Base64) => Pass as parameter

Troll Stealer sends the "init" string in the payload to the C&C server only the first time it communicates, and only when it receives the "ok" string in response does it continue to leak the stolen data.

In this case, there are a total of four communications per exfiltration of configuration or stolen items: the first communication is to perform the ping function, and the second and third communications are sent with the same data in the payload. However, we can see that the value of the *status_type* field is configured differently. Finally, the fourth communication includes the stolen filename in the payload and sets the value of the *send_type* field to 5. Once the file is successfully sent to the C&C server, delete the encrypted file in the %appdata%\local\ path.

Figure 9. Communication flow for Troll Stealer

6. Self-deletion

After executing the malware, it creates a PS1 file in the *.tmp* directory and runs it via the powershell.exe, which deletes Troll Stealer itself.

- : %USERPROFILE%\.tmp\{Random}.ps1
- : powershell.exe -executionpolicy bypass -File [ps1 file]
-

```
$target = {Stealer Path}for ($i = 0; $i -lt 50; $i++){ Remove-Item $target -Force Remove-Item $PSCommandPath -Force if (!(Test-Path $target) -and !(Test-Path $PSCommandPath)) {  break } Start-Sleep -Seconds 2}
```

Attribution

S2W speculates that the Kimsuky group may be behind the distribution of this malware based on the group's recent active use of Go-based malware and the similarity of the code to existing AppleSeed and AlphaSeed malware.

Correlation with AppleSeed/AlphaSeed

The path that the dropper malware drops Troll Stealer and the filename format it creates appear similar to the path and filename of AppleSeed, which was disclosed by ASEC.

Table 8. AppleSeed vs. Troll Stealer path and filename comparison

In addition, the hardcoded commands it executes to collect infected system information are identical to those found in the AppleSeed malware discovered in May 2023. However, in the case of the recently discovered malware, two additional commands were added to obtain information about the user's accounts and sessions.

- net user
- query user

Table 9. Comparison of commands to steal information

In addition, the same type of mutexes identified in the Troll Stealer Dropper malware were found in both AppleSeed Dropper and Meterpreter, which have been used by the Kimsuky group in the past.

Table 10. Mutexes used in the Kimsuky group's malware

Troll Stealer then compresses the folder where the stolen files are stored and encrypts them using RSA and RC4 algorithms. We found that the combniation and the encryption execution flow are the same as those used by AlphaSeed.

Figure 10. The encryption/decryption method used by AlphaSeed and Troll Stealer.

Furthermore, the Go language library used to capture the victim system's desktop screen was identified as the same kbinani package also used by AlphaSeed.

Another golang-based backdoor (GoBear)

In addition to the Troll Stealer, another Go language-based backdoor malware signed with a legitimate "D2innovation Co.,LTD certificate" was also found.

- : 87429e9223d45e0359cd1c41c0301836
- : hxxp[:]//coolsystem[.]co.kr/admin/mail/index.php
- :

The malware performs malicious behaviors based on the commands it receives from the C&C server, and the strings contained in the names of the functions it calls have been found to overlap with the commands used by **BetaSeed**, a C++-based backdoor malware used by the Kimsuky group. The DLL version of BetaSeed also steals information from the victim system and performs additional malicious actions based on the commands it receives from the C&C server.

- : d6abeeb469e2417bbcd3c122c06ba099
- :

However, the 2 malware were separated into different types because they were written in different languages and there were no similarities in the code other than the strings in the function names.

Table 11. Correlations between backdoor malware used by the Kimsuky group

It is noteworthy that GoBear adds SOCKS5 proxy functionality, which was not previously supported by the Kimsuky group's backdoor malware. Furthermore, the fact that the mutex used in the previous AppleSeed malware was reused after two years without being updated suggests that the author of the Troll Stealer malware based on AppleSeed may have made a mistake.

Conclusion

- S2W threat research and intelligence center has hunted for and analyzed a sample of a new malware from the Kimsuky group, and named .
- Troll Stealer is written in Go and identified as an Info-stealer malware that steals information from infected systems (SSH, FileZilla, C drive files/directories, browsers, system information, screen captures). —Troll Stealer is distributed by dropping and executing from a Dropper disguised as SGA Solutions' Trusted PKI installer.
- The dropper runs as a legitimate installer alongside the malware, and both the dropper and malware are signed with a , suggesting that the company's certificate was actually stolen.
- Troll Stealer includes the ability to steal the folder on infected systems, which suggests that the campaign may have been targeting devices within administrative and public organizations in South Korea — The Kimsuky group has no known history of hijacking GPKI folders or utilizing the SOCKS5 protocol in the past, so it is possible that they have set new targets, or that another group with access to the source code for AppleSeed/AlphaSeed created Troll Stealer and GoBear.
- S2W believes that the Kimsuky group is likely behind the distribution of this malware based on the group's active use of Go-based malware and the many similarities found between Troll Stealer and the existing AppleSeed and AlphaSeed malware.
- In addition to Troll Stealer, additional malware signed with the same legitimate certificate was found, so it is possible that malware signed with that certificate may be distributed in the future.

MITRE ATT&CK

Resource Development

(T1588.004) Digital Certificates

Execution

- (T1204.002) Malicious File
- (T1059.001) PowerShell
- (T1059.003) Windows Command Shell

Defense Evasion

(T1027.002) Software Packing

Credential Access

- (T1555.003) Credentials from Web Browsers
- (T1539) Steal Web Session Cookie

Discovery

- (T1057) Process Discovery
- (T1087.001) Local Account
- (T1083) File and Directory Discovery
- (T1518.001) Security Software Discovery
- (T1082) System Information Discovery
- (T1016) System Network Configuration Discovery

Collection

- (T1005) Data from Local System
- (T1113) Screen Capture
- (T1560) Archive Collected Data

Command and Control

(T1071.001) Web Protocol

Exfiltration

(T1041) Exfiltration Over C2 Channel

Appendix A. IoCs

File hash

Dropper

- 19c2decfa7271fa30e48d4750c1d18c1
- 6eebb5ed0d0b5553e40a7b1ad739589709d077aab4cbea1c64713c48ce9c96f9
- 7b6d02a459fdaa4caa1a5bf741c4bd42
- f8ab78e1db3a3cc3793f7680a90dc1d8ce087226ef59950b7acd6bb1beffd6e3
- 27ef6917fe32685fdf9b755eb8e97565
- 2e0ffaab995f22b7684052e53b8c64b9283b5e81503b88664785fe6d6569a55e

Backdoor (GoBear)

- 87429e9223d45e0359cd1c41c0301836
- a8c24a3e54a4b323973f61630c92ecaad067598ef2547350c9d108bc175774b9

Troll Stealer

- 7457dc037c4a5f3713d9243a0dfb1a2c
- ff3718ae6bd59ad479e375c602a81811718dfb2669c2d1de497f02baf7b4adca
- c8e7b0d3b6afa22e801cacaf16b37355
- 955cb4f01eb18f0d259fcb962e36a339e8fe082963dfd9f72d3851210f7d2d3b

- 88f183304b99c897aacfa321d58e1840
- bc4c1c869a03045e0b594a258ec3801369b0dcabac193e90f0a684900e9a582d

Network

- hxxp[:]//ai.kostin.p-e[.]kr/index.php
- hxxp[:]//ar.kostin.p-e[.]kr/index.php
- hxxp[:]//ai.negapa.p-e[.]kr/index.php
- hxxp[:]//ol.negapa.p-e[.]kr/index.php
- hxxp[:]//ai.limsjo.p-e[.]kr/index.php
- hxxp[:]//qi.limsjo.p-e[.]kr/index.php
- hxxp[:]//coolsystem[.]co.kr/admin/mail/index.php
- ai.kostin.p-e[.]kr
- ar.kostin.p-e[.]kr
- ai.negapa.p-e[.]kr
- ol.negapa.p-e[.]kr
- ai.limsjo.p-e[.]kr
- qi.limsjo.p-e[.]kr
- 216.189.159[.]197