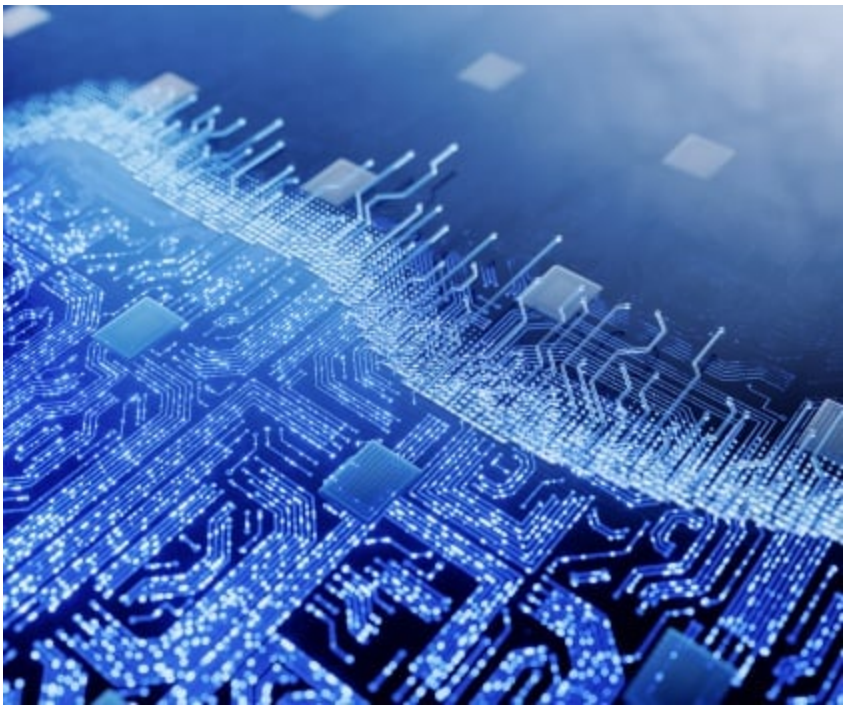
Springtail: New Linux Backdoor Added to Toolkit

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/springtail-kimsuky-backdoor-espionage



Threat Hunter TeamSymantec

Symantec's Threat Hunter Team has uncovered a new Linux backdoor developed by the North Korean Springtail espionage group (aka Kimsuky) that is linked to malware used in a recent campaign against organizations in South Korea.

The backdoor (Linux.Gomir) appears to be a Linux version of the GoBear backdoor, which was used in a recent Springtail campaign that saw the attackers deliver malware via Trojanized software installation packages. Gomir is structurally almost identical to GoBear, with extensive sharing of code between malware variants.

Background

Springtail is a tight-knit espionage group that initially specialized in attacks on public sector organizations in South Korea. The group first came to public attention in 2014, when the South Korean government said it was responsible for an attack on Korea Hydro and Nuclear Power (KHNP). Multiple employees at KHNP were targeted with spear-phishing emails containing exploits that installed disk-wiping malware on their machines. The U.S. government has said that the group is a unit of North Korea's military intelligence organization, the Reconnaissance General Bureau (RGB).

The group was the subject of a U.S. government alert in recent days due to attempts to exploit improperly configured DNS Domain-based Message Authentication, Reporting and Conformance (DMARC) record policies to conceal social engineering attempts. According to a joint advisory issued by the Federal Bureau of Investigation (FBI), the U.S. Department of State, and the National Security Agency (NSA), the group has been mounting spear phishing campaigns pretending to be journalists, academics, and experts in East Asian affairs "with credible links to North Korean policy circles".

Trojanized software packages

The campaign, which was first documented by South Korean security firm S2W in February 2024, saw Springtail deliver a new malware family named Troll Stealer using Trojanized software installation packages. Troll Stealer can steal a range of information from infected computers including files, screenshots, browser data, and system information. Written in Go, like many newer Springtail malware families, Troll Stealer contained a large amount of code overlap with earlier Springtail malware.

Troll Stealer's functionality included the ability to copy the GPKI (Government Public Key Infrastructure) folder on infected computers. GPKI is the public key infrastructure schema for South Korean government personnel and state organizations, suggesting that government agencies were among the targets of the campaign.

S2W reported that the malware was distributed inside installation packages for TrustPKI and NX_PRNMAN, software developed by SGA Solutions. The installation packages were reportedly downloaded from a page that was redirected from a specific website.

South Korean security firm AhnLab subsequently provided further details on the downloads, saying they originated from the website of an association in the construction sector. The website required users to log in and the affected packages were among those users had to install to do so.

Symantec has since discovered that Troll Stealer was also delivered in Trojanized Installation packages for Wizvera VeraPort. It is unclear how these installation packages were delivered during the current campaign. Wizvera VeraPort was previously reported to have been compromised in a North Korea-linked software supply chain attack in 2020.

Troll Stealer and GoBear

Troll Stealer appears to be related to another recently discovered Go-based backdoor named GoBear. Both threats are signed with a legitimate certificate issued to “D2innovation Co.,LTD”. GoBear also contains similar function names to an older Springtail backdoor known as BetaSeed, which was written in C++, suggesting that both threats have a common origin.

AhnLab later explicitly linked the two threats, saying that many of the malicious installers it had analyzed contained both Troll Stealer and either of the GoBear or BetaSeed backdoors, which it referred to as the Endoor malware family.

Several weeks later, GoBear was being distributed by a dropper masquerading as an installer for an app for a Korean transport organization. In this case, the attackers did not Trojanize a legitimate software package but instead disguised the dropper as an installer featuring the organization’s logos. The dropper was signed with what appeared to be a stolen certificate.

Gomir backdoor

Symantec’s investigation into the attacks uncovered a Linux version of this malware family (Linux.Gomir) which is structurally almost identical and shares an extensive amount of distinct code with the Windows Go-based backdoor GoBear. Any functionality from GoBear that is operating system-dependent is either missing or reimplemented in Gomir.

When executed, it checks its command line and if contains the string “install” as its only argument, it will attempt to install itself with persistence.

To determine how it installs itself, Gomir checks the effective group ID (as reported by the getegid32() syscall) of its own process. If the process is running as group 0, Gomir assumes that it is running with superuser privileges and attempts to copy itself as the following file:

```
/var/log/syslogd
```

It then attempts to create a systemd service with the name "syslogd" by creating the file:

```
/etc/systemd/system/syslogd.service
```

The file contains:

```
[Unit]

After=network.target

Description=syslogd
```

```
[Service]

ExecStart=/bin/sh -c "/var/log/syslogd"

Restart=always

[Install]

WantedBy=multi-user.target
```

Gomir will then enable and start the created service by executing the following sequence of commands:

```
${SHELL} -c systemctl daemon-reload

${SHELL} -c systemctl reenable syslogd

${SHELL} -c systemctl start syslogd
```

It will then delete the original executable and terminate the original process.

If the process is running as any group other than 0, Gomir attempts to configure a crontab to start the backdoor on every reboot. It first creates a helper file (cron.txt) in the current working directory with the following content:

```
@reboot [PATHNAME_OF_THE_EXECUTING_PROCESS]
```

Next, it seems to attempt to list any pre-existing crontab entries by running the following command:

```
/bin/sh -c crontab -l
```

It appends the output to the created helper file.

Gomir then updates the crontab configuration by executing the following command:

```
${SHELL} -c crontab cron.txt
```

Gomir then deletes the helper file before executing itself without any command-line parameters.

Once installed and running, Gomir periodically communicates with its command-and-control (C&C) server by sending HTTP POST requests to: http://216.189.159[.]34/mir/index.php

When pooling for commands to execute, Gomir requests with the following HTTP request body:

```
a[9_RANDOM_ALPHANUMERIC_CHARACTERS]=2&b[9_RANDOM_ALPHANUMERIC_CHARACTERS]=
[INFECTION_ID]1&c[9_RANDOM_ALPHANUMERIC_CHARACTERS]=
```

The INFECTION_ID is generated using the following method:

```
def generate_infection_id(hostname, username):

   hexdigest = hashlib.md5(hostname + username).hexdigest()

    return "g-" + hexdigest[:10]
```

The expected body of the HTTP server response is a string starting with the letter S. Gomir then attempts to decode the remaining characters of the string using the Base64 algorithm. The decoded blob has the following structure:

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.