

Log4j

# 威胁快讯：Log4j漏洞已经被用来组建botnet，针对Linux设备



RootKiter, Hui Wang, Genshen Ye

Dec 11, 2021 • 5 min read

年末曝光的Log4j漏洞无疑可以算是今年的安全界大事了。作为专注于蜜罐和botnet检测跟踪的团队，我们自该漏洞被公开后就一直关注它会被哪些botnet利用。今早我们等来了首批答案，我们的Anglerfish和Apacket蜜罐先后捕获到2波利用Log4j漏洞组建botnet的攻击，快速的样本分析表明它们分别用于组建 Muhstik 和Mirai botnet，针对的都是Linux设备。

## 样本分析

### MIRAI

这一波传播的为miria新变种，相比最初代码，它做了如下变动：

1. 移除了 table\_init/table\_lock\_val/table\_unlock\_val 等mirai特有的配置管理函数。
2. attack\_init 函数也被抛弃，ddos攻击函数会被指令处理函数直接调用。

同时，其C2域名选用了一个 uy 顶级域的域名，这在国内也是很少见的。

### Muhstik

Muhstik 这个网络最早被披露于 [2018](#) 年，系一个借鉴了Mirai代码的Tsunami变种。在本次捕获的样本中，我们注意到新Muhstik变种增加了一个后门模块ldm，它具有增加SSH后门公钥的能力，其安装的后门公钥为：

```
ssh-rsa AAAAB3NzaC1yc2EAAAQABtGZHLQ1MLkr0NMACHDVPZf+9gNG5s2rdTMBk0p6P7mKIQ/0kbq
```

该公钥被增加到`~/.ssh/authorized_keys`文件后，攻击者即可无需密码认证直接登陆远程服务器，实现对目标服务器的持续操控。

考虑到`log4j2`的漏洞机理比较特殊，“攻击者只需漫无目的的散播payload即会有机器被攻击，有点愿者上钩的意思。所以，攻击者很难直接判断被攻击的机器实际在哪里”，为确保后续可以使用这个后门，攻击者还要建立一个汇报机制，将受控机器的实际位置/用户名汇报到攻击者指定的服务器。Muhstik通过TOR网络完成该汇报任务，这可能会给溯源工作增加一层难度。

Muhstik在访问TOR网络前，会通过一些公开的DoH服务查询`relay.l33t-ppl.inf`的内容。在这个过程中，会产生一些与之相关的DNS请求。考虑到这些请求可能为判断失陷主机提供一些帮助。所以这里把相关域名列在下面。注意：这些域名不是CC域名，不是黑域名，而是正常的DoH服务。各运维相关读者需要根据自身业务情况酌情处理。

```
doh.defaultroutes.de  
dns.hostux.net  
dns.dns-over-https.com  
uncensored.lux1.dns.nixnet.xyz  
dns.rubyfish.cn dns.twnic.tw  
doh.centraleu.pi-dns.com  
doh.dns.sb doh-fi.blahdns.com  
fi.doh.dns.snopyta.org  
dns.flatuslifir.is  
doh.li  
dns.digitale-gesellschaft.ch
```

当无法直接从TOR网络汇报攻陷信息时，Muhstik还会通过TOR的公网映射域名进行提交，相关域名列表如下：

```
bvprzqhoz7j2ltin.onion.ws  
bvprzqhoz7j2ltin.onion.ly  
bvprzqhoz7j2ltin.tor2web.s
```

Muhstik的ELF样本则集成了如下命令：



其中log.exposedbotnets.ru便是C2，它刚好解析到37.44.244.124。作者注册一个log开头的域名也许是故意切合Log4j这个漏洞。

## 结论

鉴于Log4j的漏洞影响面比较大，我们预计后续会有更多的botnet使用它来传播。对此我们会持续保持关注，有新的观察会第一时间在这里公布。

## IOC:

**Mirai**

C2:

```
nazi.uy
```

URL:

```
http://62.210.130.250/lh.sh  
http://62.210.130.250:80/web/admin/x86_64  
http://62.210.130.250:80/web/admin/x86  
http://62.210.130.250:80/web/admin/x86_g
```

## Muhstik

C2:

```
log.exposedbotnets.ru
```

URL:

```
http://45.130.229.168:9999/Exploit.class  
http://18.228.7.109/.log/log  
http://18.228.7.109/.log/pty1;  
http://18.228.7.109/.log/pty2;  
http://18.228.7.109/.log/pty3;
```

http://18.228.7.109/.log/pty4;  
http://18.228.7.109/.log/pty5;  
http://210.141.105.67:80/wp-content/themes/twentythirteen/m8  
http://159.89.182.117/wp-content/themes/twentyseventeen/ldm

0 Comments

1 Login ▾

G

Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS [?](#)

Name



Share

Best [Newest](#) [Oldest](#)

Be the first to comment.

Subscribe

Privacy

Do Not Sell My Data

— 360 Netlab Blog - Network Security Research Lab at 360 —

Log4j



Day 10: where we are with log4j from honeypot's perspective

Botnet

**Threat Alert:  
Log4j  
Vulnerability Has  
Been adopted by  
two Linux Botnets**

公有云威胁情报

**公有云网络安全威  
胁情报  
(202111): 云上  
多个资源对外发起  
攻击**

## 从蜜罐视角看Apache Log4j2漏洞攻击趋势

已有10个家族的恶意样本利用Log4j2漏洞传播

[See all 3 posts →](#)

The Log4j vulnerability that came to light at the end of the year can undoubtedly be considered a major event in the security community. Honeypot and botnet are our bread and butter, and we have been concerned about which botnets would be exploiting this since the vulnerability was made public.



Dec 11, 4 min



2021 · read

1 概述 2021年11月，360网络安全研究院 Anglerfish蜜罐（以下简称“蜜罐系统”）共监测到全球53745个云服务器发起的网络会话9016万次，与10月份的数据相比略有下降，IP数量下降7.7%，会话数量下降2.1%。本月我们发现了涉及政府、事业单位、新闻媒体等多个行业的单位的8个云服务器IP地址在互联网上发起扫描和攻击。 2 云服务器攻击总体情况 11月22...

· Dec 9, 2021 · 14 min read