Botnet

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

RootKiter, Hui Wang, Genshen Ye

Dec 11, 2021 • 4 min read

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. This morning we got the first answers, our Anglerfish and Apacket honeypots have caught 2 waves of attacks using the Log4j vulnerability to form botnets, and a quick sample analysis showed that they were used to form Muhstik and Mirai botnets respectively, both targeting Linux devices.

Sample Analysis

MIRAI

This wave propagates a new variant of miria, which has made the following changes compared to the initial code.

1. table_init/table_lock_val/table_unlock_val and other mirai-specific configuration management functions have been removed.
2. The attack_init function is also discarded, and the ddos attack function is called directly by the command processing function.

Also, a uy top-level domain is chosen for its C2 domain name, which is also rare.

Muhstik

Muhstik, a botnet we disclosed in 2018, is a variant of Tsunami that borrows from the Mirai code. In this captured sample, we note that the new Muhstik variant adds a backdoor module, ldm, which has the ability to add an SSH backdoor public key with the following installed backdoor public key.

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQBtGZHLQlMLkrONMAChDVPZf+9gNG5s2rdTMBkOp6P7mKIQ/Okbg
```

After the public key is added to the ~/.ssh/authorized_keys file, the attacker can directly log into the remote server without password authentication.

Considering the special vulnerability mechanism of log4j2, Muhstik takes a blunt approach to spread the payload aimlessly knowing that there will be vulnerable machines, and in order to know who has been infected, Muhstik adopts TOR network for its reporting mechanism.

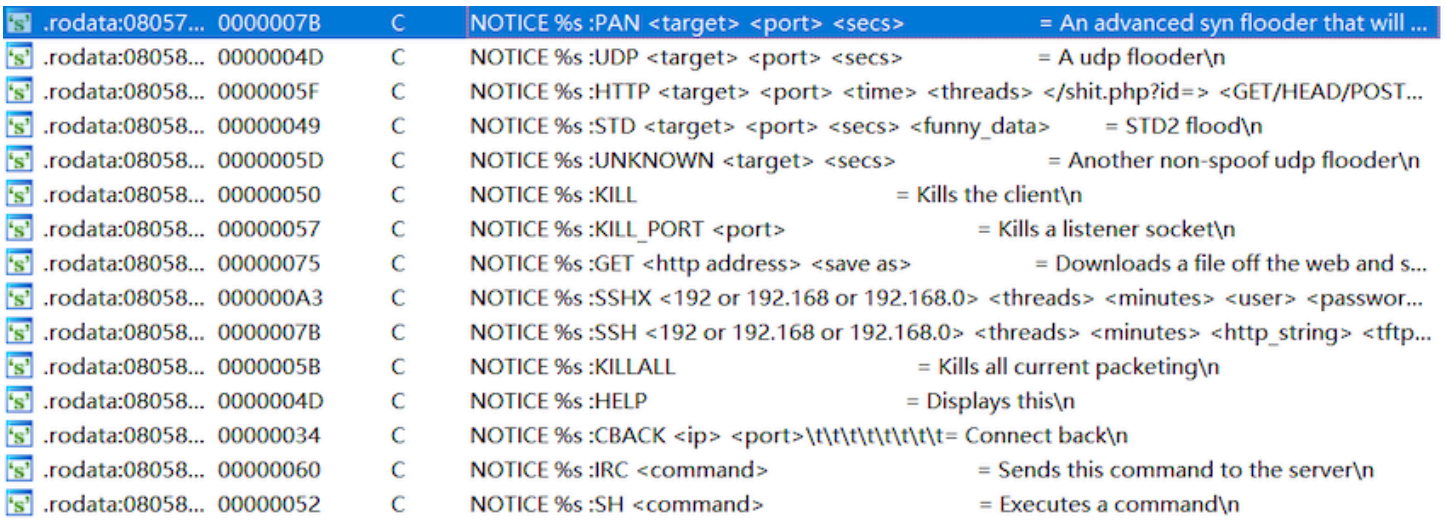
Before accessing the TOR network, Muhstik queries relay.l33t-ppl.inf through some publicly available DoH services(see the list beflow). During this process, a number of DNS requests are generated. Note: The following domains are not C2 domains but DoH service providers, depends on the situation, readers might be able to use the list to crosscheck their network for possible infections if they are not expect DoH usage on their network.

```
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
```

When it is not possible to report infect information directly from the TOR network, Muhstik will try to use TOR's public mapped domains, the list of relevant domains is as follows

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

Muhstik's ELF sample has the following codes.:



We can see that the sample supports DDoS and backdoor commands. The C2 of the sample is stored in a mirai-style configuration with the following configuration information in plain text.:

```
  [0x02]: "listening tun0\x00", size=15
  [0x03]: "irc.de-za"\x1f\x90"listening tun0\x00"l", size=30
  [0x04]: "\x1f\x90", size=2
  [0x05]: "log.exposedbotnets.ru\x00", size=22
  [0x06]: "log.exposedbotnets.ru\x00", size=22
  [0x07]: "log.exposedbotnets.ru\x00", size=22
  [0x08]: "log.exposedbotnets.ru\x00", size=22
  [0x0a]: "/proc/\x00", size=7
  [0x0c]: "/exe\x00", size=5
  [0x0d]: "/status\x00", size=8
  [0x0e]: "/fd\x00", size=4
  [0x0f]: "\x58\x4D\x4E\x4E\x43\x50\x46\x22\x00", size=33
  [0x10]: "zollard\x00", size=8
  [0x11]: "muhstik-11052018\x00", size=17
  [0x12]: "\x02^nL\x0b\x1a\x06_nL\x02\x0f\x00", size=13
  [0x13]: "eth1\x00", size=5
  [0x14]: "lan0\x00", size=5
  [0x15]: "-\x00", size=2
  [0x16]: "eth0\x00", size=5
```

```
[0x17]: "inet0\x00", size=6
[0x18]: "lano\x00", size=5
[0x19]: "log.exposedbotnets.ru\x00", size=22
[0x1a]: "log.exposedbotnets.ru\x00", size=22
[0x1b]: "d4cf8e4ab26f7fd15ef7df9f7937493d\x00", size=33
[0x1c]: "log.exposedbotnets.ru\x00", size=22
[0x1d]: "37.44.244.124\x00", size=14
[0x1e]: "37.44.244.124\x00", size=14
[0x1f]: "37.44.244.124\x00", size=14
[0x20]: "37.44.244.124\x00", size=14
[0x21]: "37.44.244.124\x00", size=14
[0x22]: "log.exposedbotnets.ru\x00", size=22
[0x23]: "log.exposedbotnets.ru\x00", size=22
```

The `log.exposedbotnets.ru` is C2, which resolves to `37.44.244.124`. The author registered a domain starting with log perhaps intentionally to fit the Log4j vulnerability.

Conclusion

Considering the huge impact of the Log4j vulnerability, we expect more botnets to support it to spread. We will keep an eye on this and will share new observations here.

Contact us

Readers are always welcomed to reach us on Twitter or email us to netlab at 360 dot cn.

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
```

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

Botnet

僵尸网络911 S5的数字遗产

Heads up! Xdr33, A Variant Of CIA's HIVE Attack Kit Emerges

警惕：魔改后的CIA攻击套件Hive进入黑灰产领域

Log4j

已有10个家族的恶意样本利用Log4j2漏洞传播

背景介绍 2021年12月11号8点整，我们率先捕获到Muhstik僵尸网络样本通过Log4j2 RCE漏洞传播，并首发披露Mirai和Muhstik僵尸网络在野利用详情[1]。 2天来，我们陆续又捕获到其它家族的样本，目前，这个家族列表已经超过10个，这里从漏洞、payload、攻击IP 和样本分析等几个维度介绍我们的捕获情况。 Apache Log4j2 漏洞攻击分布 360网络安全研...

Log4j

威胁快讯：Log4j漏洞已经被用来组建botnet，针对Linux设备

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...

See all 114 posts →

Dec 13, 2021 · 18 min read

Dec 11, 2021 · 5 min read