

关于新型 P2P 僵尸网络 PBot 的分析报告

本报告由国家互联网应急中心（CNCERT）与北京奇虎科技有限公司（360）共同发布。

一、概述

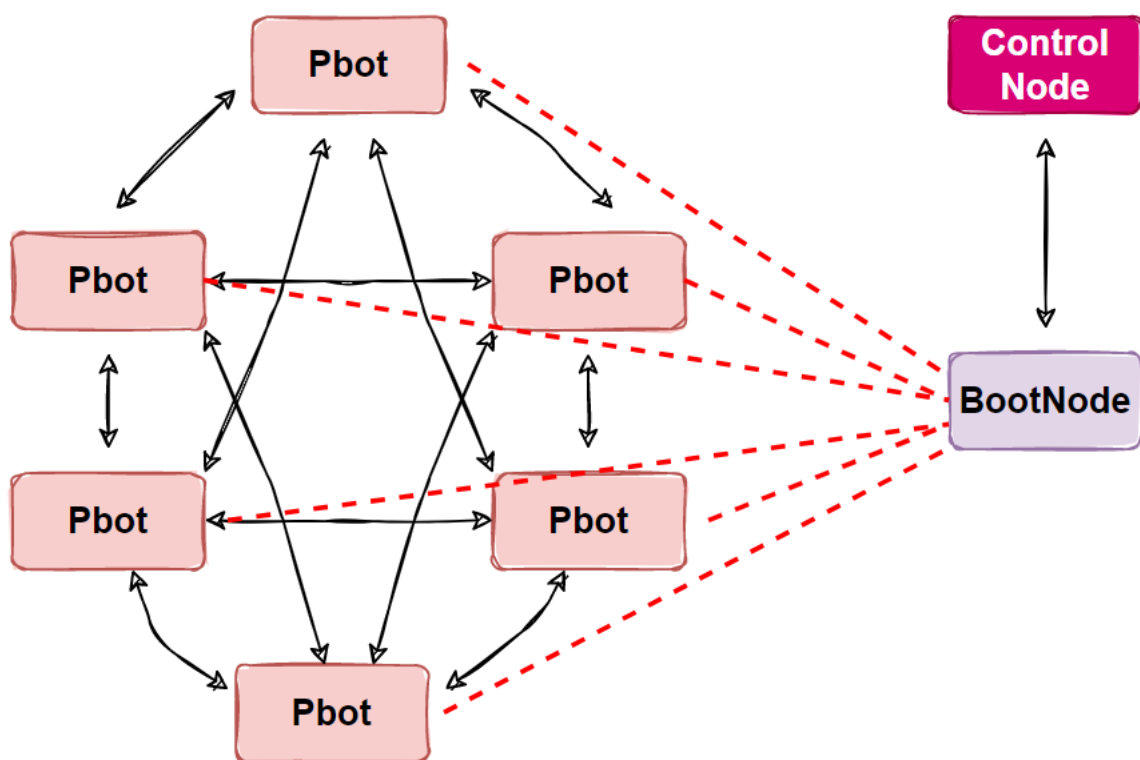
CNCERT 监测发现从 2020 年以来 P2P 僵尸网络异常活跃，如 Mozi、Pinkbot 等 P2P 僵尸网络家族在 2020 年均异常活跃，感染规模大、追溯源头难且难以治理，给网络空间带来较大威胁。

2021 年 5 月 31 日，CNCERT 和 360 捕获到一个全新的使用自定义 P2P 协议的僵尸网络，其主要功能为 DDoS。（当前很多杀毒引擎将其识别为 Mirai 或 Gafgyt 家族，我们将之命名 PBot）。

二、相关样本分析

（一）僵尸网络组织结构

Pbot 最独特的地方在于它实现了 P2P 网络通信，基于对 Bot 样本和控制端的逆向分析，它的简化网络结构如下所示：



事实上 Pbot 的功能比较简单，执行时首先会在 Console 输出 [main] bot deployed\r\n 字样，然后通过绑定本地端口实现单一实例，接着通过算法解密出 BootNode、身份认证 KEY 等敏感的资源信息，最后通过 BootNode 节点加入到 P2P 网络中，等待执行 ControlNode 下发的指令，主要有指令中 DDoS 攻击，开启 telnet 扫描传播等。其中支持的 DDoS 攻击方法如下所示：

f	attacks_vector_game_killer	.text	000081D0	000000A4
f	attacks_vector_nfo_v6	.text	00008274	00000144
f	attacks_vector_plainudp	.text	000083C4	000000A8
f	attacks_vector_plaintcp	.text	0000846C	000001D0
f	attacks_vector_l7_ghp	.text	0000863C	00000278
f	attacks_vector_ovh_l7	.text	000088DC	000000FC

(1) attacks_vector_game_killer: UDP DDoS 攻击，连续发送 768 个随机字符串；

(2) attacks_vector_nfo_v6: 使用特定 Payload 对 nfo 服务器发起 TCP DDoS 攻击；

(3) attacks_vector_plainudp: UDP DDoS 攻击, 连续发送 511 个随机字符串 UDP 包 500 次;

(4) attacks_vector_plaintcp: TCP DDoS 攻击, 连续发送 511 个随机字符串 TCP 包 2500 次;

(5) attacks_vector_l7_ghp: HTTP DDoS 攻击, 连续发送 HTTP 数据包 500 次。

(6) attacks_vector_ovh_l7: 使用特定 Payload 对 OVH 服务器发起 HTTP DDoS 攻击。

BootNode, 是一个超级节点, 除了与各 Bot 相同的 p2p 通信功能之外, 还具有以下功能:

(1) 统计各 Peer 信息 (Peer 会向它注册, 上传自身信息);

(2) 协助各 Peer 间寻找对方, BootNode 保存了大量的 P2P Peers 列表, Bot 向其注册后, 可以请求一部分节点信息分享给 Bot;

(3) 承载样本, 恶意 shell 脚本的下载服务。

而 ControlNode, 则是管理节点, 主要功能为向节点发送具体的指令, 如 DDoS 攻击, 开启扫描等。

(二) 传播方式

该家族样本主要通过 SSH/Telnet 弱口令以及一些 NDay 漏洞传播。相关 NDay 漏洞如下:

漏洞	影响设备
MVPower DVR Shell 未经身份验证的命令执行	MVPower DVR
ZTE 路由器 F460, F660 后门命令执行	ZTE Router
Netcore 路由器 UDP 端口 53413 后门	Netis Router

（三）感染规模

通过监测分析发现，该僵尸网络日均活跃 Bot 数在一千台以上。

```
[TELNET.WGET.ARM]: 189
[TELNET.TFTP.ARM]: 31
[EXPLOIT.GOAHEAD]: 763
[EXPLOIT.UCHTTTPD]: 134
[TELNET.TFTP.SH4]: 2
[10000]: 30
[TELNET.WGET.MIPS]: 1
[KORPZETEL.WGET.ARM7]: 1
[TELNET.ECHO.ARM]: 3
[LILB.0DAYS]: 1
[TELNET.TFTP.MIPS]: 1
[unknown]: 18
Bots: 1174
```

三、 相关 IOC

样本 MD5:

0e86f26659eb6a32a09e82e42ee5d720

3155dd24f5377de6f43ff06981a6bbf2

3255a45b2ebe187c429fd088508db6b0

3484b80b33ee8d53336090d91ad31a6b

769bc673d858b063265d331ed226464f

8de9de4e14117e3ce4dfa60dacd673ef

9cb73e83b48062432871539b3f625a21

d209fe7d62f517de8b1cf1a5697e67c2

e84a59bb18afff664e887744d8afebd0

下载链接:

<http://205.185.126.254/bins/controller.x86>

<http://205.185.126.254/bins/exxsdee.arm7>

<http://205.185.126.254/bins/exxsdee.i586>

<http://205.185.126.254/ssh.sh>

<http://205.185.126.254:80/bins/crsfi.arm>

<http://205.185.126.254:80/bins/exxsdee.arm>

http://205.185.126.254/korpze_jaws.sh

<http://205.185.126.254/korpze.sh>

<http://205.185.126.254/sv.sh>

http://205.185.126.254/korpze_jaws.sh

<http://205.185.126.254///exxsdee.mpsl>

<http://monke.tw/armz.sh>

<http://monke.tw/u>