国家互联网应急中心

cert.org.cn/publish/main/11/2021/20210628133948926376206/20210628133948926376206_.html

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

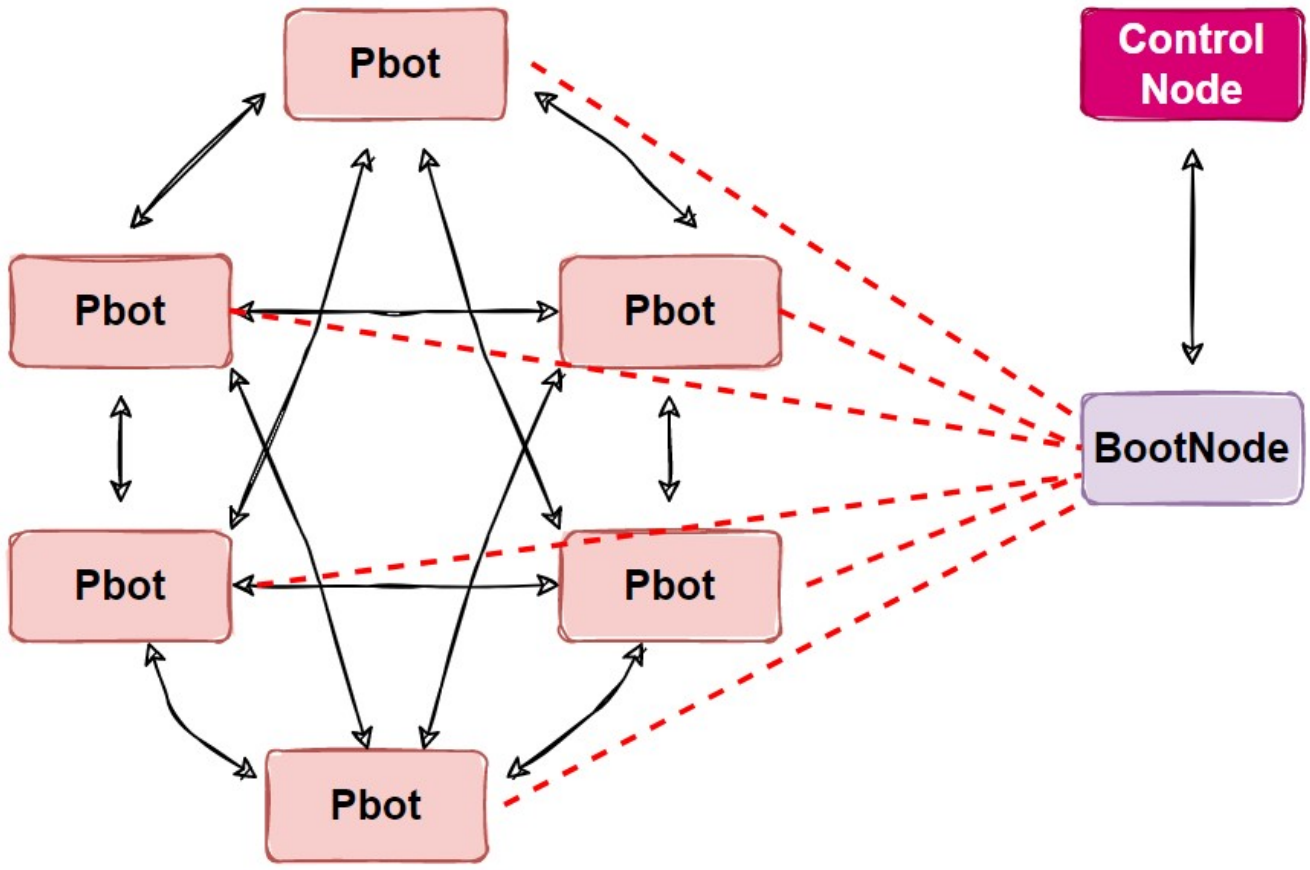
CNCERT监测发现从2020年以来P2P僵尸网络异常活跃，如Mozi、Pinkbot等P2P僵尸网络家族在2020年均异常活跃，感染规模大、追溯源头难且难以治理，给网络空间带来较大威胁。

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）。

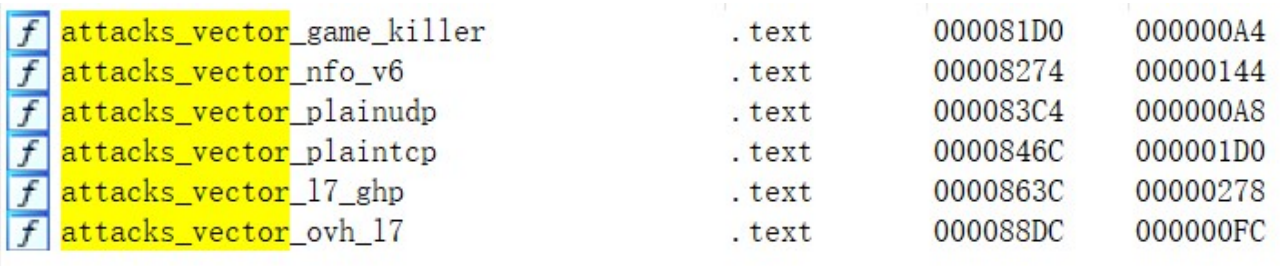
二、相关样本分析

（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 deployedrn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：



（1）attacks_vector_game_killer：UDP DDos攻击，连续发送768个随机字串；

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

（3）attacks_vector_plainudp：UDP DDos攻击，连续发送511个随机字串UDP包500次；

（4）attacks_vector_plaintcp：TCP DDoS攻击，连续发送511个随机字串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

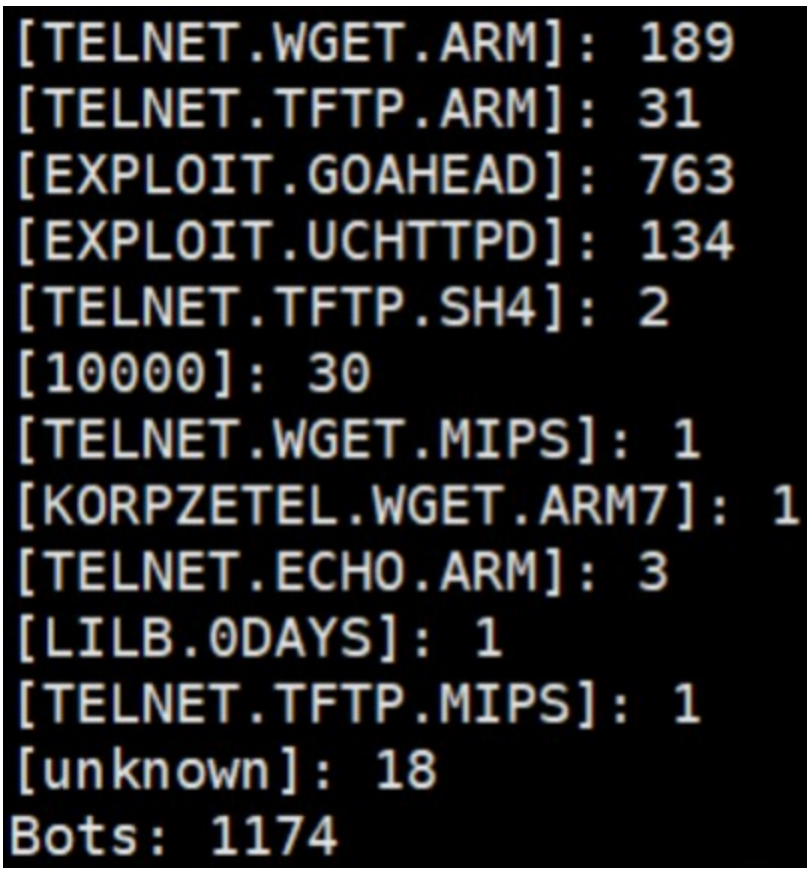
该家族样本主要通过SSH/Telnet弱口令以及一些NDay漏洞传播。相关NDay漏洞如下：

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。



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

附件：关于新型P2P僵尸网络PBot的分析报告