云时代DDoS溯源实践与解析

金山云高级安全产品经理梁洋洋

FIT · FREEBUF

About Me

网名：bt0sea 海啸

Freebuf特约作者

个人公众号：GSGSoft

个人微信号：lyyer2010

目前研究领域：抗D产品、 WAF、蜜罐、服务器安全、AI

#C++ #Python #vue.js

Symantec SE

青藤云安全产品经理

长亭科技产品经理

金山云安全高级产品经理

企业安全工坊

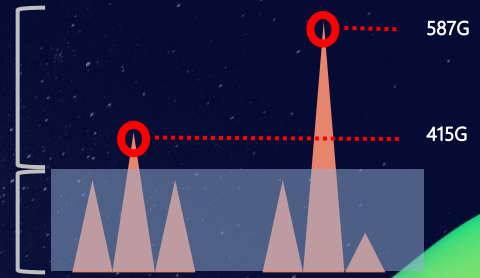
目录

CONTENTS

01 面对行业内恶意竞争，为高防用户提供攻击证据链技术支持，方便警方立案

02 购买高防服务期间，降低用户遭受DDoS攻击峰值，减少高防支出

03 公有云高防服务的辅助产品



目录

CONTENTS

DDoS溯源流程

DPI数据合作

攻击数据获取

4层攻击数据获取

7层攻击数据获取

攻击数据清洗

4层攻击源伪造处理

CC攻击特征分析

C&2外联获取

攻击样本获取

攻击源定向渗透

控制端溯源

逆向分析

C&C Server渗透

威胁情报溯源

身份溯源

团伙溯源

社交关系分析

行业竞争分析

商业攻击事件溯源报告

向警方提供攻击证据链

企业安全工坊

攻击数据获取

- 全流量溯源系统
- 7层CC防护日志

攻击数据清洗

- 回扫分析&IP信誉API
- 路由追踪系统
- 自动化分析脚本

攻击样本获取

- M3渗透测试小组

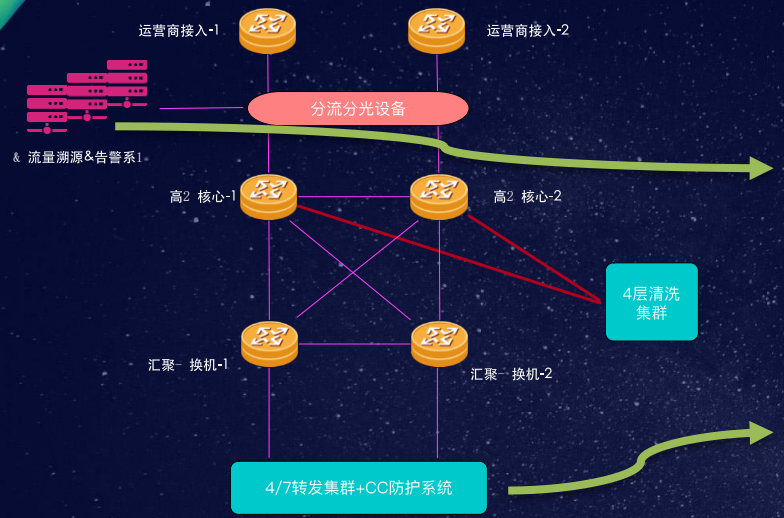
控制端溯源

- M3渗透测试小组
- 商业威胁情报溯源API

团伙溯源

- M3渗透测试小组
- 溯源分析平台&情报交换系统

攻击数据获取



- 全流量溯源系统
  - 攻击告警
    - 攻击类型 — SYN/TCP/UDP flood/CC 排除反射攻击
    - 攻击流量图 — 定位攻击时间段/攻击峰值
  - 攻击源IP统计
    - Top N 源IP — Top 100 by byte/pkg
    - 简单IP分析 — 地址位置/运营商
  - 自动化抓包系统 — 根据攻击告警自动抓/手工下发任务抓
- 7层CC防护日志
  - 攻击源IP统计
    - Top N 源IP — Top 1000 by QPS
    - 简单IP分析 — 地址位置/运营商
  - 攻击告警 — 连接数告警/https flood告警

攻击数据清洗

4层攻击伪造IP处理

URPF协议
同段伪造

路由追踪
系统

全国500+CDN节点 netbench MTR
数据汇总-对定位出口机房定位

ASN关联分析

DPI数据合作

回扫分析
&IP信誉API

IP信誉API IP类型=IDC

IP信誉API IP类型!=
tor/vpn/proxy/lvs

攻击包个数>1000 or byte>100M

源IP回扫探活
服务指纹收集
通用漏洞收集
IP信誉确认

攻击源定向渗透

企业安全工坊


样本数据非实时
抓包数据非实时
结果不准确
IP
WWW
商业威胁情报溯源
清洗后攻击IP
IP关联的样本
C&C外联
域名溯源

M3溯源项目能力

- 渗透测试小组（国家队）
- 逆向分析小组
- 情报分析小组

法律问题

- 渗透IoT设备
- 周边资源分析
- 只下载攻击样本

合作方

- 公安部
- 公有云厂商
- 拥有安全数据资源专业公司

溯源平台&情报交换系统

溯源平台

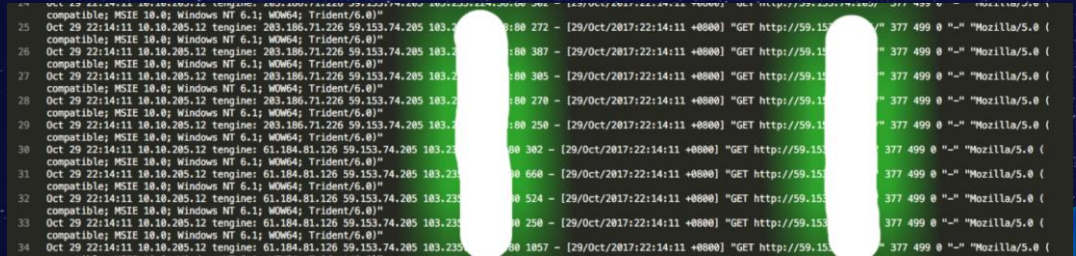
- 情报交换模块
  - 持久化购买&交换数据
  - 对外交换接口(脱敏)
  - 开源IP信誉数据对接
- 溯源分析展示
  - 多维关联展示
  - 商业溯源报告生成器
- 内部历史数据
  - 高防机房DDoS攻击数据
  - 公有云DDoS攻击数据
  - 蜜罐收集DDoS样本数据

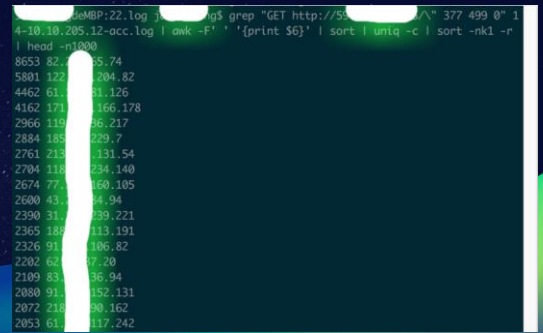
目录

CONTENTS

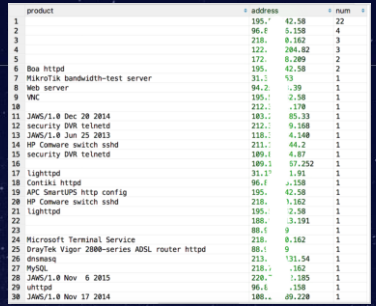
1、XXX用户在2017年10月29日 22:38，发现高防IP连接数 10万+，用户才3000多连接数，
攻击类型为CC攻击

2、获取转发系统上对应时间的访问日志&统计频率 Top1000





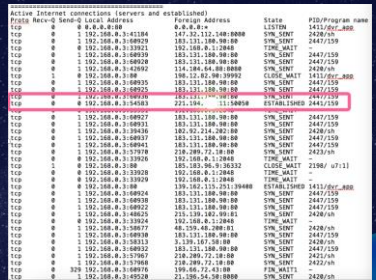
3、由于CC是建立session连接，略过伪造源检测步骤，
攻击源IP回扫，寻找服务特征：IoT设备。
通过DVR漏洞远程得到root访问权限。



	product	address	num
1		195.[42.58	22
2		96.[5.158	4
3		218. 0.162	3
4		122. 204.82	3
5		172. 0.209	2
6	Boa httpd	195. 42.58	2
7	MikroTik bandwidth-test server	31.[53	1
8	Web server	94.2[.39	1
9	VNC	195.[2.58	1
10		212.[.170	1
11	JAWS/1.0 Dec 20 2014	103.[85.33	1
12	security DVR telnetd	212.[9.168	1
13	JAWS/1.0 Jun 25 2013	118.[4.140	1
14	HP Comware switch sshd	211.[44.2	1
15	security DVR telnetd	109.[4.87	1
16		109.1 57.252	1
17	lighttpd	31.17[1.91	1
18	Contiki httpd	96.[.158	1
19	APC SmartUPS http config	195. 42.58	1
20	HP Comware switch sshd	218.[9.162	1
21	lighttpd	195.[2.58	1
22		188.[3.191	1
23		80.[9	1
24	Microsoft Terminal Service	218. 0.162	1
25	DrayTek Vigor 2800-series ADSL router httpd	88.[9	1
26	dnsmasq	213.[131.54	1
27	MySQL	218.[.162	1
28	JAWS/1.0 Nov 6 2015	220.[1.185	1
29	uhttpd	96.[.158	1
30	JAWS/1.0 Nov 17 2014	180.[89.220	1

JAWS/1.0

4、查询网络连接状态(netstat)&获取攻击样本，
发现C&C服务器

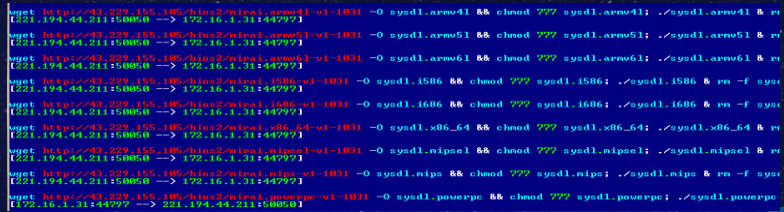


```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      1411/dvr_app
tcp        0      1 192.168.0.3:41184       147.32.112.140:8888     SYN_SENT    2428/sh
tcp        0      1 192.168.0.3:58920       183.131.188.90:80       SYN_SENT    2447/159
tcp        0      0 192.168.0.3:33921       183.131.188.90:80       TIME_WAIT   -
tcp        0      1 192.168.0.3:58930       183.131.188.90:80       SYN_SENT    2447/159
tcp        0      1 192.168.0.3:60928       183.131.188.90:80       SYN_SENT    2447/159
tcp        0      1 192.168.0.3:42692       114.104.64.80:8888      SYN_SENT    2428/sh
tcp        0      0 192.168.0.3:80          198.12.82.90:39992      CLOSE_WAIT  1411/dvr_app
tcp        0      1 192.168.0.3:58935       183.131.188.90:80       SYN_SENT    2447/159
tcp        0      1 192.168.0.3:60925       183.131.188.90:80       SYN_SENT    2447/159
tcp        0      1 192.168.0.3:58920       183.131.188.90:80       SYN_SENT    2447/159
tcp        0      0 192.168.0.3:54583       221.194.  11:58050      ESTABLISHED 2441/159
tcp        0      1 192.168.0.3:60927       183.131.188.90:80       SYN_SENT    2447/159
tcp        0      1 192.168.0.3:58931       183.131.188.90:80       SYN_SENT    2447/159
tcp        0      1 192.168.0.3:39436       182.92.214.202:80       SYN_SENT    2428/sh
tcp        0      1 192.168.0.3:58937       183.131.188.90:80       SYN_SENT    2447/159
tcp        0      1 192.168.0.3:60941       183.131.188.90:80       SYN_SENT    2447/159
tcp        0      1 192.168.0.3:57970       210.209.72.18:80        SYN_SENT    2423/sh
tcp        0      0 192.168.0.3:33926       192.168.0.1:2048        TIME_WAIT   -
tcp        1      0 192.168.0.3:80          185.183.96.9:36332      CLOSE_WAIT  2198/ u7:1]
tcp        0      0 192.168.0.3:33928       192.168.0.1:2048        TIME_WAIT   -
tcp        0      0 192.168.0.3:33929       192.168.0.1:2048        TIME_WAIT   -
tcp        0      0 192.168.0.3:80          139.162.115.251:39488   ESTABLISHED 1411/dvr_app
tcp        0      1 192.168.0.3:60924       183.131.188.90:80       SYN_SENT    2447/159
tcp        0      1 192.168.0.3:60938       183.131.188.90:80       SYN_SENT    2447/159
tcp        0      1 192.168.0.3:60922       183.131.188.90:80       SYN_SENT    2447/159
tcp        0      1 192.168.0.3:44025       213.139.182.99:81       SYN_SENT    2428/sh
tcp        0      0 192.168.0.3:33924       192.168.0.1:2048        TIME_WAIT   -
tcp        0      1 192.168.0.3:58077       46.159.48.200:81        SYN_SENT    2428/sh
tcp        0      1 192.168.0.3:60930       183.131.188.90:80       SYN_SENT    2447/159
tcp        0      1 192.168.0.3:58313       5.139.167.58:80         SYN_SENT    2428/sh
tcp        0      1 192.168.0.3:60932       183.131.188.90:80       SYN_SENT    2447/159
tcp        0      1 192.168.0.3:57967       210.209.72.18:80        SYN_SENT    2421/sh
tcp        0      1 192.168.0.3:57968       210.209.72.18:80        SYN_SENT    2422/sh
tcp        0    329 192.168.0.3:60976       199.66.72.41:80         FIN_WAIT1   -
tcp        0      1 192.168.0.3:49520       21.196.54.58:8080       SYN_SENT    2428/sh
```

159/sh

5、逆向分析 159样本

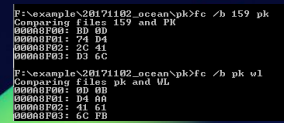
```
pthread_create(&InfoUpdate, 0, SendInfo, 0);
pthread_create(&back_doorA, 0, backdoorA, 0);
pthread_create(&back_doorM, 0, backdoorM, 0);
v7 = getlocalip();
memcpy(&rawip, v7, 20);
while ( 1 )
{
  _ConnectServer();
  puts("connnect server.");
  if ( pid && owner == 1 )
  {
    kill(pid, 9);
    StopFlag = 1;
    pid = 0;
  }
  usleep(5000000);
}
```



沙箱：SendInfo函数会向样本内置的3个cnc服务器报告当前设备的cpu利用率， 当前网速等信息

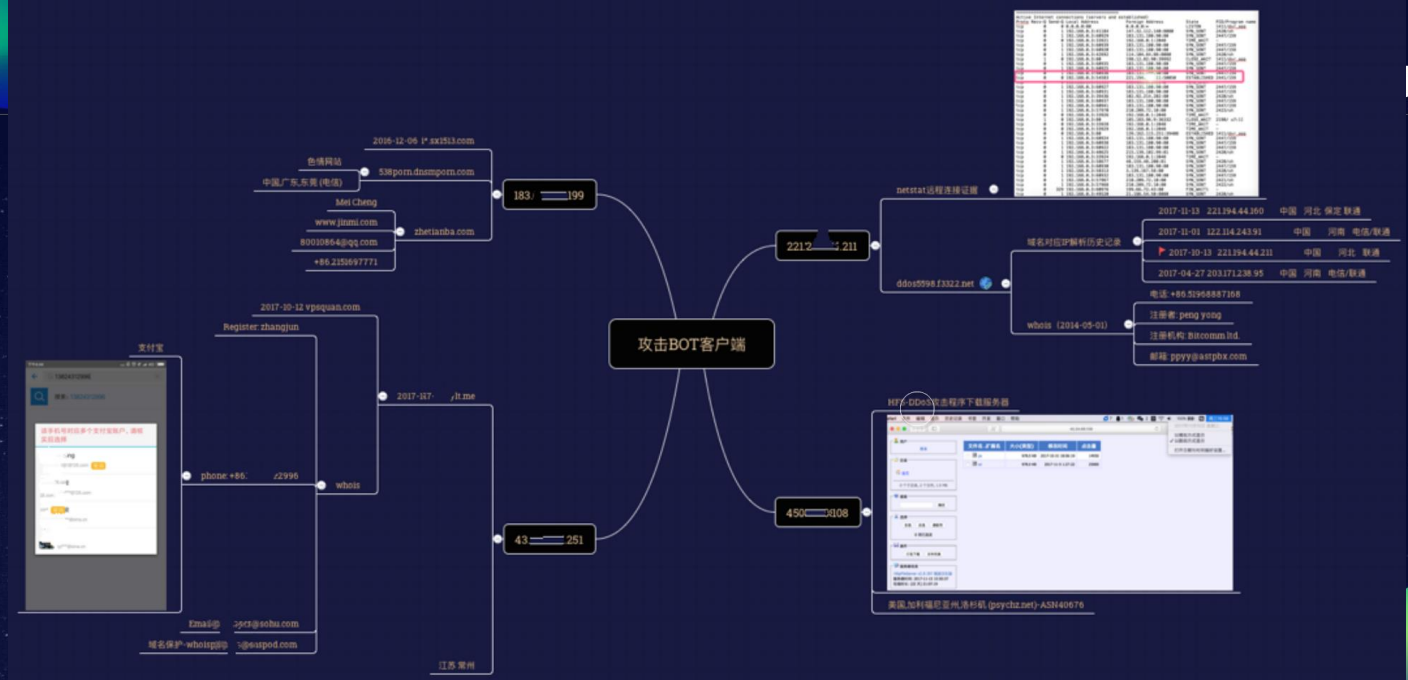
backdoorA，backdoorM，_ConnectServer开头有个很长时间的延时， 在15个小时之后， 尝试连接到内置的cnc服务器：
183.60.149.199:48080
bot作为一个样本分发器， 用来传播新的Mirai样本

221.194.44.211:50050
45.34.66.108:50050
43.248.97.251:50050

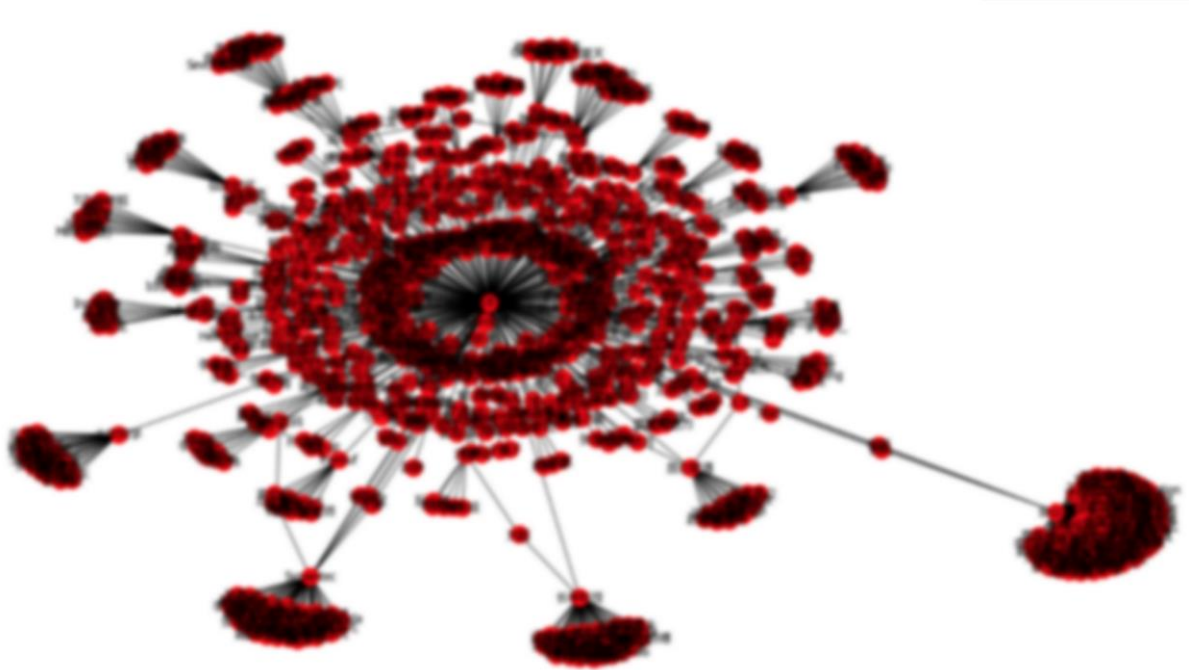


TCP_Flood, CC_Flood, CC2_Flood, CC3_Flood.

6、身份溯源


攻击BOT客户端
183.[redacted]199
2016-12-06 l*.sx1513.com
色情网站
538porn.dnsmporn.com
中国,广东,东莞 (电信)
Mei Cheng
www.jinmi.com
80010864@qq.com
zhetianba.com
+86.2151697771
43[redacted]251
2017-10-12 vpsquan.com
Register: zhangjun
支付宝
2017-11-[redacted]jt.me
phone:+86[redacted]2996
whois
Email@[redacted]qcn@sohu.com
域名保护-whoisp[redacted]@yeahpod.com
江苏 常州
221.2[redacted].211
netstat远程连接证据
ddos5598.f3322.net
域名对应IP解析历史记录
2017-11-13 221.194.44.160 中国 河北 保定 联通
2017-11-01 122.114.243.91 中国 河南 电信/联通
2017-10-13 221.194.44.211 中国 河北 联通
2017-04-27 203.171.238.95 中国 河南 电信/联通
whois (2014-05-01)
电话:+86.51968887168
注册者: peng yong
注册机构: Bitcomm ltd.
邮箱: ppyy@asrpbx.com
450[redacted]0108
HTTP DDos攻击程序下载服务器
美国,加利福尼亚州,洛杉矶 (psychz.net)-ASN40676

社会关系分析



FIT · FREEBUF

微信/itchat

QQ/QQbot

SINA/模拟登陆

。。。/。。。

企业安全工坊

目录

CONTENTS

金山云高防服务

【*】产品售卖方式的灵活性，总有一款属于你

- 【*】大带宽BGP全弹性
- 【*】BGP+静态单线
- 电信+联通+BGP
- 电信+联通+移动
- 【*】灵活升降配

高防资源覆盖率高（5T）

- BGP线路
  - 北方山东
  - 南方福建
- 单线静态
  - 福建电信/山东电信
  - 山东联通/河北联通
  - 江苏移动 /山东移动

金山云高防服务3.0

高防3.0业务需求

提供基于分线路解析多机房调度的全新三线静态套餐

- 基于KDNS灵活的机房&用户高防IP清洗集群调度
- CDN&MobileSDK全国覆盖的线路质量监控系统
- 攻击峰值水位&超卖比业务调度

通过高可用设计提升高防产品SLA

- 高防业务系统冗余网络架构&机柜设备摆放2N设计 可用性 99.995%
- 清洗设备容量大于入向带宽容量25%
- 清洗中心国干直连，机房T3级别，可用性99.982%

提供高度自动化监控和自愈手段

- 业务异常检测（KADS、XGW、KTengine）
- 高防系统监控（清洗&检测设备监控、转发设备监控（转发服务器、API服务器））
- IDC监控（机柜掉电、运营商线路故障、高防交换设备异常、KDNS监控）