“魔鼬”木马 DDoS 事件分析

安天-安全研究与应急处理中心

报告初稿完成时间：2017 年 08 月 02 日 01 时 34 分

首次发布时间：2017 年 08 月 02 日 02 时 26 分

本版本更新时间：2017 年 08 月 02 日 16 时 30 分

目 录

©安天实验室 版权所有，欢迎无损转载

1 概述

2017 年 7 月 30 日，安天安全研究与应急处理中心（Antiy CERT）的工程师发现一种具备拒绝服务（DDoS）攻击能力的新型木马。经初步分析，安天 CERT 工程师认为该木马属于一个新家族，并将其命名为“魔鼬”。通过关联查询安天对于 DDoS 攻击的历史监测数据，发现本次事件中受攻击的域名同时也在遭受 Trojan/Linux.BillGates、Trojan/Linux.Mayday 等家族的 DDoS 攻击。

2 受攻击目标

通过样本分析，发现被攻击域名或 IP 多为操作系统下载站点，受攻击的域名/IP 和对应的网站名如表 2-1 所示。

表 2-1 受攻击的域名/IP 对应的网站

域名/IP	网站名
win7.bdxsa.com	系统之家
www.swerrt.cn	系统之家
x1.xy1758.com	
www.xiaomaxitong.cn	小马一键重装系统
win7.hangzhouhongcaib.cn	
win.geelai.cn	系统下载
xz.xamy119.com	小猪一键重装系统
xm.0537yiyao.com	小马一键重装系统
blog.xy1758.com	
win7.yahung5.com	系统之家
win7.shangshai-qibao.cn	系统下载
183.134.16.11	
43.230.72.134	
14.152.83.24	

通过电信云堤的协助分析，我们在部分网络出口提取攻击数据，部分域名访问量抽样统计如下：

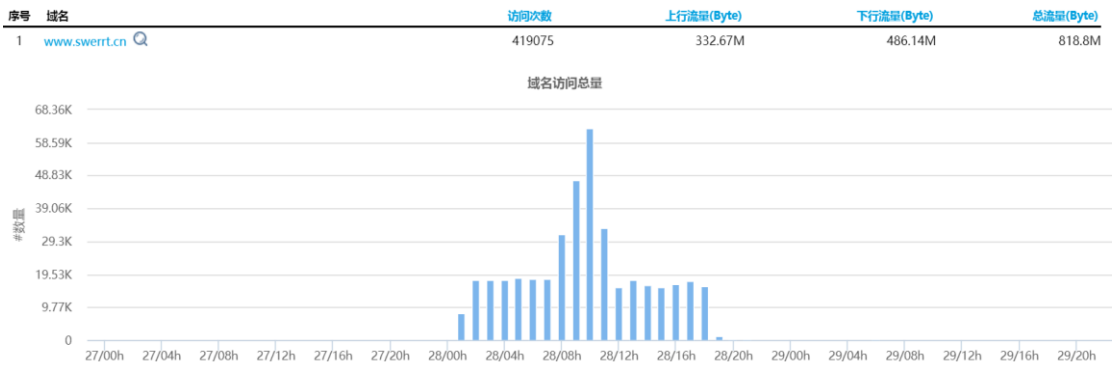


图 2-1 对 www.swerrt.cn 域名的访问量

©安天实验室 版权所有，欢迎无损转载

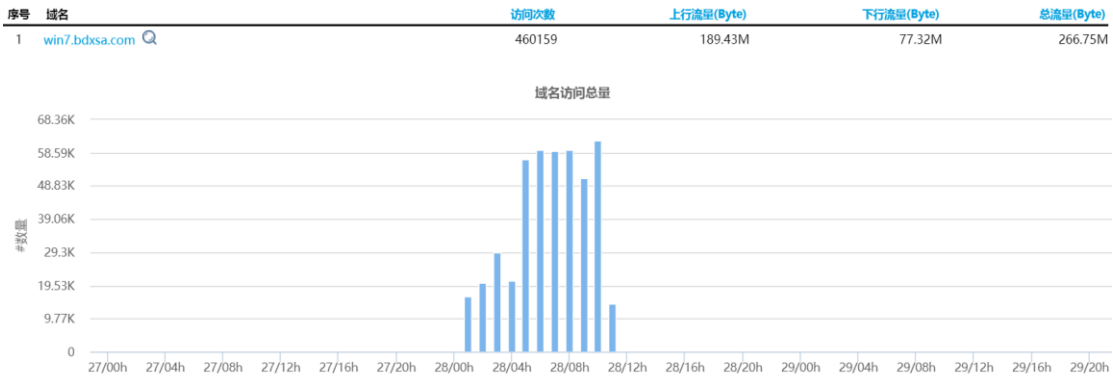


图 2-2 对 win7.bdxsa.com 域名的访问量

在运营商的大部分骨干网设备都可以观察到攻击流量和 C2 心跳，具体感染数量有待进一步核查。

3 事件样本分析

样本的编译时间为 2017-07-01 21:22:54（时间戳 5957A22E），根据前面的攻击事件发现时间，初步认为该时间是未经过篡改的，可见该木马家族出现时间仅有短短的 1 个月。

```
000000F8   50 45 00 00  ASCII "PE"      PE signature (PE)
000000FC   4C01         DW 014C         Machine = IMAGE_FILE_MACHINE_I386
000000FE   0400         DW 0004          NumberOfSections = 4
00000100   2EA25759     DD 5957A22E      TimeDateStamp = 5957A22E
00000104   00000000     DD 00000000      PointerToSymbolTable = 0
00000108   00000000     DD 00000000      NumberOfSymbols = 0
0000010C   E000         DW 00E0          SizeOfOptionalHeader = E0 (224.)
```

图 3-1 样本时间戳

样本的运行流程和主要行为如下：

1. 创建互斥量保证唯一实例运行。

```
call    sub_401130
push    offset a73b66e4c194a4a ; "{73B66E4C-194A-4af1-B541-BF3DC3FB3ED5}"
push    0               ; bInitialOwner
push    0               ; lpMutexAttributes
call    ds:CreateMutexA
mov     esi, eax
call    ds:GetLastError
test    esi, esi
jz      short loc_4011F4
cmp     eax, 0B7h
jnz     short loc_4011F4
mov     ecx, [esp+58h+var_4]
pop     edi
pop     esi
pop     ebx
xor     ecx, esp
xor     eax, eax
call    @__security_check_cookie@4 ; __security_check_cookie(x)
mov     esp, ebp
```

图 3-2 创建互斥量

2. 加载资源数据，读取指定偏移的内容作为 C2 地址（www.linux288.com）。

©安天实验室 版权所有，欢迎无损转载

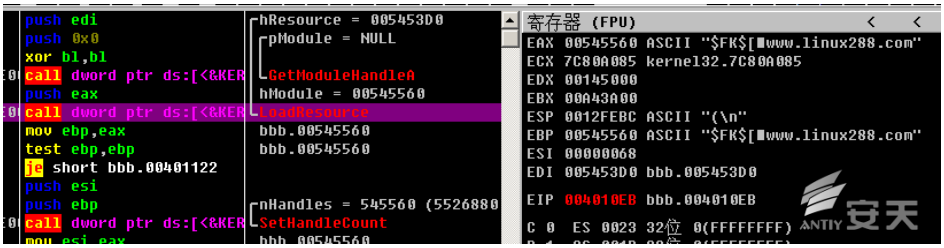


图 3-3 加载资源数据

3. 连接 C2 服务器，发送本机系统信息（包括主机名、CPU、内存、系统版本等），接收 C2 返回的攻击目标列表。

```
                        ; CODE XREF: sub_40D4B0+293Tj
mov     eax, [esi+18h]
lea     edx, [esp+948h+readfds]
push    edx             ; fd_set *
push    eax             ; fd
call    __WSAFDIsSet
test    eax, eax
jz      short loc_40D899
mov     edx, [esi+18h]
push    0               ; flags
push    800h            ; len
lea     ecx, [esp+950h+buf]
push    ecx             ; buf
push    edx             ; s
call    ds:recv         ; 接收远程服务器返回的数据（待攻击地址列表）
cmp     eax, 1
jl      short loc_40D8C5
mov     edx, [esi]
mov     edx, [edx+8]
push    eax
lea     eax, [esp+94Ch+buf]
push    eax
mov     ecx, esi
call    edx
```

图 3-4 接受服务器返回数据

4. 在分析中我们发现，C2 返回的攻击目标列表数据每隔一段时间会发生变化，从而控制受害主机向不同的 IP 或域名发动攻击。

图 3-5 服务器返回不同的攻击目标列表

5. 接收到数据后，样本按指定的格式解析攻击列表数据（link_list 和 task_list）。

©安天实验室 版权所有，欢迎无损转载

```
push    offset aTask_list ; "task_list"
lea     esi, [eax+4]
mov     [ecx+4], bl
call    sub_4015E0
mov     ecx, esi
call    sub_415310
add     esp, 1Ch
cmp     al, bl
jz      loc_40C665
push    9
push    offset aTask_list ; "task_list"
lea     ecx, [esp+98h+var_4C]
mov     [esp+98h+var_34], edi
mov     [esp+98h+var_38], ebx
mov     byte ptr [esp+98h+var_48], bl
call    sub_4015E0
lea     ecx, [esp+90h+var_4C]
push    ecx
mov     ecx, esi
mov     byte ptr [esp+94h+var_4], 1
call    sub_40DAC0
mov     edx, [eax]
push    ebx
push    offset off_53FD80 ; int
push    offset off_53FD6C ; int
push    ebx             ; int
push    edx             ; int
call    sub_41A92A
```

图 3-6 解析数据包内容

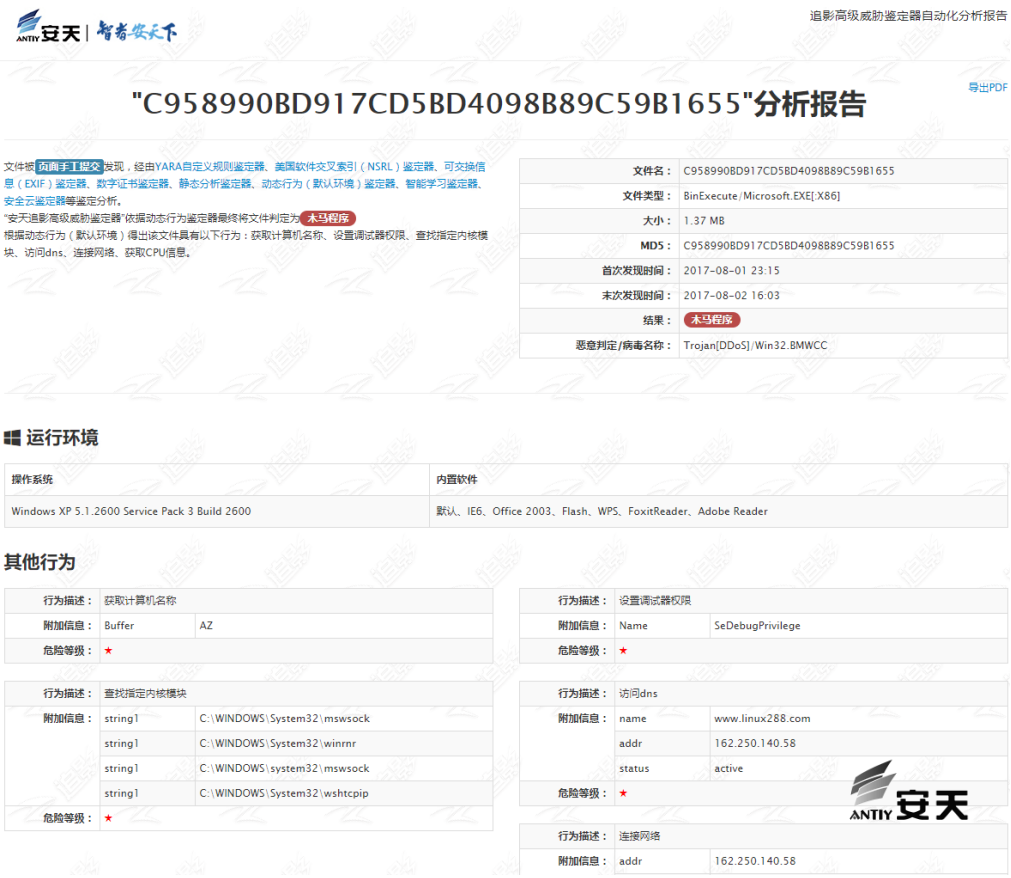
6. 样本根据 task_list 地址和配置，创建大量线程，向目标地址发起 DDoS 攻击。

```
call    ds:htons
mov     ecx, [edi+4]
mov     word ptr [esp+5Ch+name.sa_data], ax
push    10h             ; namelen
lea     eax, [esp+60h+name]
push    eax             ; name
push    ecx             ; s
mov     dword ptr [esp+68h+name.sa_data+2], esi
call    ds:connect      ; DDoS
mov     ecx, [esp+5Ch+var_8]
pop     esi
neg     eax
pop     ebp
sbb     eax, eax
pop     ebx
xor     ecx, esp
call    @__security_check_cookie@4 ; __security_check_cookie(x)
add     esp, 50h
retn
```

图 3-7 发起 DDoS 攻击

7. 在分析样本的同时，我们人工提交至安天追影高级威胁检测系统，系统通过智能动态行鉴定器检测出样本主要的恶意行为和网络请求并判定为木马程序，检出报告如下图：

©安天实验室 版权所有，欢迎无损转载


追影高级威胁鉴定器自动化分析报告

"C958990BD917CD5BD4098B89C59B1655"分析报告

导出PDF

文件被 页面手工提交 发现，经由YARA自定义规则鉴定器、美国软件交叉索引（NSRL）鉴定器、可交换信息（EXIF）鉴定器、数字证书鉴定器、静态分析鉴定器、动态行为（默认环境）鉴定器、智能学习鉴定器、安全云鉴定器等鉴定分析。
"安天追影高级威胁鉴定器"依据动态行为鉴定器最终将文件判定为 木马程序
根据动态行为（默认环境）得出该文件具有以下行为：获取计算机名称、设置调试器权限、查找指定内核模块、访问dns、连接网络、获取CPU信息。

文件名：	C958990BD917CD5BD4098889C59B1655
文件类型：	BinExecute/Microsoft.EXE[:X86]
大小：	1.37 MB
MD5：	C958990BD917CD5BD4098889C59B1655
首次发现时间：	2017-08-01 23:15
末次发现时间：	2017-08-02 16:03
结果：	木马程序
恶意判定/病毒名称：	Trojan[DDoS]/Win32.BMWCC

运行环境

操作系统	内置软件
Windows XP 5.1.2600 Service Pack 3 Build 2600	默认、IE6、Office 2003、Flash、WPS、FoxitReader、Adobe Reader

其他行为

行为描述：	获取计算机名称	
附加信息：	Buffer	AZ
危险等级：	★	

行为描述：	设置调试器权限	
附加信息：	Name	SeDebugPrivilege
危险等级：	★	

行为描述：	查找指定内核模块	
附加信息：	string1	C:\WINDOWS\System32\mswsock
	string1	C:\WINDOWS\System32\winrnr
	string1	C:\WINDOWS\system32\mswsock
	string1	C:\WINDOWS\System32\wshtcpip
危险等级：	★	

行为描述：	访问dns	
附加信息：	name	www.linux288.com
	addr	162.250.140.58
	status	active
危险等级：	★	

行为描述：	连接网络	
附加信息：	addr	162.250.140.58

图 3-8 安天追影高级威胁检测系统分析报告

4 相关事件关联

对本次事件中的被攻击域名进行关联查询，发现部分域名在相近时间也遭受了其他组织的 DDoS 攻击，详细信息如下：

表 4-1 关联查询结果

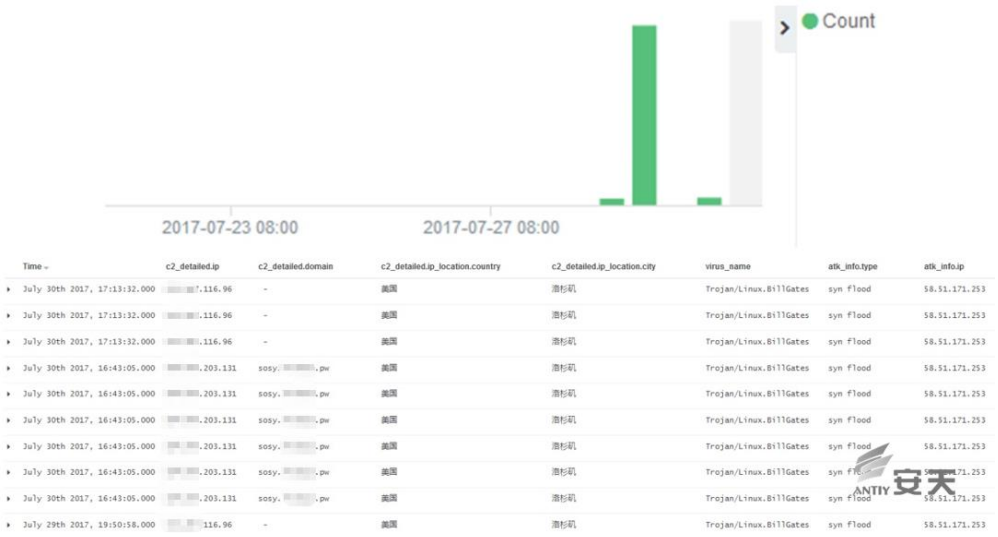
受害者	攻击开始时间	攻击结束时间	攻击者	攻击者地域	攻击类型	攻击次数	攻击家族
www.swerrt.cn、win7.bdxsa.com、win7.hangzhouhongcaib.cn 对应 122.228.91.13	2017 年 7 月 14 日	2017 年 7 月 31 日	*.*.77.34、*.*.203.131、*.*.116.96、sosy.*.pw、	美国洛杉矶	syn flood	8226	Trojan/Linux.BillGates
win7.hangzhouhongcaib.cn 对应 58.51.171.253	2017 年 7 月 29 日	2017 年 7 月 30 日	*.*.203.131、*.*.116.96、sosy.*.pw、network.*.net	美国洛杉矶	syn flood	212	Trojan/Linux.BillGates

©安天实验室 版权所有，欢迎无损转载

www.xiaomaxitong.cn 对应 104.31.184.2、104.31.185.2	2017 年 7 月 26 日	2017 年 7 月 29 日	*.*.203.131 *.*.116.96、sosy.*.pw、network.*.net	美国洛杉矶	syn flood	320	Trojan/Linux.BillGates
x1.xy1758.com 对应 58.222.43.221、122.228.91.14	2017 年 7 月 29 日	2017 年 7 月 31 日	*.*.203.131、*.*.116.96、sosy.*.pw、network.*.net	美国洛杉矶	syn flood	2525	Trojan/Linux.BillGates
xz.xamy119.com 对应 104.31.192.2、104.31.193.2	2017 年 7 月 26 日	2017 年 7 月 26 日	*.*.203.131、*.*.116.96、sosy.*.pw	美国洛杉矶	syn flood	314	Trojan/Linux.BillGates
xm.0537yiyao.com 对应 104.18.32.54、104.18.33.54	2017 年 7 月 19 日	2017 年 7 月 25 日	*.*.77.34、*.*.77.51、hadess520.*.net	美国洛杉矶	syn flood	31	Trojan/Linux.BillGates
blog.xy1758.com 对应 27.148.147.10、27.155.87.165	2017 年 3 月 11 日	2017 年 7 月 28 日	*.*.50.12、*.*.77.34、*.*.203.131、*.*.183.5、*.*.238.54、*.*.125.187、*.*.191.52、*.*.173.148、*.*.5.113、*.*.116.96、*.*.54.93、*.*.105.144、sosy.*.pw、hades2624.*.net、network.*.net	美国、中国	syn flood、tcp flood	2018	Trojan/Linux.BillGates、Trojan/Linux.Mayday

部分域名受攻击的数据如下所示：

©安天实验室 版权所有，欢迎无损转载



Time	c2_detailed.ip	c2_detailed.domain	c2_detailed.ip_location.country	c2_detailed.ip_location.city	virus_name	atk_info.type	atk_info.ip
July 30th 2017, 17:13:32.000	[redacted].116.96	-	美国	洛杉矶	Trojan/Linux.BillGates	syn flood	58.51.171.253
July 30th 2017, 17:13:32.000	[redacted].116.96	-	美国	洛杉矶	Trojan/Linux.BillGates	syn flood	58.51.171.253
July 30th 2017, 17:13:32.000	[redacted].116.96	-	美国	洛杉矶	Trojan/Linux.BillGates	syn flood	58.51.171.253
July 30th 2017, 16:43:05.000	[redacted].203.131	sosy.[redacted].pw	美国	洛杉矶	Trojan/Linux.BillGates	syn flood	58.51.171.253
July 30th 2017, 16:43:05.000	[redacted].203.131	sosy.[redacted].pw	美国	洛杉矶	Trojan/Linux.BillGates	syn flood	58.51.171.253
July 30th 2017, 16:43:05.000	[redacted].203.131	sosy.[redacted].pw	美国	洛杉矶	Trojan/Linux.BillGates	syn flood	58.51.171.253
July 30th 2017, 16:43:05.000	[redacted].203.131	sosy.[redacted].pw	美国	洛杉矶	Trojan/Linux.BillGates	syn flood	58.51.171.253
July 30th 2017, 16:43:05.000	[redacted].203.131	sosy.[redacted].pw	美国	洛杉矶	Trojan/Linux.BillGates	syn f[illegible]	5[illegible]71.253
July 30th 2017, 16:43:05.000	[redacted].203.131	sosy.[redacted].pw	美国	洛杉矶	Trojan/Linux.BillGates	syn flood	58.51.171.253
July 29th 2017, 19:50:58.000	[redacted]116.96	-	美国	洛杉矶	Trojan/Linux.BillGates	syn flood	58.51.171.253

ANTIY 安天

图 4-1 域名 win7.hangzhouhongcaib.cn 的攻击数据

Time	c2_detailed.ip	c2_detailed.domain	c2_detailed.ip_location.country	c2_detailed.ip_location.city	virus_name	atk_info.type	atk_info.ip
July 29th 2017, 10:09:20.000	[redacted].116.96	network[redacted].net	美国	洛杉矶	Trojan/Linux.BillGates	syn flood	104.31.184.2
July 29th 2017, 10:09:20.000	[redacted].116.96	-	美国	洛杉矶	Trojan/Linux.BillGates	syn flood	104.31.184.2
July 29th 2017, 10:09:20.000	[redacted].116.96	-	美国	洛杉矶	Trojan/Linux.BillGates	syn flood	104.31.184.2
July 29th 2017, 10:09:20.000	[redacted].116.96	network[redacted]net	美国	洛杉矶	Trojan/Linux.BillGates	syn flood	104.31.184.2
July 29th 2017, 10:09:20.000	[redacted].203.131	sosy[redacted].pw	美国	洛杉矶	Trojan/Linux.BillGates	syn [illegible]	104.31.184.2
July 29th 2017, 10:09:20.000	[redacted].116.96	-	美国	洛杉矶	Trojan/Linux.BillGates	syn flood	[illegible]1.184.2
July 29th 2017, 10:09:20.000	[redacted].116.96	-	美国	洛杉矶	Trojan/Linux.BillGates	syn flood	104.31.184.2

ANTIY 安天

图 4-2 域名 www.xiaomaxitong.cn 的攻击数据

Time	c2_detailed.ip	c2_detailed.domain	c2_detailed.ip_location.country	c2_detailed.ip_location.city	virus_name	atk_info.type	atk_info.ip
July 30th 2017, 18:07:27.000	[redacted]203.131	sosy.[redacted].pw	美国	洛杉矶	Trojan/Linux.BillGates	syn flood	58.222.43.221
July 30th 2017, 18:07:27.000	[redacted].203.131	sosy.[redacted].pw	美国	洛杉矶	Trojan/Linux.BillGates	syn flood	58.222.43.221
July 30th 2017, 18:07:27.000	[redacted].203.131	sosy[redacted].pw	美国	洛杉矶	Trojan/Linux.BillGates	syn flood	58.222.43.221
July 30th 2017, 18:06:49.000	[redacted]116.96	-	美国	洛杉矶	Trojan/Linux.BillGates	syn flood	58.222.43.221
July 30th 2017, 18:06:49.000	[redacted]116.96	-	美国	洛杉矶	Trojan/Linux.BillGates	syn flood	58.222.43.221
July 30th 2017, 18:06:49.000	[redacted]116.96	-	美国	洛杉矶	Trojan/Linux.BillGates	syn flood	58.222.43.221
July 30th 2017, 18:06:49.000	[redacted]116.96	-	美国	洛杉矶	Trojan/Linux.BillGates	syn flo[illegible]	58.222.43.221
July 30th 2017, 18:06:48.000	[redacted]203.131	sosy.[redacted].pw	美国	洛杉矶	Trojan/Linux.BillGates	syn flood	58[illegible]3.221
July 30th 2017, 18:06:48.000	[redacted].203.131	sosy.[redacted]pw	美国	洛杉矶	Trojan/Linux.BillGates	syn flood	58.222.43.221

ANTIY 安天

图 4-3 域名 x1.xy1758.com 的攻击数据

5 总结

经过分析和关联查询，发现在相近时间内多个组织对相同目标发起 DDoS 攻击。从目前掌握的资料来看，本次 DDoS 事件的攻击强度足以瘫痪一般的网站，但是部分受攻击网站采用了 CDN 服务，因此没有受到严重影响。该木马家族出现时间仅有短短的 1 个月，却发现较多起由该家族发起的 DDoS 攻击事件，说明木马传播速度较快，需要引起重视。

对于本次事件，安天建议用户尽快排查自身网络内是否有 C2 地址及被攻击目标地址的访问，并对可疑终端进行检测与排查，一旦发现有终端主机对上述地址有大量请求、连接极有可能已感染该木马程序。请您联系安天寻求专业帮助，400-840-9234。

安天再次提醒用户，安装能力型厂商提供的终端安全产品，推动积极防御、威胁情报与架构安全和被动防御的有效融合，建立攻击者难以预测的安全能力，达成有效防护和高度自动化和可操作化的安全业务价值。安全研究与应急处理中心（Antiy CERT）研究人员还在继续跟进，并将持续更新本分析报告。

特别鸣谢：黑龙江省委网信办、重庆市网信办、哈尔滨工业大学网络安全响应组、电信云堤

附录一：关于安天

安天是专注于威胁检测防御技术的领导厂商。安天以提升用户应对网络空间威胁的核心能力、改善用户对威胁的认知为企业使命，依托自主先进的威胁检测引擎等系列核心技术和专家团队，为用户提供端点防护、流量监测、深度分析、威胁情报和态势感知等相关产品、解决方案与服务。

安天的监控预警能力覆盖全国、产品与服务辐射多个国家。安天将大数据分析、安全可视化等方面的技术与产品体系有效结合，以海量样本自动化分析平台延展分析师团队作业能力、缩短产品响应周期。安天结合多年积累的海量安全威胁知识库，综合应用大数据分析、安全可视化等方面经验，推出了可抵御各类已知和未知威胁的多样化解决方案。

全球超过一百家以上的著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的威胁检测引擎目前已为全球近十万台网络设备和网络安全设备、超过八亿部移动终端设备提供安全防护，其中安天移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品，并在国际权威认证机构 AV-C 的 2015 年度移动安全产品测评中，成为全球唯一两次检出率均为 100%的产品。

安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续五届蝉联国家级网络安全应急服务支撑单位资质，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。

©安天实验室 版权所有，欢迎无损转载

安天是中国应急响应体系中重要的企业节点，在红色代码 II、口令蠕虫、震网、破壳、沙虫、方程式、白象、魔窟等重大安全事件中，安天提供了先发预警、深度分析或系统的解决方案。

安天实验室更多信息请访问： *http://www.antiy.com（中文）*

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： *http://www.antiy.cn*

安天移动安全公司（AVL TEAM）更多信息请访问： *http://www.avlsec.com*

©安天实验室 版权所有，欢迎无损转载