DDoS 攻击组织肉鸡美眉分析 V0.1

安天实验室 ShadowHunter Team

2015 年 1 月 13 日

文 档 信 息	
摘 要	本文主要针对一个跨平台 DDoS 攻击组织“肉鸡美眉”进行了分析，该组织所开发的 DDoS 工具利用 SSH 弱密码和服务器漏洞控制了众多 Linux 肉鸡，经验证，该组织的恶意代码可追溯到 2009 年。本文主要分析了该工具的控制端、生成器以及 Windows 和 Linux 被控端变种，并对这些样本进行了同源分析和网络感染疫情的展示。 **关键发现** ● 该组织活动至少可以追溯到 2009 年； ● 两名开发者昵称； ● 可能采用 SVN 协作方式开发； ● 字符串、调试信息、配置文件的同源分析； ● Windows 版本生成器和 Linux 版本生成器、控制器； ● 被控端 4 个 Windows 版本变种，5 个 Linux 版本变种。
版 权 说 明	

一、 概要

2014 年，安天实验室 ShadowHunter 团队分析发现了一个恶意代码，其创建的系统互斥量的名字为“Chicken_Mutex_MM”，故命名其为“肉鸡美眉”。该样本的主要功能是收集服务器基本信息并进行 DDoS 攻击。经过关联分析，我们发现其衍生变种还具有跨平台能力，主要包括 Windows 和 Linux 系统两个版本，而 Windows 版本样本最早在 2009 年 12 月就已出现。“肉鸡美眉”开发者采用了 SVN 协作开发，跨越 5 年持续演进，随着 Linux 服务器在国内不断增加且 Windows 系统受到诸多限制，从事 DDoS 的黑客也从 Windows 转向 Linux，被攻击的 Linux 服务器大幅增加。同时由于 Linux 服务器的带宽优势和长期在线的特点使 DDoS 攻击的威力更加增强。

该样本的某些变种在之前的报道中也有提及，但是大部分报道只介绍了其中的某个变种，并没有能够全面、深入地讲述该组织的来龙去脉，而本文则将为大家逐一揭晓。

1.1 组织运作概览

“肉鸡美眉”组织截至目前已经持续运作了超过 4 年的时间，主要进行 DDoS 工具的开发和销售。据判断，该组织至少有两名开发者，其中开发者“小陈”（昵称）应该是开发主力，在多个版本的变种中均有其昵称出现，而开发者“毛毛”（昵称）应该是副手。软件开发后通过搭建黑客论坛等方式进行地下传播，主要是销售给国内的私服技术维护人员，以及通过 DDoS 攻击进行敲诈的黑客，同时还有部分破解版本被传播出去。

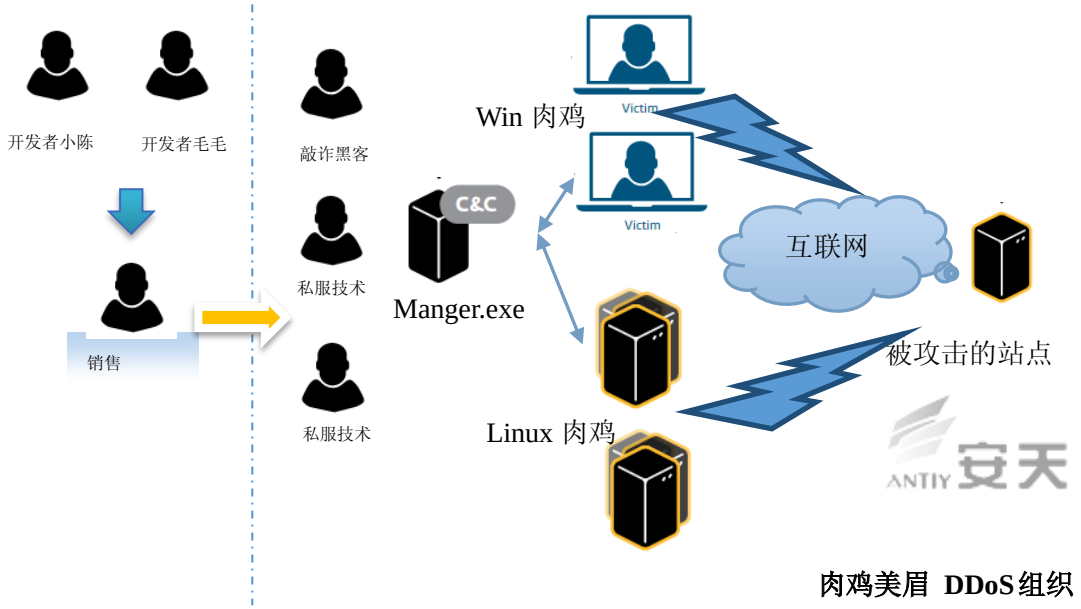

图 1 肉鸡美眉组织概览

1.2 肉鸡 MM 演化变种

目前安天实验室截获到的 Windows 变种主要有 4 类，分别为 Chicken、rjshell、svchost 和 IntergrateCHK，通过编译时间我们可以看到样本变种的时间演化关系（参见图 2）。从 2009 年 12 月开始出现 Windows 版本；2012 年 10 月和 2013 年 11 月的版本在传播上有两个高峰；2013 年 4 月开始出现 Linux 版本，并支持 32 位和 64 位；在 2013 年末开始较大范围攻击 Linux，其 Linux 版本变种主要以端口号区分，包括 10771、10991、36000、58000 以及 M4（参见图 3）。目前监测到的活跃被控端主要是 Linux 机器。

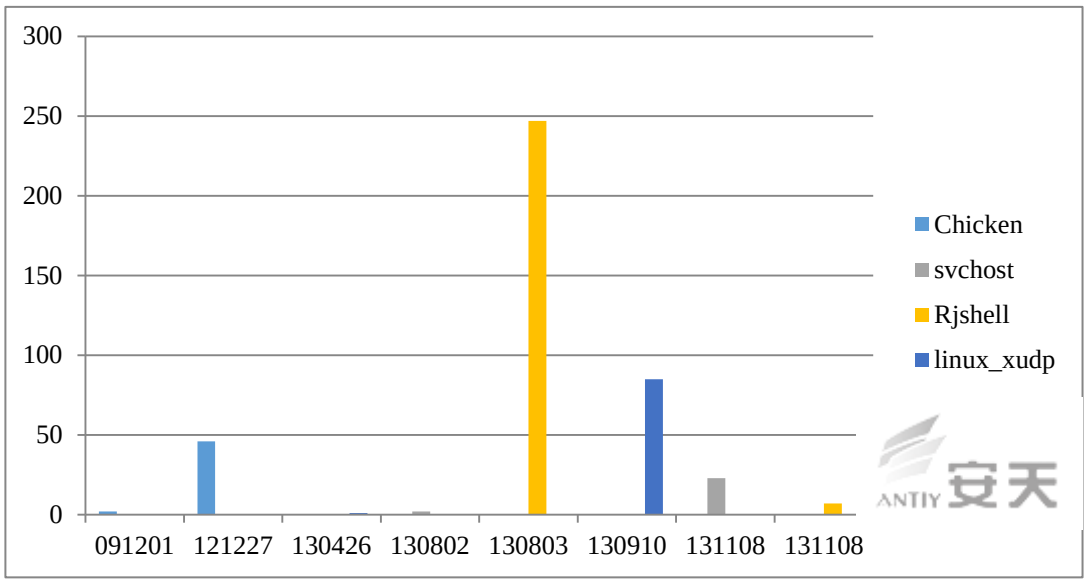

图 2 截获变种样本

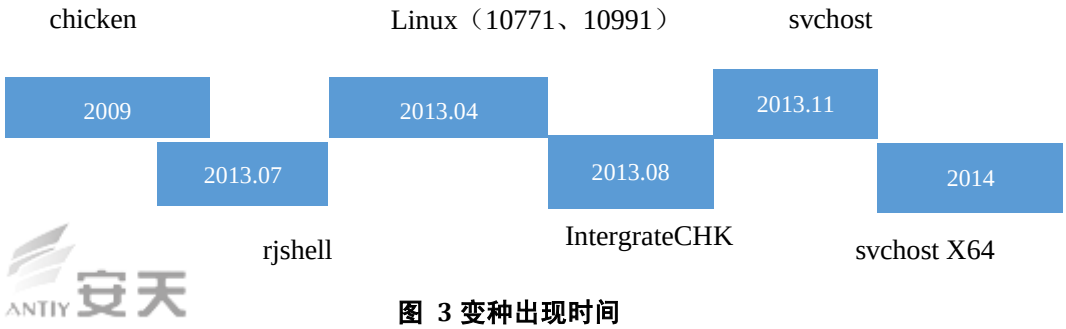

图 3 变种出现时间

二、 恶意代码分析

2.1 恶意代码组成

2.1.1 生成器

在样本库中检测到该生成器，由于该样本与众不同，通过其界面我们发现是 Windows 版生成器，生成器的编译时间是 2013 年 10 月 10 日 23 点 57 分 0 秒，默认生成的端口是 6009，生成的变种为 IntergrateCHK。

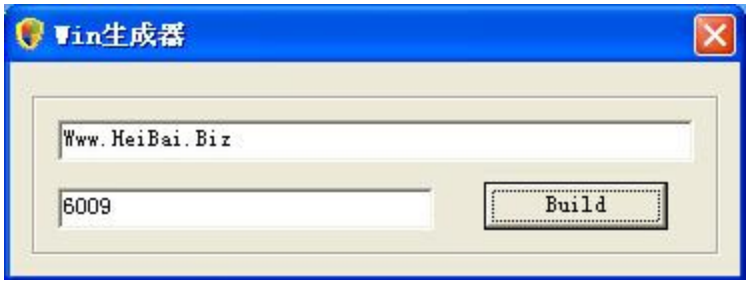

图 4 Windows 生成器

同样简洁的是 Linux 生成器，其中生成的 Linux 变种是 UDP 洪水 DDoS 攻击的变种 xudp，该变种出现在亚马逊 EC2 的服务器上，并出现在国内多个 Linux 系统上。

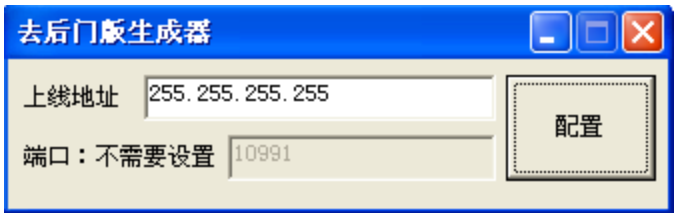

图 5 Xudp 版 10991 生成器错误!未找到引用源。

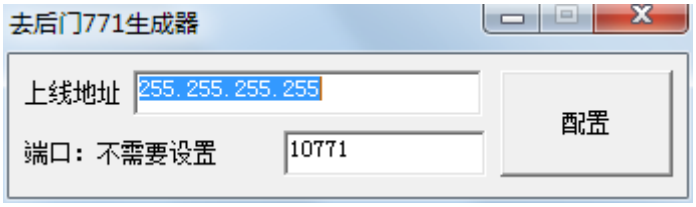

图 6 10771 生成器

图 7 M4 版生成器

2.1.2 控制端

通过控制端我们可以看到监控机器的列表，包含被控端的机器名、操作系统、CPU 和网络速度信息。具有半连接、SYN 洪水、UDP 洪水攻击功能，同时还具有批量伪造功能。

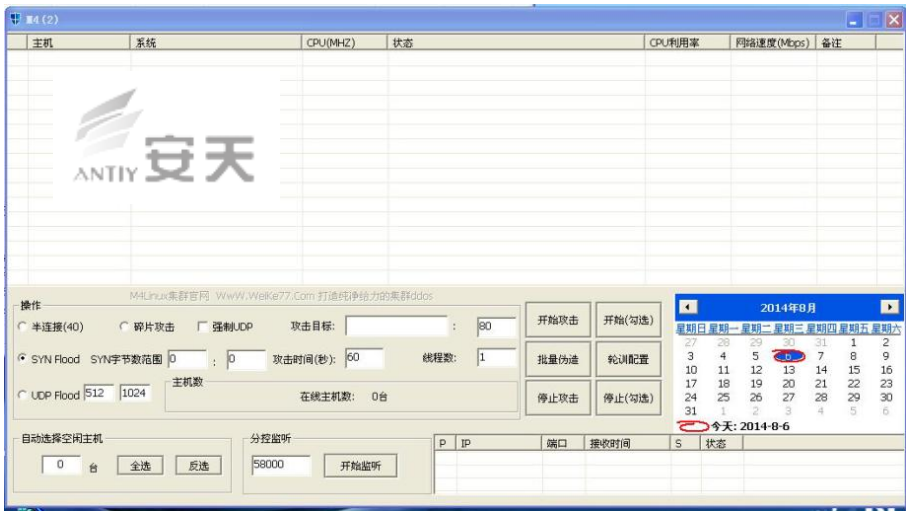

图 8 M4 控制端 Manger

2.1.3 被控端

- Chicken 变种

Windows 被控端 Chicken 变种经过自动分析运行后，它将创建 Chicken_mutex_mm 互斥量，释放 c:\mm.ini 配置文件，该文件主要用于保存伪造 IP 和端口的配置文件，获取 CPU 信息，并发起 DNS 请求，同时向控制端发送机器相关信息。

图 9 Chicken 变种自动分析

其字符串分析见表 1：

表 1 变种字符串

字符串	说明
Chicken_Mutex_MM	Chicken_mm 互斥量
\Chicken\Release\Chicken.pdb	PDB 信息
L:\SVN2\trunk\	PDB 路径
HARDWARE\DESCRIPTION\System\CentralProcessor\0 HARDWARE\DESCRIPTION\System\CentralProcessor\%d	获取 CPU 信息
\Processor(%d)\%% Processor Time PdhGetFormattedCounterValue	用于查询单个核心 CPU 使用率
JanFebMarAprMayJunJulAugSepOctNovDec SunMonTueWedThuFriSat	日期信息
Windows NT Windows 2000 Windows XP Windows Server 2003 Windows Vista Windows Server 2008 Windows 7 Windows Server 2008 R2 Windows 32s Windows Unknown	系统版本信息匹配

- **IntergrateCHK 变种**

Windows 被控端的 IntergrateCHK 变种运行后，会释放伪造端口 IP 的配置文件 fake.cfg，而 Chicken 变种释放的伪造配置文件是 mm.ini，而两者的内容格式是相同的。

第一行：0 是一个攻击标志位，0 表示停止，1 表示开始攻击；

第二行：192.168.50.132:192.168.50.132 是局域网伪造包的 IP 地址范围；

第三行：10000:60000 是伪造包端口范围；

图 10 fake.cfg 配置信息

图 11 IntergrateCHK 变种自动化分析

- **svchost x64 变种**

图 12 Windows 64 位 svchost 被控端变种分析

- **Linux 版本变种**

Linux 被控端使用 C++编写，具有提取信息上报，并接收指令等待攻击的功能，最新版还有 DNS 放大攻击的能力，部分 Linux 的被控端也会释放 fake.cfg 配置文件。Linux 变种被控端样本 22D0FA8571E1691CF2FFB1B20C1D536A 经过“安天追影自动化分析系统（http://zhuiying.antiy.cn/）”，发现其样本具有获取系统网卡、CPU、内存信息，释放 ELF 文件以及访问域名 zj.passwd1.com，反向连接等操作。

图 13 Linux 自动化分析

图 14 Linux 行为

域名解析

域名	ip
zj.passwd1.com	

进程监控

操作	进程名	ID	命令行
创建	/tmp/bulong-1420780825.52.elf		[/tmp/bulong-1420780825.52.elf]
创建	/bin/sh		[sh,-c,ln-s/etc/init.d/DbSecuritySpt...]
创建	/bin/ln		[ln,-s,/etc/init.d/DbSecuritySpt,/etc/rc1.d/S97DbSecuritySpt]
创建	/bin/ln		[ln,-s,/etc/init.d/DbSecuritySpt,/etc/rc2.d/S97DbSecuritySpt]
创建	/bin/ln		[ln,-s,/etc/init.d/DbSecuritySpt,/etc/rc3.d/S97DbSecuritySpt]
创建	/bin/ln		[ln,-s,/etc/init.d/DbSecuritySpt,/etc/rc4.d/S97DbSecuritySpt]

图 15 域名和进程操作

2.2 恶意代码同源分析

根据字符串、调试信息、配置文件、配置格式、路径等信息，我们可以找到变种样本之间的同源关系，通过这些信息可以将控制端、Windows 版本变种以及 Linux 版本变种关联起来，同时也可以把控制端 10771、10991、58000、M4 以及 Windows 版被控端、Linux 版被控端都关联起来。

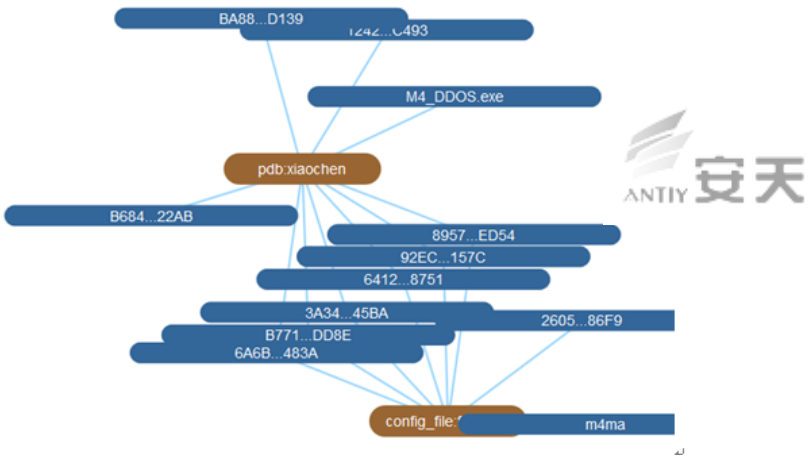

图 16 恶意代码同源分析关联图谱

2.3 开发者信息

通过样本中包含的调试信息中的路径“SVN\trunk”，我们可以推测出该 DDoS 工具的开发者是采用 SVN 进行共享代码编写的。同时在调试路径中有一些显示乱码，经分析发现是开发者的中文昵称“小陈”，“毛毛”，并且在中文昵称后面有“反向”，“被控”等中文，指明所开发的组件代码是反向连接被控端。

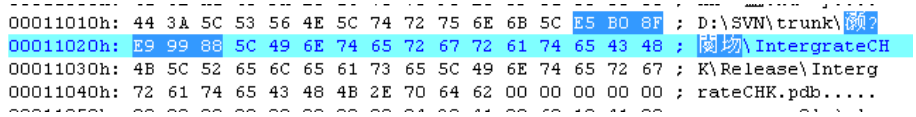

图 17 控制端包含 pdb

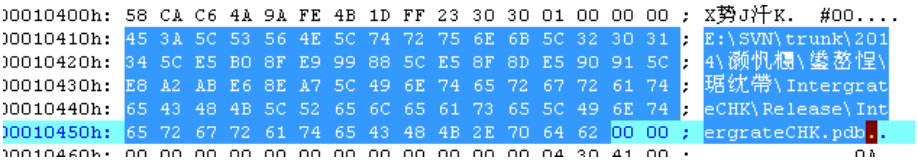

图 18 控制端包含 pdb

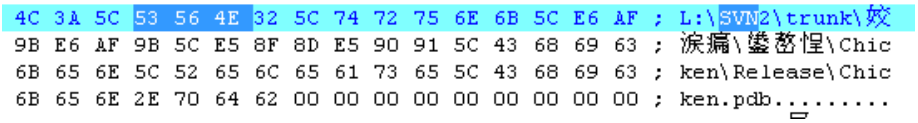

图 19 控制端包含 pdb

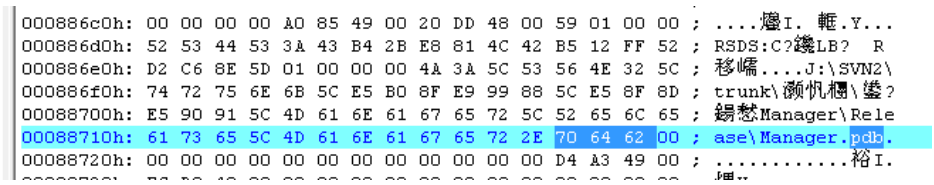

图 20 控制端包含 pdb

其中乱码部分采用的是 URL 编码，经过解码如下：

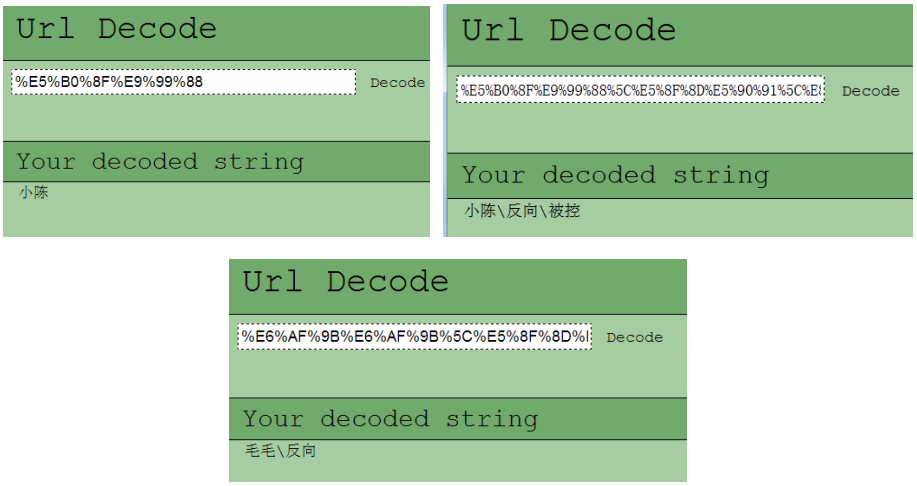

图 21 URL 编码解码信息

经判断，其主要利用搭建黑客论坛的方式销售攻击软件：

图 22 销售 QQ 截图

三、 网络控制和感染情况

攻击者使用的域名和控制 IP：

fymy.8800.org

kk.netbot.cc 70.39.77.126

yqv.3322.org 115.221.42.158

lindashuaiddos.f3322.org 222.186.52.153

192.161.177.203

98.126.193.143

61.153.104.230

198.148.92.100

111.cf22.com

syn.netbot.cc

DNS jj94.3322.org 42.51.4.216

ttlatale.3322.org

aaa.swhk.net

75.148my.com

199.36.72.222

四、 总结

随着Linux服务器的占比越来越高，DDoS攻击的肉鸡已经从Windows转向Linux系统，除了用于 Web 的 Linux 服务器外，包括智能摄像头、NVR 等 Linux 系统也逐渐成为攻击目标。

五、 参考资料

[1] New DDos Malware Targets Linux and Windows Systems

http://www.networkworld.com/article/2172819/smb/new-ddos-malware-targets-Linux-and-Windows-systems.html

[2] A quick look at a (new?) cross-platform DDoS botnet

http://www.cert.pl/news/7849/langswitch_lang/en

[3] versatile-ddos-trojan-for-Linux

https://securelist.com/analysis/publications/64361/versatile-ddos-trojan-for-Linux/

[4] Securelist – Information about Viruses, Hackers and Spam

https://securelist.com/blog/65192/elasticsearch-vuln-abuse-on-amazon-cloud-and-more-for-ddos-and-profit/

[5] V2EX 论坛：服务器被入侵，麻烦高手帮忙分析下

http://www.v2ex.com/t/121336

[6] 内部 OpenStack 云平台被黑

http://longgeek.com/2014/04/08/hacked-internal-openstack-cloud-platform/

[7] 从服务器登录互联网开始,就要注意安全

http://mo2g.com/view/81/

[8]

http://blog.malwaremustdie.org/2013/12/lets-be-more-serious-about-dns-amp-elf.html

[9] Another look at cross platform DDos

http://sempersecurus.blogspot.com/2013/12/another-look-at-cross-platform-ddos.html

[10] Linux.BackDoor.Gates.5 — yet another Linux Trojan

http://news.drweb.com/?i=5801&c=5&lng=en&p=0

[11] APPSTAR：Unix.Trojan.Elknot 病毒处理手记

http://bbs.appstar.com.cn/thread-10205-1-1.html

[12] Some tools to monitor BillGates CnC servers

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

[13] 百度贴吧：谁来帮忙看看是不是被黑了？

http://tieba.baidu.com/p/2817141932

[14] Linux 中 sfewfesfs 病毒删除记

http://blog.csdn.net/aaqqxx1910/article/details/41010279，2014.11.11

[15] V2EX 论坛：站点密码被暴力破解留下了操作记录，有几个命令不是太理解

http://www.v2ex.com/t/119848

附录一：

安天是专业的下一代安全检测引擎研发企业，安天的检测引擎为网络安全产品和移动设备提供病毒和各种恶意代码的检测能力，并被超过十家以上的著名安全厂商所采用，全球有数万台防火墙和数千万部手机的安全软件内置有安天的引擎。安天获得了 2013 年度 AV-TEST 年度移动设备最佳保护奖。依托引擎、沙箱和后台体系的能力，安天进一步为行业企业提供有自身特色的基于流量的反 APT 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）

关于安天反 APT 相关产品更多信息请访问：
http://www.antiy.cn

分享此报告二维码：