盗用数字签名 DDOS 样本分析

安天追影小组

报告初稿完成时间：2016 年 1 月 6 日

首次公开发布时间：2016 年 1 月 13 日

本版本更新时间：2016 年 1 月 13 日

目 录

1 概述

2016 年 1 月，安天追影小组通过安天态势感知系统发现了一款带有过期签名的 DDoS 恶意程序，该样本盗用了韩国 NHN 公司美国分公司的数字签名，NHN 旗下包括韩国本土最大的搜索引擎网站，美国分公司主要从事网络游戏开发，被盗用的数字签名已经过期，恶意代码添加过期的数字签名主要是为了躲避杀软检测。该数字签名被多个恶意样本使用，应该已经在地下市场流传。该 DDoS 样本包含多种 DDoS 攻击方式，并主要针对国内的在线销售减肥药、在线赌博、电子交易平台进行攻击。攻击者对灰色或非法网站进行 DDoS 攻击的目的可能是敲诈或者同业竞争。通过追影设备分析发现该病毒为 DDOS 恶意样本，病毒样本运行后释放 rasmedia.dll 到 system32 目录下，安装 WinHelp32 服务，运行 CMD 自删除。并创建两个线程分别防止服务自身被删除和进行 DDoS 攻击。攻击者使用 fabao.309420.com:7002 作为 C2 与 DDoS 病毒样本进行通信并分发攻击任务。短时间内已捕获到对多个网站被 DDoS 攻击。

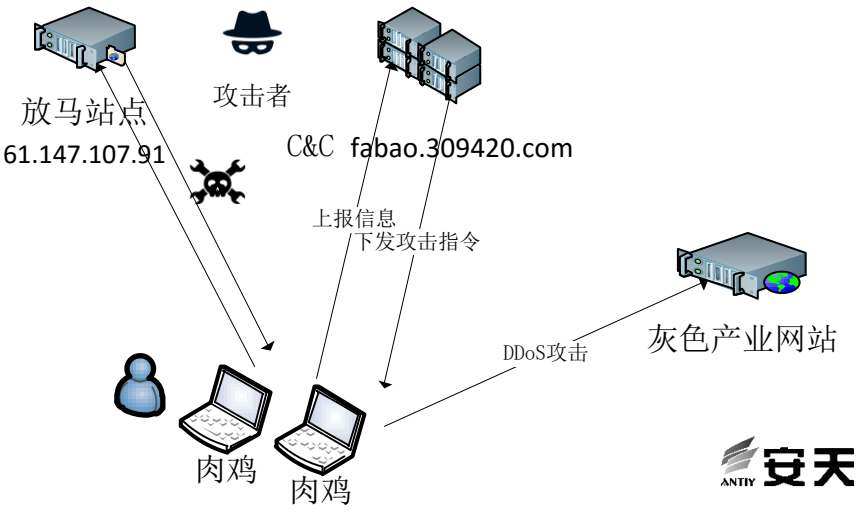


图 签名样本 DDoS 攻击

2 样本分析

2.1 样本标签

探海威胁检测系统检测都 hxxp://61.147.107.91:8082/get.exe 的恶意代码传输事件，经过分析该样本的基本信息如下：

病毒名称	Trojan[Backdoor]/Win32.DDOS
原始文件名	get.exe
MD5	b8f83b1e12ac61d8045a44561c5b7863
处理器架构	X86-32
文件大小	327.19 KB
文件格式	BinExecute/Microsoft.EXE[:X86]

时间戳	2015-10-28 14:07:22
数字签名	NO
加壳类型	无
编译语言	Compiler/Microsoft.VISUAL_C[:v6.0]
VT 首次上传时间	2015-12-06
VT 检测结果	47/55

2.2 样本运行流程

病毒样本运行后释放 rasmedia.dll 文件到 system32 目录下，安装 WinHelp32 服务，运行 CMD 自删除。服务程序反弹连接 fabao.309420.com:7002，上报受害者机器信息，并创建两个线程分别防止服务自身被删除和等待服务器攻击指令，进行 DDoS 攻击。

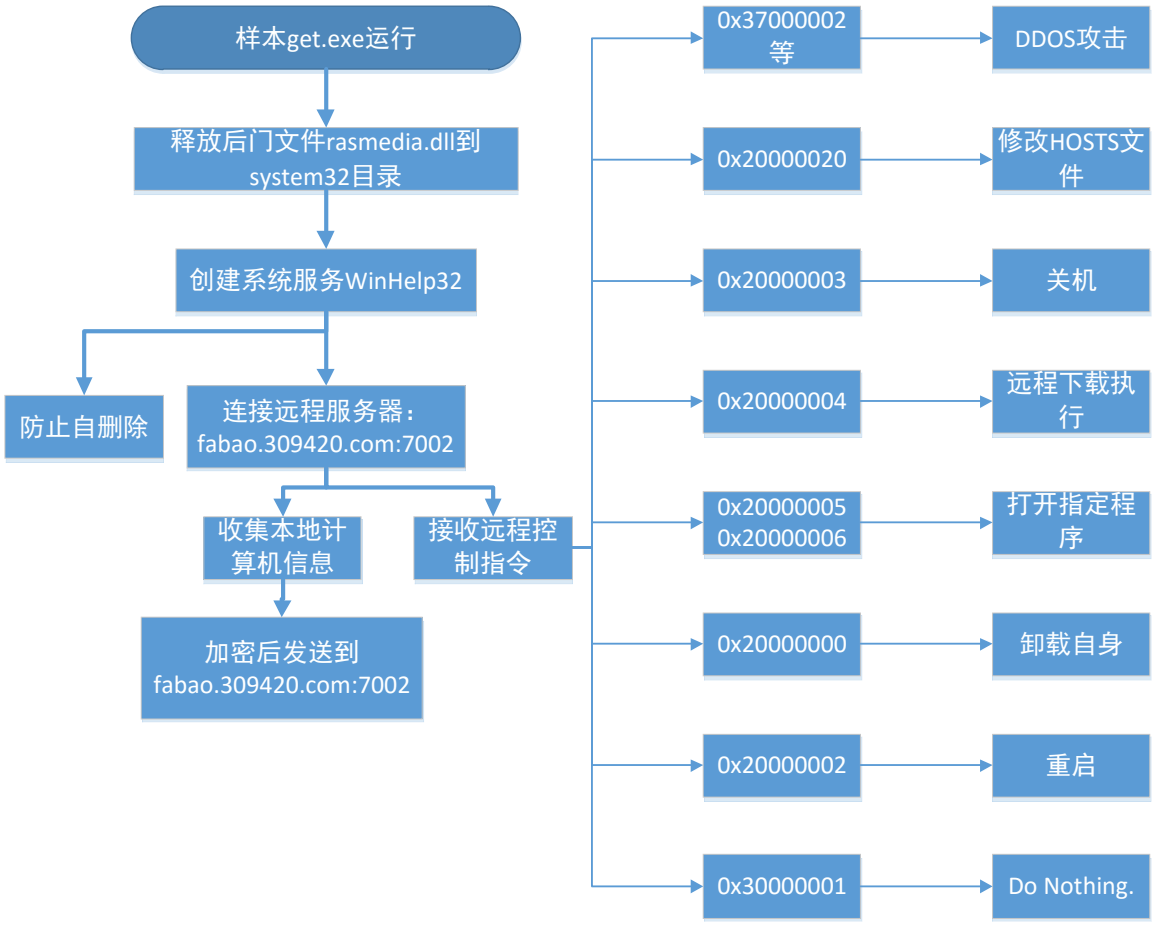
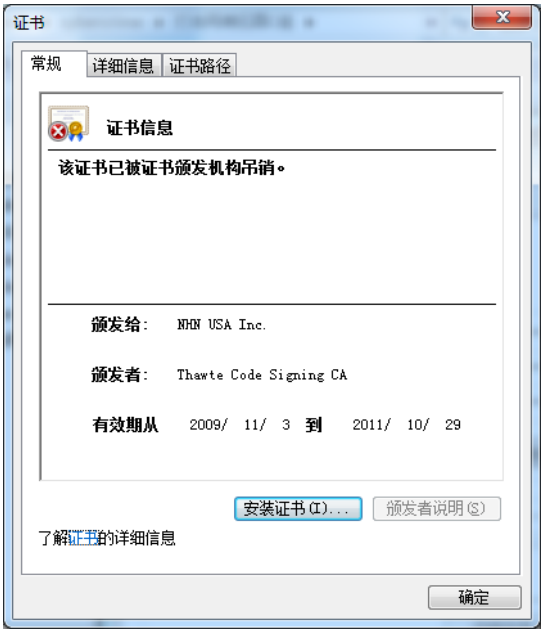


图 1 样本运行流程

2.3 样本详细分析

该样本包含 NHN USA Inc.公司的数字签名信息，该数字签名有效期是 2009/11/3 到 2011/10/29，已经过期。



样本 get.exe 运行后会释放后门文件 rasmedia.dll 到 system32 目录下，每次释放，此文件末尾会被随机填充一些数据形成不同的文件 hash，在开启了 UAC 的系统上，释放文件到 system32 目录会失败，样本会动态加载 rasmedia.dll，调用其导出的 Install 函数使得 rasmedia.dll 可以以服务的方式启动。最后样本 get.exe 会调用 cmd.exe 进行自删除。服务的属性信息以及对应的 dll 路径如下：

在 WinHelp32 服务启动后，对应的后门 dll 文件就被加载运行了，首先，dll 会动态解密要连接的域名端口：fabao.309420.com:7002 以及其他一些信息，方便后续使用，如下：

```
10007224 fabao.309420.com:7002...........
10007244 ................................
10007264 ................................
10007284 ................................
100072A4 Pri20130313.........WinHelp32...
100072C4 ...................Windows Help
100072E4  System.........................
10007304 ................................
10007324 ........................Windows
10007344 Help System for X32 windows desk
10007364 top.............................
```

此后 rasmedia.dll 会创建两个主要的线程，一个线程是为了防止自身被删除，另一个就是联网获取远端指令，然后执行相关的操作,例如 DDoS。

为了防止被删除，其首先会读取自身数据存放在缓冲区里，然后循环判断自身文件是否存在，如果不存在就把缓冲区里的内容重新写入文件，主要代码如下：

```
v2 = CreateFileA(&Filename, 0x80000000, 0, 0, 3u, 0x80u, 0);
hObject = v2;
v3 = GetFileSize(v2, 0);
v13 = v3;
v4 = VirtualAlloc(0, v3, 0x3000u, 4u);
ReadFile(v2, v4, v3, &NumberOfBytesRead, 0);
CloseHandle(v2);
while ( 1 )
{
  v5 = FindFirstFileA(&Filename, &FindFileData);
  hFindFile = v5;
  if ( v5 == (HANDLE)-1 )
  {
    v6 = CreateFileA(&Filename, 0x40000000u, 0, 0, 2u, 0x80u, 0);
    v7 = v6;
    hObject = v6;
    WriteFile(v6, v4, v3, &NumberOfBytesRead, 0);
    CloseHandle(v7);
    v5 = hFindFile;
```

另一个线程首先会收集本地主机的计算机名、系统版本、磁盘大小等信息， 然后把这些收集到的信息加密后，发送到远控端，其加密算法如下：

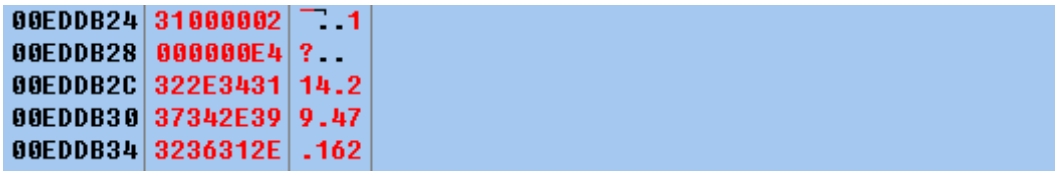
```
void    call(BYTE *buf, int len,int res)
{
    int i=0;
    BYTE tmp=res&0xff;
    tmp=tmp % 0xfe;
    tmp++;
    while(len)
    {
        buf[i] = tmp+ tmp ^ buf[i];
        i++;
        len--;
    }
}
```

而此加密函数的调用方式是以 call(buf,0x60,0x0c)这种形式出现，其中的 buf 里存放的就是收集到的一些信息，0x60 是信息长度

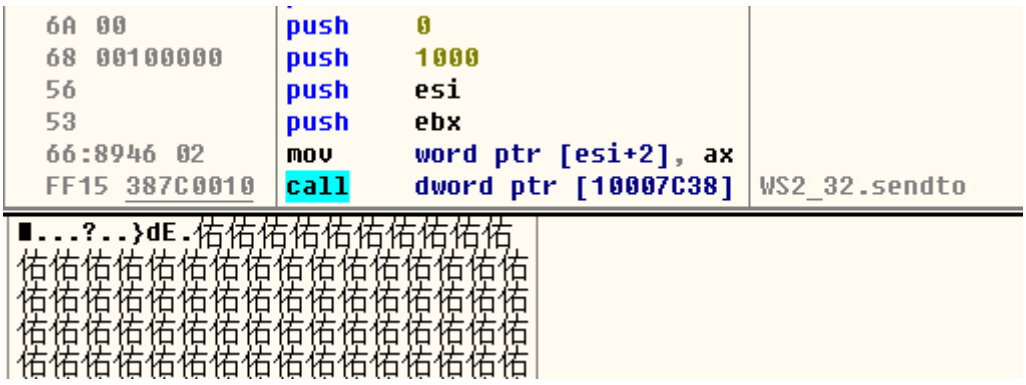
然后，dll 会循环从 fabao.309420.com:7002 上获取数据，在解密接收的数据后，会再次对数据进行格式解析，其解密算法如下：

```
void call2(BYTE *buf, int len,int res)
{
    int i=0;
    BYTE tmp=res&0xff;
    tmp=tmp % 0xfe;
    tmp++;
    while(len)
    {
        buf[i] = (buf[i]-tmp)^tmp;
        i++;
        len--;
    }
}
```

通过观察上面的两个函数可以看出，这里的加密函数和解密函数正好相对应。
通信数据协议为：控制指令(4 字节)+数据大小(4 字节)+数据
然后通过匹配控制码，来执行相关的操作，分析发现，这里经常接收到的控制码有 0x31000002 和 0x32000002，这两个控制指令都跟 DDOS 相关，当控制码为 0x31000002 时，解密后的数据如下：



可以看到，这种情形下获取的数据是一个 IP 地址，然后 dll 会创建很多线程，每个线程都循环对获取到的 IP 进行 DDOS 攻击，每次发送的数据包大小为 0x1000，而数据内容是随机生成的，代码如下：



当控制码为 0x32000002 时，解密后的数据如下：

```
00DED544 32000002 ?..2
00DED548 000000E4 ?...
00DED54C 70747468 http
00DED550 772F2F3A ://w
```

在这里获取到的数据是一个带参数的网址，其内容如下：

```
00DED544 ?..2?..http://wap.10230000.cn/w
00DED564 forder/wftemplate/wapdd1.php?p=p
00DED584 _1&t=t_3&i=&r=.................
00DED5A4 ................................
```

然后也会创建很多线程循环对这个网址发起大量 GET 请求，造成 DDoS，其发送的 GET 请求的数据如下：

```
0119FB00 GET /wforder/wftemplate/wapdd1.p
0119FB20 hp?p=p_1&t=t_3&i=&r= HTTP/1.1..H
0119FB40 ost: wap.10230000.cn..User-Agent
0119FB60 : Mozilla/5.0 (compatible; Baidu
0119FB80 spider/2.0; +http://www.baidu.co
0119FBA0 m/search/spider.html)..Cache-Con
0119FBC0 trol: no-store, must-revalidate.
0119FBE0 .Referer: http://wap.10230000.cn
0119FC00 ..Connection: Close.............
```

如上图所示，其 GET 请求的数据的组成方式是以事先准备好的模版来填充的，其对应的模版为：

```
'GET %s HTTP/1.1',0Dh,0Ah
'Host: %s',0Dh,0Ah
'User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www'
'.baidu.com/search/spider.html)',0Dh,0Ah
'Cache-Control: no-store, must-revalidate',0Dh,0Ah
'Referer: http://%s',0Dh,0Ah
'Connection: Close',0Dh,0Ah
0Dh,0Ah,0
```

当然，在 dll 里还有其他的模版，总数多达十种，下面列出其中的几种：

其一：

```
'GET / HTTP/1.1',0Dh,0Ah
'Host: %s:%d',0Dh,0Ah
0Dh,0Ah,0
```

其二：

```
'GET / HTTP/1.1',0Dh,0Ah
'Host: %s',0Dh,0Ah
'User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www'
'.baidu.com/search/spider.html)',0Dh,0Ah
'Cache-Control: no-cache',0Dh,0Ah
'Connection: Close',0Dh,0Ah
0Dh,0Ah,0
```

其三：

```
'GET %s HTTP/1.1',0Dh,0Ah
'Host: %s:%d',0Dh,0Ah
'User-Agent: Mozilla/5.0+(compatible;+Baiduspider/2.0;++http://www'
'.baidu.com/search/spider.html)',0Dh,0Ah
'Cache-Control: no-store, must-revalidate',0Dh,0Ah
'Referer: http://%s',0Dh,0Ah
'Connection: Close',0Dh,0Ah
0Dh,0Ah,0
```

其四：

```
'GET %s HTTP/1.1',0Dh,0Ah
'Host: %s:%d',0Dh,0Ah
'User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www'
'.baidu.com/search/spider.html)',0Dh,0Ah
'Cache-Control: no-store, must-revalidate',0Dh,0Ah
'Referer: http://%s',0Dh,0Ah
'Connection: Close',0Dh,0Ah
0Dh,0Ah,0
```

其五：

```
'GET %s HTTP/1.1',0Dh,0Ah
'Host: %s',0Dh,0Ah
'User-Agent: Mozilla/5.0+(compatible;+Baiduspider/2.0;++http://www'
'.baidu.com/search/spider.html)',0Dh,0Ah
'Cache-Control: no-store, must-revalidate',0Dh,0Ah
'Referer: http://%s',0Dh,0Ah
'Connection: Close',0Dh,0Ah
0Dh,0Ah,0
```

其六：

```
'GET %s?=%d HTTP/1.1',0Dh,0Ah

'User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www'
'.baidu.com/search/spider.html)',0Dh,0Ah
'Host: %s:%d',0Dh,0Ah
'Cache-Control: no-cache',0Dh,0Ah,0
```

其七：

```
'GET %s?=%d HTTP/1.1',0Dh,0Ah

'User-Agent: Mozilla/5.0 (compatible; Baiduspider/2.0; +http://www'
'.baidu.com/search/spider.html)',0Dh,0Ah
'Host: %s',0Dh,0Ah
'Cache-Control: no-cache',0Dh,0Ah,0
```

除了上面提及的 DDOS 功能外，此 dll 文件还有其他远控类型的功能，在通过分析后发现，此 DLL 后门中的控制指令多达 20 种，其主要指令如下：

控制码	功能
0x37000002	DDoS
0x41000001	DDoS
0x37000001	DDoS
0x32000004	DDoS

0x33000001	DDoS
0x36000001	DDoS
0x32000002	DDoS
0x31000005	DDoS
0x32000001	DDoS
0x31000003	DDoS
0x30000001	Do nothing
0x31000001	DDoS
0x31000002	DDoS
0x20000020	修改 HOSTS
0x20000003	关机
0x20000004	远程下载执行
0x20000005	打开指定程序
0x20000006	打开指定程序
0x20000000	卸载自身
0x20000002	重启

3 网络架构分析

3.1 网络基础设施

黑客控制网络基础，由样本分析可知，攻击者使用 fabao.309420.com:7002 指向的 61.147.107.91 作为服务器进行分发 DDOS 攻击任务，同时该 IP 的另外端口作为木马下载服务器。该域名并未部署 web 网站。由 ping 的 TTL 返回值为 118，可猜测其操作系统为 Win NT/2000/2003/XP。同时该域名在不同时间段指向了多个威胁 IP。该黑客组织从 2013 年即开始活动，其 IP 地址均位于江苏省扬州市电信。

域名	IP 端口	操作系统	最早时间	作用	描述
fabao.309420.com:7002	61.147.107.91:7002	Windows 2003	2015-10-12	C2 控制服务器	
	61.147.107.91:8082	Windows 2003	2015-10-12	放马服务器	
fabao.309420.com:7002	61.147.70.142:7002	Windows 2003	2015-11-19	C2 控制服务器	
fabao.309420.com:7002	61.147.103.178:7002		2015-06-18	C2 控制服务器	
fabao.309420.com:7002	61.147.103.117:7002		2013-06-03	C2 控制服务器	
fabao.309420.com:7002	61.147.103.99:7002		2013-04-17	C2 控制服务器	

```
C:\Users\Administrator>ping fabao.309420.com

正在 Ping fabao.309420.com [61.147.107.91] 具有 32 字节的数据:
来自 61.147.107.91 的回复: 字节=32 时间=29ms TTL=118
来自 61.147.107.91 的回复: 字节=32 时间=28ms TTL=118
来自 61.147.107.91 的回复: 字节=32 时间=28ms TTL=118
来自 61.147.107.91 的回复: 字节=32 时间=28ms TTL=118

61.147.107.91 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 28ms, 最长 = 29ms, 平均 = 28ms
```

使用 X-Scan 扫描目标服务器，发现目标开放了如下端口：135、139、21、22、3389

主机地址	端口/服务
fabao.309420.com	netbios-ssn (139/tcp)
fabao.309420.com	chargen (19/tcp)
fabao.309420.com	SSH, Remote Login Protocol (22/tcp)
fabao.309420.com	echo (7/tcp)
fabao.309420.com	ftp (21/tcp)
fabao.309420.com	Windows Terminal Services (3389/tcp)
fabao.309420.com	epmap (135/tcp)
fabao.309420.com	DCE/12345778-1234-abcd-ef00-0123456789ac (1026/tcp)
fabao.309420.com	msrdp (3389/tcp)
fabao.309420.com	tcp

其中 21 端口经检测，运行的为 Serv-U FTP Server v6.4

提示	ftp (21/tcp)	**开放服务** "FTP"服务运行于该端口. BANNER信息： 220 Serv-U FTP Server v6.4 for WinSock ready... NESSUS_ID : 10330
提示	ftp (21/tcp)	**FTP服务的版本和类型** 通过登陆目标服务器并经过缓冲器接收可查出FTP服务的类型和版本。这些注册过的标识信息将本和类型会在可能的地方被泄露。 解决方案：将这些注册过的标识信息转变为普通类别的信息。。 风险等级：低 Remote FTP server banner : 220 Serv-U FTP Server v6.4 for WinSock ready... NESSUS_ID : 10092

尝试连接登陆,发现存在 root 用户:

```
C:\Documents and Settings\Administrator>ftp fabao.309420.com
Connected to fabao.309420.com.
220 Serv-U FTP Server v6.4 for WinSock ready...
User (fabao.309420.com:(none)): root
331 User name okay, need password.
Password:
530 Not logged in.
Login failed.
```

使用 Serv-U 的默认管理员：LocalAdministrator，默认密码：#l@$ak#.lk;0@P，尝试登陆,发现默认管理员存在,但是默认密码被更改。

```
C:\Documents and Settings\Administrator>ftp fabao.309420.com
Connected to fabao.309420.com.
220 Serv-U FTP Server v6.4 for WinSock ready...
User (fabao.309420.com:(none)): LocalAdministrator
331 User name okay, need password.
Password:
530 Not logged in.
Login failed.
```

注意到目标服务器开放了 22 端口和 SSH 服务，尝试连接得到如下提示，怀疑可能是限制了登陆 IP。

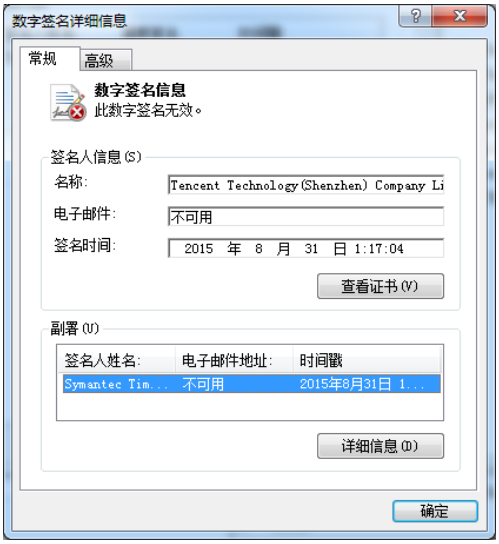
```
Host 'fabao.309420.com' resolved to 61.147.107.91.
Connecting to 61.147.107.91:22...
Connection established.
To escape to local shell, press 'Ctrl+Alt+]'.

Connection closed by foreign host.

Disconnected from remote host(fabao.309420.com:22) at 17:46:18.
```

目标服务器还开放了 3389 端口，使用系统自带的远程桌面连接连接至目标服务器，可以看到目标服务器系统为 Windows Server 2003，符合前边的推测。

目前尚未发现存在弱口令等。与控制端通信的其它样本 84747986208f11f326a890451988064f 则采用了伪造腾讯数字签名信息来逃避检测。



4 危害影响

4.1 受害者网站

根据监测发现，被攻击目标列表如下：

控制码	功能
http://wapkk.xford.cn/	减肥药网站
http://le.bjwcyls.com/	新年支付
http://pqt.zoosnet.net	网页商务通
http://www.dfr4fs.com	棋牌游戏
http://www.sbuluo.com	香水售卖网站
http://www.a0686.com	娱乐场网站
http://mmmoffice.com/	
http://xs.igreenport.com.cn/	
http://www.10230000.cn/	一件代发
http://www.qiuyun.sh.cn/	
http://flm.flmapp.com/	
http://xq2015.228.zj.cn/	
http://vip6.airuis.net/	
http://wapkf.huxiwa.cn/	
http://wap.1008tuan.com/	
http://www.shop3m.cn/	
http://flm.alibag.cn/	
http://le1s.xndnhc.com/	

http://www.gzmfl.cn	
http://willittt.aliapp.com	
http://183.131.85.140:888	
http://guanfang123.aliapp.com	
http://wap.pichia.cn	
http://mjgw.weizhangchaxun.com.cn	
http://aaa8.shengmingjiguang.cn	
http://flm.flm315.com	网赚
http://vip6.zyhlwlc.com	

主要攻击目标包括网络销售减肥产品、娱乐城以及电子商务平台，属于网络上的灰色相关产业，这些产业竞争比较激励。

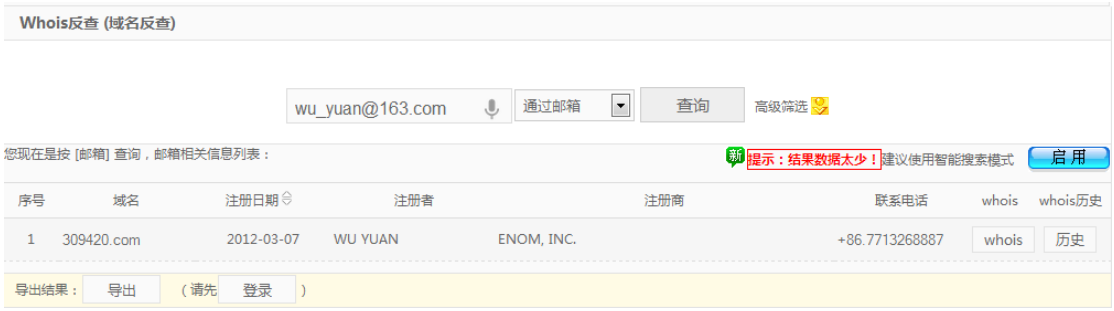
5 黑客追踪

5.1 攻击者推理

通过追影设备提取 C2 可以锁定以下域名：fabao.309420.com ,查询 whois 信息可以得到如下的注册信息：

```
Registrant Name: WU YUAN
Registrant Organization: WU YUAN
Registrant Street: DA XUE LU 58 HAO
Registrant City: NAN NIN
Registrant State/Province: GUANGXI
Registrant Postal Code: 538000
Registrant Country: CN
Registrant Phone: +86.7713268887
Registrant Phone Ext:
Registrant Fax: +86.7713268887
Registrant Fax Ext:
Registrant Email: WU_YUAN@163.COM
```

根据域名注册的英文信息，域名所有者是在广西省南宁市大学路 58 号申请注册的该域名，可能使用过号码为 0771-3268887 的固定电话，经查该号码地址为广西南宁。通过输入域名反查，我们获取到了注册域名的 163 邮箱。通过这个邮箱，搜索申请的域名：



发现该邮箱仅仅申请了 309420.com 这一个域名。

5.2 获利分析

攻击的目标主要是灰色网站，该领域存在激烈的同行商业竞争，如果有新加入这个销售减肥药品在线销售网站将会受到之前的该领域的共同攻击。

6 总结

该 DDoS 攻击组织利用窃取的企业过期签名以及伪造数字签名来逃避杀软检测，对可信体系的信任链条是一种冲击，目前杀毒软件厂商也都增加了对数字签名的检验，从粗糙的检验数字签名是否存在到对数字签名的期限，数字签名伪造等进行检测。

7 相关信息

相关 MD5 列表

0b149f4ea7618a1d009409e889541b89
82d25d47c82246aed948031597141763
84747986208f11f326a890451988064f
801905dd2ff5b92355ba4c21a9ec1477
b8f83b1e12ac61d8045a44561c5b7863
7afeb59f339d3af22b8b1f51b8e01f15
4f6f7e8d6400fad699793449834153c1
087e5fbde0dec2d19eafbf749433792c
2ec8c7c9a3b051e2b44d74ebe4f53aa4
429b2d49ebf58634df7c6d2def01b406
685157a415112954f94a2ea7cfd796f4
b7d9c12c12a86fcea50371a0fe545641
9d390bd6a71eb4e2a0d3ba8d1fead3c6
572b568cfd3ce67b81ed980cfa6520b0
84bb036c3ee8681dec8e98c6356190b7

附录一：参考资料

[1] NHN USA

http://www.nhnentusa.com/usa/index.nhn

附录二：关于安天

安天从反病毒引擎研发团队起步，目前已发展成为拥有四个研发中心、监控预警能力覆盖全国、产品与服务辐射多个国家的先进安全产品供应商。安天历经十五年持续积累，形成了海量安全威胁知识库，并综合应用网络检测、主机防御、未知威胁鉴定、大数据分析、安全可视化等方面经验，推出了应对持续、高级威胁（APT）的先进产品和解决方案。

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 CNNVD 六家一级支撑单位之一。安天移动检测引擎获得全球首个 AV-TEST（2013）年度奖项的中国产品，全球超过十家以上的著名安全厂商都选择安天作为检测能力合作伙伴。

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

附录三：文档更新日志

更新日期	更新版本	更新内容
yyyy-mm-dd 00:00		
yyyy-mm-dd 00:00		
yyyy-mm-dd 00:00		
yyyy-mm-dd 00:00		