

从果粉到黑吃黑：一个论坛挂马的奇异反转

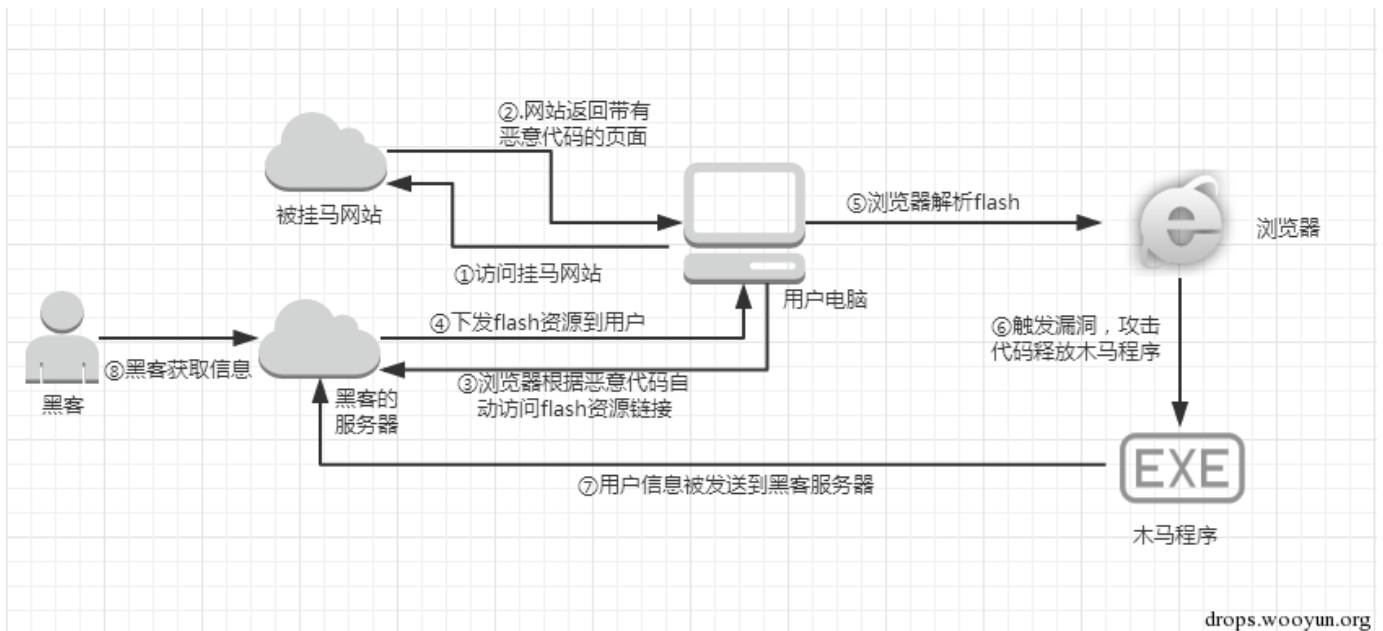
0x00 前言

继上个星期国内知名果粉社区威锋网(上周事件一出, 威锋网已修复)遭黑客挂马事件后, 360安全卫士再度发现该黑客还在其他网站论坛进行挂马。从3月开始, 360互联网安全中心检测到该样本的零星打点记录, 此情况从4月11日呈上升趋势, 多个论坛内大量帖子被插入Flash漏洞攻击程序。因威锋网是国内最大的苹果用户中文论坛, 每天有百万级浏览量, 360安全卫士对威锋挂马攻击的拦截量因此急剧增加。后续我们还在小七论坛以及游戏藏宝湾等论坛发现该样本的踪迹。

0x01 攻击手段

攻击者主要通过热门帖子内回复并插入经过改造Hacking Team的Adobe Flash Player漏洞(CVE-2015-5122)攻击的Flash元素, 浏览帖子的用户如果没有及时更新Flash或安装可靠的安全软件, 电脑会自动下载运行木马程序, 感染的木马是PlugX系列远控程序, 在进入受害者系统后, 它会连接位于香港的控制服务器, 黑客可以由此完全控制、监视受害者电脑, 窃取隐私文件以及账号密码等重要信息。由于被国内有很多论坛允许任意用户直接插入任意外网Flash文件, 这就导致黑客有机可乘。

攻击流程



该样本中使用的攻击手段

1. 该挂马者通过写注册表来过UAC
2. 该挂马者通过释放一个带签名的iexplore.exe(非微软签名), 来逃避杀软的查杀.
3. 该挂马者通过还进行了白利用, 通过将数据注入到explore.exe来进行敏感操作来逃避杀软的查杀
4. 该挂马者通过利用白进程来写服务, 让自己的程序以服务的形式启动。长期驻扎在用户系统中

新解密出来的dll会先遍历进程查看是否存在杀毒软件

下面是该样本检测的杀软列表

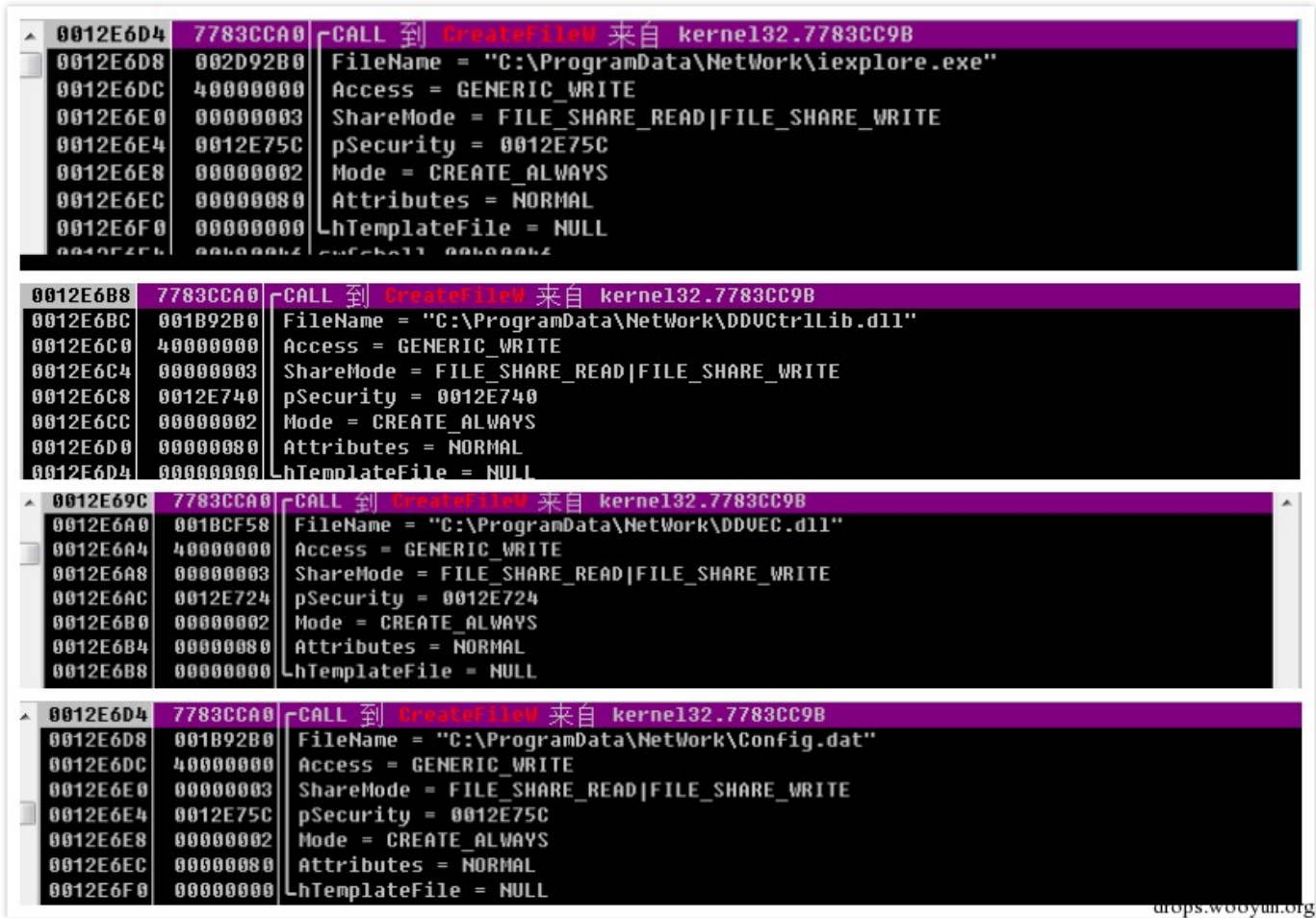
kxetray.exe 金山

ravmonf.exe 瑞星

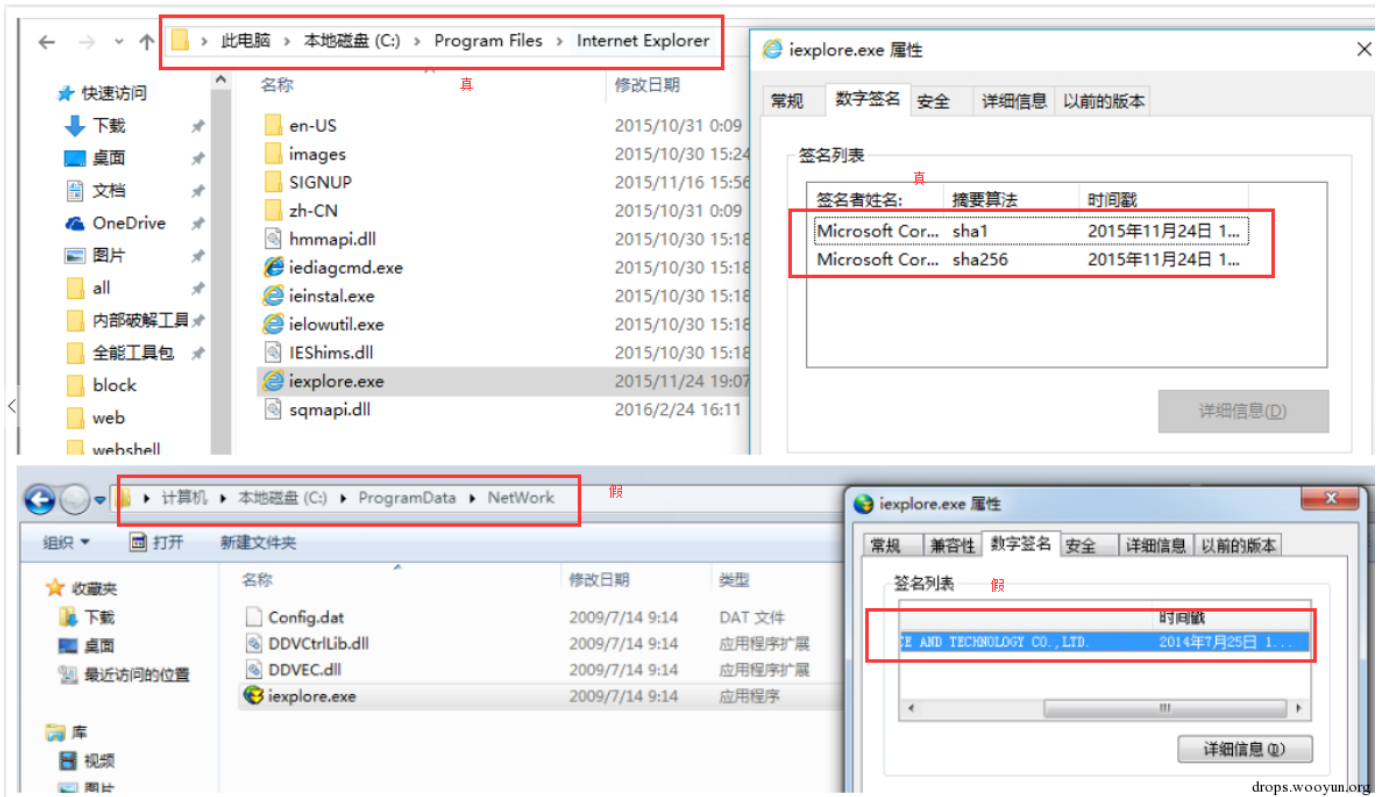
avp.exe 卡巴斯基

uiSeAgt.exe 趋势科技

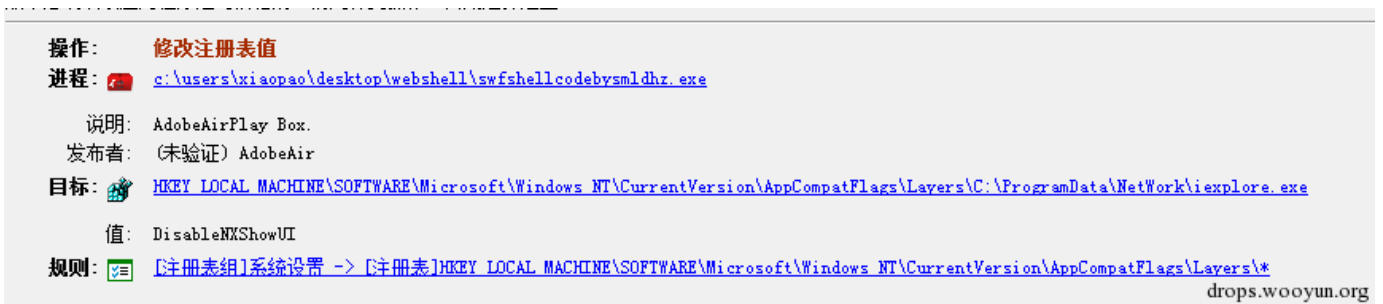
检测环境后就开始释放多个文件



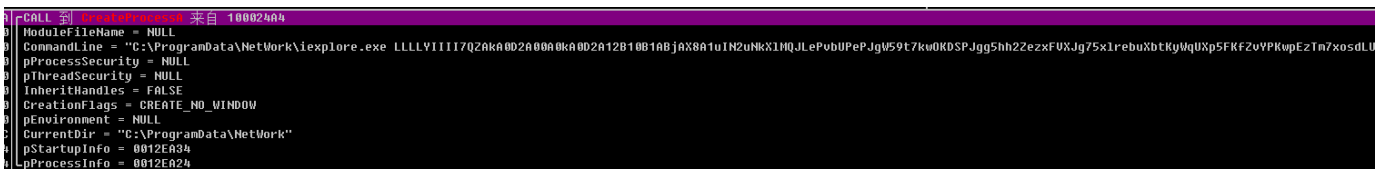
挂马者释放一个带数字签名的iexplore.exe，该程序带有9158(一个大型多人网络视屏平台)的数字签名。下图是正常iexplore和挂马者释放的iexplore的比较图。用白利用的方式绕过杀软的查杀



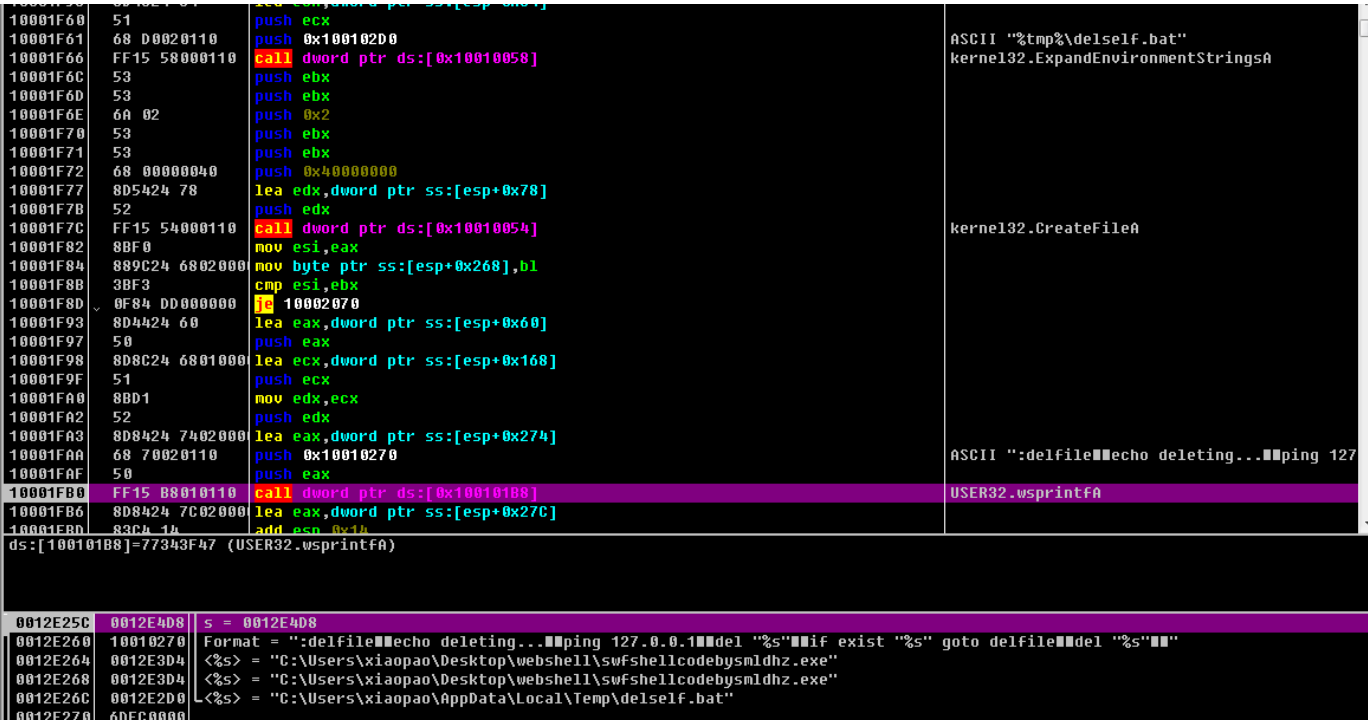
该挂马者通过让 `HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers` 的键值指向新释放的 `iexplore` 处来来绕过 UAC。达到以管理员权限的模式来启动“`iexplore`”



写好注册表后就启动 `iexplore`，传递一个超级超级长的乱码参数，非人类设计 o(∩_∩)o。



准备工作都做好了就开始毁尸灭迹了。删除自身



新创建的iexplore程序会将自身携带的数据注入到explore.exe 中

操作：**修改其他进程的内存**

进程： [c:\programdata\network\iexplore.exe](#)

说明：Download Microsoft 基础类应用程序

发布者：(已验证) JINHUA 9158 NETWORK SCIENCE AND TECHNOLOGY CO.,LTD.

目标： [c:\windows\explorer.exe](#)

规则： [\[应用程序\]*](#)

drops.wooyun.org

创建服务，使iexplore在用户电脑启动的时候以服务的形式自启动。以服务的形式启动一般情况下很难察觉出中招了。因为电脑平时有很多个svchost进程。

操作：**修改注册表值 (安装驱动程序或服务)**

进程： [c:\windows\system32\services.msc](#)

说明：服务和控制应用程序

发布者：(已验证) Microsoft Corporation

目标： [HKLM\LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetworkService\ImagePath](#)

值：[C:\ProgramData\Network\iexplore.exe](#)

规则： [\[注册表项\]自动运行程序所在位置 -> \[注册表\]HKLM\LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services*.ImagePath](#)

drops.wooyun.org

写完在服务后就以服务的方式启动程序

操作：**创建新进程**

进程： [c:\programdata\network\iexplore.exe](#)

说明：Download Microsoft 基础类应用程序

发布者：(已验证) JINHUA 9158 NETWORK SCIENCE AND TECHNOLOGY CO.,LTD.

目标： [c:\windows\system32\svchost.exe](#)

命令行：[C:\Windows\system32\svchost.exe NetworkService 1520](#)

规则： [\[应用程序\]*](#)

drops.wooyun.org

创建网络连接，对用户电脑进行监控

```
1  if ( !*((_DWORD *)v26 - 2) )
2      goto LABEL_31;
3  v14 = gethostbyname(v26); |
4  if ( !v14 )
5      goto LABEL_31;
6  v15 = inet_ntoa(*(struct in_addr **)v14->h_addr_list);
7  040D986(&v25, v15);
8  if ( *((_DWORD *)v25 - 2) )
9  {
10     *(_DWORD *)(a3 + 136) = inet_addr(v25);
11     v23 = 1;
12 }
13 040D7F4((#70 *)&v25);
14  if ( !v23 )
```

drops.wooyun.org

服务启动后，解析其域名，然后一直不停的在162.251.20.165处发送心跳包。通过反ip查询到到挂马者用的是公云动态域名。

序	协议	源IP	源端口	目标IP	目标端口	操作	大小	速率	时间	备注			
91	UDP	192.168.142.1...	192.168.142.2	64284	53	domain	4	148 Bytes	325 Bytes	0.0 KB/Sec	2016/4/28 10:12...	2016/4/28 10:12...	00:00:04.040
92	UDP	192.168.142.1...	192.168.142.2	63492	53	domain	1	45 Bytes	146 Bytes	0.0 KB/Sec	2016/4/28 10:12...	2016/4/28 10:12...	00:00:00.000
93	UDP	192.168.142.1...	162.251.20.165	137	137	netbios-ns	6	300 Bytes	546 Bytes	0.0 KB/Sec	2016/4/28 10:12...	2016/4/28 10:15...	00:02:47.341
94	UDP	192.168.142.1...	192.168.142.2	53009	53	domain	1	43 Bytes	142 Bytes	0.0 KB/Sec	2016/4/28 10:12...	2016/4/28 10:12...	00:00:00.000

00000000 7E 72 01 00 00 01 00 00 00 00 00 06 6F 6E 6C ~r.....onl

00000010 69 6E 65 06 70 75 62 79 75 6E 05 73 70 61 63 65 ine.puby un.space

00000020 00 00 01 00 01 7E 72 01 00 00 01 00 00 00 00 00r.....

00000030 00 06 6F 6E 6C 69 6E 65 06 70 75 62 79 75 6E 05 ..online .pubyun.

00000040 73 70 61 63 65 00 00 01 00 01 7E 72 01 00 00 01 space.....r...

00000050 00 00 00 00 00 00 06 6F 6E 6C 69 6E 65 06 70 75o nline.pu

00000060 62 79 75 6E 05 73 70 61 63 65 00 01 00 01 7E byun.spa ce.....~

00000070 72 01 00 00 01 00 00 00 00 00 06 6F 6E 6C 69 r.....onli

00000080 6E 65 06 70 75 62 79 75 6E 05 73 70 61 63 65 00 ne.pubyu n.space.

00000090 00 01 00 01

drops.wooyun.org

信息追踪

在最近找到两个论坛中，其中该挂马着在小七论坛上注册的用户是一个老用户。从2014年就注册了，小七论坛是国内的一个免杀论坛，黑吃黑啊。在这个充满利益的地方，有多少想着给别人种马的人，却在不知不觉中已经被别人种上了马。不要老想着做不好的事，小心螳螂捕蝉黄雀在后。

用户组 老百姓

在线时间 44 小时

最后访问 2016-4-10 19:43

上次发表时间 2016-4-10 16:54

注册时间 2014-9-4 13:38

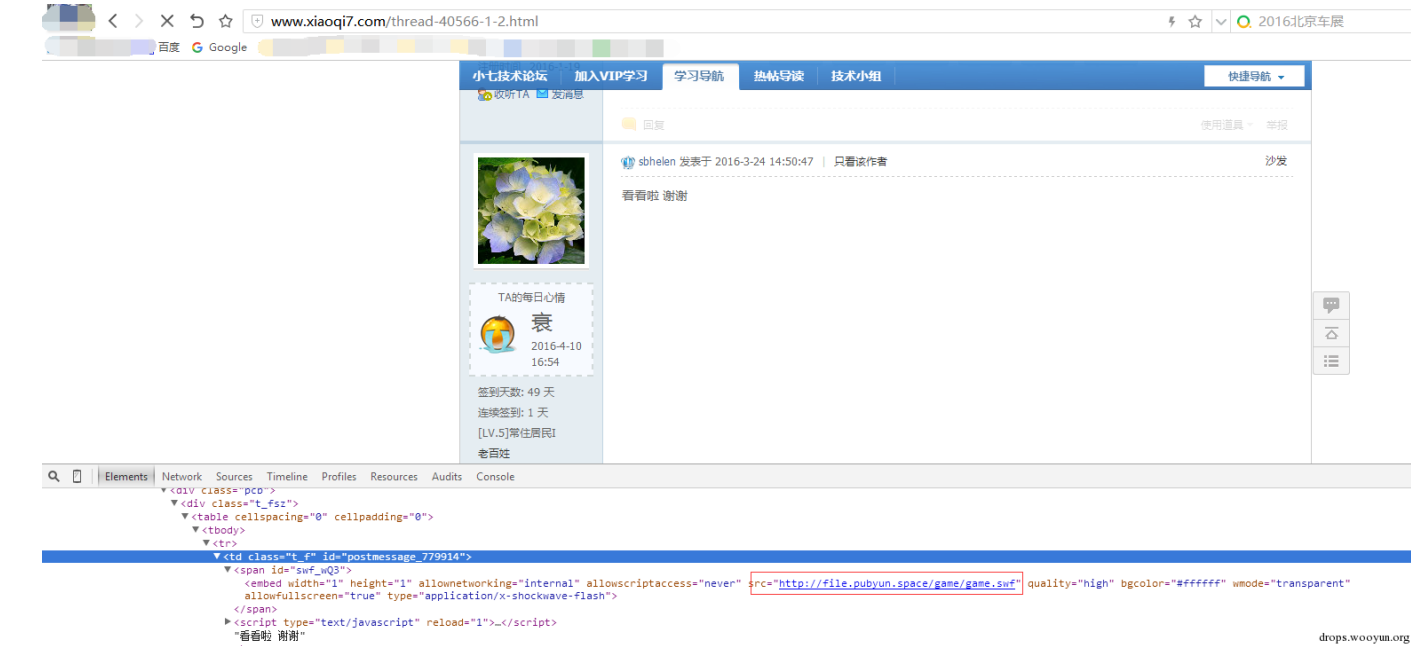
上次活动时间 2016-4-10 16:54

所在时区 使用系统默认

drops.wooyun.org

这个是该挂马者在小七论坛上挂马截图，就一个简简单单回复，平时一般这种都会被看做是水贴啥的，也不会有人会怎么去关注，但是这条回复后面却藏者一个链接。在你什么也不操作的情况下，只要触发了

Adobe Flash Player漏洞（CVE-2015-5122），你就中招了。



从该用户分享资源的连接我们找到该用户的百度云账号。卧槽居然有QQ号，看到的时候激动了一下。但是该QQ号应该是该挂马者专门用来做不干净的东西的，所以并没找到有价值的东西。o(′ □ ′)o白开心

冷言冷语冷透心 + 立即订阅

Ta还没有个人说明呢

8分享 0专辑

全部分享

专辑

图片

文档

音乐

视频

其他

分享文件	分享时间 ↓
百度云不限速pc版5.3.1.7z	2016-04-09 12:54
李毅吧内涵贴.txt等	2016-03-12 14:08
CVE-2016-0051-master.zip	2016-02-15 17:11
DroidJack.4.4.Cracked.zip	2016-01-11 14:32
【踏月传奇】诛仙3 【14职业+全时装+全坐骑+全副本】...	2015-12-05 20:21
Oday演示视频[解压密码QQ860566734].rar	2015-10-24 22:01
街机游戏1000合1	2015-07-21 09:32
Flashexp生成器.rar	2014-06-19 12:40

车道山前必有路但是在小七论坛中我们还看到该挂马者发布的一个帖子。

查看: 185 | 回复: 8



TA的每日心情

截至20150814仍可用的Flash挂马 [复制链接]

 **sbhelen** 发表于 2015-8-14 14:42:33 | 显示全部楼层

回复可见
<http://sadboy.org/forum.php?mod=viewthread&tid=114&highlight=flash>

“ <http://sadboy.org/forum.php?mod=viewthread&tid=114&highlight=flash> ”

drops.wooyun.org

该贴直接跳转到sadboy.org论坛的一个flash挂马视频帖，居然是管理员。o(∩_∩)o

查看: 4528 | 回复: 80



53 344 3万
主题 帖子 积分

管理员
★★★九转仙君★★★

积分 30419

[视频]FLASH漏洞利用到挂马录像  [复制链接]

 发表于 2015-7-28 10:23:10 | 只看该作者 ▶

CVE-2015-5122
早在很久之前就发布了文字教程
应论坛兄弟要求 就录制了一个视频
有什么地方指出来 一起交流一下

也鼓励更多的弟兄们录制有意义的视频 不分能力 一起进步

 游客，如果您要查看本帖隐藏内容请[回复](#)

 FLASH

drops.wooyun.org

从上面信息找到该挂马者就是该论坛的站长。在查询该论坛信息时发现该论坛注册时使用的信息都是假信息(保密工作还是做得不错的)。唯独一个foxmail邮箱是真的

Domain Name: SADBOY.ORG
Domain ID: D176268263-LROR
WHOIS Server:
Referral URL: http://www.godaddy.com
Updated Date: 2015-07-15T03:45:52Z
Creation Date: 2015-05-15T09:10:20Z
Registry Expiry Date: 2016-05-15T09:10:20Z
Sponsoring Registrar: GoDaddy.com, LLC
Sponsoring Registrar IANA ID: 146
Domain Status: ok https://www.icann.org/epp#ok
Registrant ID: CR194800595
Registrant Name: Fang ShengXian
Registrant Organization:
Registrant Street: ShangHai
Registrant Street: Beijing
Registrant City: ShangHai
Registrant State/Province: ShangHai
Registrant Postal Code: 332612
Registrant Country: CN
Registrant Phone: +51.15512312312
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: Sadboy_org@foxmail.com
Admin ID: CR194800597
Admin Name: Fang ShengXian
Admin Organization:
Admin Street: ShangHai
Admin Street: Beijing
Admin City: ShangHai
Admin State/Province: ShangHai
Admin Postal Code: 332612
Admin Country: CN
Admin Phone: +51.15512312312

假电话号码

真邮箱

假名

drops.wooyun.org

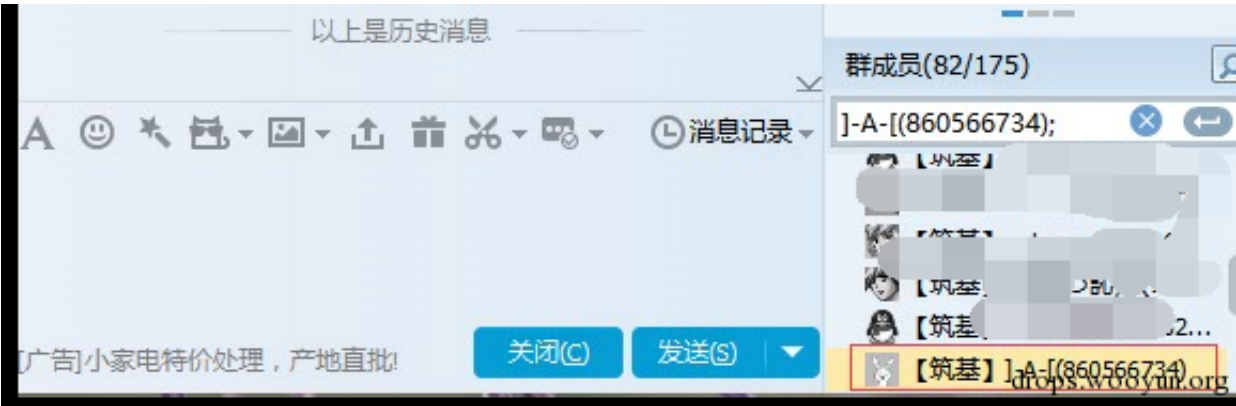
在该挂马者的论坛上，我们找到一个卖远控的群

论坛商业版远程管理V1.2.1
超强功能, 高效免杀
限时120!!

论坛官方交流QQ群
欢迎您的加入
群: 480257002

drops.wooyun.org

在该群内，我们还找到了该挂马者。丧病啊，不仅挂马还卖远控。真的是什么黑钱都赚啊。我就想问黑钱不烫手么？



不仅卖远控还卖各种泄露出来了的数据库o(′ □ ′)o

各地银行会员数据 - [售价 5 金钱]	晴 2015-5-29	6 933	haomyl23 2015-8-3 10:59
联通用户资料全集 - [售价 5 金钱] ... 2	晴 2015-5-29	11 1447	admin 2015-8-2 13:08
猴岛游戏论坛数据库300M - [售价 5 金钱]	晴 2015-5-29	3 642	左手 2015-7-31 15:51
当当网的数据库 - [售价 8 金钱]	晴 2015-5-29	5 925	dieinggame1 2015-7-31 15:19
圆通主站数据库打包下载 (内部人员账号密码泄漏) - [售价 5 金钱]	晴 2015-5-29	6 909	koobao 2015-7-29 14:06

在注册该论坛的时候发现需要购买邀请码，点过去就看到该挂马者的一部分名字



然后我们在论坛发现了一个支付宝账号，刚好就是该论坛注册时的那个邮箱账号

首页 > 聊天灌水 > 情感娱乐 > [每日任务]20150814金币发放帖

发帖

返回列表121 / 2页下一页

查看: 954 | 回复: 19

[每日任务]20150814金币发放帖 [复制链接]

发表于 2015-8-15 03:35:00 | 只看该作者

楼主 电梯直达

光之创造神



113主题209帖子2万积分

*****钻石会员*****

积分 29887

发消息

论坛已经正式开启金币兑换服务 利于有些嫌麻烦,却又急于想要下载某些工具的朋友 目前汇率是1:5

论坛绝大部分会员主题最高售价30,即意味着最贵不会超过6RMB

充值方式: 转账到sadboy_org@foxmail.com 请注明论坛ID,1-5分钟到账

--->

以上是收费信息,以后呢。每日会给广大会员发放金币

大家不着急的 可以每天攒一点每天攒一点 去下载自己想下载的东西

也算是没有违背初衷吧

分享到: QQ好友和群 QQ空间 腾讯微博 腾讯朋友

收藏 支持 反对

drops.wooyun.org

然后在手机上的支付宝上看了一下，是和论坛的购买邀请码的那个是同一个账号。并且我们还拿到了该作者的全名

![][27]

0x02 总结

小七论坛是国内知名的一个免杀论坛，一个 免杀论坛被挂马，每日访问量上万。多少有点偷鸡不成蚀把米的意味在里面。都想着免杀过杀软。但是却被别人在背后插了缝。想想挂马者控制了大量到处散播免杀木马人的电脑，自己掌握的用户就变double了。常在河边走哪有不湿鞋啊。

http://drops.wooyun.org/news/15451

12/12