从果粉到黑吃黑：一个论坛挂马的奇异反转

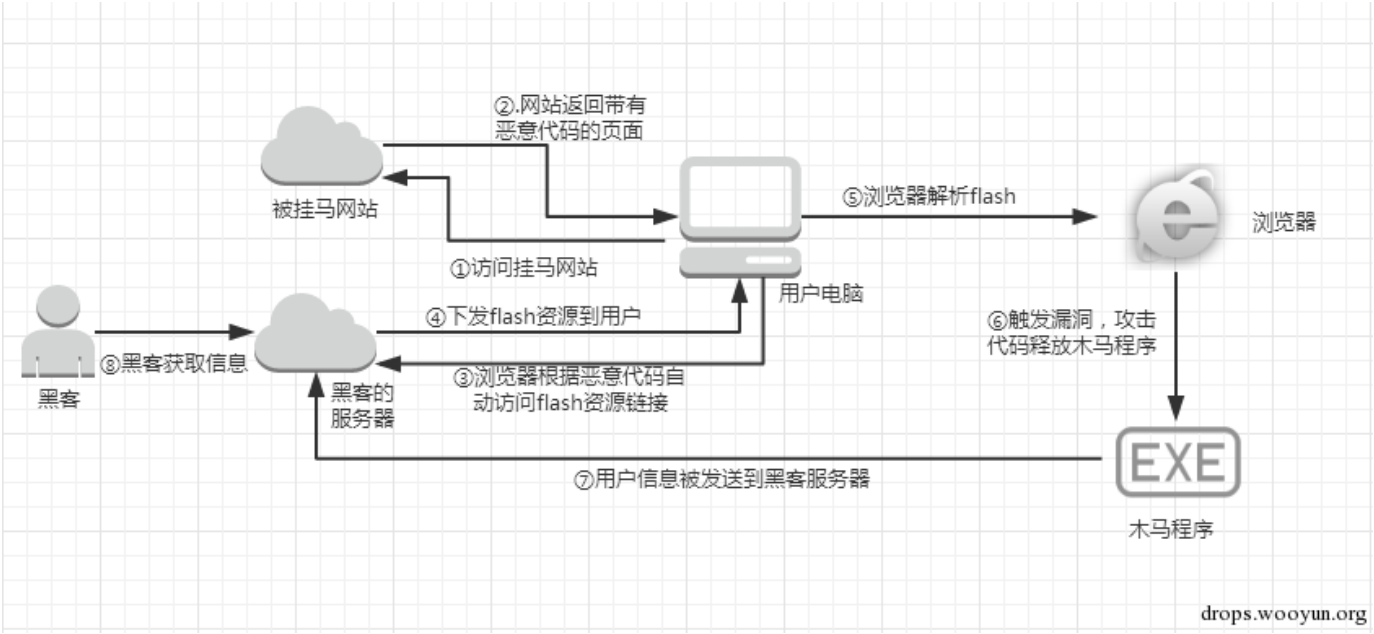
0x00 前言

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

攻击者主要通过在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。由于被国内有很多都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。

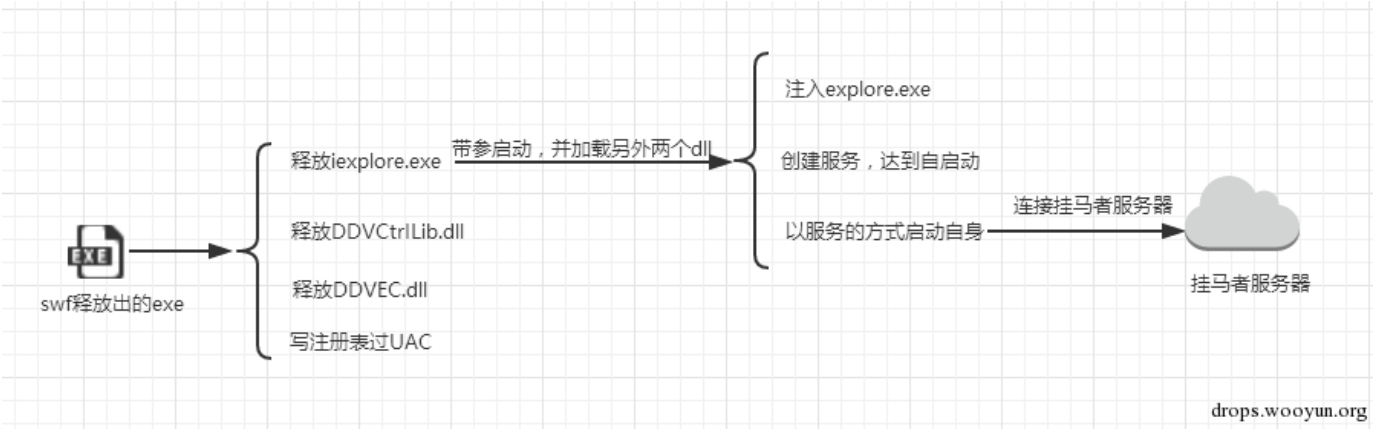
攻击流程



该样本中使用的攻击手段

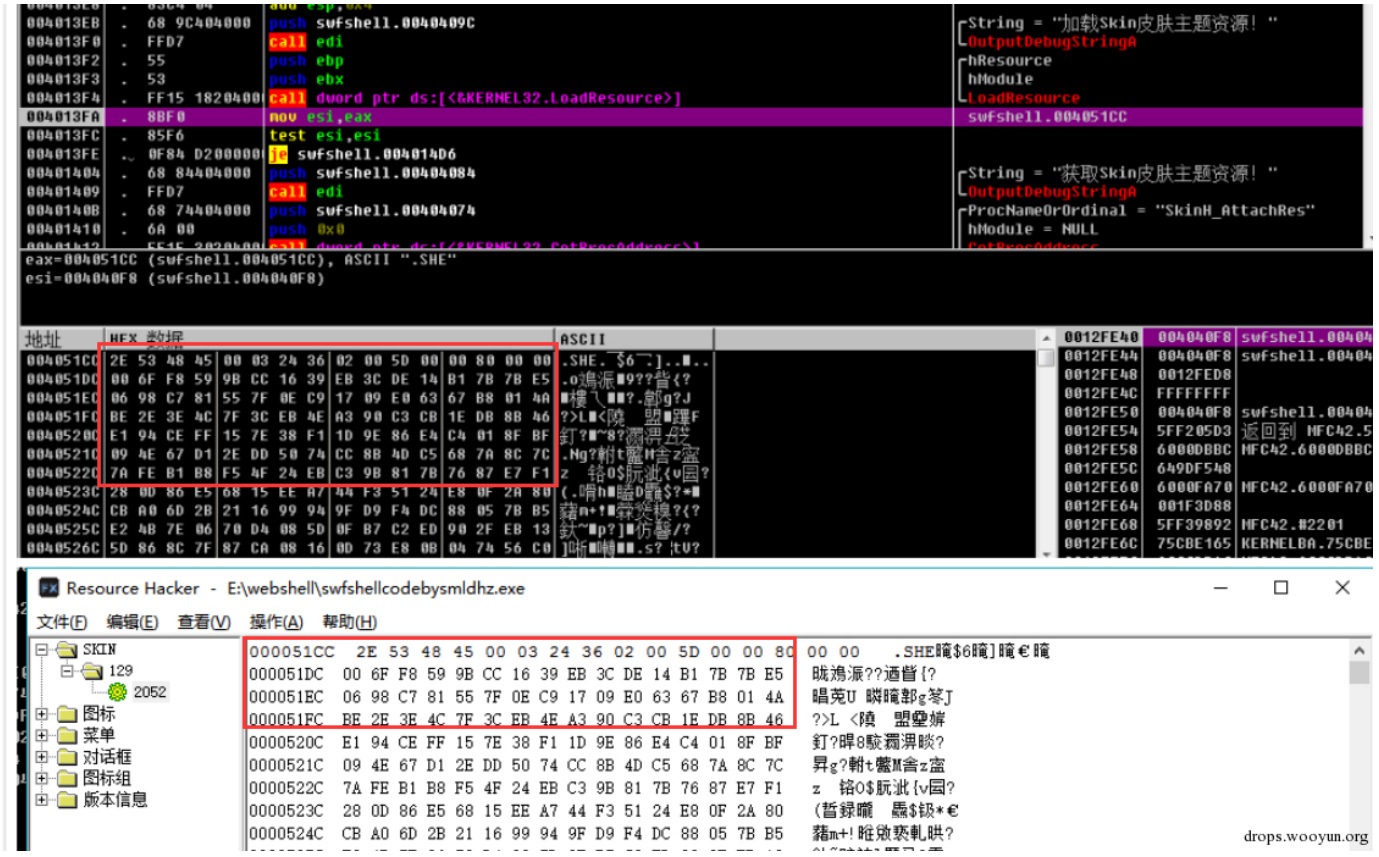
1. 该挂马者通过写注册表来过UAC
2. 该挂马者通过释放一个带签名的iexplore.exe(非微软签名),来逃避杀软的查杀.
3. 该挂马者通过还进行了白利用，通过将数据注入到explore.exe来进行敏感操作来逃避杀软的查杀
4. 该挂马者通过利用白进程来写服务，让自己的程序以服务的形式启动。长期驻扎在用户系统中

5. 该挂马者通过购买动态域名来进行挂马，让分析者很难追踪其信息

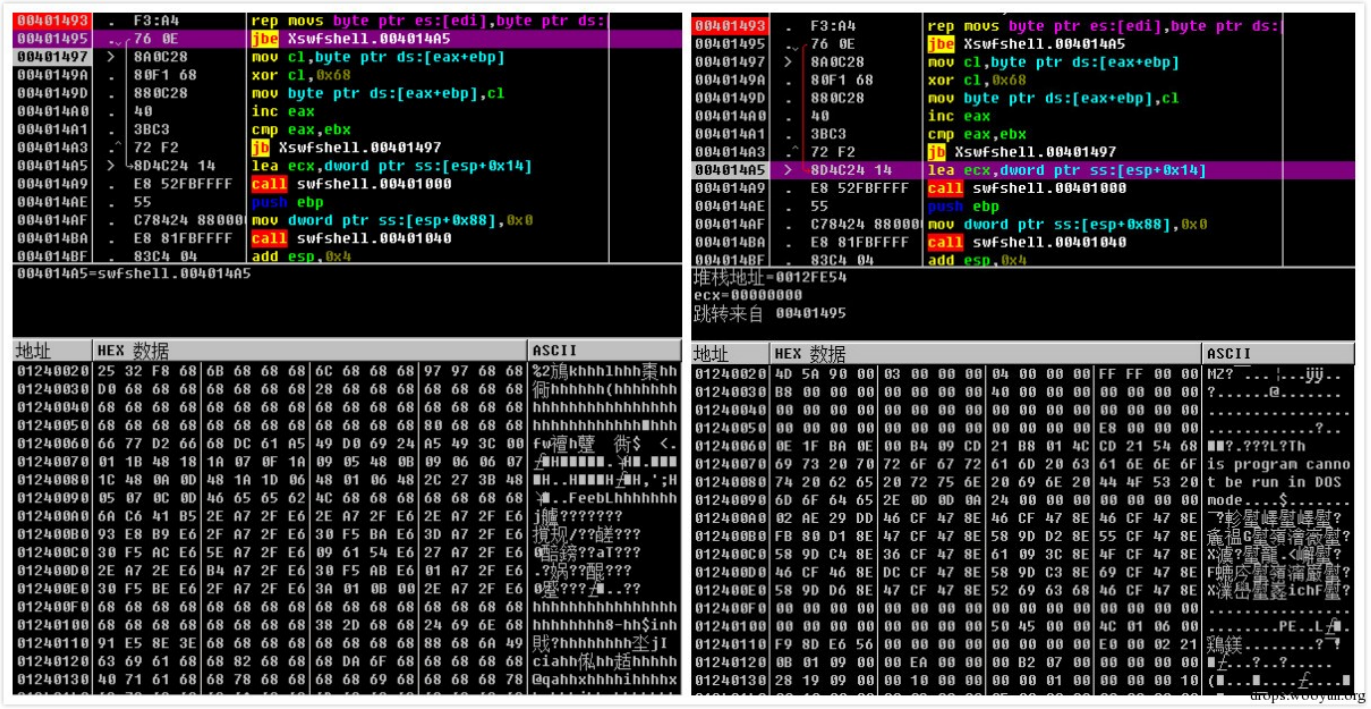


样本分析

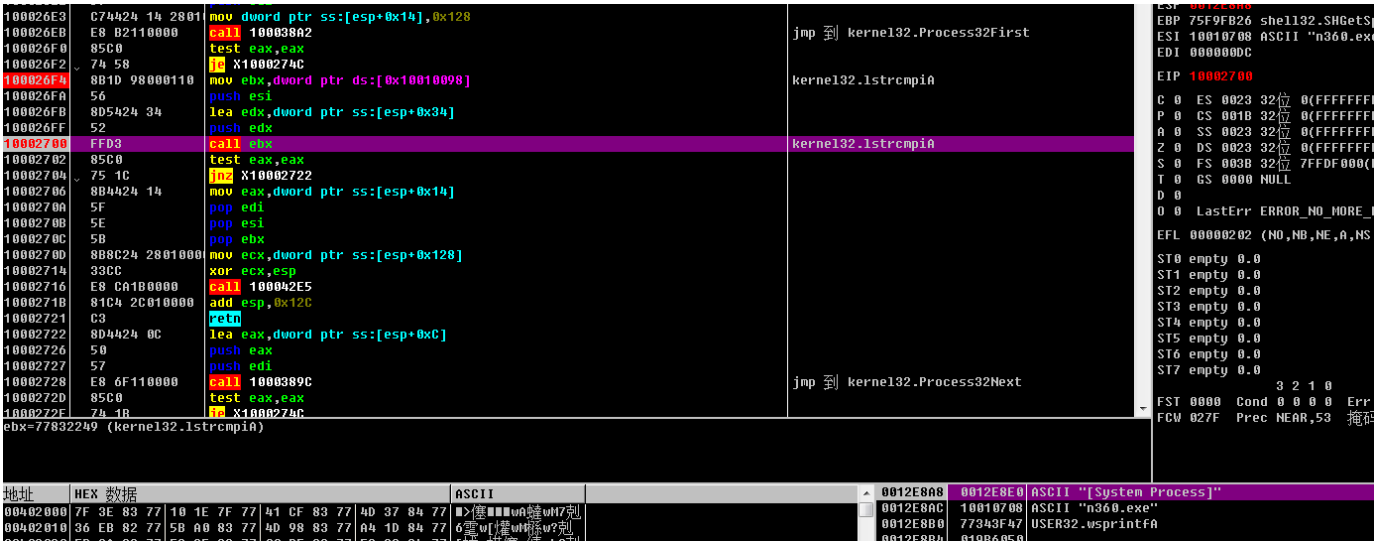
读取主体程序中自带的被加密过的数据文件。下面是读取该资源数据



读取到该该资源数据后，程序先对该资源文件中的部分数据进行解密，解密后得到一个pe文件。该文件是一个dll，主体程序在内存中载入该dll。



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

360tray.exe 360安全卫士

qqpctray.exe 腾讯管家

alyac.exe 韩国免费杀软

kvmonxp 江民杀软

ccsvchst.exe 诺顿

baiduhips 百度

kvfw.exe 江民kv防火墙

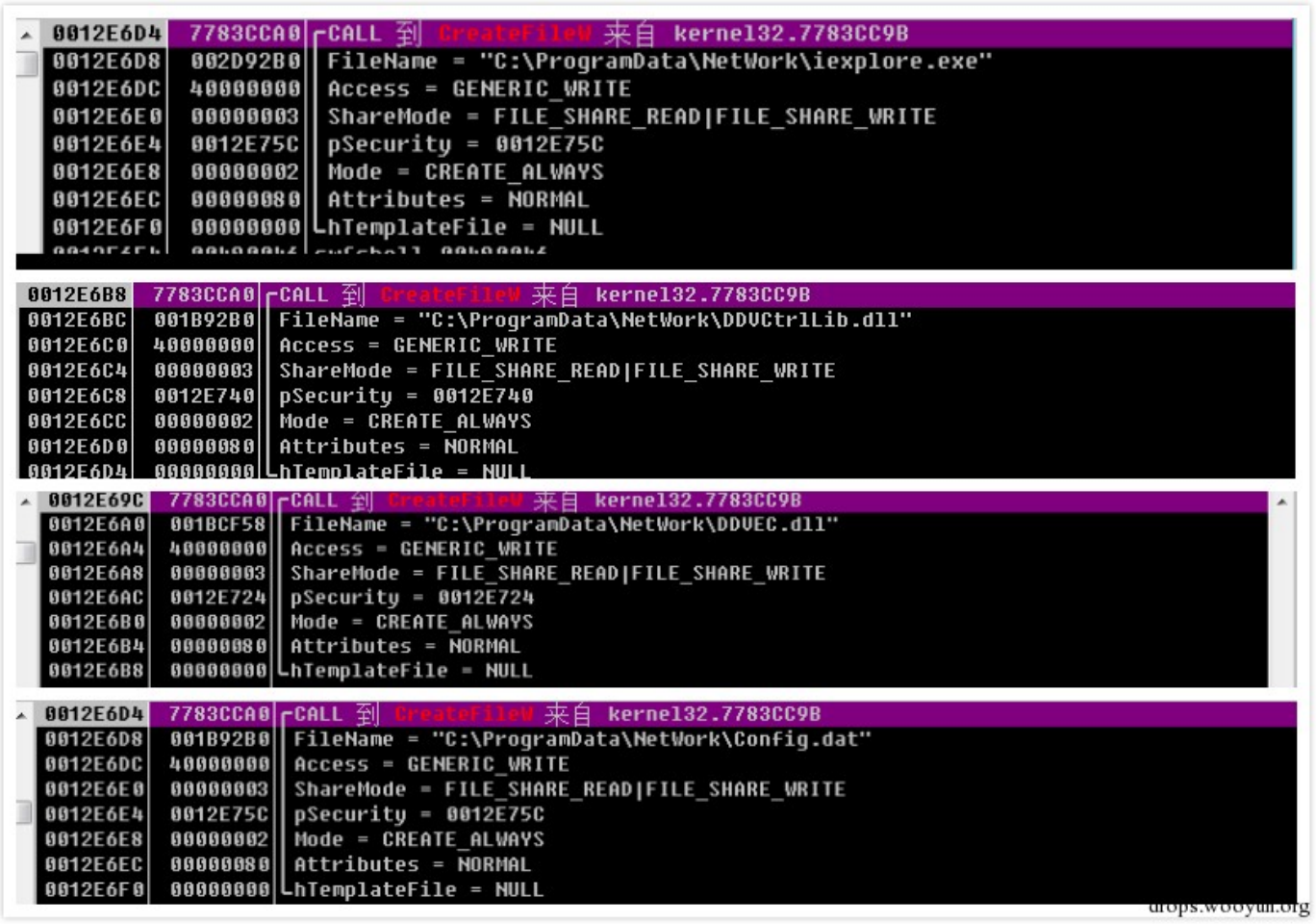
kxetray.exe 金山

ravmonf.exe 瑞星

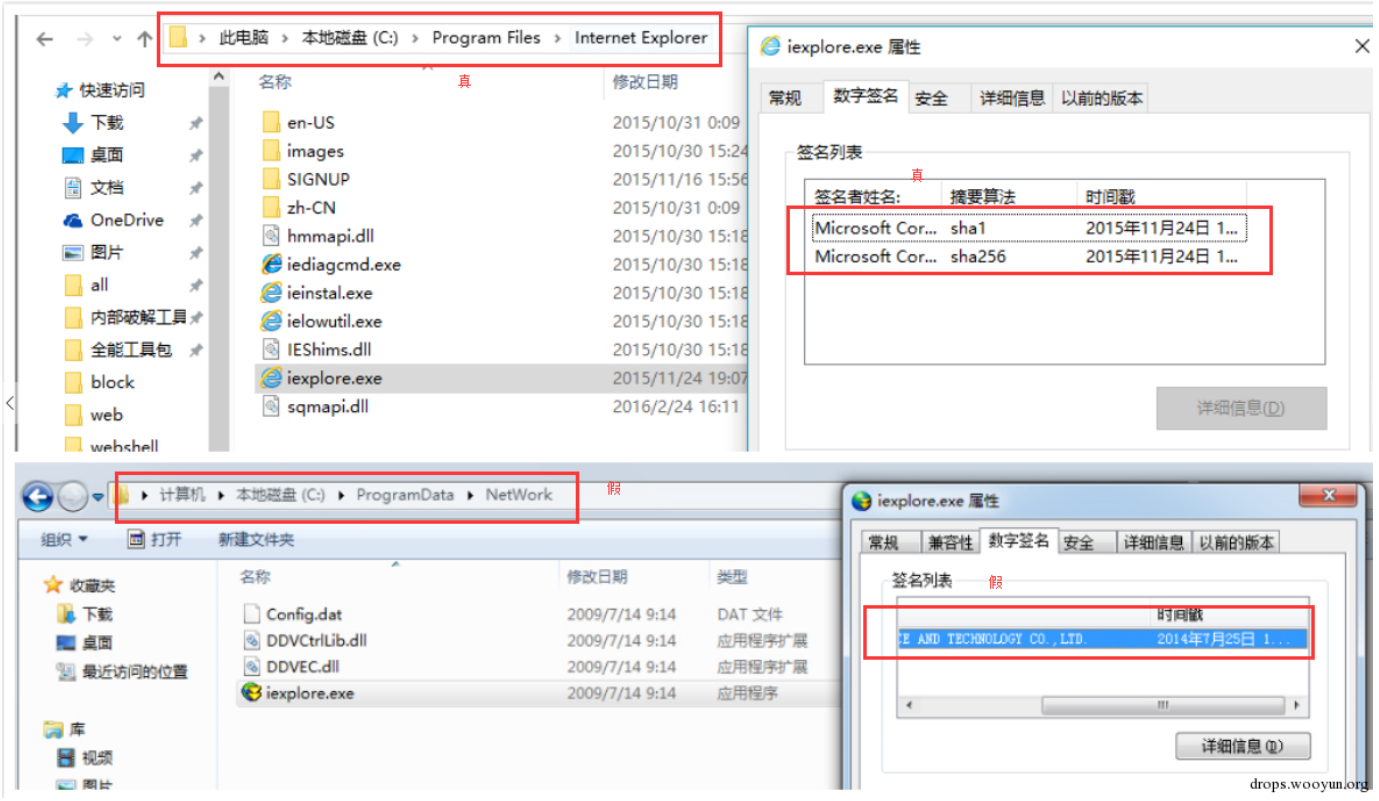
avp.exe 卡巴斯基

uiSeAgnt.exe 趋势科技

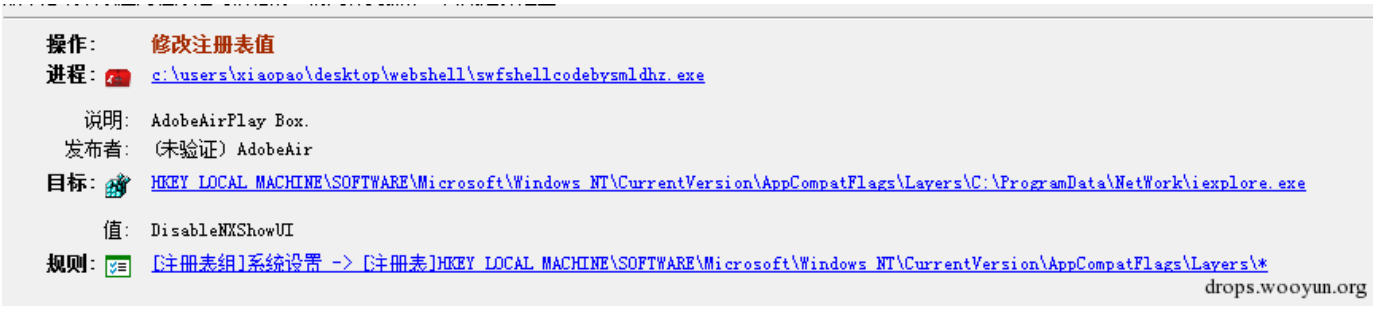
检测环境后就开始释放多个文件



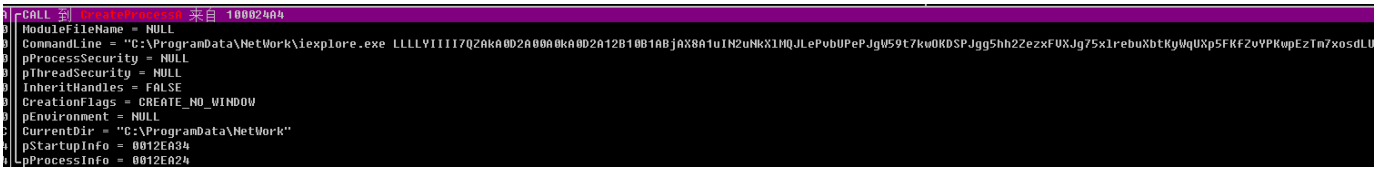
挂马者释放一个带数字签名的iexplore.exe，该程序带有9158(一个大型多人网络视屏平台)的数字签名。下图是正常iexplore和挂马者释放的iexplore的比较图。用白利用的方式绕过杀软的查杀



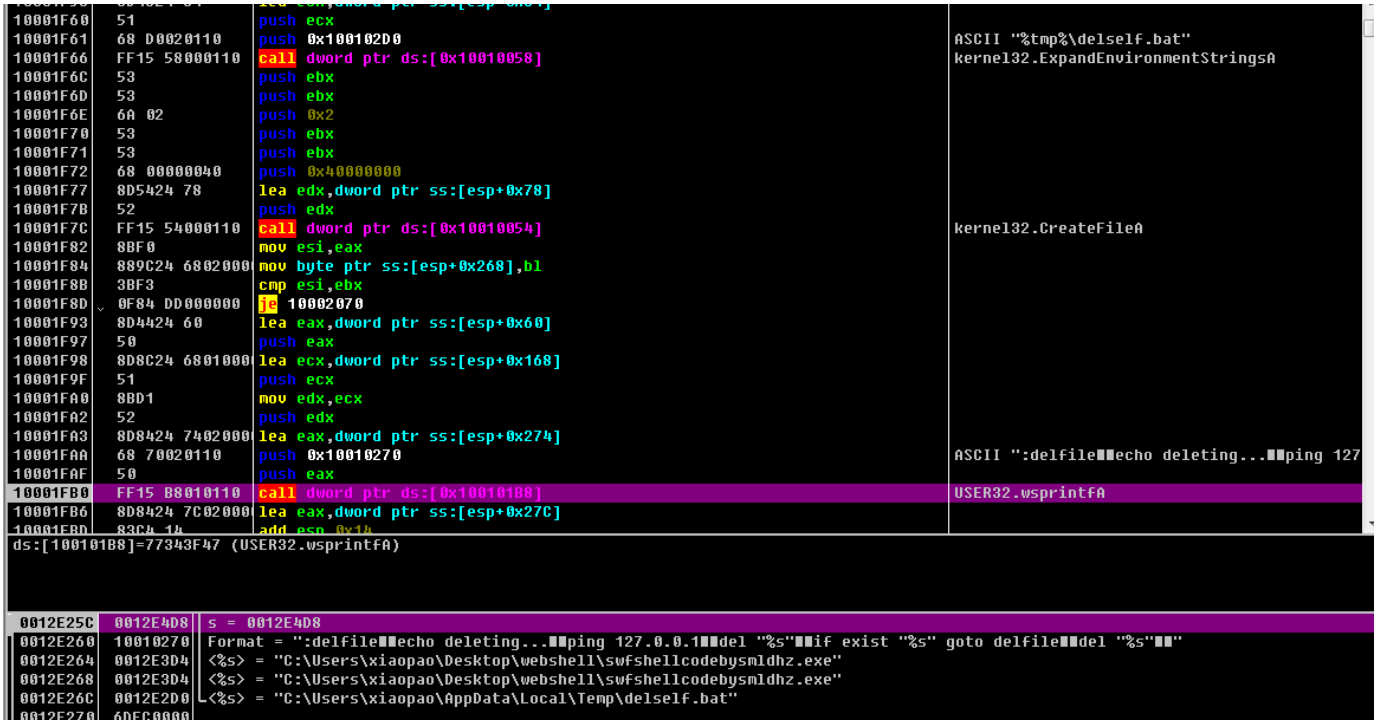
该挂马者通过让HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers 的键值指向新释放的iexplore处来来绕过UAC。达到以管理员权限的模式来启动“iexplore”



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

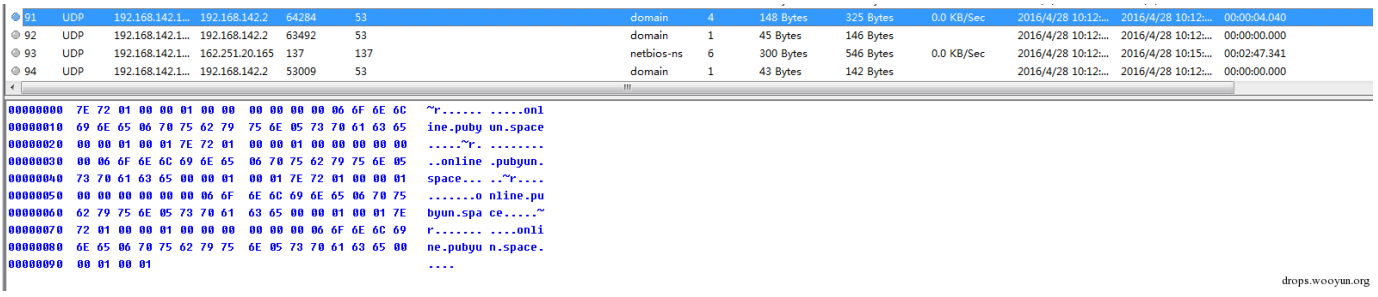
创建服务，使iexplore在用户电脑启动的时候以服务的形式自启动。以服务的形式启动一般情况下很难察觉出中招了。因为电脑平时有很多个svchost进程。

写完在服务后就以服务的方式启动程序

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  v40D986(&v25, v15);
8  if ( *((_DWORD *)v25 - 2) )
9  {
0    *(_DWORD *)(a3 + 136) = inet_addr(v25);
1    v23 = 1;
2  }
3  v40D7F4((#70 *)&v25);
4  if ( !v23 )
```


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。

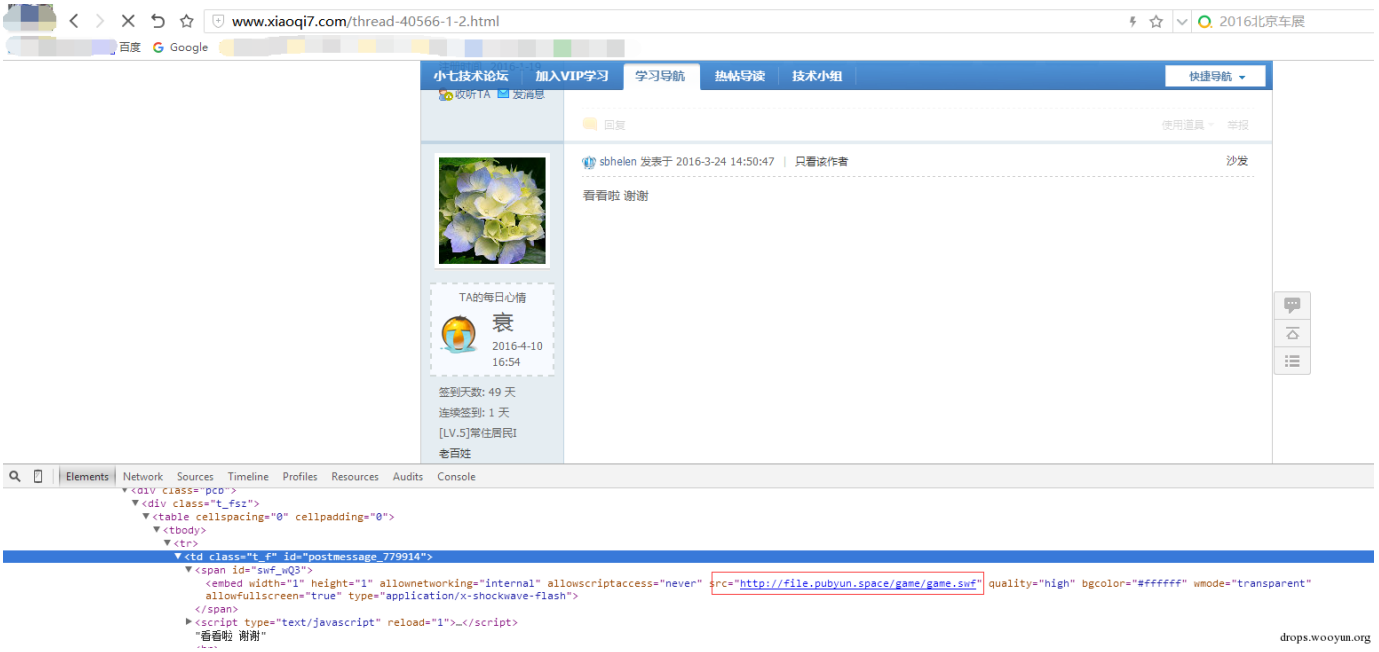


信息追踪

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。

这个是该挂马者在小七论坛上挂马截图，就一个简简单单的回复，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

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。

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

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

在该挂马者的论坛上，我们找到一个卖远控的群

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

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

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。