“小马激活”病毒新变种分析报告

火绒博锐（北京）科技有限公司

一、概述

随着安全软件与病毒之间攻防对抗的不断白热化，病毒的更新换代也日益频繁，其所使用的手段也日趋多样化。以最近大范围流行的“小马激活”病毒为例，其传播至今，据火绒发现的样本中已经演变出了五个变种。“小马激活”病毒，我们之前称其为“苏拉克”病毒，因为其核心驱动名为“surak.sys”故得此名，但是随着其不断地改变与安全软件的对抗方式，“苏拉克”这个名字已经不被病毒作者使用，所以我们将其统称为“小马激活”病毒。

“小马激活”病毒的第一变种只是单纯地在浏览器快捷方式后面添加网址参数和修改浏览器首页的注册表项，以达到首页劫持的目的。由于安全软件的查杀和首页保护功能，该版本并没有长时间流行太长时间。其第二变种，在原有基础上增强了与安全软件的对抗能力。由于其作为“系统激活工具”具有入场时间较早的优势，使用驱动与安全软件进行主动对抗，使安全软件无法正常运行。在其第三个变种中，其加入了文件保护和注册表保护，不但增加了病毒受害者自救的难度，还使得反病毒工程师在处理用户现场时无法在短时间之内发现病毒文件和病毒相关的注册表项。其第四个变种中，利用 WMI 中的永久事件消费者（ActiveScriptEventConsumer）注册恶意脚本，利用定时器触发事件每隔一段时间就会执行一段 VBS 脚本，该脚本执行之后会在浏览器快捷方式后面添加网址参数。该变种在感染计算机后，不会在计算机中产生任何文件，使得病毒分析人员很难发现病毒行为的来源，大大增加了病毒的查杀难度。通过如下表格我们可以更直观的了解其发展过程：

	主要传播时间	病毒行为	对抗方式
第一代	2015 年 9 月 至 2015 年 12 月	• 流量劫持： 1) 修改浏览器快捷方式	• 无
第二代	2015 年 12 月 至 2016 年 2 月	• 进程入侵 1) 将病毒动态库注入 explorer.exe 进程 • 流量劫持 1) 修改浏览器快捷方式 2) 通过驱动劫持首页	• 禁止安全软件加载驱动
第三代	2016 年 2 月 至 2016 年 3 月	• 进程入侵 1) 将病毒动态库注入 explorer.exe 进程 • 流量劫持 1) 修改浏览器快捷方式 2) 通过驱动劫持首页	• 禁止安全软件加载驱动 • 随机驱动名 • 文件保护 • 注册表保护

第四代	2016 年 3 月 至 2016 年 4 月	• 流量劫持： 1) 利用 WMI 脚本，定时修改浏览器快捷方式	• 病毒行为在 WMI 脚本进行，本地无其病毒文件
第五代	2016 年 4 月至今	• 进程入侵 1) 将病毒动态库注入 explorer.exe 进程 • 流量劫持 1) 修改浏览器快捷方式 2) 通过注入 explorer.exe 中的动态库劫持浏览器首页 3) 修改注册表锁定浏览器首页	• 每次重启后重新生成随机驱动名 • 文件保护 • 注册表保护

表 1、 “小马激活”病毒发展过程

通过我们近期接到的用户反馈，我们发现了“小马激活”病毒的新变种。该变种所运用的对抗技术十分复杂，进一步增加了安全软件对其有效处理的难度，甚至使得病毒分析人员通过远程协助处理用户现场变得更困难。这个“小马激活”病毒的最新变种运行界面如下：

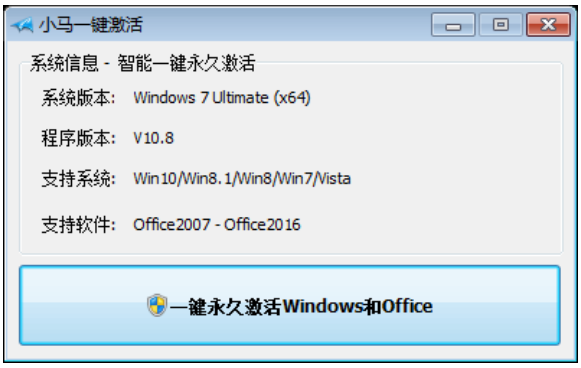

图 1、 “小马激活”新变种运行界面

二、样本分析

该病毒释放的驱动文件通过 VMProtect 加壳，并通过过滤驱动的方式拦截文件系统操作（图 2），其目的是保护其释放的动态库文件无法被删除。通过文件系统过滤驱动，使得系统中的其他进程在打开该驱动文件句柄时获得却是 tcpip.sys 文件的句柄，如果强行删除该驱动文件则会变为删除 tcpip.sys 文件，造成系统无法正常连接网络。我们通过下图可以看到火绒剑在查看文件信息时，读取的其实是 tcpip.sys 文件的文件信息。由于此功能，使得病毒分析人员无法在系统中正常获取该驱动的样本。

驱动名称	类型	修改位置	目标地址	目标位置	目标模块	公司名	描述
\FileSystem\NTFS	Attach	NTFS.sys!<unnamed>	0xFFFFF800F754A3EC	hkszbytsi.sys!<unnamed>	C:\WINDOWS\system32\drivers\hkszbytsi.sys	Microsoft Corporation	TCP/IP Driver
\FileSystem\NTFS	Attach	NTFS.sys!<unnamed>	0xFFFFF800F754A3EC	hkszbytsi.sys!<unnamed>	C:\WINDOWS\system32\drivers\hkszbytsi.sys	Microsoft Corporation	TCP/IP Driver
\FileSystem\NTFS	Attach	NTFS.sys!\Ntfs	0xFFFFF800F754A3EC	hkszbytsi.sys!<unnamed>	C:\WINDOWS\system32\drivers\hkszbytsi.sys	Microsoft Corporation	TCP/IP Driver
关机通知	0xFFFFF880064879B0	tplink.sys!IRP_MJ_CREATE	[\Device\ffert (0xFFFFFA800E4FE060)]	数字签名文件	C:\Windows\system32\drivers\tplink.sys	Microsoft Corporation	TCP/IP Driver

图 2、文件驱动钩子和关机通知

该驱动通过注册关机回调（图 2）在系统关机时该驱动会将自身在%SystemRoot%\System32\Drivers 目录重新拷贝成随机名字的新驱动文件，并将驱动信息写入注册表，以便于下一次时启动加载。在驱动加载之后，其会将 locc.dll 注入到 explorer.exe 进程中。该驱动对 locc.dll 文件也进行了保护，当试图修改或者删除该动态库时，会弹出错误提示“文件过大”。如图 3 所示：

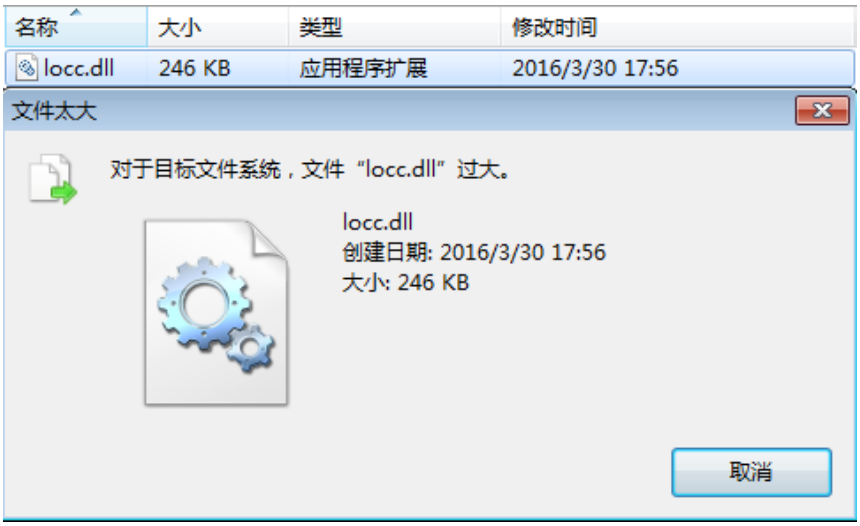

图 3、文件驱动钩子和关机通知

当病毒的驱动将 locc.dll 注入到 explorer.exe 进程后会执行首页劫持相关逻辑。通过火绒剑的内存转储，我们可以看到该病毒锁定的所有网址。

- http://qd.227237.com/?sg_64

- http://qd.227237.com/?360js_64
- http://qd.227237.com/?sjzc_64
- http://qd.227237.com/?hh_64
- http://qd.227237.com/?op_64
- http://qd.227237.com/?gg_64
- http://qd.227237.com/?pg_64
- http://qd.227237.com/?ay_64
- http://qd.227237.com/?2345_64
- http://qd.227237.com/?bd_64
- http://qd.227237.com/?lb_64
- http://qd.227237.com/?qq_64
- http://qd.227237.com/?114_64
- http://qd.227237.com/?115_64
- http://qd.227237.com/?tb_64
- http://qd.227237.com/?jz_64
- http://qd.227237.com/?sy_64

通过抓取上述网址中的网页信息（图 4），我们可以发现上述网址中存放的其实是一个跳转页。通过使用跳转页面，病毒作者可以灵活调整计费链接和推广网址，并且对来自不同浏览器的流量进行分类统计。

```
1  <meta http-equiv='refresh' content='0.0; url=https://web.sogou.com/?12[redacted]0'>
2  <div style='display:none'>
3  <script src='http://s95.cnzz.com/z_stat.php?id=1258001121&web_id=1258001121' language='JavaScript'></script>
4  <script src='http://s4.cnzz.com/z_stat.php?id=1258001060&web_id=1258001060' language='JavaScript'></script>
5  </div>
```

图 4、网页内容

三、信息追踪

通过测试我们现有的最新该病毒样本，我们发现该病毒不但推广了国内的一些导航站和电商门户网站（图 5），还推广了仿冒的小马激活网站（www.xiaomajihuo.net）用来进一步传播病毒。其推广网址如下：

- 淘宝特卖：temai.taobao.com
- Hao123 网址导航：cn.hao123.com
- 京东商城：www.jd.com
- 淘宝聚划算：ju.taobao.com
- 2345 影视大全：v.2345.com
- 爱淘宝：ai.taobao.com
- 爱美眉：www.aimm.cc
- 仿冒的小马激活网站：www.xiaomajihuo.net

图 5、病毒推广效果图

仿冒的小马激活网站访问效果如下：

图 6、网址访问效果图

病毒下载地址为百度云盘下载链接，如下图所示：

图 7、百度云盘链接访问效果图

通过反查仿冒的“小马激活”官网（xiaomajihuo.net）域名，我们找到了其域名注册时使用的邮箱——vo******o@enamewhois.com。通过该邮箱，我们找到了所有使用该邮箱注册的域名信息。如下图所示：

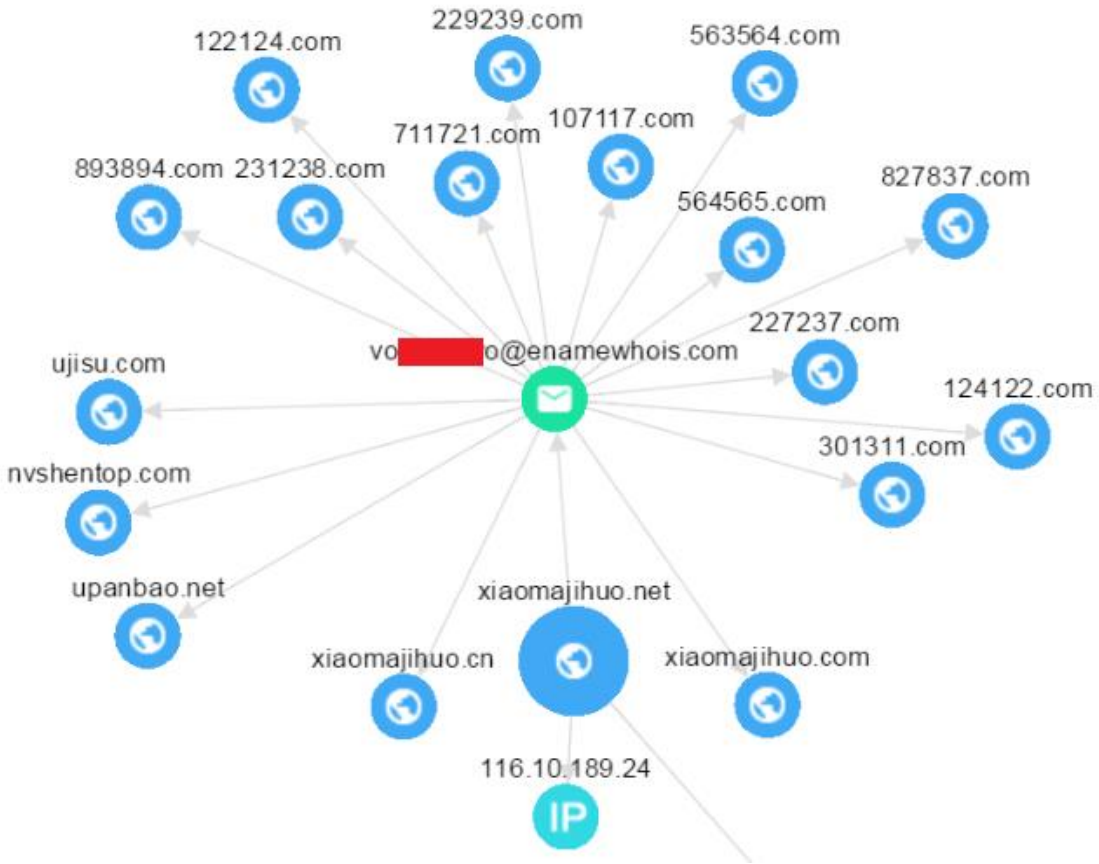

图 8、使用 vo******o@enamewhois.com 邮箱注册的域名关系图

通过访问上述关系图中的域名，我们发现：

- 该“病毒推广公司”利用“小马激活”病毒进行推广，利用多个仿冒小马激活官网在互联网中进行传播。
- 6 位数字加“.com”结尾的域名（下文称数字域名）中用来架设其首页劫持要用到的跳转页面。

由于我们通过“xiaomajihuo.net”域名可以获取的信息比较有限，我们对关系网中（上图所示）的“xiaomajihuo.cn”域名进行了反查。我们发现有超过 50 个域名指向这一 IP 地址，如下图所示：

指向同一IP的域名列表

域名	域名
xiaomajihuo.com.cn	www.xiaomajihuo.com.cn
xiaomajihuo.org.cn	www.xiaomajihuo.org.cn
xiaomajihuo.cn	www.xiaomajihuo.cn
gjssb.com	www.gjssb.com
hlbfs.com	www.hlbfs.com
hrxwh.com	www.hrxwh.com
ksqdq.com	www.ksqdq.com
rymsq.com	www.rymsq.com
xiaomajihuo.com	www.xiaomajihuo.com
xmhdss.com	www.xmhdss.com
xmhxhc.com	www.xmhxhc.com
xmhycx.com	www.xmhycx.com
xmjrhb.com	www.xmjrhb.com
xmjwlx.com	www.xmjwlx.com
xmktpd.com	www.xmktpd.com
xmlflc.com	www.xmlflc.com
xmshyf.com	www.xmshyf.com
xmsqjd.com	www.xmsqjd.com
xmxyzx.com	www.xmxyzx.com
xmzdsj.com	www.xmzdsj.com
xmzjsp.com	www.xmzjsp.com
xmzrct.com	www.xmzrct.com
ydjph.com	www.ydjph.com
yrdqm.com	www.yrdqm.com
ytjdl.com	www.ytjdl.com
www.xiaomajihuo.net	

图 9、同一 IP 下的域名列表

观察这些域名，很容易发现有多个域名带有“xiaomajihuo”的字样。在这些域名中，还有很多 XM 开头的域名，我们猜测其本意应为“小马”的拼音缩写。在对其关联网址进行访问时我们发现：

带有“xiaomajihuo”字样的网址全部都是仿冒的“小马激活”官网，其网页样式与前文提到的“www.xiaomajihuo.net”样式相同。

XM 开头的所有网址都为该病毒的下载页面，其网页样式模仿了当前的主流下载站，具有很强的迷惑性（图 10）。

图 10、网页访问效果图

在网址 www.ydjph.com 和 www.yrdqm.com 中，我们发现虽然页面样式相同，下载文件名为“win7 activation v1.8”，根据我们的分析，该样本也同为该病毒，其下载地址也为百度云盘链接，链接地址为“pan.baidu.com/s/1o79KKII”。

在域名列表中的其他域名，虽然看上去名字随机性很强，但是我们通过访问其页面后发现如下网址为该“病毒生产厂商”的业务推广站：

- www.hrxwh.com
- www.rymsq.com
- www.gjssb.com
- www.hlbfs.com

就在正在完成这份文档的同时，最后两个域名内容已经变为了类似图 10 的病毒下载页面。

根据工商局企业查询系统和搜索引擎的查询结果，上述网址中出现的公司经营范围均为传统行业，且均有正规官网。所以上述网址中出现的公司名为盗用（图 11），用来扰乱人们视线。其公司服务项目中涵盖了广告推广、网页制作、软件开发和技术支持（图 12），这与“小马激活”病毒的首页劫持推广功能相吻合，即该病毒就是该“病毒推广公司”的广告推广工具之一。如下图所示：

图 11、其盗用的公司名

图 12、“病毒推广公司”的业务推广站

在同一 IP 下还有两个软件推广网址，分别推广 QQ 浏览器（图 13）和 2345 浏览器（图 14），其推广域名如下。

- www.ytjdl.com
- www.ksqdq.com

软件推广网址如下图所示：

图 13、该 IP 下的 QQ 浏览器推广网址

图 14、该 IP 下的 QQ 浏览器推广网址

我们进一步查询了“xiaomajihuo.com.cn”域名信息的相互联系（图 15），我们不难发现与该域名相关的大部分仿冒的小马激活网站都是使用“as*****0@qq.com”这个 QQ 邮箱进行注册。通过对其 QQ 邮箱的查询，我们定位到了该病毒作者的 QQ 号码为 133*****7，名叫“叶*”。

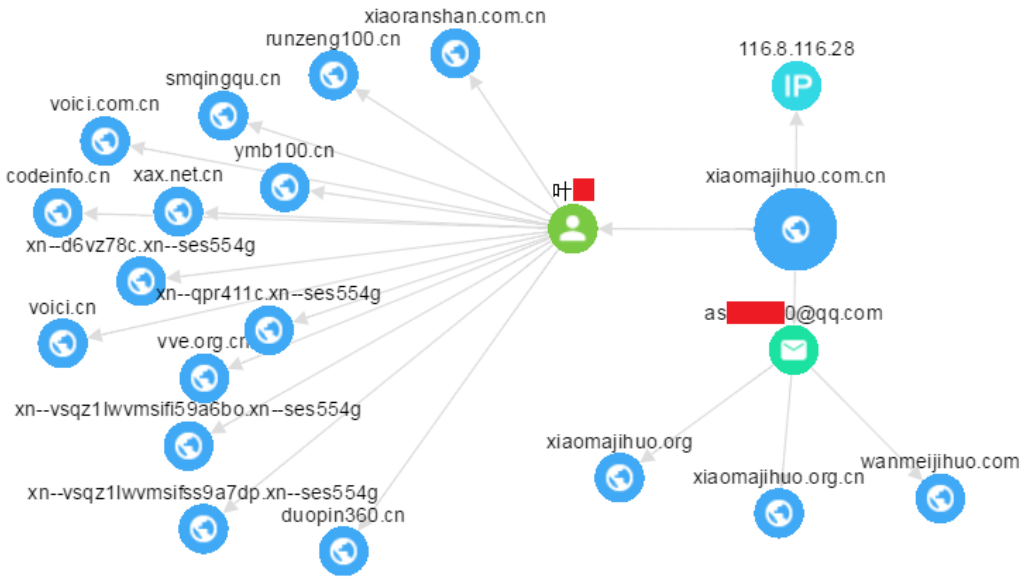

图 15、xiaomajihuo.com.cn 域名信息联系图

样本在执行过程中还访问了网址“tongji.227237.com”,通过访问该网址我们了解到在该域名所在服务器中架设着一套“推广流量监控系统”（图 16），所有其推广的流量都会先经过该站，以用于其查看推广效果。

图 16、该病毒的流量统计系统

根据这些线索，我们理清了该“恶意推广”业务的主要流程。其首先制作系统激活工具作为其“恶意推广工具”，之后再通过百度推广等推广方式进行大范围扩散，在用户

运行这些程序之后，将用户首页劫持为数字域名，在该域名下的网页中加入跳转网址和付费链接，最终以推广互联网公司的产品或主页进行谋利。

为了躲避安全软件的网址拦截，其申请的数字域名变动非常频繁，大部分数字域名已经无法访问，现在依然可以存活的跳转站除了上文中提到的“227237.com”还有“827837.com”和“107117.com”，他们分别是“爱淘宝”和“搜狗网址导航”的推广链接，如下图所示：

```
<link rel="shortcut icon" href="favicon.ico" />
<meta http-equiv="refresh" content="0.1; url=http://www.301311.com/go/taobao.html">
<div style="display:none">
    <script src="http://s4.cnzz.com/z_stat.php?id=1256694901&web_id=1256694901" language="JavaScript"></script>
</div>
```

图 17、827837.com 下跳转页内容

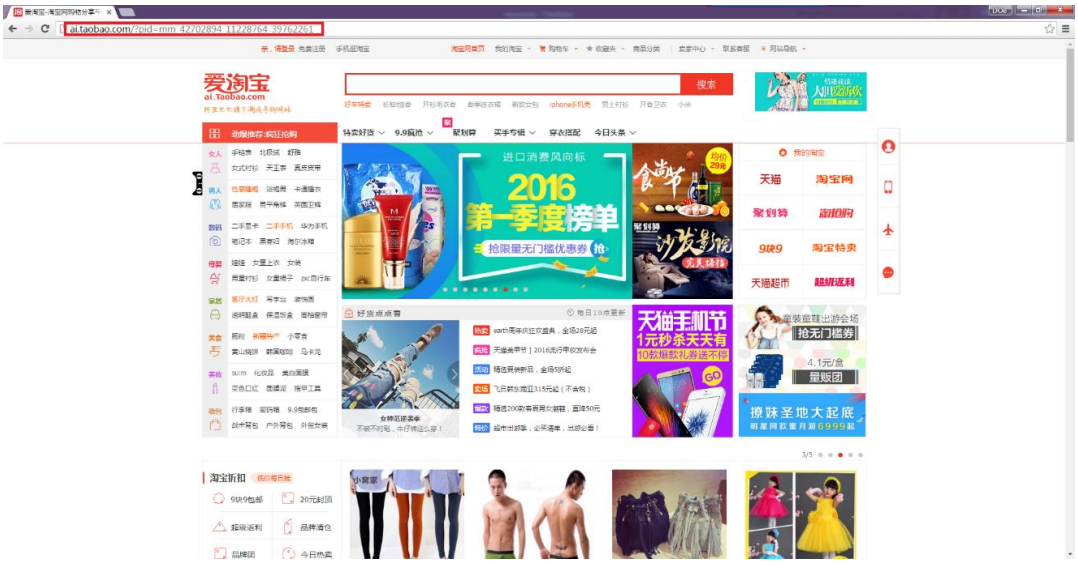

图 18、827837.com 推广“爱淘宝”效果图

```
<meta http-equiv='refresh' content='0.0; url=https://web.sogou.com/?12[redacted]9'>
<meta http-equiv="Content-Type" content="text/html; charset=gb2312" />
<title>搜狗网址导航</title>
<div style='display:none'>
<script src="http://s4.cnzz.com/z_stat.php?id=1256195762&web_id=1256195762" language="JavaScript"></script>
<script src="http://s11.cnzz.com/z_stat.php?id=1256694671&web_id=1256694671" language="JavaScript"></script>
</div>
```

图 19、107117.com 下跳转页内容

图 20、107117.com 推广“搜狗网址导航”效果图

通过上述信息，我们可以清楚看到，绝大部分推广的网址都来自于国内的大型互联网企业，阿里巴巴、京东商城这种超大型网络公司甚至也在其中之列。由于当今国内互联网企业之间的竞争日益激烈，国内的大型互联网公司为了推广自己的产品更是可以“豪掷千金”，这一现象极大地刺激了“广告推广公司”的迅速壮大，其推广手段也不断翻新，更有甚者制作病毒进行广告推广，使得国内的互联网大环境中广告类病毒（Adware）的种类与传播范围在短时间之内迅速增加。普通用户在使用计算机时只要 “稍有疏忽”就会被捆绑上许多自己本不需要的应用，或者是首页被随意修改、浏览网页时被加上广告。广大用户深受其害，但是某些软件厂商不但没有加大推广商的审查力度，反而为了提高推广“成功率”提高了其软件的 “卸载难度”，使用户更加苦不堪言。我们从而可以得出结论，广告推广商与“病毒生产厂商”之间存在很大的交集，这些“病毒推广公司”的推广业务主要服务于国内的主流互联网企业并不断地从中谋取暴利。利用这种盈利模式，“病毒推广公司”可以不断推动其黑色链条的运转，对互联网行业的健康发展造成十分恶劣的影响。

最后，我们在工信部的《ICP/IP 地址/域名信息备案管理系统》上找到了与“vo******o@enamewhois.com”邮箱相关网站的 ICP 备案信息，我们以域名备案时间为主轴，梳理出了其“病毒推广公司”的主要成员信息及关键运营过程。

2015 年 7 月 13 日，葛**首先备案了网站域名“301311.com”和上文中提到的“爱淘宝”推广网址“827837.com”（图 21）。“301311.com”域名的“go”目录下存放着众多被推广的网址跳转页。这与该类型第一个变种出现的时间基本吻合。

主办单位名称	主办单位性质	网站备案/许可证号	网站名称	网站首页网址	审核时间
葛[redacted]	个人	黔ICP备15010128号-2	我的301311网	www.301311.com	2015-07-13
主办单位名称	主办单位性质	网站备案/许可证号	网站名称	网站首页网址	审核时间
葛[redacted]	个人	黔ICP备15010128号-3	我的827837网	www.827837.com	2015-07-13

图 21、葛**备案的网站信息

2015 年 9 月 21 日，殷**备案了网站域名“ujisu.com”和“231238.com”（图 22）。前者为“U 盘极速启动”官网，该工具可用于制作 U 盘启动盘。火绒希望广大用户在使用操作系统或者软件时可以支持正版，谨慎对待此类工具。与后者同时备案的同一类型域名还有很多，但都已无法访问。

主办单位名称	主办单位性质	网站备案/许可证号	网站名称	网站首页网址	审核时间
殷[redacted]	个人	赣ICP备15008514号-2	数据线导航网	www.231238.com	2015-09-21
主办单位名称	主办单位性质	网站备案/许可证号	网站名称	网站首页网址	审核时间
殷[redacted]	个人	赣ICP备15008514号-1	U极速	www.ujisu.com	2015-09-21

图 22、殷**备案的网站信息

2015 年 12 月 9 日，杨**使用“上海******有限公司”的公司名备案了域名“xiaomajihuo.com”和“227237.com”（图 23）。前者为仿冒的小马激活官网，该网址现在已无法访问，后者域名架设着其“推广流量监控系统”，所以初步推断其可能为该“病毒推广公司”的主要成员。


ICP备案主体信息

备案/许可证号：	沪ICP备15044716号	审核通过时间：	2015-12-09
主办单位名称：	上海[redacted]有限公司	主办单位性质：	企业

ICP备案网站信息

网站名称：	最美优出	网站首页网址：	www.227237.com
网站负责人姓名：	杨[redacted]	网站域名：	227237.com
网站备案/许可证号：	沪ICP备15044716号-7	网站前置审批项：	

ICP备案主体信息

备案/许可证号：	沪ICP备15044716号	审核通过时间：	2015-12-09
主办单位名称：	上海[redacted]有限公司	主办单位性质：	企业

ICP备案网站信息

网站名称：	优出网	网站首页网址：	www.xiaomajihuo.com
网站负责人姓名：	杨[redacted]	网站域名：	xiaomajihuo.com
网站备案/许可证号：	沪ICP备15044716号-4	网站前置审批项：	

图 23、杨**备案的网站信息

由于 2016 年初，国内很多安全厂商对“小马激活”进行了全面查杀，其域名也被很多安全软件拦截。所以在 2016 年 1 月 13 日至 20 日，张**、叶*、陈*等人备案了如下

五个域名用于架设仿冒的小马激活官网（图 24）。其域名开放时间有很强的随机性，所以当安全厂商认为其域名已经废弃，并将拦截记录“优化”掉的时候，其域名很有可能会再次“复活”。

- xiaomajihuo.cn
- xiaomajihuo.net
- xiaomajihuo.com.cn
- xiaomajihuo.org
- xiaomajihuo.org.cn

ICP备案主体信息			
备案/许可证号：	沪ICP备15044239号	审核通过时间：	2016-01-13
主办单位名称：	[redacted]（上海）[redacted]有限公司	主办单位性质：	企业
ICP备案网站信息			
网站名称：	[redacted]	网站首页网址：	www.xiaomaijihuo.cn
网站负责人姓名：	孙[redacted]	网站域名：	xiaomajihuo.cn
网站备案/许可证号：	沪ICP备15044239号-6	网站前置审批项：	
ICP备案主体信息			
备案/许可证号：	沪ICP备15044239号	审核通过时间：	2016-01-13
主办单位名称：	[redacted]（上海）[redacted]有限公司	主办单位性质：	企业
ICP备案网站信息			
网站名称：	[redacted]	网站首页网址：	www.xiaomaijihuo.net
网站负责人姓名：	孙[redacted]	网站域名：	xiaomajihuo.net
网站备案/许可证号：	沪ICP备15044239号-7	网站前置审批项：	
ICP备案主体信息			
备案/许可证号：	沪ICP备16001668号	审核通过时间：	2016-01-15
主办单位名称：	叶[redacted]	主办单位性质：	个人
ICP备案网站信息			
网站名称：	平静的湖面	网站首页网址：	www.xiaomaijihuo.com.cn
网站负责人姓名：	叶[redacted]	网站域名：	xiaomajihuo.com.cn
网站备案/许可证号：	沪ICP备16001668号-6	网站前置审批项：	
ICP备案主体信息			
备案/许可证号：	沪ICP备16002459号	审核通过时间：	2016-01-20
主办单位名称：	陈[redacted]	主办单位性质：	个人
ICP备案网站信息			
网站名称：	雨打芭蕉烦	网站首页网址：	www.xiaomaijihuo.org
网站负责人姓名：	陈[redacted]	网站域名：	xiaomajihuo.org
网站备案/许可证号：	沪ICP备16002459号-8	网站前置审批项：	
ICP备案主体信息			
备案/许可证号：	沪ICP备16002459号	审核通过时间：	2016-01-20
主办单位名称：	陈[redacted]	主办单位性质：	个人
ICP备案网站信息			
网站名称：	遍地梧桐花	网站首页网址：	www.xiaomaijihuo.org.cn
网站负责人姓名：	陈[redacted]	网站域名：	xiaomajihuo.org.cn
网站备案/许可证号：	沪ICP备16002459号-5	网站前置审批项：	

图 24、2016 年 1 月 13 日至 20 日注册的假小马激活域名

2016 年 3 月 20 日，杨**在有关部门备案了域名“wanmeijihuo.com”（图 25）。至今为止，该域名并未启用，但根据备案时间我们初步推断，该域名很有可能为其下一“恶意推广产品”的主要传播渠道。针对该情况，火绒已经针对其域名进行了提前拦截。

主办单位名称	主办单位性质	网站备案/许可证号	网站名称	网站首页网址	审核时间
杨[redacted]	个人	沪ICP备16008094号-7	提灯寻梦忆	www.wanmeijihuo.com	2016-03-16

图 25、“wangmeijihuo.com”域名备案信息

为彻底查明事实真相，我们浏览了小马激活所谓的官方网站（www.pccppc.com），当进入其官网时页面最上方弹出了其“严正声明”，在其小马激活的下载专区我们发现其停止更新的公告。页面中还给出了其官方 QQ 群号，提示信息中写着“小马工具箱 V1.01 版已经发布”字样。如下图：

图 26、“小马激活官网”访问效果图

我们尝试加入该群，我们发现其群共享文件中并没有其所谓的“小马工具箱”，而是有两个最近一个月左右上传的“小马激活工具”，其文件上传者就是其 QQ 群的创建者（图 27-28），也就是其所谓“小马官方人士”上传。

图 27、小马激活官方 QQ 群文件共享展示图

图 28、群成员展示图

在下载时，我们发现文件刚刚落地就被火绒的下载扫描报毒（图 29）。经过我们进一步分析，其样本正是我们在概述中所提到的“小马激活”病毒的第四类变种。这些证据指明，原“小马激活工具”的制作团队可能与该病毒运作团队之间存在着直接关系。

图 29、火绒下载扫描效果图

我们通过上述所有跟踪分析，推断了该“病毒推广公司”的运作体系和业务结构。如下图所示：

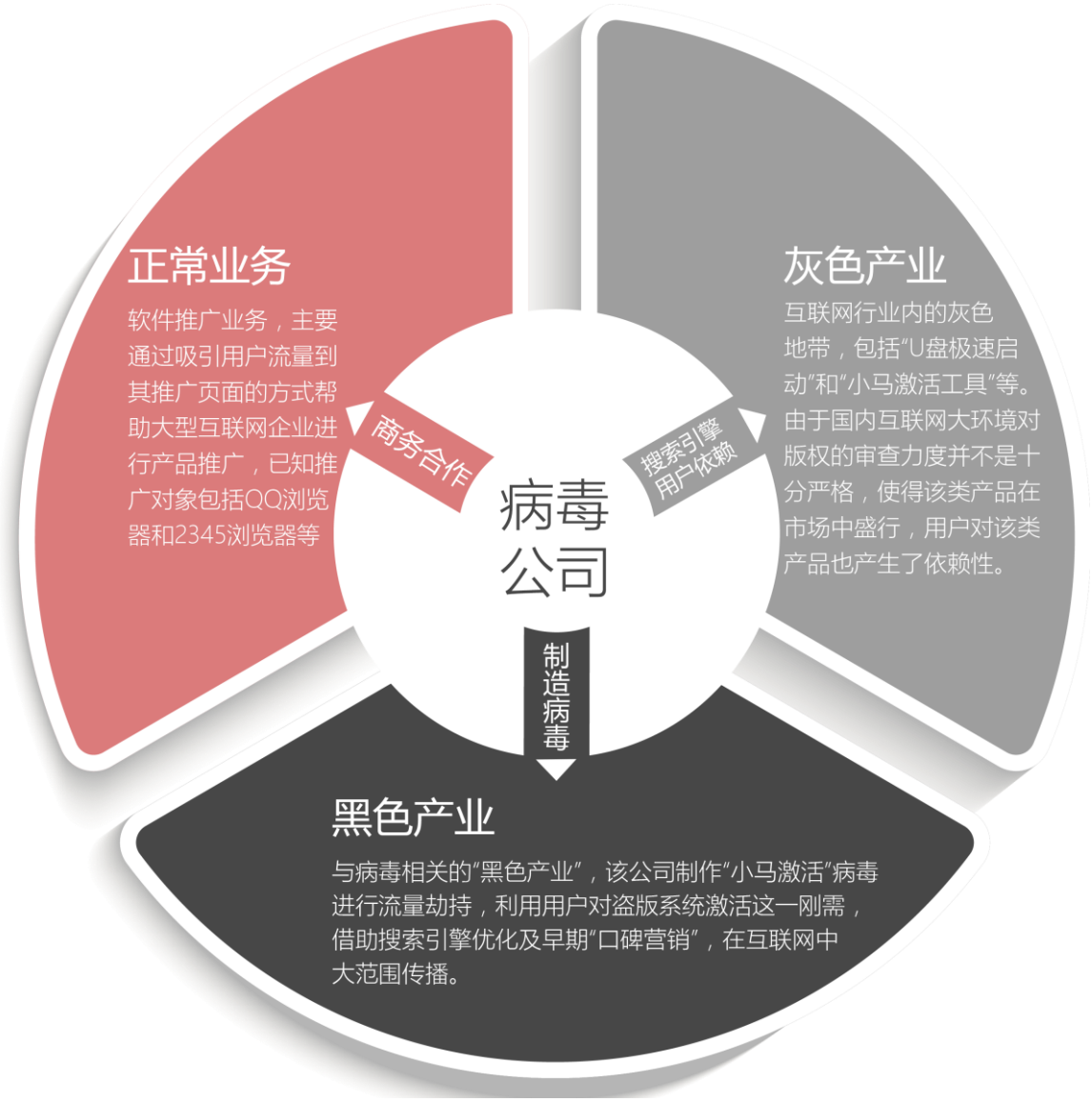

图 30、“病毒推广公司”的运作体系和业务结构图

该“病毒推广公司”涉及到“白、灰、黑”三个领域的业务。

- “白”：软件推广业务，主要通过吸引用户流量到其推广页面的方式帮助大型互联网企业进行广告推广，已知推广对象包括 QQ 浏览器和 2345 浏览器等；
- “灰”：互联网行业内的灰色地带，包括“U 盘极速启动”和“小马激活工具”。由于国内互联网大环境对于版权的审查力度并不是十分严格，使得该类产品在市场中盛行，用户对该类产品也产生了依赖性；

- “黑” ：与病毒相关的“黑色产业”，该公司制作“小马激活”病毒进行流量劫持，利用用户对盗版系统激活这一刚需，借助搜索引擎优化及早期“口碑营销”，在互联网中大范围传播；

四、综述

随着国内互联网企业之间的竞争进入白热化，产品推广作为最接近市场的最后环节成为各大软件厂商用来竞争的众矢之的。国内的各个互联网公司不惜一切代价地向市场推广自己的软件产品，由于受到利益驱使软件推广商在推广力度上不断加大，最终跨过网络安全的红线，制作病毒推广工具进行广告推广。作为收益方，被推广的互联网企业也并没有在发现这一现象后及时制止，而是继续为这些“病毒推广厂商”所提供的服务买单，促使了整个黑色产业链条的形成。

对于“小马激活”病毒，在国内安全厂商开始对其进行全面查杀时，其贼喊抓贼、监守自盗，使很多用户甚至安全厂商都蒙在鼓里。其利用用户的长期信任与用户对于系统激活工具的麻痹大意，使得该病毒在短时间之内大范围传播。其使用十分恶劣的手段进行广告推广，严重影响了用户对计算机的正常使用，甚至对互联网行业的发展造成了不良影响。放眼中国互联网市场，“小马激活”病毒也只是 “病毒推广”黑色产业链中的一个缩影，类似于“小马激活”病毒制作团体的“病毒推广厂商”还有很多。究其本质，监管力度不足和被推广的互联网企业对于推广手段的放任、不作为才是造成“病毒推广厂商”肆意妄为的主要原因。

随着中国互联网热潮的到来，近年来崛起的互联网公司如同雨后春笋一般快速增多，人们的内心越来越浮躁，人们渐渐变得只看重结果不在乎过程，最终舍本逐末，变成了追逐利润的淘金工具。作为互联网企业，其本职工作应该是对于其产品及服务的精益求精，更多的是要为用户着想，因为我们的身上肩负着用户对我们的信任。