007 黑客组织及其地下黑产活动分析报告

主编　360 追日团队

360互联网安全中心

2015 年 12 月 9 日

摘　要

- 最早可以追溯到 2007 年开始进行制作并传播恶意代码等互联网地下产业链活动，一直活跃至今。
- 制作并传播的 Hook007 类样本 HASH 数量达到 17 万个，相关恶意代码云查询拦截次数达到 1.3 亿次，相关恶意代码主要以后门和盗号程序为主。
- 主要针对中国用户，累计受影响用户超过千万，单就 Hook007 家族统计近一年被感染用户达到 50 万。
- 相关初始攻击主要依托即时通讯工具（QQ\YY 等）采用社会工程学方法进行对特定对象进行攻击；相关攻击对象主要为网络游戏玩家等普通网民，另外对教育、金融领域有几次针对性攻击。
- 进一步攻击方式主要是将恶意代码伪装为图片、文档等发送给特定对象，另外是制作虚假游戏平台网站，网站提供伪装游戏平台（game456 等）安装包的恶意代码。
- 该组织持续与安全厂商进行对抗，至少针对包括 360 在内的 3 款国内安全软件，以及卡巴斯基、比特梵德等国外相关安全产品采取过针对性技术措施，对抗行为最早可以追溯到 2008 年。对抗手段从实体文件到通信协议进行相关对抗，主要针对本地静态扫描、云查杀、主动防御策略和网络层等环节的检测。另外值得注意的是该组织成员会主动将恶意代码上报给安全厂商，目的是申请将恶意程序添加白名单或者探测安全厂商检测机制。单就 Hook007 这个家族，我们对相关产品进行了多次升级或检测策略调整。
- 该组织主要以窃取用户数据、互联网资源与服务滥用进行牟利。经过推算作者单就 Hook007 这一种远控，每年至少获利超过百万。另外通过窃取用户数据和虚拟财产，造成每年普通网民财产损失逾千万元。Hook007 这条地下产业链获利总额已经过亿。
- 该组织相关成员分工明确，从制作恶意代码到最终获利组成了一条完整的地下产业链。主要包含制作恶意代码、传播、更新、获利等环节。

360互联网安全中心

目　　录

第一章　存在若干年的地下产业链活动

一、　关于 007 组织的产业链

我们从 2011 年开始发现 Hook007 家族恶意代码，通过我们的持续监控和分析，幕后庞大的黑客组织逐渐浮出水面，我们将该组织命名 007 组织。该组织最早从 2007 年开始进行制作并传播恶意代码，窃取用户数据、虚拟财产等互联网地下产业链活动，一直活跃至今。这是我们目前捕获到的影响范围最大，持续时间最长的地下产业链活动。

以 007 组织为主的地下产业链主要涉及商品是技术服务和恶意代码，该组织的核心商品是 Hook007 远程控制恶意代码，进一步主要包含制作恶意代码、传播、更新、获利等环节。Hook007 远程控制是该组织独立开发并进行持续的更新维护。007 组织具备严密完整的组织结构，其中核心成员主要为开发和一级代理销售，目前我们能明确掌握的是通过恶意代码这种商品的交易是该组织牟利的主要手段之一。相关恶意代码传播到最终通过窃取用户数据进行牟利这一环节我们可以确定是该地下产业链的一部分。

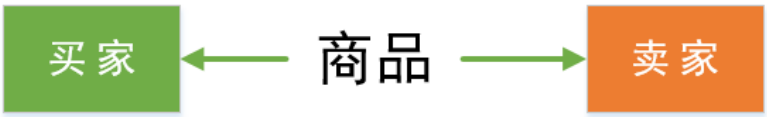


图 1 消费者与生产者基本关系

007 组织涉及的地下产业链中主要还是充当卖家（生产者）的角色。从下图商品分类中，可以看出 007 组织涉及的商品主要为恶意代码（远控、免杀等工具）和提供相关技术服务。另外该地下产业链中其他环节会包括数据信息、权限、漏洞等商品，但不是 007 组织主要涉及的商品类型。

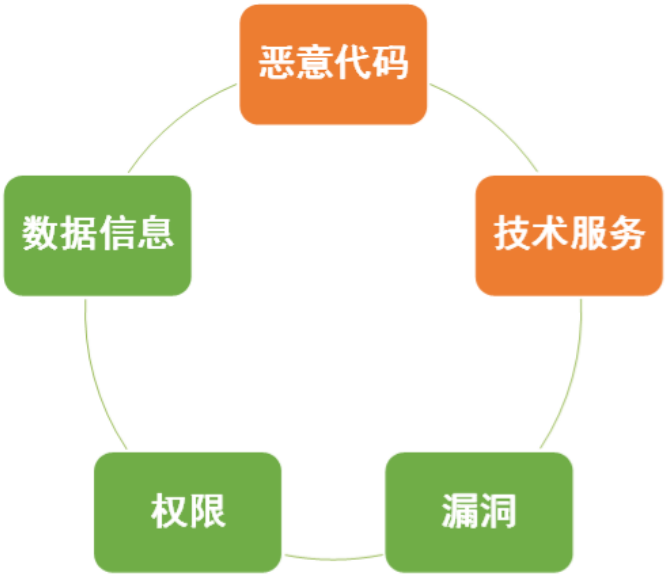


图 2 地下产业经济链体系中商品分类

二、 影响范围最大的地下产业链

007 组织相关攻击活动最早可以追溯到 2007 年，从 2011 年开始非常活跃。制作并传播的 Hook007 类样本 HASH 数量达到 17 万个，变种数量达到 66 种，相关恶意代码传播达到 1.3 亿次。另外我们近三个月捕获到该家族的免杀器版本已超过上百个，购买用户超过 600 个。该组织的相关攻击活动主要针对中国用户，累计受感染用户超过千万，单就 Hook007 家族统计近一年被感染用户达到 50 万。

该组织在攻击成功后会通过远程控制强行阻止用户操作游戏，并直接将用户的虚假财产、游戏装备进行交易转给盗号者帐号。另外该组织一直与安全厂商进行持续的对抗，从静态查杀、动态检测到网络不同层面进行躲避和对抗。

这是我们历年来捕获到的影响范围最大，持续时间最长的地下产业链活动。

三、 攻击目标

通过我们的研究分析可以得出，007 组织主要针对中国地区的用户，其中主要关注网络游戏玩家等普通网民。

另外对教育、金融领域有几次针对性攻击：

相关恶意代码原始文件名
2015 证券数据-验证.exe
2015 年注册化工工程师-验证.exe
2015 年重庆市社会工作员职业水平考试.exe
2015 年执业医师(临床).exe
2015 年山东地区第三季度会计从业.exe
2015 江苏第四季会计从业-部分验证.exe
2015cpa 注册会计师数据-验证.exe
15 年造价工程师-验证.exe
15 贵州会计从业数据.exe
15 高级职称考生报名.exe

表 1 相关恶意代码原始文件名

相关统计项	具体内容
开始时间	2014 年 10 月 10 日
结束时间	2015 年 10 月 10 日
被感染用户数量	500559 个
恶意代码数量	161581 个

表 2 Hook007 家族感染情况统计

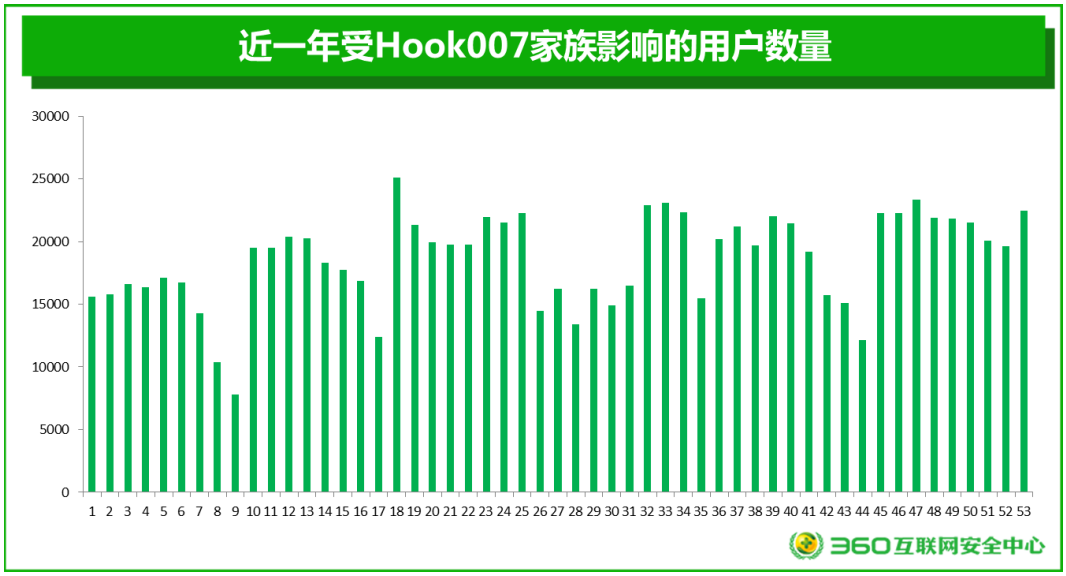


图 3 近一年受 Hook007 家族影响的用户数量

四、 攻击时间（变化趋势）

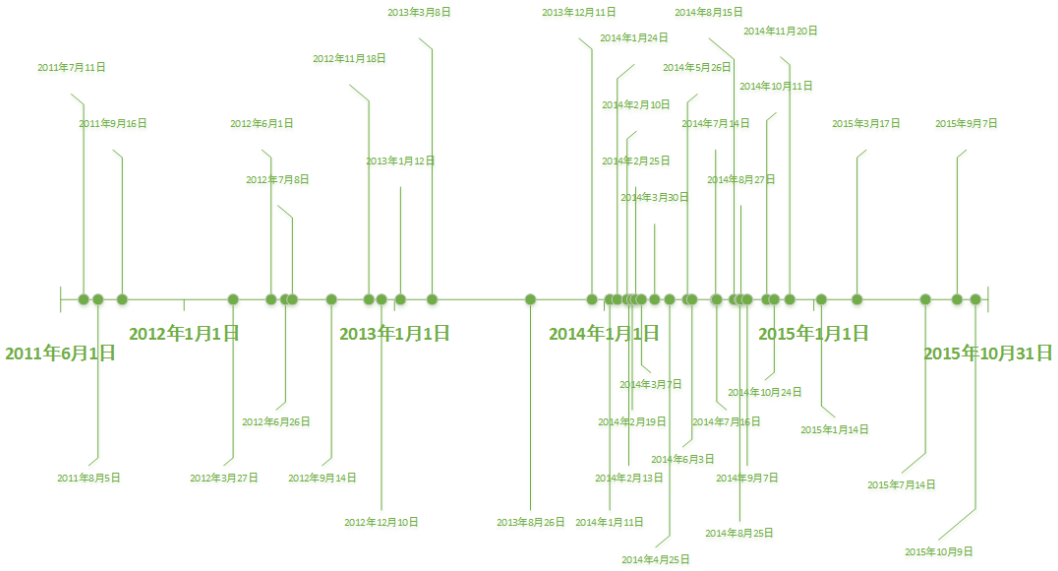


图 4 恶意代码更新记录

上图是我们就 Hook007 家族变化趋势的记录，每个时间点都是 Hook007 家族新增变种或者相关攻击方式或资源有重大变化的记录。

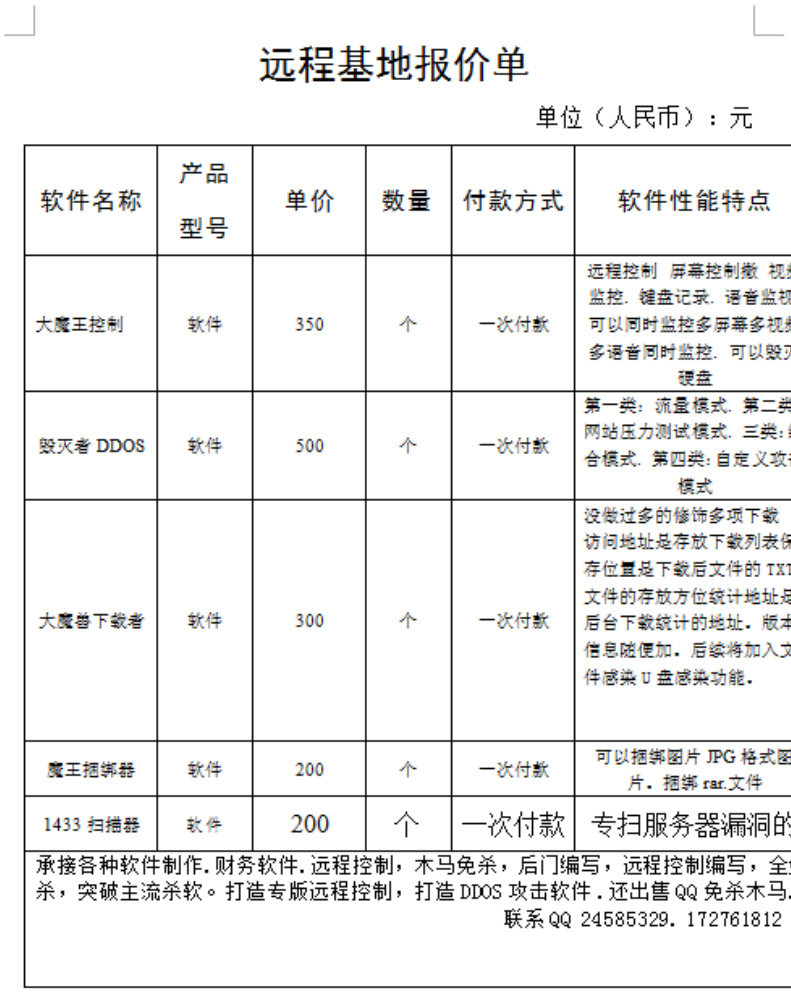
007 组织相关攻击活动最早可以追溯到 2007 年，而从 2011 年开始 Hook007 家族开始影响比较广泛，可以看出在 2014 年到 2015 年期间 Hook007 版本更新迭代非常频繁。

五、 牟利

（一） 恶意代码

恶意代码的制作和更新维护是 007 组织的核心业务。进一步相关类型主要是木马生成器、免杀和一些定制木马。作者每年单就 Hook007 这一种远程控制恶意程序获利就已超过百万。

下图是我们截获的该组织相关恶意程序的报价单。



远程基地报价单

单位（人民币）：元

软件名称	产品型号	单价	数量	付款方式	软件性能特点
大魔王控制	软件	350	个	一次付款	远程控制 屏幕控制撤 视频监控. 键盘记录. 语音监机. 可以同时监控多屏幕多视频多语音同时监控. 可以毁灭硬盘
毁灭者 DDOS	软件	500	个	一次付款	第一类：流量模式. 第二类：网站压力测试模式. 三类：综合模式. 第四类：自定义攻击模式
大魔兽下载者	软件	300	个	一次付款	设做过多的修饰多项下载访问地址是存放下载列表保存位置是下载后文件的 TXT 文件的存放方位统计地址是后台下载统计的地址. 版本信息随便加. 后续将加入文件感染 U 盘感染功能.
魔王捆绑器	软件	200	个	一次付款	可以捆绑图片 JPG 格式图片. 捆绑 rar.文件
1433 扫描器	软件	200	个	一次付款	专扫服务器漏洞的
承接各种软件制作.财务软件.远程控制，木马免杀，后门编写，远程控制编写，全免杀，突破主流杀软。打造专版远程控制，打造 DDOS 攻击软件.还出售 QQ 免杀木马. 联系 QQ 24585329. 172761812					

图 5 007 组织相关恶意代码报价单（更新时间为 2010 年 7 月）

我们近三个月捕获到该家族的免杀器版本已超过上百个，购买用户超过 600 个。下图是购买相关恶意程序的地下产业链成员的分布情况，可以看出以广东省最多，其次是河南和山东省。

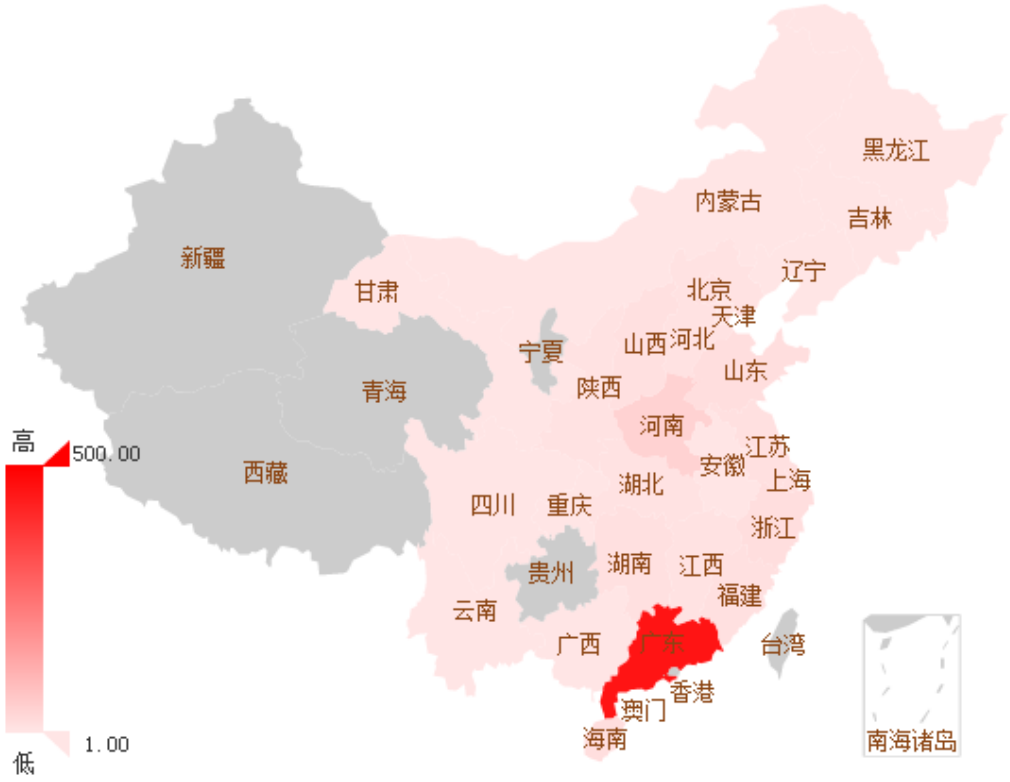


图 6 购买 Hook007 远控的地下产业链成员分布（最近三个月数据）

（二） 窃取用户数据

Hook007 远程控制主要功能就是攻击者可以完全控制受害者的机器，攻击者可以下发任意控制指令。从我们收到的大量被感染 Hook007 木马的用户反馈中可以得知，该组织在攻击成功后通常会通过远程控制强行阻止用户操作游戏，并直接将用户的虚假财产、游戏装备进行交易转给盗号者帐号。也就是主要以窃取用户虚拟货币、网游装备来进行牟利。通过窃取用户数据和虚拟财产，造成每年普通网民财产损失逾千万元。

（三） 其他

DDOS：该组织成员有开发如“毁灭者 DDOS”等 DDOS 工具，由此我们怀疑除了工具的开发，相应地下产业链可能有涉及相关 DDOS 攻击业务。

恶意推广：通过我们监控发现，该组织在控制受害者主机之后，可能会远程控制下载执行推广包，通过安装量来达到牟利的目的。

六、 用户反馈

我们从第三方平台和 360 论坛等平台收到大量用户反馈，相关反馈主要集中在已经造成用户财产损失的用户求助信息。

以下是一些典型用户反馈的截图和链接：

图 7 用户反馈截图 1

参考链接：http://china.findlaw.cn/ask/question_1720116.html

图 8 用户反馈截图 2

参考链接：http://bbs.open.qq.com/thread-7593006-1-1.html

图 9 用户反馈截图 3

参考链接：http://bbs.360safe.com/thread-3943057-1-1.html

图 10 用户反馈截图 4

参考链接：http://bbs.360safe.com/thread-6119441-1-1.html

第二章　攻击手法分析

一、　典型攻击流程

（一） 基于即时通讯工具

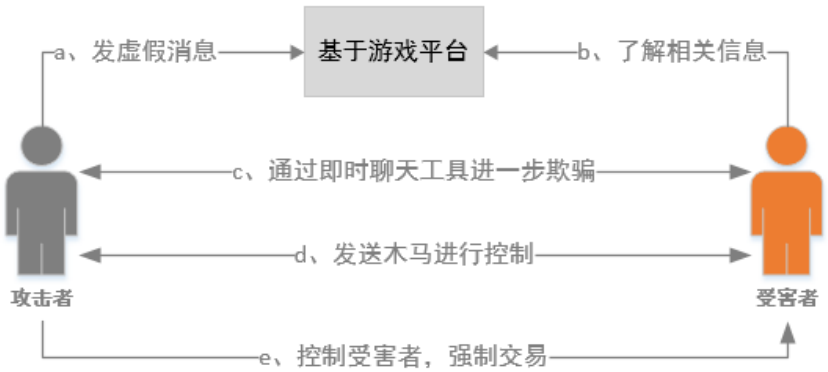


图 11 典型攻击流程（基于即时聊天工具）

具体攻击步骤：

a、 攻击者首先依托游戏平台进行“喊话”或发站内信，以出售、收购或交换游戏装备的名义发送虚假消息，并留下 QQ 号。

b、 受害者通过游戏平台了解到攻击者发送的消息，如果受害者不知情则有可能添加攻击者联系方式，主动联系攻击者。

c、 进一步攻击者通过 QQ 等即时聊天工具进一步获取受害者信任。

d、 当攻击者取得受害者一定程度信任后，攻击者会将木马文件伪装成“装备图片”等发送给受害者，受害者接收执行后则被植入相关后门木马，被攻击者控制。

e、 远程控制玩家电脑，锁定计算机的键盘、鼠标，或设置屏幕黑屏。并短时间内将玩家的游戏装备，金币交易给盗号者的帐号。

（二） 基于假冒网站

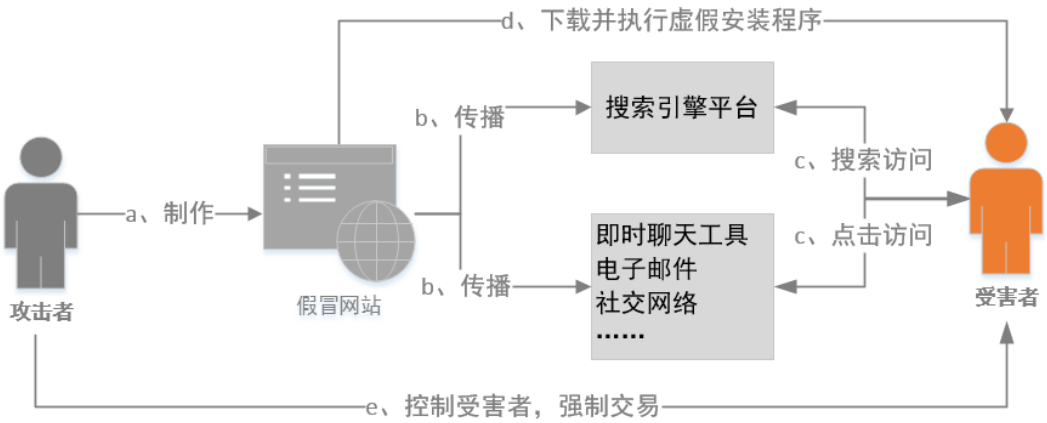


图 12 典型攻击流程（基于假冒网站）

具体攻击步骤：

a、 攻击者首先制作假冒网站，这里主要是假冒如 game456 类游戏平台网站，同时会制作相应虚假的恶意安装包程序。最终假冒网站上的下载链接会指向这个虚假安装包程序。

b、 进一步攻击者需要让相应用户访问假冒网站，主要途径是通过搜索引擎和基于即时聊天工具等平台。攻击者会使用付费推广等方法，使得相关假冒网站在搜索某些关键字的时候，可以优先呈现在搜索结果中。

c、 受害者从搜索引擎搜索出或者从聊天工具中收到相关假冒网站链接，并点击打开假冒网站，则有可能下载相应虚假安装程序。假冒网站制作的与正常官方网站从外观看基本一致，用户很难辨别真伪。另外相关游戏平台官方网站或者安装包的来源是否为官方源本来就没有清晰明确的提示，所以用户从搜索结果中很难识别哪些是可信，那些是恶意的。

d、 当受害者下载并执行了虚假安装包，则操作系统会被攻击者控制。

e、 远程控制玩家电脑，锁定计算机的键盘、鼠标，或设置屏幕黑屏。并短时间内将玩家的游戏装备，金币交易给盗号者的帐号。

注：

以上是主流的攻击流程，一些非主流攻击流程没有具体展开。如利用邮件附件传播、挂马传播等传播方式，DDOS 攻击，在受害主机上下载执行推广包等获利模式等。

二、 恶意代码传播

恶意代码的传播方法主要集中在依托即时通讯工具和网站。其中以依托即时通讯工具这种方式占主流。

（一） 即时通讯工具

攻击者主要依托即时通讯工具进行恶意代码传播，从目前捕获到的情况主要分为直接发送 PE 可执行程序，另一种是 QQ 群共享。该方法针对性强，但也容易被受害者感知到。

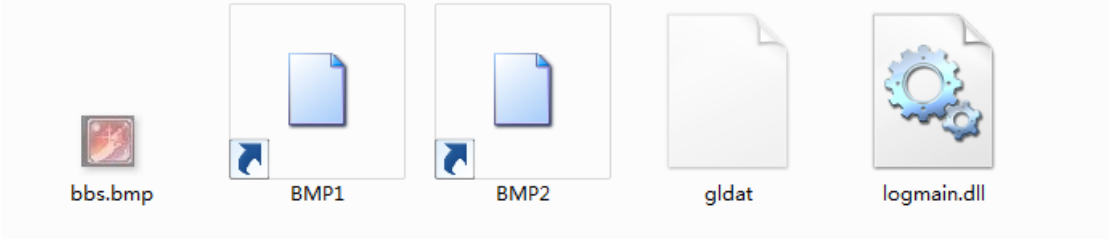


图 13 通过 QQ 传播的文件形态示例

图 14 通过 YY 传播的文件形态示例

由于 Windows 系统默认是不开启显示后缀和隐藏文件的。所以受害者们接收到这些文件压缩包解压后，发现木马文件里面只含有“BMP 格式”的图片（实则是指向病毒程序的

快捷方式），而真正含有恶意代码的文件则被隐藏起来

（二） 网站

1) 假冒游戏平台网站

攻击者会搭建虚假的游戏平台，并通过搜索引擎、弹窗等手段推广。假冒的游戏平台网站与官方网站外观一致，受害者很难分辨真伪。攻击者会将虚假的恶意安装包放置到假冒的网站上，当用户访问网站下载并执行相应虚假安装包则会被攻击者控制。

下图是我们在某知名搜索引擎上搜索凤凰山庄的搜索结果。可以看到，第一页的两条推广结果为假冒的网站。

图 15“凤凰山庄”搜索结果

图 16 假冒凤凰山庄网站（左），凤凰山庄官网（右）

上图假冒凤凰山庄和官网的对比截图，我们可以看出除了网址不同，其他页面外观均一致。很难分辨真伪。

攻击者不是单一选择一款游戏平台进行假冒伪装。我们可以从下表看出，攻击者假冒了很多游戏平台。具体参看下表：

假冒游戏平台名称	虚假恶意网站	备注说明
199 游戏		
235 游戏中心	game235.top	
883XX 游戏中心	game88369.com.cn www.game88369.gyemw.com www.game88369.zxshy.com www.game88369.nmqzx.com www.game88369.yjfjn.cn www.ycttcy.net	该系列其他名称还有88370-88381，总共 12 个
K7 豫游游戏中心	qipai007.aliapp.com	
凤凰游戏山庄	fhgame.sdforging.com.cn tlwt1258.cn vikodrive.cn fhgame.sdforging.com.cn	
汉游天下安装包	shlvxun.gamr89.com	
集结号游戏中心	www.jjhggame.com	
建德游戏	www.byjd571.net	
宁波游戏大厅	www.nbgame.org	
四川游戏家园	28qp.com.tw	
天妃游戏		
网狐游戏家园	foxuc.com.cn foxuc.com.tw	
襄阳同城游戏	0710yx.aliapp.com www.hnzcs.com 0710yx.xmwwy.com cng.minsun.cc 07l0yx.co 07l0.gamr89.com 0710yx.yksyx.org 0710yx.asia	
云海游戏	yunhai78.07l0yx.co	
众安棋牌 89 游戏中心	fjtu123.gamr89.com www.ftqp888.com	

表 3 假冒游戏平台网站列表

2) 官方网站安装包被替换

我们捕获到从某些游戏平台官方网站下载的安装包被替换为包含恶意代码的虚假游戏平台安装包。

进一步我们分析官方可信网站存在恶意虚假安装包这种情况，可能由以下两种情况导致：

第一、 相关官方可信网站被攻陷，正常安装包被攻击者替换；

第二、 官方可信网站的相关工作人员可能刻意替换放置恶意虚假安装包。

从我们的分析来看，更倾向于第一种情况。下面是凤凰游戏山庄网站存在恶意虚假安装包的情况：

凤凰游戏山庄官方网站	
时间	2015-09-15 19:03:20
父页面	http://game.fhgame.com/download.html
下载 URL	http://down.fhgame.com/fhgame/FHGameLobby/FHGameLobby.exe
恶意文件 MD5	ef749aecd9a292cd0c6873840d6f9115

表 4 被替换恶意虚假安装包具体信息

三、 持续对抗

该组织持续与安全厂商进行对抗，至少针对包括 360 在内的 3 款国内安全软件，以及卡巴斯基、比特梵德等国外相关安全产品采取过针对性技术措施，对抗行为最早可以追溯到 2008 年。对抗手段从实体文件到通信协议进行相关对抗，主要针对本地静态扫描、云查杀、主动防御策略和网络层等环节的检测。另外值得注意的是该组织成员会主动联系安全厂商，目的是申请将恶意程序添加白名单或者探测安全厂商检测机制。单就 Hook007 这个家族，我们对相关产品进行了多次升级或检测策略调整。以下将从静态查杀、动态检测、网络监控和探测厂商检测，这四个方面逐一展开相关对抗手法的介绍

（一） 静态查杀

图 17 静态查杀对抗相关发展变化趋势

从上图可以清晰看出 Hook007 在静态查杀相关对抗发展历程，如字符串从明文更新到加密字符串，最后为无字符串特征。

早期的 Hook007 家族是通过暴风白利用，然后再扩展到其他厂商（如迅雷等）白文件利用。所谓“白利用”通常指的是病毒利用正规厂商的正常程序作为掩护，通过这些程序在判断逻辑上的一些缺陷利用其加载木马作者的提供的恶意代，用以逃避安全软件的查杀。最近一段时间，该族系木马则改为利用微软的 rundll32.exe 文件运行含有恶意代码的 dll 文件。

（二） 动态检测

1） 使用特殊浮点指令 bypass 虚拟机查杀

2） LDTDetect：检测 LDT 基址位于 0x0000 时为真实主机，否则为虚拟机

3） GDTDetect：检测 GDT 基址位于 0xFFXXXXXX 时说明处于虚拟机中，否则为真实主机

4） VMwareDetect：检测 VMware 特权指令来检测虚拟机

5） 起初是自启动，之后进一步更新为一次性

6） 逐渐阉割 Gh0st 后门敏感功能

（三） 网络监控

1） 使用 3322 上线->其他动态域名->顶级域名->直接 ip->微博，网盘中转

2） Gh0st 上线协议->修改协议头->逐渐修改成无特征协议

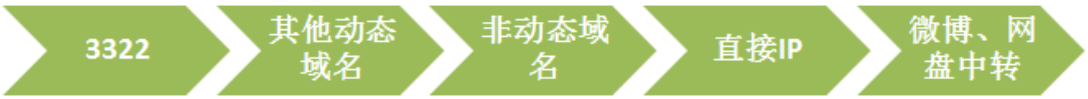


图 18 恶意代码与服务器通信变化趋势

（四） 探测安全厂商检测机制

为了木马能更有效的避免安全厂商检测，该组织成员有主动提交相关样本，来探测安全厂商检测机制的活动。

攻击者探测的方式主要通过给安全厂商样本上报邮箱发送邮件和通过安全厂商官方论坛反馈问题和样本。下图是攻击者给比特梵德、卡巴斯基和 360 安全厂商发送的探测邮件截图。

图 19 攻击者探测（通过邮件 1）

图 20 攻击者探测（通过邮件 2）

被探测的厂商	相关被探测的邮箱地址
比特梵德	sample <sample@bitdefender-cn.com>
卡巴斯基	newvirus <newvirus@kaspersky.com>
360	opensoft <opensoft@360.cn>

表 5 被探测相关安全厂商列表

下面两张图片是该组织在 2013 年 12 月和 2015 年 9 月分别提交的两个贴，均提交到 360 论坛问题反馈子板块。

图 21 攻击者探测（通过论坛反馈 1）

参考链接：http://bbs.360safe.com/thread-3248178-1-1.html

图 22 攻击者探测（通过论坛反馈 2）

参考链接：http://bbs.360safe.com/thread-6202909-1-1.html

四、 制作和更新

007 组织在开发的恶意代码工具种类比较多，其中以给力远程控制工具和给力免杀器为主。而相关更新维护则主要是针对 Hook007 家族进行相关更新。

（一） 007 相关恶意软件

图 23 Hook007 相关恶意软件种类

从上图我们可以看出 007 组织会涉及到制作或传播给力免杀、给力远控、盗号木马、DDOS、漏洞扫描、下载者和其他远控，其中给力免杀和给力远控是 007 组织主要开发和维护的工具。

以下主要是该组织核心成员开发的相关工具的截图。作者在工具上都会留下自己的昵称（早期为小寡妇 007，后期主要是 Hook007）和 QQ 号（24585329）。

图 24 remote007 工具截图

图 25 大牛 B 下载者生成器截图

图 26 阿凡提远程控制软件截图

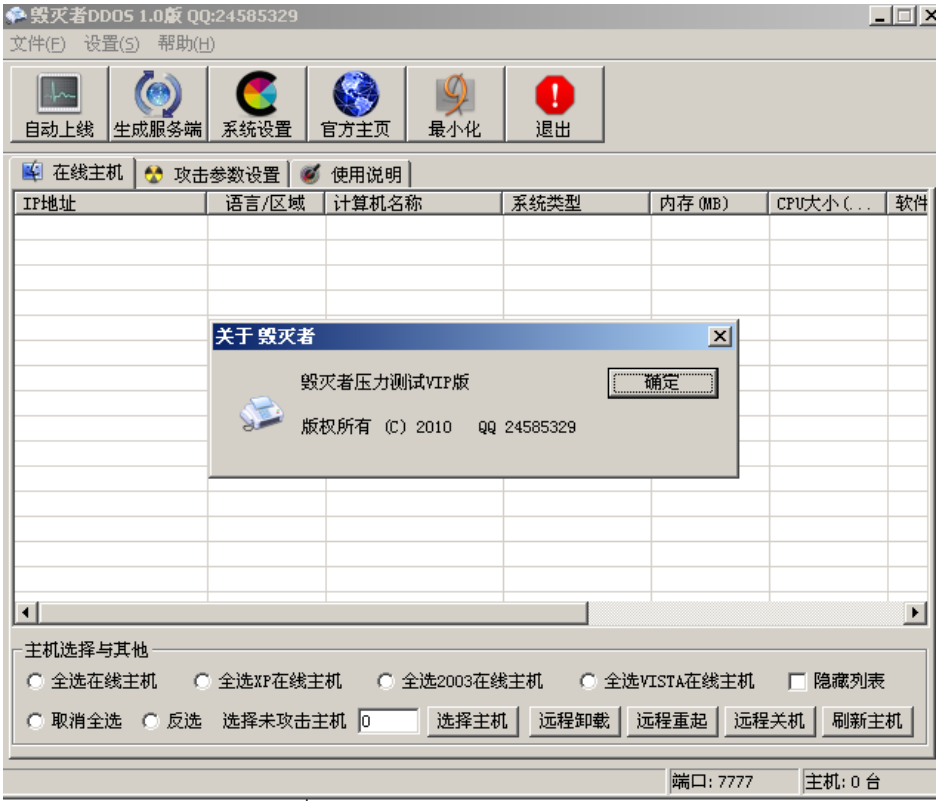


图 27 毁灭者 DDOS 界面

图 28 相关捆绑工具截图

（二） Hook007 远程控制（给力远控）

我们一直持续跟踪监控的 Hook007 家族，其生成器作者命名为“给力”远控。

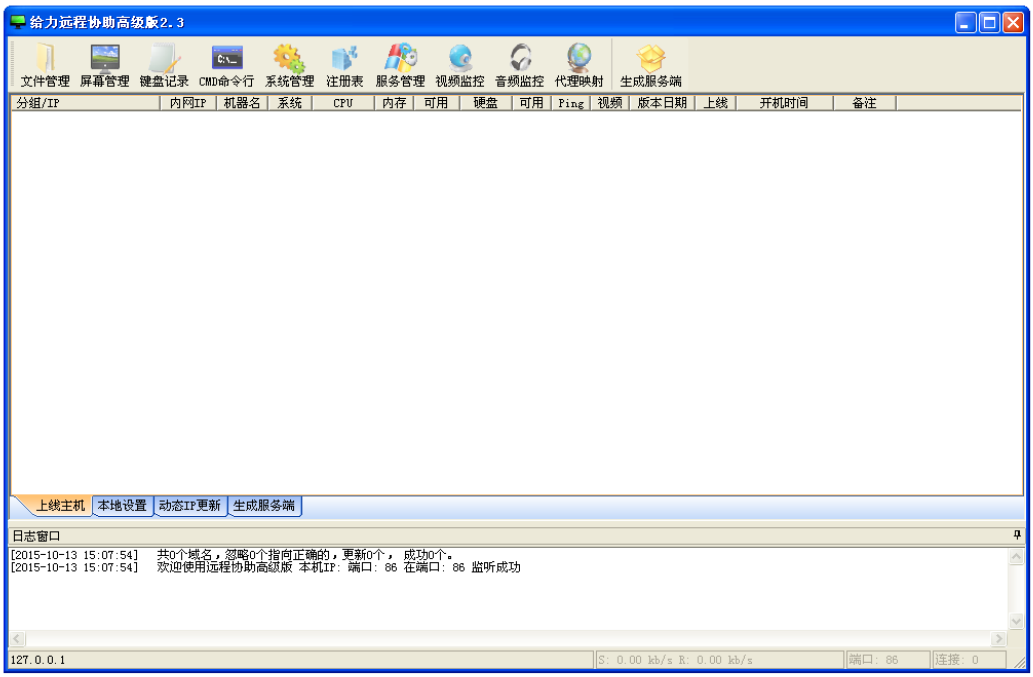


图 29 给力远程协助工具

图 30 给力远程协助工具登录验证工具

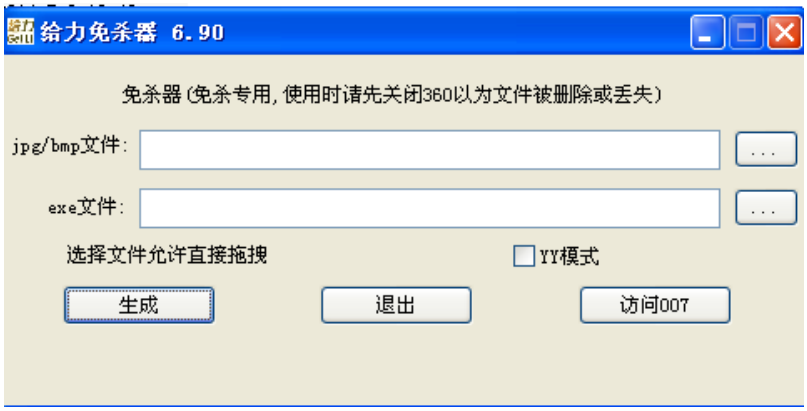


图 31 给力免杀器

（三） Hook007 远程控制迭代更新

该组织制作的恶意代码主要以伪装图片或文档，虚假安装包这两种形态，这两种最终后门程序均为 Hook007 家族，是基于 Gh0st 进行修改的版本。

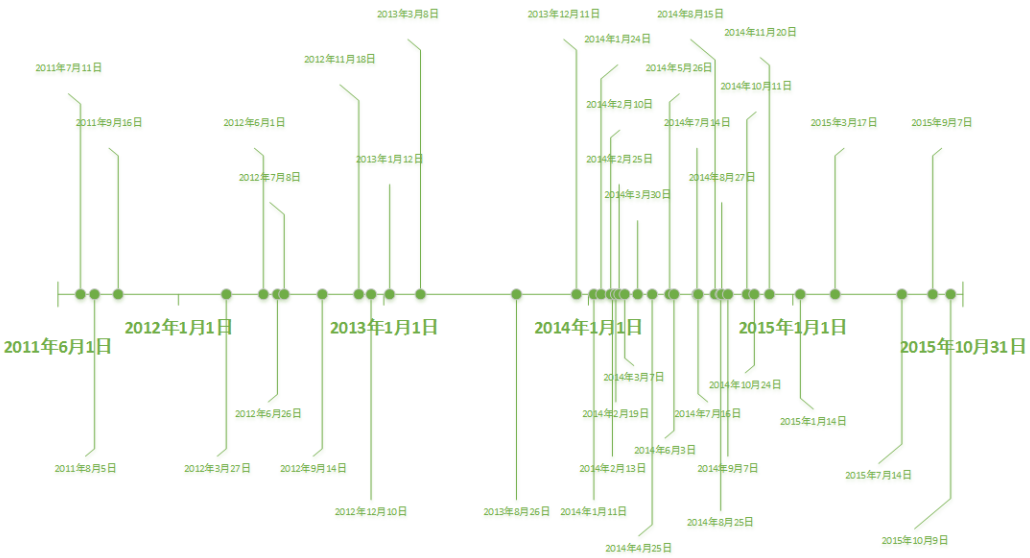


图 32 恶意代码更新记录

Hook007 家族主要更新变化趋势

2012 年之前，Hook007 家族，还是原始版本的 Gh0st 远控，启动参数带有 Hook007，fuck360，fuck007 等，通过不同的启动参数，决定木马执行安装流程还是远控流程。

2012 年中旬，基于开源远控协议，大约每两三天发一批新域名的木马。IP 由域名解析得到。

2012 年底，基于开源协议进行小幅度变种。大约每两三天发一批新域名的木马。IP 由域名解析得到。

2013 年中旬，基于开源协议进行大幅度变种，需通过大数据分析捕获协议特征。大约每天发一到两批新域名的木马。IP 由域名解析得到。

2013 年中下旬，基于开源协议，针对 360 监控模式，加入混淆数据，大约每天发三到

四批新域名的木马，IP 由域名解析得到。

2014 年初，基于开源协议加入迷惑性数据，伪造成其他常见数据协议，难与主流协议区分。无新域名，采用直接访问 IP，大约每天发七到八批新 IP 的木马。

2014 年中旬，网络协议为自定义协议，同时伪造成其他常见数据协议，通过第三方平台网站的自定义内容跳转到制定 IP，大约每天发六到七批新木马。

2015 年初，网络协议为自定义协议，直接请求 IP，如果无法上线，再通过第三方平台网站的自定义页面查找新 IP，约每半小时一批新 IP 木马。

2015 年中下旬，更新自定义协议，直接请求 IP，如果无法上线，再通过第三方平台网站的自定义页面查找新 IP，约每半小时一批新 IP、新协议木马。

第三章　该组织使用的 C&C

一、　C&C 分类

该组织出现使用的 C&C（Command and control，通信控制）非常多，相关域名、IP 也是分工明确。我们大概从 C&C 功能的角度分析出相关 C&C 的种类：

1) 直接连 IP
2) 连攻击者所持有的域名，进一步解析域名指向 IP
3) 连接腾讯微博，解析页面中 IP
4) 连接永硕 E 盘，解析页面中 IP
5) 验证或更新的 IP：专用于后门更新的服务器。
6) 伪造游戏平台网站的域名和 IP

另外在本报告“第三章 攻击手法分析”中“三、持续对抗”章节，我们已经介绍了攻击者在网络层面是如何进行持续对抗的，也就是下图可以看出攻击者在选择 C&C 的变化趋势。

图 33 恶意代码与服务器通信变化趋势

二、　依托第三方平台中转

下面两个图是永硕 E 盘和腾讯微博获得上线 IP 的具体截图：

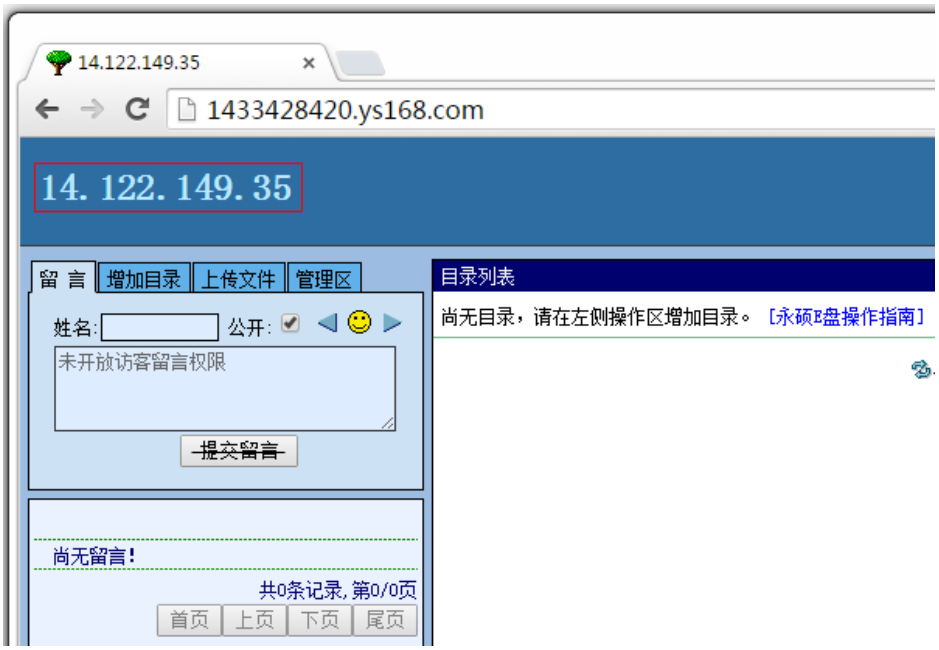


图 34 利用永硕 E 盘获得上线 IP

图 35 利用腾讯微博获得上线 IP

下面两个截图是攻击者用来解析腾讯微博上线 IP 地址的工具，和该工具相关代码截图。

图 36 解析微博、网盘工具

```
wsprintfA(&szUrl, "http://%s", v10);
v5 = sub_401360((int)&v12, &szUrl, 0, 0, 0xFFFFFFFF);
if ( v5 )
{
  v6 = strstr(v5, "IP&#61;");
  if ( v6 )
  {
    v7 = lstrlenA("IP&#61;");
    v8 = strtok(&v6[v7], "&#");
    if ( v8 )
      CWnd::MessageBoxA(v1, v8, "查询结果", 0);
  }
```

图 37 微博 IP 查询器相关代码截图

第四章　幕后始作俑者

007 组织相关成员分工明确，从制作恶意代码到最终获利组成了一条完整的地下产业链。主要包含制作恶意代码、传播、更新、获利等环节。

从目前我们已知的数据来看，该组织相关成员主要分布在湖北、山东和广东三个地区。

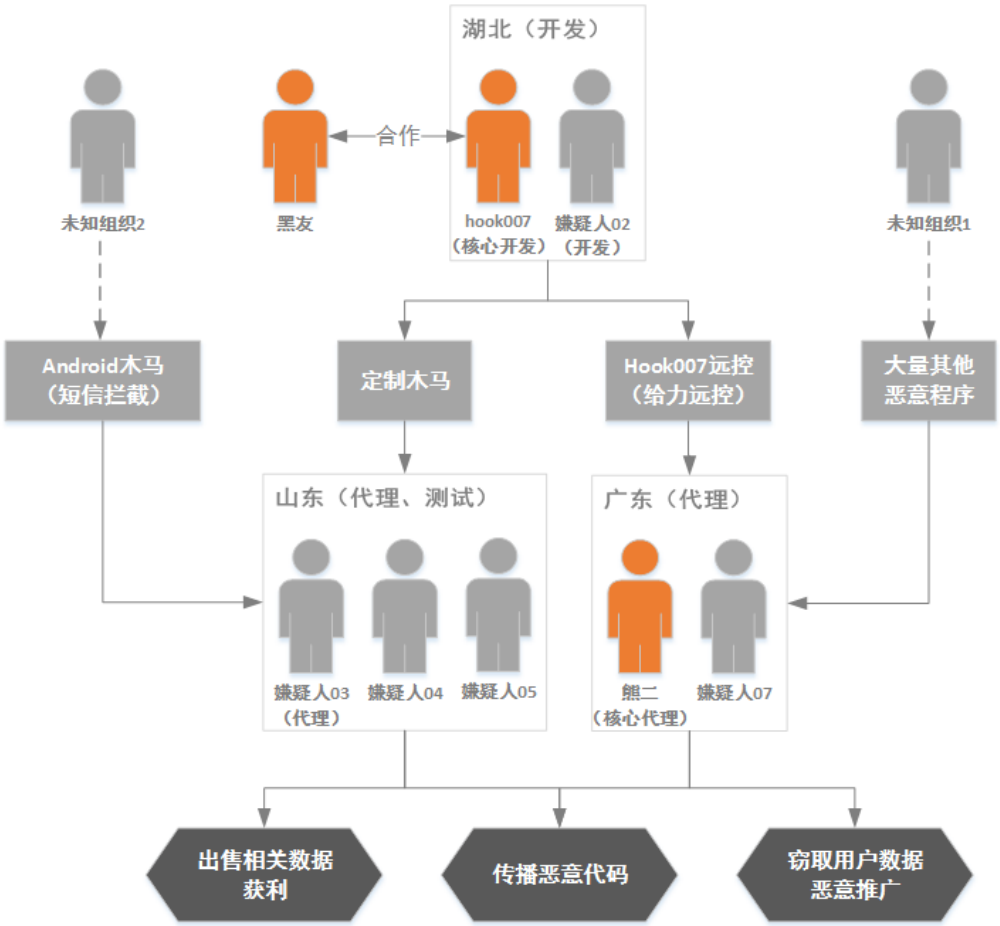


图 38 007 组织架构

007 组织主要以 Hook007（嫌疑人 01）为主，Hook007 和另一名嫌疑人 02 是主要开发人员，开发的恶意软件以 Hook007 远控（给力远控）为主。另外 Hook007 与黑友（又名黑色经济，嫌疑人 08）在早期就有相关业务合作，黑友的角色与广东熊二（嫌疑人 06）相似。相关更新维护工作主要围绕 Hook007 远控展开。以 Hook007 远控为主的恶意软件会提供给山东相关同伙和广东同伙，其中以广东的熊二为主。以广东熊二为例，熊二作为代理商的角色会将相关远控工具在提供给其他下级买家。

进一步后续会有专人负责传播恶意代码和相关窃取用户数据、恶意推广。由于相关传播过程需要社会工程学欺骗受害者，以及需要与受害者多次交互，所以我们推测相关传播恶意代码的人员和窃取用户数据的人员会有重叠的情况。最后相关人员将窃取的数据信息通过第三方网络游戏交易平台或其他渠道进行交易，最终达到获利。

另外值得我们注意的是广东相关同伙的上家除了 Hook007，还有其他组织提供大量的恶意程序。另外山东同伙涉及 Android 木马（以短信拦截马为主）的相关业务。

附录 1　Hook007 家族样本分析报告

具体请参看：

1、“罪恶家族——Hook007 木马”，http://blogs.360.cn/blog/Hook007_trojan/

2、“罪恶家族 Hook007 之潜伏篇”，http://blogs.360.cn/blog/hoook007/

附录 2　007 组织涉案金额估算

007 组织核心成员涉案金额（单对 Hook007 生成器估算）	
估算方法	单价：300 元 生成器数量（三个月）：120 个 拥有生成器的人数：1 个生成器对应 10 个人
结论	一年估算：300*120*10*4=144 万元

受害用户损失金额（单对受 Hook007 家族影响的估算）	
估算方法	近一年受影响用户约：50 万左右 真正被窃取装备的用户估算为受影响的 1/100：5000 根据专业反诈骗平台猎网平台的统计数字显示，因游戏帐号被盗而导致的用户损失人均为：2338 元
结论	一年估算：5000*2338=1169 万元

附录 3　C&C

涉及到的部分域名和 IP：

0710yx.aliapp.com
0710yx.asia
0710yx.xmwwy.com
0710yx.yksyx.org
07l0.gamr89.com
07l0yx.co
106.111.140.16
106.226.228.105
106.80.54.138
106.80.56.59
111.195.244.20
14.119.236.212
14.119.237.103
14.119.239.174
14.119.241.1
654004572.ys168.com
983830035.ys168.com
a594250576.ys168.com
a6601251.ys168.com
bobo.haoyue1688.com
ccl0579.com
cng.minsun.cc
dioeopp.org
ewq889966.ys168.com
t.qq.com/a_739377521
t.qq.com/a1005561469
t.qq.com/a1156573029
t.qq.com/a125245585
t.qq.com/a12d132
t.qq.com/a136410138

附录 4　MD5 值

部分恶意代码的 MD5 值：

5d8d0fd05af1264abb1d22cdb0406f83
f4f56532dea762d1be186bbe0f9e616e
12e71fc967f54fe989d500d38925eceb
4df813d38430d5ca988cb8d42cdf8e0b
7a005b7b22abc69b247e1c031688fe7e
f9ccb246b6b86c7f0d92c86c4560a17a
bfcc17fb2d5662b0b08727eb1ac243c0
1e657ebc26731ee8655eeeeed179bb62
efca9a583e86aa4ca2da424498799583
09b78b16f5c54093cc658c21fb028802
e30cd3b3d3bd4702d179858d0a0143fb
4991f063a1119a682ac82964303fd8cd
6132d5867eef96b69f67ee25a46b70da
8da89564a0259b29d7f9455443427e6f
8e21131ce2b38e1b000fc7ff980e40c2
17643d8a6e5982bce1e5647450f8365e
7ee1e4a7e61d5df97c52563d7a2838e7
ded24dc5158a3bd57546e02af0419317
70fa304c459d280d5b506d54362762a2
8c5d4c868b61d0e1d26fc5bc31369181
8e46b65ff218bc4e7d116c3bf5fddc61
3b3fd6e9ebd9e47bb221693f5aa3a770
557d573cccf1e71d43ce9f49b3bc116c
42cfc7c9bcb595e5eb3a857974605cd0
73be41e111bb5598ec14b13e6472099f
041536acfd00fe9f10b51c3fefdb9798
31e8889d79aad982323faef454e59f6e
71b7b652330c94cb7c9d42197b04a600
448e84bbdb9721d80b65c27a0278644c
353264b562660a940d5d761bfa2e1ced