腾讯安全2018上半年互联网黑产研究报告

腾讯安全 | 腾讯安全联合实验室

目录

序言

病毒木马的演变史，就是一部互联网黑产演变史。病毒木马从最初的以炫技为目的，逐步过渡到与利益相关：哪里有流量，哪里能够获利，哪里便会有黑产聚集。

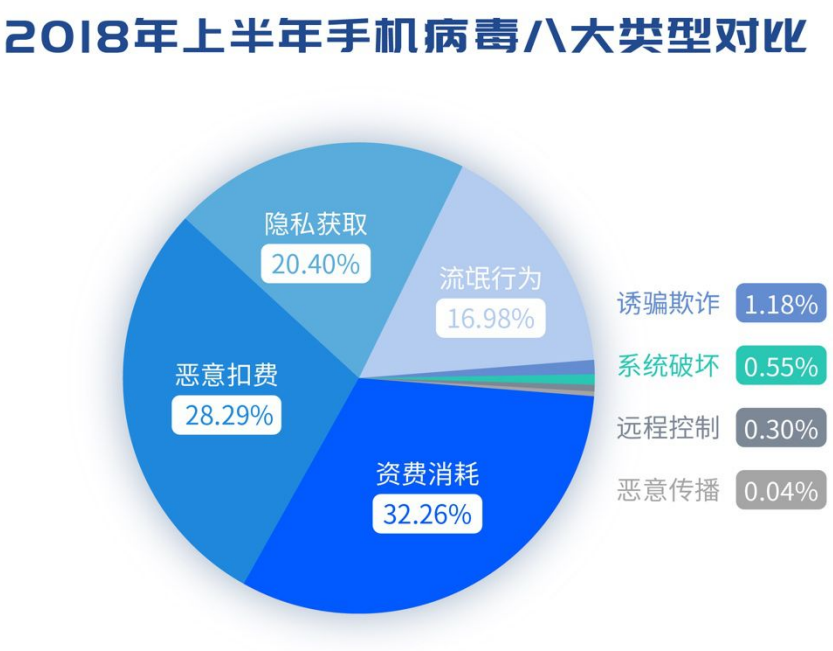
2018 年，伴随移动应用的影响力超过电脑应用，主要互联网黑产也迁移到手机平台。腾讯安全反诈骗实验室观测数据表明，以持续多年的暗扣费黑产、恶意移动广告黑产、手机应用分发黑产、App 推广刷量黑产为典型，这些移动端的互联网黑产，给用户和软件开发者带来了巨大的经济损失。

同时，2018 年是区块链大年，几乎所有的新兴产业，都绕不开区块链这个关键词。与之相应，2017 年下半年至今，互联网病毒木马的主流也都围绕区块链、比特币、以太坊、门罗币而来。由于比特币具备交易不便于警方追查的特性，全球范围内的黑市交易，大多选择比特币充当交易货币。由比特币等数字货币引发的网络犯罪活动继续流行，挖矿木马成为了 2018 年影响面最广的恶意程序。对于挖矿而言，除了大规模投入资本购买矿机自建矿场，黑产的作法是控制尽可能多的肉鸡电脑组建僵尸网络进行挖矿。而僵尸网络除了可以挖矿牟利，控制肉鸡电脑执行 DDoS 攻击也是历史悠久的黑产赢利模式之一。

为此，腾讯安全联合实验室整理了 2018 年上半年互联网黑产攻击数据和发展现状，分别从移动端和 PC 端两个方面详细解读黑色产业链的具体特征、攻防技术和发展态势，为大家揭开互联网黑产的面纱。

一、移动端黑产规模宏大，恶意推广日均影响用户超千万

2018 年上半年，手机病毒类型多达几十种，大部分病毒都属于资费消耗、恶意扣费和隐私获取这三种类型，占比分别为 32.26%、28.29%和 20.40%。此外，手机病毒的功能日益复杂化，一款病毒往往兼具多种特性和恶意行为。4 月初腾讯 TRP-AI 反病毒引擎曾捕获一款名为“银行节日提款机”的恶意木马，伪装成正常的支付插件，在用户不知情的情况下，私自发送订购短信，同时上传用户手机固件信息和隐私，给用户造成资费损耗和隐私泄露。



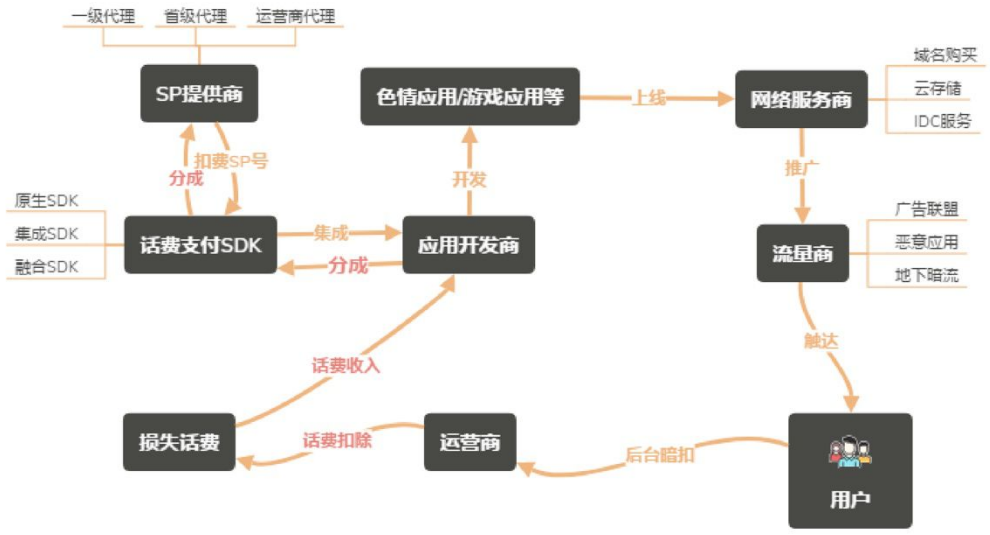
1.四大主流黑产链条

1.1 暗扣话费黑产：日掠夺千万的“抢钱”产业链

暗扣话费是非常古老的互联网黑产。大部分用户会预充值一些话费用于支付套餐的消耗，平时也很少再关注话费，实际上，这些预存的话费余额还可以用来订阅各种增值服务。移动黑产正是利用这一点，串通利益共同体一起窃取用户话费余额并牟取暴利。

据腾讯安全反诈骗实验室数据显示，每天互联网上约新增 2750 个左右的新病毒变种，伪装成各种打色情擦边球的游戏、聊天交友等应用诱导用户下载安装。此类手机恶意应用每天影响数百万用户，按人均消耗几十元话费估算，日掠夺话费金额数千万，可谓掘金机器。受暗扣话费影响的最多的省份有广东、河南、江苏等地。

腾讯安全反诈骗实验室研究发现，此类黑产以稀缺的 SP 提供商为上游，SDK 根据掌握的不同 SP 资源开发相应的 SDK，并将这些 SDK 植入到伪装成色情、游戏、交友等容易吸引网民的应用中。实现暗扣话费变现后，利润通过分成的方式被整个产业链瓜分。此类黑产核心的扣费 SDK 开发团队大概有 20 家左右，主要分布在北京、深圳、杭州等地。

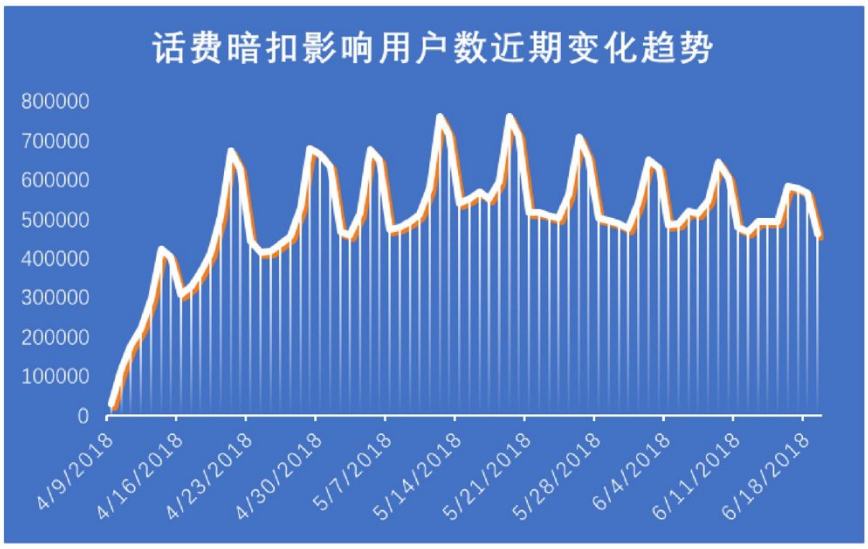


腾讯安全2018上半年互联网黑产研究报告

图片来源：腾讯安全反诈骗实验室

腾讯安全

据腾讯安全反诈骗实验室观测，暗扣话费的手机恶意软件的影响近期又呈增长之势。



腾讯安全2018上半年互联网黑产研究报告

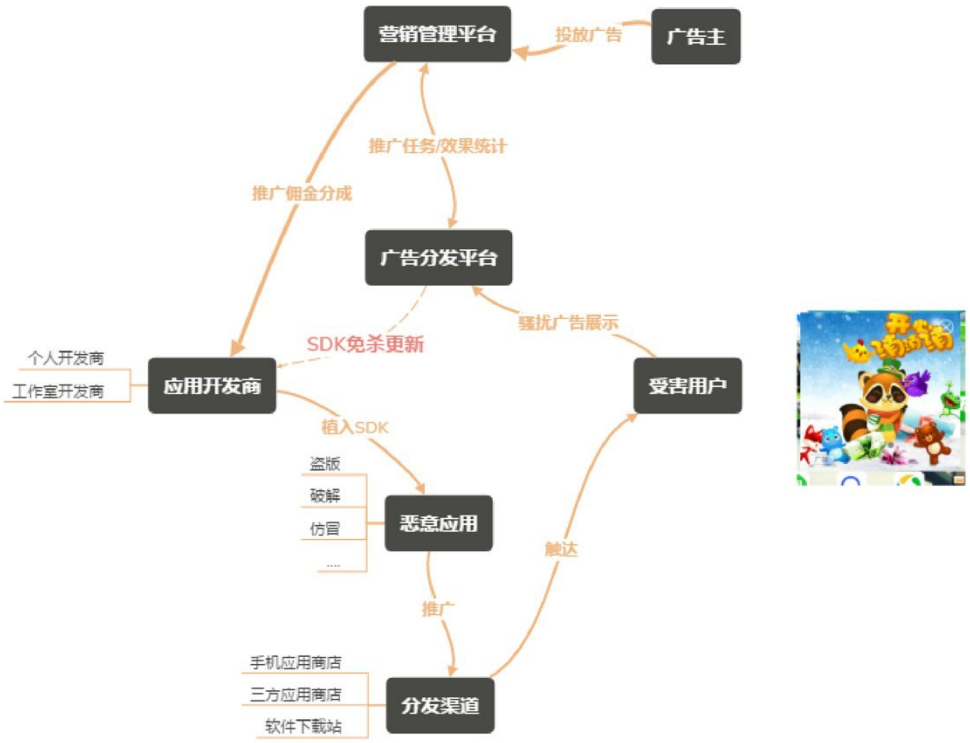
数据来源：腾讯安全反诈骗实验室

腾讯安全

1.2 广告流量变现：九大家族控制数百万广告流量牟取暴利

当前中国网民对手机应用中广告的态度整体较为宽容，国内消费者为应用付费的习惯尚待养成，正规的软件开发者同样需要通过广告流量来获利收益。然而，某些内置于各类应用中的恶意广告联盟，主要通过恶意推送广告进行流量变现的形式来牟利，平均每天新增广告病毒变种 257 个，影响大约 676 万的巨大用户群。这些恶意广告联盟推送的广告，内容更加无底线，在某些时候突然推送出色情擦边球应用、博彩甚至手机病毒也不足为奇。

恶意广告黑色产业链

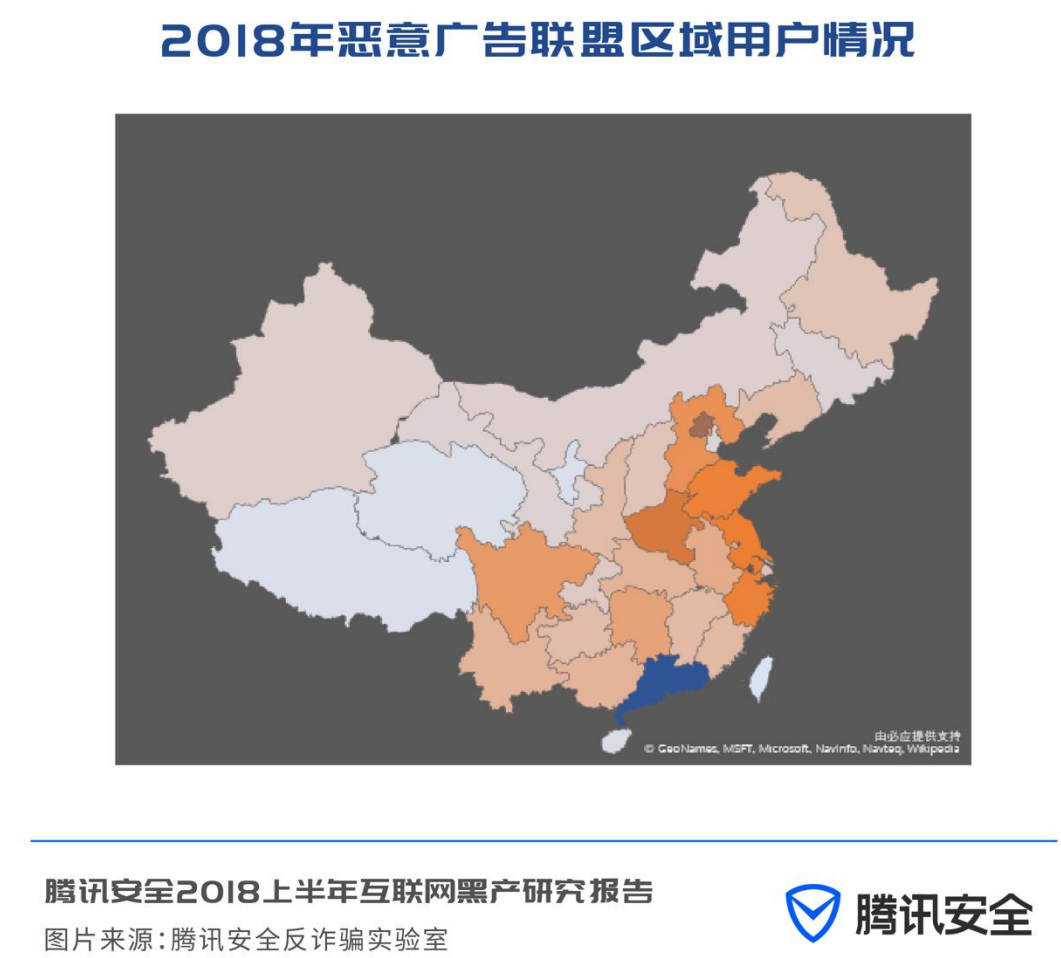


腾讯安全2018上半年互联网黑产研究报告

图片来源：腾讯安全反诈骗实验室

腾讯安全

腾讯安全反诈骗实验室的监测数据表明，越是经济发达的地区，恶意广告流量变现的情况也越发严重。珠三角、长三角、京津冀遭受恶意广告流量的影响远大于全国其他区域。



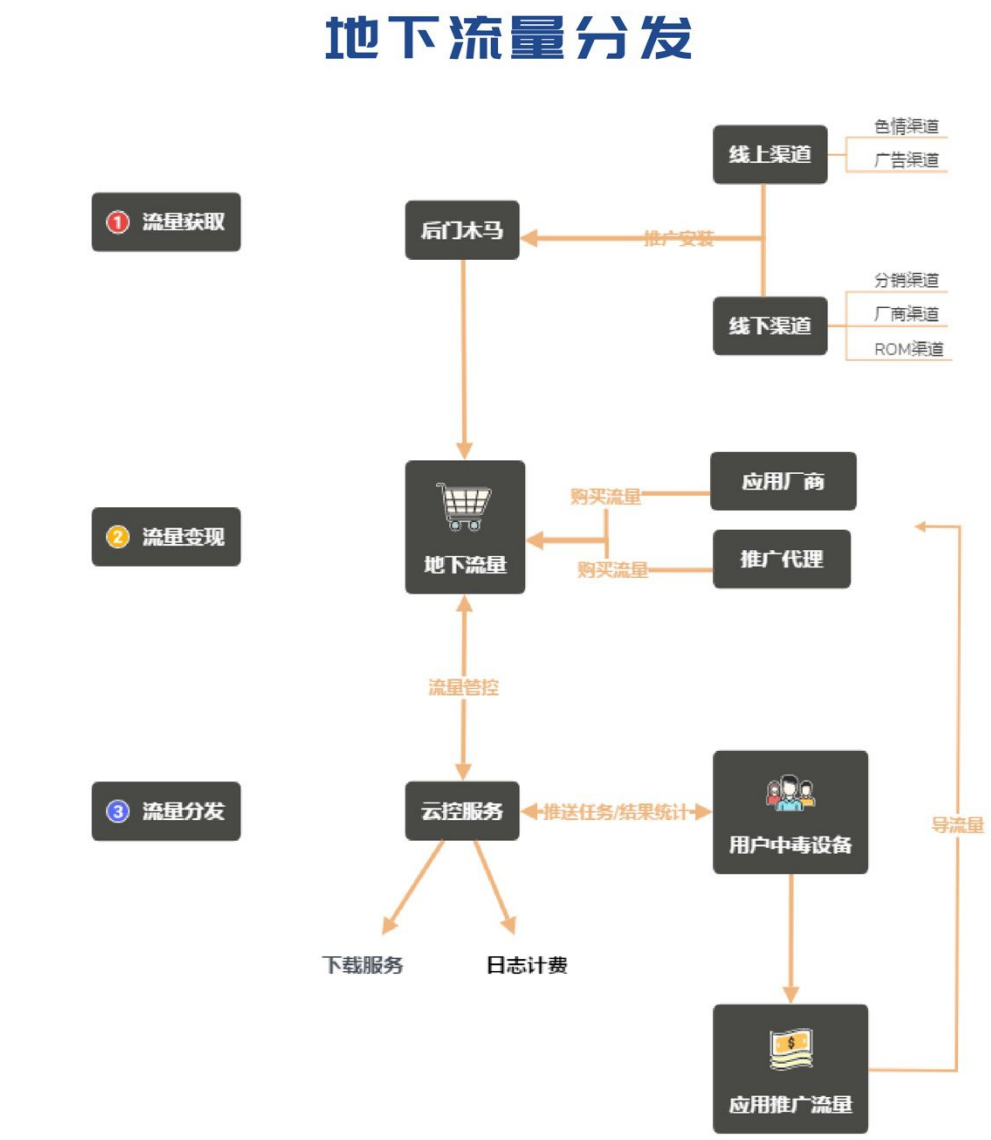
腾讯安全2018上半年互联网黑产研究报告

图片来源：腾讯安全反诈骗实验室

腾讯安全

1.3 手机应用分发黑产：沉默但不简单的地下软件分发渠道

在应用市场竞争日益激烈的情况下，软件推广的成本也在升高。一些初创公司较难在软件推广上投入大量成本，部分厂商便找到了相对便宜的软件推广渠道：通过手机应用分发黑产，采用类似病毒的手法在用户手机上安装软件。据腾讯安全反诈骗实验室监测数据显示，软件恶意推广地下暗流整体规模在千万级上下，主要影响中低端手机用户。例如部分用户使用的手机系统并非官方版本，经常会发现手机里莫名其妙冒出来一些应用，这就是地下软件黑产的杰作。



腾讯安全2018上半年互联网黑产研究报告

图片来源：腾讯安全反诈骗实验室

腾讯安全

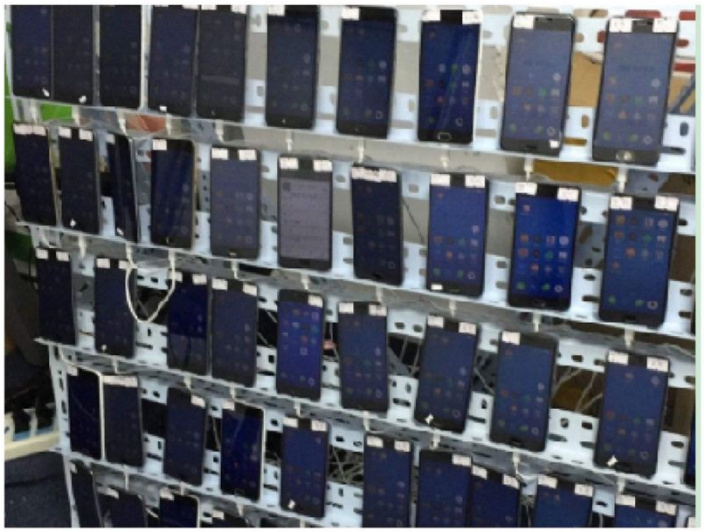
通过手机恶意软件后台下载推广应用，是手机黑产的重要变现途径。腾讯安全反诈骗实验室的研究数据表明，手机恶意推广的病毒变种每天新增超过 2200 个，每天受影响的网民超过 1000 万。

1.4 App 刷量产业链：作弊手段骗取开发者推广费

为了将自己开发的手机应用安装在用户手机上，软件开发者会寻找推广渠道并为此付费。一部分掌握网络流量的人，又动起歪脑筋：利用种种作弊手段去虚报推广业绩，欺骗软件开发者。根据腾讯安全反诈骗实验室对 App 刷量产业链的研究，该产业链主要有三个阶段：

第一阶段：机刷时代(模拟刷、群控)

前期通过模拟器模拟出大量手机设备伪装真实用户，随着对抗后期则主要通过购买部分真实手机设备通过群控系统来实现。模拟器易被检测，群控规模有限，加上开发商对抗技术的升级，该模式逐渐没落，刷量产业和开发者也处于长器的博弈之中。



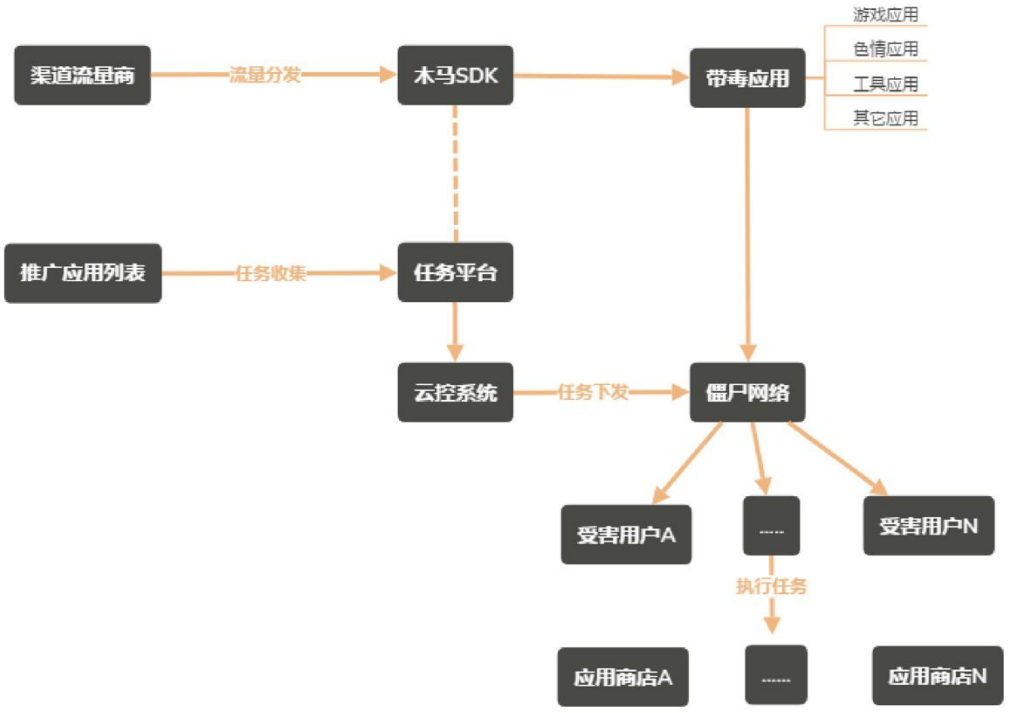
第二阶段：众筹肉刷

常常以手机做任务就可以轻松赚钱为噱头吸引用户入驻平台，用户可以通过 APP 提供的各种任务来获取报酬，比如安装某个应用玩十分钟可以获取一块钱。然而这些平台由于失信太多，骗用户做任务又不愿意付费，导致愿意参与此类游戏的网友数量越来越少，模式已逐渐消亡。

图片来源：网络

第三阶段：木马技术自动刷量

人工刷量需要大量的真实用户帐号，或者较多的设备，还得人肉操作，导致效率较低。2018 年有一批聪明的开发商已经开始布局木马自动刷量平台。木马 SDK 通过合作的方式植入到一些用户刚需应用中进行传播，然后通过云端控制系统下发任务到用户设备中自动执行刷量操作。



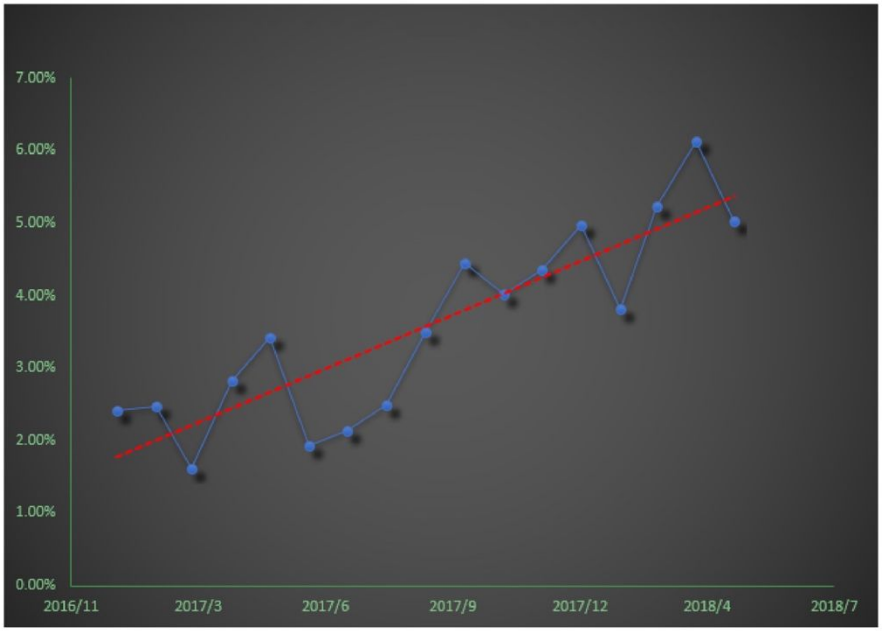
2.三大新兴攻击手段

2.1 黑产利用加固技术进程在加速

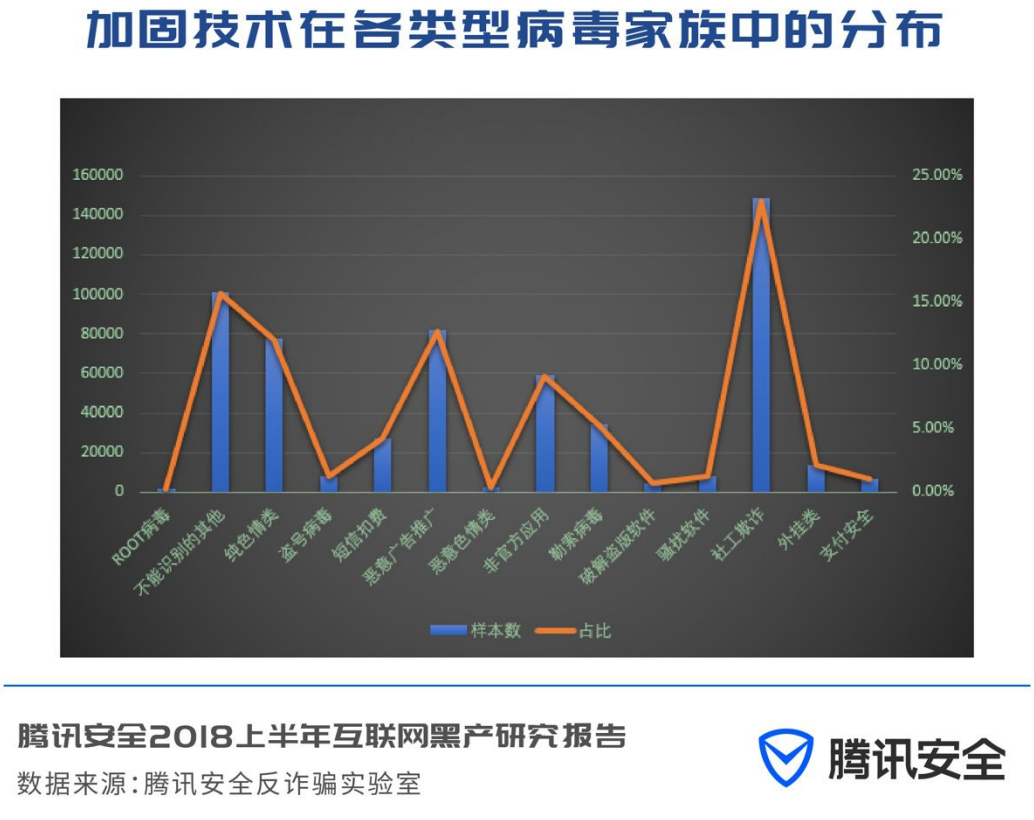
加固技术开发的本来目的是用于保护应用核心源代码不被窃取，随着病毒对抗的不断提升，越来越多的病毒应用开始采用加固来保护自己的恶意代码不被安全软件发现。

目前国内外有很多成熟的加固方案解决厂商，这些厂商存在很多先进的加固技术和较完善的兼容性解决方案，但是这些方案解决商的这些优点正成为黑产很好的保护伞。根据腾讯安全反诈骗实验室的数据显示，进入 2018 年以后利用这些知名加固解决方案的病毒应用正在快速增加。

病毒样本中使用加固技术的样本占比变化趋势



从病毒家族的维度看，社工欺诈类、恶意广告类、色情类、勒索类等对抗更激烈的病毒家族更喜欢使用加固技术来保护自己。

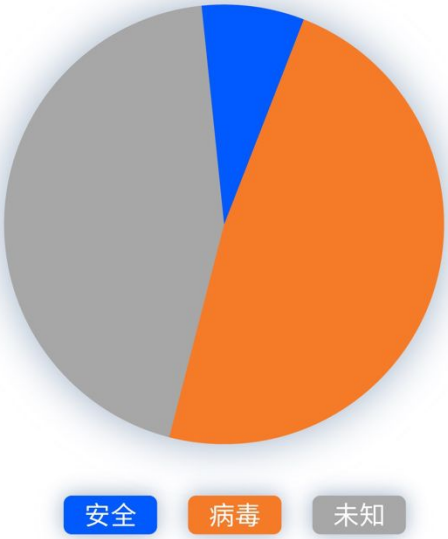


2.2 黑产超级武器云加载进入 3.0 时代

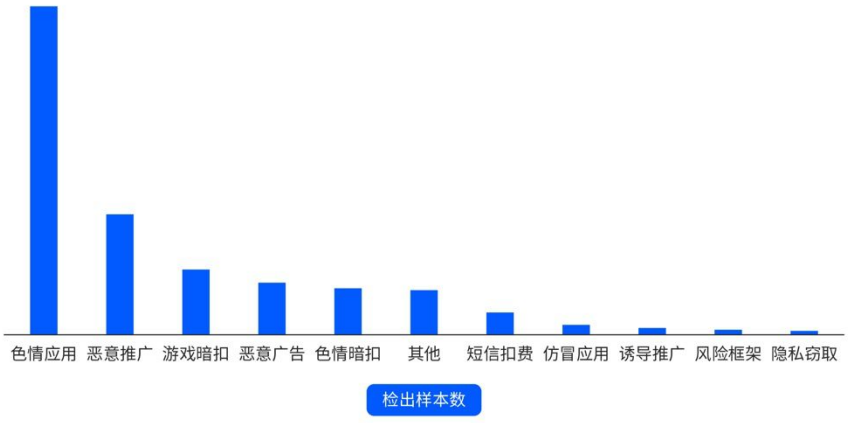
随着恶意应用开发商与安全厂商的攻防日趋激烈和深入，恶意软件的开发者倾向于使用将恶意代码隐藏在云服务器并采用云端控制的方式下发恶意功能，最终通过本地框架进行动态加载来达到最佳隐藏恶意行为的效果，云加载技术是目前对抗传统安全软件最好的对抗手段。

根据腾讯安全反诈骗实验室大数据显示，目前使用动态加载技术的应用中，接近一半都是病毒。云加载技术正在成为病毒开发者最喜欢的攻击手段，色情、恶意应用分发、游戏暗扣等最赚钱的病毒家族，普遍标配云加载攻击技术来实现利益最大化。

使用动态加载技术的样本安全性分布



使用动态加载技术的病毒类型分布



该技术在病毒黑产中的作恶特点是：剥离恶意代码封装成 payload，客户端上传特定的信息流交由云服务器控制是否下发执行 payload 功能，下发的代码最终在内存中加载执行，恶意代码可及时清理并保证恶意文件不落地，防止传统安全客户端感知。腾讯安全专家把这种利用技术成为“云加载”技术。

近年来，随着开发人员对 Android 系统架构和动态加载技术的理解的深入，各种代码热更新方案和插件化框架被发明并且免费开源，为病毒技术开发者实施云控作恶提供了技术基础，云控技术已经成为绝大多数高危木马的标配，腾讯安全反诈骗实验室近期也发现了若干使用云控技术的病毒家族。

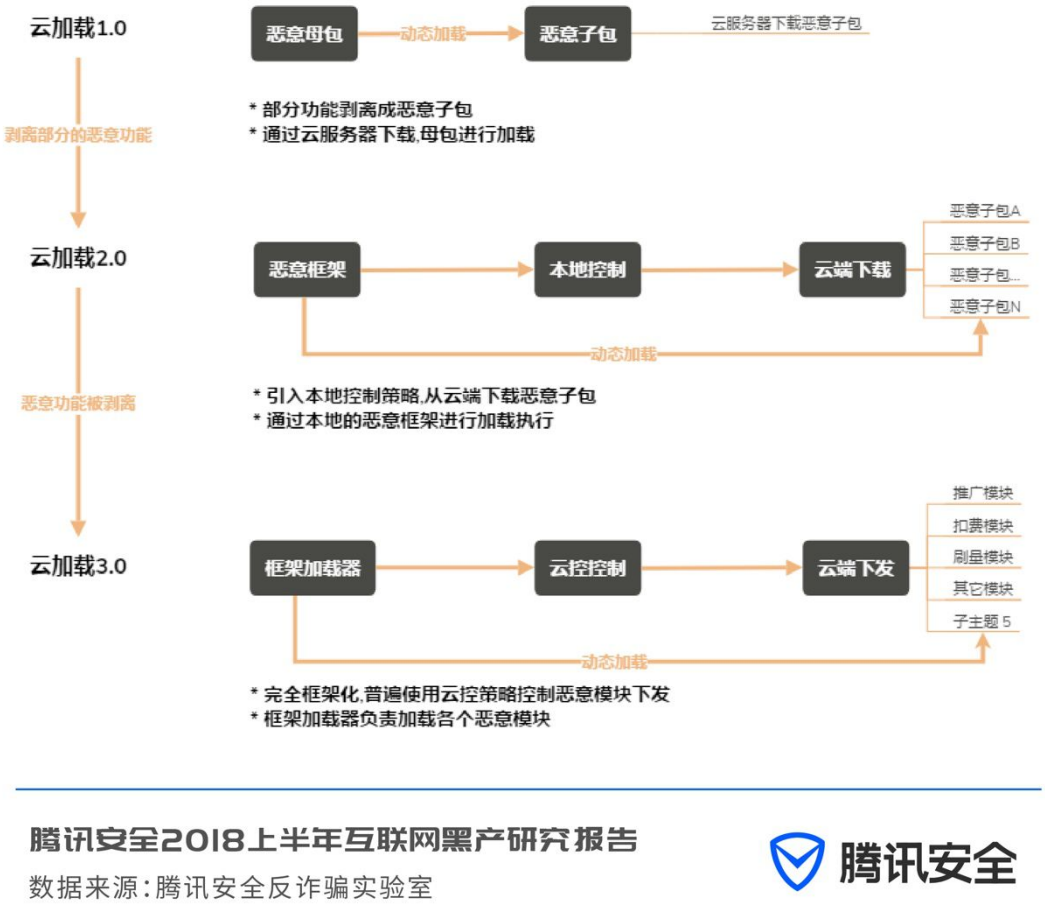
日期	文章标题	影响规模(日)	特点	潜伏期
2018/5/31	警惕新型儿童游戏木马，守护孩子们的天空	100万+	植入某广告SDK, 云端控制文件下发	一年以上
2018/5/21	“隐流者”家族盯上70%的国内应用市场	17万	植入到恶意支付SDK, 通过色情/游戏传播	数年
2018/4/18	“寄生推”SDK云控作恶，300多款应用不幸躺枪	40万	植入爱心推SDK中 ,通过正规应用传播	一年以上
2017/12/17	TigerEyeing病毒云控推广上千应用	14万	DroidPlugin框架, 恶意功能按需加载	半年左右
2017/11/29	百万地下暗流EvilJS隐匿者家族	180万	通过SDK植入正规应用	一年以上

腾讯安全2018上半年互联网黑产研究报告

数据来源：腾讯安全反诈骗实验室

腾讯安全

云加载技术目前已经更新到 3.0 版本，该版本框架病毒开发者不仅可以通过地域、运营商、机型、设备等维度限制感染用户群，还能利用 VA 等虚拟加载技术彻底剥离恶意代码，通过一个白框架来按需加载扩展各种恶意功能，普通安全厂商很难再捕获到病毒的恶意行为。



2.3 黑产渗透更多的供应链，供应链安全风险加剧

回顾整个 Android 应用供应链相关的重大安全事件可以发现，针对供应链攻击的安全事件在用户影响、危害程度上绝不低于传统的恶意应用和针对操作系统的 0day 漏洞攻击，腾讯安全专家研究发现针对 Android 应用供应链的攻击的呈现以下趋势：

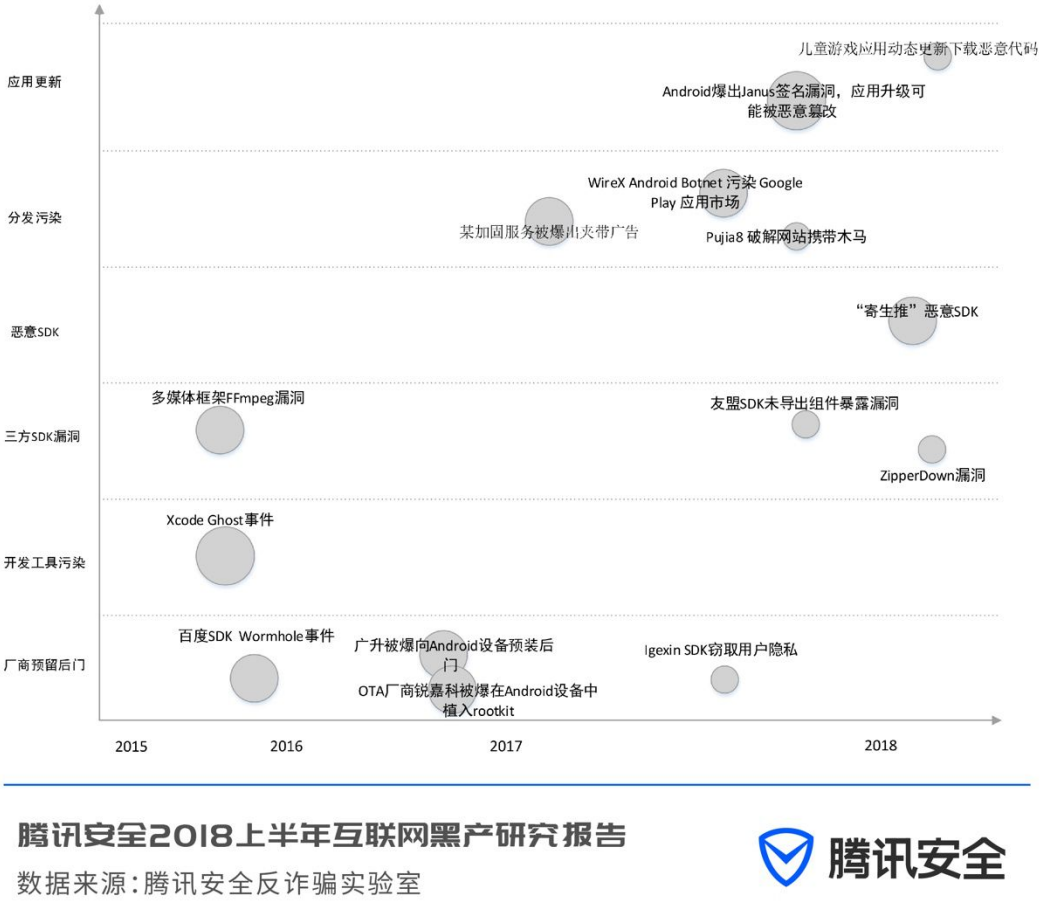
1）针对供应链下游（分发环节）攻击的安全事件占据了供应链攻击的大头，受影响用户数多在百万级别，且层出不穷。类似于 XcodeGhost 这类污染开发工具针对软

件供应链上游（开发环境）进行攻击的安全事件较少，但攻击一旦成功，却可能影响上亿用户。

2）第三方 SDK 安全事件和厂商预留后门也是 Android 供应链中频发的安全事件，这类攻击大多采用了白签名绕过查杀体系的机制，其行为也介于黑白之间，从影响用户数来说远超一般的漏洞利用类攻击。

3）从攻击的隐蔽性来讲，基于供应链各环节的攻击较传统的恶意应用来说，隐蔽性更强，潜伏周期更久，攻击的发现和清理也都比较复杂。

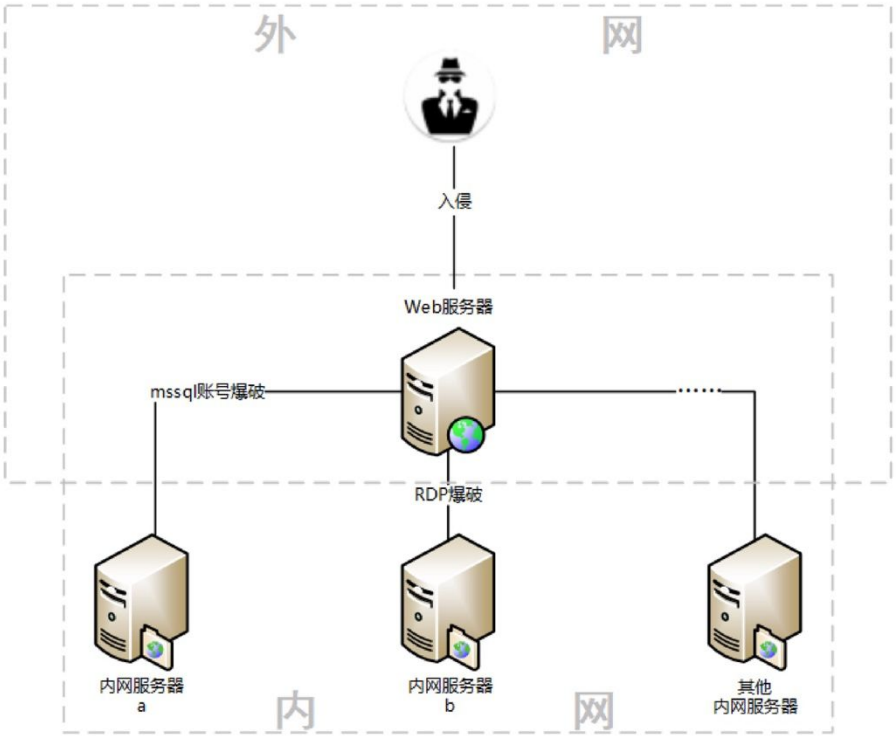
4）针对供应链各环节被揭露出来的攻击在近几年都呈上升趋势，在趋于更加复杂化的互联网环境下，软件供应链所暴露给攻击者的攻击面越来越多，并且越来越多的攻击者也发现针对供应链的攻击相对针对应用本身或系统的漏洞攻击可能更加容易，成本更低。



二、PC 端黑色产业链日趋成熟，攻击更加精准化

1.勒索病毒解密产业链，对企业及公共机构造成严重威胁

2018 年，大量企业、政府机关和公共服务机构由于遭遇勒索病毒，生产系统数据被加密破坏，重要业务系统陷入崩溃。勒索病毒攻击者利用各种手段尝试入侵重要机构网络系统，例如通过弱口令漏洞入侵企业网站，再将企业 Web 服务器作为跳板，渗透到内网，然后利用强大的局域网漏洞攻击工具将勒索病毒分发到内网关键服务器，将企业核心业务服务器、备份服务器数据加密。

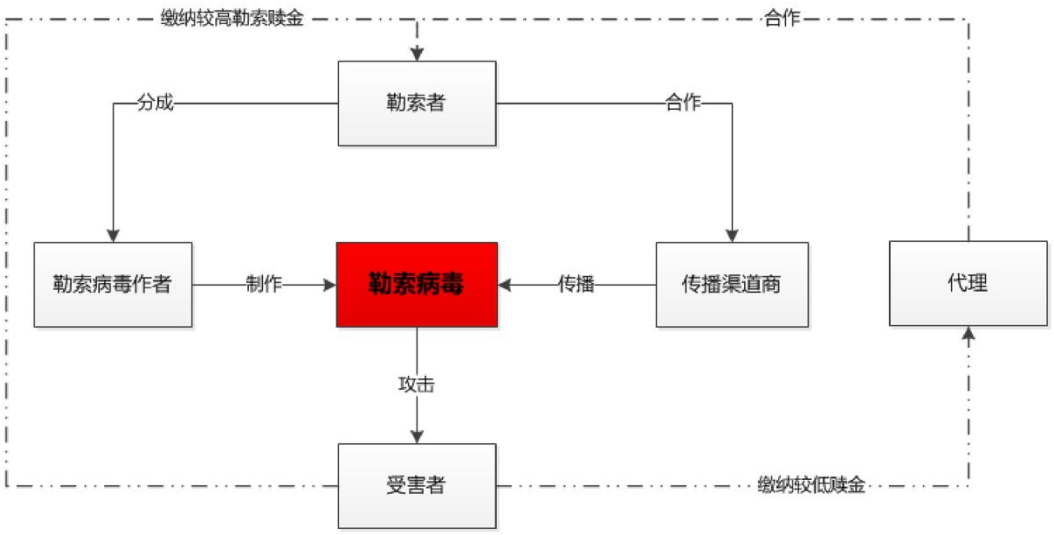


腾讯安全2018上半年互联网黑产研究报告

图片来源：腾讯御见威胁情报中心

腾讯安全

病毒一旦得手，企业日常业务立刻陷于崩溃状态，关键业务因此停摆。如果企业网管发现连备份系统也一样被破坏了。那基本只剩下一条路：缴纳赎金。众所周知，勒索病毒的加密技术是高强度的非对称加密，除非得到密钥，解密在理论上都是不可能的。正因为如此，腾讯御见威胁情报中心监测发现了这个不为人知的奇葩产业链：勒索病毒解密产业链。



腾讯安全2018上半年互联网黑产研究报告

图片来源：腾讯御见威胁情报中心

腾讯安全

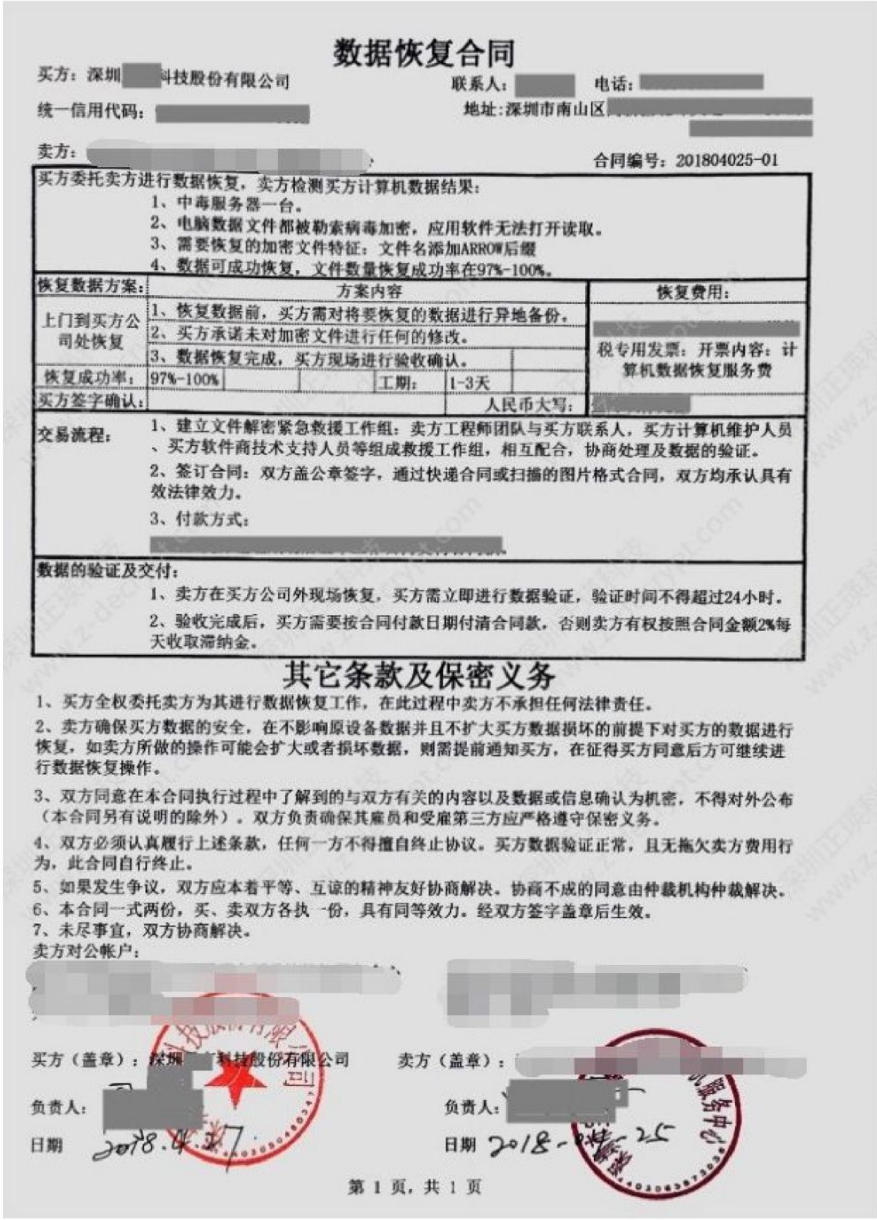
该产业链的从业者甚至通过购买搜索引擎关键字广告来拓展业务。

腾讯安全2018上半年互联网黑产研究报告

图片来源：网络

腾讯安全

当受害企业寻求解决办法时，正规的安全厂商往往会回复，“没有备份数据就找不回来了”。而受害企业通过互联网上的方法寻找到的解密服务商，这些人充当了受害企业联系勒索病毒传播者的中介，相对受害企业，更熟悉虚拟数字币的交易，在一番讨价还价之后，代理受害企业买回解密密钥，从而解密数据。某些情况下，亦不能排除负责解密的中介机构，是否和勒索病毒传播者之间存在某些联系。



数据恢复合同

买方：深圳[redacted]科技股份有限公司　　联系人：[redacted]　电话：[redacted]

统一信用代码：[redacted]　　地址：深圳市南山区[redacted]

卖方：[redacted]　　合同编号：201804025-01

买方委托卖方进行数据恢复，卖方检测买方计算机数据结果：
1、中毒服务器一台。
2、电脑数据文件都被勒索病毒加密，应用软件无法打开读取。
3、需要恢复的加密文件特征：文件名添加ARRO#后缀
4、数据可成功恢复，文件数量恢复成功率在97%-100%。

恢复数据方案：	方案内容			恢复费用：
上门到买方公司处恢复	1、恢复数据前，买方需对将要恢复的数据进行异地备份。 2、买方承诺未对加密文件进行任何的修改。 3、数据恢复完成，买方现场进行验收确认。			[redacted] 税专用发票：开票内容：计算机数据恢复服务费
恢复成功率：	97%-100%	工期：	1-3天	
买方签字确认：		人民币大写：	[redacted]	

交易流程：
1、建立文件解密紧急救援工作组：卖方工程师团队与买方联系人，买方计算机维护人员、买方软件商技术支持人员等组成救援工作组，相互配合，协商处理及数据的验证。
2、签订合同：双方盖公章签字，通过快递合同或扫描的图片格式合同，双方均承认具有效法律效力。
3、付款方式：[redacted]

数据的验证及交付：
1、卖方在买方公司外现场恢复，买方需立即进行数据验证，验证时间不得超过24小时。
2、验收完成后，买方需要按合同付款日期付清合同款，否则卖方有权按照合同金额2%每天收取滞纳金。

其它条款及保密义务

1、买方全权委托卖方为其进行数据恢复工作，在此过程中卖方不承担任何法律责任。
2、卖方确保买方数据的安全，在不影响原设备数据并且不扩大买方数据损坏的前提下对买方的数据进行恢复，如卖方所做的操作可能会扩大或者损坏数据，则需提前通知买方，在征得买方同意后方可继续进行数据恢复操作。
3、双方同意在本合同执行过程中了解到的与双方有关的内容以及数据或信息确认为机密，不得对外公布（本合同另有说明的除外）。双方负责确保其雇员和受雇第三方应严格遵守保密义务。
4、双方必须认真履行上述条款，任何一方不得擅自终止协议。买方数据验证正常，且无拖欠卖方费用行为，此合同自行终止。
5、如果发生争议，双方应本着平等、互谅的精神友好协商解决。协商不成的同意由仲裁机构仲裁解决。
6、本合同一式两份，买、卖双方各执一份，具有同等效力。经双方签字盖章后生效。
7、未尽事宜，双方协商解决。

卖方对公帐户：[redacted]

买方（盖章）：深圳[redacted]科技股份有限公司　　卖方（盖章）：[redacted]

负责人：[redacted]　　负责人：[redacted]

日期 2018.4.27　　日期 2018-[redacted]-25

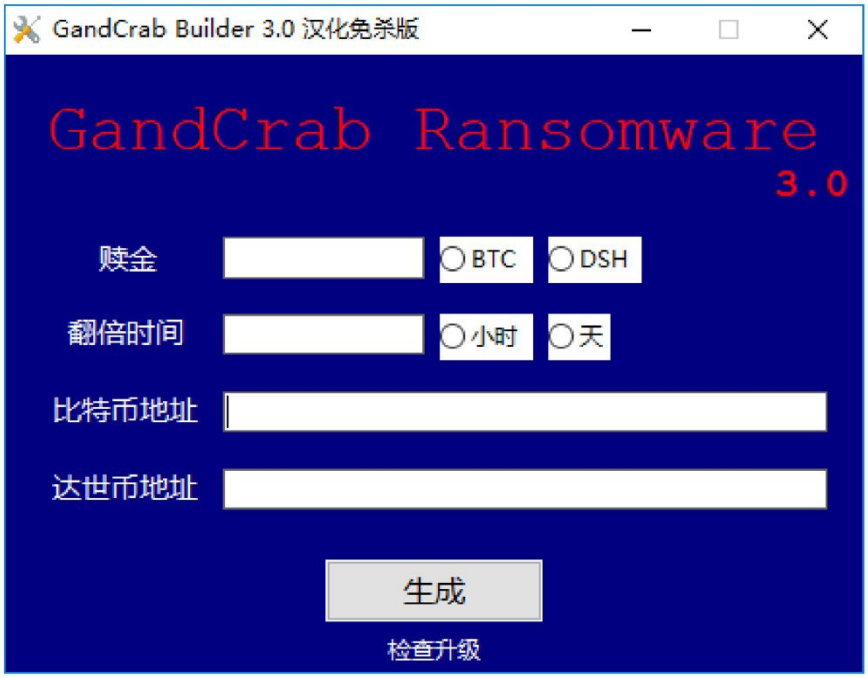
第 1 页，共 1 页

腾讯安全2018上半年互联网黑产研究报告

图片来源：网络

腾讯安全

除此之外，勒索病毒传播链本身也有专业分工，有人负责制作勒索病毒生成器，交给有网站资源的人分发，各方参与利益分成。



腾讯安全2018上半年互联网黑产研究报告

图片来源：网络

腾讯安全

2.控制肉鸡挖矿产业链，游戏外挂成挖矿木马“重灾区”

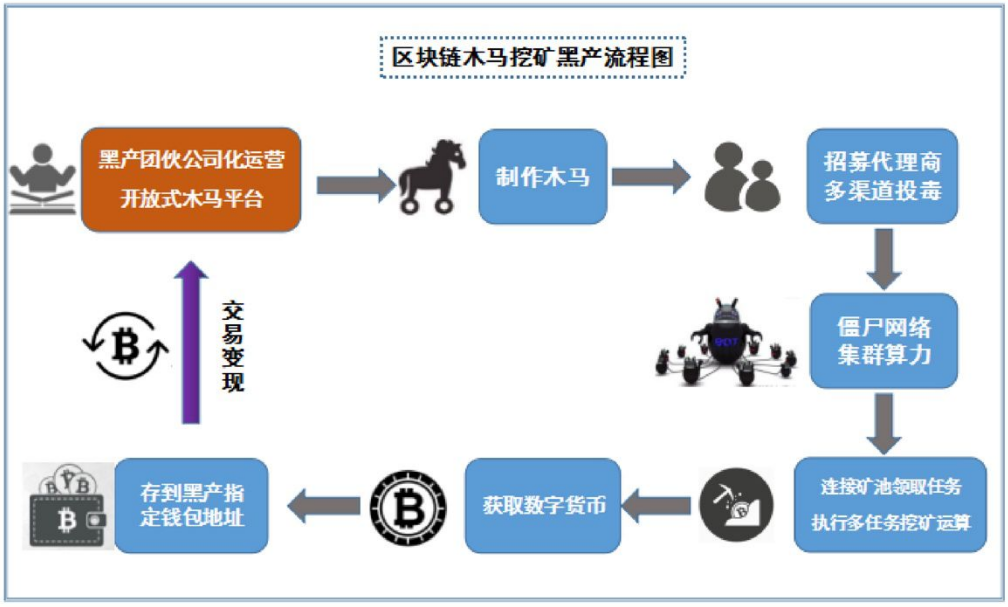
去年年底，温州市区一家公司的网站被恶意攻击，网警梳理线索时，发现犯罪嫌疑人徐某有重大嫌疑，经过调查，警方果然发现一个利用漏洞安装挖矿木马的犯罪团伙。该团伙有 12 名成员，利用漏洞攻击别人电脑，获利控制权之后，植入挖矿木马。专案组查明 这一团伙共租赁 20 余台服务器远程控制了 5000 余台“肉鸡” 非法挖矿 1000 余枚门罗币等数字货币（价值约 60 余万元）。

无独有偶，2017 年底，腾讯电脑管家通过安全大数据监测发现，一款名为“tlMiner”的挖矿木马在 2017 年 12 月 20 日的传播量达到峰值，当天有近 20 万台机器受到该挖矿木马影响。此次发现的“tlMiner”挖矿木马，植入在“吃鸡”游戏（steam 版绝地求生）外挂“吃鸡小程序”中。由于“吃鸡”游戏对电脑性能要求较高，黑产团伙瞄准“吃鸡”玩家、网吧的高配电脑，搭建挖矿集群。

腾讯电脑管家团队立即配合守护者计划将该案线索提供给警方，协助山东警方于 2018 年 3 月初立案打击“tlMiner”木马黑产。据分析，“tlMiner”木马作者在“吃鸡”游戏外挂、海豚加速器（修改版）、高仿盗版腾讯视频网站（dy600.com）、酷艺影视网吧 VIP 等程序中植入“tlminer”挖矿木马，通过网吧联盟、QQ 群、论坛、下载站和云盘等渠道传播。

腾讯电脑管家安全团队继续加深对挖矿木马黑产链条的研究，协助警方深挖，进一步分析挖掘到木马作者上游：一个公司化运营的大型挖矿木马黑色产业链。4 月 11 日，警方在辽宁大连一举查封该挖矿木马黑产公司。

该公司为大连当地高新技术企业，为非法牟利，搭建木马平台，招募发展下级代理商近 3500 个，通过网吧渠道、吃鸡外挂、盗版视频软件传播投放木马，非法控制用户电脑终端 389 万台，进行数字加密货币挖矿、强制广告等非法业务，合计挖掘 DGB（极特币）、HSR（红烧肉币）、XMR（门罗币）、SHR（超级现金币）、BCD（比特币钻石）、SIA（云储币）等各类数字货币超过 2000 万枚，非法获利 1500 余万元。



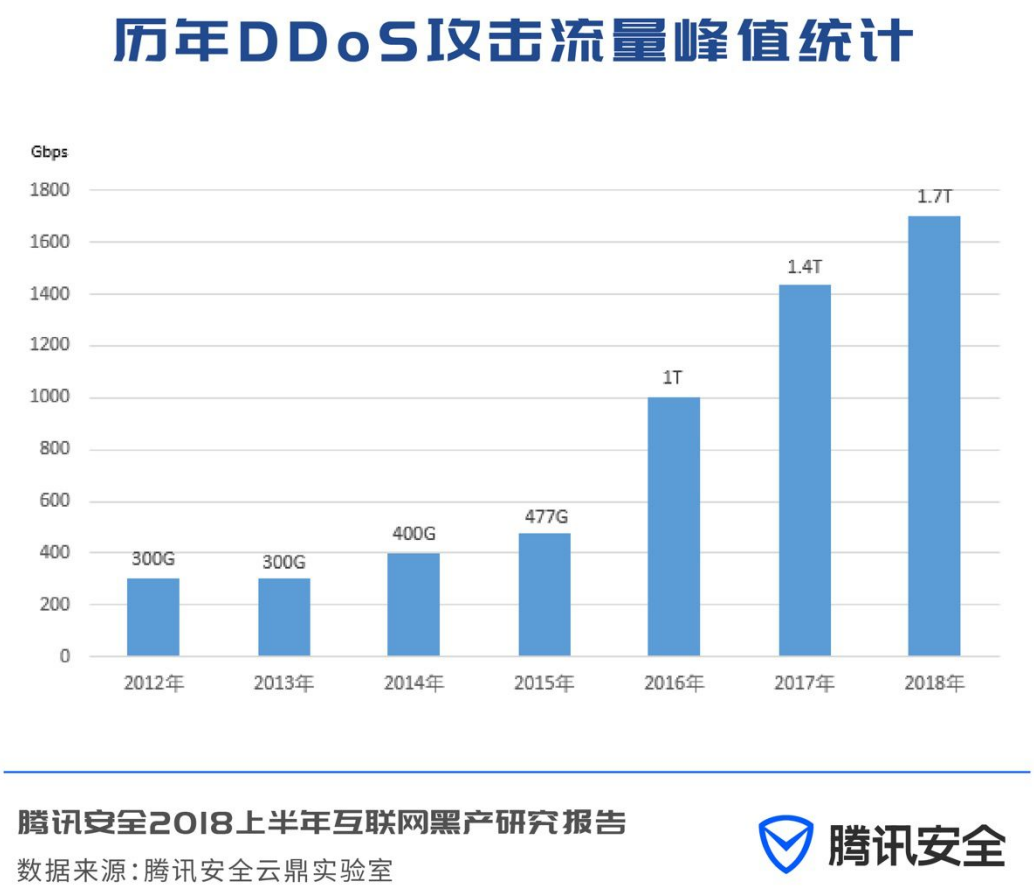
腾讯安全2018上半年互联网黑产研究报告

图片来源：腾讯电脑管家

腾讯安全

3.DDoS 攻击技术不断演进，团伙作案趋势明显

DDoS 攻击在分工上由工具开发者向人员多维化发展，也出现了技术、销售、渠道等分工，在 DDoS 攻击产业链中一般称为接发单人、担保商、肉鸡商、攻击软件开发人员等。随着 DDoS 的新技术不断的被挖掘出来，DDoS 攻击正在规模化、自动化、平台化的发展。由于 DDoS 在技术与平台上始终是站在互联网的最前沿，往往我们看到一个峰值的出现，便是互联网的一场灾难。



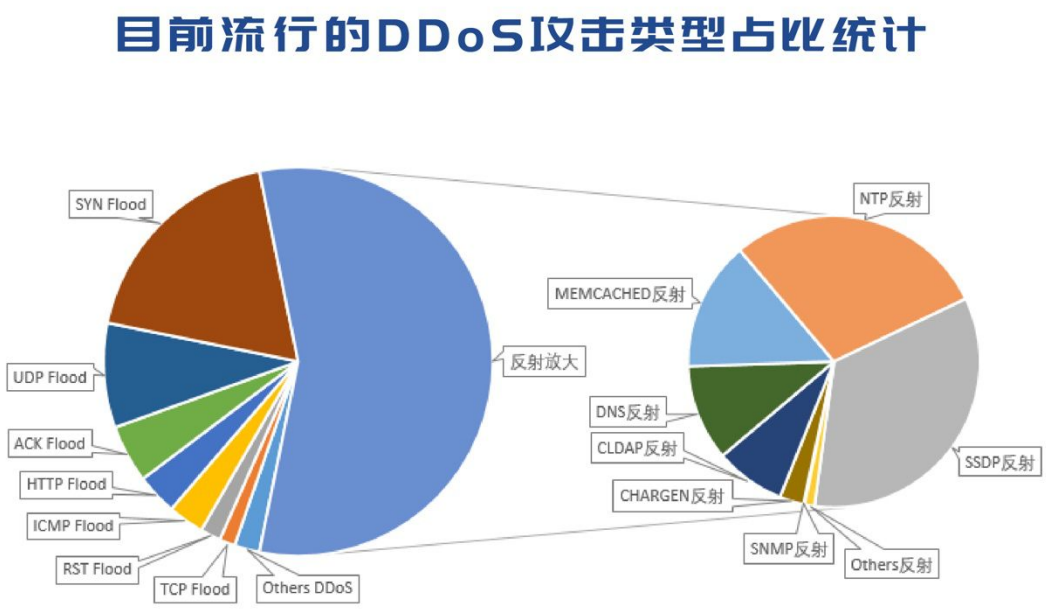
每一个攻击类型的出现或每一个攻击类型的技术的更新，都是一场攻击者的狂欢，例如今年的 Memcached 反射放大攻击，不仅仅在技术上达到了 5 万倍的反射放大效果，而且在流量上更是达到了 1.7Tbps 的峰值效果。

1）DDoS 的攻击类型

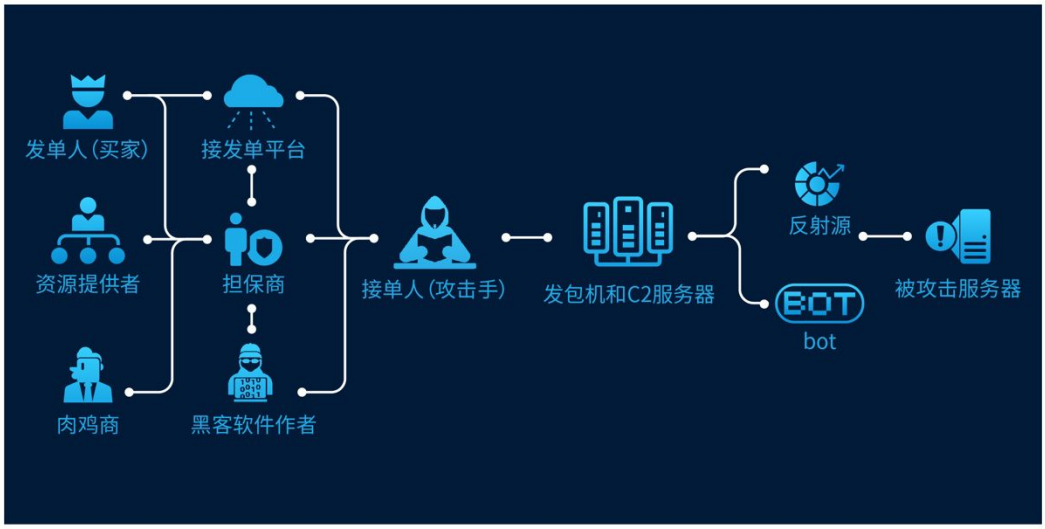
SYN Flood 做为早期的攻击类型，占比近 20%，主要原因是其攻击效果有良好的穿透力，无论是在攻击服务器，还是中间的基础网络设施上，都能在到良好的效果。

同样 UDP Flood 以其数据包构造灵活的特点仍占有大量比重。占比最大的是排名第一的反射放大攻击（占比 60%），反射放大以其攻击成本小、构造发包简单、反射倍数高、在自动化平台后端调用方便等特点，成为流量攻击中的首选。

在流行的 DDoS 攻击类型占比统计中,以 IoT 设备为反射源的 SSDP 反射放大已连续几年都占比最高，今年的一支新秀 Memcached 反射也没有盖过其占比的锋芒。



因为攻击手法的增多，DDoS 攻击效果立竿见影，利用 DDoS 进行勒索、攻击竞争对手的情况越来越普及；催生了 DDoS 黑色产业链越来越细化，除发单人、担保商、黑客软件作者外，又增加了肉鸡商、接单人、资源提供者、接发单平台几个维度。



腾讯安全2018上半年互联网黑产研究报告

图片来源：腾讯安全云鼎实验室

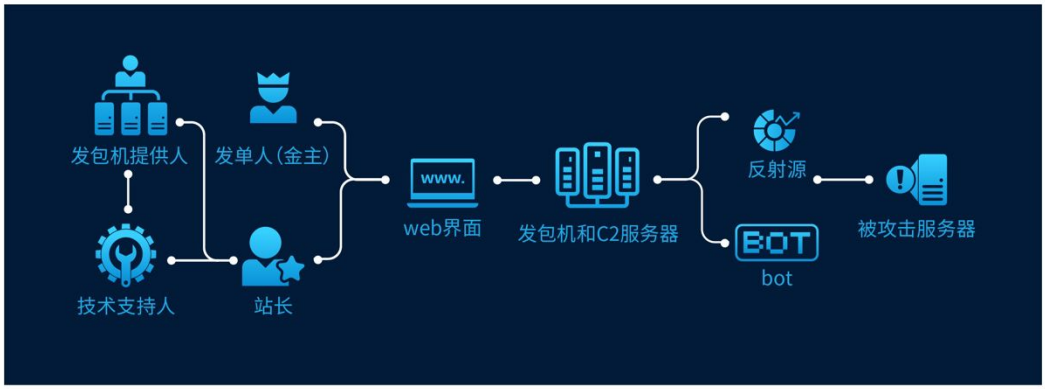
腾讯安全

在巨大经济利益面前，DDoS 攻击黑产在多个环节逐渐完成自动化，使整个链条无需人工参与，发单人直接在 DDoS 平台下单，我们称这样的平台为“页端 DDoS 攻击平台”。

“页端 DDoS 攻击平台”包括用户注册、套餐付费、攻击发起等一系列操作，且在用户侧都可以完成，不需要其他人员参与。页端 DDoS 攻击平台在发起攻击时，是以 API 形式调用发包机或支持 API 的 C2 服务器进行攻击，延迟时间一般小于 10 秒；对

比传统 DDoS 攻击来看，已完成了全自动的无人值守攻击方式。页端 DDoS 攻击平台其高度集成管理，在成单率、响应时长、攻击效果等方面都得到了可行的解决。

在平台化外，DDoS 攻击类型也有长足的发展。例如 IoT（物联网）僵尸网络的典型代表 mirai 针对互联网基础架构服务提供商 Dyn DNS(如今的 Oracle DYN)进行功击。今年 3 月份的 Memcached 反射更是一剂强心针，以 5 万的反射放大倍数、1.7Tbps 的流量峰值再一次刷新了 DDoS 的认知。



腾讯安全2018上半年互联网黑产研究报告

图片来源：腾讯安全云鼎实验室

腾讯安全

2）DDoS 攻击典型案例--“暗夜”攻击团伙案

DDoS 攻击黑产会严重影响企业线上业务开展，腾讯云鼎实验室曾配合公安机关破获暗夜 DDoS 攻击团伙案，该团伙攻击对某客户的游戏业务产生严重影响，玩家访问缓慢，登录掉线，甚至完全没有响应。

腾讯云鼎实验室根据系统日志判断为大流量持续 DDoS 攻击，单日攻击流量峰会达462G，该团伙掌握的 DDoS 攻击资源十分庞大。腾讯云鼎实验室通过努力，最终在该团伙控制的其中一台 C2 服务器发现可疑线索，通过流量、日志、关联等多维度的数据分析，最终定位到证据所在，公安机关根据这些信息在境外将暗夜 DDoS 黑产团伙一网打尽。

三、互联网黑产对抗的技术趋势与实践

1.人工智能成移动端黑产对抗技术突破口

移动黑产以趋利为目的，为了保护自己的利益，黑产从业人员会想尽一切办法来隐藏自己，与安全厂商之间的对抗也愈发激烈。根据多年积累的对抗经验，腾讯安全团队认为移动黑产对抗技术发展主要有以下几个方向：

1）立体式安全检测体系

从应用传播、应用安装、应用运行、应用变现等维度，将各种安全检测手段融入到应用的不同生命周期。如接入 URL 安装检测引擎可以在下载阶段即可阻断恶意行为继续，又如行为检测引擎可以在病毒执行敏感操作时候及时阻止避免进一步破坏操作。

2）用户端侧的主动防御

安全厂商使用的传统静态引擎由于缺乏真实的行为数据，黑产团伙很容易就可以突破其防线。不管黑产采用多少种先进的对抗手段，其最终的目的还是通过执行恶意行为

来实现牟利的目的，手机厂商通过系统层原生集成应用敏感行为检测点，真实的捕获到恶意行为。数据脱敏以后可以辅助深度学习等方法实现更快，更准确的检测效果。

3）引入人工智能算法，智能识别未知样本

传统杀毒引擎从病毒的发现到检出会存在一段时间的空窗期(比如样本的收集)。安全研究人员可以将丰富的人工经验，通过深度学习技术，泛化成通用的病毒检测模型，提升未知病毒的检出能力。

腾讯安全团队基于第三种思路研发的腾讯 TRP-AI 反病毒引擎已经在腾讯手机管家云引擎中得到应用，并且该技术通过深入集成的方式在魅族 Flyme7 系统中率先全面应用。集成 TRP 反病毒引擎的系统新病毒发现能力提升 8.3%，新检出病毒中使用云加载技术的占比 60.1%，使用加固加壳技术的占比 12.%，并且病毒平均潜伏期为 35min。

2.化被动为主动的 PC 端黑产对抗技术

伴随互联网产业的加速发展，PC 端黑产技术也在不断进化。为了最大限度获利，黑产会尽可能在用户电脑驻留存活更长时间。同时，2018 年区块链的火爆令加密山寨币迅速成为黑色产业地下流通的硬通货，通过挖矿获取山寨虚拟加密币，使得黑产变现链条更加直接。为了更好地狙击 PC 端黑产，安全厂商的对抗技术主要包括以下方面：

1）更快速的安全漏洞响应机制

安全漏洞始终是网络攻击的绝佳通道，0day 漏洞往往被应用在高价值目标的精准攻击上。2018 年“永恒之蓝”漏洞攻击包被经常提起，这个武器级的漏洞攻击包在被

黑客完全公开后，一度被黑产广泛使用，成为入侵企业网络、传播勒索病毒，植入挖矿木马的利器。

网络黑产可以在极短的时间内将 Windows 已经发布补丁的高危漏洞迅速利用起来，然而，目前仍有大部分的网民因为使用盗版系统等种种原因，补丁安装率普遍不高。这种现状使得漏洞攻击工具在补丁发布之后很长时间，都大有用武之地。杀毒软件更新补丁修复功能，对于帮助这类用户排除干扰，修补系统漏洞起到了关键作用。

对于一些突然爆发的 0day 漏洞，也需要安全软件进行提前防御。2018 年，Office 公式编辑器漏洞和 Flash 0day 漏洞是黑产利用最广泛的攻击武器，利用此类漏洞进行攻击，用户打开一个 Office 文档或浏览一个网页也可能立即中毒。腾讯电脑管家针对攻击者的这一特性集成“女娲石”防御技术，可以让电脑在即使遭遇部分 0day 攻击时，也能够实现有效拦截。补丁修复方案的升级，让腾讯电脑管家用户电脑的漏洞修复率大幅上升，黑产作案的技术成本也明显提升。

2）对抗勒索病毒破坏的数据备份机制

2017 年，以 WannaCry 为首的勒索病毒采取相对盲目的广撒网式破坏，却并未因勒索病毒的广泛传播而取得足够的经济回报：绝大多数的普通用户在遭遇勒索病毒攻击之后，放弃了缴纳赎金解锁数据，而是选择重装系统。对于网络黑产来说，这类广撒网式攻击损人不利己，攻击者开始转向针对高价值目标的精确打击。通过系统漏洞、社会工程学欺骗、精心设计的钓鱼邮件来诱使目标用户运行危险程序。

然而，勒索病毒的感染量下降了，勒索病毒造成的损失却依然严重：许多重要信息系统被勒索病毒破坏，受害者被迫支付赎金。面对勒索病毒越来越精准的打击，高价值用户需要更加完善的数据保护方案，腾讯电脑管家迅速升级“文档守护者”功能，通过充分利用用户电脑冗余的磁盘空间自动备份数据文档，既使电脑不幸染毒，数据文档被加密，也能通过文档守护者来恢复文档，尽最大可能减小损失。

3）能够揭示黑产全貌的威胁情报系统

为逃避杀毒软件的查杀，病毒木马的行为变得更加隐蔽，病毒样本的更新、木马控制服务器的变化的速度都比以往更快，部分攻击者甚至会限制恶意程序扩散的范围，黑产的攻击正在变得愈发难以捕捉和缺少规律性。

腾讯御见威胁情报系统基于安全大数据分析的处理系统，通过分析成千上万个恶意软件的行为并创建一系列的规则库，再利用这些规则去匹配每个新发现的网络威胁，像完成一幅拼图一样，将一个个分散的病毒木马行为完整拼接，从中发现木马病毒的活动规律，追溯病毒木马传播的源头。2018 年，腾讯御见威胁情报系统已成功协助警方破获多起网络黑产大案，成为打击黑产的有力武器。

四、2018 年下半年的安全趋势分析

1.MAPT 攻击威胁持续上升，移动设备或成重大安全隐患

2018 年随着互联网+进程的不断推进，通过智能设备我们可以享受到非常便捷的移动互联网服务，如移动医疗服务，社保服务，电子身份证，电子驾照等政府贴心的民生

服务。同时也有大量的企业和政府部门开始习惯通过智能终端来管理内部工作，这些基于智能手机的服务方便大众的同时，也暴露出巨大的安全隐患：移动互联网时代的智能手机承载着全面而巨量的个人和组织的隐私数据，一旦个人智能手机被操控，黑客团伙通过这个设备获取到各种敏感数据，从而导致不可估量的损失。

虽然目前主流关于 APT 的讨论仍集中于 PC 电脑，但是趋势表明 APT 攻击组织正在往网络军火库中添加 MAPT(Mobile Advanced Persistent Threat)武器以获得精准而全面的信息。比如 APT-C-27 组织从 2015 年开始更新维护基于安卓的 RAT 工具，利用这些工具来收集用户手机上的文档、图片、短信、GPS 位置等情报信息。Skygofree 会监控上传录制的 amr 音频数据，并尝试 root 用户设备以获取用户 whatsapp.facebook 等社交软件的数据。Pallas 则全球部署试图攻击包括政府、军队、公用事业、金融机构、制造公司和国防承包商的各类目标。

全平台覆盖加上国家级黑客团队攻击技术的加持，无边界智能办公时代被忽视的移动智能设备正在成为重大安全隐患，MAPT 正在威胁企业，重点机构乃至政府部门。它们需要拥有移动/PC 一体化反 APT 安全解决方案。

2.恶意应用的检测和反检测对抗将愈发激烈，安全攻防进入焦灼局势

黑产团伙对抗技术日趋完善，安全攻防进入焦灼局势，并且传统安全监测方案正在逐渐处于劣势的一方。一方面在巨大利益的驱使下企业化运作的黑产团伙有更多的财力开发基于云加载技术的恶意应用(恶意代码变得很难捕获)，并且有充沛的人力进行免杀对抗(传统引擎基于特征检测，很容易被免杀绕过)。另一方面一些供应链的厂商也在知

情或不知情的情况下成为黑产团伙的保护伞，在自己的框架中引入包含恶意功能的 SDK，导致有大量的恶意应用潜伏一年甚至数年才被新技术手段发现。

3.黑产团伙拓宽安卓挖矿平台市场，移动挖矿应用或迎来爆发

相比电脑平台，移动智能设备普及率高，使用频率极高，但是移动设备受限于电池容量和处理器能力，而且挖矿容易导致设备卡顿、发热、电池寿命下降，甚至出现手机电池爆浆等物理损坏，移动平台似乎并不是一个可用于可持续挖矿的平台。

随着移动设备性能不断提升，2018 年黑产团伙还在尝试利用手机平台生产电子货币。比如 HiddenMiner 潜伏于三方应用市场诱导用户下载，然后控制用户手机设备窃取 Monero，又如 ADB.Miner 通过端口扫描的方式发现基于安卓的 TV 设备进行挖矿，还发现过多起 Google play 官方应用市场应用包含挖矿恶意代码的事件，这些事件的不断发生预示这黑产团伙正在拓宽安卓挖矿平台市场。

4.勒索病毒攻击更加趋向于精准化的定向打击

御见威胁情报中心监测发现，勒索病毒正在抛弃过去无差别的广撒网式盲目攻击，而是转向高价值的攻击目标进行精确打击。攻击者利用系统漏洞或精心构造的钓鱼邮件入侵企业网络，渗透到企业内网之后，选择最有可能敲诈成功的高价值数据来加密勒索

2018 年上半年较多的教育机构、医疗机构、进出口贸易企业、制造业等高价值目标的计算机系统被勒索病毒攻击，这一趋势正变得日益明显。同时，这意味着高价值目标需要加强安全防护，特别重要的是做好系统漏洞修补和关键业务数据的备份。

5.挖矿病毒比重明显增大，手段更加隐蔽

挖矿病毒正在成为最常见的病毒类型，因为区块链相关产业的火爆，各种流行的虚拟加密货币可以在交易所直接获利。除非区块链相关的空气币泡沫破灭，否则挖矿病毒都将是最直接的黑产赢利模式，远超前几年流行的盗号木马。

比特币挖矿需要高性能的矿机运行，成本高昂，对控制肉鸡挖矿来说，性价比太低。挖矿病毒大多利用受害电脑的 CPU 资源挖山寨币，而且为了避免被受害者发现，很多挖矿病毒对系统资源的消耗控制更严。

监测发现，大量挖矿病毒会限制 CPU 资源消耗的上限，当用户在运行高资源消耗的程序时，暂时退出挖矿；在用户系统闲置时全速挖矿等等。挖矿病毒也基本限于三种形式：普通客户端木马挖矿、网页挖矿（入侵网站，植入挖矿代码，打开网页就挖矿），入侵控制企业服务器挖矿。

6.高级可持续性 APT 攻击威胁距离普通人越来越近

高级可持续性威胁（简称 APT），是利用先进的攻击手段对特定目标进行长期持续性网络攻击的攻击形式。安全厂商近期披露的跨国 APT 组织，利用高价值安全漏洞，构造精准欺诈邮件，利用所有可能的方式入侵目标网络，窃取情报，破坏目标系统。

除了以上高价值目标，腾讯御见威胁情报中心发现，部分商业化的黑客组织，可能正在使用 APT 攻击的方式针对普通企业，目标是获得商业情报，出售给特定买家。使

得比较接近高价值目标的商业机构，也成为下一个 APT 攻击的领域。而普通企业的网络安全防护体系，远弱于国家、政府、大型企业网络，更容易成为 APT 攻击的受害者。

7.刷量刷单类灰色产业依然严重

互联网创新企业容易遭遇羊毛党的攻击，国家实行实名制对网络服务帐号严格管理，但随着物联网的兴起，大量未实行实名制的物联网卡流入市场。羊毛党大量买入物联网卡，注册大量帐号待价而沽。这些虚假帐号在刷单刷量的薅羊毛产业中普通使用，打造虚假繁荣，给相关企业造成严重损失。

腾讯安全联合实验室

腾讯电脑管家 | 腾讯手机管家 | 腾讯云