安天 ANTIY

2015年网络安全威胁的回顾与展望

2015

Antiy Annual Security Report

初稿完成时间：2015 年 12 月 08 日 14 时 21 分

首次发布时间：2016 年 01 月 07 日 09 时 00 分

本版更新时间：2016 年 01 月 17 日 17 时 30 分

安天安全研究与应急处理中心

目 录

1 导语

面对威胁高速演进变化、防御技术同样快速改善的现状，无论我们做怎样的努力，都已无法用一篇年报来涵盖网络安全威胁的全景，这亦使参与本文档编写的安天分析工程师们无比纠结。对于安天安全研究与应急处理中心（安天 CERT）来说，在数年前，年报工作是相对简单的，我们只需从恶意代码存储和分析的后台系统导出足够多的统计图表，就可以构成一篇年度报告。在网络安全领域，恶意代码自动化分析是一个成型较早的基础设施，恶意代码样本集更是一个非常容易进行统计的大集合，这一度让我们偏离了网络安全的本质，弱化了我们对保障用户价值的信念。

从去年开始，安天颠覆了自身传统的数据表年报的风格，面对当前威胁的纵深化、复杂化特点，大量简单的统计已经失去意义，我们非常明确地提出了做“观点型年报”的自我要求。尽管我们拥有更多的样本、更多的数据，但我们依然不敢说已经能够驾驭安全大数据，目前我们能做到的只有学习和思考，我们要学习更丰富的数据分析方式，我们要做能独立思考、有观点、有立场的安全团队，而非做大数据和计算资源的奴隶。

同时，我们也深知，我们自己的工作是局限的，安天的分析工作更多地是围绕如何防御高级持续性威胁（APT）攻击和恶意代码展开，我们坦诚面对自己对 WEB 安全、漏洞挖掘等领域技能积累的一贯不足。此外，由于安天 CERT 的部门分工所决定的分析视野的不同，本年报涉及到的移动安全相关内容较少，安天移动安全公司（AVL TEAM）后续会单独发布移动安全年报。

2 高级持续性威胁（APT）的层次分化

图 I 2015 年 APT 事件时间与地理位置分布

2.1 2015 年被曝光的高级持续性威胁（APT）事件

APT 攻击继续引领 2015 年的威胁大潮。从 2 月，方程式（Equation）组织浮出水面；到 5、6 月，APT-TOCS 和 Duqu2.0 相继露出峥嵘；再到 8 月，蓝白蚁（Blue Termitex）事件的公布，2015 年全年共曝光了十多起 APT 事件。虽然相较于 2014 年，曝光事件总体数量有所减少，但从威胁事件的影响力和技术水准来看，高水准的攻击手法、系统化的攻击平台、商用木马和标准化渗透平台的使用，使得方程式、Duqu2.0 和 APT-TOCS 等事件都极具代表性。

在 2015 年的 APT 事件中，“方程式（Equation）”[1]攻击是较早被披露且含金量极高的攻击事件。方程式（Equation）组织是一个活跃了近 20 年的攻击组织，其将 APT 的特点 P（持久化）展现的淋漓尽致。该组织不仅能够早于其他组织发现更多 0day 漏洞，且拥有一套用于植入恶意代码的超级制式信息武器库，其中最受关注、最具特色的攻击武器是两个可以对数十种常见品牌硬盘实现固件植入的恶意模块。作为一种高级的持久化手段，其既可以用于感染后的植入，也可以与臭名昭著的“物流链”劫持搭配使用。相比之前我们分析过的 BIOSKIT 和 BOOTKIT，该恶意模块具有更高的隐蔽性，更加难以分析。但多数被方程式（Equation）“光顾”过的节点，并未触发持久化功能，这说明该组织具有坚持获取高价值目标的原则。根据对相关硬盘固件接口的分析，我们认为，相关接口和参数的获取，通过人力和时间投入，依托技术文档

和逆向分析完全可以实现。因此，安天 CERT 不倾向于固件接口的获得是相关情报机构与产业界协作的结果，其更多体现出的是攻击组织及其资源体系强大的分析能力和坚定的作业意志，也包含其针对上游进行渗透作业的可能性。而方程式组织所采用的加密策略，则体现出了其作业的严密性，安天 CERT 于 2015 年 4 月发布的《方程式（EQUATION），组件加密策略分析》[2]，对此进行了进一步分析。

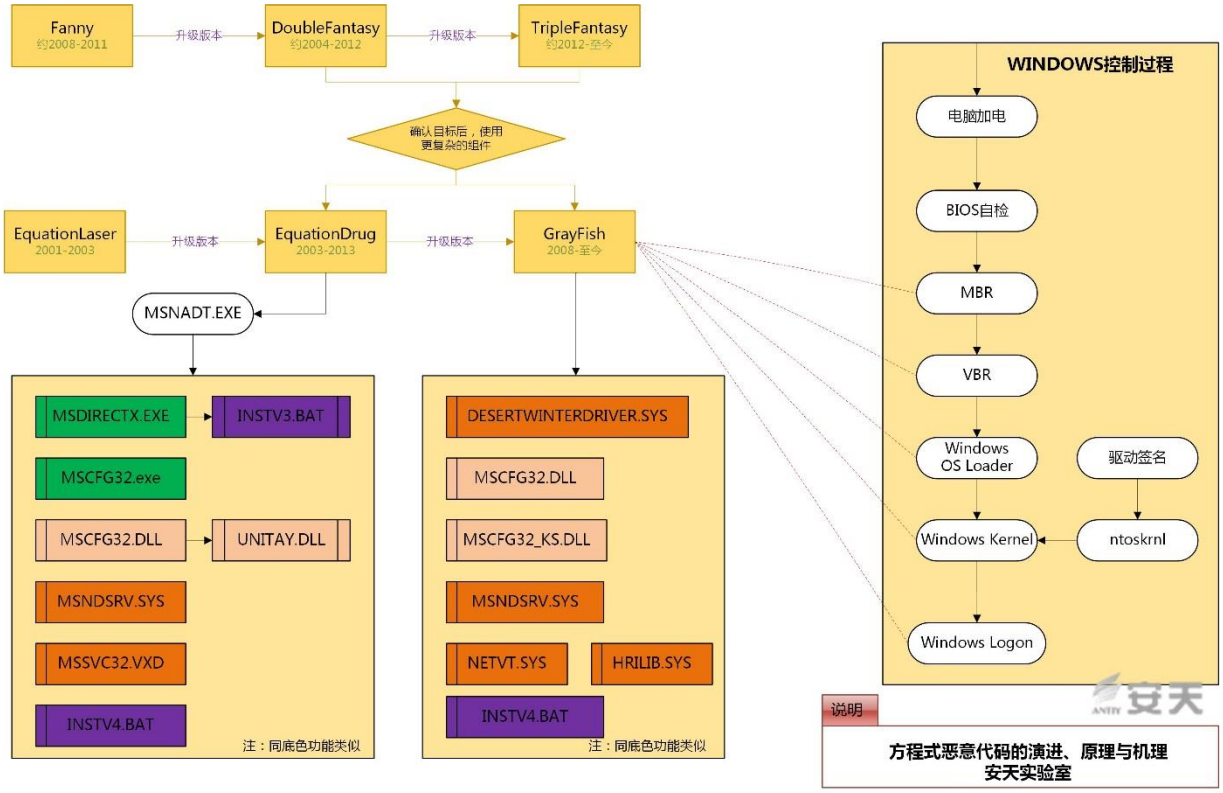

图 II 方程式（Equation）恶意代码的演进、原理与机理

2011 年后，没有安全厂商或组织报道 Duqu 继续活跃的迹象，业内一度认为其已经停止活动。然而在 2015 年初发现的一系列攻击事件中，出现了 Duqu 的全新版本，Duqu2.0 就此重装上阵，并对卡巴斯基进行了渗透攻击。Duqu2.0 的重要特点是恶意代码只会驻留在被感染机器的内存当中，利用漏洞执行内核级别的代码，硬盘中无法查到痕迹。虽然重启系统时恶意代码会被暂时清除，但是攻击者可以在直接联网的少数计算机中部署驱动程序，从而通过远程桌面会话或之前获得的用户凭证将 Duqu2.0 重新部署到整个平台。不得不说的是，像 Duqu 这样有着政府支持的高成本的 APT 攻击基础设施，不仅拥有复杂的、插件化模块体系，其作业组织也具备直接挑战世界顶级安全公司的自信。

与“方程式（Equation）”所拥有的装备武库和 Duqu2.0 强大的体系化能力相比，有些 APT 组织难有雄厚的资金支持、先进的武器储备和强大的攻击能力，特别是难以具备建制化的高水平攻击队伍，所以他们另辟蹊径，利用开放或商业化的标准化的渗透平台生成恶意代码和其他攻击载荷，向目标进行部署和攻击。2015 年 5 月，在安天发现的一例针对中国官方机构的攻击事件（APT-TOCS）[3]中，攻击者就是使用自动化

攻击测试平台 Cobalt Strike 生成了利用信标模式进行通信的 Shellcode，实现了对目标主机的远程控制能力。这种利用测试平台进行攻击渗透的方式以及无恶意代码实体文件、定时发送心跳包等行为在一定程度上可以规避主机安全防护软件的查杀与防火墙的拦截，同时对可信计算环境、云检测、沙箱检测等安全环节和手段均有对抗能力。该攻击控制目标主机的方式非常隐蔽，难以被发现，并且具备攻击多种平台的能力，如 Windows、Linux、Mac 等。经过线索关联，这一事件被认为与友商所公布的“海莲花”事件，源于同一攻击组织，但其作业方式与既往相比显现出较大差异。从本次事件的分析结果及我们长期的监控情况来看，商用木马、标准化的渗透平台等已经被广泛用于各种定向持续攻击中，特别是针对中国目标的攻击中。这种成本较低的攻击模式不仅降低了对攻击者能力和资源储备的要求，还导致对依托大数据分析来辨识线索链的过程产生更多的干扰，并使“编码心理学”等一些我们过去更擅长的分析方法失去作用。

2.2 日趋活跃的“商业军火”

传统意义的 APT 攻击更多地让人联想到精干的作业团队、强大的用于攻击的基础设施、专业的 0day 漏洞挖掘小组以及恶意代码的编写小组等。因此，多数的 APT 研究者更愿意把更多目光放在具有这些特点的事件上。但 APT-TOCS 等事件则用一种新的方式，为一些技术能力和资源相对有限的国家和组织提供了另一种选择。该事件也说明，随着攻击平台、商用木马和开源恶意工具的使用，网络军火被更加广泛的使用可能成为一种趋势。从安天过去的跟踪来看，这种威胁已经存在近五年之久，但依然缺乏有效检测这类威胁的产品和手段。安天 CERT 分析小组之所以将 APT-TOCS 事件定位为准 APT 事件，是因为该攻击事件一方面符合 APT 攻击针对高度定向目标作业的特点，同时隐蔽性较强、具有多种反侦测手段。但同时，与我们过去所熟悉的很多 APT 事件中，进攻方具备极高的成本承担能力与巨大的能力储备不同，其成本门槛并不高，事件的恶意代码并非由攻击者自身进行编写构造，商业攻击平台使事件的攻击者不再需要高昂的恶意代码的开发成本，相关攻击平台亦为攻击者提供了大量可选注入手段，为恶意代码的加载和持久化提供了配套方法，这种方式降低了攻击的成本，使得缺少雄厚资金、也没有精英黑客的国家和组织依托现有商业攻击平台提供的服务即可进行接近 APT 级的攻击水准，而这种高度“模式化”攻击也会让攻击缺少鲜明的基因特点，从而更难追溯。

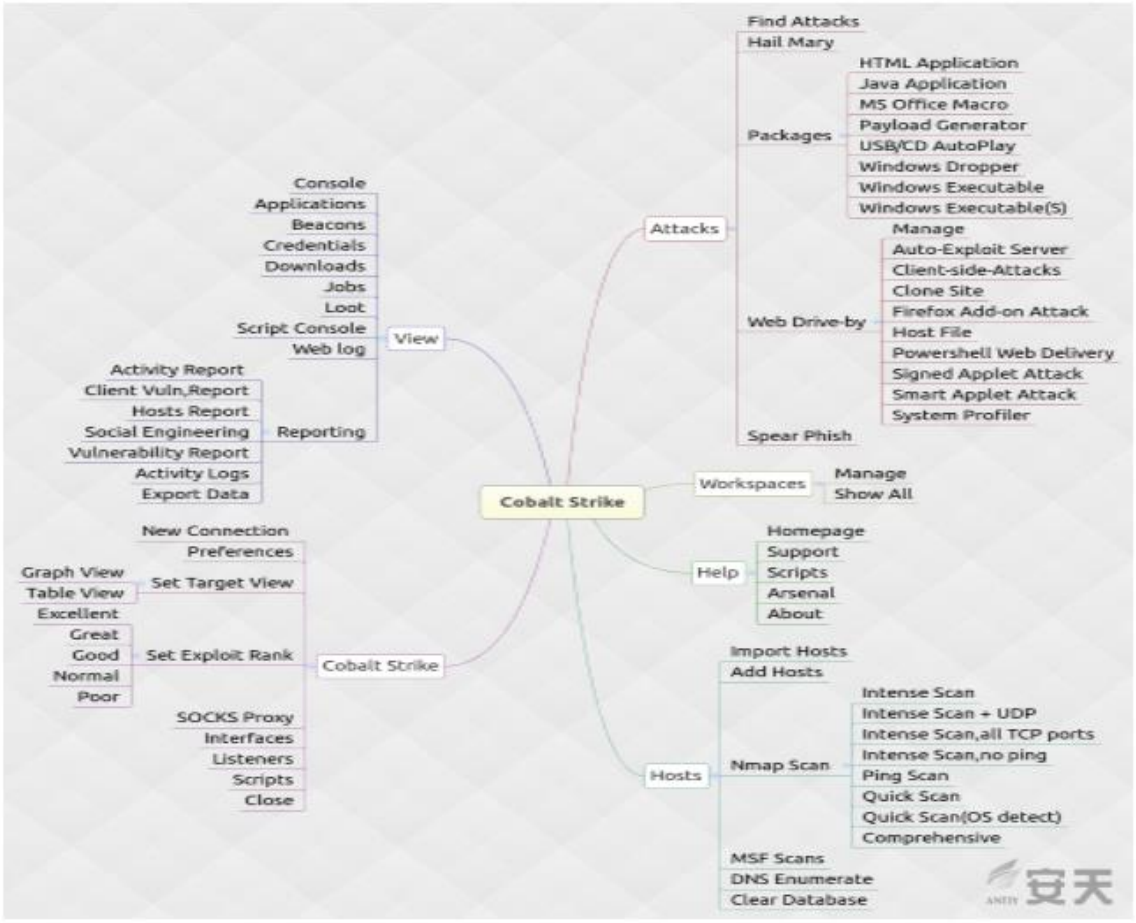

图 III Cobalt Strike 渗透测试平台的能力覆盖图

图 IV 安天对 APT-TOCS 攻击的可视化复现

与 APT-TOCS 事件中的 Cobalt Strike 所扮演的角色有所不同，Hacking-Team 是一个专门为攻击者提供工具和手段的公司。2015 年 7 月，由于遭到入侵，Hacking Team 逾 400G 数据泄露。关于 Hacking-Team 被盗了什么的问题，形象的回答就是“军火库、账房和衣橱都被洗劫了”。大量含源代码的木马程序、多个未公开的 0day 漏洞、电子邮件、商业合同、项目资料和监听录音遭到泄露，无异于向本就充满着威胁的网络环境投放了一枚重磅炸弹。这种具有商用水准的多平台木马的泄露，瞬间提升了黑产编写木马的能力，泄露的漏洞也迅速出现在一些普通的攻击中。

安天 AVL TEAM 亦发现类似 Giige 等商业手机木马，被攻击者用来攻击中国的机构和人员。

正如我们今年在 APT-TOCS 事件报告中指出的那样“鉴于网络攻击技术具有极低的复制成本的特点，当前已经存在严峻的网络军备扩散风险。商业渗透攻击测试平台的出现，一方面成为高效检验系统安全的有利工具，但对于缺少足够的安全预算、难以承担更多安全成本的国家、行业和机构来说，会成为一场噩梦。在这个问题上，一方面需要各方面建立更多的沟通和共识；而另一方面毫无疑问的是当前在攻防两端均拥有全球最顶级能力的超级大国，对于有效控制这种武器级攻击手段的扩散，应该负起更多的责任”。

2.3 APT 的层次化能力

近年来的 APT 事件中，超级 APT 组织拥有大量 0day 漏洞和豪华的攻击装备储备，甚至是“挥霍”0day 漏洞，而同时，我们一些攻击组织则利用现有平台和商用木马来完成的攻击事件；同样也有一些技术相对粗糙，手段亦不高明的攻击事件也同样体现出攻击方持续和定向攻击作业的特点。因此，我们不禁要问，近年来的攻击事件在攻击手法、能力和技术储备上存在诸多差异，那么究竟该以何种标准去定义 APT？

从技术能力、资源储备、攻击手段等方面综合考虑，安天将 APT 攻击能力细分为 A^2PT（“高级的”APT）、APT、准 APT、轻量级 APT 几个等级。A^2PT，顾名思义，就是高级的 APT，该命名我们受到 Michael Cloppert 的 《Why Stuxnet Isn't APT》一文启发。在 2015 年全年的 APT 事件中，我们前文介绍的“方程式”用修改硬盘固件的方式作为持久化支点，被称为“世界上最复杂的网络攻击”；Duqu2.0 沿用当年的 Duqu 和 Stuxnet 的思路，形成了系统化的攻击基础设施，并让卡巴斯基这样的世界级公司承认自己沦为此次事件的受害者。这些攻击组织综合能力明显具有领先一代的特点，因此他们是 A^2PT，我们也注意到一些同行称之为 GPT（上帝模式的 APT 攻击）。

而类似 HAVEX 这样具有较高攻击水准和较强资源储备的攻击，则毫无疑问是我们传统意义上的经典 APT 的代表。

然而，有一些攻击组织并不能与以上具有的较高的攻击水准和较强的资源储备的攻击组织相比，他们无论是技术水平还是资源储备，都逊色得多。为了完成攻击目标，攻击者只能开发水准较低的恶意代码，

或者直接利用现有的攻击平台和商用木马生成恶意代码。APT-TOCS 事件即由此而来，安天的分析人员经过对本次事件的分析，发现攻击者具有较高的攻击水准和持久、定向的攻击意图，然而经过更深层次的分析，我们发现，本次事件所体现的高水准竟是来源于 Cobalt Strike 这个自动化攻击测试平台。较高的攻击水准、持久化能力和与之相反的较低的研发成本相结合，成就了 APT-TOCS 事件，也让我们为之设定了“准 APT”的定义。

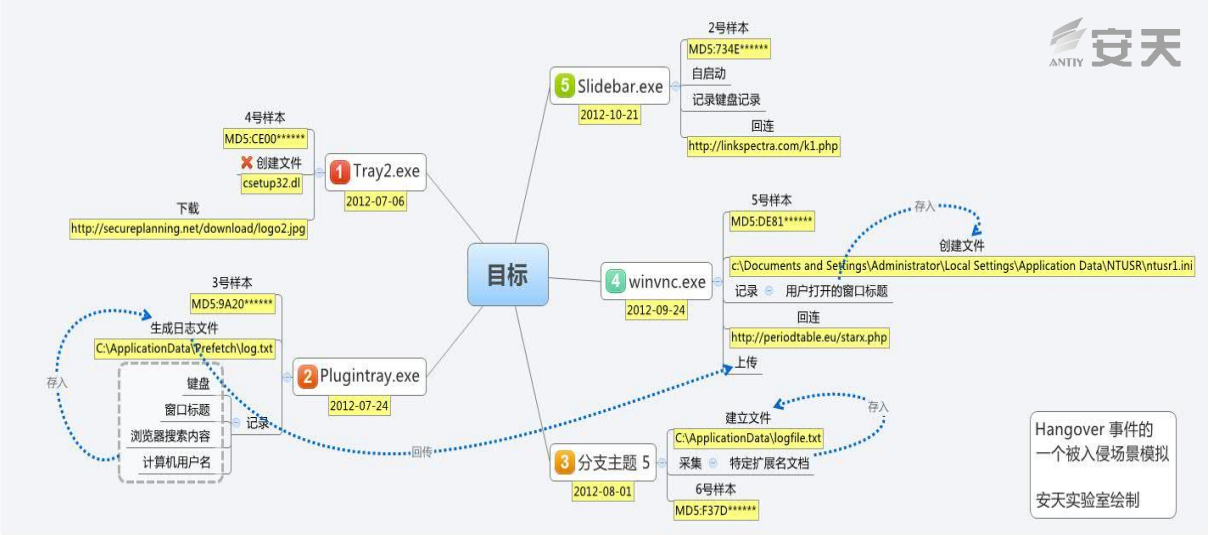

图 V 安天复盘 HangOver 事件中被攻击某个主机的场景

安天 CERT 在 2015 年底，全文公开了两年前对 HangOver 组织攻击中国两所大学的分析报告[4]，让研究者进一步回顾了这个“乱扔 EXE”的 APT 攻击组织。这种粗糙的攻击水准不仅无法与“方程式”这种超级攻击相比，也明显低于其他已知的 APT 攻击。基于此前对“HangOver 行动”的捕获与分析，以及后来的事件关联和可视化复现工作，我们把这种基于“人海战术”的不够“高级”的 APT 攻击，称为轻量级 APT 攻击。

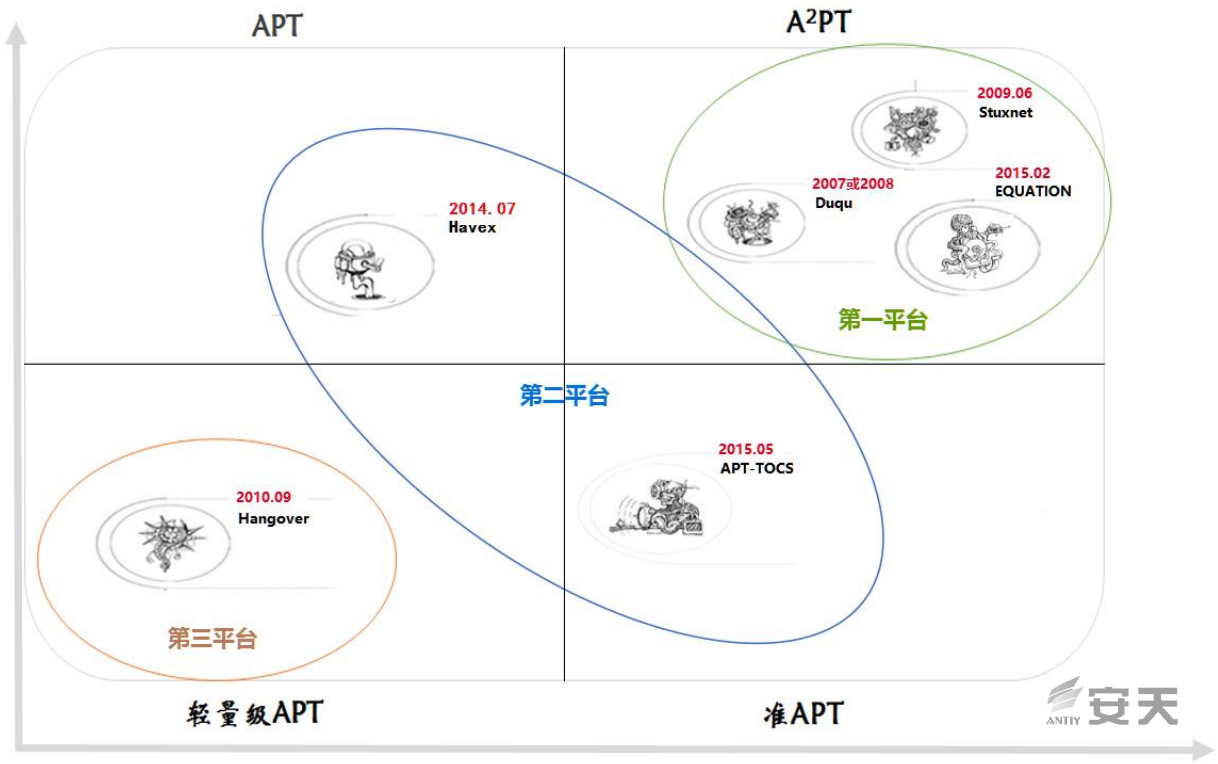

图 VI 安天在《A²PT 与准 APT 中的攻击武器》报告中绘制的 APT 的能力层次示意图

2.4 不要误读 APT

安天反复强调的一个观点是，APT 不是一个新概念，该词由美国空军上校 Greg Rattray 于 2006 年首次提出，用以概括具有坚定攻击意志的战略对手的攻击行为，距今已有九年的时间，APT 并不是对此类攻击唯一的概括、甚至亦不是最早的表达，只是其他的一些概念未得到更多关注罢了。如从技术手法上看，曾有部分新兴厂商提出了高级逃逸技术(Advanced Evasion Technique, AET)的概念，其对攻击逃逸技术的一些基础特点进行概括，目的是推广一些具有新的安全特性的产品。AET 描述的是一类具体的攻击技术和方法，显然没有 APT 这样宏观。而从历史延续来看，更具有传统的是“定向性威胁”一词，在一些研究者眼中，很多人认为“定向性威胁”比 APT 在技术表达上更为准确，并且它的历史也更为悠久。包括 IDC 等咨询机构至今仍然没有单独划分 APT 领域，而是把反 APT 的厂商和产品归类到反定向性威胁的领域中。而在这种情况下，APT 依然是热度最高的一个词汇，是因为其具有非常深厚的政治和经济背景。政治背景是指：APT 本身承载着超级大国在全球博弈中将对手脸谱化的需要；经济背景则是指：以 FireEye 为代表的新锐厂商，在防御美国所遭受攻击的工程中，需要借助一个概念来细分市场。因此，如果我们脱离这些背景，或者说完全站在 FireEye 等美国厂商的视角去解读 APT，特别是中国所面临的 APT 攻击风险，那么我们极有可能会被误导。

在 APT 事件的持续跟踪分析中，安天一直在避免两种倾向：一种是因为某些环节的技术不够高明，而草率否定某个攻击属于 APT；另一种则是因为某个攻击利用了较新的漏洞或者采用了较为高明的技巧，就盲目宣布发现了 APT 事件。我们目前并不能给 APT 的层次制定一个准确的边界，至少不能够仅凭在攻击事件中利用社工等手段采取针对性攻击就判定其为 APT 事件。例如，2015 年 12 月 2 日夜间，安天监控预警体系感知到如下信息线索：某知名作家在新浪微博发布消息，称有人以发送“采访提纲”为借口，利用微博私信功能，发送恶意代码链接，利用百度网盘向目标人群投送恶意代码[5]。此次事件显然与上文中提到的定向威胁等因素相吻合，但最终我们综合分析后，认为从目标的分布等因素来看，认为这不是一组 APT 事件。因此将一个攻击事件定性为 APT 事件，决不能以偏概全，要综合更深入的因素，并占有更多数据，才不会有所疏漏。而 APT 的层次划分，则应视事件定性后对作业手段和资源储备等进行全面评估而定。

我们至今在追影等产品界面上坚持使用“疑似 APT 攻击”一词，其原因是我们认为，APT 是不能依据简单的条件来判定的，APT 的定性首先要结合发起方与受害方、攻击的动机与后果，其次才看作业过程与手段。一个高明的攻击技巧，或者几个疑似 0day 漏洞的利用，都不足以将一起攻击事件定性为 APT。否则，一个数据采集能力非常有限的分析者，就很容易因其无法发现某个攻击的大面积分布，而简单声称其发现了 APT 事件。

对于 APT 的高级性与持续性，我们需要重新思考。高级不是绝对的，而是相对性的概念，它可能是相对于攻击者所拥有的资源攻击体系中位于高点能力；更是攻防所使用的能力相对于攻击者防御反制能力的势能落差。持续性以具象的行动为依托，一定会映射到一些具体的行为，如加密通讯、隐秘信道等。从微观上看，持续性未必是通过长久的链接或心跳实现，还可能是体现在持续化的能力或者反复进入的能力；而从宏观上看，这种持续并不因被防御方短时间内切断而终止，取决于攻击方的作业意志和成本支撑能力。

3 非法泄露的数据和隐私正在汇入地下经济的基础设施

在 2015 年，由网络攻击引发的数据泄露事件依旧猖獗，医疗、保健、电信运营商等行业和人事管理、社保、税务等政府部门受灾严重，身份证、社保、电话、信用卡、医疗、财务、保险等相关信息都是黑客窃取的目标。从目前来看，拖库攻击、终端木马和 APP 的超量采集、流量侧的信息劫持获取，已经成为数据泄露的三个主要渠道。信息泄露的背后已经形成了一条完整的利益链，这些用户信息或被用于团伙诈骗、钓鱼，或被用于精准营销。

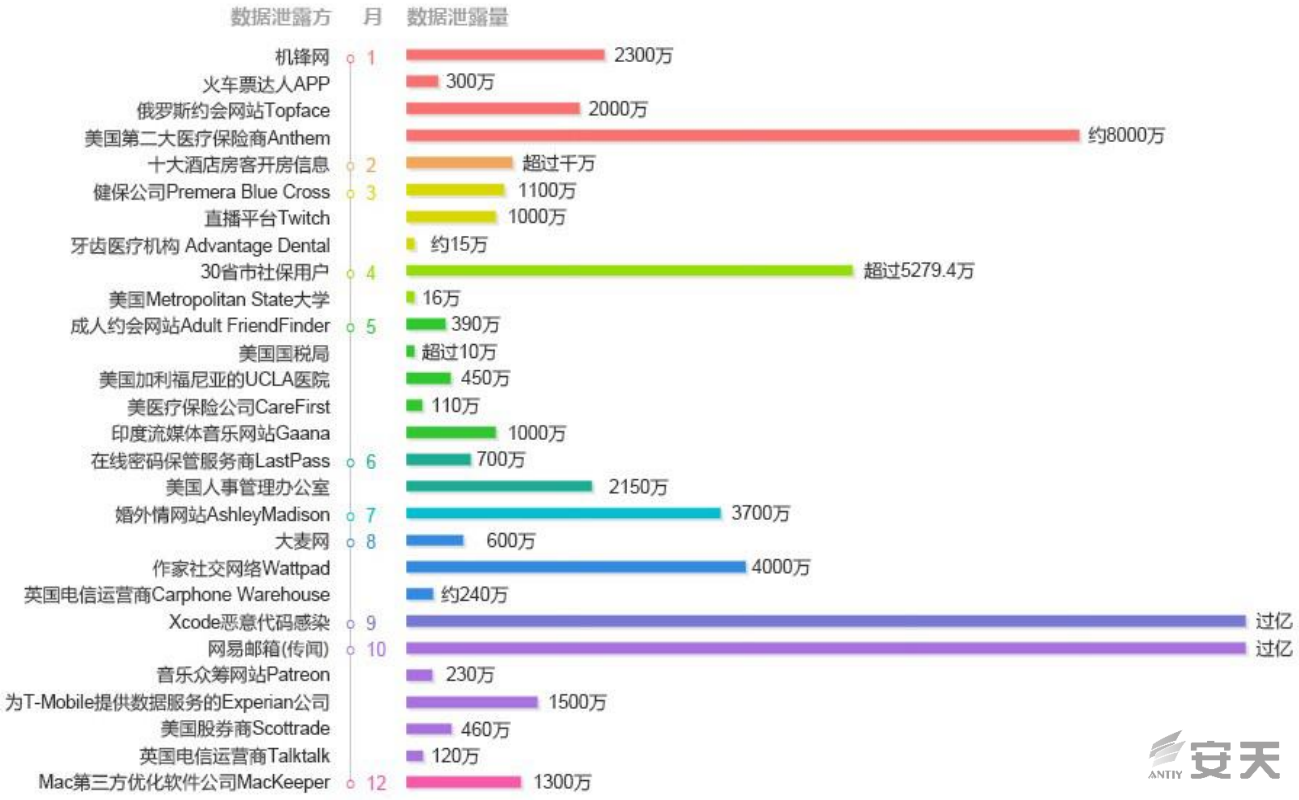

图 VII 2015 年重大数据泄露事件

“拖库门”事件的每一次曝光都令人关注，但实际上，依托这些数据达成的侵害往往早已存在，在其曝光时，其“价值”已经衰减。很多拖库数据都是在被攻击者充分利用、经过多手转卖后才会曝光。当前，数据泄露的地下产业链已经成熟，并且有了完整的分工协作程序。其模式往往包括：拖库、洗库、撞库和再洗库等阶段。当前，地下产业已经形成了与需求对接的一个“综合业务代理机制”，在“需求方”提出目标后，“业务代理”会找到接手的“攻击者”，“攻击者”成功拖库后拿到客户的佣金，并且将获得的数据库洗库，可以直接提取其中可变现的部分（如有预存款或虚拟货币的账户）；之后，这些数据会被用来撞库，尝试登陆其他有价值的网站，再对撞库成功的数据进行层层利用。经过日积月累，和相互交换，攻击组织和黑产团伙的数据库会越来越庞大，数据类型越来越丰富，危害也就越来越严重。

并非所有数据都是从“拖库”攻击中获得的，同样也有直接从终端和流量获取的。2015 年，因恶意代码导致的信息泄露事件中，XcodeGhost 事件[6]是一个值得所有 IT 从业人员深刻反思的事件。截止到 2015 年 9 月 20 日，各方累计确认发现共 692 种 APP 受到污染，其中包括微信、滴滴、网易云音乐等流行应用。尽管有人认为被窃取的信息“价值有限”，但一方面其数量十分庞大，随之衍生的风险也可能十分严重；另一方面，通过向开发工具中植入代码来污染其产品，这种方式值得我们警醒。同时，本次事件采用非官方供应链污染的方式，也反映出了我国互联网厂商研发环境的缺陷和安全意识薄弱的现状。

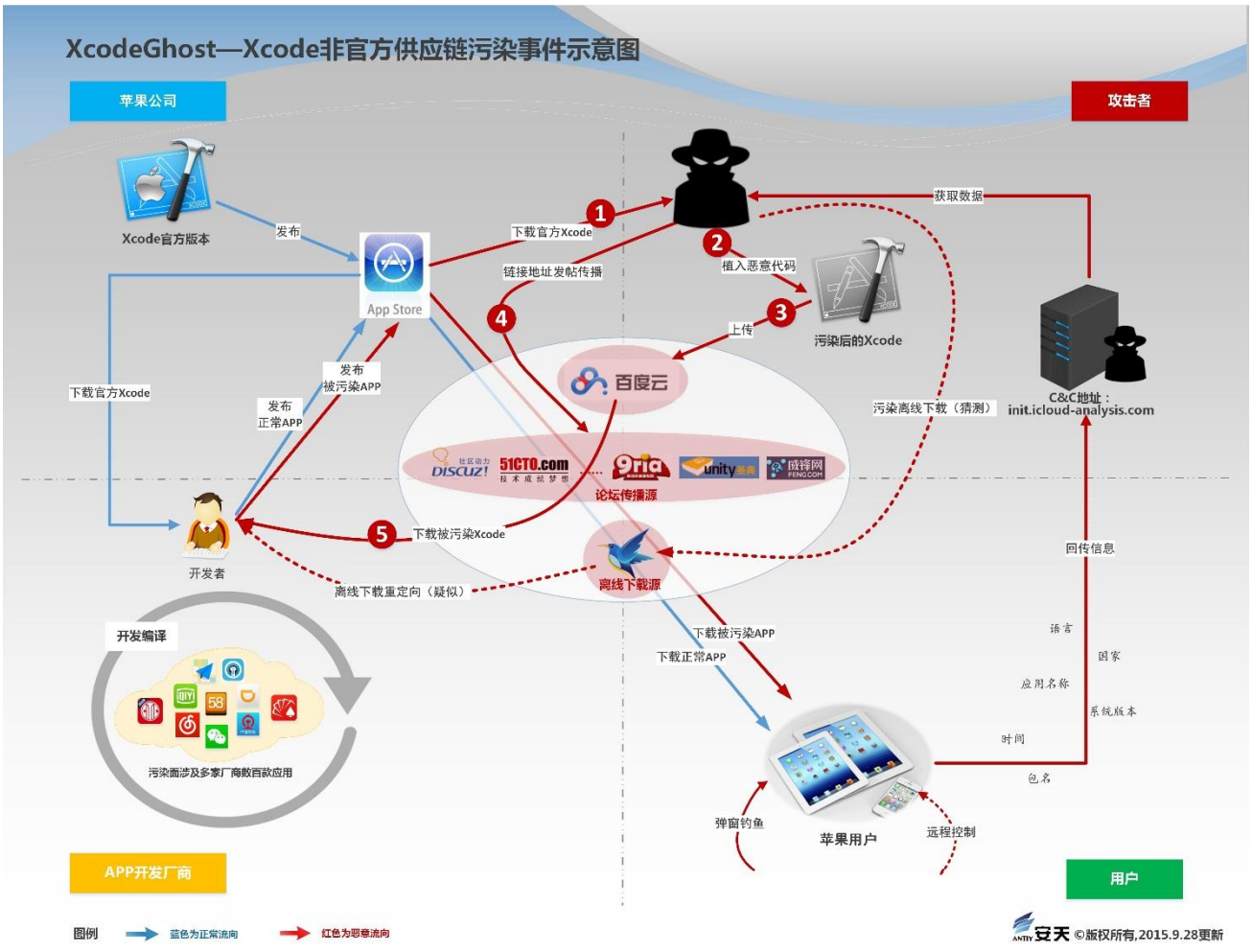

图 VIII 安天在 XcodeGhost 事件报告中绘制的非官方供应链污染示意图

近两年在国内肆虐的短信拦截木马在 2015 年不断出现新变种，并结合社会工程学手段疯狂传播，窃取用户的联系人、短信、设备信息等，如安天本年度重点分析处理的“相册木马”[7]。从 PC 侧上看，2011 年出现的 Tepfer 木马家族目前依旧活跃，且已有数十万变种，Tepfer 家族可以盗取 60 种以上的 FTP 客户端软件保存的密码、10 种以上的浏览器保存的密码、31 种比特币信息；还能获取多个邮件客户端保存的密码，是一个利用垃圾邮件传播，无需交互、自动窃密并上传的木马家族[8]。

大量数据的泄露一方面让用户的虚拟财产受到威胁，另一方面也使各种诈骗、精准钓鱼攻击变得更简单。之前大多数的诈骗都是采用广撒网的形式，而大量数据泄露使黑客的社工库完善后，可以有针对性地利用泄露信息匹配并精确定位用户，以此进行的诈骗和钓鱼攻击将更具欺骗性。

从过去来看，流量侧的灰色活动，更多用来劫持页面、骗取点击的方式来变现，但这种普遍性的流量劫持，同样具备着流量侧窃取的能力，这一点对于 HTTPS 尚未有效普及的国内网络应用来看，是具有高度杀伤力的。更何况 HTTPS 在过去两年，同样暴露出了大量工程实现层面的问题，包括 CDN 等的挑战。

人的身份几乎是永久的，关系是基本稳定的，此类数据泄露带来的影响，很难在短时间内被冲淡。一个值得关注的情况是，**随着黑产的规模化，这些数据将持续汇入黑产的“基础设施”当中，从而使其可能具备超越公共安全和安全厂商的资源能力**，同时也不排除这种地下基础设施摇身一变，以“威胁情报”的形式，同时为黑产和白帽子服务。

4 用户需要负责任的漏洞披露机制和更细腻的漏洞应急指导

2015 年，安天向 CNVD 报送漏洞数量为 7,780 条，但需要坦诚的是，这并不是我们擅长的领域。

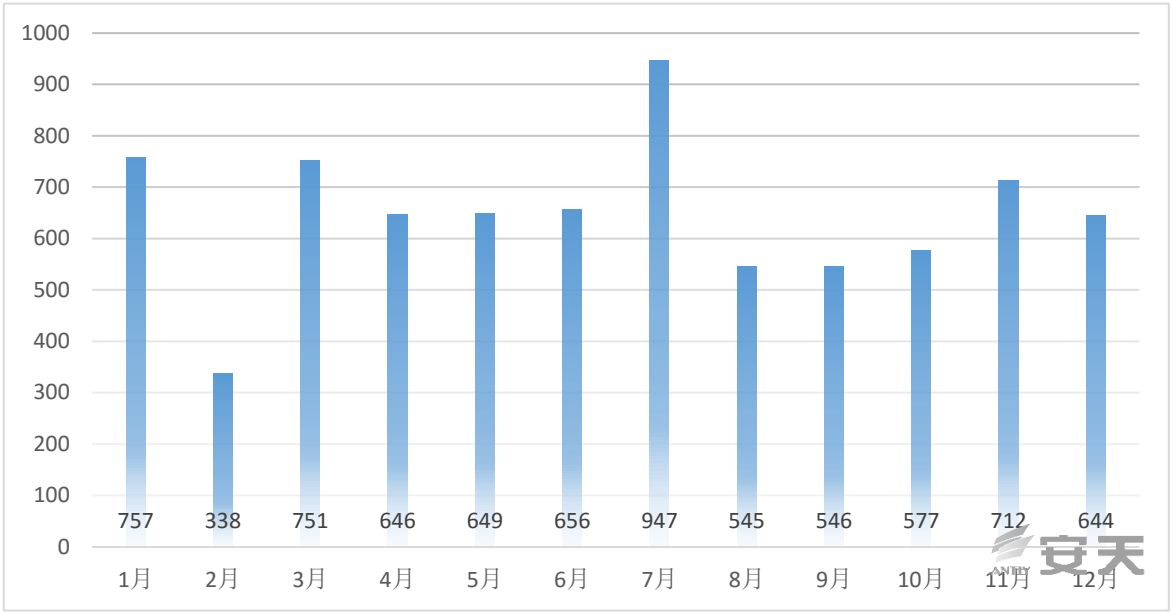

图 IX 2015 年安天每月上报漏洞情况

2015 年初的一个漏洞（CVE-2015-0002）引发了业内的广泛讨论。起因是 Google 的安全小组发现了一个 Windows8.1 的漏洞，在微软尚未对漏洞做出修补的情况下，Google 严格按照自身的标准，在第 90 天公布了漏洞详情。此举迅速引发了业内对漏洞披露方式的探讨，微软称谷歌这么做“完全把个人私心放在了用户安全之上”，也有人认为谷歌的做法“充分地尊重了用户”。为了在保护用户安全和保障用户的知情权之间寻求平衡，一些漏洞披露方采用了更灵活的漏洞披露方式。例如，一些漏洞平台在今年的漏洞信息中屏蔽掉一些敏感的 IP 地址、域名等信息，尽量避免出现漏洞的厂商遭遇微软类似的尴尬。2015 年业内出现了对某伪基站漏洞的激烈争论，对有极大修复成本、缺少快速修复可能性的基础设施和重要系统漏洞，该如何进行负责任的漏洞披露，也是业内需要讨论的问题。“幽灵（Ghost）”漏洞在 2015 年年初被发现，该漏洞存在于 GLib 库中。GLib 是 Linux 系统中最底层的 API，几乎其它任何运行库都会依赖于 GLib。由于 GLib

除了封装 Linux 操作系统所提供的系统服务外，本身也提供了许多其它功能的服务，“幽灵”漏洞几乎影响了所有 Linux 操作系统，一些研究者认为，其影响力堪比“破壳”漏洞。

Adobe Flash 的安全性一直饱受争议，被誉为“黑产军团的军火库”。APT28 和 Pawn Strom 都利用了 Adobe Flash 的 0day 漏洞进行 APT 攻击，2015 年全年上报的 Flash 漏洞更是多达 300 余条。Hacking -Team 的数据泄露事件，将 Flash 漏洞的实际危害性和影响力推到当年顶点，暴露出的三个漏洞几乎能够影响所有平台、所有版本的 Flash。其中被发现的第二个漏洞（CVE-2015-5122）甚至被黑客团队戏称为“过去四年里最漂亮的 Flash 漏洞”。

年底，被称为“破坏之王”的 Java 反序列化漏洞事件爆发。早在 2015 年 1 月 28 日，就有报告介绍了 Java 反序列化漏洞能够利用常用 Java 库 Apache Commons Collections 实现任意代码的执行，然而当时并没有引起太多关注。其在 WebLogic、WebSphere、JBoss、Jenkins 和 OpenNMS 中均能实现远程代码执行，获取权限后泄漏数据库。该漏洞被曝出九个月后依然没有发布有效的补丁，其危害影响时间较长。目前，大量政府门户网站和信息管理系统受该漏洞的影响十分严重，目前受影响最大的是 WebLogic 和 JBoss 两个应用服务器。

不得不说，业内对严重漏洞的预判能力正在下降，从 2014 年的“心脏出血（HeartBleed）”、“破壳（Bash Shellshock）”，到 2015 年的“幽灵（Ghost）”，都给人以措手不及感，而在漏洞出现后的快速跟进中，业内反而开始逐步丧失耐心指导用户止损和进行精细处置的应急传统。但这些工作尽管并不吸引眼球，却对于机构、行业用户来说具有更有效的价值。

5 勒索软件引领 PC 恶意代码威胁关注度，成为用户的噩梦

2015 年安天捕获 PC 端恶意代码新增家族数为 3,109 个、新增变种 2,243,062 种，这些变种覆盖了亿级的样本 HASH。相比于 2014 年，恶意代码总数虽然有所增加，但已经不再是 2006~2012 年间那种爆炸式的增长。

需要说明的是，我们无法确保这个统计足够精确，新增家族数的减少，并不能完全反映恶意代码的实际情况，更多的是我们过度依赖自动化命名的结果，从而对大量样本只能给出通用命名。尽管我们还在尽力维护一个完整的命名体系，但面对恶意代码数量多年的快速膨胀，以及恶意代码的开源和交易，几乎所有的安全厂商都失去了完整的基于严格编码继承性的家族命名关联跟进能力。各厂商大量采用编译器、行为等为恶意代码命名以及类似 Agent 这样粗糙的自动化命名，就是这种窘境的明证。而很多短小的 WebShell，本身亦未有足够的信息，去判定其演进和关联。在今天，我们应该更多地在分析实践中，通过基于向量、

行为之间的关系搜索，去寻觅恶意代码之间、安全事件与恶意代码之间的关系，而不是希望自动化给我们带来一切。

在 2015 年恶意代码家族变种数量排行榜前十名中，木马程序占六席，而其他四席被相对轻量级的 Hacktool、和 Grayware 所占据（也有一些安全厂商将这些称为 PUA，即：用户不需要的应用）。这个比例相对此前数年木马垄断排行榜的情况已经有了很大变化。在互联网经济带来更多变通道的情况下，一些攻击者的作业方式开始具有更强的隐蔽性。上榜恶意代码的主要功能是下载、捆绑、窃密、远程控制等行为，例如 Trojan/Win32.Badur 是一个通过向用户系统中下载、安装大量应用程序获利的木马程序，该木马会在后台下载多款推广软件，使用静默安装的方法在用户系统中安装指定的应用程序，并从软件厂商或推广人处获取利益。今年，广告程序有三个家族进入了排行榜，除 AdLoad 这个以行为命名的家族（家族样本未必具备同源性）外，另外两个广告程序家族都是具有亲缘性的庞大家族 Eorezo 和 Browsefox，两个家族中带有数字签名的样本占总样本比重分别为 32.9%和 79.9%，它们通过与其他程序捆绑、下载网站、下载者等进行传播，其安装模式通常为静默安装，主要的功能是浏览器劫持和域名重定向，通过修改用户搜索结果显示各种在线广告公司的广告来获利。而排名第八位的恶作剧程序 ArchSMS 实际上是一个勒索软件，今年在全球范围内有较大规模的感染，国内感染量也非常多，它会弹出警告窗体，通知用户系统磁盘被格式化（实际上未格式化，因此我们将其暂定为恶作剧程序）等虚假消息，恐吓用户发送短信并以此进行敲诈。

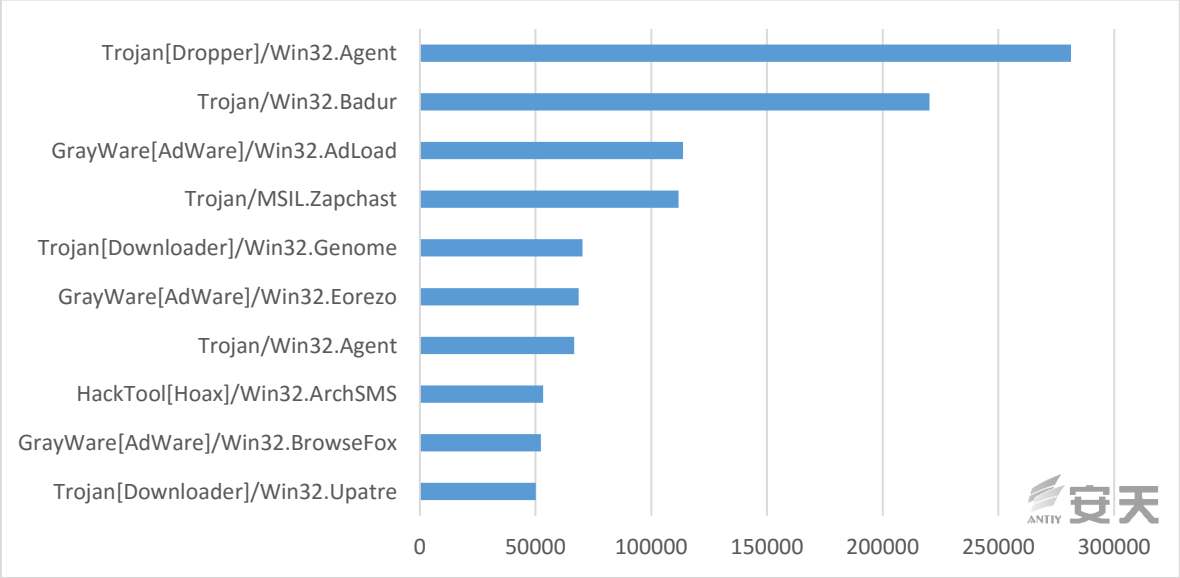

图 X 2015 年恶意代码家族变种数量排行榜

在 2015 年 PC 平台恶意代码行为分类排行榜中（HASH），以获取利益为目的的广告行为再次排在第一位，下载行为因其隐蔽性、实用性强的特点数量依然较多，捆绑行为与后门行为分列三、四位，备受关注的勒索软件位列第九位。安天 CERT 在 2015 年 8 月 3 日发布报告《揭开勒索软件的真面目》[9]，详细地揭

露了勒索软件的传播方式、勒索形式、历史演进以及相应的防御策略。而在 2015 年 12 月 4 日，我们又跟据敲诈软件依托JS脚本进行邮件传播的新特点，跟进发布了《邮件发送JS脚本传播敲诈者木马的分析报告》[10]。

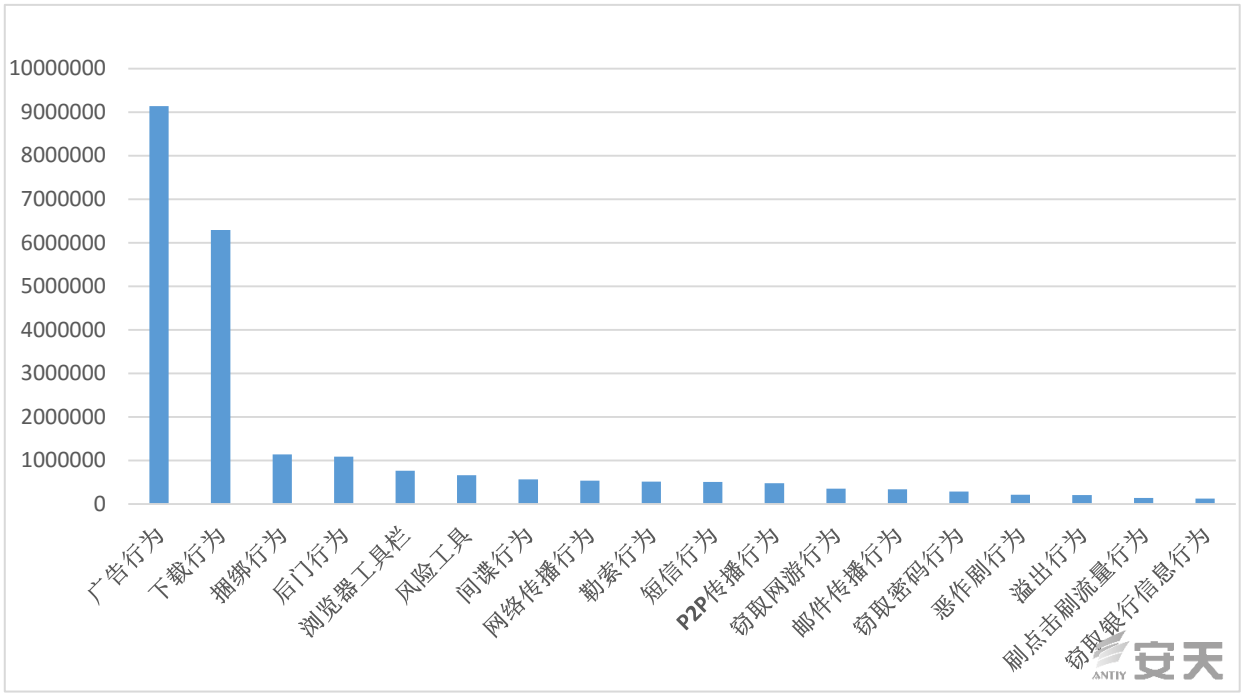

图 XI 2015 年 PC 平台恶意代码行为分类排行

6 威胁将随“互联网+”向纵深领域扩散与泛化

2013 年，我们用泛化（Malware/Other）一词，说明安全威胁向智能设备等新领域的演进，之后泛化（Malware/Other）一直被作为主要的威胁趋势，占据了安天威胁通缉令的“小王”位置两年之久。在这两年，除我们熟悉的 Windows、Linux 和其他类 Unix 系统、iOS、Android 等平台外，安全威胁在小到智能汽车、智能家居、智能穿戴，大到智慧城市中已经无所不在。

在 2015 年，这种安全威胁泛化已经成为常态，但我们依然采用与我们在上一年年报中发布“2014 年网络安全威胁泛化与分布”一样的方式，以一张新的图表来说明 2015 年威胁泛化的形势。

2015网络安全威胁泛化与分布

本图引自《安天实验室2015网络安全年报》© 安天

7 思考 2016

7.1 2016 年网络安全形势预测

高级威胁向普通威胁转化的速度会日趋加快，任何在精妙的 APT 攻击中所使用的思路一旦被曝光，就会迅速被更多的普通攻击者学习和模仿。而以国家和政经集团为背景的攻击者也会与地下黑产有更多的耦合。由于商业化攻击平台和商用木马具有节省开发成本、干扰追踪等特点，越来越多的攻击组织将使用成型或半成型的商业攻击平台、商业木马和黑产大数据基础设施作为网络攻击的组合武器。“核威慑”的时代令人远虑，但“武器扩散”的年代则会带来更多现实的困扰。

勒索软件将成为全球个人用户甚至企业客户最直接的威胁，除加密用户文件、敲诈比特币外，勒索攻击者极有可能发起更有针对性的攻击来扩大战果，如结合内网渗透威胁更多的企业重要资料及数据。也不排除其会尝试邮件之外更多的投送方式，在更多邮件服务商开启默认全程加密后，在流量侧难以有效发现和阻断，因此对敲诈者过滤的责任除了邮件服务商本身，则又回到了终端安全厂商。

基于简单信标共享层次的威胁情报会遭遇挑战，利用脚本、内存驻留、无实体文件等隐藏踪迹的攻击方法将更为盛行。例如，APT-TOCS 中使用 PowerShell 作为文件载体进行加载恶意代码。在这种技术面前，简单的文件 HASH 共享将无法有效应对。此外，随着更多攻击者占据种种网络设备资源，更为隐蔽的通讯方式将逐渐让更多攻击者摆脱对固定域名 C&C 的依赖。**因此这种基于文件 HASH 和地址的通讯信标检测，未来注定在对抗 APT 攻击中难以占据上风**。同时，我们需要提醒我们的同仁，**威胁情报的共享体系，同样使其具有了很大被污染的可能性**。

“上游厂商”将遭受更多的攻击，导致整个**供应链、工具链的脆弱性增加**。攻击者会将目光转向防护能力稍弱的第三方供应商，以其受信任的身份为跳板，攻击防护能力较强的企业，从而带来更大面积的影响。例如，攻击者对分析工具、安全工具等的攻击可以影响逆向爱好者和恶意代码分析师；对开发场景的攻击可以影响其大量用户和高敏感的用户，使用者会将其判定为受信程序或软件；对出厂设备预安装恶意代码可以直接影响用户。因此，上游厂商和开发商需要担负起更有效的布防责任。同时，因为中国行业资质门槛的问题，OEM、贴牌等行为更为普遍，而盗版工具链、伪原创等问题也十分常见，因此威胁图谱往往更为复杂，供应链透明化的呼声需要变成行动。

我们还需要注意到的是，**随着中国政府以“互联网+”盘活传统产业的努力，中国所面临的安全威胁也将向传统的工业和基础设施中快速逼近**。

7.2 我们在行动、我们在路上

我们终于要插播广告了……

在过去的 2015 年，安天完成了从反病毒检测引擎供应商，到高级威胁检测能力厂商的角色调整，初步形成了以“安天实验室”为母体，“企业安全”与“移动安全（AVL TEAM）”为两翼的集团化布局。我们希望以有效的检测分析能力和数据储备为基础，依托在反恶意代码和反 APT 方面长期的尝试和积累，为用户创造更有效、更直接的安全价值。

同时在过去一年中，我们改善了自身的一些产品，以使之获得更有效的缓存和向前回溯的能力。我们改进了沙箱技术，使之能够更有效地触发恶意行为，同时对 PE 样本有更深的行为揭示能力；我们让反病毒引擎不再简单地充当一个鉴定器，而是变成一个知识体系；我们也继续加大了对移动安全相关领域的研究和投入，并在 AV-C 上下半年的两次测试中，成为全球唯一一个获得检出率双百分成绩的厂商。通过这些工作所带来的产品改进，安天已经形成了以 PTD 探海威胁检测系统（前身是安天 VDS 网络病毒检测系统）为流量侧探针，以 IEP 智甲终端防御系统为终端防线，以 PTA 追影威胁分析系统为分析纵深能力的高级威胁检测防护方案，并通过结合态势感知和监控预警通报来满足行业用户和主管部门的需求。

我们对威胁情报共享机制和大数据都给予了足够的关注，我们也坚信威胁情报不是简单的信标挖掘与互换，其需要可靠的安全威胁检测能力作为支撑。同时更要警惕情报共享体系遭到上游污染，从而导致情报价值降低，甚至产生反作用。

向前台产品的转型，可以让我们更好地为用户服务，但我们依然专注于反 APT 与反恶意代码领域，既不会跟随新概念而摇摆，也不会被提供“无死角”解决方案的想象所诱惑。

除了我们对用户的责任外，安天珍惜通过自身长期与兄弟厂商互动，提供反病毒引擎所形成的产业角色。

我们以可靠检测能力支撑威胁情报，我们以检测能力输出共建安全生态。

这是我们对于安天自身的产业责任和未来的理解。

8 2015 的辞岁心语

在安天度过第 15 个年头，在最早加入安天 CERT 的分析工程师已经四十不惑的时候，我们承认我们都有过彷徨、有过动摇。但如果你认真地问我们，“你心力憔悴么？”——我们要回答：“不！”。

安全工作者与安全威胁间进行的本身就是一场永不终止的心力长跑，双方进行的不止是力量的抗衡，同样也是心灵与意志的较量。无论是地下经济从业者对利益的孜孜以求，还是 APT 的发起者坚定的攻击意志，都驱动着对手的不知疲倦，这终将会使网络安全成为靠勤奋者和坚定者坚持的行业。

但我们需要坚持的不止是这种勤奋和坚定，还有我们的正直。**我们坚持防御者的立场，坚持对保障用户价值的使命，坚持对安全威胁受害者感同身受的情感，坚持对原则和底线的敬畏**，这是我们事业的基础和前提。因为唯有此，我们的努力和进步，才有真正的意义！

附录一：参考资料

[1] 修改硬盘固件的木马——探索方程式（EQUATION）组织的攻击组件
http://www.antiy.com/response/EQUATION_ANTIY_REPORT.html

[2] 方程式（EQUATION）部分组件中的加密技巧分析
http://www.antiy.com/response/Equation_part_of_the_component_analysis_of_cryptographic_techniques.html

[3] 一例针对中方机构的准 APT 攻击中所使用的样本分析
http://www.antiy.com/response/APT-TOCS.html

[4] 安天技术文章汇编（十•二）APT（高级持续性威胁）专题（第二分册）

[5] 一例以“采访”为社工手段的定向木马攻击分析
http://www.antiy.com/response/RemoteABC/RemoteABC.html

[6] Xcode 非官方版本恶意代码污染事件（XcodeGhost）的分析与综述
http://www.antiy.com/response/xcodeghost.html

[7] 短信拦截马"相册"综合分析报告
http://www.antiy.com/response/emial.html

[8] 疯狂的窃密者——TEPFER
http://www.antiy.com/response/tepfer.html

[9] 揭开勒索软件的真面目
http://www.antiy.com/response/ransomware.html

[10] 邮件发送 JS 脚本传播敲诈者木马的分析报告
http://www.antiy.com/response/TeslaCrypt2.html

附录二：关于安天

安天从反病毒引擎研发团队起步，目前已发展成为拥有四个研发中心、监控预警能力覆盖全国、产品与服务辐射多个国家的先进安全产品供应商。安天历经十五年持续积累，形成了海量安全威胁知识库，并综合应用网络检测、主机防御、未知威胁鉴定、大数据分析、安全可视化等方面经验，推出了应对持续、高级威胁（APT）的先进产品和解决方案。安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续四届蝉联国家级安全应急支撑单位资质，亦是 CNNVD 六家一级支撑单位之一。安天移动检测引擎是获得全球首个 AV-TEST（2013）年度奖项的中国产品，全球超过十家以上的著名安全厂商都选择安天作为检测能力合作伙伴。

关于反病毒引擎更多信息请访问：http://www.antiy.com（中文）

http://www.antiy.net （英文）

关于安天反 APT 相关产品更多信息请访问：http://www.antiy.cn