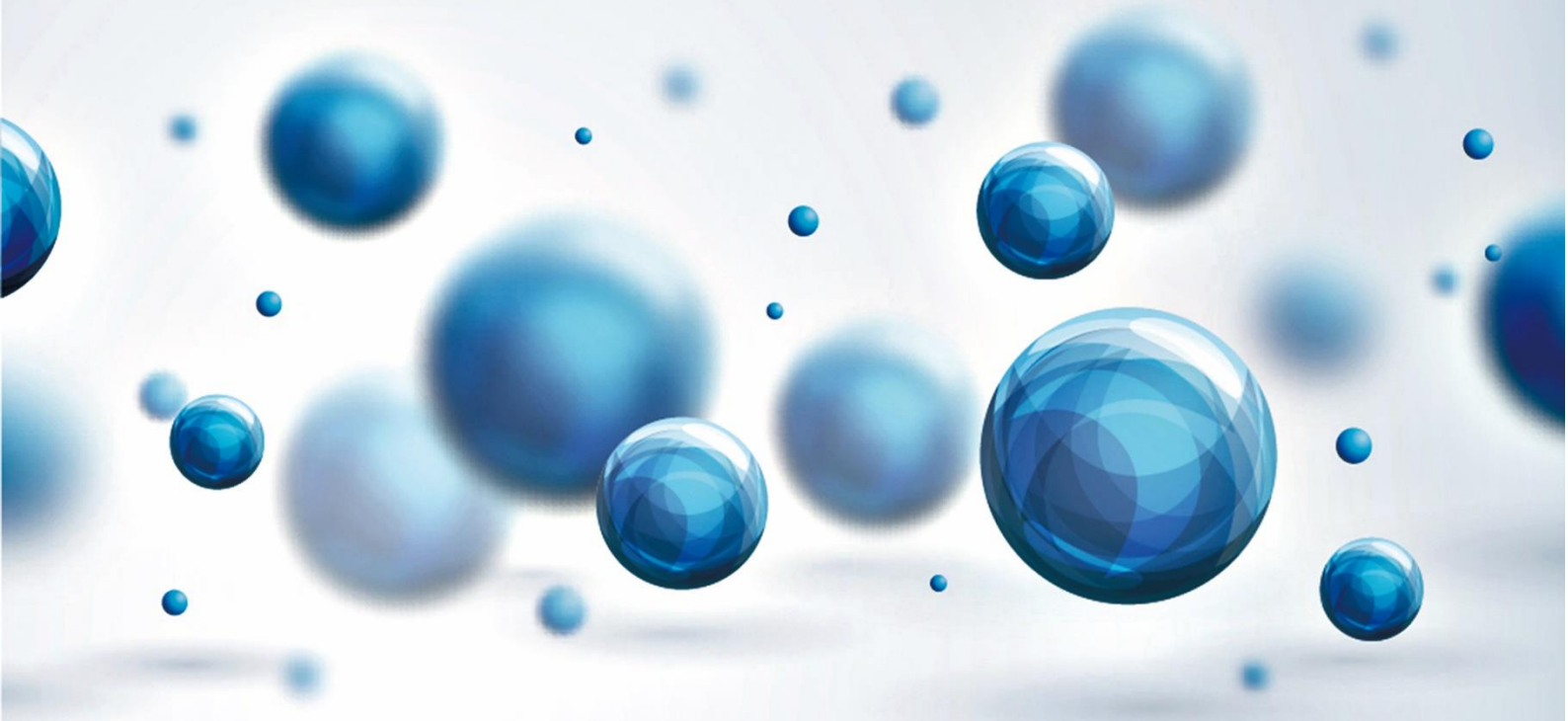
安天 ANTIY

2016 网络安全威胁的回顾与展望

Antiy Annual Security Report

公开版



初稿完成时间：2016年12月20日 18时15分
首次发布时间：2017年01月06日 10时00分
本版更新时间：2017年04月14日 09时00分

安天安全研究与应急处理中心

目录

1 努力让思考适配年代（代导语）

在中国网络安全的发展过程中，2016 年云集着众多的里程碑节点——习近平总书记在 4.19 网信工作会议上发表重要讲话；《网络安全法》正式通过，强调全面加强关键基础设施防御；“十三五”规划提出“自主先进”的全新要求……一个未来清晰的地平线正在向远方展开。对中国网安从业者来说，如果说此前十余年的摸索前进，更像是一个为这个“大时代”积蓄力量的过程，那么在 2016 年则已经正式开启了新时代的大幕。无论对“乐观坚持者”，亦或“悲观放弃者”，还是“临时转型者”来说，这个时代都真实地到来了。

在这个大背景下，安天一直坚持的年度规定动作“安天基础威胁年报”和“安天移动威胁年报”的正式发布日期被一推再推，移动威胁年报直至 3 月 10 日才发布，而基础威胁年报的发布，距离我们在今年 1 月的安天第四届网络安全冬训营上，向营员分发预发布版已经过去了整整 90 天，如果说在其他年份，这种拖延和不断修改是因为我们对技术的敬畏和对威胁的警惕，而这一次我们的反复推敲，则是因为我们在自我反思和检验：**我们的行动是否跟进了我们的思考，我们的思考是否适配了这个时代！**

自 2014 年起，我们提出了“观点型年报”的自我要求，我们需要有自己的视角、立场和分析预测，我们放弃了传统的以后台恶意代码的数据输出来构筑模板式“统计型”年报，我们深知那些精确到行为和静态标签的“蔚为壮观”的统计数据，虽然看上去很美，但其并不具备足够的参考价值；而用扫描传播次数作为威胁严重程度的度量衡，尽管对部分类型的风险依旧有效，但作为蠕虫和 DDoS 时代的产物，其掩盖了那些更为严重的、更为隐蔽的威胁。而仅仅有“观点型年报”这样的意识就足够吗？我们回看了此前几年安天自己的年报，在充满着“全面转向”、“日趋严重”、“不断浮现”、“接踵而至”等这些成语的描述中，是否真的揭示了威胁的现状和趋势？

在这份年报中，我们非常谨慎又沉重地提出了以下思考和观点：

“APT 行为”的历史比“APT”这一名词的历史更为久远，今天我们看到的 APT 事件的“频发”，更多的是曝光度的增加，而这种曝光度的增加是由于 APT 攻击被更多的安全资源聚焦和媒体关注所导致的。我们认为对 APT 攻击的趋势最合理的表述是：**APT 攻击是网络空间的常态存在，而其增量更多地来自新兴目标场景的拉动和新玩家的不断入场。**

APT 的攻击重点“转移”到关键信息基础设施既是一种趋势，更是一种**既定事实**，对超级攻击者来说，**关键信息基础设施一直是 APT 攻击的重点目标，这种攻击围绕持续的信息获取和战场预制展开，在**

这个过程中，CNE（Cyber Network Exploitation，网络情报利用）的行为是 CNA（Cyber Network Attack，网络攻击）的前提准备。

商用攻击平台、商用木马和漏洞利用工具等网络商业军火全面降低了 APT 攻击成本，提升了攻击追溯难度。商业军火的泛滥，首先带来的是金字塔的底层混乱，而**不受控的商业武器，更有利于巩固一个单极的世界**。

将 APT 概念泛化到一些使用高级手段和技巧的攻击行为，是不负责任的，**没有攻击意图和攻击意志的 APT 分析，不是可靠的 APT 分析判定**。而恰恰相反的是，高级的网络攻击未必使用高级的技巧和装备，APT 攻击者劫持普通恶意代码，包括全面伪装成普通的黑产犯罪，可能会成为一种趋势。

在我国的信息化建设中，IT 基础设施的不完备、信息化建设的“小生产化”等原因导致了我国在架构安全和被动防御层面存在严重的先天基础不足，这也是我国应对风险能力不足的根本原因之一。我们不仅需要守卫一条漫长的、充满弱点的边界，还拥有大量的“防御孤岛”和散点。对此，如果**没有更进一步的信息化与安全的同步建设，没有“安全与发展同步推进”，安全防御依然将无法有效展开**。

跟随硅谷安全产业圈实践的亦步亦趋，不能有效地全面应对中国所面对的 APT 风险。硅谷的安全探索更多的是在发达国家政企和行业客户的基础安全投入已经全面产生基础价值的情况下，进行积极防御和威胁情报的加强，但如果脱离了基础能力的高阶安全手段，是不能有效发挥作用的。从具体的风险对抗层面来看，超级攻击者在信道侧的物理优势，以及与传统人力和电磁能力结合的作业特点，将导致 C&C、文件 Hash、信标型威胁情报对其行动的检测价值被大大削弱。

“物理隔离+好人假定+规定推演”构成了一种安全假象和自我安慰，网络分区策略和隔离手段无疑是必备且必要的安全策略，但如果不能伴随更强有力的内网安全策略，其可能带来更大的安全风险。安全策略和安全投入，需要以内网已被穿透和“内鬼”已经存在为前提假定来实行。

黑产大数据所带来的个体悲剧案例，还只是这一问题的冰山一角。当前的**数据流失总量已经构成了准全民化的画像能力，**其带来的“威胁情报反用”已经构筑了高精度单点打击，从而带来了较大的国家安全风险。信息采集的不受控、信息资产的离散化、问责体制的不明确，构成了风险加速的主因。

传统 Windows PC 恶意代码增速已开始下降，移动等新兴场景恶意代码则继续加速发展，同时各种平台下**高级恶意代码的隐蔽性和抗分析能力都在不断提升**。

威胁情报不只是防御方的资源，威胁情报也是情报威胁，是攻防双方的公共地带。同样的数据，对防御方来说是规则和线索，对攻击方来说则是攻击资源和痕迹。

“敲诈者”是当前值得关注的高发性恶意代码行为，其从最早的邮件恶意代码投放，到开始和“僵尸网络”、“蠕虫传播”、“网站渗透”、“内网传播”、“手机病毒”等叠加，其影响范围已经全面从个人用户到达政企网络，**其不再只是一种恶意代码类型，而成为一种典型的黑色经济模式**。

大规模 IoT 设备的蠕虫感染事件，不能单纯地将其作为 DDoS 攻击跳板来看，被入侵的这些设备本身具有更多的资源纵深价值，这比使用这些设备参与 DDoS 攻击所带来的危险更为严重。**IoT 设备大面积存在的脆弱性，带来了更为隐蔽、危害更大的社会安全风险和国家安全风险**，只是这种风险，更不容易被感知到罢了。

今天从供应链安全的视角来看，更多的人依然采用从上游抵达下游的“间接路线”来审视。供应链防御作为高价值场景防御的延展，已逐渐为安全管理者所接受，但仅仅把供应链风险视为达到关键目标的外延风险是不够的，供应链不仅是攻击入口，其本身更是重要的目标，**未来的网络空间攻防的主战场将围绕“供应链”和“大数据”展开**。

面对威胁和挑战，安天将选择做**具有体系化视野和解决方案的能力型安全厂商**。**基于自主创新的威胁检测防御核心技术产品服务，推动积极防御、威胁情报与架构安全和被动防御的有效融合，致力于提供在攻击者难以绕过的攻击环节上叠加攻击者难以预测的安全能力，达成有效防护和高度自动化以及可操作化的安全业务价值，这将是未来安天所选择的道路**。

2 高级持续性威胁（APT）的普遍存在是网络空间的常态

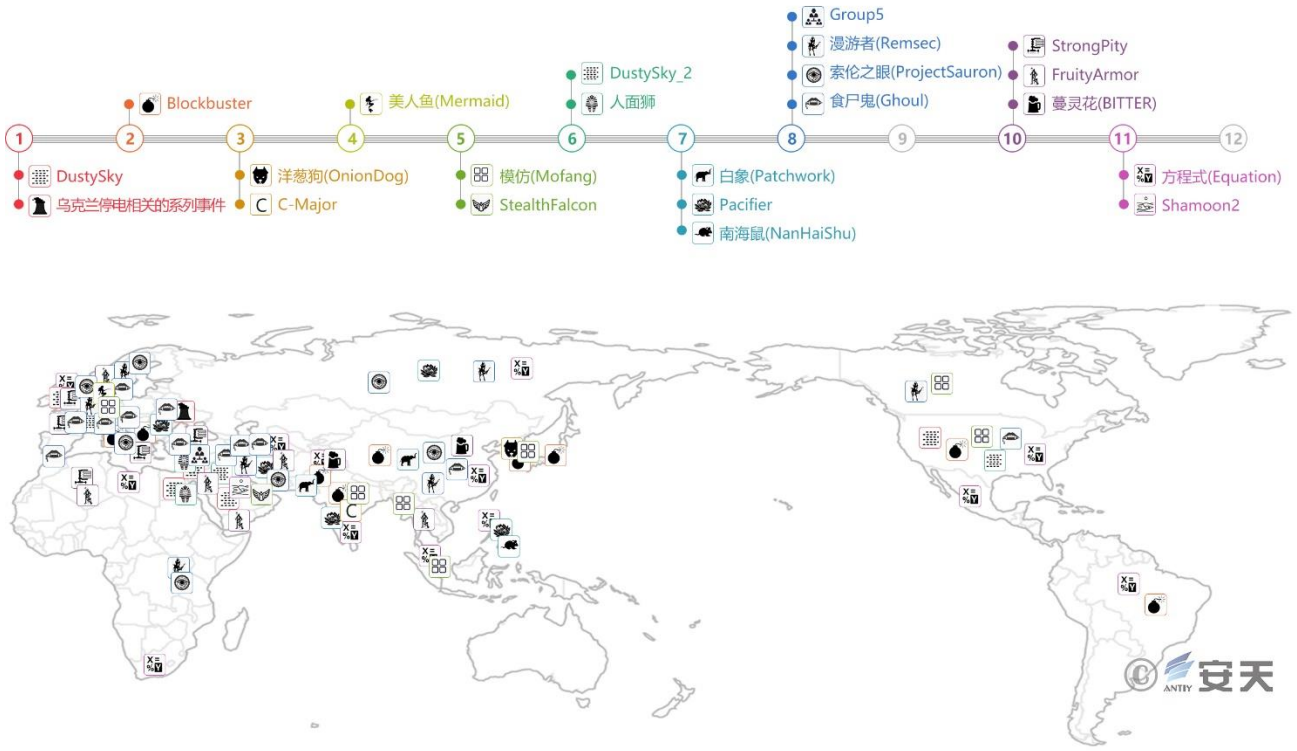


图 1 2016 年发生及被曝光的 APT 事件的时间与地理位置分布

2016 年是在乌克兰国家电力系统遭受网络攻击的余震中开始的，在随后的几个月中，各国安全厂商陆续曝光多起 APT 事件，如 Blockbuster、洋葱狗（OnionDog）、C-Major 等；7 月，“白象（Patchwork）”组织成为多方曝光的焦点，多个安全厂商发布对该组织的分析报告；而到年底，随着“影子经济人（Shadow Brokers）”不断曝光新的信息和安天等安全厂商释放储备报告，“方程式（Equation）”的全平台能力图谱也逐渐被还原出来。而当更多的事件被沿其时间轨迹展开后，我们能看到的是，将“日趋严重”、“成为趋势”等陈词用于 APT 攻击其实是不负责任的，APT 频繁被曝光更多是因其成为国际媒体关注的焦点后，吸引了更多的安全分析资源。尽管 APT 一词最早于 2006 年被提出，但如果以此标准去衡量更久远的攻击行为（如“方程式”组织于 2000 年开始对全球服务器节点展开攻击），我们可以说，**APT 攻击一直是网络空间的常态存在，而其未来的增量部分将主要来自两个因素：一是针对新兴的关键信息基础设施和传统基础设施的信息化；二是由于攻击面不断扩大、攻击成本不断下降而导致的新玩家入场门槛降低。与此同时，对 APT 攻击的检测、追溯、曝光和全网止损也同样成为常态化的反制动作。**

2.1 关键信息基础设施是 APT 攻击的主要目标

“乌克兰电力系统遭受攻击事件”[1]尽管发生于 2015 年底，但对其系统有效地梳理分析是 SANS ICS[2]、ESET[3]、安天等团队在 2016 年初陆续完成的，与其相关的乌克兰机场、矿业公司、轨道交通和电视台等多起遭遇入侵的事件也是在 2016 年初被陆续曝光出来的。而同样引发全球关注的通过网络手段和恶意代码攻击关键基础设施事件，即十年前*的“震网（Stuxnet）”事件很容易被作为参照系，这让我们看到，随着整个互联网更快地与关键基础设施相融合，在效率提升、成本下降、服务便利的同时，关键基础设施的防御正面在不断变宽，攻击成本则不断下降。安天在专题报告《乌克兰电力系统遭受攻击事件综合分析报告》[1]中对两起事件做了要素对比：

*注：“震网”虽然是在 2010 年曝光的，但其计划是从 2006 年开始实施的，故我们称之为十年前。

表 1 “震网”事件与“乌克兰电力系统遭受攻击事件”对比

	“震网”事件	乌克兰电力系统遭受攻击事件
主要攻击目标	伊朗核工业设施	乌克兰电力系统
关联被攻击目标	Foolad Technic Engineering Co（该公司为伊朗工业设施生产自动化系统） Behpajooh Co.Elec & Comp.Engineering（开发工业自动化系统） Neda Industrial Group（该公司为工控领域提供自动化服务） Control-Gostar Jahed Company（工业自动化公司） Kala Electric（该公司是铀浓缩离心机设备主要供应商）	乌克兰最大机场基辅鲍里斯波尔机场 乌克兰矿业公司 乌克兰铁路运营商 乌克兰国有电力公司 UKrenergo 乌克兰 TBS 电视台
作用目标	上位机（Windows、WinCC）、PLC 控制系统、PLC	办公机（Windows）、上位机（Windows）、以太网-串口网关
造成后果	延迟了伊朗的核计划，使之错过了成为有核国家的历史机遇。	乌克兰伊万诺-弗兰科夫斯克地区大面积停电
核心攻击原理	修改离心机压力参数、修改离心机转子转速参数	通过控制 SCADA 系统直接进行界面操作，下达断电指令
使用漏洞	MS08-067（RPC 远程执行漏洞） MS10-046（快捷方式文件解析漏洞） MS10-061（打印机后台程序服务漏洞） MS10-07（内核模式驱动程序漏洞） MS10-092（任务计划程序漏洞） WINCC 口令硬编码	未发现
攻击入口	USB 摆渡	邮件发送带有恶意代码宏的文档

	人员植入（猜测）	
前置信息采集和环境预置	可能与 Duqu、Flame 相关	采集打击一体
通讯与控制	高度严密的加密通讯、控制体系	相对比较简单
恶意代码模块情况	庞大严密的模块体系，具有高度的复用性	模块体系，具有复用性
抗分析能力	高强度的本地加密，复杂的调用机制	相对比较简单，易于分析
数字签名	盗用三个主流厂商数字签名	未使用数字签名
攻击成本	超高开发成本 超高维护成本	相对较低

安天所领衔的联合分析小组认为：这是一起以电力基础设施为目标；以 BlackEnergy（黑色能量）等相关恶意代码为主要攻击工具；通过 Botnet 体系进行前期的资料采集和环境预置；以邮件发送恶意代码载荷为最终攻击的直接突破入口；以远程控制 SCADA 节点下达指令为断电手段；以摧毁破坏 SCADA 系统实现迟滞恢复和状态致盲；以 DDoS 服务电话作为干扰，最后达成长时间停电并制造整个社会混乱的具有信息战水准的网络攻击事件。“乌克兰电力系统遭受攻击事件”充分诠释了现代社会基础设施的脆弱性，攻击装备相对几年前的“震网”来说，看起来似乎并不够“高明”，但同样达成了其战术使命。如果说“震网”这样的 A^2PT（即“高级的”高级持续性威胁）攻击让人更多看到的是 0 Day 漏洞、复杂严密的加密策略、PLC 与固件等，那“乌克兰电力系统遭受攻击事件”的“战果”则是攻击者在未使用任何 0 Day 漏洞，也未使用位于生产系统侧的攻击组件，而是在仅仅依托 PC 端的恶意代码作业的情况下取得的。从攻击的效费比来看，这是一起更能诠释战争的“暴力美学”的作业行动。

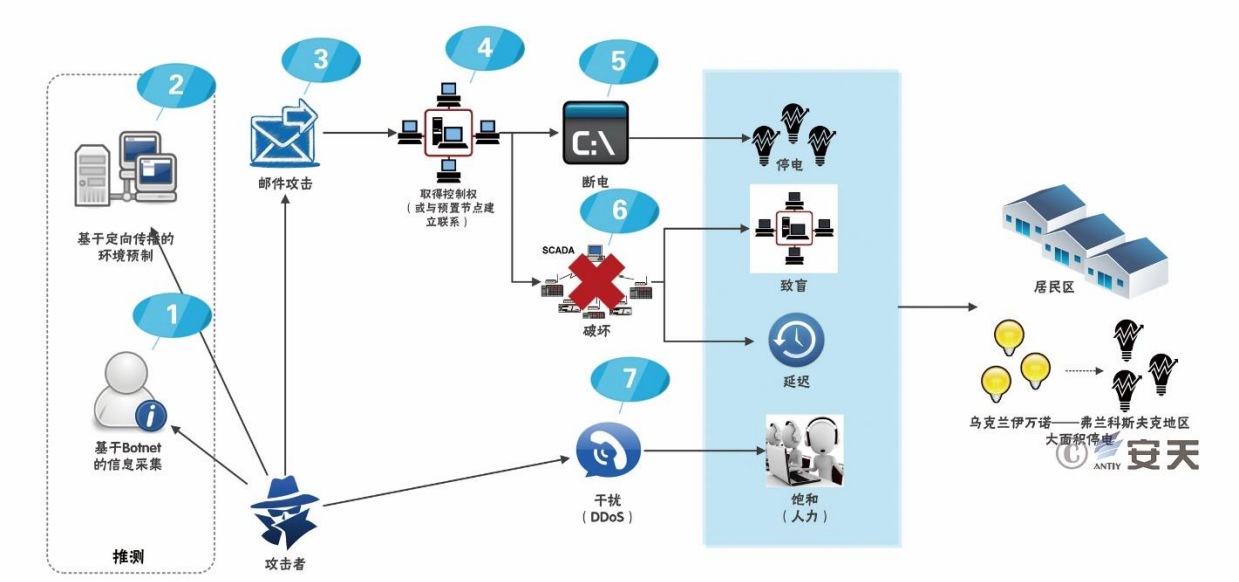


图 2“乌克兰电力系统遭受攻击事件”过程总结

“孟加拉国央行遭受网络攻击致 8100 万资金被窃取事件”也是 2016 年得到广泛关注的针对金融基础设施的攻击事件，之后针对银行 SWIFT 系统的其他网络攻击事件逐一被公开。在国内安全厂商中，360 企业安全对此做了比安天更多的分析披露工作。攻击组织对目标银行的业务流程非常熟悉，对目标进行了长时间高度定向的持续性分析。通过对孟加拉国央行和越南先锋银行的恶意代码同源性进行分析，可以推测出攻击组织与 Lazarus 组织有关。

在孟加拉国央行被黑客攻击事件中，攻击者通过网络攻击获得 SWIFT 系统权限并执行业务操作，通过恶意代码修改 SWIFT 系统的校验绕过安全验证，篡改报文数据掩盖了非法转账痕迹。以上种种攻击手段的有效利用充分暴露出银行系统自身安全的防护缺陷。传统的银行更多的依赖于封闭式物理隔离提供安全保障，随着网络金融的不断发展，越来越多的交易支付入口、大量离散的 ATM 节点、更多的跨行汇兑的出现，导致了从网络上对银行进行攻击，已经从预言变成一种广泛发生的事实。

关键信息基础设施的防护要防患于未然，而不能完全依赖“事件”推动，更多的针对关键信息基础设施的攻击是高度隐秘的，**这种攻击围绕持续的信息获取和战场预制展开，在这个过程中，CNE（网络情报利用）的行为是常态化的，是 CNA（网络攻击）的前提准备。**

2.2 线上线下结合的复合式作业在高级网络攻击中普遍出现

“乌克兰电力系统遭受攻击事件”的另一个重要的特点是，攻击者采用了线上和线下相结合的攻击方式，即通过网络攻击导致基础设施的故障，同时又通过对故障处置电话进行拒绝服务式攻击的方式，来干扰应急处置能力，提升恢复成本。

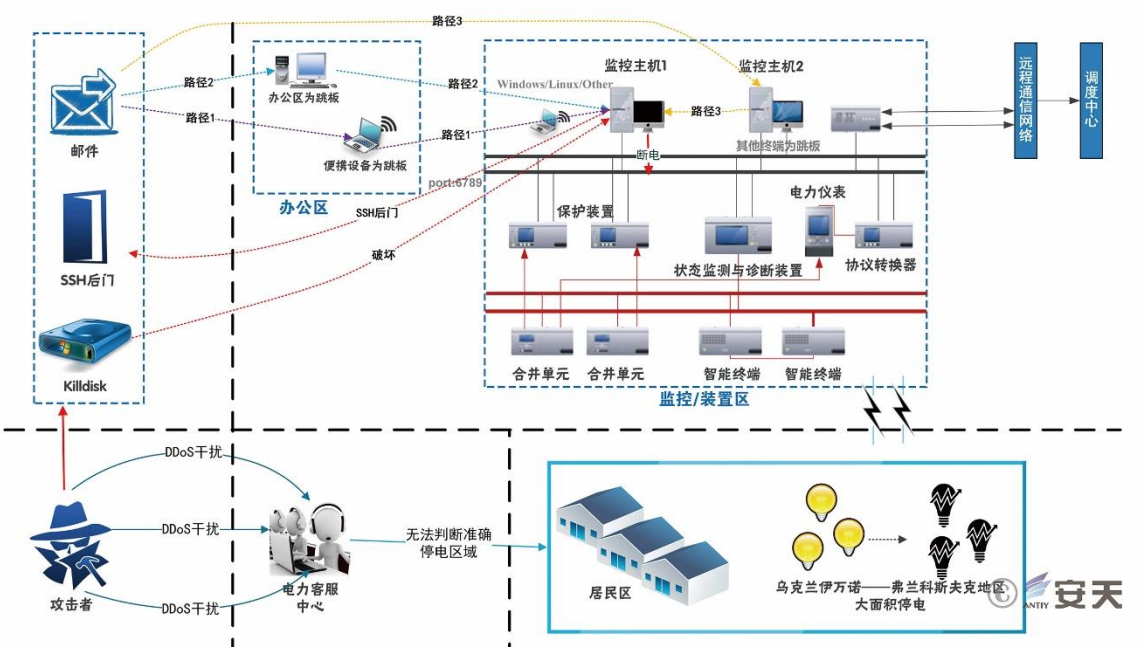


图 3“乌克兰电力系统遭受攻击事件”线上线下攻击作业图

“方程式”组织在 2009 年就已经被发现采用线下攻击手段扩展其作业流程，其将携带恶意代码的 CD 光盘伪装成正常的会议资料邮寄，通过光盘的自启动代码感染目标主机，然后再通过一系列的线上攻击完成整个攻击。

随着我们对风险的认知加深，从网络到达网络空间，我们需要看到的是，我们传统的把虚拟世界安全和物理世界安全割裂看待的思维以及界定网络风险和现实风险泾渭分明的执念，都会被动摇。我们看到的将只是形形色色攻击者为达成攻击目的所采用的各种攻击手段，至于是单纯地通过网络进行攻击，还是在攻击路径上结合传统的物理和电磁手段，只是高级攻击者的武备选择。

从安全威胁的演进史上来看，传统物理空间和网络空间本来就是联通的，早期黑客针对大型机系统的攻击，很多就是依靠人员混入办公场所踩点的方式完成的，就像上世纪凯文·米特尼克装扮成清洁工偷取计算机的操作手册一样，只是随着网络的普及，这种踩点逐步脱离了距离的困扰，并使成本逐渐下降。网络攻击和传统攻击的合流，有两个路径，一方面对于那些习惯网络作业的人而言，网络攻击只是一种能让攻击者获得心理安全感的方式，并在不断地试探社会法律底线的过程中，逐渐与网络风险威胁正面碰撞；而另外一方面，传统恐怖组织、犯罪团伙也在不断寻觅新的机会。当两者间有足够多的交集时，两害合流就成为必然。

在未来的网络空间博弈中，线上线下的复合式攻击将会越来越多。

2.3 网络空间防御能力最终是由攻击者和窥视者检验的

当前世界各国都执行了很多网络安全方面的检查和评估制度来发现安全问题、提升安全能力，但高级网络攻击依然屡屡得手。相关的合规安全检查和手段是必须的，但它并不能用来代替实战标准的检验。在我国应对境外 APT 攻击事件的过程中，同样面临着从技术角度衡量，能力不强的攻击者也能带来较大威胁的现实。

安天在 2016 年 7 月 10 日，依托持续捕获跟踪 4 年的成果，曝光了“白象”攻击组织，并发布《白象的舞步——来自南亚次大陆的网络攻击》[4]。这一攻击组织的样本在 2012 年 7 月被安天首次捕获发现。2013 年 5 月，挪威安全厂商 Norman 将这一组织命名为 HangOver，并判定这一组织的主要攻击目标为巴基斯坦，也从一定程度上威胁到了中国。而安天则称该组织为“白象”，安天通过持续分析发现，这一攻击组织的主要攻击方向已经从巴基斯坦转向中国，这反映了相关攻击组织和其背后国家的战略目标及战略阶段的转变。该组织在 2016 年的攻击波能力，相比此前有了较高提升，因此安天将这一波攻击称为“白象二代”。“白象二代”相比“白象一代”的技术手段更为高级，其攻击行动在整体性和技术能力上的提

升，可能带来攻击成功率的提升，而且其采用了更加暴力和野蛮的投放方式，使其攻击次数和影响范围远比“白象一代”更大。

表 2 “白象一代”和“白象二代”的分析对比

	白象一代	白象二代
主要威胁目标	巴基斯坦大面积的目标和中国的少数目标(如高等院校)	巴基斯坦和中国的大面积目标 ,包括教育、军事、科研、媒体等各种目标
先导攻击手段	鱼叉式钓鱼邮件，含直接发送附件	鱼叉式钓鱼邮件 ,发送带有格式漏洞文档的链接
窃取的文件类型	*.doc *.docx *.xls *.ppt *.pps *.pptx *.xlsx *.pdf	*.doc *.docx *.xls *.ppt *.pptx *.xlsx *.pdf *.csv *.pst *.jpeg
社会工程技巧	PE 双扩展名、打开内嵌图片，图片伪造为军事情报、法院判决书等，较为粗糙	伪造相关军事、政治信息，较为精细
使用漏洞	未见使用	CVE-2014-4114、CVE-2012-0158、CVE-2015-1761
二进制攻击载荷开发编译环境	VC、VB、DEV C++、AutoIT	Visual C#、AutoIT
二进制攻击载荷加壳情况	少数使用 UPX	不加壳
数字签名盗用/仿冒	未见	未见
攻击组织规模猜想	10~16 人，水平参差不齐	有较高攻击能力的小分队
威胁后果判断	造成一定威胁后果	可能造成严重后果

安天通过长期深入分析，追踪挖掘攻击组织的线索，并基于互联网公开信息，进行了攻击者画像，认为这是一个由 10~16 人组成的攻击小组。

图 4“白象一代”攻击组织画像

在过去数年间，中国的信息系统和用户遭遇了来自多方网络入侵的持续考验，这些攻击使用了各种高级的（也包括看起来并不足够高级的）攻击技巧，主要以获取机要信息、科研成果和其他秘密为目标。攻击组织在关键基础设施和关键信息系统中实现长期持久化，以窃密和获取更多行动主动权为目的，其潜在威胁之大、影响领域之深，绝非网站篡改涂鸦或传统 DDoS 所能比拟。这些攻击也随实施方的战略意图、能力和关注点的不同，表现出不同的方法和特点。尽管中国用户更多焦虑于那些来自上帝视角的攻击，但从我们针对“白象”的分析可以看到，来自地缘利益竞合国家与地区的网络攻击，同样是中国信息化的重大风险和挑战，而且这些攻击虽然往往显得有些粗糙，但却更为频繁和直接，挥之不去。

对于类似“白象”这样的攻击组织，因缺少人脉和电磁能力作为掩护，其更多依赖于类似电子邮件这样的互联网入口。从一个全景的防御视图来看，这本来是一个可以收紧的入口，但对于基础感知、检测、防御能力不足的社会肌体来说，这种具有定向性的远程攻击是高度有效的，而且会淹没在大量其他的非定向的安全事件中。

而当前一种值得反思的状态是，在一种“没有对手”的状态下推进和推演网络安全。**“物理隔离+好人假定+规定推演”，构成了一种安全假象和自我安慰，**网络分区策略和隔离手段无疑是必备且必要的安全策略，但如果不能伴随更强有力的内网安全策略，其可能带来更大的安全风险。安全策略和安全投入，需要以内网已被穿透和“内鬼”已经存在为前提假定来实行。

大国防御力，由设计所引导、以产业为基础、与投入相辅相成，但最终其真实水平，要在与攻击者和窥探者的真实对垒中来检验。

2.4 超级攻击组织攻击载荷具备全平台覆盖能力

在 2015 年初卡巴斯基和安天先后对“方程式”组织使用的恶意代码进行分析曝光后，“方程式”组织的一系列事件又在 2016 年浮出水面。在 2016 年 8 月和 10 月，一个自称“影子经纪人”的黑客团体所曝光的资料显示了“方程式”组织和此前被斯诺登曝光的 ANT 攻击装备存在一定联系，并由此看到其针对 Cisco、Juniper、Fortinet 等防火墙产品所达成的注入和持久化能力。“影子经纪人”爆料“方程式”组织从 2000 年开始入侵全球大量服务器，包括部分 Solaris、Oracle-owned Unix 等版本的操作系统，尽管并未提供证据，但这与安天的捕获分析工作相互印证，一个关于这个超级攻击组织的几乎无死角的、全平台化的攻击能力已经日趋清晰。在这种情况下，安天于 2016 年 11 月 4 日发布了《从“方程式”到“方程组”——Equation 攻击组织高级恶意代码的全平台能力解析》[5]报告，独家分析了其在 Solaris 平台和 Linux 平台上的攻击样本，这是业内首次正式证实这些“恶灵”真实存在的公开分析。

图 5“影子经济人”爆料的“方程式”组织在 2000~2010 年间在全球范围内入侵服务器的情况

在过去数年，这种分析如此漫长、复杂和艰难，超出了我们之前对“震网（Stuxnet）”、“火焰（Flame）”的分析和复现中所面临的挑战。这种高度复杂、隐蔽的全能高级恶意代码，无论是对受害者，还是分析者来说，都是一个巨大的挑战。特别是当其打击范围几乎覆盖所有体系结构与操作系统的时候，相对更擅长 Windows、Linux 和 Android 等主流操作系统平台下恶意代码分析的传统安全分析团队明显感受到了巨大的压力和挑战。如果用这个组织的名称“方程式”做一个关于分析难度的比喻，我们需要破解的已经并不只是一个“方程式”，而是更为复杂的、多元多次的“方程组”。通过梳理当前对“方程式”组织的主要分析成果和爆料，可以看到“方程式”组织的多平台操作系统覆盖能力图表：

表 3 “方程式”组织多平台操作系统覆盖能力拼图

信息	Windows	Linux	Solaris	Oracle-owned Unix	FreeBSD	Mac OS
安天：修改硬盘固件的木马探索方程式（EQUATION）组织的攻击组件[6]	分析样本载荷和硬盘持久化能力					
安天：方程式（EQUATION）部分组件中的加密技巧分析[7]	分析加密算法					
卡巴斯基：Equation: The Death Star of Malware Galaxy[8]	揭秘方程式攻击组织					
卡巴斯基 :A Fanny Equation: "I am your father, Stuxnet"[9]	Fanny 组件分析					
卡巴斯基：Equation Group: from Houston with love[10]	Doublefantasy 分析					
卡巴斯基：《EQUATION GROUP: QUESTIONS AND ANSWERS》[11]	方程式组织：问与答					猜测
The Hacker News：《Shadow Brokers			曝光存在	曝光存在	曝光存在	

reveals list of Servers Hacked by the NSA》						
安天：《从“方程式”到“方程组”——Equation 攻击组织高级恶意代码的全平台能力解析》[5]		曝光存在，分析相关载荷	正式存在，分析相关载荷			

注：安天在 Solaris 样本中分析出的 User Agent 具有 Solaris 标识，而卡巴斯基在“EQUATION GROUP: QUESTIONS AND ANSWERS”中披露出曾捕获到 Mac OS X 的 User Agent 的信息，由此来看，尽管安天、卡巴斯基等厂商，目前都尚未捕获 Mac OS X 的样本，但“方程式”组织针对 Mac OS X 的攻击载荷是真实存在的。

安天希望用自己的工作告诉用户，那些关于超级攻击组织的全平台覆盖能力的种种爆料并非传说，而且是一种真实的威胁，是一种既定的事实。而这种武器，不仅被用于攻击隔离网内的传统高等级目标，也被用于攻击互联网节点。

在我国安全防御的实践中，有一种先入为主的观点，即认为由于各种规定和约束，暴露在互联网上的节点，乃至能够访问的互联网内网中，并不存放高价值的信息。“一切有价值的信息都存在于隔离网内”——这是一个美好的愿景和想象，但并非是这个信息大量产生、高速流动时代的真实情况。同时在大数据时代，高价值信息的定义和范围也在不断变化着，更多的信息资产已经不可避免地分布在公共网络体系中，而对这些资产的窥视和攻击也在持续增加着，而超级攻击组织则是类似攻击的始作俑者和长期实践者。

针对 DNS 服务器的入侵，可以辅助对其他网络目标实现恶意代码注入和信息劫持；针对邮件服务器的植入可以将用户所有的邮件通联一网打尽；针对运营商骨干节点的持久化，可以用来获取全方位的信息，包括收获类似 Camberdada[12]计划中所说的那种“轻而易举的胜利（An Easy Win）”。

注：Camberdada 计划是斯诺登曝光的一份监听行动计划，相关机构通过运营商被持久化的节点，监听用户发放给杀毒厂商的邮件，以发现自己的攻击是否暴露，并实现对其他方投放的样本捕获和再利用。

就像我们此前所概括的那样，相关超级攻击组织拥有“成建制的网络攻击团队、庞大的支撑工程体系与制式化的攻击装备库、强大的漏洞采集和分析挖掘能力、关联资源储备以及系统化的作业规程和手册，具有装备体系覆盖全场景、漏洞利用工具和恶意代码载荷覆盖全平台、持久化能力覆盖全环节的特点。面对这种体系化，既具备工业级水准，又具有高度定向性的攻击，‘永动机’将注定停摆，‘银弹’将注定哑火。想要达成防御效果，实现追踪溯源，唯有以清晰的战略、充分的成本投入，以体系化的防守对决体系化的攻击，通过长期艰苦、扎实的工作和能力建设，才能逐渐取得主动。”

2.5 网络空间的商业军火进一步降低 APT 成本

网络空间安全中的“商业军火”，是指以商业产品的方式进行销售和交易的、具有武器级水准的攻击平台、恶意代码、漏洞及其利用程序，以及其他用于助力达成攻击的工具或组件等，其中包括 Cobalt

Strike 等商用攻击平台，也包括 RIG、Magnitude 等漏洞工具包等。安天在 2015 年 5 月 27 日发布的《一例针对中国官方机构的准 APT 攻击事件中的样本分析》[13]中，充分解读了商业攻击平台 Cobalt Strike 在攻击中所发挥的作用，并指出“商业攻击平台使事件的攻击者不再需要高昂的恶意代码开发成本，相关攻击平台亦为攻击者提供了大量可选的注入手段，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、也缺少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 级水准的攻击，而这种高度‘模式化’的攻击也会让攻击缺少鲜明的基因特点，从而更难追溯。”而在 2016 年全年中国所遭遇到的 APT 攻击中，能反复看到 Cobalt Strike 的痕迹，友商 360 企业安全对此发布了报告并进行了跟进分析[14]。

商业军火通常具有以下几个特点：

- **具备武器级水准**

商业军火不是一般性质的恶意代码或者漏洞情报，而是具有武器级水准的攻击装备，以 Cobalt Strike 为例，其尽管号称是开源漏洞测试平台 Metasploit 和 Armitage（Metasploit 的图形界面）的商用版本，但其 Payload 能力完全是按照实战设计的——可投放载荷覆盖全操作系统平台、格式文档载荷包括大量的可构造溢出格式、载荷可以实现样本不落地、窃密加密回传和远程加密控制，其根本不是一般意义上的漏洞扫描测试平台，更不是军火商自我比喻的靶弹，而是真实的、带有战斗目的的导弹。

- **高附加值交易是维持商业军火交易供需关系的纽带**

商业军火尽管反复出现在 APT 攻击中，但商业军火的供应是商业行为，而不是类似 TAO 等攻击组织人员的职务行为。同时，尽管木马交易和漏洞交易一直都存在，但商业军火不是传统黑产低水准的木马交易买卖，也不是传统的漏洞收购，而是高质量的攻击装备“商品”，这使得这种交易既是高附加值的，也是规模化的。如其提供的是实际有效的能力，包括 0Day 漏洞利用工具，而不是基本的漏洞信息或 POC，其木马往往带有较高的模块化水平和 Rootkit 能力。

- **商业军火的出品机构往往具有一定的政经背景**

以 Cobalt Strike 的出品人 Raphael Mudge 为例，他曾经是美国空军的安全研究员、渗透实验的测试者，并深度参与了 Red Team 项目。

表 4　Raphael Mudge 的履历

公司/项目/机构	职位	时间
Strategic cyber LLC	创始者和负责人	2012.1-至今
特拉华州空军国民警卫队	领导，传统预备役	2009-至今
Cobalt Strike	项目负责人	2011.11-2012.5
TDI	高级安全工程师	2010.8-2011.6

Automattic	代码 Wrangler	2009.7-2010.8
Feedback Army, After the Deadline	创始人	2008.7-2009.11
美国空军研究实验室	系统工程师	2006.4-2008.3
美国空军	通信与信息军官	2004.3-2008-3

- **商业军火背景下的能力流动导致威胁复杂化**

信息武器的一个特点是其复制成本几乎为零，商业军火能力流动呈现出一定规律，一方面通过以斯诺登泄密、“影子经济人”爆料为代表的事件使商业军火有了更多的高级参考模式和样板；另一方面通过以 Hacking Team 信息泄露为代表的事件，则又使商业军火能力可以迅速在短时间内达到地下黑产的普遍水平。

一定程度上，商业军火被作为一种“以攻验防”的安全产品在出售，但其对于信息安全的先发国家和发展中国家的影响明显是不同的，对长期落实纵深防御理念、基础防护手段实现了长期有效投入、积极防御和威胁情报已经产生作用的信息系统来说，商业军火的影响是有限的，但对于发展中国家的信息体系来说，则可能是一种灾难。因此商业军火的泛滥，首先带来的是金字塔的底层混乱，而**不受控的商业武器，更有利于巩固一个单极的世界**。

图 6 网络攻击中的商业军火覆盖面

2.6 APT 攻击并不必然使用高级的攻击装备和手段

APT 攻击事件更容易令人联想到高级攻击手段，或是专属开发攻击装备、购买商业军火等装备，或是使用盗取的数字签名、使用独有或购买的漏洞等手段。在 APT 事件的攻击装备和手段被曝光后，其攻击装备和手段被其他攻击组织、地下黑色产业链、普通黑客等效仿，使得 APT 攻击技术常态化。反之，APT 攻击以目的达成为目标，以对针对性目标造成破坏或信息窃取为最终目的，其达成最终目的的攻击装备和手段并不必然是高级的攻击装备和手段。

从美国的国土安全部（DHS）与国家网络安全和通信集成中心（NCCIC）发布的《灰熊草原-俄罗斯的恶意网络活动》(GRIZZLY STEPPE – Russian Malicious Cyber Activity) 报告[15]来看，攻击者所使用的攻击手段如传统的鱼叉式电子邮件攻击、水坑攻击等，投放的载荷为带有恶意宏代码的 Office 文档，利用的是已知漏洞嵌入恶意代码的 RTF 格式文件，安装到目标主机的恶意代码是常规的远程控制工具。在这种看起来很普通的攻击装备和技巧下，攻击组织通过单方面爆料的方式，试图影响政治平衡。正如物理学中，力有大小、方向和作用点三要素一样，看似同样的攻击技巧和攻击手段，施加于不同作业面，完全可能产生不同的效果。因此，APT 判断的核心依然是对作业背景和攻击组织的判定，将 APT 概念泛化到一些使用高级手段和技巧的非定向性攻击行为，是不负责任的，没有攻击意图和攻击意志的 APT 分析判定，是不可靠的。

3 大规模数据泄露导致“威胁情报反用”

“雅虎 5 亿条账户信息泄露事件”是 2016 年数据泄露的标志性事件，其为雅虎带来了超过 20 项集体诉讼并导致高管辞职的后果。但这一事件其实早在 2014 年已经发生，只是在 2016 年被曝光而已。这种时间差，代表着比大规模数据泄露事件更令人恐惧的威胁是，大量个人信息被隐秘地利用和买卖，但用户对此浑然不觉。

单纯从泄露事件曝光的数量来看，2016 年并不是历史上最多的，但相关威胁和各种传统犯罪形式的融合已经更加深入，例如在针对 IRS（美国国家税务局）的攻击中，攻击者破坏了 PIN 码重置申请，获取了超过 10 万个 PIN 码，并企图提交诈骗性的退税申请；在国内，则发生了震惊全国的“徐玉玉事件”，其个人信息被攻击者窃取后倒卖给诈骗团伙，并在被诈骗学费后身亡。

3.1 黑产大数据已经具备了接近全民画像能力

网络黑色产业链造成了大量数据泄露，这些海量敏感数据构成了黑产大数据。黑产大数据除了用于精准的广告投放，还会被不法分子滥用，给互联网用户带来更严重、更直接的经济损失。交通、医疗、教

育、金融、酒店、物流等公共服务行业机构都掌握了大量的用户信息，因此，这些与社会生活紧密相关的行业成为了黑色产业链紧盯的目标。图 7 中总结了 2016 年我国发生的部分数据泄露事件，而实际发生的泄露事件要远多于图中所示内容。这些事件的背后均有网络黑色产业链的身影，数据泄露的原因除了黑客通过入侵网站并拖库外，撞库攻击、企业内部员工倒卖、钓鱼网站骗取信息以及恶意代码盗取信息也都是黑产从业者非法获取数据的手段。

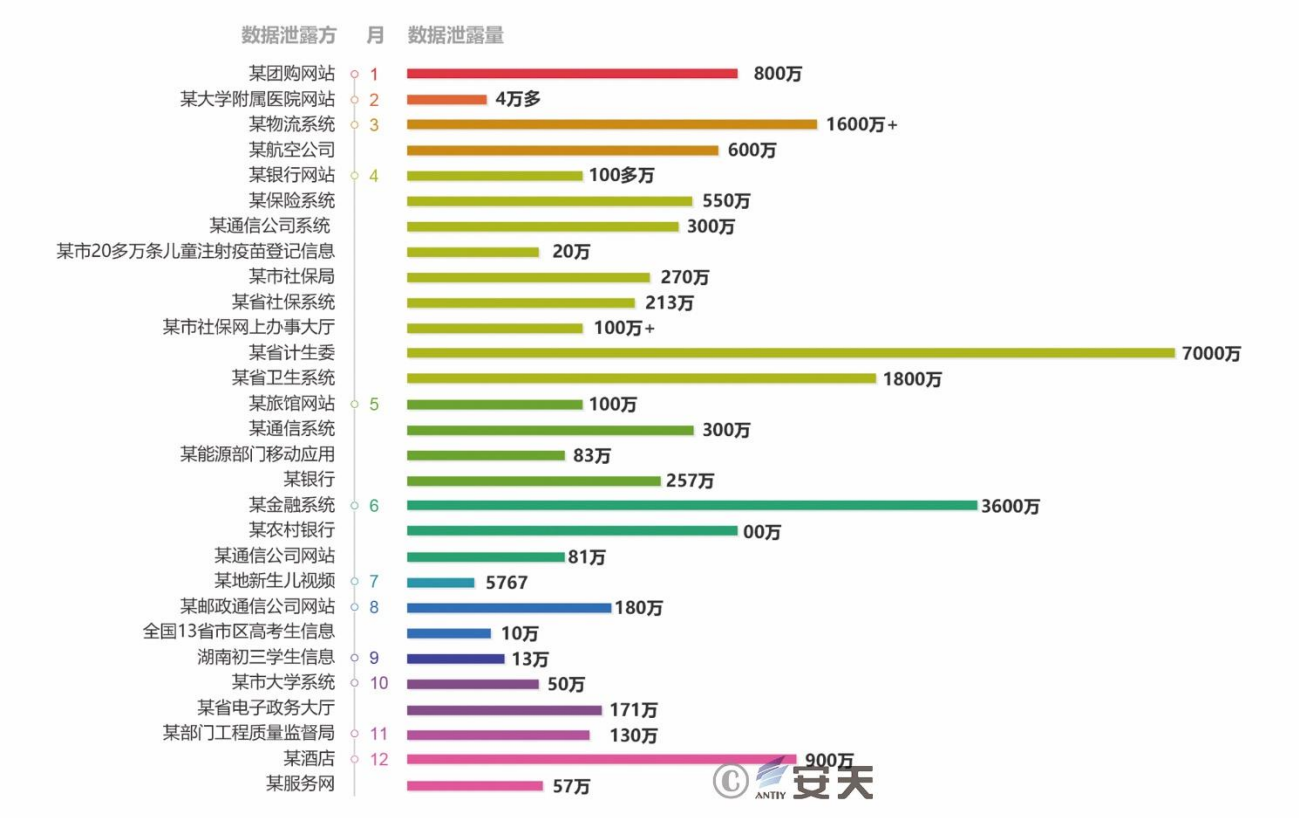


图 7 2016 年国内重大数据泄露事件

窃取用户敏感数据已经形成产业化，黑色产业链的各业务线上均有明确分工，各业务线之间相互协作，形成了从多方面侵害互联网用户的利益链条。最上游的是掌握攻击技术的黑客，他们是整个产业链上最隐蔽的群体，通过漏洞挖掘、渗透网站、拖库、撞库甚至是传播恶意代码的方法获取用户的敏感信息，随后通过一系列技术手段清洗数据，提炼出具有价值的黑产大数据，贩卖给下游的业务线。黑产的中游主要利用从上游买来的黑产大数据编造专门的诈骗“脚本”，通过社会工程学的方式对用户实施具体的欺诈行为或进行精准的广告投放。黑产的下游是支撑整个黑色产业链各个周边的组织，如取钱和洗钱团伙、收卡团伙、贩卖身份证团伙等。

3.2 威胁情报也是情报威胁

有部分观点认为大规模的数据泄露也是一种威胁情报来源，但其中的尴尬是，这些数据其实属于网民个体的信息，同时其数据组织本质上是泄露方的资产。

威胁情报是攻防双方的公共地带，例如 C&C，对防御方来说是规则和线索，对攻击方来说则是攻击资源和痕迹。安全事件的追踪溯源是为了定性事件性质、实施针对性防御策略、追踪溯源攻击者或组织机构等，而追踪溯源技术中使用的关键基因在威胁情报中具有非常具象的表现。威胁情报的共享，为更高效、全面的事件追踪提供了有力的支撑，而广泛的威胁情报开放查询，也为攻击者分析自身是否存在暴露和反向分析防御者的手段带来了入口。虽然威胁情报提供厂商可以通过对查询者的查询数据及过程进行目的分析，但在这种反向作业手段并未形成行业共识、反向作业技术也并不成熟时，威胁情报提供厂商并不能明确地区分自身用户和攻击者是否有重叠的部分。**如果不能把威胁情报服务收敛于客户的自有资产范围，可能会带来新的目标制导。**

4 PC 恶意代码针对重要目标，移动恶意代码快速增长，勒索软件成焦点

2016 年安天捕获的新增传统恶意代码家族数为*1,280 个，新增变种数为 912,279 种，这些变种覆盖了亿级的样本 Hash。传统恶意代码的增量开始放缓，移动和新兴场景的恶意代码开始不断上升。同时，APT 攻击作业中的恶意代码样本的模块化和抗分析特性也在进一步增强。而无论在 PC 端还是移动端，勒索软件都将成为重要威胁。

*注：由于“安天基础威胁年报”和“安天移动威胁年报”是分开发布的，所以基础威胁年报的统计中不包括移动系统的恶意代码。

4.1 灰色地带比重进一步加大

在 2016 年恶意代码家族数量排行榜前十名中，具有广告行为的 Grayware 和 Riskware 共占了五个席位，另外五席均为木马程序，与去年的 TOP10 列表相比，木马程序减少了一位。

- 排行第一的是灰色软件家族 BrowseFox，它是一种通过与免费软件和共享软件捆绑传播的具有正常数据签名的广告软件，无论在用户知情还是不知情的情况下都可以进入计算机；BrowseFox 将侵入所有的浏览器，包括 Internet Explorer、Google Chrome、Mozilla Firefox 等，然后就会弹出各种各样的广告，这些广告主要推广第三方产品和服务，甚至修改浏览器的起始页、默认搜索引擎等设置；最后，BrowseFox 还将收集用户在网上的浏览历史、搜索词语等信息，再回传到后端的数据库中，其被数据分析后，将用来进行更精准的推广行为。

- 排行第二的是风险软件家族 DownloaderGuide，这是一个专业的下载器，其唯一的目的就是下载其他程序到主机中，被下载安装的程序通常不会被用户发现，它们通常都有名称为“Freemium GmbH”的无效数据签名。
- 排行第三的是风险软件家族 LMN，其具有使用 BT 协议下载第三方程序到本地安装的功能，例如：下载安装浏览器 Amigo、浏览器插件 Unity Web Player、俄罗斯邮箱客户端 Mail.Ru 等，某些安装程序在重启系统时并不会提示用户，而直接关机重启，这些情况都会影响用户对计算机的正常使用。
- 排行第四的是自动化命名的木马 Agent。
- 排行第五的是远程控制家族 IRCBot，该家族通过 IRC 通信信道进行传播或发送远程控制命令，该家族的核心行为是接受 IRC 远程控制，同时对文件进行上传下载、发起 DDoS 攻击等，它是一个较早的恶意代码家族，但在 2016 年依然非常活跃。
- 排行第六的是使用 VBS 编写的捆绑类木马程序，其家族主要功能是下载其他恶意代码到系统中运行，在 2016 年被 VBS、JS、PowerShell 等下载最多的恶意程序就是臭名昭著的勒索软件。
- 排行第七的是木马家族 Reconyc，其更像一个广告程序，因为它的主要功能是弹出广告、浏览器重定向、添加浏览器工具栏或插件。
- 排行第八的是具有释放或捆绑行为的木马类程序 Dinwod，该家族在感染用户系统之后，会自动释放并安装其它恶意程序，很多容易被查杀的恶意程序通过隐藏在此类木马内部来躲过反病毒软件的检测，进而感染用户计算机，该家族的部分变种还具有强制关闭杀毒软件的能力。
- 排行第九的是一种可以下载并安装风险应用的风险软件家族 OutBrowse，该家族样本运行后下载并安装名为“FLV Player”的安装程序，点击接受开始下载后，将会弹出广告页面、占用系统资源、影响用户使用。
- 排行第十的是一种可以下载并安装推广应用的灰色软件程序 ICLoader，该家族样本运行后连接网络下载推广应用并安装，占用系统资源，影响用户正常使用计算机。

在 2016 年 PC 平台恶意代码行为排行榜中（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、实用性强的特点而数量依然较多。网络传播行为和风险工具分列三、四位，溢出行为上升到了第五位，勒索行为虽然从行为数量统计上排在第十二位，但其带来的损失巨大，显然勒索行为是 2016 年最值得关注的恶意行为。

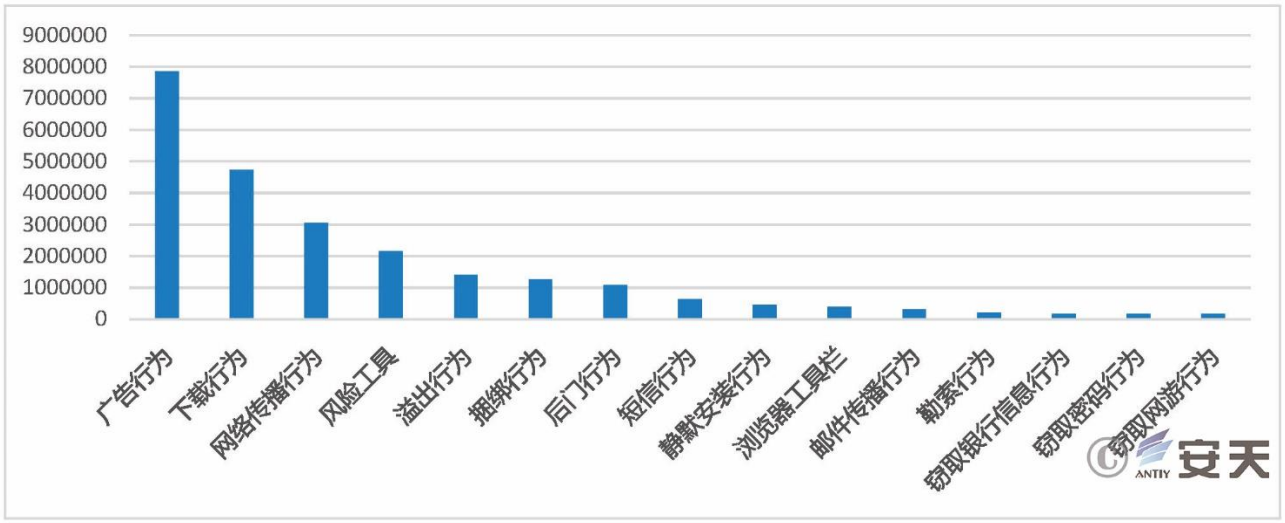


图 8 2016 年 PC 平台恶意代码行为分类排行

4.2 勒索软件从一种恶意代码行为扩展到一种经济模式

国外研究者 Danahy 认为[16] “敲诈者”病毒的崛起是由两个因素造成的：其一是越来越多的不法分子发现这种攻击方式利润丰厚；其二是勒索工具、开发包和服务的易用性和破坏力不断提高。安天研究人员对此的补充观点是——“比特币匿名支付和匿名网络带来的犯罪隐蔽性也是其中重要的原因。”[17]

2016 年全球多家医院遭受勒索软件 SamSam 的袭击，在医院电子资产、患者信息等被加密后，被敲诈了上百万美金的赎金，同时患者的健康与生命均受到不同程度的威胁。这是 2016 年首例曝光的大规模针对企业客户的勒索软件事件，勒索软件通过由 JBoss 漏洞或其他漏洞攻击包组成的攻击组件对企业客户进行攻击，其在成功入侵一台终端计算机后，利用这台计算机作为“支点”，通过半自动化手段进行内网攻击，尽可能的感染内网中的其他计算机，扩大加密的电子资产数量，甚至加密用以备份的电子资产。在安天《2015 年网络安全威胁的回顾与展望》[18]中曾提出的**“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”**等观点已经完全被 2016 年发生的勒索攻击事件所验证。

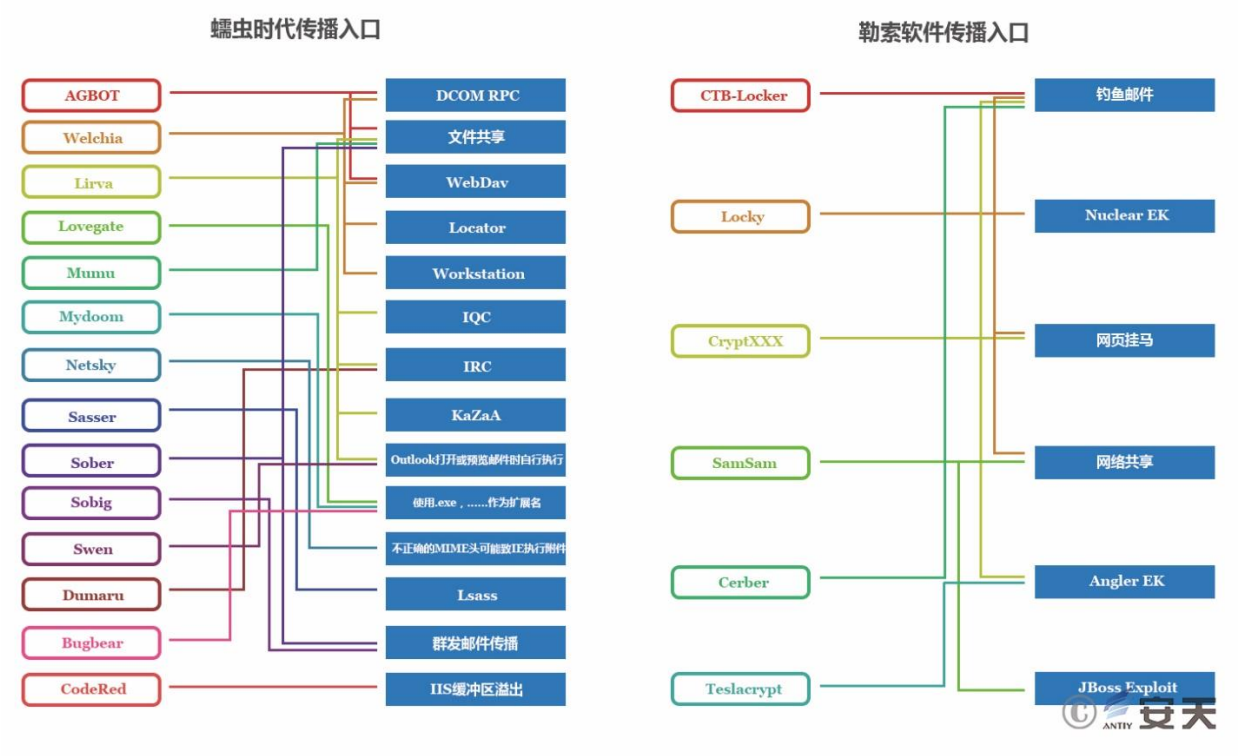


图 9 蠕虫时代的传播入口到勒索软件的传播入口

图 10 需要警惕的勒索软件入口

安天 CERT 曾在 2004 年绘制了当时的主流蠕虫与传播入口示意图（图 9 左图早期图表），该图曾被多位研究者引用。可以肯定的是，尽管其中很多方式在 DEP（Data Execution Prevention，数据执行保护）和 ASLR（Address Space Layout Randomization，地址空间布局随机化）等安全强化措施下已经失效，但存在问题的老版本系统依然存在。勒索模式带动的蠕虫回潮不可避免，同时利用现有僵尸网络分发，针对新兴 IoT 场景的漏洞传播和制造危害等问题都会广泛出现。而从已经发生的事件来看，被敲诈者不仅包括最终用户，而且在大规模用户被绑架后，厂商也遭到敲诈。

勒索软件给国内政企网络安全也带来了新的挑战。在较长时间内，国内部分政企机构把安全的重心放在类似网站是否被篡改或 DDoS 等比较容易被感知和发现的安全事件上，但对网络内部的窃密威胁和资产侵害则往往不够重视，对恶意代码治理更投入不足。因为多数恶意代码感染事件难以被直观地发现，但“敲诈者”以端点为侵害目标，其威胁后果则粗暴可见。同时，对于类似威胁，仅仅依靠网络拦截是不够的，必须强化端点的最后一道防线，必须强调终端防御的有效回归。安天智甲终端防御系统研发团队依托团队对“敲诈者”的分析和预判，依托安天反病毒引擎和主动防御内核，完善了多点布防，包括文档访问的进程白名单、批量文件篡改行为监控、诱饵文件和快速文件锁定等。通过这些功能的强化，安天不仅能够有效检测防御目前“敲诈者”的样本，并能够分析其破坏机理，还对后续“敲诈者”可能使用的技巧进行了布防。除了 PC 端的防护产品，安天移动安全团队（AVL TEAM）对 Android 平台的反勒索技术做了很多前瞻性的研究工作，并应用于安天移动反病毒引擎中。

金钱夜未眠，在巨大的经济利益驱使下，未来勒索软件的传播途径和破坏方式也会变得愈加复杂和难以防范。作为安天智甲的开发者，我们期望帮助更多用户防患于未然。

5 IoT 威胁影响国家基础设施安全，车联网安全成为威胁泛化的年度热点

在 2013 年，我们用恶意代码泛化（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”一直是我们所关注的重要威胁趋势。

当前，安全威胁泛化已经成为常态，我们依然采用与我们在前两次年报中发布“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 2016 年威胁泛化的形势。

2016网络安全威胁泛化与分布

5.1 IoT 威胁影响国家基础设施安全

物联网是由不需要人工干预的具有传感系统的智能设备组成的网络，在现今的人类社会中，IoT 存在于社会应用的各个角落，如可穿戴设备、车联网、智能家庭、智慧城市、工业 4.0 等。当 IoT 产生威胁时，它会不分地域、不分行业的影响到全社会。

2016 年最具影响力的安全事件，无疑是美国东海岸 DNS 服务商 Dyn 遭遇源自 IoT 设备的 DDoS 攻击所导致的断网事件。Dyn 公司在事发当天早上确认，其位于美国东海岸的 DNS 基础设施所遭受的 DDoS 攻击来自全球范围，严重影响其 DNS 服务客户业务，甚至导致客户网站无法访问。该攻击事件一直持续到当地时间 13 点 45 分左右。本次 Dyn 遭到攻击影响到的厂商服务包括：Twitter、Etsy、GitHub、Soundcloud、Spotify、Heroku、PagerDuty、Shopify、Intercom，据称 PayPal、BBC、华尔街日报、Xbox 官网、CNN、HBO Now、星巴克、纽约时报、The Verge、金融时报等的网站访问也受到了影响。Dyn 公司称此次 DDoS 攻击事件所涉及的 IP 数量达到千万量级，其中很大部分来自物联网和智能设备，并认为攻击来自名为“Mirai”的恶意代码。安天发布了《IoT 僵尸网络严重威胁网络基础设施安全——北美 DNS 服务商遭 Mirai 木马 DDoS 攻击的分析思考》[19]，对这一事件做出了深度分析。

目前，依托 IoT 设备的僵尸网络的规模不断增长，典型的 IoT DDoS 僵尸网络家族包括 2013 年出现的 CCTV 系列、肉鸡 MM 系列[20]（Chicken MM，数字系列 10771、10991、25000、36000）、BillGates、Mayday、PNScan、gafgyt 等众多基于 Linux 的跨平台 DDoS 僵尸网络家族，安天对这些木马的规范命名如下：

表 5 截止到 Mirai 事件发生时，IoT 僵尸网络的样本情况

家族名称	变种数量	样本 Hash 数量
Trojan[DDoS]/Linux.Mirai	2	大于 100
Trojan[DDoS]/Linux.Xarcen	5	大于 1000
Trojan[DDoS]/Linux.Znaich	3	大于 500
Trojan/Linux.PNScan	2	大于 50
Trojan[Backdoor]/Linux.Mayday	11	大于 1000
Trojan[DDoS]/Linux.DnsAmp	5	大于 500
Trojan[Backdoor]/Linux.Ganiw	5	大于 3000
Trojan[Backdoor]/Linux.Dofloo	5	大于 2000
Trojan[Backdoor]/Linux.Gafgyt	28	大于 8000
Trojan[Backdoor]/Linux.Tsunami	71	大于 1000
Worm/Linux.Moose	1	大于 10

Worm[Net]/Linux.Darlloz	3	大于 10

其中在本次事件中被广泛关注的 Mirai 的主要感染对象是物联网设备，包括路由器、网络摄像头、DVR 设备。DDoS 网络犯罪组织早在 2013 年开始就将抓取僵尸主机的目标由 Windows 转向 Linux，并从 x86 架构的 Linux 服务器设备扩展到以嵌入式 Linux 操作系统为主的 IoT 设备。安天捕获并分析了大量关于智能设备、路由器的恶意样本，并配合主管部门对部分设备进行了现场取证。这些设备主要是 MIPS、ARM 等架构，因存在默认密码、弱密码、严重漏洞未及时修复等因素，导致被攻击者植入木马。由于物联网设备的大规模批量生产、批量部署，使得在很多应用场景中，集成商和运维人员的能力不足导致了设备中有很大比例使用默认密码、漏洞得不到及时修复，也包括 Mirai 等针对物联网设备的 DDoS 入侵主要以通过 Telnet 端口进行流行密码档的暴力破解，或通过默认密码登陆等方式实现，如果通过 Telnet 登陆成功，就尝试利用 BusyBox 等嵌入式必备的工具进行 wget 下载具有 DDoS 功能的 bot，修改可执行属性，运行控制物联网设备。由于 CPU 指令架构的不同，在判断了系统架构后，一些僵尸网络可以选择 MIPS、ARM、x86 等架构的样本进行下载。运行后接收相关攻击指令进行攻击。安天在此前跟进 IoT 僵尸网络跟踪分析过程中，发现了部分 DVR、网络摄像头、智能路由器的品牌中有部分型号存在单一默认密码的问题。

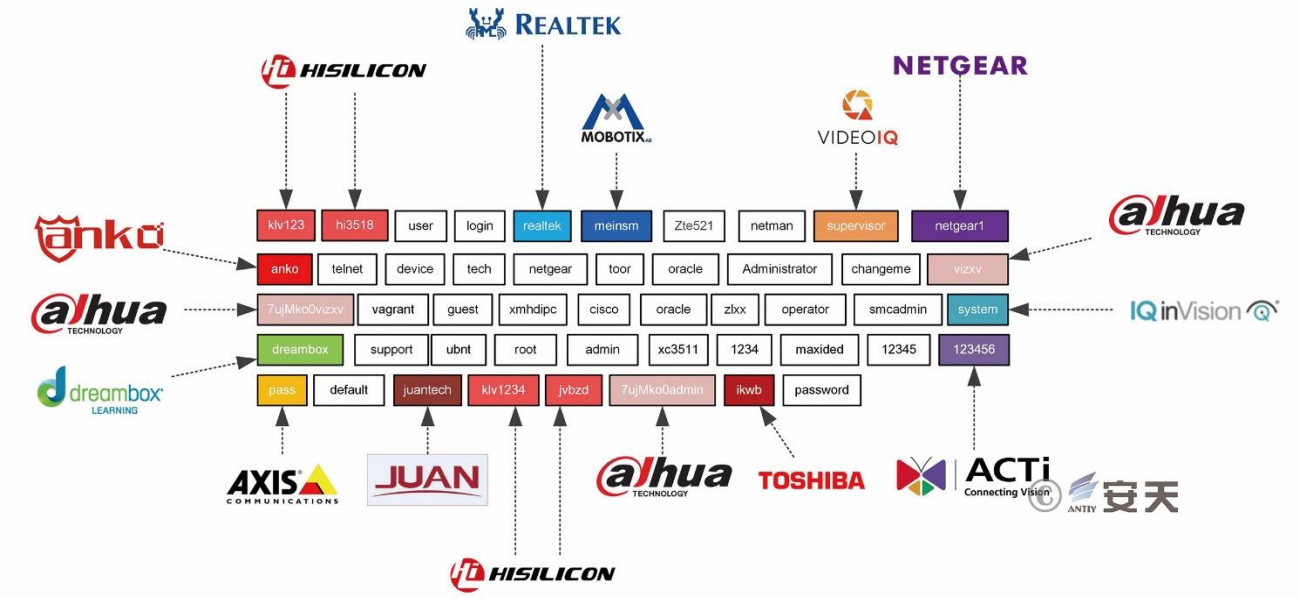


图 11 Mirai 的破解密码档针对品牌默认口令的攻击映射

IoT 设备利用种类繁多的网络协议技术使得网络空间与来自物理世界的信息交互成为可能，但是 IoT 自身具备以下不安全因素：IoT 设备自身多数未嵌入安全机制，同时其又多半不在传统的 IT 网络之内，等于游离于安全感知能力之外，一旦遇到问题也不能有效响应；大部分的 IoT 设备 24 小时在线，其是比桌面 Windows 更“稳定”的攻击源；作为主流桌面操作系统的 Windows 的内存安全（如 DEP、ASLR、

SEHOP）等方面的能力不断强化，依托远程开放端口击穿 Windows 变得日趋困难，但对普遍没有经过严格安全设计的 IoT 设备进行远程注入的成功率则高得多。

尽管 DNS 的确被很多人认为是互联网的阿喀琉斯之踵，但在这次针对 Dyn 的 DNS 服务的大规模 DDoS 事件中，暴露出的 IoT 安全问题更值得关注。IoT 僵尸网络绝不仅仅是这起攻击事件的道具，被入侵的这些设备本身具有更多的资源纵深价值，这比使用这些设备参与 DDoS 攻击所带来的危险更为严重。大面积存在的脆弱性，带来了更为隐蔽、危害更大的社会安全风险和国家安全风险，只是这种风险，更不容易被感知到罢了。

物联网就是物物相连的互联网，是未来信息社会重要基础支撑环节之一。物联网是在互联网基础上延伸和扩展的网络，物联网并不仅仅是网络，它还可以利用具有感知技术、信息传感等技术的嵌入式传感器、设备及系统构建成复杂的涉及实体社会空间的应用，这些应用所在的设备很多都是维系民生的重要节点的关键基础设施设备，甚至包括关键工控设施的基础传感器。因此，安全性必须加入到产品的设计中，而不是采用把默认密码硬编码到固件中、Web 接口轻易被绕过等方法，仅考虑部署简易，将安全置之度外，势必会留下安全威胁隐患。被入侵的这些设备本身具有更多的资源纵深价值，这比使用这些设备参与 DDoS 攻击所带来的危险更为严重。因此，无论从国家层面还是厂商层面来看，都应加强 IoT 设备的安全防护，提高攻击入侵 IoT 设备的成本，以及加强对 IoT 设备的安全威胁监测预警。

5.2 车联网安全到智能交通安全将成为一个博弈焦点

2016 年，车联网安全开始受到广泛的关注。大众汽车被爆出漏洞，可使得攻击者通过对无线钥匙的重放攻击实现对车辆的解锁，安全研究者发现可以通过 OBDII 接口对 Jeep 进行控制操作，国内的如 Keen Team、360 等安全团队都在各种极客活动上对 Tesla 等车辆的漏洞进行了曝光。

汽车行业是国民经济发展的中流砥柱，新能源汽车、智能化和网联化正在加速汽车行业的发展，催生了车联网、无人驾驶、高精度定位、大数据等技术在汽车行业的应用，为“互联网+汽车”添加催化剂。汽车行业在智能化和网联化方面的发展趋势，也催生了汽车电子行业的更新变革，从芯片、车载电子控制系统到车机系统等软硬件供应商，以 TSP 为主的车联网服务供应商，都有新玩家入局和老玩家出局的情况发生，整个汽车电子行业正在进入重新洗牌阶段。

汽车是现代社会的基本交通工具，日常生活中的手机、电脑，遭受攻击时损失更多的可能是位于虚拟空间的数据，严重时将影响财产安全，而汽车遭受攻击时，可能会威胁人身健康与生命的安全。因此汽车行业在智能化和网联化方面的发展趋势，也引起了整个行业对信息安全的关注，汽车行业正在由完全不重视信息安全转变为开始意识到信息安全对品牌和未来车联网服务的重要性。未来在政府出台相关标准、汽车安全事件的持续曝光、信息安全企业持续进行相关技术创新，以及车主的安全意识不断增强的多重影响下，整

个汽车行业会逐步建立和强化安全意识。

智能汽车面临着复杂的直接攻击风险和供应链安全风险，从直接风险来看包括：

- 物理接触：通过和车辆的物理接触实现攻击，主要攻击模式为通过在车上插入 OBD 来攻击车载系统。
- 近场通信劫持：在离车辆较近的距离方位内，主要通过劫持相应近场通信协议如 NFC、蓝牙等，进行重放攻击，典型攻击为破解无线钥匙，开启车门。
- 远程控制：该种攻击无需接触或靠近车辆，通过对“端-管-云”三者的其中一环进行攻击完成盗取用户信息、甚至控制车辆的操作。

因此汽车整体的信息安全必然涉及“两端一云”（手机端/汽车端+车联网云服务），从攻击面上来说，包括了手机终端、汽车端车机系统、汽车端电子控制系统和车联网云服务以及近场和远程通信的各种安全问题，因此所涉及到的信息安全方案一定是综合性的，涉及到的供应商也是各个层面的，比如车载安全芯片、车载防火墙、车机娱乐系统安全加固、车载 App 威胁检测与防护、车载系统安全 OTA 升级、通信加密与认证、手机 App 威胁检测与防护、云安全等。

车联网安全的未来将从单纯的车辆安全扩展到智能交通体系的安全和整个社会安全，而越来越多的 APT 攻击将会以影响社会安全为目的，因此应该在高烈度对抗的假定情景下思考智能交通的安全。

安天当前依托智能终端侧威胁检测防御的扎实基础，正在形成服务于车联网“检测+防护+服务+感知”的防护体系。

6 供应链主战场的战争序幕正在拉开

随着网络安全威胁范围的逐渐扩张，供应链安全成为当前热点的安全问题，对供应链安全的关注不仅针对最终的供给，还包括了形成供应链的所有环节。值得注意的是，攻击者可能会利用供应链各节点的安全隐患，从上游攻击、供应链传入、地下供应链等各环节，无孔不入地对其针对的目标进行信息采集、攻击载荷预制等行为。

6.1 新兴设备和场景成为新的攻击入口

从 IT 体系来看，IT 设备、智能手机、智能设备、部分产品组件、软件产品等处于供应链的上游节点，相对于供应链条上的其他节点，是难以验证的具有特定功能的黑盒，这使得攻击者在攻击意图的驱使下，可使用户在不知情的情况下遭受攻击。部分厂商可在不同的软、硬件产品中加入信息采集模块，预置后门，或在研发阶段预留调试接口，给攻击者留下可利用的途径，一旦成功入侵，重要信息泄露等安全事

件将随之而来，而这些产品可以直接影响到实体社会空间，那么造成的损失也不可估量。除此之外，硬件产品的缺省口令和硬编码也使得各种硬件产品存在安全隐患。

智能设备的快速发展与应用在改变人们学习、工作、娱乐等生活方式的同时，也存在大量的安全隐患，除了智能设备本身的安全问题与事件外，这些新兴设备和场景均可能成为新的攻击入口。与传统安全防护体系不同之处在于，除新兴设备和场景的自身安全系统不健全外，安全防护与预警体系也并未完全覆盖这些新兴设备和场景，这就给攻击者带来了新的攻击入口，例如，进入监管不到位的接入了新兴设备的内部网络甚至隔离网络。

6.2 代码签名体系已经被穿透

代码签名体系一直作为保证软件供应链体系不可篡改性和不可抵赖性的核心机制，部分主流杀毒软件在早期也多数选择了默认信任有证书程序的策略。证书窃取问题在“震网”等 APT 事件中开始被广泛关注，在 2015 年 Duqu 2.0 攻击卡巴斯基事件[21]中，恶意代码则盗用了富士康公司的证书。

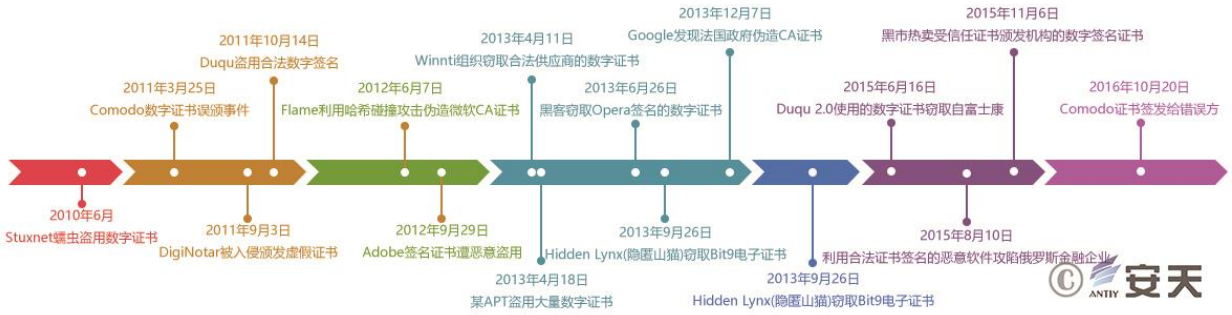


图 12 近年来与数字签名和证书有关的安全事件的曝光时间

但带有“合法”签名的恶意代码，早已不再是 APT 攻击的专利，过去几年中恶意样本带有“合法”数字签名的比率不断上升，从样本累计总量上看，已经有接近五分之一的 Windows PE 恶意代码带有数字签名域，这其中又有 20%可以通过在线验证，考虑到庞大的样本基数，这已经是非常惊人的数字了。证书盗用只占这些样本中的一小部分，而其中很大比例的签发证书并不来自盗用，而来自正常流程的申请。

相对更为失控的是，Android 系统始终坚持自签发证书，而未建立统一的证书认证管理机制。在安天移动安全团队（AVL TEAM）的监测中，已经发现了多起使用知名厂商证书签名的恶意代码事件，不排除相关厂商的 App 签名证书已经失窃。而在开发者中，亦出现过将私钥证书同步到 GitHub 的事件。

在人们的印象中，证书的安全性更多在算法层面，例如，被讨论更多的是散列算法的安全性对证书的影响，但正如我们反复指出的那样“如果没有端点的系统安全作为保障，那么加密和认证都会成为伪安全。”证书的密码协议设计固然重要，但其并不足以保证证书体系的安全。遗憾的是，以 Windows PE 格式为代表的现有代码证书体系，是在端点窃密安全威胁还没有成为主流威胁的情况下建立的，相对于在证书

格式和算法协议上的雕琢，证书签发环境的安全、证书统一管理和废止机制、证书机构自身的系统安全都没有得到足够的重视。

而迄今为止，Linux 系统未能建立起普适的签名认证体系，包括 Windows 平台下的一些著名开源软件，也依然在二进制版本的发布中没有引入数字签名机制，毫无疑问，这为 Linux 下的安全防御带来了进一步的困难。

签名体系本身是不足以独立在一个开放的场景中保证供应链安全的，但不管如何，代码签名体系依然是供应链安全体系的重要基石，其更重要的意义是实现发布者验证和追溯机制。没有代码签名体系的世界，注定是更坏的世界。

6.3 地下供应链和工具链、第三方来源市场削弱了机构客户的防御能力

随着品牌预装、集中采购等因素，操作系统和办公软件的正版化获得了一定的改进，但盗版操作系统的低安全性配置，包括预装木马和流氓软件的问题，依然危害着机构客户的安全。同时机构客户使用的部分应用工具依然依赖于互联网下载，而传统下载站、汉化站、驱动站等，普遍采用下载欺骗等方式，让用户难以发现真正的下载入口，下载的是所谓的“下载推荐器”等广告工具，同时下载站对原有软件驱动往往进行了捆绑而重新签名，在其中夹带广告工具、下载器或其他的木马。这些下载工具和所夹带的广告程序，普遍具有信息采集和二次下载功能，带来了不受控的软件安全入口。其既可能导致机构客户的安全失窃，同时这些通道也可能被高级攻击者劫持和利用。

6.4 设备和应用互联网化构成了机构网络非受控的信息通道

互联网商业模式是基于用户信息和行为的，包括部分隐私采集聚合、基于大数据分析带来价值和便利性、用户通过放弃部分系统控制权和个人信息来置换便利的免费服务。在个人用户已经将这种信息采集视为无可奈何的常态时，也为机构用户的安全带来问题，例如，与云盘等功能连接的文档编辑和笔记工具可能导致文档编辑内容的泄露，输入法的云特性导致敏感输入内容的泄露等等。

同时设备和应用的互联网化，扩大了企业的防护范围，增加了企业的防护成本，提升了内部安全防护的难度。与传统的边界防护相比，新兴设备的接入使得原有的防护边界有所扩散，并形成了一个非受控的信息通道。在新兴设备和应用场景成为新的攻击入口的同时，这些设备和应用的互联网化构成了一个带外信息流，这带来了更多内部目标被定位和画像的可能性，这些被定位的目标和画像使攻击者的目标更加确定和精准。这种设备和应用的互联网化极大地提升了内部安全防护的难度。供应链的整个链条任意环节的安全问题一旦被触发都可能造成严重影响。从国家之间的攻防角度来看供应链安全所造成的影响，从以“震网”、“方程式”和“乌克兰停电”等为代表的安全事件中已可见一斑，而供应链的整体复杂性使得其

整体脉络难于清晰可见。当前世界各国均担心超级大国将其在供应链中所处的上游优势转化为独有的服务于其情报机构的作业能力，甚至形成上游对下游的制约。供应链上游和下游之间的差距，不仅形成了上游商业公司的技术和利润优势，也驱动了信息和资源的汇聚。对供应链攻击的防御，需要建立清晰的架构和标准体系，以推动各环节增加有效安全考量；对供应商加强安全生产和开发要求，推动供应链透明化。供应链透明化的核心在于通过对供应链环节进行有效标注，厘清技术来源，定位和说明关联风险，掌握开源利用和第三方模块的风险流动；最后加强与安全厂商的合作，提高整体系统的安全性和对威胁的态势感知能力。供应链安全防御的部署不仅位于当前环节，同时要延展至前期与后续环节，使安全能力覆盖至最大化。

在过去的种种案例总结中，供应链攻击更多被作为一种“曲线”进入核心 IT 场景的外围攻击手段，这是频繁发生的事件，但如果这是我们理解这一问题的唯一方式，就是把战略问题战术化了。我们有理由确信：**未来的网络安全的对抗，是围绕“供应链”和“大数据”展开的，供应链从来就不只是网络对抗中的外围阵地，而是更为核心和致命的主战场。**

7 理念决定行动（结束语）

7.1 寻找网络安全的系统化方法

习近平总书记在 4.19 讲话中指出“**树立正确的网络安全观，理念决定行动**”，并深刻诠释了网络安全的基本认知规律，在正确网络安全观建立之后，寻找有效的方法，并进行实践就是非常重要的工作。网络安全的进步是两方面的，即一方面是在与威胁的对抗和研判中，不断提升自身能力，另一方面是不断实现对错误的观念与方法的扬弃，从而达成持续进步。

如何尊重网络安全的**整体**性、**动态**性、**开放**性、**相对**性、**共同**性，而避免割裂、静态、封闭、绝对、孤立的错误安全方法呢？如何落实“**全天候全方位感知网络安全态势**”、“**有效防护**”的要求，如何实践“**动态、综合的防护理念**”？如何达成“**安全和发展要同步推进**”？安天人也在不断地思考、总结和实践。

安天围绕“塔防”的思路持续推进安全事件，塔防的核心思想是，利用防御方拥有环境部署的先发优势，形成防御阵地，在边界、流量、端点部署可以协同联动的防御感知环节，并扩展客户的深度分析能力。安天以厂商、客户和对抗三个视角推动系统有效防护的达成，最终达到削弱、迟滞和呈现对手的目的。

我们同时也在积极寻找业内的研究成果，寻找与正确网络安全观相匹配的安全方法。安天技术公益翻译组在 2016 年参译了《网络安全滑动标尺模型》，并在冬训营等环节向业界做了积极分享。相关文献成果将网络安全划分成架构安全、被动防御、积极防御、威胁情报和进攻五个层次，除了进攻不适用于一般机构外，其他四个层次是一个有机的整体，网络安全规划以基础的安全架构和可靠的被动防御手段为基础，叠加有效的积极防御和威胁情报手段。如果没有架构安全和被动防御的基础支撑，那么上层能力难以有效发挥；如果没有积极防御和威胁情报的有效引入，仅靠基础措施也无法有效地对抗深度威胁。每个安全层次解决不同的问题，有不同的价值。相对更低的层次付出的成本更低，但解决的问题更基础广泛。从网络安全投入上看，越是在网络初期越要打好底层的工作，而越是保障高等级的资产，就越需要在积极防御和威胁层面做出投入延展。因此正如本文的联合译者 JOE 所指出的**网络安全的创新更多不是迭代式创新，而是增量叠加式创新**。在积极防御和威胁情报的技术与体系不断发展创新的过程中，架构安全和被动防御环节本身也在持续发展进步。这些思路，为安天如何改善积极防御和威胁情报产品的有效性打开了思路，也对如何认识网络安全当前各种技术、产品间的管理和价值，提出了一个体系化的视野。

7.2 我们的年度工作

一年多前，安天举办了营语为“朔雪飞扬”的第三届网络安全冬训营，在开营仪式上发布了 2015 年度的基础威胁年报的预发布稿。在那时我们已经关注到供应链遭遇攻击导致的防御正面不收敛，商业军火导致的高级攻击门槛下降，黑产大数据导致的威胁情报反用，以及线上线下结合的复合攻击方式将成为新威胁的发展趋势。潘多拉盒子一经打开，魔鬼就不可能在短时间内被关回去。

而特别让我们深入思考的是，高级攻击者普遍搭建模拟沙盘，对防御方各种安全产品进行模拟测试。如何让安全产品在客户侧形成攻击者难以预测的能力？在经过了不断的尝试、思考和对抗演练后，安天确定了以“下一代威胁检测引擎、深度客户赋能、交互式可视化分析”为导向建立安天产品基因。

2016 年，安天先后发布了全新版本的终端防护产品“智甲”、流量监测产品“探海”、深度分析产品“追影”，威胁情报产品“AVL Insight”等，对产品线进行了完善改造。安天也成功树立了在军队、公安、海关、电力、金融、运营商等高安全等级客户的标杆案例，并承担了多个态势感知与监控预警平台的总体研发工作。

2012 年，在安天早期的态势感知系统的开发中，通过引入威胁的可视化展示，提升了系统表现力，并提出了“让安全可见”的口号。在随后的安全实践中，我们致力于将安全的可视化从一种纯粹的展示技术转化为一种操作工具模式，以实现在不同时点的资产和威胁的关联分析。我们明确了态势感知首先是一种建立在可靠的基础感知检测能力、深度分析能力、顶层研判能力和操作化流程上的安全业务系统。同时我

们也经常面对的问题是，态势感知与传统的 SIEM 与 SOC 的差异是什么？SIEM 和 SOC 是一种有效的安全实践，其将更多离散的安全环节聚合为一个整体。但我们需要看到，SIEM 和 SOC 是在安全产品本身在各自为战的时代出现的，其更强调的是对既有安全能力的整合、对日志的汇集，对于如何以一个系统的安全方法为指导、以顶层安全业务价值来牵引和规划更合理的客户端和流量侧的能力，缺乏自上而下的要求。安天拥有完整的端点、网络侧和分析能力积累，检测分析能力跨越传统 PC、移动与新兴场景，这为我们从上层态势感知的业务需求反过来设计更细粒度的感知能力提供了便利。

在流量侧，我们在 2013 年的 XDEF 上指出[22]，传统的网络实时检测更多是在和蠕虫、DDoS 等威胁的对抗中，基于载荷和行为反复重现而设计的，而对于 APT 攻击中载荷高度定向而一次性的投放，则考虑不足，流量监测必须形成对载荷的有效捕获还原和联动分析的能力。而在 2016 年，我们在流量检测设备追影上，为实现基于深度定制化规则的向前追溯和向后条件守候做了更多的工作。让设备可以在高速实时化检测和全要素采集检测两个模式间切换，通过把记录从五元组扩展到十三元组，实现更有效的追溯能力，同时借助安天下一代威胁检测引擎的向量解析能力，我们把网络监测的规则扩展能力，从简单的信标扩展，升级到向量级规则的扩展。

在端点安全方面，我们在新版本智甲产品上，通过对重点主机场景的全要素采集，实现对主机运行要素和环境上下文的深度检测，我们面对纯白名单模式的矫枉过正，采用黑白双控的信誉模式，不同群组和目标可以根据自身等级选择以黑为主或以白为主的安全策略。同时根据普遍存在的“有白无防”的现象，继续深化主机主动防御的防护点和深度采集能力，基于相关研发进展，我们也将恢复反 Rootkit 工具 ATool 的更新，并发布商用取证版本。

当沙箱被当成一种“检测引擎”看待的时候，作为沙箱技术的长期探索实践者，我们认为这种思路是偏颇的。沙箱提供的检测结果是发散的，这种拆解发散后的动态向量的价值比起判断结论更为重要。安天坚持以有效触发格式文档和浏览器漏洞、细粒度揭示恶意行为细节和产生威胁情报作为安天追影分析产品的主要导向，并坚持将前置部署的沙箱转化成为用户侧私有化的安全能力。

安天在 2016 年对自身提出的下一代威胁检测引擎的理念进行了实践，使反病毒引擎从一个决策器，变成一个带有决策功能的分析器。传统反病毒引擎的基本工作原理是跳过无毒格式，对风险格式进行预处理，并输出判别结果和威胁名称。而安天下一代威胁检测引擎在上述功能的基础上，增加了全格式对象识别和深度解析的机制，从而使上层的人工分析、自动编排和人工智能，有了更细粒度的决策空间。

同时作为重要的供应链安全厂商，安天正从解决恶意代码问题的安全厂商角色，转变到能承担起更多责任的安全厂商。安天 AVL Inside 为手机厂商不仅提供了反恶意代码能力，更将 Wi-Fi 安全、支付安全、

URL 安全等融合起来。通过进入系统底层，解决安全应用和恶意程序的平权问题。供应链的全面扩展，延展了安天的威胁感知能力，形成了安天为金融等高安全需求的行业客户，提供安全风险和威胁情报的定向分析输出能力。

正是基于可靠的基础检测分析能力和供应链感知能力，安天持续提升了态势感知平台的感知粒度和业务想象力。而在形成基础大数据分析能力上，避免事件淹没，通过业务流程，实现整体研判和决策，并以资产、信誉视角展开可视化工作，使之回归资产价值保障的本质。

7.3 做具有体系化视野的能力型安全厂商

2016 年，安天、360 企业安全等厂商，在分析报告、会议报告等场合，多次使用了“能力型安全厂商”一词。我们对能力型安全厂商理解如下：

“具有坚定的解决用户安全问题的信仰，具有直面安全威胁的信念和勇气，恪守安全厂商应具备的道德与价值观。

致力于自主研发和技术创新，拥有具备独特技术价值的核心技术，在安全威胁的感知、检测、防御、分析等方面，在感知体系、大数据积累以及其他安全关键技术方面，有自己的特色和特长。”

相关能力型安全厂商，在这一年开始倡导能力型安全厂商的成果互认，尽管这种约定显得十分简单，但却是协作的第一步：

“在分析报告、技术 BLOG、早新闻等环节，积极互认和肯定对方成果，具名说明对方工作和贡献，对对方技术成果给出原厂链接。

对于重大事件、重大漏洞、关键系统等的分析工作，如果有一方已经做了较多的工作及较为深入的分析，本着积极互动，少做重复和无用功的原则，基于已经取得的合作方成果进行叠加深入分析。”

我们依然是开放的，我们依然在继续分享我们的最新分析报告和技术文章汇编，我们依然坚持每周分享一篇技术公益翻译，包括我们在这一年参译了大部头作品《Reverse Engineering for Beginners》。尽管和安天今天的体量和规模相比，这些都已经是一些支线的工作，但工程师文化传统则会持续传承。我们不仅期待有更多的有缘人加入安天的行列，我们也同样期待，中国有更多的能力型安全厂商一同并肩与威胁战斗。

基于自主创新的威胁检测防御核心技术产品服务，推动积极防御、威胁情报、架构安全和被动防御的有效融合，致力于提供攻击者在难以绕过的攻击环节上叠加攻击者难以预测的安全能力，达成有效防护、高度自动化和可操作化的安全业务价值，这将是未来安天所选择的道路。

做一个能力型厂商很难，而一个能力型厂商希望达成真正的客户价值则更难。“夫夷以近，则游者众；险以远，则至者少”。我们对网络安全事业的理解决定了我们要永远选择爬最陡的坡，走最荆棘的路。过去如此，未来也是如此。

附录一：参考资料

[1] 安天：《乌克兰电力系统遭受攻击事件综合分析报告》

http://www.antiy.com/response/A_Comprehensive_Analysis_Report_on_Ukraine_Power_Grid_Outage/A_Comprehensive_Analysis_Report_on_Ukraine_Power_Grid_Outage.html

[2] SANS ICS：关于乌克兰停电事件系列报告

https://ics.sans.org/blog/2015/12/30/current-reporting-on-the-cyber-attack-in-ukraine-resulting-in-power-outage

https://ics.sans.org/blog/2016/01/01/potentialsampleofmalwarefromtheukrainiancyberattackuncovered

https://ics.sans.org/blog/2016/01/09/confirmationofacoordinatedattackontheukrainianpowergrid

https://ics.sans.org/media/EISAC_SANS_Ukraine_DUC_5.pdf

[3] ESET：关于乌克兰停电事件系列报告

https://ics.sans.org/blog/2016/03/22/eisacandsansreportontheukrainiangridattack

https://www.welivesecurity.com/2016/01/03/blackenergysshbeardoordetails2015attacksukrainiannewsmediaelectricindustry/

https://www.welivesecurity.com/2016/01/04/blackenergytrojanstrikesagainattacksukrainianelectricpowerindustry/

https://www.welivesecurity.com/2016/01/11/blackenergyandtheukrainianpoweroutagewhatwereallyknow/

https://www.welivesecurity.com/2016/01/25/securityreviewesetstrends2016attacksukrainevirtualizedsecurity/

[4] 安天：《白象的舞步——来自南亚次大陆的网络攻击》

http://www.antiy.com/response/WhiteElephant/WhiteElephant.html

[5] 安天：《从“方程式”到“方程组——EQUATION 攻击组织高级恶意代码的全平台能力解析》

http://www.antiy.com/response/EQUATIONS/EQUATIONS.html

[6] 安天：《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

[7] 安天：《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

[8] Kaspersky：Equation: The Death Star of Malware Galaxy

http://securelist.com/blog/research/68750/equationthedeathstarofmalwaregalaxy/

[9] Kaspersky：A Fanny Equation: "I am your father, Stuxnet"

http://securelist.com/blog/research/68787/afannyequationiamyourfatherstuxnet/

[10] Kaspersky：Equation Group: from Houston with love
http://securelist.com/blog/research/68877/equationgroupfromhoustonwithlove/

[11] Kaspersky：Equation_group_questions_and_answers
https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf

[12] An Easy Win：Using SIGINT to Learn about New Viruses
https://freesnowden.is/wpcontent/uploads/2015/06/projectcamberdada.pdf

[13] 安天：《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/APTTOCS.html

[14] 360：OceanLotus（海莲花）APT 报告
http://bobao.360.cn/news/detail/1601.html

[15] US CERT: Grizzly Steppe https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

[16] Next wave of ransomware could demand millions
https://venturebeat.com/2016/03/26/next wave of ransomware could demand millions/

[17] 安天：《技术文章汇编（四·三）热点事件分册（“敲诈者”专题）》

[18] 安天：《2015 年网络安全威胁的回顾与展望》
http://www.antiy.com/response/2015_Antiy_Annual_Security_Report.html

[19] 安天：《IoT 僵尸网络严重威胁网络基础设施安全》
http://www.antiy.com/response/Mirai/Mirai.html

[20] 安天：《DDoS 攻击组织肉鸡美眉分析》
http://www.antiy.com/response/Chicken_Mutex_MM.html

[21] Kaspersky：Duqu 2.0 组织盗用富士康证书
https://securelist.com/blog/research/70641/theduqu20persistencemodule/

[22] 安天：走出蠕虫木马地带——传统反网络恶意代码方法的成因与应对 APT 的局限
http://www.antiy.com/resources/Methodology_AVER_Introspection_Trilogy_II.pdf

附录二：关于安天

安天是专注于威胁检测防御技术的领导厂商。安天以提升用户应对网络威胁的核心能力、改善用户对威胁的认知为企业使命，依托自主先进的威胁检测引擎等系列核心技术和专家团队，为用户提供端点防护、流量监测、深度分析、威胁情报和态势感知等相关产品、解决方案与服务。

全球超过一百家以上的著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的反病毒引擎得以为全球近十万台网络设备和网络安全设备、近六亿部手机提供安全防护。安天移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品。

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，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。

安天是中国应急响应体系中重要的企业节点，在红色代码、口令蠕虫、震网、破壳、沙虫、方程式等重大安全事件中，安天提供了先发预警、深度分析或系统的解决方案。

安天实验室更多信息请访问： *http://www.antiy.com*（中文）

http://www.antiy.net（英文）

安天企业安全公司更多信息请访问： *http://www.antiy.cn*

安天移动安全公司（AVL TEAM）更多信息请访问： *http://www.avlsec.com*