寻找 APT 的关键词

■安天实验室 / 肖新光

如果说一切旧制度都能在新的社会体制里借尸还魂，那么在新威胁中也同样能找到旧威胁的影子。新威胁与旧威胁中继承的部分可以让我们快速找到设防点，而新威胁与旧威胁的差异则将是我们定位新威胁的关键。

——题记

查询：APT 的起源和已有的定义

“在 2005 年，首次采用社工邮件投放木马以渗透敏感系统获得信息的事件由 UK Cert 与 US Cert 公诸于世，但并未采用 APT 这一专属名词。而在攻击伊朗核设施的震网蠕虫安全事件引起世人瞩目后，伊朗政府首次将相关威胁定义为 APT。”

以上说法是我们从维基百科词条“Advanced Persistent Threat”中翻译和概括得出的，该词条的表述清晰而精彩，但其中对 APT 来源的描述则令我们怀疑。从时间和逻辑上，这个结论似乎都存在偏差。相比而言，更合乎逻辑的说法来自微软的安全研究者 Peter Cap 在 Bruce Schneier Blog 上的留言，Peter 认为“APT 一词最初起源于 2005–2006 年间在空军工作的网络安全工程师们对于一些安全事件的描述，他们创造了这个词以使公众不对此类安全事件小题大做……”我们亦未找到更多的、权威的支撑性文档，但显然 Peter 的说法更可信。

很多机构和组织都尝试给出了 APT 的定义，如 Dell SecureWorks 的有关文献认为，APT 是“由特定组织（政府）针对某一特定目标实体具备持续且有效的攻击能力及动机的威胁。这个词通常也被视为是网络威胁，尤其是采用基于互联网（物联网）方式的情报收集技术来访问敏感信息的网络威胁。与个体入侵者相比而言，后者缺乏保持高级且长期持续的足够资源。”

Mandiant 公司则认为：能力优越的攻击团队成功地“扩展”了（攻击）目标，包括政府和国防相关的目标、研究人员、制造商、律师事务所、甚至非盈利组织。这些攻击看似由受资助的、有组织的群体实施。我们称他们为“高级持续性威胁”。而 Shawn Carpenter 则提出了 APT 的定性标准，其包括目标、时间、资源、风险容忍度、技能与方法、行动、攻击源点、攻击相关数字和影响八个方面。

溯源：从恶意代码历史寻找 APT 的前身

在现有全部的 APT 事件中，恶意代码在其中充当了关键的角色，而与恶意代码斗争的历史亦是安全技术发展史的重要组成部分。如果我们回头寻觅不同类型恶意代码的关键词，能否为我们寻找 APT 的关键词之旅带来灵感呢？

传统恶意代码可以分成三个基本类型：即具有感染能力的（感染式）病毒；不依赖感染其他文件，但具有跨节点自我复制能力的蠕虫；具有相关威胁的作用或主观故意，但不具备感染和自我主动传播能力的木马。当然这些特性也早在很多恶意代码家族中

被复合到一起。

（感染式）病毒的演进史是病毒作者不断寻找利于感染传播的新宿主，并寻觅更有效、更隐蔽的感染方式的过程。其宿主从引导区和简单的 DOS_COM 可执行文件发展到各种不同格式的文件（带有复杂格式的可执行文件、带有脚本的复合文档……），而感染方式也由最早的头尾直接插入，进化到 EPO 及 Stolen Code。因此病毒的关键词可以总结为代码和宿主的关系，即感染行为。同理，蠕虫的关键词就是传播，其体现了蠕虫文件实体同通道之间的关系，而通道又可以进一步拆解为介质和弱点两方面。而对于 APT 来说，尽管其未必使用感染的方式，也未必采用蠕虫完成初始的散布，但这些方法的思路仍在其攻击逻辑上略见些许端倪。

病毒和蠕虫的发展史，是以很多代表性的家族或变种为里程碑的，新方法的突破、0Day 或 1Day 的漏洞与这些代表性样本关联在一起。但木马的演进则与此有很大的不同。一些技术方法和设想很早被提出，但很长时间之后其才成为现实威胁或呈现出放大趋势，同时我们也很难做出究竟是哪种木马率先使用了某种方法的准确判断。这些变化与木马的趋利性和海量化的特点有关，因此我们对木马很难做出窄带、清晰的单点概括，只能笼统地说“行为 + 方法 = 后果”，这就是木马的关键词，而这似乎与 APT 更接近了一步。但无论如何，总体上看，木马在行为和方法上总体上依然呈现出与当时的系统环境发展关联的特点，即有着“时代特色”。而木马在隐蔽、反制、获取、回传等方面所积累的种种经验和技术点，也为 APT 完成了大量的前置积累。

我们之所以反复提及技术与时间的对位关系，是希望为“高级”与“持续”寻找前身，从传统的概念来看，高级可以被理解为一种技术能力的概括，而持续则显然是一个时间概念。但 APT 的演进史似乎更难于沿着时间线展开梳理，尽管被曝光的 APT 事件屈指可数，相关样本基数也很小，也很容易完成整理统计，但正因为其存在长期持续的特点，反而使其从整体上难以沿着技术线路里程碑化。从对 APT “持续”的分析中，时间是重要的因素，特别是其攻击或潜伏的起始时间，是分析者非常希望形成的结论。但由于我们对 APT 的后知后觉，其被发现和报告往往已经是潜伏许久、甚至只是找到了得手许久后的残骸。这就导致了我们对其起始时间点，只能限于粗糙关联与猜测。

从恶意代码的分析史中，还能带给我们另一方面的启示，由于恶意代码作者群体存在地缘性特点，这将影响到恶意代码的传播与分布，安全团队也积累了一整套关于地理与空间的分析和图示化方法。而 APT 的强烈定向性使这种地缘特点更加鲜明，因此其“空间”因素和“时间”因素一样重要。由于 APT 已经在地缘政治博弈中开始扮演起传统“间谍”与“特种部队”的角色，谁是主导策动者、谁是攻击目标，以及攻击过程中的节点和相关资源分布与位置，也成为重要的分析因素。

但这些反而会让我们更加困惑不解，更长的时间维系、更大的空间跨度、更大的资源调度能力，都导致我们更难接近其本质。

推导：重新审视差异化

之所以对比恶意代码的演进史与 APT 演进的异同，皆因新概念存在之必要，在于其与旧概念的鲜明差异，而差异性即应该是新概念本质，所以要详细审视两者之间的差异化，包括超越单纯的技术视角。

我们换一个角度，回顾一下上世纪 80 年代至今的 IT 技术的演进史，包括操作系统，硬件体系结构、软件环境和网络应用变化等等，如果把这些节点与恶意代码的历史整合起来考虑，我们就可以发现恶意代码从整体上表现出了三个特点：

★尾随：恶意代码的进化与改进是尾随着产业和应用发展技术的，既无孔不入，又存

在一定滞后——其本质是获利时机的选择。

★从众：多数恶意代码分布于当时主流的操作系统，以获得更大的感染量——其本质是获利空间的选择。

★择弱：通常攻击者寻找可批量化的、更脆弱、更容易获益的方法实施安全威胁，即所谓慢羊理论——其本质是获利方法的选择。

★但传统恶意代码的这三个特点均被APT颠覆，APT与产业发展规律没有必然的联系，其目标既可能针对更新锐的系统，又可能针对传统的基础设施，但其目标选择有鲜明而坚定的使命与价值导向，至于目标是否有弱点则并不重要。Bruce在Blog写到“从过去来看我们一定比某些人安全，那些人才是平时受攻击的目标……，而APT不是如此”。

或许有人认为如此赘述全无意义——APT望文生义，其关键词不就是高级与持续性吗？但问题在于高级与持续性本身在网络安全中都不是新名词，而当攻击者的呈现出前所未有的使命要求和价值判断时，传统恶意代码与攻击分析中所形成的“高级”与“持续”的概念也应该被重新解读。

高级通常来看可以被理解为“先进”，但亦有反例存在。下表是安天在Hangover事件（疑似印度针对巴基斯坦和中国实施APT攻击的事件）中最早捕获的6个样本，从中可以看出其缺少整体的规划和一致的策略，后是数百个有着同样风格的、杂乱无章的样本，这看起来是一种依托“人海战术”展开的APT攻击，所以高级并不一定代表技术的高明性。APT在先进性上，并不具有统一的、量化的标准，它可能只是代表了攻击者本身的最高能力或所能找到的最佳方式。

表 安天在Hangover事件中捕获最早的样本列表

样本编号	壳	编译器	主要行为
1	无	VB	释放的VBScript脚本，脚本执行后连接远程服务器zolipas.info（域名失效）
2	无	VS.NET	运行后将以下文件设置为Run自启 C:\WINDOWS\system32\CatRoot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\slidebar.exe，后续无其他行为
3	UPX	Dev-C++	运行后在C:\ApplicationData\Prefetch\目录下生存log.txt文件，不断的记录键盘、窗口标题、浏览器搜索内容、计算机用户名等信息
4	UPX	VC7	运行后链接域名secureplanning.net欲下载其他恶意代码（URL失效）
5	无	VS.NET	运行后在c:\Documents and Settings\Administrator\Local Settings\Application Data\NTUSR\目录下创建文件ntusr1.ini进行键盘记录
6	无	Dev-C++	样本运行后在C:\ApplicationData\目录下释放logFile.txt文件，收集各种相关扩展名文档名称

而“高级”是否可以被理解为更多在技术和方法上的创造和创新呢？APT攻击中持续的对0day漏洞的挖掘利用、对隐蔽通信方式的持续改进，确实是一个不断演进创新的过程，这是其在单点上的“微创新”。从整体上，我们尝试把APT手段和趋势进行脑图梳理，按照图1将其划分成前导、入口、持续性、通信和破坏几个环节，并进一步分支化。如果把这些分支与传统恶意代码的所有方法进行对比，我们可以发现其差异在于在前导环节中对于一些特种渗透设备和方法的使用，以及在后果上对工业系统

的实际破坏。但前者可以看成网络攻防与传统情报手段的合流，而后者并不缺少想象和预言，其能成为一种事实更多来自攻击者的决断和底气。而除此之外绝大多数分支在于既有恶意代码已经在建立方法之内，没有更多新的突破，因此高级更多的表现不在与其单点创新，而是从整体上其是一个对既往的攻击方式集大成者，是一个为了战争制定整体策略，从武器库中选择武器组合的过程。

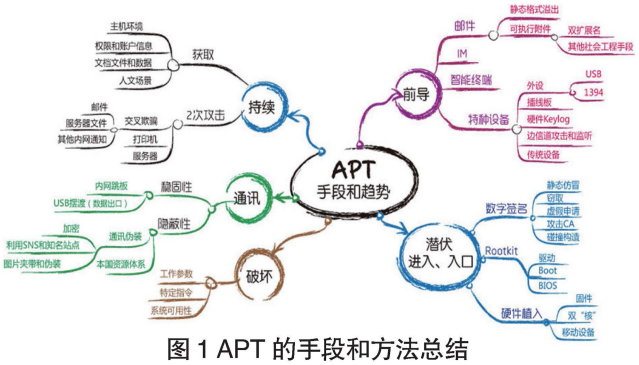


图 1 APT 的手段和方法总结

通过另一个层面也可以印证集大成者的说法，图 2 梳理了在过去一年中所有被声称可以用于 APT 分析的方法，如果细看图 2，我们会惊诧地发现它几乎涉及到了目前为止所有的网络安全技术与方法，显然由于 APT 攻击上绝不是单点的“高级”技术，防护上也注定不是单点产品的问题，而是一个用整个安全体系对抗威胁体系的过程，而这里防御一方既会受益于其在相关领域的积累，

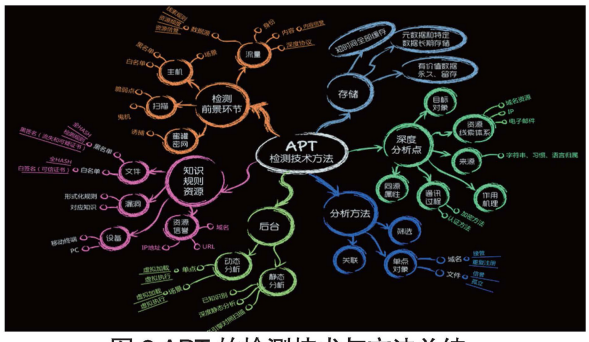


图 2 APT 的检测技术与方法总结

也会受制于旧有思想的窠臼。

APT 也打破了传统恶意代码的持续观，对传统感染式病毒来说，其持续性即样本自身的生命周期。对一种感染式病毒来说，只要有一定的感染数量和规模，我们通常就认为其流行或活跃（wildlist）。而由蠕虫或木马形成的僵尸网络，情况亦有不同，由于僵尸网络存在着“所有者”这样的地下概念，其生存周期从家族或者变种的生存，转为体系规模的生存。对一个僵尸网络威胁进行判定的重要因素，是其受控节点的数量规模，而实际上这个规模是动态的、维持的，并不需要绝对保持对固定某一台或者某一批节点的控制。而在类似用于垃圾邮件发送、DDoS 攻击等的僵尸网络中，其每个受控节点相对整个僵尸网络的体系来说，价值都是微小（而且是等同的）。当然在传统僵尸网络中也出现了“大海捞针式“的对高信息价值目标的寻找，但其绝非类似 Stuxnet 事件中通过在批量的感染中向一个确定的内网目标实现摆渡机会碰撞。

APT 虽然借鉴了僵尸网络的一些控制和数据回传的方法，但高度的定向性决定了在 APT 中所涉及的节点价值是有高度不同的。Fireeye 在的《The Advanced Cyber Attack Landscape》中对于整个 APT 做了一些标志性概括，由于其产品的特点，其更多关注的是从邮件投放到隐蔽回传的过程。但长期的指令下达和数据回传能力的保全就是持续只是 APT 的作业层面。APT 的持续不只是技术过程的维系，而是反映了攻击方明确的战略导向和意图，这是一个以资源和耐心为支撑的一个过程，不会因一时的控制服务器失连，或是在被植入终端上被清除而宣告终结。反而却可能

因其使命演进，而主动完成清理现场或者体系迭代。业内有人士推测 Flame、Duqu、Stuxnet 三个 APT 事件存在关联，构成了一整套的，前置潜伏，环境获取，数据持续回传，最后一击必杀的完整攻击链。如果这种猜测是正确的，那么在这个过程中，每个体系在达成目标之后，其会被新体系取代，此时已经完成使命的样本，即使在主机上依然存活而没有自毁，其“持续性”也已经宣告结束，但整体使命的完整性和持续性则不受影响。每个体系终止之后、使命却在保持，所以 APT 持续的不是传统代码的生命周期也不是僵尸网络体系性规模，而是其任务的使命周期。

任何持续的行为，都必然有持续的动力，行为之于动力是一种因果必然。传统的恶意代码的迭代演进也有其动力规律：最早的（感染式）病毒和蠕虫的动力是编写者通过传播感染获取心理上的满足，感染面积越大自我心理满足就越强；而木马则从原始的心理快感驱动力，转化为利益驱动力，因此其将符合经济规律，经济回报大于投入，这种循环就可以继续下去；经济回报远远大于投入，这种循环就会加速。当 APT 把网络攻防的大剧推入到新的时代时，其持续依然遵守回报与投入的关系，但这种回报不是简单的收益成本关系，而是有一种综合的考量。由于这种收益可能直接或间接影响到国家和利益集团间的战略平衡和安全态势，所以也不再有简单的、类似地下经济运行的“黑金”量纲，而需要从其广阔的动机和背景来看。政治，军事，经济，宗教，知识产权的动机和获益者为这些动机配套的资源，左右着它，使其比既往任何的网络攻击方式都具备了异乎寻常的长时间承担高成本的能力。如果我们套用“威胁是能力和意图的组合”的观点，那么 APT 的动力就是动机（意图）与能力的组合，后者不只代表技术能力，也代表对成本的耐受力 。因此 APT 行为是否会实施和持续下去，只与目标在攻击者眼中的价值和攻击者的意图、坚定性与承担攻击成本的能力有关，与目标本身是否具有传统意义上的弱点无关，后者只会影响到攻击者的方法选择。

题外话：关于话语权

从微观的技术点来看，APT 在技术上与之前恶意代码以及其他攻击技术的发展史一脉相承，并与之前的定向攻击有一定延续性，它只是被单独定义成为新概念而已。

但从更宏观的角度来看，APT 是战略性威胁，从国家间威胁来看，APT 注定服务于发起国的国家现状和国家意图。其国家安全战略越清晰、明确，其国家能力越强大，APT 就越高级，隐蔽和难于防御。而反之则也是如此。因此，笔者也担心掉入泛化的陷阱，即过度扩展 APT 的外延，而将其与整个 Cyberwar 的概念等同起来。过于泛化将让我们陷入一种面对大到无形之巨兽的恐慌，但过于量化又会使我们陷入某个单点技术或者单点产品足以应对的幻想。

从某种意义上说，我们今天纠结于此，是因为无论是 APT 还是 Cyberwar，从语汇提出，到定义和标准的建立，我们都并不拥有导向能力。这种在别人的语境中分析我们自身面对的威胁的尴尬，就是没有话语权的尴尬。在技术领域，话语权包括了定义，转义，形式化，建立标准、形成知识产权壁垒等一系列因素，而在现代大国博弈中，话语权的另一个作用则是可以为技术术语贴上技术以外的标签，这种话语权让全球更多人相信 APT 的唯一目标是西方政府和机构，同时又对西方相关机构在 Flame→Stuxnet 中扮演的角色视而不见。一个技术术语可以被赋予鲜明的倾向和价值观的时候，其背后展现出的是一种综合的可以左右全球走向、以国家能力和战略为基础的综合实力。

所以 APT 注定不会是终极威胁，威胁是无尽的，当拥有话语权的一方发现他们不能完全掌控这个游戏、或者看到更大的游戏机会时，他们会寻觅或制造新名词和新规则。而那时我们将重新焦虑、恐慌。

但无论如何，威胁不会停止，我们不会屈服，或许这才是故事的本质。

（本文根据作者 2013 年 9 月 23 日在互联网安全大会 APT 分论坛的报告录音整理，作者后期做了较多删改。感谢蒋旭宪博士及我的同事 Ying、Billy、Angle、Mappy 对本文的贡献）

（本栏责编：袁胜）