反病毒的现状、挑战与改进（上）*

肖新光
安天实验室
特邀专栏作家

关键词：反病毒方法　网络侧　蜜罐

导言

反病毒产品作为安全防护的必备要素，主要以检测、查杀攻击方的投放物及其衍生物为基本目的，通过技术手段起到提高攻击方成本的作用。反病毒产品与恶意代码的对抗不是单枪匹马的能力对抗，更多的是一种体系性的对抗。防御方（反病毒工作者）长期工作于后端成熟体系和庞大资源的支撑之下。反病毒体系前置产品环节覆盖了主机端与网络侧[1]，也可以称为一类特殊的IT资产；其捕获手段包括主动上报、蜜罐、爬虫、流量还原等十余种；而反病毒体系后端所建设的庞大的分析流水线，可以实现对绝大多数样本的黑白判断、分类命名和规则提取。因此反病毒工作者在前置经验、团队规模、计算能力方面，在很长一段时间都优于单一的攻击方（病毒制造者和使用者）。反病毒厂商会比攻击方编写制造病毒的过程付出更低的资源成本，并以更短的时间代价对所捕获的样本完成分析判定。在这个过程中，对绝大多数样本的分析判定只需要消耗分钟级的计算时间成本，而相对于反病毒厂商后台庞大的计算能力，这种时间成本几乎可以忽略不计。

上述过程从真正成为一个可维护的工程化环节开始到现在，已经持续了20余年，比绝大多数安全技术的历史都要长久；而在其持续发展中，一些被预言家们认为可以永远消亡病毒的“革命性”技术，纷纷凋落，宛如昙花。

安全技术是由安全威胁驱动变革的，而非预言家；而威胁则受攻击者的目的引导，以其**承担成本的能力**为支撑。当这几个因素发生重大变化时，安全威胁也就必然会产生全新的特点。在APT（advanced persistent threat，高级持续性威胁）时代发生了实质性的转变，而攻击方的意图更明确、更具有针对性，更重要的是因为攻击可能是由国家或政治经济集团所发起的，攻击者承担成本的**能力和意志力**相对于传统的地下经济集团或者其他个体攻击者来说，几乎是无限的[2]。

在这样一个新威胁背景下，是我们梳理现状、澄清误解，并做出反思与应变的时候了。

传统反病毒方法的现状与所面临的挑战

反病毒基本模型在主机端的鏖战

主机是恶意代码主要威胁的目标，也是反病毒技术的原点。从主机上捕获样本、后端分析、提取规则或编写对应模块、分发规则升级到主机的对抗循环一直

* 本文系根据作者在Xdef 2013会议的部分报告内容和ISF 2013会议报告内容整合并缩改而成。全文较长，本刊分两期连载。本文的前置知识可以参考作者在《程序员》2013年12月刊发表的“反病毒技术发展四部曲”一文[1]。

[1] 与上端设备或网络连接的接口叫网络侧接口。

在持续进行中，并被视为反病毒基本的工作原理，这种重复无疑易于让许多人产生审美疲劳和创新冲动，并以此鄙夷这种规律性的、持续性的工作。由于主机反病毒技术近 30 年的发展并未消亡病毒（如同警察的存在未消亡小偷，药物的存在未消亡病菌一样），导致悲观者始终认定“道高一尺，魔高一丈”。一些学术论文中，在没有对任何反病毒产品做出深度的测试分析的情况下，就把主机反病毒产品作为一种基于特征码检测已知病毒的技术来表述，从而试图衬托出某些未知检测方法的价值。而事实上，多数文章中所提到的方法，有的早已是商用反病毒流程中的某个环节，有的则因其时间成本或误报率等不能满足实用需求被早早抛弃。

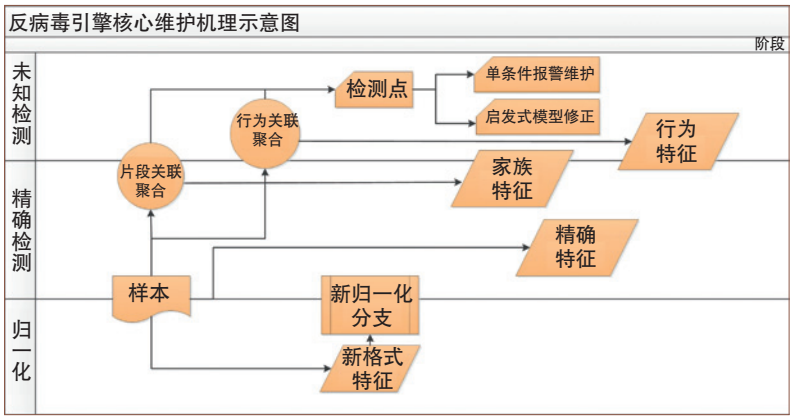

图1　现代反病毒引擎的规则维护层次

在防毒卡被历史抛弃后，反病毒软件成为主机反病毒的主流产品形态。目前，反病毒软件是由以反病毒引擎为核心的检测功能和以主动防御机制为核心的防护机制组成的。图 1 所展示的是一个商用反病毒引擎的基本维护机理。可以看出，该反病毒引擎既有对抗全新病毒家族的启发式检测机制，也有针对新变种的病毒家族特征维护机制，其绝不是一个只依赖特征匹配的简单匹配器。

反病毒引擎不能检测出所有新病毒的原因，仅仅在于早已被弗雷德·科恩 (Fred Cohen) 所证明的，没有任何机制可以检测一切病毒 [3]（除非对所有对象都报警）。而更有趣的是，认为通过签名体系就可以搭建一个绝对安全的世界的人们，至今不仅不能让所有应用开发厂商接受签名机制，而且目睹了在 APT 攻击中大量采用被盗用的签名证书 [4]、电子商务认证授权机构 (Certificate Authority, CA) 遭遇入侵 [5] 以及荷兰电子商务认证授权机构的倒闭 [6]。

传统反病毒软件的软肋并不在于其检测能力问题，而是主机上普遍部署的反病毒产品是一种易于获得的安全资源，从而可以让攻击者低成本地搭建环境进行对抗测试，直到确认反病毒软件无法检测后，再进行投放。这个问题对于任何一种需要广泛使用的安全技术来说，几乎是无解的。既能广泛地起到防护的作用，又能不让攻击者获得安全技术是不现实的。而到了 APT 时代，这个问题已经不是反病毒的软肋，攻击方可以完全承担获取各种安全产品进行对抗测试的成本。寄托于让某种安全产品只服务于某一个领域、足够专用，从而不被攻击方获取的愿景，完全不足以博弈 APT 背后的政治经济集团的情报能力和财力。

反病毒软件面临的另一个问题是，作为主要服务于桌面系统的安全环节，其必须准许用户按照自己的意愿执行程序。这给反病毒软件留下了非常窄的作业空间。而目前来看，除了让主动防御的策略更苛刻一些，似乎没有其他更好的办法。当然这会给用户带来一定的不便。

失守的网络侧

2000 年开始的蠕虫病毒爆发，对传统的以安全边界思想为主的网关产品和以行为检测为主的旁路产品构成了重大挑战，也驱动了反病毒技术与网络侧技术的融合。

蠕虫病毒和同时代的相关网络威胁首先给网络设备或端点流量和连接数带来了压力，也包括邮件蠕虫病毒的大量发送甚至给邮件服务器带来了巨大的存储压

力。而相关威胁的连接关系，也呈现出一些鲜明的拓扑特点和行为因果关系，如通过蠕虫感染去建立一个僵尸网络 (botnet)，而后再利用僵尸网络去进行分布式拒绝服务攻击 (distributed denial of service, DDoS)。这些行为会呈现出一种多点关系，如蠕虫传播是从单点到多点的扩散过程，僵尸网络则实现了一点对多点的集中控制过程，分布式拒绝服务攻击实现了多点对一点的攻击过程。

我们对蠕虫时代威胁的特点做了概括，这些特性决定了所采取的安全方法。

扩散 基本特性是病毒体会从一个节点传播到多个节点，而其到达的节点又成为新的源头。扩散是蠕虫威胁的手段。

重复 在扩散过程中，其扫描、攻击载荷和病毒体是不断被重放的。重放是其传播特点。

分布 在扩散完成后，蠕虫节点会呈现分布特性，这是蠕虫传播的结果。其分布的数量，也体现出进行后续关联威胁的能力。

这种概括不仅对蠕虫有效，对分布式拒绝服务攻击、僵尸网络控制等也同样有效，发现其扩散过程、检测其重复载荷（也包括控制指令）、处置其分布节点，成为蠕虫时代安全分析和响应的主要工作。蠕虫时代的威胁尽管给网络和处置带来了很大压力，但却是易于被感知、容易被捕获的威胁，对抗手段也容易想象和设计。

从检测方法来看，蠕虫样本因其自我传播可以很快被安全厂商捕获到，对于那些采用了传统反病毒引擎与网络流量还原设备进行叠加的设备来说，不难通过反病毒引擎的升级实现检测，同时可以增加一些基于流量统计、拓扑分析、网络行为检测的手段作为预警辅助条件。

从评价标准上看，由于蠕虫导致的网络压力可对全局造成影响，这一时代有很多网络侧产品的思想不是偏重于定位具体感染目标，分析其受到的威胁，而是**偏重统计和发展趋势**。

从处置体系上看，由于评价标准更看重对网络运行效率的影响评价，因此其处置着眼点偏重于通过感染源定位来指导对源头的遏制、封堵和拦截，而没有更多关注恶意代码对目标节点和系统的威胁。

应该说这些方法对付当时的安全威胁是有效的，但从目前的网络侧产品来看，其恶意代码检测能力比想象要糟。目前网络侧设备核心反病毒有三种方式：

1. **采用流还原与传统反病毒引擎相结合的方式**。这是一种看起来更简单的方式，但实际上并非如此。一些 x86 的设备更倾向于采用类似方案，由于很多老牌的引擎无法移植到非 x86 环境下，因此类似基于 Cavium（凯为半导体）等架构的设备中可能没有全面的反病毒能力。

2. **采用反病毒厂商提供的轻量级规则与安全设备能力相组合的方式**。Safestream[7]、TrustStream 等方法实际上都是通过反病毒厂商提供统一资源定位符 (URL) 和哈希 (Hash) 规则的方式，而这种方式病毒检测能力非常有限。

3. **采用网络侧厂商自定义规则的方式**。一些厂商的恶意代码检测能力受到了硬件架构的限制，比如有的单板只支持十万条规则。这对于恶意代码的全量规则空间显然是远远不够的，反病毒厂商也不乐于提供这种可匹配的规则。这时网络侧厂商则尝试对恶意代码样本建立一些轻量级的规则检测方式。

此外，网络侧设备的入侵预防系统 (intrusion prevention system, IPS) 层次，例如 C&C(command and control) IP 地址规则、Agent 域规则等检测方式，辅助以持续的规则维护，也是一种有效的恶意代码对抗能力。

APT 攻击对网络侧设备的主要挑战，还在于 0day 攻击[2]（如溢出附件）和事件的小众性。对于前者的讨论已经很多，而对后者，我们举例来看。Hangover 事件是一组**疑似印度针对巴基斯坦和中国进行 APT 攻击的事件**[8]，挪威安全公司诺曼 (Norman) 于 2013 年 5 月对此进行公开报道。从 2012 年 3 月起，我

[2] 0day通常是指还没有补丁的漏洞，而0day攻击则是指利用这种漏洞进行的攻击。

们已经陆续捕获了该事件的一些相关样本（如图2所示）。而这些样本对应的网络事件非常稀少，呈现出高度定向的特点。由于APT手段从原有的扩散传播

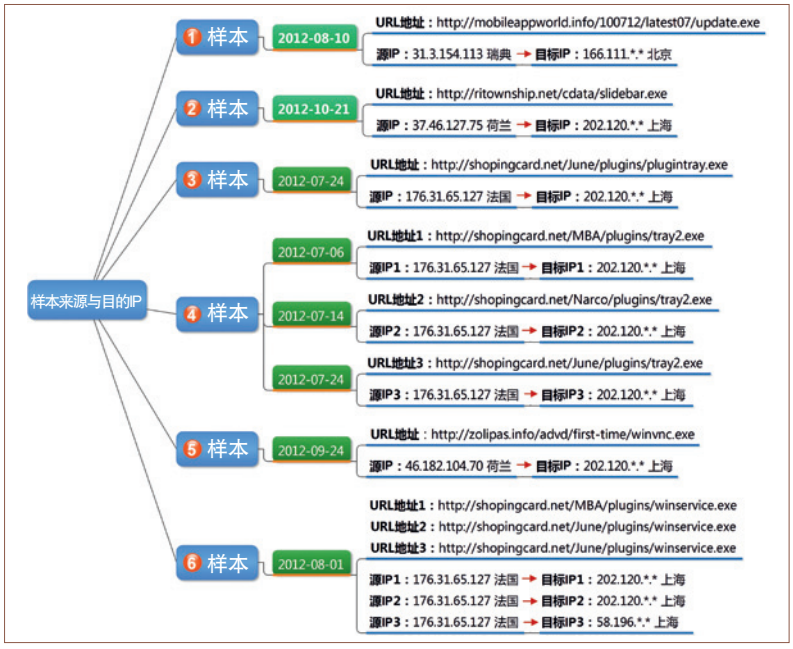

图2　安天实验室捕获Hangover事件前6个样本对应的网络事件

转化为单点投放，其获取利益不依赖感染大量结果，而源自单点目标，因此可能不会形成大面积的感染分布。而这些少量的事件也被淹没在海量的安全威胁和风险中，难以引起关注。

总体上来看，在过去的十年，多数网络侧设备逐渐陷入了追求吞吐量、检测速度的轨道，其在基本反病毒能力上尚有缺损，更谈不上为应对APT这种新威胁做好准备。

蜜罐——原始人的陷阱

蜜罐早期并不是反病毒体系的一员，而更多的是服务于入侵检测和取证领域，主要用于针对攻击者进行吸引和诱捕。蜜罐随着蠕虫的广泛传播，成为反病毒团队必备的捕获手段。用于病毒捕获的蜜罐，弱化了蜜罐乃至蜜网更细腻的目标仿真诉求，而可以追求更大量的分布式部署，以能更快地感知威胁、获得样本。

为了捕获恶意代码，不同的蜜罐模仿了下列不同的情景：

1. 系统或者系统上加载的应用有可被利用的缺陷；

2. 人的活动，如访问网页、下载安装软件、执行邮件附件等等。

这使蜜罐项目呈现出不同的发展倾向，有的偏重于可探测端口漏洞模拟，用于捕获扫描溢出的蠕虫。同时类似机遇网页爬虫+虚拟执行的Honey Monkey，以及类似诱饵信箱系统等等，也可以看成异构的蜜罐。

蜜罐的有效性是有前提的。首先，蜜罐所模拟的资源与真实的资源相比，对于恶意代码的传播注入过程来说是**等效**的；其次，蜜罐所模拟的弱点是暴露的、或者可以被攻击者感知的，因为泛化的威胁优先寻找最脆弱的系统（慢羊理论）。蜜罐产生效果的根本原因是**其部署与安全威胁的扩散过程发生碰撞**。但无论怎样广泛部署，蜜罐和真实IT资源相比都是少量节点，因此对于蠕虫类威胁来说，蜜罐的效果还是取决于威胁本身的**扩散**能力。

当云安全方法开始普遍成为安全厂商标准能力时，蜜罐的能力就被弱化了，由于所有新的可执行对象均会被提交鉴定，拥有大量客户端的安全产品采集能力注定要比任何蜜罐部署都强得多。而传统样本捕获蜜罐更不适合与APT攻击对抗，因为是否被APT威胁只取决于系统所承载的价值，而与它是否有明显的弱点或它本身防御能力的强弱无关。

因此，在蠕虫时代兴起的众多安全手段中，蜜罐是最有争议性和临时性的产品。从捕获价值上来看，其注定远不能与海量的产品客户端部署相比，也不及基于流量的还原具有无条件性和不可感知性；而从发现价值来看，其可能在应对大规模扫描探测方面还有一定价值，但传统的蜜罐对APT攻击的价值微乎其微。但如果蜜罐回到其本源概念——

即一种具有诱惑力的假目标，蜜罐也并不是在APT时代没有用武之地。蜜罐在与APT的对抗中，应该回到引诱与分析的原有细粒度轨迹上去，它的新用武之地应该是高价值目标的仿真与模拟。

分析流水线——笨拙的蒸汽机

不论是传统的赛门铁克(Symantec)、卡巴斯基(Kaspersky)，还是新兴的帕洛阿尔托网络公司(Palo Alto Networks)或火眼(Fireeye)，几乎所有的与恶意代码打交道的厂商都有一套庞大的基于云的后台分析系统。笔者习惯性地称类似系统为分析流水线。

多数分析流水线都是围绕以文件样本为主要分析对象展开的。文件样本经历静态分析、对照扫描、动态分析等环节后，完成大量的向量提取，并基于这些向量完成相关的判定，最后再进行对应的规则和知识分发。传统流水线的各个环节是否有效都有一定的前提基础。静态分析的有效性是建立在代码的功能和意图可以通过载荷进行判断的基础上；对照扫描的可靠性则建立在安全厂商之间对判定结果的交叉信任的基础上；而动态分析的有效性则建立在动态环境中的行为可以重现在用户场景中的行为的前提下。

分析流水线在过去面临的两大挑战是：

海量数量 流水线最大的压力不是完成恶意代码的行为分析或者特征提取，而是对海量的未知文件完成黑白判定。

长尾价值 早期大量Hash不同的样本文件，往往是同一个感染式病毒感染的结果。在完成感染式病毒的分析、规则提取和清除参数或脚本的编写后，后续同类样本就没有价值了。而木马时代则有很大不同，尽管同一个变种的大量Hash可能是批量制作免杀的结果，但也有连接不同C&C地址的可能性，因此需要投入更高比例的样本完成完整的分析过程。

针对上述挑战，传统人工分析的细粒度方法和关联想象，在海量样本分析流水线中是难以实现的。多数流水线是依托单样本分析任务管理的思想来设计的，这种流水线用以解决APT样本的一些特点是困难的：

第一、复杂主机场景。图3是我们在2007年参与分析的一例入侵事件。多个样本构成了一个复杂主机场景，这个场景中的多个工具，都不是传统意义上的恶意代码，而是开源或者商用工具，甚至部分在反病毒厂商的白名单之列。单样本分析对于类似场景的分析虽然有一定辅助价值，但不能起到关键作用。

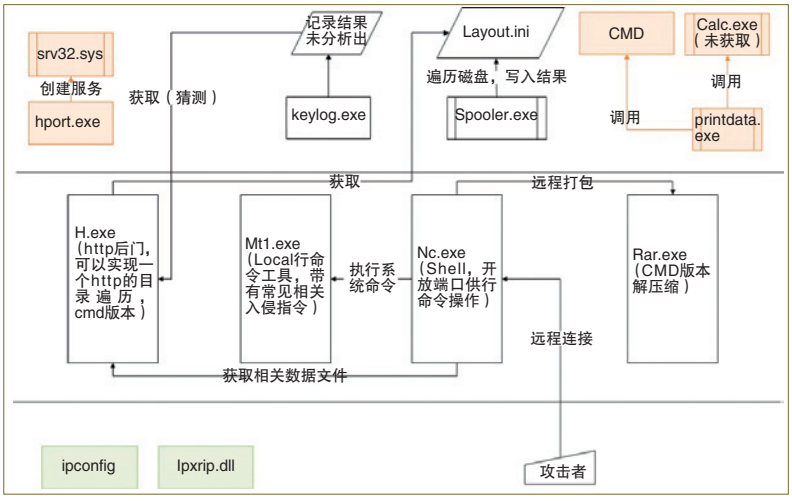

图3 安天实验室2007年分析的某入侵事件主机场景

第二、行为不可复现。由于多数APT事件是事后发现，往往存在C&C已经失效、功能无法触发和样本无法完整获取等情况。

第三、场景外延。由于APT涉及更多环节，包括工业或者其他的非传统网络设备与系统，这超出了传统流水线的能力。比如震网可能对WinCC和PLC[3]进行攻击，就超出了传统厂商基于大量的x86设备加虚拟机的分析环境。

[3] WinCC是西门子公司为工业控制开发的组态软件，PLC是工业控制中较常用的自动化设备。

目前的分析流水线面对APT事件的复杂性必然具有一定的分析障碍，反病毒团队还需要更大的投入来改善自身的能力纵深，在流水线之外搭建一些小的分析场景。传统分析流水线的另一个问题是，将APT样本判定为黑或者可疑并不困难，但如何将其从海量的黑名单中筛选出来，对人工分析做出“制导”却是一个严峻的课题。

本章小结

尽管面临很多问题，反病毒体系依然是信息安全史上最庞大、精密的安全“机器”，对抗了难以计数的威胁，这台“机器”却一直持续运转并持续改良、渐进推演。尽管对出现颠覆式的革命性技术的期待从没停止过，但这种期待多半是简单的类比和缺少实验基础的想象。如认定计算机体系架构改变就能消亡病毒的设计想象多年来不绝于耳，暂且不论其具体设计的合理性，信息技术本该首先服务于人类的便利性与发展，而不是追求自身的绝对安全。就如宵禁虽然可以消亡街头抢劫，但显然我们需要的是自由出行的世界。而那些认为生物免疫技术可以彻底改变反病毒被动局面的人们忘记了，生物界的细菌病毒只是缓慢地自然演进，而计算机病毒则是来自对抗式的制造。人类的医药多数情况下对抗的是疾病，而不是持续的生化战争。而对反病毒工作者和他们背后的机器来说，每天都在进行着战争。

对安全的道路与方法的选择来说，只有事实能打破虚妄，只有威胁能变革现状。■

肖新光

网名江海客。CCF高级会员。安天实验室首席技术架构师。主要研究方向为反病毒引擎、大规模恶意事件样本的流水线处理等。seak@antiy.com

参考文献

[1] 反病毒技术发展四部曲. 程序员, 2013(12):68~71.

[2] 寻找APT的关键词.中国信息安全, 2013(10):100~104.

[3] An undetectable computer virus, https://www.hackerzvoice.net/madchat/vxdevl/avtech/An%20Undetectable%20Computer%20Virus.pdf.

[4] 对Stuxnet蠕虫攻击工业控制系统事件的综合报告（安天实验室）. http://cert.antiy.net/security-research/20101012-043322/.

[5] Hack obtains 9 bogus certificates for prominent Websites：trace to Iran. http://www.wired.com/threatlevel/2011/03/comodo-compromise/.

[6] Broken CA DigiNotar files for bankruptcy. http://www.pcpro.co.uk/news/security/370048/broken-ca-diginotar-files-for-bankruptcy.

[7] Kaspersky® SafeStream ll. http://www.kaspersky.com/safestream.

[8] Unveiling an Indian cyberattack infrastructure a special report. http://normanshark.com/wp-content/uploads/2013/08/NS-Unveiling-an-Indian-Cyberattack-Infrastructure_FINAL_Web.pdf.

CCF公共政策委员会工作启动

2014年3月15日，新成立的CCF公共政策委员会工作会议在北京召开。CCF秘书长杜子德、公共政策委员会主任赵沁平和常务委员尹宝林、方兴东、周兴社、单志广、高江海（代王震）、纪震、胡钢、陈谊出席了会议。会议明确了公共政策工委的定位与工作方向，讨论了2014年工作计划。

根据CCF公共政策委员会的职责要求，该委员会将在教育、人才评价、科技项目（立项、申报、经费使用、成果评价）、技术标准、产业政策等方面进行选题，提出CCF见解，向政府建言或向公众发布。该工委的工作将分政策建议和政策评价两部分。

会议决定2014年将围绕网络安全、国家重大基础软件如何发展、高校学科评价、面向智慧工业的IT技术、存储技术、云端操作系统、863项目30年、软件工程硕士评价、反禁运法等涉及国家科技政策、高技术发展、社会服务等选题，通过专题论坛或调研课题等方式开展活动，并对选题进行了分工。