

反病毒方法的现状、挑战与改进(下)*

肖新光

安天实验室

特邀专栏作家

关键词：高级持续性威胁 黑白名单 归一化 沙箱

基本方法的再解读与 APT 场景下的新思考

黑与白：关于识别模型

黑名单与白名单的模式选择

对于恶意代码的检测和防护问题，长期以来无休止的争论是，以黑名单还是以白名单为主导更为合理。由于反病毒技术从特征到行为的识别模式可以视为一套以黑名单为主的机制，而这套机制看起来更容易被绕过，也容易遭到白名单技术倡导者的诟病。

但如果回到反病毒产品发展的起点，即 1986 年个人电脑病毒出现之后的 DOS 操作系统，我们就会注意到以下事实：

第一，绝大部分软件是以磁盘为发布介质的商业收费软件，加之没有广泛覆盖的网络通讯条件，所以广泛搜集这些软件用以形成白名单本身就非常困难；

第二，恰成对比的是，当时的病毒多数是主动传播的，病毒

样本的采集反而更有针对性、也能形成一定的覆盖率；

第三，DOS 时代的可执行文件格式非常简单，设计可执行文件时未考虑签名与验证问题，如 DOS_COM 甚至没有一个固定的文件头部的标识，这就导致其不可能基于一套证书签名验证机制来实现可靠的文件验证，而当时的网络发展也不具备建立一套动态的 CA(certificate authority) 认证体系的条件；

第四，在没有数字签名机制的情况下，必然要采用以“一文件一全文 HASH”的机制来建立白名单。而病毒检测恰恰相反，一条高质量的规则能检测多个样本，在当时正常软件的文件数量远多于病毒种类的情况下，必然导致正常文件 HASH 数将远多于反病毒规则的条数。在当时内存和计算资源非常有限的情况下，一个安全软件如果使用了过多的内存资源，用户肯定是不能接受的。

因此，反病毒技术选择黑名

单机制有其历史必然性，这也是在当时的计算机场景条件下，逐个淘汰选择出的唯一可行方法。

但今天的反病毒技术也并非一个纯黑的机制，也有多个技术点使用了白名单机制。而检测位置有基于客户端的，也有基于云的，其作用是误报的快速解除、未知检测方法的检出能力与误报率的合理平衡、文件上报前的消重等。

在 2006 年前后，反病毒的模式也已经从简单的黑、白思想转为信誉模型。信誉模式综合考虑了一些轻度的安全威胁，以及同样的文件出现在不同的场景中可能有不同的安全结论。很多安全产品在初次安装时，将主机现有的可执行文件建立为安全基线，而对于新出现的文件，则在首次执行时会进行沙箱执行分析，以及向云端提交，同时对终端的信誉评级也会影响到文件的采集策略。卡巴斯基的 KSN^[1]、赛门铁克的 Insight^[2] 等都是代表

* “反病毒方法的现状、挑战与改进(上)”一文见 CCCC 2014 年第 4 期 P40。

性技术。

从2012年起, Bit9等安全厂商倡导的“白名单+安全基线”为主模型的企业级安全产品开始进入用户视野。国内的金山安全、奇虎360等厂商也推出了私有安全云的产品对位跟进。而这种方法变革的可能性又与一些场景和条件变化相关。

第一, 这种模式并不是基于普通个人用户的, 而是针对企业网络的, 其基本思想并非只是由安全厂商发布一个公共的白名单作为通用规则, 而是需要通过产品部署的采集, 通过网管的维护建立一套安全基线规则作为辅助。由于多数企业网络的环境比较简单、近似, 而其运行的软件数量也是收敛的, 因此其安全基线有维护的可行性。

第二, 黑白名单的数量在过去10年发生了显著变化。在反病毒技术发展初期, 只有几十种感染式病毒, 却有成千上万种软件; 而2000年后, 由于地下经济的参与者对样本持续进行加壳、编译器伪装等免杀改动, 即使抛开被感染式病毒感染的样本实体, 目前各安全厂商也都存放了亿级的黑样本文件(从HASH来看), 而从可信白名单数量来计算, 却反而低于这个数量, 因此从HASH云的角度来看, 两者的代价基本持平。而计算和存储能力的发展, 也使HASH云有前置到用户端的可能性。

第三, 由于APT攻击的出现, 高价值网络的使用和管理者

比过去更愿意接受通过牺牲方便性来获得安全, 也愿意承担更多的管理成本。而安全基线的维护无疑是需要承担的管理成本之一, 而这才是以白名单为主导的方法可以存在的前提。

归一化：关于检测处理的基本思想

“归一化”是反病毒领域最重要和最基本的技术方法。但这里所讲的“归一化”已经脱离了其原有领域的学术定义, 而是一种工程方法。通过预处理和降维的手段, 把大量异构异种的恶意代码威胁转化为通过同一个检测模式的规则维护问题(而且是可以低成本维护)来对抗的方法, 就是反病毒领域的“归一化”, 即将大量行为和表现都有巨大差异的恶意代码样本的检测问题, 转变成一种依托反病毒引擎分支与形式化规则(包括规则对应的参数、脚本和模块)的持续对抗。这个思路在20世纪80年代后期成熟, 也是反病毒技术获得快速工程化并发展进步的重要原因。而传统恶意代码对反病毒产品的挑战也是对归一化方法的对抗与“穿透”。

传统的对抗方式包括:

规则层面 攻击者将一个可以检测的恶意代码通过源码修改、入口点修改、加壳和伪装等, 改造成一个不可识别的功能等效样本。

分支层面 一种新的威胁形势如果不能简单地通过原有的

检测分支增加规则处理, 而需要增加新的检测分支, 就可以视为分支层面的对抗。例如在出现宏病毒之前, Office文件是被当作无毒格式跳过的, 但有了宏病毒之后, 就必须要建立新的分支去应对这样的格式, 当需要进行分支级别的增加和维护时, 就意味着出现了分支的穿透。

场景层面 反病毒检测要基于对象的读取完成, 而一些Rootkit、驱动级木马则会造成反病毒软件无法正常读取到有害文件或假的检测对象, 这可能导致无法提取或检测文件; 即使相关样本可以被动态检测到, 但在实际场景下, 检测能力已经失效了。

2005年之前, 病毒和反病毒对抗的核心也是围绕归一化的穿透与反穿透展开的。但实际上, 2005年以后, 这种对抗已经从单点的方法对抗变为一种体系对抗, 其代表性事件包括地下经济集团通过僵尸网络提交大量垃圾使安全厂商的分析能力饱和, 通过误报构造攻击、干扰安全厂商的后台系统, 而自身则通过公钥基础设施(public key infrastructure, PKI)通讯建立更严密的体系等^[3]。而在反病毒方面, 特征维护机制已经高度成熟和自动化, 其更多的精力已经投入到庞大的后端系统的完善、更新的基于文件和位置的信誉机制的建立以及前台产品的防护能力和体验上。

而今天我们再从APT角度来看反病毒的归一化和代码辨识能力(特别是前端产品场景的代

码辨识),在整个反APT作业中,其实不是有效与无效的问题,而是一个必备的基础环节。

归一化的思想灵魂也不再停留在基本规则、分支和场景层面的围观对抗与应对,而可以视为如何使问题简单、如何使威胁回到利于解决的场景中来。该思路可以在 PaloAlto Networks 等安全厂商解决 BYOD 威胁的思路中体现。当移动设备的多信道问题挑战到企业内网安全的时候,这些厂商的解决思路并不是把产品扩展到移动运营商的平台上去,而是通过在企业内网的设备上安装一个小的安全代理(agent)的方式,让流量重回到企业网的网关上来。

在复杂的新威胁时代,归一

化的思想更多地演变成如何让问题收敛。

预测与回溯：关于反病毒的时空特性

笔者已经多次批判“所谓反病毒只是一种基于捕获后再查杀的被动安全方法”。从时间维度上来看,传统的反病毒体系总体上说是一个“基于已知威胁分析的基础上对未来威胁形成预见”的技术体制。

从时间性上来看,这是一种“向后推导”的方法。当新的检测规则和检测机理生效后,其将从事件日志和产品表现上提供相应的检测结果与统计。

如果回到安天实验室所捕获到的 Hangover 事件的前 6 个样

本上¹,我们可以比较一下 6 种反病毒产品在不同时间的检测情况(如表 1 所示)。

在 6 个样本初次活动时,各个安全厂商对其的检测能力都较低,但这并不意味着样本被捕获之后,安全厂商不能将其判断为一个恶意代码。但对 APT 行为来说,仅仅完成“向后的预见”是不够的,样本已经形成的感染分布和纵深影响才更为关键。而同时,安全厂商面临着更大的压力:每天有如此多的恶意代码,其中是否有 APT 样本、以及哪些是 APT 样本?分析确认工作并非简单地依托后端的分析系统所能完成。当情报被视为一种重要的方法时,未来反 APT 工作的重点是向前追溯。

表1 6种反病毒产品在不同时间检测到Hangover事件早期样本的对比情况

样本	卡巴斯基 (Kaspersky)	比特凡德 (Bitdefender)	微软反病毒软件	小红伞 (Avair)	迈克菲 (McAfee)	赛门铁克 (Symantec)	检出数
样本 1							0/6
样本2	√	√		√			3/6
样本3		√				√	2/6
样本4							0/6
样本5	√						1/6
样本6							0/6

样本捕获时入库对照扫描结果

样本2	√	√	√	√		√	5/6
样本3	√	√	√	√		√	5/6
样本4	√	√		√		√	4/6
样本5	√	√		√			3/6
样本6	√	√	√	√		√	5/6

注：以上是2013年8月20日对应样本对照扫描结果

¹ 参见CCCF 2014年第4期P40的“反病毒的现状、挑战与改进（上）”一文中的图2。

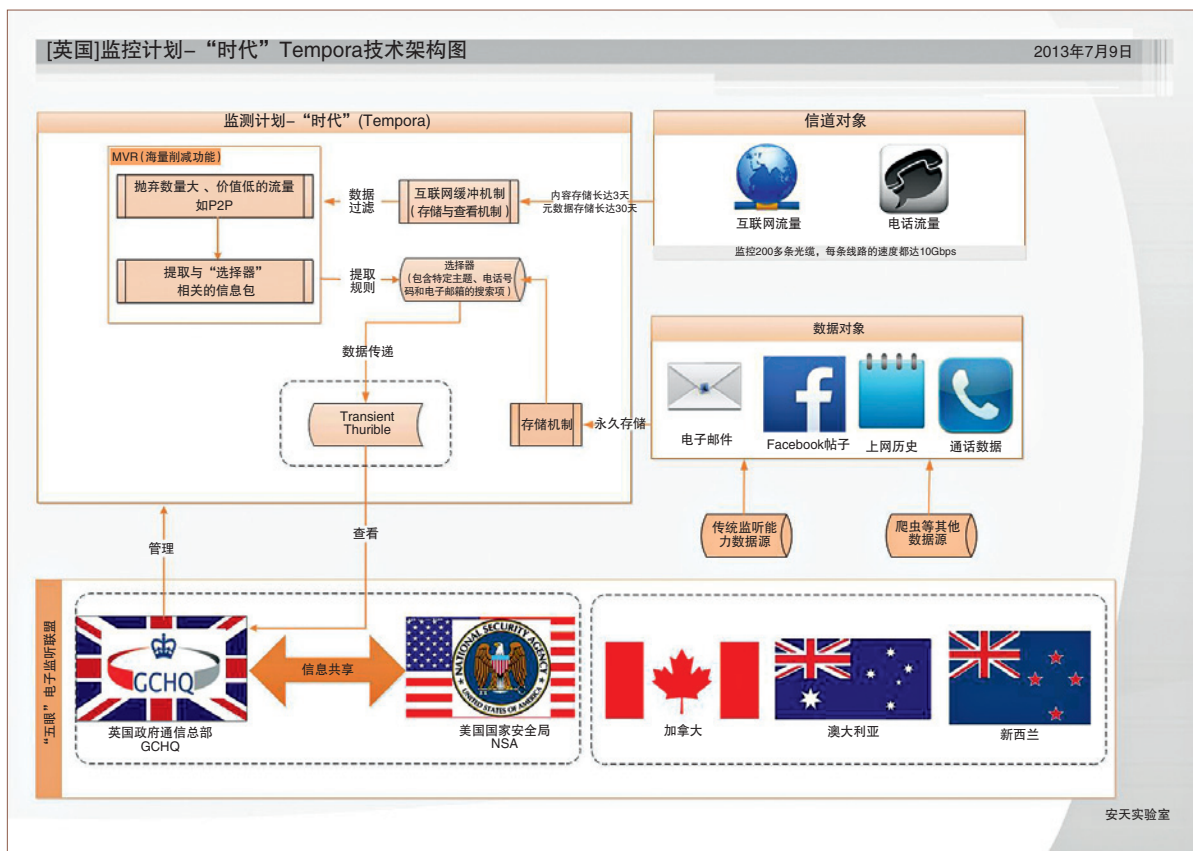


图1 英国GCHQ的“时代(Tempora)”计划示意图

如何建立向前追溯的作业能力,是APT时代的挑战。而一些“传统”的情报设施却能给我们一种启示和参考。在“斯诺登事件”引发的曝光信息中,英国的国家通信情报局(GCHQ)的“时代(Tempora)”计划^[4]可以作为参考(如图1所示)。根据目前披露出来的资料,GCHQ对超过200条光纤实现了全流量的24~72小时的缓存,对全部的元数据实现了90天的缓存,对其中有价值的数据实现了永久存储,对加密数据一直存储到解密为止。假如一个类似的体系并非用于情报监听而是用于攻击检

测,它会产生怎样的价值呢?一个有趣的联想是,我们不仅面临0day攻击,也面临1day攻击,即攻击者是依托补丁的差异点寻找漏洞和攻击方法的。对于这种攻击,由于厂商分发补丁的负载均衡、用户及时打补丁的意识不足等因素,使补丁发布后的有限时间成为黄金攻击期。

如果有72小时的全量数据存储,则意味着攻击被发现后,可以建立出一个在黄金攻击期内的向前回溯机制。即使对于0day,假定一个高级的攻击方式不会只使用一次,长效的流量或载荷存储也将带来一个关联的发

现能力。向前分析,找到更多的事件和受害者,这是APT对抗的重要环节。基于大数据或基于向前回溯的方法是需要以有效的存储能力和分析方法为支撑的。

APT对抗也加重了另一种时间问题上的纠结,那就是网络安全产品检测的实时性问题。无论是传统引擎还是网络设备,都长期面对检测效率和检测效力的平衡问题。带宽的增长要求有更高的检测能力;而安全设备的中央处理器和内存能力的提高、以及多核架构的广泛使用也提升了安全产品的载体能力,但规则的膨胀、分支的增多、解析力度的

不断深入也部分冲抵了硬件能力的成长。而对于以发现 APT 攻击为目标的检测来说,更细粒度的分析、更多的向量提取似乎又是必要的。安全工作者对此的解决方案是抛弃必须实时检测的幻觉,引入异步检测的机制,比如火眼公司 (FireEye) 所倡导的前台设备与沙箱结合。它的沙箱虚拟加载执行,本质上是一个高耗时的异步过程,但在此过程中一旦发现高级威胁行为 (如链接 C&C Server),就可以提取 IPS 规则分发给前端设备,从而将异步能力转化为实时规则。这种内部联动的方式达成了检测深度和检测性能的平衡。此前过度追求检测的实时性有一定的误区,但如果没有实时性,只有异步性,那就没有充分利用传统安全产品的边界能力。

APT 不仅在时间特性上改变着安全产品,也在空间上提出了挑战。安全产品必须满足一定的空间分布才能感知更多威胁,但也没有一种安全产品能覆盖所有空间。而这个问题在过去一直是弹性伸缩的。早期感染式病毒由于依靠磁盘传播,传播速度较慢,因此反病毒产品从地理位置上覆盖更多国家和地区很重要,但能在局部范围内解决流行病毒的产品就能良好地生存。而到了蠕虫时代,由于蠕虫病毒传播迅速,一些研究者认为,通过在网络中部署有限的感知节点,就可以完成对蠕虫病毒的感知 (假定蠕虫是充分扩散的)。部署位置主要

依靠个体的统计,尽量保证均匀,然后考虑实际情况进行修正^[5,6]。但随着定向木马的出现,蠕虫感知器的少量部署就显得不足。而到了 APT 时代,威胁既非全球扩散,也不是简单地承担地缘色彩,而是阵营色彩。这时需要的是安全厂商的产品更多地贴近受到 APT 威胁的高价值用户,包括与用户建立良好的联动分析体制,而非幻想通过大量的基本用户部署就可以感知到威胁。

公有与私有:关于反病毒的资产特性

传统的公司首席信息官更倾向于把安全产品视为能力或者手段,而非一种资产。这种做法是有道理的。安全产品尽管与 IT 基础设施一样消耗了 IT 预算,但并不会提高用户的计算、存储和传输能力,反而会消耗用户相应的资源,与防火墙设备对网络速度的影响、主机安全产品对主机资源的影响类似。这也是保障安全必然要付出的代价。同时安全产品也是一种 IT 资产,这点也应为 IT 资产管理者们所认识到。而反病毒产品作为资产的特性也值得分析:

1. 反病毒产品的资产价值完全依赖于厂商端的支持,如果脱离了厂商的支持,其资产价值将迅速降低和贬值。
2. 反病毒产品在作为其他的信息资产保障手段的同时,亦可能带来新的风险,比如将

未知文件和安全情况向厂商云端汇集。此特性在格式溢出成为 APT 中普遍的前导攻击形式后,变为一个微妙的问题。传统反病毒产品将采集到的未知的可执行文件置于云端分析,用户是可以接受的。但用户显然不可能把文档提交给厂商鉴定。安全与隐私之间的矛盾,就此爆发。

3. 反病毒产品的重要价值在于其规则与知识,但这些对于用户来说更多的是一个基于公有知识的黑箱。用户缺少与此知识体系足够的互动和对它的把握能力。

而 APT 威胁在推动着反病毒产品形态变革的同时,也改变着反病毒产品的资产特性。

流量设备与沙箱结合是将原有安全厂商的后台能力环节向用户端迁移,这种迁移使用户在获得鉴定服务的同时,降低了信息泄露的风险,而沙箱和设备间闭环的规则循环,形成了用户面对威胁的“私有能力”,从而降低了产品自身的贬值速度。私有安全云基于厂商公共知识与用户安全基线组合的方式,建立了用户的“私有知识”,这种知识的价值可能会随着系统的持续运行而提升。

能力的前置化、知识的私有化积累都推动着安全产品在“智能”道路上前行,但这是一种趋势,而非可以完全达成的理想境界。

破除单点迷思

反病毒技术从单点技术走向一个庞大体系的历史过程本身就说明了,依靠任何单点技术都不足以对抗病毒这个“潘多拉盒子”里的魔鬼。而依靠某个单点技术或者体系结构变化来消亡病毒的声音却一直不绝于耳。期待毕其功于一役解决所有安全问题的人们总是喜欢把旧有的安全工程实践视为墓穴中的遗骸,而把某个理想化的单点技术视为长生不老的灵丹。

关于“互联网免费安全模式”将消亡病毒

最近几年的媒体报道中,鲜有类似“红色代码”、“冲击波”、“熊猫烧香”这样对公众影响巨大的病毒出现,于是一些网络评论认为,反病毒软件免费模式导致新病毒数量的增速度在降低,甚至认为病毒会消失。笔者在《木马雪崩到APT的关联与必然》^[7]一文中所公布的样本统计数据表明,上述观点是站不住脚的。如果单纯从恶意代码的数量上来看,病毒过去几年依然呈现增量增长趋势,而Android等新平台是每年一个新的数量级的增长。但同时,在过去几年,病毒的感染率相对本世纪初的几年确实有了明显的下降;而另一个需要重视的情况是恶意代码的可感知性也在下降。

广泛安装的互联网免费客户端和云查杀模式,确实为降低感

染率作出了贡献。但也不要忘记,云查杀的方式是被传统反病毒界提出的,其较早的践行者是熊猫^[8]、趋势等安全厂商,互联网安全厂商对此更大的贡献是,通过反病毒软件免费提升了反病毒产品的覆盖率。这确实是病毒感染率下降的重要原因。

另一个关联因素是操作系统和关联环节的安全改善,微软不断强化DEP、ASLR等内存安全机制,强化UAC等安全策略,弱化U盘自动运行等可能被病毒利用的系统入口,这些做法都在降低传统的大面积感染蠕虫传播的可能性。

但同时,地下经济体系对漏洞的使用定向化,尽量避免对社会造成广泛影响的辨识特性(如很少再像熊猫烧香一样留下图标)等,则使用户对恶意代码的感知度在下降

更值得关注的是,恶意代码正在泛化到互联网触及的各个角落——从路由器中埋设的后门到智能电源中的跳板程序。而反病毒工作者亦将在这些新的平台上展开分析和对抗。

关于可信计算与白名单

可信计算正在全球快速发展,但笔者认为,对“在可信计算条件下,已经不再需要反病毒产品或反病毒能力的观点”需要进行严肃的讨论。

早期,可信计算可以消亡病毒的观点更多地来自病毒的原始定义,即“编制者在计算机程序

中插入的破坏计算机功能或者破坏数据,影响计算机使用并且能够自我复制的一组计算机指令或者程序代码”,因此利用签名验证的思想来对抗“感染”行为的思路是有价值的。但在今天,“病毒”一词已经超越了传统概念,成为一切具有主观恶意代码的代名词(其中包括但不限于蠕虫、木马、后门、恶意脚本、广告色情件和一些带有风险的工具),这其中绝大部分是独立执行的木马,而非感染式病毒,他们同样可以拥有数字签名。

可信计算对数字证书和签名体制有高度的依赖,在过去几年,基于证书窃取的攻击作业比较普遍,在Stuxnet、Flame中我们都见到了这种手法,而且被窃取对象往往都是知名厂商。在Winnti事件中^[9],安全分析者们更是看到了专门进行签名证书窃取的恶意代码。同时,可信计算模型也没能有效地覆盖到能够应对格式溢出、脚本、Webshell等威胁。

白名单与安全基线的组合虽然能提升企业安全能力,但也肯定不是绝对安全的解决之道,该方案的主导厂商Bit9自身的证书就曾被窃取。从这个案例就可以看出,高级威胁防护任重道远。同时,如何保证规模近亿的公有白名单规则的可信度也是一个问题。

有趣的问题正在这里,反病毒是假定一切开发者都是不可信的,而可信计算是基于产业链条彼此互信的思路建立的。在一个互信体系中,反病毒可以作为一

个检查点和一个快速响应机制显然是一个有效的补充。

微软作为可信计算的重要支持厂商,同时也是TPM和UEFI的坚定推动者,尽管其拥有庞大的可信赖计算部门,尽管其开始强力推进驱动签名机制,但微软面临的安全威胁以及对应的安全实践值得我们借鉴和思考。Vista、Win7和Win8系统都没有有效摆脱病毒的威胁,微软的Windows Defender、MSE、MSRT等杀毒工具和补丁体系依然扮演着非常重要的角色。

关于沙箱万能论

对沙箱万能的崇拜,不仅存在于不了解反病毒技术的人们,也影响到反病毒工作者。这种崇拜与寻找可以无限分支回溯的代码分析器,这与对虚拟机和内存检测过高的期待一脉相承,都是在寻求“万能分析器”。

对APT来说,沙箱并不是要简单地解决判别问题,而是要将其从“普通”的恶意代码中区别开来。而无论在沙箱检测机理上做了多么细致入微的工作,能诱发实现这种区别的行为都是重要的。但实际上,即使对普通的恶意代码来说,沙箱的分析能力也在下降。

沙箱是传统反病毒工程师分析PE样本的必备工具,但沙箱对抗有针对性二进制病毒的能力恰恰是有限的,其原因是各种对虚拟环境的检测方法正在普遍被恶意代码使用。尽管反病毒工

作者不断提高虚拟环境的伪装能力,并把检测虚拟环境作为一个可疑的行为条件来看待,但相对这些工作来说,对虚拟环境的检查判断手段显然是非常丰富的,有的甚至是难以感知的。其重要的原因是,沙箱与二进制可执行程度的对抗是代码与代码的对抗,分析手段仅仅拥有前置加载的环境优势,而二进制可执行样本的形态本身有足够的对抗作业空间和想象力。

沙箱的真正优势是对抗APT攻击的重要前导环节,即格式溢出文件,这也正是反APT产品把沙箱前置到用户场景最重要的原因。格式溢出攻击的高成功率在于其社工特点和隐蔽性,其弱点是其需要完成从数据到代码的转换。对于一个已经布设好的捕获环境来说,该转换过程是脆弱并易于暴露的。而格式溢出中,编码作业空间如果想同时对虚拟分析环境的欺骗等操作则相对困难,会提高构造难度与成本。

用户还需要意识到的是,无论产品级沙箱能力多强,其也注定无法与海量计算节点和超大知识体系构建的后端分析平台的能力相比。

尾声：继承历史、达成未来

病毒之所以会长期存在,皆在于攻击者必然会用代码自动完成其自身期望的一些行为。只要攻击的动机存在,病毒的生

命周期就会继续下去,不会被任何新技术所终结。在APT攻击中,病毒只会不断向高阶演变,呈现出制式信息装备的特点,以及更广泛的新威胁领域与特种硬件装备的一体化作业能力。人类与病毒的斗争将贯穿今后的信息技术史,尽管这是我们不愿看到的现实。而对反病毒技术的批判则往往植根于对彻底消亡病毒的想象,或者对某个新技术“永动机”般的期待。

反病毒技术是不断迭代发展的,确实有些技术的历史使命已经终结,而有的则是有趣的“异想天开”。前者包括防毒卡、在可执行程序上添加感染标志的免疫技术等;而后者则包括笔者批驳过多次的“以毒攻毒”的观点。而对于那些试图把现有信息系统推倒来消亡病毒的观点,笔者总是联想到费尔巴哈对黑格尔进行一系列坚决彻底的批判,马克思曾对此评价说:“费尔巴哈像一个糊涂的老太婆,在给婴孩洗澡后,把婴孩和脏水一块泼到门外去了”^[10,11]。2013年美国国防预算法案932.b提出:

“为了克服当前面临的问题和局限性(下一代网络安全)系统不应依赖于:

- a. 已知特征机制;
- b. 需要经常更新的特征机制;
- c. 需要以数据库形式存储下来的特征机制。”^[12]

这种观点被印证作为传统的基于特征检测和特征更新的反病毒技术应该消亡的支撑,也作为

新兴厂商可以取代现有反病毒企业的佐证。但问题是对新技术的需求并不代表传统技术失去了历史价值,否则就难以解释为什么美国多数号称解决新威胁的厂商几乎都购买了 Virustotal² 的最高级别账号,火眼公司为什么要使用 ClamAV 引擎作为其自身动态检测能力的补充。传统的反病毒技术,特别是反病毒引擎,就像所有其他单点防御技术一样,在面对 APT 攻击问题上确有不足,但在检测 APT 攻击的安全体系中,传统反病毒引擎是否还是一个必须的环节?答案是肯定的。因为在一个产品情报化的时代,传统反病毒的精确检测能力成为一种知识,其精确检测海量的恶意代码,并回馈提高风险级别,包括其内置的向量提取机制,将成为反 APT 攻击联合作业的重要支撑。

技术进化史更多的是高阶迭代,而非推倒重来。在多数情况下,那些看上去很美的颠覆性安全思路最终都被证明是“云端布谷之乡中的幻想”^[13]。而更多传统的安全能力与环节之所以不再被我们关注,不是因为它们失去了作用,而是成为一些必须存在的基本能力或者既定事实。传统反病毒技术环节的成熟和自动化,解放了反病毒工程师的思想,使之可以专注于新威胁与新方法的研究,更何况无论对于沙箱还是白名单,反病毒企业本身都有很好的储备和理解。也许,用户未来看到的是**拥有更多传统资源的人更好地驾驭新方法**。

在大玩家^[14]终于登上威胁擂台发起挑战的时候,习惯了刀锋行走、穿越火线的反病毒团队与工程师注定不会认为自己只是一个配角。■

致谢:

感谢我的同事 Angel Li、Billy 等对本文的贡献。



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] Kaspersky security network. <http://ksn.kaspersky.com/en>.
- [2] Symantec Insight. <http://www.symantec.com/reputation-based-security>.
- [3] 后“冷战”时代的病毒捕获体制.
- [4] http://www.antiy.com/resources/The_Virus_Capture_System_in_Post-Cold_War_Era.pdf.
- [5] 维基百科: Tempora. <http://en.wikipedia.org/wiki/Tempora>.
- [6] 王平, 方滨兴, 云晓春等. 基于用户习惯的蠕虫的早期发现. 哈尔滨工业大学.
http://wenku.baidu.com/link?url=6JT2Ykvmo05TsUBMchhnPgvikhe9JEYTVj-k5ole2YpvRpuYBu2WHrtI ZWkhkKjt1hvhSD_x16GFJnWZId2uN4HcHrKcdzXIVtYOnHaW.
- [7] 王平, 方滨兴, 云晓春. 基于自动特征提取的大规模网络蠕虫检测. 哈尔滨工业大学国家计算机信息内容安全重点实验室.
http://wenku.baidu.com/link?url=c606iWtoP7Z_EHDCigMA9kDQ5eV5aAeM9mmWMCOiXoKKwMabvn_TMv-5eJkdsPDT3GMXT0fzTbm1SCzN9UUIj2Ssm44eitnk0CCbfx37je.
- [8] 木马雪崩到APT的关联与必然. http://blog.csdn.net/antiy_seak/article/details/8584182.
- [9] 维基百科: Panda Cloud Antivirus. http://en.wikipedia.org/wiki/Panda_Cloud_Antivirus.
- [10] Winnti. More than just a game. http://www.securelist.com/en/analysis/204792287/Winnti_More_than_just_a_game.
- [11] Marx Notes. <http://wolfweb.unr.edu/homepage/nickles/wthonors/marx-notes.htm>.
- [12] The origins and influences of Marxism. <http://www.socialistpartyaustralia.org/archives/286>.
- [13] 2013美国国防预算法案932.b. <http://www.gpo.gov/fdsys/pkg/BILLS-112hr4310enr/pdf/BILLS-112hr4310enr.pdf>.
- [14] 科尼利厄斯·瑞恩. 最长的一天. <http://book.sina.com.cn/nzt/his/thelongestday/9.shtml>.
- [15] 杜跃进. “大玩家”的APT攻击. 2013中国互联网安全大会. http://wenku.baidu.com/link?url=ak16RJWJBQE_hUTF2A2Y0iHQfBLNIP0-vy2lQOb7Ab3-EBO3aXdghORKST4STKE6-btPzqjO2o12OILFLJwnDt0s3Vu1blLUZjqvBthuuNy.

² Virustotal是全球最大的反病毒引擎扫描服务网站,已被谷歌收购。