

如何理解“下一代反病毒”

非官方中文译文·安天技术公益翻译组 译注

| 文档信息 | | | |
|--------|--|--------|------------------|
| 原文名称 | What' s The Deal With “Next Gen” ? | | |
| 原文作者 | Andy Patel | 原文发布日期 | 2016 年 11 月 16 日 |
| 作者简介 | Andy Patel 目前就职于 F-Secure 公司，任项目经理，系统管理和技术推广方向。他毕业于帝国理工学院，曾就职于 Oracle 等知名公司。 | | |
| 原文发布单位 | F-Secure | | |
| 原文出处 | https://labsblog.f-secure.com/2016/11/16/whats-the-deal-with-next-gen/ | | |
| 译者 | 安天技术公益翻译组 | 校对者 | 安天技术公益翻译组 |
| 免责声明 | <ul style="list-style-type: none"> 本译文译者为安天实验室工程师，本文系出自个人兴趣在业余时间所译，本文原文来自互联网的公共方式，译者力图忠于所获得之电子版本进行翻译，但受翻译水平和技术水平所限，不能完全保证译文完全与原文含义一致，同时对所获得原文是否存在臆造、或者是否与其原始版本一致未进行可靠性验证和评价。 本译文对应原文所有观点亦不受本译文中任何打字、排版、印刷或翻译错误的影响。译者与安天实验室不对译文及原文中包含或引用的信息的真实性、准确性、可靠性、或完整性提供任何明示或暗示的保证。译者与安天实验室亦对原文和译文的任何内容不承担任何责任。翻译本文的行为不代表译者和安天实验室对原文立场持有任何立场和态度。 译者与安天实验室均与原作者与原始发布者没有联系，亦未获得相关的版权授权，鉴于译者及安天实验室出于学习参考之目的翻译本文，而无出版、发售译文等任何商业利益意图，因此亦不对任何可能因此导致的版权问题承担责任。 本文为安天内部参考文献，主要用于安天实验室内部进行外语和技术学习使用，亦向中国大陆境内的网络安全领域的研究人士进行有限分享。望尊重译者的劳动和意愿，不得以任何方式修改本译文。译者和安天实验室并未授权任何人士和第三方二次分享本译文，因此第三方对本译文的全部或者部分所做的分享、传播、报道、张贴行为，及所带来的后果与译者和安天实验室无关。本译文亦不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天实验室一律不予承担。 | | |

如何理解“下一代反病毒”

我们经常被问及有关“下一代”反病毒产品的问题，然而这并不奇怪，因为在过去几年里，它们一直在“喧嚣着”并提出大胆的承诺（这种行为基本始于它们建立之日）。既然如此，就让我们来一睹它的“庐山真面目”吧。

反病毒产业之竞合

在正式接触“下一代”反病毒产品之前，让我们简单回顾一下过去。在过去 30 年里，终端防护行业供应商采用的是“竞合”机制。在这种机制下，他们会在销售方面展开比较激烈的竞争，但与此同时，分析人员、开发人员以及工程师会共享信息、相互合作来加强网络安全。这种合作竞争包括共享知识（借助相关会议和活动）、样本和威胁情报，以及商定某些标准等。

我们看一个实例。2004 年 6 月，VirusTotal 作为反病毒行业的一项服务建立，旨在共享和判断样本。当前，该项服务集成了 50 多家厂商的引擎，每天可以共享大约 5 亿个样本（译者注：5 亿应该不是每日新增样本量，因为目前 VirusTotal 的日提交未去重样本总量约为 200 万），是重要的威胁情报源。

再看另一个实例。“下一代”反病毒厂商为了确保产品提供他们所要求的实际防护效果，建立了独立测试机构。将测试任务交给独立测试机构是可行的——因为消费者和企业没有时间、资源或专业技能去实时处理恶意软件，发现最新被利用的站点，并对几十种不同的产品进行测试以决定购买哪种方案。令人惊讶的是，一些“下一代”反病毒公司建议公众自行测试杀毒产品。在 2008 年，成立反恶意软件测试标准组织（AMTSO™）也是为了解决这一问题。

这种合作竞争并非一蹴而就，而是一个循序渐进的过程。因为在过去，网络安全公司之间存在更多的竞争与对抗。以下是 Alex Eckleberry 在 2011 年对安全行业道德规范的描述：

如何疏远 Virus Total

反病毒形势在几年之前发生了变化。许多“下一代”厂商（这里说的是“下一代终端安全”或“反病毒”厂商，而不是 EDR 或数据泄露检测产品）不再选择加入安全社区，而是选择了完全不同的做法。他们发起了营销活动，通过暗示现有供应商的产品仅是基于“特征”技术的做法，来损害这些供应商的声誉。

下一代反病毒产品为了标新立异，与 VT 这一固有的传统平台抗衡，所以声称 VT 服务只是静态扫描样本，并没有其他“全栈”能力，而这种全栈能力正是“下一代”反病毒产品所推崇的。虽然 VT 意识到这种意图，也采取了相应措施，但收效不大。

Big AV（大型反病毒公司）阴谋

“下一代”反病毒公司为何这样做？他们声称无法在“Big AV”（大型反病毒公司）控制下的安全行业中获得竞争优势。“下一代”反病毒公司认为，“Big AV”类似于“光明派”（Illuminati），控制着安全产业，试图诋毁“Big AV”的声誉。

有问题找 QA（质量保证）

就在最近，“下一代”反病毒产品改变了他们对独立反病毒测试行业错误的营销攻势，并制造许多言论暗示独立反病毒测试行业是不可信的，存在偏见的，付费便可通过测试的。

我们同意独立测试方法并不完美的说法，也许它们没有像相关的技术和威胁全景那样快速发展。并非产品中应用的每一项技术都会作为测试对象，但是安全行业肯定不会被有意操纵以支持某些类型的产品或供应商。

我们与独立测试机构合作的主要动机是服务产品和技术，并从这些测试中获取有价值的数据。测试机构建立并保持一套复杂的支撑体系和框架来支持反病毒软件测试，测试对象是最新流行的威胁的适配性以及最新的终端防护技术的有效性。我们每个月都会进行几项测试，通过这些测试的数据不断提高产品技术以及服务水平。这些测试机构的存在不是为了证明用户产品是“过关”的，如果真是那样的话，他们的服务就会失去意义。

许多“下一代”公司拒绝参与公共或私有的独立测试。所谓的下一代反病毒产品不容易公开下载获得并测试，所以他们特别禁止将其产品出售给测试机构，如果他们发现或怀疑来自测试机构的匿名订单，那么甚至会终止授权，禁止产品继续运行。已经有相当完备的文档对这种行为进行表述。

有人代劳，何需亲自动手

正如我在前一篇文章中所写“传统反病毒”与“下一代反病毒”是由“下一代”公司的营销部门创造的概念。许多“下一代”供应商不是将资源投入到其他独立安全公司所需的技术和基础设施中，而是将大部分相关工作外包给第三方（通常是他们所谓的“传统反病毒”公司）。他们实际上采用购买的方式获取了传统反病毒公司的一些威胁情报数据（第三方许可），甚至在其后端基础设施中运行竞争对手的产品。

我们每天接触大约 50 万个新样本，已经在基础设施、存储和自动化方面投入大量资源，以便将这些样本分类并分析。建设和完善基础设施需要十几年的时间。没有这种基础设施，以及对后端系统，样本分析自动化，样本存储和分类方向的持续改进，我们根本无法在威胁全景中保持领先地位。技术只是一方面，还有规则、逻辑、样本和元数据。这些高度依赖于相关的输入结果，而这些输入结果必须有明确来源。

风险投资支撑大量营销活动

通过适当地减少数据收集和基础设施方面的支出，将直接增加“下一代”营销部门的预算。凭借这些巨大的风险资本支持的营销预算，营销部门用“传统反病毒” vs. “下一代”的观点轰炸了新闻媒体，传播现有的反病毒产品是“仅仅基于特征”的谬论，杜撰独立测试机构的负面新闻，并且可能正在蓄谋还没露面的宣传活动。

值得注意的是，“下一代”这一术语已经在业内广泛采用，这有些遗憾，因为它是带有明显偏见的。“下一代”本意味着更新和更好，一个远离真理的概念，所以更准确和合理的描述应为“新兴反病毒公司”（Anti Virus startup）。

如果你想知道自己是如何得到保护的，那么你将需要厘清大多数“下一代”产品的工作原理，这一过程会很艰难，因为他们的博客文章和白皮书大多只是一串串营销流行语的罗列而已。许多情况下，我们很难购买到“下一代”反病毒产品的授权，所以无法轻易下载安装程序。他们声称这种做法是为了更好的保护其知识产权。而我们则将这种行为称作“隐晦式安全”（Security Through Obscurity）。

都存在 10 年了还说什么“下一代”

现有事实是，所有终端保护方案都使用类似的方法（再次说明，这里比较的是终端保护产品，而不是入侵检测解决方案，这是两种完全不同的概念），但某些产品更侧重强调特定的技术或策略。虽然所谓的“下一代”技术最初是由“传统反病毒”供应商构思和开发的，并且存在了至少十年之久，但“下一代”反病毒公司正在以自己的方式应用这些技术，同时还对这些技术实施着他们的伟大构想。也许基于他们的逻辑，我们将其称为“下一代”？

无论是否归属到“下一代”范畴，反病毒产品的目的都是保护终端系统免受恶意攻击，这一点是毋庸置疑的。竞争和创新都应该得到赞许。从新角度攻击老问题总是受欢迎的。对于这一行业积极有益的是：总会有新的成员加入，而且他们会努力工作试图告诉公众：威胁是存在的，防护是必需的，尤其是我们已经见证了网络犯罪产业和针对性攻击越来越广泛的增长。

我不知道为什么“下一代”反病毒产品通过与传统安全对抗的方式“启动”自己。正如 Kevin Townsend 指出，许多 CISO 认为这种争论是一个薄弱点（所以这可能不会帮助他们导向目标受众市场），但不管什么原因，现在改变还不算太晚。就我个人而言，我希望大家坐下来，把酒言欢，各抒己见，为提供一个更安全的网络世界携手并肩。

无论您是否同意上述观点，请在 Twitter 上告知我。