简译版

网络犯罪的五大新趋势

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	5 Emerging Trends in Cybercrime		
原文作者	Derek Manky	原文发布日期	2018 年 12 月 4 日
作者简介	Derek Manky 是 Fortinet 公司全球安全策略师。https://www.darkreading.com/author-bio.asp?author_id=2624		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/endpoint/5-emerging-trends-in-cybercrime/a/d-id/1333363		
译者	安天技术公益翻译组	校对者	安天技术公益翻译组
分享地址	请浏览创意安天论坛 bbs.antiy.cn 安天公益翻译板块		
免责声明	• 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。		

网络犯罪的五大新趋势

Derek Manky

2018 年 12 月 4 日

各机构现在就要着手防范 2019 年的威胁了，特别要警惕使用人工智能（AI）“模糊测试”技术、机器学习技术和“集群”（swarm）技术的网络犯罪分子。

为了管理日益分散和复杂的网络，各机构正在采用人工智能（AI）和机器学习技术，将繁琐、耗时、通常需要大量人工监督和干预的活动自动化。网络犯罪团伙适应安全生态系统的这一转变，也开始朝着这一技术方向演进。

根据 Fortinet 公司《2019 年威胁全景预测》报告，本文总结了五个新兴的恶意趋势。

1. AI“模糊测试”

零日漏洞利用主要涉及未知的威胁向量，因此对犯罪团伙来说，此技术常常特别有效。幸运的是，发现和利用零日漏洞涉及一种称为“模糊测试”的技术，这需要大量的时间和专业知识，因此零日漏洞并不常见。

模糊测试是一项复杂的技术，专业威胁研究人员经常在实验室环境中使用该技术，来识别硬件和软件接口及应用程序中的漏洞。他们将无效、异常或半随机数据注入接口或程序，然后监控崩溃、未记录的跳转、调试例程、失效代码和内存泄漏等事件，以此来识别漏洞。目前，大多数网络犯罪分子还不具备通过模糊测试寻找零日漏洞的能力。但是，随着人工智能和机器学习模型在模糊测试中的应用，该技术将会变得更加高效和有效。因此，网络犯罪分子将会发现更多的零日漏洞，而这也会对网络设备和系统的保护产生重大影响。

2. 零日漏洞继续肆虐

虽然大量的已知漏洞仍在肆虐，但是攻击者实际上只利用了这其中不到 6%的漏洞。然而，在一些具体的对抗场景中，我们无从知晓犯罪团伙会利用哪些具体漏洞，因此就要求安全工具不得不监控所有这些 6%的安全漏洞。此外，随着潜在威胁的数量持续增长，以及潜在漏洞利用的范围不断扩大，各机构对安全工具的性能要求不断升级。为了跟上这些要求，安全工具需要越来越智能地检测威胁（备注：原文有错误）。

虽然一些框架（如“零信任”环境）可以防御威胁，但是公平地说，大多数机构都没有为即将到来的下一代威胁（特别是那些基于 AI 的模糊测试技术）做好准备。传统的安全方法，例如对已知攻击的修复或监控，很可能会过时，因为它们无法预测设备的哪个方面可能会被利用。在一个无休止且高度商品化的零日攻击环境中，即使是用于检测未知威胁的工具（如沙箱）也会很快被攻破。

3. “集群即服务”（Swarms-as-a-Service）

基于集群的智能技术不断进步，这使得我们更容易受到基于集群的僵尸网络的攻击。这些所谓的“集群”僵尸网络可以协同、自主地运行，以攻破现有的防御系统。这些集群僵尸网络不仅会提高保护各机构的技术门槛，而且，就像零日挖矿一样，它们还会对潜在的犯罪商业模式产生影响，为网络犯罪分子提供更多的机会。

目前，犯罪生态系统是由“人”驱动的。专业黑客通过挖掘自定义的漏洞利用代码来获取不当收益。甚至像“勒索软件即服务”（Ransomware-as-a-Service，RaaS）这样的新技术也需要专业黑客来整合不同的资源。但是，当提供自主的、自我学习的“集群即服务”时，客户和专业黑客之间的直接交互量将急剧下降，从而降低了专业黑客被发现的风险，于此同时还能提高黑客的盈利能力。

4. 自定义的集群

将集群划分为多个任务以实现预期结果，这与虚拟化非常相似。在虚拟网络中，可以根据需要增加或减少虚拟机，以解决带宽等问题。同样，在集群网络中，可以分配或重新分配资源，以解决攻击链中遇到的特定挑战。在“集群即服务”环境中，犯罪分子利用一系列分析工具和漏洞利用代码，对“集群”（swarm）的各个部分进行预编程，包括感染策略、规避策略和秘密数据泄露策略等。此外，集群中有一种“自我集群”（self-swarm），它们几乎不需要来自集群主机的交互或反馈，也不需要与 C&C 中心交互。这能够克服大多数漏洞利用的致命弱点。

5. 机器学习投毒

机器学习是最有前途的网络安全工具之一。各机构可以训练设备和系统，使它们自主地执行特定任务，如确定行为基准，应用行为分析来识别复杂的威胁，或者在面对复杂的威胁

时采取有效的对策等。繁琐的手动任务，如跟踪和修复设备，也可以移交给经过适当训练的系统。但是，机器学习技术可能是一把“双刃剑”——它们无法识别“好”和“坏”，因此它们也会执行蓄意的恶意指令。通过攻击机器学习过程并投毒，网络犯罪分子可以训练设备或系统，使其不对特定设备打补丁或执行更新，忽略特定类型的应用程序或行为，或不记录特定流量，使犯罪分子更好地规避检测。

为明天的威胁做好准备

上文介绍了一些最具前瞻性的恶意行为者的前进方向。为了有效地进行防御，各机构应重新考虑他们当前的安全策略。鉴于目前的全球威胁形势，各机构必须以机器速度应对威胁——机器学习和人工智能技术能够对此提供帮助。将机器语言和 AI 集成到整个分布式网络中的端点产品中，结合自动化和创新，能够有效地帮助各机构打击日益激进的网络犯罪。然而，需要注意的是，网络犯罪分子将很快采用相同的技术来对抗我们，我们应该为此做好准备。

安天简介

安天是引领威胁检测与防御能力发展的网络安全国家队，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、导流捕获、深度分析、应急处置的安全基石。安天致力于为客户建设实战化的态势感知体系，依托全面持续监测能力，建立系统与人员协同作业机制，指挥网内各种防御机制联合响应威胁，实现从基础结构安全、纵深防御、态势感知与积极防御到威胁情报有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委行业和关键信息基础设施等高安全需求客户，提供整体安全解决方案，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

安天是全球基础安全供应链的核心赋能方，全球近百家著名安全厂商、IT 厂商选择安天作为检测能力合作伙伴 ,安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。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”、“心脏出血”、“破壳”、“魔窟”等重大安全威胁和病毒疫情方面，实现了先发预警和全面应急响应。安天针对“方程式”、“白象”、“海莲花”、“绿斑”等几十个高级网空威胁行为体及其攻击行动，进行持续监测和深度解析，协助客户在“敌情想定”下形成有效防护，为捍卫国家主权、安全和发展利益提供了有力支撑。

2016 年 4 月 19 日，在习近平总书记主持召开的网络安全和信息化工作座谈会上，安天创始人、首席架构师作为网络安全领域的发言代表，向总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了安天总部，并对安天人说，“你们也是国家队，虽然你们是民营企业”。

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