2019年（以及过去十年）网络安全趋势总结

简译版

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	A Year (and Decade) in Review: Key Takeaways From 2019 Cybersecurity Trends		
原文作者	Douglas Bonderud	原文发布日期	2019年12月13日
作者简介	Douglas Bonderud https://securityintelligence.com/author/douglas-bonderud/		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/articles/a-year-and-decade-in-review-key-takeaways-from-2019-cybersecurity-trends/		
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。		

2019 年（以及过去十年）网络安全趋势总结

Douglas Bonderud

2019 年 12 月 13 日

网络安全威胁反复无常，会在无预警的情况下突然发生变化。今年，数据泄露的平均成本上升到 392 万美元，每次事件泄露的总记录超过 25,000 条。

信息安全专家疲于应对当前事件。当前事件可以为 2020 年的网络安全态势和投资提供参考，但过去的事件也有助于确定最佳实践和策略，帮助企业逐年增强安全性。

现在离 2020 年只有几周之遥了，我们有必要回顾一下过去的趋势，以开发能够处理未来事件的新方法。

2010 年代网络安全简史

2010 年，实时搜索兴起。2012 年，公司开始大规模利用数据来推动切实可行的方案。到 2014 年，移动设备成为企业协同的主要支柱。但是，随着攻击者认识到大规模（通常是不受保护的）数据集的价值，网络安全威胁也在不断增加。

过去十年中的主要威胁包括：

- 震网蠕虫（Stuxnet）感染 SCADA 系统（2010 年）。Stuxnet 揭开了 SCADA 攻击的序幕，为 Shamoon 和其他能够将物理风险和数字风险结合起来的工业控制系统（ICS）威胁铺平了道路。随着 ICS 和 SCADA 系统通过物联网（IoT）设备链接到面向公众的服务，这种威胁的潜在影响不断扩大。
- 针对 POS 机的网络攻击（2013 年）。2013 年 12 月，一家零售巨头的 POS 系统被感染。恶意软件感染其安全服务器后，4000 万客户的支付卡信息遭窃取。这种攻击的规模和范围使第三方威胁向量成为网络安全专家的关注重心。
- 心脏滴血（Heartbleed）开源漏洞（2014 年）。Heartbleed 侵入全球数据库，为开源安全问题打开了大门，并为诸如 Shellshock 之类的其他攻击铺平了道路。
- NotPetya 试图销毁数据（2017 年）。Petya 勒索软件的新版本 NotPetya，不仅加密数据，还会破坏数据，导致数据无法修复。NotPetya 揭开了多轮勒索软件攻击的序

幕。

- 挖矿软件的兴起（2018 年）。攻击者利用加密劫持技术，通过可以加载到任何网站中的简单挖矿模块，在不引起用户注意或同意的情况下挖掘加密货币。作为响应，安全人员开发了改进的检测和识别工具。

我们得出的结论是，在过去的十年中，攻击者并没有沾沾自喜。从 SCADA 到 POS，再到开源代码、勒索软件和加密货币，攻击者并未拘泥于老一套方法——只要安全人员构建了新的防御方法，他们就会想办法进行破坏。

2019 年网络安全经验教训

过去的网络安全事件能够影响广泛的防御行动，更紧迫的安全问题则推动了目前的响应措施。今年，攻击者将新威胁和旧威胁向量组合起来，执行了如下攻击：

- 全市范围的威胁。攻击者利用恶意软件来攻击整个城市。2019 年 8 月，德克萨斯州至少 22 个城市遭到了攻击。这些攻击迫使主要服务下线，攻击者要求市政当局支付赎金以恢复服务。随着许多市政当局将传统技术和基于云的技术结合起来，防御漏洞不断出现。

- 移动恶意软件。Check Point 调查显示，与去年相比，针对移动设备的网络攻击增加了 50%。移动设备在个人和专业环境中越来越常见，针对移动设备的威胁也越来越多样化了。随着用户优先选择按需功能，移动银行应用程序成为黑客的主要攻击目标，各家银行正在努力修复漏洞。

- 网络钓鱼卷土重来。网络钓鱼又杀回来了，或更准确地说，它从未真正消失过。尽管过去三年中网络钓鱼者相对低调，但是 APWG 的最新数据显示，随着企业电子邮件泄密（BEC）技术变得越来越复杂，网络钓鱼者再次瞄准各公司。

同时，随着公司 IT 团队能够更好地检测和缓解攻击，加密劫持和勒索软件急剧减少。加之动荡的加密货币市场对挖矿和自由支付的影响，黑客选择了更唾手可得的、更有利可图的攻击方法。

攻击向量转移和攻击面扩大，导致了 2019 年的三个关键趋势：

- 更大的安全预算。FireEye 指出，公司希望提高安全团队的效率，因此增加了安全

预算。到 2020 年，安全预算预计增加 1%至 9%。

- 新技术横空出世。公司开始投资于人工智能（AI）和机器学习（ML）等新技术，以应对高级网络攻击的影响，并处理流向安全运营中心（SOC）的大量告警和数据。
- 公司信心大跌。尽管安全支出增加了，但是 Marsh 的最新调查数据发现，只有 11%的公司对其衡量、缓解和管理网络攻击的能力有高度的信心。

如何在 2020 年改善网络安全

2020 年即将来临，公司如何制定既能融合历史趋势，又能应对 2019 年网络安全攻击的防御策略呢？

将过去的经验与现在的期望相结合至关重要。实际上，公司需要三层安全方法。

1. 识别重复性攻击

电子邮件仍然是主要的网络威胁向量——无论攻击者传播勒索软件还是利用社会工程手段窃取账户凭证。正如《福布斯》所报道，尽管目前的检测工具能够更好地阻止常见垃圾邮件，但这些邮件的复杂程度仍然使安全人员大跌眼镜。

要点很简单：网络安全是循环往复的——发生过的攻击会再次出现，对于电子邮件尤其如此。要想在 2020 年及以后建立有效的防御措施，需要将分层电子邮件安全和定期内部培训相结合，以确保员工可以发现安全风险。

2. 应用和整合安全工具

攻击者会采用能够为其带来优势的策略。Petya 攻击效果不够好？ NotPetya 可以补上空缺。勒索软件和挖矿劫持带来的效益不够多？攻击者可以转向破坏性移动应用程序。在 2020 年，信息安全专家需要采用相同的方法。

没有任何方法能够保护所有关键资产并提高其安全性。从能够大规模检测威胁的云工具，到 AI 驱动的防御和智能威胁检测方法，企业可以采用多样化的防御措施以防御不同的威胁。

需要注意的是，企业还必须控制复杂性。攻击者可以改变策略，抛弃先前的渗透方法，但是公司必须全面地进行防御。为此，请寻找能够在不影响性能的情况下集成保护服务的工具。

3. 查明关键网络的薄弱环节

系统最薄弱的环节是哪里？这是一个令人头疼的问题——尽管安全团队尽了最大努力，但大多数信息安全团队仍落后于攻击者。从开源代码泄露到 POS 感染和全市范围的攻击，黑客一直在寻找新的攻击方法。

到 2020 年，企业必须关注其所有系统。公司不能想当然地认为，尚未受到攻击的系统是安全的，而是要意识这些系统遭受攻击只是早晚的问题。虽然调查显示公司的信心下降，但是信息安全团队有机会从头开始。随着攻击的不断发展，潜在攻击假设以及常规渗透测试，可以帮助查明关键网络的薄弱环节。

网络安全并不是孤立存在的。正如过去十年所证明的那样，黑客非常乐意改变策略，他们经常出其不意，并在适当的时机重新利用旧的威胁向量。将 2019 年网络安全经验教训与过去的经验相结合，我们可以为下一个十年制定更好的网络防御策略。

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，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、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的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

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企业、IT 企业选择安天作为检测能力合作伙伴，截止到 2019 年 9 月 30 日，安天的威胁检测引擎为全球超过六十万台网络设备和网络安全设备、超过十七亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

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（如 APT 组织）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，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

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