

简译版

IP 盗窃和网络敲诈风险日益严重

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	The Growing Danger of IP Theft and Cyber Extortion		
原文作者	Robert McFarlane	原文发布日期	2017 年 7 月 6 日
作者简介	<p>罗伯特·麦克法兰 (Robert McFarlane) 是托管安全服务提供商 (MMSP) 和咨询公司 Mosaic451 的首席营收官。他拥有 20 多年的电信、数据网络和网络安全业务开发经验。</p> <p>http://www.darkreading.com/author-bio.asp?author_id=3777</p>		
原文发布单位	Dark Reading		
原文出处	http://www.darkreading.com/cloud/the-growing-danger-of-ip-theft-and-cyber-extortion/a/d-id/1329247?		
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	<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。 		

IP 盗窃和网络敲诈风险日益严重

Robert McFarlane

2017 年 7 月 6 日

最近的迪士尼和 Netflix 攻击事件揭露了知识产权和公司机密所面临的风险，这些风险都是由廉价的黑客工具和加密货币驱动的。

最新的[《Verizon 数据泄露事件报告》](#)警告说，旨在窃取知识产权（IP）和公司机密的网络间谍攻击正在兴起。此后不久，就出现了活生生的例子。[娱乐巨头迪士尼被黑客入侵](#)，黑客盗走了未上映的《加勒比海盗 5：死无对证》，要求迪士尼支付赎金，否则就公开影片。迪士尼拒绝了。

在迪士尼攻击事件之前，还发生了一起重大的娱乐盗窃事件：一名黑客窃取了 Netflix 尚未播出的《女子监狱》第五季全集（共 10 集），要求 Netflix 支付赎金，否则就在网上泄露全集。Netflix 拒绝支付赎金，该剧便在网上遭全集泄露。

公司应该担心 IP 盗窃

Verizon 的报告指出，网络间谍活动尤为关注制造业（占 90%）。大多数此类网络间谍活动是由国家威胁源发动的，旨在窃取尖端技术供本国使用。

然而，迪士尼攻击事件显示，不开发耐虫超级作物或基因治疗的公司也会被当成攻击目标。有些企业对网络敲诈的概念嗤之以鼻，认为他们无关紧要，不足以吸引黑客的注意。但是，正如 Verizon 的报告所述，行业和规模并不重要，“如果您有（或者黑客认为您有）有用的信息，就会成为 IP 盗窃的潜在目标。”

如今，这一标准几乎适用于所有人，攻击者的目标包括：专有金融技术解决方案，赌场游戏软件，秘密食谱，移动应用程序，甚至公司秘密（如营销策略、员工招聘或新产品研究的资料）。当然，没有发行的书籍、电影、电视剧等都是目标。

此外，黑客不再需要雄厚的资金和高明的技术，就能够入侵企业系统。

加密货币和“傻瓜恶意软件”降低了黑客门槛

以前，计算机黑客攻击需要高超的技术实力。要想成为一名黑客，必须拥有强大的编码技能，并且能够理解操作系统、网络架构和硬件。然而，暗网（Darknet）的迅速发展使得黑客不再需要机器人级别的技能。他们[可以购买](#)廉价、易于使用的基于云的“傻瓜恶意软件”。有一群力争进取的黑客[甚至提供客户支持](#)，帮助客户解决遇到的问题。

比特币等加密货币的崛起也有助于网络勒索的增长。在比特币之前，发送和接收非常大笔的资金，同时保持机密性和匿名性是很难的。现在，任何人都可以注册一个比特币账户，随心所欲地发送、接收和花费资金，无需担心暴露自己的身份和住址。

第三方供应商可能使大企业面临风险

Netflix 攻击事件揭示了另一个 IP 安全问题：大公司的安全水平受到第三方业务伙伴的影响。

一般来说，黑客入侵大型公司的支付系统或数据库来搜索银行卡数据或敏感的个人数据，如社保号。非常小的公司不值得他们付出精力。而现在，大量易于使用的工具和不可追踪的支付方式，以及公司（包括许多第三方供应商）在网络上存储着价值数百万美元的知识产权的事实，促使网络犯罪分子越来越有创意。

入侵者不必渗透 Netflix 本身，而是劫持了 Netflix 的第三方后期制作厂商 Larson Studios。同样，犯罪分子可能会入侵服装品牌的纺织品供应商，窃取下个季度的所有款式设计；或者入侵真人秀选手的手机，在大结局播出前公布获胜者。

在某些情况下，入侵一个小供应商可能比攻击跨国公司更有利可图。由于 Larson Studios 向许多电视网络提供后期制作服务，因此可能会出现更多的勒索攻击。

对抗 IP 盗窃

网络保险公司已经注意到第三方供应商漏洞问题了；一些政策要求组织确保其业务伙伴的系统的的核心安全。但是说起来容易做起来难。虽然像迪士尼这样的大型公司能够在其系统上实施诺克斯堡（译者注：自从 1940 年美国陆军装甲兵司令部搬到 Fort Knox[诺克斯堡]以后，诺克斯堡成为美国装甲力量最重要的军事训练基地，美联储的金库也设在这里。高度戒备的

诺克斯堡是美国国库黄金存放处，有 7 道电网围护，全副武装的保安，一道重达 24 吨的安全门）级别的安全措施，但这些措施可能会破坏小企业的预算。不过，迪士尼和 Netflix 表示，只有庞大的预算并不能保证安全。

一个客户端解决方案是网络分段：公司为供应商创建一个独立的系统，使用独立的设置来处理任务，尽可能减少与公司主系统的连接和数字足迹。然而，这涉及成本问题，在某些情况下（如 Netflix 案例），供应商可能需要高度专业的软件和硬件来完成其工作，这使得创建这样一个孤立的系统不太可能。

另一个成本较低的解决方案是：供应商完全在云中工作，与大公司的系统隔离。供应商不能将数据下载到自己的网络上，云解决方案应使用双因素身份验证（密钥卡或应用程序）进行安全保护，以避免与登录凭证有关的安全问题。这种设置并不是万无一失的，而且可能要求供应商投资实现更快速的连接或处理较慢的速度，但是能够减轻其经济负担。

最后，各种规模的组织应考虑与托管安全服务提供商（MSSP）合作（请注意：Mosaic451 就是一家 MSSP，还有许多其他公司也提供这些服务）。使用 MSSP 比内部执行网络安全功能更加便宜，特别是组织不必在安全人员、软件和硬件方面投资了。

随着知识产权的存储数字化，IP 盗窃和网络勒索可能会成为像勒索软件一样严重的问题。各种规模的企业必须摆脱这种威胁，了解风险，采取积极措施防范风险。