

简译版

制造业：恶意侦察和横向移动活动飙升

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	Reconnaissance, Lateral Movement Soar in Manufacturing Industry		
原文作者	Eduard Kovacs	原文发布日期	2018 年 8 月 8 日
作者简介	Eduard Kovacs 是 SecurityWeek 的特约编辑。		
原文发布单位	SecurityWeek		
原文出处	https://www.securityweek.com/reconnaissance-lateral-movement-soar-manufacturing-industry		
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。 		

制造业：恶意侦察和横向移动活动飙升

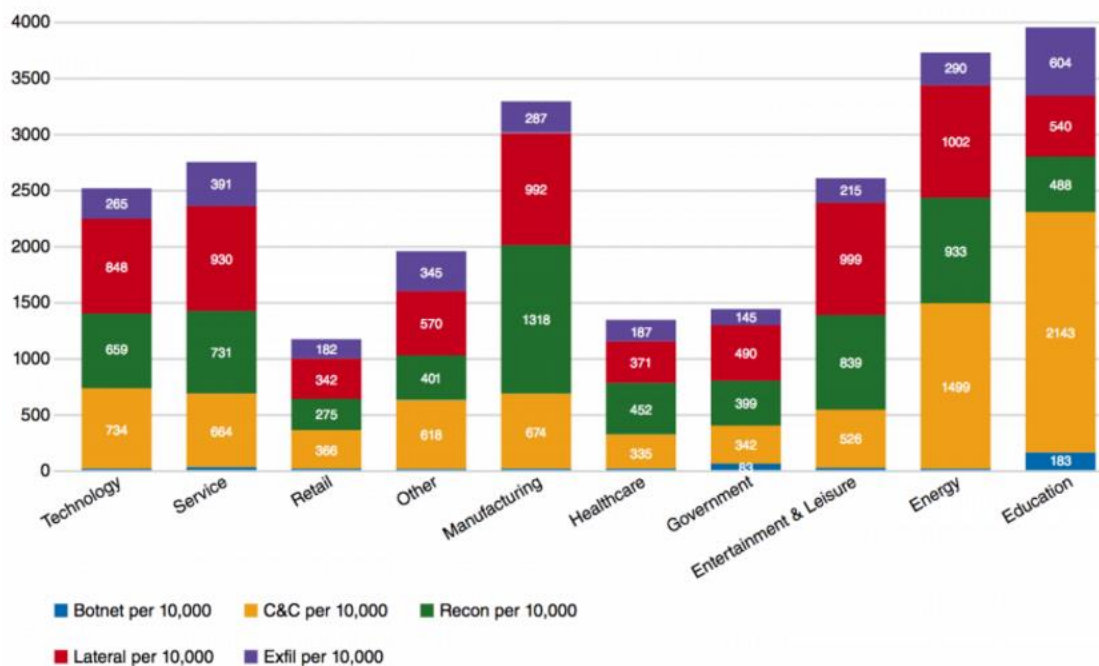
Eduard Kovacs

2018 年 8 月 8 日

最近，制造业遭遇了异常大量的恶意内部侦察和横向移动活动，专家认为这是信息技术（IT）和运营技术（OT）网络快速融合的结果。

威胁检测公司 Vectra 在本周三发布的《2018 年制造行业遭受网络攻击的报告》中介绍了这些趋势，而该报告基于该公司同一天在 2018 黑帽大会（2018 Black Hat）上发布的《针对工业行业的攻击者行为分析报告》（简称 ABIR，介绍了针对九个行业的攻击者行为和趋势）的调查结果。

ABIR 报告显示，很多制造企业遭遇了大量来自网络的威胁。整个制造行业检测到的威胁数量在研究的九个行业中排名第三，仅次于教育和能源部门。



Vectra 着重分析僵尸网络、C&C 流量、数据泄漏、侦察和横向移动五个维度，分别以不同色块表示。

该公司在制造企业中发现了大量的恶意内部行为，这说明攻击者已经进入了企业网络。例如，Vectra 指出，在许多情况下，横向移动是 C&C 流量的两倍（如上图所示）。

“这些行为反映了，由于大量不安全的工业物联网(IIoT)设备和内部访问控制的不足，攻击者能够轻松渗透制造企业的网络并在其中扩散。” Vectra 在其报告中指出，“出于商业原因，大多数制造企业都不会大量投资于安全访问控制措施，实施这些安全控制措施可能会对业已形成的制造流程造成干扰、甚至中断其生产进程，而业务连续性对追求成本控制的流水线 and 数字供应链流程都至关重要。”

许多工厂将其 IIoT 系统连接到常规计算机和企业应用，以进行数据监测和远程管理。Vectra 指出，通过广泛使用的协议（而非专有协议），攻击者更容易渗透企业网络，进行监控并窃取数据。

该公司称，最近制造企业内部侦察的飙升，是内部暗网（darknet）扫描和服务器信息块（SMB）帐户扫描的结果。内部暗网扫描是指，网络上的设备查找不存在的内部 IP 地址；而当一台主机通过 SMB 协议快速使用多个帐户时，则会发生 SMB 帐户扫描。

“制造企业的网络由许多与智能设备和机器通信的网关组成。这些网关以网状拓扑结构相互连接，以简化 P2P 通信。攻击者利用 P2P 设备的自我发现功能映射制造网络，以寻找关键资产，从而窃取信息或执行破坏。” Vectra 指出。

Vectra 还发现了大量的横向移动活动，最常见的是 SMB 暴力破解、可疑 Kerberos 客户端和自动复制（当内部主机向网络上的多个系统发送相似载荷时，会发生自动复制）。

“IIoT 系统使攻击者能够在制造企业的网络中横向移动，在非关键和关键子系统之间跳转，直到找到完成任务的方式。” 该公司解释说。

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，安天依托下一代威胁检测引擎、主动防御内核等自主先进技术、“赛博超脑”支撑平台和专家团队，为用户提供端点防护、流量监测、快速处置、深度分析等产品，以及安全管理、威胁情报、态势感知和靶场演练等解决方案。

安天为国家主管部门、军队、保密、部委行业等高安全需求部门，提供高级威胁和新兴威胁解决方案和能力体系，产品与服务保障了“载人航天”、“探月工程”、“空间站对接”、“大飞机首飞”等重大国防军工任务。安天也是全球重要的基础安全供应链上的核心节点，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，安天的检测引擎为全球近十万台网络设备和网络安全设备、超过十亿部智能设备提供安全防护。其中移动检测引擎是全球首个获得 AV-TEST 年度奖项的中国产品。

安天技术实力得到行业管理机构、客户和伙伴的认可，安天已连续五届蝉联国家级安全应急支撑单位资质，亦是中国国家信息安全漏洞库六家首批一级支撑单位之一。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，提供了先发预警和全面应急支撑。安天针对震网、毒曲、火焰、沙虫、方程式、白象等 APT 组织或 APT 行动，进行了深度的解析，对捍卫国家主权、安全和发展利益形成了有利的支撑。

在 2016 年 4 月 19 日由习近平总书记召开的网络安全和信息化工作座谈会上，安天创始人、首席技术架构师作为网络安全领域的发言代表，向习总书记进行了汇报。2016 年 5 月 25 日，习近平总书记在黑龙江调研期间，视察了位于哈尔滨科技创新城的安天公司，对安天负责人说，“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>