

精译版

## 机器人被黑揭示了新的内部威胁

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	Hacked Robots Present a New Insider Threat		
原文作者	Kelly Jackson Higgins	原文发布日期	2017 年 3 月 1 日
作者简介	<p>Kelly Jackson Higgins 是 Darkreading 的执行编辑，是一位资深技术和商业记者，拥有超过 20 年的报告和编辑经验。</p> <p><a href="http://www.darkreading.com/author-bio.asp?author_id=322">http://www.darkreading.com/author-bio.asp?author_id=322</a></p>		
原文发布单位	Darkreading		
原文出处	<a href="http://www.darkreading.com/vulnerabilities---threats/hacked-robots-present-a-new-insider-threat/d/d-id/1328292">http://www.darkreading.com/vulnerabilities---threats/hacked-robots-present-a-new-insider-threat/d/d-id/1328292</a>		
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 <a href="http://bbs.antiy.cn">bbs.antiy.cn</a> 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>		

# 机器人被黑揭示了新的内部威胁

Kelly Jackson Higgins

2017 年 3 月 1 日

**新的研究表明，机器人及其控制软件充斥着严重和明显的安全漏洞，导致它们很容易被攻击。**

流行的机器人产品包含明显和严重的安全漏洞，攻击者能够轻易地利用这些漏洞，控制机器人的操作，从而进行间谍活动或造成物理伤害，甚至会对人类带来危险。

研究人员将此称为一种新的内部威胁。IOActive 研究员 Cesar Cerrudo 和 Lucas Apa 发现，企业、工厂和家庭中使用的热门机器人和机器人控制软件存在约 50 个漏洞，黑客能够利用这些漏洞远程操纵在办公室、工厂或家庭中活动的机器人，渗透其他网络，监控和窃取信息，甚至造成物理破坏。

机器人变得“越来越聪明”。在某些情况下，它们具有更像人类的特征，如面部识别功能，这些推动了他们的流行和使用。IDC 预测，到 2020 年，全球机器人支出将达到 1880 亿美元。IDC 指出，机器人目前主要用于制造业，但是消费者和医疗保健行业也开始使用机器人了。

Apa 说，“机器人入驻企业已经成为一种现实情况。但是我们很难区分哪个机器人被黑了，哪个没有被黑。”

根据研究人员的说法，机器人会是下一代内部威胁，被黑的机器人能够秘密感染办公室内的其他网络，甚至感染其他机器人。

Apa ( IOActive 的高级安全顾问 ) 和 Cerrudo ( IOActive 的首席技术官 ) 研究了 Softbank Robotics , UBTECH Robotics , Robotis , Universal Robots , Rethink Robotics 和 Asratec Corp 生产的机器人和机器人控制软件。他们想在机器人成为主流之前，深入了解其安全问题。

机器人及其控制软件充斥着一些与臭名昭著的不安全的物联网设备相同的安全漏洞：不安全的通信漏洞，如机器人及其组件（提供命令和软件更新）之间的明文或弱加密通信；缺

乏身份验证（例如，不需要凭证就能够访问机器人的服务）；缺乏授权措施（可能会导致机器人被攻击者摆布）。

此外，他们发现机器人及其软件的弱加密导致存储在机器人中的敏感数据和信息（例如密码，加密密钥和厂商服务凭证）面临风险。一些机器人具有默认配置，用户无法自行锁定它们。Cerrudo 和 Apa 发现，一些设备甚至不支持修改密码，即使被黑并修复后也不支持。

Apa 说：“很难将机器人恢复到初始（未被感染）状态。对于一些厂商的产品来说，这根本是不可能的。”所以说，一旦机器人被黑，用户基本就毫无办法了。

研究结果显示，机器人还有一些与其他软件系统相同的开源框架和库漏洞。IOActive 指出，许多机器人运行 ROS 系统（Robot Operating System，机器人操作系统），该系统具有明文通信，身份验证和弱授权等特征。研究人员在报告中写到：“在机器人社区，为机器人开发和编程共享软件框架、库、操作系统等似乎很常见。如果软件是安全的，这不是什么坏事。不幸的是，情况并非如此。”

物联网安全专家，Lab Mouse Security 创始人兼首席执行官 Don Bailey 表示，机器人漏洞是嵌入式物联网设备漏洞的另一个例子。“它们都是嵌入式系统，你会看到相同的威胁不断出现。” Bailey 说。

他说，今天的机器人设备面临的更大风险是数据和隐私泄露。Amazon Alexa 和 Apple Siri 式智能设备等可以更多地用于间谍活动。“当机器人发展到更实质性的技术时，将会出现更多面向人类的物理危险。” Bailey 说。

他说，现在的一个严重问题是机器人产品的供应和淘汰。“机器人如何与其主人关联起来”，当主人将其转给新主人时会发生什么？安全和隐私风险。例如，我们不清楚在前主人能够访问机器人的情况下，新主人该如何保护自己。

目前，Apa 和 Cerrudo 还在等待厂商的回应，尚未发布漏洞的细节。到目前为止，只有四家厂商进行了回应。Cerrudo 说：“只有两家厂商表示会修复漏洞，另外两家则说他们理解他们应该‘做点什么’。”

由于一些设备的费用和全球航运限制问题，研究人员无法测试所有的机器人。对于这样的机器人，他们主要分析其软件，包括移动应用程序，操作系统和固件映像。他们说，这些是机器人系统的核心元素，他们可以由此分析其安全问题。

有趣的是，他们还没有深入地进行安全审查，就发现了这些漏洞。他们计划做进一步的分析，以更好地了解目前的机器人安全问题。

Apa 说：“我们认为一些漏洞很容易被利用。任何有手机和应用程序的人都可以通过这些漏洞远程控制机器人，他们不需要自己开发漏洞。”

存在漏洞的产品包括：SoftBank Robotics 的 NAO 和 Pepper 机器人；UBTECH Robotics 的 Alpha 1S 和 Alpha 2 机器人；ROBOTIS 的 OP2 和 THORMANG3 机器人；Universal Robots 的 UR3，UR5 和 UR10 机器人；Rethink Robotics 的 Baxter 和 Sawyer 机器人；Asratec Corp 使用 V-Sido 产品的机器人。

在一个令人毛骨悚然的场景中，研究人员说，具有面部识别功能的机器人会被黑客攻击，甚至操纵其他机器人。例如，机器人通常带有麦克风和摄像头，所以攻击者可以将机器人用作间谍，窃取信息。“如果攻击者控制了机器人，就可以使用内置的功能来获取机器人识别的面部信息。” Apa 说。

IOActive 不是第一个探索机器人安全问题的公司。2015 年，华盛顿大学黑了一个手术机器人，用来演示攻击者如何劫持和控制正在做手术的机器人。

研究人员说，现在，企业和家庭机器人用户基本上没什么保护措施。他们能做的只有“祈祷”。Cerrudo 说：“如果我是一个机器人用户，我会在晚上不用时关掉电源。”