简译版

IoT 安全和被遗忘的 IoT 设备

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	IoT Security and the Internet of Forgotten Things		
原文作者	乔纳森·里德（Jonathan Reed）	**原文发布日期**	2022 年 3 月 22 日
作者简介	乔纳森·里德是一位自由作家。		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/articles/iot-security-internet-forgotten-thing/		
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		
摘要	如今，全球约有 123 亿台联网设备。有多少 IoT 设备存在安全漏洞呢？又有多少被遗忘的 IoT 设备呢？这些设备还能连接到企业的网络吗？它们有什么风险呢？对此企业能做些什么呢？本文将对这些问题进行分析。		
免责声明	本译文不得用于任何商业目的，基于上述问题产生的法律责任，译者与安天集团一律不予承担。		

IoT 安全和被遗忘的 IoT 设备

乔纳森·里德

2022 年 3 月 22 日

2017 年，全球联网设备的数量超过了世界人口——这一数量非常惊人！但是，很多联网设备都没有考虑到安全问题，导致攻击者很快就能利用物联网（IoT）漏洞执行攻击。

2016 年，为 Twitter、Spotify、Netflix、Reddit、Etsy 和 Github 等公司托管网络流量的 DNS 服务公司 Dyn，遭到了大规模 DDoS 攻击。攻击者利用 Mirai 恶意软件感染了至少 10 万台设备（包括网络摄像头、DVR 等），他们将这些设备变成“僵尸”，对 Dyn 发起了大规模攻击。

如今，全球约有 123 亿台联网设备。有多少 IoT 设备存在安全漏洞呢？又有多少被遗忘的 IoT 设备呢？这些设备还能连接到企业的网络吗？它们有什么风险？对此企业能做些什么呢？本文将对这些问题进行分析。

IoT 面临巨大的安全风险

企业、家庭、医院、政府机构、车队，以及任何存在网络连接的地方，都有联网设备。2020 年，美国家庭平均使用 10 台设备。如果一个美国家庭平均有 2.6 人，那么一家拥有 1000 名员工的公司会有多少 IoT 设备呢？

IoT 设备能够快速生产，且生命周期短暂，这使其数量呈爆炸式增长。这导致的结果是，很多企业仍在使用已无法再接收安全更新的旧设备；而其新设备又面临着零日漏洞利用等威胁。

最近，研究人员发现，用于边缘计算的消息引擎和多协议消息总线 NanoMQ 存在漏洞。NanoMQ 用在智能手表、汽车、火灾探测器、患者监测和安全系统的传感器中，能够捕获实时数据。该漏洞导致超过 1 亿台设备面临风险。

很多公司担心，远程和混合办公会增加企业的网络风险。除此之外，他们还应关注巨大的 IoT 攻击面。

IoT 安全威胁影响

2021 年上半年，智能设备遭受了 15 亿次攻击。攻击者试图窃取敏感数据、加密劫持设备或创建僵尸网络等。他们甚至能够利用远程办公的设备访问公司资产。

我们以 CVE-2021-28372 漏洞为例进行说明。攻击者可以利用该漏洞远程感染受害者的 IoT 设备，从而窃听实时音频、观看实时视频，并窃取设备凭证以进行更深入的网络渗透。

要想保护企业免受勒索软件威胁，安全领导者不仅要阻止网络钓鱼攻击，还要保护其 IoT 生态系统。有些人认为，可以通过重启设备来阻止劫持或锁定设备的恶意软件。但是实际上，重启 IoT 灯泡可能会导致你的网络暴露，我们稍后会分析这一点。

监管能否解决问题?

由于 IoT 威胁到用户的安全和隐私，监管机构陆续出台了相应的法律法规。目前，一项国际 IoT 安全标准正在编制中。截至目前，美国的主要 IoT 标准源自 NIST，而加利福尼亚州也有自己的制造商法律。《2020 年物联网网络安全改进法案》规范了政府对此类设备的采购。

由于许多设备或设备部件来自海外，监管就变得更加复杂了。我们的结论是：仅靠监管并不能保护企业的数字资产。

联网灯泡的问题

智能灯泡也有可能存在漏洞。这是怎么发生的呢？我们来看下它的工作原理：

1. 攻击者远程劫持灯泡的功能。然后，他们可以更改灯泡亮度或使其打开/关闭。这导致用户认为灯泡不能正常工作。而在控制应用程序上，灯泡显示为“无法访问”。

2. 如果用户重启灯泡且应用程序重新识别它，攻击者就能够将受感染的灯泡添加到网络中了。

3. 随后，受感染的灯泡可以安装恶意软件，以实现 IP 网络渗透和恶意软件传播。

传统方法是否有效?

保护 IoT 设备的传统方法包括：

- 及时安装固件更新。更新中的补丁有助于防止零日攻击。
- 更改预设口令。使用包含大小写字母、数字和符号的复杂口令。
- 一旦你认为设备运行异常，请立即重启，这有助于阻止现有的恶意软件。（请警惕该建议！）
- 通过本地虚拟专用网络访问 IoT 设备，这可以防止设备暴露于公共互联网。
- 根据威胁数据，阻止来自恶意网络地址的网络连接。
- 将未打补丁的设备保存在单独的网络中，未经授权的用户无法访问这些设备。理想情况下，请停用、销毁或回收无法修复的设备。

在上述建议中，有些是有用的，但其中有一个弊大于利。正如我们之前所说，设备重启可能会导致恶意软件感染。

零信任最佳实践

IoT 安全挑战是更大安全问题的一部分。简言之，如今企业边界几乎已经不存在了。在企业部署了如此多的设备，并有如此多的员工远程办公的情况下，我们需要一个新的解决方案。

例如，企业可以采用零信任架构。零信任架构将用户、设备、应用程序，或者试图获得网络访问权限的 API 等都看做是“边界”。在验证其身份和真实性之前，企业应将“拒绝访问”作为默认设置。

采用零信任方法的企业，应考虑使用“安全访问服务边缘”（SASE）服务。SASE 能够在边缘建立云交付安全性，更靠近访问公司资源的用户和设备。这样一来，企业就能够将软件定义的网络和网络安全整合到单一的、基于云的服务中。

SASE 是一种零信任模型，能够集成边缘计算安全，旨在满足混合办公和各种 IoT 环境的需求。如今，企业面临快速的设备扩展和流动的边界，他们应寻求诸如零信任等解决方案，以保持安全。

安天简介

安天致力于全面提升客户的网络安全防御能力，有效应对安全威胁。通过 20 余年自主研发积累，安天形成了威胁检测引擎、高级威胁对抗、大规模威胁自动化分析等方面的技术领先优势，打造了面向服务器、云、虚拟化、容器和传统办公节点等提供全防御能力覆盖的智甲安全产品家族，满足客户对于包括终端杀毒、终端防护（EPP）、终端检测与响应（EDR）、云工作安全防护（CWPP）等系统安全层面需求；整合强化包括 ATID 威胁情报门户、追影沙箱和捕风蜜罐等产品在内的威胁情报板块产品，有效提升客户情报赋能和自主情报生产能力；基于流量产品探海有效应对客户对于网络威胁检测与响应（NDR）和网络流量分析（NTA）的安全需求，相关产品可以实现交叉联动，统一管理，形成面向从勒索软件到高级威胁（APT）的纵深安全防线。同时打造威胁对抗、威胁猎杀、威胁巡检服务三款主打安全服务，辅以平台支撑、快速到达的轻量级垂直响应服务，以运营模式有效支撑应对综合威胁对抗能力升级。

安天为网信主管部门、军队、部委、保密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，已连续七届蝉联国家级网络安全应急支撑单位。安天参与了 2005 年后历次国家重大政治社会活动的安保工作，获得杰出贡献奖、安保先进集体等荣誉称号；自 2015 年来，安天的产品与服务为包括载人航天、探月工程、空间站对接等历次重大航天飞行任务，以及大飞机首飞、主力舰护航、南极科考等重大任务提供安全保障支撑。

目前，安天的威胁检测引擎为全球超过一百万台网络设备和网络安全设备、超过三十亿部智能终端设备提供了安全检测能力，已经成为“国民级”引擎。

安天已发展成为以哈尔滨为总部基地，建有六地研发中心、两个控股子公司，参与一个国家工程实验室建设，拥有两个省级工程中心和重点实验室、一个博士后创新创业基地和多个高校联合实验室的集团化创新企业，同时在多地设有办事处和应急响应站，为客户提供全面的安全服务与技术支持。

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*