

简译版

物联网安全问题导致更加严重的后果

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	Organizations Continue to Fail at IoT Security, and the Consequences Are Growing		
原文作者	Sue Poremba	原文发布日期	2019 年 2 月 14 日
作者简介	Sue Poremba 从 2011 年开始撰写文章，专长是网络安全和技术领域。 https://securityintelligence.com/author/sue-poremba/		
原文发布单位	Security Intelligence		
原文出处	https://securityintelligence.com/organizations-continue-to-fail-at-iot-security-and-the-consequences-are-growing/		
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。 		

物联网安全问题导致更加严重的后果

Sue Poremba

2019 年 2 月 14 日

物联网 (IoT) 已经蔓延至全球——或者，至少看起来像这样的。据 Gartner 称，到 2020 年，全球预计将有超过 200 亿台在线的 IoT 设备，而在 2017 年，这一数量仅为 90 亿台。

尽管如此，IoT 设备的安全性仍然堪忧——此类设备已经成为 2018 年最大的攻击向量之一。虽然企业已经认识到 IoT 对其整体网络安全造成了威胁，但是他们未能恰当地保护 IoT 及 IoT 设备生成的数据。

企业无法保护看不到的东西

IoT 成为 2018 年最大的攻击向量之一，其中的一个原因是它在企业网络上的不可见性。根据 Gemalto 公司的一份报告，48% 的企业承认他们无法在网络上检测到这些设备。但是，消费者希望企业能够掌控物联网的安全。对于企业来说，这已经成为一种悖论：他们必须保护他们无法在网络上看到的東西。

与此同时，IoT 供应商在开发设备和软件时也未考虑到安全性——他们也不必这样做，因为关于 IoT 还未出台什么安全标准。（译者注：2019 年 2 月 20 日，欧洲刚发布了 IoT 设备的网络安全标准

https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf)

“以这些设备的操作系统为例，” Information Age 的尼克·伊斯梅尔 (Nick Ismail) 写道，“如何升级无线连接的壁挂式空调机或者智能灯的操作系统呢？如果无法升级其操作系统，那该如何修复漏洞呢？”

这就是网络犯罪分子瞄准 IoT 设备的原因。无论是在设备/软件的开发方面，还是在联网方面，它们的安全性都很薄弱，因为企业很难考虑到所有的联网设备。

在 2018 年，攻击者最青睐的目标包括路由器和防火墙。去年春，US-CERT 发布警报，称攻击者正在攻击联网设备，并表示如果他们能够控制路由器，也将能够控制流量。该警报补充说，“进入企业内部路由和交换基础设施上的攻击者可以监控、修改和拒绝发送至/来自内部关键主机的流量，并利用信任关系向其他主机进行横向移动。”旧系统或从未进行升级

的系统是最容易攻击的目标。

针对 IoT 设备的攻击

网络犯罪分子知道 IoT 设备是很容易攻击的目标，这就是为什么专家警告称，在未来几年内，特制的针对性攻击数量将会增加。例如，针对医疗行业的恶意软件不断增加。这些恶意软件不仅攻击医疗设备，还攻击医院中的其他 IoT 设备，如供暖、通风和空调（HVAC）系统或无线打印机。

攻击者也在利用勒索软件执行 IoT 攻击。针对 IoT 的勒索软件攻击与针对内部网络的勒索软件攻击有所不同。在内部网络攻击中，通过攻击计算机或服务器，勒索软件可以直接锁定企业的数据。而在 IoT 攻击中，数据本身就在云端，设备可以轻松重启，这意味着企业无需支付赎金——对攻击者来说，这是“双输的”（lose-lose）。

就像 DDoS 攻击一样，针对 IoT 的勒索软件攻击选择关键时间点发起。如果无法重置设备，勒索软件就会将设备下线，或者接管设备。例如，勒索软件可以在周末深夜接管某栋大楼的 HVAC 系统，将空调温度调高，直到受害者支付赎金为止。

恶意软件还能够将 IoT 设备组建成僵尸网络，并影响其他网络和设备的功能。除非 IoT 的安全性得到改善，否则这些僵尸网络还会进一步发展。

面向供应商和企业的 IoT 安全解决方案

在 2019 年，IoT 安全将会获得更多的关注。安全专家预测，针对 IoT 基础设施的攻击将会更多，针对 IoT 设备的恶意软件将会更多，需要保护的端点也会更多。这意味着，在 2019 年，从供应商到企业安全团队都要投资于安全方法和解决方案。

在软件方面，安全性主要取决于供应商。随着人们对 DevSecOps 的认识和日益重视，供应商将会努力在 IoT 设备中内置安全措施。美国的新隐私法也将迫使制造商给予用户更大的控制权；例如，加州通过了一项法律，从 2020 年开始，禁止在新设备上使用默认口令，并确保每台设备都内置了安全措施。（译者注：这条在上面提到的欧洲标准中就有描述。）

在企业方面，安全团队可以引入高级工具，例如“纳米代理”（nano agent）和“雾计算”（fog computing），这些工具允许对设备进行微分段（microsegmentation）。雾计算是设备和云之间的一个层，允许实时监控设备，特别是关键设备。在这些关键设备中，网络事件发生

与否可能会带来生与死的差异。未来，纳米代理可能会进一步发展，直接嵌入到各个设备中，以监控网络风险。

物联网已经蔓延至全球——如果我们不解决 IoT 设备的安全问题，那么网络犯罪分子将会利用这些问题破坏网络的正常运行。

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，始终坚持自主先进能力导向，依托下一代威胁检测引擎等先进技术和工程能力积累，研发了智甲、镇关、探海、捕风、追影、拓痕等系列产品，为客户构建端点防护、边界防护、流量监测、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有机结合，推动客户整体安全能力建设的叠加演进。安天为网信主管部门、军队、保密、部委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，产品与服务为载人航天、探月工程、空间站对接、大飞机首飞、主力舰护航、南极科考等提供了安全保障。

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厂商、IT 厂商选择安天作为检测能力合作伙伴，安天的威胁检测引擎为全球超过三十万台网络设备和网络安全设备、超过十四亿部智能终端设备提供了安全检测能力。

安天技术实力得到行业管理机构、客户和伙伴的认可，已连续五届蝉联国家级安全应急服务支撑单位。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，为捍卫国家主权、安全和发展利益提供了有力支撑。

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的发言代表，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>