精译版

当心下一波网络威胁：物联网勒索软件

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	Beware the next wave of cyber threats: IoT ransomware		
原文作者	David Balaban	原文发布日期	2017 年 6 月 12 日
作者简介	David Balaban 是一名计算机安全研究员，在恶意软件分析和反病毒软件评估方面拥有超过 15 年的经验。https://www.information-management.com/author/david-balaban		
原文发布单位	Information Management		
原文出处	https://www.information-management.com/opinion/beware-the-next-wave-of-cyber-threats-iot-ransomware		
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	• 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。		

当心下一波网络威胁：物联网勒索软件

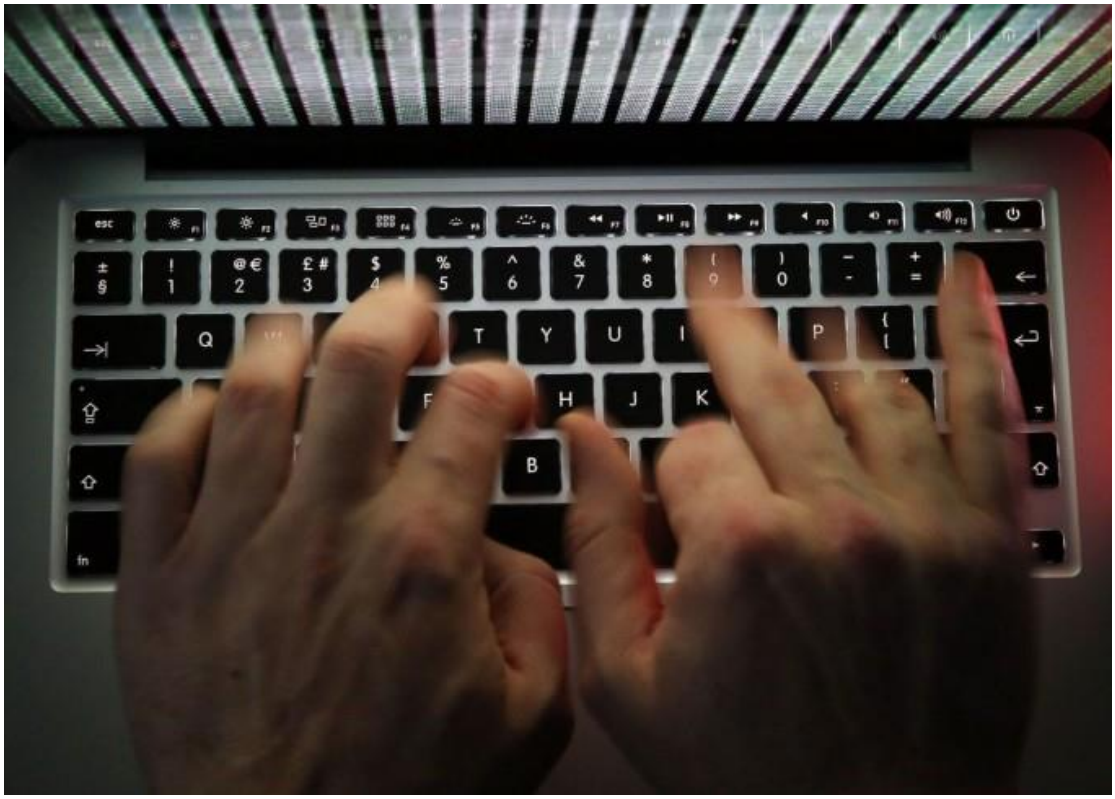
David Balaban

2017 年 6 月 12 日

勒索软件已经成为困扰组织的最严重的网络威胁之一。今天，我们所有人，从家庭用户到企业和政府机构，都在努力保护自己免受加密病毒的侵害。

但是我们没有注意到，下一波旨在加密物联网（IoT）设备的勒索攻击已经开始了。由于物联网无处不在又极其多样化，这些攻击可能会更加危险。

简而言之，物联网的一些特征导致物联网勒索软件比已经广泛传播的针对电脑和智能手机的勒索软件更加危险。



物联网勒索软件不会对您的数据进行加密

众所周知的加密勒索软件，如 Locky 和 Cerber，会锁定受感染机器上的重要文件。这种加密是不可逆转的：受害者要么支付赎金获取解密密钥，或者在没有备份的情况下和他们的

文件永别。人们通常认为，文件和重要数据的价值可用货币的形式表示，这一事实吸引了敲诈者。

物联网设备根本没有任何数据。有些人可能认为勒索软件作者对攻击物联网设备不感兴趣，情况并非如此。

相较于只锁定一些文件，物联网勒索软件可能会锁定并完全控制许多设备甚至网络。物联网恶意软件可能会迫使车辆停下，断开电力甚至终止生产线。这样的程序能够造成更大的伤害，因此黑客可能会要求更多的赎金。这增加了这一新兴地下市场的吸引力。

有人会争辩说，可以通过简单的重启来阻止物联网攻击。然而，受害者支付赎金的原因在于失去系统控制期间可能发生的损失的数量和性质，而非攻击的不可逆转性。

物联网扩展了生命支持设备（如起搏器）或工业系统（如泵站）的可能性，与此同时，阻断物联网基础设施和不及时的响应造成的损害将会呈指数增长。在工业控制系统中使用物联网设备的组织面临最大的风险，例如发电厂、大型自动化生产线等。

消费者物联网设备

针对消费者物联网设备（包括智能家居和连网汽车）的攻击早已发生。研究人员已经展示了如何使用恶意代码来控制连网的温控器，将温度设置为最大值，迫使受害者支付赎金。

可以想象一下，今天早上你坐上一辆连网汽车，准备出发去工作。突然屏幕上出现了一条消息："想要启动车子去上班，那就支付 500 美元吧。"几年前，这种情况是不可能发生的。而如今，由于技术的进步，这种情况看起来并不奇怪。

此外，物联网勒索软件可能会窃取重要数据和个人信息，例如，从连网的监控摄像头或健身工具中窃取敏感信息，威胁受害者说会公布这些信息，以此敲诈受害者。

尽管物联网设备通常存在严重的安全漏洞，但是谈论智能家居和连网汽车即将面临的勒索软件威胁为时尚早。由数千家制造商创建的各种应用程序和设备使得恶意软件的使用更加广泛和复杂。

如今，物联网行业高度分散。该行业缺乏标准化的方法、通用平台和通信系统，因此很难进行大规模的攻击。在一次攻击中，黑客通常只针对特定类型的设备，这减少了潜在受害者的数量。

我们可以得出结论：目前，黑客攻击消费者物联网设备的利润空间很小。但是随着物联网进一步深入家庭和办公室，未来，情况很可能会发生改变。

工业部门面临高风险

物联网的工业部门面临着完全不同的情况。工业系统对勒索者具有强大的吸引力。这可能是任何可能影响数千甚至数百万人生活的系统，其运作成本非常高昂。

例如，最近几家美国医院遭受了一系列的勒索软件攻击。好莱坞长老会医院的正常运作被勒索攻击打断，不得不将部分病人转移到其他诊所，医生也被迫回归到老式的纸质记录方法。

如果医院的系统遭到感染，所有患者的健康都会受到威胁，因此医院支付赎金的可能性非常高。针对关键基础设施的攻击基于类似的心理：如果人们的生活受到威胁，而且时间紧迫，业主往往会同意支付赎金。

电网和发电站也是物联网恶意软件的重要目标。它们在现代世界中的重要作用在 2003 年美加大停电事件中得到了很好的体现。在几个小时内，大停电造成了 60 亿美元的损失，影响了 5500 万人的生活。该事件不是网络攻击，而是软件故障。而今天，黑客不断扫描互联网，寻找重要的漏洞网络，所以能源公司应该做好应对准备。

如何保护物联网系统

虽然不存在通用的解决方案，但许多专家认为，遵守某些准则和方法可以帮助组织和制造商更好地保护其物联网系统免受勒索攻击。

重要的一点是：能够远程升级智能设备的固件。安全是一个旅程，而不是目的地，没有任何连网设备可以永远保持安全。因此，我们应该进行简单、有效和安全的固件更新。

要采用安全的固件更新渠道，因为不安全的更新渠道可能会成为感染入口点。我们可以采用一些经过时间考验的措施来消除这种入口点，例如阻止处理器和固件、加密设备之间的通信通道。

另一个重要的措施是可靠的认证机制。您可能会遇到这样的情况：当设备连接到互联网没有进行任何身份验证。

这就为攻击者的伪装铺平了道路。如果验证缺失成为一种普遍现象，攻击者可以利用这

一点禁用数百万台设备。如果一台连接了数百万机器的服务器被感染，这种攻击将会特别危险。

为了阻止入侵，我们必须引入可靠的安全证书生命周期管理，并规范安全系统的代码库。这将有助于减少攻击向量。

当然，保护物联网仍然是一个艰巨的任务，目前业界正在朝这个方向摸索。目前，网络犯罪分子只是在衡量和评估新市场的风险、机会和潜在的盈利能力。

同时，制造商和用户也不太在意可能的威胁。也许，在经历一次成功的物联网勒索攻击后，人们的态度会迅速转变。希望我们有时间做准备。