精译版

医疗机构面临勒索软件和物联网威胁

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	Healthcare challenges: Ransomware and the Internet of Things are		
原文作者	Lysa Myers	**原文发布日期**	2017 年 4 月 7 日
作者简介	Lysa Myers 是 ESET 安全研究员。 https://www.linkedin.com/in/lysamyers/		
原文发布单位	We Live Security		
原文出处	https://www.welivesecurity.com/2017/04/07/healthcare-challenges-ransomware-internet-things-tip-iceberg/		
译者	安天技术公益翻译组	**校对者**	安天技术公益翻译组
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。		

医疗机构面临勒索软件和物联网威胁

2015 年，Anthem 和 Premera 入侵事件使得公众更加意识到医疗护理机构安全的重要性。虽然 2016 年大规模医疗入侵案件渐少，但这并不意味着问题已得到解决。事实上，2016 年大量勒索软件攻击了各行各业，医疗设施是此类威胁尤为喜爱的攻击目标。医疗设施加上联网医疗设备和健身追踪器激增表明，未来医疗护理很可能继续面临巨大的挑战。

勒索软件只是冰山一角

有人可能认为勒索软件激增是勒索软件时兴问题。虽然造成了巨大的麻烦和钱财损失，但勒索软件泛滥只是冰山一角。勒索软件一般可以按照终端和网络最小威胁安全方法减少此类威胁。事实上，安全专家在发现第一个勒索软件变种之后，可能不怎么重视。因为它能被轻易阻止，甚至恶意软件文件本身在执行之前也无法检测到。受害者只需恢复备份就可应对赎金问题。

除非涉及实际、现实世界防护，用户执行的安全措施通常与安全部门所希望的不一致。安全措施刚开始可能给人这样一种印象，备份恢复似乎比同意支付勒索赎金所付出的代价更大。而有些公司可能根本不经常备份，且检测恶意邮件、文件、链接或流量的安全产品也配置不当或缺失。另外，由于备份方法不当使得备份在应对勒索攻击或其它威胁时极其脆弱。如果有的用户觉得这些防护措施妨碍工作，甚至可能关闭或绕开安全产品。

不管根本原因是什么，但最终结果是受影响的企业可能决定必须向罪犯支付以期取回丢失的数据。而在医疗护理行业，快速获取数据事关生死，其被勒索软件攻击的代价被急剧放大。

罪犯很清楚这一点，故意攻击医疗机构。要逆转这一趋势看似简单实则艰难。但通过在关键地方设置坚实的安全基础，我们能够减少未来恶意软件威胁和新技术风险带来的双重影响。

评估和修复风险的重要性

我们已在 WeLiveSecurity 网站上探讨过医疗护理机构进行风险评估的重要性。通过经常性的资产和数据传输方法分类，可以准确的找出可能存在漏洞和风险的地方。在考虑可能的风险成本时，就能明白哪些事情应最先解决。

就勒索软件来说，有几种风险评估方法可以帮助解决这一情况：

- 什么资产存在被勒索软件加密的风险？
- 勒索软件是使用什么传输方法进入你方网络？
- 威胁是通过什么方式接收指令、加密文件？

不幸地是，几乎所有可以通过计算机或互联网访问数据和系统的资产都存在被加密的风险。勒索软件攻击通常来自于通过网络钓鱼邮件下载的恶意文件 其中包含恶意文件或连接。因此，这种情况下需要考虑的传输方式是邮件，重点关注社会工程学技术。恶意软件一般需要调到 C2 途径接收指令，因此很多变种通过 HTTP 或 HTTPS 等常用协议进行。

减少风险的方法有很多，例如：

- 经常备份，一旦系统或网络受到影响，找出一种能最有效减少损失的方法在。
- 网络隔离可以限制计算机系统上恶意软件的影响。
- 过滤垃圾和网络钓鱼邮件以及拦击恶意软件作者常用的文件类型，可以帮助减少恶意软件不断攻击用户的风险。
- 提前培训用户通常可以减少执行恶意软件的几率。
- 鼓励用户向 IT 或安全人员提交可疑邮件或文件，可以提高过滤效果。
- 如果恶意软件成功绕过第一层防御，在网关、网络或终端部署反恶意软件可以帮助

识别和预防恶意软件进入网络或减少造成的损失。

- 防火墙和入侵防御软件可以识别未知和不需要的网络流量。这些措施不仅能减少勒索软件的风险，还能减少各类其它攻击类型的概率。全面评估风险并提高机构的整体安全态势可以极大的减少各类安全入侵的频率和严重性。

医疗和健身设备

随着医疗护理行业越来越计算机化，更多的医疗护理从业人员和患者都在使用医疗和健身设备。这些设备通常充满敏感信息，而这些设备首要考虑的不是安全和隐私问题。

据我们观察的勒索软件发展趋势，没有坚实的安全基础，非常敏感的信息可能出现重大的问题。但因为这一技术还相对较新，现在把重心放在如何确保这些设备的安全上正是好时候。

医疗网络中的设备

医院网络使用的医疗设备都非常大且非常昂贵，其运行的操作系统很普通、过于老旧（例如 Windows XP Embedded）。通过这些设备可以轻易的访问医院所有的网络，其中存储着各种敏感信息：例如，金融账单信息、保险识别信息以及患者访问产生的相关医疗信息。

从罪犯的角度看，仅医疗数据这一笔数据的价值——可能是信用卡或借记卡资料价值的 9 倍之多。且医院的医疗台式机通常使用相似的操作系统，因此可以使用同一技术确保其

安全。虽然设备使用的的操作系统严重过时（可能不支持），因此必须重视提供额外的保护。可行做法是确保机器完全断开所有的网络连接，但仍需注意移动媒体传播威胁。

家中的医疗设备和追踪器

家中使用的医疗设备和追踪器一般比较小，因此穿戴或植入都不会太显眼。大多数设备使用专用或 Linux 操作系统，可以连到网络或与手机设备或台式机同步。与医院设备一样，如果可能的话，这些设备也尽可能少更新。

患者家中的医疗设备通常不会存储支付卡信息，但存储的其它信息可能被罪犯找到用于盗窃或修改，诸如邮件地址、用户名和密码、GPS 数据包括家里或工作地址。另外，还可能显示用户什么时候不在家或在睡觉。针对植入医疗设备的攻击使得罪犯做出各种更改、发出指示措施，这可能造成严重（甚至致命）的医疗问题。

个人医疗设备最重要的是防止机器被用于伤害用户或侵入隐私。针对能够连网的胰岛素泵或心脏起搏器的攻击自然与健身追踪器不同。保护这些设备的安全措施也应当一样，虽然胰岛素泵和心脏起搏器可能需要更严格的默认设置。

确保医疗设备的安全

个人和医院医疗设备制造商在设计阶段之初就有机会进行改变，全面考虑提供更好的安全设计。设备制造商可以做很多事情使得设备更安全：

- 隐私设计——学习隐私设计七大原则。
- 加密数据——当经邮件、网页或 IM 发送或与用户计算机同步时，用强加密保护磁盘和传输数据。
- 讲明数据存储选项——给用户存储本地路径信息的能力而不只是云存储。
- 验证账户访问——确认用户身份。在允许查看、分享或修改植入设备上的信息之前，验证尤为重要，因为滥用的后果非常的高。对线上账户访问提供多重验证。
- 创建自动防护保险状态——防止错误和故障发生。设备必须默认保持访问重要功能的状态，当出现问题时不会危及用户。
- 假设代码可能被恶意使用——合法代码可能强制设备执行未验证的代码。处理错误时考虑可能出现的问题以便设备不会被恶意使用，这非常重要。
- 做好漏洞准备——建立并公开发布一份漏洞报告关于泄露信息的责任条款。
- 做好入侵准备——创建事件响应方案以便可以在数据入侵发生时反应得当。在紧急事件发生时，这不仅节约了时间、还能言辞得当。
- 做好政府审查的准备——FTC 和 FDA 都在密切注视医疗设备，因此做出改变可以避免法律问题和高额罚款。在可预见的未来，医疗护理行业安全问题很可能成为公众的焦点。虽然当前存在问题，但仍存在做出重大转变的机会作为其它行业积极变革的模式，因为物联网已走进了家庭和工作区域。