简译版

防御勒索软件攻击的五种方法

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	5 Steps to Protect Against Ransomware Attacks		
原文作者	AJ Nash	原文发布日期	2019 年 10 月 15 日
作者简介	AJ Nash 是 Anomali 网络情报战略总监。https://www.darkreading.com/author-bio.asp?author_id=5297		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/5-steps-to-protect-against-ransomware-attacks/a/d-id/1336039		
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。		

防御勒索软件攻击的五种方法

AJ Nash

2019 年 10 月 15 日

安全专家强烈建议不要支付赎金。那么，你应该如何保护企业呢？

由于以下几个关键因素，勒索软件对所有联网企业构成了越来越大的威胁。首先，勒索软件在暗网上的购买成本低廉，因此攻击者的进入壁垒非常低。其次，勒索软件通常通过电子邮件进行传播，这种传播方式成本很低（甚至是零成本），可用于针对性攻击或随机攻击。最后，勒索软件利用了网络安全最薄弱的环节：人。

最近，在亚特兰大、巴尔的摩以及德克萨斯州发生的攻击事件表明，勒索软件对州和地方政府造成了灾难性的破坏。

- 2018 年，亚特兰大遭到勒索软件攻击，攻击者索要约 5 万美元的赎金，造成的损失超过 260 万美元。
- 2019 年，巴尔的摩遭到勒索软件攻击，攻击者索要 13 比特币（约合 7.5 万美元）的赎金，造成的损失超过 1800 万美元。
- 在得克萨斯州，大规模勒索软件攻击影响了 22 个城市的计算机系统，一位市长证实攻击者索要 250 万美元的赎金。

尽管在每次攻击中使用的勒索软件不同，但是这些攻击有一个共同点：预期受害者没有做好响应的准备。

虽然勒索软件攻击持续增加，但大多数安全专家和 FBI 强烈反对受害者支付赎金，原因是：A）支付赎金并不能保证系统或数据的恢复；B）支付赎金很有可能使受害者再次沦为攻击目标。

如何应对勒索软件攻击

如果企业不愿支付赎金，那么该如何减小勒索软件攻击的影响呢？以下五种最佳实践可以极大地降低遭受攻击的可能性，更重要的是，可以在发生勒索软件攻击时大大降低攻击影响。

1. 资产识别和管理。拥有最新的配置管理数据库和高价值资产评估系统（CJA）至关重要（CJA 用于确定对完成企业任务至关重要的网络资产）。攻击者通常针对最有价值、最脆弱的系统和数据发起攻击，因此企业要从攻击者的角度审查其环境。

2. 补丁管理。如果企业了解其环境后未采取保护措施，那么了解环境也没什么意义了。大多数攻击并未利用多高级的“零日”漏洞。攻击者经常重用旧漏洞——他们乐意利用旧漏洞来攻击新目标。典型的例子是“心脏滴血”（Heartbleed）漏洞：受害企业未安装该漏洞的补丁，使攻击者得以利用这个已有五年历史的漏洞（CVE-2014-0160）执行攻击。因此，请及时打补丁，勿成为易攻击的目标！

3. 威胁情报。大多数网络安全企业主要关注内部，但从被动转变为主动的唯一方法是获取情报。了解威胁趋势和态势（包括攻击者、战术、技术和规程）的网络安全专家能够利用这些知识来防止攻击。

4. 自动化。企业经常被海量数据、信息和情报所淹没。考虑到安全行业面临的技能差距，安全人员几乎没有足够的时间来解决所有关键或高风险安全事件，更不用说中等和低风险事件了。通过自动化技术，机器可以利用高保真情报自动采取行动，无需人工干预。只有这样，网络防御者才能专注于影响最大的安全问题。

5. 培训。无论是在物理世界还是网络空间中，“人”仍然是最薄弱的一环。强大的培训计划会将奖励和再培训结合起来，帮助员工警惕经常导致勒索软件攻击的网络钓鱼活动。

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，始终坚持自主先进的能力导向，依托下一代威胁检测引擎等先进技术和赛博超脑大平台工程能力积累，研发智甲、探海、镇关、捕风、追影、拓痕等系列产品，为客户构建端点防护、流量监测、边界防护、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的有机结合，协助客户开展深度结合与全面覆盖的体系化网络安全规划与建设，支撑起协同联动的实战化运行，赋能客户筑起可对抗高级威胁的网络安全防线。

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企业、IT 企业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、超过十五亿部智能终端设备提供了安全检测能力。安天的移动检测引擎获得国际知名测试机构颁发的 2013 年度权威评测奖项。

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（如 APT 组织）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，通过深度分析高级网空威胁行为体的作业能力，安天建立了以实战化对抗场景为导向的能力体系。

安天被行业管理机构、客户和伙伴广泛认可，已连续六届蝉联国家级安全应急支撑单位，是中国国家信息安全漏洞库六家首批一级支撑单位之一，亦是国家网络与信息安全信息通报机制技术支撑单位，国家信息安全漏洞共享平台成员单位。

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