

简译版

## 从勒索软件检测转向预防

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	Shifting From Ransomware Detection to Prevention		
原文作者	Lorielle Paulk	原文发布日期	2019 年 11 月 18 日
作者简介	Lorielle Paulk 是 X-Force IRIS 产品营销经理。 <a href="https://securityintelligence.com/author/lorielle-paulk/">https://securityintelligence.com/author/lorielle-paulk/</a>		
原文发布单位	Security Intelligence		
原文出处	<a href="https://securityintelligence.com/posts/shifting-from-ransomware-detection-to-prevention/">https://securityintelligence.com/posts/shifting-from-ransomware-detection-to-prevention/</a>		
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 <a href="https://bbs.antiy.cn">bbs.antiy.cn</a> 安天公益翻译板块		
免责声明	<ul style="list-style-type: none"> <li>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。</li> <li>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。</li> <li>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。</li> <li>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。</li> </ul>		

## 从勒索软件检测转向预防

Lorielle Paulk

2019 年 11 月 18 日

想象一下：你在过去的一个月中不懈努力，为你最好的朋友制作了婚宴致敬视频。你添加了正确的图片，配上了应景的音乐，并对视频进行了完美编辑，希望能够创建美好的回忆。从选择理想的场地到选择精美的菜品，这对新婚夫妇确保已照顾好每一个细节。你的致敬视频将会“锦上添花”，为他们的婚宴画下完美的句点。

视频制作完成后，你保存了视频文件，想要站起来歇口气。此时，电脑屏幕上弹出了一条奇怪的消息：“此笔记本电脑上的文件已被加密。请在 48 小时之内支付赎金，否则你的文件将被销毁！”完美的一天急转直下——你遭到了勒索软件攻击。

现在，我们可以想象，在工作中被相同的恶意软件感染是多么容易。企业可能会遇到类似的情况——但是，他们面临的风险会更大。勒索软件攻击可能会破坏业务运营，使公司遭受数小时甚至数天的停机，并可能导致业务完全停滞。

那么，企业应如何防止勒索软件攻击呢？防止勒索软件攻击并非易事，但企业可以采取一些措施来降低机会性攻击的风险。在企业策略小组（ESG）最近的一项研究《事件准备就绪趋势：信心水平是否与准备工作相符》中，80%的网络安全决策者表示其企业已经在实施勒索软件“事件准备就绪”（incident readiness）活动，以确保攻击发生时有相应的应对计划。

如果企业环境中已经存在勒索软件，企业可以采取一些补救措施。对公司网络的勒索软件攻击可能会影响成千上万的设备，成本高昂，而且一定会干扰业务运行。建议企业参考下述建议，以了解其安全团队可以采取哪些措施来减轻攻击风险。如果企业采取这些措施，就可以更好地从勒索软件检测转向事件准备就绪和响应。

### 创建安全意识文化

勒索软件是一种恶意软件，可能会因人为错误而广泛传播。例如，员工可能会沦为社会工程手段的目标，被诱骗打开恶意电子邮件。通过培训员工或用户，帮助其识别可疑电子邮件，企业可以显著降低勒索软件感染的可能性。

## 确保有备份

防御勒索软件的一贯措施包括备份,而且不只是一个备份。如果攻击影响了企业的业务,则进行备份(离线备份和云中备份)并对备份进行定期测试,可以帮助企业恢复数据。

企业应定期进行备份,并采用经过测试的恢复过程。备份数据的公司可以最大程度地减少勒索软件攻击的影响,因为他们仅丢失了数小时而非数月或数年的数据。此外,企业还应定期测试备份,以确保备份可以将所有文件和资产配置恢复到未感染状态。

## 嵌入威胁情报

通过监控企业网络,企业可以从另一个角度审视其安全环境。但是,监控技术和工具的有效性取决于企业向其提供的信息。如果企业想要更好地发现迫在眉睫的勒索软件攻击,了解勒索软件的发展动态,以及了解防止此类感染蔓延的最新策略,则拥有最新的威胁情报至关重要。

没有什么“魔术策略”或一次性解决方案可以阻止当今的威胁。企业可能会采取一切可能的预防措施来阻止勒索软件访问其网络,但是这些措施可能无法完全阻止威胁。因此,对于当今的企业及其安全团队而言,采取主动措施及时检测勒索软件,对其进行遏制,管理事件响应并制定恢复计划至关重要。这些总体性策略有助于大大减少勒索软件攻击对业务的潜在影响。

## 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 endpoint 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,截止到 2019 年 9 月 30 日,安天的威胁检测引擎为全球超过六十万台网络设备和网络安全设备、超过十七亿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>