勒索软件觊觎备份：四种保护方法

简译版

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	Ransomware Will Target Backups: 4 Ways to Protect Your Data		
原文作者	Rod Mathews	**原文发布日期**	2017 年 10 月 4 日
作者简介	Rod Mathews 担任 Barracuda 副总裁兼数据保护业务总经理。 https://www.darkreading.com/author-bio.asp?author_id=4825		
原文发布单位	Dark Reading		
原文出处	https://www.darkreading.com/endpoint/ransomware-will-target-backups-4-ways-to-protect-your-data/a/d-id/1330029?		
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。		

勒索软件觊觎备份：四种保护方法

Rod Mathews

2017 年 10 月 4 日

备份是防御勒索攻击的最佳方式，但它们也需要保护。

今年勒索软件来势凶猛。保守估计，WannaCry 和 NotPetya 两起重大攻击造成了数亿美元的损失，而网络犯罪分子则继续瞄准用户的系统和数据。

然而，主动的公司确实有选择权。防御勒索软件的最佳方法是备份数据并设置经过充分测试的恢复过程。定期备份数据并能够快速检测勒索软件的公司能够在最短的时间内恢复数据和运作。

在某些情况下，擦除程序伪装为勒索软件（如 NotPetya 伪装为 Petya 勒索软件），给出类似的赎金要求。在这些攻击中，即使受害者支付赎金也无法取回文件，此时从备份中恢复数据就更加重要了。

因此，勒索软件背后的网络犯罪分子开始瞄准备份过程和工具。一些勒索软件，如最近的 WannaCry（WannaCrypt0r）和较新版本的 CryptoLocker，删除了微软 Windows 操作系统创建的卷影副本。卷影副本是 Windows 系统提供的一种可以轻松恢复数据的方法。

在 Mac 系统上，网络犯罪分子从一开始就瞄准了备份。研究人员在 2015 年发布的第一个 Mac 勒索软件中发现了不完整的功能，它针对 Mac OS X 操作系统的自动备份工具 Time Machine 所使用的磁盘。

该策略很简单：加密备份，个人或公司就很可能会失去恢复数据的能力，更有可能支付赎金。攻击者已经不满足于感染单个工作站，他们不断升级攻击力度，旨在摧毁备份。

以下四个建议可以帮助企业保护其备份免受勒索攻击。

1.谨慎使用网络文件服务器和网络共享服务

网络文件服务器使用简单，它的两个属性使得可以通过网络访问的“home”目录成为

集中数据并轻松备份的热门方式。但是，当暴露于勒索软件面前时，这种数据架构存在严重的安全漏洞。大多数勒索程序加密连网的磁盘，因此受害者的 home 目录也将被加密。另外，运行像 Windows 这样存在漏洞且经常被攻击的操作系统的任何服务器都可能被感染，这将导致每个用户的数据都被加密。

因此，任何拥有网络文件服务器的公司都需要将数据备份到单独的系统或服务中，并测试系统的恢复能力。

云文件服务也无法免疫勒索攻击。2015 年，一家为儿童演员及其父母提供信息的公司 Children in Film 遭到勒索攻击。该公司广泛使用云服务，包括一个常见的云盘。根据 KrebsOnSecurity 网站的一篇文章，在一名员工点击恶意电子邮件链接的 30 分钟内，存储在云盘中的 4000 多个文件被加密了。幸运的是，该公司的备份提供商能够恢复所有的文件，虽然恢复过程花费了将近一个星期。

根据云服务是否提供增量备份或容易管理的文件历史记录，恢复云中的数据可能会比恢复现场服务器中的数据更加困难。

2.实现备份过程的可视化

公司越早发现勒索软件感染，就越有可能防止重大的数据损坏。备份过程的数据可以提供勒索软件感染的预警。突然加密数据的程序会在备份日志中留下痕迹。随着每个文件的本质改变，增量备份将会突然“爆炸”，而且加密的文件不能被压缩或重名剔除。

定期（基本上是每天）监控重要的指标，如备份过程中的空间利用率，可以帮助公司检测勒索软件是否已经感染了公司内部的系统，并降低感染损害。

3.考虑解决方案

如果勒索软件能够直接访问备份映像，那么阻止它加密公司备份将非常困难。因此，一个提取备份数据的专用备份系统将能够防止勒索软件加密历史数据。

通过将备份与正常操作环境分离并确保备份过程不在通用服务器和操作系统上运行，您的备份可以有效防御攻击。基于最常用的操作系统（微软 Windows）的备份系统容易受到攻击，使得企业更难保护备份数据。

4.定期测试恢复过程

最后，除非您可以快速可靠地恢复数据，否则备份也不是什么好办法。一些勒索攻击的受害者已经备份了数据，但是仍然不得不支付赎金，这是因为他们的备份计划不够细粒度，或者他们错误地认为已经备份了某些数据。

测试恢复过程的一部分是确定数据丢失的窗口。如果一家公司每周进行一次完整备份，那么他们最多丢失一周的数据。每天或每小时进行一次备份能够大大提高保护水平。更精细的备份和及时检测勒索软件是防止损坏的关键。

最后，公司应该通过监控或反恶意软件防御措施尽早发现勒索攻击，使用专门的系统来分离备份数据和潜在受感染系统，并定期测试备份和恢复过程，以确保数据受到妥善的保护。