白皮书

勒索软件恢复与文件共享完全指南

BlackBerry Workspaces

日益肆虐的企业勒索软件

在现代办公日益呈现分布式和数字化的今天，企业文件同步和共享（EFSS）解决方案可使组织轻松实现安全有效的信息共享。但这类解决方案同时也存在漏洞，让伺机攻击企业的网络攻击者有机可乘，因为他们知道企业拥有大量有价值的数据，并且更有可能为摆脱麻烦而支付“赎金”。

问题在于，满足攻击者的要求只是从勒索软件攻击中恢复的第一步。对于一套理想的 EFSS 解决方案，如果要在受到攻击后进行快速恢复，需要能够让系统管理员将情况掌握在其手中，通过识别任何受感染的文件，让管理员能够把文件恢复到受感染之前的干净版本。

本白皮书概述了勒索软件的潜在影响，以及在选择企业文件同步和共享解决方案时，选择可降低风险、成本和恢复时间，同时可防止业务生产力损失和宕机的解决方案的重要性。

勒索软件攻击是2017年最普遍的一种恶意软件活动。[1]

什么是勒索软件？

勒索软件是一种恶意软件，旨在通过诱使用户打开损坏的电子邮件附件或链接来攻击设备，之后锁定或加密其文件，直到用户支付赎金为止。赎金通常以比特币这样的加密货币进行支付，一旦支付赎金，受害者就会收到加密密钥来解锁他们的文件。然而不幸的是，即使用户或其组织决定遵照攻击者的要求，也无法保证文件不会受到损坏。

在许多情况下，组织会遭到网络钓鱼或鱼叉式网络钓鱼的蓄意攻击，攻击者会将恶意和欺诈性电子邮件发送到一个或多个公司电子邮件账户，通常伪装成账单、运单及其他和发票相关的消息。[2] 例如，一名首席财务官可能会收到来自可信赖的供应商的一封电子邮件，希望该公司通过像 DocuSign 这样的流行支付网站进行付款，但当他点击链接时，他很快发现他已经打开了执行勒索软件程序的恶意链接，在措手不及的情况下，为避免造成重大的损失，他需要立刻找出办法阻止勒索软件的传播。

勒索软件为何如此猖獗？

虽然勒索软件早在十多年前就已出现，但如今依然是最猖獗的攻击方式之一，原因主要有两点：

1. **易于执行**

   经验老道的攻击者不断在强化他们的攻击技能，同时寻找新的方式绕过传统的防御方法。此外，“勒索软件即服务”（RaaS）模式的兴起让那些网络犯罪新手仅凭最基本的技术知识就可以发起针对性的攻击。[3] Cerber 是一种比较典型的 RaaS 软件，已成为目前分布最广泛的 RaaS 软件包之一，占2016年12月至2017年1月勒索软件活动的25%。[4]

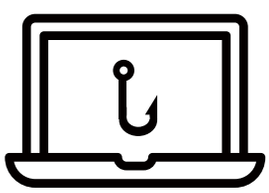
2. **高得手率**

   为避免攻击所造成的不利影响，许多组织选择支付赎金，希望以此拿回那些有价值的数据。有些企业甚至通过存储比特币以备“不时之需”。这会令问题永久化，让攻击者能够在将来有能力再次攻击这些组织，或继续瞄准类似的公司。

与任何其他恶意软件一样，勒索软件可以传播，使得员工无意的失误可能会转变为组织范围的危机，令组织的关键业务运营瘫痪甚至终结。

网络钓鱼与鱼叉式网络钓鱼

虽然两者都是最普遍的攻击方式，但网络钓鱼和鱼叉式网络钓鱼的攻击方式显著不同。前者通过广泛撒网，以期击中不幸的受害者。后者则通过狡猾的伪装，有针对性的攻击目标。



网络钓鱼

网络钓鱼攻击旨在诱骗操作者点击恶意链接或附件或者诱使其访问恶意网站。

鱼叉式网络钓鱼

鱼叉式网络钓鱼是一种更具针对性的网络钓鱼形式，由其发出的电子邮件通过伪装，好似是由收件人认识和信任的人员（如同事或业务合作伙伴）发送的，并且会包含专门针对受害者的兴趣或行业定制的内容。[5]

EFSS 如何使问题变得更复杂

通过横跨多个端点同步和共享受勒索软件影响的文件，企业文件同步和共享（EFSS）解决方案有可能会令勒索软件的破坏性更大。无论何时，当创建或保存新版本的文件，大多数EFSS解决方案都会自动将文件从用户设备同步到中央（云）存储库。如果某个文件与其他用户共享，系统还会将最新版本同步到其设备。

当某个文件被勒索软件加密时，系统会创建一个新版本。该新版本将同步到中央存储库以及（通过EFSS）与受勒索软件影响的用户共享文件的任何用户的设备上。由于该文件已经加密，因此无法再从中央存储库或跨端点访问该文件。

能够让组织横跨多个设备和最终用户安全地存储、访问和共享文件的企业文件同步和共享（EFSS）解决方案。

充分考虑自身所处的危险

从小型企业到大型企业，所有组织都应当关注勒索软件攻击的频率和严重程度。2016年，勒索软件攻击的数量增加了两倍，从当年第一季度的每两分钟一次攻击跳升至第三季度的每40秒一次。[6] 虽然没有可以绝对免疫的企业，但与其他行业相比，有些行业更容易成为攻击的目标。

以医疗卫生行业为例，预计到2020年，勒索软件攻击将增加400%。[7] 2017年5月，包括许多英国国家医疗服务体系（National Health Service）在内的两多万个系统受到 WannaCry 的攻击，凸显了导致该行业大面积受到攻击的一些可能的重大系统漏洞，其中包括：

- 患者健康信息（PHI）的数字化
- 对风险的容忍度低（危及患者生命）
- 大量相互连接的端点和技术
- 对网络安全技术的投入不足[8]

然而，医疗卫生行业并不是唯一易受影响的目标。事实上，教育、IT / 电信、娱乐 / 媒体和金融服务领域超过20%的组织也曾遭受过攻击。[9] 下面列出的攻击表明，部分被高度锁定的行业在遭到公开攻击后，所受的影响深远。

受勒索软件攻击的企业中，有近60%拥有100名以上的员工，有25%拥有1000名以上的员工。[10]

主要勒索软件一览

- WannaCry：2017年5月，利用 Windows 漏洞针对包括医疗卫生在内的各行业企业实施攻击
- Locky：2016年2月，通过凶猛的网络钓鱼活动同时利用 Dridex 基础设施进行传播
- TeslaCrypt：2015年2月，以电脑游戏文件为目标，要求以比特币换取解密密钥
- SimpleLocker：2014年末，该锁屏恶意软件通过提供新应用程序的垃圾邮件感染安卓系统（Android）用户
- CryptoLocker：2013年8月，使用公共和私人加密密钥锁定和解锁受害者的文件[13]

公共部门也未能免于勒索软件的攻击。在2018年3月22日，亚特兰大的全市系统遭到勒索软件攻击，攻击者锁定文件并要求当局支付价值约50,000美元的比特币赎金。在袭击发生后的几天里，亚特兰大居民无法进行日常的公共支付，例如支付停车罚单或公用事业账单，并且该市的公务员在五天之后才解除威胁，可以打开电脑。袭击事件发生后，亚特兰大警察局长透露，网络攻击毁掉了警方多年保存的行车记录视频资料。[11]

2017年1月至3月，勒索软件的新型变种数量达到2016年同期的4.3倍。[12]

即使像金融服务业这样受到严格监管的行业，在整体对网络安全技术进行大量投入的情况下，依然不断成为勒索软件攻击的目标，并促使美国证券交易委员会（SEC）于2018年提高了对网络安全的要求。

勒索软件导致成本高昂的后果

攻击的潜在影响远远超出最初的赎金支付。无论组织是否选择支付赎金，响应、修复和恢复所涉及的成本都会陡增。

考虑以下后果及其对企业盈亏的影响：

- **经济损失：**
  除最初的赎金支付外，组织还可能因事件响应、补救措施和监管罚款而产生额外费用。

- **生产力受损：**
  在几分钟内，组织可能会失掉数小时、数周甚至数年的工作。加之恢复文件或对损失的工作重做一遍作所需耗费的时间和资源，其对成本造成的影响将是巨大的。

- **日常业务运营中断：**
  在删除受感染的文件并将其恢复为干净版本期间，勒索软件攻击可能会冻结公司的 IT 系统，这可能会扰乱那些维持业务平稳运行的项目和日常任务。

- **声誉受损：**
  当遭遇攻击成为头条新闻时，受影响的组织有可能很快会失去通过苦心经营建立起的声誉。当遭受攻击的消息公之于众时，企业的股票价格、品牌价值和竞争优势都会受到打击。

- **客户和合作伙伴流失：**
  客户和合作伙伴希望他们宝贵的数据都得到谨慎的处理。在他们的信心受到动摇的那一刻，流失客户和合作伙伴的风险就会提高。

至2019年，勒索软件造成的损失预计将达到115亿美元[14]

未雨绸缪

尽管教育和预防非常重要，但哪怕最强大的防御也难以抵御每一次袭击。因此，通过实施计划及一整套工具使组织能够从攻击中快速、有效地恢复，其重要性不言而喻。

业务连续性计划包括组织在应对业务和/或其员工的潜在威胁时将采取的预防性和恢复性措施，其中包括对勒索软件等网络攻击的预防和恢复。拥有主动解决方案，将使 IT 管理员能够快速采取行动应对威胁，同时使员工保持工作效率。

应用场景： EFSS勒索软件恢复解决方案

Bob 是一家专门从事并购的大型金融服务公司的职员。出于工作性质，Bob 会定期以 MS Office 文件的形式处理任务关键型知识产权和客户信息，所有这些文件都会定期保存到他的桌面上。Bob 还会将他的文件同步至公司的 EFSS 解决方案，以便与其他团队成员协作。以上是 Bob 和其同事的常规操作。

一天，Bob 在电子邮件中点击了一个看似无害的链接。很快，他意识到自己已成为勒索软件攻击的目标。他的所有桌面文件都已加密，无法访问，他无法完成日常任务，措不及手地寻找解决方案。

然而不幸的是，对于 Bob 来说，其团队对云协作的依赖加剧问题的严重性。他很快发现，受感染的桌面文件已同步到云端，加密后的文件不仅仅 Bob 无法访问，任何与他人共享这些文件的人员都无法访问，更糟糕的是，这些受感染的文件已同步至所有同事的设备中。该团队的项目由数千个文件组成，由于勒索软件的潜在传播迫在眉睫，一切工作戛然而止。

Andy 在该公司的 IT 部门工作。他的工作是支持关键业务运营和最终用户，确保所有系统和技术顺利运行。在其身处的行业，时间就是金钱，生产力受损将造成巨大的损失。

当天，Andy 接到了一线用户支持团队的紧急电话。他向 Bob 提出一系列问题，以便确定 Bob 发现问题的第一时间。之后，Andy 才能够确定攻击的时间并展开工作。

一般 EFSS 解决方案的恢复办法

如果该公司使用一般 EFSS 解决方案，则 Andy 必须采取以下步骤。

1. Andy 通过执行系统报告来识别受感染的文件，查看 Bob 在计算机受感染时上传了哪些文件。

2. Andy 对每个文件进行检查，手动将受感染的文件逐个恢复到最后一次干净版本。由于勒索软件攻击已经扩散到多个端点，因此 Andy 必须对所有受影响的用户重复此操作。

3. 或者，Andy 可以委托专人编写一个自定义脚本，通过 API 恢复文件。

该解决方案要求 Andy 花费大量时间来检查每个文件，并将受感染的文件恢复到干净状态。不难想像，Andy 为每个可能已被感染的设备完成这一过程需要耗费的时间。在 Andy 解决问题这一期间内，Bob 和他的同事将无法访问完成日常任务所需的文件。即使 Andy 选择通过自定义脚本恢复文件，找到专人编写并执行该脚本也可能是一项既耗时又存在潜在风险的尝试。

使用 BlackBerry Workspaces 的恢复办法

以下是 Andy 使用 BlackBerry® Workspaces 中包含的 Ransomware Recovery 功能执行的恢复步骤：

1. Andy 要求 Bob 通过 Workspaces 桌面插件确定他桌面中的哪些工作区在从他的桌面进行同步。

2. 在某些情况下，恶意软件攻击还可能导致 Bob 失去对本地系统的访问权限。在这种情况下，Andy 可以从 Workspaces 管理控制台查看用户日志，以确定 Bob 与其桌面同步的工作区以及已同步到任何共享工作区的受感染文件。

3. 必要时，Andy 可暂时锁定 Bob 的账户，防止进一步的系统中断。

4. 一旦确定 Bob 所属的工作空间，Andy 就会指定用户，需要恢复的日期和时间，以及出现问题的工作空间（用户界面仅显示允许用户访问的工作空间）。

5. 通过恢复功能，Andy 将受影响的文件恢复为文件的干净版本（基于指定的日期和时间），该版本在勒索软件攻击发生之前为当前版本。如果存在仅具有单个版本的文件，则这些文件将保持不变。

6. 通过将干净版本转为文件的当前版本，Andy 可确保将干净版本同步到系统中并推送给与 Bob 共享文件的所有用户，从而有效消除整个网络中勒索软件加密版本的文件。

借助 Workspaces，Andy 能够以一系列简洁的步骤，通过隔离 Bob 的账户并对任何受感染文件恢复到干净版本来识别和恢复 Bob 的文件，然后将其同步到所有其他用户的账户。Andy 不需要逐个手动还原文件或在多个设备上重复这些步骤，从而为他节省了大量时间，并允许整个公司的其他用户在恢复过程中继续工作。

> 当安全性成为企业的高优先级事项时，负责安全和风险管理的企业管理者应该为他们需要支持的每一个平台寻求一流的解决方案。[15]

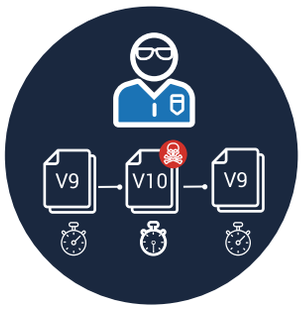
Gartner

*Gartner，《高安全性移动设备管理关键能力》（Critical Capabilities for High-Security Mobility Management），John Girard，DionisioZumerle，Rob Smith，2017年8月24日。

勒索软件恢复工作原理

1 识别受影响的用户，通过 Workspaces 桌面插件为他们提供从桌面同步的工作区列表。如果用户无法执行此操作，管理员可在 Workspaces 管理控制台中检查用户日志，以确定受影响的工作区、文件夹和文件。

2 必要时，管理员可临时锁定受影响的用户。



3 管理员可对勒索软件刚刚进行攻击前的用户、日期和时间进行指定。只需单击一个按钮，管理员就可将所有受影响的文件回退到勒索软件攻击前的最新版本。之后，指定日期和时间的文件版本将得到还原。在指定时间之后未更新的文件将不受影响。用户权限将与之前的“当前版本”保持一致。这一操作仅适用于指定用户最后一次更新的文件。由指定用户以外的其他用户更新的文件将无法还原。

4 之后，文件的干净版本将自动同步到共享工作区的所有用户，从而有效清除网络中的受损文件。

5 管理员在清除威胁后解锁用户。如果管理员选择擦除该用户的系统，则在实施恢复后，Workspaces 会将所有文件的干净版本重新同步至其设备。

通过 BlackBerry Workspaces 减少风险、损失和恢复时间

针对勒索软件攻击，采取多层次的防御措施才是上策，其中包括强大的防火墙、电子邮件安全和最终用户培训。然而，即使采取了最佳预防措施，攻击依然不可避免，且一旦受到攻击通常都会遭到破坏。在遭遇破坏的情况下，BlackBerry Workspaces 提供了一种独特的解决方案，使组织能够快速有效地做出响应，同时将攻击对业务的干扰降至最低。

通过以下勒索软件恢复功能，企业可获得更好的效果：

- 快速控制和限制受感染文件的传播。
- 快速将工具交给管理员，以便对勒索软件攻击进行响应并从中恢复，由此可以迅速恢复业务。
- 通过粒度控制，可有选择地将受影响的用户、文件和文件夹回退到攻击前的版本，从而消除由系统范围的回退和恢复机制造成的工作和生产力损失。
- 无需高级支持或服务提供商的协助。管理员可调用 BlackBerry Workspaces 的勒索软件恢复工具，让他们在攻击发生后立即恢复系统。

结语

简言之，任何拥有大量有价值数据且对宕机时间具有低容忍度的组织都会成为网络攻击者的主要目标。因此，组织必须确保他们拥有多层次的防御模式以及企业技术堆栈，因为这些措施在设计之初已对不可避免的漏洞进行了充分考量。

对攻击做好应对准备的 EFSS 解决方案可使系统管理员快速识别和隔离受感染的文件，并通过若干简单步骤将其还原为干净版本，使攻击不会对业务造成任何重大干扰，企业得以继续运营，员工可以继续协作，同时能够避免因重大财务或声誉损失造成的影响。

关于 BlackBerry

BlackBerry 是一家专注于保护和管理物联网终端的企业软件和服务公司。公司通过端到端企业物联网 (Enterprise of Things) 平台 BlackBerry® Secure™（该平台由企业通信和协作软件以及经过安全认证的嵌入式解决方案组成）实现这一目标。

欲了解更多信息，请访问 www.blackberry.com

资料来源：

1. https://www.verizonenterprise.com/verizon-insights-lab/dbir/
2. https://www.csoonline.com/article/3077434/security/93-of-phishing-emails-are-now-ransomware.html
3. https://blog.barkly.com/ransomware-statistics-2017
4. https://blog.barkly.com/cerber-ransomware-statistics-2017
5. https://www.wired.com/2015/04/hacker-lexicon-spear-phishing/
6. https://blog.barkly.com/ransomware-statistics-2017
7. https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/
8. https://healthitsecurity.com/news/hipaa-data-breaches-cyber-attacks-reported-by-47-of-orgs
9. https://blog.barkly.com/ransomware-statistics-2017
10. https://www.prnewswire.com/news-releases/report-identifies-ransomwares-biggest-cost-to-be-business-downtime-300236505.html
11. https://techcrunch.com/2018/06/06/atlanta-cyberattack-atlanta-information-management/
12. https://blog.barkly.com/ransomware-statistics-2017
13. https://www.csoonline.com/article/3212260/ransomware/the-5-biggest-ransomware-attacks-of-the-last-5-years.html
14. https://www.csoonline.com/article/3237674/ransomware/ransomware-damage-costs-predicted-to-hit-115b-by-2019.html
15. https://www.gartner.com/doc/3799963/critical-capabilities-content-collaboration-platforms