BlackBerry
Intelligent Security. Everywhere.

白皮书

阻止勒索软件并非不可能

简介

勒索软件是一种恶意软件，它会加密文件，禁止受害者访问其系统和数据。几乎在所有情况下，只有通过恢复备份副本或从勒索软件威胁犯罪分子处购买解密密钥，才能恢复文件。如果受害者没有及时响应勒索要求，攻击者可能会增加勒索金额或删除解密密钥，从而使文件彻底无法访问。

尽管执法部门建议受害者不要答应勒索要求，但许多公司还是会根据其业务受损程度、对客户和股东的潜在影响、恢复和清理的相对成本，以及风险暴露使他们可能受到的监管处罚或品牌/声誉的受损程度来支付勒索金额。

如今，对于民族国家网络攻击者和网络犯罪组织而言，勒索软件是其主要收入来源，占所有恶意软件相关安全事件的 27%[1]。请看以下这组令人担忧的统计数据：

- 截至 2021 年底，每 11 秒就会有一次针对企业的勒索软件攻击[2]。每 40 秒，就会有一次攻击成功[3]。
- 在《2020 年网络威胁防御报告》[4]的受访组织中，有 62% 表示他们曾经是勒索软件的受害者。其中 58% 的公司选择支付勒索金额，比前一年增加了 13%。

勒索软件作为网络武器

在《BlackBerry Cylance 2020 年威胁报告》中，BlackBerry 研究和情报部门注意到威胁制造者开展勒索软件活动的方式出现了许多关键趋势。其中最主要的是在具有高度针对性的攻击中使用勒索软件，例如利用 Sodinokibi、Ryuk 和 Zeppelin[5] 勒索软件系列的攻击。

这一趋势首先随着 WannaCry 在 2017 年的爆发而受到公众的广泛关注[6]。短暂式微后，勒索软件卷土重来，意欲报仇。过去，勒索软件攻击都是针对个人用户和中小型企业的、以获利为驱动力的网络犯罪。但是最近，BlackBerry 的研究和情报部门发现大公司、公共机构和政府被勒索软件攻击的案例大幅增加。

1 《Verizon 2020 年数据泄露调查报告》
2 《全球勒索软件损害成本到 2021 年预计将达 200 亿美元》
3 《营造网络安全文化意味着什么》
4 《2020 年网络威胁防御报告》
5 《BlackBerry 2020 年威胁报告》
6 《WannaCry、Petya、NotPetya：勒索软件如何在 2017 年兴风作浪》

在一些最复杂的情况下，攻击者会精心选择受害者，并实施周全的侦察以找到最佳入侵方式。一旦获取受害者网络环境的访问权限，攻击者首先会部署窃取信息的恶意软件，并在加密文件之前泄露敏感数据[7]。如果受影响的公司拒绝为获得解密工具交纳赎金，攻击者将会试图通过威胁公布窃取到的信息，对其进行勒索。这些信息通常包含公司客户的个人数据，因此这种行为构成泄露数据隐私。在 BlackBerry® 安全产品和服务检测到或应对的攻击中，约有 10% 利用了这种策略[8]。Maze 勒索软件集团就是最近的一个例子[9]。

虽然网络钓鱼仍然是最常见的攻击媒介，但威胁制造者也利用策略、技术和程序 (TTP)，使得受害者无需点击恶意链接或打开武器化文档即会被感染。例如，BlackBerry® 安全服务事件响应团队已经注意到多起攻击者攻击运行已弃用软件的 VPN 的实例。其他攻击者则利用无文件攻击（如 Cobalt Strike），通过向正在运行的进程中注入恶意代码来控制存在漏洞的系统。此类基于内存的攻击旨在打败传统的反病毒产品，后者依靠文件签名匹配和启发技术来保护终端。

一经得逞，攻击者可以安装连接到命令和控制 (C2) 服务器的后门、修改系统注册表以保持持久性，并加载有助于网络侦察、凭证窃取和横向移动的工具。只有在找到并入侵有意攻击的所有目标后，攻击者才会部署并引爆勒索软件。

发动有针对性的勒索软件攻击的幕后黑手往往会重复使用已知的恶意软件系列。其中许多软件都在地下论坛出售，或者是从勒索软件即服务 (RaaS) 供应商处购买。大多数情况下，其目的就是敲诈。然而，一些勒索软件攻击意在通过破坏重要数据来中断流程和服务，或者利用有缺陷的支付基础设施和/或加密例程，致使无法解密文件或支持赎金支付。

剖析复杂勒索软件攻击

Ryuk 最早于 2018[10] 年 8 月被发现，是与某臭名昭著的俄罗斯网络犯罪集团有关联的勒索软件，根据联邦调查局[11] 的数据显示，在 2018 年 2 月至 2019[12] 年 10 月期间，该集团从受害者那里勒索到超过 6,100 万美元的比特币付款。

在 2019 年 6 月的国家网络安全中心 (NCSC) 咨询中，Ryuk 也被标记为全球威胁[13]。作者提到，在获取访问权限后，该组织通常会花费数天到数月的时间进行侦察，然后再放置和引爆 Ryuk。然而，在某些情况下，Ryuk 则会以闪电战的形式发起攻击。一个广为人知的例子是最近对 Universal Health Services (UHS) 的攻击，这是一家位列财富 500 强的医院和医疗服务提供商，每年治疗约 350 万患者。

---

7 《勒索软件如今的另一大特点 —— 在加密数据之前窃取数据》
8 《威胁公告：勒索软件 2020 年最新情况》
9 《勒索软件团伙现将曝光不付清赎金的受害企业》
10 CISA 警报 (AA20-302A)《针对医疗保健和公共卫生部门的勒索软件活动》
11 勒索软件的受害者每月要支付数百万美元赎金。有一个版本让他们付出了最大的代价
12 RSA 演示文稿：《Feds 抗击勒索软件：FBI 如何调查以及您如何提供帮助》
13 《Ryuk 勒索软件瞄准全球各家组织》

Bleeping Computer[14] 于 2020 年 9 月 28 日首次报道了这次攻击。在最初感染的五个小时内，该公司在美国各地的数百家医疗机构，包括加利福尼亚州、佛罗里达州、德克萨斯州、亚利桑那州和华盛顿特区的医疗机构，均无法访问其计算机和电话系统。因此，UHS 的员工被迫推迟病人的预约，在某些情况下，将急诊室的病人转到其他可用设施[15]。

攻击发生后，DFIR Report[16] 的分析人员对攻击链进行了如下重建：

1. 最初的感染是由一个网络钓鱼漏洞造成的，该漏洞将 BazarLoader 恶意软件放在受害者电脑上。Bazar 是由 TrickBot 团伙[17] 开发的一种木马，能够利用代码签名证书和各种混淆技术来避免被检测到[18]。
2. 安装后，该恶意软件会创建一个与幕后团伙的 C2 服务器的后门连接，并开始使用合法的 Windows 工具（如 NItest[19]，一种生成域服务器列表的微软 Windows 服务器命令行工具）来映射 UHS 网络。
3. 在找到 UHS 主域服务器后，攻击者利用 Zerologon 获得了管理员权限，这是一个在选定的微软 Windows 服务器操作系统中发现的权限升级漏洞，在通用漏洞评分系统中被评为关键（10.0 分）[20]。
4. 接下来，Ryuk 团伙利用服务器信息块 (SMB) 文件传输和窗口管理工具 (WMI) 执行来部署 Cobalt Strike 工具包。这使他们能够定位，然后横向移动到二级域控制器，在那里他们继续用 PowerShell Active Directory 脚本进行域发现。
5. 现在，在确定域名服务器和数据存储目标后，攻击者利用同样的技术获得了对二级域名服务器的管理员控制权。
6. 在完成侦察并锁定目标后，攻击者利用 RDP 将 Ryuk 可执行文件放入主 DNS 服务器、网络存储设备和员工工作站。最后一步是执行 Ryuk 勒索软件。

14 《Ryuk 勒索软件对全美境内的 UHS 医院发动攻击》
15 《美国一家大型连锁医院遭到勒索软件攻击》
16 《感染 Ryuk 之后的 5 个小时》
17 《BazarBackdoor：TrickBot 团伙的全新隐蔽性网络黑客恶意软件》
18 《前门入侵 BazarBackdoor：隐蔽的网络犯罪武器》
19 《微软命令行参考》
20 NIST 国家漏洞数据库《CVE-2020-1472 详细信息》

具有安全意识的企业应该如何应对？

我们先从安全意识强的组织不应该做的事情开始；不应在可能已经过度复杂而无法管理的安全基础设施上再增加安全层。过多的安全控制措施会产生适得其反的效果，即降低而不是加强组织的网络弹性。根据 IBM 的一份安全报告显示[21]，近 30% 的受访企业部署了 50 个或更多安全工具。与拥有较少工具的同行相比，这些组织在检测攻击的能力方面排名低了 8%，在事件响应 (IR) 的能力方面低了 7%。

部分原因是警报疲劳，部分原因是终端和其他网络设备产生的大量遥测和事件数据的结果。分析师如何有效地梳理这些数据，从日常活动的随机噪声中检测出威胁的微妙信号？

因此，应该等到业务和安全领导团队对组织的网络风险暴露和风险容忍度有了全面的了解之后，再进行新的投资。

开始规划和评估

BlackBerry 专家通常建议客户从妥协评估 (CA) 开始。这有助于识别风险因素，并建立一个评估未来安全升级的基线。CA 应解决威胁搜寻和减少攻击面这两个领域，重点关注：

- 数据泄露和破坏
- 命令与控制活动
- 用户帐户异常情况
- 恶意软件和持久性机制
- 易受攻击的网络、主机和应用程序配置

应与客户的安全和业务领导团队一起查看 CA 的调查结果和建议。

- **威胁搜寻结果：**如果检测到过去或当前的威胁情况，则应详细说明性质、范围和对网络环境的影响。
- **攻击面减少结果：**这些建议应包括改善组织整体安全态势的策略和战术建议，以及对减少攻击面机会的风险优先级评估。例如，CA 应该标记具有关键漏洞的系统，如 Zerologon，并提供改善这些漏洞的分步说明。

21 《2020 年网络弹性组织报告》

据 IBM[22] 称，如今“绝大多数”组织都未准备好有效应对严重安全事件。根据 2020 年[23] 的一项调查显示，IBM 发现企业平均需要 315 天来识别和控制由恶意攻击造成的数据泄露。缩短此类应对时间对运营弹性至关重要。同时也对盈利有所助益。与那些需要更长时间的组织相比，在不到 200 天内解决事件的组织平均成本节约 112 万美元[24]。

为了解决上述问题，BlackBerry 建议客户正式评估其防御团队识别、遏制、消除和恢复安全漏洞的能力。调查过程应包括员工面访、安全策略差距分析，以及对防御团队在定制事件响应 (IR) 演习中的表现进行评估。基于这些结果，应重新审视 IR 计划，以确保其符合行业最佳实践和监管标准。

进行此类评估很重要，但它们不能替代在现实世界的真实攻击场景中测试防御团队的能力。例如，BlackBerry 安全服务可同时提供泄漏模拟和对手模拟服务，以满足不同客户的需求。泄露模拟很适合那些希望锻炼其防御能力、验证安全假设并查找安全态势中差距的组织。为了有效应对威胁幕后黑手团伙对自身行业发起的主动攻击，组织希望能够获得现实世界中攻击检测和应对的相关经验，对手模拟就是一个很好的选择。

有关 BlackBerry 安全服务产品组合的详细信息，请访问我们的网站。

利用 BlackBerry Protect 预防勒索软件事件的发生

防止勒索软件事件发生的最有效方法是阻止攻击者通过恶意脚本，利用系统漏洞或者利用恶意软件在受害者的计算机上存放勒索软件。BlackBerry® Protect 是一款终端保护平台 (EPP) 解决方案，利用复杂的人工智能 (AI) 和机器学习 (ML) 技术来阻止这两种策略。

BlackBerry Protect 利用 BlackBerry 统一的敏捷代理技术在终端部署，可在几毫秒内确定文件是否可以安全运行。如果可以安全运行，则允许执行文件。如果不可以安全运行，就会阻止执行，文件会被隔离，并在 BlackBerry® Cyber Suite 管理控制台显示一组警报和上下文数据。此文件检测过程在每个终端上独立进行，消耗的系统资源最少，无需查询远程数据库、安装持续的更新或连接到云端。BlackBerry Protect AI 模型可检测并防止恶意软件和勒索软件在开放和隔离的网络中执行。

22 IBM 研究：《半数以上拥有网络安全事件应对计划的组织未对自己的计划进行测试》
23 《IBM 2020 年数据泄露安全成本报告》
24 《IBM 2020 年数据泄露安全成本报告》

除了防止恶意文件执行，BlackBerry Protect 还通过监控所有 32 位和 64 位运行进程中与常见漏洞有关的行为，防止威胁制造者在系统内存中注入和执行恶意代码。如果检测到内存违规行为，BlackBerry Protect 会拦截所产生的函数调用，以此采取纠正措施，然后再允许执行函数。这些纠正措施包括从忽略违规行为和允许执行到完全终止该进程。这些功能可以防止威胁制造者利用恶意软件（如 Bazar）劫持合法的系统服务来实现其目标。

BlackBerry Protect 还可以防止执行恶意的 PowerShell、活动脚本和 Microsoft Office 宏脚本，如 UHS 威胁制造者使用的相关脚本。通常，脚本控制策略最初设置为警报模式，这样管理员就可以确定正在使用哪些脚本、谁在使用，以及是否应该允许运行以及在什么条件下允许运行。完成清单后，就可以启用阻止模式，从而阻止所有脚本运行，安装在指定文件夹中或在排除规则中明确提到名字的脚本除外。

勒索软件也可以通过被入侵的大容量存储设备侵入网络。BlackBerry Protect 设备控制策略通过防止员工安装未经授权的软件、泄露数据或无意中用被感染的设备损害业务系统，将这种风险降到最低。BlackBerry Protect 设备控制策略仅适用于大容量存储设备。鼠标和键盘等外围设备不受影响。

利用 BlackBerry Protect 应用程序控制，企业能够通过防止威胁制造者安装恶意软件或修改操作系统、固件、网络堆栈和支持应用程序，让固定功能设备持续保持在良好状态。

利用 BlackBerry Optics 技术进行勒索软件威胁的搜寻、补救和恢复

如果 BlackBerry Protect 在阻止勒索软件攻击方面如此有效，那么为什么还需要 BlackBerry® Optics 这样的终端检测与响应 (EDR) 解决方案呢？

首先，也是最明显的原因是，100% 的恶意软件防范效力与 BlackBerry Protect 可以实现超过 99% 的效力[25] 之间，尽管很微小但仍然存在可见差异。因此，更为谨慎的做法是构建一套系统，可以控制并促进对突破第一道防线的勒索软件攻击的调查。

第二个因素是威胁环境的性质在不断变化。Verizon 在《2020 年数据泄露调查报告》[26] 中评估了威胁制造者使用的策略，并得出结论：“过去五年中，恶意软件在泄露事件中的比例一直在持续稳定下降”，报告还指出：“45% 的攻击是黑客攻击，22% 的泄露事件由错误引起，22% 包括社交攻击，17% 涉及恶意软件。”这并不意味着恶意软件作为一种攻击载体正在消失，只是对手越来越多地使用那些不需要使用可移植可执行文件的 TTP，至少在攻击链的初始阶段如此。

25 NSS Labs 高级终端保护 Cylance 安全价值图，2018 年 4 月
26 《2020 年数据泄露调查报告》

BlackBerry Optics 是一款 EDR 解决方案，通过提供真正的 AI 事件预防、根本原因分析、智能威胁搜索和自动检测与响应能力，扩展了 BlackBerry Protect 提供的威胁防护能力。与其他 EDR 产品不同，BlackBerry Optics 不需要对企业内部基础设施进行大量投资，也不需要依赖连续向云端传输数据的反应式方法。相反，BlackBerry Optics 在终端应用检测和响应逻辑，消除了响应延迟，而这种延迟的消除，可能就会使一个重大的失控安全事件降级为小的安全事件。

为了检测勒索软件威胁，BlackBerry Optics 整合了上下文分析引擎 (CAE)，可以近乎实时地监控终端事件，以识别恶意或可疑活动。CAE 附带有 BlackBerry 策划的一组预先打包好的检测逻辑，可以启动无数次应对。这包括 BlackBerry 事件响应团队在现场调查和解决实际攻击得出的规则，以及 BlackBerry 威胁研究人员解构和记录的攻击。例如，BlackBerry 的威胁研究部门已经编写了定制版 BlackBerry Optics 规则，对 Ryuk 恶意软件变种所使用的技术进行标记并实施风险缓解[27]。

尽管检测规则是必要的，但它们不能为每一种攻击行为建立模型。因此，BlackBerry Optics 还包括由 BlackBerry 数据科学团队开发的机器学习威胁检测模块，可持续分析终端活动，以检测零时差、APT 和离地攻击，就像最精明的勒索软件威胁团伙所进行的攻击。

只要触发 CAE 规则或机器学习检测，BlackBerry Optics 就会提供按需和自动响应。这些措施包括收集取证数据、关闭系统网络，以及执行调查和解决勒索软件爆发所需的其他功能。

一旦检测到事故，就必须进行彻底调查，以确保在随后的控制和恢复工作中了解和说明攻击链的所有阶段。BlackBerry Optics 包括手动和自动事件调查工具，使分析师能够有效地寻找威胁并进行根本原因分析。

例如，BlackBerry Optics 使安全团队能够通过 InstaQuery (IQ) 搜索收集取证相关数据，从而简化威胁搜索过程。IQ 是一款轻型工具，可以从任何终端收集数据，汇总结果，然后以上下文和直观的格式呈现以进行分析。

BlackBerry 顾问最近利用 IQ 帮助一家大型企业调查并补救了一次勒索软件爆发。在几秒钟内，该团队确定，主要的 IOC（即勒索软件的文件扩展）只存在于美国。这使客户和 BlackBerry 团队能够将他们的调查、补救和清理工作集中在那里，而不必额外花费时间来评估客户在欧洲、亚洲和南太平洋的运营环境。BlackBerry 公司的顾问还协助客户防止进一步感染，创建和分发定制规则，确保即时检测并隔离勒索软件。

27 《Ryuk 恶意软件 Optics 规则》

BlackBerry 勒索软件防护方法的优势

BlackBerry 的勒索软件和服务解决方案组合可帮助企业：

- 防止勒索软件执行或利用合法的系统服务，来获得立足点并开始横向移动。
- 通过部署自动检测、响应和修复规程，帮助主动寻找威胁和根本原因源分析，阻止勒索软件造成损害。
- 快速响应勒索软件事件。中级供应商或大型咨询公司应对漏洞所需的等待时间可能会持续数周，导致损害扩散，并增大了恢复和清理成本。BlackBerry 勒索软件专家可随时为您提供始终如一的优质服务。
- CISO 和安全团队获得所需的专家指导和支持，以确定和消除安全结构中的差距，加强网络防御，实施强大的事件响应流程，并从被动反应有效过渡到主动预防的安全防控，最大限度减少风险暴露。

结语

我们可以在多大程度上得出结论，勒索软件事件真的可以预防？这在很大程度上取决于公司的预防理念。如果您认为这意味着有一个神奇的开关，可以关闭勒索软件的攻击，那么很遗憾，您可能会大失所望。然而，BlackBerry 的观点是，如果采取切实可行的措施来击败勒索软件，几乎所有的勒索软件攻击都可以在攻击链的最后攻击阶段被阻止。

这始于对计算基础设施的彻底评估，以识别和优先处理网络风险。系统如果存在众所周知的漏洞，则应进行修补，以避免被利用。这同样适用于系统配置错误。例如，应禁用对 RDP 系统的外部访问，以防止 BlueKeep 漏洞攻击[28]。

不应忽略基本的阻止和处理。员工需要持续接受培训来抵制社交工程攻击。应该通过实施多重身份和持续身份验证技术来加强低强度密码策略。企业还必须充分致力于持续的安全评估，以确定新出现的威胁，以及数字化转型项目如何使其面临新型的网络风险。这些举措需要长期努力，以此产生长期效益。

28 NIST 漏洞数据库 CVE-2019-0708

不过，仍然有一些措施可以帮助企业速战速决，并且立竿见影。BlackBerry Protect 可以检测并阻止勒索软件以及勒索软件威胁制造者用来获得初始立足点的无文件技术。在阻止复杂攻击方面，人工智能和机器学习发挥着重大作用，使一切变得不同。如果攻击以某种方式穿过组织的防线，BlackBerry Optics 就会介入，启动自动响应和补救程序，防止安全漏洞成为普遍的安全事件。

因此，防范勒索软件不仅是可能的，而且也是实际可行的。

了解更多关于 BlackBerry 的勒索软件预防和修复解决方案组合，或致电 +1-888-808-3119 以获得即时援助。

欲了解更多 BlackBerry 关于阻止勒索软件的观点和资源，请访问我们的网站。

关于 BlackBerry

BlackBerry 公司（NYSE：BB；TSX：BB）致力于为世界各地的企业和政府机构提供智能安全软件和服务。今天，公司为超过 5 亿台终端提供安全保障，包括 1.75 亿辆上路行驶的汽车。公司总部位于安大略省滑铁卢，运用人工智能 (AI) 和机器学习，在网络安全、安全和数据隐私领域提供创新解决方案，并且也是终端安全管理、加密和嵌入式系统领域的领军企业。BlackBerry 的愿景明确清晰，就是要打造值得信任的、安全的互联未来。

如需了解更多信息，请访问 BlackBerry.com 并关注 @BlackBerry。

BlackBerry
Intelligent Security. Everywhere.

MKTG 19-0108 | 210920