思科勒索软件防御：让勒索软件无路可走

如果您想要与勒索软件保持安全距离，而它却要尝试入侵该怎么办？只有思科能够为您提供恰当的安全产品和架构。

概述

文件和信息是组织的命脉。要掌握这些信息并保证组织的生产率，就必须彻底保证信息的完整性和安全性。

但会有勒索软件、恶意软件或代码锁定个人或组织计算机上的信息，如文档、照片和音乐等。用户必须支付费用（或赎金）才能解密并赎回这些文件。如果没有适当的防御，勒索软件可造成巨大的损害，使组织沦落到用纸笔操作。

勒索软件通常通过漏洞攻击包、恶意广告（网站上提供恶意软件的受感染广告）、网络钓鱼（冒充为可信来源的欺骗性邮件）或垃圾邮件活动来进行传播。只要人们在网络钓鱼邮件中点击一个链接或附件，就会开始感染行为。当用户浏览的站点包含可自动感染计算机的恶意广告时，也会发生感染。

进入思科® 勒索软件防御。采用分层方法降低勒索软件感染的风险，从 DNS 层、终端、网络、邮件和 Web 为您提供全方位保护。我们利用架构性方法来提供集成防御，兼具终极可视性和勒索软件终极响应速度。

优势

- **降低勒索软件的风险**，免除后顾之忧，让您专注于业务运营
- **获得即时安全保护**，在威胁尝试植入前进行阻止
- 从架构性方法**获得出色的可视性和响应速度**，从 DNS 层、网络到终端全方位保护
- 强大的网络分段，**防止恶意软件横向扩散**
- **获得业界一流的 Talos 勒索软件威胁研究**和情报

急剧增长的强大威胁

今年是勒索软件爆发年。且事实证明，勒索软件可以给攻击者带来极高的非法获利，已迅速成为目前获利最丰厚的恶意软件类型之一。

据 FBI 报告，勒索软件每年可获得将近 10 亿美元的非法收入。思科 Talos 研究表明，单个勒索软件活动每年就可以非法获利 6000 万美元。勒索软件目前深受关注，甚至已经成为广播电视节目中的热点话题。

攻击者拥有足够的资金和动力来不断创新勒索软件链条，从而增强勒索软件破坏力。我们认为勒索软件的自我传播能力将会继续增强，目标就是锁定庞大的公司网络。结果会使公司 IT 功能倒退到 20 世纪 70 年代。

当前针对勒索软件的响应趋于围绕单点产品解决方案。由于勒索软件会采用不同的媒介感染目标，我们必须考虑一种更为架构性的方法。

这种整体性解决方案可全面应对攻击者使用的各种媒介和方法。防御者必须保护邮件和网络安全，阻止对互联网恶意基础设施的访问，阻止任何设法潜入终端的勒索软件文件，阻止使用命令与控制回调，并在感染发生时轻松阻止勒索软件的横向扩散。

购买内容

思科勒索软件防御整合了思科安全架构中所有必要的部分，以应对勒索软件挑战。您可以选择所有产品或者选择满足即时安全需求的部分。

勒索软件防御包括：

- 思科 Umbrella，在 DNS 层阻止威胁和勒索软件，使其远离您的网络
- 面向终端的思科高级恶意软件防护 (AMP)，阻止恶意勒索文件在终端上运行

- 思科邮件安全（包括云和内部设备），阻止网络钓鱼和垃圾消息伺机传播勒索软件
- 高级恶意软件防护可通过静态和动态分析（沙盒处理）遍历思科邮件安全网关未知附件的简单许可，即刻添加到邮件安全产品中
- 思科 Firepower™ 下一代防火墙 (NGFW)，阻止遍历网络的命令与控制流量以及任何恶意文件
- 思科 ISE 通过思科网络对您的网络进行动态分段，从而防止勒索软件横向扩散

借助勒索软件防御，组织可以将其网络作为执行器，以遏制勒索软件传播。这样，勒索软件在最糟糕的感染情况下也不会轻而易举地进行传播。

思科安全服务可在攻击爆发后的事件响应中提供即时分类。还可简化 AMP、NGFW 及其他解决方案产品的部署。

主要功能

- 阻止勒索软件进入网络或下载到笔记本电脑
- 如果已进入网络，在最糟糕的情况遏制勒索软件

安全服务帮助抵制勒索软件

思科安全服务事件响应团队可以在勒索软件爆发时，同时提供就绪事件响应服务和被动事件响应服务。

此外，思科安全集成服务可应对解决方案级别的架构挑战，还可简化解决方案技术的部署，如面向终端的 AMP 和思科 FirePOWER NGFW。我们的团队在集成安全解决方案方面拥有雄厚的专业知识，可以加快必要安全技术的采用并减少对业务的破坏。

通常，组织还必须确保拥有适当的数据备份技术和策略，以缓解勒索软件入侵的影响。

“我们解决了勒索软件 Web 攻击媒介中的一个巨大风险，显著提高了用户在网络连接方面的体验。”

– Octapharma

思科 Capital

提供融资服务，助您实现目标

思科 Capital® 融资可以帮助您获得所需的技术，实现目标和保持竞争力。我们可以帮助您减少资本支出、加速业务发展并优化投资和回报。借助思科 Capital 融资服务，您在购买硬件、软件、服务和第三方补充设备时将拥有更多灵活性。思科 Capital 可以为您提供一种可预测的支付方式。思科 Capital 现已在 100 多个国家/地区推出。了解详情。

思科优势

勒索软件将设法以各种必要的方式潜入您的组织。需要防御许多媒介，包括网络钓鱼邮件、有漏洞的 Web 横幅和垃圾邮件等。只有思科的安全架构能够应对勒索软件挑战。单点产品孤掌难鸣。我们的解决方案由业界一流的 Talos 研究小组支持，他们已开展了广泛的勒索软件威胁相关研究，可完美助力我们的高效分层保护方案。我们将阻止勒索软件入侵，一旦有漏网之鱼侥幸入侵您的网络，我们将立即采取应对措施。

C22-737492-01 08/16