打破勒索软件杀伤链

阻止横向移动的五个步骤

勒索软件并不是通过入侵单台机器或设备来实现传播。网络犯罪分子利用这种恶意软件，加密网络中尽可能多的内容，并确保受害者支付赎金。

每 2 秒一次

到 2031 年，预计每 2 秒钟就会有一家企业、一位消费者或一台设备受到勒索软件的攻击。

《Cybersecurity Ventures 勒索软件市场报告》

您对自己的当前网络安全状况有信心吗?

如果您仍然依靠传统防火墙来执行分段，则无法阻止勒索软件在您的网络中传播，也无法阻止其锁定关键应用程序及基础架构。

勒索软件杀伤链

1. **初始立足点**
   （鱼叉式）网络钓鱼或易受攻击的服务
2. **横向移动**
   在整个网络中传播，尽可能扩大影响
3. **渗漏式攻击**
   寻找并窃取有价值的数据
4. **加密**
   使用 PKI 实施加密，以防止破解
5. **赎金通知**
   壁纸、电子邮件、赎金 txt 文件等
6. **影响**
   数据、财务、品牌等

入侵活动不可避免

您需要一套安全解决方案，以检测东西向数据中心流量中的威胁并阻止横向移动。

打破杀伤链

准备： 识别您的 IT 环境中运行的每个应用程序和资产

预防： 创建规则，以阻止常见的勒索软件传播技术

检测： 接收警报，确保及时得知访问分段应用程序与备份的企图

补救： 启动线程控制和隔离措施，在检测到攻击时立即采取行动

恢复： 借助监测能力，支持分阶段恢复策略

2022 年，勒索软件攻击增加了接近 13%，这一增幅相当于过去五年的总和。

《Verizon 2022 数据泄漏调查报告》

如果您不希望疲于应对更频繁的攻击，不想应付数目更大的赎金要求，那么现在就该将分段和监测功能纳入自己的防御策略了。

了解更多

支持 | 发布时间：2023 年 5 月