AKAMAI 客户案例

安全漏洞修复公司利用 Akamai 产品来应对勒索软件攻击并实施恢复措施

全面的网络监测能力

跨 IT 基础架构的分段

对勒索软件威胁的响应

客户

在发生了一次重大安全事件之后，某家全球设备制造商聘请了一家美国的安全漏洞修复服务公司。

挑战

快速传播的勒索软件

在遭受了一次影响业务运营的恶意软件攻击之后，这家全球制造商开始与安全漏洞修复服务公司合作，以恢复并增强其环境的安全性。这次攻击发端于一位员工的笔记本电脑，在快速传播之后影响了该企业的大多数运营场所，还入侵了该企业的备份服务器。

选择解决方案

最初的遏制方法包括在防火墙中应用互联网访问限制，但这样的方法速度缓慢，无法控制住迅速扩大的入侵行为。在分散式企业中，受到环境复杂性与网络实际情况的限制，利用防火墙实施和执行限制规则变得缓慢而无效。

此外，对于负责调查和遏制入侵的事件响应人员来说，对传统机器的监测能力也是一大问题。鉴于事态紧急，并且需要在横向传播影响更多资产前加快实施分段，这家安全漏洞修复服务提供商建议使用 Akamai Guardicore Segmentation。

Breach Remediation Company

行业
信息技术

解决方案
Akamai Guardicore Segmentation

重要影响
- 减少勒索软件通过横向移动实现的传播
- 提供网络流量的精细监测能力
- 保护现代和传统机器
- 实现快速事件响应

Akamai

Akamai Guardicore Segmentation 的优势

即时监测

在不到三个小时的时间里，这家安全漏洞修复服务企业迅速在超过 3,000 台公司服务器上配置了 Akamai 代理。而在部署完成后的数分钟内，对网络和通信流的高精度监测功能便开始发挥作用，为事件响应团队提供了调查攻击行为和验证控制措施所需的背景信息及数据。

快速制定策略

在实现急需的监测能力后，各团队很快采取措施，将关键资产与外部更广泛的环境分隔开来。他们迅速确定了在唯一一条正常运转的生产线上运行的两个关键生产级应用程序，并采取了保护措施。利用 Akamai Guardicore Segmentation，他们立即引入了一项策略来限制已感染的子网和数据中心部件与这两个应用程序的连接。这是一项非常耗时的任务，如果是采用传统防火墙，可能需要几个星期才能完成。

另外，在进行简单的查询后，他们发现连接到互联网的传统机器绕过了传统防火墙，试图反制限制措施。发现不合规的通信后，该团队几分钟内便制定出多项策略，有效地限制了包括传统机器在内的所有服务器对互联网的访问。

防止在恢复过程中发生横向移动

在恢复过程的下一个阶段中，该团队重新创建了此制造商的应用程序集群，并在其中内置了 Akamai 代理。他们配置了一项阻止所有传入连接的初始策略，并使用 Akamai Guardicore Segmentation 确定依赖关系。这样，只有在确认需求并了解背景信息后，才会将确实需要建立连接的通信加入允许列表。借助此方法，该团队恢复了受勒索软件攻击影响的应用程序并让它们重新上线，还避免了再次感染的风险。

未来的保护

利用 Akamai Guardicore Segmentation，这家安全漏洞修复服务公司能够向其客户（也就是那家制造商）展示重大的附加价值，同时帮助他们从勒索软件攻击中迅速恢复。这让该服务公司有机会增加收入、扩大业务覆盖范围，并且更好地帮助客户实现 IT 和安全目标。

在分阶段恢复期间引入的内部数据中心分段显著缩小了攻击面。现在，该企业的安全态势已得到改善，并大大降低了今后再发生入侵可能造成的影响。

请访问 akamai.com/guardicore 以了解更多信息。

> [Akamai] 使我们可以在四小时内阻止攻击传播，并在一个未遭到入侵的网段中恢复瘫痪的生产线，而且不需要对任何底层网络做出修改。在此过程中，我们还持续进行了 IR 调查，并对攻击进行控制。
>
> 安全漏洞修复公司的首席信息安全官