Akamai 客户案例

亚洲领先电信公司保护 API 免遭威胁

公司监测并保护其资产中的每个 API

随着移动设备的激增，亚洲各地的电信行业正在大力投资于新技术的开发和网络的扩展，以满足客户对更出色数字服务的需求。在幕后，API 将：

- 提供电信行业转型所需的连接，同时加速 DevOps 团队的流程
- 作为基础，向整个大陆的客户提供移动电话服务、互联网接入和其他电信产品
- 能够提供更加个性化的解决方案并最终改善客户体验

该地区一家领先的电信公司也看到了 API 带来的巨大机遇，特别是在提供全新数字语音和数据解决方案方面。伴随 5G 时代来临，该公司不再局限于电话业务，而是将目光投向了大数据、AI、物联网和其他新兴数字应用领域。不过该公司也明白，API 在数量激增的同时，也带来更多的风险。在目睹其他大型电信提供商在 2022 年和 2023 年遭受 API 攻击的影响后，该公司与 Noname Security（现已被 Akamai 收购）开展了合作。

Telecommunications Company

位置

亚洲

行业

网络运营商

解决方案

Akamai API Security

Akamai

需要监测所有 API 及其风险

与许多企业一样，缺乏对 API 及其风险的监测能力是安全团队面临的普遍挑战。我们的研究表明，仅四成掌握了完整 API 清单的企业知道哪些 API 会返回敏感数据。借助 API 安全解决方案的“发现”模块，我们确定了我们的电信客户也遇到了类似的挑战。

在与 Akamai 合作之前，客户的 API 安全控制部分主要由传统 API 管理平台和 Web 应用程序防火墙 (WAF) 组成。从应用程序安全和 API 交付的角度来看，这种安排十分合理。然而，这两种解决方案都未能提供高级别的安全控制措施和可观察性，以全面保护 API 免受当今攻击方法的威胁。一个关键原因是：并非所有 API 都通过 WAF 或 API 网关一类的代理进行路由，这些不受管理的 API 就成为了对恶意攻击者极具吸引力的目标。

但即使对 API 清单进行了精确审核，该公司仍需要能够在 API 操作和管理请求的正常运行过程中确保 API 安全。显而易见，靠企业安全团队手动识别环境中的恶意行为是不可行的。

需要实时保护的 API 端点即便没有上千，也有数百个。常用的 AppSec 解决方案通常无法及时跟踪客户环境中的每次 API 调用，在缺乏适当的 API 运行时保护功能的情况下，这可能会使公司的 IT 环境极易遭受网络攻击。

监测每个 API 并防范 API 威胁的解决方案

项目的第一阶段需要进行试点部署，以查找公司的内部 API，评估配置，并了解流经 API 的数据类型。其发现 API 的速度，掌握的 API 清单的准确程度，以及工具识别敏感数据泄露的能力很快就给客户留下印象深刻。

由于试点工作取得的积极成果，客户随后将 Noname API Security Platform（现为 Akamai API Security 的一部分）的覆盖范围扩展到其整个内部和外部 API 资产。这项工作还揭示了更多隐藏的生产 API，并暴露出环境面临的一些迫在眉睫的威胁。

我们发现，客户需要更强大的防御措施来抵御重大安全漏洞，保护他们的 API 免遭未来攻击。部署 Akamai API Security 后，客户现在可以实时检测可疑行为异常并触发事件响应方案。这使得企业可不必再依赖延后的报告和访问日志，获取启动补救过程的通知。Akamai API Security 一旦检测到可疑行为，就会报告给客户的 API 网关、SIEM 系统和其他信息安全引擎，进而通知整个安全团队。客户可以选择让员工以手动、半自动或全自动方式修复问题，具体取决于应用场景和漏洞的严重程度。