LexisNexis®
RISK SOLUTIONS

案例研究

LexisNexis® Risk Solutions 帮助大型金融机构抑制恶意软件攻击，减少欺诈损失

LexisNexis® ThreatMetrix®数字身份情报能够在不影响用户体验的同时近实时地检测高风险事件

概览

公司

一家大型金融机构

要求

- 防止利用远程访问软件潜入可信用户账户进行有针对性的社会工程攻击。
- 抑制恶意软件攻击。
- 限制登录和支付时的欺诈事件。
- 减少诈骗损失。

解决方案

LexisNexis Risk Solutions 对端到端的在线会话（包括账户注册、登录、变更详情和偏好设置、账户导航、创建新受益人和支付剖析）实施全面的、近实时的行为剖析，以检测恶意软件或远程访问软件非法用户的异常情况。从而大大减少欺诈，同时维护可信客户的无摩擦体验。

结果

- 在短时间内阻止了有针对性的恶意软件攻击，且零误报。
- 检测并阻止了身份欺骗尝试。
- 检测出尝试骗取用户身份数据的浏览器中间人攻击。
- 检测出远程访问软件非法用于账户盗用。
- 每月减少几百万美元的欺诈损失。

总览

该金融机构可以提供广泛的服务，包括个人和企业银行业务、保险、企业理财和私人银行业务。银行的企业文化核心是有效地满足客户需求并提供全面优质的服务；保护客户免受欺诈并提供无摩擦的在线体验是其主要的业务内容。

有了 LexisNexis® Risk Solutions，该金融机构可以：

- 识别使用反检测工具、试图通过更改浏览器版本、安装在浏览器中的插件、操作系统类型、时区等绕过设备指纹识别的设备发起的事件。
- 同时分析行为模式或者对网页的篡改识别恶意软件，阻止欺诈事件并标记可疑事件。
- 检测尝试盗取个人信息或者驮运合法用户登录会话的远程访问木马（RAT）。

业务问题

与许多其他金融机构一样，该金融机构也日益成为各种无懈可击的社会工程攻击的目标，这种攻击的方式通常是诱导用户无意中安装远程访问软件或恶意软件。有时，这种攻击可以驮运经过完全认证的登录对话等，通过强有力的双因素身份验证屏障。

当客户访问网址进行登录银行账户、进行支付、变更密码等操作时，这种恶意软件就会尝试监控带有个人信息（包括客户名称、账号、密码和其他保密信息）的按键和字段。

该金融机构需要一款能够分析当前事件数据并将其与历史行为对比以近实时地精确区分异常行为的高效欺诈解决方案。然后标记该种表现出异常行为的事件，根据相关的风险进行下一步审核或者直接驳回。

该金融机构需要一款能够分析当前事件数据并将其与历史行为对比以近实时地精确区分异常行为的高效欺诈解决方案。

利用全球共享情报的力量近实时地检测高风险事件

应对复杂且有组织的网络犯罪的最佳方法是利用全球共享网络的力量。LexisNexis® Digital Identity Network®从数百万日常消费者互动中收集和处理全球共享情报，包括登录、支付和新账户申请。利用 LexisNexis® ThreatMetrix®产品功能及数字身份网提供的信息，LexisNexis® Risk Solutions 能够通过分析设备、位置和匿名个人信息之间的无数连接，为每个用户创建一个唯一的数字身份。偏离这一可信数字身份的行为可以被近实时且准确地识别，提醒该金融机构可能存在欺诈行为。它可以在处理交易之前，检测并标记可疑行为，以进一步审核、提高身份认证级别或驳回，从而将可信用户的摩擦降至最低。

ThreatMetrix 产品能够：

- 为每个用户识别可信的行为和关联信息（设备、IP 地址、位置、会话行为和支付行为）。
- 识别异常行为变化以防止支付欺诈，包括识别远程访问软件以及恶意软件行为识别标志。
- 通过交叉关联到 LexisNexis Risk Solutions 网络中已知钱骡账户或者欺诈性行为，识别持续欺诈网络。
- 识别与内部欺诈相关的行为异常。

案例研究

LexisNexis® ThreatMetrix® Solution 的主要特征

- **页面指纹技术**可以近实时地检测任何页面修改，例如植入恶意软件的 HTML 或 JavaScript 组件，从而保护在线交易。
- **恶意软件保护**能够帮助企业降低风险（包括最复杂的恶意软件带来的风险），从而减少欺诈。包括保护企业免受浏览器中间人（MITB）、远程访问木马（RAT）、高速/高频网络机器人攻击到模仿合法客户行为的低慢攻击、勒索软件、key logging（键盘记录）攻击等。
- 移动软件开发工具包（SDK）中的**恶意软件检测和应用信誉**能够评估安卓设备上安装的所有应用程式，并根据来自超过 1500 万个移动应用程式的行业领先的签名数据库进行验证。在近实时标记包含恶意软件或者可疑声誉的应用程式的同时验证已知的、可信应用程式。
- **蜜罐技术**可以设置陷阱来检测浏览器中未经授权的网页修改。在恶意软件看来，蜜罐陷阱就像用户正导航到恶意软件通常针对的高价值网站类型。当恶意软件试图通过植入额外的网页内容（如额外的表单元素，或询问个人信息弹出对话框）对其进行攻击，我们的蜜罐能够近实时地检测到这些变化。
- **LexisNexis® Risk Solutions 可**通过集成中心整合新的外部威胁情报以**增强其能力**。该集成中心让机构可以启用相关的第三方数据源和定制服务，为高风险交易提供额外的认证和身份验证服务。

LexisNexis® RISK SOLUTIONS

更多信息，请拨打 852.39054010 或登陆网站：
risk.lexisnexis.com/FIM-ZH

更多信息，请登陆 risk.lexisnexis.com/FIM-ZH。NXR14090-00-0919-ZH-GL