LexisNexis®
RISK SOLUTIONS

CASE STUDY

LexisNexis® Risk Solutions Helps Curb Malware Attacks on a Large Financial Institution, Reducing Fraud Losses

LexisNexis® ThreatMetrix® digital identity intelligence detects high-risk events in near real-time, without impacting user experience

AT A GLANCE

COMPANY

A large financial institution

REQUIREMENTS

- Prevent targeted social engineering attacks that use remote access software to infiltrate trusted user accounts.
- Curb malware attacks.
- Restrict fraudulent events at login and payments.
- Reduce fraud losses.

SOLUTION

LexisNexis Risk Solutions implemented full, near real-time behavioral profiling of the end-to-end online session including account registrations, logins, change of details and preferences, account navigation, creation of new beneficiaries and payment profiling in order to detect anomalies indicative of malware or illegitimate user of remote access software. This drastically cut fraud while maintaining a friction-free experience for trusted customers.

BOTTOM LINE

- Targeted malware attacks were stopped within a short timespan with zero false positives.
- Detected and blocked identity spoofing attempts.
- Detected man-in-the-browser attacks attempting to dupe users into revealing identity data.
- Detected unlawful use of remote access software being used for account takeovers.
- Multi-million dollar fraud savings every month.

CASE STUDY

Overview

This financial institution offers a wide range of services including personal and business banking, insurance, corporate finance, and private banking. The bank's ethos focuses on effectively meeting customer needs and delivering all-round excellent service; safeguarding customers against fraud and offering them a frictionless online experience are key business imperatives.

With LexisNexis® Risk Solutions, this financial institution can:

- Identify events with devices using anti-detect tools trying to bypass device fingerprinting by changing browser versions, plug-ins installed in browser, operating system type, time zone etc.
- Recognize the presence of malware by analyzing behavior patterns or alterations to webpages, rejecting fraudulent events and flagging suspicious events.
- Detect remote access trojans (RATs) attempting to steal personal information or piggy-back a legitimate user login session.

Business Problem

This financial institution, like many others, was being increasingly targeted by pitch-perfect social engineering attacks that often led to users unwittingly installing remote access software or malware. At times these attacks were passing strong two-factor authentication barriers because they were piggy-backing fully authenticated logging sessions, for example.

When customers accessed the website to log in to their bank account, make a payment, change a password etc., these malwares attempted to monitor button clicks, fields having personal data including, customer name, account number, passwords and other confidential data.

This financial institution needed a robust fraud solution that could analyze current event data and compare to historic behavior in order to accurately distinguish anomalous behavior in near real-time. Such events demonstrating anomalous behavior then could be flagged for review or directly rejected based on the risk associated.

CASE STUDY

This financial institution needed a robust fraud solution that could analyze current event data and compare to historic behavior, to accurately distinguish anomalous behavior in near real-time.

Harnessing the Power of Global Shared Intelligence to Detect High-risk Events in Near Real-Time

The best way to tackle complex, organized cybercrime is using the power of a global shared network. The LexisNexis® Digital Identity Network® collects and processes global shared intelligence from millions of daily consumer interactions including logins, payments, and new account applications. Leveraging LexisNexis® ThreatMetrix® product capabilities and using information from the Digital Identity Network, LexisNexis® Risk Solutions is able to create a unique digital identity for each user by analyzing the myriad connections between devices, locations, and anonymized personal information. Behavior that deviates from this trusted digital identity can be accurately identified in near real-time, alerting this financial institution to potential fraud. Suspicious behavior can be detected and flagged for review, step-up authentication, or rejection before a transaction is processed, minimizing friction for trusted users.

The ThreatMetrix product was able to:

- Identify trusted behaviors and associations for each user (devices, IP addresses, locations, session behavior and payment behavior).
- Identify anomalous changes in behavior to prevent payment fraud, including identifying the presence of remote access software and malware behavioral signatures.
- Identify the presence of persistent fraud networks by cross-correlating to intelligence on known mule accounts or fraudulent behavior seen elsewhere in the LexisNexis Risk Solutions network.
- Identify behavioral anomalies related to insider fraud.

CASE STUDY

Key Features of the LexisNexis® ThreatMetrix® Solution

- **Page fingerprinting technology** can detect any page modifications such as HTML or JavaScript components injected by malwares in near real-time, protecting online transactions.
- **Malware protection** helps businesses mitigate the risk of even the most sophisticated malware, thereby reducing fraud. This includes protection from man-in-the- browser (MITB), remote access trojan (RAT), high velocity/ frequency bot attacks to low-and- slow attacks mimicking legitimate customer behavior, ransomware, key logging attempts etc.
- **Malware detection and application reputation** in the mobile software development kit (SDK) evaluates all installed applications on android devices and verifies them against an industry-leading signature database of over 15 million mobile apps. Known, trusted applications are validated while applications containing malware or suspicious reputations are flagged in near real-time.
- **Honeypot technology** sets traps to detect unauthorized webpage modifications in the browser. The honeypot trap appears to malware as if a user is navigating to the type of high value websites malware generally targets. As the malware attempts to attack this - by injecting additional web content such as additional form elements, or popup dialogues asking for personal information - our honeypot detects those changes in near real-time.
- **LexisNexis® Risk Solutions can augment its capabilities** by folding in additional external threat intelligence feeds via integration hub. The integration hub allows institutions to onboard relevant third party data sources and custom services to provide additional authentication and identity verification services for high-risk transactions.

LexisNexis® RISK SOLUTIONS

For more information,
call 866.528.0780 or visit risk.lexisnexis.com/FIM-EN

About LexisNexis Risk Solutions

LexisNexis Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX Group (LSE: REL/NYSE: RELX), a global provider of information and analytics for professional and business customers across industries. RELX is a FTSE 100 company and is based in London. For more information, please visit www.risk.lexisnexis.com, and www.relx.com

About ThreatMetrix

ThreatMetrix®, A LexisNexis® Risk Solutions Company, empowers the global economy to grow profitably and securely without compromise. With deep insight into 1.4 billion tokenized digital identities, LexID® Digital delivers the intelligence behind 110 million daily authentication and trust decisions, to differentiate legitimate customers from fraudsters in near real-time.

LexisNexis, LexID, and the Knowledge Burst logo are registered trademarks of RELX. ThreatMetrix and Digital Identity Network are registered trademarks of ThreatMetrix, Inc. Copyright © 2019 LexisNexis Risk Solutions.

Learn more at risk.lexisnexis.com/FIM-EN. NXR14090-00-0919-EN-US