LexisNexis®
RISK SOLUTIONS

FALLSTUDIE

Großes Finanzinstitut berichtet eine 50%ige Verbesserung bei der Erkennung von Money-Mule-Konten innerhalb des ersten Anwendungsjahres von LexisNexis® Risk Solutions

LexisNexis® Risk Solutions kann einer Bank bei der Rückerstattung von $ 965.000 an Opfer von Smurfern helfen

Auf einen Blick

UNTERNEHMEN

Großes Finanzinstitut

VORAUSSETZUNGEN

- Genaue Identifizierung und Blockierung von Money-Mule-Konten.
- Blockierung des Transfers betrügerischer Mittel durch Smurfer.
- Minimieren von durch Betrug im Zusammenhang mit Smurfern entstehenden Verlusten.
- Im Zentrum steht eine reibungslose, erfolgreiche Benutzererfahrung für legitime Kunden.

LÖSUNG

Dank der Nutzung der digitalen Identitätsinformationen von LexisNexis® kann dieses große Finanzinstitut Money-Mule-Konten genau identifizieren und blockieren sowie umfassenden Smurfer-Netzwerken auf die Spur kommen. Gleichzeitig wird die Benutzererfahrung für die legitimen Anwender reibungslos gestaltet.

FAZIT

- 50%ige Verbesserung bei der Identifizierung von Money Mules.
- Rückerstattung eines Betrags in Höhe von $ 965.000 aus Mule-Konten, der an die Opfer zurückgezahlt werden konnte.
- Minimisierung der Probleme für die legitimen Stammkunden.

FALLSTUDIE

Überblick

Dieses große Finanzinstitut bietet eine breite Servicepalette, wie unter anderem Personal Banking und Business Banking, Private Banking, Versicherungen und Corporate Finance. Dabei bilden die Kunden den Mittelpunkt der Deontologie der Bank: Vertrauen ist das A und O der Einrichtung im Rahmen von Kundenbeziehungen.

Geschäftliches Problem

Money Mules sind mittlerweile einer der zentralen Auslöser für zahlreiche betrügerische Vorgehensweisen durch Dritte sowie andere Scams, die eine branchenweite Auswirkung haben auf Kunden und Banken. Motiviert durch hohe Summen und basierend auf dem Raub von aus gehackten Datenbanken gestohlenen Informationen, versuchen Cyberkriminelle sich Online-Bankkonten anzueignen. Sobald es einem Betrüger jedoch gelungen ist, ein Konto basierend auf gestohlenen Logindaten zu hacken oder Social Engineering-Taktiken gegen einen legalen Kunden einzusetzen, muss das Geld auf ein anderes Konto überwiesen werden, zwecks Geldwäsche und um das unrechtmäßige Geld nutzen zu können.

Sogenannte „Mules“ oder „Smurfer“ sind Personen, deren Bankkonten innerhalb des Finanzsystems zur Geldwäsche genutzt werden, und die entweder bewusst oder unbewusst zu diesem Zweck angeworben oder rekrutiert werden. Es ist sehr schwierig, ihnen auf die Spur zu kommen, da das Geld rasant durch große Netzwerke von auf den ersten Blick unzusammenhängenden Mule-Konten geleitet wird, die bei unterschiedlichen Finanzinstituten geführt werden.

Dieses große Finanzinstitut wurde vor die Aufgabe gestellt, eine Money-Mule-Aktivität innerhalb des eigenen Online-Banking-Umfelds zu identifizieren. Hierfür wurde eine Lösung benötigt, die diesen Aktivitäten auf die Spur kommen würde und gleichzeitig dem Transfer von Geldern Einhalt gebieten könnte, um diese zeitnah wieder an die Opfer zurückzuzahlen.

FALLSTUDIE

”Dank LexisNexis® Risk Solutions können wir den Kampf gegen Smurfer jetzt aufnehmen, basierend auf einem proaktiven Ansatz bei der Aufdeckung von Money Mules. Ohne diesen neuen Ansatz wären wir nie in der Lage gewesen, eine derartig hohe Summe an die Opfer dieser Scams zurückzuzahlen.“

Vertrauenswürdige Transaktionen mit LexID® Digital

Seit der Implementierung von LexisNexis® Risk Solutions konnte die Bank 50 % mehr Mule-Konten identifizieren und betrügerische Fonds in Höhe von $ 965.000 an die Opfer von Money Mules zurückzahlen. Dieser Erfolg ist dem LexisNexis® Digital Identity Network® zu verdanken, mit welchem anomale Verhaltensweisen identifiziert werden konnten, um so Money Mules auf die Spur zu kommen, basierend auf Informationen wie Standort, Gerät und auffälligen Verhaltensweisen.

Unter Nutzung von globalen digitalen Identitätsinformationen konnte die Bank das Spinnennetz der im Rahmen der Mule-Aktivität miteinander verbundenen Konten aufdecken. Auf diese Weise können direkt bei der Anmeldung bekannt Mule-Geräte im Zusammenhang mit neuen Konten identifiziert werden, einschließlich einer Warnmeldung per E-Mail, um diese neuen Mule-Konten umgehend zu blockieren. Zur Erkennung der Geräte und Identifizierung von weiteren Mules sowie Netzwerken nutzte die Bank Informationen zu Geräten und IP. Dabei konnten ein ganzes betrügerisches Netzwerk mit 140 Mule-Konten aufgedeckt werden. Die Bank konnte zudem einen Beitrag leisten bei der Festnahme eines Mules rekrutierenden Betrügers, basierend auf Daten von LexisNexis® Risk Solutions, die bei der Lokalisierung der Aktivität des Mule-Kontos helfen konnten.

Zudem konnte die Bank ein Mule-Modul implementieren, das unter Berücksichtigung von bestimmten Verhaltensmustern die Erkennung von noch nicht aufgedeckten Mules erleichtert. Auf diese Weise konnten Verhaltensweisen und Muster auf einer tieferen Ebene identifiziert werden und es konnte eine genau Trennlinie gezogen werden zwischen neuen Mules und erklärbaren Verhaltensänderungen. Da das Mule-Modul normale Verhaltensänderungen berücksichtigt, wurden zudem die legitimen Kunden bei ihren Transaktionen nur minimal beeinträchtigt.

Das LexisNexis® Digital Identity Network arbeitet mit globalen anonymisierten Daten, um Kunden und Betrüger eindeutig zu unterscheiden, unterstützt durch Daten aus Crowdsourcing-Quellen aus Millionen von täglichen Kundeninteraktionen, wie Login, Zahlungen und neuen Kontoeröffnungen innerhalb von Tausenden Unternehmen auf der ganzen Welt.

Wichtige Merkmale von LexisNexis® Risk Solutions / Bank Partnership

- **Trust Tags** sind digitale Label, die es Unternehmen ermöglichen, vertrauenswürdige und dubiose Nutzer, Geräte, Standorte und Personas zu definieren, zu kategorisieren, zu taggen und zu differenzieren. Trust Tags können dynamisch mit den unterschiedlichsten Online-Attributen verbunden werden, wie Geräte, E-Mail-Adressen, Kartennummern oder andere Attribute im Zusammenhang mit der Genehmigung, Verweigerung oder Prüfung einer Transaktion.
- **Smart ID** erkennt Stammnutzer, die Cookies löschen, Private Browsing nutzen und andere Parameter ändern, um traditionelle Device-Fingerprinting-Tools zu umgehen, Smart ID verbessert die Erkennung von Stammnutzern und verringert Falsch-Positiv-Meldungen. Die Smart ID wird aus der Analyse vieler Browser, Plugins und der Attribute von TCP/IP-Verbindungen erhalten und erzeugt einen Vertrauenswert, der unterschiedliche betrügerische Benutzerkonto-Registrierungen oder Login-Versuche erkennt, ausgehend von einem Gerät.

- **True IP** erkennt akkurat die Nutzung von Standorten und verschleierten Identitäten, wie versteckte Proxy-Server und VPNs, und bietet der Bank die Möglichkeit, die echte IP-Adresse, den Standort und weitere Attribute der einzelnen Transaktionen zu sehen. Es ist auch in der Lage, neue Verhaltensmuster zu erkennen, wie beispielsweise ungewöhnliche Transaktionsvolumen oder Änderungen von Tempo oder Frequenz der Transaktionen. Diese dynamischen Daten leisten einen Beitrag bei der Identifizierung von betrügerischen Verhaltensweisen und liefern der Bank genaue Informationen, um darüber zu entscheiden, ob eine Transaktion genehmigt, abgelehnt oder geprüft werden sollte.
- **Die Deep-Connection-Analysis-Technologien** geben eine bessere Übersicht über verdächtige Ereignisse. Betrüger, die ein neues Konto von einem neuen oder riskanten Standort eröffnen möchten, verschleiern möglicherweise ihren Standort oder ihre Identität mithilfe von versteckten Proxy-Servern, VPN und dem TOR-Browser. Dank der Proxy-Piercing-Technologie untersucht LexisNexis Risk Solutions die Header-Daten von TCP/IP-Paketen, um sowohl die IP-Adresse des Proxy-Servers und die wahre IP-Adresse zu enthüllen.

LexisNexis® RISK SOLUTIONS

Wenn Sie weitere Informationen möchten, rufen Sie 866.528.0780 an oder besuchen Sie 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. NXR14087-00-0919-EN-US