XFraud
Telefonie-Missbrauch

Telefonie-Missbrauchs-Prävention und -Verhinderung

XFraud ist ein Applikationsmodul der XCarrier Plattform, die betrügerische Aktivitäten aus dem öffentlichen Telefonnetz detektiert und nach bestimmten Regeln proaktiv verhindert oder unterdrückt.

Carrier Switch Infrastrukturen werden automatisch und in Echtzeit durch die XFraud-Applikation überwacht und bei Bedarf entsprechend provisioniert. XFraud schützt effizient und pro-aktiv Carrier und Endkunden vor betrügerischen Telefon-Aktivitäten. Der Schutz erschliesst Trunks oder A- und B-Nummernbasen.

Gleichzeitig werden mittels Push-Notifikationen per Email, SMS oder durch proaktive Trouble Ticket operativ verantwortliche Teams alarmiert.

Begrifflichkeiten und Definitionen

Telefon- und Kommunikations-Betrug
Telefonie-Betrug oder Kommunikationsbetrug ist die Nutzung von Telecom-Services und -produkten mit der Absicht, illegal Geld von Carriern oder dessen Endkunden zu erlangen oder nicht zu bezahlen. Dabei wird oft mit anspruchsvoll-technologischen Möglichkeiten fehlerhafte Infrastrukturen von Opfern ausgenutzt.

Arten von betrügerischen Aktivitäten, die mit XFraud bekämpft werden (wichtige Beispiele, nicht abschliessend)

- Missbrauchsbetrug basierend auf Ursprungs- und/oder Ziel-Telefonnummern.
- Hacking von PBX/lokalen Telefonzentralen und Missbrauch der Telefonnummern
- Wangiri Rückruf (Einmal Läuten) von ausländischen Mehrwertnummern zum Erlangen eines Summtons
- Arbitrage/Tromboning – via das Ausland geroutete Calls zurück ins Ursprungsland
- Internationaler Revenue Share Fraud (IRSF) – Missbräuchliche Verwendung von Mehrwertnummern.

Carrier Call AG
Rank 6A, 5108 Oberflachs, Switzerland
T +41 56 544 66 00, info@carriercall.com
www.carriercall.com

Identifikation von Betrug

- Auf den Carrier-Switches und Interkonnektions-Trunks eines Operators ankommende Telefon-Verkehr wird durchgehend auf spezifische Telefonnummern, Format, Plausibilität, Volumen, Herkunft, Destination, Zeitpunkt und anderen spezifischen Parametern geprüft.
- Dazu dienen verschiedene Referenzen als Basis für spezifische Schutz-Aktionen.
  - Listen: Bekannte, betrügerische Ursprungs- oder Destinations-Nummern oder Nummernbereiche werden automatisch gesperrt.
  - Call-Volumen und Muster: Unbekannte, plötzlich stark ansteigende Telefon-Volumen werden sofort erkannt.
  - Call-Zeiten: Stark ansteigende Call-Volumen zu ungewöhnlichen Tageszeiten oder Tagen sind suspekt und werden entsprechend durch XFraud analysiert, gelernt und gegebenenfalls alarmiert oder sogar unterbunden.
- XFraud verwendet zusätzlich interne Operator-Quellen, um betrügerische Anrufe zu erkennen. Ankommende Call Data Records (CDR) werden beispielsweise von den Carrier-Switches in Nah-Echtzeit analysiert und durch verschiedenste Regelwerke, Logiken und Algorithmen blitzschnell verarbeitet.
- Frisch entdeckte Regelverstösse oder ungewöhnliche Muster werden identifiziert und entsprechende Regel-Aktionen auf spezifische Telefonnummer(n) oder Trunks sofort angewandt.
- Je nach Einsatzgebiet (Land) und Regulierung stehen länderspezifische zusätzliche, externe Informationsquellen dynamisch zur Verfügung. Diese werden bei Verfügbarkeit elektronisch via API angebunden und in die Verarbeitungs-Logiken integriert.
- Zusätzliche, manuelle Einträge können via das graphische User-Interface jederzeit additiv oder komplementär erfolgen.

Bedienung und Interfaces

- XFraud wird über die graphische Bedieneroberfläche (GUI) von XCarrier konfiguriert und bedient.
- Folgende gängigen Import File-Formate und Datenkollektions-Protokolle sind derzeit in Betrieb. Diese sind nicht abschliessend.

Import Formate	**Data Collection Protokolle**
• .xls	ftp, sftp
• .csv	http, https
• Json	SOAP
• Xml	REST
• Dblink	…
• …	

Automatisierte Schutz-Aktionen

XFraud agiert aufgrund von vorkonfigurierten Aktionsplänen und selbstlernenden Algorithmen

- Definierte, dynamische Listen mit registrierten Nummern oder Nummernbereichen
- Alarmierungen via SMS, Email und Push-Notifikationen
- Automatische Öffnung von Trouble Tickets
- Automatische Switch-Provisionierung und Listenanreiche-rungen von zu blockierenden Nummern / Trunks
  - o Blockierte Nummern und Trunks werden eindeutig und mit einem Zeitstempel gekennzeichnet, damit sie nachbearbeitet werden können
- Schwell- und Alarmierungswerte werden festgelegt, z.B. pro Monat, Tag, Stunde. Vergleiche mit Referenz- oder historischen Daten werden laufend durchgeführt.
- AdHoc Tests können manuell zusätzlich im Live-Betrieb vollzogen werden. Bei Bedarf können zusätzlich einzelne Regeln im Live-Betrieb aktiviert/deaktiviert werden.
- Destinations-Screening mittels Volumen-Schwellwerten stehen zusätzlich als High-Usage-Monitoring zur Verfügung.

Der XFraud Traffic Profiler ist logische Steuerungseinheit

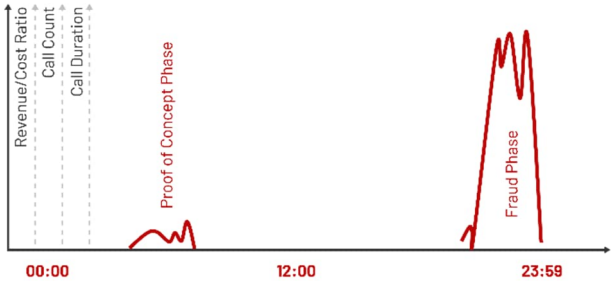
Reports nach Rufnummer, Kunde und Destination

- XFraud produziert statistische Tabellen oder graphische Reports, die User unterstützen, allfällige Qualifikationen von Betrug manuell festzustellen und einzugrenzen.
- Betrügerische Aktivitäten beginnen oft mit einem Test zu einer üblichen Tageszeit (Proof of Concept Phase). Der eigentliche Betrug findet dann absichtlich zu Zeiten statt, wenn operative Teams bei Carriern und Service Providern möglichst nicht arbeiten.
- Überraschungseffekte werden von Betrügern kommerziell ausgenutzt. XFraud unterstützt die operativen Teams, um automatisch Muster zu erkennen und nötige Switch-Blockierungen automatisch zu veranlassen. Entsprechende Push-Notifikationen werden abgesetzt.

Reporte	15.02.2021	19.11.2021	03.12.2021
Ziel	**Chad-Mobile**	**Ukraine-Mobile**	**Estland-Mobile**
Anrufdauer	**1526.05**	**20.30**	**2533.02**
Betrag	**998.94**	**20.65**	**1612.30**
Kosten	**0.00**	**0.00**	**0.00**
Anzahl	**1675**	**7**	**2628**
Anzahl Unbeantwortet	**38**	**2**	**57**

Carrier Call AG
Rank 6A, 5108 Oberflachs, Switzerland
T +41 56 544 66 00, info@carriercall.com
www.carriercall.com

- Betrügerische Aktivitäten beginnen oft mit einem Test zu einer üblichen Tageszeit (Proof of Concept Phase) und in kleiner, unauffälliger Menge.
- Der eigentliche Betrug findet dann absichtlich zu Zeiten statt, wenn operative Teams bei Carriern und Service Providern möglichst nicht arbeiten, z.B. nachts oder an Wochenenden und Feiertagen.



Kundenmehrwert

Mehrwert für Carrier

- Einhaltung von Regulierungen, z.B. Reinwaschung von Schwarzgeld
- Erhöhung der Carrier-Marken Identität durch kommunizierten und wirksamen Schutz gegenüber Kunden.
- Verhinderung von finanziellen Forderungen und Schäden.
- Gesicherte Umsätze und Margen.
- Tiefere Cost of Ownership.

Mehrwert für Carrier-Endkunden

- Schutz der Privat- und Business-Endkunden vor Voice-Betrug.
- Präventiver und additiver Sicherheitsschirm für Endkunden.
- Verhinderung von finanziellen Schäden.

Durch den Einsatz des XFraud-Systems von Carrier Call AG können wir unsere Kunden proaktiv vor grossen finanziellen Schäden schützen und sind mit diesem Service einzigartig in der Schweiz.

Josef Furger
Senior Product Manager B2B, Sunrise UPC

Carrier Call AG
Rank 6A, 5108 Oberflachs, Switzerland
T +41 56 544 66 00, info@carriercall.com
www.carriercall.com