

Cyber Fraud Fusion



Acerca de Group-IB

Group-IB es un creador de soluciones de ciberseguridad que se dedica a investigar, prevenir y combatir delitos informáticos.

1,550+

Investigaciones exitosas en casos de cibercrimen mediante tecnología avanzada

500+

Empleados en todo el mundo

600+

Clientes corporativos

60

Países

\$1 bln

Ahorrados por nuestros clientes corporativos gracias a nuestras tecnologías

1

Proveedor de retención de respuesta ante incidentes

120+

Patentes y aplicaciones

11

Centros de Resistencia contra el Crimen Digital únicos en el mundo

Colaboraciones a escala global

INTERPOL

EUROPOL

AFRIPOL

Con el reconocimiento de los principales especialistas del sector

FORRESTER

Aitê Novarica

kuppingercoie

Gartner

IDC

FROST & SULLIVAN

FROM GLOBAL TO GLOCAL INTELIGENCIA DE AMENAZAS EN TIEMPO REAL EN REGIONES CLAVE



De la inteligencia de amenazas a la inteligencia de fraude

Cyber Fraud Fusion

¿QUÉ ES CYBER FRAUD FUSION?

Gartner

Emerging Tech: Security — Cyber-Fraud Fusion Is the Future of Online Fraud Detection

Published 7 September 2023 - ID G00790000 - 16 min read

By Analyst(s): Dan Ayoub, Pete Redshaw

Initiatives: [Emerging Technologies and Trends Impact on Products and Services](#)

Organizations worldwide have begun merging cybersecurity and fraud prevention teams. This trend will grow through the remainder of the decade. Product leaders must prepare now to lead this shift in positioning and portfolio, outcompete peers, differentiate in the market, and address buyer demands.

Analysis

Trend Description

Cyber-fraud fusion is an emerging trend in online fraud prevention that combines:

- Cyberthreat intelligence
- Identity and access management
- Information security
- Fraud operations and TTPs

Gartner

Cyber-Fraud Kill Chain Has Emerged

The final example of cyber-fraud fusion occurring today includes the introduction of the cyber-fraud kill chain. This represents an emerging methodology and framework that is applied to online fraud prevention and that combines many best practices and well-defined TTPs typically leveraged in cybersecurity for online fraud prevention. The goal is to leverage the cyber-fraud kill chain to improve response and security when a threat is detected so that platform rules and policies can be crafted in a holistic manner.

Forward-leaning OFD vendors are already beginning to apply concepts from traditional cybersecurity frameworks to online fraud prevention. As of today, Gartner is aware of two vendors (Group-IB and ThreatFabric) that have implemented this framework as a form of "fraud intelligence" within their platforms. Gartner has also witnessed several organizations investing in new systems that interface with existing OFD platforms to create the ability to examine the TTPs utilized by adversaries in carrying out specific scams. These TTPs are mapped against relevant portions of the scam and compared with the MITRE ATT&CK Framework, allowing for policies and rules to be crafted to interrupt scams and fraud at multiple places within the user journey.

Strategic Planning Assumption

By 2028, 20% of large enterprises will shift to cyber-fraud fusion teams to combat internal and external adversaries targeting the organization, up from less than 5% today.

CYBER FRAUD FUSION EN ACCIÓN

Group-IB CERT has identified a new phishing scam in Brazil where cybercriminals use rogue mobile base stations to send SMS messages to steal personal and financial data

Group-IB's specialists discovered several web open directories with Python scripts allegedly used to brute force email accounts in order to get unauthorized access to SMTP servers of Brazilian companies

Breve descripción de las tendencias regionales:

01 El equipo CERT de Group-IB identificó una estafa dirigida a bancos de Argentina, que utiliza anuncios falsos para hacerse pasar por canales de contacto oficiales

Estos anuncios, que suelen diseñarse para atraer mediante ofertas de beneficios y descuentos, WhatsApp donde los estafadores utilizan la información personal y bancaria confidencial, confianza que infunden las marcas reconocidas, tendencia más amplia que tiene como objetivo de Argentina

02 El CERT de Group-IB ha identificado un sofisticado esquema de estafas dirigido a compañías de seguros y sistemas de pago de Colombia

La estafa implica un proceso que consta de varias etapas fraudulentas que se hacen pasar por marcas legítimas, utilizan bases de datos públicas de licencias de usuarios de la autenticidad del sitio, mostrando vehículos. Aquellas víctimas cuyo seguro ha vencido, es el que se les solicita que puedan informar

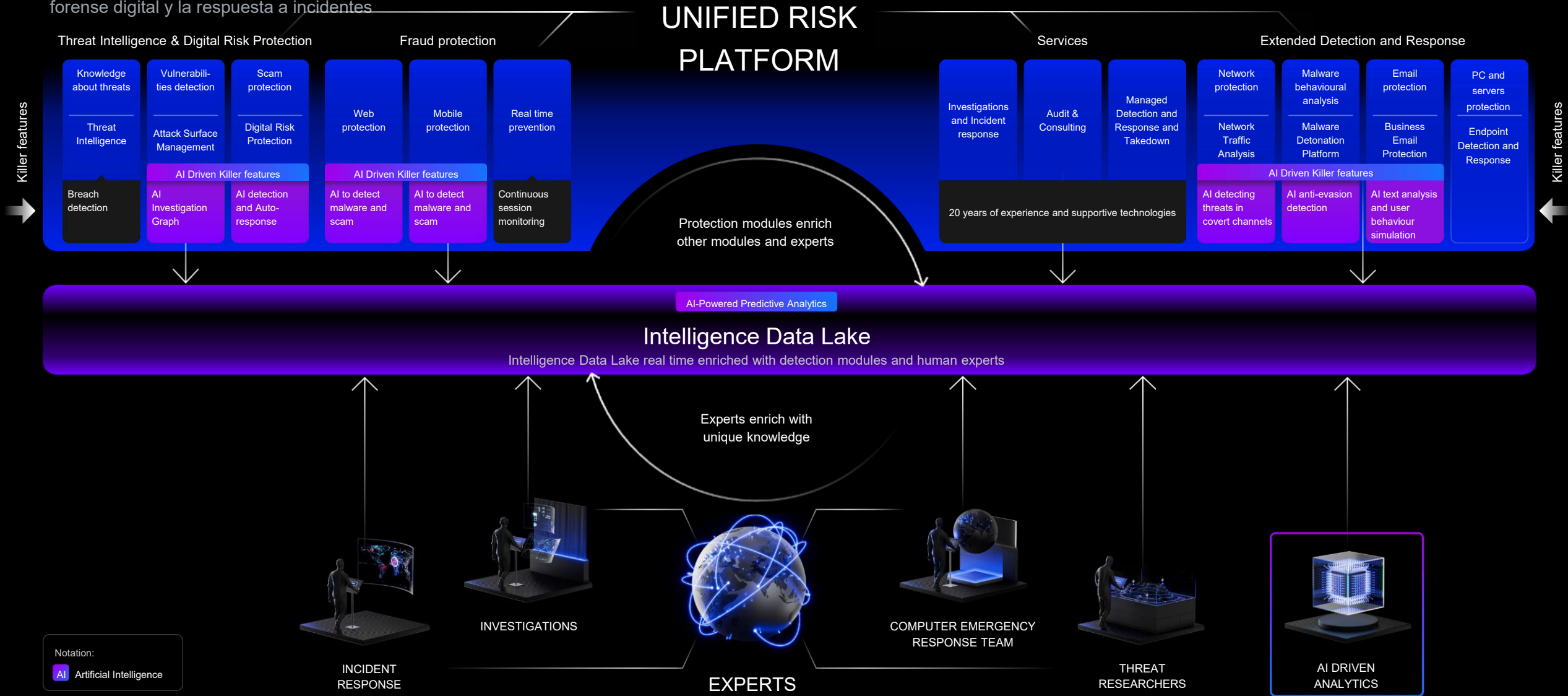
Group-IB CERT has identified a new phishing scam in Chile targeting users via SMS messages to steal personal and financial data

Group-IB's threat intelligence team discovered hundreds of LNK files used in a recent Coyote banking trojan campaign allegedly disseminated via WhatsApp targeting Brazilian Windows users

UNIQUE MISSION-DRIVEN UNIFIED PLATFORM



Creamos una plataforma única que integra productos para la ciberseguridad, la protección de la marca, la lucha contra el fraude y todos nuestros servicios, incluidas las investigaciones, la auditoría, la formación, el análisis forense digital y la respuesta a incidentes



DIVERSAS FUENTES DE INTELIGENCIA



OPEN-SOURCE INTELLIGENCE  • Paste sites • Code repositories • Exploit repositories • URL sharing services	MALWARE INTELLIGENCE  • Detonation platform • Malware emulators • Malware configuration files extraction • Public sandboxes	DATA INTELLIGENCE  • C&C server analysis • Darkweb card shops • Phishing and malware kits • Compromised data-checkers	HUMAN INTELLIGENCE  • Malware reverse engineers • Undercover dark web agents • Regional specialists • Embedded managed service teams	SENSOR INTELLIGENCE  • ISP-level sensors • Honeypot network • IP scanners • Web crawlers
VULNERABILITY INTELLIGENCE  • CVE list • Exploit repositories • Dark web discussions • Threat campaigns mapping	LAW ENFORCEMENT AND SECURITY PARTNERS  • Operations with Interpol and Europol • Local law enforcement investigations • CERT community partners • Technology partners	FRAUD INTELLIGENCE  • Web channel fingerprinting • Digital biometrics • Hosting detection • Multi-account monitoring	ENDPOINT INTELLIGENCE  • Windows and Linux clients • Android and iOS SDK • Machine learning analysis • Malware detonation	NETWORK INTELLIGENCE  • Email package scanners • Open protocol and encrypted traffic analysis • Traffic metadata • Network log collection
MARKETPLACE INTELLIGENCE  • Mobile app store scanning • Advertisement research • Marketplace analysis • Messengers & social media monitoring	BRAND INTELLIGENCE  • Search engine & domain name monitoring • Cloud storage scanning • Dark web mentions detection • Scam campaigns mapping	AUDIT  • Penetration testing • Compliance audit • Application assessment • Social engineering testings	SERVICES  • Endpoint threat hunting • Host-level artifact collection • TTP and IoC identification • Malicious behavior detection	DFIR  • Digital evidence collection • eDiscovery • Kill chain reverse engineering • Transaction analysis

CYBER FRAUD FUSION GROUP-IB FRAUD MATRIX



Proporcionamos una hoja de ruta completa para la protección contra el fraude

Threat Intelligence & Digital Risk Protection

Fraud Protection

Reconnaissance 7 techniques	Resource development 25 techniques	Trust abuse 22 techniques	End-user interaction 17 techniques	Credential access 22 techniques	Account access 8 techniques	Defence evasion 26 techniques	Perform fraud 16 techniques	Monetization 8 techniques	Laundrying 10 techniques
Gather Balance 3 via Malware 1 Bot Activity 1 SMS Interception 0 Gather Compromised Account 9 Account Stuffing 1 Buy Compromised Accounts 7 Bruteforce Accounts 0 Gather PI 11 Collect public PI 7 Buy PI 8 Gather Victim Business Relationships 0 Search Closed Sources 1 Search Open Sources 1 Testing Payment Thresholds 0	ATM Blackbox 0 ATM Switch software 0 Affiliate Phishing Program 2 Anonymity Capabilities 1 Returned Phone Number 0 VPN/Proxy/Hosting Services 1 One-Time Phone Number 0 Disposable Email 0 Virtual Phone Number 0 Fake Emailbox 0 App Repackaging 0 Creating Fake Documents 2 Data Leaks 1 Establish Accounts 2 Use Compromised Credentials 1 Corporate Compromised Account 1 Buy Pre-Established & Networks 1	Applying Additional Bank Services 2 Associating With Public Situation/Incident 4 Epidemiology-related news/regulations 0 Legislation changes 1 Conflicts 0 Bank Employee impersonation 0 Bluffing 7 Fake Internal Fraud 0 Fake Fraud Warning 3 Fake Help with Loan 0 Fake Loan Request 1 Unlocking Payment Card 1 Family Emergency 1 Scam Refund 1 Card Renewal 0 Branded Resource 6 Fake application 0	Card Hijacking 2 Comprehensive Identity Takeover 2 Drive-by Compromise 0 Fake Investment Platform Visit 3 Outbound IVR Call 0 PIN-code Peeking 0 Phishing 6 Pushing to Install Malware 3 Scam Ads 3 Scam Bill in Postbox 0 Scam Email Message 0 Scam Message in Social Network/Instant Messenger 10 Scam Sale Ads 1 Smishing 6 Spear Phishing 0	2nd Factor Capture 7 2nd Factor Disclosure 14 Access Notifications 2 SMS Interception 0 Push Interception 0 App Overlay 2 Buying Phone Number with SMS Banking Enabled 0 Card Dump Capture 0 Card PAN/EXP/CVV Capture 4 Card PAN/EXP/CVV Disclosure 4 Credential Disclosure 9 Credentials Capture 5 Fake 3-D Secure Page 1 Fake Acquiring Form 4 Illegal Access to Database 0 Keylogger 0	Access from Fraudster Device 13 Access with Stolen Session Cookie 1 Account Access on Victim Device 1 Account creation 3 on Fraudster Device 3 Automated Account Registration 0 Device Remote Access 4 Forced Account Access 0 Legitimate Account Access by Bank Employee 0	2nd Factor Bypass 6 Phishing Disclosure 6 AutoCompletion 0 Accessibility Service 0 Request permissions 0 ATM Switch Reply Manipulation 2 Adding Mule Card to Victim Mobile Wallet 1 Adding Victim Card to Fraudster Mobile Wallet 2 Authentication By Victim 2 Authentication Bypass 6 Android Accessibility Service 0 AutoCompletion 0 Token in Device 0 Compromised Credentials 6 Automated Payment Creation 1 via SMS 0	Bonus Withdrawal 1 Checkout via Online Shop 2 Depositing Funds via ATM by NFC on Mule Card 1 Depositing Money to a Phone Number via SMS Banking 0 Emptying ATM Dispenser on Command 0 Extracting Money From Dispenser 0 Issuing Transfer on Demand 0 Issuing of Withdrawal QR 0 Loan 0 NFC Payment 2 Network Interception 0 Payment for Goods 3 Payment to Mule Account 14 Internal Mule Account 8 External Mule Account 10	Cash Dispenser Jackpotting 0 Cashout 15 ATM Withdrawals 1 Conversion to Cryptocurrency 1 Cashier's Checks and Money Orders 0 Prepaid Debit Cards 1 Purchasing and Reselling 4 Gift Cards Reselling 1 Purchasing Goods and Reselling 0 Sale of Compromised Credentials to 3rd Party 2 Subscribing to Paid Service 0 Withdrawal via ATM by NFC 0	Betting and Gambling Platforms 0 Deposit Funds for Betting 0 Use P2P Betting Platforms 0 Compromised accounts 6 Crypto currency exchanges 6 Crypto currency mixer 5 E-wallets 10 Fake facilitator 3 Hotel Reservation 5 Regal Merchant 4 Mule accounts 13 Virtual cards 8

Podemos detener el ataque, en cada paso

CYBER FRAUD FUSION GROUP-IB FRAUD MATRIX

Proporcionamos una hoja de ruta completa para la protección contra el fraude

Digital Risk Protection

Reconnaissance	Resource development	Trust abuse
7 techniques	25 techniques	22 techniques
Gather Intelligence	ATM Blackbox	Applying Additional Bank Services
Use Malware	ATM Switch software	Associating With Public Situation/Incident
Bot Activity	Adware Phishing Program	Epidemiology-related news/regulations
SMS Interception	Anonymous Capabilities	Legislation changes
Gather Compromised Account	Returned Phone Number	Conflicts
Account Stuffing	VPN/Proxy/Hosting Services	Bank Employee Impersonation
Buy Compromised Accounts	One-Time Phone Number	Stuffing
Scamforce Accounts	Disposable Email	Fake Internal Fraud
Gather PI	Virtual Phone Number	Fake Fraud Warning
Collect public PI	Fake Emailbox	Fake Help with Loan
Buy PI	App Repackaging	Fake Loan Request
Gather Victim Business Relationships	Creating Fake Documents	Unlocking Payment Card
Search Closed Sources	Data Leaks	Family Emergency
Search Open Sources	Establish Accounts	Scam Refund
Testing Payment Thresholds	Use Compromised Credentials	Card Renewal
	Corporate Compromised Account	Branded Resource
	Buy Pre-Credentialed	Fake application

Screenshot of the GROUP-IB Digital Risk Protection interface showing link details for a phishing attempt.

The interface displays the following information:

- Link details:** General, Resource analysis, Events, Domain graph.
- Risk score:** General 0%, Login 0%, Screen 0%.
- Apprise state:** Not required.
- Info:**
 - Status: Detected
 - Status info: %s: 1: manual_1712544513447526 phishing
 - Type: Phishing
 - Company: [Redacted]
 - Brand: Apple (iPhone)
 - Source: Web
 - Title: Manage your Apple ID - Apple
 - Link: View HTML
 - Priority: Critical
 - Found date: 02 Oct 2025 09:12
 - Detected: 02 Oct 2025 09:12
 - Approved: --
 - In response: --
 - Resolved: --
- Matched signatures:**
 - Apple_Fortis (iPhone)
 - Detected: 4
 - Matched: 1
 - Type: Phishing
- Hosting & Admin:** Set manually.

Podemos detener el ataque, a cada paso

CYBER FRAUD FUSION GROUP-IB FRAUD MATRIX



Proporcionamos una hoja de ruta completa para la protección contra el fraude

Fraud Protection

Source development

22 techniques

Malicious BlackBox

0

Malicious Switch software

0

Malicious Phishing Program

2

Malicious Capability

1

Malicious Phone Number

0

Malicious Phishing/Hacking service

1

Malicious Time Phone Number

0

Malicious Disposable Email

0

Malicious Virtual Phone Number

0

Malicious Fake EmailBox

0

Malicious Repackaging

0

Malicious Creating Fake Documents

2

Malicious Fake Links

1

Malicious Establish Accounts

2

Malicious Fake Compromised Credentials

1

Malicious Fake Compromised Account

1

Malicious Fake Established

1

Trust abuse

22 techniques

Applying Additional Bank Services

2

Accounting With Public Situation/Incident

4

Epidemiology-related news/regulations

0

Legislation changes

1

Conflicts

0

Bank Employee Impersonation

0

Bluffing

7

Fake Internal Fraud

0

Fake Fraud Warning

3

Fake Help with Loan

0

Fake Loan Request

1

Unlocking Payment Card

1

Family Emergency

1

Scam Refund

1

Card Renewal

0

Standard Resource

4

Fake application

0

End-user interaction

17 techniques

Card Hijacking

2

Comprehensive Identity Takeover

2

Drive-by Compromise

0

Fake Investment Platforms

3

Outbound VR Call

0

PIRcode Peeking

0

Phishing

4

Pushing to Install Malware

3

Scam Ads

3

Scam Bill in Postbox

0

Scam Email Message

0

Scam Message in Social Network/Instant Messenger

10

Scam Sale Ads

1

Smishing

4

Spear Phishing

0

Credential access

22 techniques

2nd Factor Capture

7

2nd Factor Disclosure

14

Access Notifications

0

SMS Interception

0

Push Interception

0

App Overlay

0

Buying Phone Number with SMS Banking Enabled

0

Card Dump Capture

0

Card PAN/EXP/CVV Capture

0

Card PAN/EXP/CVV Disclosure

0

Credential Disclosure

0

Credentiale Capture

0

Fake 3-D Secure Page

0

Fake Anonymizing Form

0

Legal Access to Database

0

Keylogger

0

Account access

8 techniques

Access from Fraudster Device

13

Access with Stolen Session Cookie

0

Account Access on Victim Device

0

Account creation

0

on Fraudster Device

0

Automated Account Registration

0

Device Remote Access

4

Forced Account Access

0

Legitimate Account Access by Bank Employee

0

Group-IB Fraud Protection

frp-de.group-ib.com/data-hub/sessions?customerID=213157&from=1586754000000&projectId=213157&filters=%5B%5B%5Cscore%5C%2C4%2C%70%5D%5D

GROUP-IB Bookmarks

Group-IB SSO Portal

Group-IB Portal

Group-IB Website

Pre-sales | Sales...

Expensify

Group-IB Team

Group-IB Wiki

Onelink

GROUP-IB

FP Demo (2K)

26.06.2024 10:24:32.334

Identity session: 40b4001563085a35145329ea11f5c5ecb8b0eef

Sign in

More than two consecutive users from one device

Three users at the same time from one device

More than two users from the same device

Sign-in from device with multiaccounting behaviour (more than 2 users detected)

Authorization of a user from monitored_login list

Activity from hosting service

New device (hardware fingerprint and IP)

New user device (Agent ID + fingerprint)

New not the first client device (agent + fingerprint)

Threat intelligence: Compromised login

Monitored devices login

Customer session ID: r886g1kvv

User navigated to new page: https://fp-eu-demo-site.group-ib.com/accounts.php

Can't build web keystroke model due to lack of training data

Podemos detener el ataque, a cada paso

CYBER-FRAUD FUSION: INTELIGENCIA DE AMENAZAS

THREATS & ACTORS

- More than 2.800 bad actor profiles
- Global cybersecurity threats feed with attribution
- Customizable Threat landscape
- Detailed information about threats and actors including IoCs and activity timeline



DARKWEB

- Full access to our Dark web database
- Instant Messenger monitoring for Telegram and Discord
- Live translation of messages
- Unlimited Threat hunting rules to improve monitoring



COMPROMISES

- End user or employee compromised credentials
- Information leaked on public sources like Pastebin sites.
- Sensitive data leaked on code repositories like GitHub
- Corporate data leaked in public breaches



BANKING

- Compromised Bank Cards information
- Masked Bank Cards information



MALWARE

- Group-IB detonation platform
- Over 1.400 malware reports
- Malware configuration files
- Vulnerabilities feed
- Phishing kits



SUSPICIOUS INDICATORS

- Deface attacks feed
- DDoS attacks feed
- Phishing sites feed
- Malicious IPs used for: VPNs, Scanning, Thor nodes, Proxys



GRAPH

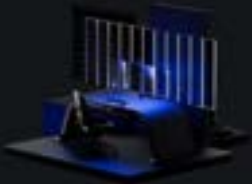
- Advanced Investigation Platform
- Visual Search engine for Group-IB Threat Intelligence data lake



CYBER-FRAUD FUSION: PROTECCIÓN DE MARCA



Analyze your digital presence



Monitoring tools:

- Parsers
- Crawlers
- APIs

Monitoring path:

- Proxy scheduler
- User-agent scheduler
- Special/ dedicated accounts

~3,000,000/day across all digital sources
24/7/365

ADVANCED FEEDS



REFERRER LOGS

DMARC/DKIM/SPF

FRAUD PROTECTION SNIPPET

CUSTOMER'S REPORTS

C&C SERVERS

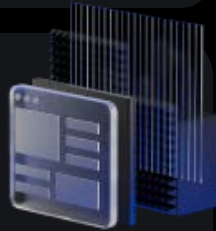
BUSINESS EMAIL PROTECTION

GRAPH ATTRIBUTION

MALWARE CONFIGS

and more..

MONITORING SOURCES



- Domain names
- Databases of phishing resources
- Search engines
- Social media
- Mobile app stores
- Online classifieds and marketplaces
- Advertising
- Instant messengers
- Deep/dark web

DIGITAL RISK PROTECTION

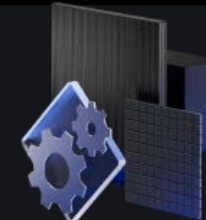


DATA ANALYSIS

- Logo analysis
- Text recognition
- Image recognition
- Regular expressions
- Signature analysis
- Neural networks
- General score
- Domain name score

IDENTIFICATION, PRIORITIZATION

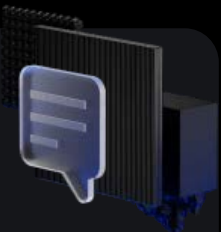
- Brand name mentions
- Violation determination
- Enforcement prioritization



AUTOMATED

RESPONSE

Comprehensive takedown procedure reaching an 85% pre-trial takedown rate on average



AUTOMATED & MANUAL

1 NOTIFICATION

Identify the resource owner and request to remove the detected violation

2 ESCALATION

Use partnership network to enforce the removal of the violation

3 CEASE-AND-DESIST

Obtain an official pre-trial order to take down the detected violation

HOW WE ENFORCE

CYBER-FRAUD FUSION: PROTECCIÓN DE FRAUDE



Protección continua en todos los canales digitales

Página Web o Aplicación Móvil



- Inteligencia de dispositivos
- Detección de bots
- Detección de malware
- Detección de acceso remoto
- Detección de llamadas telefónicas activas
- Integridad del SO
- Comprobación de ID global

Análisis de Login & Password



- Biometría de inicio de sesión
- Comprobaciones antiphishing
- Huella digital del dispositivo
- Geolocalización
- Análisis del tipo de conectividad
- Autenticador sin contraseña

Monitoreo Continuo



- Comportamiento de la navegación en comparación con sesiones anteriores
- Detección de scripts
- Detección Man-in-the-Browser
- Detección de acceso remoto
- Llamada telefónica activa

Monitoreo de Transacciones



- Tarjetas bancarias comprometidas
- Cuentas Mula
- Análisis de vínculos de cuentas (AML)

*Todos los scripts, el tráfico y los datos están encriptados para evitar su interceptación por terceros. No se recogen datos de identificación personal (PII).

CYBER-FRAUD FUSION: PROTECCIÓN DE FRAUDE

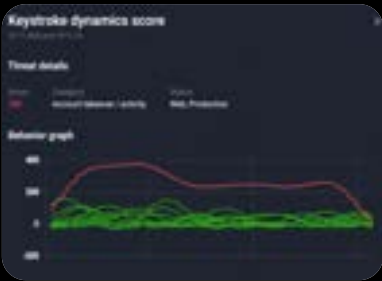


Perfiles completos de comportamiento de clientes

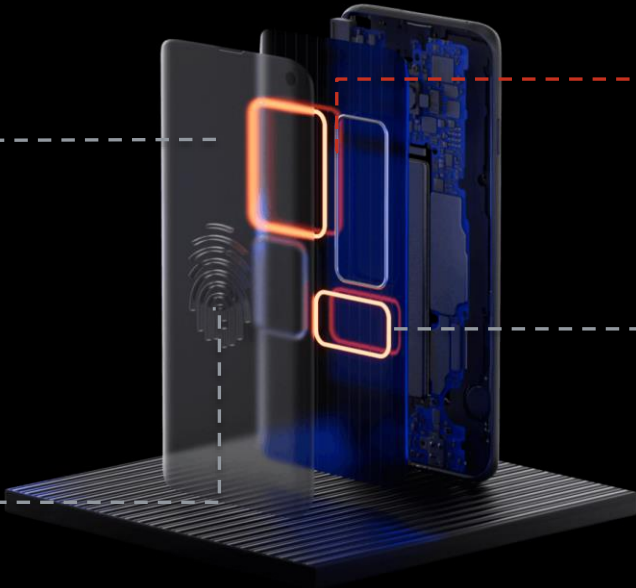
- Análisis del comportamiento
- Puntuación de onboarding
- Perfiles de geolocalización
- Detección de acciones de alto riesgo
- Perfiles de subredes IP
- Dispositivos y cuentas de confianza / bloqueados



Mapa de calor de desplazamiento de usuarios



Gráficos de pulsaciones de teclas de usuarios



Conexiones de dispositivos y cuentas de usuarios



Geolocalización de usuarios

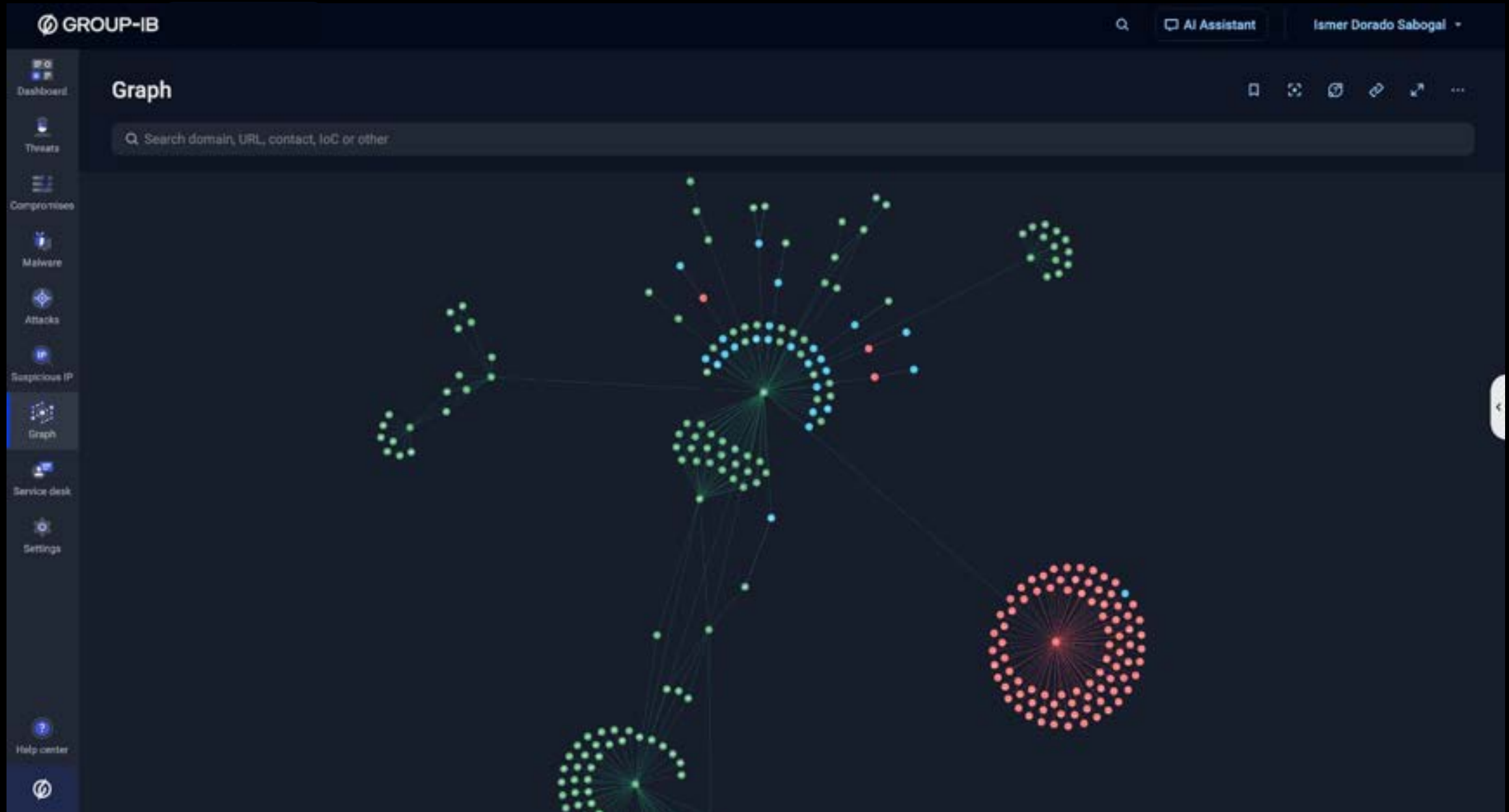
Análisis detallado del entorno técnico del usuario

- Análisis de plataforma cruzada
- Detección de VPN/Proxy
- Detección de programas maliciosos
- Detección de bots
- Huella digital de dispositivo
- Detección de navegadores antidecepción

INTELIGENCIA CONTRA EL FRAUDE

Información sobre suplantación de identidad de dispositivos y redes	Dispositivos y credenciales de usuarios comprometidos	Información sobre esquemas de fraude	Direcciones IP e infraestructura de los estafadores	Páginas de phishing y sitios web fraudulentos	Perfiles de estafadores	Tarjetas de crédito y cuentas bancarias comprometidas

CYBER-FRAUD FUSION: GRAPH



Muchas gracias