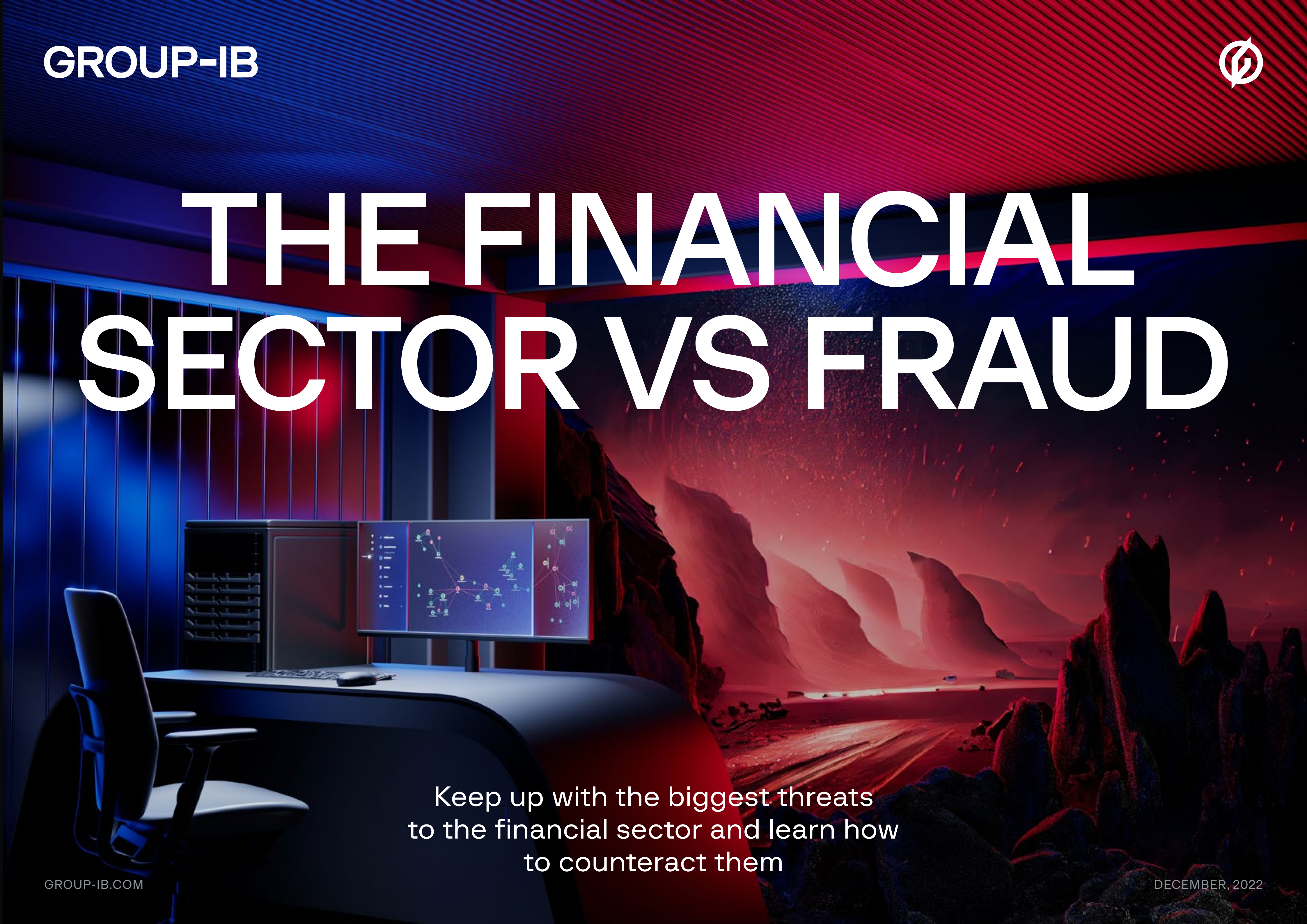
GROUP-IB



THE FINANCIAL SECTOR VS FRAUD

Keep up with the biggest threats to the financial sector and learn how to counteract them

GROUP-IB.COM

DECEMBER, 2022

Introduction

Companies in the financial sector face a particularly hostile threat landscape because they are extremely appealing to cybercriminals.

In order to defend their networks, infrastructure, and customer data effectively, security teams at financial institutions must arm themselves with the latest anti-fraud tools and leverage the most recent intelligence about common techniques and attacks. It is also crucial to understand how attacks are carried out and who is responsible.

This booklet was created to provide the finance industry with detailed information and help businesses stay one step ahead of threat actors.

Happy reading.

Group-IB team

Fraud Protection Business Unit

Methodology

This document was created together with Group-IB anti-fraud analysts and Fraud Protection (FP) specialists. All the insights shared are based on Group-IB's technological expertise; 19 years of experience in cyber-security, anti-fraud and brand protection; thorough and robust analytical work; and the latest results of successfully working with many enterprise customers from the financial sector worldwide.

THREAT 1/5

ACCOUNT TAKEOVER (ATO) ATTACKS

Threat profile

What it is:

Cybercriminals take control of online accounts using stolen usernames and passwords.

How it works:

Attackers usually buy a list of credentials on the dark web. The credentials are often obtained from data breaches, social engineering attacks, phishing, and malware attacks.

How it causes damage:

If hackers gain control of financial services, they can steal money directly using fraudulent payments.

Challenges to your business

Nobody is immune to ATO attacks. Even MFA (multi-factor authentification) doesn’t solve the problem. They are a threat to all organizations that work with user accounts. Given that the attackers are mainly motivated by stealing money, the financial sector is the one that cybercriminals are drawn to the most.

Even if the motivation is almost always the same, the means and tactics used by hackers can differ from case to case. From bad bots and credential stuffing to phishing or social engineering attacks, threat actors exploit all possible ways to deceive users.

The consequences can be truly disastrous and include financial and data loss as well as reputational damage to your brand.

Our response

At Group-IB, we leverage our client-side, AI-powered solution called Fraud Protection, which is supported by a team of experienced fraud analysts and experts. It collects anonymous data from the customer's device in order to get both holistic and granular views about your case.

The thorough data analysis helps obtain reliable results and determine whether the account is being used by a genuine customer or a potential fraudster.

Device fingerprinting

The device fingerprint module collects key attributes about the software and hardware of a device for identification.

Device fingerprints can be used to fully or partially identify individual devices even when persistent cookies (and zombie cookies) cannot be read or stored in the browser.

User behavior analytics

User behavior analytics (UBA) is a cybersecurity process that tracks a system's users to detect insider threats, targeted attacks, and financial fraud. UBA looks at patterns of human behavior and analyzes them to detect anomalies that indicate potential threats.

Continuous monitoring

Fraud Protection monitors user behavior from the moment that the webpage or mobile application is first loaded to the moment that it is closed. The aim is to continuously compare the user's current behavior to their past behavior.

THREAT 2/5 BANKING MALWARE

Threat profile

What it is:

Malware is malicious software designed to damage devices and collect sensitive data. It can infect both computers and smartphones.

How it works:

Different types of malware have different modus operandi and infection methods.
Some types of malware can monitor all operations on the screen, intercept messages, and even listen to everything by controlling the device's microphone.

How it causes damage:

As far as fraud is concerned, most types of mobile malware tend to have the same goals: to obtain authorizations in order to manage the device and intercept login credentials and other important information (SMS, OTPs, etc.).

Challenges to your business

Banking malware has become an extremely advanced and popular tool for fraudsters who have a wide range of tools at their disposal. Banking malware is used for various purposes, from credential stuffing to SMS interception and automated transfers.

Although banking Trojans for PCs are gradually disappearing, the market for Android banking Trojans remains thriving. Android Trojans such as FluBot, TeaBot, and recently MaliBot have caused headaches for financial organizations in Latin America, Europe, and many other regions.

The creators of banking malware shape their operations based on the affiliate program model, thereby attracting many hackers from various regions, especially those with experience in spreading Android Trojans and using them to commit theft.

Our response

Group-IB Fraud Protection offers many ways to eliminate this vulnerability:

Protecting with Mobile SDK

- Gathers information about the application and compares how its certificate deviates from other application certificates
- Matches known Trojan signatures to the app on a device
- Detects suspicious android permissions:
    - PROCESS_OUTGOING_CALLS
    - SEND_SMS
    - WRITE_EXTERNAL_STORAGE
    - READ_EXTERNAL_STORAGE
    - RECEIVE_SMS

The zero-day approach relies on behavior analysis

- Detects overlays
- Detects abuse of the AccessibilityService
- Monitors the default SMS application
- Detects deviations from typical user behavior:
    - The way in which the user navigates your application
    - The movement speed and the pressure on the screen while interacting with your application
    - The task they are performing

THREAT 3/5

WEB INJECTIONS, OR MAN-IN-THE-BROWSER ATTACKS

Threat profile

What it is:

Internet attack involving a Trojan.

How it works:

The Trojan is injected into the victim’s browser through a compromised browser extension or user script.

How it causes damage:

The Trojan can change a website’s appearance as well as manipulate transactions and any data or payment information that users provide.

Challenges to your business

Web injections are one of the most malicious types of MITB attacks. They are designed to intercept data as it goes through secure communication between a user and an online app.

Some injections are harmless, namely those executed by antivirus add-ons or ad plugins. The challenge is to distinguish between malicious injections and harmless ones.

Malicious web injections help hackers steal credentials and other personally identifiable information as well as create requests for additional credentials that are usually not requested by the bank (PIN codes, for example) without triggering the bank's fraud detection algorithms.

Our response

Group-IB Fraud Protection offers many ways to eliminate this vulnerability:

Detects web injections

Fraud Protection notices when there are unauthorized JavaScript code modifications injected by the user's browser, including dynamic and self-destructing JavaScript injections.

Prevents bot activity

Fraud Protection distinguishes between user actions and actions produced by a script. Fraud Protection's dedicated Preventive Proxy module is designed to counteract advanced bot activity.

Recognizes unauthorized activity

If the malicious script uses JavaScript to modify any data entered by the user (transaction amount or payment recipient), FP will detect these changes.

Determines the quality of the injection

Using patented fraud detection algorithms, machine learning, and Group-IB Threat Intelligence, Fraud Protection determines whether the injection is harmless or malicious.

THREAT 4/5

FRAUD ON THE 3DS PAGE

Threat profile

What it is:

3DS (Three-Domain Secure) is a secure authorization protocol for CNP transactions. A 3DS page is the page of the issuing bank where the cardholder is required to enter a confirmation code for the transaction.

How it works:

Three scenarios are possible:

1. The threat actors replace a 3DS page by a fake one that asks users to enter their payment data,
2. The fraudsters confirm multiple payments from one device, and
3. The hackers use bots to scale up attacks.

How it causes damage:

Users risk losing all their money and having their payment data leaked. This type of fraud can also damage the reputation of the financial institution involved and negatively affect customer loyalty.

THREAT 4 FRAUD ON THE 3DS PAGE

Challenges to your business

It was initially assumed that using a 3DS protocol would eliminate fraud for CNP operations, but **fraudsters have learned to bypass this protection.**

There are three possible scenarios for 3DS fraud:

1. The fraudsters replace the 3DS page itself
2. The fraudsters confirm payments with many cards from one device
3. The fraudsters use bots on the 3DS page to quickly confirm multiple payments

Our response

Stop multiple payment confirmations

Fraud Protection identifies devices and detects connections between devices even when fraudsters try to hide such data.

Prevent bot activity on the 3DS page

Fraudsters tend to use bots to automate payments and directly access the API of the ACS server. The Preventive Proxy module combined with Fraud Protection by Group-IB prevents even tricky and large-scale bot activity.

Prevent payments from phishing or illegal resources

Fraud Protection makes it possible to obtain relevant information about fraudulent infrastructure (such as referrer domains) in order to protect banks and end user payment data.

THREAT 5/5

IMPERSONATION SCAMS

Threat profile

What it is:

The fraudster calls the victim from an “official” bank phone number via SIP services with Caller ID spoofing capabilities in order to impersonate a bank employee.

How it works:

The strategy makes the victim more likely to trust the caller and provide the necessary credentials for the fraudster to execute a fraudulent payment.

How it causes damage:

If the victim believes the caller, they might share their login/password or payment card details and the OTPs/TANs needed for payment and other actions requiring approval.

Challenges to your business

Impersonation scams and scam calls are prominent nowadays. Your team members, customers, or users could easily fall victim to them. Fraudsters use various social engineering tools and techniques to gain access to user data and accounts.

Sometimes fraudsters hide their real phone numbers and use VoIP technology to convince users and lure them into the trap. Impersonation scams are likely to lead to financial losses, data leaks, and reputational damage.

Our response

The most effective countermeasures to impersonation scams are:

Detecting caller ID spoofing on the application level

Scam calls can be detected on the mobile application level. Android and iOS provide capabilities to collect meta information about calls while the end user uses the mobile application. With special permission, Android applications can read the call history, phone numbers, the call duration, the type of call (incoming/outgoing), etc., and even collect such data during a call.

Device fingerprinting

Device fingerprinting makes it possible to distinguish the fraudster's device from the victim's usual devices when the fraudster uses disclosed credentials in the bank's web/ mobile application on their device. Device profiling provides additional hints of fraudulent activity.

User behavior analytics

User behavior analytics (UBA) is a cybersecurity process that tracks a system's users to identify insider threats, targeted attacks, and financial fraud. UBA looks at patterns of human behavior and analyzes them to detect anomalies that could indicate potential threats.

Identifying money mule accounts

If the money mule account and the victim use the same bank, then money mule accounts can be detected when they are prepared, using the following non-transactional indicators:

- Access from one device to multiple bank accounts
- The intersection between devices and user accounts that should not be related to work, family, and other relationships

About Fraud Protection

REQUEST A CUSTOM DEMO

Group-IB Fraud Protection is a full-featured solution developed to eradicate digital fraud, protect the digital identities of users, and block malicious bot activity. It acts in real time and across both mobile and web channels using ML technologies, device fingerprinting, and analysis of user behavior and contextual data relating to the user session.

Fraud Protection Leaflet

Download ↗

GROUP-IB

PRODUCT OVERVIEW

FRAUD PROTECTION

Eliminate fraud across all digital channels in real time

GROUP-IB.COM

Call ID Technology Leaflet

Download ↗

GROUP-IB

CALL ID

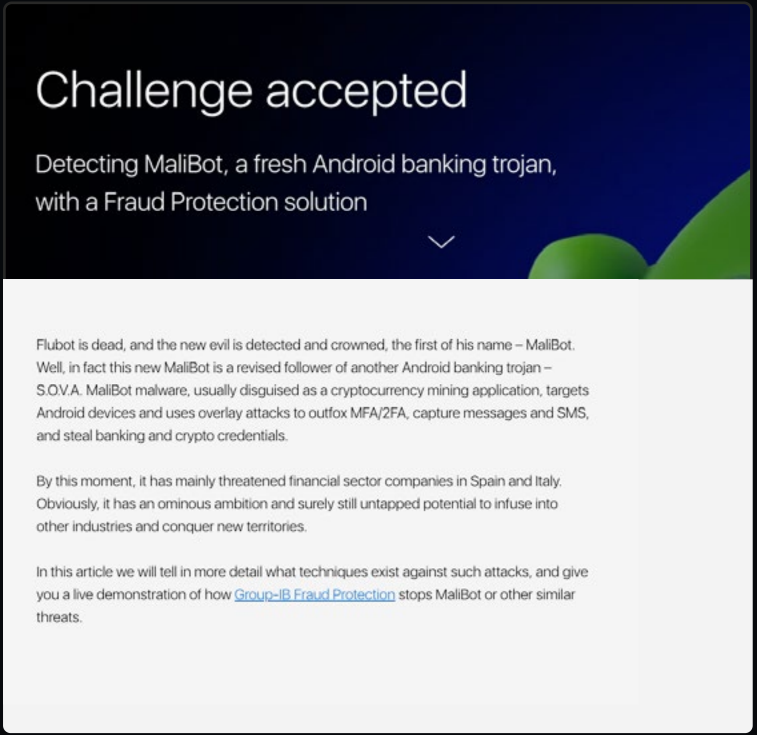
FRAUD PROTECTION

Preemptive protection against phone fraud

GROUP-IB.COM

Banking Trojan Detection – Live demo by Group-IB

Watch ↗



Challenge accepted

Detecting MaliBot, a fresh Android banking trojan, with a Fraud Protection solution

Flubot is dead, and the new evil is detected and crowned, the first of his name – MaliBot. Well, in fact this new MaliBot is a revised follower of another Android banking trojan – S.O.V.A. MaliBot malware, usually disguised as a cryptocurrency mining application, targets Android devices and uses overlay attacks to outfox MFA/2FA, capture messages and SMS, and steal banking and crypto credentials.

By this moment, it has mainly threatened financial sector companies in Spain and Italy. Obviously, it has an ominous ambition and surely still untapped potential to infuse into other industries and conquer new territories.

In this article we will tell in more detail what techniques exist against such attacks, and give you a live demonstration of how Group-IB Fraud Protection stops MaliBot or other similar threats.

Group-IB's mission: Fight against cybercrime

Group-IB is a leading provider of innovations and solutions for detecting and preventing cyberattacks, eliminating fraud, and protecting brands from digital risks worldwide.

19 years of hands-on experience

1,300+ cybercrime investigations worldwide

70,000+ hours of incident response

600+ world-class cybersecurity experts

Active partner in global investigations

INTERPOL

Europol

Recognized by top industry experts

FORRESTER®

kuppingercole ANALYSTS

Gartner®

IDC

FROST & SULLIVAN

Technologies and innovations

Cybersecurity

- Threat intelligence
- Attack surface management
- Email protection
- Network traffic analysis
- Malware detonation
- EDR
- XDR

Anti-fraud

- Client-side anti-fraud
- Adaptive authentication
- Bot prevention
- Fraud intelligence
- User and entity behavior analysis

Brand protection

- Anti-phishing
- Anti-piracy
- Anti-scam
- Anti-counterfeit
- Protection from data leaks
- VIP protection

Intelligence-driven services

Audit & Consulting

- Security Assessment
- Penetration Testing
- Red Teaming
- Compliance & Consulting

Education & Training

- For technical specialists
- For wider audiences

DFIR

- Incident Response
- Incident Response Retainer
- Incident Response Readiness Assessment
- Compromise Assessment
- Digital Forensics
- eDiscovery

Managed Services

- Managed Detection
- Managed Threat Hunting
- Managed Response

High-Tech Crime Investigation

- Cyber Investigation
- Investigation Subscription

GROUP-IB

Preventing and investigating cybercrime since 2003

FIGHT AGAINST
CYBERCRIME

GROUP-IB.COM
INFO@GROUP-IB.COM

APAC
+65 3159 3798

EU & NA
+31 20 226 90 90

MEA
+971 4 508 1605