Fraud shall not pass!

kaspersky

kfp@kaspersky.com

Fraud against individuals – concern of an enterprise

High availability and low price for personal data

High involvement in cashless payments of users with their lack of financial literacy

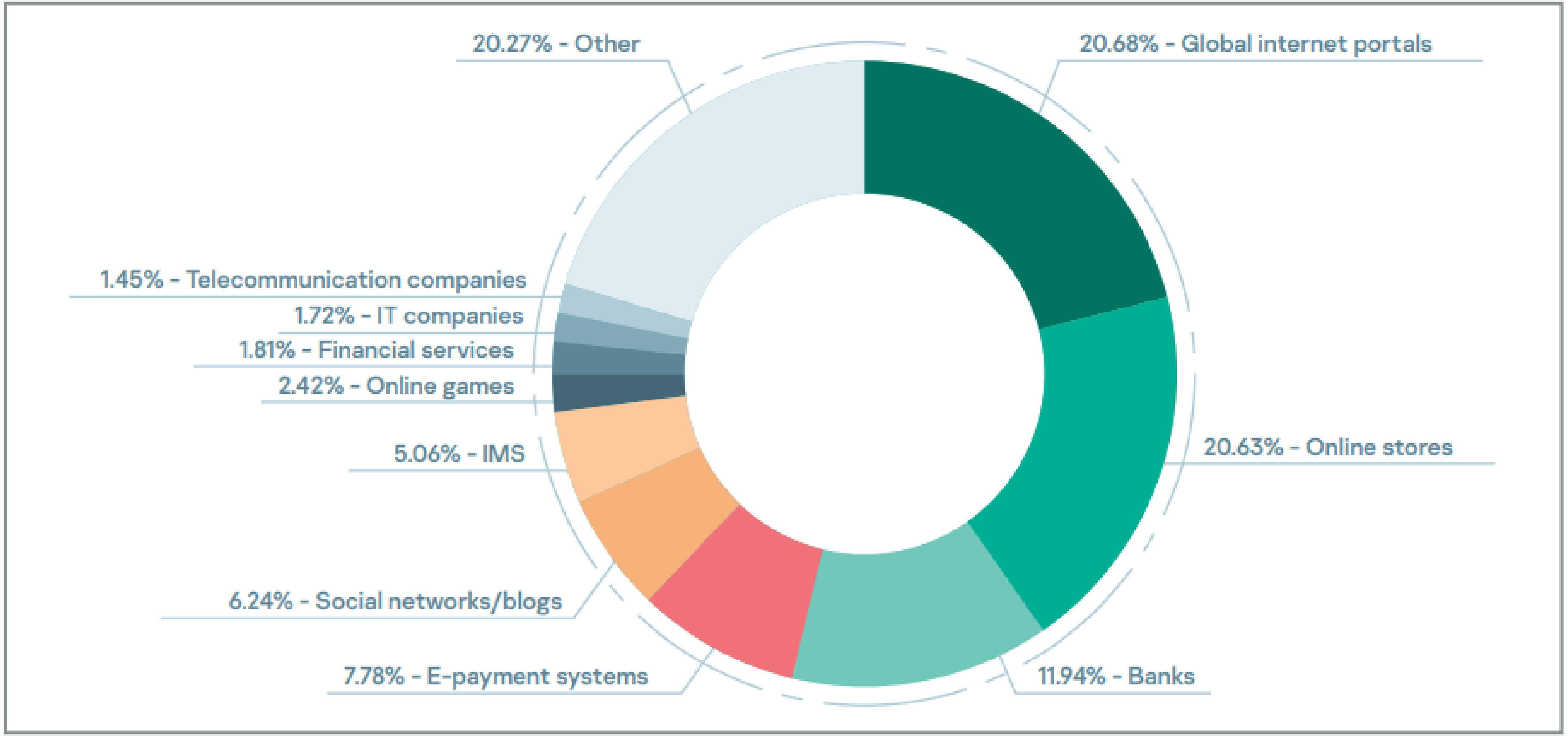
Some facts and statistics

Access to a stolen online banking account with a minimum balance of $2000 can cost $65 on the dark web.

95% of users are confident that their personal data is being provided with an excellent level by the bank.

Kaspersky experts connect these changes with the lockdown measures due to the pandemic – at home most of the time, people turned to online shopping and digital entertainment.

Organizations whose users were targeted by phishers



Behavior and threat analysis

Level	User session characteristics				
Device	Fingerprint Root/Jailbreak/Emulator	Position in network		Device Spoofing	
Threats	Network connectivity anomalies Content changing	Malware Brute Force\Credential Stuffing		Fraud Calls	Remote access Bots
Relationships and correlations	Anonymization	Fast travel		Search for relationships with other users and devices	
Global characteristics	IP reputation (Kaspersky Threat Intelligence)	User reputation (KFP)	Malicious/Phishing/ Botnet C&C URL Feeds	Device reputation(KFP)	Phone number reputation (KWC*)
Passive biometrics and behavioral analysis	Anomalies in the user's historical profile	Remote control Bots (imitation of human behavior)		Navigation analysis	Speed and frequency of interaction with the online service

Machine learning techniques

Account & Device profiling. Identify typical and stable devices and user accounts.

Static and dynamic device identification. Exact and probable approaches.

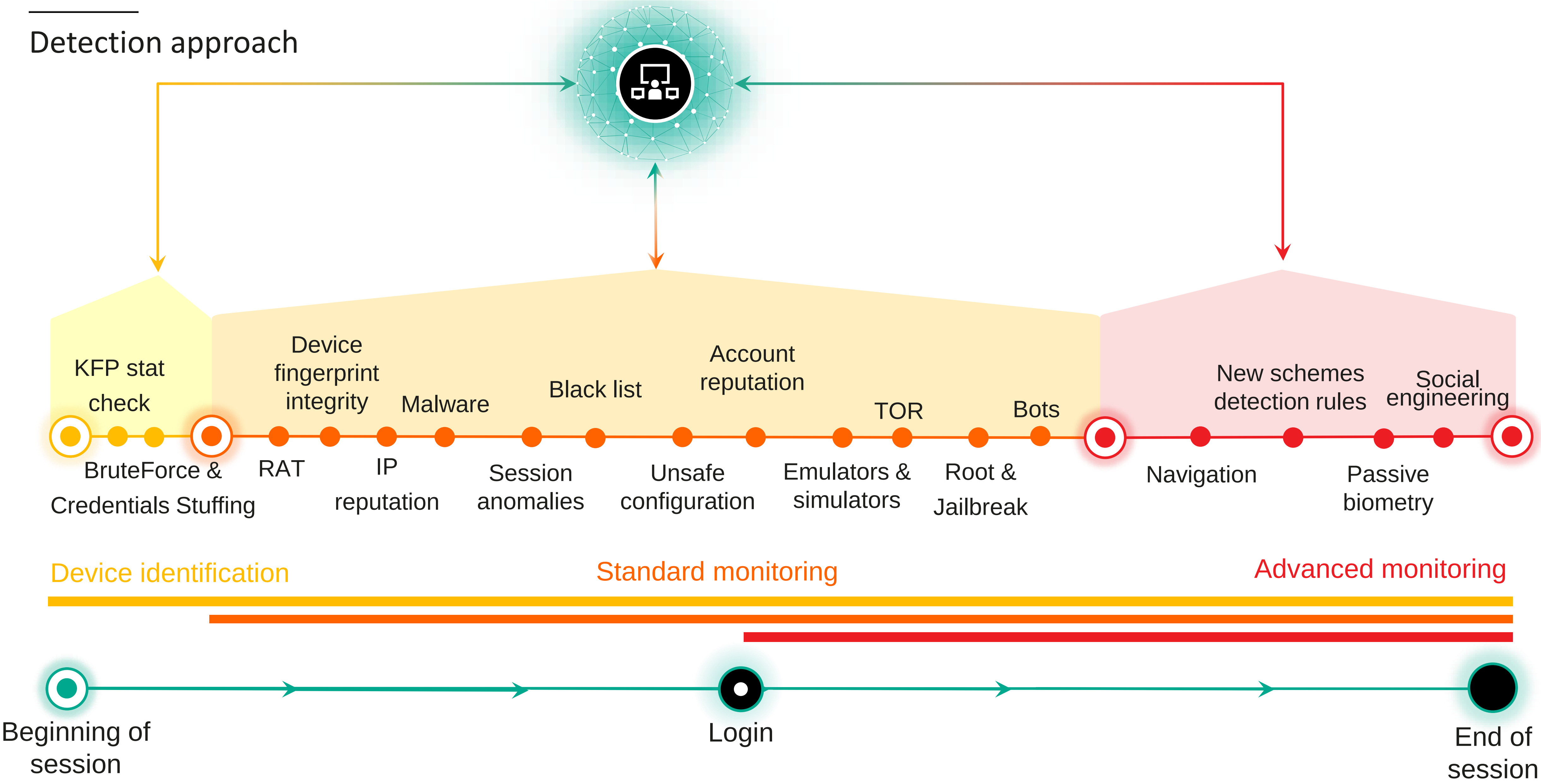
Behavioral analysis. Semantic analysis of actions: which form field is activated, etc.

Passive biometrics. Analysis of how a device is used.

Malware detection

Traffic anomalies. Evaluation of all sessions for their legitimacy and authenticity.

Detection approach



What is Kaspersky Fraud Prevention?

We provide session-based antifraud that analyses the user’s device and behavior to benefit both the business and its security.

Reduced operating costs

Flexible setting of rules

Machine learning

Kaspersky Fraud Prevention

Advanced Authentication

Improving the convenience of service

Account theft protection

Reducing the cost of the second factor of authentication

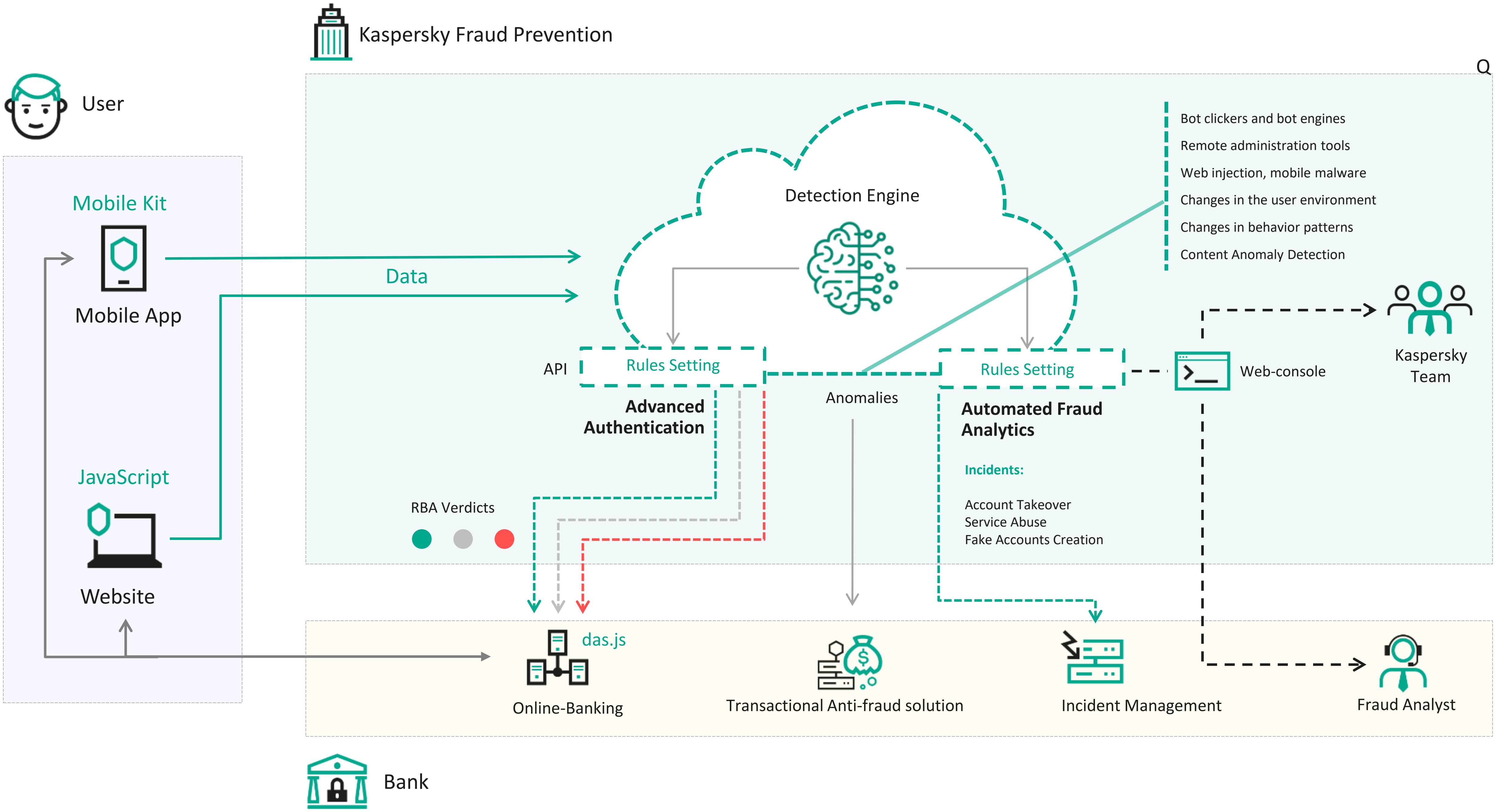
Rapid reaction

Automated Fraud Analytics

Real-time anomaly and incident detection

Identification of account compromise, fraudulent accounts and money laundering

Detailed analytics on incidents for investigation



Kaspersky Fraud Prevention

User

Mobile Kit

Mobile App

JavaScript

Website

Data

Detection Engine

- Bot clickers and bot engines
- Remote administration tools
- Web injection, mobile malware
- Changes in the user environment
- Changes in behavior patterns
- Content Anomaly Detection

API

Rules Setting

Advanced Authentication

Anomalies

Rules Setting

Automated Fraud Analytics

Incidents:

Account Takeover
Service Abuse
Fake Accounts Creation

RBA Verdicts

● ● ●

Web-console

Kaspersky Team

das.js

Online-Banking

Transactional Anti-fraud solution

Incident Management

Fraud Analyst

Bank

Q

Key use cases

Good user verification. Seamless digital experience for legitimate users.

Account takeover detection. Proactive real-time discovery of early signs or ATO.

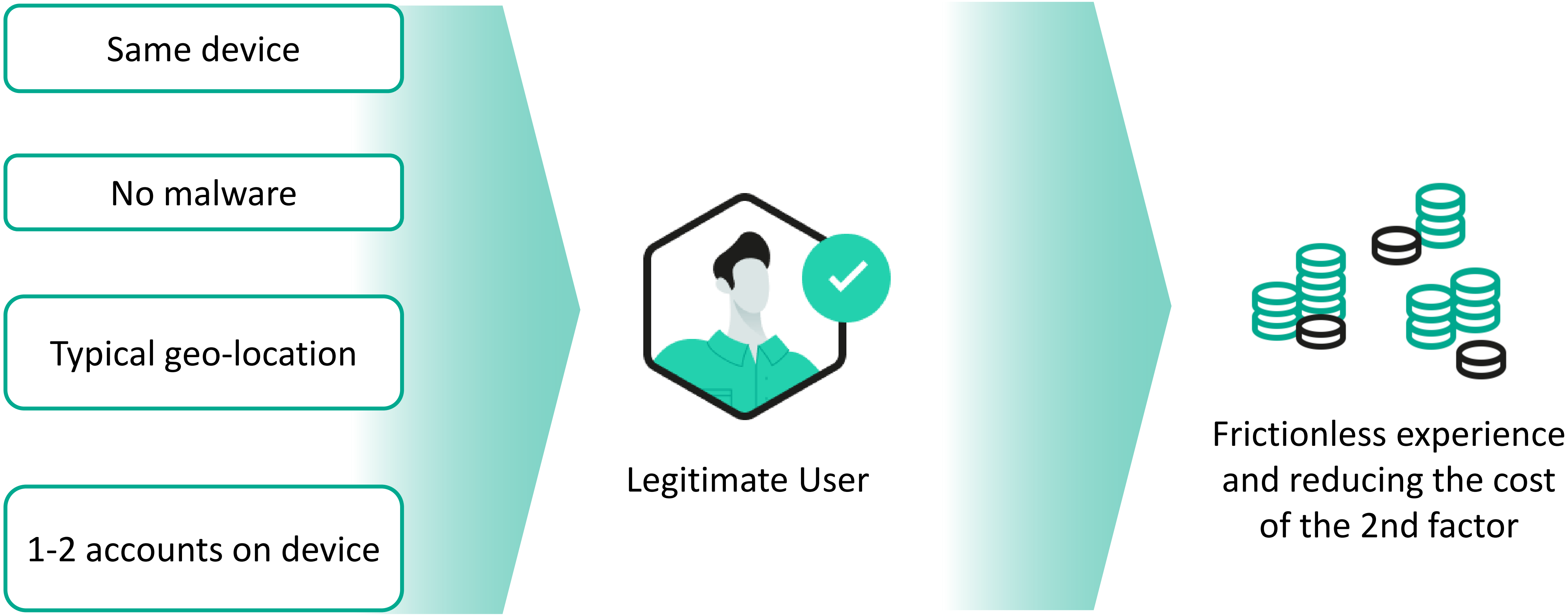
New account fraud detection. Identification of multiple fraudulent accounts and their interconnection.

Enrichment of analytics. Additional layer of data about risks and fraudulent activity to enrich internal systems (EFM, SIEM).

Early signs of money laundering detection. Possibility of combining session and business data and organizing interbank exchange.

Fighting new fraudulent schemes. The ability to respond quickly to new fraud approaches and new regulatory requirements.

Reducing the cost of the 2nd factor up to 85%



Same device

No malware

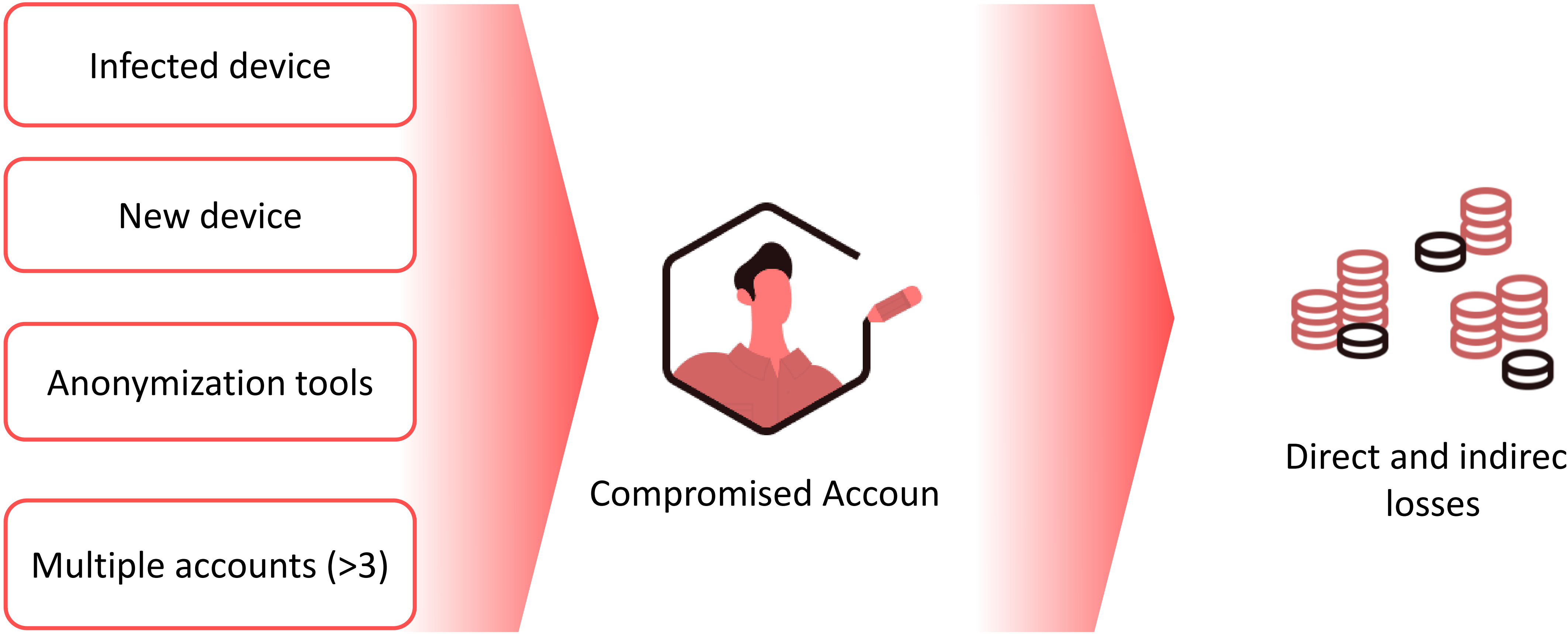
Typical geo-location

1-2 accounts on device

Legitimate User

Frictionless experience and reducing the cost of the 2nd factor

Signs of account compromise



Infected device

New device

Anonymization tools

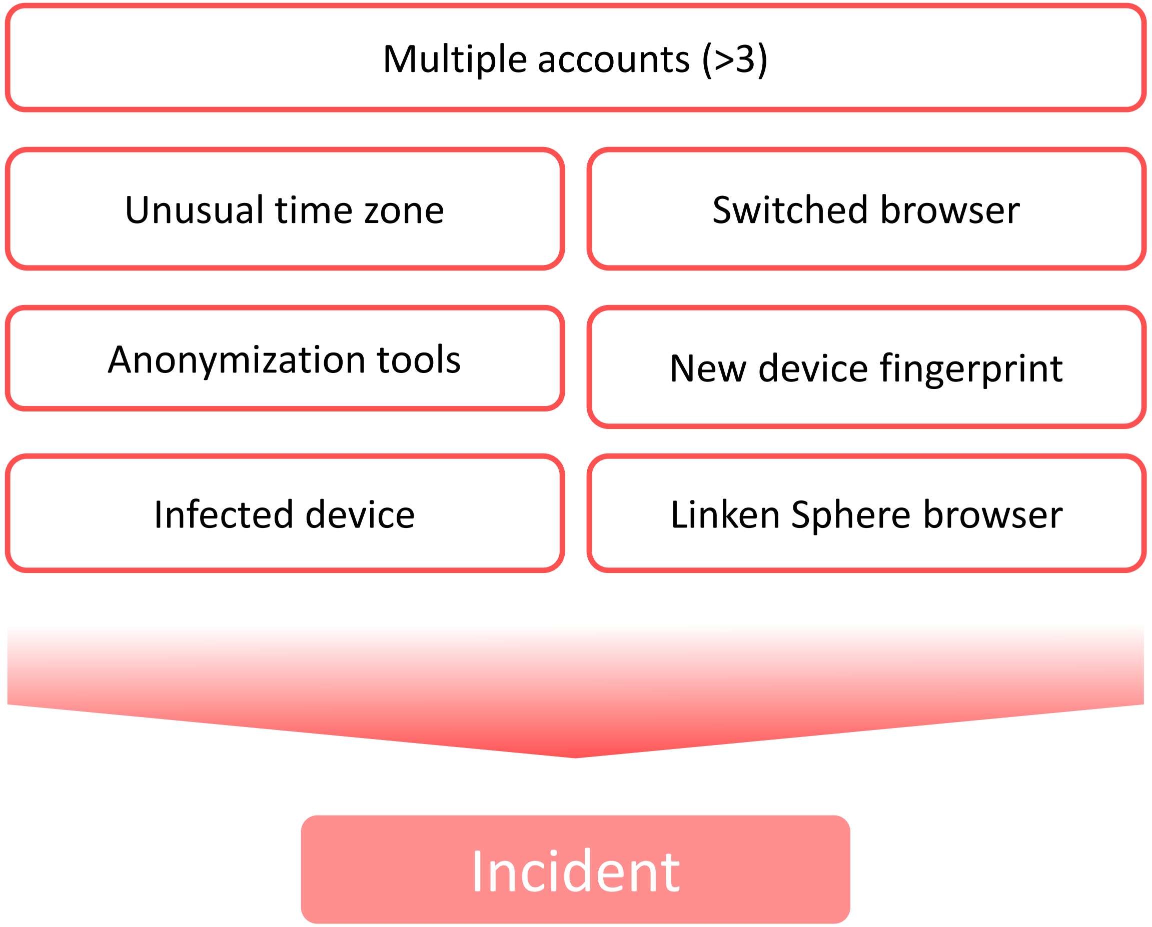
Multiple accounts (>3)

Compromised Accoun

Direct and indirect losses

Configuring Fraud Detection Rules

Automated Fraud Analytics



Multiple accounts (>3)

Unusual time zone

Switched browser

Anonymization tools

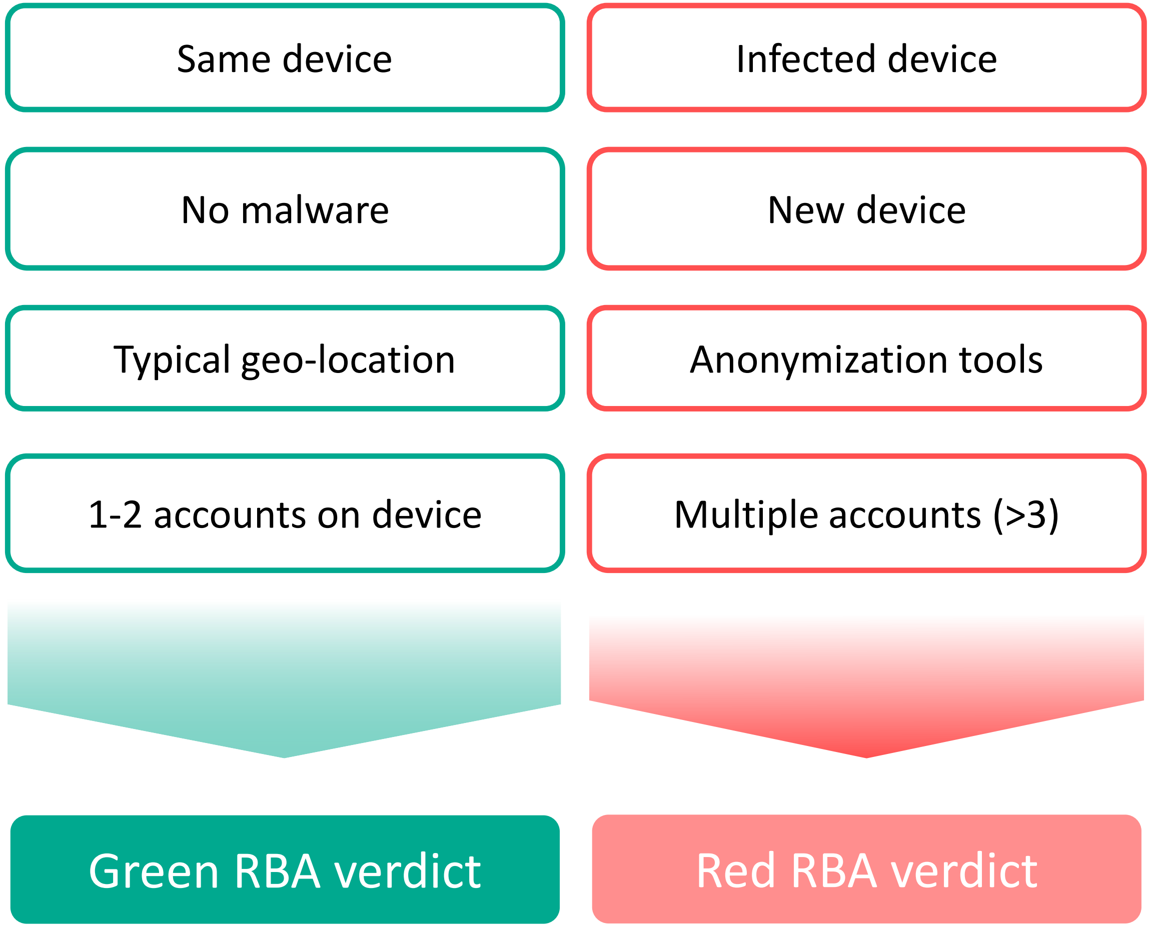
New device fingerprint

Infected device

Linken Sphere browser

Incident

Advanced Authentication



Same device

Infected device

No malware

New device

Typical geo-location

Anonymization tools

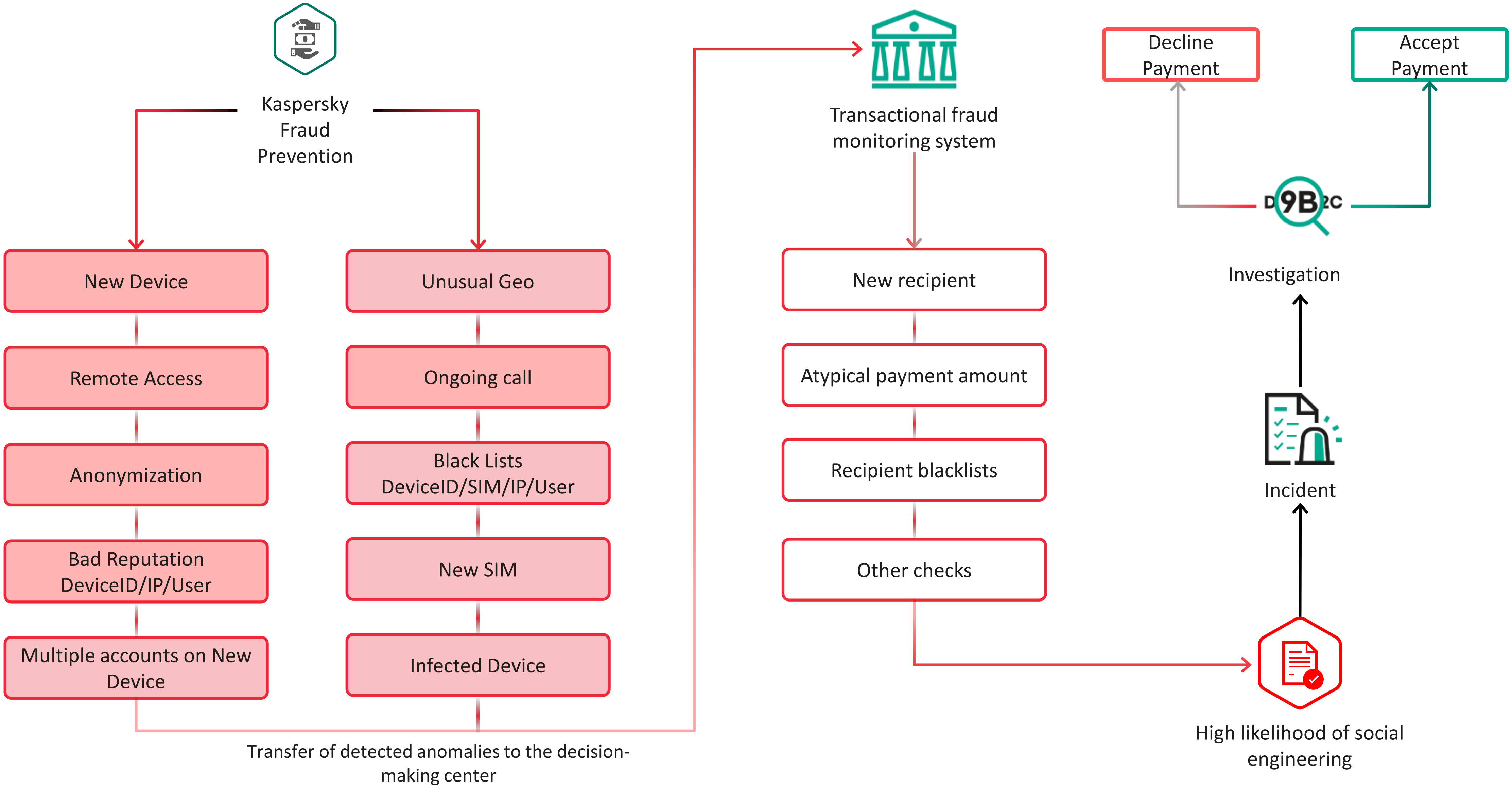
1-2 accounts on device

Multiple accounts (>3)

Green RBA verdict

Red RBA verdict

170+ categories of suspicious activity



Kaspersky Fraud Prevention

New Device

Remote Access

Anonymization

Bad Reputation DeviceID/IP/User

Multiple accounts on New Device

Unusual Geo

Ongoing call

Black Lists DeviceID/SIM/IP/User

New SIM

Infected Device

Transfer of detected anomalies to the decision-making center

Transactional fraud monitoring system

New recipient

Atypical payment amount

Recipient blacklists

Other checks

High likelihood of social engineering

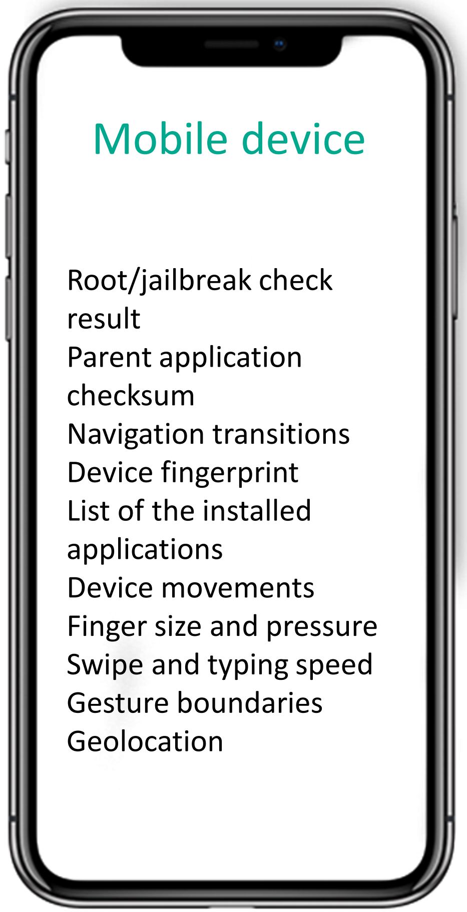
Incident

Investigation

Decline Payment

Accept Payment

Short list of collected parameters for device fingerprint profiling



Mobile device

Root/jailbreak check result
Parent application checksum
Navigation transitions
Device fingerprint
List of the installed applications
Device movements
Finger size and pressure
Swipe and typing speed
Gesture boundaries
Geolocation

Mobile channel

Operator: SIM-card, operator’s details

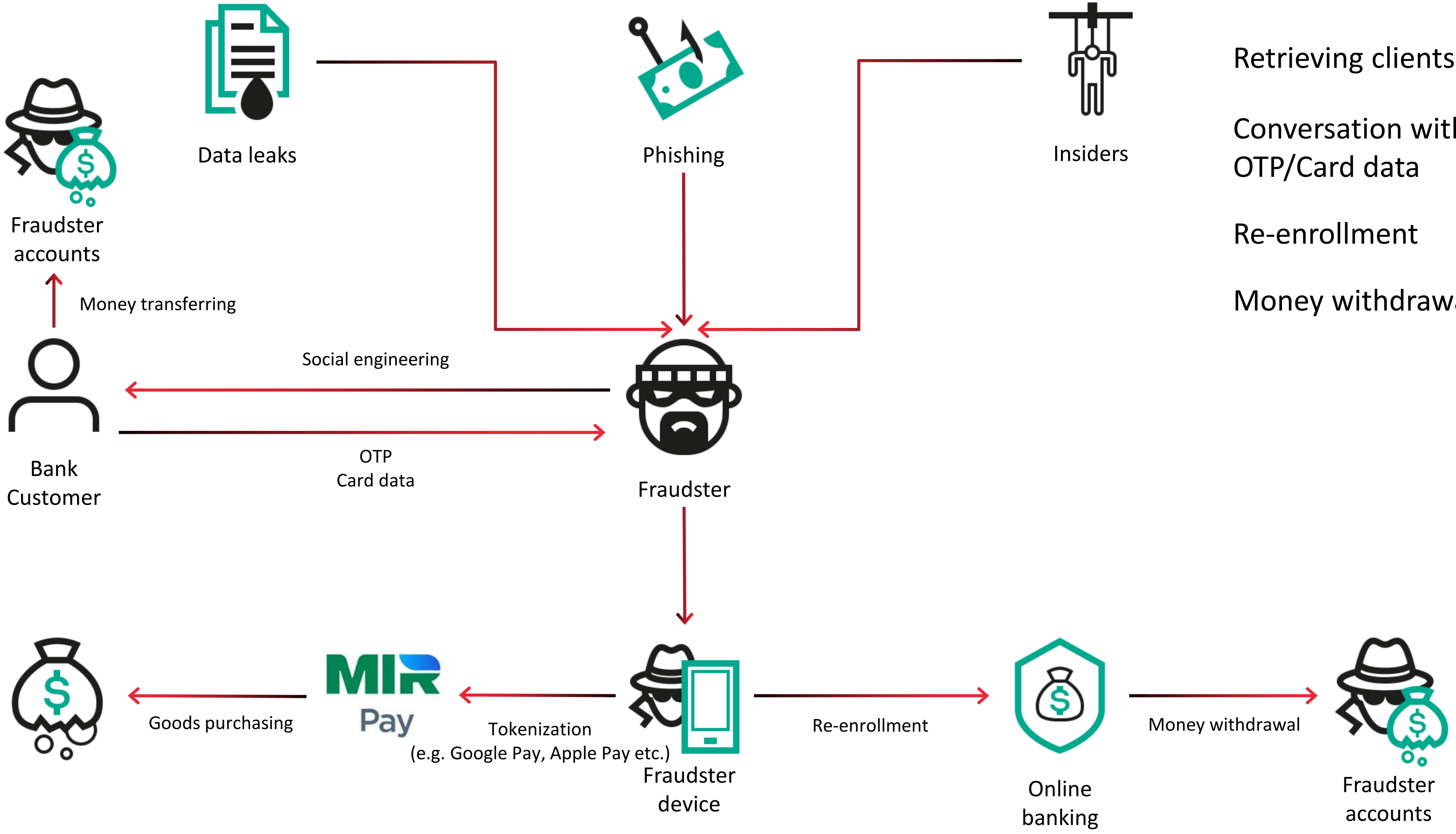
Hardware: CPU, display, memory, input devices and sensors

System: version, environment, specific parameters

Web channel

OS, UserAgent, language, display, time zone, fonts,
Browser info, Navigation transitions
Fonts installed, Display info
Canvas info, WebGL parameters
HTML tags, HTML forms,
input fields and Iframes checksums
DOM changes, Password field changes
Device ID, Session ID
Mouse moves and clicks
Keyboard strokes

Typical social engineering scheme



Retrieving clients data

Conversation with client, luring out OTP/Card data

Re-enrollment

Money withdrawal

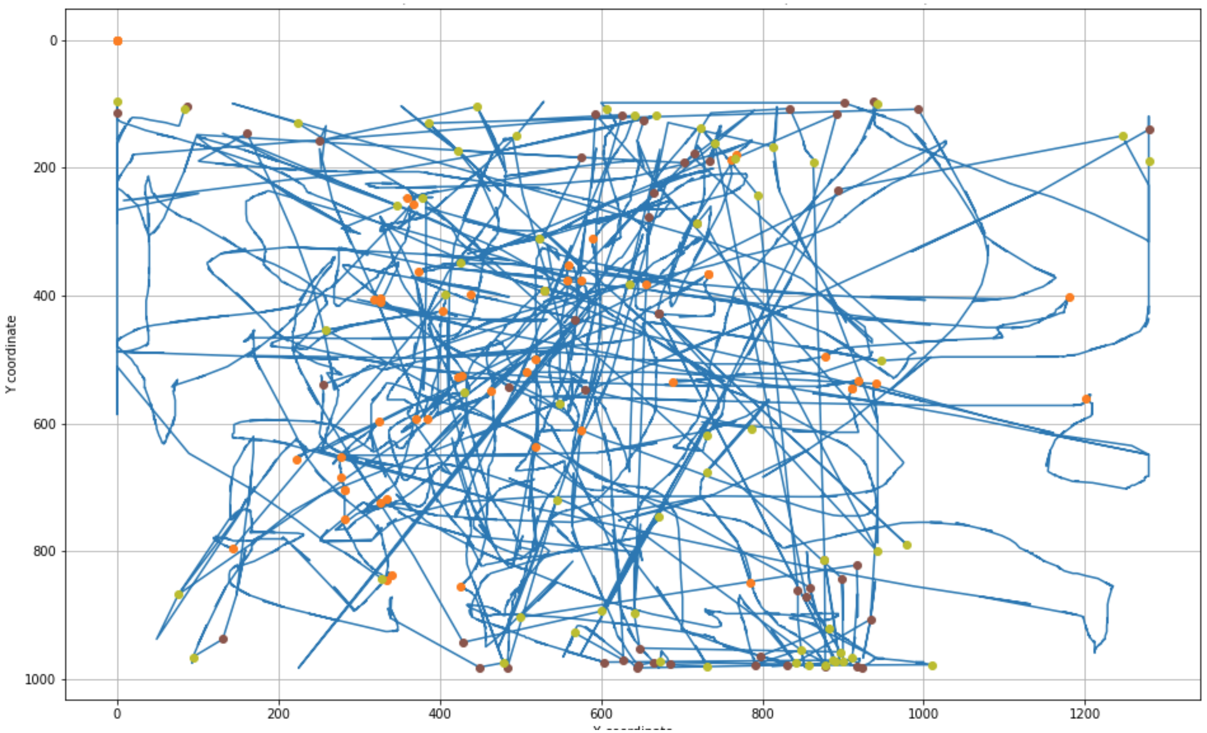
Social engineering scenarios in online-banking

Rescuer - to provide assistance, “rescuers” ask the client to verify themselves through a code sent in an SMS or push-notification under the idea of verifying the client, stopping a suspicious transaction or transferring funds to a “safe account”.

Police officer - potential victims tend to get nervous and surprised when they get contacted by police regarding “an occurring financial crime/theft” and they are more willing to share personal information.

Investor - calling clients, scammers offer them to make quick money by investing in crypto-currency or in company shares directly from the client's account without additional calls to the bank branch.

Kaspersky Fraud Prevention Cases



This was a 10 minute session. Lots of enter/leave events.

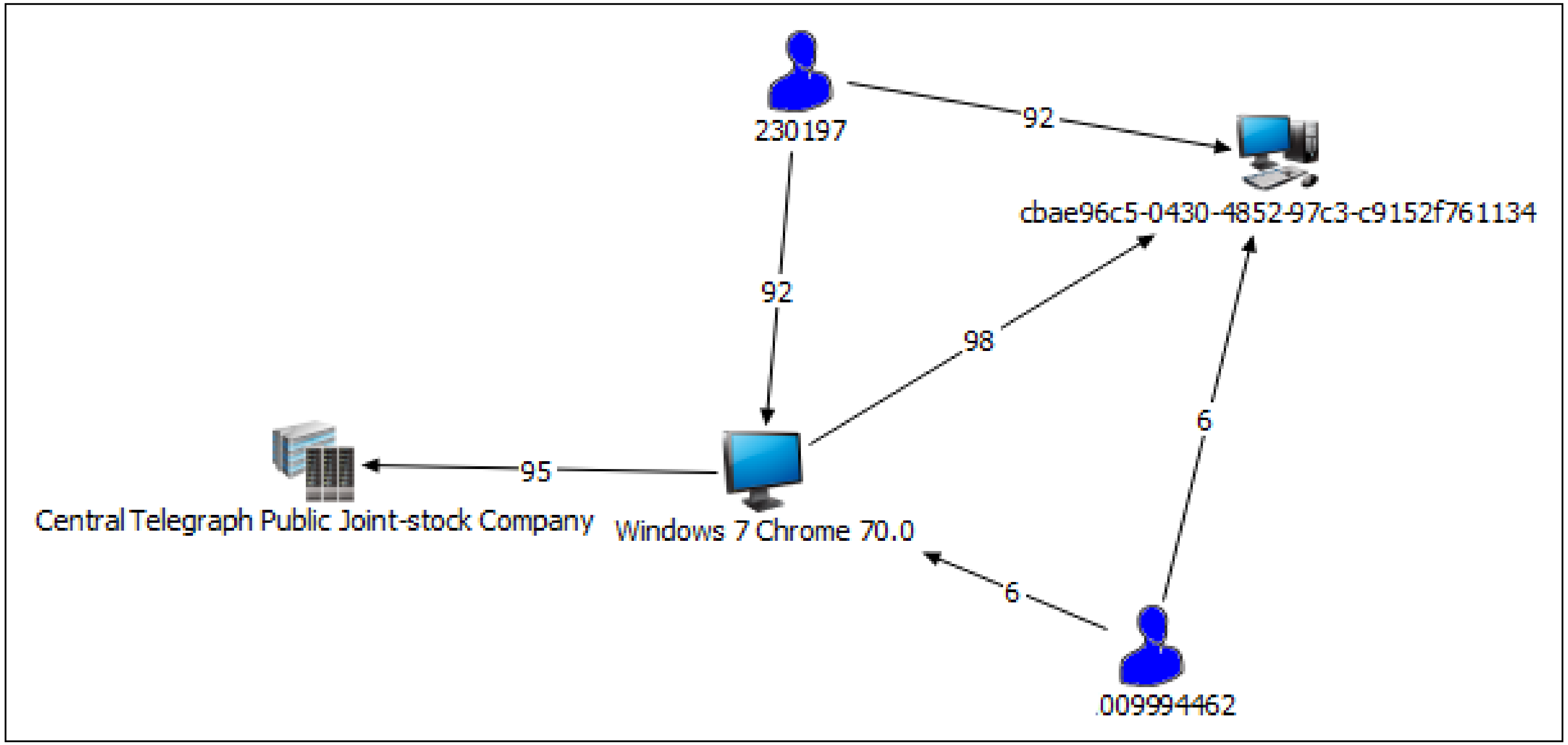
Call from a bank

The wrong bank

Spoofed IP/SIP number

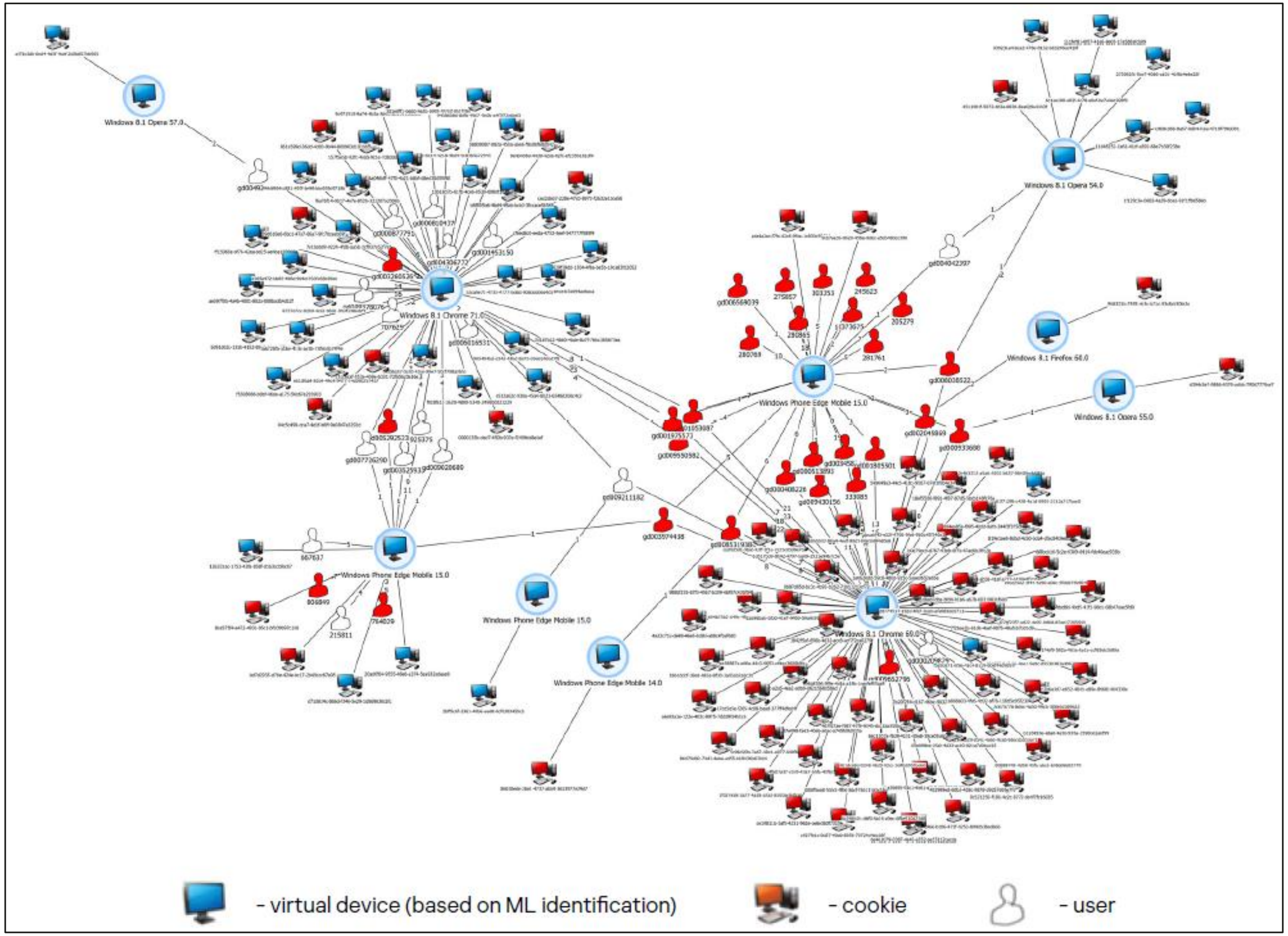
Accessing account

How does a legitimate user device map look


230197
92
cbae96c5-0430-4852-97c3-c9152f761134
92
98
6
95
Central Telegraph Public Joint-stock Company
Windows 7 Chrome 70.0
6
009994462

A normal user usually has no connections with other user accounts or devices. One person can access the service from several devices - yes, but it is usually limited to a reasonable number - from 3 to 5 devices.

Money laundering and mules


Windows 8.1 Opera 57.0
Windows 8.1 Chrome 71.0
Windows 8.1 Opera 54.0
Windows Phone Edge Mobile 15.0
Windows 8.1 Firefox 60.0
Windows 8.1 Opera 55.0
Windows Phone Edge Mobile 15.0
Windows Phone Edge Mobile 15.0
Windows Phone Edge Mobile 14.0
Windows 8.1 Chrome 69.0
- virtual device (based on ML identification)
- cookie
- user

One device can be used to control hundreds of transit accounts.

By implementing global device reputation and global entity linking methods, Kaspersky Fraud Prevention was able to uncover large abnormal clusters of devices and accounts.

Effective counteraction methods

Analysis of user interaction with an online service based on passive biometrics and behavioral analytics technologies

Building a digital user profile, analyzing its devices and environment

Detecting fraudulent calls to the user and notifying him

Analysis of domains from which the online service is accessed

User and device reputation analysis

Detection of malware on the user's device

Transferring data about suspicious activity in user sessions to EFM\SIEM\CRM

Increasing user awareness through an online service using educational promotions

The Total Economic Impact™ of Kaspersky Fraud Prevention

A Forrester Total Economic Impact™
Study Commissioned By Kaspersky
June 2020
The Total Economic Impact™ Of Kaspersky Fraud Prevention
Cost Savings And Business Benefits Enabled By Fraud Prevention
FORRESTER

Reduced fraud losses, totaling $3.4 million over three years.

Savings in customer service interactions, totaling $121K over three years.

Savings from eliminating second-tier authentication for verified customers, totaling $17.6K over three years.

available at kfp.kaspersky.com/total-economic-impact/

A Forrester Total Economic Impact™
Study Commissioned By Kaspersky
June 2020

The Total Economic Impact™ Of Kaspersky Fraud Prevention

Cost Savings And Business Benefits Enabled By Fraud Prevention

FORRESTER

Thank you for your attention!

Use the QR code below to access The Total Economic Impact™ of Kaspersky Fraud Prevention PDF