GROUP-IB

The Evolution of Identity Theft

How Criminals are Redefining Identity Theft in 2025 and Beyond

GROUP-IB

Maximilian Bode

Head of Pre-Sales

Linkedin

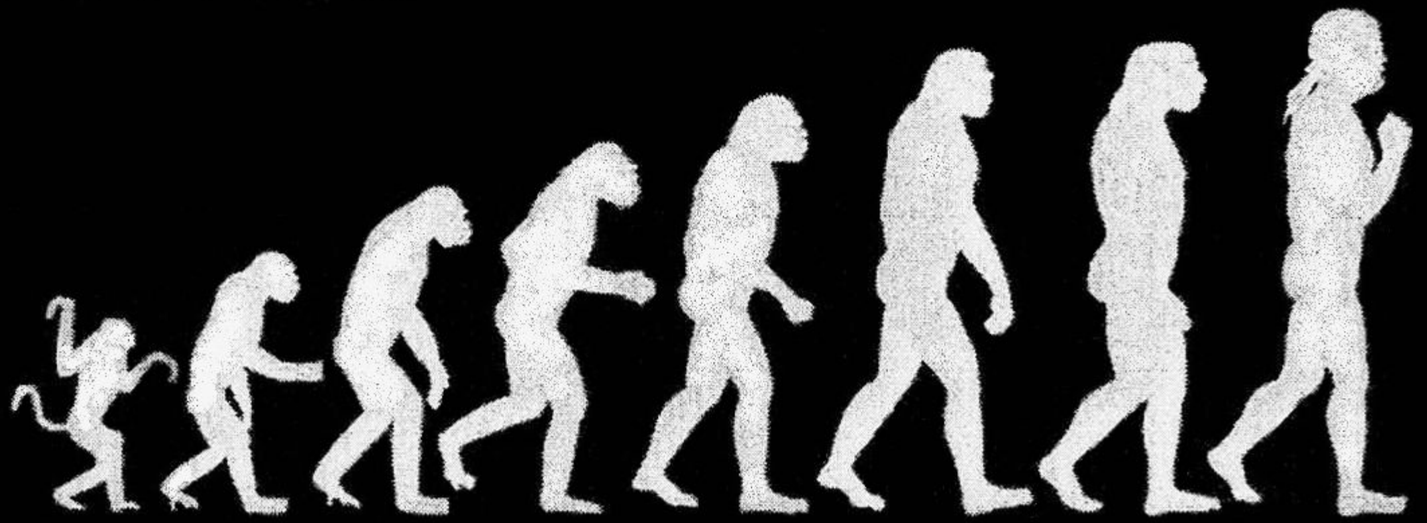
GROUP-IB

The Past of Identity Theft

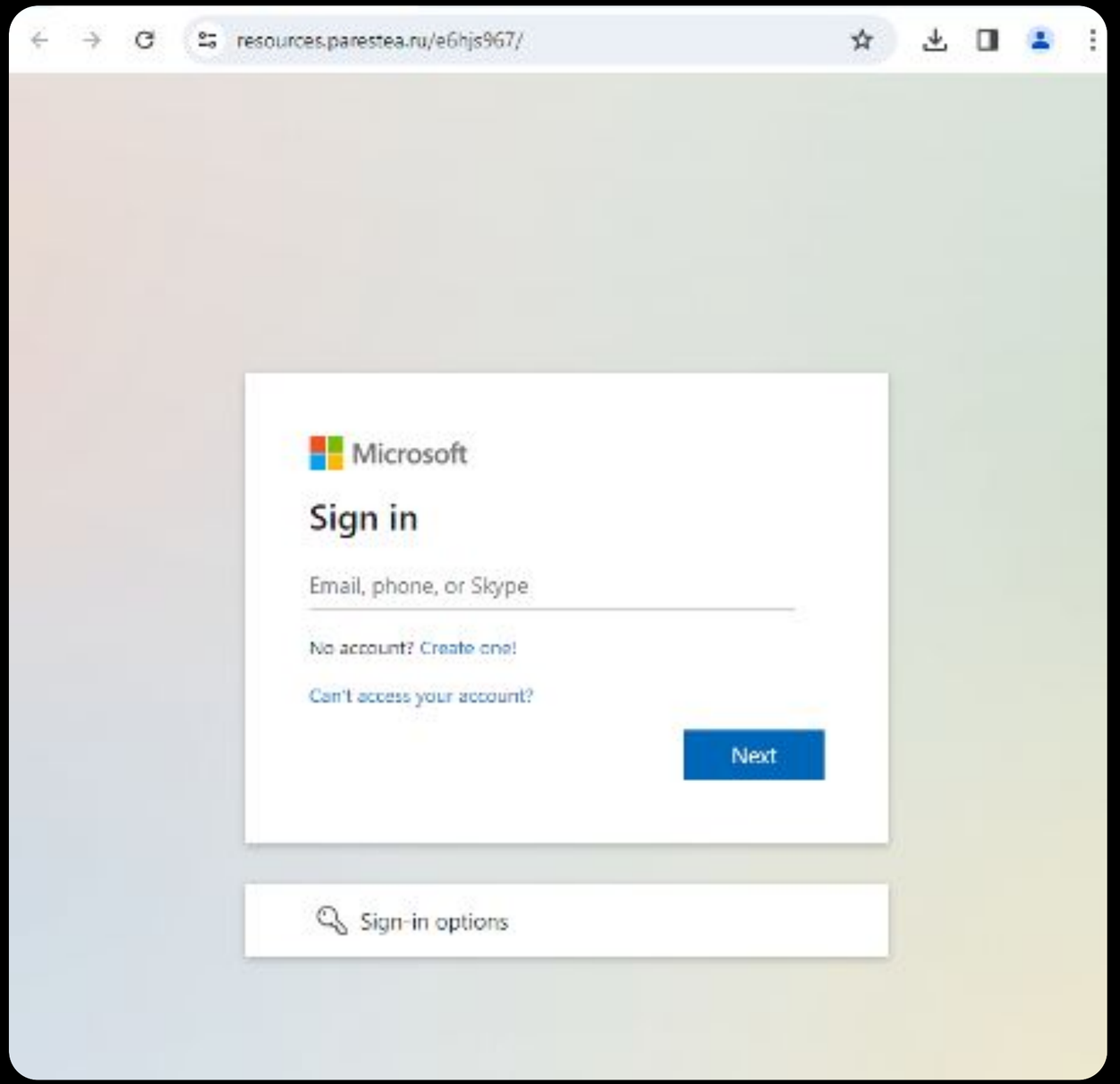
Introduction

GROUP-IB

- Account Credential Theft
- Peeling the Authentication Onion
- Identity-Based Attacks



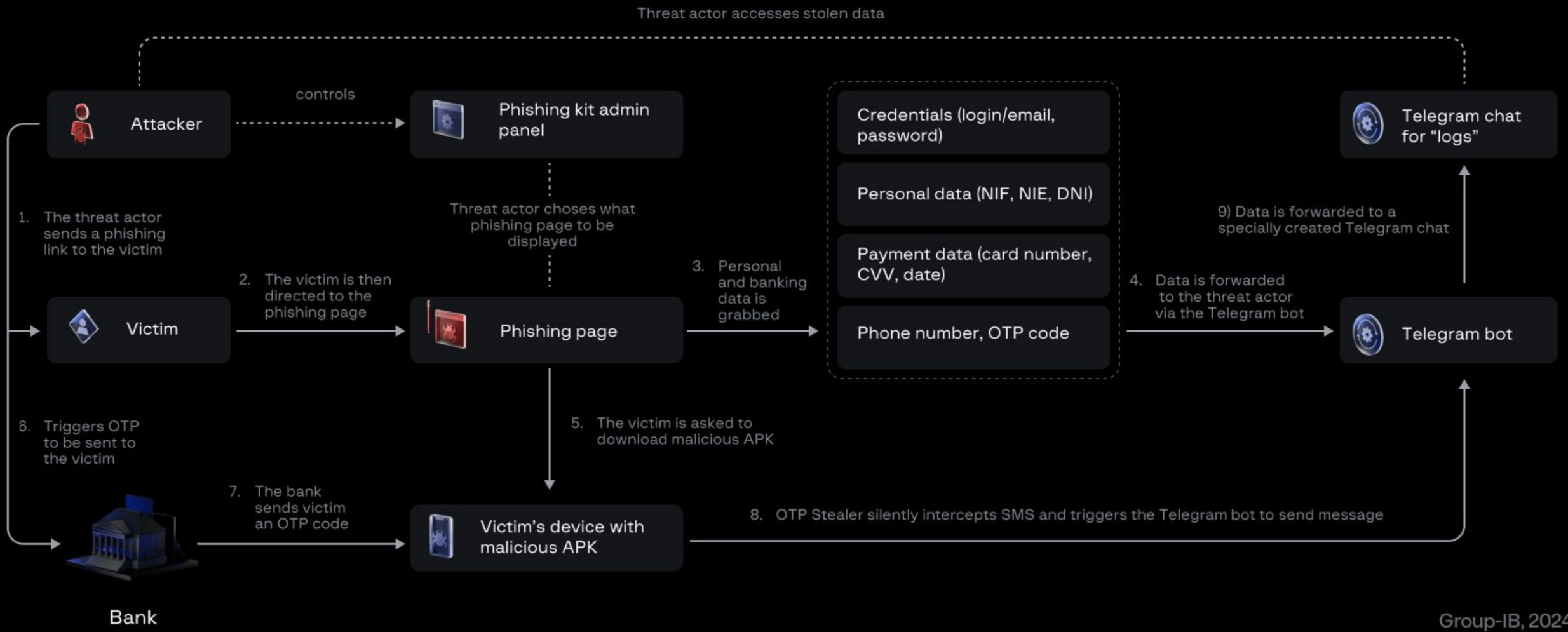
Account Credential Theft



Account Credential Theft

GROUP-IB

Peeling the Authentication Onion

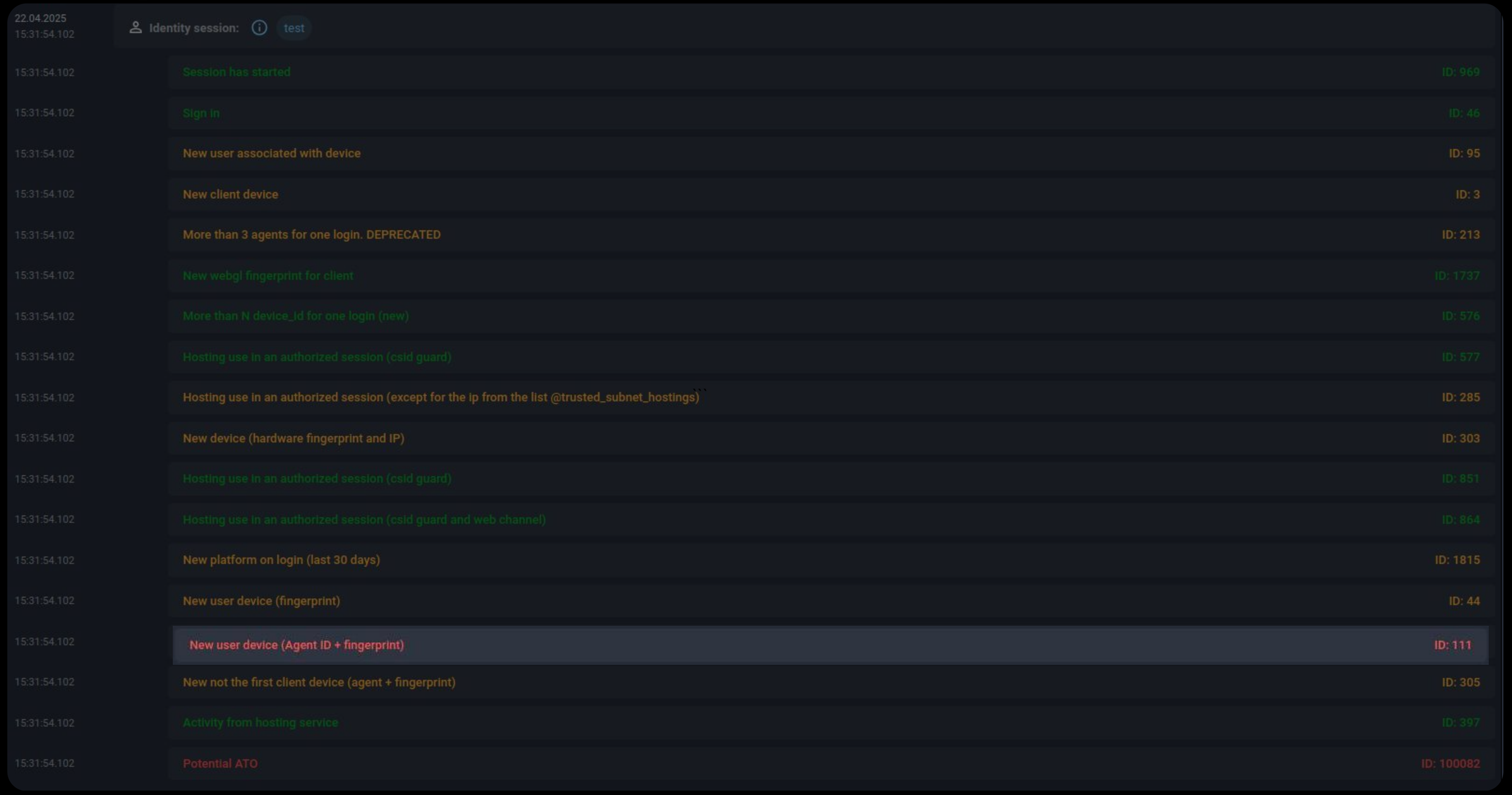


Peeling the Authentication Onion

GROUP-IB

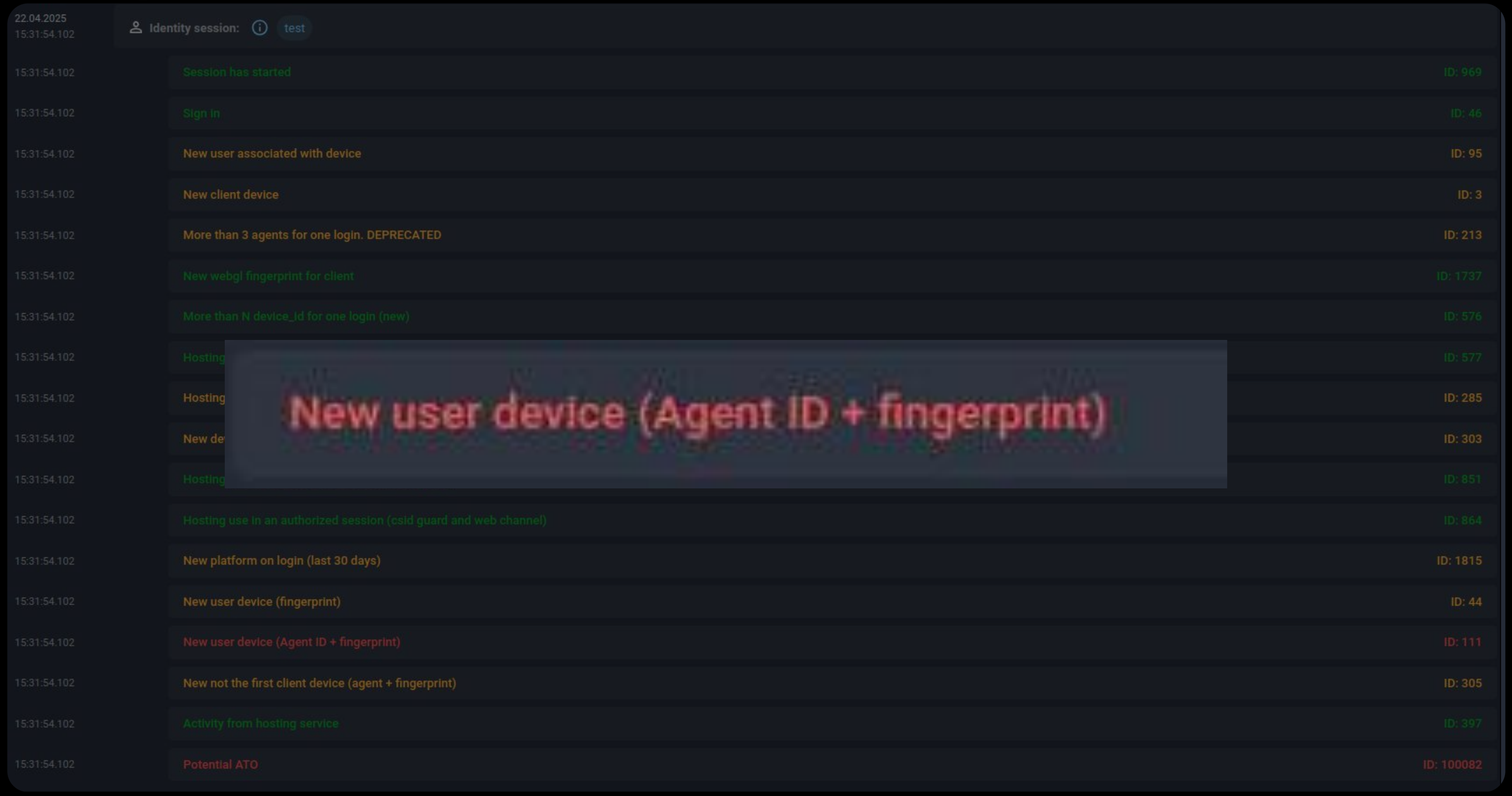
Peeling the Authentication Onion

GROUP-IB



Peeling the Authentication Onion

GROUP-IB



Identity-Based Attacks

GROUP-IB

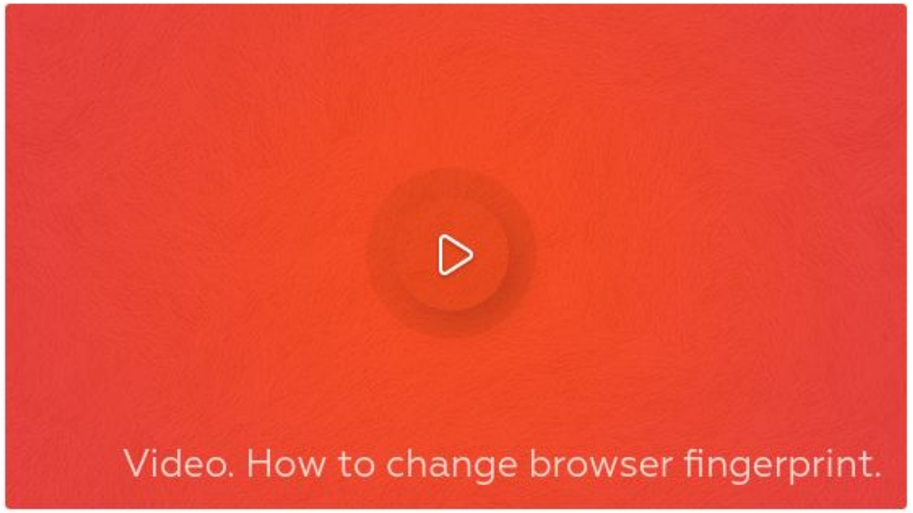
https://fp.bablosoft.com/#home

HOME ABOUT CAPABILITIES TESTING KEYS PRICING FAQ

ABOUT

FingerprintSwitcher

Browser fingerprints - is a technique, which allows to identify user by a combination of browser properties, like: resolution, plugins list, fonts, navigator properties, etc.



FingerprintSwitcher service allows to replace all those properties and thus you will act as a completely new user. It also means that site will be unable to identify you among other users. Service provides access to database with about **50,000 fingerprints** obtained from real devices which is constantly updated.

more →

Identity-Based Attacks

GROUP-IB

Web page or Mobile App Loading

- Device Intelligence
- Bot Detection
- Malware Detection
- Remote Access Detection
- Active phone call detection
- OS integrity
- Global ID check

User Enter Login & Password

- Login Biometrics
- Anti-phishing Checks
- Device Fingerprinting
- Geo Location
- Connectivity type Analysis
- Passwordless Authenticator

Continuous Monitoring

- Navigation behavior compared to previous sessions
- Script detection
- Man-in-the-Browser detection
- Remote access detection
- Active phone call

Transaction Monitoring

- Compromised Credit Card
- Mule Accounts
- Account link Analysis (AML)

GROUP-IB

Arms Race

GROUP-IB

Emerging and Existing Methods of Identity Theft

Introduction

- Mobile Trojans
- Biometric(k)s
- Device Fingerprint Theft

Mobile Trojans

GROUP-IB

PROFILE

20 GROUP-IB

GoldFactory

Language
Chinese-speaking

Activity
June 2023 – Present

Specialization
Mobile banking Trojans

Developed malware
- GoldDigger
- GoldDiggerPlus
- GoldKefu
- GoldPickaxe

Targeted operating systems
iOS, Android

Goals
- Harvesting sensitive data
- Money theft

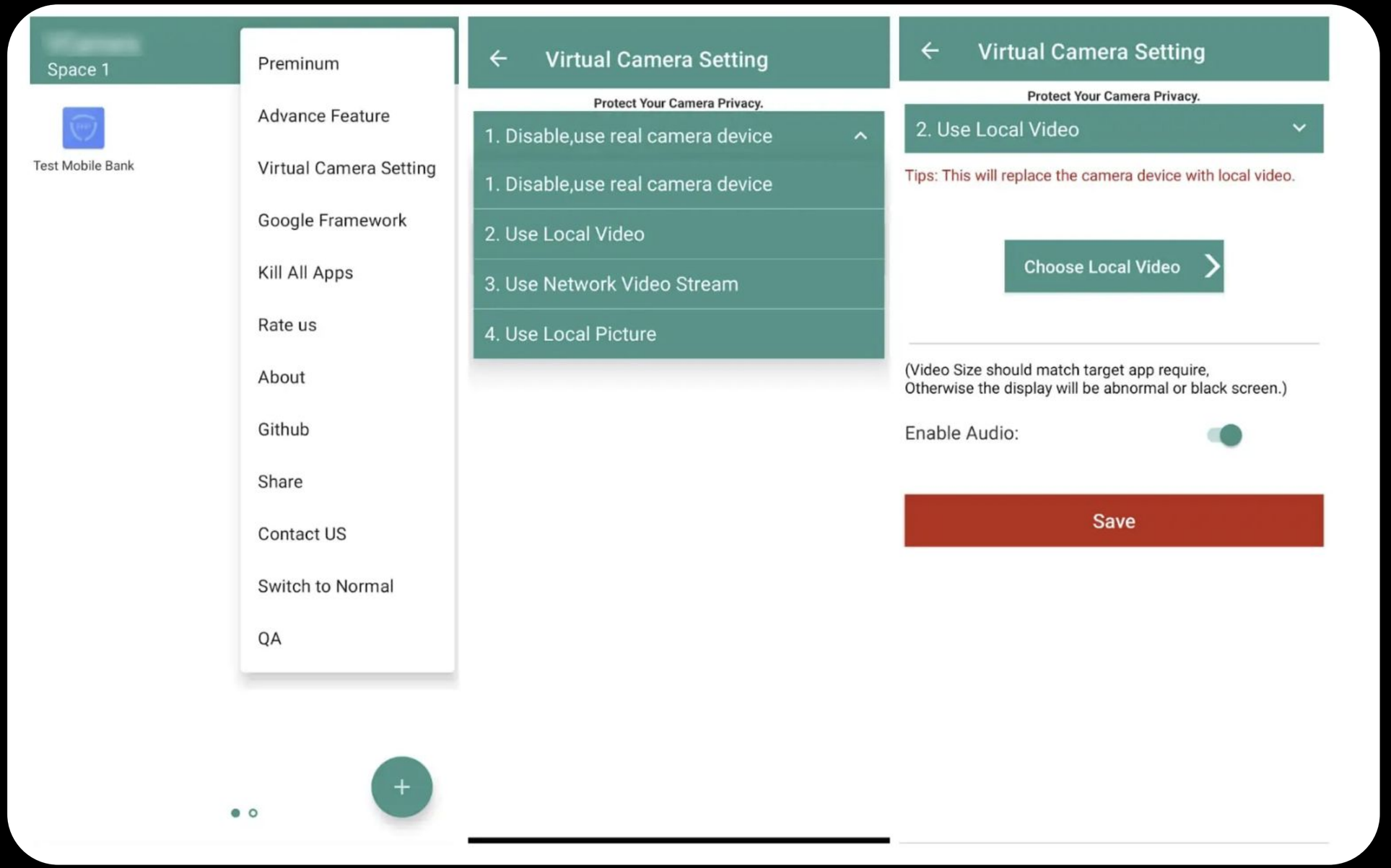
Geography
- Vietnam
- Thailand

Group-IB, 2024

Scan to read more in our blog

Biometric(k)s

GROUP-IB



Biometric(k)s

GROUP-IB

Device Fingerprint Theft

GROUP-IB

	https://customfingerprints.bablosoft.com	OPTIONS	/save?publickey=xc3blub4pxwvxhj0oc4ddtqgkkpm42my84uqo7hyv6zwfetg7hiwnnl9wlzwnso7
05	https://customfingerprints.bablosoft.com	POST	/save?publickey=xc3blub4pxwvxhj0oc4ddtqgkkpm42my84uqo7hyv6zwfetg7hiwnnl9wlzwnso7
506	https://customcanvas.bablosoft.com	GET	/connection

Request Response

Pretty Raw Hex


```
34
35 {
     "version_client":"2.0",
     "url":[redacted],
     "webgl":{
       "unmaskedVendor":"Google Inc. (Google)",
       "unmaskedRenderer":"ANGLE (Google, Vulkan 1.3.0 (SwiftShader Device (Subzero) (0x0000C0DE)), SwiftShader driver)",
       "vendor":"WebKit",
       "renderer":"WebKit WebGL",
       "shadingLanguage":"WebGL GLSL ES 1.0 (OpenGL ES GLSL ES 1.0 Chromium)",
       "version":"WebGL 1.0 (OpenGL ES 2.0 Chromium)",
       "maxAnisotropy":"16",
       "shadingLanguage2":"WebGL GLSL ES 3.00 (OpenGL ES GLSL ES 3.0 Chromium)",
       "version2":"WebGL 2.0 (OpenGL ES 3.0 Chromium)",
       "aliasedLineWidthRange":{
         "0":1,
         "1":1
       },
       "aliasedPointSizeRange":{
         "0":1,
         "1":1023
       },
```


Scan to read more in our blog

Device Fingerprint Theft

GROUP-IB

https://bablosoft.com

Bablosoft | Manual | Community | Register | Login | Translate

BrowserAutomationStudio (by bablosoft)

Price : Free

Create your own applications at **0$** cost with BrowserAutomationStudio. Automate everything that Chrome can! **No coding skills required.**

- **100% browser emulation**.
- Optimized multithreading.
- Visual code creator(no coding skills required).
- Compile **standalone script and sell** in 2 clicks!
- Visual user interface creator(no coding skills required)..
- And many more...

Read More

BASPremium (by bablosoft)

Price : 80$
Duration : 365 days
Machines : 3
Buy license for 365 days

Price : 40$
Duration : 180 days
Machines : 3
Buy license for 180 days

With *BAS Premium* you can:

- Protect your scripts from unlicensed copying.
- Premium support.
- Manage users through web interface.
- Script delivery.

FingerprintSwitcher (by bablosoft)

Price : 20$
Duration : 30 days
Machines : 2
Buy license for 30 days

Price : 40$
Duration : 90 days
Machines : 2
Buy license for 90 days

FingerprintSwitcher is like user agent switcher on steroids. It changes not only user agent, but a lot of browser internals to make BAS actually look like firefox, chrome, safari, on desktop or on mobile platforms.

Key Takeaways

- Malware as a Service (MaaS)
- Sophisticated threat actors

GROUP-IB

THE INCOMING THREATS

FUTURE FRAUDSTER TACTICS: PREDICTIONS

GROUP-IB

Hyper-Realistic & Automated Deepfakes	Deepfakes used for KYC/identity verification will become increasingly sophisticated, harder to detect by current liveness checks, and potentially automated. Expect AI-generated faces and voices capable of mimicking specific individuals or creating entirely new, plausible personas that can interact in real-time or pass video verification checks designed to fool both AI and human reviewers. The BASPremium technique of tricking users into providing video is just the start; stolen PII combined with AI will generate these fakes without needing the victim's active participation.
AI-Powered Adaptive Spoofing	Fraudsters will use AI not just to create fakes, but to actively probe defenses and adapt their spoofing methods in real-time. This could involve dynamically altering device fingerprints (beyond FingerprintSwitcher's capabilities), adjusting deepfake parameters, or modifying behavioral patterns to bypass anomaly detection systems based on the responses they receive.
Authentication Ecosystem Weaknesses	Attacks like Chameleon, which force fallback mechanisms, will become more common and target a wider range of MFA weaknesses. This includes exploiting insecure account recovery processes, vulnerabilities in API integrations (especially with Open Banking), session hijacking (stealing authenticated session tokens rather than credentials), and weaknesses in the orchestration logic of multi-factor authentication systems.
Advanced Synthetic Identity Fraud	The creation and use of synthetic identities (combining real stolen data with fabricated information) will become more industrialized. Expect AI-generated profiles complete with plausible (but fake) credit histories, social footprints, and behavioral patterns, making them incredibly difficult to distinguish from legitimate new customers using traditional checks. These will be used for large-scale application fraud, loan stacking, and establishing footholds for other illicit activities.
Diversification of Biometric Attacks	While facial recognition is a current focus, expect increased attacks targeting other biometric modalities as they become more common. This includes sophisticated voice cloning/deepfake voice attacks to bypass voice authentication, and potentially attempts to spoof behavioral biometrics using bots or AI trained to mimic human interaction patterns.
Weaponization of Automation Frameworks	Easy-to-use frameworks like Bablosoft's BrowserAutomationStudio (linked to BASPremium and fingerprint switching) will proliferate, lowering the barrier for entry. Expect more threat actors leveraging these tools to automate complex attacks, including credential stuffing, fingerprint spoofing, application fraud, and manipulating web interactions at scale.

INDUSTRY PREPAREDNESS: RECOMMENDATIONS

GROUP-IB

Embrace Cyber Fraud Fusion	Break down internal silos. Foster deep collaboration and integrated workflows between Cybersecurity, Fraud Prevention, Identity Access Management (IAM), AML, and Financial Crime units. Share intelligence and telemetry across these teams to get a holistic view of threats that span cyber intrusion and fraud execution
Multi-Layered, Dynamic Identity Verification	**Next-Gen Liveness Detection**: Employ advanced passive liveness techniques (analyzing texture, light reflection, micro-movements) and potentially adaptive active challenges that are harder for deepfakes to beat. Use AI to detect digital forgery artifacts. **Robust Multi-Modal Biometrics:** Combine facial recognition with voice, behavioral, or other biometrics for higher assurance levels. Don't rely on a single modality.
Mobile App Security & Monitoring	Secure mobile banking apps against tampering, overlay attacks, and forced fallback mechanisms exploited by malware like Chameleon. Implement robust runtime application self-protection (RASP) and monitor for anomalous API calls or behavior indicative of compromise.
Deploy AI for Defense	Leverage AI and Machine Learning defensively. Use it for advanced anomaly detection across diverse data sources (device, network, behavior, biometrics, transaction), identifying subtle patterns indicative of deepfakes, synthetic identities, or automated attacks.
Specific Synthetic Identity Countermeasures	Implement specific strategies targeting synthetic identity fraud. This involves advanced data analysis, cross-referencing data points across applications and institutions (where possible and permissible), utilizing consortium data, and potentially exploring emerging identity graph technologies.
Foster Information Sharing & Threat Intelligence	Actively participate in information sharing communities like FS-ISAC. Share indicators of compromise (IoCs) and tactics, techniques, and procedures (TTPs) related to new identity fraud schemes, deepfake methods, and malware variants promptly.

Reports

GROUP-IB

Fingerprint Heists

GoldDigger/GoldPickaxe

GXC Team Unmasked

GROUP-IB

FIGHT AGAINST CYBERCRIME

CYBER ACT FORUM 2025

GROUP-IB.COM
INFO@GROUP-IB.COM
GROUP-IB.COM/BLOG
+65 3159 37 98

LINKEDIN FACEBOOK TWITTER INSTAGRAM