Cyber Threat Barometer *Finance & Insurance*

Key figures and trends shaping the cyber threat to banks, insurers and financial services, drawn from the Citalid 2025/2026 sector report.

PERIOD · 2025/2026

AT A GLANCE

4.7%

of all cyber incidents collected by ENISA involved the finance sector.

SOURCE · ENISA THREAT LANDSCAPE 2025

11%

of significant impact incidents reported under the NIS directive in 2024 occurred in the finance sector.

SOURCE · ENISA THREAT LANDSCAPE 2025

+738%

rise worldwide in the median duration of Layer 3 and 4 DDoS attacks on financial services since 2024.

SOURCE · AKAMAI, MAY 2026

700+

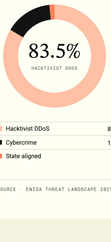
financial institutions had data exposed by a single vendor breach in December 2025.

SOURCE · AKAMAI, MAY 2026

01 · THREAT ACTORS

Hacktivism drives incident volume

Breakdown of finance sector incidents by threat actor type, and the hacktivist groups most active against the sector.



Hacktivist DDoS	83.5%
Cybercrime	14.8%
State aligned	1.7%

MOST ACTIVE HACKTIVIST GROUPS AGAINST THE SECTOR

NoName057(16)	71.1%
DarkStorm Team	15.2%
Keymous+	13.7%

69%

of hacktivist targeting in the finance sector hits banks.

TIMING

Activity peaks around electoral processes and tense political contexts.

SOURCE · ENISA THREAT LANDSCAPE 2025

Incident counts measure frequency, not severity.

02 · CYBERCRIME

Data theft and extortion

Cybercriminals target the data that financial institutions process at scale. Insider access and regulatory exposure add to the cost.

CYBERCRIME INCIDENTS AGAINST THE FINANCE SECTOR

Data breaches	Ransomware
64%	36%

SOURCE · ENISA THREAT LANDSCAPE 2025

RANSOMWARE STRAINS DEPLOYED AGAINST FINANCIAL INSTITUTIONS

Akira	20.0%
Datacarry	12.0%
BlackLock	4.0%

SOURCE · ENISA THREAT LANDSCAPE 2025

INSIDER THREAT · ITALY

€31.8M

fine imposed on Intesa Sanpaolo by the Italian data protection authority. One employee accessed the banking data of 3,573 customers over more than two years, undetected by internal controls.

SOURCE · THE RECORD, MARCH 2026

REGULATORY FRAME

DORA

in force since early 2025. The ECB supervisory priorities for 2026 to 2028 place ICT third party risk and incident response management at the centre of operational resilience.

SOURCE · ECB BANKING SUPERVISION, NOVEMBER 2025

03 · MOBILE FRAUD

Banking trojans target retail customers

OverlayPhantom, an Android banking trojan active since May 2025, illustrates how mobile malware now goes after retail banking customers.

180+

banking, finance and cryptocurrency apps targeted

30+

remote commands, including real time screen streaming

SOURCE · CYBLE, MAY 2026

RECURRING CAPABILITIES

OVERLAY ATTACKS · ACCESSIBILITY ABUSE · SMS AND OTP INTERCEPTION · SCREEN STREAMING · ON DEVICE FRAUD · FAKE APPS AND SMISHING

A crowded ecosystem

WORLDWIDE · 2025/2026

Coyote FatBoyPanel SpyLend **TgToxic** *Grandoreiro* ClipBanker CliptoShuffler **BitStealer** *TsarBot* Crocodilus Anatsa **Octor** *Hook* Zanubis GodFather **ToxicMonda** *PlayPraetor* DoubleTrouble Klopatra **SORVEPOTEL** *Maverick* GHOSTGRAB Herodotus **Brokewell** *Ermac* TrickMo Eternidade **Sturnus** *RadzaRAT* Albiriox Spiderman **Froglight** *deVixor* VENON NGate **TCLBanker** OverlayPhantom BananaRAT SilabRAT **Rokarolla**

Banking trojan families observed in Citalid CTI monitoring over the period.

04 · FRANCE SPOTLIGHT

Claimed breaches at insurers and brokers

French insurance intermediaries hold dense customer files: identity, bank details, vehicle and sometimes medical data.

3 claimed data breaches at French insurers and insurance brokers between January and April 2026.

FEB 2025
Harvest
WEALTH MANAGEMENT SOFTWARE

Ransomware attack claimed by Run Some Wares. The O2S platform used by wealth advisers was unavailable for several days.

JAN 2026
RUN Assurance
MOTORCYCLE INSURANCE BROKER

Breach claimed on a criminal forum. Samples include SEPA mandates, registration certificates and medical information.

FEB 2026
Maxance
CAR INSURER

348,346 customer records claimed, including contract numbers, vehicle details and contact data.

APR 2026
Assurea
INSURANCE BROKER

About 150 GB claimed, covering eight years of activity, with more than two million internal messages and IBAN documents.

Claims published by threat actors, not all have been confirmed by the companies concerned. Source · Citalid CTI incident monitoring.

05 · OUTLOOK

Five trends to watch

Each trend is positioned against the previous edition of the report: continuity, evolution or emergence.

1 DDoS as a geopolitical signal — EVOLUTION

Attacks last longer and adapt in real time. Peaks follow elections and international tensions.

SOURCE · AKAMAI 2026, ENISA 2025

2 Industrialised mobile fraud — EVOLUTION

Overlay attacks, accessibility abuse and on device fraud, distributed through fake apps and smishing.

SOURCE · CYBLE 2026, CITALID CTI

3 Shared suppliers as a force multiplier — CONTINUITY

A single vendor breach in December 2025 exposed data from more than 700 financial institutions.

SOURCE · AKAMAI, MAY 2026

4 Offensive AI, now observed — EMERGENCE

Documented cases include multilingual phishing lures, AI assisted malware refactoring and code conversion.

SOURCE · CITALID CTI

5 Blurred lines between actor types — EVOLUTION

Hacktivist fronts, state interests and criminal tooling increasingly overlap.

SOURCE · CITALID CTI

SOURCES · ENISA Threat Landscape 2025 (October 2025) · Akamai, Attack Trends in Financial Services (May 2026) · Cyble, OverlayPhantom (May 2026) · ECB Banking Supervision, Supervisory priorities 2026/2028 (November 2025) · The Record (March 2026) · Citalid CTI monitoring and sector report Finance & Insurance 2025/2026.