STRATEGIC BRIEF · BOARD

Annual threat landscape

The board-level view of a year of brand-abuse exposure: total tracked volume, how the threat evolved, where you stand against the sector, the performance and return of the monitoring programme, and the regulatory evidence it produced across DORA, NIS2 and eIDAS.

Prepared for **Sample Bank · BE-RETAIL-01 — board of directors & risk committee** · indicators defanged · EU-resident corpus

01 Executive summary

Over 2025, PhishNet tracked **18,400 malicious assets** impersonating the brand across roughly 68 Belgian financial brands in the corpus — a **34% year-on-year increase** and a structural step up rather than a seasonal swing. The threat moved toward dedicated attacker infrastructure and mobile app clones, both raising the odds of live credential capture. The brand remained, by a wide margin, the most-impersonated bank in the sample set. The monitoring and takedown programme resolved **712 assets**, held collection **100% within EU jurisdiction**, and produced **11 DORA evidence packs** plus context for several NIS2 assessments — the same intelligence serving security and compliance from one source. The strategic conclusion: brand-abuse exposure should be treated as a standing, board-level operational-resilience risk, funded and measured accordingly.

Methodology. Passive aggregation of public threat-intelligence feeds (openphish, phishdestroy, threatfox, phishdb, krogza and others). No intrusive testing is performed and no personal data is processed; collection is GDPR-aligned and EU-resident end to end. Each asset is normalised, scored 0–100 for risk, SHA-256 hashed and timestamped on capture. Indicators in this document are defanged. Risk scores are PhishNet assessments derived from public feeds and are independently verifiable.

02 The year in numbers

FY 2025

18.4k

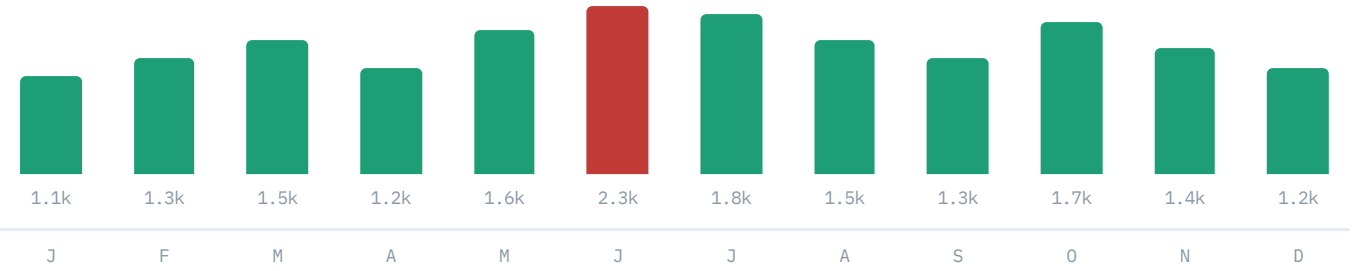
malicious assets tracked in 2025

~68 Belgian brands · 100% EU-resident

+34%	712
VOLUME VS 2024	TAKEDOWNS RESOLVED
11	**100%**
DORA EVIDENCE PACKS	EU JURISDICTION

03 Volume across the year

ASSETS / MONTH



The June peak (2,300) was driven by a coordinated app-clone campaign. Volume never returned to the early-year baseline — a structural increase, not a blip.

04 Sector landscape — 2025 totals

SAME METHOD

Bank A (you)	**6,100**
Bank B	1,100
Bank C	670
Bank D	310
Bank E	95

Annual assets attributed per brand. One institution absorbs the majority of sector impersonation — market leadership and target concentration move together.

05 How the threat evolved

YEAR-ON-YEAR

Dedicated infrastructure

+61%

Purpose-built attacker hosts replaced hijacked sites as the high-severity norm.

App clones

+47%

Mobile-banking clone kits became the dominant credential-capture vector.

Smishing domains

+39%

SMS-lure domains on low-cost TLDs evaded static, list-based defences.

06 Major campaigns of the year

- **Q2 app-clone wave.** A single kit fingerprint produced the year's largest clone cluster; drove the June volume peak.
- **Recurring credential harvest on fixed IPs.** Dedicated-infrastructure capture pages reappeared across multiple quarters at risk ≥ 88.
- **H2 smishing escalation.** Rapid-rotation SMS lure domains targeting retail customers, sustained through year-end.

07 Programme performance & return

Assets tracked

18.4k

Takedowns resolved

712

Median resolution

3.3d

EU jurisdiction

100%

Return framing: 712 confirmed removals plus continuous pre-block coverage materially reduce the window in which a customer can reach a working clone — the dominant driver of impersonation-led fraud loss.

08 Regulatory evidence produced

DORA · NIS2 · EIDAS

DORA

ICT third-party & incident evidence captured with timestamped provenance for the resilience file.

NIS2

Threat context supporting reportable-incident assessment and supervisory review.

eIDAS

Qualified RFC 3161 timestamps on every cited finding — audit-grade to court-grade.

Across the year the programme produced 11 DORA ICT/incident evidence packs and context for several NIS2 assessments, each carrying a qualified RFC 3161 timestamp — audit-grade evidence with no separate compliance project.

09 Strategic roadmap — 2026

01 **Treat brand-abuse as a board-level resilience risk.** Fund continuous monitoring at sector-leader scale and report it alongside other operational-resilience metrics.

02 **Industrialise takedown.** Standing registrar/host escalation paths convert reactive removals into a measured SLA.

03 **Operationalise operator fingerprints.** Most high-severity volume traces to a few operators; standing detections catch new clones immediately.

04 **Unify security and compliance evidence.** Continue producing DORA/NIS2 evidence from the same timestamped corpus — one programme, two regulatory outcomes.

A Appendix · feed coverage, method & glossary

FEED	CONTRIBUTES	COVERAGE	CADENCE
phishdb	phishing URLs & kits	high	continuous
krogza	look-alike / app-clone domains	high	continuous
openphish	verified phishing feed	medium	continuous
phishdestroy	takedown & abuse corpus	medium	continuous
threatfox	IOC exchange (abuse.ch)	medium	continuous
closed channels	leaked-credential mentions	contextual	monitored

Methodology. Passive aggregation of public threat-intelligence feeds (openphish, phishdestroy, threatfox, phishdb, krogza and others). No intrusive testing is performed and no personal data is processed; collection is GDPR-aligned and EU-resident end to end. Each asset is normalised, scored 0–100 for risk, SHA-256 hashed and timestamped on capture. Indicators in this document are defanged. Risk scores are PhishNet assessments derived from public feeds and are independently verifiable.

Glossary

Live asset	A malicious URL, domain or IP confirmed reachable at observation time.
High-severity	Risk score ≥ 85 — typically dedicated infrastructure or working credential capture.
Dedicated infra	Attacker-controlled host stood up to target the brand, not a hijacked legitimate site.
Kit fingerprint	Shared code/asset signature linking multiple clones to one operator.
Defanged	Indicator rendered non-clickable (e.g. [.]) for safe handling.
MTTD	Median time to detect a new asset from first public appearance.
TLPT	Threat-led penetration testing — DORA-defined exercise the evidence base can support.
RFC 3161	Standard for a trusted timestamp token; eIDAS-qualified when issued by a qualified TSA.
YoY	Year-on-year — change versus the equivalent prior-year period.

A year of exposure the board can govern.

Twelve months of brand-abuse intelligence that doubles as your DORA and NIS2 evidence base — EU-resident, every figure traceable to a timestamped source.

DIRECT CONTACT

stijn@galacticautomation.com

galacticautomation.com · phishnet.be

Stijn Van Hijfte

Method. Passive aggregation of public threat-intelligence feeds. No intrusive testing, no personal data processed, GDPR-aligned.

Galactic Automation BV · Zottegem, Belgium — Founder, PhishNet (EU-sovereign CTI)

CISSP · CRISC · IAAP Data Protection Fellow

Indicators defanged; live as of report date.

SAMPLE report. All institutions, indicators, IPs (RFC 5737 TEST-NET) and domains (.example / .invalid) are illustrative and do not represent a real client or live threat. Risk scores are PhishNet assessments derived from public feeds.