TACTICAL BRIEF · CISO

Monthly threat report

The month's brand-impersonation exposure for security management: volume and trend, campaign clustering, attacker infrastructure, credential exposure, takedown performance and the recommendations to carry into next month.

Prepared for **Sample Bank · BE-RETAIL-01 — CISO, security management & fraud** · indicators defanged · EU-resident corpus

01 Executive summary

In May the brand remained the most-impersonated bank in the Belgian sample set, with **482 live assets at month-end** and **1,240 observed across the month** (+12% MoM). High-severity volume rose to 28, driven by a mid-month dedicated-infrastructure campaign concentrated on a single provider block. Takedown throughput improved — 64 submitted, 41 resolved, median detection 1.8 days — but registration of new look-alikes is outpacing removals. Four leaked credential sets referencing the brand surfaced on closed channels and warrant forced-reset triggers.

CURRENTLY LIVE

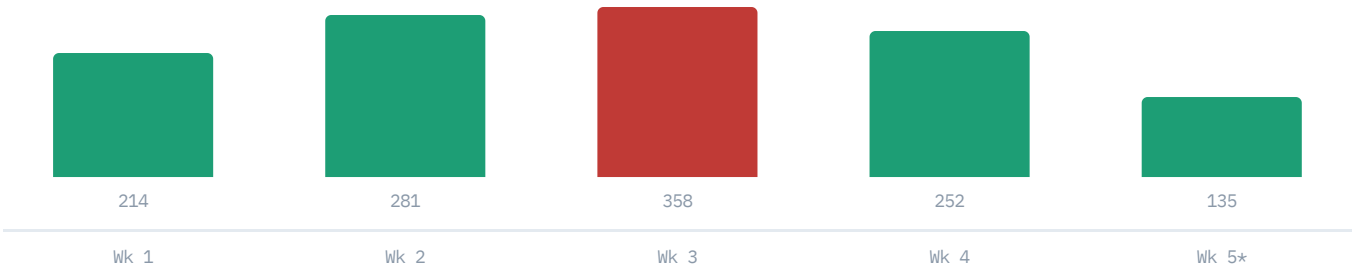
482

live malicious assets at month-end

1,240 observed across May · +12% MoM

28	1.8d
HIGH-SEVERITY ASSETS	MEDIAN TIME TO DETECT
64	41
TAKEDOWNS SUBMITTED	TAKEDOWNS RESOLVED

02 Impersonation volume — May, by week



New assets observed per week. The Week 3 spike coincides with the dedicated-infrastructure campaign (§04). *Week 5 partial.

03 Sector context — Belgian banks, same method

POINT-IN-TIME

Bank A (you)	482
Bank B	96
Bank C	44
Bank D	18
Bank E	3

You are the most-impersonated bank in the sample set — roughly 5× the next institution. At this volume, monitoring is not optional.

04 Campaign clusters & infrastructure

App-clone

51%

Mobile & online-banking login clones sharing one kit fingerprint.

Credential harvest

33%

Dedicated-IP capture pages; 4 hosts on one ASN block.

Smishing

16%

SMS lure domains on low-cost TLDs with fast rotation.

Top hosting block

198.51.100.0/24 — 22% of dedicated-infra assets this month.

Top registrar abuse

One registrar accounts for 38% of new typosquat domains.

Dedicated vs hijacked

41% of high-severity assets ran on attacker-owned infrastructure.

05 Credential exposure

Leaked credential sets referencing the brand, observed on closed channels. Not verified as valid; recommend treating as forced-reset candidates.

SET	RECORDS REFERENCING BRAND	CHANNEL	FIRST SEEN
CE-2605-01	~1,800	closed forum	04 May
CE-2605-02	~640	paste site	12 May
CE-2605-03	~2,300	combo list	19 May
+ 1 further set	channel withheld — detail on request		**full**

06 Top indicators this month

INDICATORS DEFANGED

MALICIOUS ASSET	TYPE	SOURCE / KIT	RISK	OBSERVED
`203.0.113.70/origin/onlinebanking/home1.php` dedicated IP · credential capture	IP / URL	phishdb	89	18 May
`login-be-retail01[.]example/internetbanking` fake online-banking login	URL	phishdb	85	16 May
`be-retail01-app-login[.]example` app clone ×2 (shared kit)	URL ×2	krogza	80	15 May
`verify-be-retail01[.]invalid` credential phish landing	domain	openphish	76	22 May
+ 1,234 further assets this month	phishdb 812 · krogza 311 · phishdestroy 64 · openphish 47 — full IOC set on request			**full**

07 Takedown performance

Submitted	Resolved	Median resolution	Resolution rate
64	41	3.4d	64%

Resolution rate is constrained by two registrars with slow abuse handling — addressed in recommendation 02.

08 Recommendations

01 **ASN-level watch on 198.51.100.0/24.** One provider block carries the dedicated-infrastructure campaign; pre-emptive blocking cuts exposure before assets go live.

02 **Prioritise the registrar driving 38% of typosquats.** A standing abuse relationship shortens takedown time on the highest-volume source.

03 **Trigger forced resets on the 4 leaked credential sets.** Exposed credentials referencing the brand are the most direct route to account takeover.

04 **Promote the app-clone kit fingerprint to a standing detection.** One operator drives most high-severity volume; fingerprinting catches new clones on day one.

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.

A defensible month-end record, not just a feed.

Every figure here traces to a timestamped, SHA-256-hashed finding — the same evidence that feeds your DORA file and survives audit.

DIRECT CONTACT

stijn@galacticautomation.com

galacticautomation.com · phishnet.be

Stijn Van Hijfte

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

CISSP · CRISC · IAAP Data Protection Fellow

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