PhishNet
EU PHISHING INTELLIGENCE

EXTERNAL THREAT EXPOSURE BRIEF
05 JUNE 2026 · PASSIVE OSINT

SAMPLE · NOT A REAL INSTITUTION

PREPARED FOR SAMPLE BANK · BELGIUM

Someone is building a copy of your bank.

Across three independent threat feeds, we are tracking a coordinated effort to impersonate your brand and harvest live customer credentials. **This is the most impersonation activity we see against any Belgian bank in our sample set — by an order of magnitude.**

428 live malicious assets impersonating the brand

11 high-severity · risk up to 88 · 3 independent feeds

Prepared for Sample Bank · BE-RETAIL-01
CISO · fraud · board
Indicators defanged · live as of 05 Jun 2026

Galactic Automation BV
PhishNet — EU-sovereign CTI
Zottegem, Belgium

THE 60-SECOND READOUT

If you read nothing else.

Five findings, in order of how much they should worry you. Every one is backed by defanged, independently verifiable evidence later in this brief.

Executive readout	SAMPLE BANK · BELGIUM
01	**You are the most-impersonated bank in the set — and it isn't close.** 428 live fakes, roughly 6× the next Belgian bank.
02	**This is targeted, not opportunistic.** A credential-harvesting page runs on dedicated attacker infrastructure (203.0.113.70, risk 88) — stood up to target you, not a hijacked site.
03	**The fakes are industrialised.** A single kit fingerprint links 30+ mobile-app and online-banking clones to one operator.
04	**The evidence would hold up.** Every indicator is SHA-256 hashed and RFC 3161 timestamped — admissible to an auditor, insurer or court, not a screenshot.
05	**A snapshot is the floor, not the picture.** New look-alikes register faster than they can be removed; only continuous monitoring closes the exposure window.

01 The lead: a bank that doesn't exist

DEDICATED INFRASTRUCTURE

One of the 428 assets is not like the others. Most phishing reuses a hijacked website or a free host — cheap, disposable, gone in days. This one is different: a credential-harvesting page running on a **fixed IP address stood up specifically to target your customers**. It serves a pixel-accurate copy of your online-banking login, captures whatever a customer types, and relays it onward in real time. It is purpose-built infrastructure, and it scores 88 out of 100 on our risk model — the highest in this set.

LEAD INDICATOR · CONFIRMED LIVE

`203.0.113.70/origin/onlinebanking/home1.php`

Dedicated-IP credential capture · serving an online-banking login clone · first observed 5 Jun 2026 · source: phishdb

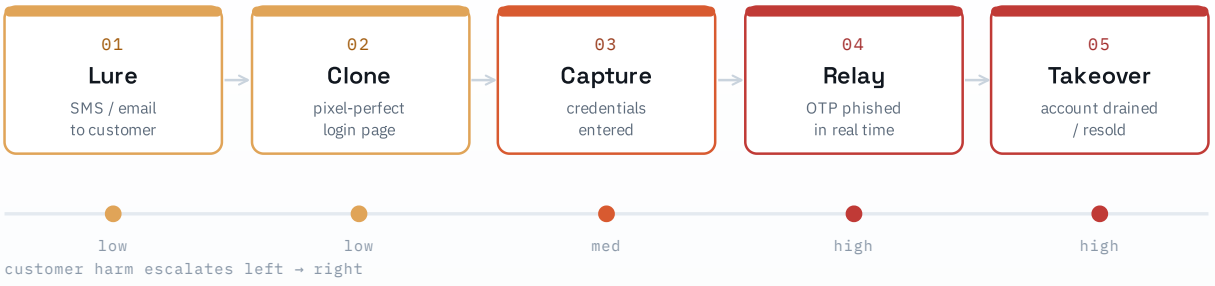
88
RISK / 100

> **“This is not a hijacked website. It is a purpose-built replica of your bank, on infrastructure that exists for one reason: to take your customers’ passwords.”**
>
> PHISHNET ANALYSIS · LEAD FINDING

02 Anatomy of the attack

LURE → TAKEOVER

The clone is one piece of a chain. Here is how a single customer goes from an unremarkable text message to a drained account — and where the window to intervene actually is.



HOW ONE IMPERSONATION ASSET CONVERTS INTO ACCOUNT TAKEOVER

The decisive interval is stages 01–02: once the lure is sent and the clone is live, intervention means *removing the asset*. Every hour it stays up is exposure. This is why time-to-takedown, not just detection, is the metric that matters.

03 The evidence

INDICATORS DEFANGED

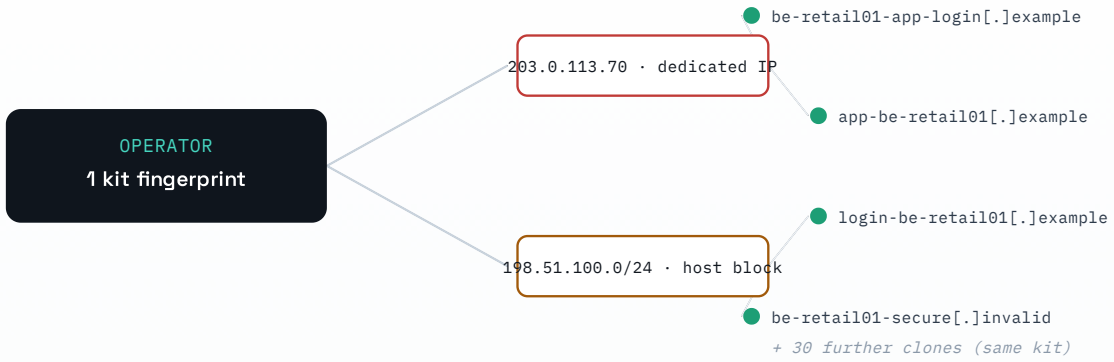
Confirmed live assets, highest-risk first. The full IOC set — all 428 — is available to your SOC on request, in STIX 2.1 / MISP / CSV.

MALICIOUS ASSET	TYPE	SOURCE / KIT	RISK	OBSERVED
`203.0.113.70/origin/onlinebanking/home1.php` dedicated IP infrastructure · credential capture	IP / URL	phishdb	88	5 Jun 2026
`be-retail01-login[.]example/internetbanking` fake online-banking login	URL	phishdb	81	5 Jun 2026
`app-be-retail01[.]example / be-retail01-app-login[.]example` mobile app clones ×2 (shared kit)	URL ×2	krogza	79	5 Jun 2026
`sms-be-retail01[.]invalid` smishing lure infrastructure	domain	phishdb	72	5 Jun 2026
+ 424 further assets impersonating the brand	phishdb 312 · krogza 98 · phishdestroy 18 — full IOC set available on request			**full**

04 The operator behind it

ONE KIT, MANY STOREFRONTS

These are not 428 unrelated incidents. A shared **kit fingerprint** — the same reused code and assets — links the high-severity clones back to a single operator running infrastructure at scale. Treating each domain as a one-off misses the point: take down one storefront and the operator opens another.



ONE OPERATOR → DEDICATED HOSTS → 30+ BRAND CLONES

Shared kit

41%

of high-severity clones trace to one fingerprint.

Dedicated infra

2

attacker-owned host clusters, not hijacked sites.

Clone storefronts

30+

live domains from the same operator.

05 The sector reckoning

BELGIAN BANKS · SAME METHOD

The same passive method, applied identically across the Belgian banking sector, puts the scale in context. Being the market leader and being the primary target turn out to be the same thing.

Sample Bank	428
Bank B	71
Bank C	33
Bank D	12
Bank E	0

> **428 live assets — roughly six times the next Belgian bank, and more than the rest of the sector combined. At this volume, monitoring is not a project. It is a control.**
>
> POINT-IN-TIME COUNTS · PUBLIC THREAT FEEDS · 5 JUN 2026

06 Why this evidence holds

AUDIT → COURT-GRADE

Most threat intelligence is a screenshot and a claim. Ours is a record. Every finding in this brief carries its full chain of custody — captured from an EU source, SHA-256 hashed, and (where required) sealed with a qualified RFC 3161 timestamp. That is the difference between “we saw it” and evidence an auditor, insurer or court will accept.

EVERY INDICATOR: CAPTURED, HASHED, TIMESTAMPED, EXPORTABLE

DORA
ICT third-party & incident evidence, ready for the resilience file.

NIS2
threat context that survives reporting and supervisory review.

eIDAS
qualified timestamps give findings evidentiary weight.

07 What a snapshot can’t show you

This brief is a single point in time. It cannot show you the look-alike registered tomorrow, the credential set leaked next week, or the takedown that should already be in flight. Continuous monitoring is what turns a striking snapshot into a closed exposure window.

- + Real-time alerting on new kits & domains
- + Look-alike / typosquat registration watch
- + Takedown support & registrar abuse reports
- + Full domain estate & sub-brand coverage
- + Exposed / leaked credential monitoring
- + Reporting dashboard & IOC export to your SOC

How we know this. PhishNet passively aggregates public threat-intelligence feeds (openphish, phishdestroy, threatfox, phishdb, krogza and others), normalises and de-duplicates the signal, scores each asset for risk, and preserves the source trail. No intrusive testing is performed against your systems and no personal data is processed; collection is GDPR-aligned and EU-resident end to end. Every figure in this brief is independently verifiable from the indicators provided.

20 minutes. I’ll hand your SOC every live indicator.

This brief is a passive-OSINT snapshot. On a call I’ll walk through each indicator, show the evidence behind the risk scores, and explain how PhishNet keeps the brand monitored — EU-sovereign, self-hosted, no data leaving the EU.

DIRECT CONTACT

stijn@galacticautomation.com

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 (openphish, phishdestroy, threatfox, phishdb, krogza & others). No intrusive testing, no personal data processed, GDPR-aligned. Every asset SHA-256 hashed and timestamped on capture; indicators defanged.

SAMPLE flagship brief. “Sample Bank”, all comparison banks, indicators, IPs (RFC 5737 TEST-NET) and domains (.example / .invalid) are illustrative and do not represent a real institution or live threat. The flagship brief is normally prepared for a single named institution as an unsolicited security courtesy. Risk scores are PhishNet assessments derived from public feeds; indicators are independently verifiable.