OPERATIONAL BRIEF · SOC

Weekly threat pulse

What changed in the last seven days against the monitored brand estate, and what to action now — new malicious assets, fresh attacker infrastructure, takedown movement and the pre-block watchlist.

Prepared for **Sample Bank · BE-RETAIL-01 — SOC & fraud operations** · indicators defanged · EU-resident corpus

Headline: 37 new live assets impersonating the brand surfaced this week — the highest seven-day count in the rolling window. Four reached high-severity, including a credential-harvest page on a fixed IP. Six earlier assets were confirmed taken down. The trend is sustained, not a spike.

01 This week at a glance

NEW THIS WEEK

+37

new live malicious assets

142 currently live · +9% vs last week

4 NEW HIGH-SEVERITY	**6** CONFIRMED TAKEN DOWN
2 NEW INFRA CLUSTERS	**2.1d** AVG TAKEDOWN TIME

02 Action this week

BLOCK / REPORT NOW

MALICIOUS ASSET	TYPE	SOURCE / KIT	RISK	OBSERVED
`secure-be-retail01-login[.]example/auth` credential capture · dedicated host	URL	phishdb	86	11 Jun
`203.0.113.44/onlinebank/home.php` cred-harvest on fixed IP	IP / URL	phishdb	84	13 Jun
`app-be-retail01[.]example` mobile app clone	URL	krogza	79	12 Jun
`be-retail01-secure[.]invalid` typosquat landing	domain	openphish	71	14 Jun
`sms-be-retail01[.]example` smishing lure infrastructure	domain	phishdb	68	15 Jun

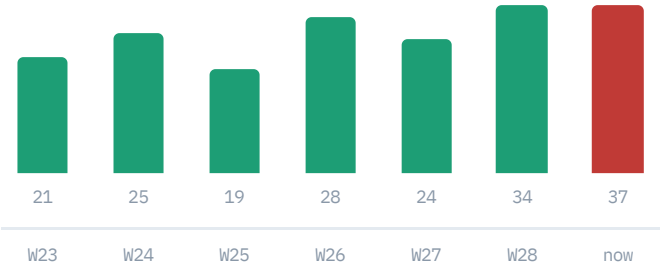
03 New infrastructure & week trend

Cluster A · 198.51.100.0/24

3 new credential-harvest hosts on one provider block — purpose-built, not hijacked. Recommend ASN-level watch.

Cluster B · shared-host clones

2 app-clone domains reusing one kit fingerprint; likely the same operator as last week.



New-asset volume, 7-week view. This week is the highest in the window — sustained pressure, not a one-off.

04 Takedown status

STAGE	COUNT	DETAIL
Submitted	9	registrar & host abuse reports filed
Resolved	6	asset offline / suspended
Pending	3	awaiting provider action (3 assets)

05 Pre-block watchlist

NEXT 7 DAYS

Newly registered look-alikes not yet weaponised — recommend pre-emptive blocking before they go live.

MALICIOUS ASSET	TYPE	SOURCE / KIT	RISK	OBSERVED
be-retail01-verify[.]example fresh registration · parked	domain	krogza	62	15 Jun
retail01-be-login[.]invalid MX configured, no content yet	domain	krogza	58	15 Jun
+ 11 further look-alike registrations	krogza 9 · openphish 2 — full watchlist on request			**full**

A Appendix · feed coverage & method

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.

Hand this to your SOC every Monday.

The weekly pulse runs on the same EU-resident corpus behind the monthly, quarterly and annual reports — every indicator timestamped and traceable to source.

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.