PhishNet
EU PHISHING INTELLIGENCE

EXTERNAL THREAT EXPOSURE BRIEF
05 JUNE 2026 · PASSIVE OSINT

SAMPLE · NOT A REAL HOSPITAL

PREPARED FOR SAMPLE HOSPITAL · BELGIUM

One stolen staff login is all the ransomware needs.

We are tracking exposed credentials for your staff on stealer logs and combo lists — the exact entry point behind the ransomware that has shut Belgian hospitals down — alongside live fakes of your patient services. **The leak is the precursor; the encrypted EMR is the consequence.**

1,940

exposed staff credentials referencing your domain

+ 96 live fakes of your patient services · risk up to 90

Prepared for Sample Hospital · BE-HOSP-01
CISO · CMIO · 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 HOSPITAL · BELGIUM
01	**Your staff credentials are leaking — that is how the ransomware gets in.** 1,940 exposed credentials referencing your domain on stealer logs and combo lists.
02	**The pattern is proven in Belgium.** In January 2026 a ransomware attack on a Belgian hospital paralysed IT for three weeks, cancelled surgeries and diverted emergencies. The entry point in cases like this is a stolen login.
03	**Your patients are phished with your name.** 96 live fakes of your patient portal and eHealth / itsme login, built to harvest patient identity credentials.
04	**You are an essential entity — this is on the CCB's desk.** Hospitals face ex-ante supervision and fines up to €10M or 2% of turnover, and must evidence their measures under CyberFundamentals.
05	**A snapshot is the floor.** New leaks and fakes appear continuously; only ongoing monitoring closes the window before it is used.

01 The lead: the credential before the crisis

CREDENTIAL EXPOSURE

Hospital ransomware almost never starts with the ransomware. It starts weeks earlier, with a single staff credential captured by an info-stealer on a home device or sold in a combo list. We are tracking a fresh set referencing your domain — valid-looking logins for clinical and administrative staff. On their own they look harmless. To an access broker they are the front door, and they price accordingly.

LEAD FINDING · CREDENTIAL EXPOSURE

CE-2606-01 · ~640 records · @sample-hospital[.]be

Info-stealer log · clinical & admin accounts · surfaced on a closed channel · first seen 03 Jun 2026

90

RISK / 100

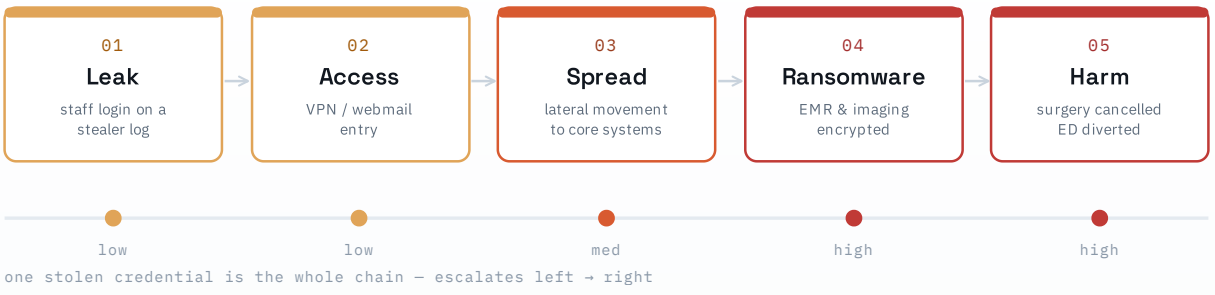
> **“The encrypted EMR is the headline. The leaked login that opened the door was on sale weeks before — and it was findable.”**

PHISHNET ANALYSIS · LEAD FINDING

02 Anatomy of the attack

LEAK → CANCELLED SURGERY

How one exposed credential becomes a hospital-wide outage — and where the only cheap intervention is.



FROM A STEALER-LOG ENTRY TO DIVERTED EMERGENCIES

The cheap intervention is stage 01: a forced reset on an exposed credential costs minutes. Every stage after it costs clinical capacity. This is why credential-exposure monitoring is an operational-resilience control, not an IT nicety.

03 The evidence

INDICATORS DEFANGED

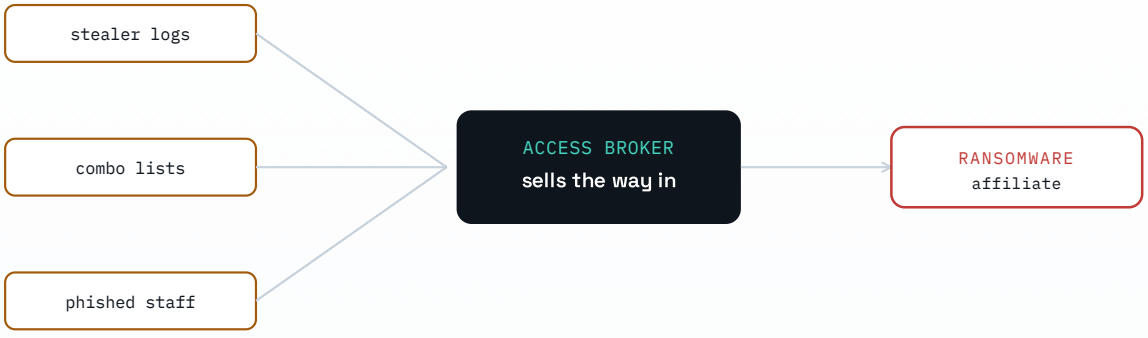
Highest-risk first — the credential exposure and the patient-facing fakes. Full sets available to your security team on request.

FINDING	TYPE	SOURCE	RISK	OBSERVED
CE-2606-01 · ~640 staff records info-stealer log referencing @sample-hospital[.]be	credential set	closed channel	90	3 Jun 2026
mijn-sample-hospital[.]example/aanmelden cloned patient portal · eID / itsme harvest	URL	phishdb	84	5 Jun 2026
ehealth-sample-hospital[.]example fake eHealth / appointment login	domain	krogza	78	5 Jun 2026
CE-2605-04 · ~1,300 records combo-list mentions of the hospital domain	credential set	combo list	72	28 May 2026
+ 93 further fakes & mentions	phishdb 61 · krogza 24 · closed channels 8 — full set on request			**full**

04 Where your credentials surface

THE ACCESS-BROKER ECONOMY

Leaked hospital credentials are not random noise — they feed a market. Info-stealers and combo lists supply access brokers, who package and sell a working way in to ransomware affiliates. Monitoring the supply side lets you reset a credential before it is ever bought.



your leaked credentials are the raw material of the access-broker economy

YOUR LEAKED CREDENTIALS → ACCESS BROKER → RANSOMWARE AFFILIATE

05 Why hospitals, why now

SECTOR CONTEXT

Healthcare is the CCB's most visible enforcement priority, and the threat is rising: Belgian incident reports were up nearly 70% in 2025. Hospitals are classified as essential entities, which means the strictest obligations and the highest penalties — and, after the 2026 incidents, board-level attention.

Essential entity

2%

max fine of turnover (or €10M) — fines apply, unlike public administrations.

Incident reports

+70%

rise in Belgian NIS2 incident reports across 2025.

Supervision

ex-ante

essential entities must proactively evidence their measures to the CCB.

06 How this evidence serves NIS2

CCB · CYBERFUNDAMENTALS

Every finding here carries its chain of custody — captured from an EU source, SHA-256 hashed, timestamped. That makes it reporting-grade for the CCB notifications and usable as evidence of your risk-management measures under CyberFundamentals. The same monitoring that prevents the incident also evidences your compliance.

EVERY INDICATOR: CAPTURED, HASHED, TIMESTAMPED, EXPORTABLE

Incident reporting

evidence for the CCB 24h / 72h / 30-day notifications via Safeonweb@Work.

CyberFundamentals

continuous external-threat monitoring & measurement for essential-level verification.

Evidence integrity

eIDAS-qualified RFC 3161 timestamps make findings independently verifiable.

07 What a snapshot can't show you

This brief is one point in time. It cannot show the credential leaked tonight or the fake portal registered tomorrow. Continuous, managed monitoring — no SOC required — turns a snapshot into a closed window, with a forced-reset trigger the moment a staff credential surfaces.

- + Staff credential-exposure monitoring & reset triggers
- + Takedown support & registrar abuse reports
- + Patient-portal & eHealth impersonation watch
- + Supplier / invoice (BEC) impersonation
- + Look-alike / typosquat registration watch
- + NIS2 evidence & CCB reporting support

How we know this. PhishNet passively aggregates public threat-intelligence feeds and monitored closed channels for leaked-credential mentions, normalises and scores each finding, and preserves the source trail. No intrusive testing is performed against your systems; collection is GDPR-aligned and EU-resident end to end. PhishNet is the external early-warning and evidence layer — it complements your internal controls (EDR, backups, segmentation), it does not replace them.

20 minutes. I'll show you which staff logins are already for sale.

This brief is a passive-OSINT snapshot. On a call I'll walk through the exposed credentials and every fake of your patient services, and show how PhishNet keeps you monitored — fully managed, EU-sovereign, self-hosted, no data leaving the EU.

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 and monitored closed channels. No intrusive testing, no personal data processed beyond defanged indicator handling, GDPR-aligned. Findings SHA-256 hashed and timestamped on capture.

SAMPLE brief. "Sample Hospital", all indicators, credential-set identifiers, IPs (RFC 5737 TEST-NET) and domains (.example / .invalid) are illustrative and do not represent a real hospital or live threat. The January 2026 Belgian hospital ransomware incident is referenced as publicly reported industry context only. Risk scores are PhishNet assessments derived from public feeds; indicators are independently verifiable.