PhishNet
EU PHISHING INTELLIGENCE

EXTERNAL THREAT EXPOSURE BRIEF
05 JUNE 2026 · PASSIVE OSINT

SAMPLE · NOT A REAL MUNICIPALITY

PREPARED FOR GEMEENTE SAMPLE · BELGIUM

# Your residents are being scammed in your name.

Across public threat feeds we are tracking fake versions of your municipal services — payment pages, e-loket logins, official notices — built to defraud your residents and harvest their eID credentials. **This is impersonation of a public authority, and it lands on the people you serve.**

**213**

live fakes impersonating your municipal services

7 high-severity · risk up to 86 · 3 independent feeds

Prepared for Gemeente Sample · BE-LOCAL-01
College van burgemeester en schepenen · IT / DPO
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 | GEMEENTE SAMPLE · BELGIUM |
|---|---|
| 01 | **Your residents are the target, not your servers.** 213 live fakes impersonate municipal services — payment pages, e-loket logins and official notices. |
| 02 | **The worst one harvests eID / itsme logins.** A cloned e-loket capture page (risk 86) collects citizens' identity credentials, which unlock far more than a stolen card. |
| 03 | **You are cloned with a reusable kit.** One operator clones dozens of Belgian municipalities from a single template — your town is one of many. |
| 04 | **NIS2 puts this on your desk.** As an in-scope public authority you must monitor, report incidents to the CCB (24h / 72h / 30-day) and evidence your measures under CyberFundamentals. This brief is exactly that evidence. |
| 05 | **A snapshot is the floor.** New fakes register continuously; only ongoing monitoring and takedown protects residents between reports. |

## 01 The lead: a copy of your e-loket

EID HARVESTING

Most municipal phishing is a throwaway fake payment page — annoying, short-lived. This one is worse. It is a pixel-accurate clone of **your e-loket login**, and instead of grabbing a card number it captures the resident's **eID / itsme identity credentials**. That unlocks tax records, benefits, address changes and document requests — the keys to a citizen's relationship with the state, taken in your municipality's name. It scores 86 of 100, the highest in this set.

LEAD INDICATOR · CONFIRMED LIVE

`e-loket-gemeente-sample[.]example/aanmelden`

Cloned e-loket login · harvests eID / itsme credentials · first observed 5 Jun 2026 · source: phishdb

86
RISK / 100

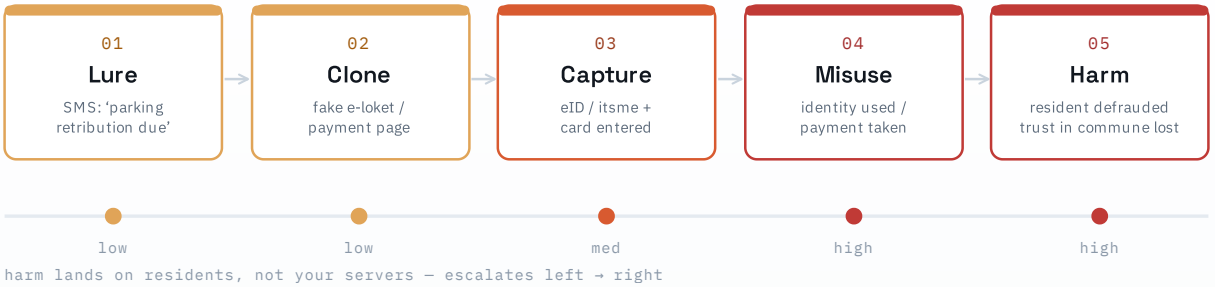
> **“This is not a fake invoice. It is a working copy of the front door to your residents’ digital identity — serving under your name.”**

PHISHNET ANALYSIS · LEAD FINDING

## 02 Anatomy of the attack

LURE → RESIDENT HARM

The clone is one link in a chain that ends with a defrauded resident and a dent in public trust. Here is how a single citizen gets there — and where you can still intervene.




HOW ONE IMPERSONATION ASSET CONVERTS A RESIDENT INTO A VICTIM

The decisive interval is stages 01–02. Once the lure is sent and the clone is live, the only protection is *removing the asset fast*. Every hour it stays up, more residents reach a working fake of your services.

## 03 The evidence

INDICATORS DEFANGED

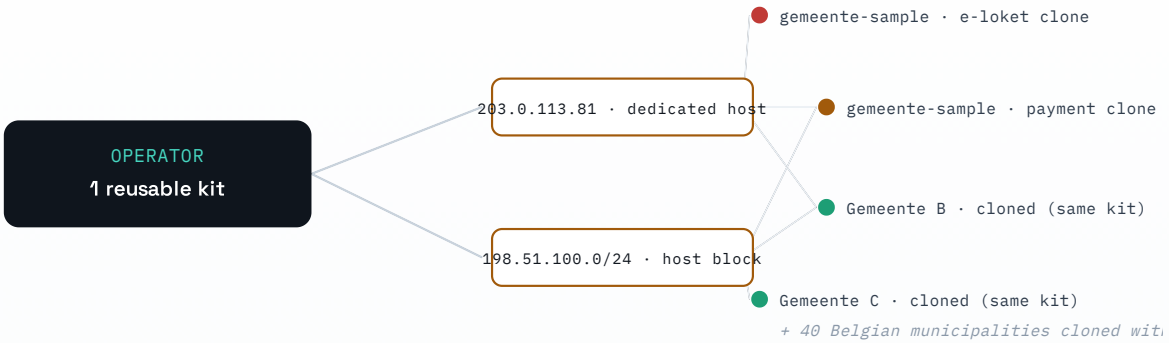
Confirmed live assets, highest-risk first. The full set is available to your IT team or provider on request, in STIX 2.1 / MISP / CSV.

| MALICIOUS ASSET | TYPE | SOURCE / KIT | RISK | OBSERVED |
|---|---|---|---|---|
| `e-loket-gemeente-sample[.]example/aanmelden`<br>cloned e-loket · eID / itsme credential harvest | URL | phishdb | 86 | 5 Jun 2026 |
| `betaal-gemeente-sample[.]example/retributie`<br>fake municipal payment page (parking / tax) | URL | phishdb | 79 | 5 Jun 2026 |
| `gemeente-sample-eloket[.]invalid`<br>typosquat of the municipal portal domain | domain | krogza | 74 | 5 Jun 2026 |
| `sms-gemeente-sample[.]example`<br>smishing lure infrastructure | domain | phishdb | 70 | 5 Jun 2026 |
| **+ 209 further assets impersonating the municipality** | phishdb 151 · krogza 49 · phishdestroy 9 — full IOC set on request | | | **full** |

## 04 The operator — one kit, many towns

WHY THIS IS A SECTOR PROBLEM

You are not being singled out by a lone scammer. A shared **kit fingerprint** links your clones back to an operator who reuses the same template against municipality after municipality. Take down one fake and they spin up the next — for your town and forty others.




ONE OPERATOR AND ONE REUSABLE KIT → YOUR SERVICES AND DOZENS OF OTHER BELGIAN TOWNS

**Same kit**

**40+**

Belgian municipalities cloned from one template.

**eID-harvest clones**

**7**

high-severity assets target identity, not just cards.

**Lifespan**

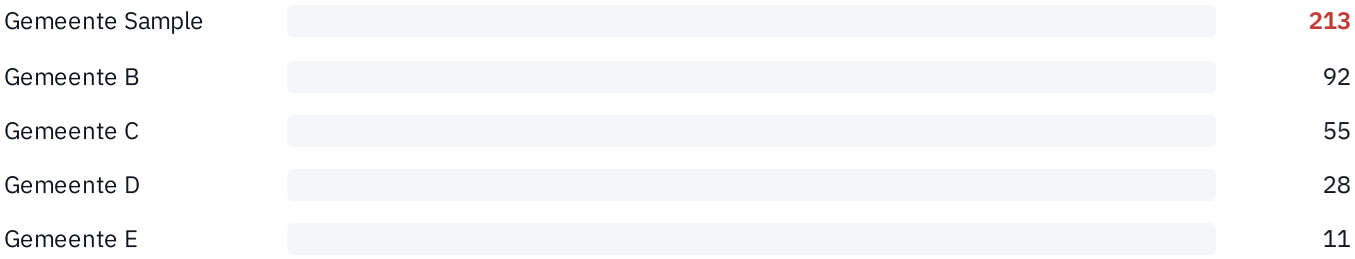
**days**

fakes rotate fast — detection alone is not enough.

## 05 Municipal impersonation, same method

POINT-IN-TIME

The same passive method applied across comparable Belgian towns. Larger and more digitised municipalities draw more impersonation — an e-loket is a bigger prize than a static info site.




> **An attacker who can fake one Belgian commune can fake fifty. That is exactly why monitoring works better pooled across towns than fought alone.**

POINT-IN-TIME COUNTS · PUBLIC THREAT FEEDS · 5 JUN 2026

## 06 How this evidence serves NIS2

CCB · CYBERFUNDAMENTALS

As an in-scope public authority you owe the CCB monitoring, incident reports and evidence that your measures work. Every finding here carries its chain of custody — captured from an EU source, SHA-256 hashed, and timestamped — so it is reporting-grade, not a screenshot. The same intelligence that protects residents also evidences your compliance.


EVERY INDICATOR: CAPTURED, HASHED, TIMESTAMPED, EXPORTABLE

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

**CyberFundamentals**
external-threat monitoring & measurement that supports CyFun verification.

**Evidence integrity**
eIDAS-qualified RFC 3161 timestamps make findings independently verifiable.

Belgian public administrations are not subject to NIS2 administrative fines — the CCB issues binding instructions instead. The driver here is protecting residents, demonstrating your measures, and not being the town that left a fake of its e-loket online for weeks.

## 07 What a snapshot can't show you

This brief is one point in time. It cannot show the look-alike registered tomorrow or the takedown that should already be in flight. Continuous, managed monitoring — you do not need a SOC — is what turns a striking snapshot into a closed exposure window.

- + Real-time alerting on new fakes & domains
- + Look-alike / typosquat registration watch
- + Takedown support & registrar abuse reports
- + Full e-loket & service-portal coverage
- + Resident-facing scam & smishing monitoring
- + NIS2 evidence & CCB reporting support

**How we know this.** PhishNet passively aggregates public threat-intelligence feeds (openphish, phishdestroy, threatfox, phishdb, krogza and others), normalises and scores each asset, 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 is independently verifiable from the indicators provided.

## 20 minutes. I'll show you every fake of your services.

This brief is a passive-OSINT snapshot. On a call I'll walk through each indicator and show how PhishNet keeps your services monitored and your residents protected — 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. No intrusive testing, no personal data processed, GDPR-aligned. Every asset SHA-256 hashed and timestamped on capture; indicators defanged.

SAMPLE brief. "Gemeente Sample", all comparison towns, indicators, IPs (RFC 5737 TEST-NET) and domains (.example / .invalid) are illustrative and do not represent a real municipality or live threat. NIS2 scope for local authorities depends on size and activity thresholds or CCB designation. Risk scores are PhishNet assessments derived from public feeds; indicators are independently verifiable.