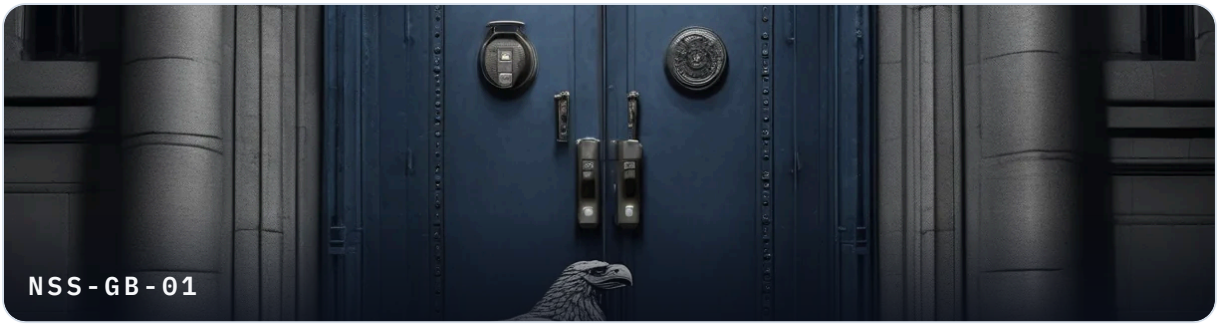


From public lists

Names from public lists. NSS's work: the link format, a check of all 19 domains, a correction

Polish official and e-banking lookalike domains aimed at PKO business-banking users: technical analysis

From 23 October to 5 November 2026, 19 domains built on Polish words for the authorities, the government, a company and electronic banking carried 576 one-time phishing links aimed at PKO Bank Polski's business-banking customers. Every name came from public lists and the domains are now down. NSS adds the one link format that ties them, a log search to find who received a link, and a correction to NSS's own earlier record.

PUBLISHED 13 Nov 2026
LAST UPDATED 13 Nov 2026
READING TIME 10 min
MARKING TLP:CLEAR

19 registered domains

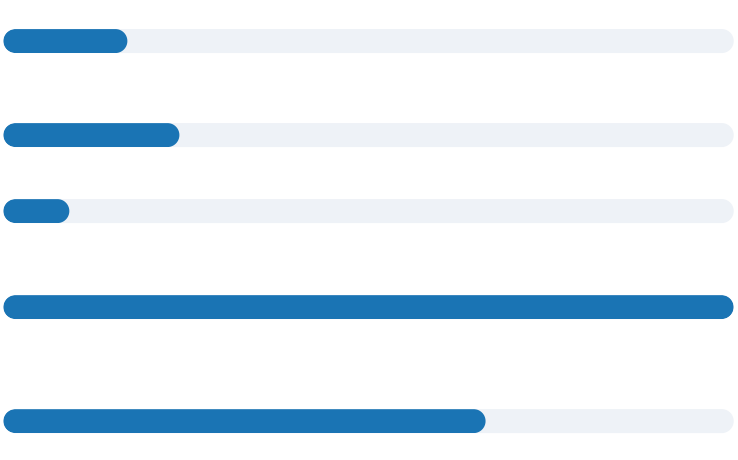
576 one-time links, 574 codes used once

1 link format, search pattern in findings

0 of 19

domains resolving on 13 Nov 2026

THE 595 NAMES BY THE WORDS IN THEIR DOMAIN



In the order the domains were registered. Each group is a set of domains built on one Polish word or theme.

Key findings

1. 595 names under 19 registered domains reached NSS from public lists between 24 October and 7 November 2026. NSS did not discover them; its work here is tying them together, checking every domain and correcting its own first reading. Search mail and web logs from 23 October 2026 for names matching (^|//)(sesja|pl)-[0-9][a-z][0-9][a-z] and for any name under the 19 domains.
2. One link format ties them. Each of the 576 link names is the Polish word for session (sesja) or the letters pl, then a four-character code of digit, letter, digit, letter, and in 566 of them the name of PKO Bank Polski or its business banking service. 574 of the 576 codes are different: these are one-time links, not sites.
3. The domain names moved through four themes in two weeks: the Polish words for the authorities (five domains, 23 to 25 October), the government (four, 25 to 26 October), a company (two, 26 October) and electronic banking (four, 31 October to 5 November). Four domains

with no meaning in Polish were added on 27 October and carried 275 names.

4. 18 of the 19 domains were registered at one registrar, one to three a day; no five were bought within 30 seconds of each other, so there is no purchase batch. The 19th was first registered in 2011 and came into use on 27 October.

5. Each domain was set up to answer for any name under it, so the link names never appeared in certificate logs on their own. In NSS's records one address on a network in Vietnam answered for 203 names under 10 of the domains; NSS cannot tell who else uses that server, so the address is not an indicator.

6. Public reporting from October 2026 described emails to PKO Bank Polski's business customers and a fake business-banking login under one of these 19 domains that asked for the login, the password and the second factor. NSS never loaded a page from the set itself.

7. The set is down. Between 11:38 and 11:50 UTC on 13 November none of the 19 domains resolved, and nine of them, holding 473 names, were on hold at the registrar. The value now is looking back through logs from 23 October and spotting the next domains that use the same format.

Timeline

23 Oct 2026, 11:03 UTC
The first domain is registered: the letters pl and the Polish word for the authorities.

24 Oct, 08:58 UTC
The first entry from the set, a web address, reaches NSS from public lists; the first name follows at 11:40.

25 and 26 Oct
Four domains on the Polish word for the government are registered, then two on the word for a company.

27 Oct, 09:06 to 11:50 UTC
Three domains with no meaning in Polish are registered and a fourth, first registered in 2011, comes into use. They carry 275 names.

28 and 30 Oct
Public reporting describes emails to the bank's business customers and names a fake business-banking login under one of the 19 domains.

31 Oct to 5 Nov
Four domains on the Polish words for electronic banking are registered. On 5 November 160 names under one of them reach NSS within ten minutes.

4 Nov
NSS's register files the address that served most of the names as a confirmed cluster that NSS found itself. NSS retired that entry on 13 November.

7 Nov, 16:37 UTC
The last name reaches NSS.

13 Nov, 11:38 to 11:50 UTC
NSS checks every domain: none resolves, nine are on hold at the registrar. The same day NSS retires its register entry for the address.

What reached NSS

Between 24 October and 7 November 2026 public warning lists carried 595 names that NSS took in. Each was listed as phishing. NSS did not find these names itself: its own certificate-log and new-registration records hold none of the 19 domains from before the lists carried them. What NSS adds is the link between them, a check of every domain and the evidence for what can and cannot be said.

The 595 names sit under 19 registered domains. 19 of the names are the domains themselves and 576 are names under them.

One link format

Every one of the 576 names under the domains follows one format: a word, a four-character code, and usually a brand label, then the domain.

FORM	NAMES	EXAMPLE
pl-code-pkobiznes	177	`pl-0a5y-pkobiznes[.]bankowosc-elektroniczna[.]net`
sesja-code-pkobiznes-firma	151	`sesja-0f7z-pkobiznes-firma[.]wabze[.]net`
pl-code-pkobiznes-firma	120	`pl-0a7r-pkobiznes-firma[.]mozesz[.]net`
sesja-code-pkobiznes	100	`sesja-0g6k-pkobiznes[.]rzad-pl[.]net`
sesja-code-pkobp	16	`sesja-1w3x-pkobp[.]pl-wladze[.]com`
sesja-code, no label	10	`sesja-2p0l[.]wladze-pkobiznes[.]com`
sesja-code-ipkobiznes	2	under `pl-wladze[.]net`

Sesja is Polish for session. The label names PKO Bank Polski (pkobp) or its business banking service, iPKO biznes (pkobiznes and ipkobiznes); firma is Polish for company. The code is always a digit, a letter, a digit and a letter, and 574 of the 576 codes are different. A code used once is most likely a link made for one message or one recipient. Counting these names counts links that were sent, not sites that were built: the sites are the 19 domains.

Four themes in two weeks

The domains themselves were chosen to read as official or as banking in Polish, and the theme changed as the days went on.

THEME	DOMAINS	REGISTERED	NAMES
Władze, the authorities	`pl-wladze[.]com`, `wladze-pl[.]com`, `pl-wlad`	23 to 25 Oct	47

	`ze[.]net`, `wladze-pkobiznes[.]com`, `wladze-pl[.]net`		
Rząd, the government	`rzad-pl[.]com`, `pl-rzad[.]com`, `pl-rzad[.]net`, `rzad-pl[.]net`	25 to 26 Oct	67
Firma, a company	`pl-firma[.]com`, `pl-firma[.]net`	26 Oct	25
No meaning in Polish	`lapax[.]net`, `wabze[.]net`, `mozesz[.]net`, `lapaxe[.]com`	27 Oct (`lapaxe[.]com` in 2011)	275
Bankowość elektroniczna, electronic banking	`bankowosc-elektroniczna[.]com`, `bankowosc-elektroniczna[.]net`, `elektroniczna-bankowosc[.]com`, `elektroniczna-bankowosc[.]net`	31 Oct to 5 Nov	181

Mozesz is close to the Polish for "you can"; the other three in that row carry no meaning NSS could find. The themed domains come in pairs and fours that swap the order of the words and the ending, a common way to buy look-alikes. Registration times are public records, read on 13 November.

How the domains were set up

Four things were the same across the set. Only the first is counted as a link.

- **The link format.** Every domain carried names in the same format, with the same words, the same code shape and the same labels. This is what ties the 19 domains into one set.
- **One registrar.** 18 of the 19 were registered at the same registrar, one to three a day. That is context: the registrar serves many unrelated customers, and no group of five was bought inside 30 seconds, so there is no purchase batch.

- **One DNS service.** All 17 domains for which NSS holds name-server records used the same pair of name servers at a large DNS provider. That provider hands the same pair to many unrelated accounts, so it is not a link.
- **A certificate for every name.** For the four domains whose certificates NSS has stored, each certificate covered the domain and every name under it. That is why none of the 576 link names appeared in certificate logs on its own, and why watching certificate logs for the brand would not have shown them.

Where the names pointed is context, not an indicator. In NSS's resolution records one address on a network in Vietnam answered for 203 names under 10 of the domains between 25 October and 2 November, a second address answered for 43 names under `lapax[.]net` and `lapaxe[.]com`, and the others resolved to a content-delivery network or to two further addresses. NSS could not establish whether anyone else uses the first address: it showed only a web server's default page, file transfer and remote login when NSS's probe read it, and it stopped answering on 12 November. The addresses are not in the indicator list.

The 19th domain is the odd one. `lapaxe[.]com` was first registered in 2011 at a different registrar and carried names in the same format from 27 October, the day `lapax[.]net` was registered. NSS does not know whether it was bought, reused or taken over.

What the pages did

NSS did not see a page from this set. Its capture attempts on 31 October and 13 November found nothing to load. What the pages did comes from public reporting from October 2026: emails to the bank's business customers asked them to update company documents or verify their identity, and a fake business-banking login under `rzad-pl[.]net`, one of the 19, asked for the login, the password and the second factor. That reporting named no group, and neither does this paper.

A correction to NSS's register

On 4 November NSS's register filed the address that served most of these names as a confirmed cluster on a dedicated host, found by NSS. The records do not support that reading. Every name on the address came from public lists, the address's host type is unknown, and nothing NSS holds shows that only this operator used it. On 13 November NSS retired that register entry. The address is now recorded as context, host type unknown, not operator infrastructure. The set is tied by its link format.

What a defender can look for

- In mail and web logs from 23 October 2026 on, names that match `(^|//)(sesja|pl)-[0-9][a-z][0-9][a-z](-[a-z-]+)?\.` followed by any domain. A hit is a link that was sent; look for who received it and whether anyone entered details.
- Treat any name under the 19 domains as part of the set, not only names in this format: the login that public reporting named was `biznes[.]rzad-pl[.]net`. In web gateway logs, also match `/logowanie?sid=` followed by 32 hexadecimal characters (`/logowanie\?sid=[0-9a-f]{32}`).
- The 19 registered domains in the indicator list. Blocking a domain covers every link name under it.
- New domains that join a Polish word for an authority, the government or electronic banking with pl or a bank's name, bought one or two a day. The theme may change again; the link format is the stronger sign.
- Business-banking users at Polish banks: a request to update company documents or re-verify identity that leads to a login page outside the bank's own address.
- Do not block the addresses. NSS could not show they belong only to this set.

The NSS tools used

> Hunt
Found all 595 names in the lists NSS takes in by their link format and their 19 domains, with the time each one reached NSS.

> Investigate
Read the public registration record of all 19 domains on 13 November and built a casefile for each: registrar, registration time, hold status, certificates and verdict.

> Capture
Tried to load sample names on 31 October and every domain on 13 November. No page loaded; on 13 November no domain resolved.

> Probe
Read the open services on the address that served 203 of the names 12 times between 28 October and 12 November: a default web page, file transfer and remote login, then no answer.

> Register
Filed the address as a confirmed cluster on 4 November; NSS retired that entry on 13 November after this analysis.

Indicators

The first 25 of 595 indicators. Each is written defanged so it cannot be opened by accident.

INDICATOR	TYPE	NOTE
`pl-wladze[.]com`	Domain	Registered domain, registered 23 O 2026; on hold a the registrar or 13 Nov 2026
`wladze-pl[.]com`	Domain	Registered domain, registered 23 O 2026; did not resolve on 13 Nov 2026

pl-wladze[.]net	Domain	Registered domain, registered 24 O 2026; did not resolve on 13 Nov 2026
wladze-pkobiznes[.]com	Domain	Registered domain, registered 25 O 2026; did not resolve on 13 Nov 2026
wladze-pl[.]net	Domain	Registered domain, registered 25 O 2026; did not resolve on 13 Nov 2026
rzad-pl[.]com	Domain	Registered domain, registered 25 O 2026; on hold a the registrar on 13 Nov 2026
pl-rzad[.]com	Domain	Registered domain, registered 26 O 2026; did not resolve on 13 Nov 2026
pl-rzad[.]net	Domain	Registered domain, registered 26 O 2026; did not resolve on 13 Nov 2026
rzad-pl[.]net	Domain	Registered domain, registered 26 O 2026; did not

		resolve on 13 Nov 2026
pl-firma[.]com	Domain	Registered domain, registered 26 O 2026; did not resolve on 13 Nov 2026
pl-firma[.]net	Domain	Registered domain, registered 26 O 2026; on hold a the registrar or 13 Nov 2026
lapax[.]net	Domain	Registered domain, registered 27 O 2026; on hold a the registrar or 13 Nov 2026
lapaxe[.]com	Domain	Registered domain, first registered in 2011, in the se from 27 Oct 2026; did not resolve on 13 Nov 2026
wabze[.]net	Domain	Registered domain, registered 27 O 2026; on hold a the registrar or 13 Nov 2026
mozesz[.]net	Domain	Registered domain, registered 27 O 2026; on hold a the registrar or 13 Nov 2026

bankowosc-elektroniczna[.]com	Domain	Registered domain, registered 31 O 2026; did not resolve on 13 Nov 2026
bankowosc-elektroniczna[.]net	Domain	Registered domain, registered 31 O 2026; on hold a the registrar or 13 Nov 2026
elektroniczna-bankowosc[.]com	Domain	Registered domain, registered 5 No 2026; on hold a the registrar or 13 Nov 2026
elektroniczna-bankowosc[.]net	Domain	Registered domain, registered 5 No 2026; on hold a the registrar or 13 Nov 2026
sesja-1w3x-pkobp[.]pl-wladze[.]com	Domain	Link name (ses code-pkobp); reached NSS from public list 24 Oct 2026
sesja-2p0l[.]wladze-pkobiznes[.]com	Domain	Link name (ses code); reached NSS from publ lists 25 Oct 20
sesja-0g6k-pkobiznes[.]rzad-pl[.]net	Domain	Link name (ses code-pkobizne reached NSS from public list 26 Oct 2026

sesja-0f7z-pkobiznes-firma[.]wabze[.]net	Domain	Link name (ses code-pkobizne firma); reached NSS from publ lists 27 Oct 20
pl-0a7r-pkobiznes-firma[.]mozesz[.]net	Domain	Link name (pl- code-pkobizne firma); reached NSS from publ lists 28 Oct 20
pl-0a5y-pkobiznes[.]bankowosc-elektroniczna[.]net	Domain	Link name (pl- code-pkobizne reached NSS from public list 5 Nov 2026

FULL LIST CSV JSON

How we know

What this rests on

- The 595 names and the time each reached NSS are from the lists NSS takes in, read on 13 November 2026. Each name was carried by one to four lists.
- Registration times, registrars and hold status are the public registration records of the 19 domains, read on 13 November 2026.
- The live state is from one check of every domain on 13 November 2026 between 11:38 and 11:50 UTC: nine on hold at the registrar, ten that did not resolve.
- Where the names pointed is from NSS's resolution records of 25 October to 7 November. Certificates are from NSS's certificate store, which holds records for four of the 19 domains.
- What the pages asked for is from public reporting from October 2026. NSS did not load a page from the set.

What we cannot say

- NSS did not discover these names; public lists carried them first. Nothing here is a claim of being first.
- NSS saw no page, no email and no victim. The purpose of the set rests on its names, on the lists that carried them and on public reporting about one of its domains.
- The 576 link names are links that were sent, not separate sites. They are listed so that logs can be searched for them.
- One link format ties the names. It may be one operator, or one kit used by more than one; NSS cannot tell which.
- Addresses are not in the indicator list. NSS could not show that anyone but this set used them.
- This paper is not attributed to any named group.

Use and citation

This paper is marked TLP:CLEAR: it may be shared without restriction. Cite as:

```
Nexus Sentinel Station (NSS), "Polish official and e-banking lookalike
domains aimed at PKO business-banking users: technical analysis", NSS-
GB-01, 13 Nov 2026. https://nsshq.com/research/official-lookalike-names
```

See something wrong? corrections@nsshq.com

NSS is not affiliated with PKO Bank Polski, the Polish government or any registrar, network or service named in this paper. They are named because the names in the set or the public records name them; nothing here says any of them knew of or took part in the activity.