

Found by NSS

All 48 names recorded by NSS's own sensors; listing state checked on 16 and 18 November 2026

Tracking since 28 Oct 2026 · Last checked 18 Nov 2026

Numbered bank "auth gateways": one generator, 18 brands, an empty page for anyone without the link

Fraud and brand protection: jump to what to do about it.

Between 27 October and 16 November 2026 one generator bought 48 names such as 42708-fifth-third-auth-gateway[.]icu, 46208-capone-auth-gateway[.]icu and 94709-citi-auth-gateway[.]credit: a number, a bank or carrier and a word like "auth gateway" or "identity verif", on cheap domain endings. Every one of them uses the same DNS service, and on 16 November 47 resolved to a pool of 13 small rented servers where names of different banks share the same address. 15 of the 21 names NSS tried answered with an empty page at the root, consistent with content served only on the message link; one led to a picture puzzle. On 16 November none of

the 48 was on a threat list NSS takes in. Read again two days later, 44 of the 48 still answered on the same 13 servers, three had gone to a registry hold, still none was on a list, and the generator had bought six more names, two of them in a shape that reads as a credit union's own fraud-prevention line.

PUBLISHED	LAST UPDATED	READING TIME	MARKING
18 Nov 2026	18 Nov 2026	28 min	TLP:CLEAR

48
names from one generator, bought 27 October to 16 November 2026, all on one DNS service

18
brands read from the names: 16 US banks, credit unions and fintechs and two mobile carriers

13
small rented servers holding 47 of the names on 16 November; names of different banks share them

0 of 54
names on any threat list NSS takes in, on 16 and 18 November 2026: the 48 measured, plus six found later

Key findings

1. One generator, 48 names. Between 27 October and 16 November 2026, 48 names were bought that read as a bank, credit-union, fintech or mobile-carrier verification step: 42708-fifth-third-auth-gateway[.]icu, 46208-capone-auth-gateway[.]icu, 94709-citi-auth-gateway[.]credit, 8228-great-lakes-acceweb-auth[.]info, 19251-vz-auth-access[.]icu, 51954-robins-member-auth[.]icu, and 42 more. Thirty-four of them start with a number of three to five digits; the rest use verification words such as selfverify[.]top or wellsfargosecure[.]support.
2. Eighteen brands, read from the names: ten banks (Fifth Third, Capital One, Citi, U.S. Bank, Wells Fargo, PNC, Regions, BMO, Orrstown, BCB), five credit unions (Great Lakes, Grow Financial, SAFE, NYMCU, Robins), one fintech (Chime) and two mobile carriers (Verizon and the Canadian

carrier Freedom Mobile). Twenty-seven names carry no brand at all: a number and "auth-gateway", "access-auth" or "identity-verif", ready for any target.

3. One DNS service, and a shape seen nowhere else. All 48 names use the same pair of name servers at one DNS service, a service other customers use too, so on its own it ties nothing. What it adds is this: all 33 names of the numbered shape that NSS saw appear between 15 October and 15 November sit on that pair and on no other, and the two bought on 16 November use it too. The pair took on 23 other names in that time (16 new, 7 moved over), none about banks. One more name on the pair, myfreedommobile[.]info, points somewhere else and is left out.

4. One shared pool of servers. On 16 November 47 of the 48 names resolved to 13 small rented servers, going by their address blocks in two hosting networks (ten and three), and names of different banks share them: 138.124.79[.]185 held eight names for Orrstown, NYMCU, Fifth Third, Chime and generic targets; 153.80.249[.]234 held eight for Fifth Third, Wells Fargo, Robins and generic targets. Five of the 13 addresses carry names of two or more brands. A bank-by-bank operation would not mix them; one generator does. The servers themselves are plain. NSS has a reading of the first answer from eight of the 13 addresses: six send one stock web-server banner and two, 94.26.106[.]184 and 185.112.59[.]33, send another, both of them default packages of one widely used operating system. Which banner a name gets follows its address, not its brand, and nothing is added to the answer and no cookie set except on the one gate name. That reads as a plain off-the-shelf build on rented servers; it is not a fingerprint, because both banners sit on a large share of the web.

5. Bought in bursts, at one registrar and later a second. All 48 registration records name the same registrar, and the six later names found by the re-check show a second one in use as well. Ten names were bought on 10 November between 05:31 and 22:05 UTC, among them the Citi, U.S. Bank, Regions, PNC, BCB, NYMCU and both Wells Fargo names. On 14 November three were bought between 03:02 and 03:20 UTC and six

more between 21:56 and 22:11 UTC: the Fifth Third, BMO, Capital One, Robins and Chime names and one generic name. The registrar alone ties nothing; the shape, the DNS service and the pool together do.

6. Certificates in the same seconds. On 12 November the certificates for 42708-fifth-third-auth-gateway[.]icu and 44102-access-auth[.]icu were logged three seconds apart, at 17:27 UTC, and those for 19102-auth-gateway[.]icu and 19251-vz-auth-access[.]icu two seconds apart, at 23:07 UTC: one hand setting up two names at once.

7. Empty pages, and one gate. On 16 November NSS tried to capture 21 of the names, between 04:52 and 05:02 UTC and between 15:24 and 15:34 UTC. 15 of them answered with an empty page at the root, consistent with a page served only on the message link. Two did not: 9353-safe-acceweb-auth[.]info showed a page titled "Loading" and nothing else, and 7008-grow-acceweb-auth[.]xyz, the Grow Financial name, sent NSS from its root to a home-made picture puzzle ("Select all images with a plus sign", step 1 of 2) whose onward path is named for a Gmail sign-in step and tagged with an id. NSS did not solve the puzzle, so that step is unread; the generator is no longer only staged.

8. Nothing on the lists, twice. On 16 November none of the 48 names was on a threat list NSS takes in, and on 18 November none of them was either, nor any of the six later names. Of the 13 addresses, one, 176.65.132[.]55, has been on a list since November 2025, a year before these names, in an address block that lists carry widely; the other 12 were on none on either day.

9. Two days later: three names held, 44 still answering, six more bought. NSS read all 48 names again on 18 November from public infrastructure alone, at 00:03 to 00:30 UTC. 44 still resolve, on the same 13 addresses and through the same pair of name servers. Three that were resolving on 16 November now carry a registry-level hold and no longer resolve: 12145-auth-gateway[.]icu, 3097authgateway[.]xyz and 319-fifth-third-identity-verif[.]icu, which had answered a page two days earlier. Not one of the 48 was deleted; every registry record still says registered, so a hold can come off and the names belong on a block list well past the

day they stop resolving. In the same two days the generator did not stop: NSS's own records hold six more of its names, all bought on 16 November, all on the same name-server pair and in the same server pool, and none of them on any list. Two of the six, bought 92 seconds apart at a second registrar, are bcufraud-prevention[.]org and vacufraud-prevention[.]org: initials that read as a credit union's, joined to that credit union's own fraud-prevention line. NSS does not say which institution either set of initials means, because initials are not enough to name one. What did not move is the one page there was to see. On 18 November at 00:14 UTC 7008-grow-acceweb-auth[.]xyz still sent NSS from its root to the same picture puzzle, with the same onward path to an e-mail sign-in step and the same id on the end, and it was still on no list. Three names of the set were put on a registry hold in those two days; the one serving a gate was not.

10. Evidence at operator level, and what the per-name bands show. NSS lists all 48 names, and the six later ones, on what ties them: 54 rows in the files. Investigate and Scan agree on every name and every address. The two Wells Fargo names read Suspicious; five names read Low risk; the other 41 read Clean on 16 November, including the Grow Financial name behind its puzzle. A per-name band rates what a name shows, and these names show nothing to anyone without the message link. This paper lists all 48 on the generator evidence (the shape on one DNS service, one server pool, bursts and paired certificates), not on the per-name verdicts. Of the 13 servers, 153.80.249[.]234 and 176.65.132[.]55 read Suspicious; the servers are in the files to watch, not in the indicator list.

If you work in bank fraud or brand protection

This set is aimed at your customers and is almost invisible to the controls security owns: the names show nothing to a scanner, none of them reached a public list in three weeks, and the operator bought six more on the day NSS wrote this paper. These are the moves that work on it.

1. Take the names, not the pattern, to the registrar and the hosting company. A take-down request carrying a dated record of what a name is and where it resolves gets further than a suspicion. This paper's files are built to be forwarded: every row has the registration time, the address and what the name answered, with the day each was read.
2. Treat a hold as a pause. Three of these names were put on a registry hold within two days of NSS's reading and not one of the 54 was deleted, so every registration still stands and a hold can come off. Keep held names on your block list and re-check them rather than closing the ticket.
3. Ask for the full link, and keep it. These pages show nothing to anyone who opens the bare name, so the link out of the message is the only way anyone sees what a customer saw. When a customer forwards a text or an e-mail, keep the whole address and the time it arrived, and get it to whoever handles your take-downs.
4. Watch for your own brand in a shape no bank uses: a number joined to your name and a word like "auth gateway" or "identity verif", and now your initials joined to your own fraud-prevention line. The patterns are under What a defender can look for. A name of that shape younger than a month that nobody in your business can account for is worth a take-down request while you ask.
5. Guard the anti-fraud voice hardest. The two newest names borrow a credit union's own fraud-prevention wording, which is the message you ask customers to act on. If your fraud alerts tell customers what you will never ask them for, and how to reach you without using a link, that wording is worth more to them than any name you block.
6. Register your own obvious variants before someone else does, and tell your customers the one address you will

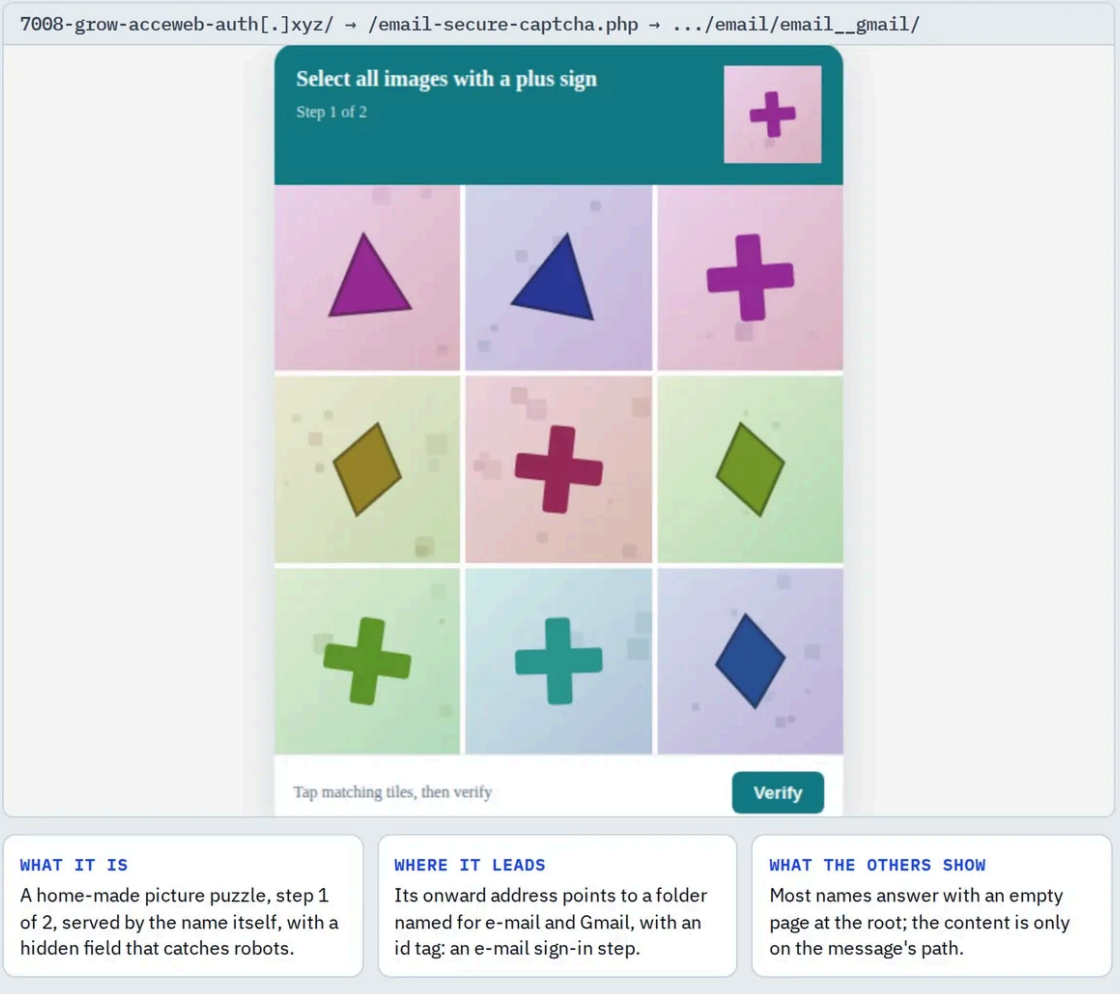
always use. Neither costs much, and both shrink what this kind of generator has to work with.

7. Do not wait for a list to agree with you. None of the 54 names was carried by any threat list NSS takes in on either day it looked, and the one listed address in the pool was listed a year before these names arrived, for something else. The name serving the one gate NSS found had been registered a fortnight and was still on no list.

NSS has not seen a message, a victim or a payment, and this paper claims none. It gives you the names, the servers and the dates; the loss data, if any exists, is yours.

The gate on 7008-grow-acceweb-auth[.]xyz, 16 November 2026, 15:32 UTC

NSS's stored capture, cropped to the puzzle; the address bar line is added for the reader. NSS did not solve the puzzle.



The one gate NSS saw, on the Grow Financial name. NSS did not solve the puzzle, so the e-mail step behind it is unread. Address defanged.

One generator, 13 servers: which brands share which address

Fresh DNS, 16 November 2026. 47 of the 48 names resolved; each chip is one name, labelled with the brand read from it, its outline the shape of the name. 1 name did not resolve.

number + auth-gateway · number + brand + acceweb-auth · number + access-auth or member-auth · number + identity-verif · verification or bank word

138.124.79[.]185 8 names, 4 brands	generic · generic · Orrstown Bank · generic · NYMCU · generic · Fifth Third Bank · Chime
153.80.249[.]234 8 names, 3 brands	generic · generic · Fifth Third Bank · Wells Fargo · Wells Fargo · generic · Robins · generic
147.45.61[.]154 6 names, 2 brands	generic · Great Lakes · generic · generic · generic · BMO
153.80.249[.]5 5 names, 3 brands	generic · BCB · generic · Verizon · Capital One
147.45.61[.]183 4 names, 1 brand	generic · generic · Regions Bank · generic
176.65.132[.]54 4 names, 1 brand	generic · generic · Citi · generic
94.26.106[.]184 3 names, 2 brands	U.S. Bank · PNC · generic
147.45.61[.]246 2 names, 0 brands	generic · generic
168.113.215[.]244 2 names, 1 brand	Grow Financial · generic
176.65.132[.]55 2 names, 0 brands	generic · generic
138.124.79[.]163 1 name, 1 brand	Great Lakes
185.112.59[.]33 1 name, 1 brand	Freedom Mobile
94.103.1[.]244 1 name, 1 brand	SAFE

Which brands share which server, from fresh DNS on 16 November 2026. Each row is one address of the pool; each chip is one name on it, labelled with the brand read from the name. Names of different banks share most addresses.

When the 48 names were bought (UTC)

One dot per name, from public registration records read on 16 November 2026; names bought within a few hours of each other are stacked. All 48 at one registrar. The two bursts: ten names on 10 November (05:31 to 22:05 UTC) and six on 14 November between 21:56 and 22:11 UTC.

number + auth-gateway · number + brand + acceweb-auth · number + access-auth or member-auth · number + identity-verif · verification or bank word

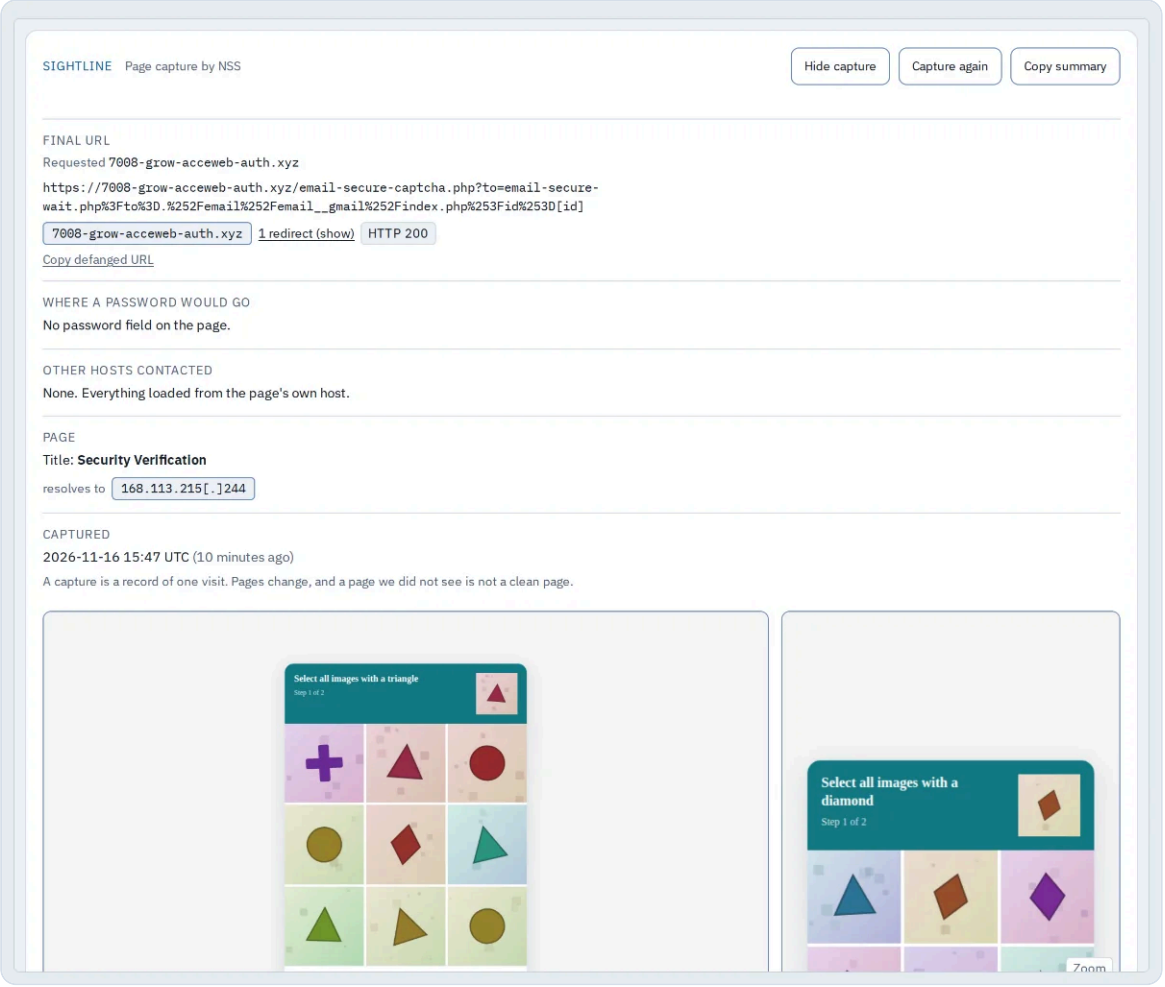


When the 48 names were bought, from public registration records read on 16 November 2026. Two bursts stand out: ten names on 10 November and six in 16 minutes on 14 November.

How an analyst finds this with NSS

The same case, worked the way a defender works it in NSS: from one bank name to its server, out to the other banks on that server, to the whole shape, and on to the thing to watch. Every picture is the real Station on 16 November 2026, cropped to the panel in use.

01 Open one of the bank names in Investigate. Its Sightline card shows what NSS's capture got from the name: a redirect from the bare name to a page titled "Security Verification", a picture puzzle, and an onward address into a folder named for e-mail and Gmail.



Investigate, 16 November 2026. The id tag at the end of the address is masked. The capture is the evidence: the redirect, the puzzle and the e-mail path, stored and dated. The

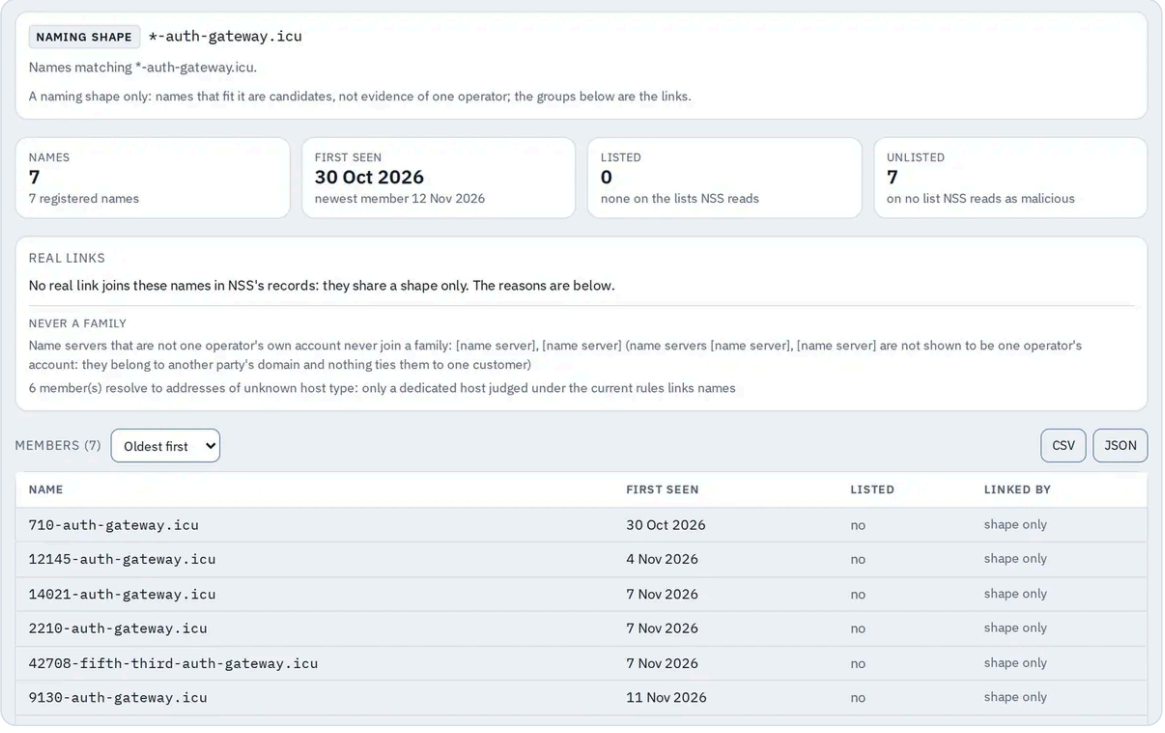
per-name band waits for the page behind the puzzle (see Key findings).

02 Pivot on a server. A two-step tool chain from 51954-robins-member-auth[.]icu returns the address NSS has on record for it, then every name NSS has seen on that address: eight, for Wells Fargo, Fifth Third, Robins and generic targets.



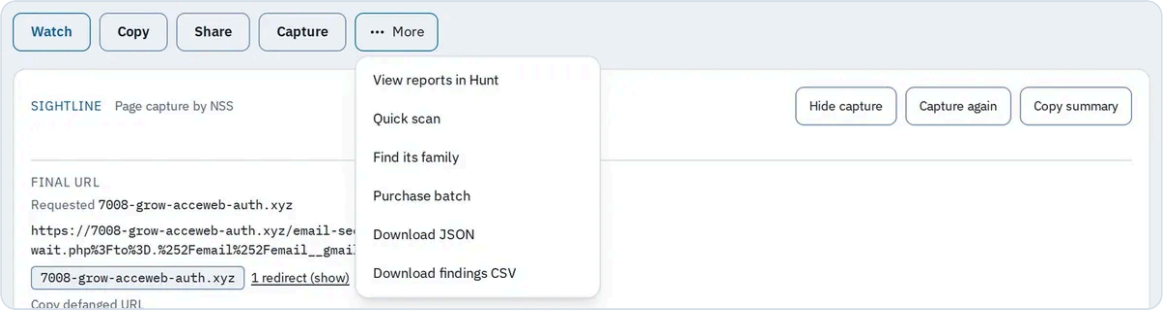
The chain run on 16 November 2026: one Robins credit-union name leads to Wells Fargo and Fifth Third names on the same server.

03 Widen the shape. The Family finder on *-auth-gateway[.]icu returns seven registered names, none on a list. The finder lists them; the tie in this paper is the shape on one DNS service and the pool.



Family finder, 16 November 2026, cropped to the first six members. Its index lagged that day: it shows 7 of the paper's 9 names of this shape (not yet the BMO and Capital One names of 14 November).

04 Then act: watch the servers for the next name, share the casefile, or download it as JSON or CSV for your own tools (Full features).



The casefile's actions, 16 November 2026 (Full features). Nothing was clicked for the picture but the More menu.

Automate it with the NSS API

Every NSS check is JSON: a risk band, the host class, how many names share the host (on an address check), the public-listing state and the time of the answer. The public check needs no key and takes one domain name or one IP address, a few checks a day for each network. A Full account adds API keys, each with its own daily allowance and a limit per minute, made on the account's API keys page.

One check from a shell

```
NAME=$(jq -r '.indicators[0].value' nss-bk-01.json)   # the first indicato
curl -s "https://nsshq.com/api/v1/check?value=$NAME"
```

The paper's indicator file, in JSON or CSV, is linked at the end of this page.

The answer for wellsfargosecure[.]support on 16 November 2026


```
{
  "as_of": "2026-11-16T15:54:31Z",
  "band": "Suspicious",
```

```
  "band_is_host_class": false,
  "found": true,
  "host_class": {
    "class": "unknown",
    "label": "Host type unknown",
    "sentence": "Host type unknown (8 name(s) seen on it, (...)"
  },
  "known_good": false,
  "names": { "at_least": false, "listed": null, "total": 8 },
  "public_listing": { "state": "not_listed", (...) },
  "reports": 0,
  "type": "domain",
  "value": "wellsfargosecure[.]support",
  "view": "public"
}
```

The real public answer, read on 16 November 2026 at 16:22 UTC (the verdict itself dated 15:54 UTC). Here the value is defanged and two long fields shortened. This is one of the two names NSS rates Suspicious; most names in this paper answer Clean or Low risk, so check the generator's shape and servers, not only each name's band. When a network's public checks for the day are used up, the same request answers HTTP 429 with a body that says when they reset (00:00 UTC); a Full key has its own allowance.

Check the whole file every day and flag changes (Python 3, standard library only)

```
#!/usr/bin/env python3
"""Check every name and address in an NSS paper's indicator file and flag

  python3 nss_check_file.py nss-bk-01.json
Without a key it uses the public check (no key needed, a few checks a day
page, then set NSS_API_KEY to the key and NSS_API_URL to the request that
header, never in the address. Prints one JSON line per indicator; exits 2
"""
import json, os, sys, time, urllib.error, urllib.parse, urllib.request

URL = os.environ.get("NSS_API_URL", "https://nsshq.com/api/v1/check?value=
KEY = os.environ.get("NSS_API_KEY", "")
STATE = os.environ.get("NSS_STATE", "nss-verdicts.json")
```

```
def request_url(value):
    u = urllib.parse.urlsplit(URL)
    q = urllib.parse.parse_qsl(u.query)
    q = [(k, value if v == "example.org" else v) for k, v in q] if any(v =
    return urllib.parse.urlunsplit(u._replace(query=urllib.parse.urlencode


def check(value):
    req = urllib.request.Request(request_url(value), headers={"Accept": "a
    while True:
        try:
            with urllib.request.urlopen(req, timeout=120) as r:
                return json.load(r), r.headers.get("NSS-Quota-Remaining")
        except urllib.error.HTTPError as e:
            try:
                body = json.loads(e.read() or b"{}")
            except ValueError:                                      # an e
                body = {}
            if e.code == 429 and e.headers.get("Retry-After"):      # per-
                time.sleep(int(e.headers["Retry-After"]) + 1)
                continue
            if e.code == 429:                                       # the
                return {"stopped": body.get("resets_at") or "daily limit r
            return {"error": e.code, "detail": body.get("error")}, None


def verdict(answer):
    return answer.get("band") or answer.get("label") or answer.get("verdic


def main(path):
    items = json.load(open(path))["indicators"]
    old = json.load(open(STATE)) if os.path.exists(STATE) else {}
    new, changed = dict(old), False
    for it in items:
        if it["type"] not in ("domain", "ipv4"):                    # the
            continue
        answer, left = check(it["value"])
        if "stopped" in answer:
            print(json.dumps({"stopped": answer["stopped"]}), file=sys.std
            break
        v = verdict(answer)
        row = {"value": it["value"], "type": it["type"], "verdict": v, "as
        row["changed"] = bool(row["previous"]) and v != row["previous"]
```

```
            changed |= row["changed"]
            if v:
                new[it["value"]] = v
            print(json.dumps(row))
            if left == "0":
                break
            time.sleep(1.1)                                                 # stay
    json.dump(new, open(STATE, "w"), indent=1)
    sys.exit(2 if changed else 0)


if __name__ == "__main__":
    main(sys.argv[1] if len(sys.argv) > 1 else "nss-bk-01.json")
```

One JSON line per indicator for a SIEM or a log, and exit code 2 when a verdict changed since the last run. With a Full key, set NSS_API_KEY and NSS_API_URL (the request your API keys page shows); the key travels only in the Authorization header, and the script waits when told to slow down and stops when the day's allowance is spent. This generator keeps buying names, six of them on 16 November alone: re-read the paper's file when it is updated. The script checks the indicators; the pool addresses are in the same JSON file under watch[.]rows, to add by hand.

Every morning, with a mail when a verdict changes

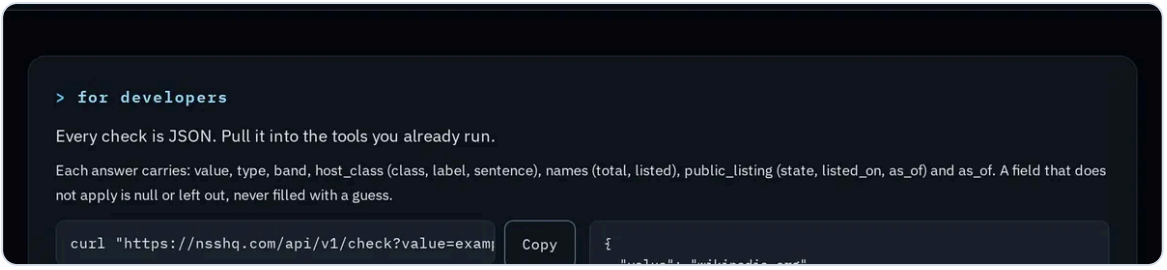
```
0 6 * * * cd /opt/nss && python3 nss_check_file.py nss-bk-01.json >> check
```

STIX 2.1 and MISP

```
git clone https://github.com/nsshq/nssresearch
# each paper's folder holds stix2.1-bundle.json, misp-event.json and iocs.
```

This paper's folder is added when it is published.

The cheapest control here is the shape: a number, a brand and "auth gateway", "acceweb auth", "access auth" or "identity verif" is not a name a bank uses. The first regular expression under What a defender can look for matches all 35 numbered names in this paper's files and none of the other 19, and a second one covers the "fraud prevention" shape that turned up on 16 November.



The public Developers page on nsshq.com, 16 November 2026: the request, the fields every answer carries and a live answer.

Timeline

27 Oct 2026
The first names are bought: selfverify[.]top and member-identity-verification6645[.]xyz, 75 seconds apart. NSS first records names of the set the next day.

29 to 30 Oct
The first numbered names: 710-auth-gateway[.]icu, 55835-access-auth[.]icu, and the two Great Lakes credit union names, bought 16 minutes apart.

3 to 8 Nov
Orrstown, Grow Financial, Fifth Third and SAFE names, and more generic numbered names.

10 Nov
Ten names in one day: Citi, U.S. Bank, Regions, PNC, BCB, NYMCU and two Wells Fargo names among them.

11 to 12 Nov
Freedom Mobile and Verizon names. On 12 Nov two pairs of certificates are logged seconds apart.

14 Nov
Nine names: three generic names before dawn, then six between 21:56 and 22:11 UTC for Fifth Third, BMO, Capital One, Robins, Chime and one generic target.

16 Nov, 00:06 to 23:41 UTC

Seven names are bought across the day. 11408-auth-access[.]icu, at 03:32 UTC, resolves into the pool the same afternoon and is one of this paper's 48. The other six reached NSS's own records on 16 and 17 November, after the set below was counted, and the 18 November re-check brought them in: a Wells Fargo name on a new ending, a second Freedom Mobile name, two generic names, and two credit-union "fraud prevention" names bought 92 seconds apart at a second registrar.

16 Nov

NSS reads the set back: 48 names, one DNS service, 13 servers, 0 names listed. NSS tries to capture 21 names: empty pages, a "Loading" page and, on the Grow Financial name, a picture puzzle with an onward path to an e-mail sign-in step.

18 Nov, 00:03 to 00:30 UTC

All 48 names are read again from one public resolver and from the public registry records: 44 still resolve on the same 13 servers and the same name-server pair, three have gone to a registry hold since the 16 November reading, none of the 48 is deleted and none is on a list. The six later names are on the same pair and in the same pool, and on no list either.

The names

A name from this generator has up to three parts: a number of three to five digits, a brand, and a word that sounds like a bank's sign-in step. The parts are joined by hyphens on cheap domain endings.

SHAPE	NAMES	EXAMPLES
number + [brand] + auth-gateway	12	42708-fifth-third-auth-gateway[.]icu, 46208-capone-auth-gateway[.]icu, 94709-citi-auth-gateway[.]credit, 710-auth-gateway[.]icu
number + [brand] + access-auth, auth-access or member-auth	11	19251-vz-auth-access[.]icu, 4581-chime-access-auth[.]icu, 51954-robins-member-auth[.]icu, 1954-regionsmember-auth[.]credit

number + brand + acceweb-auth	7	8228-great-lakes-acceweb-auth[.]info, 87134-orrstown-acceweb-auth[.]site, 3992-pncacceweb-authent[.]net
number + [brand] + identity-verif	4	319-fifth-third-identity-verif[.]icu, 085-identity-verif[.]icu, 24952usbankidentityverif[.]credit
verification or bank word, number at the end or none	14	wellsfargosecure[.]support, wellsfargo-risk-management[.]com, nymcuverify[.]support, loginfreedommobile[.]com, selfverify[.]top

The numbers do not repeat. They look like tags the operator uses to tell campaigns or targets apart, and "acceweb" (access plus web) is a word no bank uses. The endings are mostly cheap: .icu, .credit, .info, .live, .site, .xyz, .support, .financial, .digital and .top, plus .net and .com.

What ties them

Three things tie the 48 names together, and none of them depends on spelling. "Together" here means one hand made and set them up; it does not mean NSS knows whose hand.

- **A shape seen on one DNS service only.** Every name uses the same pair of name servers at one DNS service. The service has other customers, so the pair alone ties nothing; but all 33 names of the numbered shape that NSS saw appear between 15 October and 15 November sit on that pair and on no other, and the two bought on 16 November use it too. The pair took on 23 other names in that time (16 new, 7 moved over), none about banks.
- **One shared pool of servers.** On 16 November 47 names resolved to 13 small rented servers, and names of different brands share five of them. The figure above shows which.

- **Bursts and paired certificates.** The names arrive in bursts (ten on 10 November, six in 16 minutes on 14 November), and on 12 November two pairs of certificates were logged seconds apart.

All 48 registration records name one registrar, which many unrelated operators use; it is consistent with the rest but proves nothing by itself. The same goes for the servers' own answers. NSS read the first answer from eight of the 13 addresses, on 16 and again on 18 November. Six send one stock web-server banner and two send another, both default packages of one widely used operating system, and which one a name gets follows its address rather than its brand. Nothing is added to the answer beyond what the package sends. That reads as one plain, copied build rather than a careful one, and it is useful background, but those two banners sit on a large share of the web, so they are not a fingerprint and no part of this paper's tie rests on them.

The servers

ADDRESS	NAMES, 16 NOV	BRANDS ON IT
138.124.79[.]185	8	Orrstown, NYMCU, Fifth Third, Chime, generic
153.80.249[.]234	8	Fifth Third, Wells Fargo (2), Robins, generic
147.45.61[.]154	6	Great Lakes, BMO, generic
153.80.249[.]5	5	BCB, Verizon, Capital One, generic
147.45.61[.]183	4	Regions, generic
176.65.132[.]54	4	Citi, generic
94.26.106[.]184	3	U.S. Bank, PNC, generic
147.45.61[.]246, 176.65.132[.]55	2 each	generic
168.113.215[.]244	2	Grow Financial, generic

138.124.79[.]163, 185.112.59[.]33, 94.103.1[.]244	1 each	Great Lakes, Freedom Mobile, SAFE

Going by their address blocks, ten of the 13 addresses sit in one small hosting network and three in another. NSS's records show no other name on any of them. One, 176.65.132[.]55, has been on a list since November 2025, a year before these names, in a block that lists carry widely: read that as the block's history, not as a tie.

All 13 addresses were still in use on 18 November and the pool had not moved; only the counts changed. Counting the 48 alone, the three names put on a registry hold took 138.124.79[.]185 from eight to six and 176.65.132[.]54 from four to three, and every other row was the same. Counting the six later names as well, five rows go the other way: 147.45.61[.]154 to eight, 138.124.79[.]185 back to seven, 153.80.249[.]5 to six, 147.45.61[.]183 to five and 185.112.59[.]33 to two. The JSON file carries both counts for every address.

What the names show

On 16 November NSS tried to capture 21 of the names: 8 between 04:52 and 05:02 UTC and 14 between 15:24 and 15:34 UTC, the Citi name in both.

WHAT NSS SAW	NAMES
An empty page at the root (HTTP 200, nothing in it)	15, including names for Wells Fargo, Fifth Third, Capital One, Robins, Great Lakes, Orrstown, BMO, Chime, Verizon, PNC, U.S. Bank, BCB and NYMCU
A page titled "Loading" and nothing else	9353-safe-acceweb-auth[.]info
A picture puzzle in front of an e-mail sign-in step	7008-grow-acceweb-auth[.]xyz

No answer	the Citi and Regions names; two more (11408-auth-access[.]icu and loginfreedommobile[.]com) could not be read that day

The empty page is the interesting part: a scanner or a curious visitor who opens the bare name sees nothing; the plain reading is that only the full link from the message reaches the page. The Grow Financial name went one step further. Its root sent NSS to a home-made picture puzzle ("Select all images with a plus sign", step 1 of 2) with a form that posts back to the same server and a hidden field of the kind used to catch an automated form fill. The puzzle's onward address points to a folder named for e-mail and Gmail, with an id tag on the end. That is a gate with an onward path named for an e-mail sign-in step. NSS did not solve the puzzle, so the page behind it is unread.

Three of these pages were read again on 18 November, between 00:14 and 00:15 UTC, and none of them had changed. 7008-grow-acceweb-auth[.]xyz still sends a visitor from its root to the same picture puzzle, with the same onward path to the e-mail step and the same id on the end. wellsfargosecure[.]support still answers with an empty page, and 9353-safe-acceweb-auth[.]info still shows the same "Loading" page. The Citi name gave no answer on 18 November either, as on 16 November. NSS still solved no puzzle and typed nothing into any form.

What it is not

NSS compared this generator with the other US bank phishing sets it tracked in November 2026: bank "support chat" names, a cluster of staged bank names on other servers, an investment-fraud front and a set of brand "notice mail" names. They share brands and, in one case, the registrar; none shares the DNS service, the server pool or the shape. On the evidence NSS holds, this set stands on its own and is not part of any of them. One pool address, 94.26.106[.]184, sits in the same block of addresses as a server from an earlier NSS paper; that is a shared hosting range, not a tie.

Operator evidence, and where it stops

What the records prove:

- **A shape seen on one DNS service only.** All 48 names on one pair of name servers of a shared DNS service; every numbered name of the shape since 15 October on that pair alone.
- **One pool of servers across brands.** 47 names on 13 addresses, five of them shared by two or more brands.
- **Bursts and paired certificates.** Names bought in bursts and certificates logged seconds apart.

What they do not prove:

- **Who the operator is.** No actor is named. "One generator" means these names were made and set up together, which the records above show; it is a grouping in NSS's own records, not an operator identity. No person, company or group is identified, and none is implied.
- **What the pages show to a victim.** The content sits behind the path in the message; NSS has not seen a message or a full link.
- **That anyone was harmed.** NSS has no victim, no count of people who opened a link, and no figure for money moved. None of that is claimed anywhere in this paper, and a reader should not infer it from the size of the name set.
- **That each brand is the target.** The brand is read from the name. A credit-union name such as "robins" or "safe" is the plain reading, not a certainty, and the initials in the two later "fraud prevention" names are weaker still.
- **That the generic names are the same campaign.** They share the DNS service, the pool and the shape; their targets are unknown. One of them, client-support-verification-7139[.]support, does not resolve and is on hold at its registrar; it is tied by the DNS service, the registrar and timing only (bought five minutes before user-verification-agent939[.]financial, which is on the pool).

What changed by 18 November

The readings behind the rest of this paper were taken on 16 November. Two days later NSS read the whole set again, this time from public infrastructure only: one public resolver for the address and the name servers of every one of the 48 names, and the public registry record of every one of them. The 48 names are unchanged in this paper, because they are the set NSS measured between 27 October and 16 November; this section says what two days did to it.

44 of the 48 still resolve, on the same 13 addresses and through the same pair of name servers. Three names that were resolving on 16 November no longer do, and the registry record of each says why: a registry-level hold that was not there before. They are 12145-auth-gateway[.]icu, 3097authgateway[.]xyz and 319-fifth-third-identity-verif[.]icu, and the third of those had answered a page when NSS looked on 16 November. The fourth name that does not resolve, client-support-verification-7139[.]support, carries the registrar hold it already had. Nothing was deleted: all 48 registry records still read as registered, and a hold can be lifted, so these names are worth keeping on a block list well past the day they stop resolving.

The generator did not pause while that happened. NSS's own records hold six more of its names, every one of them bought on 16 November, every one on the same name-server pair, and every one resolving into the same pool of servers. Three were bought before NSS's reading that day and three after it, and they reached NSS's records on 16 and 17 November, after the set above was counted.

NAME	BOUGHT, 16 NOV	ADDRESS, 18 NOV	READS AS
bcufraud-prevention[.]org	00:06	147.45.61[.]154	a credit union's initials plus its own fraud-prevention line

vacufraud-prevention[.]org	00:07	153.80.249[.]5	the same shape, different initials
96408-wells-acceweb-auth[.]creditcard	06:37	138.124.79[.]185	Wells Fargo, the numbered "acceweb auth" shape, a new ending
loginfreedommobile[.]digital	16:58	185.112.59[.]33	Freedom Mobile, beside loginfreedommobile[.]com there
securemobileonlinesupport[.]com	21:57	147.45.61[.]183	generic, no brand
rlwqj6xm06ps4[.]xyz	23:41	147.45.61[.]154	a random label, unlike the rest of the set

All six times are UTC.

Two of them matter more than the others. bcufraud-prevention[.]org and vacufraud-prevention[.]org were bought 92 seconds apart at a **second registrar**, which the first 48 never used, and they are the first names of this generator built on an institution's own fraud-prevention wording rather than a word from its sign-in step. NSS has seen no message carrying either name, so that is a change in the naming and not an observed lure; it is worth saying because the fraud-prevention line is the one a bank tells its customers to trust. NSS does not say which institution either set of initials stands for. Initials are thinner evidence than a spelled-out brand, and naming the wrong credit union would be a harm of its own; any institution whose initials these are should read both names as aimed at it.

Three of the six were read on 18 November, between 00:20 and 00:25 UTC: bcufraud-prevention[.]org, vacufraud-prevention[.]org and 96408-wells-acceweb-auth[.]creditcard. All three answer the way the rest of the set does, with an empty page at the root, nothing in it, no form and no cookie. Two more, loginfreedommobile[.]digital and securemobileonlinesupport[.]com, did not return a page to NSS that night, and the sixth was not read.

None of the six is on a threat list NSS takes in. All six were read on Investigate and on Scan and agree: four read Low risk and the two "fraud prevention" names read Clean, which is the same gap between the per-name bands and the generator evidence that the rest of this paper describes, on names bought the day it was written. The count of 18 brands does not change: the Wells Fargo and Freedom Mobile names add no brand this paper did not already carry, and NSS does not attribute the two sets of initials to anyone.

How it maps to ATT&CK

TECHNIQUE	WHAT NSS SAW
T1583.001 Acquire Infrastructure: Domains	54 names bought 27 October to 16 November 2026, in bursts, 48 at one registrar and the last two at a second
T1583.003 Acquire Infrastructure: Virtual Private Server	13 rented servers shared across brands
T1608.005 Stage Capabilities: Link Target	Names that show an empty page at the root, and one picture-puzzle gate
T1656 Impersonation	Ten banks, five credit unions, one fintech and two mobile carriers

What a defender can look for

In order of priority:

1. Block all 54 names in the files: the 48 of the measured set and the six the 18 November re-check added. They carry a bank word, a brand or a set of initials in the name and have no other use. Block on the evidence that ties them; a per-name band rates what a page shows, and these show nothing without the link.

2. Banks, credit unions and carriers: alert on DNS look-ups that match `^[0-9]{3,5}-?([a-z]+-?){0,3}(auth-?gateway|acceweb-?auth|access-?auth|auth-?access|member-?auth|identity-?verif)` on any ending. Anchored to the leftmost label, so strip any www. first. Use it case-insensitive. It matches all 35 numbered names in this paper's files, including the one bought on 16 November, and none of the other 19. Alert, do not block: it can match an ordinary name.
3. Add the newer shape, and read it as a warning rather than a finished pattern: `^[a-z]{2,6}-?fraud-?(prevention|prevent|alert|centre|center|protection)$` on the leftmost label, case-insensitive, matches the two names of 16 November and nothing else in this paper. It rests on two names only, and it will also match genuine domains a bank owns, so allowlist your own names first and alert, never block.
4. Watch, do not block, the 13 pool addresses (in the JSON file's watch section) for new names: the generator keeps buying, and the next name for your brand is likely to land on one of them. Five of the six names added on 16 November landed on addresses already in that list.
5. Watch the DNS service for the shape: new names on the same pair of name servers that fit either pattern are most likely this generator. NSS tracks it and will update this paper when it grows.
6. Fraud and brand-protection teams, not only security: the box above is written for you, because the controls that work on this set are a take-down request and a customer-facing message, not a firewall rule.
7. Brand owners: the message path is where the page is. If a customer forwards a text or e-mail with one of these names, the full link is the evidence that unlocks the page; keep it, and pass it to whoever handles your take-downs with the time it arrived.

All indicators are in the list below, and each one opens as a casefile in NSS Investigate.

The NSS tools used

> Investigate
Read the casefile of every name and of every pool address, with the stored captures in its Sightline card.

> Scan
Re-read every indicator on 16 November so that Investigate and Scan agree.

> Sightline
Captured a sample of the names on 16 November: empty pages at the root.

> Tools
Chained two reads of NSS's own records over one name: its addresses, then every name seen on them.

> Family finder
Widened one numbered name to every registered name of its shape.

> Discovery
Recorded the 48 names, and then the six more of 16 November, from NSS's own sensors.

> Watch
Keeps the names and the pool addresses under passive re-check, which is what the 18 November reading came out of (a Full feature).

Indicators

The first 25 of 54 indicators. Each is written defanged so it cannot be opened by accident. TLP:CLEAR. Use them in your own tools; no account needed.

INDICATOR	TYPE	NOTE
loginfreedommobile[.]digital	Domain	Imitates Freedom Mobile (read from the name). Shape verification or bank word, number at the end or none. Registered 2026-11-16 16:58 UTC, at the same registrar as the rest of the set. Not in the set measured to 16 Nov 2026; resolves on

		185[.]112[.]59[.]33, same name-server pair; no page answered the read (18 Nov 2026); on the same address as loginfreedommobile[.]com.
96408-wells-acceweb-auth[.]creditcard	Domain	Imitates Wells Fargo (read from the name). Shape <number>-<brand>-acceweb-auth. Registered 2026-11-16 06:37 UTC, at the same registrar as the rest of the set. Not in the set measured to 16 Nov 2026; resolves on 138[.]124[.]79[.]185, same name-server pair; answers with an empty page at the root (18 Nov 2026, 00:24 UTC).
4581-chime-access-auth[.]icu	Domain	Imitates Chime (read from the name). Shape <number>-[<brand>-]access-auth. Registered 2026-11-14 22:11 UTC. Answers with an empty page at the root (16 Nov 2026). On 18 Nov 2026 it resolves on 138[.]124[.]79[.]185, same name-server pair.
51954-robins-member-auth[.]icu	Domain	Imitates Robins (credit union) (read from the name). Shape <number>-[<brand>-]access-auth. Registered 2026-11-14 22:09 UTC. Answers with an empty page at the root (16 Nov 2026). On 18 Nov 2026 it resolves on

		153[.]80[.]249[.]234, same name-server pair.
46208-capone-auth-gateway[.]icu	Domain	Imitates Capital One (read from the name). Shape <number>-[<brand>-]auth-gateway. Registered 2026-11-14 22:06 UTC. Answers with an empty page at the root (16 Nov 2026). On 18 Nov 2026 it resolves on 153[.]80[.]249[.]5, same name-server pair.
4856-bmo-auth-gateway[.]icu	Domain	Imitates BMO (read from the name). Shape <number>-[<brand>-]auth-gateway. Registered 2026-11-14 22:02 UTC. Answers with an empty page at the root (16 Nov 2026). On 18 Nov 2026 it resolves on 147[.]45[.]61[.]154, same name-server pair.
319-fifth-third-identity-verif[.]icu	Domain	Imitates Fifth Third Bank (read from the name). Shape <number>-[<brand>-]identity-verif. Registered 2026-11-14 22:00 UTC. Answers with an empty page at the root (16 Nov 2026). On 18 Nov 2026 it no longer resolves; the registry record carries a registry-level hold and the name is still registered.
19251-vz-auth-access[.]icu	Domain	Imitates Verizon (read from the name). Shape <number>-[<brand>-]access-auth. Registered 2026-11-12

		23:03 UTC. Answers with an empty page at the root (16 Nov 2026). On 18 Nov 2026 it resolves on 153[.]80[.]249[.]5, same name-server pair.
`loginfreedommobile[.]com`	Domain	Imitates Freedom Mobile (read from the name). Shape verification or bank word, number at the end or none. Registered 2026-11-11 17:30 UTC. No page answered the capture (16 Nov 2026). On 18 Nov 2026 it resolves on 185[.]112[.]59[.]33, same name-server pair.
`wellsfargosecure[.]support`	Domain	Imitates Wells Fargo (read from the name). Shape verification or bank word, number at the end or none. Registered 2026-11-10 22:05 UTC. Answers with an empty page at the root (16 Nov 2026). On 18 Nov 2026 it resolves on 153[.]80[.]249[.]234, same name-server pair.
`3992-pncacceweb-authent[.]net`	Domain	Imitates PNC (read from the name). Shape <number>-<brand>-acceweb-auth. Registered 2026-11-10 21:44 UTC. Answers with an empty page at the root (16 Nov 2026). On 18 Nov 2026 it resolves on 94[.]26[.]106[.]184, same name-server pair.

94709-citi-auth-gateway[.]credit	Domain	Imitates Citi (read from the name). Shape <number>-[<brand>-]auth-gateway. Registered 2026-11-10 19:10 UTC. Did not answer the capture (16 Nov 2026). On 18 Nov 2026 it resolves on 176[.]65[.]132[.]54, same name-server pair.
nymcuverify[.]support	Domain	Imitates NYMCU (credit union) (read from the name). Shape verification or bank word, number at the end or none. Registered 2026-11-10 18:34 UTC. Answers with an empty page at the root (16 Nov 2026). On 18 Nov 2026 it resolves on 138[.]124[.]79[.]185, same name-server pair.
wellsfargo-risk-management[.]com	Domain	Imitates Wells Fargo (read from the name). Shape verification or bank word, number at the end or none. Registered 2026-11-10 18:19 UTC. Answers with an empty page at the root (16 Nov 2026). On 18 Nov 2026 it resolves on 153[.]80[.]249[.]234, same name-server pair.
1404-bcb-acceweb-auth[.]live	Domain	Imitates BCB (bank) (read from the name). Shape <number>-<brand>-acceweb-auth. Registered 2026-11-10 17:08 UTC. Answers with an empty page at the root

		(16 Nov 2026). On 18 Nov 2026 it resolves on 153[.]80[.]249[.]5, same name-server pair.
1954-regionsmember-auth[.]credit	Domain	Imitates Regions Bank (read from the name). Shape <number>-[<brand>-]access-auth. Registered 2026-11-10 16:13 UTC. Did not answer the capture (16 Nov 2026). On 18 Nov 2026 it resolves on 147[.]45[.]61[.]183, same name-server pair.
24952usbankidentityverif[.]credit	Domain	Imitates U.S. Bank (read from the name). Shape <number>-[<brand>-]identity-verif. Registered 2026-11-10 05:31 UTC. Answers with an empty page at the root (16 Nov 2026). On 18 Nov 2026 it resolves on 94[.]26[.]106[.]184, same name-server pair.
9353-safe-acceweb-auth[.]info	Domain	Imitates SAFE (credit union) (read from the name). Shape <number>-<brand>-acceweb-auth. Registered 2026-11-08 21:34 UTC. Shows a page titled Loading and nothing else (16 Nov 2026). On 18 Nov 2026 it resolves on 94[.]103[.]1[.]244, same name-server pair.
42708-fifth-third-auth-gateway[.]icu	Domain	Imitates Fifth Third Bank (read from the name). Shape <number>-[<brand>-]auth-gateway.

		Registered 2026-11-05 21:36 UTC. Answers with an empty page at the root (16 Nov 2026). On 18 Nov 2026 it resolves on 153[.]80[.]249[.]234, same name-server pair.
87134-orrstown-acceweb-auth[.]site	Domain	Imitates Orrstown Bank (read from the name). Shape <number>-<brand>-acceweb-auth. Registered 2026-11-05 16:30 UTC. Answers with an empty page at the root (16 Nov 2026). On 18 Nov 2026 it resolves on 138[.]124[.]79[.]185, same name-server pair.
7008-grow-acceweb-auth[.]xyz	Domain	Imitates Grow Financial (credit union) (read from the name). Shape <number>-<brand>-acceweb-auth. Registered 2026-11-04 00:36 UTC. Redirects from its root to a picture puzzle in front of an e-mail sign-in step (16 Nov 2026). On 18 Nov 2026 it resolves on 168[.]113[.]215[.]244, same name-server pair.

21198-great-lakes-acceweb-auth[.]info	Domain	Imitates Great Lakes (credit union) (read from the name). Shape <number>-<brand>-acceweb-auth. Registered 2026-10-30 21:35 UTC. Resolves, page not captured. On 18 Nov 2026 it resolves on 138[.]124[.]79[.]163, same name-server pair.
8228-great-lakes-acceweb-auth[.]info	Domain	Imitates Great Lakes (credit union) (read from the name). Shape <number>-<brand>-acceweb-auth. Registered 2026-10-30 21:19 UTC. Answers with an empty page at the root (16 Nov 2026). On 18 Nov 2026 it resolves on 147[.]45[.]61[.]154, same name-server pair.
selfverify[.]top	Domain	Generic verification name. Shape verification or bank word, number at the end or none. Registered 2026-10-27 17:37 UTC. Resolves, page not captured. On 18 Nov 2026 it resolves on 176[.]65[.]132[.]54, same name-server pair.
member-identity-verification6645[.]xyz	Domain	Generic verification name. Shape verification or bank word, number at the end or none. Registered 2026-10-27 17:38 UTC. Resolves, page not captured. On 18 Nov 2026 it resolves on

176[.]65[.]132[.]55, same name-server pair.

ALL 54 INDICATORS: CSV JSON also on GitHub No sign-up.

Check an indicator from this paper

How we know

What this rests on

- The 48 names are every name of this generator that NSS's records held on its DNS service from 27 October to 16 November 2026, read on 16 November 2026; the shape check covers every name of the numbered shape NSS saw appear from 15 October to 15 November, and a fresh name-server lookup on 16 November for the one bought that day. The 18 November re-check found six more, all bought on 16 November and in NSS's records on 16 and 17 November, after that count closed. They are in the files, bringing them to 54 rows, and in "What changed by 18 November"; the number 48 is used throughout for the set as measured.
- Registration times and registrars are public registration records read by NSS on 16 November 2026. Certificate times are the public certificate logs' own times.
- The addresses are fresh DNS answers of 16 November 2026, 13:39 UTC (14:54 UTC for 11408-auth-access[.]icu).
- The listing state was checked on 16 November 2026 against every list NSS takes in, for the names, any web address on them and the 13 addresses.
- Every page described here is an NSS capture of 16 November 2026, 04:52 to 05:02 UTC and 15:24 to 15:34 UTC. NSS solved no puzzle and typed nothing into any form.
- Every verdict in this paper was read on Investigate and then on Scan on 16 November 2026, and both gave the same band on every indicator;

the list rests on the generator evidence, not on the bands (see the limits).

- The 18 November 2026 re-check is public infrastructure only. The address and the name servers of all 48 names came from one public resolver at 00:03 to 00:04 UTC; the public registry record of every one of the 48 was read at 00:05 to 00:15 UTC, and that is where the hold states in this paper come from. The listing state was re-read on the same day for the 48 names, the six later names and the 13 addresses. A reader with no access to NSS can repeat all of it.
- The six names of 16 November are in NSS's own records on the same name-server pair as the rest; their public registry records were read on 18 November 2026 at 00:14 to 00:16 UTC and their addresses and name servers at 00:27 UTC. Six pages were read again on 18 November between 00:14 and 00:25 UTC, three of the 48 and three of the six; two further names returned no page and one was not read. All six later names were read on Investigate and on Scan, which agreed on each.
- The server banners described in this paper are read back from the pages NSS already held from 16 November and from the pages read again on 18 November, which together cover eight of the 13 addresses. They are what each server sent in its first answer; how the pages were read is not described.

What we cannot say

- The pages are unread: 15 of the 21 names NSS tried answered with an empty page at the root, consistent with content served only on the full link from the message. What each name targets is read from the name.
- "On no threat list NSS takes in" is not "on no threat list anywhere". All 48 names were under three weeks old at the first check and under four at the second.
- The 23 other names on the same DNS service are company and random names with no bank theme; NSS does not tie them to this generator.
- NSS's own verdicts lag this paper's evidence: 41 of the 48 names read Clean and five Low risk on 16 November, and of the six later names four

read Low risk and two Clean on 18 November, most likely because their pages are hidden behind the message link. The indicator list rests on the generator evidence, and the files carry no bands.

- "One generator" is a grouping in NSS's own records, not an operator identity. It rests on infrastructure and buying behaviour: one name-server pair carrying the whole numbered shape and nothing else of it, one pool of servers shared across brands, names bought in bursts, and certificates logged seconds apart. The servers' own answers point the same way but add nothing hard, because the two web-server banners NSS read are among the most common on the web. No person, company or group is identified, and no actor is named.
- The 18 November re-check is narrower than the 16 November reading behind the rest of the paper. It is public DNS and public registry records for every name, one re-reading of the listing state, and six pages read again; the 13 addresses were not re-read as casefiles, and nothing here says what any name serves beyond those six pages. A name that stopped resolving is on hold, not gone, and a hold can be lifted.
- NSS has no victim data of any kind for this set: no count of people who received a message, no count who opened a link, no account takeover and no sum of money. Nothing in this paper should be read as a loss figure or as evidence that any customer of any named institution was harmed.
- The initials in bcufraud-prevention[.]org and vacufraud-prevention[.]org are not matched to an institution. NSS treats initials as weaker than a spelled-out brand and does not guess, so the two names are reported by their shape.
- 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), "Numbered bank "auth gateways": one
generator, 18 brands, an empty page for anyone without the link", NSS-
BK-01, 18 Nov 2026. https://nsshq.com/research/numbered-bank-auth-
gateways
```

See something wrong? corrections@nsshq.com

More from NSS Research

NSS-GB-01: Polish official and e-banking lookalike domains aimed at PKO business-banking users: technical analysis

NSS-OC-01: Linked hosting clusters and the purchase batches behind them: technical analysis

NSS-GR-01: A name generator behind 294 Aldi and Lidl look-alike .shop names: technical analysis

---

NSS is not affiliated with any bank, credit union, fintech or mobile carrier named or implied by the names in this paper, or with any registrar, hosting company, DNS service or network behind them. Every institution named here is named because a domain name imitates it, and each one is the target of that imitation, not a party to it: nothing in this paper says any of them knew of, took part in, or is in any way responsible for the activity described, and none of these names is operated by them. NSS has no evidence of any customer loss at any of them and makes no such claim.