

Expanded by NSS

104 names on six servers from NSS's own resolution record, 62 first recorded by NSS's own sensors; the first server's names and the name shape were on public lists first

One wallet-phishing operator, six servers in three weeks: followed by the names it carried host to host

Twenty-four names moved with one wallet-phishing operation across six servers between 27 October and 14 November 2026, the stretch NSS's own resolution record covers; six of them went the whole way from the first server NSS recorded to the sixth, the server behind NSS-TK-01, the fake imToken download sites. Twenty-two of the moved names sat behind the operation's forwarding layer, each keeping its own label while the address behind it changed. The operation's oldest names were bought in July and on lists from August. Of the 104 names NSS saw on the six servers, 34 were on a threat list NSS takes in on 14 November; the 43 names that first appeared on the current server were on none.

PUBLISHED	LAST UPDATED	READING TIME	MARKING
14 Nov 2026	14 Nov 2026	21 min	TLP:CLEAR

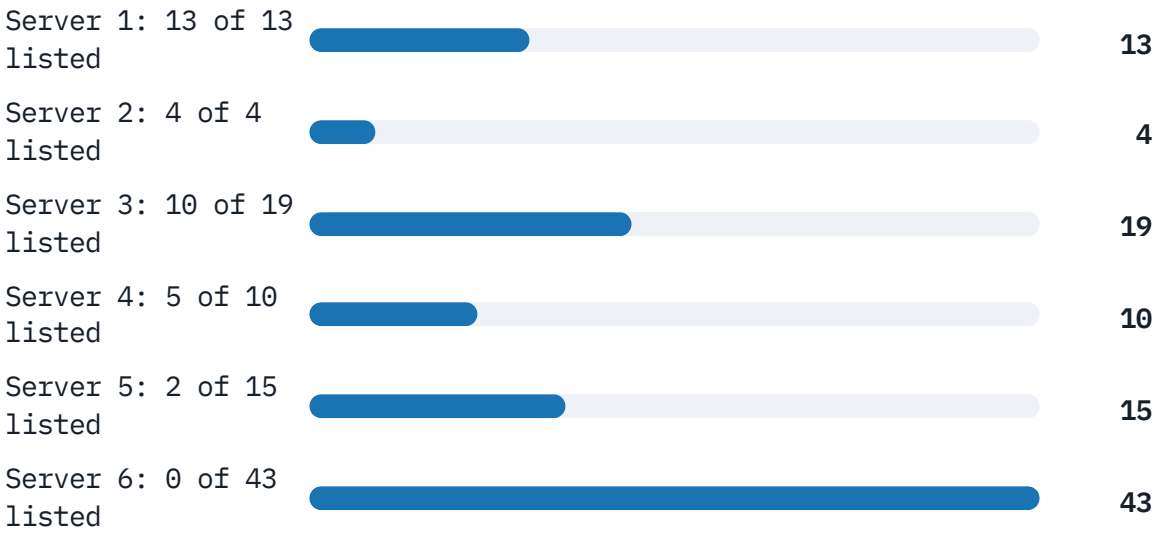
24
names that moved from an earlier server to a later one; six went the whole way from the first to the sixth

6
servers used by one operation between 27 October and 14 November 2026, in NSS's record

104
names NSS saw on the six servers; 62 first recorded by NSS's own sensors

0 of 43
names new on the current server that were on a threat list NSS takes in on 14 November; 41 of them were registered 8 to 13 November

NAMES NEW TO THE CHAIN AT EACH SERVER, AND HOW MANY A LIST CARRIED ON 14 NOVEMBER



A name is new at the first server NSS saw it on. The bar is the count of new names; the label gives how many of them were on a threat list NSS takes in on 14 November 2026. Server dates are in the table under The chain.

Key findings

1. One operation, six servers. NSS's own resolution record shows the same names resolving to six addresses between 27 October and 14 November 2026: 94.26.106[.]72 (27 to 31 October), then 103.38.82[.]152, 103.38.82[.]202, 156.225.24[.]233 and 156.225.24[.]119 side by side

(1 to 10 November), then 82.158.231[.]42, the server of the NSS-TK-01 paper, from 11 November. 104 names in all: 103 registered names and one forwarding label.

2. Twenty-four names moved. Each was seen on two or more of the six servers, in date order. Six went the whole way: telegramorg-cn[.]co, telegramorg-cn[.]com, mtoken-im[.]cv and three telergam-cdn names under aa9977rt[.]com went from the first server on 31 October to a middle server on 6 November (the third, fifth, second or fourth) and to the sixth on 12 November. Four more went from the first server to a middle one; seven relay-shaped wallet names and one Telegram look-alike moved among the middle servers between 1 and 8 November; six went from a middle server to the sixth on 12 November. Wallet, Telegram and mtoken names moved on the same days to the same servers.

3. Twenty-two of the 24 moved behind the forwarding layer. Each of them kept one label under the forwarding apex while the address behind it changed: telegramorg-cn[.]co pointed at its label under ikunzf[.]online from 31 October to 12 November while it resolved to the first, the third and then the sixth server. Whoever runs the forwarding chose every server for those names. The other two, mtoken[.]online and mtoken[.]download, have no forwarding record; their own records changed.

4. The forwarding apexes look like the operator's own. ikunzf[.]online (bought 1 December 2025), yumsihjkk[.]cc and shenswdns[.]cc (bought ten minutes apart on 11 November 2026 at 04:47 and 04:57 UTC) sit at one registrar and use the same two hosted name servers. In NSS's record nothing resolves under them but this operation's names and four fake-software download names. Under five hours after yumsihjkk[.]cc was bought, ten relay-shaped names were bought behind it, and on 12 November the three telergam-cdn names were re-pointed to the same label, atzuqs2x, under the new apex.

5. What the lists carried, and when. Of the 104 names, 34 were on a threat list NSS takes in on 14 November 2026. Thirty of the 34 were on a list

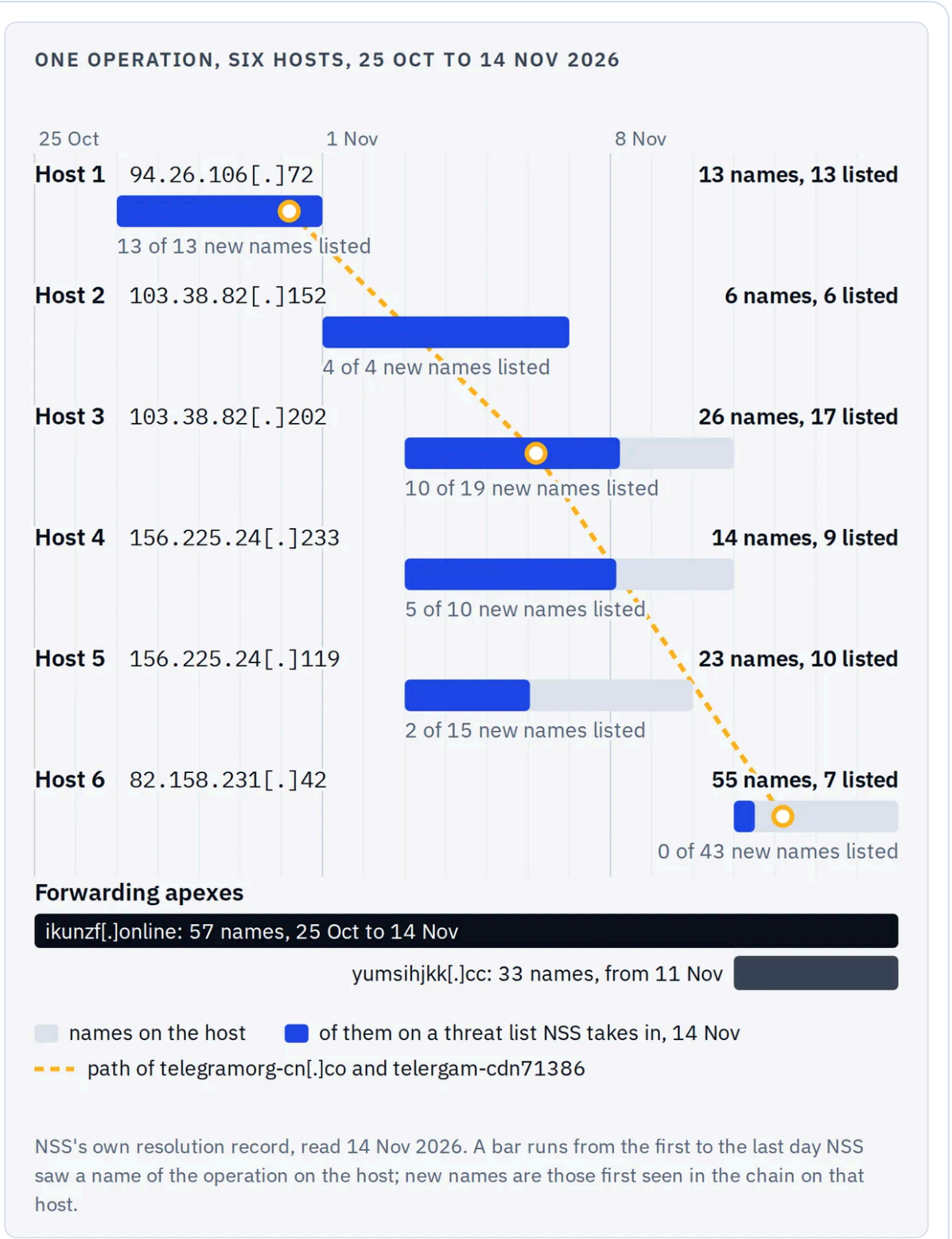
on or before the day NSS first saw them on a server of the chain; four were listed one to three days after. The names new to the chain at each server were listed 13 of 13, 4 of 4, 10 of 19, 5 of 10, 2 of 15 and 0 of 43. The 7 listed names on the current server are the six that went the whole way and one moved name.

6. The operation is older than NSS's record of it. The carried names were bought between 13 July and 10 September 2026 at three registrars other than the one that holds the rest, and were on lists from 2 August; the first server's address has been on a list since 6 July. All 13 names of the first server entered NSS's record from lists. From the third server on, NSS's own sensors recorded most new names first, from new registrations and certificate logs: 13 of 19 on the third server, 5 of 10 on the fourth, 7 of 15 on the fifth and 37 of 43 on the sixth; 62 of the 104 in all, 58 of them on no list on 14 November.

7. The forwarding layer also fronted fake-software downloads. Three names that threat lists carry as malware-download hosts, download[.]google-chrome[.]cyou (list date 15 March 2026), download[.]tfyxzai[.]com (6 August) and download-sougou[.]com[.]cn (31 August), pointed at labels under ikunzf[.]online when NSS first resolved them, between 25 October and 1 November; a fourth, app[.]app-lestalk[.]com[.]cn, joined on 10 November. On 26 and 27 October one address, 93.152.221[.]188, answered for download-sougou[.]com[.]cn and a relay-shaped wallet name together. They did not move with the chain, and the paper does not attribute them to the operator.

8. Host types and verdicts. NSS classes the four later servers as dedicated hosts: every name NSS saw on them fits this forwarding set, though NSS cannot rule out other customers of the forwarding. Investigate and Scan agree on all 116 indicators in this paper: High risk for the four later servers, the two labels, 102 of the 103 names and three of the four download names; Suspicious for the first two servers, the apex yumsihjkk[.]cc, one name and one download name. The older apex ikunzf[.]online reads Clean on both surfaces because its labels no

longer resolve to an address; it is named in the body and left out of the indicator list.

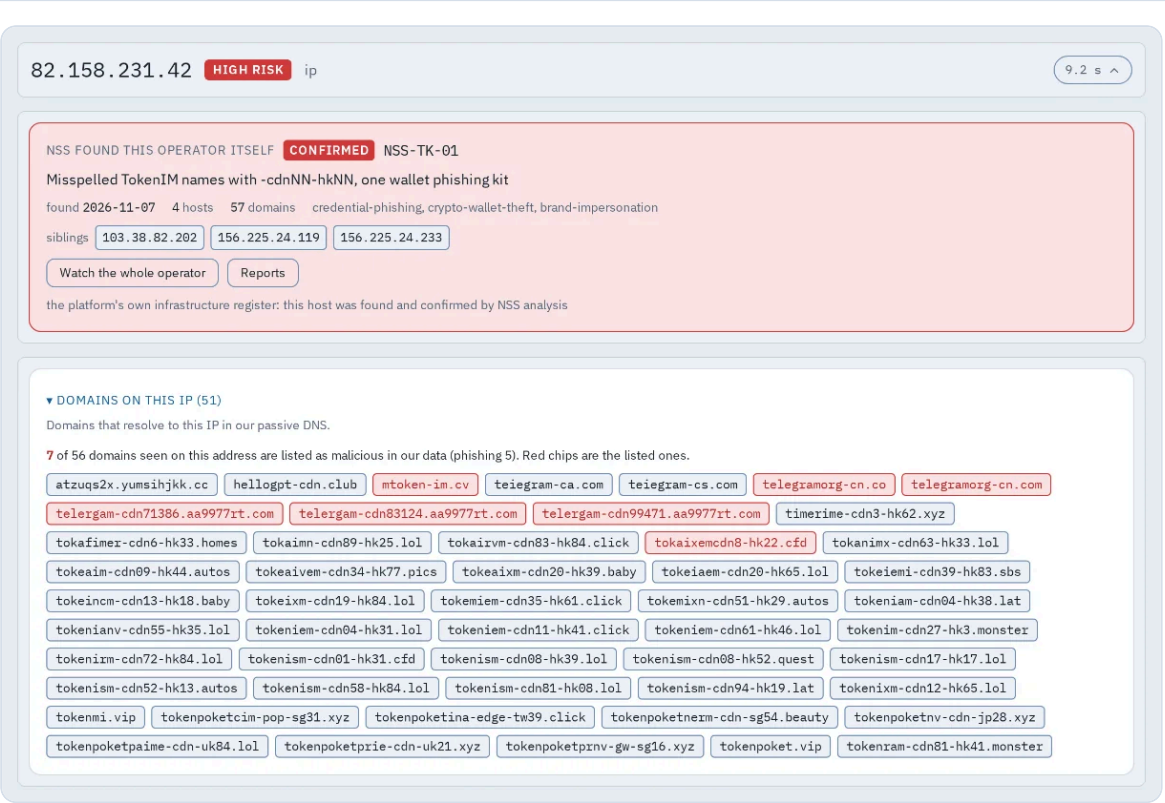


The chain, from NSS's own resolution record, read 14 November 2026. The darker part of each bar is the share of that host's names that a threat list NSS takes in carried on 14 November. Hosts 2 to 5 ran side by side; the names that first appeared on each later host were increasingly on no list, and on the current host none of the 43 new names was.

How an analyst finds this with NSS

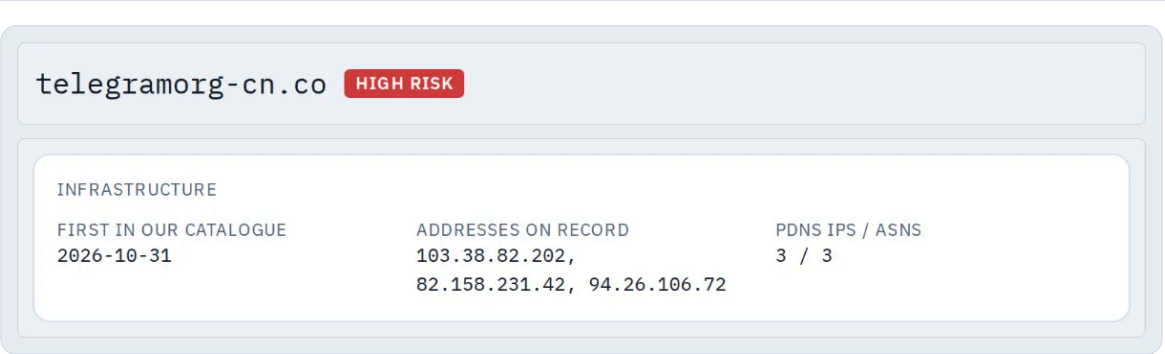
The same case, worked the way a defender works it in NSS: from the current server back to the first server in NSS's record, then forward to the thing to watch. Every picture is the real Station on 14 November 2026, cropped to the panel in use.

01 Start from the server in the NSS-TK-01 paper. Investigate rates it High risk, shows NSS's register entry for the operator with its sibling servers, and lists the names seen on it; the red chips are the seven a threat list carries.



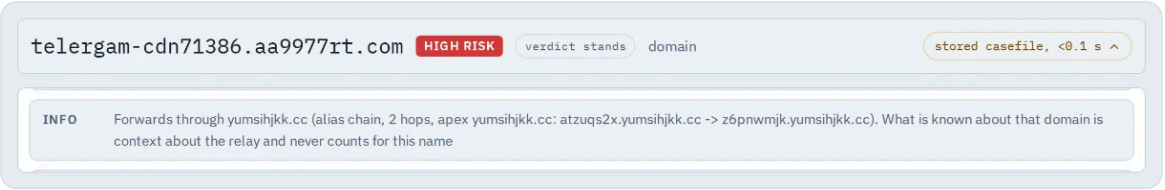
Investigate, 14 November 2026. The register card covers the current server set, which NSS recorded itself from 7 November; the earlier servers in this paper reached NSS from public lists first, so the paper is marked Expanded by NSS, not Found by NSS. The panel counts 56 names on the address: the operation's 55 (one of them the label z6pnwmjk) and the label atzuqs2x; the grid shows 51 of them.

02 Open one of the red chips on Scan. telegramorg-cn[.]co has been in NSS's catalogue since 31 October and has three addresses on record: the first server, a middle one and the current one. That is a name moving host to host.



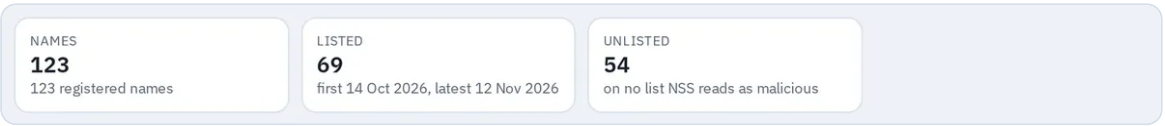
Scan, 14 November 2026: three addresses on record for one name, and the first of them is the first server in NSS's record. Network and registrar rows are left out of the shot.

03 Open a forwarded name. Its casefile shows the alias chain: the name points at its own label, atzuqs2x, under the forwarding apex, and on 14 November that label pointed at a shared host label that gave the address. The three telergam-cdn names were re-pointed to the same label under the new apex on 12 November, a day after it was bought.



Investigate, 14 November 2026: the two-hop alias chain. The same label sat under ikunzf[.]online from 31 October to 6 November and under yumsihjkk[.]cc from 12 November. The labels are what to watch.

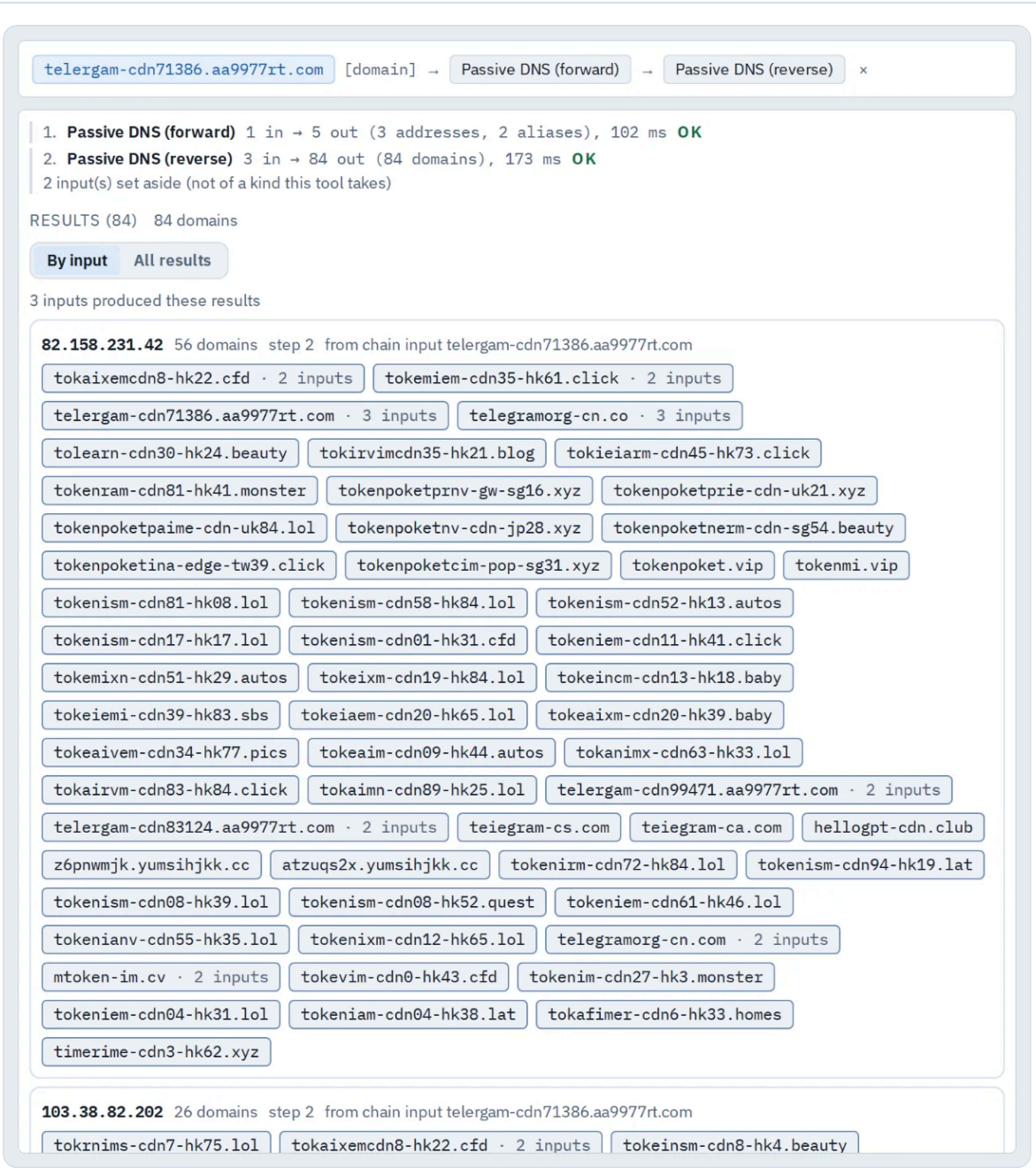
04 Widen one relay-shaped name to its family. The family finder returns every registered name of the same shape, with how many a list carries.



Family finder, 14 November 2026: 123 registered names of the shape, 69 on a threat list, the first on 14 October. The paper counts less: the 87 relay-shaped names among the 104 NSS saw on the six servers; the finder also counts names of the shape NSS holds only from lists or zone files.

05 Run a tool chain on the forwarded name: the addresses and aliases NSS has on record for it, then every name NSS has seen on those

addresses. Two steps give the three servers it sat on and the 84 names that shared them.



The chain run on 14 November 2026. A name marked "3 inputs" came back from all three servers: it is a name that moved the whole way with this one. The results are cropped to the current server's block; the two other servers' blocks follow it in the same form.

06 Then act: watch the server, watch the whole operator from the register card, share the casefile, or download it as JSON or CSV for your own tools (Full features).



The casefile's actions, 14 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, 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=$(jq -r '.indicators[0].value' nss-tl-01.json)   # the first indicato
curl -s "https://nsshq.com/api/v1/check?value=$NAME"
```

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

The answer for yumsihjkk[.]cc on 14 November 2026


```
{
  "as_of": "2026-11-14T20:41:48Z",
  "band": "Suspicious",
  "band_is_host_class": false,
  "found": true,
  "host_class": {
    "class": "unknown",
    "label": "Host type unknown",
    "sentence": "No address on record for this name."
  },
  "known_good": false,
  "names": null,
  "public_listing": { "state": "not_checked", (...) },
```

```
  "reports": 0,
  "type": "domain",
  "value": "yumsihjkk[.]cc",
  "view": "public"
}
```

The real public answer for the forwarding apex, read on 14 November 2026 at 21:27 UTC (the verdict itself dated 20:41 UTC). Here the value is defanged and the public-listing block shortened. The apex reads Suspicious with no address of its own: the addresses sit on the labels under it, which read High risk. 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-tl-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-tl-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. For this operator the records that matter most are the labels under the forwarding apex: a new server appears as a changed label answer.

Every morning, with a mail when a verdict changes

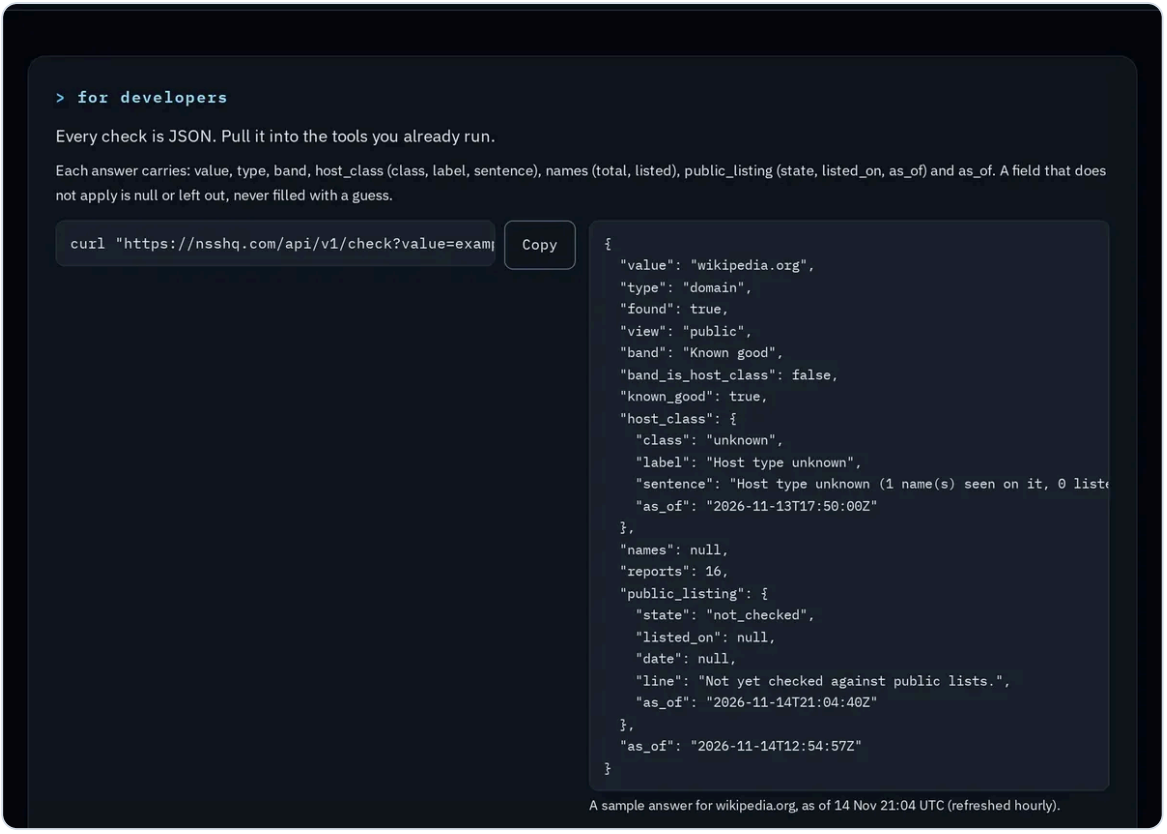
```
0 6 * * * cd /opt/nss && python3 nss_check_file.py nss-tl-01.json >> check
```

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.

At the DNS layer the cheapest control is the forwarding apex: block yumsihjkk[.]cc and any name that resolves through it. Any server the operator wires behind that apex is covered by the same block; names on the old apex or with no forwarding record need the address block too.



The public Developers page on nsshq.com, 14 November 2026: the request, the fields every answer carries and a live answer.

Timeline

1 Dec 2025
ikunzf[.]online is registered. It becomes the first forwarding apex.

15 Mar 2026
download[.]google-chrome[.]cyou, a fake-software download name that will later sit under the apex, is listed as a malware-download host.

6 Jul 2026
94.26.106[.]72, later the first server in NSS's record, is on a list.

13 Jul to 10 Sep 2026
The names the operation will carry from server to server are bought at three registrars: telegramorg-cn[.]com, telegramorg-cn[.]co, mtoken-im[.]cv, then the two mtoken names. They are on lists from 2 August.

6 and 31 Aug 2026

Two more download names, download[.]tfyxzai[.]com and download-sougou[.]com[.]cn, are listed as malware-download hosts.

14 Oct

The first relay-shaped wallet name of the family is listed.

25 to 27 Oct

NSS first resolves names forwarded through ikunzf[.]online, from public lists: eight relay-shaped wallet names and one other name on two addresses, and three download names under labels of the apex.

27 Oct

The first name of the chain, tokevim-cdn32-hk61[.]lol, resolves to 94.26.106[.]72 and is listed the same day.

31 Oct

Twelve more names arrive on the first server: wallet, Telegram and mtoken names together, among them the three telergam-cdn names on the atzuqs2x label. Ten of them were on lists since August or September; two are listed that day.

1 to 3 Nov

The operation spreads over four servers in two networks. Names already on lists since 18 to 22 October join them.

6 to 8 Nov

The carried names move to the middle servers, keeping their labels; wallet names move among the four. NSS's own sensors start recording the new names first.

10 Nov

Last day a name of the operation is seen on any of the middle servers.

11 Nov, 04:47 and 04:57 UTC

yumsihjkk[.]cc and shenswdns[.]cc are bought ten minutes apart at the apex's registrar. Ten names are bought behind yumsihjkk[.]cc at 09:39 UTC, and the first names appear on 82.158.231[.]42, the sixth server, the same day.

12 Nov

The three telergam-cdn names are re-pointed to atzuqs2x under yumsihjkk[.]cc. The carried names resolve to the sixth server; eleven names on it still use their ikunzf[.]online labels.

13 Nov

NSS publishes NSS-TK-01 on the sixth server's fake imToken sites and app.

14 Nov

NSS reads the chain back from its own records: 104 names, six servers, 24 moved names, 34 listed.

The chain

NSS keeps a record of every name it resolves and the address it resolved to, with the first and last day. Reading that record for the server of the NSS-TK-01 paper, then for every name on it, then for every address those names had resolved to before, gives six addresses that share names. Nothing in this paper comes from anywhere else.

SERVER	ADDRESS	NAMES SEEN	NAMES ON A LIST, 14 NOV	NEW TO THE CHAIN HERE
1	94.26.106[.]72	13 (27 to 31 Oct)	13	13
2	103.38.82[.]152	6 (1 to 6 Nov)	6	4
3	103.38.82[.]202	26 (3 to 10 Nov)	17	19
4	156.225.24[.]233	14 (3 to 10 Nov)	9	10
5	156.225.24[.]119	23 (3 to 9 Nov)	10	15
6	82.158.231[.]42	55 (11 to 14 Nov)	7	43

The second to fifth servers overlapped in time, in two networks. The first server was used alone in NSS's record, and the sixth is used alone now. Of the 55 names on the sixth server, 32 are in the TK-01 paper's indicator list (31 of its names and the shared host label z6pnwmjk[.]yumsihjkk[.]cc, which is a forwarding label, not a bought name); the other 23 are the six names that moved there from the first server, two Telegram look-alikes, seven TokenPocket names that TK-01's counts did not include (bought from 13 November), and eight relay-shaped names that joined on 12 to 14 November. The TK-01 paper's own counts are unchanged.

The names that moved

Twenty-four of the 104 names were seen on two or more of the six servers, in date order. The six that went the whole way:

NAME	SERVER 1	MIDDLE SERVER, 6 NOV	SERVER 6
telegramorg-cn[.]co	31 Oct	3	12 Nov
telegramorg-cn[.]com	31 Oct	5	12 Nov
mtoken-im[.]cv	31 Oct	5	12 Nov
telergam-cdn71386.aa9977rt[.]com	31 Oct	3	12 to 13 Nov
telergam-cdn83124.aa9977rt[.]com	31 Oct	2	12 to 13 Nov
telergam-cdn99471.aa9977rt[.]com	31 Oct	4	12 to 13 Nov

The other eighteen: four went from the first server to a middle one (mtoken[.]online, mtoken[.]download, im-token-xjp-cdn[.]wiki, tokenim-cdn-sg[.]biz); seven relay-shaped wallet names and one Telegram look-alike, telegam-zh-cn[.]com, moved among the middle servers between 1

and 8 November (tokanim-cdn13-hk13[.]club was on servers 3 and 5 on 3 November, then on 4 on 8 November); and six went from a middle server to the sixth on 12 November (timerime-cdn3-hk62[.]xyz, tokemiem-cdn35-hk61[.]click, tokenim-cdn27-hk3[.]monster, tokaixemcdn8-hk22[.]cfd, tokafimer-cdn6-hk33[.]homes and tokenmi[.]vip). Nineteen of the 24 are on a list; the five that are not all went from a middle server to the sixth.

How the names moved matters. For 22 of the 24, the name's own record did not change: it kept one forwarding label, and the address behind the label changed. telegramorg-cn[.]co, telegramorg-cn[.]com and mtoken-im[.]cv each held their label under ikunzf[.]online (uzvn8r64, q54ae7mj and zwc9j6s4) from 31 October to 12 November while their address went from the first server to a middle one and then to the sixth. So whoever runs the forwarding chose every server for those names. For mtoken[.]online and mtoken[.]download, which have no forwarding record, the names' own records changed.

Wallet, Telegram and mtoken names moved on the same days to the same servers. The TK-01 paper left open whether the Telegram look-alikes on its server belonged to the same operator as the wallet pages or to another customer of the same forwarding. The movement narrows that question but does not close it. The three telergam-cdn names were re-pointed to the same label under the new apex a day after it was bought, which needs whoever holds those names to act together with whoever runs the forwarding. But the carried names were bought between July and September at three registrars other than the one behind the batch-bought names, which still fits several customers of one service.

The forwarding layer

Every forwarded name points at its own random eight-character label under an apex. On 14 November one forwarded name resolved through its label to a shared host label, z6pnwmjk, which gave the address (Investigate, walkthrough step 3). Where that holds, one record change moves every name behind the shared label. It did not always hold: from 3 to 10

November names under the same apex went to four servers at once, so that period used more than one host record.

When the operation added a new apex, it recreated labels under it:

LABEL	UNDER IKUNZF[.]ONLINE	UNDER YUMSIHJKK[.]CC	POINTS AT
atzuqs2x	31 Oct to 6 Nov	12 Nov	the three telergam-cdn names
z6pnwmjk	not in NSS's record	13 Nov (record), 14 Nov (fresh resolution)	82.158.231[.]42

The TK-01 paper recorded three more labels recreated the same way: fmr635hz and 2r36s5d9 under both apexes, and 9r2b8vj7 under ikunzf[.]online and shenswdns[.]cc. The old apex stayed in use alongside the new one: on 12 November eleven of the names on the sixth server still resolved through ikunzf[.]online labels, and NSS stored alias answers under it until 14 November. Of the 55 names on the sixth server, 33 resolved through yumsihjkk[.]cc in NSS's record, 11 through ikunzf[.]online and 11 have no stored alias answer.

NSS's stored alias answers hold at least 87 names under the two apexes, on 86 labels: 57 under ikunzf[.]online since 25 October and 33 under yumsihjkk[.]cc since 11 November. These are the answers NSS stored; the TK-01 paper, which followed its names through the forwarding as it resolved them, counted 33 of its 53 under ikunzf[.]online and 36 earlier names, not all of which were stored as alias answers.

The three apexes were bought at one registrar, which is not the registrar of the names, and all three use the same two hosted name servers. Under them NSS has recorded only this operation's names and the four download names below. That, the purchase of yumsihjkk[.]cc under five hours before the first batch of names behind it, and the labels recreated across apexes are why the paper reads the layer as the operator's own. If the download

names belong to other hands, the layer is a small service with more than one customer; the paper does not decide that.

ikunzf[.]online itself reads Clean on Investigate and Scan on 14 November: its labels no longer resolve to an address, and NSS judges a name by what it serves. It is named here as a fact about the operation's history and is not in the indicator list. yumsihjkk[.]cc reads Suspicious, and its labels and the current server read High risk; all of them are in the indicator list.

What the lists carried, and when

The operator's names reach threat lists. The question is which ones, and when relative to the move. A listing date here is the date the list gives, not the day NSS took the listing in.

MEASURE (THE 104 NAMES, LISTS NSS TAKES IN, CHECKED 14 NOV 2026)	RESULT
On a list	34
On a list on or before the day NSS first saw the name on a chain server	30 of 34 (23 before, 7 the same day)
Listed one to three days after that day	4 of 34
Listed names that moved from the first server to the current one	6 (all six that went the whole way)
Names first seen on the current server (11 to 14 Nov) that a list carried	0 of 43
Names NSS's own sensors recorded first (new registrations and certificate logs)	62 of 104, 58 of them on no list

The names a list knows are the names the operator bought weeks or months ago and keeps carrying along. The names it adds at each new server, bought in batches at one registrar a day or two before use, were not on a list while that server was in use. A defender who blocks the listed names blocks the operator's oldest assets; the forwarding apex, the labels and the relay shape cover the new ones.

"On no threat list NSS takes in" is not "on no threat list anywhere". Of the 43 new names on the current server, 41 have a registration record, all dated 8 to 13 November; one has none, and one is the shared host label.

Where the record starts, and the download names

NSS's record of the forwarding apex begins on 25 October, two days before the chain's first server, with names NSS resolved from public lists: eight relay-shaped wallet names forwarded through ikunzf[.]online and one other name, on two addresses that never held a moved name (111.92.242[.]95 and 149.88.95[.]146), and the download names. The operation itself is older: its carried names were bought from July and listed from August, before NSS resolved any of them.

Three of the download names are on threat lists as malware-download hosts from well before the chain: download[.]google-chrome[.]cyou (a fake Chrome download, list date 15 March 2026), download[.]tfyxzai[.]com (a fake ProtonVPN installer, 6 August) and download-sougou[.]com[.]cn (a fake Sogou browser installer, 31 August). When NSS first resolved them, on 25 October, 1 November and 26 October, each pointed at its own label under ikunzf[.]online, as the wallet names do. A fourth, app[.]app-lestalk[.]com[.]cn, joined on 10 November.

On 26 and 27 October one address, 93.152.221[.]188, answered for download-sougou[.]com[.]cn and for a relay-shaped wallet name, tokeimx-cdn22-hk22[.]sbs. That is a host-level tie between the download names and the wallet names, a day before the chain begins. It is one address for two days, and NSS reads it Low risk today, so it is a tie and not a verdict.

What NSS can say is that by late October one forwarding layer stood in front of fake-software downloads, wallet phishing and Telegram look-alikes at once. What it cannot say is when the download names first used the apex, or whether the same hands run them: its record of them starts on 25 October, their listings in March and August predate it, and they did not move with the chain.

Operator evidence, and where it stops

What the records prove:

- **Names moved between the six servers.** Twenty-four names, each seen on two or more of the servers in date order, six of them from the first server to the sixth; 22 of them on labels that stayed fixed while the address behind them changed. This is the tie that makes six addresses one operation; shared hosting alone would not.
- **Coordinated changes across names and forwarding.** The three telergam-cdn names were re-pointed to the same label under a new apex a day after that apex was bought, and labels were recreated across apexes.
- **One registrar for the batch-bought names.** 69 of the 74 registration records NSS read are at one registrar, bought in bursts of ten (TK-01); the other five are the carried names, at three other registrars. 50 of the 54 names in NSS's zone data use that registrar's default name servers, which on their own tie nothing.
- **Dedicated hosts.** The four later servers are classed dedicated by NSS: every name NSS saw on them fits this forwarding set.

What they do not prove:

- **Who the operator is.** No actor is named. NSS-TK-01 is NSS's register name for this operation, not a group.
- **That one party holds both the carried names and the batch-bought names.** The coordinated re-pointing argues for it; the different registrars and the earlier purchase dates fit several customers of one forwarding service as well.
- **That the download names belong to the same hands.** They share the forwarding layer and, for two days, an address with a wallet name. They did not move with the chain.

- **That the first two servers are still the operator's.** They hold no name of the operation after 31 October and 6 November, and NSS reads them Suspicious on what they served.
- **What was served on the earlier servers.** NSS holds captures of the current server's pages (the TK-01 paper) and none of the earlier servers' pages.

How it maps to ATT&CK

TECHNIQUE	WHAT NSS SAW
T1583.001 Acquire Infrastructure: Domains	103 names and three forwarding apexes, 1 Dec 2025 to 13 Nov 2026
T1583.004 Acquire Infrastructure: Server	Six servers in NSS's record over three weeks, four of them side by side
T1656 Impersonation	Wallet, Telegram and mtoken look-alike names

What a defender can look for

In order of priority:

1. Block, at DNS, yumsihjkk[.]cc and any name that resolves through it. That covers the 33 names NSS saw forwarded through it and any server the operator wires behind it later. The last move came with a new apex, so also watch new labels under shenswdns[.]cc (NSS reads it Clean today because nothing resolves through it; it was bought with yumsihjkk[.]cc), and block the current address (item 2) for the names that do not use the apex.
2. Block the four later addresses, 103.38.82[.]202, 156.225.24[.]233, 156.225.24[.]119 and 82.158.231[.]42, which NSS classes dedicated to this operation. Alert on the first two, 94.26.106[.]72 and 103.38.82[.]152, idle since 31 October and 6 November: they held

nothing else while in use, but NSS cannot say they are still the operator's.

3. Alert on DNS look-ups that match `^[a-z]{4,16}(-?(cdn|edge|pop|gw)[a-z0-9]*)+-(hk|sg|jp|uk|tw)[0-9]{0,2}\.` on .lol, .xyz, .autos, .click, .cfd, .homes, .pics, .beauty, .monster, .quest, .lat, .baby, .club, .sbs, .blog or .biz. It is anchored to the leftmost label, so strip any www. first. It matches all 87 relay-shaped names in this paper. Alert, do not block: it can match an ordinary name.
4. Alert on any name whose records point at an eight-character label under an apex that resolves to one of the six addresses. That is the operator's wiring, and it does not depend on the name's spelling.
5. Treat telegramorg-cn[.]co, telegramorg-cn[.]com, mtoken-im[.]cv and the telergam-cdn names as the operator's long-lived assets: they have been carried through three servers since 31 October.

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 the current server, of every moved name and of the forwarding labels; its alias-chain finding showed the two-hop forwarding and its register card the operator's sibling servers.

> Scan
Re-read every indicator on 14 November so that Investigate and Scan agree; its infrastructure panel listed the addresses on record for each moved name.

> Tools
Chained two reads of NSS's own records over a forwarded name: its addresses and aliases on record, then every name seen on those addresses.

> Family finder
Widened one relay-shaped name to the 123 registered names of its shape and their listing state.

> Register

> Discovery

Holds the four later servers under NSS-TK-01 and classes them dedicated.

Recorded 62 of the 104 names first, from new registrations and certificate logs; 58 of them were on no threat list on 14 November.

Indicators

The first 25 of 116 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
94[.]26[.]106[.]72	IP address	Host 1 of the chain: 13 names of the operator seen on it 27 Oct 2026 to 31 Oct 2026, 13 of them on a threat list NSS takes in on 14 Nov 2026; no name of the operation on it after 31 Oct 2026
103[.]38[.]82[.]152	IP address	Host 2 of the chain: 6 names of the operator seen on it 1 Nov 2026 to 6 Nov 2026, 6 of them on a threat list NSS takes in on 14 Nov 2026; no name of the operation on it after 6 Nov 2026
103[.]38[.]82[.]202	IP address	Host 3 of the chain: 26 names of the operator seen on it 3 Nov 2026 to 10 Nov 2026, 17 of them on a threat list NSS takes in on 14 Nov 2026; classed a dedicated host by NSS
156[.]225[.]24[.]233	IP address	Host 4 of the chain: 14 names of the operator seen on it 3 Nov 2026 to 10 Nov 2026, 9 of them on a threat list NSS takes in on 14 Nov

		2026; classed a dedicated host by NSS
156[.]225[.]24[.]119	IP address	Host 5 of the chain: 23 names of the operator seen on it 3 Nov 2026 to 9 Nov 2026, 10 of them on a threat list NSS takes in on 14 Nov 2026; classed a dedicated host by NSS
82[.]158[.]231[.]42	IP address	Host 6 of the chain: 55 names of the operator seen on it 11 Nov 2026 to 14 Nov 2026, 7 of them on a threat list NSS takes in on 14 Nov 2026; classed a dedicated host by NSS
atzuqs2x[.]yumsihjkk[.]cc	Domain	The constant forwarding label: the three telergam-cdn names point at it; the same label sat under ikunzf[.]online from 31 Oct to 6 Nov 2026 and under this apex from 12 Nov 2026; on no threat list NSS takes in
yumsihjkk[.]cc	Domain	Forwarding apex of the operator, registered 11 Nov 2026 04:47 UTC; 33 names forwarded through labels under it in NSS's record; on no threat list NSS takes in
z6pnwmjk[.]yumsihjkk[.]cc	Domain	The shared host label under the apex: on 14 Nov 2026 a forwarded name resolved through its own label to this one, which gave the current server, 82[.]158[.]231[.]42; on no threat list NSS takes in

im-token-xjp-cdn[.]wiki	Domain	Moved host to host: host 1 (31 Oct 2026), then host 5 (7 Nov 2026); forwarded through label xwsjqutn under ikunzf[.]online; on a threat list NSS takes in, list date 28 Sep 2026
mtoken-im[.]cv	Domain	Moved host to host: host 1 (31 Oct 2026), then host 5 (6 Nov 2026), then host 6 (12 Nov 2026); forwarded through label zwc9j6s4 under ikunzf[.]online; on a threat list NSS takes in, list date 2 Aug 2026
mtoken[.]download	Domain	Moved host to host: host 1 (31 Oct 2026), then host 5 (7 Nov 2026); on a threat list NSS takes in, list date 14 Sep 2026
mtoken[.]online	Domain	Moved host to host: host 1 (31 Oct 2026), then host 3 (7 Nov 2026); on a threat list NSS takes in, list date 14 Sep 2026
telegam-zh-cn[.]com	Domain	Moved host to host: host 2 (1 Nov 2026), then host 4 (7 Nov 2026); forwarded through label 6xd8fw3p under ikunzf[.]online; on a threat list NSS takes in, list date 4 Aug 2026
telegramorg-cn[.]co	Domain	Moved host to host: host 1 (31 Oct 2026), then host 3 (6 Nov 2026), then host 6 (12 Nov 2026); forwarded through label uzvn8r64 under ikunzf[.]online; on a threat list NSS takes in, list date 4 Aug 2026

telegramorg-cn[.]com	Domain	Moved host to host: host 1 (31 Oct 2026), then host 5 (6 Nov 2026), then host 6 (12 Nov 2026); forwarded through label q54ae7mj under ikunzf[.]online; on a threat list NSS takes in, list date 4 Aug 2026
telergam-cdn71386[.]aa9977rt[.]com	Domain	Moved host to host: host 1 (31 Oct 2026), then host 3 (6 Nov 2026), then host 6 (12 Nov 2026); forwarded through label atzuqs2x under ikunzf[.]online, then yumsihjkk[.]cc; on a threat list NSS takes in, list date 4 Aug 2026
telergam-cdn83124[.]aa9977rt[.]com	Domain	Moved host to host: host 1 (31 Oct 2026), then host 2 (6 Nov 2026), then host 6 (12 Nov 2026); forwarded through label atzuqs2x under ikunzf[.]online, then yumsihjkk[.]cc; on a threat list NSS takes in, list date 4 Aug 2026
telergam-cdn99471[.]aa9977rt[.]com	Domain	Moved host to host: host 1 (31 Oct 2026), then host 4 (6 Nov 2026), then host 6 (12 Nov 2026); forwarded through label atzuqs2x under ikunzf[.]online, then yumsihjkk[.]cc; on a threat list NSS takes in, list date 4 Aug 2026
timerime-cdn3-hk62[.]xyz	Domain	Moved host to host: host 4 (10 Nov 2026), then host 6 (12 Nov 2026); forwarded through label 59e8ragw under ikunzf[.]online; on

		no threat list NSS takes in (14 Nov 2026)
timerime-cdn3-hk73[.]quest	Domain	Moved host to host: host 3 (7 Nov 2026), then host 5 (8 Nov 2026); forwarded through label e4bqfth8 under ikunzf[.]online; on a threat list NSS takes in, list date 8 Nov 2026
tokafimer-cdn6-hk33[.]homes	Domain	Moved host to host: host 5 (9 Nov 2026), then host 6 (12 Nov 2026); forwarded through label bmrq8n59 under ikunzf[.]online; on no threat list NSS takes in (14 Nov 2026)
tokaixemcdn8-hk22[.]cfd	Domain	Moved host to host: host 3 (10 Nov 2026), then host 6 (12 Nov 2026); forwarded through label cgz593am under ikunzf[.]online; on a threat list NSS takes in, list date 11 Nov 2026
tokanim-cdn13-hk13[.]club	Domain	Moved host to host: host 5 (3 Nov 2026), then host 3 (3 Nov 2026), then host 4 (8 Nov 2026); forwarded through label 45gnmx6k under ikunzf[.]online; on a threat list NSS takes in, list date 18 Oct 2026
tokanim-cdn19-hk19[.]club	Domain	Moved host to host: host 2 (3 Nov 2026), then host 4 (3 Nov 2026), then host 5 (8 Nov 2026); forwarded through label pz43re72 under ikunzf[.]online; on a threat list NSS takes in, list date 18 Oct 2026

ALL 116 INDICATORS: CSV JSON STIX More formats on GitHub

No sign-up. Check an indicator from this paper

How we know

What this rests on

- Which name resolved to which server, and on which days, is NSS's own resolution record, read on 14 November 2026 at 20:36 UTC. A move is a name with records on two or more of the six servers whose first days are in order.
- The listing state was checked on 14 November 2026 at 20:36 UTC against every list NSS takes in. A listing of the name or of any web address on it counts. A listing date is the date the list gives for the indicator, not the day NSS took the listing in.
- The forwarding labels are the alias answers stored in the same resolution record. The label-to-label hop was read from a fresh resolution through Investigate on 14 November (atzuqs2x[.]yumsihjkk[.]cc to z6pnwmjk[.]yumsihjkk[.]cc to 82.158.231[.]42); it is not in the stored record.
- Registration dates and registrars are public registration records read by NSS on 13 and 14 November 2026; name-server pairs are from NSS's zone data.
- The host type of each server is as NSS classed it on 13 and 14 November 2026. Every verdict in this paper was read on Investigate (page stage skipped) and then on Scan on 14 November 2026 between 20:38 and 21:41 UTC; the indicator list holds only indicators on which both agree at Suspicious or higher.
- The sixth server's pages and app are described in NSS-TK-01, from NSS's captures and download of 12 and 13 November 2026; this paper adds no new capture.

What we cannot say

- NSS's certificate-log intake has been behind since 13 November 2026 01:33 UTC and was still catching up when this paper was read, so names that appeared only in certificate logs after that time may be missing from the counts. The resolution record, zone data and list store were current.
- The record starts where NSS's data starts, on 25 October. The operation is older: its carried names were bought from July. The first server's names, the earlier addresses of 25 to 27 October and the download names reached NSS from public lists; names the operator used before then, or on servers NSS never resolved a name to, are not counted.
- A move is read from first and last days in NSS's record, which depend on when NSS resolved each name; a name may have moved a day earlier or later than the record shows. Two records on the same day may be one name answering with several addresses, not a move.
- Hosts 2 to 5 overlapped, so the chain is not a strict sequence, and the paper does not claim a cadence of moves.
- The download names share the forwarding layer and, for two days, an address with a wallet name; they did not move with the chain, and the paper does not attribute them to the operator. The carried names and the batch-bought names may have different holders who share one forwarding service.
- "On no threat list NSS takes in" is not "on no threat list anywhere". The 43 names new on the current server were under a week old at the check.
- This paper is not attributed to any named group. NSS-TK-01 is NSS's register name for this operation, not a group.

Use and citation

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

```
Nexus Sentinel Station (NSS), "One wallet-phishing operator, six servers
in three weeks: followed by the names it carried host to host", NSS-TL-
```

```
01, 14 Nov 2026. https://nsshq.com/research/wallet-phishing-host-lineage
```

See something wrong? corrections@nsshq.com

More from NSS Research

NSS-TK-01: Fake imToken download sites push an Android app that sends recovery phrases and private keys to one server: technical analysis

NSS-RH-01: Lottery redirect names on a shared delivery network: technical analysis

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

---

NSS is not affiliated with imToken, TokenPocket, Telegram, Google, Proton, Sogou or any registrar, hosting company, DNS service or network behind the names in this paper. They are named because the names and the public records name them; nothing here says they knew of or took part in the activity.