

Found by NSS

53 names from NSS's own registration records, 40 unlisted on 13 Nov; app read by NSS

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

Copies of imToken's Chinese website offer an Android app from outside the official store. It is not imToken. NSS downloaded it and read its code: it sends the recovery phrase of every wallet created or imported in it to pt888999[.]com, and private keys to api.quick-node[.]com, a name that imitates QuickNode, which is not involved. On 13 November 2026 both names pointed to one server. Block both domains, look for the package com.anonymous.wallet, and treat any wallet made in it as exposed. NSS recorded 53 of the look-alike names; 40 were on no threat list NSS takes in on 13 November.

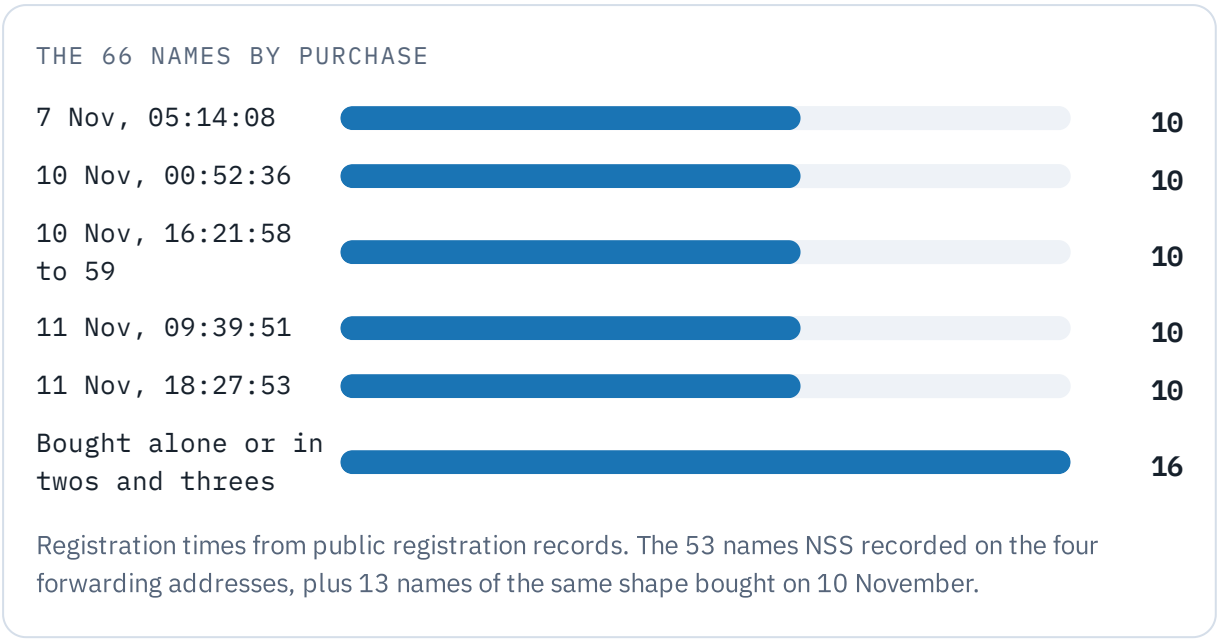
PUBLISHED	LAST UPDATED	READING TIME	MARKING
13 Nov 2026	13 Nov 2026	19 min	TLP:CLEAR

1
server behind both names the app sends recovery phrases and private keys to

53
look-alike names NSS recorded from new registrations, 8 to 12 November

5
purchases of ten names each, every one inside 2 seconds

40 of 53
names on no threat list NSS takes in on 13 November



Registration times from public registration records. The 53 names NSS recorded on the four forwarding addresses, plus 13 names of the same shape bought on 10 November.

Key findings

1. The download page offers an Android app that is not imToken. NSS downloaded the file on 13 November 2026 and read it without running it. Its package name is com[.]anonymous[.]wallet, not the official im[.]token[.]app, and it is signed with a generic debug certificate. The page shows a SHA-256 beside the download button, as the real page does; the file it links has a different one.

2. The app's code sends the recovery phrase and account list of every wallet created or imported in it to pt888999[.]com. It hands phrase creation, wallet creation, phrase and key import, and every transfer, private key included, to api[.]quick-node[.]com, its main back end, a name that imitates QuickNode, a real blockchain-node provider that is not involved. A browser that opens api[.]quick-node[.]com is sent on to the real provider's website. On 13 November both names resolved to

one address, 195.245.242[.]143. Neither name is on any threat list NSS takes in.

3. No page NSS loaded asks for a recovery phrase, a private key or a wallet connection. The pages copy the Chinese imToken website behind a visitor check that only a real browser passes, and ask the visitor to install the app. NSS loaded the imToken copy on 2 of the 53 names on 13 November; its 23 stored capture attempts on 12 November saw only the visitor check. The "Android APK" button links to a cloud storage bucket named imtokemapp (a misspelling); the "Google Play" button goes to a redirect link on another domain, not to Google Play.

4. NSS recorded 53 look-alike names from the daily lists of newly registered names, registered between 7 and 11 November 2026 and resolving to four forwarding addresses. 49 share one shape: a short made-up word, 45 of them starting "tok" (tokenism, tokeniem, tokinbin) and four not (two timerime names, timeaim, tolearn), then "-cdn" and a number, then a place code such as hk or sg and a number, on a cheap ending such as .lol or .xyz. The other four are mtokeni[.]vip, mtokeni[.]biz, tokenmi[.]vip and hellogpt-cdn[.]club.

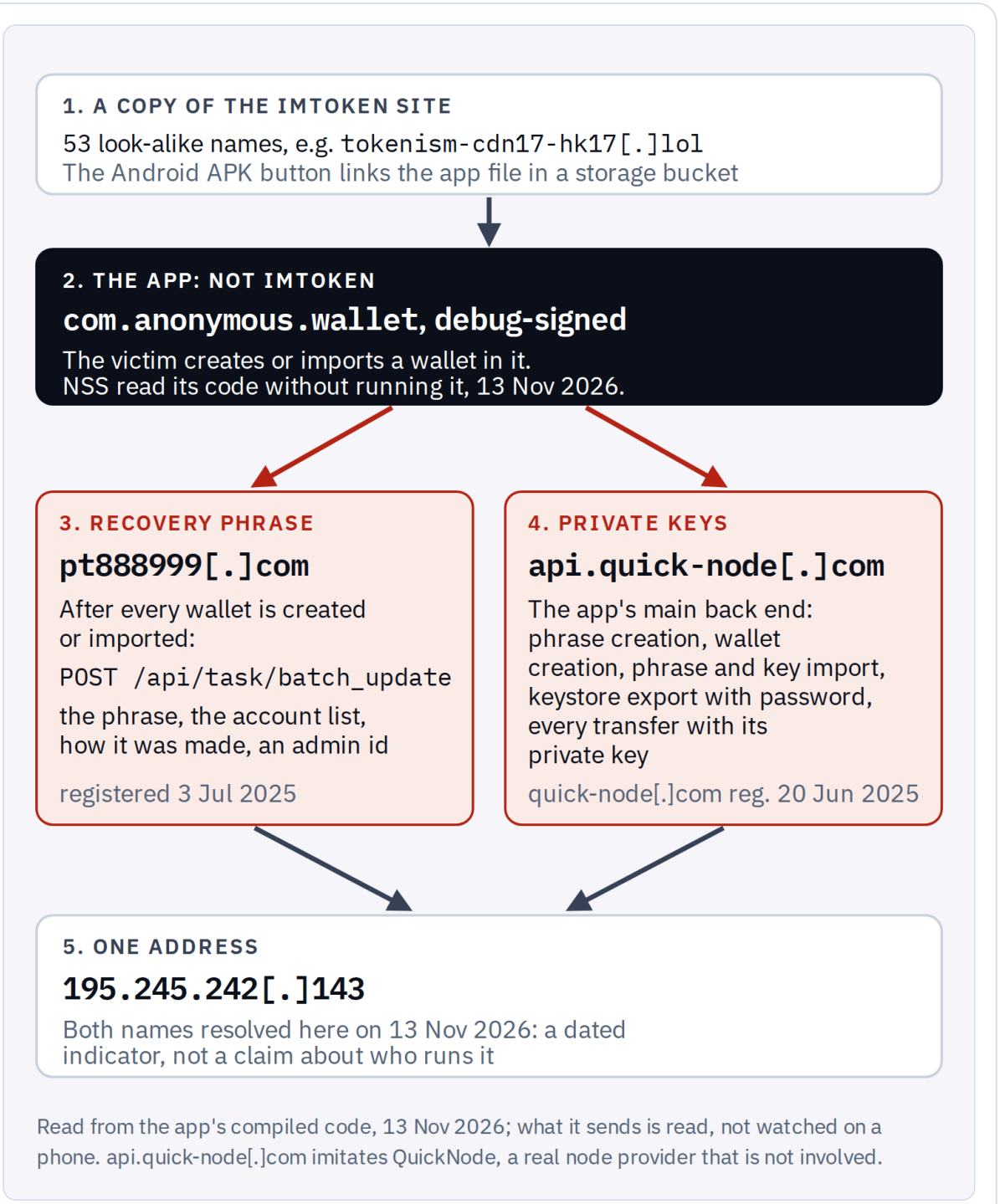
5. The names were bought at one registrar, most of them in bursts. With 13 more names of the same shape bought on 10 November, which NSS also recorded itself, there are 66: five purchases of ten names, each inside 2 seconds, hold 50 of them. 24 of the 53 were on registry hold by 13 November, so they no longer resolve.

6. Each name points at its own random eight-character label under a forwarding domain, and every label points at one shared host under the same domain. 33 of the 53 used ikunzf[.]online, which has carried names of this shape since at least 25 October; the last 20 used yumsihjkk[.]cc, bought on 11 November at 04:47 UTC; a third, shenswdns[.]cc, was bought ten minutes later. Labels keep their names when a site moves between these domains, so one table of labels sits behind all three.

7. Four addresses carried the 53 when NSS first resolved them: 82.158.231[.]42 (20 names), 103.38.82[.]202 (14), 156.225.24[.]119

(10) and 156.225.24[.]233 (9). NSS classes all four as dedicated: every name seen on them belongs to this forwarding set of look-alikes. NSS cannot rule out other customers of the service.

8. NSS's own record is not complete. At least 2 names from the same purchases reached NSS only from lists: tokininx-cdn18-hk78[.]lol, bought in the same second as tokieninn-cdn18-hk79[.]homes on 8 November, and tokeimxn-cdnnode-sg53[.]lol, bought in the same second as timerime-cdn3-hk62[.]xyz on 9 November. Lists also carried tokanix-cdn87-hk43[.]lol, a name of the same shape on the same forwarding, on 7 November, before NSS recorded any of the 53.



Read from the app's compiled code, 13 Nov 2026; what it sends is read, not watched on a phone. api.quick-node[.]com imitates QuickNode, a real node provider that is not involved.

What the app does with a wallet, read from its code on 13 November 2026 without running it: the recovery phrase goes to pt888999[.]com, and everything else, private keys included, to api[.]quick-node[.]com. Both names resolved to one address.

1. AFTER A WALLET IS CREATED OR IMPORTED

The names one function of the app loads, in their order: 21 of its 80, unchanged.

text	`"successAccounts"`	
reads	`sourceCreateType`	
text	`"create"`	
reads	`source`	
text	`"通过"`	"via"
text	`"导入"`	"import"
text	`"创建"`	"create"
reads	`HermesInternal`	
reads	`concat`	
text	`" ("`	
text	`"Android"`	
text	`")"`	
reads	`default`	
reads	**`post`**	an HTTP POST
sets	`data`	
reads	`mnemonic`	
sets	**`mnemonic`**	the recovery phrase
sets	**`note`**	how the wallet was made
sets	**`admin_id`**	an id (its value is not read)
text	**`"https://pt888999[.]com/api/task/batch_update"`**	
text	**`"accounts"`**	the account list

2. THE APP'S HTTP CLIENT

Base address **`https://api.quick-node[.]com`**; four of its 37 calls:

`createAccount`	`POST /api/wallet/create-from-mnemonic`	mnemonic
`importPrivateKey`	`POST /api/wallet/import-from-private-key`	the key it is given
`ethTransfer`	`POST /api/ethereum/transfer`	fromPrivateKey, toAddress, amount
`exportKeystore`	`POST /api/ethereum/export-keystore`	mnemonic, password

From NSS's stored read of the app file (SHA-256 66a22b70…ab26a), compiled JavaScript, 21,060 functions decoded; the app was not run.

The code behind the claim, from NSS's stored read of the app's compiled JavaScript, 13 November 2026: one function posts the phrase, the account list, how the wallet was made and an id to pt888999[.]com, and the app's HTTP client points at api[.]quick-node[.]com, whose calls carry the phrase, the password and the private key. An excerpt in the code's own order; the app was not run.

How an analyst finds this with NSS

The same case, worked the way a defender works it in NSS: from one new name to the action. Every picture is the real Station on 13 November 2026,

cropped to the panel in use.

01 A new name such as tokenism-cdn14-hk19[.]lol comes in. Investigate rates it Suspicious and ties it to the other names bought in the same second.



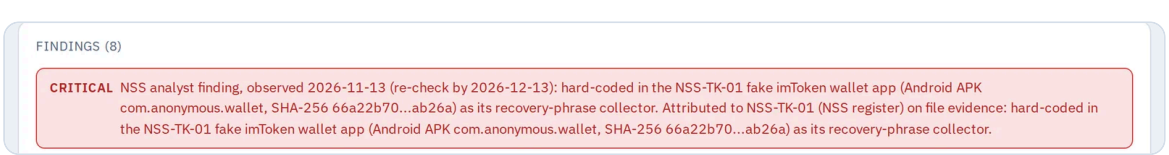
Investigate, 13 November 2026. The registrar's name is left out of the shot.

02 Sightline shows what the page served when NSS captured it: a visitor check on a dedicated host, with nothing loaded from anywhere else.



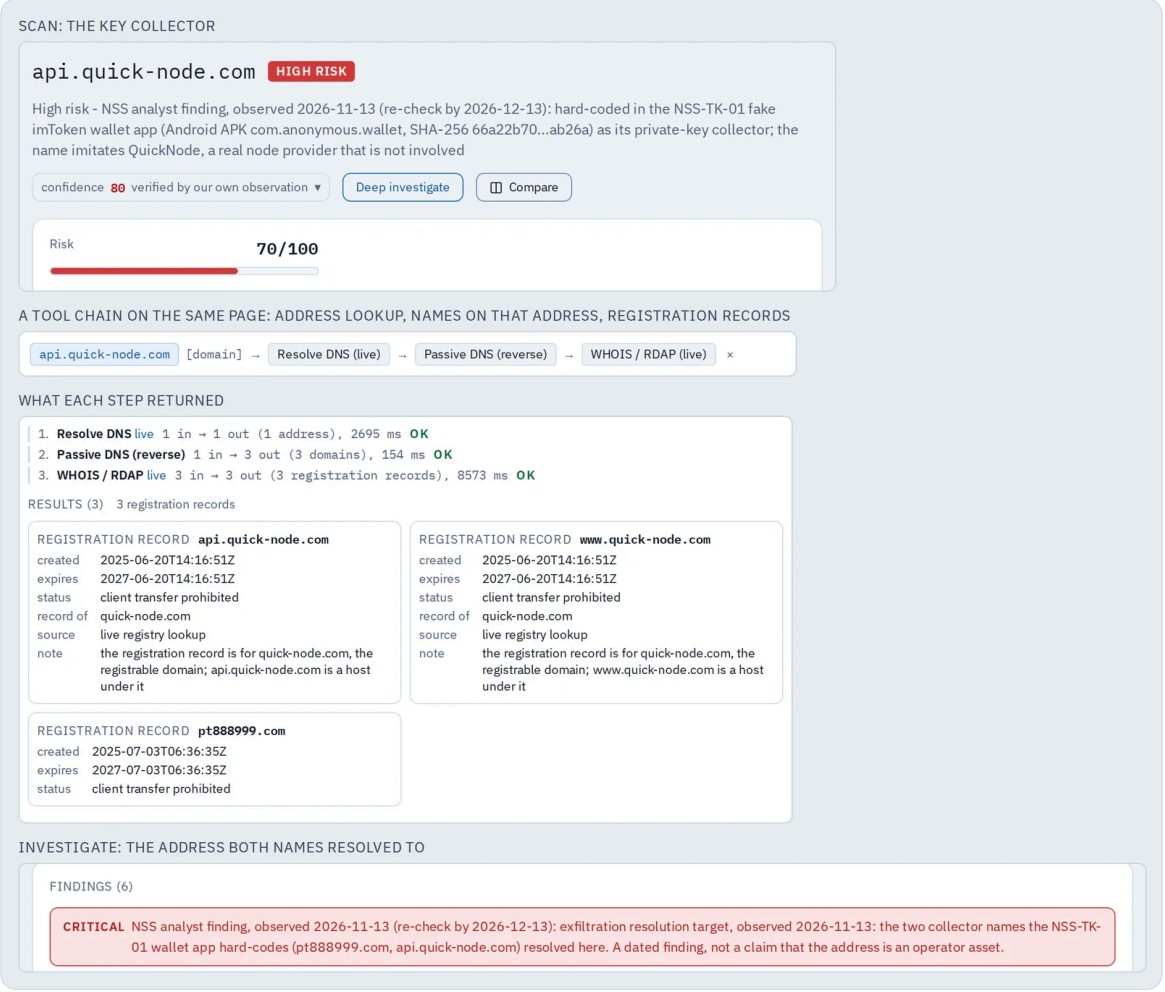
NSS's stored capture of tokaimn-cdn89-hk25[.]lol, 12 November 2026, 04:38 UTC. A browser that runs the page's script gets the imToken copy.

03 The casefile of pt888999[.]com cites the app NSS read: its hash, its package and the job the name does in it.



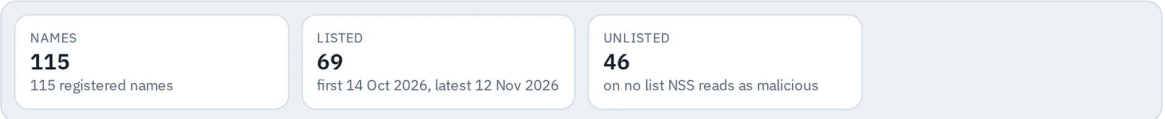
Investigate, 13 November 2026: the casefile's top finding, marked Critical, re-checked every 30 days. NSS-TK-01 is NSS's register name for this case, not a named group.

04 On Scan, a three-step tool chain links the two collector names to one server: address lookup, the names NSS has seen on that address, and their registration records.



Scan of api[.]quick-node[.]com and a tool chain run on 13 November 2026: one address carries pt888999[.]com and two quick-node[.]com hosts, and both domains were registered in mid-2025. Registrar and hosting names are left out of the shot.

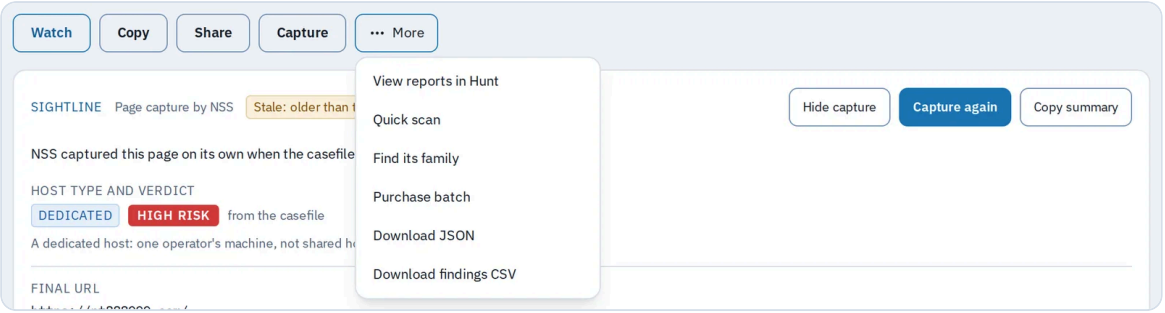
05 The family finder widens one name to its whole naming family.



Family finder, 13 November 2026: 115 registered names of the same shape, 69 of them on a threat list. The paper counts less: the 66 names NSS recorded itself from new registrations,

62 of them in this shape; the finder also counts names of the shape that NSS holds from threat lists and its own resolution records.

06 Then act: watch the names and the address, share the casefile, or download it as JSON or CSV for your own tools (Full features).



The casefile's actions, 13 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=$(jq -r '.indicators[0].value' nss-tk-01.json)   # the first name in
curl -s "https://nsshq.com/api/v1/check?value=$NAME"
```

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

The answer for that name on 13 November 2026

```
{
  "as_of": "2026-11-13T18:37:47Z",
  "band": "High risk",
  "band_is_host_class": false,
```

```
  "found": true,
  "host_class": {
    "as_of": "2026-11-13T17:30:47Z",
    "class": "dedicated",
    "label": "Dedicated host",
    "sentence": "Dedicated host (...)."
  },
  "known_good": false,
  "names": {
    "at_least": false,
    "listed": null,
    "total": 3
  },
  "public_listing": { (...) },
  "reports": 0,
  "type": "domain",
  "value": "pt888999[.]com",
  "view": "public"
}
```

The real answer of 13 November 2026, 18:37 UTC. Here the value is defanged, the host-type sentence shortened and the public-listing block left out: when this answer was read, the public view had not yet checked the name against public lists. The paper's listing state is from NSS's own check of 13 November, 14:31 UTC. When a network's checks for the day are used up, the same request answers HTTP 429 with a body that says when they reset (00:00 UTC).

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-tk-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:
            body = json.loads(e.read() or b"{}")
            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-tk-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.

Every morning, with a mail when a verdict changes

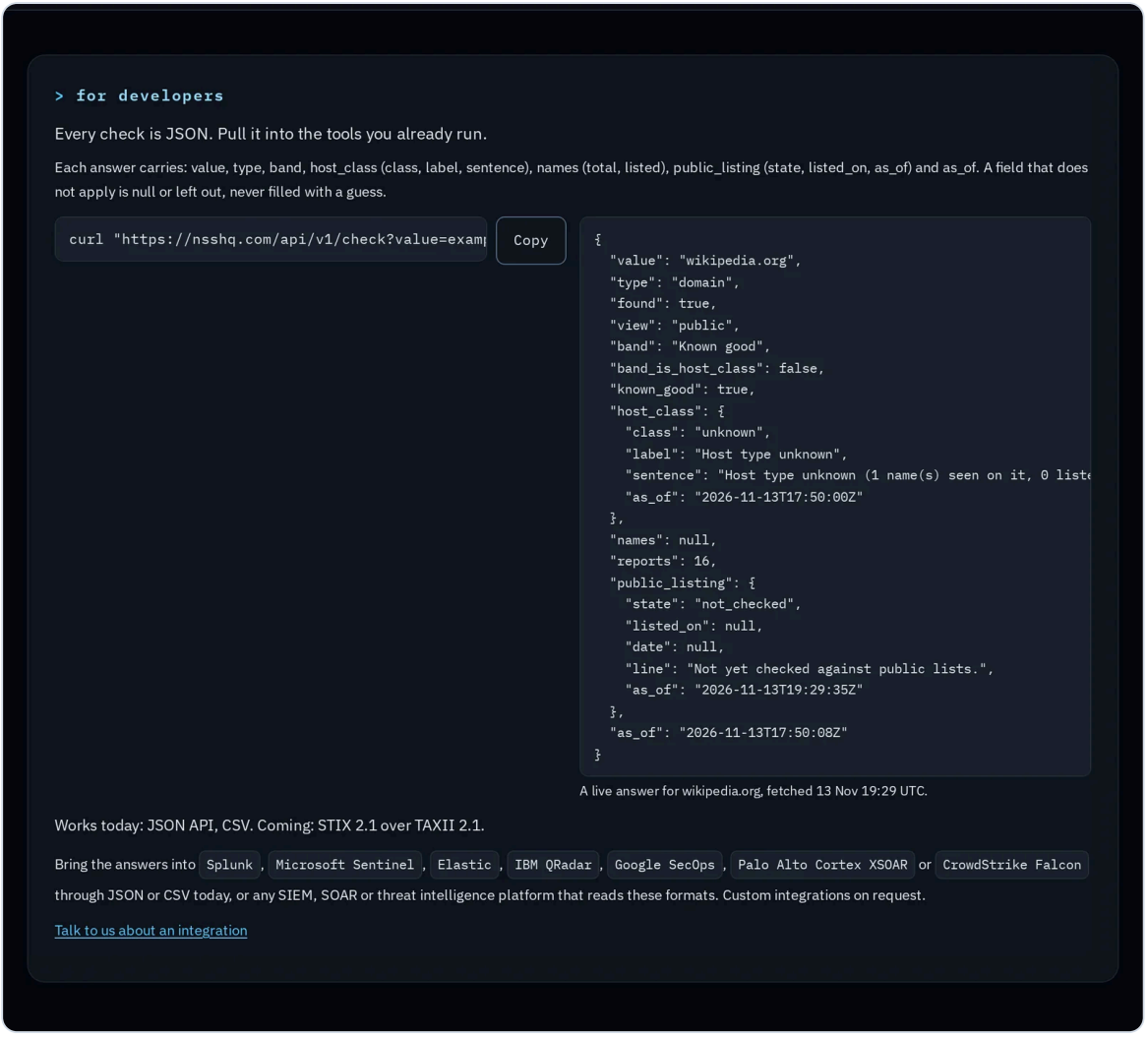
```
0 6 * * * cd /opt/nss && python3 nss_check_file.py nss-tk-01.json >> check
```

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.

For managed phones: alert on the package com[.]anonymous[.]wallet and on the file's SHA-256 from the file table above, and allow wallet apps only from the official stores.



The public Developers page on nsshq.com, 13 November 2026: the request, the fields every answer carries and a live answer.

Timeline

20 Jun and 3 Jul 2025

quick-node[.]com and pt888999[.]com are registered, at two different registrars. They will receive the app's private keys and recovery phrases.

1 Dec 2025

ikunzf[.]online is registered. It becomes the first forwarding domain.

25 Oct 2026

NSS first resolves names of this shape forwarded through ikunzf[.]online. It takes them from public lists.

7 Nov, 05:14:08

Ten names of the shape are registered in the same second.

7 Nov, by 16:37

Public lists carry tokanix-cdn87-hk43[.]lol, a name of the same shape bought on 30 October. NSS has not yet recorded any of the 53.

8 Nov, 04:16 to 04:17

NSS records the 12 names of 7 November from the day's new registrations. They resolve through ikunzf[.]online to three of the four addresses.

10 Nov, 00:52 and 16:21

Two more purchases of ten names each, the first in one second, the second in two. Three names spelled like TokenPocket follow at 16:27.

11 Nov, 04:47 and 04:57

Two new forwarding domains, yumsihjkk[.]cc and shenswdns[.]cc, are bought ten minutes apart.

11 Nov, 09:39 and 18:27

Two more purchases of ten names, all behind yumsihjkk[.]cc and the address 82.158.231[.]42.

12 Nov, 04:08

NSS records those 20 names. Its first captures half an hour later see only the visitor check.

12 Nov, from 05:20

Older names, still under their ikunzf[.]online labels, begin to resolve to 82.158.231[.]42 as well.

13 Nov, 00:43 to 00:55

NSS loads the pages as a desktop, an Android phone and an iPhone and reads the imToken copy and its download links.

13 Nov, 01:18

NSS downloads the app and reads its code without running it: package com[.]anonymous[.]wallet, and the two names it sends wallet secrets to.

13 Nov, from 06:56

NSS records seven more names spelled like TokenPocket on 82.158.231[.]42. They are not counted in this paper.

13 Nov, 11:06 to 11:07

NSS resolves pt888999[.]com and api[.]quick-node[.]com: both on 195.245.242[.]143. A browser opening api[.]quick-node[.]com lands on the real provider's website.

The app and where it sends wallets

NSS downloaded the file on 13 November 2026 at 01:18 UTC and read it without running it: the manifest, the signature and the app's compiled code, function by function. The read is stored in NSS's records with the file's hash.

PROPERTY	VALUE
File name	imToken-v2.apk
Size	99,053,451 bytes
SHA-256	66a22b70bedd816888333155fbe469781ccbf8be8ad158541bdaf162d85ab26a
MD5	888e0a07c612a7d57c6cc91675ef7622
Package name	com[.]anonymous[.]wallet (the official app is im[.]token[.]app)
Version in the file	2.21.0 (the page says v2.13.5)
Signed with	A generic debug certificate (CN=Android Debug), not a publisher's key
Built with	React Native; one compiled JavaScript bundle, read function by function
Sends recovery phrases to	pt888999[.]com: the phrase and account list of every wallet created or imported (POST /api/task/batch_update)
Sends private keys to	api[.]quick-node[.]com, the app's main back end: phrase creation, wallet creation, phrase and key import, keystore export with its password, and every transfer, private key included

Both names on 13 Nov	195.245.242[.]143

The theft happens inside the app, after it is installed. A victim types or creates a recovery phrase in what looks like imToken, and the app sends it on. Anyone holding a recovery phrase or a private key controls the wallet, so a copy sent to pt888999[.]com or api[.]quick-node[.]com is enough to empty it.

api[.]quick-node[.]com is spelled like QuickNode, a real blockchain-node provider. It belongs to quick-node[.]com, registered on 20 June 2025 (2025-06-20). quick-node[.]com rates High because its own DNS publishes the private-key collector; its www host copies QuickNode's site. QuickNode is not involved, and the domain is not attributed to an operator. A browser that opens api[.]quick-node[.]com is sent on to the real provider's website, so a hand check of the name looks harmless. pt888999[.]com was registered on 3 July 2025 at another registrar. Both names are older than any of the look-alike names, and neither is on any threat list NSS takes in.

The copied download page shows a version number, v2.13.5, and a SHA-256 under "Android APK SHA256", as the real page does, which makes the file look checked. The file the button links has a different SHA-256 (above) and calls itself version 2.21.0. The hash on the page does not belong to the file.

What the pages serve

A plain request to any of the live names returns a short page that says, in Chinese, that many people are visiting and the page is loading. It runs a script, /btwaf_aes_forge_6d7584ebbc8099962ec31133b1a1bdde.js, sets a cookie and reloads. A browser that runs the script gets the real page; a scanner that does not sees only the loading notice. Every page NSS loaded set the same session cookie name, server_session_c098fd19: the 12 stored captures that loaded on 12 November (11 names, all of them stopped at the visitor check) and the page loads of 13 November.

Behind the check is a copy of the Chinese imToken home page, titled "imToken | Ethereum & Bitcoin Wallet", with its download buttons. NSS saw it in its page loads of 13 November on 2 of the 53 names, from different purchases, which returned byte-identical pages, 9,317 bytes each; no stored capture holds the copy. The download page is a copy of the real one, with two links changed:

BUTTON	WHERE IT GOES
Android APK	imToken-v2.apk in a cloud storage bucket named imtokemapp: hxxps://imtokemapp[.]s3[.]ap-southeast-1[.]amazonaws[.]com/imToken-v2.apk
Google Play	A redirect link, hxxps://zty4o[.]1za5ww[.]com/URmQ3pa/3vGnXHsGlZgt24W3, that forwards on to a content-delivery address, not to Google Play

These two download addresses and the file's two hashes (in the file table above) are file evidence, not entries in the indicator list: NSS gives verdicts to names and addresses, not to single download addresses or to files, so none of the four carries an NSS verdict.

The copied page also loads one script from tekcen[.]im, a look-alike of the real site's name that no longer resolves, which suggests where the copy was first built.

Two other pages share the forwarding set-up. hellogpt-cdn[.]club and tokenmi[.]vip answer at their front page with a "contact customer service" panel that offers WeChat, Telegram, WhatsApp, LINE, Zalo and Skype, filled in from /service[.]php. tokenmi[.]vip then sends a visitor's browser to the admin page of a home router on a private address, a way to send unwanted visitors nowhere. The three names spelled like TokenPocket showed a stock web-design template on 13 November.

How the names are bought and wired

All 66 names in this paper were bought at one registrar. Five purchases of ten names each, every one inside 2 seconds, hold 50 of them; the rest were bought alone or in twos and threes. 24 of the 53 were on registry hold by 13 November.

Every name is a forwarding record. It points at a random eight-character label under a forwarding domain, for example j8mhacg6[.]yumsihjkk[.]cc, and every label points at one shared host, z6pnwmjk, under the same domain. That host gives the address.

FORWARDING DOMAIN	BOUGHT	NAMES OF THE 53	ON 13 NOVEMBER
ikunzf[.]online	1 Dec 2025	33 (7 to 9 Nov)	Its shared host no longer resolves
yumsihjkk[.]cc	11 Nov 2026, 04:47	20 (11 Nov)	25 names point to it, 20 of them live on 82.158.231[.]42
shenswdns[.]cc	11 Nov 2026, 04:57	none; 7 of the 13 names from 10 Nov	Its labels do not resolve

What NSS measured, and which names each number counts

This paper uses three sets of names. Each number says which one it counts.

SET	NAMES	WHAT IT IS
The 53	53	Names registered 7 to 11 November that NSS recorded itself from the daily lists of new registrations and that resolved to the four forwarding addresses
The 66	66	The 53, plus 13 names of the same shape bought on 10 November that NSS also

		recorded itself (ten in one purchase at 16:21 and three spelled like TokenPocket at 16:27)
Indicators	75	65 of the 66 names (all but mtokeni[.]vip, below), the forwarding domain yumsihjkk[.]cc and the shared host under it, the four forwarding addresses, the two names the app sends to, their registered domain, and the address both resolved to

The indicator list holds only what NSS gives a verdict, read on Investigate and Scan on 13 November 2026. Left out for that reason: mtokeni[.]vip, one of the 53, which NSS rates Clean because nothing but its look links it to the others; the forwarding domains ikunzf[.]online and shenswdns[.]cc, which NSS rates Clean; and the download addresses and hashes (file evidence, above).

MEASURE (THE 53)	RESULT
Time from registration to NSS record	4.3 to 26.2 hours, median 18.5, over all 53
On a threat list NSS takes in, 13 Nov 2026, 14:31 UTC	13 of 53, each listed after NSS recorded it
On no threat list NSS takes in, 13 Nov 2026, 14:31 UTC	40 of 53
Names from the same purchases that reached NSS only from lists	At least 2

The 53 are, by definition, names NSS recorded itself, so they say nothing about how much NSS misses. It did miss some. tokininx-cdn18-hk78[.]lol was bought in the same second as tokieninn-cdn18-hk79[.]homes (8 Nov, 06:02:24) and sat on 103.38.82[.]202, and tokeimxn-cdnnode-sg53[.]lol was bought in the same second as timerime-cdn3-hk62[.]xyz (9 Nov, 03:57:11). NSS has both only from public lists. Lists also carried tokanix-cdn87-hk43[.]lol, forwarded through ikunzf[.]online, on 7 November, before NSS recorded any of the 53. And the same forwarding domain carried 36 earlier names, wallet, Telegram and download look-alikes, from 25 October, all of which reached NSS from public lists.

"On no threat list NSS takes in" is not "on no threat list anywhere". The 20 names bought on 11 November were about two days old at the check.

Operator evidence, and where it stops

What the records prove:

- **One label table behind three domains.** Labels keep their names when a site moves: fmr635hz and 2r36s5d9 went from ikunzf[.]online to yumsihjkk[.]cc with hellogpt-cdn[.]club and tokenmi[.]vip by 13 November, the label atzuqs2x moved the same way for three other sites, and 9r2b8vj7 appears under both ikunzf[.]online and shenswdns[.]cc. Whoever runs the forwarding runs all three domains.
- **Bought together.** The two new forwarding domains were bought ten minutes apart at the registrar that holds ikunzf[.]online, five hours before the first names that use them.
- **Bought in bursts.** Five purchases of ten names, each inside 2 seconds, at one registrar, hold 50 of the 66 names.
- **One kit.** The same visitor-check script and the same session cookie name on every name NSS loaded, and the same copied page, byte for byte, on the two names where NSS saw it.
- **One app, one server.** The copied page links one app file, and both names the app sends wallet secrets to resolved to one address on 13 November.
- **Dedicated hosts.** 82.158.231[.]42, 103.38.82[.]202, 156.225.24[.]119 and 156.225.24[.]233 are classed dedicated by NSS: every name seen on them belongs to this forwarding set of look-alikes. NSS cannot rule out other customers of the service. The four sit in two networks run by one hosting company.

What they do not prove:

- That the imToken pages and the Telegram and download look-alikes on the same forwarding are one operator. They share the label table and the servers. But those names were bought months earlier at other registrars, were listed from August, and run as a separate site with its own session cookie. That fits a forwarding and hosting service with several customers as well as one operator.
- That 195.245.242[.]143 belongs to the operator. It is where both exfiltration names resolved on 13 November; NSS lists it as an indicator as of that date and re-checks it every 30 days.
- Who is sent to the pages, or whether anyone installed the app.
- The name servers and the hosted DNS that the names and forwarding domains use are shared services and count for nothing here.

Seen before: the same method in public reporting

NSS Hunt searched NSS's library of past reporting for fake imToken apps and for wallet apps handed out from outside the official stores. The method is established. Closest first:

REPORTED	WHO, AS REPORTED	LURE	PAYLOAD	HOW CLOSE
Mar to Apr 2026	FakeWallet, no named group	20+ App Store apps posing as wallets, among them imToken and TokenPocket, that open pages styled as an app store	Modified copies of real wallet apps	Same brand same kind o payload, oth first step
Apr 2026	No named group	Wallet look-alike apps in a Chinese app store and installable	Recovery-phrase theft and modified wallet apps	Same brand same goal

		configuration profiles		
Mar 2026	No named group	A browser add-on posing as a colour tool	Theft of imToken private keys and recovery phrases	Same brand other lure
Oct 2023	Enchant Android malware, no named group	Fake adult sites aimed at cryptocurrency users in China	Android malware that reads recovery phrases and keys from wallet apps	Same victim and goal, otl lure

NSS found none of this paper's names, addresses or file hashes in these reports or in any report NSS holds. The match is in method only, and this paper does not link the operator to anyone above.

How it maps to ATT&CK

TECHNIQUE	WHAT NSS SAW
T1583.001 Acquire Infrastructure: Domains	66 names in bursts and three forwarding domains, 1 Dec 2025 to 11 Nov 2026
T1608.001 Stage Capabilities: Upload Malware	An app package staged in a cloud storage bucket, linked from the copied page
T1656 Impersonation	A copy of the imToken website and download page; a back-end name spelled like a real node provider
T1204.002 User Execution: Malicious File	The visitor must install the app themselves
T1646 Exfiltration Over C2 Channel (Mobile)	The app sends each wallet's recovery phrase to pt888999[.]com and private keys to api[.]quick-node[.]com over the web

What a defender can look for

In order of priority:

1. Block pt888999[.]com and quick-node[.]com at DNS and gateway. This blocks further exfiltration from installed copies; it does not undo theft already done. Treat any wallet created or imported in the app as exposed and move funds to a new wallet made on a clean device.
2. On managed phones, look for the package com[.]anonymous[.]wallet and the SHA-256 above, and allow wallet apps only from the official stores. imToken's own site and the official stores are the only sources of its app.
3. Block, at DNS, any name that forwards to ikunzf[.]online, yumsihjkk[.]cc or shenswdns[.]cc. New names join through these forwarding domains.
4. Block the APK address and the Google Play redirect, given in the download-button table above, at the web gateway. Block only that bucket, never the storage service.
5. 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]{1,2}\.` on .lol, .xyz, .autos, .click, .cfd, .homes, .pics, .beauty, .monster, .quest, .lat or .baby. It matches all 62 names of this shape in the paper, and the TokenPocket names NSS recorded on 13 November that use edge, pop or gw in place of cdn. Alert, do not block: it can match an ordinary name.
6. Block the four forwarding addresses, and 195.245.242[.]143 while the exfiltration names point to it.

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

The NSS tools used

> Discovery
Took all 53 names, and the 13 more of 10 November, from the daily lists of new

> Register
Holds the four forwarding addresses as tracked hosts and classes them, and the

registrations, between 4.3 and 26.2 hours after purchase, and resolved each through its forwarding chain.

address behind the app's two names, as dedicated.

> Capture
Made 23 capture attempts on 12 November between 04:38 and 05:33 UTC: 12 loaded a page (11 names), and every stored image shows the visitor check. On 13 November, loaded the pages as a desktop, an Android phone and an iPhone and read the imToken copy and its download links on 2 names; captured api.quick-node[.]com sending a browser to the real provider's site; downloaded the app file and read its code without running it.

> Scan
Re-checked where every name resolves on 13 November and read live certificates; a tool chain on Scan tied the two collector names to one address and read their registration records.

> Family finder
Grouped the names of the same shape around one of them and showed their purchase batches.

> Investigate
Read the public registration record of every name and forwarding domain and found the purchase bursts.

> Hunt
Searched NSS's library of past reporting for the same brand and method: four earlier reports, and no shared name, address or file.

Indicators

The first 25 of 75 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
pt888999[.]com	Domain	Receives the recovery phrase and account list of every wallet the app creates or imports (POST /api/task/batch_update); registered

		3 Jul 2025; resolved to 195[.]245[.]242[.]143 on 13 Nov 2026; on no threat list NSS takes in
`api[.]quick-node[.]com`	Domain	The app's main back end: receives phrase creation, wallet creation, phrase and key import, keystore export and every transfer, private key included; imitates QuickNode, a real blockchain-node provider that is not involved; a browser is sent on to the real provider's site; resolved to 195[.]245[.]242[.]143 on 13 Nov 2026; on no threat list NSS takes in
`quick-node[.]com`	Domain	Registered 2025-06-20; rates High because its own DNS publishes the private-key collector; its www host copies QuickNode's site. QuickNode is not involved, and the domain is not attributed to an operator. Block this name only, never the real provider's domain
`195[.]245[.]242[.]143`	IP address	Where both exfiltration names resolved on 13 Nov 2026; an indicator as of that date, not an operator asset; re-checked every 30 days
`yumsihjkk[.]cc`	Domain	Forwarding domain, registered 11 Nov 04:47 UTC; 25 of the names pointed to it on 13 Nov
`z6pnwmjk[.]yumsihjkk[.]cc`	Domain	The shared host every forwarding label points to; resolved to 82[.]158[.]231[.]42 on 13 Nov
`82[.]158[.]231[.]42`	IP address	Forwarding address; classed dedicated by NSS; 20 of the 53 names on first resolution; served the imToken copy on 13 Nov
`103[.]38[.]82[.]202`	IP address	Forwarding address; classed dedicated by NSS since 13 Nov

		2026 10:26 UTC; 14 of the 53 names on first resolution
156[.]225[.]24[.]119	IP address	Forwarding address; classed dedicated by NSS; 10 of the 53 names on first resolution
156[.]225[.]24[.]233	IP address	Forwarding address; classed dedicated by NSS; 9 of the 53 names on first resolution
hellogpt-cdn[.]club	Domain	Registered 8 Nov 14:57 UTC; NSS record 9 Nov 06:52; on no threat list NSS takes in; live on 82[.]158[.]231[.]42 on 13 Nov
tokairvm-cdn83-hk84[.]click	Domain	Registered 11 Nov 18:27 UTC in a batch of 10; NSS record 12 Nov 04:08; on no threat list NSS takes in; live on 82[.]158[.]231[.]42 on 13 Nov
tokeaim-cdn09-hk44[.]autos	Domain	Registered 11 Nov 09:39 UTC in a batch of 10; NSS record 12 Nov 04:08; on no threat list NSS takes in; live on 82[.]158[.]231[.]42 on 13 Nov
tokeaivem-cdn34-hk77[.]pics	Domain	Registered 11 Nov 09:39 UTC in a batch of 10; NSS record 12 Nov 04:08; on no threat list NSS takes in; live on 82[.]158[.]231[.]42 on 13 Nov
tokenianv-cdn55-hk35[.]lol	Domain	Registered 11 Nov 18:27 UTC in a batch of 10; NSS record 12 Nov 04:08; on no threat list NSS takes in; live on 82[.]158[.]231[.]42 on 13 Nov
tokeniem-cdn11-hk41[.]click	Domain	Registered 11 Nov 18:27 UTC in a batch of 10; NSS record 12 Nov 04:08; on no threat list NSS takes in; live on 82[.]158[.]231[.]42 on 13 Nov

tokeniem-cdn61-hk46[.]lol	Domain	Registered 11 Nov 18:27 UTC in a batch of 10; NSS record 12 Nov 04:08; on no threat list NSS takes in; live on 82[.]158[.]231[.]42 on 13 Nov
tokenirm-cdn72-hk84[.]lol	Domain	Registered 11 Nov 18:27 UTC in a batch of 10; NSS record 12 Nov 04:08; on no threat list NSS takes in; live on 82[.]158[.]231[.]42 on 13 Nov
tokenism-cdn08-hk39[.]lol	Domain	Registered 11 Nov 09:39 UTC in a batch of 10; NSS record 12 Nov 04:08; on no threat list NSS takes in; live on 82[.]158[.]231[.]42 on 13 Nov
tokenism-cdn17-hk17[.]lol	Domain	Registered 11 Nov 09:39 UTC in a batch of 10; NSS record 12 Nov 04:08; on no threat list NSS takes in; live on 82[.]158[.]231[.]42 on 13 Nov
tokenism-cdn52-hk13[.]autos	Domain	Registered 11 Nov 18:27 UTC in a batch of 10; NSS record 12 Nov 04:08; on no threat list NSS takes in; live on 82[.]158[.]231[.]42 on 13 Nov
tokenism-cdn58-hk84[.]lol	Domain	Registered 11 Nov 09:39 UTC in a batch of 10; NSS record 12 Nov 04:08; on no threat list NSS takes in; live on 82[.]158[.]231[.]42 on 13 Nov
tokenism-cdn81-hk08[.]lol	Domain	Registered 11 Nov 09:39 UTC in a batch of 10; NSS record 12 Nov 04:08; on no threat list NSS takes in; live on 82[.]158[.]231[.]42 on 13 Nov
tokenism-cdn94-hk19[.]lat	Domain	Registered 11 Nov 09:39 UTC in a batch of 10; NSS record 12 Nov 04:08; on no threat list NSS takes

		in; live on 82[.]158[.]231[.]42 on 13 Nov
`tokenixm-cdn12-hk65[.]lol`	Domain	Registered 11 Nov 18:27 UTC in a batch of 10; NSS record 12 Nov 04:08; on no threat list NSS takes in; live on 82[.]158[.]231[.]42 on 13 Nov

ALL 75 INDICATORS: CSV JSON STIX More formats on GitHub

No sign-up.

How we know

What this rests on

- Where each name resolves and what it forwards to is from NSS's own resolution records from 8 to 13 November and one fresh check of every name on 13 November 2026 at 00:39 UTC. The two exfiltration names were resolved on 13 November at 11:06 and 11:07 UTC.
- The listing state was checked on 13 November 2026 at 14:31 UTC against every list NSS takes in. A listing of the name or of any web address on it counts.
- Registration times and registrars are public registration records, read on 12 and 13 November 2026. A burst is several names from one registrar in the same one or two seconds.
- Page descriptions are from NSS's 23 stored capture attempts on 12 November 2026 between 04:38 and 05:33 UTC (12 loaded, all at the visitor check) and from pages NSS loaded on 13 November 2026 between 00:43 and 00:55 UTC (the imToken copy, on 2 names). The app file was downloaded by NSS on 13 November 2026 at 01:18 UTC and read without being installed or run (SHA-256 66a22b70...ab26a, in full in the file table and the indicator list); the read, its manifest, signature and the code that sends each secret, is stored in NSS's records with the hash.

- The host type of each address is as NSS classed it on 13 November 2026 (103.38.82[.]202 from 10:26 UTC).
- NSS's stored captures of the pages are from 12 November 2026, and NSS loaded the pages again on 13 November. Every verdict in this paper is as read on 13 November 2026; the two collector names and their address are re-checked every 30 days.

What we cannot say

- NSS did not see how visitors are sent to the pages, who received the links, or whether anyone installed the app.
- NSS downloaded and read the app but did not run it, so what it sends is read from its code, not watched on a phone.
- 195.245.242[.]143 is an indicator as of 13 November 2026, where both exfiltration names resolved, not a claim about who runs it. NSS re-checks it every 30 days.
- The 53 are names NSS recorded itself. At least 2 names from the same purchases reached NSS only from lists, so NSS's record of this set is not complete.
- "On no threat list NSS takes in" is not "on no threat list anywhere". The 20 names bought on 11 November were about two days old at the check.
- The forwarding service may serve more than one customer. The Telegram and download look-alikes on it, and the seven TokenPocket names of 13 November, are not counted in this paper's numbers.
- This paper is not attributed to any named group. NSS-TK-01 is NSS's register name for this case, not a named group.

Use and citation

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

```
Nexus Sentinel Station (NSS), "Fake imToken download sites push an
Android app that sends recovery phrases and private keys to one server:
technical analysis", NSS-TK-01, 13 Nov 2026.
https://nsshq.com/research/fake-imtoken-download-sites
```

See something wrong? corrections@nsshq.com

NSS is not affiliated with imToken, TokenPocket, QuickNode, Google, or any registrar, hosting company, storage service or network behind the names in this paper. They are named because the pages, the app and the public records name them; nothing here says they knew of or took part in the activity. api.quick-node[.]com is not the real node provider and is not linked to it; block only quick-node[.]com, never the real provider's domain.