

Found by NSS 100 of 319 names recorded by NSS and on no list NSS holds

Lottery redirect names on a shared delivery network: technical analysis

Two address blocks on two different networks answer for the same 319 throwaway names, and the names open Chinese-language lottery and betting pages. NSS recorded 100 of those names itself, a median of 21 minutes after their certificates appeared, and none of the 100 is on any list NSS holds. This paper sets out what ties the names together, why the two blocks are a shared delivery network and not one operator's servers, and what a defender can look for.

PUBLISHED	LAST UPDATED	READING TIME	MARKING
11 Nov 2026	11 Nov 2026	8 min	TLP:CLEAR

319
names answering from the two blocks

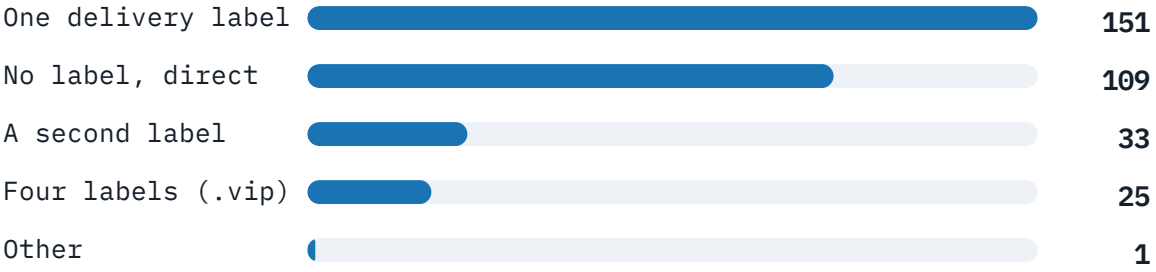
100
recorded by NSS and on no list NSS holds

21 min

13
purchase batches holding 140 registered names

median from certificate log to NSS record

THE 319 NAMES BY WHAT STANDS IN FRONT OF THEM



From one check of every name on 11 November 2026. A label is the forwarding name a delivery service gives one customer set-up.

Key findings

1. 319 names under 191 registered domains answered from two address blocks on two different networks. On 11 November 2026, 318 of them still resolved.
2. The pages are lottery and betting sites. Of 21 sample names NSS captured, 15 opened a Chinese-language lottery or betting page; six of those forwarded on to one family of three landing names.
3. NSS recorded 100 of the names itself between 3 and 11 November, from certificate logs and new registrations. None of the 100 is on any list NSS holds. For the 73 found in certificate logs, the median time from the log entry to the NSS record was 21 minutes.
4. The names were bought in batches. 13 batches of five or more hold 140 of the 191 registered domains; the tightest put 32 names through one registrar in 6 seconds.
5. The two blocks are not one operator's servers. Every probed host presents the same default certificate of a delivery product, the names now answer from five further blocks as well, and the names fall into separate sets that share no batch, no registered domain and no forwarding label.

6. What ties names together is the label in front of them. 151 names forward through one delivery label and 33 through a second; 25 new .vip names forward through four labels of another service.
7. The activity is current. Five batches of five .vip names were registered on 7 and 10 November 2026, and NSS recorded all 25.

Timeline

31 Jan 2026, 03:08 UTC
Earliest batch in the set: 15 names of sixteen random characters registered in 2 seconds.

11 Jul 2026
Two batches of numeric names through one registrar, 6 and 29 names, under an hour apart. NSS later finds a name from each forwarding to the landing family.

27 Jul 2026, 05:22 UTC
The tightest batch: 32 names in 6 seconds.

19 and 31 Oct 2026
219 of the names reach NSS from public lists.

3 Nov, 09:26 UTC
NSS records the first name that is on no list, from a certificate log.

4 Nov
NSS probes the hosts and files the two blocks in its register as operator clusters. This paper corrects that reading.

3 to 7 Nov
73 names recorded from certificate logs, each within 9 to 32 minutes of its log entry.

7 and 10 Nov
Five batches of five .vip names are registered. NSS records all 25.

11 Nov, 12:04 UTC
Fresh check: 318 of 319 names resolve. NSS captures 21 sample sites.

What NSS saw first

On 4 November 2026 NSS's register flagged two address blocks, one on a network in Taiwan and one on a network in the United States, because the same names kept resolving to both. Ten addresses, five in each block, answered for the same 179 names. The register filed each block as an operator cluster on dedicated hosts.

That reading was too strong, and this paper replaces it. What the records support is narrower and more useful.

A delivery network, not an operator

Three records say the two blocks are part of a shared delivery network, the kind of service that sits in front of many customers' sites.

- **One default certificate.** All 16 hosts NSS probed present the same self-signed certificate, valid from 2021 to 2031 and named for a generic delivery domain. A certificate shipped with a product is on every installation of that product. It says the hosts run the same software, not that one party runs them.
- **A moving pool.** On 11 November the same names also answered from five further address blocks. 194 names answered from two blocks, and 109 from three or more.
- **Separate sets of names.** The 319 names fall into sets that share nothing with each other but the pool: no purchase batch, no registered domain and no forwarding label is common to the names NSS recorded and the names the public lists carry.

So the addresses are not indicators. Blocking them would block whatever else the delivery network carries.

What does tie names together

Inside each set the links are strong, and they are public records.

LINK	WHAT NSS MEASURED
Forwarding label	151 names forward through one delivery label, 33 through a second, 25 through four labels of another service
Purchase batch	13 batches of five or more names from one registrar, each name within 30 seconds of the last: 140 of 191 registered domains
Name pattern	Within a batch the names differ by a letter or a digit, for example a six-digit number followed by one or two letters
Landing	Six sample names, two of them from the July batches, forward to three landing names that differ by three letters

A forwarding label is the most useful of these. A delivery service gives a customer set-up one label, and every name placed behind it points at that label. The two labels that carry 184 of the listed names are `061a016-h002[.]cdncname[.]com` and `zy7wph[.]cdncname[.]com`. Any other name that forwards to either is worth a look.

The names NSS recorded itself

219 of the 319 names reached NSS from public lists in October. The other 100 did not. NSS recorded them from two of its own sources: certificate logs, where a new certificate for a name becomes public, and the daily lists of newly registered names.

MEASURE	RESULT
Names recorded by NSS and on no list NSS holds	100, under 99 registered domains
Recorded from certificate logs	73
Time from log entry to NSS record	median 21 minutes, shortest 9, longest 32
Recorded from new registrations	26

Registered in a batch of five or more	65 of the 99 registered domains

Two things are not claimed. NSS has not checked every public list, only the ones it holds, so "on no list" means on none of those. And the 21 minutes is the time from a public log entry to NSS's record, not a lead over anyone else.

The newest are the clearest. On 7 November three batches of five .vip names were registered within an hour, and on 10 November two more. Each batch went through one registrar inside 4 seconds, and the 25 names were placed behind four forwarding labels. NSS recorded all 25.

What the sites served

NSS captured 21 sample names on 11 November as a phone and as a desktop. 20 loaded.

- 15 opened a Chinese-language lottery or betting page: draw results billed as live from Macau, a numbered-draw directory, and two sites offering to sell lottery tickets.
- One opened a Vietnamese-language page titled as an official home page. NSS did not classify it.
- Six of the 15 did not show their own page. They forwarded through four steps to one of three landing names, `pc[.]66111xxx1[.]com`, `pc[.]66111yyy1[.]com` and `pc[.]66111zzz1[.]com`.
- Two showed a "link expired" notice, one a web server's default page and one an empty page.

NSS saw no sign-in copy of another brand and no file download on these samples, and its own casefiles rate most of the names it had checked as clean of phishing. The public lists that carry 219 of the names treat them as harmful. NSS records what the pages are, lottery and betting sites behind throwaway names, and does not rule on their lawfulness in any country.

What a defender can look for

- Names that forward to the labels `061a016-h002[.]cdncname[.]com` or `zy7wph[.]cdncname[.]com`.
- Names that forward to one of the three landing names above, or to a name built the same way with other letters.
- Batches of five random eight-letter .vip names from one registrar inside a few seconds.
- Numeric names that differ only in a trailing letter or two, registered together.
- The indicator list below, for policy that restricts gambling sites and for looking back through logs. Nearly every name was live on 11 November 2026.
- Do not block the addresses. They belong to a shared delivery network.

The NSS tools used

> Discovery
Recorded 100 names from certificate logs and new registrations between 3 and 11 November, 73 of them within 9 to 32 minutes of the certificate log entry.

> Register
Flagged the two blocks on 4 November because the same names resolved to both. Its first reading, operator clusters on dedicated hosts, is corrected by this paper.

> Probe
Read the open services and the certificate on 16 hosts in the two blocks. Every one presented the same default certificate.

> Investigate
Read the public registration record of all 191 registered domains and found the purchase batches.

> Capture
Loaded 21 sample sites as a phone and as a desktop and recorded each forwarding step and the page at the end.

> Watch
Re-checked where all 319 names resolve on 11 November, which showed the forwarding labels and the five further blocks.

Indicators

The first 25 of 319 indicators. Each is written defanged so it cannot be opened by accident.

INDICATOR	TYPE	NOTE
ahnahgsp[.]vip	Domain	Recorded by NSS on 11 Nov 2026; on no list NSS holds; behind a forwarding label
avovhmix[.]vip	Domain	Recorded by NSS on 11 Nov 2026; on no list NSS holds; behind a forwarding label
dabygfql[.]vip	Domain	Recorded by NSS on 8 Nov 2026; on no list NSS holds; behind a forwarding label
epmhbuga[.]vip	Domain	Recorded by NSS on 8 Nov 2026; on no list NSS holds; behind a forwarding label
gltnorwx[.]vip	Domain	Recorded by NSS on 8 Nov 2026; on no list NSS holds; behind a forwarding label
hccooup[.]vip	Domain	Recorded by NSS on 8 Nov 2026; on no list NSS holds; behind a forwarding label
igpjflpz[.]vip	Domain	Recorded by NSS on 11 Nov 2026; on no list NSS holds;

		behind a forwarding label
kqclepov[.]vip	Domain	Recorded by NSS on 11 Nov 2026; on no list NSS holds; behind a forwarding label
kqqqhojh[.]vip	Domain	Recorded by NSS on 11 Nov 2026; on no list NSS holds; behind a forwarding label
03902i[.]com	Domain	Recorded by NSS on 4 Nov 2026; on no list NSS holds
1110571l[.]com	Domain	Recorded by NSS on 6 Nov 2026; on no list NSS holds
255571gg[.]com	Domain	Recorded by NSS on 4 Nov 2026; on no list NSS holds
255571mm[.]com	Domain	Recorded by NSS on 3 Nov 2026; on no list NSS holds
255571oo[.]com	Domain	Recorded by NSS on 3 Nov 2026; on no list NSS holds
277752aaa[.]com	Domain	Recorded by NSS on 3 Nov 2026; on no list NSS holds
45678a005[.]cc	Domain	Recorded by NSS on 4 Nov 2026; on no list NSS holds
45678a008[.]cc	Domain	Recorded by NSS on 4 Nov 2026; on no list NSS holds

0149tie[.]temawangtmw[.]com	Domain	On public lists; behind a forwarding label
2025tiaozhuan[.]gabdtz66[.]com	Domain	On public lists; behind a forwarding label
246-baidu260804[.]www01490267dd[.]com	Domain	On public lists; behind a forwarding label
251224001gwbd-tk[.]ou53t[.]com	Domain	On public lists; behind a forwarding label
251224002gwbd-tk[.]ou53t[.]com	Domain	On public lists; behind a forwarding label
33cfj-baidu260804q[.]jinbaobb[.]com	Domain	On public lists; behind a forwarding label
3sd3g-baidu260804q[.]bowenaa[.]com	Domain	On public lists; behind a forwarding label
aahgdop-baidu2026730z[.]014901490149y[.]com	Domain	On public lists; behind a forwarding label

FULL LIST CSV JSON

How we know

What this rests on

- Where each name resolves and what it forwards to is from one check of every name on 11 November 2026 between 12:04 and 12:06 UTC.
- Registration times and registrars are public registration records, read on 11 November 2026. A batch is five or more names from one registrar,

each within 30 seconds of the one before.

- The time from certificate log to NSS record compares the log's own timestamp with the time NSS stored the name, for the 73 names found that way.
- Page descriptions are from NSS captures of 21 sample names on 11 November 2026. The other 298 names were not captured for this paper.

What we cannot say

- NSS did not see who runs the sites, how visitors are sent to them, or whether anyone lost money.
- "On no list NSS holds" is not "on no list anywhere". NSS checked the lists it takes in, not every list that exists.
- The sets of names may or may not be the same people. They share a delivery network and a kind of page, and nothing else NSS could measure.
- Addresses are not in the indicator list. They are shared delivery-network addresses that serve other, unrelated sites.
- This paper is not attributed to any named group, and it does not rule on whether the sites are lawful where they are used.

Use and citation

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

```
Nexus Sentinel Station (NSS), "Lottery redirect names on a shared
delivery network: technical analysis", NSS-RH-01, 11 Nov 2026.
https://nsshq.com/research/redirect-host-clusters
```

See something wrong? corrections@nsshq.com

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