


Found by NSS

All 80 names recorded by NSS's own sensors; the first 51 a median of 18 h after registration

**Updated 16 Nov 2026.**

● Tracking since 28 Oct 2026 · Last checked 16 Nov 2026 · 1 update

# WhatsApp lookalike kit: technical analysis

Over three days in late October 2026, 51 domain names imitating WhatsApp were registered in three batches, each batch within a single minute. NSS recorded every one within 27 hours of its registration, tied the 51 together from public registration and hosting records, and read a copy of the WhatsApp sign-in page on 11 of them. This paper sets out what was observed, how the names were tied together, and what a defender can look for. Updated 16 November 2026: 29 more names since publication, and the relay behind them has moved to a new domain.

| PUBLISHED | LAST UPDATED | READING TIME | MARKING |
|---|---|---|---|
| 10 Nov 2026 | 16 Nov 2026 | 10 min | TLP:CLEAR |

16 NOV 2026

## Update, 16 November 2026: 29 more names, and the relay moved

The kit kept growing after this paper was published on 10 November, and the relay behind it moved to a new domain. Everything in this update was read from NSS's own records on 16 November 2026. The paper below this box is unchanged from 10 November; the items it supersedes are listed at the end.

### What changed

- **29 more names.** From 7 to 16 November, NSS recorded 29 more names of the same shape, tied to the kit by forwarding or address records: .top (9), .cyou (7), .icu (6), .cc (3), .shop (3) and .xyz (1). Most use new prefixes in front of the hyphen. Four were first recorded on 14 November, five on 15 November and one in the first hours of 16 November (UTC).
- **How they tie to the kit.** 23 of the 29 forward through the relay under their own label, as most of the first 51 did. The other six resolved to the same addresses, in the same days, as names already in the kit.
- **The relay moved to cname360[.]com.** The relay domain in this paper, 2027facai[.]com, carried 73 names in NSS's record from 26 October; its last forwarding record is on 12 November at 15:45 UTC. From 17:35 UTC the same day, the operator's labels answer under a new domain, cname360[.]com. Seven labels moved across unchanged, each still serving the same name, and on 14 November the hub label msc3nbqr, which the per-name labels point at, answered under the new domain too. By 16 November NSS had recorded 22 names under cname360[.]com: 13 of the new WhatsApp names and 9 names imitating crypto wallets and marketplaces.
- **The old domain went after the move.** 2027facai[.]com was gone from the .com zone by 14 November, about two days after the

operator had already moved off it.

- **The published names went quiet; the new ones did not.** NSS's record holds no answer for any of the 51 published names after 12 November, 15:45 UTC. On the morning of 16 November, 11 of the 29 new names answered, all from the same two addresses.
- **Still on no list.** On 16 November, none of the 80 names (the 51 published and the 29 new) and neither relay domain was on any threat list NSS takes in.
- **How NSS reads them.** Investigate holds casefiles on 26 of the 29 new names, the latest from 16 November. It reads each one Suspicious, and none has reached High. NSS has not read a sign-in page on them; they are in the kit by their records, as 40 of the first 51 were.

Each new name is a prefix, a hyphen, "vvhatsapp" and an ending, for example wevv-vvhatsapp[.]top:

| PREFIX | ENDINGS | FIRST RECORDED BY NSS |
|---|---|---|
| asc, asx | .shop | 7 Nov |
| wac | .cyou, .icu | 10 Nov |
| wae | .icu, .xyz | 10 Nov |
| vww | .cyou, .icu, .top | 11 to 12 Nov |
| vvww | .cyou, .top | 11 to 12 Nov |
| wwvv | .cyou, .top | 11 to 12 Nov |
| wwv | .shop, .top | 12 Nov |
| wnvv | .cyou, .cc, .icu, .top | 12 to 14 Nov |
| wevv | .icu, .top, .cyou, .cc | 13 to 14 Nov |
| wsvv | .icu, .top, .cyou, .cc | 15 to 16 Nov |
| wzvv, wavv | .top | 15 Nov |

### What to add to blocks

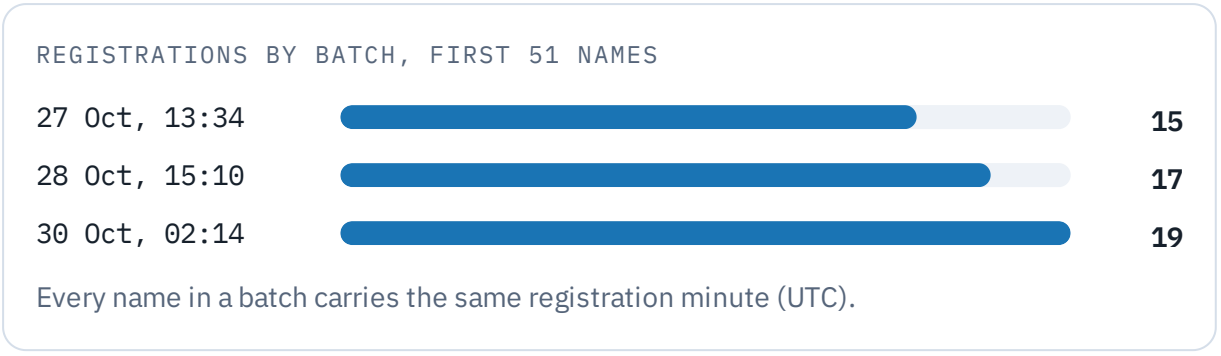
- The 29 new names. They are at the end of the indicator files (CSV, JSON and the STIX bundle on GitHub), each marked as added on 16 November with the time NSS first recorded it. The original rows are unchanged.
- **cname360[.]com, and every name that forwards through it.** Unlike the old relay domain, every name NSS recorded under it up to 16 November belongs to this kit or to the crypto lookalikes that moved with it, so a block on the domain reached no other customer NSS has seen.
- The relay label `msc3nbqr[.]cname360[.]com` as a pivot: any other name that points at it is a sibling.
- To look back through logs, search for names forwarding to labels under 2027facai[.]com from 26 October to 12 November, and under cname360[.]com from 12 November on.
- A pattern catches what the list cannot: three or four letters, a hyphen, then "vvhatsapp". From 6 to 13 November, 61 more names of that shape were registered and never resolved in NSS's record. They share no record with the kit, so they are not in the list, but a pattern rule covers them.

### What this update supersedes

- Under "What a defender can look for", the relay label `msc3nbqr[.]2027facai[.]com` now answers as `msc3nbqr[.]cname360[.]com`. The old row stays in the indicator list for searches of logs up to 12 November.
- The body says the relay domain is not an indicator on its own because the relay has other customers. That held for 2027facai[.]com, which carried other names; it does not hold for cname360[.]com, which is why the new domain is in the list.
- The key findings, the numbers at a glance for the first 51 names and the timeline rows up to 10 November describe the kit as published,

and are kept as they were.

| 80 | 3 | 11 | 18 h |
|---|---|---|---|
| lookalike names tied to the kit by 16 Nov (51 at publication) | registration minutes for the first 51 | names where NSS read the sign-in copy | median from registration to first NSS record (first 51) |




## Key findings

1. 51 names share one pattern: three letters, a hyphen, then "vvhatsapp" (two letters v standing in for the w), under four endings: .cyou (16), .top (16), .icu (10) and .shop (9).
2. All 51 were registered in three single minutes: 15 names at 13:34 UTC on 27 October, 17 at 15:10 on 28 October and 19 at 02:14 on 30 October 2026.
3. 41 of the names forwarded through one relay service, each under its own label, and 33 of those labels pointed on to the same single label behind them.
4. NSS read a copy of the WhatsApp sign-in page, with a code to scan, on 11 of the names. On the real WhatsApp Web, scanning that code with a phone links the phone's account to the browser showing it, so a copy on a lookalike name is the shape of account-takeover phishing.
5. On 20 names the site blocked a phone visitor while serving a page to a desktop visitor. Seven names showed a search engine's home page in

place of their own.

6. NSS rated 47 of the 51 High risk at some point between 28 October and 5 November.

7. The set was short-lived. At least 19 names were put on hold by the registry. On 10 November, 34 of the 51 no longer resolved at all and 8 still reached a live address.

## Timeline

**27 Oct, 13:34 UTC**
First batch registered: 15 names in one minute.

**28 Oct, 07:21 UTC**
NSS records the first name, under 18 hours after its registration.

**28 Oct, 15:10 UTC**
Second batch registered: 17 names in one minute.

**28 Oct, 16:41 UTC**
First High risk verdict on a name in the set.

**29 Oct, 06:13 UTC**
NSS reads a WhatsApp sign-in copy, with a code to scan, on a name in the set.

**30 Oct, 02:14 UTC**
Third batch registered: 19 names in one minute.

**31 Oct, 04:55 UTC**
NSS records the last of the 51 names. Every name was recorded within 27 hours of its registration.

**2 Nov**
Investigate reports the 51 names as one kit.

**10 Nov, 23:00 UTC**
34 of the 51 no longer resolve. 17 still forward to the relay; 8 of those reach a live address.

**7 to 16 Nov**

Update: NSS records 29 more names of the same shape tied to the kit, four of them on 14 November.

**12 Nov, 17:35 UTC**
Update: the relay's labels start answering under a new domain, cname360[.]com. The last forwarding record under 2027facai[.]com was at 15:45 UTC.

**14 Nov**
Update: 2027facai[.]com is gone from the .com zone, two days after the move.

**16 Nov**
Update published. None of the 80 names, and neither relay domain, is on any threat list NSS takes in.

## How the names were tied together

A name pattern is not proof. Anyone can register a name that looks like another, and a lookalike name that shared no record with the set stayed out of it. NSS joined a name to the kit only when it shared a public record with a name already in it. Five kinds of link were used:

| LINK | WHAT IT MEANS |
|---|---|
| Same registrar, same registration minute | Names bought together in one order |
| Same address, registered close together | Names set up together on one host |
| Same address, same registrar | Names bought and hosted the same way |
| Same address, switched on close together | Names switched on together |
| Same relay | Names placed behind the same forwarding service, on the same label |

The registration minute is the strongest of these. All 51 names fall in three minutes: 13:34 UTC on 27 October, 15:10 on 28 October and 02:14 on 30

October. The registration records name two registrars, Global Asset Domains Inc. for 42 names and Gname[.]com Pte. Ltd. for 9, and the first two batches include names from both in the same minute.

The relay is the second. 41 of the names forwarded through one relay service, each under its own label. 33 of those labels pointed on to a single label behind them, `msc3nbqr[.]2027facai[.]com`. The relay is a service with other customers, so its domain is not an indicator on its own. The single label is useful: any other name that forwards to it is worth a look.

One record was set aside. The names use the same pair of name servers, but it is a default pair that many unrelated customers share. NSS did not count that as a link.

## What the sites served

On 11 names NSS read the page. It was a copy of the WhatsApp sign-in page: a code to scan, the WhatsApp logo, and sign-in wording naming WhatsApp, on a name that is not WhatsApp's. Seven of the names carried the page title `wa-logo`. A visitor who scans a code on such a page can hand their session to whoever runs the site.

On the other names NSS did not read a sign-in page, and the paper does not claim one was there. What NSS recorded instead:

- On 20 names the phone view was blocked while the desktop view served a page.
- Seven names showed a search engine's home page in place of their own content.
- Three names showed the relay's "domain not configured" page and three its "access blocked" page.

A blocked or swapped page on a name that copies a brand is recorded as a finding in its own right. NSS does not treat an unread page as a clean one.

## What a defender can look for

- New registrations that put a short prefix and a hyphen in front of a misspelt brand name, several in the same minute, under low-cost endings.
- Names that forward to the relay label `msc3nbqr[.]2027facai[.]com`. (Superseded 16 November 2026: the label now answers as `msc3nbqr[.]cname360[.]com`. See the update at the top.)
- A sign-in page copy with the title `wa-logo`.
- A site that blocks a phone visitor and serves a desktop visitor, or shows a search engine's home page under a brand lookalike name.
- The indicator list below. Most of the names no longer resolve, so the list is of most use for looking back through logs from 27 October to 10 November 2026.

## The NSS tools used

**> Discovery**
Recorded each name through NSS's own sensors. All 51 were recorded within 27 hours of registration; the median was 18 hours.

**> Investigate**
Built a casefile on each name: registration, name servers, addresses, forwarding, certificates and the page each name served. Every name was re-checked throughout.

**> Kit grouping**
Joined the names on shared public records and reported the kit as one finding, with its members and the record that joined each.

**> Brand**
Listed the set under the brand it copies, apart from the brand's own domains.

**> Watch**
Re-checked the kit and recorded when names changed address, went on hold or stopped resolving.

## Indicators

The first 25 of 83 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 |
|---|---|---|
| occ-vvhatsapp[.]cyou | Domain | Registered 27 Oct 13:34 UTC; WhatsApp sign-in copy read by NSS |
| occ-vvhatsapp[.]shop | Domain | Registered 27 Oct 13:34 UTC; WhatsApp sign-in copy read by NSS |
| occ-vvhatsapp[.]top | Domain | Registered 27 Oct 13:34 UTC; WhatsApp sign-in copy read by NSS |
| oce-vvhatsapp[.]cyou | Domain | Registered 27 Oct 13:34 UTC; WhatsApp sign-in copy read by NSS |
| oce-vvhatsapp[.]shop | Domain | Registered 27 Oct 13:34 UTC; WhatsApp sign-in copy read by NSS |
| oce-vvhatsapp[.]top | Domain | Registered 27 Oct 13:34 UTC; WhatsApp sign-in copy read by NSS |
| ocz-vvhatsapp[.]shop | Domain | Registered 27 Oct 13:34 UTC; WhatsApp sign-in copy read by NSS |
| esx-vvhatsapp[.]cyou | Domain | Registered 28 Oct 15:10 UTC; WhatsApp sign-in copy read by NSS |
| esx-vvhatsapp[.]shop | Domain | Registered 28 Oct 15:10 UTC; WhatsApp sign-in copy read by NSS |
| esz-vvhatsapp[.]cyou | Domain | Registered 28 Oct 15:10 UTC; WhatsApp sign-in copy read by NSS |
| esz-vvhatsapp[.]top | Domain | Registered 28 Oct 15:10 UTC; WhatsApp sign-in copy read by NSS |
| ccs-vvhatsapp[.]cyou | Domain | Registered 27 Oct 13:34 UTC |
| ccs-vvhatsapp[.]shop | Domain | Registered 27 Oct 13:34 UTC |
| ccs-vvhatsapp[.]top | Domain | Registered 27 Oct 13:34 UTC |
| ocs-vvhatsapp[.]cyou | Domain | Registered 27 Oct 13:34 UTC |

| | | |
|---|---|---|
| ocs-vvhatsapp[.]shop | Domain | Registered 27 Oct 13:34 UTC |
| ocs-vvhatsapp[.]top | Domain | Registered 27 Oct 13:34 UTC |
| ocz-vvhatsapp[.]cyou | Domain | Registered 27 Oct 13:34 UTC |
| ocz-vvhatsapp[.]top | Domain | Registered 27 Oct 13:34 UTC |
| esa-vvhatsapp[.]cyou | Domain | Registered 28 Oct 15:10 UTC |
| esa-vvhatsapp[.]shop | Domain | Registered 28 Oct 15:10 UTC |
| esa-vvhatsapp[.]top | Domain | Registered 28 Oct 15:10 UTC |
| esc-vvhatsapp[.]cyou | Domain | Registered 28 Oct 15:10 UTC |
| esc-vvhatsapp[.]icu | Domain | Registered 28 Oct 15:10 UTC |
| esc-vvhatsapp[.]top | Domain | Registered 28 Oct 15:10 UTC |

ALL 83 INDICATORS: CSV JSON also on GitHub No sign-up.

## How we know

### What this rests on

- Registration times and registrars are public registration records, read at the time of each casefile.
- Forwarding and addresses are what each name resolved to at the time of each casefile, and again on 10 November 2026 at 23:00 UTC.
- The sign-in copy was read by NSS on 11 names. The other 40 are in the kit by the records that join them, not by a page.
- Counts are of names unless a line says otherwise.
- Update of 16 November 2026: the 29 added names, their forwarding and the relay move are from NSS's own records, read on 16 November; listing state and live answers were checked the same day.

### What we cannot say

- NSS did not see who runs the sites, how visitors were sent to them, or whether anyone was harmed.
- 40 of the 51 names are tied by registration and hosting records only.
- NSS has not read a sign-in page on the 29 names added on 16 November; they are in the kit by forwarding and address records. Their registration minutes were not read, so they are dated by when NSS first recorded each.
- Addresses are not in the indicator list. The names sat behind a relay whose addresses serve other, unrelated sites, and blocking them would block those too.
- This paper is not attributed to any named group.

## Use and citation

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

```
Nexus Sentinel Station (NSS), "WhatsApp lookalike kit: technical
analysis", NSS-WA-01, 10 Nov 2026. https://nsshq.com/research/whatsapp-
lookalike-kit
```

See something wrong? corrections@nsshq.com

Related topics: Lookalike domains How NSS confirms infrastructure

---

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