

Expanded by NSS

27 names from a public report of 16 Nov 2026, enriched and expanded to 110 by NSS; the 83 siblings are NSS's own discovery by registration record

Tracking since 19 Nov 2026 · Last checked 19 Nov 2026

Are the IOCs You Were Sent Actually IOCs? 110 domains, scored low, wired for mail

A public writeup on 16 November 2026 shared 27 typosquat domains as indicators of compromise. Pasted into a tool to triage, most score low or are absent, and every one is parked, so the list looks dismissible. Enrichment tells a different story. A single, still-active operator is running a one-letter-edit campaign of at least 110 names across two registrars, a shared nameserver pair and one parking pool. On the web every name is a dormant park; in the mail records every name has a working mail server already wired on dedicated infrastructure, staged for a benefit, rebate, claims or class-action settlement notification email. And 108 of the 110, every one of the 83 we add, are in no feed we ingest. A low score on a bare indicator is where the work starts, not where it ends.

PUBLISHED	LAST UPDATED	READING TIME	MARKING
19 Nov 2026	19 Nov 2026	11 min	TLP:CLEAR

110
lookalike domains in the operator set, 83 of them unreported and confirmed by NSS (a roughly four-fold expansion of the public 27)

108 of 110
in no feed or list NSS ingests: the public report surfaced 2 of the operation

110 of 110
parked on the web yet mail-provisioned on dedicated infrastructure off the parking pool

81
of the 110 registered in November 2026 at a steady 4 to 19 a day, the campaign still growing

Key findings

1. A public report of 16 November 2026 shared 27 typosquat domains as IOCs and did the valuable part: without it none of these names would be on anyone's radar. On a first-pass check 25 of the 27 are absent from our data and the other 2 are present only because we ingested the report's own feed, and every one is parked on a shared bulk pool. A bare, dormant domain correctly scores low; that is the hook, not the conclusion.
2. Enriched against public registration, DNS and mail records, the full operator set is parked on the web but wired for mail: every name resolves to the same four parking addresses with no live page, yet every name designates a working mail server on dedicated infrastructure off the parking pool. The mail host is a commodity provider, not a fingerprint by itself; the uniformity is, a mail channel stood up on every name while the storefront stays blank.
3. Each lookalike is a one-letter edit of a brand's genuine new domain, registered about a day after the brand registered the real name through a corporate brand-protection registrar. Confirmed on six brand pairs, each a plus-one-day registration against a CSC or MarkMonitor original.

4. Using the operator's signature we confirmed by registration record 83 further names not in the report, bringing the set to 110, a roughly four-fold expansion, in two strands: brand benefit and rewards portals, and class-action settlement-administrator lookalikes. The run is months old and accelerating, with names registered the same week this note was written.
5. We have it ahead of the feeds. Of the 110, only 2 appear in any feed or list NSS ingests, the pair the report named; the other 108 are absent from every feed we take in. Other vendors' private telemetry may hold them; across the public and commercial sources we ingest, the public report surfaced 2 of a 110-name operation.

The list that looked ignorable

A public writeup on 16 November 2026 shared 27 typosquat domains as indicators of compromise, "Typosquatters Copy Big Brands' New Domains Within a Day of Registration" (Symantec, via security[.]com). That report did the valuable part: without it, none of these names would be on anyone's radar. Credit where it is due.

Now stand at the receiving end. A defender pastes those 27 domains into a tool to triage them, and this is what comes back:

- **25 of the 27 do not appear in our data at all.** No verdict, no sightings. Unknown, which reads as low risk.
- **The other 2** (carmaxclaim[.]com, kmxclaim[.]com) are present only because we ingested this report's own feed on 16 November, with zero independent sightings and no detection of our own.
- **Every one of them is parked** on the web: all point at a shared bulk parking pool that also holds thousands of unrelated typosquats. No live page, nothing to score. A bare, dormant domain correctly scores low.

So the honest first-pass answer is that the list looks dismissible. And we will own the uncomfortable part up front: our own NSS Daily Ledger ships

raw indicators every day and says so plainly, "not enriched or vetted." Raw distribution is legitimate and useful. But a low score on a bare indicator is not a conclusion. It is where the work starts.

A note on the word IOC

It is worth asking a plain question of any daily threat or ISAC report that lands in your inbox: are the IOCs in it actually IOCs? An indicator of compromise is, by the term's own definition, forensic evidence that a compromise has occurred, an artifact seen in a real intrusion: a file hash pulled from live malware, an address a victim's machine actually reached, a header from a phishing message that actually arrived. Measured against that, a freshly registered, parked lookalike that has compromised no one is not an indicator of compromise. It is an indicator of preparation. That distinction is not pedantry; it is exactly why these names score low: they are being read as evidence of an attack that has not happened yet. Our own NSS Daily Ledger publishes names like these every day under the heading of indicators, and states plainly that they are not enriched or vetted, so we hold the point against our own output too. Attaching the label is the easy part. Working out which stage an indicator really belongs to, preparation, delivery, or an actual compromise, is the enrichment this note is about.

The finding: parked on the web, wired for mail

Enrichment of the full operator set (below) over public DNS gives the result that the web score hides:

- **The web face is dormant.** All of the campaign's domains resolve to the same four parking addresses. None has moved to dedicated web hosting. On the web alone, every single one looks like the 27 did: ignorable.
- **The mail channel is wired.** Every domain designates a working mail server (an MX record) on dedicated infrastructure off the parking pool. The mail host is a commodity provider that unrelated domains also use,

so, like the shared nameservers and the parking pool, it is not an operator fingerprint by itself. What is notable is the uniformity: while the storefront sits empty, the operator has configured mail on every one of its names.

That is the point of the whole note. For a campaign built on fake benefit, rebate, claims and class-action settlement themes, the natural vector is a notification email ("your settlement payment is ready," "confirm your benefit enrollment"), and the parked lookalike is only the landing page such an email would point to. The mail channel is already configured on every name while the pages that would trip a scanner stay blank. A web-only verdict sees a dormant park; the mail records show an operation with its mail channel already stood up. (An MX record proves the channel is configured and can receive mail; it does not by itself prove the operator can send cleanly, and here the sender-authentication record is only a non-working placeholder, so the set reads as staged, not yet firing. That staging is exactly the window in which a low web score is most misleading.)

What enrichment shows about the operator

The uniformity is the fingerprint:

- **Two registrars only:** Cloud Yuqu LLC (IANA 3824, 98 of 110) and Chengdu West Dimension Digital Technology (IANA 1556, 12 of 110). The operator carried the older names on Chengdu and moved almost entirely to Cloud Yuqu for the November scale-up (78 of the 81 November names).
- **One nameserver pair** and **one parking pool** (four addresses) across the set, and **one shared mail host** for every MX.
- **A sustained, accelerating run:** 29 names from July, August and October; 81 registered in November at a steady 4 to 19 a day; 8 on 18 November and **9 today, 19 November.** Months old, surging now, still going.

The technique, confirmed

Each lookalike is a one-letter edit of a brand's genuine new domain, registered about a day after the brand registered the real name through a corporate brand-protection registrar (CSC or MarkMonitor). Confirmed on six pairs:

AUTHENTIC DOMAIN (BRAND-PROTECTION REGISTRAR)	CREATED	OPERATOR ONE-LETTER EDIT	CREATED	GAP
greystarbenefits[.]com (CSC)	25 Aug	greystarbenfits[.]com	26 Aug	+1 day
carmaxclaims[.]com (CSC)	26 Aug	carmaxclaim[.]com (dropped s)	27 Aug	+1 day
myolinhuntsmanbenefits[.]com (CSC)	26 Oct	myolinhuntsmanbenifits[.]com	27 Oct	+1 day
cortevapartnerconnect[.]com (MarkMonitor)	12 Nov	cortevapartnerconect[.]com (dropped n)	13 Nov	+1 day
resideoconnect[.]com (MarkMonitor)	13 Nov	resideoconect[.]com (dropped n)	14 Nov	+1 day
yourmsdbenefits[.]com (MarkMonitor)	11 Aug	yourmsdbenefit[.]com	12 Aug	+1 day

The edits stay readable: a dropped plural "s," a single missing letter, a collapsed double letter. The operator watches the registrars that signal "a large company cares about this name," then registers the twin before the public ever sees the real one.

What the list did not include

The 27 are one slice. Using the operator's full signature (the two registrars + the shared nameservers + the parking pool + the one-letter-edit grammar), we confirmed by registration record **83 further names not in the report, bringing the operator set to 110, a roughly four-fold expansion of the published list.** It runs in two strands:

- **Brand benefit and rewards portals** (about 65): savings, rebate, claims, sweepstakes and member portals for named consumer and employer brands, including Greystar, CarMax, Merck/MSD, Olin Huntsman, McDonald's, Aetna, Corteva, Resideo, Carnival, World Hotels, SoloFunds and Honda.
- **Class-action settlement-administrator lookalikes** (45 of 110): typosquats of the domains that administer data-breach, TCPA and fee settlements, where a victim fully expects an email telling them to file a claim. One data-breach settlement name is squatted in seven spelling variants, another in five.

And we have it ahead of the feeds. Of the 110, only 2 appear in any feed or list NSS ingests, the carmaxclaim pair, and only via the 16 November report. The other 108, every one of the 83 siblings, are absent from every feed we take in. Other vendors' private telemetry may hold them; what we can state is that across the many public and commercial sources we ingest, 108 of the 110 are not listed. The public report surfaced 2 of a 110-name operation.

Why it matters

- Do not triage brand lookalikes on first-pass web score alone. A parked lookalike registered one day after a brand-protection registration, with mail already wired to dedicated infrastructure, is a staged asset, not a benign park.
- Watch the mail records, not just the web. A dormant web page paired with live, dedicated MX on a claims or benefits themed lookalike is mail configured to carry a notification campaign, not a benign park.

- Block on the operator pattern, not the 27 names. The campaign is still registering daily; a static list is stale the day it ships.
- If you register campaign domains through CSC or MarkMonitor, watch for next-working-day one-letter variants at Cloud Yuqu (IANA 3824) and Chengdu West Dimension (IANA 1556).

Scope and method

The campaign and the original 27 indicators are Symantec's public reporting, credited. Our contribution is the finishing work: scoring the list, enriching it against public registration, DNS, mail and certificate records, confirming the technique, discovering the unreported remainder, and establishing that the operation is mail-provisioned and still growing. Indicators are defanged here; the full per-name table (all 110, each with registrar, creation date, strand and status) ships as CSV, JSON, STIX 2.1 and MISP alongside this note.

Shared indicators are a gift. Intelligence is what you do with them.

The NSS tools used

> Investigate
Scored each of the 27 reported names and read its casefile: the registration record, the DNS and mail records, and the listing state.

> Scan
Re-read each name's verdict to agree with Investigate, and confirmed every name is parked on the web while its mail records are live.

> Tools
Chained public registration, DNS and mail lookups over the operator's signature, each step feeding the next, to confirm the unreported siblings.

> Family finder
Grouped the 110 names by the shared registrar, nameserver pair, parking pool and one-letter-edit grammar, and stated plainly where names share only a shape.

> Hunt

Searched NSS's library for the campaign and set every name against every feed NSS ingests to establish what is and is not already listed.

Indicators

The first 25 of 110 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
carmaxclaim[.]com	Domain	Operator lookalike (brand benefit/rewards portal strand); registered 27 Aug 2026 at Cloud Yuqu LLC (IANA 3824); parked on the shared pool, mail-provisioned (MX on dedicated off-pool infrastructure); in the reported set
kmxclaim[.]com	Domain	Operator lookalike (brand benefit/rewards portal strand); registered 27 Aug 2026 at Cloud Yuqu LLC (IANA 3824); parked on the shared pool, mail-provisioned (MX on dedicated off-pool infrastructure); in the reported set
aildatasettlment[.]com	Domain	Operator lookalike (class-action settlement-administrator strand); registered 6 Aug 2026 at Cloud Yuqu LLC (IANA 3824); parked on the shared pool, mail-provisioned (MX on dedicated off-pool infrastructure); in the reported set
mypgsweep[.]com	Domain	Operator lookalike (brand benefit/rewards portal strand); registered 6 Aug 2026 at Chengdu West Dimension Digital Technology (IANA 1556); parked on the shared pool, mail-provisioned (MX on

		dedicated off-pool infrastructure); in the reported set
ontherockrebate[.]com	Domain	Operator lookalike (brand benefit/rewards portal strand); registered 6 Aug 2026 at Cloud Yuqu LLC (IANA 3824); parked on the shared pool, mail-provisioned (MX on dedicated off-pool infrastructure); in the reported set
asrelbisaving[.]com	Domain	Operator lookalike (brand benefit/rewards portal strand); registered 7 Aug 2026 at Chengdu West Dimension Digital Technology (IANA 1556); parked on the shared pool, mail-provisioned (MX on dedicated off-pool infrastructure); in the reported set
fyzadasaving[.]com	Domain	Operator lookalike (brand benefit/rewards portal strand); registered 7 Aug 2026 at Chengdu West Dimension Digital Technology (IANA 1556); parked on the shared pool, mail-provisioned (MX on dedicated off-pool infrastructure); in the reported set
healthspringproducer[.]com	Domain	Operator lookalike (brand benefit/rewards portal strand); registered 7 Aug 2026 at Cloud Yuqu LLC (IANA 3824); parked on the shared pool, mail-provisioned (MX on dedicated off-pool infrastructure); in the reported set
ijornisavings[.]com	Domain	Operator lookalike (brand benefit/rewards portal strand); registered 7 Aug 2026 at Chengdu West Dimension Digital Technology (IANA 1556); parked on the shared pool, mail-provisioned (MX on dedicated off-pool infrastructure); in the reported set

arlocareheath[.]com	Domain	Operator lookalike (brand benefit/rewards portal strand); registered 8 Aug 2026 at Cloud Yuqu LLC (IANA 3824); parked on the shared pool, mail-provisioned (MX on dedicated off-pool infrastructure); in the reported set
hithebeamsweeps[.]com	Domain	Operator lookalike (brand benefit/rewards portal strand); registered 11 Aug 2026 at Cloud Yuqu LLC (IANA 3824); parked on the shared pool, mail-provisioned (MX on dedicated off-pool infrastructure); in the reported set
mywayconect[.]com	Domain	Operator lookalike (brand benefit/rewards portal strand); registered 11 Aug 2026 at Chengdu West Dimension Digital Technology (IANA 1556); parked on the shared pool, mail-provisioned (MX on dedicated off-pool infrastructure); in the reported set
sunharbosaving[.]com	Domain	Operator lookalike (brand benefit/rewards portal strand); registered 12 Aug 2026 at Cloud Yuqu LLC (IANA 3824); parked on the shared pool, mail-provisioned (MX on dedicated off-pool infrastructure); in the reported set
tradealgotcpassettlement[.]com	Domain	Operator lookalike (class-action settlement-administrator strand); registered 12 Aug 2026 at Cloud Yuqu LLC (IANA 3824); parked on the shared pool, mail-provisioned (MX on dedicated off-pool infrastructure); in the reported set
tradealgotcpsettlement[.]com	Domain	Operator lookalike (class-action settlement-administrator strand); registered 12 Aug 2026 at Chengdu West Dimension Digital

		Technology (IANA 1556); parked on the shared pool, mail-provisioned (MX on dedicated off-pool infrastructure); in the reported set
youmsdbenefits[.]com	Domain	Operator lookalike (brand benefit/rewards portal strand); registered 12 Aug 2026 at Chengdu West Dimension Digital Technology (IANA 1556); parked on the shared pool, mail-provisioned (MX on dedicated off-pool infrastructure); in the reported set
yourmsdbenefit[.]com	Domain	Operator lookalike (brand benefit/rewards portal strand); registered 12 Aug 2026 at Cloud Yuqu LLC (IANA 3824); parked on the shared pool, mail-provisioned (MX on dedicated off-pool infrastructure); in the reported set
yourmsdbenifits[.]com	Domain	Operator lookalike (brand benefit/rewards portal strand); registered 12 Aug 2026 at Cloud Yuqu LLC (IANA 3824); parked on the shared pool, mail-provisioned (MX on dedicated off-pool infrastructure); in the reported set
getpgsoffer[.]com	Domain	Operator lookalike (brand benefit/rewards portal strand); registered 13 Aug 2026 at Cloud Yuqu LLC (IANA 3824); parked on the shared pool, mail-provisioned (MX on dedicated off-pool infrastructure); in the reported set
celmodpharmacy[.]com	Domain	Operator lookalike (brand benefit/rewards portal strand); registered 14 Aug 2026 at Cloud Yuqu LLC (IANA 3824); parked on the shared pool, mail-provisioned

		(MX on dedicated off-pool infrastructure); in the reported set
mcdonaldmedianetwork[.]com	Domain	Operator lookalike (brand benefit/rewards portal strand); registered 14 Aug 2026 at Cloud Yuqu LLC (IANA 3824); parked on the shared pool, mail-provisioned (MX on dedicated off-pool infrastructure); in the reported set
aveirwirless[.]com	Domain	Operator lookalike (brand benefit/rewards portal strand); registered 18 Aug 2026 at Cloud Yuqu LLC (IANA 3824); parked on the shared pool, mail-provisioned (MX on dedicated off-pool infrastructure); in the reported set
insulinsavingprogram[.]com	Domain	Operator lookalike (brand benefit/rewards portal strand); registered 19 Aug 2026 at Cloud Yuqu LLC (IANA 3824); parked on the shared pool, mail-provisioned (MX on dedicated off-pool infrastructure); in the reported set
ukvaluestudy[.]com	Domain	Operator lookalike (brand benefit/rewards portal strand); registered 21 Aug 2026 at Cloud Yuqu LLC (IANA 3824); parked on the shared pool, mail-provisioned (MX on dedicated off-pool infrastructure); in the reported set
greystarbenfits[.]com	Domain	Operator lookalike (brand benefit/rewards portal strand); registered 26 Aug 2026 at Cloud Yuqu LLC (IANA 3824); parked on the shared pool, mail-provisioned (MX on dedicated off-pool infrastructure); in the reported set

ALL 110 INDICATORS: CSV JSON also on GitHub No sign-up.

Check an indicator from this paper

How we know

What this rests on

- Registration records (registrar, IANA registrar id and creation day) are public registration data read by NSS on 19 November 2026.
- The web posture is a fresh look-up of every name on 19 November 2026 over two independent public resolvers; all 110 resolved to the same four parking addresses.
- The mail posture is each name's public MX record, read the same day; all 110 designate the same mail host, which resolves to dedicated addresses off the parking pool. An MX record proves the mail channel is configured and can receive mail; it does not by itself prove the operator can send cleanly, and the sender-authentication record is only a non-working placeholder.
- The six technique pairs are public registration records: the authentic domain at a brand-protection registrar and the operator's one-letter edit, with each creation day and the gap between them.
- The listing state was checked on 19 November 2026 against every feed and list NSS ingests. Only the two reported names were present, and only via the 16 November report's own feed.

What we cannot say

- "In no feed NSS ingests" is not "on no list anywhere". Other vendors' private telemetry may hold these names; the claim is scoped to the many public and commercial sources NSS takes in.
- An MX record shows the mail channel is configured and can receive mail. It does not prove the operator can send cleanly: here the sender-authentication record is a non-working placeholder, so the set reads as staged, not yet firing.

- The shared mail host is a commodity provider that unrelated domains also use. Like the shared nameservers and the parking pool it is not an operator fingerprint by itself; the operator signature is the whole stack, and the mail host's uniformity across the set is what is notable.
- The strand of each name (brand portal or settlement administrator) is read from the name and the brand it imitates, not from any live page: every name is parked, so no lure content was seen.
- The 110 are a floor, confirmed by registration record against the operator's grammar; broader spelling variants would add more. Parked and mail-provisioned is the posture on 19 November 2026 and can change as names activate.
- NSS records infrastructure. It holds no victim data and makes no claim about who has received any message or who operates the campaign; NSS names no actor.

Use and citation

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

```
Nexus Sentinel Station (NSS), "Are the IOCs You Were Sent Actually IOCs?
110 domains, scored low, wired for mail", NSS-EN-01, 19 Nov 2026.
https://nsshq.com/research/iocs-you-were-sent
```

What you can do with this

Check one of these now. Paste any indicator from the list above into the NSS check. You get the band, the host type and the reasons at once, no account needed.

Use this in your tools. Pull verdicts into your SIEM or SOAR today via JSON or CSV.

See something wrong? corrections@nsshq.com

More from NSS Research

NSS-AX-01: 24 additional ARTEX consoles live on 14 November 2026, and the reseller layer behind them: a companion to the FBI FLASH

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

NSS-TL-01: One wallet-phishing operator, six servers in three weeks: followed by the names it carried host to host

---

The campaign and the original 27 indicators are the public reporting of Symantec (via security.com), credited; NSS's contribution is the enrichment, the confirmed technique, the discovery of the unreported remainder and the finding that the set is mail-provisioned and still growing. NSS is not affiliated with Symantec or security.com, with the brands and settlement administrators whose names are imitated, or with any registrar, hosting company, DNS service, mail host or network behind the names in this paper. They are named because the public records name them; nothing here says any of them knew of or took part in the activity. NSS names no actor and makes no country-of-origin claim. NSS-EN-01 is NSS's own name for this case.