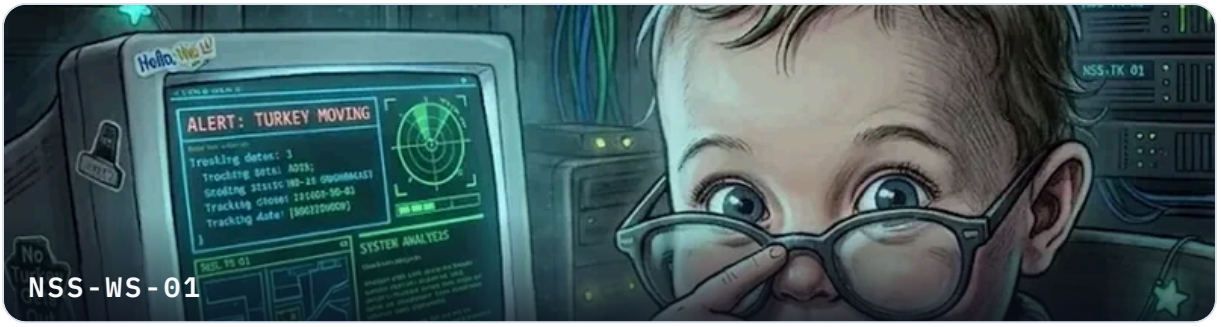


Found by NSS

Both operators were found by NSS in its own data, reported by NSS, and tracked through the operator's next move; the takedown correspondence and the dated resolution history are NSS's own records

Tracking since 14 Nov 2026 · Last checked 19 Nov 2026

We see you, Baby! We reported two operators, both were knocked offline, and we tracked what they did next

NSS does not publish an indicator and move on. When a lure is reported and knocked offline, the operator moves, and the value is catching the next move. This is a follow-up in the NSS-ZM-01 fake-Zoom line: NSS found a fake Zoom lure, reported it to the host it ran on, the host suspended the account, and within about a day the operator kept the same domain and re-pointed it to another rented host and re-staged a lure, which NSS tracked the whole way. Alongside it, a Telegram account-takeover generator: NSS reported it to its registrar, and of all 993 generated names the registry held exactly the two NSS had captured serving the kit, and nothing else. The operator's only durable asset is the domain. Reporting it once

is a snapshot; tracking the domain is the product. Do not retire an indicator the day it is knocked offline: the operator may be back on new infrastructure within a day.

PUBLISHED	LAST UPDATED	READING TIME	MARKING
20 Nov 2026	20 Nov 2026	12 min	TLP:CLEAR

2 of 993
Telegram generated names the registry held: exactly the two NSS had captured serving the kit, and nothing else

about 1 day
from the fake Zoom host being suspended to the operator re-pointing the same domain to another rented host

163 to 169 to 163
the fake Zoom domain's dated resolution path across two rented hosts, tracked in NSS's own passive DNS

36
Telegram names parked at 0.0.0.0 right now: dormant, not dead, still registered and reactivatable

Key findings

1. The host was suspended after NSS reported it; the operator kept the domain and re-pointed it to another rented host within a day. NSS reported the live fake Zoom update and join-meeting lure meeting-zoom-room[.]online (then on the HostAfrica host 169.239.181[.]96) to that host's abuse desk; the host confirmed on 18 Nov 2026 06:21 UTC that it had suspended the account (ticket 0013116, "We have suspended the domain name"). By 19 Nov 15:58:08 UTC the operator had re-pointed the same name to 163.61.188[.]9 (a Bangladesh reseller pool) with new name servers. The suspension was a hosting-account action, not a registry one: the domain carries clientTransferProhibited only, never any registry hold. The lure went offline; the domain lived; the operator simply re-pointed it.

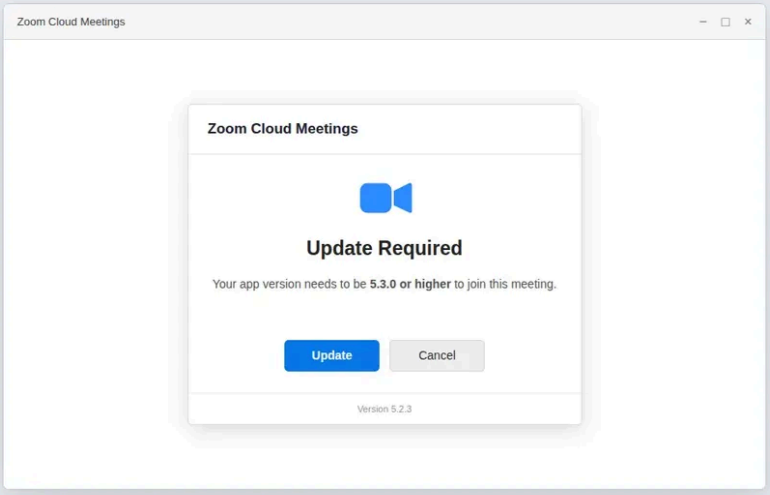
2. The operator's only durable asset is the domain, which is why host-level takedown is whack-a-mole. Neither address is the operator's: both are rented shared hosting, so co-residence ties nothing. The domain is one continuous registration (created 12 Nov 2026, never dropped, never re-registered), which is what makes this the same operator rather than a squatter grabbing a lapsed name. NSS's own resolution history shows the name on the Bangladesh host 12 to 13 Nov, on the South Africa host 14 to 18 Nov while it was live and reported, then back to the Bangladesh host on 19 Nov: the operator fell back to a rented host it had already staged on, fast and deliberate.

3. Of all 993 names in the Telegram generator, the registry held exactly the two NSS had captured serving, and nothing else. NSS reported the account-takeover kit to its registrar; on 19 Nov 2026 06:36:09 UTC the registrar placed a client hold on teleakflow[.]help and telealproi[.]click, the two names NSS had captured serving the live kit, at the same second in two different registries, while every sibling, including the label twin telealproi[.]help, stayed live. A full census of all 993 generated names confirms no broad registry wave landed: the live edge of 407 names is essentially intact two days on. The names NSS flagged as serving are the names that were held.

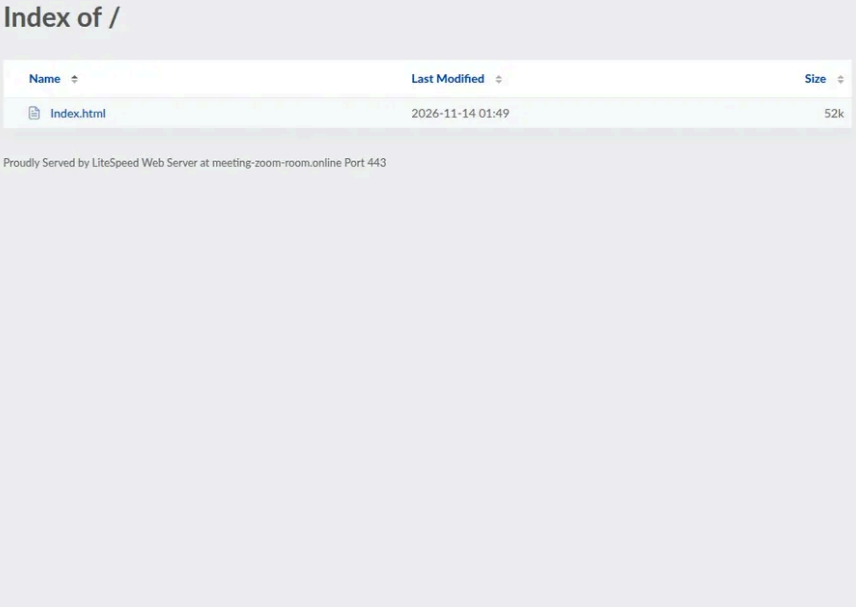
4. 0[.]0[.]0[.]0 is a dormancy flag, not a takedown, and both operators use it. The fake Zoom domain sat at 0[.]0[.]0[.]0 (a null route) from 17 to 19 Nov before the operator re-pointed it; 36 of the Telegram names sit at 0[.]0[.]0[.]0 right now, each still registered, in the zone, on the operator's content-network name servers and under no registry hold, so each is reactivatable in minutes. A domain at 0[.]0[.]0[.]0 is not dead; it is parked by the operator and can come back. That is exactly why you keep watching after an indicator goes quiet.

5. Both cases have a documented report-to-takedown chain, and together they are the two exits an operator takes. For Zoom, NSS reported the lure to its host on 14 Nov and the host confirmed suspension on 18 Nov (a hosting-account action). For Telegram, NSS reported the campaign to the registrar's abuse desk, both held names named in the thread, and

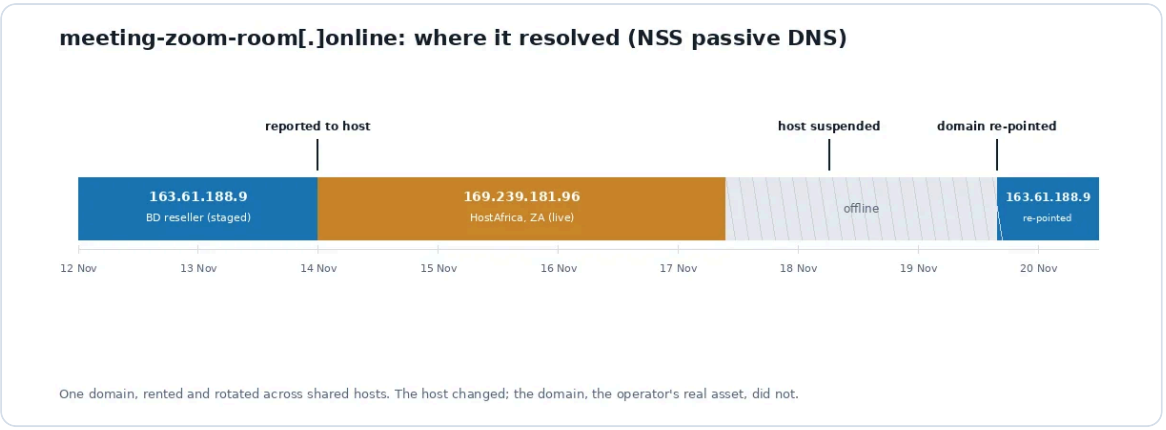
the registrar held exactly those two names on 19 Nov. The defensible claim is "we reported them, they were knocked offline", by the host for Zoom and by the registrar for Telegram, stated without overstating causation beyond the report-then-action sequence and the dates. A one-time report would have missed both the Zoom re-point and the fact that the held Telegram names were precisely the serving ones.



For comparison: the reference fake-Zoom lure from NSS-ZM-01 (a distinct earlier operator). The case in this paper is a separate lure in the same research line.



The re-pointed host captured through NSS's lane, 19 Nov 2026 22:10 UTC: an open directory staging one 52 KB lure file. The lure itself is gated (direct requests return 404s), so this listing, not a rendered page, is the evidence that a lure was re-staged.



The domain's real resolution path, as dated first-party data: Bangladesh (staging), to South Africa (live and reported), to Bangladesh again (re-pointed). The host changed twice; the domain never did.

Timeline

12 Nov 2026, 17:40 UTC
meeting-zoom-room[.]online registered, one continuous registration (Global Domain Group LLC).

12 to 13 Nov
The Zoom domain is staged on the Bangladesh reseller host 163.61.188[.]9 (NSS passive DNS).

14 Nov, 05:59 UTC
The fake Zoom lure goes live on the HostAfrica host 169.239.181[.]96; NSS flags it (High risk).

14 Nov
NSS reports the lure to HostAfrica (ticket 0013116).

16 Nov, 06:38 UTC
NSS's registrar abuse report for the Telegram generator is acknowledged; both later-held names are in the thread.

17 Nov, about 10:2x UTC

The Zoom lure goes dark; the HostAfrica host is null-routed (the domain points at 0[.]0[.]0[.]0).

18 Nov, 06:21 UTC
HostAfrica confirms it suspended the account (ticket 0013116).

19 Nov, 06:36:09 UTC
The registrar places a client hold on teleakflow[.]help and telealproi[.]click, the two captured serving names, at the same second in two registries; the siblings stay live.

19 Nov, 15:58:08 UTC
The same Zoom domain is re-pointed back to the Bangladesh reseller host 163.61.188[.]9.

19 Nov, 22:10 UTC
NSS captures the re-pointed host: an open directory staging a 52 KB lure file; the lure itself is gated (it returns 404s).

A report is a snapshot

Reporting an indicator once is table stakes. The value is what happens next. When a lure is reported and knocked offline, the operator does not stop; it moves. This note follows two operators on NSS's list through the two ways operators move, with a dated public record of both. It is a follow-up in the NSS-ZM-01 fake-Zoom line: the original documented a fake Zoom update kit that delivers a remote-access client, and this one follows one such lure through its whole life. (meeting-zoom-room[.]online is a distinct lure from the one in NSS-ZM-01, with no shared infrastructure and no same-operator claim between them; the continuity is the research line and the method.)

The fake Zoom lure: found, reported, knocked offline, re-pointed

NSS found meeting-zoom-room[.]online while it was live, serving a fake "Zoom - Update" page and then a "Zoom - Join Meeting" page (High risk on NSS, 14 Nov 2026). It ran on a HostAfrica shared server, 169.239.181[.]96.

NSS reported it to HostAfrica's abuse desk the same day (ticket 0013116). On 18 Nov at 06:21 UTC the host replied: "We have suspended the domain name." The lure went dark.

That is where a one-time indicator would end, and it would be wrong. The suspension was a hosting-account action, not a registry one. The domain itself was never touched: its registration record shows clientTransferProhibited only, no registry hold, one continuous registration created 12 Nov 2026 (registrar Global Domain Group LLC). So the host was dead, but the domain lived. By 19 Nov at 15:58:08 UTC the operator had re-pointed the same name to another rented host, 163.61.188[.]9 in Bangladesh, with new name servers, and re-staged a lure.

The domain is the asset; the host is disposable

This is why host-level takedown alone is whack-a-mole. Neither address the lure used is the operator's. 169.239.181[.]96 is a shared server on a mixed pool of unrelated tenants; 163.61.188[.]9 is a reseller pool, and the new name servers sit in that same pool, so the name-server change is just "moved to the reseller's shared DNS", not an operator signal. Because the hosts are shared, co-residence on them ties nothing together, and this paper claims no siblings from it. The one thing the operator keeps is the domain.

And the move was a fallback, not a fresh build. NSS's own resolution history has the domain on the Bangladesh host 12 to 13 Nov (pre-live staging), on the HostAfrica host 14 to 18 Nov (live and reported), then back on the Bangladesh host on 19 Nov. The operator returned to a rented host it had already staged on, within about a day of the suspension. A team that ingested the first address and marked it resolved at takedown would be holding a dead host while the domain ran on somewhere else.

What the re-pointed host serves now

Captured through NSS's own lane on 19 Nov at 22:10 UTC, the re-pointed host is a server whose web root is an open directory exposing one staged lure file (52,538 bytes, staged 14 Nov), under a wildcard certificate issued on the domain's creation day. The lure itself is gated: every direct request returns a 404, so it sits behind a campaign link or an anti-bot step that the original lure did not have. So a lure is confirmed re-staged, but its content could not be retrieved, and the deployment differs from the original NSS-ZM-01 lure. State it precisely: the same operator re-pointed the domain and re-staged a lure, now hardened against analysis, not the same kit relaunched verbatim. The added analysis gate is itself a finding: the operator is adapting.

The Telegram kit: the registry held exactly the two serving names

The second operator runs a generator of Telegram account-takeover names (the "tele" family). NSS captured two of them serving the live takeover kit, teleakflow[.]help and telealproi[.]click, and reported the campaign to the registrar's abuse desk (Chengdu West Dimension), both names in the thread. On 19 Nov at 06:36:09 UTC the registrar placed a client hold on exactly those two names, at the same second, in two different registries (.help and .click), while every sibling stayed live, including telealproi[.]help, the label twin of the held .click name.

A full census of all 993 names in the generator confirms the enforcement was name-specific: across the whole family, only those two names carry the 19 Nov hold, and nothing else. No broad registry wave landed; the live edge of 407 names, all behind the same content network, is essentially intact two days on. A family-shape list tells you a pattern exists. NSS tells you which members are live weapons right now, and those are the ones that got held.

0[.]0[.]0[.]0 is a dormancy flag, not a takedown

Both operators use the same trick, and it is worth naming because it fools a one-time check. A domain pointed at 0[.]0[.]0[.]0 (a null route) looks dead. It is not. The fake Zoom domain sat at 0[.]0[.]0[.]0 from 17 to 19 Nov, between the host suspension and the re-point. And right now, 36 of the Telegram names sit at 0[.]0[.]0[.]0: each is still registered, still in the zone, still on the operator's content-network name servers, and under no registry hold, so each can be brought back in minutes. Dormancy is not enforcement. A domain at 0[.]0[.]0[.]0 is parked by the operator, not taken down, which is exactly why you keep watching after an indicator goes quiet.

Why it matters

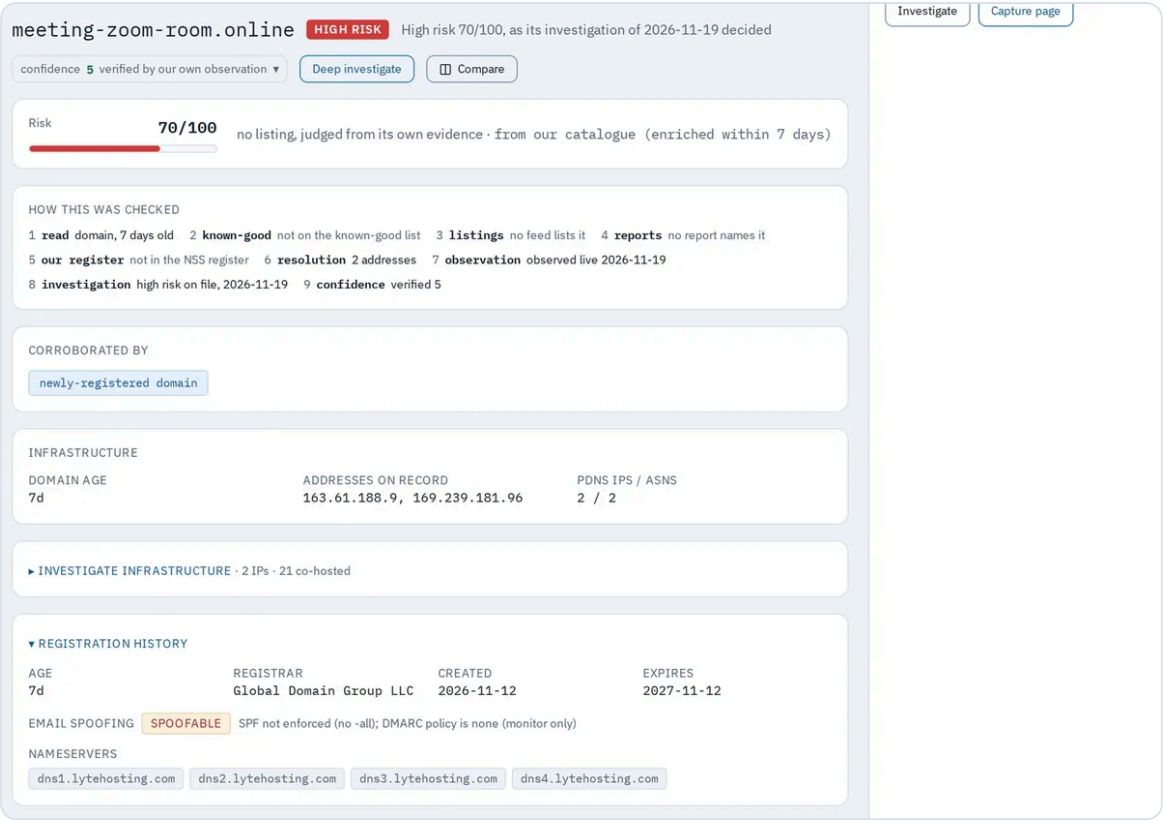
- Do not retire an indicator the day it is knocked offline. The operator may re-point the same domain to another rented host within a day. Track the domain, not the host.
- Host-level takedown is whack-a-mole. The durable levers are the registrar or registry and each hosting account's abuse desk; the durable thing to track is the domain.
- Know which names actually serve. Across a 993-name family the registry held exactly the two NSS had captured serving; the rest are a shape, and some are dormant, not gone.
- A domain at 0[.]0[.]0[.]0 is parked, not dead. Keep it on watch until the registration itself is gone.

Scope and method

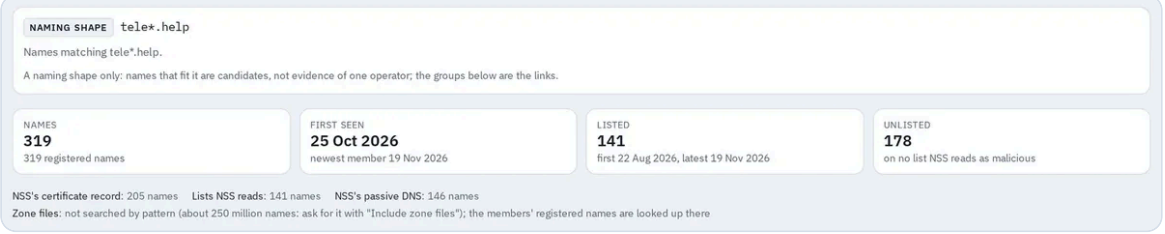
Both operators were found by NSS in its own data and reported by NSS. The dated facts rest on public registration records (RDAP), fresh look-ups over independent public resolvers, the public routing record, NSS's own resolution history and page captures, and the two abuse-desk replies (the host's, ticket 0013116, and the registrar's). Honest boundaries, kept on the page: the Zoom action was a hosting-account suspension, not a registry takedown; the hosts are shared, so co-residence links nothing; the re-

staged Zoom lure's content is gated and so is unverified; and 0[.]0[.]0[.]0 is operator dormancy, not enforcement. Indicators are defanged here and ship in full as CSV and JSON.

A feed tells you a domain was bad once. Tracking tells you what the operator did next.



NSS Station, the casefile for the Zoom domain: High risk, both addresses on record and the registration history, so a defender sees the move with no manual lookup. The address is masked.



NSS Station, the family finder for the Telegram generator: which names actually serve versus which are only a shape. Across all 993, the two captured serving names are the two that were held.

The NSS tools used

> Investigate
Read the casefile for the Zoom domain: its verdict (High risk), both addresses on record, the automatic checks and the registration history, so the re-point reads without a manual lookup.

> Scan
Re-read each indicator so that Investigate and Scan agree on the verdict.

> Sightline
Captured the live Zoom lure (14 Nov) and the re-pointed host (19 Nov): the open directory staging the gated lure file.

> Family finder
Grouped the Telegram generator by naming shape and listing state, and showed which members actually serve versus which are a shape or dormant.

> Tools
Chained the domain's resolution history and registration record so the 163 to 169 to 163 move reads as one dated path.

> Hunt
Ran the full 993-name census of the generator to confirm the registry held exactly the two captured serving names and nothing else.

Indicators

All 5 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
meeting-zoom-room[.]online	Domain	Fake Zoom update / join-meeting lure (NSS-ZM-01 line). One continuous registration created 12 Nov 2026 at Global Domain Group LLC (IANA 3956); status clientTransferProhibited only, never any registry hold. Reported to its host 14 Nov (ticket 0013116); host suspended the account 18 Nov 06:21 UTC; the operator re-pointed the same domain 19 Nov 15:58:08 UTC. Resolution path (NSS passive DNS): 163[.]61[.]188[.]9 (AS153568,

		Bangladesh reseller pool) 12-13 Nov, 169[.]239[.]181[.]96 (HostAfrica shared, South Africa) 14-18 Nov, 163[.]61[.]188[.]9 again 19 Nov; name servers moved to lytehosting (same reseller pool) on the re-point. Both addresses are rented shared hosting, not an operator tie.
`teleakflow[.]help`	Domain	Telegram account-takeover lure, captured serving. Registered at Chengdu West Dimension Digital Technology (IANA 1556). Registrar client hold applied 19 Nov 2026 06:36:09 UTC after NSS's abuse report; now NXDOMAIN. One of exactly two names held across the full 993-name generator.
`telealproi[.]click`	Domain	Telegram account-takeover lure, captured serving. Registered at Chengdu West Dimension Digital Technology (IANA 1556). Registrar client hold applied 19 Nov 2026 06:36:09 UTC (same second as teleakflow[.]help, in a second registry) after NSS's abuse report; now NXDOMAIN. The other of the two names held across the 993-name generator.
`telealproi[.]help`	Domain	Live control: the label twin of the held telealproi[.]click, at the same registrar (IANA 1556), with no hold and still resolving on 19 Nov 2026 (last changed 6 Nov). Shows the 19 Nov hold was name-specific, not family-wide.
`teleandxtr[.]click`	Domain	Live control: a family sibling at the same registrar (IANA 1556), status active, no hold on 19 Nov 2026 (last changed 18 Nov). Part of the family's intact live edge.

ALL 5 INDICATORS: CSV JSON also on GitHub No sign-up.

Check an indicator from this paper

How we know

What this rests on

- The Zoom host suspension is HostAfrica's own abuse-desk reply, ticket 0013116, dated 18 November 2026 06:21 UTC, received to NSS's inbox in reply to NSS's report of 14 November.
- The Zoom domain's registration (one continuous registration created 12 November 2026, registrar Global Domain Group LLC, status clientTransferProhibited with no registry hold, re-pointed 19 November 15:58:08 UTC) is public registration data read by NSS on 19 November 2026.
- The resolution path (163.61.188[.]9 on 12 to 13 Nov, 169.239.181[.]96 on 14 to 18 Nov, 163.61.188[.]9 on 19 Nov) is NSS's own first-party resolution record, with the 19 November state re-checked over independent public resolvers.
- The re-pointed host's open directory and the single 52 KB staged lure file, under a wildcard certificate issued on the domain's creation day, are an NSS page capture of 19 November 2026 22:10 UTC; the lure content itself returned 404 and was not retrieved.
- The Telegram holds are public registration records: teleakflow[.]help and telealproi[.]click both carry a client hold last changed 19 November 2026 06:36:09 UTC, while the control siblings telealproi[.]help and teleandxtr[.]click carry no hold on the same day.
- The 993-name census and the count of 36 names at 0[.]0[.]0[.]0 are a full look-up of the generator's names over public DNS and registration records on 19 November 2026.

What we cannot say

- The Zoom action was a hosting-account suspension by the host, not a registry or registrar takedown. The domain was never held at the registry, which is why the operator could re-point it.
- Both Zoom hosts are shared rented hosting used by unrelated tenants. Co-residence on them is not an operator tie, and this paper claims no siblings from it; the operator signature here is the single continuous domain registration, not the hosts.
- The re-staged Zoom lure's content is unverified: the lure is gated and returned 404 to a direct request, so NSS confirms a lure was re-staged but not that it is the same kit as before.
- A domain at 0[.]0[.]0[.]0 is operator dormancy, not enforcement. NSS states it as reactivatable, not as taken down.
- "We reported them, they were knocked offline" is the report-then-action sequence with dates; NSS does not claim its report was the sole cause of either action.
- NSS records infrastructure. It holds no victim data and makes no claim about who operates either 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), "We see you, Baby! We reported two
operators, both were knocked offline, and we tracked what they did
next", NSS-WS-01, 20 Nov 2026. https://nsshq.com/research/we-see-you
```

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-ZM-01: Fake Zoom update page installs a self-hosted ScreenConnect client: technical analysis

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

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 is not affiliated with Zoom or Telegram, with the brands imitated, or with any registrar, hosting company, DNS service 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. The fake Zoom lure in this paper is a distinct operator from the one in NSS-ZM-01; no link is claimed between them. NSS names no actor and makes no country-of-origin claim. NSS-WS-01 is NSS's own name for this case.