[N S S | > research]

TECHNICAL ANALYSIS / NSS-AX-01 TLP:CLEAR Deep Research



Expanded by NSS

24 additional consoles live on 14 Nov, offered to complement the FBI FLASH; all 25 FLASH indicators already held

Updated 18 Nov 2026.

Tracking since 9 Oct 2026 · Last checked 18 Nov 2026 · 1 update

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

On 13 November 2026 the FBI published FLASH-20261113-001 on ARTEX, a framework public reporting ties to intrusions against finance and managed-service providers, with 24 addresses and one domain, and asked defenders for console and reseller indicators. NSS Research offers this paper in support of that request. All 25 FLASH indicators are corroborated here, each with the date it entered NSS's records. On 14 November NSS confirmed 24 additional ARTEX consoles active, and this edition takes the

console fingerprint apart: the page identity and the certificate issuer that name the framework, the two-class structure NSS sees across the set, per-claim confidence, a dated timeline, and detection NSS validated against its own stored readings. It maps the reseller layer behind the FLASH's domain and records one apparent operator tie it tested and rejected. Under NSS's disclosure plan every console address stays held; the counts, the fingerprint and the detection are what ship here.

PUBLISHED	LAST UPDATED	READING TIME	MARKING
17 Nov 2026	18 Nov 2026	33 min	TLP:CLEAR

18 NOV 2026

Update, 18 November 2026: the consoles re-read twice, more confirmed, and where the two signatures stop

On 18 November 2026 NSS read the landing page of each of the 24 additional consoles this paper counts twice, both times through its controlled capture path: one plain page load each, nothing typed, no login. The first read ran from 19:26 to 20:08 UTC. The second ran from about 20:34 to 20:36 UTC and also read each console's certificate. NSS took no readings of the consoles on 15, 16 or 17 November, so anything that changed since 14 November is dated only as "by 18 November". Where a console did not serve its page, this update says only that; it does not say any console was taken down. Every console address stays held, as before.

RESULT FOR THE 24	FIRST READ, 19:26 TO 20:08 UTC	SECOND READ, ABOUT 20:34 TO 20:36 UTC
Served the console page, with the same page title as on 14 November	21	22

A gateway error instead of the console page	2	1
Accepted the connection and sent nothing	0	1
Not read	1	0

The two reads agree on 21 consoles: 20 served the console page both times and 1 gave a gateway error both times. They differ on 3. One that gave a gateway error in the first read served the console in the second. One that served the console in the first read sent nothing in the second. One not read in the first read served the console in the second. So 23 of the 24 served the console page at least once on 18 November, and 22 did in the later read. Both reads are given here; neither is preferred.

Consoles confirmed since 14 November

On 18 November 2026 NSS confirmed 23 further consoles live by its own reads, each read twice through the same controlled capture path; the reads ran from about 20:43 UTC on 18 November into the early hours of 19 November UTC. None is in the FBI FLASH or among the 24 above. How each lead arose and how each was confirmed are kept apart: every one of the 23 was confirmed the same way, by NSS's own read matching the console fingerprint, and the leads came from three places.

- 9 NSS found in its own records and pivots: its passive DNS, its certificate and zone records, a pivot from software installed beside a known console, and reads of the networks around consoles it already knew.
- 5 NSS verified from public search listings and public certificate logs, after its own read confirmed each one.
- 9 are addresses other researchers had already published, which NSS found still serving a console on 18 November. These are persistence, not an NSS discovery, and are never counted as found by NSS.

3 of the 23 are renamed: their page titles do not carry the framework's name, so the page-title rule in this paper, and the public title rules, miss all three. NSS recognised them by the console's own static web assets and icon, which a rename of the displayed brand leaves in place.

There are about 45 live console endpoints beyond the FLASH as of 18 November 2026, and fewer when counted strictly by build identifier, because several consoles share one build and some published address blocks are a single install answering on many addresses. A single install answered across hundreds of addresses in published blocks, so NSS counts by distinct build, not by the addresses that answer. Where consoles share one build, NSS cannot tell from outside whether that is one operator or one shared image.

The addresses of these consoles were sent to the FBI, through the reporting route the FLASH gives, before this update was published, and are held from this page under the same disclosure plan.

Install dates: of the 7 consoles whose own self-signed or locally issued certificate dates the install, none was installed after the FLASH of 13 November; those certificates date from 9 October to 4 November 2026. The other consoles cannot be dated this way.

The page-title signature: what it covers, and what it misses

The page-title signature keys on the framework's name in the console's page title. A change of hostname or address does not evade it, because it reads the page, not the name the page is served under. It does miss a renamed console. The brand shown in the console's title is a setting whoever runs the console can change, a fork that began from an early ARTEX release and runs under its own name has been reported, and NSS confirmed three renamed consoles on 18 November. A console renamed either way does not carry the framework's name in its title, and the title rule in this paper will not match it. Keep the framework-name match as one signal, and pair it with what public reporting says stays the

same across a rename: the console's sign-in flow, its static web assets and its icon.

Title-only detection also matches pages that are not consoles. On 18 November one page matched the title rule and is not a console: it is a product site for the framework, and it fails every other check.

Earlier public research described title-based console detection and the rebrand before this paper did. The first edition did not cite it; it is cited here:

- Console detection by page title together with static web assets: Censys, "ARTEX: Agentic Asbestos", 5 November 2026, which detects the console by its page title together with the framework's static web assets. Read the Censys post
- Title-based console detection: MalwareMustDie, "MMD-072-2026 - ARTEX detection signature pack - from IOC w/playbook process", 13 November 2026, whose console rules count a page-title match on a console port as stronger evidence than the port alone.

  Read the MalwareMustDie post
- The editable brand: SOCRadar, a study of exposed ARTEX consoles in the United States, November 2026, which reports that the brand in the console's title is set by whoever runs it and that the sign-in flow, asset layout and icon stay the same across rebrands.

  Read the SOCRadar study
- The renamed fork: Arctic Wolf research, reported by BleepingComputer on 11 November 2026, on a platform that began as a fork of ARTEX 0.1.1 and is published under its own name.

  Read the BleepingComputer report

The certificate-issuer signature: where it applies

The framework-named certificate issuers in this paper are self-signed or locally issued, not from a trusted authority. The public certificate record holds only certificates from trusted authorities, so this signature cannot be searched for there. It applies to a certificate read from the host itself: run it across your own certificate inventory and your passive TLS records, and match the framework's name in the whole issuer, not one field of it. In the second read of 18 November it matched 3 of the 24 consoles, and none of the others.

The FLASH's domain and the reseller layer

On 18 November 2026 at 19:21 UTC the FLASH's one domain still did not resolve, as on 14 November, and the public certificate record showed no certificate for it issued after 4 October 2026. At the same time the nine reseller and routing names this paper counts behind it were unchanged: seven resolved to the same address as on 14 November, and the other two still had no address, as on 14 November.

What this update corrects

- In Detection you can deploy, "Written to the title, not one hostname, so a name change does not evade it" claimed more than holds. It now reads: "Written to the title, not one hostname, so a hostname change does not evade it; a console whose displayed brand has been renamed does (see the update of 18 November 2026)."
- In the same section, "because addresses rotate and the fingerprint lasts" claimed more than holds. It now reads: "because addresses rotate and the fingerprint outlasts them, though not a rename of the console's displayed brand (see the update of 18 November 2026)."
- The certificate split of the 24 as read on 14 November. This paper gives 2 consoles with a self-signed certificate whose issuer names the framework, 11 with a public certificate authority, 3 with a delivery-network origin certificate, 7 self-signed or locally issued without the framework's name and 1 on plain web. Read 3, 11, 3, 6 and 1. The earlier read looked at one issuer field, the organisation;

the read of 18 November, at about 20:34 to 20:36 UTC, looked at both the organisation and the common name, and one console names the framework in the common name only. It serves the same certificate as on 14 November. Read the paper's counts of 2 and 7 for the certificate split, wherever they appear, as 3 and 6.

- For the same reason, where the key findings, Detection you can deploy and How we know say the certificate-issuer signature matched the 2 self-hosted consoles, read 3. The three are the same consoles on 14 and 18 November.
- Since 14 November one console has changed its certificate: on 18 November it presents a certificate from a public authority where on 14 November it presented a self-signed one. The split above is as of 14 November.
- Everything else stays as read on 14 November 2026: the 24 consoles confirmed active that day, the page-title validation and the country figure.

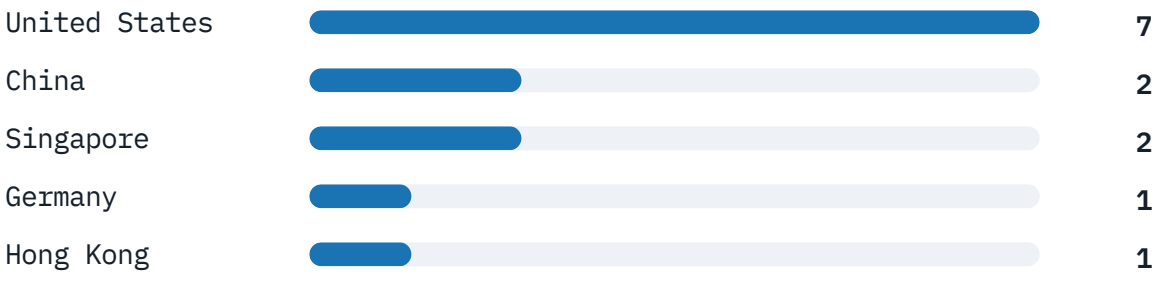
24
additional ARTEX consoles NSS confirmed active on 14 Nov 2026, offered in support of the FBI FLASH

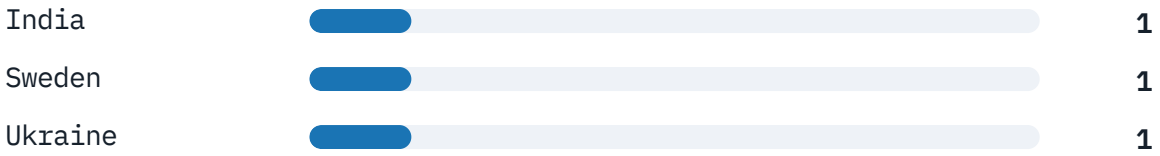
25 of 25
FLASH indicators corroborated in NSS's records, each with the date it entered them

2
detection signatures NSS validated against its stored console readings: the page identity and the certificate issuer that name the framework

9
reseller and routing names of the layer behind the one domain the FLASH names, mapped for defenders

CONFIRMED CONSOLES BY COUNTRY OF THE HOSTING NETWORK





The hosting country from public routing records, 14 November 2026, for the 16 of the 24 consoles that carry one; 8 have none yet and are not counted. Hosting companies are not named. A console on a cloud range is most likely an exposed tenant, not the operator.

What the FLASH asked for

Four passages from FBI FLASH-20261113-001, quoted as written, that this paper sets out to answer. The FLASH is marked TLP:CLEAR and says it may be shared without restriction, subject to copyright.

> "As of early November 2026, researchers identified over 1,600 publicly exposed ARTEX console instances, with total deployments likely significantly higher when including systems behind firewalls or in private networks."
>
> `FLASH-20261113-001, page 1, Summary`
>
> `ANSWERED IN` finding 5 and the section The consoles: NSS confirmed 24 additional consoles active on 14 November 2026 from its own records and places them inside the wider count the FLASH cites; it does not try to reproduce that count.

> "ARTEX Infrastructure Artifacts: Source code or screenshots of suspected ARTEX console interfaces and ARTEX configuration files"
>
> `FLASH-20261113-001, page 8, Information Requested, item 1`
>
> `ANSWERED IN` findings 3 and 4, the console figure and the sections Teardown and Detection you can deploy: the page identity and the certificate issuer NSS read on each of the 24 consoles, with a masked reading of one and tested detection, so any defender can repeat the check.

> "LLM and SI Infrastructure Indicators: Outbound connections to LLM API endpoints; evidence of self-hosted LLM gateway or reseller software (CLIProxyAPI, New API); unfamiliar LLM proxies

> or resellers in egress logs; token consumption patterns or API billing anomalies"
>
> `FLASH-20261113-001, page 8, Information Requested, item 4`
>
> `ANSWERED IN` finding 6, walkthrough steps 2 and 3 and the section The reseller and gateway layer: the 9 reseller and routing names behind the FLASH's one domain, mapped from NSS's own records, and the 10 candidate gateway names NSS adds as leads.

> "these indicators should be interpreted as historically observed infrastructure within the activity window and should be corroborated with current network telemetry or additional intelligence sources when used for defensive or investigative purposes."
>
> `FLASH-20261113-001, page 6, Indicators`
>
> `ANSWERED IN` finding 2, walkthrough step 1 and the API section: the date each FLASH indicator entered NSS's records, the verdict each read on 14 November 2026, and a script that re-checks the whole list against current NSS verdicts.

The FLASH is the FBI's document and is quoted here, not copied. For the FLASH itself and to report what you find, use the FBI's own channel, the one the FLASH names: [FBI Internet Crime Complaint Center (ic3.gov)]

Key findings

1. This paper is a companion to FBI FLASH-20261113-001 and to the public reporting of October and November 2026 that the FLASH cites, and it is offered in support of the defenders both are written for. The FLASH gives defenders a vetted list, the framework's behaviour and mitigations, and asks for infrastructure artefacts (passage 2 above); this paper is one answer to that request. NSS adds three things to what the FLASH gives: the date each FLASH indicator entered NSS's records, as a dated point to corroborate against; a confirmed reading on 14 November 2026 of 24 additional consoles, with the fingerprint taken apart so any defender can repeat the check; and the reseller and routing layer the FLASH tells defenders to watch for, mapped from the one

domain it gives to 9 more, with a set of candidate gateway names from NSS's own records.

2. All 25 indicators in the FLASH, its 24 addresses and its one domain, are corroborated in NSS's records, each with the date it entered them. The earliest entered NSS's records on 9 October 2026, two days after the first public report. Three of the addresses in this list, 144[.]172[.]64[.]60, .99 and .128, are the same ones Microsoft and Wiz tie to the campaign in their reporting; that is their attribution, offered here as corroboration of the FLASH set, not an NSS finding. This answers passage 4 above: a dated source a defender can set beside the FLASH's list and corroborate against current telemetry.

3. NSS confirmed 24 additional ARTEX consoles active on the internet on 14 November 2026, every one an addition to the FLASH's list, from candidate addresses it already held. It read each one's public page and certificate only: no login, no form, no payload. Public reporting corroborates why this surface exists and is findable: Google Threat Intelligence Group describes ARTEX as shipping an embedded Next[.]js web console, which is exactly the surface these exposed instances present. The fingerprint is two elements. First, the page identity: every one of the 24 served a page whose title names the framework. Second, the certificate issuer: 2 of the 24 present a self-signed certificate whose issuer organisation names the framework; 11 use a public certificate authority, 3 a delivery-network origin certificate, 7 a self-signed or locally issued certificate with no framework name, and 1 serves the page over plain web with no certificate. 21 of the 24 answer on the standard secured web port. These are the console-interface artefacts passage 2 above asks for, as seen from outside.

4. NSS ships tested detection, not just the names. Two signatures carry the fingerprint: an alert on an HTTP response whose page title names the framework, and an alert on a certificate whose issuer organisation names the framework. Both were validated against NSS's stored readings of the 24 consoles from 14 November 2026: the title signature matched all 24, the issuer signature the 2 self-hosted consoles. The

fingerprint is already in public reporting from early November, so publishing it costs the investigation nothing and gives defenders a check they can run across their own estate today.

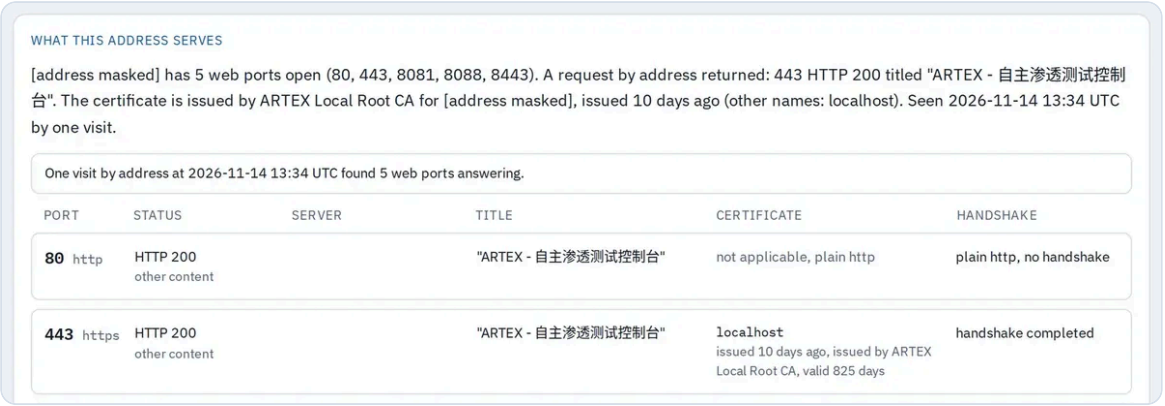
5. NSS does not run an internet-wide census of exposed consoles. The 24 consoles are the ones it confirmed from hosts already in its own records. The researchers the FLASH cites put the total exposed count above 1,600 (passage 1 above); this paper does not try to reproduce that number and treats it as the wider picture these 24 sit in. Most of the 24 sit on commercial cloud or hosting addresses and are most likely exposed third-party tenants, not the operator's own machines; NSS draws no operator link between them. Under NSS's disclosure plan every console address is held from this edition: law enforcement is handled first, and the hosts of exposed deployments are notified before any address is published.

6. The FLASH gives one reseller domain and asks defenders to watch the layer it belongs to (passage 3 above). NSS holds 9 additional reseller and routing names of that layer in its own records. Beyond them, two things NSS adds as leads: 3 host names under the FLASH's own domain on no list NSS reads, carrying certificates from 5 August 2026 in the public record, two months before the first public report; and 10 names shaped like gateways for the model family public reporting says the framework uses, in NSS's own records before the FLASH, on no list NSS reads. These are candidates by naming and certificate history; NSS draws no tie between them.

7. NSS tested the one apparent link between the gateway names, a shared name-server pair, and rejected it: each name server of the pair fronts hundreds of unrelated zones (more than 400 behind one, more than 190 behind the other), so the pair is a provider default, not an operator tie. The platform states this on the family panel as "linked by: shape only". Shared infrastructure is a lead, never a conclusion; a rejected tie is reported here with the same weight as a confirmed one.

8. NSS makes no actor attribution. Others do, and those assessments are theirs, offered here only as context: the FLASH ties parts of this activity

to named clusters; Microsoft attributes the intrusion activity to Storm-0940, which it describes as PRC-nexus; Google Threat Intelligence Group tracks the campaign as UNC7228, overlapping Storm-0940; and Amazon Threat Intelligence assesses disparate Chinese-nexus groups at moderate confidence. NSS does not print those names as its own finding, does not merge them, and makes no country-of-origin claim. NSS-AX-01 is NSS's own name for this case, not a named group.



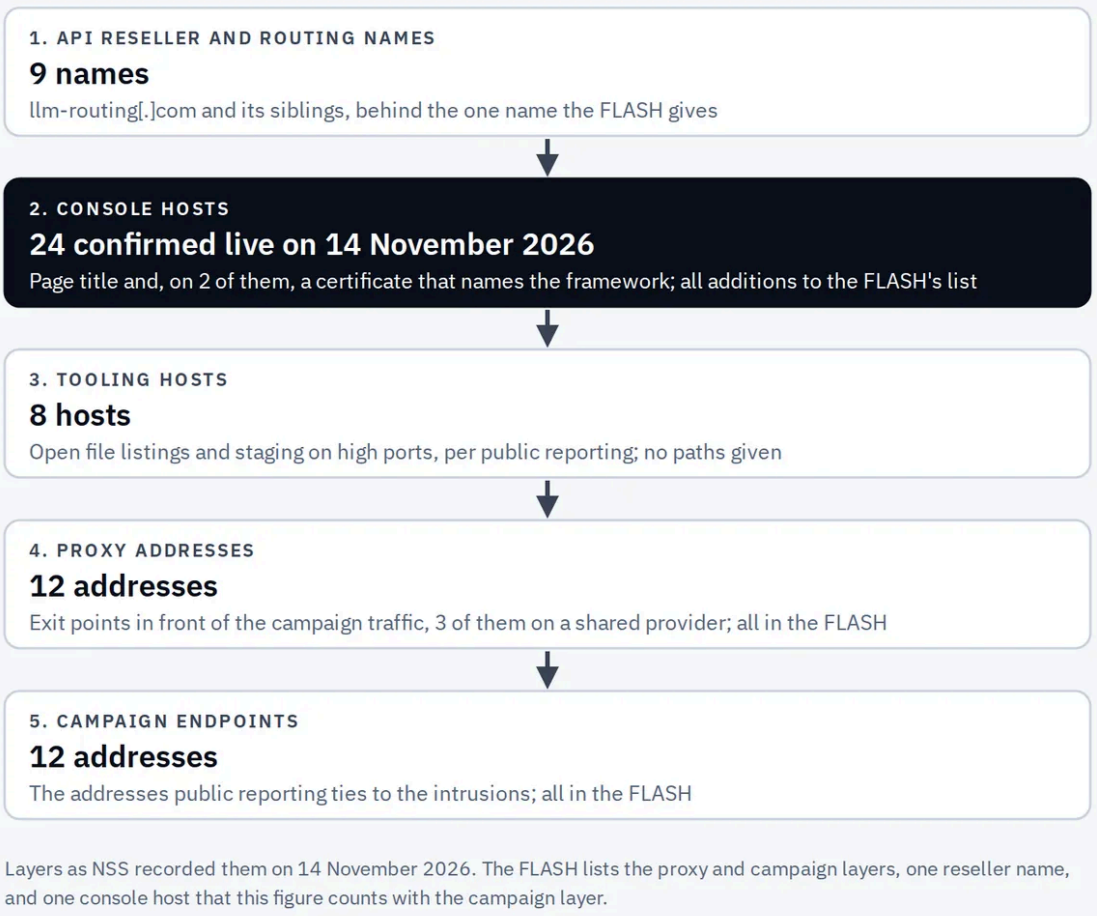
WHAT THIS ADDRESS SERVES

[address masked] has 5 web ports open (80, 443, 8081, 8088, 8443). A request by address returned: 443 HTTP 200 titled "ARTEX - 自主渗透测试控制台". The certificate is issued by ARTEX Local Root CA for [address masked], issued 10 days ago (other names: localhost). Seen 2026-11-14 13:34 UTC by one visit.

One visit by address at 2026-11-14 13:34 UTC found 5 web ports answering.

PORT	STATUS	SERVER	TITLE	CERTIFICATE	HANDSHAKE
80 http	HTTP 200 other content		"ARTEX - 自主渗透测试控制台"	not applicable, plain http	plain http, no handshake
443 https	HTTP 200 other content		"ARTEX - 自主渗透测试控制台"	localhost issued 10 days ago, issued by ARTEX Local Root CA, valid 825 days	handshake completed

One confirmed console, 14 November 2026: the page identity on the secured port and a certificate whose issuer names the framework. These two elements are the whole fingerprint. The address is masked, the shot is cropped to the plain and secured web-port rows, and the hosting is left out.



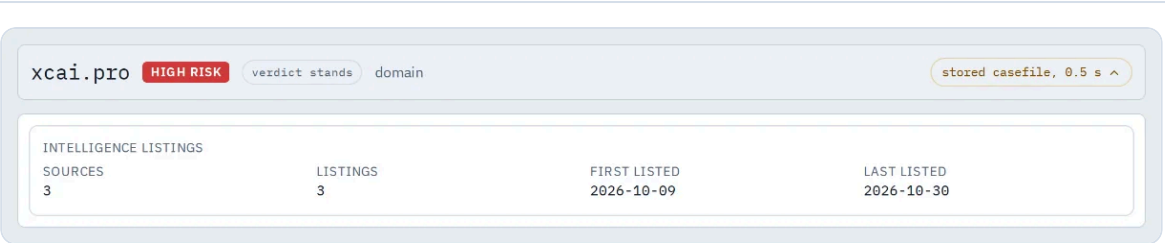
Layers as NSS recorded them on 14 November 2026. The FLASH lists the proxy and campaign layers, one reseller name, and one console host that this figure counts with the campaign layer.

The layers this paper covers, building on the FLASH. The FLASH gives the proxy and campaign layers, one reseller name and one console host (counted here with the campaign layer); NSS adds the confirmed reading of the console layer and the map of the reseller layer. Counts are what NSS holds for each layer; every console address is held, so the indicator file ships the FLASH's own indicators that NSS corroborates.

How an analyst finds this with NSS

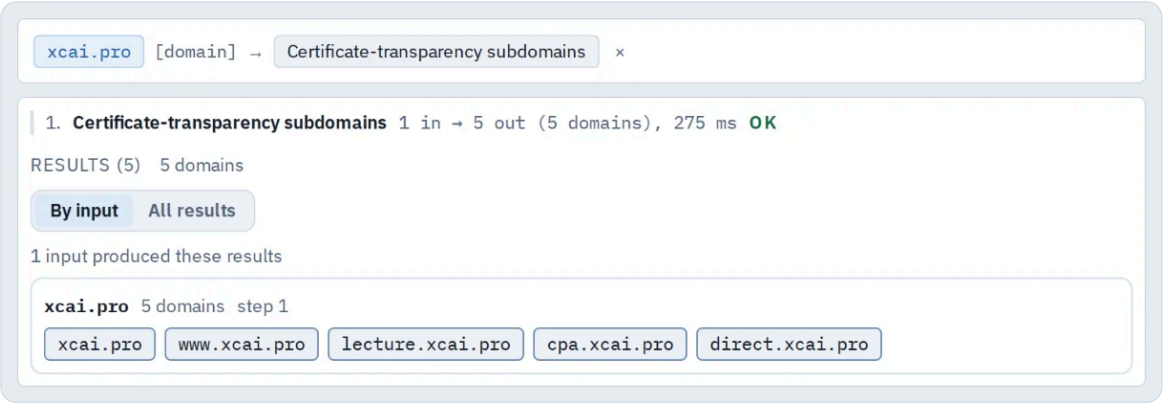
The same case, worked the way a defender works it in NSS: from the FLASH's own indicators, to the additional consoles NSS confirmed, to the leads NSS adds from its own records, and to one apparent tie NSS tested and threw out. Every picture is the real Station on 14 November 2026, cropped to the panel in use; addresses are masked.

01 Start where the FLASH starts: its one domain. Investigate already holds it, with a verdict on its own evidence and the date it entered NSS's records, 9 October, shown beside it. This is the kind of dated source passage 4 of the FLASH asks defenders to set beside its list.



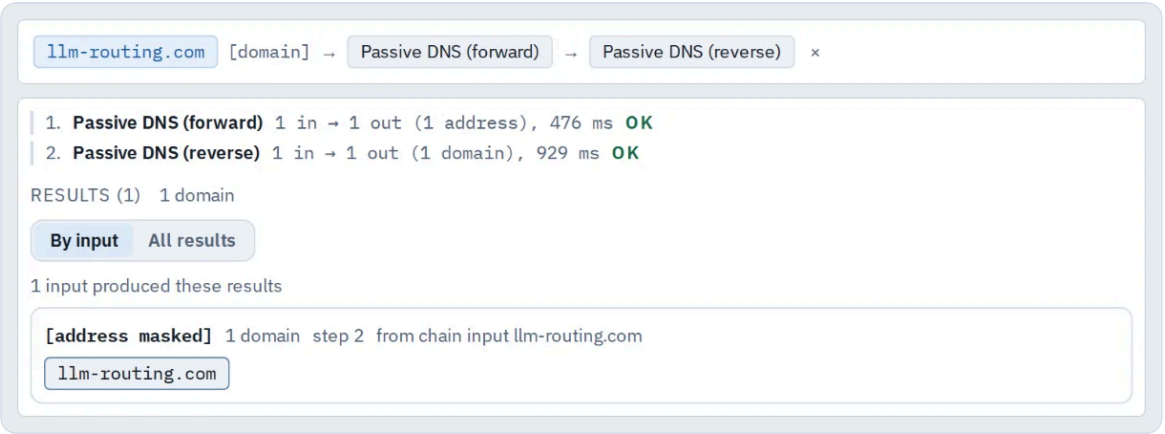
Investigate, 14 November 2026. The record date beside the FLASH date, as a dated point to corroborate against. The badge is the band as read that day.

02 One tool on the Scan page returns the other host names the public record carries under the domain. Starting from the one name the FLASH gives, it surfaces four additional host names under it, three of them on no list NSS reads and one already held from partner sources.



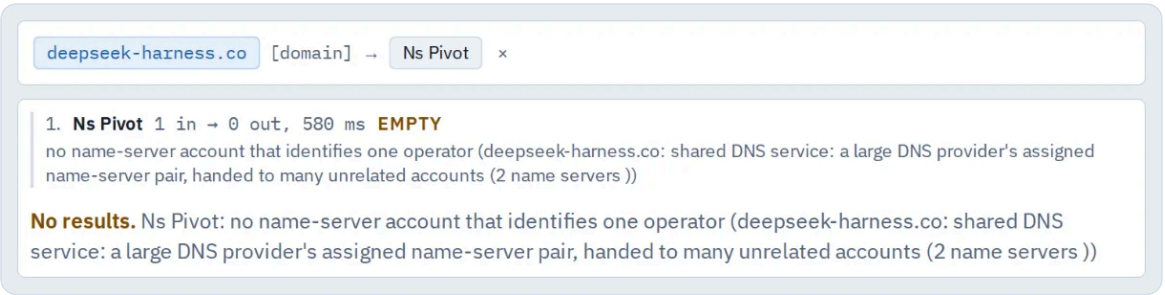
NSS Scan for the FLASH domain, 14 November 2026: four additional host names under it, from the public record, not records NSS held before.

03 Open a sibling reseller name in Tools and chain two reads of NSS's own records: the address NSS has on record for the name, then every name NSS has seen on that address. Nothing is contacted; each step feeds the next. This is the reseller layer the FLASH's fourth request (passage 3 above) asks defenders to look for.



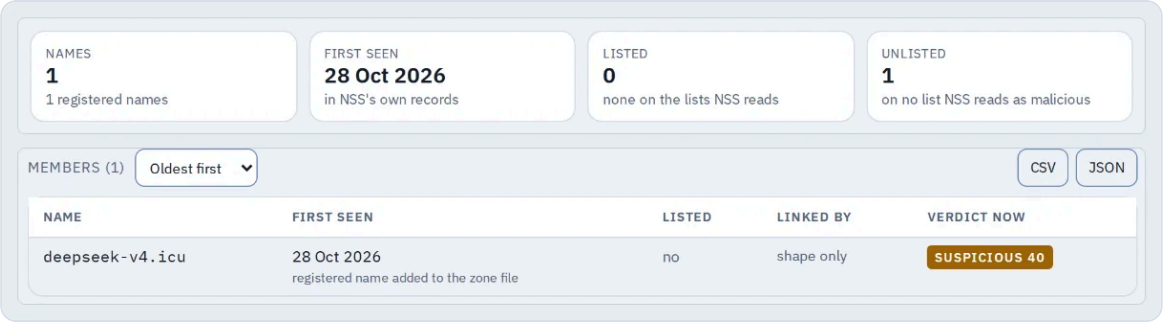
Tools, 14 November 2026: the reseller layer behind the FLASH's domain, read from NSS's own records. The address is masked.

04 Before calling the gateway names a set, test the link. The one apparent tie is a shared name-server pair. The platform rejects it and says why: the pair is a shared DNS service handed to many unrelated accounts, with more than 400 unrelated zones behind one of its two name servers and more than 190 behind the other, so the analyst drops the tie.



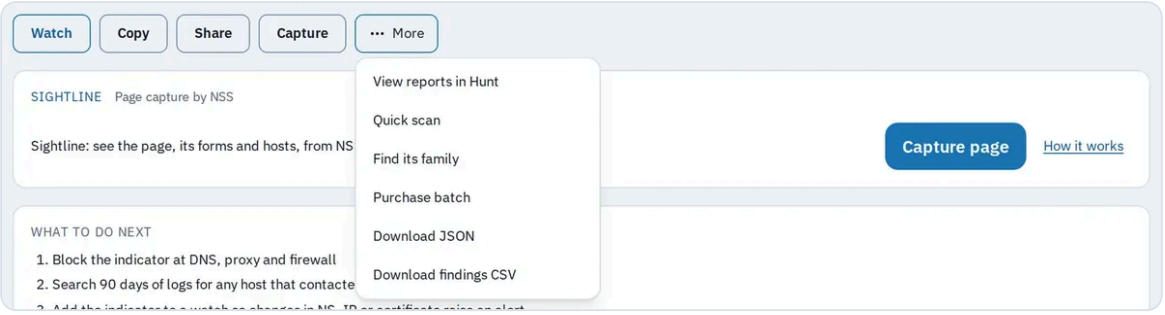
The shared-infrastructure check, 14 November 2026: the platform rejects the shared name-server pair as a link and prints why. Each name server of the pair sits in front of hundreds of unrelated zones, so it is a provider default and not an operator tie. The provider is not named.

05 The family view takes a gateway-style name NSS recorded itself, on no list NSS reads. It shows its record date and its verdict, and says plainly what links such names: a shared shape, not a shared operator.



Family view, 14 November 2026: a gateway-style name NSS recorded itself, on no public list, with its record date and verdict band. "Linked by: shape only" is the platform's own restraint, printed on the panel. The name imitates the brand of DeepSeek, a model vendor that is not involved and whose service NSS did not query; the imitation is the point, not the vendor.

06 Then act: watch the names and addresses, share the casefile, or download the whole list as JSON or CSV for your own tools. The downloads and watches in this step are Full features.



The casefile's actions, 14 November 2026 (Full features). Nothing was clicked for the picture but the More menu.

A Community account is approved by hand and runs Investigate and Scan on your own indicators.

Automate it with the NSS API

Every NSS check is JSON: a risk band, the host class, 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

```
VALUE=$(jq -r '.indicators[0].value' nss-ax-01.json)   # the first indicat
curl -s "https://nsshq.com/api/v1/check?value=$VALUE"
```

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

The answer for the FLASH's one domain on 14 November 2026


```
{
  "as_of": "2026-11-14T13:36:04Z",
  "band": "High risk",
  "band_is_host_class": false,
  "found": true,
  "host_class": {
    "as_of": null,
    "class": "unknown",
    "label": "Host type unknown",
    "sentence": "No address on record for this name."
  },
  "known_good": false,
  "names": null,
  "public_listing": {
    "as_of": "2026-11-14T13:36:23Z",
    "date": "2026-10-09",
    "line": "Listed publicly on 2026-10-09.",
    "listed_on": "2026-10-09",
    "state": "listed"
  },
  "registration": null,
  "reports": 6,
  "type": "domain",
  "value": "xcai[.]pro",
  "view": "public"
}
```


The real public answer of 14 November 2026, 13:36 UTC, for the FLASH's one domain (value defanged here). It reads High risk, reports the public listing of 9 October, and, as of that read, holds no address: the domain had gone dark. 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 and flag verdict changes (Python 3, standard library only)

```
#!/usr/bin/env python3
"""Check every name and address in an NSS paper's indicator file and flag
(cron or SIEM enrichment).

  python3 nss_check_file.py nss-ax-01.json

Without a key it uses the public check (no key needed, a few checks a day
With a Full account, create a key on the API keys page, then set NSS_API_K
NSS_API_URL to the request that page shows. The key is sent only in the Au
never in the address. Prints one JSON line per indicator; exits 2 when a v
the last run.
"""
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)
    if any(v == "example.org" for _, v in q):
        q = [(k, value if v == "example.org" else v) for k, v in q]
    else:
        q = q + [("value", value)]
    return urllib.parse.urlunsplit(u._replace(query=urllib.parse.urlencode


def check(value):
    headers = {"Accept": "application/json"}
    if KEY:
        headers["Authorization"] = "Bearer " + KEY
    req = urllib.request.Request(request_url(value), headers=headers)
    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"):
```

```
                time.sleep(int(e.headers["Retry-After"]) + 1)   # per-minu
                continue
            if e.code == 429:                                   # the day'
                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 check takes one c
            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_of": answer.get("as_of"), "previous": old.get(it["value
        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)   # stays under a key's default 60 calls a minute
    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-ax-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

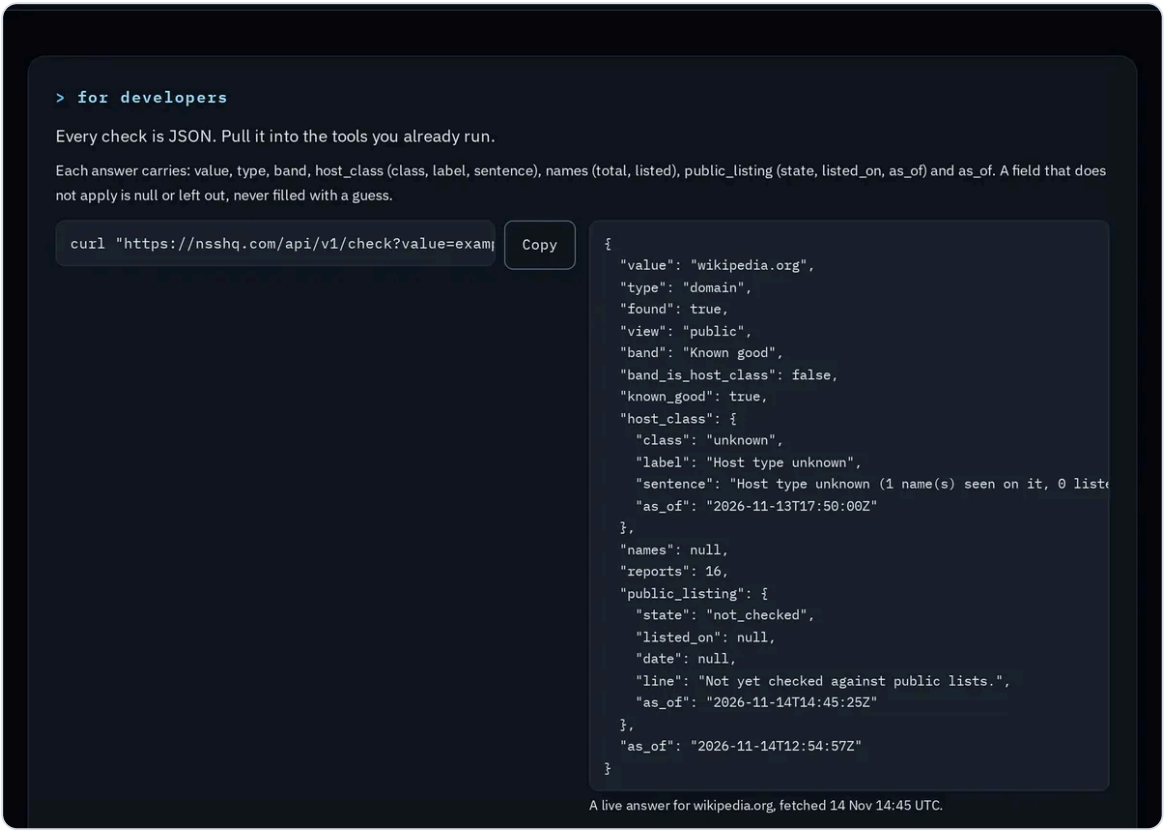
and stops when the day's allowance is spent. Lines are kept under 100 columns so the script copies cleanly from the PDF.

STIX 2.1 and other formats

```
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.

The fingerprint a defender can reuse is in the open, and it follows from the behaviour the public reporting described: a console serves a page whose identity names the framework, most on the standard secured web port and the rest on a high port or plain web, and a self-hosted one presents a certificate whose issuer names the framework. Alert on that page identity and that certificate issuer across your own estate, and treat any match as an exposed console to isolate.



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

Timeline

5 Aug 2026
Public certificate records later show certificates for the FLASH's one domain from this date, two months before the first public report.

7 to 8 Oct
First public reporting describes the ARTEX framework and its exposed consoles; the project's code repository is taken down on 8 October, per the FLASH.

9 Oct
The FLASH's one domain and its South Korea campaign proxy addresses enter NSS's records, two days after the first public report.

17 to 22 Oct
Further FLASH addresses enter NSS's records: the ConnectWise campaign addresses, and three shared-provider addresses the FLASH itself marks transient.

28 Oct
The first of the gateway-style names NSS adds as a lead enters its records, on no list NSS reads.

31 Oct
Five reseller and routing names of the layer behind the FLASH's domain enter NSS's records.

3 to 5 Nov
Public vendor reporting sets out the console fingerprint: a landing page whose identity names the framework and a self-signed certificate whose issuer names the framework.

7 Nov
The FLASH's command-and-control and framework-server addresses enter NSS's records.

13 Nov
The FBI publishes FLASH-20261113-001 (TLP:CLEAR): 24 addresses, one domain, the framework's behaviour and mitigations, and a request for console and reseller indicators.

14 Nov

NSS confirms 24 additional ARTEX consoles active, reads each one's public page and certificate, and records the fingerprint, the two-class split and the apparent tie it tested and rejected.

18 Nov

Update: NSS reads the 24 consoles twice; 21, then 22, serve the console page. It confirms 23 more consoles live, 3 renamed past the page-title rule; about 45 live console endpoints beyond the FLASH, fewer by distinct build. The FLASH's domain and the nine reseller and routing names are unchanged.

What the FLASH gave, what NSS confirmed, and what NSS adds

This paper has three layers, kept apart on purpose so a reader can tell them apart. It builds on the FLASH and on the public reporting the FLASH cites; where this paper goes further, it says so and says how.

This paper is offered alongside a body of public reporting on ARTEX, and builds on it. Microsoft reported the ARTEX intrusion activity on 21 October 2026; Wiz followed on 22 October; Google Threat Intelligence Group and Mandiant published a technical account on 30 October and a wider agentic-threat tracker on 16 November; Amazon Threat Intelligence, on 13 November, the same day as the FBI FLASH, reported threat actors running campaigns with ARTEX agents from its own honeypot telemetry (industrial-scale theft of model-API keys from exposed aggregator applications, and deepfake identity-verification bypass at two crypto exchanges). Between them, those teams cover the tradecraft, the behaviour and the attribution well. The part this paper adds is the exposed infrastructure none of them maps: the live consoles from which the framework is driven, counted and fingerprinted, and the reseller and model-API gateway layer behind them. The pieces are complementary, which is why they are useful together.

What the FLASH gave. FBI FLASH-20261113-001, published on 13 November 2026, lists 24 addresses and one domain, describes the framework's behaviour and mitigations, and asks defenders for ARTEX

infrastructure artefacts; the passages this paper answers are quoted, as written, at the top of the page. Every one of those 25 indicators is corroborated in NSS's records, each with the date it entered them. The earliest reached NSS on 9 October, two days after the first public report. The record date is shown in this paper beside the FLASH date as a dated point a defender can corroborate against, and nothing more is claimed from it.

What NSS confirmed active. On 14 November NSS confirmed 24 additional ARTEX consoles active on the internet, every one an addition to the FLASH's list. It worked from a fingerprint that follows from the behaviour the public reporting described: the console serves a page whose identity names the framework, most on the standard secured web port and the rest on a high port or plain web, and a self-hosted one presents a certificate whose issuer names the framework. For each candidate address NSS already held, it loaded the single public page and read the certificate, nothing else. 2 of the 24 present a certificate whose issuer names the framework; 11 use a public certificate authority, 3 a delivery-network origin certificate, 7 a self-signed or locally issued certificate, and 1 serves the page over plain web with no certificate. The Teardown below takes the fingerprint apart, marks each claim by confidence, and gives the detection a defender can deploy.

What NSS adds from its own records. The FLASH gives one reseller domain. NSS holds 9 additional reseller and routing names of that layer in its own records. Beyond them, two things NSS offers as leads. First: 3 host names under the FLASH's own domain on no list NSS reads, carrying certificates from 5 August 2026 in the public record, two months before the first public report. Second, from NSS's own records before the FLASH: 10 names shaped like gateways for the model family public reporting says the framework uses, on no list NSS reads. These are candidates by naming and certificate history; NSS reports them as its own leads and draws no tie between them.

The consoles

A console is a web page from which the framework is driven. NSS confirmed 24 additional consoles active on 14 November 2026, offered in support of the FLASH's list. Each was confirmed by loading its single public page and reading its certificate: NSS did not log in, submit any form, send any payload, or fetch anything but the landing page. The page identity and, where present, the certificate issuer are the whole fingerprint, and both are things a defender can look for across their own estate.

The 24 sit on commercial cloud and hosting addresses in several countries; by public routing records the United States leads the sample, then China and Singapore. Most have no other name on them in NSS's records and are most likely exposed third-party tenants rather than the operator's own machines; NSS draws no operator link between them. The bar figure above gives the country split from public routing records.

NSS does not run an internet-wide census of exposed consoles, so this is not an exhaustive count. The researchers the FLASH cites put the total number of exposed consoles above 1,600; the 24 here are the ones NSS confirmed active from hosts already in its records, which makes them high-confidence rather than exhaustive, and a small part of the wider picture that reporting describes.

Teardown: the ARTEX console fingerprint

This paper carries NSS's Deep Research label: the console fingerprint taken apart, the structure NSS sees across the set, and tested detection a defender can deploy. This is the technical section. It describes the operator's console as seen from outside, only: its page identity, its certificate and the detection you can build from them. It does not describe how NSS found or read any of it. Each claim is marked by confidence: **observed** (NSS read it directly, with the page or the certificate in hand), **assessed** (NSS's reading of the evidence, a judgement rather than a direct reading), and **public-reporting** (from the FLASH or the vendor reporting it cites, read for context, not confirmed by NSS here).

The fingerprint, element by element

Two elements confirmed every console, and both were already described in public reporting from early November 2026, so setting them out here costs the investigation nothing and gives a defender a check to run.

The page identity (observed). All 24 consoles answered with HTTP 200 and served a landing page whose title names the framework, in the framework's own localised words for its console. The title was identical across all 24. Because that exact string carries a non-ASCII separator this page does not reproduce, the full localised title ships in the indicator file and the detection repository as data, keyed in the rules below on the framework name itself. The title alone confirmed all 24.

The certificate issuer (observed). 2 of the 24 present a self-signed certificate whose issuer organisation names the framework, with a long validity period; this is the self-hosted install giving itself away. The issuer confirmed those 2 a second, independent way. The other certificates do not name the framework: 11 are from a public certificate authority, 3 are a delivery-network origin certificate, 7 are self-signed or locally issued with no framework name, and 1 serves the page over plain web with no certificate. A self-signed certificate that names no issuer organisation is not a framework-issued certificate and is not counted as one.

The ports (observed). 21 of the 24 answer on the standard secured web port; the rest answer on a high port or on the plain web port. The check therefore belongs on every web-facing port, not one.

The two-class structure

The certificate splits the set into two classes, and the split is where the operator structure shows (assessed). **Class A** is the self-hosted console whose certificate issuer names the framework: 2 of the 24, assessed as probable operator-controlled or evidentiary. **Class B** is the console on a public-authority, delivery-network or plain certificate with no framework name: the remaining 22, assessed as probable exposed third-party

deployments, most of them most likely a rented box or an exposed tenant rather than the operator's own machine. The class is an assessment from the certificate, not proof of who runs any one host; a class B console co-located with reseller infrastructure would move to class A, and a class A console that goes dark on its own moves to the public record. Under NSS's disclosure plan the class A consoles are held first for law enforcement, and the class B hosts are notified before any address is published, so no console address is printed in this edition.

The artifacts, and how far they go

Every console was read read-only on 14 November 2026: for each, NSS holds the address, the port, the HTTP status (200 on all 24), the exact page title, the certificate issuer organisation and validity, and the UTC time of the reading. The readings hold no credential, no form content and nothing beyond the single public landing page; a fake value was never submitted because no form was touched. The machine-readable, per-console evidence set, with the exact strings and each reading's time, travels with the restricted edition shared with law enforcement and the notified hosts; it is held from this public edition under the disclosure plan. What ships publicly is the counts, the fingerprint and the detection below.

What NSS cannot say

- NSS read each console's public landing page and certificate from outside. It did not log in, drive the console, or see who is sent to one or who operates it. The operators are unknown.
- The class A and class B split is an assessment from the certificate, not proof of control of any one host. NSS names no operator and makes no country-of-origin claim.
- NSS does not run an internet-wide census of exposed consoles, so the 24 are what it confirmed from hosts already in its records, not an exhaustive list; the researchers the FLASH cites put the exposed total above 1,600.

- The gateway-style names NSS adds are candidates by naming and certificate history. The one apparent tie between them, a shared name-server pair, was tested and rejected; NSS does not claim they are one operator's.

Detection you can deploy

NSS ships signatures for the behaviour, not only the names, because addresses rotate and the fingerprint outlasts them, though not a rename of the console's displayed brand (see the update of 18 November 2026). Each carries a false-positive note, and each was validated against NSS's stored readings of the 24 consoles from 14 November 2026. The rules key on the framework name, which is public in the FBI FLASH and in the vendor reporting it cites; the full localised console title and the two class A issuer strings ship as data in the indicator file and the detection repository, so a rule can be tightened from the file. No console address appears in any rule.

- **The page-identity signature (primary, high recall).** Alert on an HTTP 200 response whose HTML title names the framework in its localised console wording. Validated: matched all 24 stored console readings; it is the element that confirmed every one. Written to the title, not one hostname, so a hostname change does not evade it; a console whose displayed brand has been renamed does (see the update of 18 November 2026). False-positive note: the framework name is an uncommon token in a page title, but confirm a match is not your own asset-management or design software of a similar name before you block.

- **The certificate-issuer signature (secondary, high precision).** Alert on a TLS certificate whose issuer organisation names the framework. Validated: matched the 2 self-hosted consoles and nothing else in the set. Near-zero false positive: an issuer organisation that names the framework is the self-hosted install naming itself. Run it across your own certificate inventory and your passive TLS records.

The two signatures, as rules you can drop in and then tighten with the full strings from the indicator file:

```
# Suricata: a self-hosted console's certificate issuer names the framework
alert tls any any -> any any (msg:"NSS-AX-01 ARTEX console self-signed cer
  tls.cert_issuer; content:"ARTEX"; nocase; sid:3200101; rev:1;)

# Suricata: a console landing page whose title names the framework (high r
alert http any any -> any any (msg:"NSS-AX-01 ARTEX console page identity"
  file_data; content:"<title"; content:"ARTEX"; distance:0; within:120; no

// YARA: run over a captured HTTP response body
rule NSS_AX01_artex_console_identity {
  meta:
    author = "NSS Research"
    reference = "NSS-AX-01; FBI FLASH-20261113-001"
    date = "2026-11-17"
    note = "validated against NSS's stored readings of 24 consoles, 14 Nov
  strings:
    $title = /<title>[^<]{0,40}ARTEX/ nocase
    $o     = "ARTEX" nocase        // also the self-signed issuer organisa
  condition:
    $title and #o >= 1
}
```

A Sigma rule for a proxy or web-gateway log follows the same shape: `title|contains: 'ARTEX'` on an HTTP 200, flagged as assessed where you cannot read the page title from your logs. Tighten any of these with the exact localised title and the two issuer strings from the indicator file; keep the framework-name match as the portable core, since it is what survives an address change.

- **Blocklist-ready, each on its own.** The FLASH's own 24 addresses and one domain and the reseller and routing names below, at DNS and at the egress gateway; the page-title match for a web-gateway rule; and the certificate-issuer string for a TLS rule. Take only what fits your controls. The console addresses are held, so block the fingerprint, not an address list.

The reseller and gateway layer

The FLASH tells defenders to watch for the model-gateway and reseller infrastructure the framework uses (passage 3 at the top of the page), and gives one domain. NSS holds 9 additional reseller and routing names of that layer; five of them entered its records on 31 October. Public certificate records show certificates for the FLASH's domain from 5 August 2026 and 3 host names under it on no list NSS reads. NSS's own records hold 10 gateway-style names from before the FLASH that no list NSS reads carries.

Keep two kinds of thing apart here. The self-hosted model-gateway and aggregator applications the FLASH names, and that Amazon Threat Intelligence reports the actors harvesting model-API keys from, are legitimate software and an exposed attack surface, not the operators' own infrastructure. A name or a service that simply runs one of those products is a watch indicator for egress logs, to alert on and to inventory for exposure, never a thing to block outright. The ${C[.]gatewayNames} gateway-style names NSS adds are the other kind: registered names that imitate a model vendor's brand, offered as candidate leads by naming shape alone, with no tie to a console established.

Several of these names share a name-server pair at a large delivery network, which looks like an operator link. NSS tested that link and rejected it: each of the pair's two name servers fronts hundreds of unrelated zones, from retail to casinos (more than 400 behind one, more than 190 behind the other), so the pair is a provider default, not a tie. NSS draws no tie between these names: they share a naming shape and nothing in NSS's records links them to one operator. This paper reports the apparent tie that failed as well as the ones that held, because a defender deciding what to block needs both.

How it maps to ATT&CK

TECHNIQUE	WHAT NSS SAW

T1583.001 Acquire Infrastructure: Domains	Reseller, routing and gateway-style names of the same layer; the FLASH's domain certificated from 5 August 2026 in the public record
T1583.004 Acquire Infrastructure: Server	Consoles stood up on commercial cloud and hosting addresses
T1588.002 Obtain Capabilities: Tool	The framework itself, driven from the consoles confirmed here

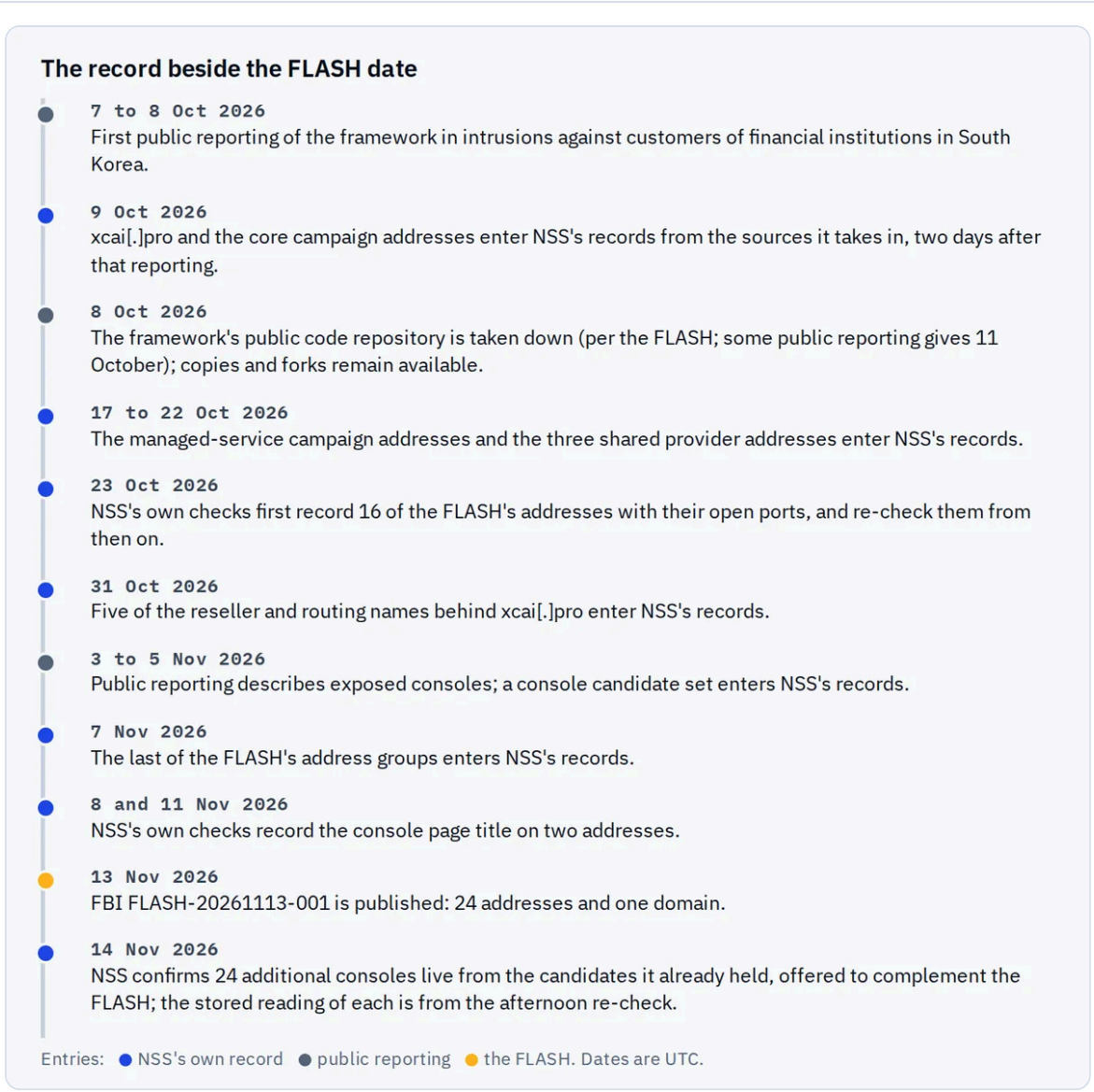
What a defender can look for

In order of priority, and alongside the FLASH's own mitigations:

1. Alert on the console's page identity and, where present, on a certificate whose issuer names the framework, across your own internet-facing estate. Treat any match as an exposed console to isolate.
2. Block the FLASH's 24 addresses and one domain, and the reseller and routing names in the list below, at DNS and gateway.
3. Watch the gateway names NSS surfaced as leads: they are candidates, not confirmed, so alert rather than block, and tell us if you see them resolve to something you can act on.
4. For the consoles on commercial cloud, the host is most likely an exposed tenant: notify the hosting network rather than treat the tenant as the operator.

NSS keeps checking these indicators and will update this page; a name that stops resolving is recorded with the date.

The list below is the FLASH's own indicators that NSS corroborates, each already public in the FBI FLASH, and each opens as a casefile in NSS Investigate. No console address is printed here or in the download file: every one of the 24 is held under NSS's disclosure plan while law enforcement and the exposed hosts are handled. The console deliverable in this edition is the counts, the fingerprint and the tested detection above; the download file carries each listed row's provenance and host type.



The record beside the FLASH date. NSS's own entries, the public reporting the FLASH cites and the FLASH itself are marked apart, so a reader has a dated record to corroborate against. Dates are UTC.

The NSS tools used

> Investigate

Read the casefile of every FLASH indicator and of each console candidate: the dated record, what the address served, and the certificate.

> Scan

Re-read each indicator's verdict to agree with Investigate, surfaced the host names the public record carries under the FLASH's domain, and tested the shared-infrastructure link on a gateway name.

> Tools

> Family finder

Chained reads of NSS's own records over a reseller name, its recorded address and the names seen on it, each step feeding the next.

Grouped the gateway names NSS recorded itself and showed each name's record date and verdict, and stated plainly where names share only a shape.

> Hunt
Searched NSS's library of reporting for the framework and returned the public reporting this paper builds on.

Indicators

All 22 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
xcai[.]pro	Domain	The one domain in FBI FLASH-20261113-001: a model API reseller name used with the framework; in NSS's records from 9 Oct 2026; no longer resolving on 14 Nov 2026
101[.]53[.]80[.]20	IP address	Listed in FBI FLASH-20261113-001; in NSS's records from 9 Oct 2026
103[.]248[.]148[.]84	IP address	Listed in FBI FLASH-20261113-001; in NSS's records from 9 Oct 2026
124[.]155[.]252[.]63	IP address	Listed in FBI FLASH-20261113-001; in NSS's records from 9 Oct 2026
144[.]172[.]64[.]128	IP address	Listed in FBI FLASH-20261113-001; in NSS's records from 17 Oct 2026
144[.]172[.]64[.]60	IP address	Listed in FBI FLASH-20261113-001; in NSS's records from 19 Oct 2026
144[.]172[.]64[.]99	IP address	Listed in FBI FLASH-20261113-001; in NSS's records from 19 Oct 2026
154[.]201[.]79[.]246	IP address	Proxy address named in FBI FLASH-20261113-001; in NSS's records from 9 Oct 2026

178[.]16[.]54[.]129	IP address	Listed in FBI FLASH-20261113-001; in NSS's records from 7 Nov 2026
199[.]19[.]95[.]66	IP address	Listed in FBI FLASH-20261113-001; in NSS's records from 7 Nov 2026
199[.]19[.]95[.]67	IP address	Listed in FBI FLASH-20261113-001; in NSS's records from 7 Nov 2026
199[.]19[.]95[.]68	IP address	Listed in FBI FLASH-20261113-001; in NSS's records from 7 Nov 2026
203[.]160[.]133[.]172	IP address	Listed in FBI FLASH-20261113-001; in NSS's records from 9 Oct 2026
205[.]214[.]59[.]31	IP address	Listed in FBI FLASH-20261113-001; in NSS's records from 9 Oct 2026
209[.]209[.]85[.]38	IP address	Listed in FBI FLASH-20261113-001; in NSS's records from 9 Oct 2026
23[.]158[.]220[.]98	IP address	Listed in FBI FLASH-20261113-001; in NSS's records from 9 Oct 2026
23[.]248[.]249[.]90	IP address	Listed in FBI FLASH-20261113-001; in NSS's records from 9 Oct 2026
31[.]77[.]229[.]35	IP address	Listed in FBI FLASH-20261113-001; in NSS's records from 7 Nov 2026
38[.]244[.]50[.]120	IP address	Console host named in FBI FLASH-20261113-001; in NSS's records from 9 Oct 2026, with NSS's own checks from 23 Oct
85[.]11[.]167[.]52	IP address	Listed in FBI FLASH-20261113-001; a listing in NSS's records since June 2026 for unrelated activity; in the framework's context from 7 Nov 2026
85[.]11[.]168[.]45	IP address	Listed in FBI FLASH-20261113-001; in NSS's records from 7 Nov 2026
91[.]92[.]240[.]238	IP address	Listed in FBI FLASH-20261113-001; a listing in NSS's records since 2024 for unrelated activity; in the framework's context from 7 Nov 2026

ALL 22 INDICATORS: CSV JSON also on GitHub No sign-up.

Check an indicator from this paper

How we know

What this rests on

- Every FLASH indicator is corroborated in NSS's records, each with the date it entered them, as read on 14 November 2026. The listing state of the FLASH domain was read through the public check on 14 November 2026 at 13:36 UTC.
- Each console was confirmed by loading its single public landing page and reading its certificate on 14 November 2026: the HTML page title, the HTTP status, and the certificate issuer and expiry. No login, no form, no payload, no directory listing, nothing beyond the one page. All 24 answered HTTP 200 and carried the same page title; 2 carried a certificate whose issuer organisation names the framework.
- The reseller names and the gateway-style names are from NSS's own records, with their record dates. The host names under the FLASH domain, and its certificate dates from 5 August 2026, are from the public certificate record. The shared-infrastructure test and its zone counts are from NSS's own records, read the same day.
- The detection signatures were validated against NSS's stored readings of the 24 consoles from 14 November 2026: the page-identity signature matched all 24; the certificate-issuer signature matched the 2 self-hosted consoles. The exact strings behind the rules ship as data in the detection repository.
- Verdicts in the indicator list are as read on both Investigate and Scan on 14 November 2026; only indicators where the two agree on a band of Suspicious or higher are listed. Every console address is held from this edition under NSS's disclosure plan, so the indicator file carries the

FLASH's own corroborated indicators, each already public in the FBI FLASH.

- Update of 18 November 2026: the 24 consoles were read twice through NSS's controlled capture path, one landing-page load each: from 19:26 to 20:08 UTC (page title and HTTP status), and again at about 20:34 to 20:36 UTC (page title, HTTP status and the certificate, with both issuer fields read). The 23 consoles confirmed since 14 November were read the same way, each twice, from about 20:43 UTC on 18 November into the early hours of 19 November UTC. The FLASH's domain and the nine reseller and routing names were read from public DNS on two independent resolvers at 19:21 UTC, and the FLASH's domain from the public certificate record the same evening.

What we cannot say

- NSS does not run an internet-wide census of exposed consoles. The 24 consoles are those it confirmed from addresses already in its records, not an exhaustive list; the researchers the FLASH cites put the exposed total above 1,600.
- Most consoles sit on commercial cloud or hosting addresses and are most likely exposed third-party tenants, not the operator's machines. The two-class split is an assessment from the certificate, not proof of who runs any host; NSS draws no operator link between the consoles.
- The gateway-style names NSS surfaced from its own records are candidates by naming and certificate history. The one apparent link between them, a shared name-server pair, was tested and rejected; several sit behind a delivery network whose origin NSS did not fetch.
- The country split counts the 16 consoles with a hosting-country record in the public routing data; 8 have none yet.
- NSS reads an address's public page and certificate; it does not see who is sent to a console or who operates it. The operators are unknown.
- Every console address, the reseller resolved addresses and the gateway-set backend address are held from this public edition under NSS's disclosure plan (docs/207), while law enforcement and the

exposed hosts are handled; the counts and the fingerprint are complete.

- No console was read on 15, 16 or 17 November 2026, so a change seen on 18 November is dated only as by that day. The two reads of 18 November differ on 3 of the 24 consoles; both are given and neither is preferred.
- This paper is not attributed to any named group. Public reporting names clusters; NSS makes no attribution and does not merge those names. NSS-AX-01 is NSS's own name for this case.

Use and citation

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

```
Nexus Sentinel Station (NSS), "24 additional ARTEX consoles live on 14 November 2026, and the reseller layer behind them: a companion to the FBI FLASH", NSS-AX-01, 17 Nov 2026. https://nsshq.com/research/artex-consoles-beyond-the-flash
```

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-RH-01: Lottery redirect names on a shared delivery network: technical analysis

NSS-OC-01: Linked hosting clusters and the purchase batches behind them: technical analysis

NSS-TK-01: Fake imToken download sites push an Android app that sends recovery phrases and private keys to one server: technical analysis

---

This paper is offered in support of FBI FLASH-20261113-001 and of the public research on ARTEX from Microsoft, Wiz, Google Threat Intelligence Group and Mandiant, Amazon Threat Intelligence and the other teams the FLASH cites; it builds on that work and does not stand against any of it. NSS is not affiliated with the FBI, with those research teams, with any hosting company, delivery network, certificate authority or model provider referred to here, or with any product vendor whose customers public reporting says were targeted. They are named, where they are, only because the FLASH or the public records name them; nothing here says any of them knew of or took part in the activity. The gateway-style names in this paper imitate the brand of DeepSeek, a model vendor that is not involved. The console operators are unknown, and many console hosts are likely exposed or compromised third parties.