FULL REPORT · ENTERPRISE EXPLOITATION · MONOGRAPH 70 / 69 · 16 MIN READ

Seeyon OA Spraying: JNDI Listeners and SSRF Polling

Inside a 1,180-entry China-hosted adversary workbench combining Seeyon OA password spraying, seven-port JNDI callback logs, 21-subdomain web-backup harvesters, and minute-interval SSRF polling

BY
Odin by Brandefense

PUBLISHED
19 November 2026

READING TIME
16 min read

EDITION
Version 1.1 · TLP:CLEAR

SCOPE
Prepared November 2026

1. Executive Summary

IN SHORT

An open TCP 8000 directory on a China-hosted adversary workbench recorded on 19-26 November 2026 reported 2,105 files and yielded 1,180 deduplicated entries (51.24 MB). Stored logs record seven-port JNDI and TCP callbacks, 445 invalid Seeyon OA login attempts, 21-subdomain backup sweeps, and 9,363 refused SSRF polls. Enforce OA MFA, delete webroot backups, and block JVM internet egress.

Enterprise office-automation portals and education gateways often share edge networks with Java backend services and legacy web roots. Disabled login challenges or forgotten site archives let operators combine credential spraying, naming callbacks, backup harvesting, and proxy polling on one host. This adversary workbench groups active activity into three tracks and shows the older batch-script folder separately.

Between 19 and 26 November 2026, Odin by Brandefense analyzed an open HTTP directory on TCP port 8000 of a China-hosted VPS (`Workbench A`). When last recorded on 26 November 2026 at 04:46 UTC, that directory reported 2,105 files.

The reviewed inventory contains 1,180 distinct entries across 816 sized files totaling 51,239,679 bytes (51.24 megabytes) and 364 unsized entries. Analysts inspected 59 stored files directly in content.

Stored logs and target lists reference higher-education and government portals. Odin by Brandefense therefore publishes zero IPv4 addresses and zero file SHA-256 digests. `Workbench A` 's address, target addresses, portal domains, archive names, and range names are withheld.

1. **Seven listener ports logged live target callbacks on 16 and `18 November 2026`.**
   Logs `log4j_hits.log` and `oob_out.log` (1,363 lines each) bound `TCP 1099`, 1389, and 8888 on `16 November` and logged hits within 13 seconds. On `18 November`, `i5884_hits.log` (747 lines) bound `TCP 10990`, 13890, 13891, and 18888, logging `hello-test-13890` (`target RCE unverified`).

2. **Seeyon OA password spraying failed across 445 records while REST probes returned `HTTP 200`.**
   Scripts `spray_oa3.py` and `puredes.py` tested `'1234567890'` and `'111111'` on `/seeyon/main.do` when `verifyCode='false'`, logging 0 valid logins. Separately, `pjxt/probe1.tsv` (519 lines) hit `/api/v2/AIReport/reports` and `/api/v2/article/articles`, receiving `HTTP 200` and state 2003 warnings.

3. **Automated harvesters swept `.rar` and `.zip` backups across 21 portal subdomains.**
   Folders `wb/` and `wb2/` (245 entries) pair `fetch_rar.py`, `fetch_remote.py`, and `fetch2.py` to pull exposed webroot archives. Across the full workbench, 17 archive entries account for 30.01 megabytes (58.6% of sized bytes).

4. **Minute-interval SSRF pollers, port sweeps, and `31 May` scripts complete `Workbench A`.**
   Log `ssrf782/poll.log` (9,363 lines) polled an endpoint every minute from `16 November` and logged repeated connection-refused errors. Scan file `i6530/probe_out.jsonl` checked 26 hosts on `TCP 1433, 3306, 4444, 5000`, while `/awd_tools/` holds 44 files dated `31 May 2026`.

Three Decisions for Enterprise Security Leaders

1. **Enforce server-side CAPTCHA lockouts and MFA on Seeyon OA and REST APIs.** Never rely on client-visible CAPTCHA flags, block weak default passwords, and validate bearer tokens strictly on `/api/v2/*` routes.
2. **Delete compressed backup archives from webroots and block archive URLs.** Purge `.rar`, `.zip`, and `.dbf` files across all portal subdomains and block archive extensions at reverse proxies.
3. **Upgrade Log4j2, block outbound JVM callback ports, and normalize proxy headers.** Keep Log4j2 on `2.17.1` or later, enforce default-deny JVM egress rules, and reject dual `Content-Length` and `Transfer-Encoding` headers.

The Study in Numbers

Number	What it is
2,105	Files reported by the open `TCP 8000` directory on `Workbench A` when last recorded on `26 November 2026 at 04:46 UTC`
1,180	Distinct reviewed entries across six workspace zones (816 sized files and 364 unsized entries)
816	Sized files totaling 51,239,679 bytes (51.24 MB), including 17 archive entries (11 sized = 30,007,700 bytes, 58.6% of sized bytes)
59	Stored files inspected directly in content (1,121 entries analyzed from paths, byte sizes, and extensions)
21	Provincial education portal subdomains swept by `wb/` and `wb2/` web-root archive harvesters (245 entries; subdomain names withheld)

2. Workbench Architecture, Six-Zone Reconciliation, and Callback Ports

`Workbench A` ran on a **China-hosted cloud virtual private server** (IPv4 address withheld) exposing an open HTTP directory on `TCP 8000`. Odin by Brandefense recorded the server across `19-26 November 2026`, with the final capture on `26 November 2026 at 04:46 UTC`. Platform defenders

use external attack surface management to find forgotten subdomain backup archives and exposed OA login pages early.

SOC analysts also apply cyber threat intelligence to connect multi-port JNDI callback infrastructure with portal spraying and proxy probes. Figure 1 maps the three active tracks and the retained May folder on `Workbench A`.

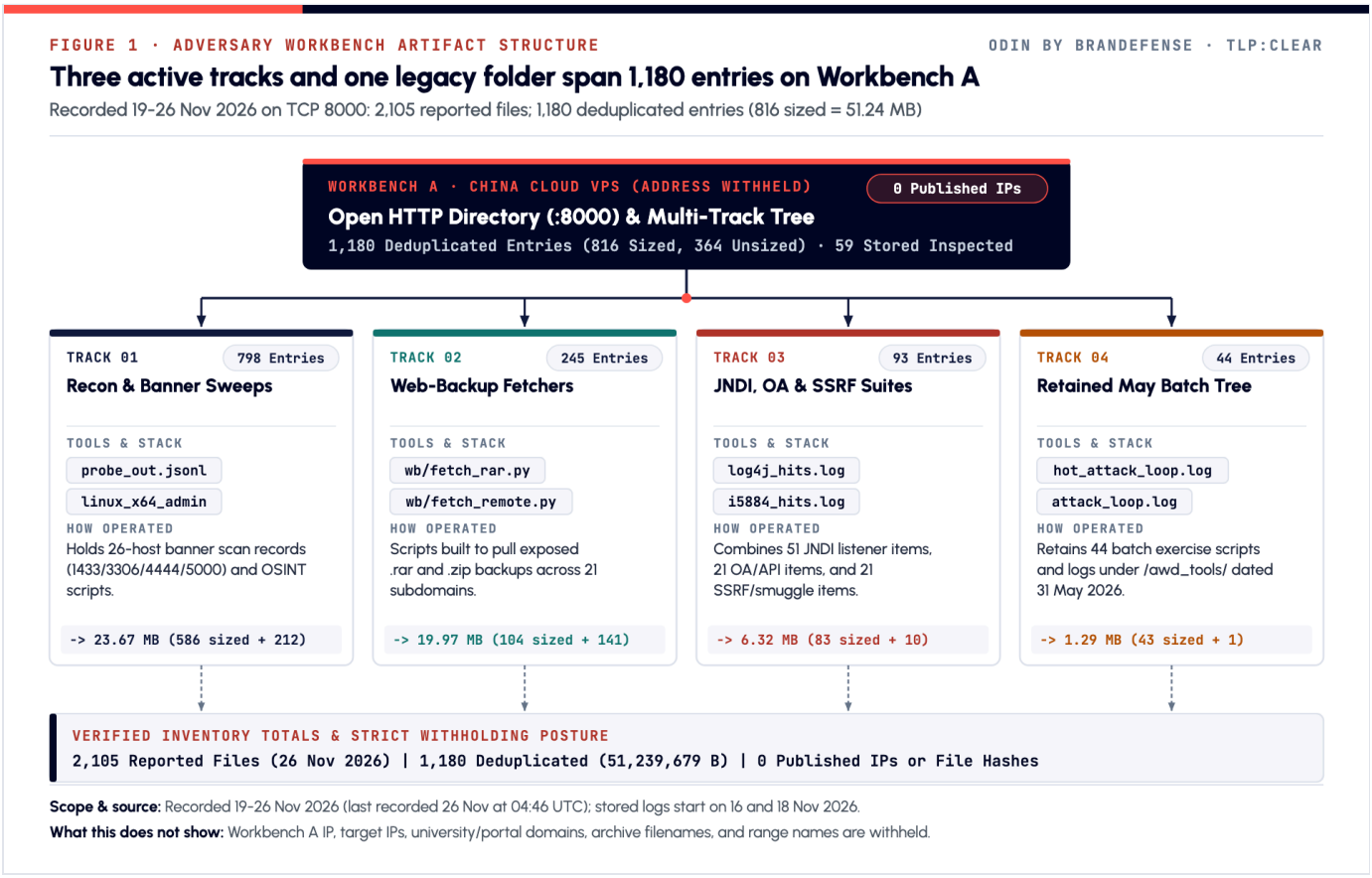

Figure 1: Three active tracks and one legacy folder span 1,180 entries on Workbench A

Reconciling the 2,105 Reported Files and 1,180 Deduplicated Entries

On `26 November 2026 at 04:46 UTC`, the `TCP 8000` directory listing reported **2,105 files**. This report covers **1,180 distinct entries**; it does not characterize the remainder of the server's reported files.

Those **1,180** entries comprise **816 sized files** totaling **51,239,679 bytes (51.24 MB)** and **364 unsized entries**. Analysts inspected **59 stored files** in content, while the other **1,121** entries are analyzed from paths, byte sizes, and extensions.

Evidence across the **59** stored files consistently establishes `Workbench A` as an **adversary staging workbench**. It combines live external callback logs, university OA password spraying, portal API probing, **21**-subdomain backup harvesting, and minute-interval SSRF polling. All server and target IPs, portal domains, victim-named archives, and file hashes are withheld.

Workspace zone	Top-level dirs	Deduplicated entries	Share (%)	Sized files	Unsized entries	Sized bytes	Operational role
Issue-Numbered Exploit, JNDI & Probe Trees (`/iNNNN/` & Root Listeners)	1+	588	49.8%	469	119	9,981,449	Holds JNDI logs (`log4j_hits.log`, `oob_out.log`, `i5884_hits.log`), `ldap_responder.py`, `probe_out.jsonl`, and smuggling scripts.
Web-Archive Harvester Trees (`/wb/` & `/wb2/`)	2	245	20.8%	104	141	19,968,187	Holds `fetch_rar.py`, `fetch_remote.py`, `fetch2.py`, JSONL logs, and batch lists across **21** subdomains (names withheld).
Root Controller Binaries, Telemetry & Environment Configs	0 (root)	184	15.6%	155	29	19,097,216	Holds `/linux_x64_admin` (**2.50 MB**), RPM shards, `log4j_payload_sent.json`, `spray_11457.log`, and withheld snapshots.
External OSINT & Code-Search Scripts (`/osint/`)	1	94	8.0%	22	72	128,088	Holds **22** sized OSINT and code-search scripts/outputs (**128,088** B) and **72** unsized items.

Workspace zone	Top-level dirs	Deduplicated entries	Share (%)	Sized files	Unsized entries	Sized bytes	Operational role
Legacy Batch-Exploit Harness Folder (`/awd_tools/`)	1	44	3.7%	43	1	1,289,047	Holds **44** entries dated `31 May 2026` (`hot_attack_loop.log` , `attack_loop.log` , and batch scripts).
OA Password-Spray, Portal API & SSRF Polling Modules	3	25	2.1%	23	2	775,692	Holds `oa_spray/` (`spray_oa3.jsonl`), `pjxt/` (`probe1.tsv`), and `ssrf782/` (`poll.log` 403,032 B).
Combined deduplicated inventory	**8 + trees + root**	**1,180**	**100.0%**	**816**	**364**	**51,239,679**	**Reported 2,105 files on `TCP 8000` (`26 Nov 2026`); 59 stored files inspected.**

A second breakdown reconciles the same **1,180** entries (**816** sized, **364** unsized, **51,239,679** bytes) across seven file types. Text logs and structured captures lead by count (**650**, **55.1%**), whereas **17** archives make up **58.6%** of sized bytes (**30.01 MB**).

Artifact class (`kind`)	Deduplicated entries	Share (%)	Sized files	Unsized entries	Sized bytes	Verified extensions & contents
Logs, captures & structured text (`text`)	650	55.1%	537	113	10,604,554	149 `.txt`, 79 `.body`, 70 `.html`, 61 `.hdr`, 58 `.bin`, 51 `.log`, 36 `.json`, 22 `.out`, 22 `.xml`, 18 none, and 84 JSONL/TSV items.
Python, shell & web scripts (`script`)	285	24.2%	232	53	7,137,591	155 `.py`, 86 `.sh`, 12 `.aspx`, 11 `.js`, 11 `.asp`, 8 `.php`, and 2 `.jsp` files.
Database table files (`data`)	139	11.8%	7	132	148,362	139 `.dbf` database table items (7 sized = 148,362 B + 132 unsized).
Error traces, headers & DB shards (`other`)	84	7.1%	24	60	796,183	34 `.err`, 21 extensionless, 12 `.hdr`, 7 `.body`, 2 `.css`, 2 `.lock`, 3 RPM shards, 1 `.ser`, and 2 misc items.
RAR & ZIP archives (`archive`)	17	1.4%	11	6	30,007,700	13 `.rar` and 4 `.zip` archives (11 sized = 30.01 MB + 6 unsized; victim-subdomain filenames withheld).
Compiled Linux & utility binaries (`exe`)	4	0.3%	4	0	2,542,932	4 sized extensionless Linux binaries including `/linux_x64_admin` (2,495,372 B).
Binary image/asset payload (`image`)	1	0.1%	1	0	2,357	1 sized `.bin` asset file (2,357 B).
Total	**1,180**	**100.0%**	**816**	**364**	**51,239,679**	**Exact byte-level parity (51.24 MB).**

Figure 5 partitions all **1,180** entries into six mutually exclusive clusters (`798 + 245 + 51 + 44 + 21 + 21 = 1,180`). Target recon sweeps (**798**) and web-root archive fetchers (**245**) account for **88.4%** of all entries.

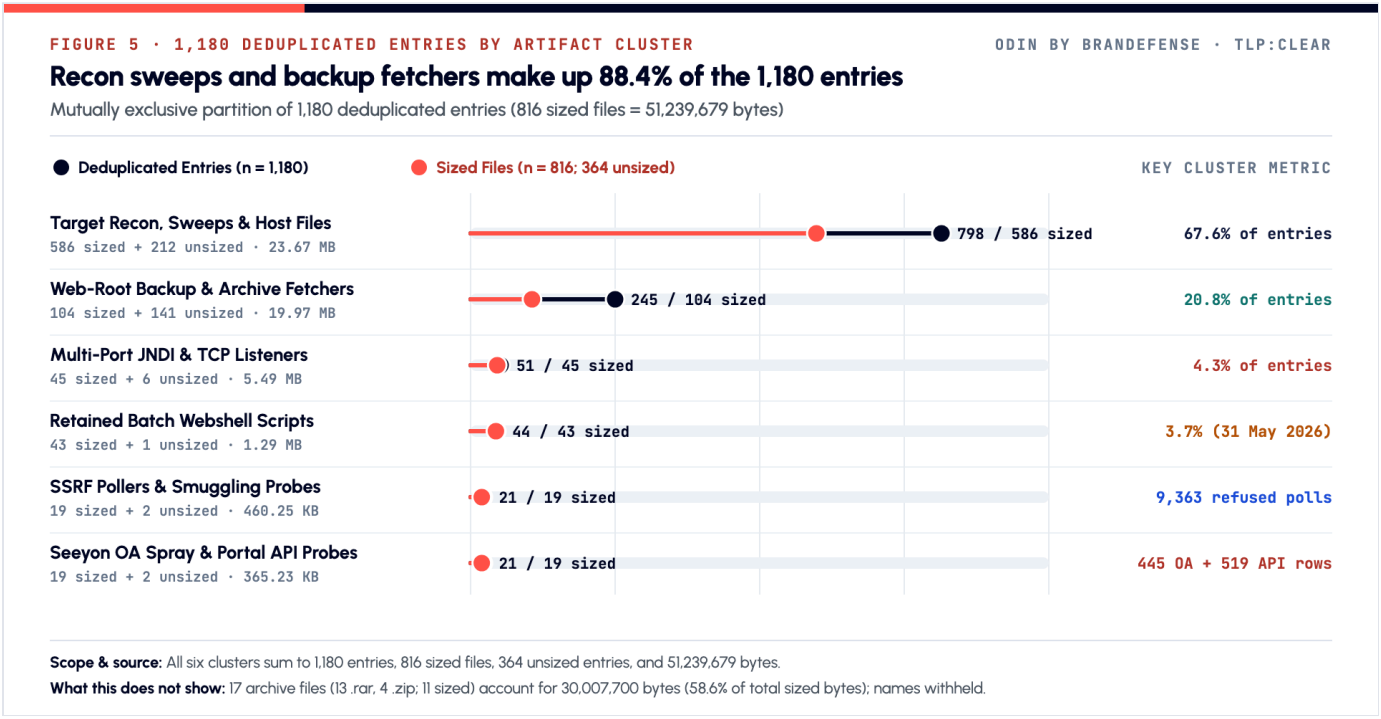

Figure 5: Recon sweeps and backup fetchers make up 88.4% of the 1,180 entries

Seven Callback Ports Alongside Open `TCP 8000`

Stored listener logs document seven TCP callback ports alongside the open `TCP 8000` HTTP directory on `Workbench A`:

- **Primary callback ports (`TCP 1099` , 1389, and 8888).** Bound on `16 November 2026 at 15:26:46 UTC` under `PID 1138045` (`log4j_hits.log` and `oob_out.log`), logging inbound TCP/LDAP hits within **13** seconds.
- **Shifted high callback ports (`TCP 10990` , 13890, 13891, and 18888).** Bound on `18 November 2026 at 10:47:13 UTC` under `PID 1355974` (`i5884_hits.log`), shifting standard JNDI ports upward and logging `hello-test-13890` .

3. Seeyon OA Credential Spraying, Portal API Sweeps, and JNDI Callback Logs

Stored November logs link out-of-band JNDI callback listeners with Seeyon OA password spraying and portal REST enumeration. Figure 3 presents an analytical model distinguishing verified `Workbench A` log events (solid) from refused SSRF polls, staged smuggling scripts, and unverified target RCE (dashed).

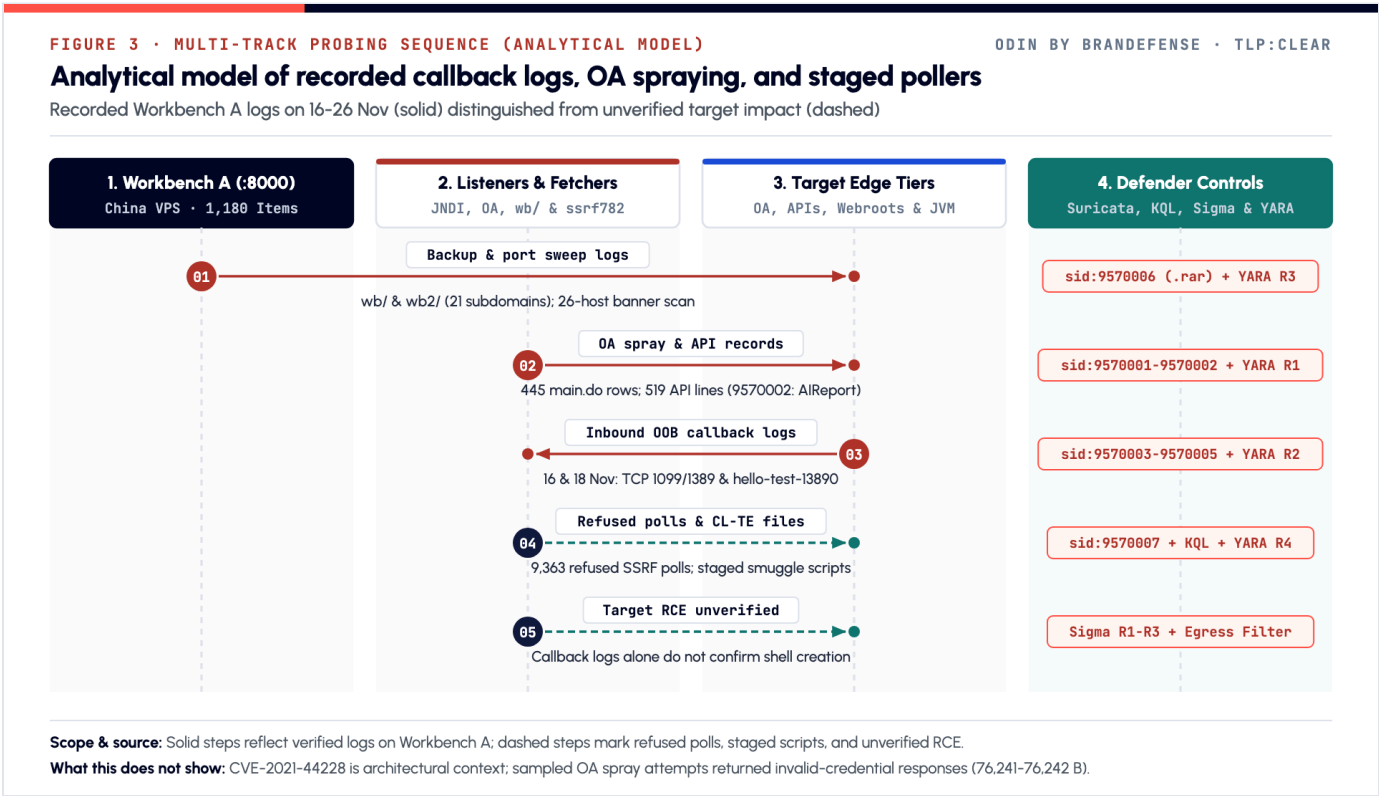

Figure 3: Analytical model of recorded callback logs, OA spraying, and staged pollers

Multi-Port JNDI, LDAP, and Shifted TCP Callback Logs (51 Entries)

Fifty-one entries (**45** sized files = **5,490,096** bytes + **6** unsized) capture out-of-band callback listeners (`[REF-01]` , `[REF-07]`). Root files `log4j_hits.log` and `oob_out.log` measure **1,275,815 bytes (1,363 lines)** each, beside `log4j_payload_sent.json` (**34,030** B). Both logs started on `16 November 2026 at 15:26:46 UTC` (`PID 1138045`) on `TCP 1099` , **1389**, and **8888**. They recorded inbound TCP and LDAP callbacks within **13 seconds** from a withheld target IPv4.

Two days later, `i5884_hits.log` (**112,102** bytes; **747 lines**) started on `18 November 2026 at 10:47:13 UTC` (`PID 1355974`). It bound `TCP 10990` , **13890**, **13891**, and **18888**, recording inbound hits including the **16-byte string** `hello-test-13890` . Issue folders add

`/i8022/ldap_responder.py` (**6,674** B), `/i8022/conn.log` (**1,381,378** B), `/i8022/responder.out` (**1,380,459** B), and `/i1601/lsn.py` (**2,415** B).

NVD describes `CVE-2021-44228` in Apache Log4j2 `2.0-beta9` **through** `2.15.0`, excluding `2.12.2`, `2.12.3`, and `2.3.1` (`[REF-01]`). Version `2.15.0` disabled lookup substitution by default; `2.16.0` removed the vulnerable functionality (`[REF-01]`, `[REF-03]`). Here, callback logs confirm outbound network reachability from the target network, while remote class loading and target command execution remain unverified.

Seeyon OA Credential Spraying and Portal REST API Probes (21 Entries)

Twenty-one entries (**19** sized files = **365,230** bytes + **2** unsized) target higher-education OA and portal endpoints (`[REF-06]`, `[REF-10]`). Inside `oa_spray/`, `spray_oa3.py` (**6,259** B) and `puredes.py` (**4,406** B) sit beside `spray_11457.log` (**17,584** B). Output file `spray_oa3.jsonl` measures **85,057** bytes across **445 JSONL records**.

Those scripts target a regional university's Seeyon OA `/seeyon/main.do` login endpoint (domain withheld), testing `'1234567890'` and `'111111'` when `verifyCode='false'`. Every sampled attempt returned invalid-credential responses of **76,241 to 76,242 bytes**, confirming **0 valid logins** in sampled records.

Inside `pjxt/`, `probe1.tsv` (**79,727** bytes; **519 lines**) sits with `probe_postall.tsv` (**51,745** B) and `api_paths.txt` (**17,946** B). Companion files include `chunks.tsv` (**17,029** B), `dl.log` (**15,242** B), and a **32,309**-byte withheld URL list. File `probe1.tsv` sweeps `/api/v2/AIReport/reports` and `/api/v2/article/articles`, logging `HTTP 200` JSON payloads and state **2003** concurrent-session warnings.

4. Web-Root Backup Harvesters, SSRF Pollers, and Retained Batch Scripts

`Workbench A` also runs multi-subdomain web-backup harvesters, minute-interval server-side request forgery pollers, HTTP request-smuggling scripts, and multi-port banner scans. Figure 4 shows the directory layout and bound listener ports on the China VPS.



Figure 4: Workbench A pairs an open TCP 8000 directory with seven callback ports

Automated Web-Root Archive Harvesters (245 Entries)

Folders `wb/` and `wb2/` hold **245** entries (**104** sized files = **19,968,187** bytes + **141** unsized; `[REF-08]`). Harvester scripts include `wb/fetch_rar.py` (**2,522** B), `wb/fetch_remote.py` (**3,998** B), and `wb2/fetch2.py` (**5,064** B). Run outputs sit in `wb2/out/_log.jsonl` (**57,362** B), `_log_prev.jsonl` (**18,420** B), and `wb2/run.log` (**11,696** B). Three withheld JSON batch lists measure **28,196** B, **16,057** B, and **10,142** B.

Together they pull exposed `.rar` and `.zip` web-root backups across **21 subdomains** of a provincial education portal (all subdomain and archive names withheld). Across the entire **1,180**-entry inventory, **17** archive items (**13** `.rar`, **4** `.zip`; **11** sized) total **30,007,700 bytes (58.6% of sized bytes)**.

SSRF Pollers, Request Smuggling, Banner Sweeps, and `31 May` Scripts (863 Entries)

Twenty-one entries (**19** sized = **460,248** B + **2** unsized) form the SSRF and proxy-smuggling cluster (`[REF-04]`, `[REF-05]`). Wrappers `watchdog.sh` and `ssrf_test.sh` (**3,236** B) pair with `ssrf782/poll.log` (**403,032** bytes; **9,363 lines**) and `http.log` (**9,563** B). Starting `16 November`

`2026`, that loop polled a withheld endpoint every minute and logged repeated connection-refused states.

Sibling scripts `i1616_smuggle3.py` (**12,480** B), `i1616_smuggle.py` (**7,295** B), and `i8059/probe_smug.py` (**6,122** B) stage `CL-TE` smuggling probes (`target bypass unverified`). Companion files `i350/rawhttp.py` (**2,697** B) and `i8059/webvpn_443.json` (**6,842** B) complete the cluster.

Meanwhile, **798** recon entries (**586** sized = **23,666,871** B + **212** unsized) include `i6530/probe_out.jsonl` (**240,202** B). That file records **26 host records** scanned across `TCP 1433`, **3306**, **4444**, and **5000**. The same cluster holds `/linux_x64_admin` (**2,495,372** B), `/osint/` (**94** entries = **128,088** B), and **139** `.dbf` entries (**148,362** B). It also holds RPM shards (**286,719** B and **266,239** B) and withheld snapshots.

Finally, `/awd_tools/` holds **44** entries (**43** sized = **1,289,047** B + **1** unsized), led by `hot_attack_loop.log` (**565,011** B) and `attack_loop.log` (**330,090** B). It also holds `known_path_attack_loop.log` (**200,616** B), `exploit_persist_seed_batch.py` (**10,865** B), and `exploit_php_webshell_batch.py` (**10,160** B). All **44** entries date to `31 May 2026` cyber-range batch exercises retained on the server, and Figure 2 maps all **1,180** entries to detections.

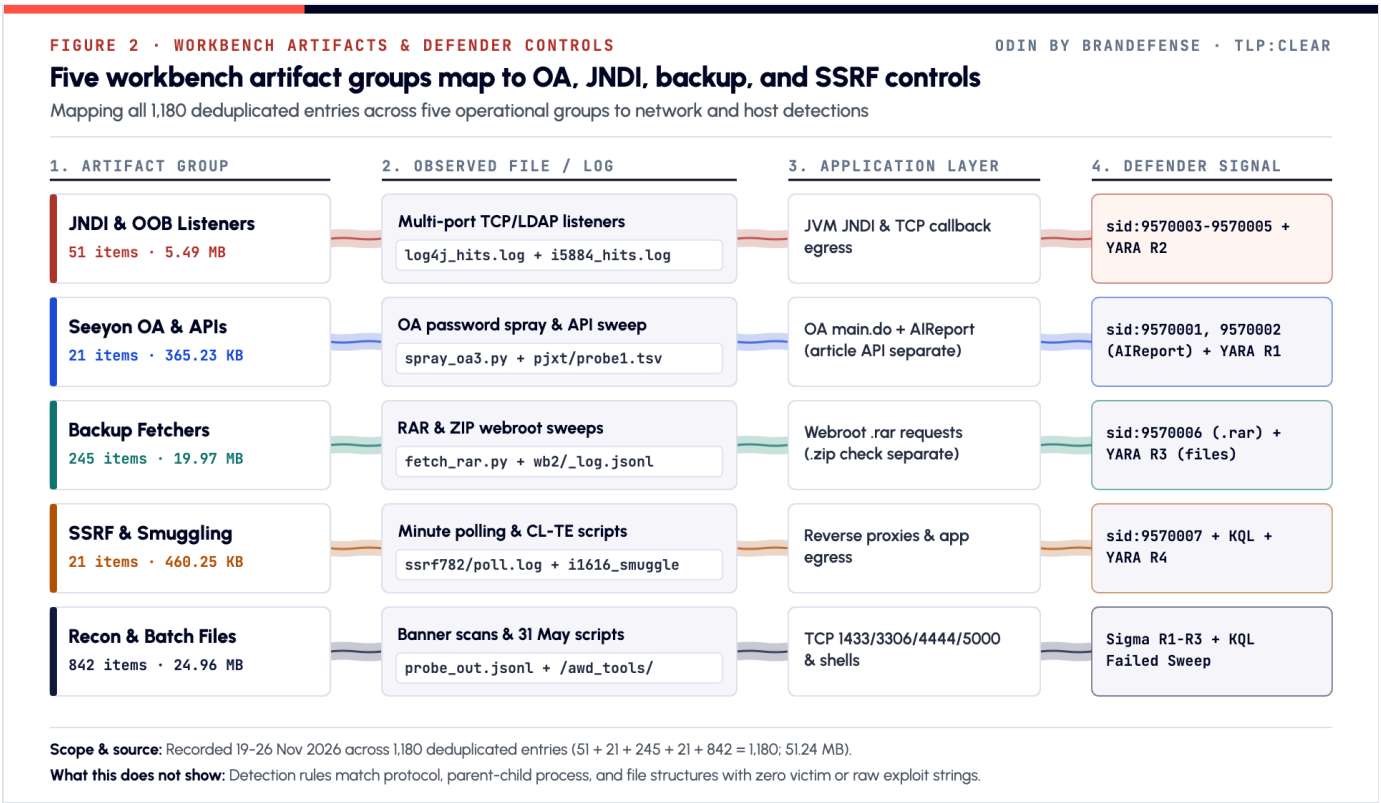

Figure 2: Five workbench artifact groups map to OA, JNDI, backup, and SSRF controls

5. Enterprise OA, JVM, Webroot, and Proxy Exposure Analysis

Platform and security teams should verify four defensive controls mapped directly to `Workbench A`'s artifacts:

Exposure layer	Observed Workbench A evidence	Control to verify	Operational risk
Seeyon OA & REST API auth	`spray_oa3.jsonl` (445 `/seeyon/main.do` records when `verifyCode='false'`; 0 valid) + `pjxt/probe1.tsv` (519 lines, state 2003).	Verify whether OA portals enforce unconditional server-side CAPTCHA/lockouts and MFA (`[REF-06]`, `[REF-10]`) and strict API token checks.	Disabled CAPTCHA challenges let scripts spray weak passwords (1234567890, 111111) without lockouts.
JVM JNDI & high-port egress	`log4j_hits.log` (1,363 lines on 1099/1389/8888) + `i5884_hits.log` (747 lines on 10990/13890/13891/18888, `hello-test-13890`).	Verify Log4j2 (`>= 2.17.1`, `[REF-01]`, `[REF-03]`) and default-deny firewall rules blocking outbound LDAP, RMI, and high TCP ports from JVM subnets.	Unpatched JNDI sinks with open TCP egress permit external naming lookups and callback verification.
Public webroot backup hygiene	`wb/` and `wb2/` (245 entries; `fetch_rar.py`, `fetch_remote.py`) across 21 subdomains; 17 archives = 30.01 MB.	Verify whether deployment scripts delete `.rar`, `.zip`, `.bak`, and `.dbf` files from webroots and block archive extensions at proxies (`[REF-07]`).	Exposed webroot backups leak full source trees, DES/JWT keys, and database credentials.

Exposure layer	Observed Workbench A evidence	Control to verify	Operational risk
Edge proxies & SSRF egress	`ssrf782/poll.log` (9,363 refused polls), `i1616_smuggle*.py`, `probe_smug.py`, and `probe_out.jsonl` (1433/3306/4444/5000).	Verify whether reverse proxies reject dual `Content-Length` + `Transfer-Encoding` headers (`[REF-05]`) and enforce SSRF allowlists (`[REF-04]`).	Proxy smuggling or SSRF sinks let external callers probe loopback services and internal SQL databases.

6. Alternative Hypotheses

Hypothesis	Evidence for	Evidence against	Assessment
Callback logs (`log4j_hits.log`, `i5884_hits.log`) confirm target RCE	Logs record inbound hits within 13s on 1099/1389/8888 (`16 Nov`) and `hello-test-13890` on 13890 (`18 Nov`).	Modern JDKs set `trustURLCodebase=false`, and TCP/LDAP connection logs do not show remote class loading or shell creation.	**Confirmed for OOB reachability only; target RCE unverified.** Treat logs as callback reachability, not target RCE.
Seeyon OA spraying (`spray_oa3.jsonl`) yielded valid logins	`spray_oa3.py` and `puredes.py` logged 445 attempts when `verifyCode='false'`, while `probe1.tsv` got `HTTP 200` JSON replies.	All sampled `spray_oa3.jsonl` rows returned 76,241–76,242-byte invalid-credential responses, and `probe1.tsv` hit separate `/api/v2/*` routes.	**Refuted for sampled OA records.** Zero valid OA logins appear in sampled `spray_oa3.jsonl` entries.
`Workbench A` is a benign student or cyber-range server	Retains 44 `/awd_tools/` flag-loop files dated `31 May 2026` alongside `/osint/` scripts.	Active November 2026 trees spray a university's `/seeyon/main.do`, pull archives across 21 education subdomains, and log live callbacks.	**Contradicted.** Assessed consistently as an **adversary staging workbench** retaining older `31 May 2026` files.

Hypothesis	Evidence for	Evidence against	Assessment
`ssrf782/poll.log` (9,363 lines) retrieved internal data	`watchdog.sh` and `ssrf_test.sh` ran minute-interval polling from `16 November 2026` across 9,363 lines.	Inspected `poll.log` lines record repeated connection-refused errors rather than internal responses.	**Refuted for extraction.** Line volume reflects automated watchdog retries against a refused endpoint.

7. What Defenders Should Do

OA administrators, Java teams, and network defenders should apply five controls in priority order:

1. **Harden Seeyon OA authentication and REST API tokens (`0-48 Hours`).** Patch Seeyon OA portals, enforce unconditional server-side CAPTCHA lockouts and MFA regardless of `verifyCode` flags, and block weak passwords (**1234567890**, **111111**; `[REF-06]` , `[REF-10]`). Enforce strict bearer-token expiration on `/api/v2/*` endpoints returning state **2003** warnings.
2. **Purge compressed backup archives from public webroots (`0-72 Hours`).** Audit every subdomain document root to delete `.rar` , `.zip` , `.bak` , `.sql` , and `.dbf` files (`[REF-07]` , `[REF-08]`). Configure reverse proxies to deny requests ending in archive extensions.
3. **Upgrade Log4j2 and block shifted high-port JVM egress (`Days 1-7`).** Keep Apache Log4j2 on **`2.17.1` or later** (`CVE-2021-44228` in `2.0-beta9` through `2.15.0` , excluding `2.12.2` , `2.12.3` , and `2.3.1` ; `2.16.0` removed lookup functionality; `[REF-01]` , `[REF-02]` , `[REF-03]`). Enforce default-deny outbound TCP firewall rules on JVM subnets so shifted listeners (**10990/13890/13891/18888**) fail closed (`[REF-09]`).
4. **Normalize HTTP framing at edge proxies (`Days 7-14`).** Reject HTTP/1.1 requests carrying both `Content-Length` and `Transfer-Encoding` headers across CDN, WAF, and WebVPN gateways, and prefer end-to-end HTTP/2 (`[REF-05]`).
5. **Enforce SSRF destination allowlists and segment SQL ports (`Days 14-30`).** Restrict URL-fetching services to explicit destination allowlists while blocking loopback and RFC1918 subnets (`[REF-04]`). Isolate `TCP 1433` , **3306**, **4444**, and **5000** inside authenticated database VLANs.

8. Detection Rules

The full rules are in the Detection rules tab. Because all IPv4 addresses and file SHA-256 digests are withheld, each rule file targets protocol, process, egress, and file-structure signals across OA, JVM, and proxy tiers. Static checks passed in the Odin Suricata linter (**0** problems) and offline structural checks across KQL, **3** Sigma rules, and **4** YARA rules. Because live `suricata -T`, `Kusto.Language`, `pySigma`, and `YARA` binaries were not run locally, test each rule in staging first.

Rule file	What it catches
`odin_seeyon_oa_jndi_backup_and_ssrf_hunt.rules`	Suricata 7.x (7 `alert` rules, `sid:9570001`–9570007): inbound `/seeyon/main.do` `verifyCode` POSTs, `/api/v2/AIReport/reports` GETs, hex-escaped `|24 7B|jndi:` headers, `jndi:ldap://` bodies, outbound `hello-test-13890` TCP callbacks on 1099/1389/8888/10990/13890/13891/18888, inbound `.rar` GETs, and dual `Transfer-Encoding: chunked` + `Content-Length:` headers.
`sentinel_jndi_oa_and_ssrf_egress_hunt.kql`	Microsoft Sentinel KQL (7-day lookback): correlates Linux/Windows JVM or web worker child shells and named workbench CLI arguments in `DeviceProcessEvents` with public JNDI egress (389/636/1099/1389/8888/10990/13890/13891/18888) and `ConnectionFailed` sweeps (1433/3306/4444/5000) in `DeviceNetworkEvents`.
`sigma_jvm_shells_harvesters_and_ssrf_loops.yml`	Sigma (3 `process_creation` rules): Linux `/java`, `/nginx`, or `/httpd` spawning shells or transfer tools (Rule 1), Windows `java.exe` or `tomcat9.exe` spawning shells, `curl.exe`, or `whoami.exe` (Rule 2), and Linux execution of `/linux_x64_admin` or named workbench scripts (Rule 3).

Rule file	What it catches
`odin_jndi_oa_and_harvester_artifacts.yar`	YARA (4 `filesize`-bounded rules): Seeyon OA `/seeyon/main.do` DES password-spray scripts (< 128KB), multi-port JNDI/LDAP callback responders (< 256KB), `.rar` and `.zip` web-root archive harvester scripts (< 128KB), and raw-socket `CL-TE` smuggling / SSRF scripts (< 128KB).

8.1 Suricata 7.x Network Signatures (`sid:9570001` –9570007)

Six HTTP `alert` rules and one TCP `alert` rule (`sid:9570005`) cover `Workbench A` 's traffic. Rules `sid:9570001` –**9570004** match `/seeyon/main.do` `verifyCode` POSTs, `/api/v2/AIReport/reports` GETs (hunt `/api/v2/article/articles` separately), hex-escaped `|24 7B|jndi:` headers, and `jndi:ldap://` bodies. Rules `sid:9570005` –**9570007** match outbound `hello-test-13890` TCP payloads, inbound `.rar` GETs (check `.zip` requests separately), and HTTP headers combining `Transfer-Encoding:` , `chunked` , and `Content-Length:` .

None of these `alert` signatures block traffic inline. The six HTTP rules require cleartext HTTP visibility or a TLS-terminating proxy; tune `sid:9570001` around legitimate OA portals and exclude approved mirrors from `sid:9570006` .

8.2 Microsoft Sentinel KQL Hunt

This 7-day Sentinel KQL query correlates JVM and web worker shell spawns with workbench CLI markers. It also flags public JNDI egress (**389**, **636**, **1099**, **1389**, **8888**, **10990**–**18888**) and failed `ConnectionFailed` sweeps to `TCP 1433, 3306, 4444, 5000` . Replace `app-ci-01.corp[.]example` and `sec-bastion-01.corp[.]example` in `ApprovedAdminAndBuildHosts` before scheduling.

8.3 Portable Sigma Process-Creation Rules

Rule 1 catches Linux `/java` , `/nginx` , or `/httpd` spawning shells or transfer tools outside `oa-maint-01.corp[.]example` . Rule 2 catches Windows `java.exe` or `tomcat9.exe` spawning shells, `curl.exe` , or `whoami.exe` outside `oa-win-maint-01.corp[.]example` . Rule 3 catches

`/linux_x64_admin` or named workbench script execution (`ldap_responder.py` , `spray_oa3.py` , `puredes.py` , `fetch_rar.py` , `ssrf_test.sh` , `hello-test-13890`) outside `sec-lab-01.corp[.]example` .

8.4 Bounded YARA File-Structure Rules

Four `filesize` -bounded YARA rules cover these files. Rule 1 matches Seeyon OA DES spray scripts; Rule 2 matches multi-port JNDI callback responders. Rule 3 matches `.rar` and `.zip` harvester scripts; Rule 4 matches `CL-TE` smuggling scripts.

9. Indicators

The Indicators tab holds **0** published indicators (**0** IPv4 addresses and **0** file SHA-256 digests) to protect targeted education and government portals. `Workbench A` 's IPv4 address, all target IPv4 addresses, all portal domains, all victim-named archive filenames, and all file hashes are withheld. Defenders can hunt using the **10** report-only behavioral and protocol markers below.

Marker category	Pattern / protocol artifact	Layer	Defensive hunt & control
Seeyon OA login spray	`POST /seeyon/main.do` with `verifyCode`	HTTP / WAF ingress	Enforce server-side CAPTCHA and MFA (`[REF-06]` , `[REF-10]`); alert via `sid:9570001` and YARA Rule 1.
Portal REST API sweep	`GET /api/v2/AIReport/reports` & `/api/v2/article/articles`	HTTP / API gateway	Enforce strict token validation and rate limits; `sid:9570002` alerts on the AIReport route. Hunt `/api/v2/article/articles` separately.

Marker category	Pattern / protocol artifact	Layer	Defensive hunt & control
JNDI header lookup	Hex 24 7B + `jndi:` prefix in HTTP header	HTTP / WAF ingress	Upgrade Log4j2 `>= 2.17.1` (`[REF-01]` , `[REF-03]`) and alert via `sid:9570003` .
JNDI LDAP body URI	`jndi:ldap://` scheme in HTTP request body	HTTP / API gateway	Disable JNDI lookups (`[REF-02]`) and alert via `sid:9570004` .
Shifted TCP callback	`hello-test-13890` (16-byte payload)	TCP egress (10990–18888)	Block unapproved app-tier TCP egress and alert via `sid:9570005` and YARA Rule 2.
Webroot backup probe	`GET *.rar` archive requests	HTTP / Reverse proxy	Delete archives from webroots and alert on `.rar` requests via `sid:9570006` ; check `.zip` requests separately. YARA Rule 3 hunts harvester files.

Marker category	Pattern / protocol artifact	Layer	Defensive hunt & control
`CL-TE` smuggling	Dual `Transfer-Encoding: chunked` + `Content-Length:`	HTTP edge proxy	Reject ambiguous framing (`[REF-05]`) and alert via `sid:9570007` and YARA Rule 4.
JVM/OA child shell	`java` / `tomcat9.exe` -> `sh` , `bash` , `cmd.exe` , `powershell.exe`	Linux / Windows EDR	Alert immediately on OA or JVM child shells (Sigma Rules 1–2; KQL; `[REF-07]`).
JVM JNDI public egress	`java` / `tomcat9.exe` -> public 389/636/1099/1389/8888/10990/13890/13891/18888	Firewall / EDR	Enforce default-deny internet egress on JVM and OA VLANs (Sentinel KQL; `[REF-09]`).
Failed SSRF sweep	Repeated `ConnectionFailed` from web/JVM worker to 1433, 3306, 4444, 5000	Host / Internal FW	Enforce SSRF allowlists (`[REF-04]`) and hunt failed backend sweeps with KQL; Sigma Rule 3 flags named workbench scripts.

10. Scope and Limits

Odin by Brandefense analyzed adversary staging workbench `Workbench A` on a China-hosted VPS (`TCP 8000`) recorded across `19-26 November 2026` (last recorded `26 November 2026 at 04:46 UTC`). The open directory reported **2,105** files and the reviewed inventory covers **1,180** distinct entries (**816** sized files = **51,239,679** bytes + **364** unsized entries; **59** stored files inspected).

Stored listener and polling logs start on `16 November 2026` (`log4j_hits.log` , `oob_out.log` , `ssrf782/poll.log`) and `18 November 2026` (`i5884_hits.log`). Separately, **44** `/awd_tools/` entries date to `31 May 2026` . Callback hits confirm outbound reachability without confirming

target RCE, sampled `spray_oa3.jsonl` rows (**445**) returned **0** valid logins, and `poll.log` (**9,363** lines) logged connection-refused states. All IPs, SHA-256 digests, portal domains, victim-named archives, and range names are withheld.

11. Sources

1. `[REF-01]` NIST NVD, *NIST NVD - CVE-2021-44228 (Apache Log4j2 JNDI Lookup Remote Code Execution)* (verified on 27 November 2026).
2. `[REF-02]` CISA, *CISA Apache Log4j Vulnerability Guidance* (verified on 27 November 2026).
3. `[REF-03]` Apache Logging Services, *Apache Logging Services - Log4j Security Vulnerabilities Advisory* (verified on 27 November 2026).
4. `[REF-04]` OWASP, *OWASP Server-Side Request Forgery Prevention Cheat Sheet* (verified on 27 November 2026).
5. `[REF-05]` PortSwigger Web Security Academy, *PortSwigger Web Security Academy - HTTP Request Smuggling* (verified on 27 November 2026).
6. `[REF-06]` MITRE ATT&CK, *MITRE ATT&CK - Password Spraying (T1110.003)* (verified on 27 November 2026).
7. `[REF-07]` MITRE ATT&CK, *MITRE ATT&CK - Exploit Public-Facing Application (T1190)* (verified on 27 November 2026).
8. `[REF-08]` MITRE ATT&CK, *MITRE ATT&CK - Active Scanning: Vulnerability Scanning (T1595.002)* (verified on 27 November 2026).
9. `[REF-09]` MITRE ATT&CK, *MITRE ATT&CK - Application Layer Protocol: Web Protocols (T1071.001)* (verified on 27 November 2026).
10. `[REF-10]` NIST, *NIST SP 800-63B Digital Identity Guidelines - Authentication and Lifecycle Management* (verified on 27 November 2026).

BRANDEFENSE CAPABILITIES RELATED TO THIS RESEARCH

Cyber Threat Intelligence

Track the actors, infrastructure and campaigns

Vulnerability Intel

Prioritise the flaws that attackers actually stage.

External Attack Surface

Find exposed middleware before it is targeted.

behind threats like these.

DEFENDER KIT

Indicators of compromise

Verified adversary infrastructure and tool hashes from this study. Every value below is also discussed in the report.

No network or file indicators are published for this study

The hosts in this report are exposed or unattributed systems rather than confirmed adversary infrastructure, so they stay anonymous. Use the detection rules below to find the same exposure in your own estate.

10 records from this study are not published in this table: candidate, suspected and dual-use hosts, victim-related values, and hashes of exposed secrets or files.

DEFENDER KIT

Detection rules

The rule files exactly as printed in the report. Test them in your own engine before deployment.

YARA **odin_jndi_oa_and_harvester_artifacts.yar** 78 lines

```
/*
   Odin by Brandefense - Monograph 70 (Seeyon OA Spraying: JNDI Listeners and SSRF Poll
ing) YARA Suite
   4 filesize-bounded structural rules covering Seeyon OA DES password-spray scripts,
   multi-port JNDI/LDAP callback responders, web-root archive harvesters, and
   HTTP request-smuggling / SSRF polling scripts (zero victim, organization, or raw exp
loit strings).
*/

rule ODIN_R70_Seeyon_OA_DES_Password_Spray_Script
{
    meta:
        author = "Odin by Brandefense"
        monograph = "70"
        description = "Detects Python password-spraying scripts targeting Seeyon OA /se
eyon/main.do with verifyCode checks and DES routines"
        date = "2026-11-26"
    strings:
        $u1 = "/seeyon/main.do" ascii
        $v1 = "verifyCode" ascii
        $m1 = "puredes" ascii nocase
        $m2 = "requests" ascii
        $m3 = ".jsonl" ascii
    condition:
        filesize < 128KB and $u1 and $v1 and 2 of ($m*)
}

rule ODIN_R70_MultiPort_JNDI_LDAP_Callback_Responder
{
    meta:
        author = "Odin by Brandefense"
        monograph = "70"
        description = "Detects Python JNDI/LDAP out-of-band callback listeners and high
-port TCP verification scripts"
        date = "2026-11-26"
    strings:
        $s1 = "socket" ascii
        $p1 = "1389" ascii
        $p2 = "1099" ascii
```

```
        $c1 = "hello-test-13890" ascii
        $c2 = "jndi:ldap://" ascii nocase
        $c3 = "13890" ascii
    condition:
        filesize < 256KB and $s1 and 1 of ($p*) and 1 of ($c*)
}

rule ODIN_R70_WebRoot_Backup_Archive_Harvester
{
    meta:
        author = "Odin by Brandefense"
        monograph = "70"
        description = "Detects automated Python web-root RAR and ZIP backup archive har
vester scripts"
        date = "2026-11-26"
    strings:
        $a1 = ".rar" ascii nocase
        $a2 = ".zip" ascii nocase
        $h1 = "requests" ascii
        $h2 = "urllib" ascii
        $o1 = ".jsonl" ascii
        $o2 = "targets" ascii nocase
    condition:
        filesize < 128KB and $a1 and $a2 and 1 of ($h*) and 1 of ($o*)
}

rule ODIN_R70_HTTP_Request_Smuggling_and_SSRF_Poller
{
    meta:
        author = "Odin by Brandefense"
        monograph = "70"
        description = "Detects raw-socket HTTP CL-TE request-smuggling and SSRF probe s
cripts"
        date = "2026-11-26"
    strings:
        $t1 = "Transfer-Encoding" ascii nocase
        $t2 = "Content-Length" ascii nocase
        $c1 = "chunked" ascii nocase
        $n1 = "socket" ascii
        $n2 = "ssl" ascii
        $n3 = "\\r\\n0\\r\\n\\r\\n" ascii
    condition:
        filesize < 128KB and $t1 and $t2 and $c1 and 1 of ($n*)
}
```

Suricata **odin_seeyon_oa_jndi_backup_and_ssrf_hunt.rules** 11 lines

```
# Odin by Brandefense - Monograph 70 (Seeyon OA Spraying: JNDI Listeners and SSRF Polli
ng) Suricata 7.x Ruleset
# Static syntax checked with Odin Suricata linter (0 problems); test with suricata -T b
efore deployment.

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-R70 Inbound Seeyon OA main.do
Credential Spray POST"; flow:established,to_server; http.method; content:"POST"; bsize:
4; http.uri; content:"/seeyon/main.do"; startswith; fast_pattern; http.request_body; co
ntent:"verifyCode"; nocase; classtype:web-application-attack; sid:9570001; rev:1;)
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-R70 Inbound Portal API AIRepor
t Endpoint Enumeration"; flow:established,to_server; http.method; content:"GET"; bsize:
3; http.uri; content:"/api/v2/AIReport/reports"; startswith; fast_pattern; classtype:at
tempted-recon; sid:9570002; rev:1;)
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-R70 Inbound HTTP Header JNDI L
ookup Prefix"; flow:established,to_server; http.header; content:"|24 7B|jndi:"; nocase;
fast_pattern; classtype:web-application-attack; sid:9570003; rev:1;)
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-R70 Inbound HTTP Body jndi lda
p Lookup Scheme"; flow:established,to_server; http.request_body; content:"jndi:lda
p://"; nocase; fast_pattern; classtype:web-application-attack; sid:9570004; rev:1;)
alert tcp $HOME_NET any -> $EXTERNAL_NET [1099,1389,8888,10990,13890,13891,18888] (ms
g:"ODIN-R70 Outbound TCP Callback Verification Payload hello-test-13890"; flow:establis
hed,to_server; content:"hello-test-13890"; fast_pattern; classtype:trojan-activity; si
d:9570005; rev:1;)
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-R70 Inbound Web-Root RAR Archi
ve Harvester GET"; flow:established,to_server; http.method; content:"GET"; bsize:3; htt
p.uri; content:".rar"; endswith; fast_pattern; classtype:attempted-recon; sid:9570006;
rev:1;)
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-R70 Inbound HTTP Request Smugg
ling CL-TE Header Pair"; flow:established,to_server; http.header; content:"Transfer-Enc
oding:"; nocase; fast_pattern; content:"chunked"; nocase; content:"Content-Length:"; no
case; classtype:web-application-attack; sid:9570007; rev:1;)
```

Show full rule

Sentinel KQL **sentinel_jndi_oa_and_ssrf_egress_hunt.kql** 27 lines

```
// Odin by Brandefense - Monograph 70 (Seeyon OA Spraying: JNDI Listeners and SSRF Poll
ing)
// Hunts JVM/OA worker shell spawns, JNDI/OA/harvester CLI markers, public JNDI egress,
and failed SSRF port sweeps.
let Lookback = 7d;
let ApprovedAdminAndBuildHosts = dynamic(["app-ci-01.corp.example", "sec-bastion-01.cor
```

```
p.example"]);
let JavaOrWebShellAndHarvesterCli =
    DeviceProcessEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedAdminAndBuildHosts))
    | where (
        (InitiatingProcessFileName in~ ("java", "java.exe", "tomcat9.exe", "w3wp.exe",
"nginx", "httpd") and FileName in~ ("sh", "bash", "dash", "cmd.exe", "powershell.exe",
"pwsh.exe", "curl", "curl.exe", "wget"))
        or FileName =~ "linux_x64_admin"
        or ProcessCommandLine has_any ("ldap_responder.py", "spray_oa3.py", "puredes.p
y", "fetch_rar.py", "ssrf_test.sh", "hello-test-13890")
    )
    | project Timestamp, DeviceName, AccountName, SignalType = "HostJvmShellOrWorkbench
Cli", Detail = strcat(InitiatingProcessFileName, " -> ", FileName, ": ", ProcessCommand
Line);
let UnexpectedJndiOrFailedSweepEgress =
    DeviceNetworkEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedAdminAndBuildHosts))
    | where (
        (RemoteIPType == "Public" and InitiatingProcessFileName in~ ("java", "java.ex
e", "tomcat9.exe", "w3wp.exe") and RemotePort in (389, 636, 1099, 1389, 8888, 10990, 13
890, 13891, 18888))
        or (ActionType == "ConnectionFailed" and InitiatingProcessFileName in~ ("java",
"java.exe", "tomcat9.exe", "w3wp.exe", "nginx", "httpd") and RemotePort in (1433, 3306,
4444, 5000))
    )
    | project Timestamp, DeviceName, AccountName = InitiatingProcessAccountName, Signal
Type = "UnexpectedJndiEgressOrFailedSweep", Detail = strcat(InitiatingProcessFileName,
" [", ActionType, "] -> ", RemoteIP, ":", tostring(RemotePort), " (", RemoteUrl, ")");
union JavaOrWebShellAndHarvesterCli, UnexpectedJndiOrFailedSweepEgress
| summarize FirstSeen = min(Timestamp), LastSeen = max(Timestamp), EventCount = count
(), Signals = make_set(SignalType, 6), SampleDetails = make_set(Detail, 5) by DeviceNam
e, AccountName
| order by LastSeen desc
```

Sigma `sigma_jvm_shells_harvesters_and_ssrf_loops.yml` 97 lines

```
title: Linux Java or Web Worker Spawning Shell or Transfer Binary
id: 7a34b8c2-19d4-4e56-8f12-70a10c92e401
status: experimental
description: Detects Linux Java or web server worker processes spawning interactive she
lls or transfer utilities consistent with OA or JNDI post-exploitation.
author: Odin by Brandefense
date: 2026-11-26
```

```
logsource:
  category: process_creation
  product: linux
detection:
  selection_parent:
    ParentImage|endswith:
      - '/java'
      - '/nginx'
      - '/httpd'
  selection_child:
    Image|endswith:
      - '/sh'
      - '/bash'
      - '/dash'
      - '/curl'
      - '/wget'
  filter_oa_maint:
    ComputerName:
      - 'oa-maint-01.corp.example'
  condition: selection_parent and selection_child and not filter_oa_maint
falsepositives:
  - Approved OA maintenance or deployment hosts executing scripted health checks
level: high
tags:
  - attack.initial-access
  - attack.t1190
---
title: Windows Java or Tomcat Service Spawning Command or Recon Utility
id: 7a34b8c2-19d4-4e56-8f12-70a10c92e402
status: experimental
description: Detects Windows Java or Tomcat processes used by enterprise OA portals spa
wning command shells or host reconnaissance binaries outside approved maintenance node
s.
author: Odin by Brandefense
date: 2026-11-26
logsource:
  category: process_creation
  product: windows
detection:
  selection_parent:
    ParentImage|endswith:
      - '\java.exe'
      - '\tomcat9.exe'
  selection_child:
    Image|endswith:
      - '\cmd.exe'
      - '\powershell.exe'
```

```
      - '\pwsh.exe'
      - '\curl.exe'
      - '\whoami.exe'
  filter_oa_win_maint:
    ComputerName:
      - 'oa-win-maint-01.corp.example'
  condition: selection_parent and selection_child and not filter_oa_win_maint
falsepositives:
  - Self-hosted OA diagnostic scripts on explicitly allowlisted administrative nodes
level: high
tags:
  - attack.initial-access
  - attack.t1190
---
title: JNDI Callback Responder, OA Spray, or SSRF Poller Script Execution
id: 7a34b8c2-19d4-4e56-8f12-70a10c92e403
status: experimental
description: Detects execution of JNDI LDAP callback responders, Seeyon OA password-spr
aying helpers, RAR backup harvesters, or SSRF polling scripts observed on Workbench A.
author: Odin by Brandefense
date: 2026-11-26
logsource:
  category: process_creation
  product: linux
detection:
  selection_bin:
    Image|endswith:
      - '/linux_x64_admin'
  selection_cli:
    CommandLine|contains:
      - 'ldap_responder.py'
      - 'spray_oa3.py'
      - 'puredes.py'
      - 'fetch_rar.py'
      - 'ssrf_test.sh'
      - 'hello-test-13890'
  filter_sec_lab:
    ComputerName:
      - 'sec-lab-01.corp.example'
  condition: (selection_bin or selection_cli) and not filter_sec_lab
falsepositives:
  - Authorized security assessment hosts explicitly listed in sec-lab-01.corp.example
level: high
tags:
  - attack.reconnaissance
  - attack.t1595.002
```

