ODIN

TLP:CLEAR

ODIN RESEARCH · MONOGRAPH 47 / 30 · RECON WORKBENCHES

Mobile APK Unpacking and SSRF Canaries

A CDN Origin Hunt

Static Analysis of Two Multi-Port Reconnaissance and Out-of-Band Callback Workspaces, 3,292 Callback Log Lines, Including 1,877 HTTP Requests, and 600 Interactsh Endpoints

Two-week observation window ending 21 November 2026 · Prepared November 2026
Full Report · Public edition · Version 1.1

57 + 114
57 scheduled CDN origin-discovery logs and 114 staged PHP and gateway YAML templates on the origin-hunt listener

194 / 120
Feed-labelled Interactsh cloud ports (186 on SMTP ports 465 and 587) across 120 withheld cloud IPv4s

0
Published indicators of compromise

4
Detection rule files

What Is in This Report. 11 chapters and two appendices.

Static Analysis of Two Multi-Port Reconnaissance and Out-of-Band Callback Workspaces, 3,292 Callback Log Lines, Including 1,877 HTTP Requests, and 600 Interactsh Endpoints

01	Executive Summary	04
02	Multi-Port Recon, SSRF Canary, and Origin-Hunt Analytical Model	07
03	US Four-Port Workspace: Mobile APK Unpacking, SSRF Canaries, and Callback Logs	12
04	Hong Kong Workspace: Scheduled CDN Origin Hunting and PHP Templates	15
05	Cloud Interactsh OAST Cohort: 120 Feed-Labelled Cloud Addresses vs Dual-Use Suites	19
06	Why Most Feed Records and Callback Log Entries Stay Off Blocklists	22
07	What Defenders Should Do	24
08	Detection Rules	26
09	Indicators	29
10	Scope and Limits	32
11	Sources	34
A	Indicators of compromise (0)	36
B	Detection rules (4 files)	37

IN SHORT

During a two-week observation window ending 21 November 2026, Odin by Brandefense analyzed 1,084 sampled entries across five open HTTP ports on two servers. We also examined a 373,784-byte callback log (3,292 lines across 271 peers) alongside 600 Interactsh endpoints from 31,117 sightings. Hunt outbound OAST and SMTP callbacks, enforce mutual TLS on CDN origins, and alert on backend image canary requests.

01

CHAPTER 01

Executive Summary

IN SHORT

During a two-week observation window ending 21 November 2026, Odin by Brandefense analyzed 1,084 sampled entries across five open HTTP ports on two servers. We also examined a 373,784-byte callback log (3,292 lines across 271 peers) alongside 600 Interactsh endpoints from 31,117 sightings. Hunt outbound OAST and SMTP callbacks, enforce mutual TLS on CDN origins, and alert on backend image canary requests.

INSIDE THIS CHAPTER

Three Decisions for Leaders 04

The Study in Numbers 05

01 Executive Summary

Perimeter defenses often assume external reconnaissance starts at a content delivery network (`CDN`) edge. The files suggest three reconnaissance paths that could work around web application firewalls (`WAFs`): unpacked Android packages, one-byte server-side request forgery (`SSRF`) canaries, and CDN origin mapping.

We reviewed static file metadata and callback logs across five open HTTP ports on two servers observed from 13 to 20 November 2026. We also examined 600 recent `Interactsh` endpoints from 31,117 sightings. No captured binary was run and no external target was contacted. Because independent per-address confirmation is absent for the 600 `Interactsh` endpoints, all 407 OAST host addresses, both open directories, 271 callback peers, and all 929 file hashes stay withheld.

1. **A four-port US server pairs unpacked Android packages with one-byte SSRF canaries.**
   Observed from 13 to 20 November 2026 across four withheld HTTP listener ports, a US workspace exposes unpacked `.apk` archives, ARM64 libraries, JavaScript bundles, and GlobalProtect login pages. Its canary listener serves a one-byte image canary (filename withheld), while its callback listener logs 1,877 HTTP requests, including 166 requests targeting the image canary and 356 automated bot hits.

2. **A Hong Kong server stages CDN origin hunting beside 114 PHP templates.**
   Observed from 13 to 20 November 2026 on a withheld HTTP listener port, a second directory reports 2,132 files centered on a 128.88-megabyte SQLite origin database and 57 scheduled logs. Beside cloud ASN files and FOFA tables sit 114 PHP and gateway YAML templates, a `CVE-2019-11043` `PHP-FPM` exploit binary, and captured appliance pages.

3. **Upstream feed labels mark 194 cloud Interactsh ports across 120 unconfirmed IPv4s.**
   Out of 31,117 sightings spanning `ARL` (19,828), `Interactsh` (10,757), and `ScopeSentry` (532), we reviewed 600 `Interactsh` endpoints across 407 hosts. The upstream feed labels 194 cloud ports on 120 IPv4s as confirmed, including 186 on SMTP ports 465 and 587 across 115 hosts. All 600 endpoints lack independent per-address confirmation and stay withheld.

Three Decisions for Leaders

1. **Lock down outbound URL fetchers and enforce session-based cloud metadata.** Restrict avatar, webhook, and preview workers to approved external hosts, block private and link-local IPs, and require AWS `IMDSv2` across all workloads.
2. **Close direct-to-origin HTTP and HTTPS paths behind CDN perimeters.** Accept origin traffic solely from published CDN IP ranges and require mutual TLS (`Authenticated Origin Pulls`) to prevent edge WAF bypasses.
3. **Hunt outbound OAST callbacks and block unauthorized application SMTP egress.** Hunt outbound TCP 26, 80, 443, 465, and 587 traffic for `Interactsh` domains before blocking any feed-listed cloud host, and block direct outbound SMTP from non-mail application subnets.

The Study in Numbers

Number	What it is
2 Hosts / 5 Ports	Open HTTP workspaces in the US (4 ports) and Hong Kong (1 port), addresses and ports withheld (0 shared hosts)
11,947 / 1,084	Reported directory files across the five listeners and 1,084 sampled entries across six artifact groups
3,292 / 1,877	Lines inside the 373,784-byte callback log and 1,877 HTTP requests across 271 peers
166 vs 356	166 HTTP requests targeting the image canary vs 356 opportunistic `/.env`, `/.git`, and config bot hits on the callback listener
57 + 114	57 scheduled CDN origin-discovery logs and 114 staged PHP and gateway YAML templates on the origin-hunt listener
31,117 / 600	Sightings across ARL, Interactsh, and ScopeSentry, with 600 Interactsh endpoints reviewed on 407 hosts
194 / 120	Feed-labelled Interactsh cloud ports (186 on SMTP ports 465 and 587) across 120 withheld cloud IPv4s

How to use this report.

Security leaders should read Chapters 1, 6, and 7. Mobile, API, and cloud architects should review Chapters 3, 4, and 7. SOC analysts and detection engineers should use Chapters 5, 8, and 9 with the Detection rules and Appendix As.

02

CHAPTER 02

Multi-Port Recon, SSRF Canary, and Origin-Hunt Analytical Model

IN SHORT

Odin by Brandefense reviewed 1,084 sampled entries (11,947 reported files) across five open HTTP ports alongside 600 Interactsh endpoints across 407 hosts. Zero shared IPv4 addresses connect the two open directories or the Interactsh hosts. Treat these findings as an analytical model and hunt outbound OAST, SSRF canary, and origin-bypass traffic.

INSIDE THIS CHAPTER

Five Open HTTP Directory Listeners Across Two Hosts (1,084 Sampled Entries) 08

Six Artifact Groups Across the 1,084 Sampled Entries 09

02 Multi-Port Recon, SSRF Canary, and Origin-Hunt Analytical Model

Comparing the US four-port workspace, the Hong Kong origin-hunt workspace, and all 407 `Interactsh` hosts shows **zero shared IPv4 addresses** and **zero shared `/24` subnets**. We therefore present them explicitly as an **analytical model** of application reconnaissance for cyber threat intelligence teams rather than a single actor. Figure 1 maps the four functional groups to their defensive actions.



Figure 1: APK unpacking, SSRF canaries, and origin hunting split recon roles

Five Open HTTP Directory Listeners Across Two Hosts (1,084 Sampled Entries)

Operators on rented virtual private servers often start unauthenticated `Python` HTTP servers across multiple high ports to move scripts, inspect logs, or serve `SSRF` callback files. Binding those listeners to `0.0.0.0` exposes the underlying folders that external attack surface management can help defenders find. Table 2.1 summarizes all five listeners across both withheld hosts.

Workspace & listener	Geo	Engine	Reported	Sampled	Hash rec.	Unhashed	Observed dates	Primary staged contents
Workspace 1, shared-directory listener A	US	`python`	4,897	360	336	24	13 to 20 Nov 2026	80 `.py` & 22 `.sh` scripts, VPN login template, fuzzing outputs & `.apk`
Workspace 1, shared-directory listener B	US	`python`	4,897	359	236	123	13 to 20 Nov 2026	Shared 4,897-file root (168 ARM64 `.so`, 21 DEX & 49 JS)
Workspace 1, callback listener	US	`python`	20	20	19	1	13 to 20 Nov 2026	UID sweep scripts, 28.08 MB seed CSV, 15.77 MB SQLite DB & callback log
Workspace 1, canary listener	US	`python`	1	1	1	0	13 to 20 Nov 2026	Standalone HTTP listener serving `1-byte` image canary (filename withheld)
Workspace 2, origin-hunt listener	HK	`python`	2,132	344	337	7	13 to 20 Nov 2026	Origin-discovery script & DB, 57 logs, 114 PHP/gateway YAMLs & captures
Total	**US/HK**	`python`	**11,947**	**1,084**	**929**	**155**	**13 to 20 Nov 2026**	**0 shared hosts; 0 ports or file hashes published**

On Workspace 1, shared-directory listeners A and B expose the same 4,897-file root and share 261 sampled paths. The callback listener isolates 20 UID-sweep and callback files (44,497,959 B combined), while the canary listener serves solely the `1-byte` image canary.

Six Artifact Groups Across the 1,084 Sampled Entries

Publishing file digests from open reconnaissance workspaces would sweep legitimate Android SDK libraries, GeoIP country databases, and scraped tables into endpoint blocklists. Because owner authorization is also unestablished on both servers, **zero file SHA-256 digests are published**. Static review partitions all 1,084 sampled entries into six mutually exclusive groups (`460 + 237 + 163 + 107 + 92 + 25 = 1,084`):

Artifact group	Entries	Share	Hash rec.	Unhashed	Workspace	Size range (`B`)	Defensive handling
Mobile APK, DEX, ARM64 `.so` & JS unpacking	460	42.4%	353	107	US (shared listeners A/B)	235 to 130,575,320	Hold SDK/APK digests; harden API signing
CDN origin hunt & PHP/ gateway YAML templates	237	21.9%	230	7	HK (origin-hunt listener)	286 to 128,880,640	Enforce origin mTLS; patch `PHP-FPM`
API signing, VPN & subdomain recon scripts	163	15.0%	159	4	US (shared listeners A/B)	13 to 2,135,517	Enforce API auth & VPN phishing-resistant MFA
Appliance config captures & build cache	107	9.9%	107	0	HK (origin-hunt listener)	221 to 11,995,616	Hold captured configs & Go cache files
Harvested portal datasets & table exports	92	8.5%	56	36	US (shared listeners A/B)	108 to 875,148,439	Hold exported tables; UID rate limits
SSRF image canary & UID sweep pipeline	25	2.3%	24	1	US (canary, callback & listener A)	1 to 28,080,948	Alert on `1-byte` JPEG responses (`SID 9547002`)

Figure 2 connects these slices and the 194 feed-listed cloud `Interactsh` ports to target surfaces and published rules.

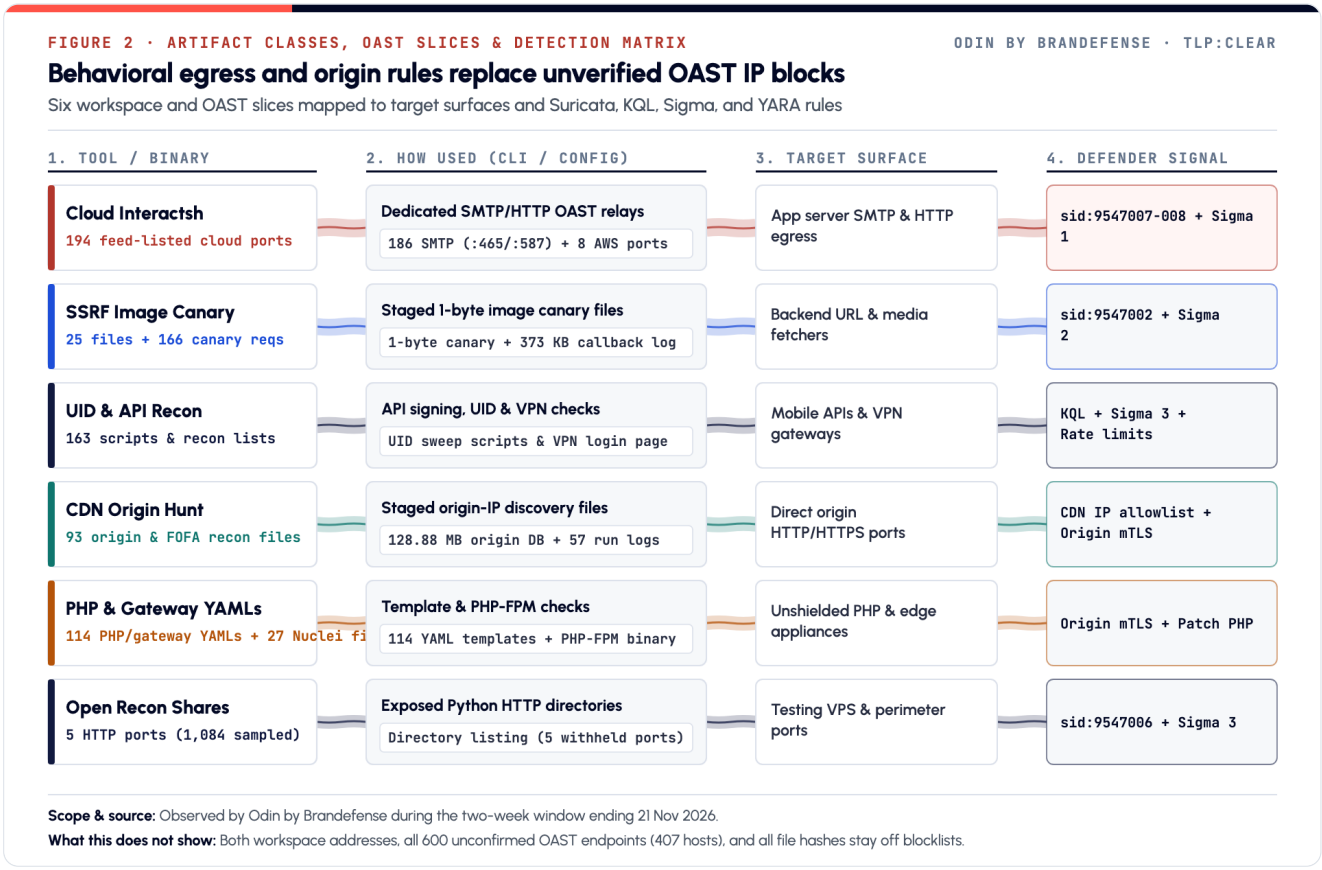


Figure 2: Behavioral egress and origin rules replace unverified OAST IP blocks

CHAPTER 03

US Four-Port Workspace: Mobile APK Unpacking, SSRF Canaries, and Callback Logs

IN SHORT

Observed in the United States from 13 to 20 November 2026, Workspace 1 exposes 740 sampled entries across four withheld HTTP listener ports. Its 373,784-byte callback log records 3,292 lines (1,877 HTTP requests across 271 peers), including 166 requests targeting the one-byte image canary and 356 automated bot requests. Restrict backend URL fetchers and enforce per-account API rate limits.

INSIDE THIS CHAPTER

Shared-Directory Listeners A and B: Mobile APK Unpacking, API Signing, and VPN Recon 12

Callback and Canary Listeners: One-Byte Image Canary, UID Sweeps, and Callback Log Forensics 12

03 US Four-Port Workspace: Mobile APK Unpacking, SSRF Canaries, and Callback Logs

Workspace 1 (United States, address withheld) spans 238 ARM64 `.so` libraries, 102 `.js` bundles, 92 `.py` scripts, 76 `.txt` lists, 62 `.jsonl` files, 43 `.dex` files, and 23 `.sh` scripts. Smaller groups cover 14 `.log` files, 12 `.html` pages, 12 `.json` files, 9 `.csv` files, 4 `.apk` packages, 3 SQLite `.db` files, and 2 `1-byte` image canaries.

Shared-Directory Listeners A and B: Mobile APK Unpacking, API Signing, and VPN Recon

Mobile binaries often embed staging subdomains, storage buckets, local SQLite schemas, and request-signing keys omitted from browser apps:

- **Unpacked Android `.apk`, `.dex`, ARM64 `.so`, and SQLite assets (460 entries).** The directory holds two Android packages (130,575,320 B and 86,224,736 B) and Dalvik bytecode. Unpacked ARM64 native libraries include application (18,154,416 B), mapping-SDK (13,323,992 B), Flutter (11,037,032 B), Hermes (2,338,376 B and 1,978,248 B), and HTTP-DNS (255,328 B) binaries. Extracted assets include a SQLite database (245,760 B), a decompiled `Hermes` JavaScript bundle (57,802,087 B), and three application JavaScript bundles (770,989 B, 751,798 B, and 644,198 B).
- **API signature testing and subdomain mapping (163 entries).** Asset-extraction scripts generate extracted URL and host lists (50,251 B, 12,672 B, and 645 B). Root scripts test signatures, JWTs, IDOR, SQL injection, storage buckets, and virtual hosts (558 B to 1,686 B). Beside them sit two fuzzing JSON files (2,295 B and 1,693 B), two subdomain enumeration files (1,615 B and 874 B), and two port-scan logs (2,902 B and 654 B).
- **GlobalProtect VPN template and timing scripts.** Shared-directory listener A stages a Palo Alto GlobalProtect login page (11,705 B), a generic login page (3,371 B), password lists and a proxy list (10,373 B). It also holds eight GlobalProtect authentication and timing scripts, while 92 `.jsonl` and table exports stay withheld.

Callback and Canary Listeners: One-Byte Image Canary, UID Sweeps, and Callback Log Forensics

The callback listener (20 files) and canary listener (1 file) form a dedicated `SSRF` canary and UID-sweep pair, joined on shared-directory listener A by companion SSRF, LDAP-listener, and header-testing scripts:

- **One-byte image canary and UID sweep files.** A one-byte image canary was mirrored across two listeners to test filename suffix checks on avatar and media fetchers; its filename and listener ports are withheld. The callback listener also stages five Python UID-sweep scripts (2,340 B, 2,294 B, 1,446 B, 800 B, and 658 B). Beside them sit a CSV seed table (28,080,948 B), a SQLite database (15,769,600 B), five worker logs (29,546 B, 22,033 B, plus three shard logs), and six shard text files (310 B to 122,863 B).
- **Inside the 3,292 lines of the callback log (373,784 B).** Carrying log dates from 11 to 18 November 2026, the callback listener log holds 1,877 HTTP requests from 271 external peers, 91 TLS handshakes on the HTTP port, and 1,324 `Python` 400/404 status lines. Table 3.1 breaks down all 1,877 HTTP requests.

Callback log dimension	Category	Count	Share	Plain meaning
Request path	Other HTTP paths	666	35.5%	Non-canary URI checks and unattributed path requests
Request path	Root path (`/`)	632	33.7%	Root reachability checks and internet port sweeps
Request path	Automated bot cross-traffic	356	19.0%	Opportunistic `/.env`, `/.git/config` & config bots hitting the callback listener
Request path	**SSRF image canary (filename withheld)**	**166**	**8.8%**	**Requests targeting the `1-byte` image canary logged on the listener**
Request path	Favicon (`/favicon.ico`)	57	3.0%	Browser or preview-renderer `/favicon.ico` requests
HTTP verb	`GET` and `HEAD`	1,662 / 167	88.5% / 8.9%	Standard requests (`GET`) and header checks (`HEAD`)
HTTP verb	`OPTIONS`, `POST`, `PRI`, `CONNECT`	13 / 12 / 8 / 8	2.2% combined	CORS preflights, `POST` tests, HTTP/2 `PRI` & proxy checks
HTTP verb	Seven 4-letter random verbs	7	0.4%	`YTBO`, `ONWO`, `RTXJ`, `USDB`, `AGNL`, `SWVZ`, `QFUL` (1 each)
Non-HTTP lines	TLS (91) + HTTP errors (1,324)	1,415	(of 3,292)	TLS handshakes sent to HTTP port + `Python` 400/404 lines

Daily HTTP requests rose from 27 on 11 November to 608 on 17 November. They fell to 54 on 18 November.

The top 15 peers sent 1,367 requests (72.8%); the other 256 sent 510 (27.2%). The log also includes 356 configuration-path requests and 91 TLS handshakes from internet scanners. All 271 peer addresses remain withheld.

CHAPTER 04

Hong Kong Workspace: Scheduled CDN Origin Hunting and PHP Templates

IN SHORT

Observed in Hong Kong on a withheld HTTP listener port from 13 to 20 November 2026, Workspace 2 reports 2,132 files (344 sampled) for scheduled CDN origin discovery. Beside a 128.88 MB origin-discovery SQLite database and 57 scheduled logs sit 114 PHP and gateway YAML templates, a `CVE-2019-11043` exploit binary, and captured appliance pages. Restrict origin ingress to CDN IP ranges and require mutual TLS origin pulls.

INSIDE THIS CHAPTER

Origin-Discovery Suite, 57 Scheduled Logs, Cloud ASN Tables, and FOFA Exports (93 Entries) 15

Custom PHP and Gateway Templates (114 YAML Files), `CVE-2019-11043` Exploit Binary, and Appliance Captures 16

04 Hong Kong Workspace: Scheduled CDN Origin Hunting and PHP Templates

Putting a cloud `CDN` in front of an application protects nothing if the origin server still answers direct HTTP or HTTPS requests from the internet. Workspace 2 (Hong Kong, address and listener port withheld) exposes 2,132 reported files (344 sampled) built for origin-IP discovery and direct template scanning. Figures 3 and 4 map the modeled sequence and five-port workspace layout.



Figure 3: Unpacked mobile endpoints feed SSRF image canaries and origin sweeps

Origin-Discovery Suite, 57 Scheduled Logs, Cloud ASN Tables, and FOFA Exports (93 Entries)

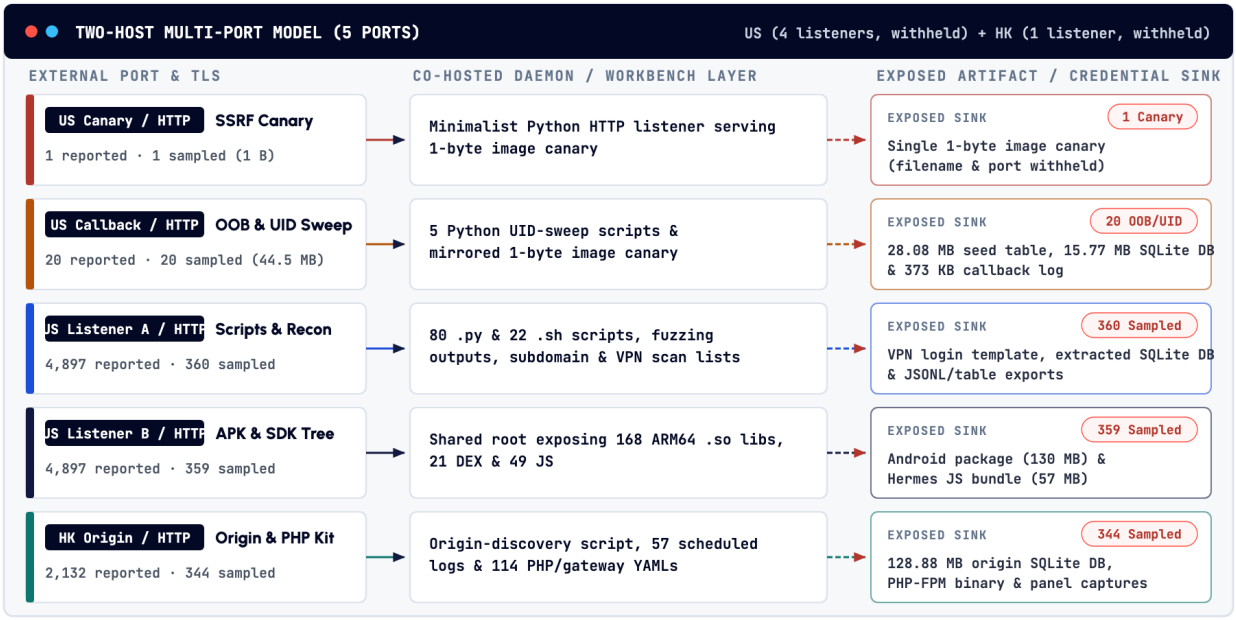
- **Active 128.88 MB SQLite database vs 65.5 KB clean baseline.** A clean baseline directory (5 entries) holds a template Python origin-discovery script (18,807 B), an empty SQLite database (65,536 B), a GeoIP country database (3,389,216 B), and two Alibaba Cloud prefix tables (156,140 B and 33,581 B). The active origin-discovery directory (66 entries) expands the Python script to 24,112 B (plus a 9 November 2026 backup at 21,899 B), adds a temporary port-scan file (216,984 B), and populates a **128,880,640 B (`122.91 MiB`) SQLite database**.
- **Fifty-seven scheduled logs and certificate/FOFA inputs.** Inside the log subfolder, 57 scheduled log files carry filename dates from 6 to 20 November 2026 (up to 5,889 B). Companion FOFA files (4 entries, including a 14,882 B origin-IP CSV and a 15,443 B host-mapping JSON) supply candidate subdomains. Reconnaissance folders (18 entries) add certificate subjects: archived subdomain and DNS scanners at 10.31 MB and 9.83 MB, subdomain and scan lists at 1.31 MB and 2.57 MB, and certificate CSVs at 254,538 B and 254,227 B.

FIGURE 4 · MULTI-PORT RECON & ORIGIN-HUNT DIRECTORY BLUEPRINT

ODIN BY BRANDEFENSE · TLP:CLEAR

Five HTTP ports across US and HK expose 1,084 sampled recon artifacts

Listener-level directory layout across US (4 listeners, ports withheld) and HK (1 listener, port withheld)



Scope & source: Observed on two withheld HTTP workspaces (US and HK) during the window ending 21 Nov 2026.

What this does not show: Both host addresses, their five listener ports, and all 929 recorded file hashes remain withheld from public blocklists.

Figure 4: Five HTTP ports across US and HK expose 1,084 sampled recon artifacts

Custom PHP and Gateway Templates (114 YAML Files), `CVE-2019-11043` Exploit Binary, and Appliance Captures

- **Curated PHP and gateway template suite (114 YAML files) and stock Nuclei templates (27 files).** Alongside 27 stock `Nuclei` files and a `Nuclei` configuration file (15,402 B), a custom template directory stages 114 YAML templates (51 miscellaneous, 40 PHP, 12 backup, and 11 across seven smaller category folders).
- **Compiled exploit binary for `CVE-2019-11043` (9,904,337 B, filename withheld).** Staged alongside 23 Go cache files, a compiled Go exploit binary targets `CVE-2019-11043`. Per NIST NVD, `CVE-2019-11043` is a `PHP-FPM` buffer underflow in **PHP 7.1.x below `7.1.33`, 7.2.x below `7.2.24`, and 7.3.x below `7.3.11`** under vulnerable Nginx `fastcgi_split_path_info` rules (fixed in `7.1.33`, `7.2.24`, and `7.3.11`).
- **Network-appliance management captures (80 entries).** Three configuration folders (29, 28, and 7 entries) plus 16 archived panel pages store captured management outputs (10,012 B to 42,725 B), including password, backup, rate-limit, menu, and system-configuration pages. All captures stay withheld.

Workspace & listener	Staged artifact or group	Byte size (B)	Role & indicator handling
Workspace 1 (US , canary listener)	Standalone 1-byte image canary	1	Dedicated SSRF canary (filename withheld) · **Alert on 1-byte JPEG responses (SID 9547002)**
Workspace 1 (US , callback listener)	Callback log & mirrored 1-byte image canary	373,784 / 1	3,292 lines (166 canary requests) · **Filename, peers & hash withheld**
Workspace 1 (US , callback listener)	Five Python UID-sweep scripts & seed datasets	658 to 28,080,948	UID enumeration scripts & tables · **Paths & hashes withheld**
Workspace 2 (HK , origin-hunt listener)	Origin-discovery Python script & SQLite database	24,112 / 128,880,640	CDN origin matcher & populated DB · **Paths & hashes withheld**
Workspace 2 (HK , origin-hunt listener)	Scheduled origin-discovery logs (57 files)	up to 5,889	Scheduled run logs (file dates 6 to 20 Nov 2026) · **Withheld**
Workspace 2 (HK , origin-hunt listener)	Custom PHP/gateway YAML templates (114) & CVE-2019-11043 binary	up to 4,004 / 9,904,337	PHP YAML suite & PHP-FPM exploit binary · **Filename & hashes withheld**

CHAPTER 05

Cloud Interactsh OAST Cohort: 120 Feed-Labelled Cloud Addresses vs Dual-Use Suites

IN SHORT

Drawn from 31,117 sightings across ARL, Interactsh, and ScopeSentry, our 600-endpoint Interactsh review across 407 hosts identifies 194 feed-labelled cloud listener ports on 120 IPv4 addresses. Dedicated SMTP and SMTPS callback ports 465 and 587 account for 186 of those 194 ports (95.9%). Because independent per-address confirmation is absent, withhold all 407 hosts and hunt outbound OAST and SMTP egress.

INSIDE THIS CHAPTER

194 Feed-Labelled `Interactsh` Ports Across 120 Commercial Cloud IPv4s 19

Three Patterns Behind the Remaining 406 Withheld `Interactsh` Endpoints 20

05 Cloud Interactsh OAST Cohort: 120 Feed-Labelled Cloud Addresses vs Dual-Use Suites

We reviewed 31,117 sightings across `ARL`, `Interactsh`, and `ScopeSentry` and examined 600 recent `Interactsh` endpoints (observed 13 to 18 November 2026) across 407 distinct hosts and 398 `/24` subnets. Table 5.1 summarizes all three cohorts.

Tool	Category	Sightings	Feed-verified	Countries	Reviewed	Hosts	Feed-confirmed cloud (`Hunt`)	Other rows (`Withheld`)
`ARL`	Asset recon	19,828	4	53	(baseline)	-	**0**	Dual-use recon suite (hunt only)
`Interactsh`	OAST callback	10,757	530	54	600	407	**194 (120 IPs withheld)**	**406 (287 hosts withheld)**
`ScopeSentry`	Recon suite	532	0	32	(baseline)	-	**0**	Dual-use recon platform (hunt only)
Total	**3 Tools**	**31,117**	**534**	**-**	**600**	**407**	**194 (120 IPs withheld)**	**406 endpoints (287 hosts)**

194 Feed-Labelled `Interactsh` Ports Across 120 Commercial Cloud IPv4s

We reviewed 600 `Interactsh` endpoints (300 feed-labelled `confirmed` and 300 feed-labelled `suspected`). The upstream feed labels 194 endpoints on 120 cloud IPv4 addresses as confirmed; independent per-address confirmation is absent, so these addresses remain unconfirmed.

- **SMTP submission (:587) and SMTPS (:465) dominance (186 of 194 ports = 95.9%).** Self-hosted `Interactsh` servers bind SMTP/SMTPS alongside DNS and HTTP/HTTPS to catch mail-header and `JavaMail` SSRF callbacks. Among the 120 feed-labelled cloud IPv4s, 71 hosts expose paired 465 + 587 listeners (142 ports), 37 expose 587, 7 expose 465, and one AWS host in France exposes port 26.
- **Four feed-labelled AWS US HTTP/HTTPS hosts (7 ports).** Three US `Amazon.com, Inc.` hosts (addresses withheld) expose paired :80 and :443 listeners sharing one custom certificate domain (withheld) and Go TLS JARM `29d29d00029d29d00041d41d00041dcb3f8752a2d70d1dbf446fc46ab5df96`, while a fourth US AWS host exposes HTTP :80.
- **Eight cloud providers across 18 countries.** The 120 feed-labelled cloud hosts span `Amazon.com, Inc.` (44 hosts / 70 ports), `DigitalOcean, LLC` (34 / 55), `Hetzner Online GmbH` (15 / 25), and `Contabo GmbH` (11 / 18). Remaining hosts sit on `OVH SAS` (6 / 10), `Microsoft Corporation` (5 / 8), `Contabo Inc.` (4 / 6), and `LEASEWEB SINGAPORE PTE. LTD.` (1 / 2). Top countries are the US (49), Germany (26), Singapore (9), the Netherlands (7), France (6), and India (5). Withhold all 120 addresses from blocklists and hunt egress until each address is validated.

Cloud slice (addresses withheld)	Port(s)	Geo & cloud provider	Protocol / TLS profile	Action
3 Dual-port AWS HTTP/HTTPS hosts	80, 443	US · Amazon.com, Inc.	HTTP/HTTPS `Interactsh`; shared cert & Go TLS JARM	Withheld (hunt egress; validate first)
1 Plaintext AWS HTTP host	80	US · Amazon.com, Inc.	Plaintext HTTP `Interactsh` listener	Withheld (hunt egress; validate first)
1 Alternate-port AWS SMTP host	26	FR · Amazon.com, Inc.	Alternate SMTP `Interactsh` listener	Withheld (hunt egress; validate first)
39 Additional AWS SMTP/SMTPS hosts	465, 587	9 countries · Amazon.com, Inc.	62 SMTP/SMTPS ports (23 dual, 14 :587, 2 :465)	Withheld (hunt egress; validate first)
34 DigitalOcean SMTP/SMTPS hosts	465, 587	6 countries · DigitalOcean, LLC	55 SMTP/SMTPS ports (21 dual, 10 : 587, 3 :465)	Withheld (hunt egress; validate first)
42 Hetzner/Contabo/OVH/ Azure/Leaseweb hosts	465, 587	10 countries · 6 cloud providers	69 SMTP/SMTPS ports (27 dual, 13 :587, 2 :465)	Withheld (hunt egress; validate first)

Three Patterns Behind the Remaining 406 Withheld `Interactsh` Endpoints

1. **Shared edge and cloud space on `Akamai` (9 endpoints on 6 hosts).** Nine feed-confirmed :465 and :587 rows in `NL`, `DE`, `GB`, and `US` sit on `Akamai Technologies, Inc.`, where shared edge or reassigned cloud addresses risk collateral disruption.
2. **Unverified secondary-provider SMTP listeners (97 endpoints on 63 hosts).** Ninety-seven :587 (61), :465 (35), and :2525 (1) rows across `Google LLC` (18), `Oracle Corporation` (11), `Scaleway SAS` (6), `The Constant Company, LLC` (6), `Alibaba` (6), and regional hosts lack secondary domain or HTTP confirmation.
3. **Suspected AWS custom-domain TLS candidates and JARM collisions (300 endpoints on 218 hosts).** All 300 feed-suspected rows sit on `Amazon.com, Inc.` (296 US, 3 SG, 1 JP) across ports 443 (211), 80 (87), and 5000 (2), with 297 presenting custom-domain TLS certificates. JARM `29d29d00029d29d00041d41d00041dcb3f8752a2d70d1dbf446fc46ab5df96` sits on 3 feed-confirmed AWS `Interactsh` hosts and 141 feed-suspected endpoints (144 total), confirming why defenders must never block on JARM alone.

06

CHAPTER 06

Why Most Feed Records and Callback Log Entries Stay Off Blocklists

IN SHORT

Review across 31,117 sightings, 1,084 sampled directory files, and 3,292 callback log lines places zero IPv4 addresses and zero file hashes on public blocklists. All 600 Interactsh endpoints (including 194 feed-confirmed cloud ports on 120 IPv4s) lack independent per-address confirmation. Hunt outbound OAST and canary requests instead of blocking unverified feed rows.

06 Why Most Feed Records and Callback Log Entries Stay Off Blocklists

Figure 5 compares `log10`-scaled sightings and callback log line counts against the 120 feed-listed cloud `Interactsh` IPv4s and 166 logged requests targeting the one-byte image canary.

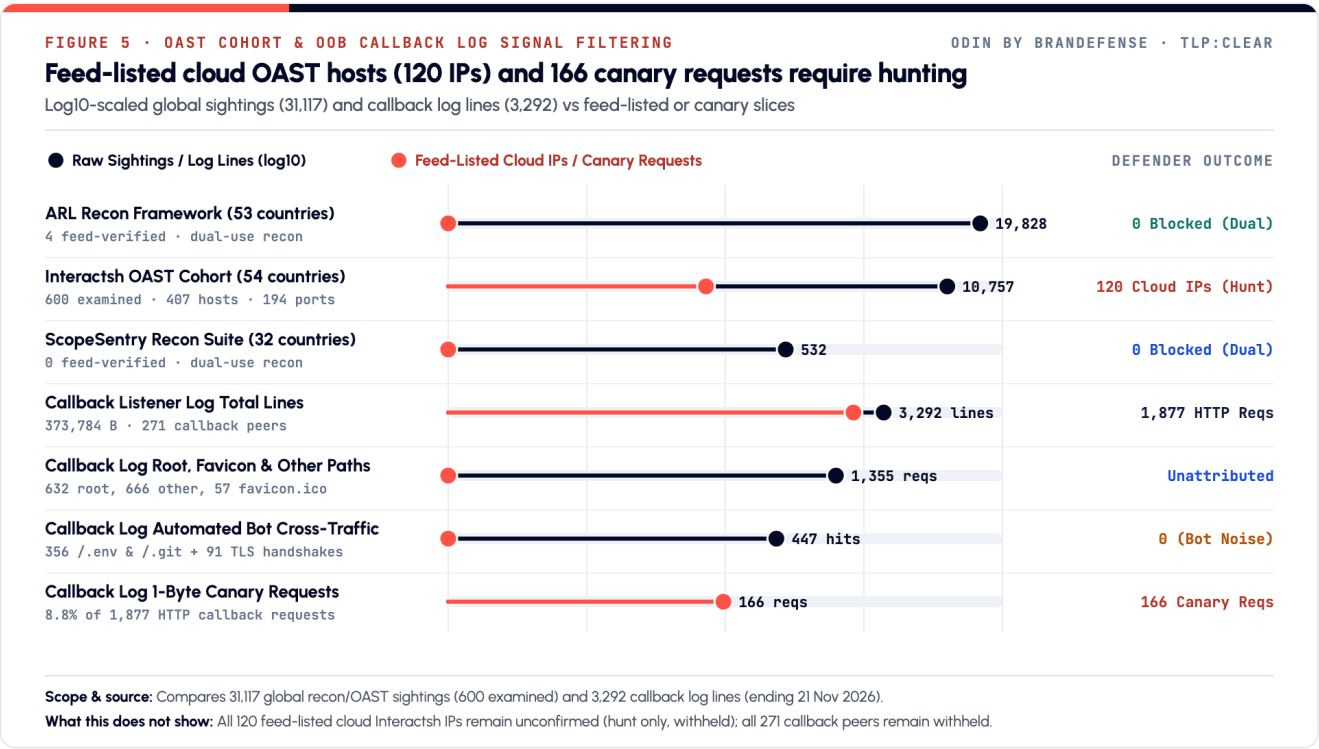


Figure 5: Feed-listed cloud OAST hosts (120 IPs) and 166 canary requests require hunting

1. **Analytical model across zero shared hosts.** Zero IPv4 addresses, `/24` subnets, or custom TLS certificates link Workspace 1, Workspace 2, and the 407 `Interactsh` hosts. They represent complementary reconnaissance workflows, not one threat group.
2. **Callback logs mix test requests, third-party servers, and bot noise.** The log records 166 requests targeting the one-byte image canary between 11 and 18 November 2026; it does not establish successful image fetches. Moreover, an HTTP log cannot separate operator self-tests, authorized checks, third-party fetchers, and internet noise (356 `/.env` and `/.git` hits plus 91 TLS handshakes). All 271 peer addresses stay withheld.
3. **Staged files and templates do not establish downstream breaches.** The servers held unpacked Android packages, a GlobalProtect login template, UID-sweep scripts, an origin-discovery database, 114 YAML files, and a `CVE-2019-11043` exploit binary. These files show staging between 13 and 20 November 2026. They do not establish a breach of an external target. Either server could belong to an unauthorized operator or to a practitioner who exposed `python -m http.server` on a testing VPS.
4. **Dual-use suites require egress and origin controls.** Security teams use `ARL`, `ScopeSentry`, `Nuclei`, `Subfinder`, and `Interactsh` daily; restricting backend egress and locking down CDN origins stops unauthorized callbacks without breaking legitimate testing.

07

CHAPTER 07

What Defenders Should Do

IN SHORT

This chapter lists the actions defenders should take, in priority order.

07 What Defenders Should Do

Cloud, network, and SMTP egress security

- [ ] Hunt outbound TCP 26, 80, 443, 465, and 587 connections for `Interactsh` domains and TLS certificates, and validate any feed-listed cloud OAST address with an independent second signal before blocking.
- [ ] Block direct outbound SMTP and SMTPS (25, 26, 465, 587) from application and container subnets outside designated corporate mail relays.

Application SSRF and cloud metadata hardening

- [ ] Enforce strict URL egress allowlists and private/link-local IP blocks (`RFC 1918`, `169.254.169.254`) on avatar, webhook, PDF, and media-preview fetchers regardless of image filename suffixes.
- [ ] Require session-oriented cloud instance metadata (`AWS IMDSv2` with `HttpTokens=required` and hop limit 1) across every cloud workload.

CDN origin and mobile API protection

- [ ] Lock origin firewalls exclusively to published CDN IP ranges, enable mutual TLS (`Authenticated Origin Pulls`), and patch legacy `PHP-FPM` servers past `CVE-2019-11043` (`PHP 7.1.33`, `7.2.24`, `7.3.11`).
- [ ] Strip staging URLs, SQLite seed secrets, and static signing keys from mobile `.apk` builds and `Hermes` bundles, and enforce per-account UID rate limits.
- [ ] Require phishing-resistant MFA on `GlobalProtect` VPN portals, and ban unauthenticated `python3 -m http.server` shares on testing VPS hosts.

CHAPTER 08

Detection Rules

IN SHORT

This chapter describes each published rule and where to deploy it.

INSIDE THIS CHAPTER

How the Suricata Signatures Work 26

How the KQL, Sigma, and YARA Rules Work 27

High-Level MITRE ATT&CK Tactic Mapping 27

08 Detection Rules

The full deployable files sit in Appendix B. On 21 November 2026, all four rule files passed static validation (0 Suricata lint problems across four rules, structured KQL check, three Sigma rules, and one bounded YARA rule). Because live engines were not run against production traffic on our build host, test and tune each file in staging before production deployment.

Rule file	What it catches
`odin_apk_unpacking_ssrf_oob_and_origin_hunt.rules`	Suricata 7: four signatures for `1-byte` JPEG canary responses, open HTTP directories exposing unpacked mobile packages, and `Interactsh` OAST HTTP/TLS connections
`sentinel_apk_ssrf_oob_origin_and_oast_hunt.kql`	Microsoft Sentinel & Defender XDR: seven-day union of separate hunts for unapproved application-server SMTP egress (:26/:465/:587), server-worker OAST domain callbacks, and unapproved Python `http.server` directory shares
`sigma_ssrf_oob_canary_origin_hunt_and_oast.yml`	Sigma (3 rules): Windows application workers initiating SMTP/SMTPS connections (:26/:465/:587), Linux workers resolving `.oast.*` or `.interact.sh` domains, and unapproved Linux `python3 -m http.server` directory shares
`odin_apk_recon_ssrf_oob_and_origin_hunt_artifacts.yar`	YARA (1 bounded rule): captured Python HTTP open-directory listings exposing unpacked Android `.apk`, `.dex`, and ARM64 native library assets

How the Suricata Signatures Work

SID	Looks for	Operational intent
9547002	Inbound HTTP 200 with `Content-Length: 1` and `image/jpeg`	Catch one-byte JPEG canary responses to internal fetchers
9547006	HTTP 200 `Directory listing for /` exposing `.apk` or `classes*.dex`	Spot exposed HTTP directories staging unpacked mobile packages
9547007	Outbound HTTP :80 with `Interactsh` OAST `Host` domains (feed-listed AWS node IPs withheld)	Alert on outbound HTTP requests whose Host matches an Interactsh OAST domain
9547008	Inbound TLS cert (`CN=`) on :443 matching `Interactsh` OAST domains (feed-listed AWS node IPs withheld)	Alert when a visible server-certificate subject matches an Interactsh OAST domain

Scope `SID 9547002` to backend server subnets and hunt outbound proxy logs for backend fetchers requesting unexpected external image files. Pair `SIDs 9547007` and 9547008 with application-subnet SMTP egress controls on ports 26, 465, and 587.

How the KQL, Sigma, and YARA Rules Work

The KQL and Sigma host allowlists use exact hostnames (`APPSEC-OAST-SCANNER-01`, `REDTEAM-RECON-LAB-01`, `CORP-SMTP-RELAY-01`, `CORP-SMTP-RELAY-02`). Sigma worker selections use exact binary paths; KQL uses executable basenames. Defenders should also audit process and HTTP logs in general terms for backend worker requests to untrusted image URLs and anomalous `PHP-FPM` child processes.

Engine & rule	Severity	Fires when
Sigma 1: App Server Unapproved Outbound SMTP/SMTPS	High	Windows web or application worker binaries initiate outbound TCP 26, 465, or 587 connections outside approved mail relays
Sigma 2: Worker Resolving `Interactsh` Domains	High	Exact Linux worker binaries query `.oast[.]pro`, `.oast[.]live`, `.oast[.]site`, `.oast[.]online`, `.oast[.]fun`, `.oast[.]me`, or `.interact[.]sh`
Sigma 3: Unapproved Python HTTP Directory Share	High	Linux `python3` runs `http.server` outside approved security testing hosts (`REDTEAM-RECON-LAB-01`)
YARA 1: Bounded APK Unpacking OpenDir Rule	High	Matches captured `Python` HTTP open-directory listings exposing unpacked Android `.apk`, `classes.dex`, `arm64-v8a`, or `libhermes.so` assets

High-Level MITRE ATT&CK Tactic Mapping

Parent tactic	Observed reconnaissance or callback behavior	Published detection coverage
`Reconnaissance (TA0043)`	Mobile `.apk`/JS unpacking, scheduled `CDN` origin discovery (57 logs), and `ARL`/`ScopeSentry`/`Subfinder` mapping	`SID 9547006`; KQL; Sigma 3; YARA 1
`Initial Access (TA0001)`	Blind `SSRF` testing via `1-byte` image canaries, staged PHP/gateway YAML templates (114), and origin `CVE-2019-11043` exploit binary	`SID 9547002`; KQL; Sigma 2
`Command and Control (TA0011)`	Commercial-cloud `Interactsh` callback listeners across SMTP/SMTPS (:465, :587, :26) and HTTP/HTTPS (:80, :443)	`SIDs 9547007`–9547008; KQL; Sigma 1–2

CHAPTER 09

Indicators

IN SHORT

This chapter lists the published indicators and explains what stays withheld.

INSIDE THIS CHAPTER

Withheld Feed-Labelled Cloud `Interactsh` Slices (120 IPv4s Withheld) 29

Text-Only JARM and Behavioral Hunt Patterns (7 Reference Patterns) 30

09 Indicators

Appendix A holds **0 published indicators**: **0 IPv4 addresses** and **0 file hashes**. The upstream feed labels 194 endpoints on 120 cloud `Interactsh` IPv4 addresses as confirmed. Independent confirmation is absent, so all 120 addresses remain unconfirmed. We withhold them and all 929 directory file hashes. Four shared TLS JARM fingerprints and three behavioral hunt patterns sit below as text-only reference patterns for hunting.

Indicator type	Published in tab	Recommended action
Feed-labelled `Interactsh` cloud IPv4 addresses (194 ports)	0	All 120 cloud IPv4s withheld (no independent per-address second signal; hunt egress first)
File SHA-256 digests	0	All 929 recorded directory hashes withheld (SDKs, tools, logs & captures)
Shared TLS JARM fingerprints (text-only below)	0 (4 in text)	TLS hunting only; never block on JARM alone
Behavioral HTTP, OAST, and process hunt patterns (text-only below)	0 (3 in text)	Proxy, NDR, and XDR command-line hunting

Withheld Feed-Labelled Cloud `Interactsh` Slices (120 IPv4s Withheld)

Provider or protocol group (addresses withheld)	Port(s)	Hosting & operational note
3 AWS Dual-Port HTTP/HTTPS Hosts	80, 443	AWS (`US`) · Feed-labelled HTTP/HTTPS `Interactsh` listeners; shared JARM; hunt only
1 AWS Plaintext HTTP Host	80	AWS (`US`) · Feed-labelled HTTP `Interactsh` listener; hunt only
1 AWS Alternate-Port SMTP Host	26	AWS (`FR`) · Feed-labelled port 26 SMTP `Interactsh` listener; hunt only
115 Dedicated SMTP/SMTPS Cloud Hosts	465, 587	71 dual 465/587, 37 :587, and 7 :465 cloud hosts across 8 providers (all 115 withheld)

Text-Only JARM and Behavioral Hunt Patterns (7 Reference Patterns)

Pattern or JARM	Context	Where to hunt
`29d29d00029d29d00041d41d00041dcb3f8752a2d70d1dbf446fc46ab5df96`	3 feed-confirmed AWS :443 hosts + 141 feed-suspected endpoints	Go TLS hunt only (never block)
`29d29d00029d29d21c29d29d29d29dab965d4179316d1f3a3c5dbe7d8829db`	47 unconfirmed AWS :443 custom-domain candidates	App-server TLS hunt only
`29d29d00029d29d00029d29d29d29da8f16e8f0a21d89b06fef5080cbd1b2a`	19 unconfirmed AWS :443 custom-domain candidates	App-server TLS hunt only
`29d29d00029d29d21c29d29d29d29df87756699516520cdc45e9e59a5a77db`	4 unconfirmed AWS :443 custom-domain candidates	App-server TLS hunt only
`Content-Length: 1` + `image/jpeg` (`HTTP 200`)	`1-byte` SSRF JPEG canary response profile (canary filename & listener ports withheld)	`SID 9547002` and backend proxy egress hunting
`.oast.*` / `.interact.sh` + SMTP :26/:465/:587	Outbound OAST domain resolution and application-server SMTP egress	KQL and Sigma 1–2 for SMTP egress; SIDs 9547007–9547008 for HTTP/TLS OAST domains
`python -m http.server` + `Directory listing for /` (`.apk` / `classes*.dex`)	Unapproved Python HTTP directory shares exposing unpacked mobile assets	KQL and Sigma 3 for processes; SID 9547006 and YARA 1 for directory listings

Withheld: both open-directory host addresses, their five HTTP listener ports, all 271 callback peer addresses, and all 407 reviewed `Interactsh` host addresses remain unpublished. The latter comprise 120 feed-labelled cloud hosts across 194 ports and 287 other hosts across 406 endpoints. Custom certificate domain names, host-derived directory filenames and paths (including the one-byte image canary filename and the `CVE-2019-11043` binary filename), and all 929 recorded directory file hashes also stay withheld.

10

CHAPTER 10

Scope and Limits

IN SHORT

This chapter sets out what the evidence can show and what it cannot.

10 Scope and Limits

This public edition covers a **two-week observation window ending 21 November 2026** across five open HTTP listeners (1,084 sampled entries) and 600 reviewed `Interactsh` endpoints (407 hosts). Earlier dates inside the callback listener log (11 to `18 November 2026`) and the 57 scheduled origin-discovery logs (6 to `20 November 2026`) are timestamps inside files on those servers. They do not represent an extended monitoring period by Odin by Brandefense.

All workspace findings rest on static directory listings and log metadata; no captured binary, script, or template was run, and no external system was contacted. Zero shared IPv4 addresses connect the two workspaces or the 407 reviewed `Interactsh` hosts, so treat this study strictly as an analytical model. Validate any feed-listed `Interactsh` cloud IPv4 address with an independent second signal before placing it on a firewall blocklist.

11

CHAPTER 11

Sources

IN SHORT

This chapter lists the public references used in the report.

11 Sources

1. **OWASP Cheat Sheet Series**, Server-Side Request Forgery Prevention Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html (verified on 21 November 2026).
2. **OWASP Foundation**, OWASP Mobile Application Security Testing Guide (MASTG): https://mas.owasp.org/MASTG/ (verified on 21 November 2026).
3. **ProjectDiscovery**, Interactsh: Out-of-Band Interaction Gathering Server and Client: https://github.com/projectdiscovery/interactsh (verified on 21 November 2026).
4. **ProjectDiscovery**, Nuclei: Fast and Customizable YAML Vulnerability Scanner: https://github.com/projectdiscovery/nuclei (verified on 21 November 2026).
5. **ProjectDiscovery**, Subfinder: Fast Passive Subdomain Enumeration Tool: https://github.com/projectdiscovery/subfinder (verified on 21 November 2026).
6. **Cloudflare Fundamentals Documentation**, Protect Your Origin Server: https://developers.cloudflare.com/fundamentals/security/protect-your-origin-server/ (verified on 21 November 2026).
7. **MITRE ATT&CK**, Enterprise Tactic TA0043: Reconnaissance: https://attack.mitre.org/tactics/TA0043/ (verified on 21 November 2026).
8. **NIST National Vulnerability Database**, CVE-2019-11043 Detail (PHP-FPM `fastcgi_split_path_info` Buffer Underflow in PHP < 7.1.33, < 7.2.24, < 7.3.11): https://nvd.nist.gov/vuln/detail/CVE-2019-11043 (verified on 21 November 2026).
9. **Amazon Web Services Documentation**, Use the Instance Metadata Service (IMDSv2) to Access Instance Metadata: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/configuring-instance-metadata-service.html (verified on 21 November 2026).

APPENDICES

Indicators and Detection Rules

FOR DEFENDERS

No individual indicators are published for this study; Appendix A explains why. Appendix B carries every published detection rule in full.

INSIDE

A. Indicators of compromise (0) 36

B. Detection rules (4 files) 37

A Indicators of Compromise

No individual addresses or file hashes 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 in Appendix B.

B Detection Rules

Each rule file loads in its own engine (YARA-X, Suricata 7, Kusto, pySigma). Tune thresholds and allow-lists to your environment before alerting or blocking. The same files can be downloaded from the online edition.

odin_apk_recon_ssrf_oob_and_origin_hunt_artifacts.yar

YARA

```
/*
   Odin by Brandefense - Monograph 47 / 52 YARA Artifact Suite
   Scope: Structural detection rule for exposed Python HTTP open-directory
          listings staging unpacked Android package assets.
   Classification: TLP:CLEAR
*/

rule ODIN_Exposed_APK_Unpacking_OpenDir
{
    meta:
        author = "Odin by Brandefense"
        monograph = "47 / 52"
        classification = "TLP:CLEAR"
        action = "CONTAIN_EXPOSED_RECON_DIRECTORY"
        description = "Matches captured Python HTTP open-directory listings exposing unpacked Android APK, DEX,
and ARM64 native library assets"
    strings:
        $d1 = "Directory listing for /" ascii
        $d2 = "<title>Directory listing for " ascii
        $a1 = ".apk\"" ascii
        $a2 = "classes.dex" ascii
        $a3 = "arm64-v8a" ascii
        $a4 = "libhermes.so" ascii
    condition:
        filesize < 1MB and ($d1 or $d2) and 2 of ($a1, $a2, $a3, $a4)
}
```

odin_apk_unpacking_ssrf_oob_and_origin_hunt.rules

SURICATA

```
# Odin by Brandefense - Monograph 47 / 52 Suricata 7.x Detection Suite
# Coverage: Inbound 1-byte JPEG SSRF canary HTTP responses, open Python HTTP
#           directory listings exposing unpacked mobile packages, and Interactsh
#           OAST HTTP/TLS callback traffic
# Classification: TLP:CLEAR

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN [R47] Inbound 1-Byte JPEG SSRF Canary HTTP 200
Response"; flow:established,to_client; http.stat_code; bsize:3; content:"200"; http.header; bsize:>18;
content:"Content-Length: 1|0d 0a|"; fast_pattern; content:"image/jpeg"; classtype:web-application-attack; sid:
9547002; rev:1; metadata:created_at 2026_11_21, deployment perimeter_egress, tactic command_and_control;)

alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN [R47] Open HTTP Directory Listing Exposing Unpacked
Mobile Package"; flow:established,to_client; http.stat_code; bsize:3; content:"200"; http.response_body;
bsize:>48; content:"Directory listing for /"; fast_pattern; pcre:"/(\.apk\"|classes[0-9]*\.dex\")/";
classtype:attempted-recon; sid:9547006; rev:3; metadata:created_at 2026_11_21, deployment perimeter_egress,
tactic reconnaissance;)

alert http $HOME_NET any -> $EXTERNAL_NET 80 (msg:"ODIN [R47] Outbound Plaintext HTTP Connection to Interactsh
OAST Node"; flow:established,to_server; http.host; bsize:>8; pcre:"/\.(oast\.(pro|live|site|online|fun|me)|
interact\.sh)$/i"; classtype:trojan-activity; sid:9547007; rev:2; metadata:created_at 2026_11_21, deployment
perimeter_egress, tactic command_and_control;)

alert tls $EXTERNAL_NET 443 -> $HOME_NET any (msg:"ODIN [R47] Inbound TLS Server Certificate Handshake from
Interactsh OAST Node"; flow:established,to_client; tls.cert_subject; bsize:>10; content:"CN="; fast_pattern;
pcre:"/CN=[^,]*\.(oast\.(pro|live|site|online|fun|me)|interact\.sh)/i"; classtype:trojan-activity; sid:9547008;
rev:2; metadata:created_at 2026_11_21, deployment perimeter_egress, tactic command_and_control;)
```

sentinel_apk_ssrf_oob_origin_and_oast_hunt.kql

KQL (SENTINEL / DEFENDER XDR)

```
// Odin by Brandefense - Monograph 47 / 52 Microsoft Sentinel & Defender XDR Hunt
// Unions independent hunts for application-server SMTP egress (ports 26, 465, 587),
// server worker Interactsh domain callbacks (.oast.* or .interact.sh),
// and unapproved Python http.server directory shares.
// Classification: TLP:CLEAR

let Lookback = 7d;
let ApprovedAppSecHosts = dynamic(["APPSEC-OAST-SCANNER-01", "REDTEAM-RECON-LAB-01"]);
let ApprovedMailRelays = dynamic(["CORP-SMTP-RELAY-01", "CORP-SMTP-RELAY-02"]);
let ServerRuntimes = dynamic(["java", "java.exe", "php-fpm", "php-cgi", "php-cgi.exe", "node", "node.exe",
"python3", "python.exe", "dotnet", "dotnet.exe", "w3wp.exe", "nginx", "httpd"]);
let OastSmtpEgress =
    DeviceNetworkEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedAppSecHosts) or DeviceName in~ (ApprovedMailRelays))
    | where InitiatingProcessFileName in~ (ServerRuntimes)
    | where RemotePort in (26, 465, 587)
    | project EventTime = Timestamp, DeviceId, DeviceName, InitiatingProcessAccountName,
              InitiatingProcessFileName, InitiatingProcessCommandLine, RemoteIP, RemotePort,
              RemoteUrl, SignalClass = "HUNT_APP_SERVER_SMTP_EGRESS";
let ServerOastDomainEgress =
    DeviceNetworkEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedAppSecHosts) or DeviceName in~ (ApprovedMailRelays))
    | where InitiatingProcessFileName in~ (ServerRuntimes)
    | where RemoteUrl has_any (".oast.pro", ".oast.live", ".oast.site", ".oast.online", ".oast.fun", ".oast.me",
".interact.sh")
    | project EventTime = Timestamp, DeviceId, DeviceName, InitiatingProcessAccountName,
              InitiatingProcessFileName, InitiatingProcessCommandLine, RemoteIP, RemotePort,
              RemoteUrl, SignalClass = "HUNT_SERVER_OAST_DOMAIN_CALLBACK";
let UnapprovedPythonHttpProcs =
    DeviceProcessEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedAppSecHosts))
    | where FileName in~ ("python", "python3", "python.exe") and ProcessCommandLine has "http.server"
    | project EventTime = Timestamp, DeviceId, DeviceName,
              InitiatingProcessAccountName = AccountName,
              InitiatingProcessFileName = FileName,
              InitiatingProcessCommandLine = ProcessCommandLine,
              RemoteIP = "", RemotePort = 0, RemoteUrl = "",
              SignalClass = "CONTAIN_EXPOSED_PYTHON_HTTP_SHARE";
union OastSmtpEgress, ServerOastDomainEgress, UnapprovedPythonHttpProcs
| sort by EventTime desc
```

sigma_ssrf_oob_canary_origin_hunt_and_oast.yml

SIGMA

```
title: Application Server Worker Initiating Unapproved Outbound SMTP or SMTPS
id: 7a41d8c2-5e19-4b32-9c04-202611214701
status: experimental
description: Detects Windows web or application server worker processes initiating outbound TCP connections on
SMTP submission or SMTPS ports (26, 465, 587) outside approved corporate mail relays and security testing hosts.
author: Odin by Brandefense
date: 2026/11/21
tags:
  - attack.command-and-control
  - attack.initial-access
logsource:
  category: network_connection
  product: windows
detection:
  selection_worker_smtp:
    Initiated: 'true'
    Image:
      - 'C:\Program Files\Java\jre\bin\java.exe'
```

```
        - 'C:\Program Files\nodejs\node.exe'
        - 'C:\Python311\python.exe'
        - 'C:\PHP\php-cgi.exe'
        - 'C:\Windows\System32\inetsrv\w3wp.exe'
        - 'C:\Program Files\dotnet\dotnet.exe'
      DestinationPort:
        - 26
        - 465
        - 587
    filter_approved_relays:
      ComputerName:
        - 'APPSEC-OAST-SCANNER-01'
        - 'REDTEAM-RECON-LAB-01'
        - 'CORP-SMTP-RELAY-01'
        - 'CORP-SMTP-RELAY-02'
    condition: selection_worker_smtp and not filter_approved_relays
  falsepositives:
    - Application servers configured to send transactional mail directly rather than through designated corporate
  SMTP relays
  level: high
  ---
  title: Application Server Worker Resolving Interactsh Out-of-Band Callback Domains
  id: 8b52e9d3-6f20-4c43-ad15-202611214702
  status: experimental
  description: Detects Linux web or application server worker binaries resolving ProjectDiscovery Interactsh out-
  of-band callback domains, indicating blind SSRF or server-side injection validation.
  author: Odin by Brandefense
  date: 2026/11/21
  tags:
    - attack.initial-access
    - attack.command-and-control
  logsource:
    category: dns_query
    product: linux
  detection:
    selection_worker:
      Image:
        - '/usr/bin/java'
        - '/usr/sbin/php-fpm'
        - '/usr/bin/php-cgi'
        - '/usr/bin/node'
        - '/usr/bin/python3'
        - '/usr/bin/dotnet'
    selection_oast_domain:
      QueryName|endswith:
        - '.oast.pro'
        - '.oast.live'
        - '.oast.site'
        - '.oast.online'
        - '.oast.fun'
        - '.oast.me'
        - '.interact.sh'
    filter_approved_scanners:
      ComputerName:
        - 'APPSEC-OAST-SCANNER-01'
        - 'REDTEAM-RECON-LAB-01'
    condition: selection_worker and selection_oast_domain and not filter_approved_scanners
  falsepositives:
    - Scheduled dynamic application security testing runs on non-allowlisted staging hosts
  level: high
  ---
  title: Unapproved Python HTTP Directory Share Execution
  id: 9c63fae4-7a31-4d54-be26-202611214703
  status: experimental
  description: Detects Linux execution of Python http.server directory-sharing processes outside approved security
  testing hosts.
  author: Odin by Brandefense
  date: 2026/11/21
  tags:
    - attack.reconnaissance
  logsource:
    category: process_creation
```

```
    product: linux
  detection:
    selection_runtime:
      Image:
        - '/usr/bin/python3'
        - '/usr/local/bin/python3'
    selection_http_module:
      CommandLine|contains: 'http.server'
    filter_lab_hosts:
      ComputerName:
        - 'REDTEAM-RECON-LAB-01'
    condition: selection_runtime and selection_http_module and not filter_lab_hosts
  falsepositives:
    - Authorized red-team assessment servers not yet added to REDTEAM-RECON-LAB-01
  level: high
```

ODIN

About Odin Research

Odin Research is the public research series of Odin by Brandefense. It documents adversary infrastructure seen on the internet and turns each finding into indicators and detection rules that defenders can use. Victims and third parties stay anonymous, addresses appear only for confirmed adversary infrastructure, and no working attack code is published.

Odin is the agentic analyst inside the Brandefense threat intelligence platform, which unifies Cyber Threat Intelligence, Digital Risk Protection and External Attack Surface Management.

Online edition, indicators and rules · brandefense.io/odin-research/reports/mobile-apk-unpacking-and-ssrf-canaries/
Short Read · brandefense.io/odin-research/blog/inside-multi-port-apk-unpacking-ssrf-image-canaries-and-cdn/
Defense Kit · brandefense.io/odin-research/defense-kit/