FULL REPORT · C2 INFRASTRUCTURE · MONOGRAPH 59 / 57 · 17 MIN READ

PandaV7 and AndroidRAT Panels: Two Unlinked Candidate Populations

Evaluating 362 candidate PandaV7 and AndroidRAT endpoints across 202 distinct hosts, multi-port VPS co-hosting, and defender hunt controls

BY
Odin by Brandefense

PUBLISHED
19 November 2026

READING TIME
17 min read

EDITION
Version 1.1 · TLP:CLEAR

SCOPE
Prepared November 2026

1. Executive Summary

IN SHORT

Odin by Brandefense indexed 362 candidate endpoints across 202 hosts in a two-week observation window ending 24 November 2026. The set holds 347 PandaV7 ports on 187 hosts and 15 AndroidRAT ports on 15 hosts, sharing zero IPv4s. Zero IPs are published without a second C2 beacon. Restrict TCP 3000 and 3002, block unmanaged APK sideloading, and deploy behavioral hunt rules.

Security teams often ingest feeds that label newly discovered web panels as mobile command-and-control servers. When an upstream tag rests on an HTTP title or port layout alone, automatic IP blocking creates operational risk. Commercial virtual private server subnets host app-distribution tools, developer Node.js apps, and remote administration panels side by side.

In a two-week observation window ending 24 November 2026, Odin by Brandefense examined 362 candidate endpoints across two populations. The larger group holds 347 PandaV7 endpoints across 187 distinct IPv4 hosts in 15 countries and 48 autonomous systems. The smaller group holds 15 AndroidRAT endpoints across 15 distinct IPv4 hosts in six countries and five autonomous systems.

Comparing all 187 PandaV7 addresses with all 15 AndroidRAT addresses shows zero shared IPv4 addresses and zero shared TLS certificates. Neither population overlaps with any recorded open web directory. Every record carries candidate status without an independent second C2 beacon, so zero IPv4s or certificate domains are published.

1. **Multi-port layouts define the 347 PandaV7 candidate endpoints.**
Across 187 PandaV7 hosts observed from 10 to 24 November 2026, 117 hosts expose two to five ports at once. Listeners cluster on TCP 443, 3000, 3002, and 80 (331 endpoints, 95.4%), led by Hong Kong (258 endpoints on 136 hosts).

2. **Stored banners on 29 of 187 PandaV7 hosts show shared TLS stacks and co-hosted panels.**
Across 29 hosts carrying stored HTTP and TLS banners, 35 HTTP 200 responses returned the PandaV7 HTML title. Two TLS **JARM** hashes accounted for 13 of 18 fingerprinted TLS ports, while individual hosts co-hosted Alpha App Management or Android panels.

3. **Fifteen AndroidRAT candidates form an unlinked TCP 443 cluster on dedicated servers.**
Observed on 23 and 24 November 2026, all 15 AndroidRAT candidate records are on TCP 443 across 15 hosts; one bannered host also served TCP 80. Nine sit on UAB Cherry Servers ranges, led by the United States (8) and Singapore (3).

4. **Behavioral network and Android permission rules outperform static IP blocklists.**
Standard Ubuntu nginx TLS stacks produce the same JARM hashes seen on PandaV7 hosts. Alerting on high-port panels, blocking unmanaged APK sideloading, and restricting accessibility grants gives defenders durable coverage.

Three Decisions for Security and Mobility Leaders

1. **Keep single-signal candidate panels off automated blocklists.** Route unverified panel feeds into SIEM watchlists until an implant beacon or verified APK payload confirms malicious use.
2. **Restrict outbound access to TCP ports 3000 and 3002.** Block non-browser workstation tools and managed mobile devices from reaching external ports 3000, 3002, and 8080 outside allowlisted CI hosts.
3. **Block unmanaged APK sideloading and restrict high-risk permissions.** Enforce Google Play Protect, block unknown APK sources in MDM, restrict AccessibilityService grants, and audit workstation Android Debug Bridge commands.

2. Two Non-Overlapping Candidate Populations: Ports, Geography, and Hosting

Between `10 November` and `24 November 2026`, Odin by Brandefense indexed **362 candidate management endpoints** across **202 distinct IPv4 hosts**. Those endpoints split into **347** `PandaV7` **endpoints** on **187** hosts and **15** `AndroidRAT` **endpoints** on **15** hosts. Enterprise defenders use external attack surface management to spot similar multi-port web exposures on their own cloud assets.

Nothing in the dataset links the two populations: they share **0 IPv4 addresses**, 0 TLS certificates, and 0 JARM fingerprints. Only `NetLab Global` appears in both autonomous system lists (**11** `PandaV7` ports on **8** hosts versus **1** `AndroidRAT` port on **1** host), reflecting ordinary VPS tenancy (`[REF-02]`). Figure 1 maps the population split.

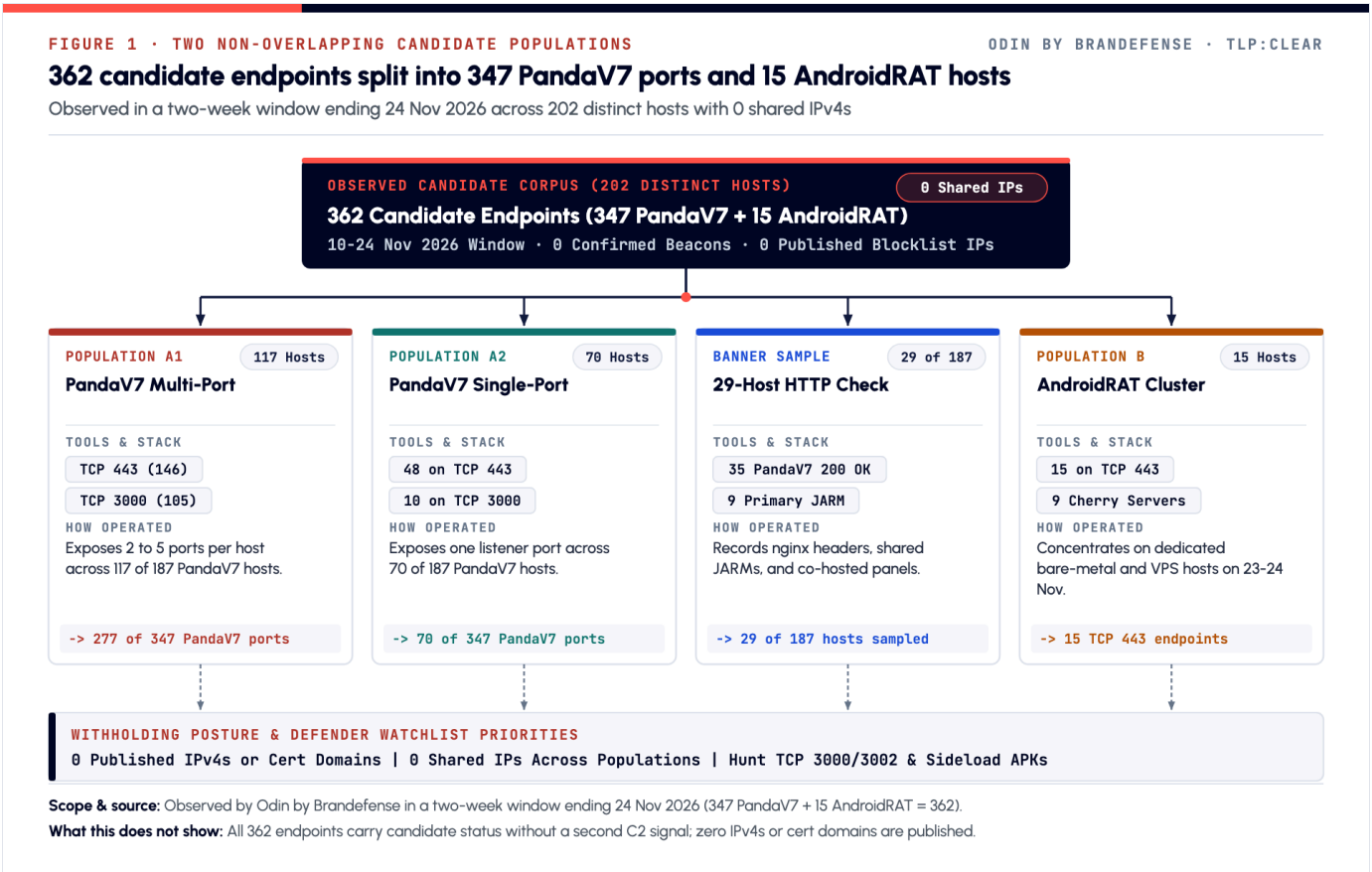

Figure 1: 362 candidate endpoints split into 347 PandaV7 ports and 15 AndroidRAT hosts

Port Distribution and Multi-Port Host Density (`n = 362` Endpoints, 202 Hosts)

Within `PandaV7` (**347** endpoints on **187** hosts), **1** endpoint was first recorded on `10 November 2026`. Another **333** appeared on `23 November` and **13** on `24 November` (**75** last seen `23 November`, **272** last seen `24 November`). All **15** `AndroidRAT` endpoints were first recorded on `23 November 2026` (**1** last seen `23 November`, **14** last seen `24 November`).

Out of **187** `PandaV7` hosts, **117 hosts (62.6%) expose two to five** `PandaV7` **ports at once**, generating **277** of **347** endpoints (**79.8%**). Seventy hosts expose **1** port (**70** endpoints) and **83** expose **2** ports (**166** endpoints). Twenty-seven hosts expose **3** ports (**81** endpoints), **5** expose **4** ports (**20** endpoints), and **2** expose **5** ports (**10** endpoints).

Across individual port pairings, **52** hosts pair **443 + 3000** (**104** endpoints), **48** expose **443** alone (**48**), and **23** expose **443 + 3000 + 3002** (**69**). Twelve hosts pair **80 + 443** (**24**), **10** expose **3000** alone (**10**), and **9** pair **3000 + 3002** (**18**). Five expose **80** alone (**5**), **5** expose **80 + 443 + 3000 + 3002** (**20**), and **23** use other pairings (**49**). All **15** `AndroidRAT` candidate records are on `TCP 443` (**1** bannered host also served `TCP 80`).

Population	TCP port	Endpoints	Family share	Port classification	Observed infrastructure role
PandaV7	443	146	42.1%	Standard HTTPS web port	Primary TLS front-end console listener (`[REF-03]`)
PandaV7	3000	105	30.3%	Non-standard Node.js / app port	Primary high-port `PandaV7` web listener (`[REF-01]`)
PandaV7	3002	47	13.5%	Secondary non-standard app port	Companion API or secondary panel port (`[REF-01]`)
PandaV7	80	33	9.5%	Cleartext HTTP web port	Cleartext `PandaV7` or co-hosted reverse-proxy listener
PandaV7	8080	5	1.4%	Alternate HTTP web port	Alternate HTTP panel port
PandaV7	8443	3	0.9%	Alternate HTTPS web port	Alternate TLS panel port
PandaV7	8 single-hit ports (3001, 3022, 3100, 3110, 8089, 8553, 20080, 39002)	8	2.3%	Custom high TCP ports (1 each)	Long-tail custom port bindings
PandaV7 subtotal	**14 distinct ports**	**347**	**100.0%**	**Across 187 distinct hosts**	**117 multi-port hosts + 70 single-port hosts**
AndroidRAT	443	15	100.0%	Standard HTTPS listener port	Candidate records on `TCP 443` across 15 hosts (`23-24 Nov 2026` ; 1 bannered host also on 80)
Combined corpus	**14 distinct TCP ports**	**362**	**100.0%**	**Across 202 distinct hosts**	**0 cross-family shared IPv4 addresses**

Geographic and Hosting Provider Concentration

In `PandaV7`, **Hong Kong (`HK`) holds 258 of 347 endpoints (74.4%) across 136 of 187 hosts (72.7%)**. The United States holds **44** endpoints on **22** hosts (**12.7%**), and Singapore holds **14** on **9** hosts (**4.0%**). Malaysia holds **6** on **4** hosts (**1.7%**), while the United Kingdom (**4** on **2**) and Japan (**4** on **4**) hold **1.2%** each.

Nine more countries hold **17** `PandaV7` endpoints across **10** hosts. Indonesia and Hungary hold **3** on **1** host each, while India, China, and Brazil hold **2** on **1** each. Germany holds **2** on **2** hosts, and France, Jordan, and Thailand hold **1** each. Across `AndroidRAT`, the United States holds **8** hosts (**53.3%**), Singapore holds **3** (**20.0%**), and Japan, Brazil, Spain, and Hong Kong hold **1** each (**6.7%**).

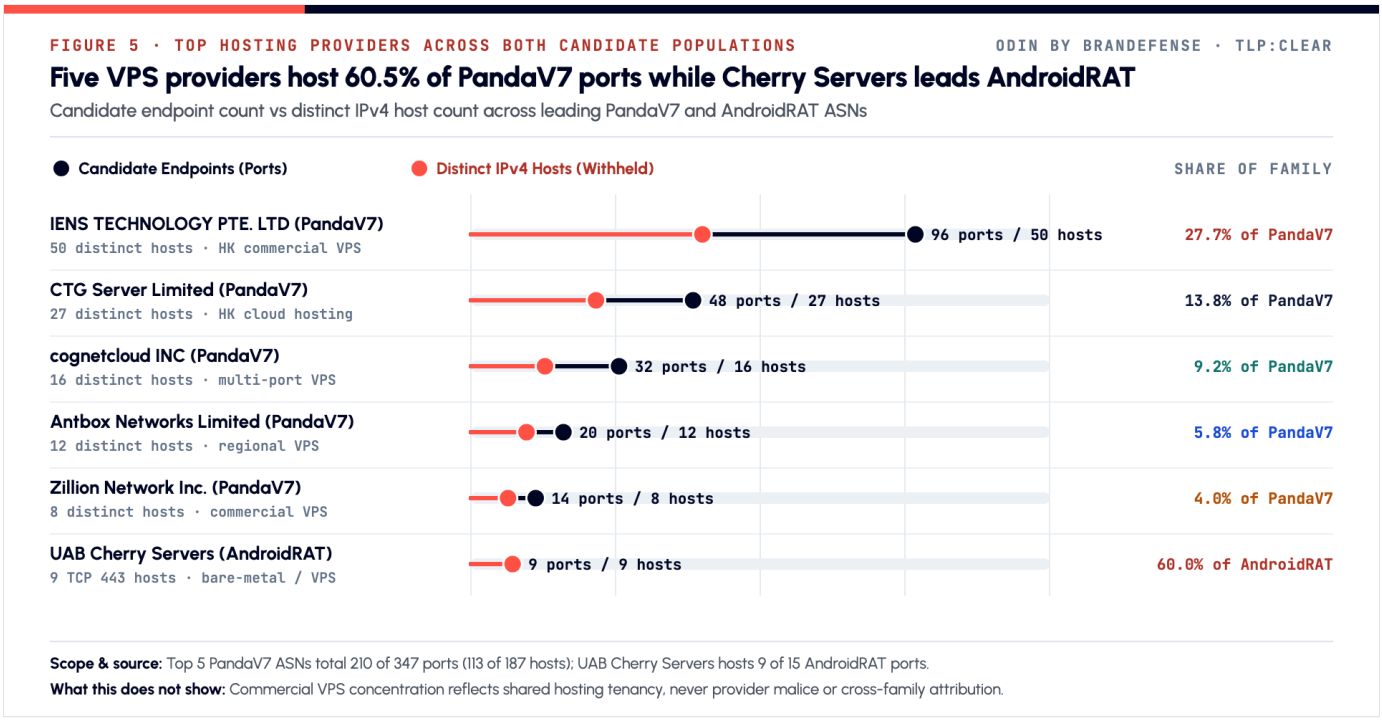

Figure 5: Five VPS providers host 60.5% of PandaV7 ports while Cherry Servers leads AndroidRAT

All **347** `PandaV7` endpoints span **48** autonomous systems (**210** endpoints, **60.5%**, across the top five ASNs, and **277**, **79.8%**, across the top **12**). In `AndroidRAT`, `UAB "Cherry Servers"` hosts **9** of **15** endpoints (**60.0%**).

Population	Autonomous system / provider	Endpoints	Distinct hosts	Family share	Hosting profile
PandaV7	`IENS TECHNOLOGY PTE. LTD`	96	50	27.7%	Regional Hong Kong / APAC commercial VPS
PandaV7	`CTG Server Limited`	48	27	13.8%	Hong Kong cloud and VPS hosting
PandaV7	`cognetcloud INC`	32	16	9.2%	Multi-port commercial cloud VPS

Population	Autonomous system / provider	Endpoints	Distinct hosts	Family share	Hosting profile
PandaV7	`Antbox Networks Limited`	20	12	5.8%	Regional commercial VPS hosting
PandaV7	`Zillion Network Inc.`	14	8	4.0%	Regional cloud VPS hosting
PandaV7	`GNET INC.`	12	5	3.5%	Commercial cloud hosting
PandaV7	`Cloudie Limited`	12	5	3.5%	Hong Kong VPS infrastructure
PandaV7	`NetLab Global`	11	8	3.2%	Commercial VPS provider
PandaV7	`Nebula Global LLC`	9	3	2.6%	Multi-port VPS hosting (3.0 ports/host)
PandaV7	`Alibaba (US) Technology Co., Ltd.`	8	4	2.3%	Public cloud compute instances
PandaV7	`Yancy Limited`	8	2	2.3%	Multi-port VPS hosting (4.0 ports/host)
PandaV7	`CORENET CLOUD SDN. BHD.`	7	3	2.0%	Southeast Asian cloud VPS
PandaV7	Other 36 commercial ASNs (1-6 endpoints each)	70	44	20.2%	Long-tail VPS and cloud providers
PandaV7 subtotal	**48 commercial ASNs**	**347**	**187**	**100.0%**	**Zero open-directory overlaps (0 of 187)**
AndroidRAT	`UAB "Cherry Servers"`	9	9	60.0%	Dedicated bare-metal and cloud VPS
AndroidRAT	`Latitude[.]sh`	2	2	13.3%	Dedicated bare-metal cloud instances
AndroidRAT	`Ultahost, Inc.`	2	2	13.3%	Commercial VPS hosting
AndroidRAT	`ByteVirt LLC`	1	1	6.7%	Budget regional VPS hosting

Population	Autonomous system / provider	Endpoints	Distinct hosts	Family share	Hosting profile
AndroidRAT	`NetLab Global`	1	1	6.7%	Commercial VPS (0 shared IPs with `PandaV7`)
AndroidRAT subtotal	5 commercial ASNs	15	15	100.0%	Zero open-directory overlaps (0 of 15)
Combined total	52 unique ASNs (1 shared provider name)	362	202	100.0%	Complete host and port reconciliation

3. PandaV7 Multi-Port Architecture, Banner Samples, and Co-Hosted Panels

Evaluating `PandaV7` requires separating full-population port counts (**347** endpoints on **187** hosts) from smaller HTTP and TLS banner subsets (`[REF-07]`). Analysts working with cyber threat intelligence can correlate these banner traits without turning unverified VPS hosts into blocklists. Figure 4 contrasts the multi-port `PandaV7` VPS stack with `AndroidRAT`.



Figure 4: Multi-port PandaV7 VPS layouts contrast with TCP 443 AndroidRAT records

Reconciling the 25-Host Spot-Check and the 29-of-187 Banner Sample

Two banner checks clarify HTTP responses and TLS profiles across the **187** `PandaV7` hosts:

- **Initial lexicographical check (25 of 187 hosts).** Checking the first **25** lexicographically sorted `PandaV7` hosts found **5** endpoints with `<title>PandaV7</title>` and the primary JARM hash below. Zero of those **25** hosts served `Alpha App Management` on `TCP 80`.
- **Full stored-banner review (29 of 187 hosts).** Checking all **187** `PandaV7` hosts identified **29 of 187 hosts (15.5%)** with stored HTTP and TLS banner records. Across those **29** hosts, **35 endpoints returned HTTP 200 with** `<title>PandaV7</title>`: **14** on `TCP 443`, **12** on `TCP 3000`, and **9** on `TCP 80`.

Response headers on those **35** `<title>PandaV7</title>` endpoints show `nginx/1.18.0 (Ubuntu)` on **15** of **35** responses and `nginx/1.24.0 (Ubuntu)` on **5** of **35**. Three report bare `nginx`, and **12** omit the `Server` header. Administrators often place `nginx` on **80** and **443** in front of app ports **3000** and **3002** while leaving both high ports open (`[REF-01]`, `[REF-03]`).

Recurring TLS JARM Fingerprints and Co-Hosted Panels (29 of 187 Hosts)

Within the **29**-of-**187** banner sample, **18** `<title>PandaV7</title>` endpoints carried TLS JARM fingerprints (`[REF-07]`). Two hashes accounted for **13** of **18** TLS listeners, while five distinct JARM hashes appeared once each. Standard Ubuntu `nginx` builds share these JARM hashes, so none is a standalone blocklist indicator.

JARM role & population	Recorded 62-character TLS JARM fingerprint	Sample count	Stack interpretation
`PandaV7` primary JARM	`2ad2ad0002ad2ad00042d42d0000000464fb8c6842ac133bede81390a48134`	9 of 18 (5 of 25 initial)	Standard Ubuntu `nginx` TLS profile (10 total ports on the 29 hosts); enrichment only.

JARM role & population	Recorded 62-character TLS JARM fingerprint	Sample count	Stack interpretation
`PandaV7` secondary JARM	`29d29d00000000000042d42d000000dd5c266caaa8baaf93008418f7774284`	4 of 18	Secondary `nginx` / TLS stack profile; enrichment only.
`PandaV7` single-hit JARMs	5 distinct single-instance JARM hashes (1 each)	5 of 18	Custom TLS cipher ordering or upstream reverse proxies.
`AndroidRAT` bannered host	`28d28d28d00028d00042d42d000000831b6af40378e2dd35eeac4e9311926e`	1 of 15 hosts	Recorded on the 1 `AndroidRAT` host carrying stored `nginx` / `nginx/1.31.3` banners.

Reviewing other open ports across the **29 banner-recorded `PandaV7` hosts** revealed co-hosted Chinese-language panels on subsets of hosts (English translations below). Because each co-hosted title appears on **1** to **4** endpoints inside a **29**-of-**187** sample, it cannot be projected onto the **158** unbannered hosts.

Observed HTTP panel title (English translation)	Port(s)	Count in 29-host sample	Analytical significance & sample boundary
`PandaV7` (`<title>PandaV7</title>`)	443, 3000, 80	35 endpoints	Core `HTTP 200` panel title (14 on 443, 12 on 3000, 9 on 80) across 29 of 187 hosts.
Fat Wealth God V7 (*PangCaishen V7*)	80, 443	4 endpoints	2 on 80 and 2 on 443; shares the `V7` naming pattern on co-hosted VPS instances.
Alpha App Management (*Alpha App Mgmt*)	80	1 endpoint	Co-hosted on `TCP 80` on 1 of 29 banner-recorded hosts (0 of 25 in initial check).

Observed HTTP panel title (English translation)	Port(s)	Count in 29-host sample	Analytical significance & sample boundary
Eagle Android Remote Management	80, 443	2 endpoints	1 on 80 and 1 on 443 on 1 of 29 hosts; Chinese-language Android management console.
BlackHole Tech Device Management Backend	443	1 endpoint	1 of 29 hosts; Chinese-language mobile device administration login page.
`BTMOB` **Mobile RAT Panel**	5000	1 endpoint	1 of 29 hosts; commodity Android RAT web administration console on `TCP 5000`.
`RAT0` **Panel**	8200	1 endpoint	1 of 29 hosts; remote-access login banner on high port 8200.

4. Dedicated AndroidRAT Cluster and Mobile Abuse Tradecraft Model

On **23** and `24 November 2026`, Odin by Brandefense indexed **15** `AndroidRAT` **candidate endpoints across 15 distinct IPv4 hosts**. Four traits separate these **15** hosts from `PandaV7`:

1. `TCP 443` **candidate record posture (100.0%).** All **15** `AndroidRAT` candidate records are on `TCP 443` across **15** hosts (`[REF-04]`). One bannered host also served a panel on `TCP 80`, while **0** hosts used **3000** or **3002**.
2. **Bare-metal and VPS provider mix.** `UAB "Cherry Servers"` hosts **9** of **15** endpoints (**60.0%**), alongside `Latitude[.]sh` (**2**) and `Ultahost, Inc.` (**2**). `ByteVirt LLC` and `NetLab Global` host **1** each, with the US (**8**) and Singapore (**3**) leading geographically.
3. **Banner sample (1 of 15 hosts).** One host carried stored banners (`nginx` / `nginx/1.31.3`), serving *Vermilion Bird Android Device Management* on **443** and *Eagle Android Remote Management* on **80**. Seeing that second title on **1** host per group reflects a shared commodity template, not an operator link.
4. **Tight** `23-24 November` **window.** All **15** records first appeared on `23 November 2026`, with **14** responsive on `24 November`.

Analytical Model: Rogue App Managers and Android RAT Clients

Odin by Brandefense observed candidate server ports without capturing victim mobile traffic or APK binaries. Client steps therefore form an **analytical defender model** grounded in MITRE ATT&CK Mobile (`[REF-04]` , `[REF-05]` , `[REF-06]`) and Android security documentation (`[REF-08]` , `[REF-09]`). Figure 3 maps that model.

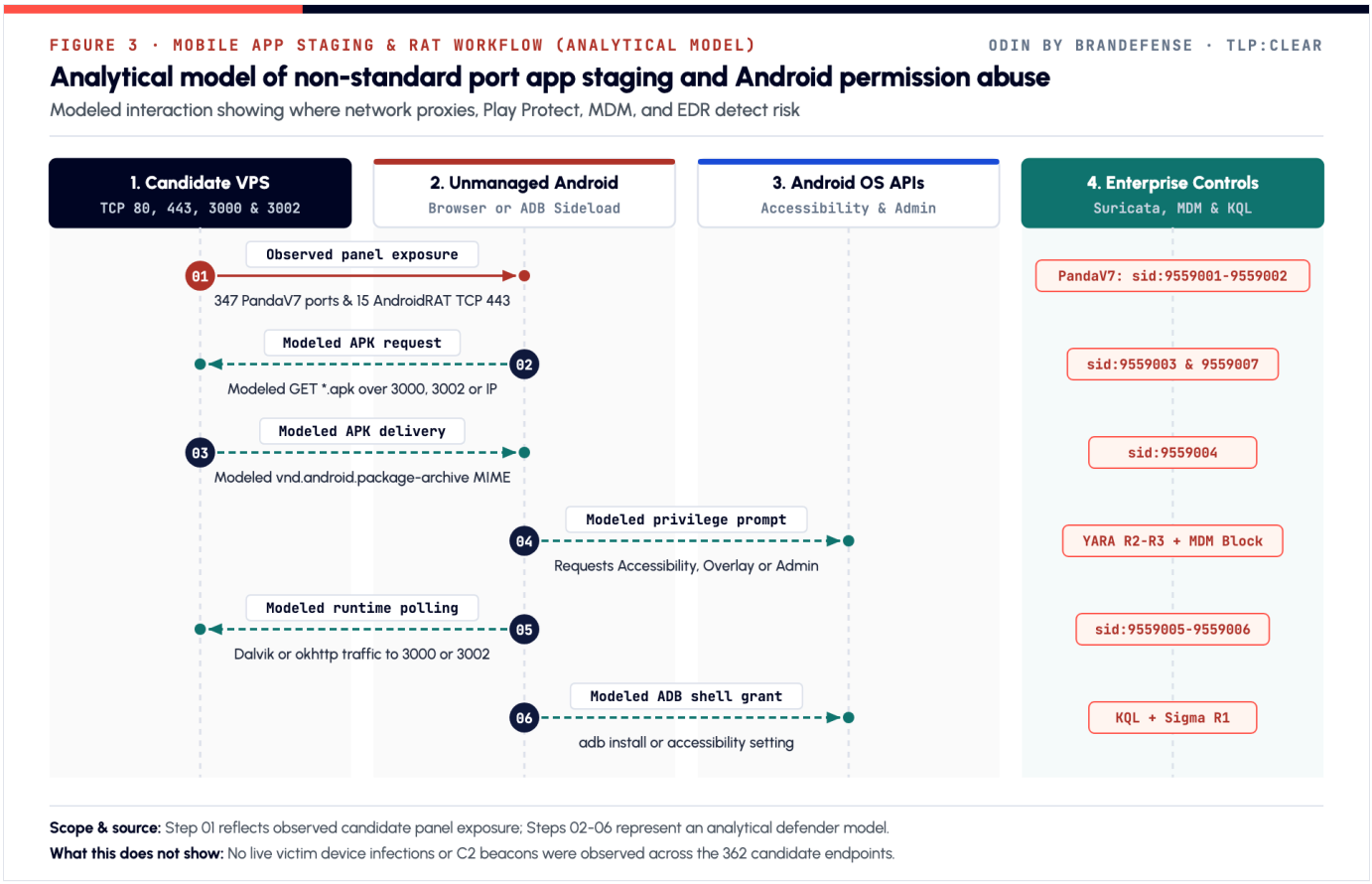

Figure 3: Analytical model of non-standard port app staging and Android permission abuse

Commodity Android RAT and rogue app-manager workflows typically span three client stages:

- **Out-of-store `.apk` delivery.** Panels or direct links serve `.apk` packages (`application/vnd.android.package-archive`) from high ports (**3000**, **3002**, **8080**) or bare IPv4 hosts, bypassing Google Play review (`[REF-09]`).
- **`AccessibilityService` and overlay prompts (`T1453`, `[REF-05]`, `[REF-08]`).** Sideloaded packages request `BIND_ACCESSIBILITY_SERVICE`, `SYSTEM_ALERT_WINDOW`, and SMS rights. Lures guide users past Android Restricted Settings or rely on `adb shell settings put secure enabled_accessibility_services` (`[REF-08]`).
- **`DeviceAdminReceiver` and runtime polling (`T1626.001`, `[REF-06]`).** Many templates request `BIND_DEVICE_ADMIN`, `BOOT_COMPLETED`, and `FOREGROUND_SERVICE` while `Dalvik/` or `okhttp/` HTTP clients poll **443**, **3000**, or **3002** (`[REF-01]`).

Figure 2 maps these observed and modeled layers to the detection rules in Chapter 7.

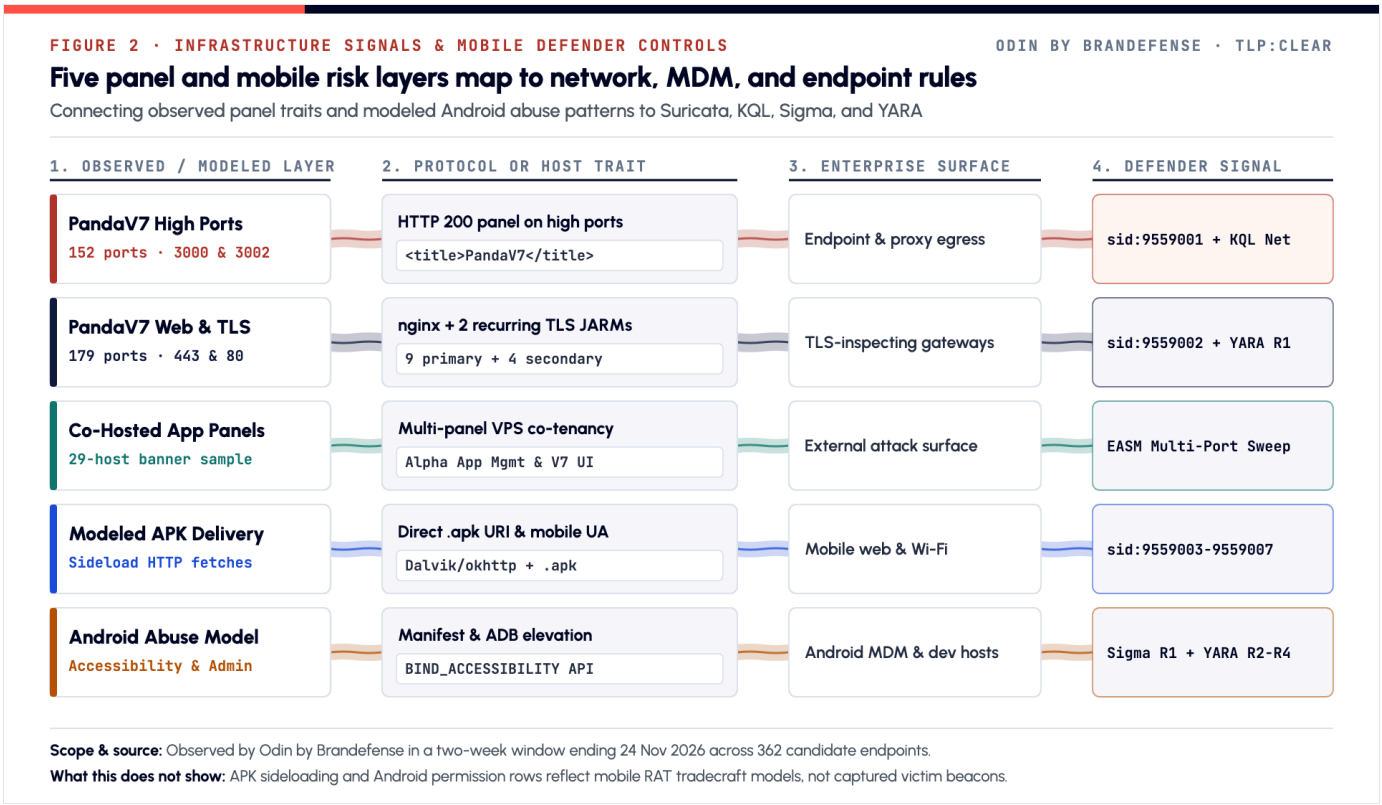

Figure 2: Five panel and mobile risk layers map to network, MDM, and endpoint rules

5. Enterprise Mobile and Perimeter Exposure Analysis

Security teams should verify four network and mobile governance controls (`[REF-10]`):

Exposure surface	Observed Monograph 59 evidence	Control to verify	Operational risk
Egress to ports 3000 & 3002	152 of 347 `PandaV7` endpoints (43.8%) use 3000 (105) or 3002 (47). At least 80 hosts pair 443 with 3000 or 3002: 52 dual-port, 23 triple-port, and 5 four-port hosts.	Verify whether firewalls and mobile gateways block outbound `TCP 3000`, 3002, and 8080 from non-CI hosts (`[REF-01]`).	Endpoints can reach high-port web panels that bypass port-80/443 policies .

Exposure surface	Observed Monograph 59 evidence	Control to verify	Operational risk
Unmanaged Android sideloading	Co-hosted `Alpha App Management` (1 of 29 banner hosts), `BTMOB` (1 of 29), and Android management panels (1 of 29 `PandaV7`; 1 of 15 `AndroidRAT`).	Verify whether MDM (`[REF-10]`) blocks unknown APK sources and requires Google Play Protect (`[REF-09]`) before SSO sign-in.	BYOD or unmanaged phones can sideload trojanized APKs that capture corporate credentials.
`AccessibilityService` & `DeviceAdmin`	Android RAT panels rely on `AccessibilityService` (`[REF-08]`) and `DeviceAdminReceiver` APIs (`[REF-05]`, `[REF-06]`).	Verify whether MDM work profiles restrict non-allowlisted accessibility services and unmanaged device admins.	Accessibility grants allow UI reading, notification scraping, and gesture injection.

Exposure surface	Observed Monograph 59 evidence	Control to verify	Operational risk
Workstation `adb` bridges	Developer laptops often carry `adb` tools able to install APKs and edit secure settings.	Verify whether EDR restricts `adb` usage to approved mobile QA hosts (`qa-appium-01.corp[.]example`).	Local scripts can sideload packages and enable accessibility services silently.

6. Alternative Hypotheses

Hypothesis	Evidence for	Evidence against	Assessment
`PandaV7` (187 hosts) and `AndroidRAT` (15 hosts) form one campaign	Both surged on `23-24 November 2026`, and 1 bannered host in each set showed *Eagle Android Remote Management*.	Comparing 187 `PandaV7` IPs and 15 `AndroidRAT` IPs shows **0 shared IPv4s**, and candidate port profiles (**62.6%** multi-port vs **100%** of `AndroidRAT` records on **443**) and top ASNs differ.	**Unsupported.** Treat them as separate populations; commodity panel templates do not link operators.
All 347 `PandaV7` ports belong on IP blocklists	**29** of **187** hosts return `<title>PandaV7</title>` or co-host `BTMOB`, `RAT0`, and Android panels.	All **347** records carry `candidate` status with **0 victim C2 beacons**, and commercial Hong Kong VPS ranges host mixed web services.	**Unconfirmed per host.** Withhold raw IPs and deploy protocol and permission hunt rules.

Hypothesis	Evidence for	Evidence against	Assessment
Primary JARM uniquely identifies `PandaV7`	Appears on 9 of 18 TLS-fingerprinted `<title>PandaV7</title>` ports (5 of 25 in initial check).	`PandaV7` runs behind standard Ubuntu `nginx/1.18` and 1.24 builds (`[REF-07]`) shared with benign sites.	**Enrichment pivot only.** Combine JARM with HTTP title and port signals, never standalone blocking.
`Alpha App Management` co-hosting is universal across `PandaV7`	Observed on `TCP 80` on 1 of 29 banner-recorded `PandaV7` hosts.	Seen on 0 of 25 hosts in the initial check and 1 of 29 bannered hosts (158 of 187 lacked stored banners).	**Localized co-hosting.** Keep exact 1-of-29 sample bounds.

7. Validated Detection Rules

Zero candidate IPv4 addresses or unverified certificate domains are published. Defenders should deploy **port-aware HTTP, proxy, MDM, and endpoint rules** across any server IP.

All rules below were checked statically against Suricata 7.x HTTP buffer syntax (**0** linter problems), Sentinel KQL schema, Sigma structure (**3** rules), and `filesize`-bounded YARA syntax (**4** rules). Live Suricata, Sentinel, Sigma, and YARA engines were not run on this build host, so validate each rule in staging first.

7.1 Suricata 7.x Network Signatures (`sid:9559001` -9559007)

Rules `sid:9559001` -**9559002** detect `HTTP 200` `<title>PandaV7</title>` responses on **3000**/**3002** and web ports. Rules `sid:9559003` and `sid:9559007` match outbound `.apk` requests over **3000**/**3002** or bare IPv4 `Host` headers. Rule `sid:9559004` matches inbound `application/vnd.android.package-archive` responses, and `sid:9559005` -**9559006** match `Dalvik/` or `okhttp/` traffic on **3000**/**3002**/**8080**. All seven are `alert` rules (not inline blocks) and require cleartext HTTP or a TLS-inspecting proxy on encrypted ports.

```
SURICATA

# Odin by Brandefense - Monograph 59 (PandaV7 Panels & Mobile RAT Clusters) Suricata 7.x Ruleset
# Static syntax checked against Suricata 7.x HTTP buffer rules and Odin Suricata linter (0 problems).

alert http $EXTERNAL_NET [3000,3002] -> $HOME_NET any (msg:"ODIN-R59 PandaV7 Web Panel Title on Non-S
tandard Ports 3000 or 3002"; flow:established,to_client; http.stat_code; content:"200"; bsize:3; htt
p.response_body; content:"<title>PandaV7</title>"; fast_pattern; classtype:trojan-activity; sid:95590
```

```
01; rev:1;)
alert http $EXTERNAL_NET [80,443,8080,8443] -> $HOME_NET any (msg:"ODIN-R59 PandaV7 Web Panel Title o
n Standard or Alt Web Ports"; flow:established,to_client; http.stat_code; content:"200"; bsize:3; htt
p.response_body; content:"<title>PandaV7</title>"; fast_pattern; classtype:trojan-activity; sid:95590
02; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET [3000,3002] (msg:"ODIN-R59 Outbound Android APK Fetch over
Non-Standard Ports 3000 or 3002"; flow:established,to_server; http.method; content:"GET"; bsize:3; ht
tp.uri; content:".apk"; nocase; endswith; fast_pattern; classtype:trojan-activity; sid:9559003; rev:
1;)
alert http $EXTERNAL_NET [3000,3002,8080] -> $HOME_NET any (msg:"ODIN-R59 Inbound Android APK Package
Delivery from Non-Standard Port"; flow:established,to_client; http.content_type; content:"applicatio
n/vnd.android.package-archive"; nocase; fast_pattern; classtype:trojan-activity; sid:9559004; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET [3000,3002,8080] (msg:"ODIN-R59 Outbound Android Dalvik Run
time Request to Non-Standard Port"; flow:established,to_server; http.user_agent; content:"Dalvik/"; s
tartswith; fast_pattern; classtype:command-and-control; sid:9559005; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET [3000,3002,8080] (msg:"ODIN-R59 Outbound Android OkHttp POS
T Beacon to Non-Standard Port"; flow:established,to_server; http.method; content:"POST"; bsize:4; htt
p.user_agent; content:"okhttp/"; startswith; fast_pattern; classtype:command-and-control; sid:955900
6; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R59 Outbound Android APK Fetch Using Bare IP
v4 Host Header"; flow:established,to_server; http.uri; content:".apk"; nocase; endswith; fast_patter
n; http.host; pcre:"/^d{1,3}(?:.d{1,3}){3}(?::d+)?$/"; classtype:trojan-activity; sid:9559007; rev:
1;)
```

7.2 Microsoft Sentinel KQL Hunt

Replace the placeholder FQDNs in `ApprovedMobileDevHosts` (`mobile-ci-01.corp[.]example` and `qa-appium-01.corp[.]example`) with your approved mobile CI and QA runners before scheduling.

```kql
// Odin by Brandefense - Monograph 59 (PandaV7 Panels & Mobile RAT Clusters)
// Hunts non-browser endpoint connections to external TCP 3000/3002, APK fetches, and ADB sideload/ac
cessibility commands.
let Lookback = 7d;
let ApprovedMobileDevHosts = dynamic(["mobile-ci-01.corp.example", "qa-appium-01.corp.example"]);
let NonBrowserClients = dynamic(["curl", "curl.exe", "wget", "python", "python3", "python.exe", "powe
rshell.exe", "pwsh", "pwsh.exe", "java", "java.exe", "adb", "adb.exe"]);
let NonStandardPortOrApkEgress =
    DeviceNetworkEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedMobileDevHosts))
    | where RemoteIPType == "Public"
    | where (
        (RemotePort in (3000, 3002) and InitiatingProcessFileName in~ (NonBrowserClients))
        or (RemotePort in (3000, 3002, 8080) and RemoteUrl endswith ".apk")
    )
    | project Timestamp, DeviceName, AccountName = InitiatingProcessAccountName, SignalType = "NonSta
ndardPortOrApkEgress", Detail = strcat(InitiatingProcessFileName, " -> ", RemoteIP, ":", tostring(Rem
otePort), " ", RemoteUrl);
let AndroidAdbSideloadOrAdminGrant =
    DeviceProcessEvents
```

```
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedMobileDevHosts))
    | where FileName in~ ("adb", "adb.exe")
    | where (
        (ProcessCommandLine has "install" and ProcessCommandLine has ".apk")
        or ProcessCommandLine has_any ("enabled_accessibility_services", "dpm set-active-admin", "BIN
D_ACCESSIBILITY_SERVICE")
    )
    | project Timestamp, DeviceName, AccountName, SignalType = "AndroidAdbSideloadOrAdminGrant", Deta
il = ProcessCommandLine;
union NonStandardPortOrApkEgress, AndroidAdbSideloadOrAdminGrant
| summarize FirstSeen = min(Timestamp), LastSeen = max(Timestamp), EventCount = count(), Signals = ma
ke_set(SignalType, 6), SampleDetails = make_set(Detail, 5) by DeviceName, AccountName
| order by LastSeen desc
```

7.3 Portable Sigma and YARA Rules

- **Sigma (`sigma_pandav7_nonstandard_ports_and_adb_sideload.yml`).** Rule 1 detects Windows `adb.exe` command lines containing `.apk`, `enabled_accessibility_services`, or `dpm set-active-admin`. Rule 2 catches Linux CLI tools (`curl`, `wget`, `python`, `python3`) connecting to **:3000/** or **:3002/**. Rule 3 catches proxy sessions to port **3000** or **3002** from `Dalvik/` or `okhttp/` clients or ending in `.apk`.
- **YARA (`odin_pandav7_panel_and_android_rat_artifacts.yar`).** Four `filesize`-bounded rules detect cached `<title>PandaV7</title>` web panels and Android manifests pairing `BIND_ACCESSIBILITY_SERVICE` with `SYSTEM_ALERT_WINDOW` and SMS or install rights. They also match `BIND_DEVICE_ADMIN` boot persistence and extracted configs pairing Android HTTP clients with **:3000/** or **:3002/**.

8. Behavioral and Protocol Hunt Markers (0 Published IPs or SHA-256s)

No candidate IPv4 addresses or unverified certificate domains appear in the indicator feeds. Defenders should hunt using the 10 protocol, TLS stack, and Android markers below.

Marker category	Pattern / protocol artifact	Layer	Defensive hunt & caution
HTTP panel title	`<title>PandaV7</title>`	HTTP 2000 (443, 30000, 80)	Seen on 35 ports across 29 bannered hosts. Alert with `sid:9559001` - 9559002 behind a TLS proxy.
Multi-port profile	`TCP 443 + TCP 3000 (+ TCP 3002)`	External VPS (443, 30000, 3002)	The two listed 443/3000 configurations cover 75 hosts; five more expose 80 + 443 + 3000 + 3002. Use in multi-port asset sweeps.

Marker category	Pattern / protocol artifact	Layer	Defensive hunt & caution
Primary TLS JARM	`2ad2ad0002ad2ad00042d42d0000000464fb8c6842ac133bede81390a48134`	TLS (443, 30000)	Seen on 9 of 18 TLS-fingerprinted `PandaV7` titles (5 of 25 initial check). Shared with Ubuntu `nginx`; enrichment only.
Secondary TLS JARM	`29d29d00000000000042d42d000000dd5c266caaa8baaf93008418f7774284`	TLS (443, 30000)	Seen on 4 of 18 TLS-fingerprinted `PandaV7` titles. Use only as an enrichment pivot.

Marker category	Pattern / protocol artifact	Layer	Defensive hunt & caution
APK MIME delivery	`application/vnd.android.package-archive`	HTTP (3000, 30002, 8080)	Alert on direct `.apk` downloads from high ports or bare IPv4 hosts (`sid:9559003`-9559004, `sid:9559007`).
Android HTTP UA	`Dalvik/` and `okhttp/`	HTTP (3000, 30002, 8080)	Alert when Android runtime clients poll external high ports (`sid:9559005`-9559006, Sigma Rule 3).

Marker category	Pattern / protocol artifact	Layer	Defensive hunt & caution
Accessibility abuse	`android.permission.BIND_ACCESSIBILITY_SERVICE`	Android APK / MDM	Hunt sideloaded APKs pairing accessibility bindings with `SYSTEM_ALERT_WINDOW` and SMS rights (YARA Rule 2).
Device admin abuse	`android.permission.BIND_DEVICE_ADMIN`	Android APK / MDM	Block unmanaged apps requesting `DEVICE_ADMIN_ENABLED` with `BOOT_COMPLETED` (YARA Rule 3).
ADB shell elevation	`enabled_accessibility_services`	Workstation EDR	Alert on `adb` commands installing `.apk` files or changing accessibility settings (Sentinel KQL, Sigma Rule 1).

Marker category	Pattern / protocol artifact	Layer	Defensive hunt & caution
High-port egress	Outbound `TCP 3000` / `TCP 3002`	Firewall / EDR	Restrict non-browser CLI and endpoint traffic to external `TCP 3000` and 3002 (Sentinel KQL, Sigma Rule 2).

9. Hardening Priorities for Enterprise Mobility and Network Teams

Enterprise teams should close non-standard port egress and unmanaged Android sideloading paths together:

1. **Keep candidate VPS lists out of automated IP blocklists (`0-48 Hours`).** Route upstream `candidate` feeds into SIEM watchlists rather than firewall drop rules across shared VPS subnets (`[REF-02]`).
2. **Block unmanaged outbound access to `TCP 3000`, 3002, and 8080 (`0-72 Hours`).** Deny direct outbound connections to ports **3000**, **3002**, and **8080** from corporate Wi-Fi, VPN, and workstation VLANs outside allowlisted CI runners (`[REF-01]`).
3. **Block unknown APK sideloading and require Google Play Protect (`Days 1-7`).** Enforce Android Enterprise `DISALLOW_INSTALL_UNKNOWN_SOURCES` policies (`[REF-10]`) and require Play Protect attestation (`[REF-09]`) before SSO sign-in.
4. **Restrict `AccessibilityService` and legacy `DeviceAdmin` bindings (`Days 7-14`).** Set Android Enterprise `permittedAccessibilityServices` allowlists (`[REF-05]`, `[REF-08]`) and audit non-MDM `DeviceAdminReceiver` grants (`[REF-06]`).
5. **Audit workstation `adb` tools and inspect mobile web traffic (`Days 14-30`).** Deploy Sentinel KQL and Sigma Rules 1-2 on endpoints, Sigma Rule 3 at web proxies, and Suricata `sid:9559001`-**9559007** behind TLS-inspecting gateways.

10. Scope, Limits, and External References

Odin by Brandefense analyzed **362** candidate endpoints recorded in a two-week observation window ending `24 November 2026`. That corpus covers **347** `PandaV7` endpoints on **187** hosts (`10 to 24 November`) and **15** `AndroidRAT` endpoints on **15** hosts (`23 to 24 November`). Zero shared IPv4 addresses or open directories link the two sets.

All **362** endpoints carry upstream `candidate` status without an independent second C2 beacon, so **0** IPv4 addresses and **0** certificate domains are published. Banner, `nginx`, JARM, and co-hosting counts cover **29** of **187** `PandaV7` hosts (**25** in the initial check) and **1** of **15** `AndroidRAT` hosts. Live Suricata, Sentinel, Sigma, and YARA engines were not run on this build host, so validate each rule in staging before deployment.

1. `[REF-01]` MITRE ATT&CK Enterprise, *Non-Standard Port (T1571)* (verified on 24 November 2026).
2. `[REF-02]` MITRE ATT&CK Enterprise, *Acquire Infrastructure: Virtual Private Server (T1583.003)* (verified on 24 November 2026).
3. `[REF-03]` MITRE ATT&CK Enterprise, *Application Layer Protocol: Web Protocols (T1071.001)* (verified on 24 November 2026).
4. `[REF-04]` MITRE ATT&CK Mobile, *Application Layer Protocol: Web Protocols (T1437.001)* (verified on 24 November 2026).
5. `[REF-05]` MITRE ATT&CK Mobile, *Abuse Accessibility Features (T1453)* (verified on 24 November 2026).
6. `[REF-06]` MITRE ATT&CK Mobile, *Abuse Elevation Control Mechanism: Device Administrator Permissions (T1626.001)* (verified on 24 November 2026).
7. `[REF-07]` Salesforce Engineering, *JARM: An Active Transport Layer Security (TLS) Server Fingerprinting Tool* (verified on 24 November 2026).
8. `[REF-08]` Android Developers, *AccessibilityService API Reference and Security Model* (verified on 24 November 2026).
9. `[REF-09]` Google Developers, *Google Play Protect Overview and Potentially Harmful Application Defenses* (verified on 24 November 2026).
10. `[REF-10]` NIST Computer Security Resource Center, *SP 800-124 Rev. 2: Guidelines for Managing the Security of Mobile Devices in the Enterprise* (verified on 24 November 2026).

BRANDEFENSE CAPABILITIES RELATED TO THIS RESEARCH

Cyber Threat Intelligence

Track the actors, infrastructure and campaigns behind threats like these.

Threat Actor Landscape

Profiles of the groups that run this kind of infrastructure.

Threat Search

Pivot on an indicator across the Brandefense dataset.

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_pandav7_panel_and_android_rat_artifacts.yar** 75 lines

```
/*
   Odin by Brandefense - Monograph 59 (PandaV7 Panels & Mobile RAT Clusters) YARA Suite
   4 filesize-bounded structural rules covering cached PandaV7 web panel HTML, sideloaded Android
   AccessibilityService/overlay abuse, DeviceAdmin boot persistence, and non-standard port C2 config
s.
*/

rule ODIN_PandaV7_Web_Management_Panel_HTML
{
    meta:
        author = "Odin by Brandefense"
        monograph = "59"
        description = "Detects cached or captured PandaV7 web management panel HTML and login bundle
markers"
        date = "2026-11-24"
    strings:
        $t1 = "<title>PandaV7</title>" ascii
        $p1 = "/api/" ascii
        $p2 = "password" ascii nocase
        $p3 = "token" ascii nocase
    condition:
        filesize < 2MB and $t1 and 2 of ($p*)
}

rule ODIN_Android_APK_Accessibility_and_Overlay_Abuse
{
    meta:
        author = "Odin by Brandefense"
        monograph = "59"
        description = "Detects Android manifest structures combining AccessibilityService binding, s
creen overlays, and SMS or install permissions"
        date = "2026-11-24"
    strings:
        $a1 = "android.permission.BIND_ACCESSIBILITY_SERVICE" ascii wide
        $o1 = "android.permission.SYSTEM_ALERT_WINDOW" ascii wide
        $s1 = "android.permission.RECEIVE_SMS" ascii wide
        $s2 = "android.permission.READ_SMS" ascii wide
        $s3 = "android.permission.REQUEST_INSTALL_PACKAGES" ascii wide
    condition:
        filesize < 50MB and $a1 and $o1 and 1 of ($s*)
}

rule ODIN_Android_RAT_DeviceAdmin_and_Boot_Persistence
{
    meta:
        author = "Odin by Brandefense"
```

```
        monograph = "59"
        description = "Detects Android manifest or DEX artifacts pairing DeviceAdminReceiver privile
ges with boot and foreground persistence"
        date = "2026-11-24"
    strings:
        $d1 = "android.permission.BIND_DEVICE_ADMIN" ascii wide
        $d2 = "android.app.action.DEVICE_ADMIN_ENABLED" ascii wide
        $b1 = "android.intent.action.BOOT_COMPLETED" ascii wide
        $f1 = "android.permission.FOREGROUND_SERVICE" ascii wide
    condition:
        filesize < 50MB and $d1 and $d2 and $b1 and $f1
}

rule ODIN_Android_RAT_NonStandard_Port_C2_Config
{
    meta:
        author = "Odin by Brandefense"
        monograph = "59"
        description = "Detects extracted mobile RAT DEX or configuration files pairing Android HTTP
clients with TCP 3000/3002 endpoints and capture commands"
        date = "2026-11-24"
    strings:
        $rt1 = "okhttp3" ascii
        $rt2 = "Dalvik" ascii
        $pt1 = ":3000/" ascii
        $pt2 = ":3002/" ascii
        $cap1 = "accessibility" ascii nocase
        $cap2 = "keylog" ascii nocase
        $cap3 = "screencap" ascii nocase
        $cap4 = "sms_intercept" ascii nocase
    condition:
        filesize < 10MB and ($rt1 or $rt2) and 1 of ($pt*) and 2 of ($cap*)
}
```

Suricata `odin_pandav7_panels_and_mobile_rat_hunt.rules` 11 lines

```
# Odin by Brandefense - Monograph 59 (PandaV7 Panels & Mobile RAT Clusters) Suricata 7.x Ruleset
# Static syntax checked against Suricata 7.x HTTP buffer rules and Odin Suricata linter (0 problem
s).

alert http $EXTERNAL_NET [3000,3002] -> $HOME_NET any (msg:"ODIN-R59 PandaV7 Web Panel Title on Non-
Standard Ports 3000 or 3002"; flow:established,to_client; http.stat_code; content:"200"; bsize:3; ht
tp.response_body; content:"<title>PandaV7</title>"; fast_pattern; classtype:trojan-activity; sid:955
9001; rev:1;)
alert http $EXTERNAL_NET [80,443,8080,8443] -> $HOME_NET any (msg:"ODIN-R59 PandaV7 Web Panel Title
on Standard or Alt Web Ports"; flow:established,to_client; http.stat_code; content:"200"; bsize:3; h
ttp.response_body; content:"<title>PandaV7</title>"; fast_pattern; classtype:trojan-activity; sid:95
59002; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET [3000,3002] (msg:"ODIN-R59 Outbound Android APK Fetch over
Non-Standard Ports 3000 or 3002"; flow:established,to_server; http.method; content:"GET"; bsize:3; h
ttp.uri; content:".apk"; nocase; endswith; fast_pattern; classtype:trojan-activity; sid:9559003; re
v:1;)
alert http $EXTERNAL_NET [3000,3002,8080] -> $HOME_NET any (msg:"ODIN-R59 Inbound Android APK Packag
```

```
e Delivery from Non-Standard Port"; flow:established,to_client; http.content_type; content:"applicat
ion/vnd.android.package-archive"; nocase; fast_pattern; classtype:trojan-activity; sid:9559004; rev:
1;)
alert http $HOME_NET any -> $EXTERNAL_NET [3000,3002,8080] (msg:"ODIN-R59 Outbound Android Dalvik Ru
ntime Request to Non-Standard Port"; flow:established,to_server; http.user_agent; content:"Dalvik/";
startswith; fast_pattern; classtype:command-and-control; sid:9559005; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET [3000,3002,8080] (msg:"ODIN-R59 Outbound Android OkHttp PO
ST Beacon to Non-Standard Port"; flow:established,to_server; http.method; content:"POST"; bsize:4; h
ttp.user_agent; content:"okhttp/"; startswith; fast_pattern; classtype:command-and-control; sid:9559
006; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R59 Outbound Android APK Fetch Using Bare I
Pv4 Host Header"; flow:established,to_server; http.uri; content:".apk"; nocase; endswith; fast_patte
rn; http.host; pcre:"/^\d{1,3}(?:\.\d{1,3}){3}(?::\d+)?$/"; classtype:trojan-activity; sid:9559007;
rev:1;)
```

Show full rule

Sentinel KQL **sentinel_pandav7_nonstandard_ports_and_android_hunt.kql** 29 lines

```
// Odin by Brandefense - Monograph 59 (PandaV7 Panels & Mobile RAT Clusters)
// Hunts non-browser endpoint connections to external TCP 3000/3002, APK fetches, and ADB sideload/a
ccessibility commands.
let Lookback = 7d;
let ApprovedMobileDevHosts = dynamic(["mobile-ci-01.corp.example", "qa-appium-01.corp.example"]);
let NonBrowserClients = dynamic(["curl", "curl.exe", "wget", "python", "python3", "python.exe", "pow
ershell.exe", "pwsh", "pwsh.exe", "java", "java.exe", "adb", "adb.exe"]);
let NonStandardPortOrApkEgress =
    DeviceNetworkEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedMobileDevHosts))
    | where RemoteIPType == "Public"
    | where (
        (RemotePort in (3000, 3002) and InitiatingProcessFileName in~ (NonBrowserClients))
        or (RemotePort in (3000, 3002, 8080) and RemoteUrl endswith ".apk")
    )
    | project Timestamp, DeviceName, AccountName = InitiatingProcessAccountName, SignalType = "NonSt
andardPortOrApkEgress", Detail = strcat(InitiatingProcessFileName, " -> ", RemoteIP, ":", tostring(R
emotePort), " ", RemoteUrl);
let AndroidAdbSideloadOrAdminGrant =
    DeviceProcessEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedMobileDevHosts))
    | where FileName in~ ("adb", "adb.exe")
    | where (
        (ProcessCommandLine has "install" and ProcessCommandLine has ".apk")
        or ProcessCommandLine has_any ("enabled_accessibility_services", "dpm set-active-admin", "BI
ND_ACCESSIBILITY_SERVICE")
    )
    | project Timestamp, DeviceName, AccountName, SignalType = "AndroidAdbSideloadOrAdminGrant", Det
ail = ProcessCommandLine;
union NonStandardPortOrApkEgress, AndroidAdbSideloadOrAdminGrant
| summarize FirstSeen = min(Timestamp), LastSeen = max(Timestamp), EventCount = count(), Signals = m
```

```
ake_set(SignalType, 6), SampleDetails = make_set(Detail, 5) by DeviceName, AccountName
| order by LastSeen desc
```

Sigma `sigma_pandav7_nonstandard_ports_and_adb_sideload.yml` 92 lines

```
title: Android ADB Sideloading or Programmatic Accessibility Grant
id: 9b42c1e8-59a1-4d72-8c10-59f10a38b901
status: experimental
description: Detects workstation or bridge invocations of Android Debug Bridge (adb) installing loca
l APK packages or enabling accessibility and device-admin services via shell settings.
author: Odin by Brandefense
date: 2026-11-24
logsource:
  category: process_creation
  product: windows
detection:
  selection_adb:
    Image|endswith: '\adb.exe'
  selection_action:
    CommandLine|contains:
      - '.apk'
      - 'enabled_accessibility_services'
      - 'dpm set-active-admin'
  filter_qa_hosts:
    ComputerName:
      - 'qa-appium-01.corp.example'
  condition: selection_adb and selection_action and not filter_qa_hosts
falsepositives:
  - Approved mobile QA automation runners running scheduled instrumentation suites
level: high
tags:
  - attack.privilege-escalation
  - attack.t1453
  - attack.t1626.001
---
title: Non-Browser CLI Polling or APK Fetch over TCP 3000 and 3002
id: 9b42c1e8-59a1-4d72-8c10-59f10a38b902
status: experimental
description: Detects command-line HTTP utilities connecting to non-standard external ports 3000 or 3
002 associated with unverified PandaV7 web management panels and app staging endpoints.
author: Odin by Brandefense
date: 2026-11-24
logsource:
  category: process_creation
  product: linux
detection:
  selection_cli:
    Image|endswith:
      - '/curl'
      - '/wget'
      - '/python'
      - '/python3'
  selection_ports:
```

```
    CommandLine|contains:
      - ':3000/'
      - ':3002/'
  filter_ci_hosts:
    ComputerName:
      - 'mobile-ci-01.corp.example'
  condition: selection_cli and selection_ports and not filter_ci_hosts
falsepositives:
  - Internal front-end build runners testing local Node.js services on designated CI hosts
level: medium
tags:
  - attack.command-and-control
  - attack.t1571
  - attack.t1071.001
---
title: Proxy Android Runtime Traffic or APK Download on Non-Standard Ports
id: 9b42c1e8-59a1-4d72-8c10-59f10a38b903
status: experimental
description: Detects web proxy sessions to non-standard ports 3000 or 3002 initiated by Android Dalv
ik or OkHttp clients or requesting APK files.
author: Odin by Brandefense
date: 2026-11-24
logsource:
  category: proxy
detection:
  selection_port:
    r-port:
      - 3000
      - 3002
  selection_mobile_ua:
    c-useragent|startswith:
      - 'Dalvik/'
      - 'okhttp/'
  selection_apk_uri:
    c-uri|endswith: '.apk'
  filter_mdm_gateway:
    ComputerName:
      - 'mdm-gateway-01.corp.example'
  condition: selection_port and (selection_mobile_ua or selection_apk_uri) and not filter_mdm_gatewa
y
falsepositives:
  - Approved enterprise mobile app staging servers hosted on internal developer gateways
level: high
tags:
  - attack.command-and-control
  - attack.t1571
  - attack.t1437.001
```