FULL REPORT · AI AGENT EXPOSURE · MONOGRAPH 69 / 68 · 19 MIN READ

AI Sandbox Micro-VM Workspaces, Custom Initramfs Images, and Egress Controls

How a misconfigured security-research workspace exposes three AI micro-VM sandbox versions, custom BusyBox initramfs images, OOB test scripts, and 42 secret records

BY
Odin by Brandefense

PUBLISHED
19 November 2026

READING TIME
19 min read

EDITION
Version 1.1 · TLP:CLEAR

SCOPE
Prepared November 2026

1. Executive Summary

IN SHORT

From 13 to 20 November 2026, Odin by Brandefense analyzed an unauthenticated HTTP directory service on a misconfigured United States research VPS (`Host R-01`). On 20 November 2026, the open directory reported 2,993 files and exposed 1,278 deduplicated AI sandbox, initramfs, binary, and key entries alongside 42 secret records. Shut down open HTTP listeners, jail micro-VMs without host mounts, and isolate ACME private keys.

Platforms that run model-generated code or headless browsers depend on virtualized micro-VMs and minimal Linux ramdisks to protect host servers. Strong guest isolation can still fail when developers or researchers leave working folders open over plain HTTP. Starting an unauthenticated directory server on a cloud box turns sandbox templates, custom boot archives, and credentials in files into public downloads.

From 13 to 20 November 2026, Odin by Brandefense examined an unauthenticated HTTP directory service on a United States commercial VPS (`Host R-01`). On 20 November 2026, that open directory reported 2,993 files and 1,340 directories across its tree. Deduplicated indexing across 13 to 20 November 2026 captured 1,278 unique workspace entries totaling 969,360,808 sized bytes (**969.36 MB**).

We classify `Host R-01` consistently as a misconfigured security-research and AI sandbox-testing workspace rather than an adversary operator. All inspection was passive and static, with zero keys or credentials tested. We withhold the server IP, TCP port, all folder, file, vendor, and domain names, all 42 secrets, and all 683 SHA-256 digests.

1. **Three AI micro-VM framework builds make up 72.6 percent of entries.**
   `Zone 1` holds 928 deduplicated entries (**690** sized files totaling **298,050,953** bytes and **238** unsized entries). Those folders hold three successive builds of an AI agent micro-VM framework across eight recurring isolation scenarios, plus hypervisor metrics and local database credentials.

2. **Three custom BusyBox initramfs variants test guest boot boundaries.**
   `Zone 4` holds 23 entries (**21** sized files totaling **50,055,564** bytes and **2** unsized entries). It pairs minimal BusyBox root filesystems with bound, self-contained, and raw `cpio.gz` ramdisk images built to compare Linux guest-to-host boot isolation.

3 **Desktop IPC binaries, web bundles, and SSRF scripts confirm research use.**
`Zones 2, 3, and 6` hold 310 entries totaling **621,027,554** sized bytes. Unpacked desktop installers in `Zone 2` represent **58.15%** of total workspace bytes (**563,655,605** bytes), sitting beside captured JavaScript web bundles and out-of-band or SSRF test scripts.

4 **Co-located configs and ACME TLS folders expose 42 secret records.**
Across all **1,278** entries sit **26** environment-template and configuration entries and **42** detected secret records. `Zone 5` alone leaves 17 ACME key and certificate state files (**226,737** bytes) inside the HTTP-served tree.

Three Decisions for Security Leaders

1. **Shut down ad-hoc HTTP file servers and isolate ACME keys.** Sweep cloud VPCs for open Python or Node directory listings and bind local dev servers to `127.0.0.1`. Store ACME account and domain private keys in **0700** root-owned `/etc` directories outside user workspaces.
2. **Run AI code interpreters in jailed micro-VMs without host mounts.** Confine untrusted agent code inside jailed KVM micro-VMs or user-space application kernels. Pair self-contained `initramfs` bootstrap with a separately enforced read-only guest root and block host-directory bind mounts into guest VMs.
3. **Drop metadata and private routes before sandbox NAT forwarding.** Block guest VM traffic to `169.254.169.254` and RFC1918 ranges on host tap interfaces. Enforce cloud `IMDSv2` with a hop limit of **1** and watch outbound callback polling.

The Study in Numbers

Number	What it represents
2,993 / 1,340	Files (2,993) and directories (1,340) reported by the live HTTP listing on `Host R-01` on `20 November 2026`
1,278	Deduplicated workspace entries indexed across `13-20 November 2026` (937 sized files + 341 unsized entries)
969,360,808	Total sized bytes (969.36 MB) across the 937 sized files (683 unique SHA-256 digests withheld)
928 (72.6%)	Entries in `Zone 1` across 3 AI micro-VM framework builds and 8 recurring isolation scenarios (298.05 MB)
23 + 17	`Zone 4` `initramfs` entries (3 variants, 50.06 MB) plus `Zone 5` ACME key and certificate state files (226.74 KB)
42 / 26	Detected secret records (42, zero tested, all withheld) and 26 environment or configuration entries
0	Published IPv4 addresses, TCP ports, filenames, vendor/domain names, or SHA-256 hashes (10 self-audit markers in text)

2. Six Functional Zones Across the 1,278-Entry Workspace

Engineers and security researchers often use Python's HTTP server to share files from a cloud VM. By default, it binds to all interfaces and serves the working directory, including dot-folders. Cloud teams can run external attack surface management scans to catch unauthenticated HTTP directory listings before outside scanners index them.

Pairing perimeter discovery with cyber threat intelligence helps analysts separate misconfigured developer hosts from threat-actor staging boxes. On `20 November 2026`, `Host R-01` reported **2,993** files and **1,340** directories. Static indexing across `13-20 November 2026` captured **1,278** deduplicated entries: **937** sized files (**969,360,808** bytes) and **341** unsized entries.

Across those **937** sized files sit **683** unique SHA-256 digests, all of which are withheld. The other **254** sized instances (`937 - 683 = 254`) reflect repeated templates and shared helpers across the three `Zone 1` builds. Figure 1 maps the six functional zones on `Host R-01`.

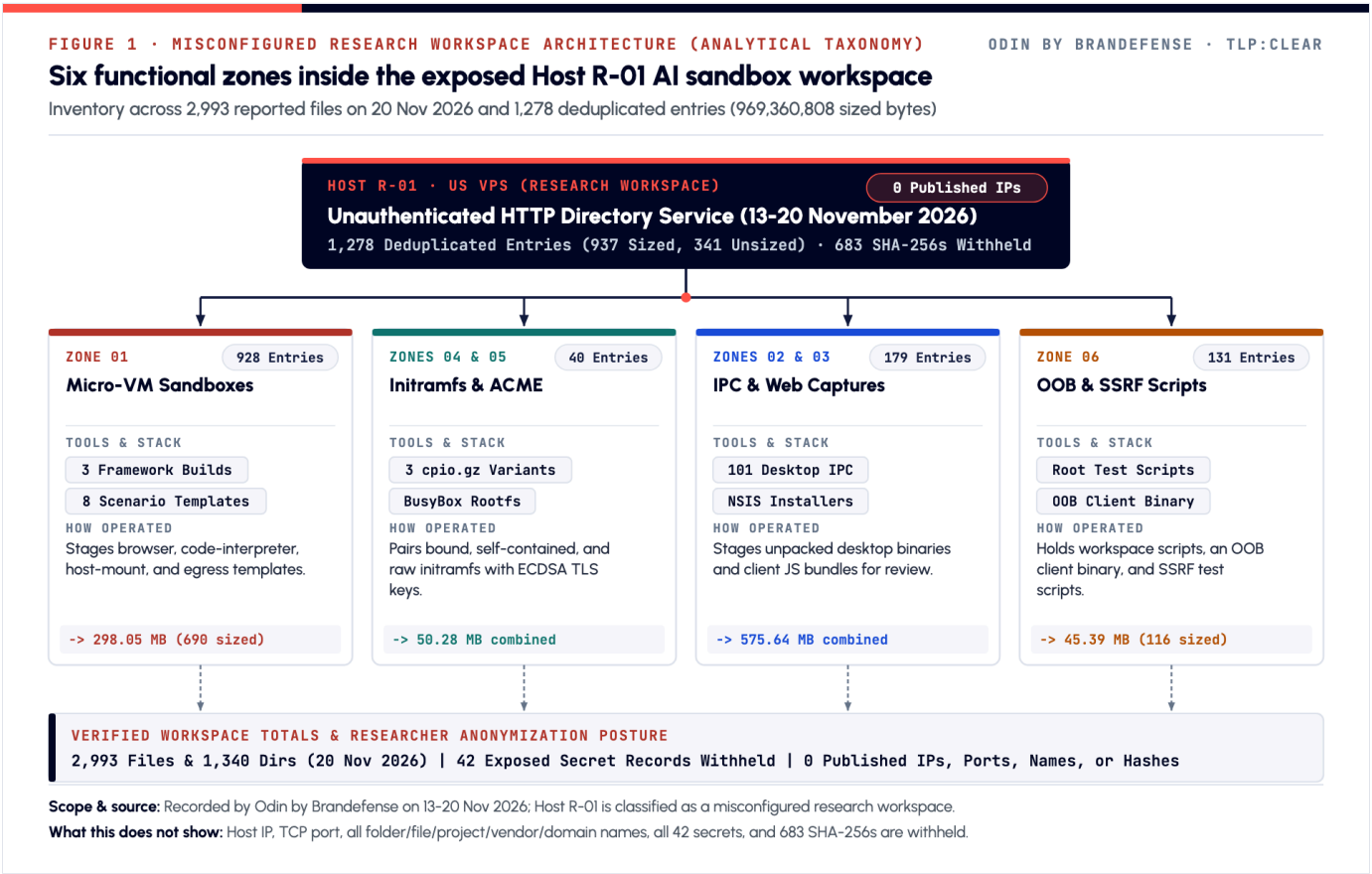


Figure 1: Six functional zones inside the exposed Host R-01 AI sandbox workspace

Six-Zone Functional Partition (`n = 1,278`)

We group the workspace into six functional zones and withhold its folder and project names. Table 1 reconciles all **1,278** entries, **937** sized files, **341** unsized entries, and **969,360,808** bytes (`928 + 131 + 101 + 78 + 23 + 17 = 1,278`).

Functional zone (`Host R-01`)	Entries	Share (%)	Sized / unsized	Sized bytes	Byte share (%)	Anonymized architectural role
`Zone 1` : AI Micro-VM Sandbox Trees	928	72.6%	690 / 238	298,050,953	30.75%	Three AI micro-VM builds, eight scenario templates, VMM metrics, and local DB configs
`Zone 6` : Root, OOB & SSRF Scripts	131	10.3%	116 / 15	45,391,964	4.68%	Root workspace scripts, compiled OOB client binary, and SSRF test scripts
`Zone 2` : Desktop Client & IPC Binaries	101	7.9%	24 / 77	563,655,605	58.15%	Unpacked desktop client binaries and NSIS payloads for local IPC review
`Zone 3` : Frontend Web Bundle Captures	78	6.1%	69 / 9	11,979,985	1.24%	Captured first-load JavaScript web bundles for client-side endpoint review

Functional zone (`Host R-01`)	Entries	Share (%)	Sized / unsized	Sized bytes	Byte share (%)	Anonymized architectural role
`Zone 4`: Custom Initramfs & BusyBox	23	1.8%	21 / 2	50,055,564	5.16%	Bound, self-contained, and raw `cpio.gz` ramdisks with BusyBox rootfs trees
`Zone 5`: ACME TLS Account & Keys	17	1.3%	17 / 0	226,737	0.02%	Automated ACME CA account keys, domain ECDSA keys, and cert state files
Total (`Host R-01`)	**1,278**	**100.0%**	**937 / 341**	**969,360,808**	**100.00%**	**2,993 files and 1,340 dirs on `20 Nov 2026`; 683 unique SHA-256s withheld**

Entry count and byte volume pull in opposite directions across `Host R-01`, as shown in Figure 5. `Zone 1` holds **928** entries (**72.6%** of items) across small sandbox scripts and configs totaling **298.05 MB** (**30.75%** of bytes). By contrast, `Zone 2` holds **101** entries (**24** sized and **77** unsized) yet accounts for **563,655,605** bytes (**58.15%** of volume). Meanwhile, `Zone 5` holds **17** ACME key and certificate state files (**226,737** bytes, **0.02%**) exposed over HTTP.

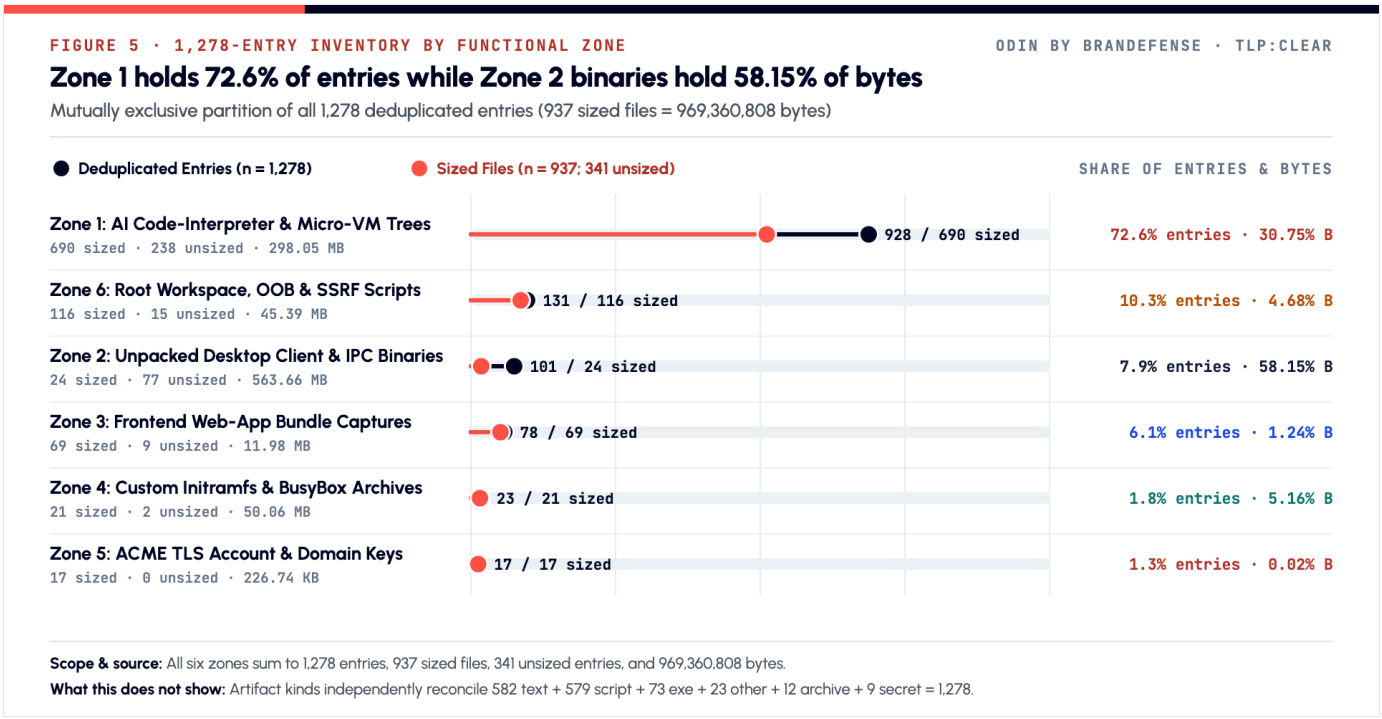


Figure 5: Zone 1 holds 72.6% of entries while Zone 2 binaries hold 58.15% of bytes

Artifact-Class Reconciliation (6 Kinds) and Secret Boundaries

Sorting the same **1,278** entries by file type confirms exact byte parity (**969,360,808** bytes across `582 + 579 + 73 + 23 + 12 + 9 = 1,278`).

Artifact class	Entries	Share (%)	Sized / unsized	Sized bytes	Byte share (%)	Structural contents
`text`	582	45.54%	377 / 205	6,534,974	0.67%	Scenario manifests, VMM metric logs, ACME state configs, and notes

Artifact class	Entries	Share (%)	Sized / unsized	Sized bytes	Byte share (%)	Structural contents
`script`	579	45.31%	**525 / 54**	16,106,168	1.66%	Micro-VM controller code, captured JS bundles, and SSRF or route scripts
`exe`	73	5.71%	**14 / 59**	639,918,578	66.01%	Unpacked desktop IPC binaries, NSIS payloads, BusyBox, and OOB binary
`other`	23	1.80%	**5 / 18**	10,829,540	1.12%	Desktop installer data segments and guest filesystem support blobs
`archive`	12	0.94%	**7 / 5**	295,949,241	30.53%	Compressed micro-VM bundles and `cpio.gz` `initramfs` root archives
`secret`	9	0.70%	**9 / 0**	22,307	0.00%	Dedicated `.key` or credential files (subset of **42** secret records)
Total	**1,278**	**100.00 %**	**937 / 341**	**969,360,808**	**100.00%**	**Exact match with Table 1 (937 sized + 341 unsized = 1,278)**

Together, `text` (**582**) and `script` (**579**) make up **1,161** of **1,278** entries (**90.85%**), but only **22,641,142** bytes (**2.34%**). Meanwhile, `exe` (**73** entries) and `archive` (**12** entries) hold **935,867,819** bytes (**96.54%** of bytes) across just **85** items (**6.65%**).

Four secret-related counts measure nested scopes without contradiction (`[REF-07]`). Nine files (**22,307** bytes) carry the `secret` file kind based on extension, while `Zone 5` holds **17** ACME files (**226,737** bytes) pairing `.key` files with certificate state files. Across the full workspace sit **26** config entries and **42 detected secret records**, spanning `Zone 5` ACME keys and `Zone 1` database and environment configs.

3. AI Code-Interpreter Micro-VM Templates and Initramfs Isolation

AI platforms that run model-generated Python, Node.js, shell, or browser tasks cannot rely on in-process language sandboxes (`[REF-01]` , `[REF-02]`). Language-level sandboxes share the host runtime and kernel, so a single object-handling flaw exposes the underlying server (`[REF-09]`).

For architectural context (`[REF-04]`), Node.js `vm2` versions before `3.9.15` carried `CVE-2023-29017` (fixed in `3.9.15` on `6 April 2023`). Under `CVE-2023-29017` , `vm2` mishandled host objects passed to `Error.prepareStackTrace` during unhandled async errors, letting untrusted code escape the sandbox and run host commands (`[REF-04]`).

We cite `CVE-2023-29017` strictly as industry context rather than a package exploited on `Host R-01` . Escapes of that class pushed AI teams toward KVM micro-VMs like **Firecracker** (`[REF-01]`) and application kernels like **gVisor** (`[REF-02]`).

Hardware virtualization still fails when host mounts, ramdisks, or network routes are misconfigured (`[REF-06]`). Figure 3 shows an analytical model of the guest boot, mount, and egress boundaries tested across `Zones 1, 4, and 6` .

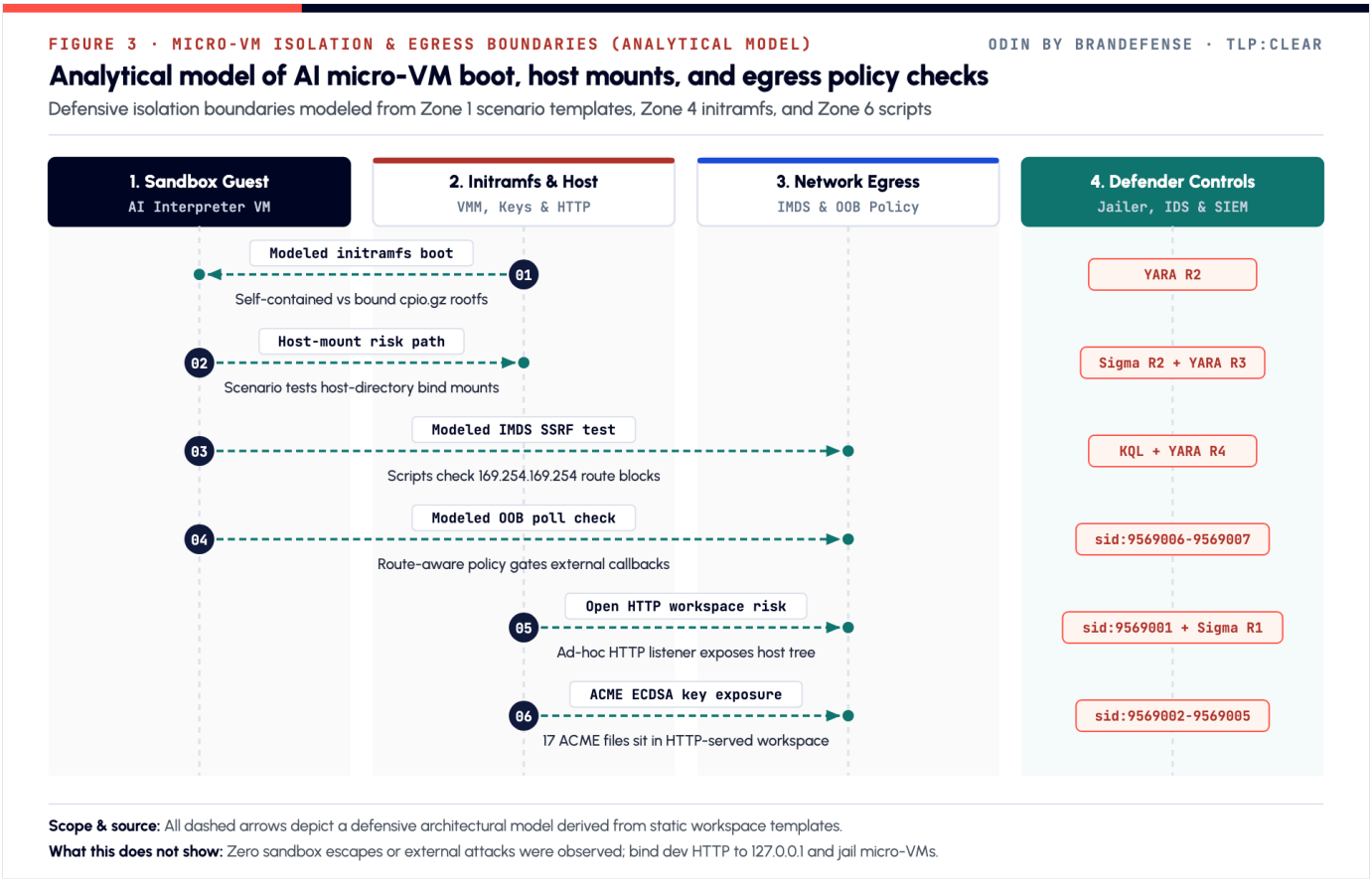


Figure 3: Analytical model of AI micro-VM boot, host mounts, and egress policy checks

Eight Scenario Templates Across Three Framework Builds (`Zone 1`)

`Zone 1` (**928** entries, **298,050,953** bytes) stores three successive builds of an AI agent micro-VM framework alongside cloud-hypervisor metric captures and local database credentials. Across all three builds, eight recurring scenario templates test distinct sandbox boundaries:

Component or template	Zone & multiplicity	Isolation boundary under review	Failure mode if misconfigured	Primary defensive control
Browser sandbox	`Zone 1` (3 builds)	Headless browser rendering untrusted pages in a guest VM	Unjailed browser escape reaches host user files (`[REF-01]`)	Confine browser VMs with `jailer` , `chroot` , and `seccomp`
Code-interpreter quickstart	`Zone 1` (3 builds)	Single-turn execution of LLM-generated Python or shell code	Reusing warm VMs across users leaks prior `/tmp` or RAM data	Boot fresh ephemeral VMs per session and wipe memory on exit
Agent code-interpreter	`Zone 1` (3 builds)	Multi-step tool loop reading and writing task artifacts	Uncapped guest CPU or disk starves host hypervisor threads	Enforce cgroup v2 CPU, RAM, and block-I/O limits (`[REF-01]`)
Host-directory mount	`Zone 1` (3 builds)	Shared host-to-guest folder passthrough (`virtio-fs` or `9p`)	Mounting `/root` , `/.ssh` , `/.acme.sh` , or `docker.sock` allows host escape (`T1611` , `[REF-05]` , `[REF-06]`)	Ban host bind mounts into untrusted VMs; pass inputs over `vsock`

Component or template	Zone & multiplicity	Isolation boundary under review	Failure mode if misconfigured	Primary defensive control
Multi-agent workflow	`Zone 1` (3 builds)	Parallel sandboxes exchanging intermediate agent outputs	Shared Linux bridges allow east-west ARP or packet spoofing	Isolate each micro-VM on a dedicated `/30` tap interface
Reinforcement-learning loop	`Zone 1` (3 builds)	High-rate rollout workers sending reward metrics to host	Exposed host metric ports accept forged guest inputs	Bind hypervisor metric sockets to host-only UNIX paths
Network-policy enforcement	`Zone 1` (3 builds)	L3/L4 firewall rules on outbound guest sandbox traffic	Default-allow NAT lets untrusted code scan external hosts	Apply default-deny egress rules on every guest tap device
Route-aware egress	`Zone 1` (3 builds)	Prefix routing checks before host NAT or proxy forwarding	Missing link-local drops expose `169.254.169.254` IAM tokens (`[REF-02]`)	Drop `169.254.0.0/16` and RFC1918 destinations before NAT
Bound `initramfs` (`cpio.gz`)	`Zone 4` (1 of 3)	Guest ramdisk mounting host-supplied shares at boot	Writable host mounts risk symlink traversal during `/init`	Mount external shares `MS_RDONLY` , `MS_NOSUID` , and `MS_NODEV`
Self-contained `initramfs`	`Zone 4` (1 of 3)	Standalone BusyBox RAM `rootfs` with zero host disk mounts	Full BusyBox builds leave `wget` or `nc` inside guest RAM (`[REF-03]`)	Strip transfer applets, enforce a separate read-only guest root, and discard VMs per session
Raw `initramfs` (`cpio.gz`)	`Zone 4` (1 of 3)	Unhardened baseline boot archive for latency comparison	Accidental CI deployment ships debug shells into production	Scan unpacked 070701 `cpio` streams in CI via YARA Rule 2

Two scenarios in Table 3 pose the highest real-world risk. First, the **host-directory mount** scenario mirrors Kubernetes `hostPath` risks restricted under `Pod Security Standards` (`[REF-05]`). Passing a writable host folder into a KVM micro-VM lets untrusted code edit host files or read co-located keys without exploiting a hypervisor bug (`T1611` , `[REF-06]`).

Second, **route-aware egress** controls decide whether a guest VM can pivot into cloud control planes. Missing `nftables` drops for `169.254.169.254` or `10.0.0.0/8` before NAT create direct SSRF risk. Untrusted guest code can then query cloud metadata roles or reach local databases on the host.

Bound, Self-Contained, and Raw `initramfs` Archives (`Zone 4`)

During Linux boot (`[REF-03]`), the kernel unpacks any `initramfs` (`cpio.gz`) archive into an in-memory `rootfs` instance and runs `/init` . In micro-VM designs, engineers either run the guest userland directly inside that RAM `rootfs` or mount an external block or shared filesystem (`[REF-01]` , `[REF-03]`).

`Zone 4` (**23** entries, **50,055,564** bytes) stages three `cpio.gz` BusyBox variants to test that trade-off:

- **Self-contained `initramfs` .** Packs BusyBox, `/dev/console` , and `/init` into one RAM image with zero host mounts. Ephemeral AI code interpreters gain clean teardown and strong isolation from this model.

- **Bound `initramfs`.** Uses early `/init` mounts to attach host-supplied runtime directories. Any bound share exposed to untrusted guest code must enforce kernel read-only flags at the hypervisor boundary.
- **Raw `initramfs`.** Serves as an unstripped reference archive for boot speed and memory comparisons. Leaving raw test images beside production builds risks accidental deployment if CI pipelines do not verify image manifests.

4. Co-Hosted Research Artifacts, OOB Harnesses, and ACME Key Sprawl

Examining `Zones 2, 3, 5, and 6` explains why `Host R-01` is a misconfigured researcher and developer VPS rather than an attacker staging server. Application auditing files, sandbox test scripts, and personal ACME TLS keys all sat under one parent workspace when an open HTTP listener exposed them (`[REF-07]`, `[REF-10]`). Figure 4 shows the structural layout of `Host R-01`.

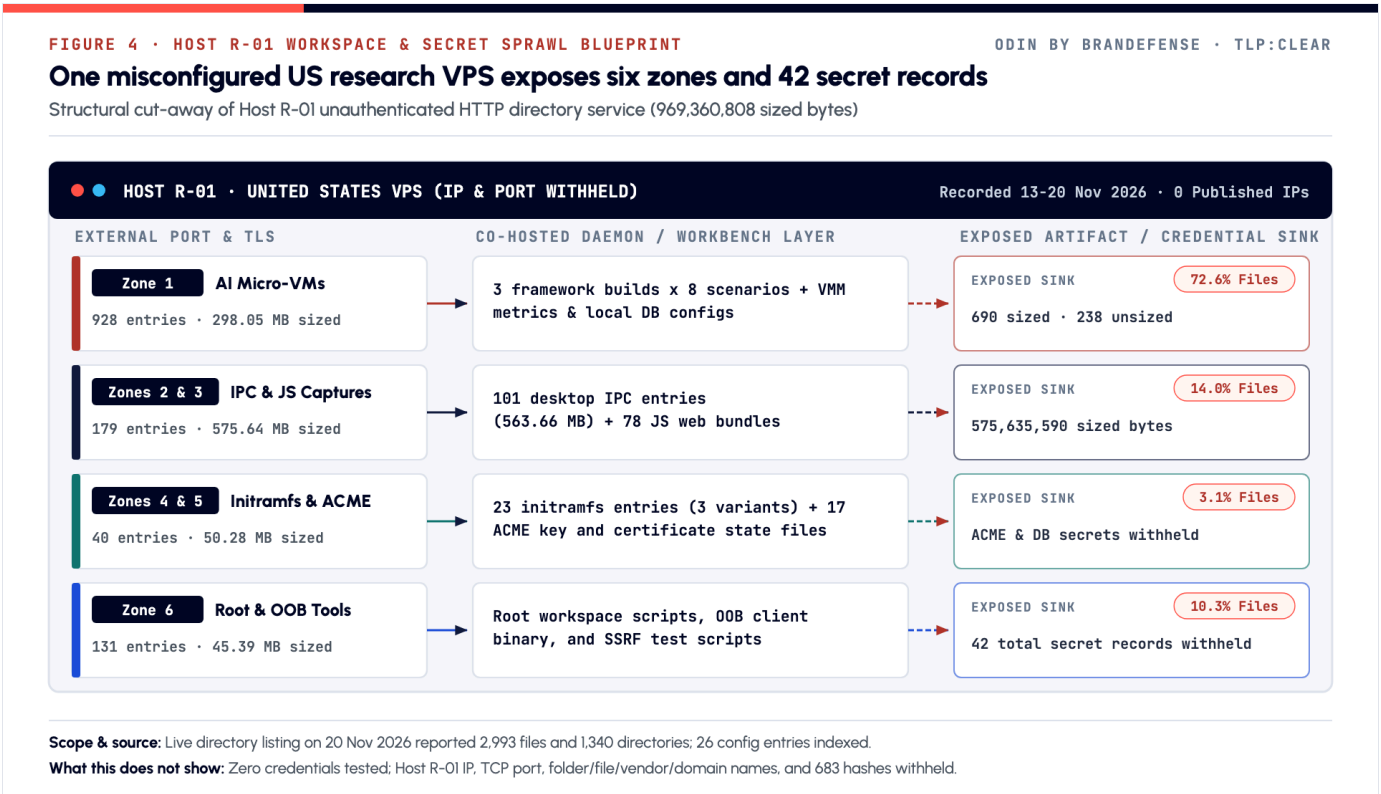


Figure 4: One misconfigured US research VPS exposes six zones and 42 secret records

Desktop IPC Binaries, Web Bundles, and SSRF Scripts (`Zones 2, 3, and 6`)

Across `Zones 2, 3, and 6` sit **310** entries (**209** sized files = **621,027,554** bytes and **101** unsized entries):

- **`Zone 2` (101 entries, 563,655,605 bytes).** Holds **24** sized files and **77** unsized entries from unpacked desktop installers and `NSIS` packages (vendors withheld) staged for local `IPC` and URI-scheme review.
- **`Zone 3` (78 entries, 11,979,985 bytes).** Holds **69** sized files and **9** unsized entries of first-load web JavaScript bundles (domains withheld) saved for static route and token-sink inspection.
- **`Zone 6` (131 entries, 45,391,964 bytes).** Holds **116** sized files and **15** unsized entries pairing workspace scripts with a compiled `OOB` client binary and SSRF scripts testing callback and `169.254.169.254` paths.

Plain-HTTP ACME ECDSA Key Sprawl (`Zone 5` and 42 Secret Records)

`Zone 5` (**17** sized files, **226,737** bytes, **0** unsized) shows how fast an open HTTP listener turns into a cryptographic leak (`T1552.001` , `[REF-07]`). Automated ACME clients such as `acme.sh` keep two key types inside `~/.acme.sh/` by default:

- **Domain ECDSA private keys.** Leaking a domain key lets outsiders impersonate that TLS service until the certificate is revoked and replaced.
- **ACME CA `account.key` files.** Rotating a leaked domain key alone is not enough. An unrevoked `account.key` can keep cached CA domain authorizations and issue or revoke certificates until deactivated.

Starting `python3 -m http.server` in a home or parent research folder serves hidden dot-directories like `.acme.sh/` with `200 OK` responses. Figure 2 links all five exposure surfaces on `Host R-01` to the defensive controls and rules in Chapters 7 and 8.

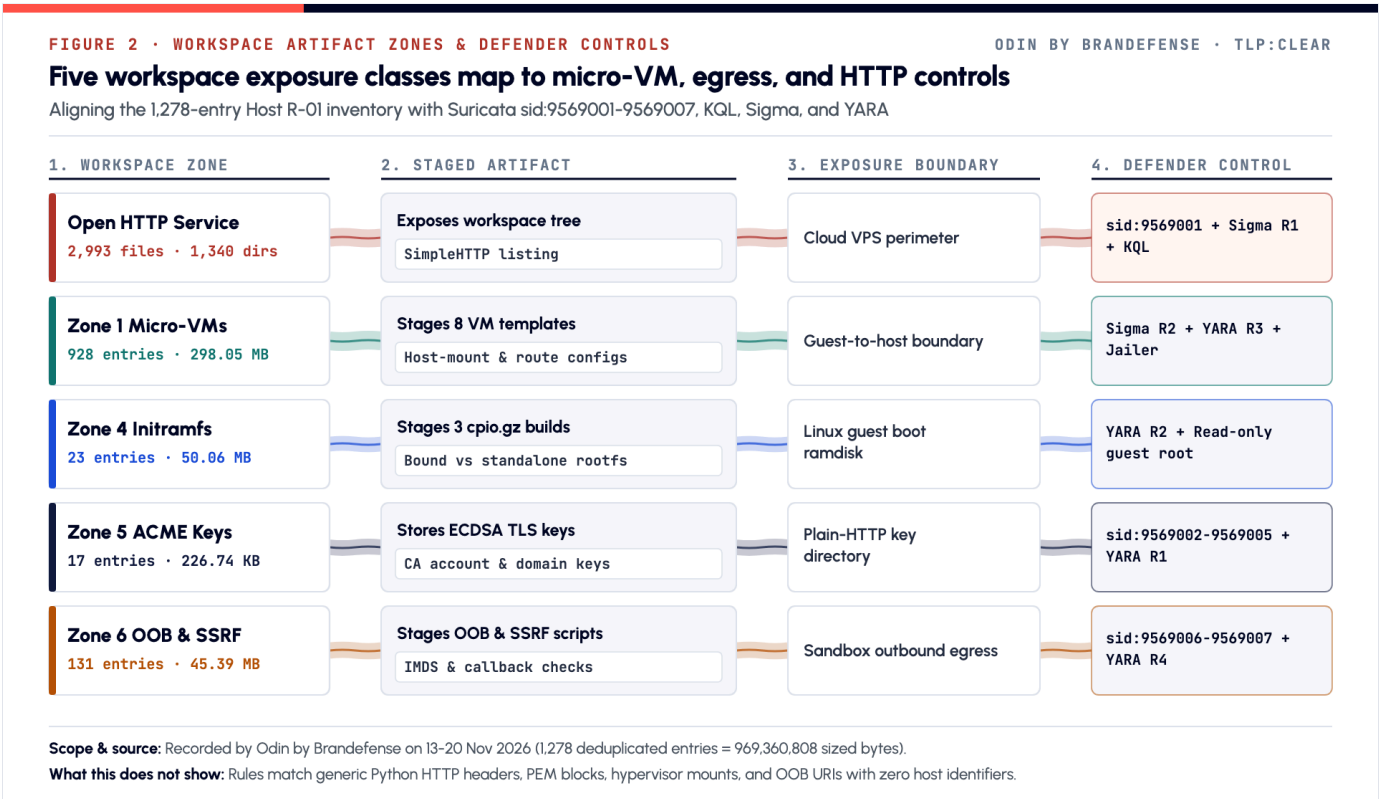


Figure 2: Five workspace exposure classes map to micro-VM, egress, and HTTP controls

5. Enterprise Exposure and Control Verification

Platform and cloud security teams running internal AI sandboxes or research VMs should verify five controls rather than assuming unverified root causes:

Exposure layer	Observed evidence on `Host R-01`	Control to verify	Operational risk
Open HTTP dev listeners	Live listing reported 2,993 files and 1,340 dirs on `20 Nov 2026` (1,278 dedup entries).	Verify whether VPC firewalls block unapproved ports and whether local dev servers bind to `127.0.0.1` (`[REF-10]`).	Internet scanners can copy sandbox code, audit files, and keys (`T1552.001`).

Exposure layer	Observed evidence on `Host R-01`	Control to verify	Operational risk
Micro-VM host bind mounts	`Zone 1` stages 3 builds of a host-directory mount scenario within 928 entries.	Verify whether micro-VMs run inside `jailer` cages (`[REF-01]`) and forbid `virtio-fs` , `9p` , or `hostPath` mounts (`[REF-05]`).	Guest code edits host files, reads host keys, or escapes to the node (`T1611` , `[REF-06]`).
Custom `initramfs` images	`Zone 4` stages 23 entries (50.06 MB) across bound, self-contained, and raw `cpio.gz` archives.	Verify whether production VMs use signed, self-contained `initramfs` bootstrap stripped of transfer tools with a separately enforced read-only guest root (`[REF-03]`), and discard guests after each session.	Bound or raw debug ramdisks leave writable mounts or BusyBox network tools in guest RAM.
Sandbox metadata & OOB egress	`Zone 1` route-aware egress templates + `Zone 6` OOB binary and SSRF scripts (131 entries).	Verify whether host `nftables` drop guest packets to `169.254.169.254` and RFC1918 ranges before NAT (`[REF-02]`).	Guest code steals cloud IAM credentials via SSRF or reaches local host databases.
ACME & DB secret storage	`Zone 5` (17 ACME files, 226.74 KB) + 26 config entries + 42 secret records.	Verify whether ACME keys sit in 0700 `/etc` folders outside web roots and whether DB secrets use vaults (`[REF-07]`).	One ad-hoc HTTP server leaks both domain ECDSA keys and CA `account.key` authority.

6. Alternative Hypotheses

Hypothesis	Evidence for	Evidence against	Assessment
Misconfigured security-research and AI sandbox workspace	Pairs 3 AI micro-VM framework builds (928 entries) and 3 `initramfs` builds (23 entries) with unpacked IPC clients, JS bundles, SSRF scripts, and personal ACME keys.	None; all six zones match sandbox engineering and app-security testing exposed by an accidental HTTP server.	**Supported.** Classify `Host R-01` consistently as a misconfigured research workspace; withhold all identifiers.
Adversary C2 or intrusion staging server	Holds an OOB interaction client binary, SSRF scripts (`Zone 6`), and web JS bundles (`Zone 3`).	Holds 0 C2 implants, 0 webshells, and 0 victim data dumps; 72.6% of files are defensive micro-VM isolation templates.	**Rejected.** Dual-use OOB and SSRF scripts beside sandbox isolation tests reflect security research (`[REF-08]`).
Custom `initramfs` and mount files show a live escape	`Zone 1` has host-mount templates and `Zone 4` has bound and raw `cpio.gz` archives.	All 8 scenarios repeat cleanly across 3 framework versions as structured templates; static listings show storage only.	**Unsupported.** Treat `Zones 1 and 4` strictly as staged engineering templates (`[REF-01]` , `[REF-03]`).
All 42 secret records and ACME keys are active	`Zone 5` stores 17 ACME files and configs hold 42 secret records across the workspace.	Odin by Brandefense tested 0 keys, made 0 login calls, and queried 0 external domains.	**Unverified.** Never call untested keys live; rotate both domain keys and ACME account keys on any exposed box.

7. What Defenders Should Do

AI platform engineers and cloud security teams can close these five gaps in order:

1. **Close ad-hoc HTTP listeners and rotate exposed ACME keys (`0-48 Hours`).** Scan research, dev, and GPU VPCs across all ports for `Directory listing for /` or `Index of /` responses (`[REF-10]` , `sid:9569001`). Bind local Python servers to `127.0.0.1` and audit `http.server` processes (Sigma Rule 1). If `.acme.sh` ever sat in an open folder, replace affected domain TLS keys and deactivate the ACME `account.key` (`[REF-07]`). Move ACME state to a **0700** root-only `/etc` folder outside user workspaces.
2. **Isolate AI code interpreters in jailed micro-VMs without host mounts (`0-72 Hours`).** Avoid in-process language sandboxes (`CVE-2023-29017` , `[REF-04]`) and privileged containers (`[REF-05]`) for untrusted LLM code. Launch Firecracker inside `jailer` (`chroot` , unprivileged UID, cgroup v2 quotas, `seccomp` , `[REF-01]`) or use gVisor `runsc` (`[REF-02]`). Ban writable `virtio-fs` , `9p` , or `hostPath` mounts into guest VMs (`T1611` , `[REF-06]` , Sigma Rule 2).
3. **Use self-contained `initramfs` bootstrap and a separately enforced read-only guest root (`Days 1-7`).** Because Linux extracts `initramfs` into a writable RAM `rootfs` , mount a read-only `squashfs` or block root for persistent guest state and discard each micro-VM after its session (`[REF-03]`). Strip BusyBox transfer applets (`wget` , `nc` , `tftp` , `mount`) from production guest images. Unpack `.cpio.gz` ramdisks in CI and scan **070701** `cpio` streams with YARA Rule 2 before signing.
4. **Drop metadata and RFC1918 routes before guest NAT (`Days 7-14`).** Use host `nftables` or eBPF rules on each micro-VM tap interface to drop packets to `169.254.0.0/16` , `127.0.0.0/8` , and RFC1918 ranges before NAT (`[REF-02]`). Require cloud `IMDSv2` with hop limit **1** on hypervisor hosts and route allowed internet calls through a TLS egress proxy watched by `sid:9569006` –**9569007**.
5. **Isolate research files from keys and schedule weekly audits (`Days 14-30`).** Keep unpacked installers (`Zone 2`), JS captures (`Zone 3`), and SSRF scripts (`Zone 6`) on isolated lab VMs with zero keys or database secrets. Run the Chapter 8 Sentinel KQL and YARA workspace checks each week.

8. Detection Rules

The full rules are in the Detection rules tab. Because all `Host R-01` identifiers and hashes are withheld, each rule file targets generic protocol headers, PEM blocks, hypervisor mount arguments, or `cpio` archive structures.

Validation scope: the Suricata rules passed the Odin Suricata linter (**0** problems). YAML and modifier checks confirmed all three Sigma rules, and structural checks verified the Sentinel KQL and YARA files. Native `suricata -T` , `Kusto.Language` , `pySigma` , and `yara` binaries were not installed locally, and rules were not replayed on live traffic. Test and tune them in staging before rollout.

Rule file	What it catches
`odin_sandbox_workspace_acme_and_oob_hunt.rules`	Suricata 7.x (**7** `alert http` rules, `sid:9569001` –**9569007**). Flags Python `SimpleHTTP` listings, `/.acme.sh/` and `account.key` probes, PEM key leaks, and OOB calls
`sentinel_sandbox_microvm_http_and_egress_hunt.kql`	Microsoft Sentinel KQL (**7**-day lookback). Unions process events with metadata-IP network events; OOB URI polling requires full-URL proxy logs.
`sigma_microvm_sandbox_http_and_acme_exposure.yml`	Portable Sigma (**3** Linux rules). Flags ad-hoc Python HTTP servers, sensitive VMM host-mount paths, and `/.acme.sh/` or `account.key` copies

Rule file	What it catches
`odin_sandbox_initramfs_acme_and_oob_artifacts.yar`	Structural YARA (4 bounded rules). Matches PEM private keys when scans are scoped to ACME state directories, unpacked 070701 BusyBox `cpio` ramdisks, micro-VM mount configs, and SSRF/OOB scripts

How the Suricata 7.x Signatures Work (`sid:9569001` –9569007)

All seven rules use `alert` and do not block packets inline; enforce blocks in WAFs, proxies, and firewalls. Because they inspect `http` buffers, `sid:9569001` –9569005 require cleartext HTTP or a TLS reverse proxy. Rules `sid:9569006` and `sid:9569007` require cleartext HTTP or a TLS-inspecting egress proxy.

SID	Direction & flow	What it matches	Defensive purpose
9569001	`$HOME_NET any -> $EXTERNAL_NET any` (`to_client`)	HTTP 200 with `Server: SimpleHTTP/` and `Directory listing for /`	Self-audit alert when an internal host exposes a Python HTTP directory
9569002	`$EXTERNAL_NET any -> $HOME_NET any` (`to_server`)	Inbound `GET` with `http.uri` containing `/.acme.sh/` (`nocase`)	Flags external requests probing ACME client state directories
9569003	`$EXTERNAL_NET any -> $HOME_NET any` (`to_server`)	Inbound `GET` with `http.uri` containing `account.key` (`nocase`)	Flags external requests targeting ACME CA account private keys
9569004	`$HOME_NET any -> $EXTERNAL_NET any` (`to_client`)	HTTP 200 body containing `-----BEGIN EC PRIVATE KEY-----`	Self-audit alert when an internal HTTP port leaks an ECDSA private key
9569005	`$HOME_NET any -> $EXTERNAL_NET any` (`to_client`)	HTTP 200 body containing `-----BEGIN PRIVATE KEY-----`	Self-audit alert when an internal HTTP port leaks a PKCS#8 private key
9569006	`$HOME_NET any -> $EXTERNAL_NET any` (`to_server`)	Outbound `POST` to exact `/register` (`bsize:9`) with `"correlation-id"` and `"public-key"`	Flags generic OOB correlation session registration from sandbox subnets
9569007	`$HOME_NET any -> $EXTERNAL_NET any` (`to_server`)	Outbound `GET` starting with `/poll?id=` followed by `&secret=`	Flags generic OOB callback polling requests from sandbox subnets

How the Sentinel KQL, Sigma, and YARA Rules Work

The Sentinel KQL hunt unions two branches over a 7-day lookback and excludes two sample FQDNs in `ApprovedSandboxBuildHosts` (`sandbox-ci-01.corp.example` and `acme-renew-01.corp.example`). Replace both placeholders

with your own build or certificate-renewal hosts before scheduling.

The first KQL branch checks `DeviceProcessEvents` for `python`, `python3`, or `python.exe` running `http.server` or `SimpleHTTPServer`. It also flags `firecracker`, `cloud-hypervisor`, or `qemu-system-x86_64` commands containing `/var/run/docker.sock`, `/etc/shadow`, `/root/`, `/.ssh/`, or `/.acme.sh/`. The second branch checks `DeviceNetworkEvents` for `python`, `python3`, `node`, `curl`, or `wget` connecting to exact `RemoteIP == "169.254.169.254"`. Because `DeviceNetworkEvents.RemoteUrl` often logs only an FQDN, hunt OOB `/poll?id=` and `/register` URIs separately in full-URL egress proxy logs.

Host or file rule	Engine	Trigger condition
`Ad-Hoc Python HTTP Directory Server Execution on Cloud or Sandbox Hosts (R1)`	Sigma (`linux`)	`/python`, `/python3`, `/python3.11`, or `/python3.12` with `http.server` or `SimpleHTTPServer` outside `sandbox-ci-01.corp.example` (`T1552.001`)
`Micro-VM or Hypervisor Launched With Sensitive Host Path Mounts (R2)`	Sigma (`linux`)	`/firecracker`, `/cloud-hypervisor`, or `/qemu-system-x86_64` with `/var/run/docker.sock`, `/etc/shadow`, `/root/`, `/.ssh/`, or `/.acme.sh/` (`T1611`)
`Unexpected Archiving or Copy of Automated ACME Private Key Directories (R3)`	Sigma (`linux`)	`/tar`, `/zip`, `/cp`, `/scp`, `/rsync`, or `/curl` referencing `/.acme.sh/` or `account.key` outside `acme-renew-01.corp.example` (`T1552.001`)
`ODIN_Unencrypted_ACME_ECDSA_or_PKCS8_Key (YARA R1)`	YARA (< 64KB)	`-----BEGIN EC PRIVATE KEY-----` or `-----BEGIN PRIVATE KEY-----` when scans are scoped to ACME state directories
`ODIN_Custom_Cpio_Newc_Initramfs_BusyBox_Archive (YARA R2)`	YARA (< 60MB)	Unpacked 070701 SVR4 `newc` `cpio` header at offset 0 with `bin/busybox`, `dev/console`, and `sbin/init` or `init`
`ODIN_MicroVM_Host_Bind_Mount_and_Egress_Config (YARA R3)`	YARA (< 1MB)	Two of `boot_source`, `vcpu_count`, `initramfs` paired with `host_path`, `virtio-fs`, `egress_policy`, or `169.254.169.254`
`ODIN_SSRF_Metadata_and_OOB_Callback_Test_Script (YARA R4)`	YARA (< 512KB)	Python/HTTP client (`urllib.request`, `requests.get`, `aiohttp`) + `169.254.169.254` or `X-aws-ec2-metadata-token` + `correlation-id` or `/poll?id=`

9. Indicators (0 Published IPs or File Hashes)

The Indicators tab holds **0** published indicators: **0** network addresses and **0** file hashes. `Host R-01` is a misconfigured security-research and developer VPS exposing **42** secret records. Its IPv4 address, TCP port, all folder, file, vendor, and domain names, and all **683** SHA-256 digests are withheld to protect the workspace owner.

Indicator or marker group	Published in Indicators tab	Status in this report
`Host R-01` IPv4 address and TCP port (United States VPS)	0	Withheld to protect the workspace owner
Workspace file SHA-256 digests (683 unique across 937 sized files)	0	Withheld (42 secret records and all names also withheld)
Generic self-audit and sandbox-boundary markers	0 (text-only table below)	10 markers published in the table below

Behavioral and Protocol Self-Audit Markers

Marker category	Pattern / protocol artifact	Layer	Defensive self-audit & control
Python HTTP listing	`Server: SimpleHTTP/` + `Directory listing for /`	Outbound HTTP 200	Alert with `sid:9569001`; close exposed listeners and bind dev tools to `127.0.0.1`.
ACME folder probe	`GET` URI containing `/.acme.sh/`	Inbound HTTP	Alert with `sid:9569002` and Sigma Rule 3; block dot-folders at reverse proxies.
ACME account key probe	`GET` URI containing `account.key`	Inbound HTTP	Alert with `sid:9569003` and Sigma Rule 3; keep ACME keys in 0700 `/etc` folders.
ECDSA key HTTP leak	`-----BEGIN EC PRIVATE KEY-----`	Outbound HTTP 200	Alert with `sid:9569004` and YARA Rule 1; rotate leaked domain ECDSA keys.
PKCS#8 key HTTP leak	`-----BEGIN PRIVATE KEY-----`	Outbound HTTP 200	Alert with `sid:9569005` and YARA Rule 1; deactivate exposed ACME CA accounts.
OOB session register	`POST /register` (`"correlation-id"` + `"public-key"`)	Outbound HTTP/TLS	Alert behind TLS egress proxy with `sid:9569006` and full-URL proxy logs.
OOB callback poll	`GET /poll?id=...&secret=...`	Outbound HTTP/TLS	Alert behind TLS egress proxy with `sid:9569007` and full-URL proxy logs.
Python HTTP server CLI	`python3 -m http.server` / `SimpleHTTPServer`	Linux / Windows CLI	Flag with Sigma Rule 1 and Sentinel `DeviceProcessEvents`; check open sockets.

Marker category	Pattern / protocol artifact	Layer	Defensive self-audit & control
Unsafe VMM host mount	`firecracker` / `cloud-hypervisor` / `qemu` with `/root/`, `/.ssh/`, `/.acme.sh/`, or `docker.sock`	Hypervisor CLI / config	Flag with Sigma Rule 2, Sentinel KQL, and YARA Rule 3; enforce `jailer`.
Unpacked `cpio` rootfs	070701 SVR4 `newc` header + `bin/busybox` + `init`	Unpacked `cpio` stream	Decompress `.cpio.gz` ramdisks in CI and scan with YARA Rule 2 before signing.

10. Scope and Limits

Odin by Brandefense passively analyzed an unauthenticated HTTP directory service on `Host R-01` (United States VPS) recorded from `13 to 20 November 2026`. On `20 November 2026`, that open directory reported **2,993** files and **1,340** directories. Static indexing across `13–20 November 2026` captured **1,278** deduplicated entries: **937** sized files (**969,360,808** bytes) and **341** unsized entries. Across those **937** sized files sit **683** unique SHA-256 digests, alongside **26** config entries and **42** secret records.

Zero credentials or ACME keys were tested, and zero binaries or scripts were run. Node.js `vm2` `CVE-2023-29017` (`< 3.9.15`, `[REF-04]`) is cited strictly as architectural context for micro-VM adoption rather than an artifact on `Host R-01`. All host IPs, ports, folder/file/project/vendor/domain names, **42** secret records, and **683** SHA-256 digests are withheld.

11. Sources

1. `[REF-01]` Firecracker MicroVM Documentation, *Firecracker Lightweight Virtualization and Jailer Isolation Architecture* (verified on 25 November 2026).
2. `[REF-02]` gVisor Official Documentation, *What is gVisor? Application Kernel for Containers* (verified on 25 November 2026).
3. `[REF-03]` The Linux Kernel Documentation, *Ramfs, rootfs and initramfs* (verified on 25 November 2026).
4. `[REF-04]` NIST NVD, *CVE-2023-29017 Detail - Node.js vm2 Sandbox Escape Prior to Version 3.9.15* (verified on 25 November 2026).
5. `[REF-05]` Kubernetes Documentation, *Pod Security Standards and HostPath Volume Restrictions* (verified on 25 November 2026).
6. `[REF-06]` MITRE ATT&CK, *Escape to Host (T1611)* (verified on 25 November 2026).
7. `[REF-07]` MITRE ATT&CK, *Unsecured Credentials: Credentials In Files (T1552.001)* (verified on 25 November 2026).
8. `[REF-08]` MITRE ATT&CK, *Exploit Public-Facing Application (T1190)* (verified on 25 November 2026).
9. `[REF-09]` MITRE ATT&CK, *Deploy Container (T1610)* (verified on 25 November 2026).
10. `[REF-10]` CISA, *BOD 23-02: Mitigating the Risk from Internet-Exposed Management Interfaces* (verified on 25 November 2026).

BRANDEFENSE CAPABILITIES RELATED TO THIS RESEARCH

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

External Attack Surface
Find exposed developer servers and agent workspaces.

Dark Web Monitoring
Catch leaked keys and tokens offered for sale.

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_sandbox_initramfs_acme_and_oob_artifacts.yar** 76 lines

```
/*
   Odin by Brandefense - Monograph 69 YARA Suite
   4 filesize-bounded structural rules covering unencrypted ACME ECDSA/PKCS8 private keys,
   unpacked SVR4 newc cpio BusyBox initramfs images, micro-VM host-mount configuration templates,
   and SSRF metadata / OOB callback verification scripts.
*/

rule ODIN_Unencrypted_ACME_ECDSA_or_PKCS8_Key
{
    meta:
        author = "Odin by Brandefense"
        monograph = "69"
        description = "Detects unencrypted EC or PKCS8 PEM private keys when scans are scoped to ACME state director
ies"
        date = "2026-11-25"
    strings:
        $pem1 = "-----BEGIN EC PRIVATE KEY-----" ascii
        $pem2 = "-----BEGIN PRIVATE KEY-----" ascii
    condition:
        filesize < 64KB and ($pem1 or $pem2)
}

rule ODIN_Custom_Cpio_Newc_Initramfs_BusyBox_Archive
{
    meta:
        author = "Odin by Brandefense"
        monograph = "69"
        description = "Detects unpacked SVR4 newc cpio initial-ramdisk archives bundling BusyBox and an init entrypo
int"
        date = "2026-11-25"
    strings:
        $magic = "070701" ascii
        $b1 = "bin/busybox" ascii
        $b2 = "dev/console" ascii
        $b3 = "sbin/init" ascii
        $b4 = "init" ascii
    condition:
        filesize < 60MB and $magic at 0 and $b1 and $b2 and ($b3 or $b4)
}

rule ODIN_MicroVM_Host_Bind_Mount_and_Egress_Config
{
    meta:
        author = "Odin by Brandefense"
        monograph = "69"
        description = "Detects micro-VM sandbox configuration files combining guest boot descriptors with host-path
bind mounts or egress route rules"
        date = "2026-11-25"
    strings:
        $vm1 = "boot_source" ascii
        $vm2 = "vcpu_count" ascii
        $vm3 = "initramfs" ascii
        $mnt1 = "host_path" ascii
        $mnt2 = "virtio-fs" ascii
```

```
        $net1 = "egress_policy" ascii
        $net2 = "169.254.169.254" ascii
    condition:
        filesize < 1MB and 2 of ($vm*) and (($mnt1 or $mnt2) or ($net1 or $net2))
}

rule ODIN_SSRF_Metadata_and_OOB_Callback_Test_Script
{
    meta:
        author = "Odin by Brandefense"
        monograph = "69"
        description = "Detects Python or shell verification scripts pairing cloud instance metadata endpoints with O
OB callback correlation parameters"
        date = "2026-11-25"
    strings:
        $http1 = "urllib.request" ascii
        $http2 = "requests.get" ascii
        $http3 = "aiohttp" ascii
        $imds1 = "169.254.169.254" ascii
        $imds2 = "X-aws-ec2-metadata-token" ascii
        $oob1 = "correlation-id" ascii
        $oob2 = "/poll?id=" ascii
    condition:
        filesize < 512KB and 1 of ($http*) and 1 of ($imds*) and 1 of ($oob*)
}
```

Suricata `odin_sandbox_workspace_acme_and_oob_hunt.rules` 11 lines

```
# Odin by Brandefense - Monograph 69 Suricata 7.x Ruleset
# Syntax-checked with Odin Suricata linter (0 problems); test with suricata -T prior to deployment.

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R69 Outbound Python SimpleHTTP Directory Listing"; flow:est
ablished,to_client; http.stat_code; content:"200"; bsize:3; http.header; content:"Server: SimpleHTTP/"; fast_patter
n; http.response_body; content:"Directory listing for /"; classtype:policy-violation; sid:9569001; rev:1;)
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-R69 Inbound HTTP GET ACME State Directory"; flow:establishe
d,to_server; http.method; content:"GET"; bsize:3; http.uri; content:"/.acme.sh/"; fast_pattern; nocase; classtype:at
tempted-recon; sid:9569002; rev:1;)
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-R69 Inbound HTTP GET ACME Account Private Key"; flow:establ
ished,to_server; http.method; content:"GET"; bsize:3; http.uri; content:"account.key"; fast_pattern; nocase; classty
pe:credential-theft; sid:9569003; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R69 Outbound HTTP 200 EC Private Key Leak"; flow:establishe
d,to_client; http.stat_code; content:"200"; bsize:3; http.response_body; content:"-----BEGIN EC PRIVATE KEY-----"; f
ast_pattern; classtype:policy-violation; sid:9569004; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R69 Outbound HTTP 200 PKCS8 Private Key Leak"; flow:establi
shed,to_client; http.stat_code; content:"200"; bsize:3; http.response_body; content:"-----BEGIN PRIVATE KEY-----"; f
ast_pattern; classtype:policy-violation; sid:9569005; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R69 Outbound OOB Correlation Register POST"; flow:establish
ed,to_server; http.method; content:"POST"; bsize:4; http.uri; content:"/register"; bsize:9; http.request_body; conte
nt:"|22|correlation-id|22|"; fast_pattern; content:"|22|public-key|22|"; classtype:policy-violation; sid:9569006; re
v:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R69 Outbound OOB Correlation Poll Request"; flow:establishe
d,to_server; http.method; content:"GET"; bsize:3; http.uri; content:"/poll?id="; startswith; fast_pattern; conten
t:"&secret="; distance:0; classtype:policy-violation; sid:9569007; rev:1;)
```

Show full rule

Sentinel KQL `sentinel_sandbox_microvm_http_and_egress_hunt.kql` 33 lines

```
// Odin by Brandefense - Monograph 69
// Unions process events (Python HTTP servers, micro-VM mounts) with metadata-IP events.
// Hunt OOB URI polling (/poll?id= and /register) separately over full-URL proxy logs.
let Lookback = 7d;
let ApprovedSandboxBuildHosts = dynamic(["sandbox-ci-01.corp.example", "acme-renew-01.corp.example"]);
let AdhocHttpOrUnsafeMicroVmMountCli =
    DeviceProcessEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedSandboxBuildHosts))
    | where (
        (FileName in~ ("python", "python3", "python.exe")
            and (ProcessCommandLine contains "http.server" or ProcessCommandLine contains "SimpleHTTPServer"))
        or (FileName in~ ("firecracker", "cloud-hypervisor", "qemu-system-x86_64")
            and (ProcessCommandLine contains "/var/run/docker.sock"
                or ProcessCommandLine contains "/etc/shadow"
                or ProcessCommandLine contains "/root/"
                or ProcessCommandLine contains "/.ssh/"
                or ProcessCommandLine contains "/.acme.sh/"))
    )
    | project Timestamp, DeviceName, AccountName, SignalType = "AdhocHttpOrUnsafeHostMount", Detail = ProcessCommand
Line;
let SandboxMetadataEgress =
    DeviceNetworkEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedSandboxBuildHosts))
    | where InitiatingProcessFileName in~ ("python", "python3", "node", "curl", "wget")
    | where RemoteIP == "169.254.169.254"
    | project Timestamp, DeviceName, AccountName = InitiatingProcessAccountName, SignalType = "MetadataIpEgress", De
tail = strcat(InitiatingProcessFileName, " -> ", RemoteIP, ":", tostring(RemotePort), " ", RemoteUrl);
union AdhocHttpOrUnsafeMicroVmMountCli, SandboxMetadataEgress
| summarize FirstSeen = min(Timestamp), LastSeen = max(Timestamp), EventCount = count(), Signals = make_set(SignalTy
pe, 6), SampleDetails = make_set(Detail, 5) by DeviceName, AccountName
| order by LastSeen desc;
// Separate hunt over full-URL egress proxy logs for OOB polling (/poll?id=, /register):
CommonSecurityLog | where TimeGenerated >= ago(7d) | where isnotempty(RequestURL) | where RequestURL contains "/pol
l?id=" or RequestURL endswith "/register" | project TimeGenerated, SourceHostName, SourceUserName, RequestMethod, De
stinationHostName, RequestURL
```

Sigma `sigma_microvm_sandbox_http_and_acme_exposure.yml` 97 lines

```
title: Ad-Hoc Python HTTP Directory Server Execution on Cloud or Sandbox Hosts
id: 69b2d4f1-7a18-4c52-8e33-69a01f74c201
status: experimental
description: Detects Python http.server or SimpleHTTPServer module execution on Linux servers, which binds to 0.0.0.
0 all interfaces by default when --bind is omitted and exposes local workspaces over HTTP.
author: Odin by Brandefense
date: 2026-11-25
logsource:
  category: process_creation
  product: linux
detection:
  selection_py:
    Image|endswith:
      - '/python'
      - '/python3'
      - '/python3.11'
      - '/python3.12'
  selection_mod:
    CommandLine|contains:
      - 'http.server'
```

```
      - 'SimpleHTTPServer'
  filter_hosts:
    ComputerName:
      - 'sandbox-ci-01.corp.example'
  condition: selection_py and selection_mod and not filter_hosts
falsepositives:
  - Local development testing bound strictly to 127.0.0.1 on non-production workstations; correlate with non-loopbac
k listening sockets in SIEM
level: high
tags:
  - attack.credential-access
  - attack.t1552.001
---
title: Micro-VM or Hypervisor Launched With Sensitive Host Path Mounts
id: 69b2d4f1-7a18-4c52-8e33-69a01f74c202
status: experimental
description: Detects Firecracker, Cloud Hypervisor, or QEMU micro-VM processes referencing sensitive host sockets, c
redential directories, or ACME key paths on the command line.
author: Odin by Brandefense
date: 2026-11-25
logsource:
  category: process_creation
  product: linux
detection:
  selection_vmm:
    Image|endswith:
      - '/firecracker'
      - '/cloud-hypervisor'
      - '/qemu-system-x86_64'
  selection_sensitive_path:
    CommandLine|contains:
      - '/var/run/docker.sock'
      - '/etc/shadow'
      - '/root/'
      - '/.ssh/'
      - '/.acme.sh/'
  filter_hosts:
    ComputerName:
      - 'sandbox-ci-01.corp.example'
  condition: selection_vmm and selection_sensitive_path and not filter_hosts
falsepositives:
  - Dedicated bare-metal hypervisor build validation nodes on explicitly allowlisted hosts
level: high
tags:
  - attack.privilege-escalation
  - attack.t1611
---
title: Unexpected Archiving or Copy of Automated ACME Private Key Directories
id: 69b2d4f1-7a18-4c52-8e33-69a01f74c203
status: experimental
description: Detects archiving, remote copy, or HTTP transfer utilities referencing .acme.sh state directories or AC
ME account.key material outside designated certificate renewal hosts.
author: Odin by Brandefense
date: 2026-11-25
logsource:
  category: process_creation
  product: linux
detection:
  selection_cli:
    Image|endswith:
      - '/tar'
      - '/zip'
      - '/cp'
```

```
      - '/scp'
      - '/rsync'
      - '/curl'
  selection_acme:
    CommandLine|contains:
      - '/.acme.sh/'
      - 'account.key'
  filter_acme_hosts:
    ComputerName:
      - 'acme-renew-01.corp.example'
  condition: selection_cli and selection_acme and not filter_acme_hosts
falsepositives:
  - Authorized TLS certificate distribution jobs running on allowlisted renewal controllers
level: medium
tags:
  - attack.credential-access
  - attack.t1552.001
```

