FULL REPORT · AI OFFENSE · MONOGRAPH 60 / 59 · 18 MIN READ

Post-Disclosure ARTEX Growth, Storm-0940 Overlaps, and Multi-Port Staging

Tracking late-November autonomous testing console growth, evaluating 10 overlapping hosts in Wiz's 156-IP disclosure, and hardening against ZQAgent persistence

BY
Odin by Brandefense

PUBLISHED
19 November 2026

READING TIME
18 min read

EDITION
Version 1.1 · TLP:CLEAR

SCOPE
Prepared November 2026

1. Executive Summary

IN SHORT

During a two-week observation window ending 24 November 2026, Odin by Brandefense tracked 5,681 seven-day candidate consoles across seven autonomous testing tools. From 20 to 24 November, four tallied tools added 1,073 new candidates, led by 841 ARTEX endpoints. An aggregate summary against Wiz's 156-IP lists records 10 overlap hosts, including one Vshell server staging 49 files. Gate exposed panels, hunt ZQAgent persistence, and lock web origins.

Public security warnings often push cloud hosts to take down abused open-source servers. Autonomous testing tools driven by large language models took the opposite turn in late November 2026. One week after the FBI issued `FLASH-20261113-001` on 13 November 2026 warning of ARTEX abuse, new candidate consoles kept appearing across cloud networks.

During a two-week observation window ending 24 November 2026, Odin by Brandefense tracked seven autonomous testing tools across public internet space. Across all seven tools, 5,681 candidate console endpoints appeared in the seven-day slice from 18 to 24 November 2026. Those 5,681 endpoints sit inside 8,311 thirty-day candidate endpoints.

Candidate consoles include red teams, university labs, and developer test VMs alongside threat actors. Odin by Brandefense therefore withholds all candidate console IPs, open-directory host IPs, and overlap host IPs. Zero IPv4 addresses or file SHA-256 hashes appear in our feeds.

1. **Late-November console growth stayed focused in ARTEX and CyberStrikeAI.**
From 20 to 24 November 2026, four tallied tools added 1,073 new candidate endpoints. That total spans 841 ARTEX endpoints, 155 CyberStrikeAI endpoints, 42 AutoHunter endpoints, and 35 PentAGI endpoints. Across the full seven-day slice, ARTEX (3,361) and CyberStrikeAI (1,388) made up 83.6 percent of all 5,681 candidates.

2. **Only 10 of 156 Wiz-published IPv4s overlapped observed consoles and directories.**
On 23 November 2026, Wiz Research released a study of agentic attack tools following its 22 October 2026 Storm-0940 report. The two cited Wiz IOC files contain 156 unique IPv4 addresses: 74 in the agentic-attacks list and 82 in the Black October list. The retained aggregate summary records 10 overlapping hosts (6.4 percent) and 146 non-overlapping IPs (93.6 percent), though the row-level comparison is unavailable for verification.

Eight overlap hosts exposed ARTEX panels across TCP ports 8787, 443, and 8080. One host paired Vshell on TCP 443 with two open HTTP directories on TCP 8085 and 8093. One overlap host paired a BrainstormV2 console with a single-file open directory; its owner is unconfirmed and its ports are withheld.

3. **Open-source ARTEX panels on shared cloud ranges do not imply Storm-0940 ownership.**
Public ARTEX forks run on shared cloud VMs around the world. Wiz also showed that broad-spray actors route active requests through rotating home and ISP proxies. Treating every exposed ARTEX panel on a shared cloud subnet as Storm-0940 infrastructure causes false claims and noisy blocklists.

4 **Multi-port staging and NVISO's ZQAgent case show the need for host and protocol hunts.**
On the Vshell overlap server (`Host W-09`), two HTTP directories held 49 staged files totaling 570,418 bytes. Those files held three ASP.NET templates and 12 Python WAF-test and matrix scripts. Also on 23 November 2026, NVISO Labs reported an ARTEX case planting ZQAgent, a Linux backdoor using RAM-only files and systemd linger.

Three Decisions for Security Leaders

1. **Find and gate exposed testing panels.** Scan corporate cloud accounts and lab subnets on standard web ports and high ports for ARTEX, CyberStrikeAI, PentAGI, HexStrikeAI, AutoCVE, AutoHunter, and BrainstormV2. Put approved panels behind mTLS or VPNs.
2. **Treat third-party agentic IP lists as short-lived context.** Separate rotating home proxy exits from static cloud panels when reviewing external IP feeds. Require matching sign-in, OAuth, and HTTP request proof before naming an actor.
3. **Run protocol, IIS origin, and Linux persistence checks together.** Lock IIS origins to verified CDN or WAF edges and alert when `w3wp.exe` starts a shell. On Linux hosts, alert on `/memfd:a` links, spoofed `dbus-daemon` flags, and unapproved `loginctl enable-linger` calls.

The Study in Numbers

Number	What it is
8,311	Rolling 30-day candidate console endpoints across seven tracked autonomous testing tools ending 24 November 2026
5,681	Trailing 7-day candidate console endpoints (18-24 November 2026), a subset of the 30-day total
1,073	New candidate endpoints from 20 to 24 November 2026 across four tallied tools (841 ARTEX, 155 CyberStrikeAI, 42 AutoHunter, 35 PentAGI)
156	Unique IPv4 addresses in the two cited Wiz 23 November 2026 IOC files (74 agentic-attacks and 82 Black October)
10	Wiz-published IPv4s (6.4%) recorded in the retained overlap summary (row-level join unavailable); 146 (93.6%) had no console or directory match
49	Staged files (570,418 bytes) on Host W-09 across TCP 8085 (36 files) and TCP 8093 (13 files) beside Vshell on TCP 443
0	Published blocklist IPv4 addresses or file SHA-256 hashes in our feeds (10 behavioral and protocol hunt markers)

2. Post-Disclosure Growth Across Seven Autonomous Frameworks

On `13 November 2026` , the FBI Cyber Division issued `FLASH-20261113-001` (`[REF-01]`) warning of malicious **ARTEX** use (`[REF-06]`). Even after the author removed the original repo in October 2026, public forks, mirrors, and peer multi-agent tools kept spreading across cloud providers (`[REF-01]` , `[REF-02]`).

During the two-week observation window ending `24 November 2026` , Odin by Brandefense tracked seven autonomous testing tools: `ARTEX` , `CyberStrikeAI` , `PentAGI` , `HexStrikeAI` , `AutoCVE` , `AutoHunter` , and `BrainstormV2` . Teams can use external attack surface management to find exposed panels on both high ports and reverse-proxied web ports. Figure 1 maps the four study tracks.

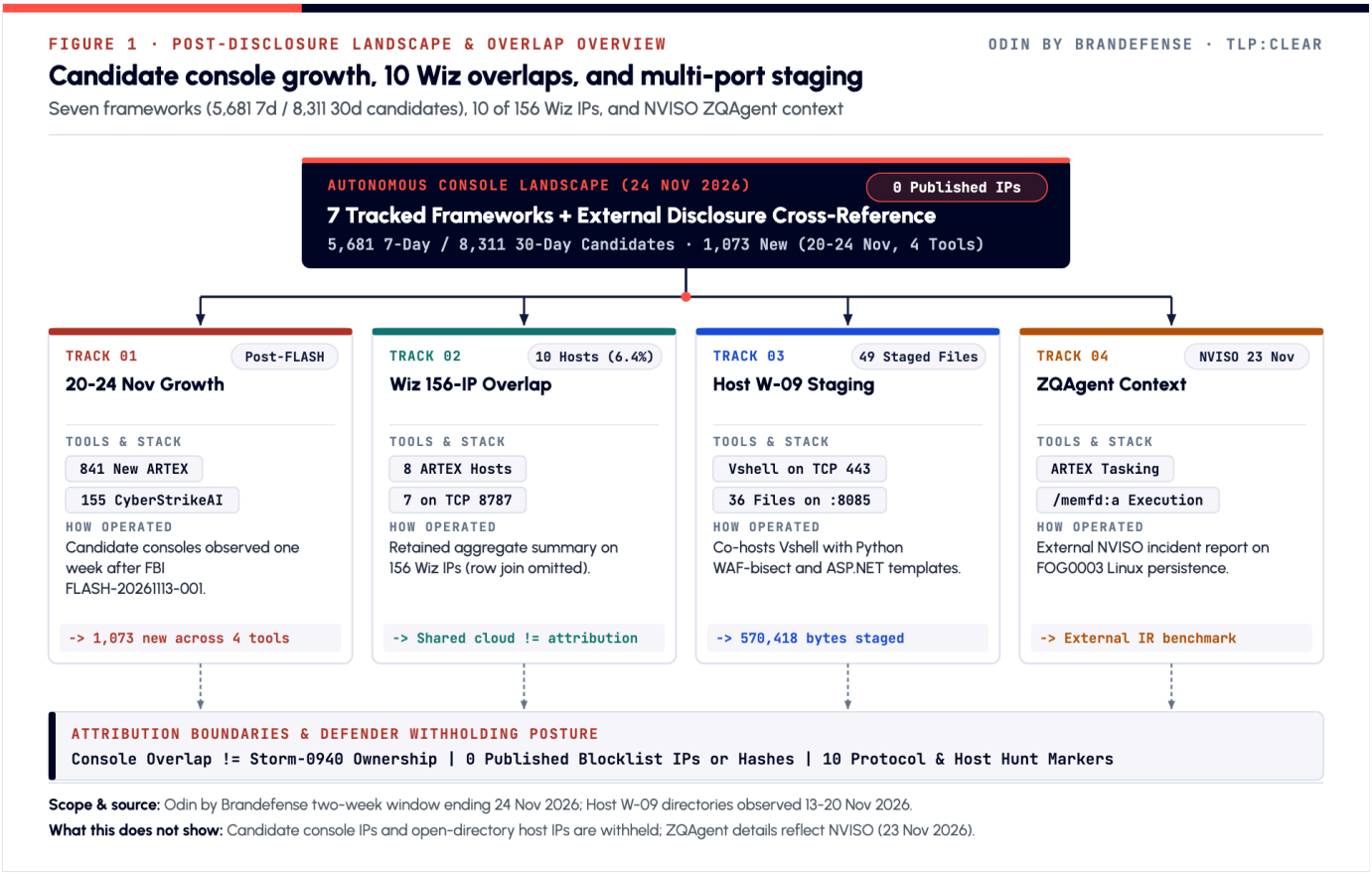

Figure 1: Candidate console growth, 10 Wiz overlaps, and multi-port staging

Rolling 30-Day, Trailing 7-Day, and `20-24 November` Candidate Counts

Table 1 separates three related counts recorded through `24 November 2026`. Rolling **30**-day candidate endpoints total **8,311** across all seven tools. Trailing **7**-day candidate endpoints (`18-24 November 2026`) form a **5,681**-endpoint subset of that **30**-day count. New candidates from `20 to 24 November 2026` total **1,073** across the four tools tallied for late-November growth.

Framework	30-day candidates	30d share (%)	7-day candidates (18-24 Nov)	7d share (%)	7d / 30d ratio (%)	New (20-24 Nov)
ARTEX	4,860	58.5%	3,361	59.2%	69.2%	841
CyberStrikeAI	2,114	25.4%	1,388	24.4%	65.7%	155
PentAGI	853	10.3%	552	9.7%	64.7%	35
HexStrikeAI	167	2.0%	123	2.2%	73.7%	not tallied
AutoCVE	159	1.9%	155	2.7%	97.5%	not tallied
AutoHunter	111	1.3%	101	1.8%	91.0%	42
BrainstormV2	47	0.6%	1	0.0%	2.1%	not tallied
Total (7 tools)	**8,311**	**100.0%**	**5,681**	**100.0%**	**68.4%**	**1,073 (4 tools)**

Three clear trends stand out in Table 1 and Figure 5. First, `ARTEX` (**3,361**) and `CyberStrikeAI` (**1,388**) account for **4,749** of the **5,681** seven-day endpoints (**83.6%**).

Second, from `20 to 24 November 2026` , one week after `FLASH-20261113-001` , four tools added **1,073** new candidates (**841** `ARTEX` , **155** `CyberStrikeAI` , **42** `AutoHunter` , and **35** `PentAGI`). Third, `AutoCVE` (**155** of **159**; **97.5%**) and `AutoHunter` (**101** of **111**; **91.0%**) cluster in the recent

seven-day slice, while `BrainstormV2` dropped to **1** seven-day endpoint (**2.1%**).

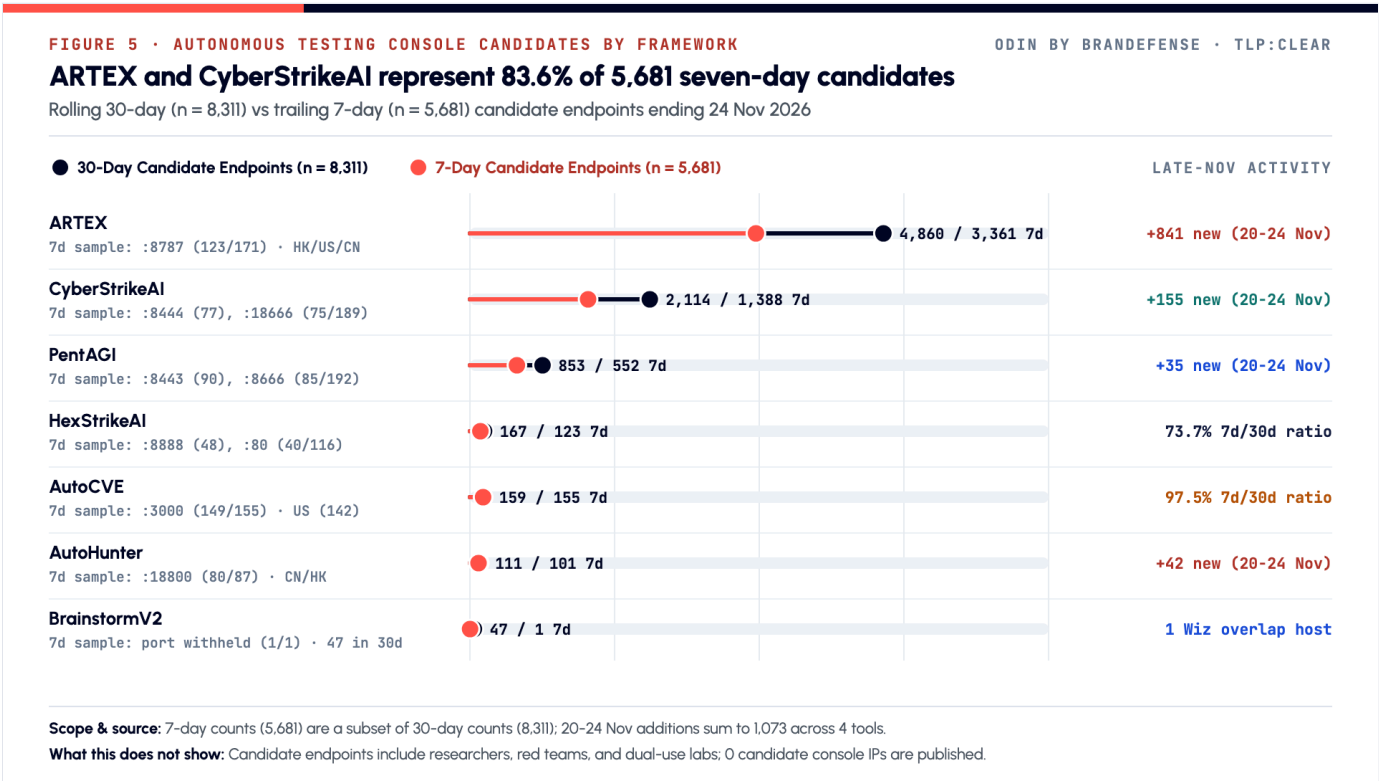

Figure 5: ARTEX and CyberStrikeAI represent 83.6% of 5,681 seven-day candidates

Sampled Seven-Day Port and Country Subsets

Users bind these panels to both default high ports and standard web ports. Because our port and country counts come from top-six seven-day samples per tool, Table 2 gives each sample size (`n`) beside its counts.

Framework	Port sample (n)	Sampled 7-day TCP ports (count)	Country sample (n)	Sampled 7-day countries (count)
ARTEX	171	8787 (123), 443 (22), 80 (12), 18787 (5), 39721 (5), 8443 (4)	177	HK (63), US (43), CN (43), JP (12), SG (11), NL (5)
CyberStrikeAI	189	8444 (77), 18666 (75), 8080 (31), 18080 (3), 8443 (2), 8085 (1)	196	US (158), CN (24), MD (4), HK (4), KR (4), JP (2)
PentAGI	192	8443 (90), 8666 (85), 443 (11), 8444 (3), 18443 (2), 9521 (1)	165	US (112), CN (17), HK (13), DE (10), SG (7), FR (6)
HexStrikeAI	116	8888 (48), 80 (40), 5000 (13), 443 (6), 8080 (5), 8000 (4)	79	US (28), IN (13), DE (12), SG (11), SE (8), AU (7)
AutoCVE	155	3000 (149), 13000 (4), 18080 (1), 8088 (1)	155	US (142), CN (12), JP (1)
AutoHunter	87	18800 (80), 443 (3), 26398 (1), 1880 (1), 10001 (1), 8080 (1)	100	CN (68), HK (21), US (7), SG (2), KR (1), FR (1)
BrainstormV2	1	port withheld (1)	1	US (1)

In the **171**-endpoint `ARTEX` port sample, **123** endpoints used default `TCP 8787` and **5** used `TCP 18787`. Another **38** sampled `ARTEX` endpoints listened on `TCP 443`, **80**, or **8443**. Asset sweeps should match HTTP banners and icon hashes across all web ports. Checking `TCP 8787` alone misses proxied panels that still serve the `ARTEX` favicon MD5 (`cd3ebd16437d6d3963592f7365dd3980`).

3. Wiz 23 November 2026 Indicator Overlaps and Multi-Port Staging

On `23 November 2026`, Wiz Research published *Agentic Attacks in the Wild: ARTEX & Offensive AI Frameworks* (`[REF-02]`, `[REF-05]`), following its `22 October 2026` report on `Storm-0940` (`[REF-03]`). The two cited Wiz IOC files contain 156 unique IPv4 addresses: 74 in the agentic-attacks list and 82 in the Black October list.

Analysts can use cyber threat intelligence to separate rotating proxy traffic from static staging servers when reviewing external feeds. The retained aggregate summary records **10** overlapping hosts among **156** Wiz IPv4s, but the row-level comparison is unavailable for independent verification.



Figure 4: Aggregate summary records 10 Wiz IP overlaps across consoles and directories

Segmentation of the 156 Published Wiz IPv4s

Segment	Host count	Share of 156 (%)	Observed TCP ports & co-hosted services	IP status
`ARTEX` single- or multi-port hosts	8	5.1%	10 `ARTEX` bindings on 8 hosts: `TCP 8787` (7), `TCP 443` (2), `TCP 8080` (1).	Withheld (0 IPs)
`Vshell` + dual directory server (`Host W-09`)	1	0.6%	`TCP 443` (`Vshell`), `TCP 8085` (36 files, 453,430 B), `TCP 8093` (13 files, 116,988 B).	Withheld (0 IPs)
`BrainstormV2` + open directory (`Host W-10`)	1	0.6%	One overlap host paired a `BrainstormV2` console with a single-file open directory; its owner is unconfirmed and its ports are withheld.	Withheld (0 IPs)
Wiz IPv4s without a console or directory	146	93.6%	No observed console or open directory; other Wiz IP types unclassified (`[REF-02]`, `[REF-05]`).	External Wiz list
Total	**156**	**100.0%**	10 console/directory overlaps (6.4%) + 146 non-overlapping IPs (93.6%).	0 IPs in Odin feed

Two clear lessons come from Figure 4 and Table 3. First, **146** of the **156** Wiz IPs (**93.6%**) had no observed console or open directory in our data. A missing console match leaves those **146** addresses unclassified by console role, though Wiz separately noted that broad-spray actors also route requests through home and ISP proxy pools (`[REF-02]`).

Second, across the **8** overlapping `ARTEX` hosts, listeners span `TCP 8787` (**7** hosts), `TCP 443` (**2** hosts), and `TCP 8080` (**1** host). Wiz's `23 November` lists group several campaigns alongside `Black October` cases rather than a single actor (`[REF-02]` , `[REF-05]`).

Finding an open-source `ARTEX` panel on a shared cloud subnet **does not establish `Storm-0940` ownership**. Shared cloud IPs churn often, and public `ARTEX` forks are easy to copy. Teams need matching sign-in and tooling proof before claiming a named actor.

`Host W-09` : `Vshell` (:443) Paired with 49 Staged Files on :8085 and :8093

One overlap host (`Host W-10`) paired a `BrainstormV2` console with a single-file open directory; its owner is unconfirmed and its ports are withheld. By contrast, `Host W-09` (IP withheld) shows a multi-port staging server (`[REF-07]` , `[REF-08]`). Alongside `Vshell` on `TCP 443` , `Host W-09` exposed two open HTTP directories first seen on `13 November 2026` and last seen on `20 November 2026` .

Across both ports, `Host W-09` held **49 files totaling 570,418 bytes** (**36** files = **453,430** B on **:8085**; **13** files = **116,988** B on **:8093**). Fifteen script files (**12** `.py` and **3** `.aspx`) total **25,537** bytes. Thirty-four text, JSON, HTML, and log files total **544,881** bytes. Table 4 groups all **49** files into five staging clusters.

Staging cluster on `Host W-09`	Kind	:8085 files	:8085 bytes	:8093 files	:8093 bytes	Total files	Total bytes	Staged examples
Python WAF & Matrix Scripts	`script`	8	10,360	4	7,604	12	17,964	Port 8085 holds `waf_bisect.py` , `urlvar.py` , `write_ws.py` , `write_mgmt.py` , and 4 more scripts. Port 8093 adds `write_classic.py` , `verify_http_281.py` , `fill_matrix_281.py` , and `probe_dirs.py` .
Staged ASP.NET Templates	`script`	1	3,178	2	4,395	3	7,573	`Photos.aspx` (3,178 B on :8085). `GetStart.aspx` (3,932 B) and `Classic.aspx` (463 B) on :8093.
HTML Edge & Origin Captures	`text`	17	178,590	2	20	19	178,610	`h1.html` - `h3.html` (56,611 B each), `ar.html` , `ws1.html` - `ws3.html` , `mg1.html` - `mg6.html` , `og1.html` - `og3.html` . Also `body_edge1.txt` , `body_origin1.txt` , and `out.txt` .
JSON State & Web-Config Text	`text`	1	2,015	4	67,684	5	69,699	`probe_dirs.json` (55,136 B), `write_classic.json` (7,400 B), `verify_http_281.json` , and `fill_matrix_281.json` . Also 1 web-config text file (2,015 B, name withheld).
HTTP Daemon & Run Logs	`text`	9	259,287	1	37,285	10	296,572	`httpd.log` (249,645 B), `httpd_8093.log` (37,285 B), `write_matrix_ws.log` , `write_mgmt.out` , and `write_ws.out` . Also `write_matrix_mgmt.log` , `http_verify_ws.log` , `write_matrix.log` , `delete_old.log` , `del_old.out` .
Total	**All**	**36**	**453,430**	**13**	**116,988**	**49**	**570,418**	**Seen `13-20 November 2026` ; host IP withheld.**

Three strict rules guide how we read `Host W-09` :

- **Split-port HTTP staging.** Keeping `Vshell` on **:443** while hosting file servers on **:8085** and **:8093** splits C2 traffic from staged scripts. Log sizes (**249,645** B and **37,285** B) show verbose HTTP logs, not how long an operation lasted.
- **WAF testing and edge-vs-origin checks.** File names such as `waf_bisect.py` , `urlvar.py` , `body_edge1.txt` , and `body_origin1.txt` point to scripts built to compare CDN edges with origin hosts. They pair with benign-named `.aspx` templates (`[REF-08]`).
- **Staged prep, not confirmed target impact.** Directory listings show operator prep only. Nothing confirms that `Photos.aspx` , `GetStart.aspx` , or `Classic.aspx` worked on a victim host. One **2,015**-byte web-config file name on **:8085** is withheld along with `Host W-09` 's IP.

4. External ZQAgent Persistence Context (`23 November 2026`)

Early LLM-driven intrusions mostly looked like fast, noisy key-theft runs (`[REF-01]` , `[REF-02]`). In Wiz's `23 November 2026` cases (`[REF-02]`), actors sprayed OAuth and sign-up flows while leaving self-labeled strings like `pentest-recon` user-agents, `pentest-iNNNNNN` counters, and `csai-pentest-role` names.

On `23 November 2026` , **NVISO Labs** shared incident findings (`[REF-04]`) showing that operators also use `ARTEX` to plant long-term Linux malware. Figure 3 shows an analytical model joining our `Host W-09` staging data with Wiz's proxy recon findings (`[REF-02]`) and NVISO's `ZQAgent` report (`[REF-04]`).

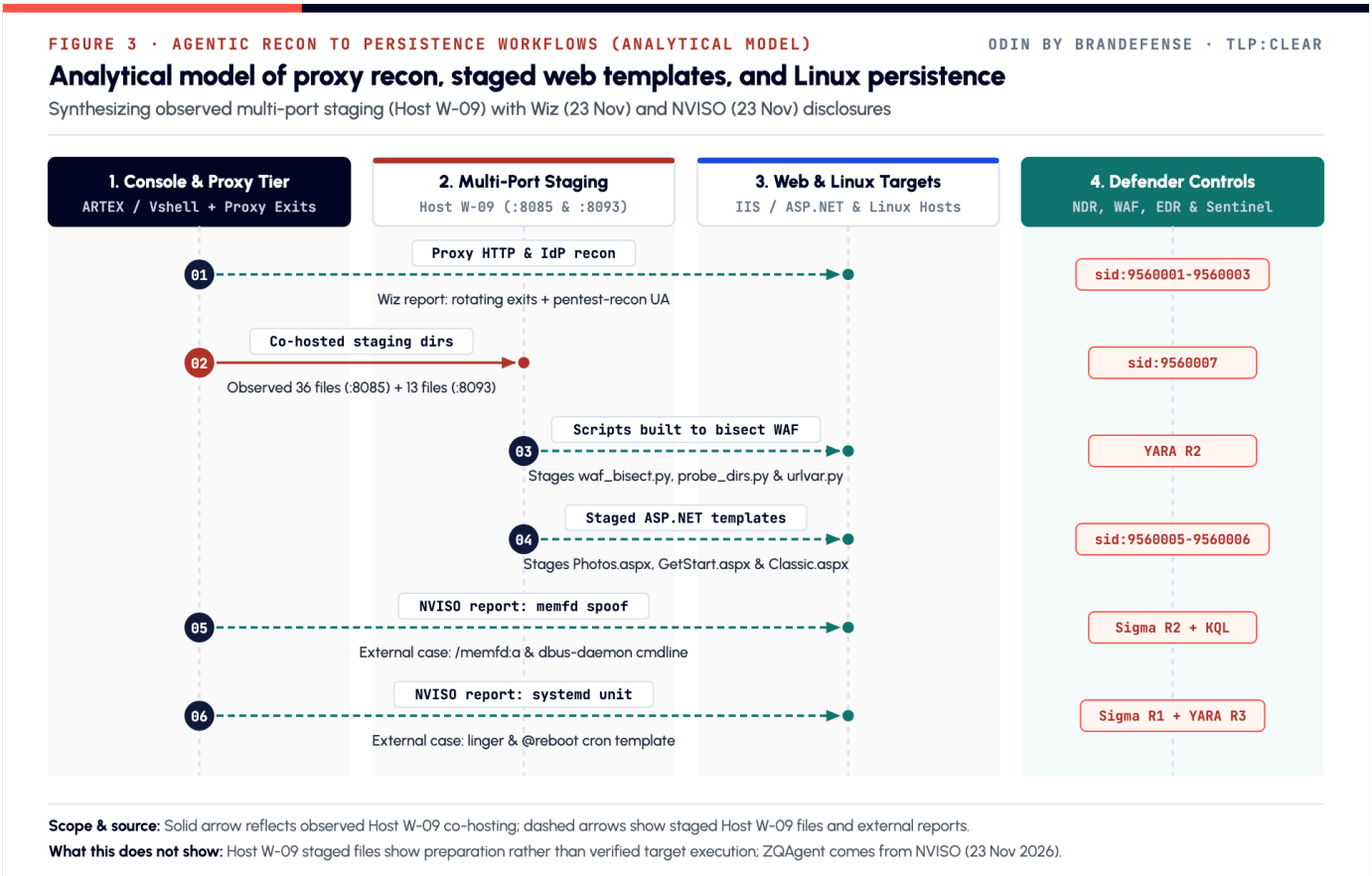

Figure 3: Analytical model of proxy recon, staged web templates, and Linux persistence

How `ZQAgent` Establishes Linux Persistence (`[REF-04]`)

Odin by Brandefense did **not** find `ZQAgent` on `Host W-09` . We include NVISO's `23 November 2026` report (`[REF-04]`) so teams hunting `ARTEX` cases check Linux hosts for quiet backdoors. In a Belgian incident tied to `FOG0003` (with related links in Asia), NVISO saw `ARTEX` plant `ZQAgent` under direct operator tasking (`[REF-04]`):

- **RAM-only `memfd` move (`[REF-09]`).** `ZQAgent` copies itself into an unnamed RAM file via `memfd` , so `/proc/<pid>/exe` points to `/memfd:a (deleted)` .
- **Spoofed `dbus-daemon` command line.** After detaching, `ZQAgent` spoofs `/usr/bin/dbus-daemon --session --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only` without linking to `/usr/bin/dbus-daemon` on disk.
- **Dual `systemd` (`[REF-10]`) and `cron` survival.** `ZQAgent` writes a `systemd` unit (`Description=Device event journal daemon`) and `@reboot` cron jobs. For non-root users, it enables a `--user` unit and runs `loginctl enable-linger` to outlive logouts while offering shell, file, and TCP/UDP tunnel features (`[REF-04]`).

Figure 2 links all five exposure and persistence layers to the defender actions in Chapter 7 and the rules in Chapter 8.

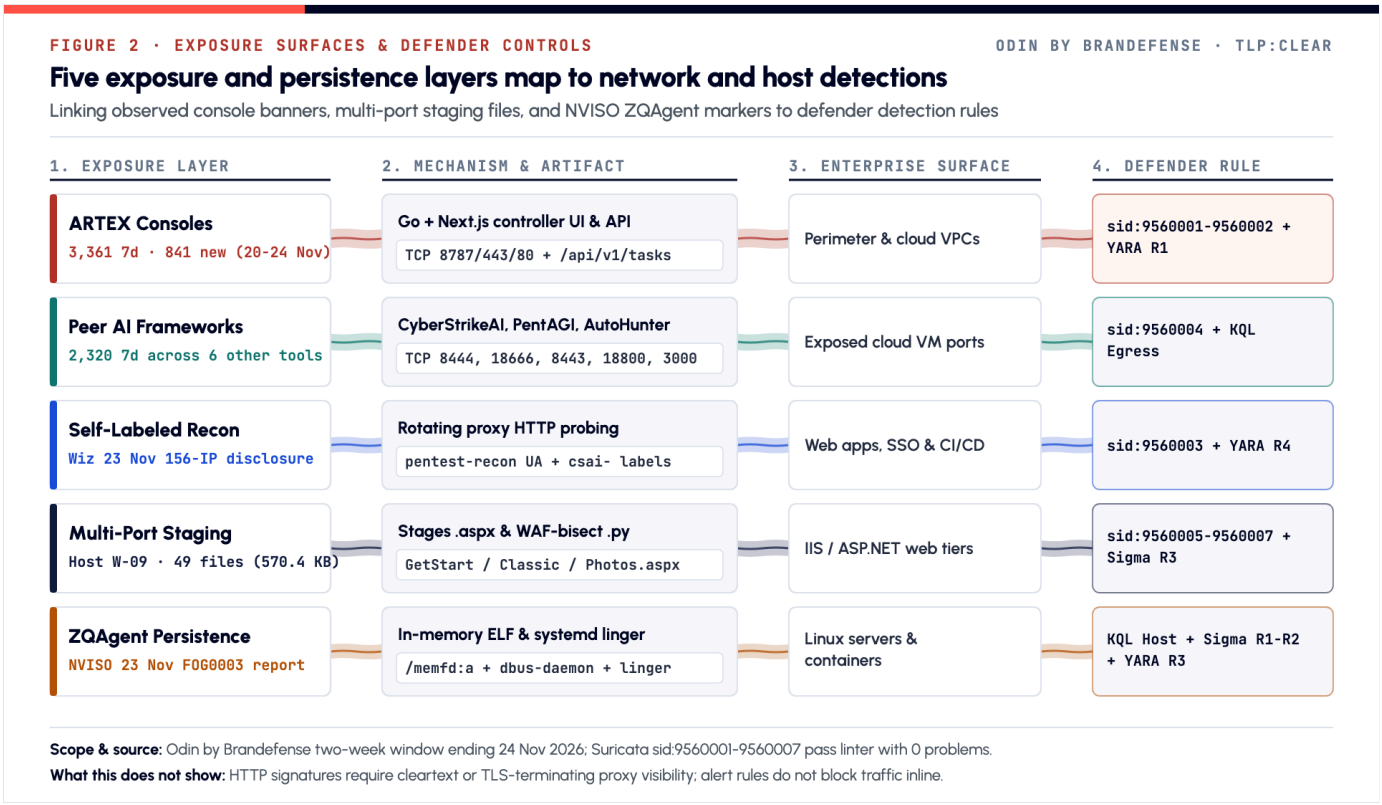

Figure 2: Five exposure and persistence layers map to network and host detections

5. Enterprise Exposure and Control Verification

Teams should check five concrete controls across cloud, web, sign-in, and Linux tiers rather than assuming unverified root causes:

Exposure layer	Observed or reported evidence	Control to verify	Operational risk
Exposed testing panels	5,681 7d / 8,311 30d candidates; 841 new `ARTEX` (`20-24 Nov`).	Verify whether cloud VPCs expose 8787, 8444, 18666, 8443, 18800, 3000, or proxied 443 panels without mTLS.	Open panels leak target scopes, LLM keys, and cloud tokens (`[REF-01]`, `[REF-02]`).
Proxy sprays & OAuth	146 of 156 Wiz IPs (93.6%) had no console match; `pentest-recon` labels (`[REF-02]`).	Verify whether IdPs and WAFs enforce MFA, rate limits, and OAuth or CI checks regardless of source IP.	IP blocklists miss home-proxy password sprays and CI secret theft (`[REF-02]`).
Origin bypass & `.aspx`	`Host W-09` stages `waf_bisect.py`, `body_edge1.txt`, `body_origin1.txt`, and 3 `.aspx` files.	Verify whether IIS origins drop non-CDN traffic and block `.aspx` writes in web roots (`[REF-07]`, `[REF-08]`).	Direct origin access lets attackers skip edge WAF rules and test web shells.
High-port file fetches	`Host W-09` serves 49 files on :8085 and :8093. One overlap host (`Host W-10`) paired a `BrainstormV2` console with a single-file open directory; its owner is unconfirmed and its ports are withheld.	Verify whether server VLANs block direct outbound HTTP calls to random high ports.	Web hosts could pull staging scripts from external high ports.
Linux `memfd` & linger	NVISO `23 Nov` `ZQAgent` report (`/memfd:a`, spoofed `dbus-daemon`, `enable-linger`, `[REF-04]`).	Verify whether Linux EDR flags `/memfd:*` links (`[REF-09]`) and non-root `systemd` linger edits (`[REF-10]`).	Treating agentic cases as brief smash-and-grab runs misses Linux implants.

6. Alternative Hypotheses

Hypothesis	Evidence for	Evidence against	Assessment
All 8 overlap `ARTEX` hosts belong to `Storm-0940`	Listed in Wiz's `23 Nov` 156-IP files (`[REF-02]` , `[REF-05]`) and run `ARTEX` on 8787, 443, or 8080.	Wiz's `23 Nov` lists span several campaigns and `Black October` cases. `ARTEX` is open-source (3,361 7d candidates) on shared clouds.	**Unsupported as single-actor proof.** Shared cloud panels do not imply `Storm-0940` ownership.
All 3,361 7d `ARTEX` candidates are attacker C2s	FBI `FLASH-20261113-001` (`[REF-01]`) and vendor posts confirm real abuse.	Red teams, researchers, and builders test `ARTEX` forks on cloud VMs after major alerts.	**Rejected for blanket blocking.** Withhold candidate IPs (0 published IPs) and hunt behavior.
`Host W-09` is a benign dev test box	Serves HTML pages (`h1.html` - `h3.html`) and Python HTTP logs.	Sits in Wiz's intrusion list (`[REF-05]`), runs `Vshell` on :443, and stages `waf_bisect.py` , `run_cmd.py` , and 3 `.aspx` files.	**Contradicted.** Treated consistently as an attacker staging box; IP and 1 config name stay withheld.
`ARTEX` cases never plant host persistence	Many broad-spray runs focus on quick cloud key theft (`[REF-02]`).	NVISO (`23 Nov 2026` , `[REF-04]`) saw `ARTEX` plant `ZQAgent` using `/memfd:a` and `systemd` linger.	**Refuted as a blanket rule.** Pair cloud key resets with Linux host sweeps.

7. What Defenders Should Do

Security teams can close console, web-origin, and Linux persistence gaps in five practical steps:

1. **Sweep and gate testing panels (`0-48 Hours`).** Scan cloud accounts and lab ranges across standard web ports and default high ports (**8787**, **18787**, **8444**, **18666**, **8443**, **8666**, **18800**, **3000**) (`[REF-01]`). Put approved testing tools behind VPNs or mTLS proxies, and rotate LLM or cloud keys kept on exposed boxes.
2. **Harden sign-in and CI flows against proxy sprays (`0-72 Hours`).** Because **146** of **156** Wiz IPs (**93.6%**) had no console match and Wiz reported proxy-routed sprays (`[REF-02]`), enforce phishing-resistant MFA, rate-limit sign-up and reset pages, govern OAuth app consent, and gate CI workload branches. Hunt `pentest-recon` , `pentest-i` , and `csai-` strings in cloud logs (`[REF-02]`).
3. **Lock IIS and ASP.NET origins behind CDN or WAF edges (`Days 1-7`).** Set origin firewalls to accept HTTP and HTTPS traffic only from verified CDN or WAF proxy ranges using origin-pull certs (`[REF-07]`). Mount web code folders read-only outside releases and alert for web shell behavior when `w3wp.exe` starts `cmd.exe` or PowerShell (`[REF-08]` , Sigma Rule 3).
4. **Block direct server egress to random high ports (`Days 7-14`).** Stop DMZ and app VLANs from making direct outbound calls to external hosts on ports like **8085**, **8093**, **8787**, **8444**, **18666**, and **18800**. Send allowed web traffic through a TLS proxy watched by Suricata `sid:9560001` -**9560007**.
5. **Check Linux hosts for `memfd` links and `systemd` linger (`Days 7-21`).** Alert when `/proc/<pid>/exe` points to `/memfd:* (deleted)` (`[REF-04]` , `[REF-09]`) or when `dbus-daemon` flags run outside `/usr/bin/dbus-daemon` (Sigma Rule 2). Check `/var/lib/systemd/linger/` , user `systemd` folders, and `/etc/cron.d/` for unapproved `Device event journal daemon` or `@reboot` entries (`[REF-10]` , Sigma Rule 1).

8. Detection Rules

The full rules are in the Detection rules tab. Because all candidate console IPs, open-directory IPs, and overlap host IPs are withheld, each rule file targets protocol, process, or file structure signals.

Check scope (`Publication Rules §6`): the Suricata rules passed the Odin Suricata linter (**0** problems). YAML checks confirmed all three Sigma rules, and structural checks verified the Sentinel KQL and YARA files. Live engine binaries (`suricata -T` , `Kusto.Language` , `pySigma` , and `yara`) were not installed on the build host. Rules were not replayed on live traffic, so test and tune them before rollout.

Rule file	What it catches
`odin_artex_console_staging_and_recon_hunt.rules`	Suricata 7.x (**7** `alert http` rules, `sid:9560001` -9560007): exposed home-network `ARTEX` and `CyberStrikeAI` banners, outbound `POST /api/v1/tasks` calls, inbound `pentest-recon` user-agents, inbound `POST` calls to `/GetStart.aspx` or `/Classic.aspx` , and high-port `.aspx` directory listings

Rule file	What it catches
`sentinel_artex_console_zqagent_and_staging_hunt.kql`	Microsoft Sentinel KQL (7-day lookback): correlates `DeviceProcessEvents` (`ZQAgent` `/memfd:a` , spoofed `dbus-daemon` flags, `loginctl enable-linger` , and IIS `w3wp.exe` shells) with `DeviceNetworkEvents` (default console ports or `RemoteUrl contains "/api/v1/tasks"`)
`sigma_artex_zqagent_memfd_and_iis_webshell.yml`	Portable Sigma (3 process-creation rules): Linux `loginctl enable-linger` or `systemctl --user` enablement, spoofed `dbus-daemon` arguments outside `/usr/bin/dbus-daemon` and `/bin/dbus-daemon` , and Windows `w3wp.exe` child shells
`odin_artex_console_and_staging_artifacts.yar`	Structural YARA (4 `filesize` -bounded rules): exposed `ARTEX` console bundles, Python WAF-bisect and matrix scripts, `ZQAgent` `systemd` and `dbus-daemon` strings (`[REF-04]`), and self-labeled agentic task logs (`[REF-02]`)

How the Suricata 7.x Signatures Work (`sid:9560001` -9560007)

All seven `http` signatures require cleartext HTTP traffic or a sensor behind a TLS proxy. Because `alert` rules do not block packets inline, enforce blocks in your WAF or egress proxy.

SID	Direction & flow	What it matches	Defensive purpose
9560001	`$HOME_NET any -> $EXTERNAL_NET any` (`to_client`)	`http.response_body` containing `ARTEX - Autonomous Red-Team Expert`	Flags exposed home-network `ARTEX` panels answering external clients
9560002	`$HOME_NET any -> $EXTERNAL_NET any` (`to_server`)	`POST` request with `http.uri` starting with `/api/v1/tasks`	Flags outbound task dispatch calls to an `ARTEX` controller
9560003	`$EXTERNAL_NET any -> $HOME_NET any` (`to_server`)	`http.user_agent` containing `pentest-recon` (`nocase`)	Flags self-labeled agentic recon sweeps (`[REF-02]`)
9560004	`$HOME_NET any -> $EXTERNAL_NET any` (`to_client`)	`http.response_body` containing `CyberStrikeAI`	Flags exposed home-network `CyberStrikeAI` panels answering external clients
9560005	`$EXTERNAL_NET any -> $HOME_NET any` (`to_server`)	Inbound `POST` with `http.uri` ending in `/GetStart.aspx` (`nocase`)	Flags calls to the staged `GetStart.aspx` template path (`Host W-09`)
9560006	`$EXTERNAL_NET any -> $HOME_NET any` (`to_server`)	Inbound `POST` with `http.uri` ending in `/Classic.aspx` (`nocase`)	Flags calls to the staged `Classic.aspx` template path (`Host W-09`)
9560007	`$EXTERNAL_NET [8085,8093] -> $HOME_NET any` (`to_client`)	HTTP 200 response body containing `Index of /` and `.aspx`	Flags responses from high-port open staging directories

How the Sentinel KQL, Sigma, and YARA Rules Work

The Sentinel KQL hunt unions two branches over a 7-day lookback. Replace the two sample FQDNs in `ApprovedSecurityHosts` (`app-ci-01.corp.example` , `sec-scanner-01.corp.example`) with your own scanner host list before scheduling.

The first branch checks `DeviceProcessEvents` for `ProcessCommandLine contains "--address=systemd: --nofork --nopidfile"` outside `/usr/bin/dbus-daemon` and `/bin/dbus-daemon`. It also flags `ProcessCommandLine contains "enable-linger"` with `loginctl`, `FolderPath startswith "/memfd:a"`, or `w3wp.exe` starting `cmd.exe` or PowerShell. The second branch checks `DeviceNetworkEvents` for `RemotePort in (ConsolePorts)` (**8787**, **18787**, **8444**, **18666**, **8666**, **18800**) or `RemoteUrl contains "/api/v1/tasks"`.

Host or file rule	Engine	Trigger condition
`Linux ZQAgent Non-Root Systemd User Service and Linger Persistence` (`R1`)	Sigma (`linux`)	`/loginctl` with `CommandLine|contains: 'enable-linger` `daemon-reload` (`T1543.002`)
`Linux ZQAgent Spoofed dbus-daemon Command Line Outside System Paths` (`R2`)	Sigma (`linux`)	`CommandLine|contains: '--address=systemd: --nofork` where `Image` is not `/usr/bin/dbus-daemon` or `/bin/dbus-`
`Windows IIS Worker Spawning Command Shell After ASP.NET Staging` (`R3`)	Sigma (`windows`)	`ParentImage|endswith: 'w3wp.exe'` spawning `cmd.exe`,
`ODIN_R60_ARTEX_Console_Bundle_and_Task_API` (`YARA R1`)	YARA (< 5MB)	`ARTEX - Autonomous Red-Team Expert` paired with `/api/`
`ODIN_R60_Python_WAF_Bisect_and_Matrix_Deployer` (`YARA R2`)	YARA (< 128KB)	`import requests` or `urllib.request`, `.aspx`, and `waf_b`
`ODIN_R60_ZQAgent_Memfd_and_Systemd_Template` (`YARA R3`)	YARA (< 4MB)	`Description=Device event journal daemon`, `--address=systemd: --nofork --nopidfile --systemd-`
`ODIN_R60_Agentic_Self_Labeled_Recon_Log` (`YARA R4`)	YARA (< 2MB)	`pentest-recon` paired with `csai-pentest-role` or `/api/`

9. Indicators

The Indicators tab holds **0** published blocklist IPv4 addresses and **0** file SHA-256 hashes. Candidate console IPs, open-directory host IPs, all **10** Wiz-overlapping host IPs, and staged file SHA-256 hashes are withheld under Publication Rules §1. We also withhold one **2,015**-byte web-config file name on `Host W-09` (:**8085**).

Indicator or marker group	Published in Indicators tab	Status in this report
Candidate console and open-directory host IPv4s (8,311 **30d** / 5,681 **7d**)	0	Withheld (`Publication Rules §1.3`)
Wiz-overlapping host IPv4s (10 **of** 156 **unique Wiz IPs**)	0	Withheld (8 `ARTEX` candidates, `Host W-09`, and `Host W-10` IPs and `W-10` ports)
Staged file SHA-256 digests (49 **files on** `Host W-09`)	0	Withheld (1 web-config file name on :8085 also withheld)
Behavioral, protocol, and host hunt markers	0 (text-only table below)	10 markers listed in the table below

Behavioral and Protocol Hunt Markers

Marker category	Pattern / protocol artifact	Layer	Defensive hunt & control
ARTEX icon MD5	`cd3ebd16437d6d3963592f7365dd3980`	All web ports	Scan cloud ranges for `/favicon.ico` (15,406 B) on 8787, 443, 80, and 8080.

Marker category	Pattern / protocol artifact	Layer	Defensive hunt & control
ARTEX HTML banner	`ARTEX - Autonomous Red-Team Expert`	HTTP / TLS proxy	Alert on exposed home panels with `sid:9560001`. Put approved panels behind mTLS.
ARTEX task API	`POST /api/v1/tasks`	HTTP / TLS egress	Alert on outbound calls (`sid:9560002`) and Sentinel `DeviceNetworkEvents`.
Agentic User-Agent	`pentest-recon`	HTTP / WAF ingress	Hunt WAF and IdP logs (`[REF-02]`). Rule `sid:9560003` flags visible headers.
CyberStrikeAI banner	`CyberStrikeAI`	8444, 18666, 8080	Sweep external assets and alert on exposed home responses (`sid:9560004`).
Staged ASP.NET path A	`/GetStart.aspx`	IIS / WAF ingress	Staged (3,932 B) on `Host W-09` (:8093). Alert on `POST` calls (`sid:9560005`).
Staged ASP.NET path B	`/Classic.aspx` (with `Photos.aspx`)	IIS / WAF ingress	Staged (463 B) on `Host W-09` (:8093). Alert with `sid:9560006` and Sigma R3.
Directory index	`Index of /` (`.aspx` + `.py`)	`TCP 8085 / 8093`	Alert on high-port file indexes (`sid:9560007`) and block high-port egress.
ZQAgent `memfd` spoof	`/memfd:a (deleted)` + `dbus-daemon`	Linux EDR	NVISO `23 Nov` report (`[REF-04]`). Hunt with Sentinel KQL and Sigma R2.
ZQAgent `systemd` unit	`Description=Device event journal daemon`	Linux `systemd`	NVISO `23 Nov` report (`[REF-04]`). Check `enable-linger` with Sigma R1 and YARA R3.

10. Scope and Limits

Odin by Brandefense studied autonomous testing console counts and open-directory listings during a two-week observation window ending `24 November 2026`. Rolling **30**-day (**8,311**) and trailing **7**-day (**5,681**, `18-24 November 2026`) counts cover seven tools (`ARTEX` , `CyberStrikeAI` , `PentAGI` , `HexStrikeAI` , `AutoCVE` , `AutoHunter` , and `BrainstormV2`). Newly observed `20-24 November 2026` counts (**1,073**) cover four tallied tools (`ARTEX` , `CyberStrikeAI` , `AutoHunter` , and `PentAGI`). Port and country counts reflect top-six sampled subsets (`n = 1` to **196**).

Overlap counts (**10** of **156** unique IPv4s) come from an aggregate summary against the two cited Wiz Research `23 November 2026` IOC files (`[REF-02]` , `[REF-05]`). Those files list **74** unique IPv4s in the agentic-attacks CSV and **82** in the `Black October` CSV, while the row-level comparison is unavailable for independent verification.

A missing console match across the remaining **146** Wiz IPv4s (**93.6%**) does not classify their roles (`Other Wiz IP Types Unclassified`). Staged files on `Host W-09` (**36** on :**8085** and **13** on :**8093**, seen `13-20 November 2026`) show prep rather than verified victim impact.

All `ZQAgent` details come from NVISO Labs (`23 November 2026` , `[REF-04]`) and were not seen on `Host W-09`. All candidate console IPs, open-directory IPs, overlap host IPs, `Host W-10` 's ports, and one **2,015**-byte web-config file name on `Host W-09` are withheld.

11. Sources

1. `[REF-01]` FBI Cyber Division, *FLASH-20261113-001: Malicious Use of Autonomous Penetration Testing Tool ARTEX* (13 November 2026; verified on 24 November 2026).
2. `[REF-02]` Wiz Research, *Agentic Attacks in the Wild: ARTEX & Offensive AI Frameworks* (23 November 2026; verified on 24 November 2026).
3. `[REF-03]` Wiz Research, *ARTEX in the Wild: Storm-0940 Expands Targeting of IT and Software Vendors* (22 October 2026; verified on 24 November 2026).
4. `[REF-04]` NVISO Labs, *ARTEX Leads to Persistent ZQAgent Backdoor* (23 November 2026; verified on 24 November 2026).
5. `[REF-05]` Wiz Research, *Wiz Research Public IOC Repository (Agentic Attacks in the Wild & Black October CSVs)* (23 November 2026; verified on 24 November 2026).

6. [REF-06] Help Net Security, *ARTEX Goes from Pentesting Tool to Attacker Staple in Three Months* (9 November 2026; verified on 24 November 2026).
7. [REF-07] MITRE ATT&CK, *Exploit Public-Facing Application (T1190)* (verified on 24 November 2026).
8. [REF-08] MITRE ATT&CK, *Server Software Component: Web Shell (T1505.003)* (verified on 24 November 2026).
9. [REF-09] MITRE ATT&CK, *Reflective Code Loading (T1620)* (verified on 24 November 2026).
10. [REF-10] MITRE ATT&CK, *Create or Modify System Process: Systemd Service (T1543.002)* (verified on 24 November 2026).

BRANDEFENSE CAPABILITIES RELATED TO THIS RESEARCH

Cyber Threat Intelligence

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

Odin, the Agentic Analyst

AI that investigates for your team, on your data.

External Attack Surface

Find exposed services before automated tools reach them.

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_artex_console_and_staging_artifacts.yar** 70 lines

```
/*
   Odin by Brandefense - Monograph 60 YARA Suite
   4 filesize-bounded structural rules covering exposed ARTEX console bundles,
   Python WAF-bisect/matrix staging scripts, ZQAgent persistence templates, and agentic recon logs.
*/

rule ODIN_R60_ARTEX_Console_Bundle_and_Task_API
{
    meta:
        author = "Odin by Brandefense"
        monograph = "60"
        description = "Detects exposed ARTEX autonomous testing console bundles and task API definitions"
        date = "2026-11-24"
    strings:
        $a1 = "ARTEX - Autonomous Red-Team Expert" ascii
        $a2 = "/api/v1/tasks" ascii
        $a3 = "artex-swarm-root" ascii
    condition:
        filesize < 5MB and $a1 and ($a2 or $a3)
}

rule ODIN_R60_Python_WAF_Bisect_and_Matrix_Deployer
{
    meta:
        author = "Odin by Brandefense"
        monograph = "60"
        description = "Detects structural Python HTTP WAF-bisection and ASP.NET matrix verification scripts"
        date = "2026-11-24"
    strings:
        $p1 = "import requests" ascii
        $p2 = "urllib.request" ascii
        $m1 = "waf_bisect" ascii
        $m2 = "fill_matrix" ascii
        $m3 = "write_classic" ascii
        $x1 = ".aspx" ascii nocase
    condition:
        filesize < 128KB and ($p1 or $p2) and $x1 and ($m1 or $m2 or $m3)
}

rule ODIN_R60_ZQAgent_Memfd_and_Systemd_Template
{
    meta:
        author = "Odin by Brandefense"
        monograph = "60"
        description = "Detects ZQAgent systemd persistence unit strings and spoofed dbus-daemon runtime markers"
        date = "2026-11-24"
    strings:
        $z1 = "Description=Device event journal daemon" ascii
        $z2 = "--address=systemd: --nofork --nopidfile --systemd-activation" ascii
        $z3 = "enable-linger" ascii
        $z4 = "memfd" ascii
    condition:
        filesize < 4MB and $z1 and $z2 and ($z3 or $z4)
}

rule ODIN_R60_Agentic_Self_Labeled_Recon_Log
{
    meta:
        author = "Odin by Brandefense"
        monograph = "60"
        description = "Detects agentic offensive framework self-labeling strings across exposed task logs"
        date = "2026-11-24"
```

```
    strings:
        $r1 = "pentest-recon" ascii nocase
        $r2 = "csai-pentest-role" ascii nocase
        $r3 = "/api/v1/tasks" ascii
    condition:
        filesize < 2MB and ($r1 and ($r2 or $r3))
}
```

Suricata **odin_artex_console_staging_and_recon_hunt.rules** 11 lines

```
# Odin by Brandefense - Monograph 60 Suricata 7.x Ruleset (sid:9560001-9560007)
# Syntax-checked with Odin Suricata linter (0 problems); requires HTTP or TLS proxy visibility.

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R60. Exposed ARTEX Banner"; flow:established,to_client; http.response_body;
content:"ARTEX - Autonomous Red-Team Expert"; fast_pattern; classtype:trojan-activity; sid:9560001; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R60. ARTEX Task API"; flow:established,to_server; http.method; content:"POS
T"; bsize:4; http.uri; content:"/api/v1/tasks"; startswith; fast_pattern; classtype:trojan-activity; sid:9560002; rev:1;)
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-R60. Agentic Recon UA"; flow:established,to_server; http.user_agent; conten
t:"pentest-recon"; nocase; fast_pattern; classtype:attempted-recon; sid:9560003; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R60. CyberStrikeAI Banner"; flow:established,to_client; http.response_body;
content:"CyberStrikeAI"; fast_pattern; classtype:trojan-activity; sid:9560004; rev:1;)
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-R60. Staged GetStart"; flow:established,to_server; http.method; content:"PO
ST"; bsize:4; http.uri; content:"/GetStart.aspx"; endswith; nocase; fast_pattern; classtype:web-application-attack; sid:9560005; re
v:1;)
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-R60. Staged Classic"; flow:established,to_server; http.method; content:"POS
T"; bsize:4; http.uri; content:"/Classic.aspx"; endswith; nocase; fast_pattern; classtype:web-application-attack; sid:9560006; rev:
1;)
alert http $EXTERNAL_NET [8085,8093] -> $HOME_NET any (msg:"ODIN-R60. Staging Index"; flow:established,to_client; http.stat_code; co
ntent:"200"; bsize:3; http.response_body; content:"Index of /"; fast_pattern; content:".aspx"; classtype:bad-unknown; sid:9560007; r
ev:1;)
```

Show full rule

Sentinel KQL **sentinel_artex_console_zqagent_and_staging_hunt.kql** 26 lines

```
// Odin by Brandefense - Monograph 60
// Hunts ZQAgent memfd/systemd persistence, IIS web-shell spawns, and outbound console port calls.
let Lookback = 7d;
let ApprovedSecurityHosts = dynamic(["app-ci-01.corp.example", "sec-scanner-01.corp.example"]);
let ConsolePorts = dynamic([8787, 18787, 8444, 18666, 8666, 18800]);
let HostPersistenceAndWebShells =
    DeviceProcessEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedSecurityHosts))
    | where (
        (ProcessCommandLine contains "--address=systemd: --nofork --nopidfile" and not(FolderPath in ("/usr/bin/dbus-daemon", "/bin/
dbus-daemon")))
        or (ProcessCommandLine contains "enable-linger" and ProcessCommandLine has "loginctl")
        or (FolderPath startswith "/memfd:a")
        or (InitiatingProcessFileName =~ "w3wp.exe" and FileName in~ ("cmd.exe", "powershell.exe", "pwsh.exe"))
    )
    | project Timestamp, DeviceName, AccountName, SignalType = "HostPersistenceOrWebShell", Detail = ProcessCommandLine;
let OutboundConsoleCalls =
    DeviceNetworkEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedSecurityHosts))
    | where RemotePort in (ConsolePorts) or RemoteUrl contains "/api/v1/tasks"
    | project Timestamp, DeviceName, AccountName = InitiatingProcessAccountName, SignalType = "AutonomousConsoleEgress", Detail = st
rcat(InitiatingProcessFileName, " -> ", RemoteIP, ":", tostring(RemotePort));
union HostPersistenceAndWebShells, OutboundConsoleCalls
| summarize FirstSeen = min(Timestamp), LastSeen = max(Timestamp), EventCount = count(), Signals = make_set(SignalType, 5), SampleDe
tails = make_set(Detail, 5) by DeviceName, AccountName
| order by LastSeen desc
```

Sigma **sigma_artex_zqagent_memfd_and_iis_webshell.yml** 87 lines

```
title: Linux ZQAgent Non-Root Systemd User Service and Linger Persistence
id: 60a4d912-8b31-4e72-9c10-60b20f84d601
status: experimental
description: Detects Linux command lines enabling systemd user linger or user service units associated with ZQAgent persistence.
author: Odin by Brandefense
date: 2026-11-24
logsource:
  category: process_creation
  product: linux
detection:
  selection_linger:
    CommandLine|contains: 'enable-linger'
    Image|endswith: '/loginctl'
  selection_user_unit:
    Image|endswith: '/systemctl'
    CommandLine|contains: '--user'
  selection_enable:
    CommandLine|contains:
      - 'enable '
      - 'daemon-reload'
  filter_approved_hosts:
    ComputerName:
      - 'app-ci-01.corp.example'
  condition: (selection_linger or (selection_user_unit and selection_enable)) and not filter_approved_hosts
falsepositives:
  - Approved Linux developer or container hosts configuring rootless Podman or user-scoped systemd units
level: high
tags:
  - attack.persistence
  - attack.t1543.002
---
title: Linux ZQAgent Spoofed dbus-daemon Command Line Outside System Paths
id: 60a4d912-8b31-4e72-9c10-60b20f84d602
status: experimental
description: Detects processes spoofing the ZQAgent dbus-daemon session arguments while running from non-standard or memfd paths.
author: Odin by Brandefense
date: 2026-11-24
logsource:
  category: process_creation
  product: linux
detection:
  selection_cmdline:
    CommandLine|contains: '--address=systemd: --nofork --nopidfile --systemd-activation --syslog-only'
  filter_real_dbus:
    Image:
      - '/usr/bin/dbus-daemon'
      - '/bin/dbus-daemon'
  filter_approved_hosts:
    ComputerName:
      - 'app-ci-01.corp.example'
  condition: selection_cmdline and not filter_real_dbus and not filter_approved_hosts
falsepositives:
  - Custom container root filesystems mounting dbus-daemon at non-standard immutable paths
level: critical
tags:
  - attack.defense-evasion
  - attack.t1620
  - attack.t1036.004
---
title: Windows IIS Worker Spawning Command Shell After ASP.NET Staging
id: 60a4d912-8b31-4e72-9c10-60b20f84d603
status: experimental
description: Detects IIS w3wp.exe spawning cmd.exe or PowerShell consistent with ASP.NET web-shell handlers staged on multi-port wor
kbenches.
author: Odin by Brandefense
date: 2026-11-24
logsource:
  category: process_creation
  product: windows
detection:
```

```
  selection_parent:
    ParentImage|endswith: '\w3wp.exe'
  selection_child:
    Image|endswith:
      - '\cmd.exe'
      - '\powershell.exe'
      - '\pwsh.exe'
  filter_build_hosts:
    ComputerName:
      - 'iis-build-01.corp.example'
  condition: selection_parent and selection_child and not filter_build_hosts
falsepositives:
  - Legacy internal IIS administrative portals invoking approved maintenance scripts
level: high
tags:
  - attack.persistence
  - attack.t1505.003
```

