ODIN

TLP:CLEAR

ODIN RESEARCH · MONOGRAPH 54 / 30 · OPERATIONS

Operation NightShift

Enterprise Middleware Intrusion, Off-Hours Mining, and SEO Cloaking

Inside an operator's 1,580-entry workbench, returned outputs from three environments, active November transfer logs, and dual monetization

Two-week observation window ending 20 November 2026 · Prepared November 2026
Full Report · Public edition · Version 1.1

1,580
Non-mirrored directory entries across the four primary HTTP ports on 38.60.227[.]210 (1,561 unique paths and 895 unique SHA-256 digests).

602.61 MB
Total byte volume across the 1,090 sized files (602,605,284 bytes; 490 entries omit byte size in listings).

3
Distinct affected target environments confirmed by returned output stores (Windows/IIS, Oracle E-Business Suite, and higher education).

505
Captured command outputs inside the 466-entry Windows and IIS store on TCP 8000 (201 sized files, 326,376 bytes).

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

Inside an operator's 1,580-entry workbench, returned outputs from three environments, active November transfer logs, and dual monetization

01	Executive Summary	04
02	Operational Scope, Multi-Port Inventory, and Monograph 03 Update	07
03	Middleware Pivoting, Fileless Persistence, and Returned Target Outputs	11
04	Dual Monetization: Night-Shift Mining, Rival Eviction, and Search-Bot Cloaking	15
05	Exposure Analysis Across Enterprise Middleware	18
06	Alternative Hypotheses	20
07	What Defenders Should Do	22
08	Detection Rules	24
09	Indicators	26
10	Scope and Limits	29
11	Sources	31
A	Indicators of compromise (9)	33
B	Detection rules (4 files)	34

IN SHORT

Operation NightShift links enterprise middleware intrusion across Oracle E-Business Suite, Zimbra, and Windows IIS servers with off-hours Monero mining and search-bot SEO spam scripts. Odin by Brandefense analyzed the multi-port workbench on 38.60.227[.]210 during a two-week observation window ending 20 November 2026. The server exposed 1,580 entries and returned outputs from three affected environments. Audit Oracle database links, enforce Microsoft Defender Tamper Protection, hunt Linux anonymous-memory loaders paired with lock files, and block the three operator hosts.

01

CHAPTER 01

Executive Summary

IN SHORT

Operation NightShift links enterprise middleware intrusion across Oracle E-Business Suite, Zimbra, and Windows IIS servers with off-hours Monero mining and search-bot SEO spam scripts. Odin by Brandefense analyzed the multi-port workbench on 38.60.227[.]210 during a two-week observation window ending 20 November 2026. The server exposed 1,580 entries and returned outputs from three affected environments. Audit Oracle database links, enforce Microsoft Defender Tamper Protection, hunt Linux anonymous-memory loaders paired with lock files, and block the three operator hosts.

INSIDE THIS CHAPTER

Three Decisions for Leaders 04

The Study in Numbers 05

01 Executive Summary

Security teams often treat enterprise database lateral movement and compute or search-spam monetization as separate threat categories. High-end intrusion groups are expected to pursue data theft or extortion. Cryptomining and search-spam crews are assumed to rely on opportunistic web exploits. Defenders can use cyber threat intelligence to connect this middleware intrusion with the mining and search-spam scripts on the operator's server.

Odin by Brandefense analyzed the expanded workbench at 38.60.227[.]210 during the two-week window ending 20 November 2026. The analysis also covered check-in host 38.60.252[.]110 and TLS proxy 38.54.14[.]162.

Monograph 03 covered the static scripts on this server during an earlier four-day window. Adding the four-port directory inventory and returned target stores turns that toolkit study into an operation profile. All victim output paths, log filenames, disk serials, database schemas, and institution names are withheld.

1. **Returned outputs confirm activity across at least three distinct target environments.**
   Across four primary HTTP ports on 38.60.227[.]210 (plus a fifth mirror port), the server exposed 1,580 entries and 895 unique file digests. Two withheld stores hold returned outputs from affected targets rather than outbound tools.

One store holds 505 captured command outputs from a Windows and IIS server environment. A second store holds 22 Oracle E-Business Suite job outputs and 4 higher-education database outputs.

2. **An active upload receiver logged chunked host dumps through 20 November 2026.**
   On TCP port 8093, an upload receiver held 382 entries. These include 380 chunk and recon items plus two transfer logs totaling 3.90 megabytes.

Those logs record active callbacks between 6 November and 20 November 2026. Recorded transfers include seven-part dumps of roughly one megabyte plus status, network, host, key, memory-agent, rollback, and self-check reports.

3. **Staged scripts pair off-hours mining and search-bot cloaking with rival eviction.**
   Instead of deploying noisy ransomware, the scripts are built to extract steady value from multi-core servers without daytime alerts. One staged track is designed to sweep rival miners every two minutes and run a disguised Monero miner between 22:00 and 06:00 local time. A second staged track holds PHP prepend hooks designed to show normal pages to people while feeding spam to search bots.

4. **Public research links the server to post-exploitation behind Ivanti Connect Secure flaws.**
   On 3 November 2026, Etugen Research noted 38.60.227[.]210 in post-exploitation activity behind Ivanti Connect Secure authentication bypass intrusions. Etugen separated this operator from the tracked group UTA0576. Our 1,580 directory entries hold post-exploitation tools rather than the perimeter exploit code itself.

Three Decisions for Leaders

1. **Treat database links and collaboration servers as lateral boundaries.** Audit Oracle database links, revoke unneeded remote job privileges, and use external attack surface management to find exposed Zimbra and VPN appliances for patching.

2. **Pair host tamper protection with off-hours CPU and egress checks.** Enable Microsoft Defender Tamper Protection on Windows Server, hunt Linux memory-only loaders paired with lock files, and inspect 22:00 to 06:00 CPU spikes.
3. **Audit web prepend settings and block operator infrastructure.** Check PHP configurations and IIS modules for unauthorized prepend hooks, and block the operator addresses, cloud buckets, and spam feeds in Chapter 9.

The Study in Numbers

Number	What it is
1,580	Non-mirrored directory entries across the four primary HTTP ports on `38.60.227[.]210` (1,561 unique paths and 895 unique SHA-256 digests).
602.61 MB	Total byte volume across the 1,090 sized files (602,605,284 bytes; 490 entries omit byte size in listings).
3	Distinct affected target environments confirmed by returned output stores (Windows/IIS, Oracle E-Business Suite, and higher education).
505	Captured command outputs inside the 466-entry Windows and IIS store on TCP 8000 (201 sized files, 326,376 bytes).
26	Returned database output files on TCP 8083 (22 Oracle E-Business Suite job outputs plus 4 higher-education database outputs, 2,486 bytes).
382	Entries in the active TCP 8093 upload receiver (380 items plus two transfer logs totaling 3.90 MB, active 6 to `20 November 2026`).
10	Published network and file indicators (3 operator IPv4 hosts and 7 SHA-256 digests), plus 6 report-only cloud, domain, and host markers.

02

CHAPTER 02

Operational Scope, Multi-Port Inventory, and Monograph 03 Update

IN SHORT

Operation NightShift runs from a multi-port virtual private server at 38.60.227[.]210 (LIGHT NODE). That server connects to a host-profiling listener at 38.60.252[.]110:8900 and a custom TLS proxy at 38.54.14[.]162:5556 (wa.theshyc[.]xyz).

INSIDE THIS CHAPTER

Reconciling the Monograph 03 Snapshot with the Four-Port Inventory 07

Update on Public Correlation (`CVE-2026-104935`) 09

02 Operational Scope, Multi-Port Inventory, and Monograph 03 Update

Operation NightShift runs from a multi-port virtual private server at `38.60.227[.]210` (`LIGHT NODE`). That server connects to a host-profiling listener at `38.60.252[.]110:8900` and a custom TLS proxy at `38.54.14[.]162:5556` (`wa.theshyc[.]xyz`).

Two public cloud buckets support payload delivery. Cloudflare R2 (`pub-307c565a487b43c5bee73d21edc4d83b.r2[.]dev`) serves mining archives, and Alibaba Cloud OSS (`imagefiles-backup.oss-ap-southeast-7.aliyuncs[.]com`) serves Windows modules. Figure 1 maps the four operational tracks across this infrastructure.

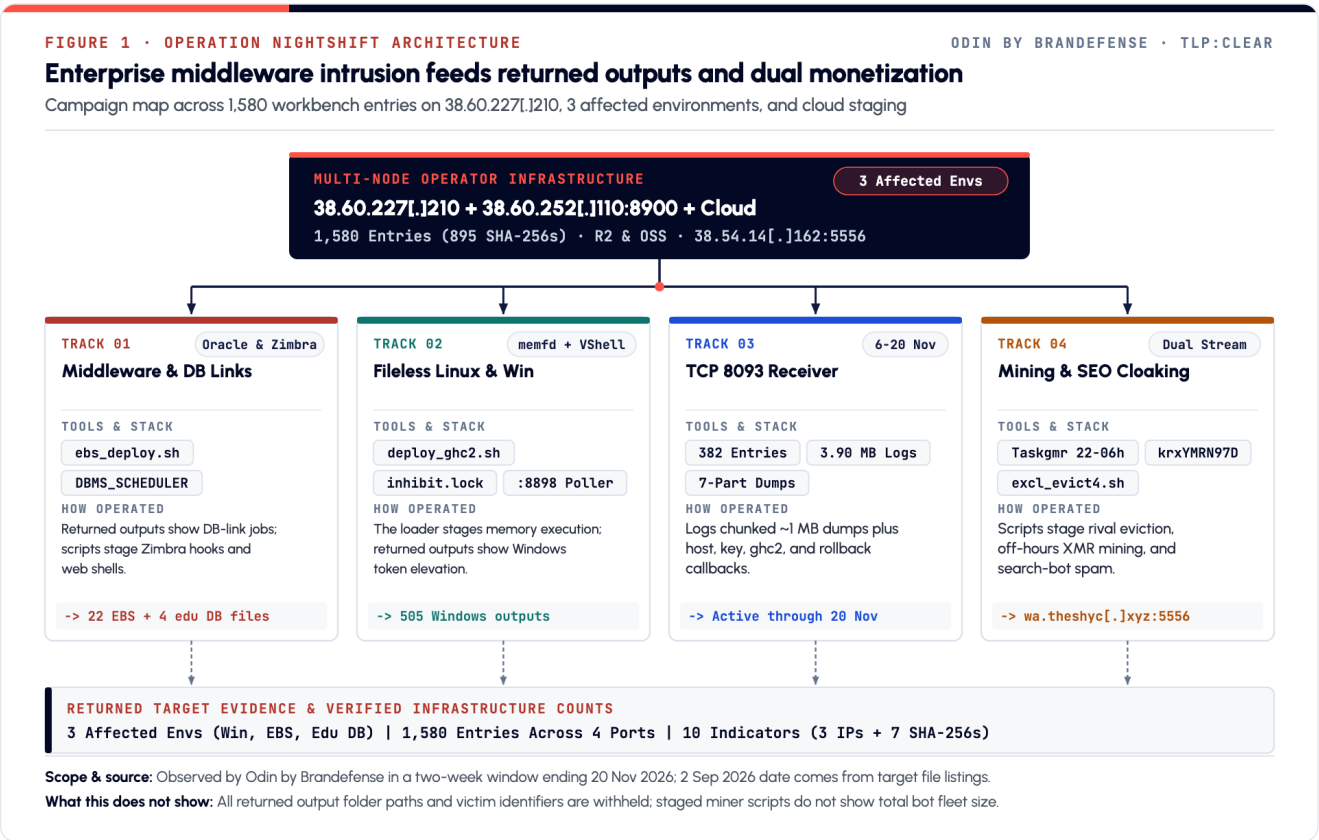


Figure 1: Enterprise middleware intrusion feeds returned outputs and dual monetization

Reconciling the Monograph 03 Snapshot with the Four-Port Inventory

Monograph 03 examined an initial snapshot of `38.60.227[.]210` collected from 13 to 16 November 2026. That snapshot held 1,824 raw rows across five HTTP ports (8000, 8082, 8083, 8093, and 9002). TCP 9002 mirrored TCP 8000 (645 rows then), and 8 paths overlapped across ports. That left 1,171 unique paths alongside 99 retrieved script and config files (94 unique SHA-256 digests).

Continued observation through `20 November 2026` recorded new returned outputs and receiver uploads across the primary ports. Without the 9002 mirror, the four primary ports (8000, 8082, 8083, and 8093) hold **1,580 entries** and **1,561 unique paths**. Those entries map to **895 unique SHA-256 digests**. Within the 1,580 entries, 1,090 sized files total **602,605,284 bytes (602.61 MB)**, while 490 entries omit byte size.

Primary TCP port	Total entries	Sized files	Unsized entries	Sized volume (bytes)	Unique SHA-256	Scripts	Text & logs	Binaries	Archives	Other	Primary operational role
TCP 8000 (mirrored on 9002)	952	685	267	202,846,214	625	198	666	38	2	48	Linux/ Windows staging, miners, SEO cloakers, and returned Windows outputs.
TCP 8082	144	144	0	391,617,257	128	19	26	50	8	41	Fileless `github-c2-agent-dual` binaries, Linux LPE archives, and Windows tools.
TCP 8083	102	91	11	122,152	89	62	4	1	1	34	Oracle EBS DB-link scripts, Zimbra persistence, and returned DB outputs.
TCP 8093	382	170	212	8,019,661	151	0	113	212	57	0	Active chunked upload receiver and transfer logs (`6-20 Nov 2026`).
Combined 4-port total	**1,580**	**1,090**	**490**	**602,605,284**	**895** (cross-port)	**279**	**809**	**301**	**68**	**123**	**Full non-mirrored Operation NightShift inventory.**

Figure 5 shows how returned outputs and receiver uploads place 84.4% of all entries (1,334 of 1,580) onto TCP 8000 and TCP 8093. Meanwhile, TCP 8082 holds 65.0% of sized byte volume (391.62 MB) through compiled agents and post-exploitation binaries.

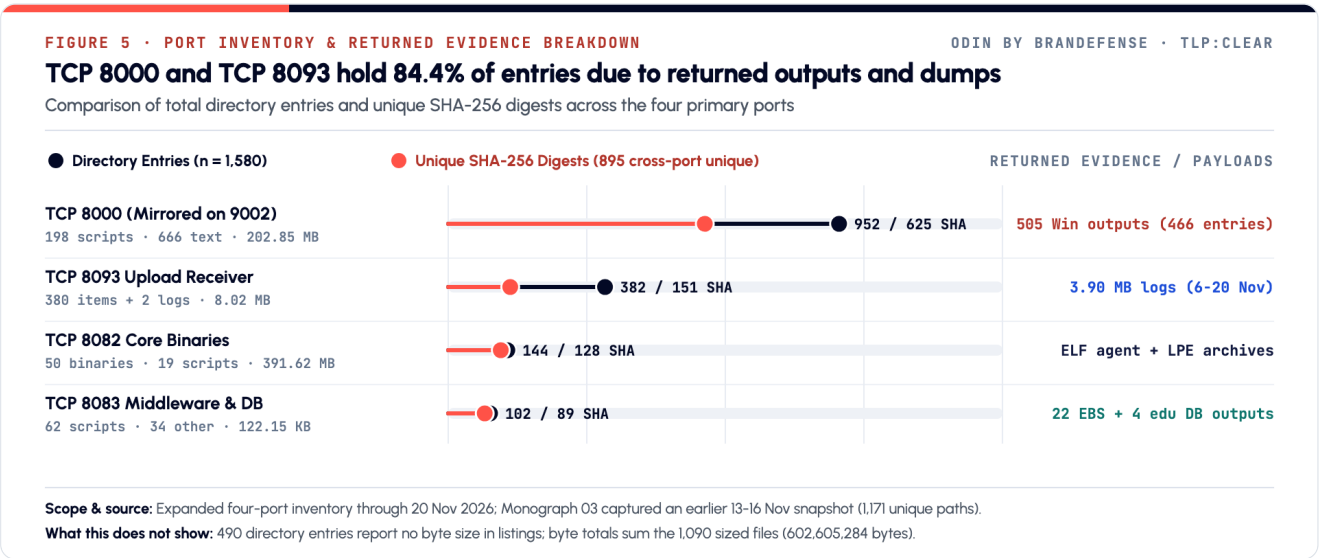


Figure 5: TCP 8000 and TCP 8093 hold 84.4% of entries due to returned outputs and dumps

Update on Public Correlation (`CVE-2026-104935`)

Monograph 03 reported zero hits across five threat-intelligence sources checked on `16 November 2026`. Broader web correlation identified a `3 November 2026` post by Etugen Research (`[REF-01]`). That post studied Ivanti Connect Secure authentication bypass flaw `CVE-2026-104935` (`[REF-02]`, `CWE-290`, CVSS 8.6).

NVD lists affected `25.1.0.0-25.1.1.1`, `25.1.2.0-25.1.2.2`, and `22.8R2-22.8R2.4`. Ivanti lists `25.1.1.2`, `25.1.3.0`, and `22.8R2.5` as fixes for this CVE; `22.7R2.14` and earlier are unaffected.

Two facts keep that correlation accurate.

- **Distinct from `UTA0576`.** Etugen documented `38.60.227[.]210` (staging `VShell`, `Mimikatz`, and Garble binaries) as a **separate actor** distinct from `UTA0576` (`[REF-01]`).
- **Second-stage role.** None of the 1,580 directory entries on `38.60.227[.]210` holds an Ivanti exploit script. The host serves post-exploitation persistence, lateral movement, and monetization scripts after initial entry.

CHAPTER 03

Middleware Pivoting, Fileless Persistence, and Returned Target Outputs

INSIDE THIS CHAPTER

Windows and IIS Post-Exploitation Outputs 12
Oracle Database-Link Pivoting and Zimbra Persistence 12
Fileless Linux Staging and Active November Receiver Logs 13

03 Middleware Pivoting, Fileless Persistence, and Returned Target Outputs

Withheld directories on `38.60.227[.]210` hold returned command outputs, database job logs, and active upload records from affected environments. Because `38.60.227[.]210` is a public indicator, all output folder names and log filenames are withheld. Disk serials, database schemas, and institution names are also withheld under Odin Publication Rules.

Stream	Anonymized environment / stream	Port	Entries	Sized files	Sized bytes	Captured units	Recorded dates	Observed mechanics
Environment 1	Windows and IIS Server Environment	8000	466	201	326,376	505 cmd outputs	Target file dates `2 Sep 2026`; observed `Nov 2026`	Defender Real-Time Monitoring tamper attempts, `CreateProcessAsUser` elevation, IIS module staging, and Alibaba OSS pulls.
Environment 2	Enterprise Oracle E-Business Suite Environment	8083	22	22	2,349	22 job outputs	Observed `Nov 2026`	`DBMS_SCHEDULER` OS job outputs returned across Oracle database links (`EXEC_DDL_STATEMENT@` / `CREATE_JOB@`).
Environment 3	Higher-Education Database Environment	8083	4	4	137	4 DB outputs	Observed `Nov 2026`	Separate institutional database output files returned to TCP 8083 (`22 + 4 = 26` DB outputs, 2,486 B).
Receiver Logs	Active Upload Receiver Store	8093	382	170	8,019,661	380 items + 2 logs	`6 Nov` to `20 Nov 2026`	Two transfer logs (3,887,512 B + 13,180 B = 3,900,692 B) logging 7-part ~1 MB dumps plus host, key, `ghc2`, and rollback callbacks.

Figure 3 separates steps backed by returned outputs and `6-20 November` receiver logs (solid arrows) from staged monetization scripts (dashed arrows).



Figure 3: Middleware access enables returned host dumps alongside off-hours monetization

Windows and IIS Post-Exploitation Outputs

A withheld directory on TCP 8000 holds 466 entries (201 sized files totaling 326,376 bytes) from one Windows and IIS environment. A consolidated transcript inside that store holds **505 command outputs**. Target directory listings in those outputs carry file dates of `2 September 2026`. Those dates reflect either older files on the target or access before November.

Those 505 outputs record four operator steps.

1. **Defender tamper attempts.** PowerShell commands run `Set-MpPreference -DisableRealtimeMonitoring $true` and add path exclusions (`[REF-10]`).
2. **Token elevation.** Privilege escalation via `CreateProcessAsUser()` (`OK` logged in console output) steps up from IIS worker pools (`w3wp.exe`) to `SYSTEM`.
3. **Alibaba OSS payload pulls.** Outbound HTTPS fetches download modules from `imagefiles-backup.oss-ap-southeast-7.aliyuncs[.]com`.
4. **IIS module deployment.** Scripts register native or managed IIS modules alongside encoded PowerShell web-shell requests (`?c=powershell ... -enc`).

Oracle Database-Link Pivoting and Zimbra Persistence

On TCP 8083, 62 middleware scripts sit beside a withheld folder holding 26 returned database output files (2,486 bytes). Twenty-two files (2,349 bytes) come from an enterprise **Oracle E-Business Suite (EBS) and RAC** environment. The other 4 files (137 bytes) come from a **higher-education database environment**.

The script `ebs_deploy.sh` (4,199 bytes, 63 lines) crosses internal network boundaries without SSH brute force. Enterprise ERP systems often keep pre-authenticated Oracle database links (`DB_LINK`) across production, reporting, and standby instances. The script queries link tables and calls `DBMS_UTILITY.EXEC_DDL_STATEMENT@` and `DBMS_SCHEDULER.CREATE_JOB@` to schedule OS commands on linked database hosts (`[REF-06]`). Those remote jobs pull loaders from `38.60.227[.]210` and return output to TCP 8083.

Companion scripts target **Zimbra Collaboration Suite** (`CVE-2026-73570`, `[REF-03]`, CVSS 8.9, unauthenticated command injection before `10.1.20` when optional `zimbra-snmp` is installed and SNMP notifications are enabled). Other scripts target **Ahsay Backup** and **Pentaho**. For Zimbra servers, staged scripts `persist.sh` and `ops.sh` edit `.swatchrc` under the `zimbra` account (tagged `z_73570_ok`). That hook is built to run a 45-second `curl` poller against `38.60.227[.]210:8898` (`/ping/`, `/c/`, and `/o/`).

Fileless Linux Staging and Active November Receiver Logs

For Linux servers where `/tmp` may carry `noexec`, the staged script `deploy_ghc2.sh` (5,796 bytes, 156 lines) is built to load its payload from memory (`[REF-07]`).

- **Kernel `flock` mutex.** The script acquires a non-blocking lock on `/var/tmp/.systemd/inhibit.lock` (with two fallback paths) so cron runs do not start duplicate agents.
- **Verified `memfd_create` loader.** It downloads `github-c2-agent-dual` from `38.60.227[.]210:8082` and checks its exact SHA-256 digest. It then loads the ELF binary into anonymous memory via Python or Perl `memfd_create` (`/proc/self/fd/N`).
- **Fallback `VShell` and LPE archives.** Companion script `vsdeploy.sh` tests `/tmp`, `$HOME/.cache`, `/dev/shm`, and `$HOME` for executable mounts before dropping a `VShell` client (:13574). Archives for `CVE-2021-3156` (`sudo` before `1.9.5p2`, `[REF-04]`) and `CVE-2021-4034` (`polkit` `pkexec`, `[REF-05]`) also sit on TCP 8082.

On **TCP 8093**, 382 entries (8,019,661 sized bytes) include 380 uploaded items and two transfer logs. Those two logs measure 3,887,512 B and 13,180 B, totaling 3,900,692 B (3.90 MB). They record active callbacks from **`6 November` (`20:32 UTC`) through `20 November 2026`**. Logged callbacks include seven-part dumps (~1 MB) plus host status, network tables, keys, `ghc2` checks, rollback notices, and self-checks.

CHAPTER 04

Dual Monetization: Night-Shift Mining, Rival Eviction, and Search-Bot Cloaking

IN SHORT

Rather than deploying ransomware that causes immediate outages, Operation NightShift stages two quiet revenue modules for multi-core servers and trusted web domains. Figure 4 shows the four-port server layout.

INSIDE THIS CHAPTER

Rival Eviction (`excl_evict4.sh`) and 22:00-06:00 Mining (`install_user.sh`) 15

Search-Bot Conditional SEO Spam Cloaking (`z_prepend.php` and `wbi_v10.php`) 16

04 Dual Monetization: Night-Shift Mining, Rival Eviction, and Search-Bot Cloaking

Rather than deploying ransomware that causes immediate outages, Operation NightShift stages two quiet revenue modules for multi-core servers and trusted web domains. Figure 4 shows the four-port server layout. Figure 2 maps all five operational layers to defender controls.

FIGURE 4 · MULTI-PORT WORKBENCH & RECEIVER BLUEPRINT — ODIN BY BRANDEFENSE · TLP:CLEAR

Four primary ports separate payload staging from returned target outputs

Cut-away of 38.60.227[.]210 (1,580 entries, 602.61 MB across sized files) and linked nodes



Scope & source: Observed by Odin by Brandefense in a two-week window ending 20 Nov 2026; callbacks also reference 8898, 8899, 9001, 13574.
What this does not show: Victim output folder names, console log filenames, disk serials, and schema names are withheld.

Figure 4: Four primary ports separate payload staging from returned target outputs

Rival Eviction (`excl_evict4.sh`) and 22:00-06:00 Mining (`install_user.sh`)

Exposed middleware servers often draw rival attackers. The operator pairs `excl_evict4.sh` (7,153 bytes, 131 lines) with `install_user.sh` (16,351 bytes, 425 lines) to claim off-hours CPU resources (`[REF-08]`).

- **Two-minute rival sweep.** The staged script `excl_evict4.sh` is built to scan `/proc`, `/tmp`, `/var/tmp`, `/dev/shm`, crontabs, and `systemd` units every 120 seconds. It kills rival miners (`xmrig`, `kinsing`, and `kdevtmpfsi`) while keeping operator markers (`.sysjvd`, `java_update`, `z_73570`, `38.60.227[.]210`, and :8899). It then posts status reports to `38.60.227[.]210:8899`.
- **R2 delivery and night-shift throttling.** The installer `install_user.sh` beacons to `38.60.252[.]110:8900/GEO_TOP_` and pulls mining bundles from Cloudflare R2 (`pub-307c565a487b43c5bee73d21edc4d83b.r2[.]dev`). It stages the miner as `Taskgmr` (with `WinRing0` on Windows) under pool prefix `krxYMRN97D`. Wrapper rules limit daytime CPU load and ramp threads between **22:00 and 06:00 local time** via TLS proxy `wa.theshyc[.]xyz:5556` (`38.54.14[.]162:5556`). Staged scripts do not show how many hosts mined at once.

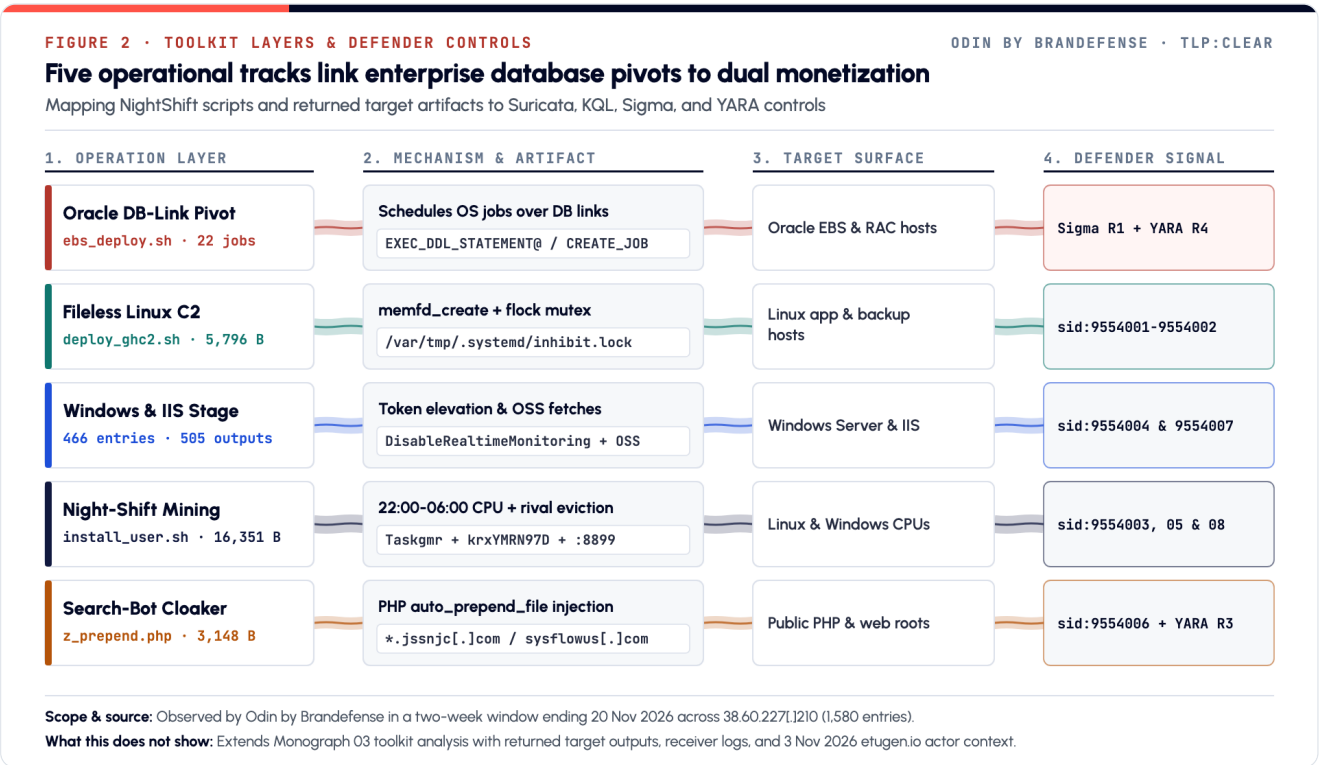


Figure 2: Five operational tracks link enterprise database pivots to dual monetization

Search-Bot Conditional SEO Spam Cloaking (`z_prepend.php` and `wbi_v10.php`)

Corporate and university web servers carry strong search-engine trust. Staged scripts `z_prepend.php` (3,148 bytes, 58 lines) and `wbi_v10.php` (3,655 bytes, 74 lines) are built to abuse that web reputation without alerting staff.

- **Clean pages for human visitors.** Loaded via PHP `auto_prepend_file` in `.htaccess`, `.user.ini`, or `php.ini`, `z_prepend.php` checks `HTTP_USER_AGENT` before normal page code runs. If deployed, the script is designed to leave ordinary visitors on the normal site.
- **Spam feeds for search bots.** Visits from `Googlebot`, `bingbot`, `Slurp`, or `Yahoo` trigger a server-side fetch to `*.jssnjc[.]com` and `t1.sysflowus[.]com` (`[REF-09]`). It could serve doorway spam to search bots; this evidence does not show that search engines indexed it.

05

CHAPTER 05

Exposure Analysis Across Enterprise Middleware

05 Exposure Analysis Across Enterprise Middleware

The returned outputs and 62 middleware scripts point to one clear target profile: **stateful enterprise database, mail, backup, and web servers**.

Platform class	Observed evidence	Why this layer attracts hybrid operators	Primary operational risk
Oracle E-Business Suite & RAC	**22 returned job files** + `ebs_deploy.sh`	High core counts, pre-authenticated `DB_LINK` trust, and frequent EDR exclusions on DB paths.	Cross-subnet OS command scheduling, key dumps (`TCP 8093`), and nocturnal CPU theft.
Windows Server & IIS	**505 command outputs (466 entries)** + OSS modules	Combines trusted public web domains with service accounts open to `CreateProcessAsUser` elevation.	Antivirus tampering, native IIS request hooks, and search-index spam.
Higher-Education Databases	**4 returned DB files**	High academic domain trust for SEO spam paired with legacy linked database schemas.	Unauthorized SQL/OS jobs and search reputation harm.
Zimbra (`CVE-2026-73570`), Ahsay & Pentaho	**Staged persistence & web-shell scripts**	Internet-facing mail and backup consoles sit directly inside internal server subnets.	Persistent `.swatchrc` or web-shell callbacks to :8898 and :8093.

Two operational gaps stand out across these environments. First, database and IIS folders may have file-scan exclusions that reduce visibility into staged files. Monitor process and behavior signals for `memfd_create` loaders and Defender tamper attempts. Second, database teams, SOC analysts, and web teams rarely compare off-hours CPU spikes with Google Search Console spam alerts (`[REF-09]`).

06

CHAPTER 06

Alternative Hypotheses

06 Alternative Hypotheses

Hypothesis	Evidence for	Evidence against	Assessment
Single integrated operation (`Operation NightShift`)	Shared hardcoded wiring across `38.60.227[.]210`, `38.60.252[.]110:8900`, `38.54.14[.]162:5556` (`krxYMRN97D`), R2, and OSS; shared whitelist tags (`z_73570`, `.sysjvd`); active `6-20 Nov` receiver logs.	Bundled LPEs (`CVE-2021-3156`, `CVE-2021-4034`) and `Invoke-SMBExec` are public tools.	**Supported.** Commodity LPEs sit inside one custom-wired operator workflow.
Same group as `UTA 0576`	Both appeared in investigations around Ivanti `CVE-2026-104935` in early November 2026 (`[REF-01]`).	Etugen Research separated `38.60.227[.]210` as a **distinct actor** from `UTA0576`, with different post-exploitation goals.	**Refuted.** Treat Operation NightShift as a separate financially driven operator.
Multi-thousand-node botnet	`install_user.sh` uses CDN staging and automated CPU profiling.	Returned stores confirm **at least three** target environments plus 382 receiver entries; pool worker counts are unseen.	**Unverified beyond confirmed floor.** State only verified counts.

07

CHAPTER 07

What Defenders Should Do

IN SHORT

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

07 What Defenders Should Do

Prioritize these five engineering actions:

1. **Patch Ivanti and Zimbra and inspect post-patch persistence (`0-48 Hours`).** Upgrade Ivanti Connect Secure (a branch-compatible release addressing the related chain: `25.1.1.3`, `25.1.3.0+`, or `22.8R2.6+`, `[REF-02]`) and Zimbra (`10.1.20+`, `[REF-03]`). Inspect `/opt/zimbra/.swatchrc`, crontabs, and `/proc/*/exe memfd` links right after patching.
2. **Audit and restrict Oracle database links (`Days 1-7`).** Review `DBA_DB_LINKS` across Oracle EBS and RAC instances (`[REF-06]`). Drop unneeded links and revoke `CREATE JOB` from link accounts. Enable Unified Auditing on `DBMS_SCHEDULER` and `EXEC_DDL_STATEMENT`.
3. **Enforce Defender Tamper Protection and review web hooks (`Days 1-7`).** Turn on Microsoft Defender Tamper Protection (`[REF-10]`) on Windows Server hosts. Inspect IIS `<globalModules>` and check PHP `auto_prepend_file` settings.
4. **Block server-tier cloud bucket and Stratum egress (`Days 7-14`).** Enforce proxy allowlists on database and middleware VLANs. Compare 22:00-06:00 CPU baselines against daytime load (`[REF-08]`).
5. **Test public pages with search-bot user agents (`Days 14-30`).** Request key pages internally with a `Googlebot User-Agent` header. Monitor Google Search Console (`[REF-09]`) for unauthorized doorway URLs.

08

CHAPTER 08

Detection Rules

IN SHORT

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

INSIDE THIS CHAPTER

How the Suricata and KQL detections work 24

08 Detection Rules

The full rules are in Appendix B. All four rule files were tested before release against Suricata `7.0.12` (0 linter warnings), Microsoft `Kusto.Language` (0 errors), `pySigma` (3 rules), and `YARA-X` (4 `filesize`-bounded rules).

Rule file	What it catches
`odin_nightshift_middleware_mining_and_cloaking.rules`	Suricata 7.x (`sid:9554001`-9554008): :8898 `/ping/` polling, :8900 `/GEO_TOP_` check-ins, R2 and OSS bucket TLS SNI, `wa.theshyc[.]xyz:5556` proxy TLS SNI, `.jssnjc[.]com` spam feeds, encoded PowerShell web-shell queries, and plaintext `krxYMRN97D` Stratum logins.
`sentinel_nightshift_dblink_memfd_and_taskgmr_hunt.kql`	Microsoft Sentinel KQL (7-day lookback): Linux `memfd_create` loaders paired with `inhibit.lock` or `github-c2-agent-dual`, Oracle `DBMS_SCHEDULER` / `EXEC_DDL_STATEMENT@` job creation, Windows `DisableRealtimeMonitoring` or `Taskgmr` staging, and egress to operator IPs or cloud buckets.
`sigma_nightshift_oracle_dblink_flock_and_taskgmr.yml`	Sigma (3 rules): Linux CLI calls to `EXEC_DDL_STATEMENT@`, `DBMS_SCHEDULER.CREATE_JOB@`, or `ebs_deploy.sh`; Linux `memfd_create` paired with `inhibit.lock` or `github-c2-agent-dual`, or `zimbra .swatchrc` edits; and Windows `Taskgmr`, pool, or OSS CLI markers, or Defender tamper commands from `w3wp.exe` or `sqlservr.exe`.
`odin_nightshift_ghc2_eviction_and_cloaker_artifacts.yar`	YARA (4 `filesize`-bounded rules): `deploy_ghc2.sh` (< 128 KB), `excl_evict4.sh` (< 128 KB), `z_prepend.php` (< 128 KB), and `ebs_deploy.sh` (< 256 KB).

How the Suricata and KQL detections work

The eight Suricata rules cover both direct operator callbacks and cloud staging traffic. Rules 9554001 and 9554002 alert on HTTP check-ins to `38.60.227[.]210:8898` (`/ping/`) and `38.60.252[.]110:8900` (`/GEO_TOP_`). Rules 9554003 through 9554006 match TLS SNI values for the Cloudflare R2 bucket, the Alibaba OSS bucket, `wa.theshyc[.]xyz:5556`, and `.jssnjc[.]com`. Rules 9554007 and 9554008 catch inbound encoded PowerShell URI queries (`c=powershell` with `-enc`) and plaintext `krxYMRN97D` Stratum pool logins.

The Microsoft Sentinel KQL hunt uses a 7-day lookback across `DeviceProcessEvents` and `DeviceNetworkEvents`. Before scheduling the query, replace the two placeholder hostnames in `ApprovedAdminHosts` (`dba-jump-01.corp.example` and `patch-runner-01.corp.example`) with your DBA jump-host allowlist. The query groups process and network hits by device and account so analysts can review linked events together.

09

CHAPTER 09

Indicators

IN SHORT

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

INSIDE THIS CHAPTER

9.1 Published Network and File Hash Indicators (10 Indicators) 26

9.2 Report-Only Cloud, Domain, and Behavioral Markers (6 Markers) 27

09 Indicators

The full indicator list is available in Appendix A. The public set contains 10 network and file hash indicators (3 operator IPv4 hosts and 7 SHA-256 digests) plus 6 report-only cloud, domain, and host markers. All victim output folder names, transfer log filenames, disk serials, database schema names, and third-party shared mining-pool addresses are withheld.

9.1 Published Network and File Hash Indicators (10 Indicators)

Type	Defanged value / SHA-256 digest	Port / size	Operational context & action
`ipv4`	`38.60.227[.]210`	8082 (8000, 8083, 8093, 9002, 8898, 8899, 9001, 13574)	Primary NightShift workbench and upload receiver (`LIGHT NODE`) · **Block & hunt egress**
`ipv4`	`38.60.252[.]110`	8900	Secondary `/GEO_TOP_` host-profiling listener · **Block & hunt egress**
`ipv4`	`38.54.14[.]162`	5556	Custom TLS mining proxy backing `wa.theshyc[.]xyz` · **Block & inspect SNI**
`sha256`	`d11b12d628615d5eff982e3e312f4c406fde38373eee76bc056be780a9e2e665`	ELF binary	`github-c2-agent-dual` enforced digest in `deploy_ghc2.sh` · **Hunt in EDR & `/dev/shm`**
`sha256`	`549d39ceceb57866c0ade97fa02897d29f3141034ff6a02732118324c4ca1ce7`	5,796 B	`deploy_ghc2.sh` (156 lines) Linux `flock` + `memfd_create` loader · **Hunt on Linux hosts**
`sha256`	`73fe311d3323b6bbc9f97854e43eaf33ed45d3122b236675f68350b820640b01`	16,351 B	`install_user.sh` (425 lines) R2 `Taskgmr` night-shift miner installer · **Hunt on Linux hosts**
`sha256`	`2a271c5cbf9bcc000b914c6f1f23cabc168fb98ed1628c555a4e4c416a456cde`	7,153 B	`excl_evict4.sh` (131 lines) 120-second rival eviction script · **Hunt in cron & `/tmp`**
`sha256`	`dbf856873b8142dac2d29118d60532f6d7bdafd8eb8763e9e149b9ef46ec832d`	3,148 B	`z_prepend.php` (58 lines) PHP `auto_prepend_file` bot cloaker · **Hunt in web roots**
`sha256`	`a7423702c637bd84d96d69d14b1bbefacebb3bfcbecac44b2990c5f59ab4f720`	3,655 B	`wbi_v10.php` (74 lines) companion PHP web shell · **Hunt in PHP web roots**
`sha256`	`9bb5852cb65e3f9eb102f41f04062cc9c8a0d645e48735918208a08d5554eeb0`	4,199 B	`ebs_deploy.sh` (63 lines) Oracle EBS DB-link job deployer · **Hunt on DB jump hosts**

9.2 Report-Only Cloud, Domain, and Behavioral Markers (6 Markers)

Marker type	Defanged value / pattern	Hunt surface & note
Cloud bucket	`pub-307c565a487b43c5bee73d21edc4d83b.r2[.]dev`	Cloudflare R2 bucket hosting staged mining archives (`sid:9554003`).
Cloud bucket	`imagefiles-backup.oss-ap-southeast-7.aliyuncs[.]com`	Alibaba Cloud OSS bucket fetched in returned Windows outputs (`sid:9554004`).
TLS proxy host	`wa.theshyc[.]xyz` (:5556)	Custom TLS Stratum proxy hostname on `38.54.14[.]162:5556` (`sid:9554005`).
Spam feed domains	`*.jssnjc[.]com` / `t1.sysflowus[.]com`	Upstream SEO spam servers queried by `z_prepend.php` (`sid:9554006`).
Pool prefix	`krxYMRN97D`	Monero/Kryptex pool account prefix in miner configs (`sid:9554008`).
Mutex path	`/var/tmp/.systemd/inhibit.lock`	Primary `flock` lock file paired with `memfd_create` in `deploy_ghc2.sh` .

10

CHAPTER 10

Scope and Limits

IN SHORT

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

10 Scope and Limits

Odin by Brandefense conducted this analysis during a two-week observation window ending `20 November 2026`. Earlier dates in this report come from target file listings (`2 September 2026`), public research (`3 November 2026`), and receiver logs (`6 November 2026`). Returned files confirm at least three affected environments.

Staged miner and cloaker scripts do not show total active miner counts or revenue. All victim paths, filenames, and identifiers are withheld.

11

CHAPTER 11

Sources

IN SHORT

This chapter lists the public references used in the report.

11 Sources

1. [REF-01] Etugen Research, An Ivanti Zero-Day Operation Where the Dead Proxy Was Named in the Operator's Notes (3 November 2026; verified on 22 November 2026): https://etugen.io/blog/ivanti-zero-day-operation/
2. [REF-02] NIST NVD, CVE-2026-104935 - Ivanti Connect Secure Authentication Bypass (verified on 22 November 2026): https://nvd.nist.gov/vuln/detail/cve-2026-104935
3. [REF-03] NIST NVD, CVE-2026-73570 - Zimbra Collaboration Suite zimbra-snmp Command Injection (verified on 22 November 2026): https://nvd.nist.gov/vuln/detail/cve-2026-73570
4. [REF-04] NIST NVD, CVE-2021-3156 - Sudo Heap-Based Buffer Overflow (verified on 22 November 2026): https://nvd.nist.gov/vuln/detail/cve-2021-3156
5. [REF-05] NIST NVD, CVE-2021-4034 - Polkit pkexec Local Privilege Escalation (verified on 22 November 2026): https://nvd.nist.gov/vuln/detail/cve-2021-4034
6. [REF-06] Oracle, Oracle Database 19c Security Guide - Configuring Audit Policies (verified on 22 November 2026): https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/configuring-audit-policies.html
7. [REF-07] MITRE ATT&CK, Reflective Code Loading (T1620) (verified on 22 November 2026): https://attack.mitre.org/techniques/T1620/
8. [REF-08] MITRE ATT&CK, Resource Hijacking (T1496) (verified on 22 November 2026): https://attack.mitre.org/techniques/T1496/
9. [REF-09] Google Search Central, Spam Policies for Google Web Search (verified on 22 November 2026): https://developers.google.com/search/docs/essentials/spam-policies
10. [REF-10] Microsoft Learn, Protect Security Settings with Tamper Protection (verified on 22 November 2026): https://learn.microsoft.com/en-us/defender-endpoint/tamper-protection-overview

APPENDICES

Indicators and Detection Rules

FOR DEFENDERS

Appendix A lists the indicators published for this study. Appendix B carries every published detection rule in full.

INSIDE

A. Indicators of compromise (9) 33

B. Detection rules (4 files) 34

A Indicators of Compromise

Values are defanged for display. The CSV, JSON and STIX files on the online edition carry the raw values. Values the report marks as withheld are not listed.

ID	Type	Indicator	Port	Context	Action
R54-IOC-01	IPv4	38.60.227[.]210	8082	Operation NightShift primary workbench (HTTP staging on 8000, 8082, 8083, 8093, 9002; callbacks on 8898, 8899, 9001, 13574)	BLOCK
R54-IOC-02	IPv4	38.60.252[.]110	8900	GEO_TOP_ · Operation NightShift secondary host-profiling check-in endpoint	BLOCK
R54-IOC-03	IPv4	38.54.14[.]162	5556	Operation NightShift custom TLS mining-pool proxy host backing wa.theshyc.xyz	BLOCK
R54-IOC-04	SHA-256	549d39ceceb57866c0ade97fa02897d29f3141034ff6a02732118324c4ca1ce7		deploy_ghc2.sh · Fileless Linux C2 loader enforcing flock mutex and Perl/Python memfd_create execution (156 lines)	HUNT
R54-IOC-05	SHA-256	73fe311d3323b6bbc9f97854e43eaf33ed45d3122b236675f68350b820640b01		install_user.sh · Cloudflare R2 miner installer staging Taskgmr binary and 22:00-06:00 night-shift schedule (425 lines)	HUNT
R54-IOC-06	SHA-256	2a271c5cbf9bcc000b914c6f1f23cabc168fb98ed1628c555a4e4c416a456cde		excl_evict4.sh · Rival-malware eviction watchdog sweeping processes and crontabs every 120 seconds (131 lines)	HUNT
R54-IOC-07	SHA-256	dbf856873b8142dac2d29118d60532f6d7bdafd8eb8763e9e149b9ef46ec832d		z_prepend.php · PHP auto_prepend_file search-bot SEO spam cloaker targeting Google, Bing, and Yahoo crawlers (58 lines)	HUNT
R54-IOC-08	SHA-256	a7423702c637bd84d96d69d14b1bbefacebb3bfcbecac44b2990c5f59ab4f720		wbi_v10.php · Multi-function PHP web shell deployed alongside SEO cloaking hooks (74 lines)	HUNT
R54-IOC-09	SHA-256	9bb5852cb65e3f9eb102f41f04062cc9c8a0d645e48735918208a08d5554eeb0		ebs_deploy.sh · Oracle E-Business Suite lateral deployment script invoking DBMS_SCHEDULER jobs across DB links (63 lines)	HUNT

B Detection Rules

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

odin_nightshift_ghc2_eviction_and_cloaker_artifacts.yar

YARA

```
/*
   Odin by Brandefense  -  Monograph 54 (Operation NightShift) YARA Suite
   4 filesize-bounded structural rules covering fileless C2, rival eviction, SEO cloaking, and Oracle DB-link
pivoting.
*/

rule ODIN_NightShift_GitHubC2_Memfd_Loader
{
    meta:
        author = "Odin by Brandefense"
        monograph = "54"
        description = "Detects NightShift fileless Linux C2 loader combining flock mutex locking with Perl/Python
memfd_create"
        date = "2026-11-22"
    strings:
        $m1 = "memfd_create" ascii
        $m2 = "inhibit.lock" ascii
        $m3 = "github-c2-agent-dual" ascii
        $m4 = "/proc/self/fd/" ascii
    condition:
        filesize < 128KB and $m1 and ($m2 or $m3) and $m4
}

rule ODIN_NightShift_Rival_Eviction_Watchdog
{
    meta:
        author = "Odin by Brandefense"
        monograph = "54"
        description = "Detects NightShift rival-malware eviction script sweeping processes and crontabs while
whitelisting operator markers"
        date = "2026-11-22"
    strings:
        $e1 = ".sysjvd" ascii
        $e2 = "selfok" ascii
        $e3 = "crontab" ascii
        $e4 = ":8899" ascii
    condition:
        filesize < 128KB and 3 of ($e*)
}

rule ODIN_NightShift_PHP_SearchBot_SEO_Cloaker
{
    meta:
        author = "Odin by Brandefense"
        monograph = "54"
        description = "Detects NightShift PHP auto_prepend_file search-bot SEO spam cloaker querying upstream
spam feeds"
        date = "2026-11-22"
    strings:
        $c1 = "HTTP_USER_AGENT" ascii
        $c2 = "googlebot" ascii nocase
        $c3 = "bingbot" ascii nocase
        $f1 = "jssnjc.com" ascii nocase
        $f2 = "sysflowus.com" ascii nocase
    condition:
        filesize < 128KB and $c1 and ($c2 or $c3) and ($f1 or $f2)
}

rule ODIN_NightShift_Oracle_EBS_DBLink_Deployer
{
```

```
    meta:
        author = "Odin by Brandefense"
        monograph = "54"
        description = "Detects NightShift Oracle E-Business Suite lateral script scheduling OS jobs over database
links"
        date = "2026-11-22"
    strings:
        $o1 = "DBMS_SCHEDULER" ascii nocase
        $o2 = "CREATE_JOB" ascii nocase
        $o3 = "EXEC_DDL_STATEMENT@" ascii nocase
    condition:
        filesize < 256KB and all of ($o*)
}
```

odin_nightshift_middleware_mining_and_cloaking.rules

SURICATA

```
# Odin by Brandefense  -  Monograph 54 (Operation NightShift) Suricata 7.x Ruleset
# Validated against Suricata 7.0.12 (-T) and Odin Suricata linter (0 warnings).

alert http $HOME_NET any -> 38.60.227.210 8898 (msg:"ODIN-R54 NightShift Linux 45s Persistence Poller Check-In";
flow:established,to_server; http.uri; content:"/ping/"; startswith; fast_pattern; classtype:command-and-control;
sid:9554001; rev:1;)
alert http $HOME_NET any -> 38.60.252.110 8900 (msg:"ODIN-R54 NightShift Secondary Host-Profiling GEO_TOP
Beacon"; flow:established,to_server; http.uri; content:"/GEO_TOP_"; startswith; fast_pattern; classtype:command-
and-control; sid:9554002; rev:1;)
alert tls $HOME_NET any -> $EXTERNAL_NET 443 (msg:"ODIN-R54 NightShift Cloudflare R2 Miner Staging Bucket SNI";
flow:established,to_server; tls.sni; content:"pub-307c565a487b43c5bee73d21edc4d83b.r2.dev"; bsize:43; nocase;
fast_pattern; classtype:trojan-activity; sid:9554003; rev:1;)
alert tls $HOME_NET any -> $EXTERNAL_NET 443 (msg:"ODIN-R54 NightShift Alibaba OSS Windows Payload Bucket SNI";
flow:established,to_server; tls.sni; content:"imagefiles-backup.oss-ap-southeast-7.aliyuncs.com"; bsize:49;
nocase; fast_pattern; classtype:trojan-activity; sid:9554004; rev:1;)
alert tls $HOME_NET any -> 38.54.14.162 5556 (msg:"ODIN-R54 NightShift Custom TLS Mining Pool Proxy SNI
wa.theshyc.xyz"; flow:established,to_server; tls.sni; content:"wa.theshyc.xyz"; bsize:14; nocase; fast_pattern;
classtype:trojan-activity; sid:9554005; rev:1;)
alert tls $HOME_NET any -> $EXTERNAL_NET 443 (msg:"ODIN-R54 NightShift PHP SEO Cloaker Upstream Spam Feed SNI";
flow:established,to_server; tls.sni; content:".jssnjc.com"; endswith; nocase; fast_pattern; classtype:bad-
unknown; sid:9554006; rev:1;)
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-R54 NightShift Inbound Encoded PowerShell Web-Shell
Query"; flow:established,to_server; http.uri; content:"c=powershell"; nocase; fast_pattern; content:"-enc";
distance:0; nocase; classtype:web-application-attack; sid:9554007; rev:1;)
alert tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R54 NightShift Plaintext Stratum Pool Login krxYMRN97D";
flow:established,to_server; content:"krxYMRN97D"; fast_pattern; content:"\"method\""; classtype:policy-violation;
sid:9554008; rev:1;)
```

sentinel_nightshift_dblink_memfd_and_taskgmr_hunt.kql

KQL (SENTINEL / DEFENDER XDR)

```
// Odin by Brandefense  -  Monograph 54 (Operation NightShift)
// Hunts Linux memfd/flock C2 loaders, Oracle DB-link job creation, Windows Defender/Taskgmr staging, and
NightShift C2/bucket egress.
let Lookback = 7d;
let ApprovedAdminHosts = dynamic(["dba-jump-01.corp.example", "patch-runner-01.corp.example"]);
let NightShiftIPs = dynamic(["38.60.227.210", "38.60.252.110", "38.54.14.162"]);
let NightShiftDomains = dynamic([
    "pub-307c565a487b43c5bee73d21edc4d83b.r2.dev",
    "imagefiles-backup.oss-ap-southeast-7.aliyuncs.com",
    "wa.theshyc.xyz",
    "t1.sysflowus.com"
]);
let HostProcessSignals =
    DeviceProcessEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedAdminHosts))
    | where (
        (ProcessCommandLine has "memfd_create" and (ProcessCommandLine has "inhibit.lock" or ProcessCommandLine
```

```
has "github-c2-agent-dual"))
        or (ProcessCommandLine has_any ("DBMS_SCHEDULER", "EXEC_DDL_STATEMENT@") and ProcessCommandLine has
"CREATE_JOB")
        or (ProcessCommandLine has "Set-MpPreference" and ProcessCommandLine has "DisableRealtimeMonitoring")
        or (ProcessCommandLine has_any ("Taskgmr", "krxYMRN97D", "excl_evict4", "z_prepend.php"))
    )
    | project Timestamp, DeviceName, AccountName, SignalType = "HostProcessSignal", Detail = ProcessCommandLine;
let NetworkEgressSignals =
    DeviceNetworkEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedAdminHosts))
    | where RemoteIP in (NightShiftIPs)
        or RemoteUrl has_any (NightShiftDomains)
        or RemoteUrl endswith ".jssnjc.com"
    | project Timestamp, DeviceName, AccountName = InitiatingProcessAccountName, SignalType = "NightShiftEgress",
Detail = strcat(RemoteIP, ":", tostring(RemotePort), " ", RemoteUrl);
union HostProcessSignals, NetworkEgressSignals
| summarize FirstSeen = min(Timestamp), LastSeen = max(Timestamp), EventCount = count(), Signals =
make_set(SignalType, 8), SampleDetails = make_set(Detail, 5) by DeviceName, AccountName
| order by LastSeen desc
```

sigma_nightshift_oracle_dblink_flock_and_taskgmr.yml

SIGMA

```
title: NightShift Oracle Database Link Remote Job Creation via CLI
id: 6d48a7c2-8c1e-4e89-9b41-54a10f92c101
status: experimental
description: Detects command-line SQL or shell scripts invoking Oracle DBMS_SCHEDULER.CREATE_JOB or
DBMS_UTILITY.EXEC_DDL_STATEMENT across database links as observed in Operation NightShift.
author: Odin by Brandefense
date: 2026-11-22
logsource:
  category: process_creation
  product: linux
detection:
  selection_ora:
    CommandLine|contains:
      - 'EXEC_DDL_STATEMENT@'
      - 'DBMS_SCHEDULER.CREATE_JOB@'
      - 'ebs_deploy.sh'
  filter_dba_hosts:
    ComputerName:
      - 'dba-jump-01.corp.example'
      - 'ora-maint-01.corp.example'
  condition: selection_ora and not filter_dba_hosts
falsepositives:
  - Approved cross-instance database maintenance scripts on designated DBA jump hosts
level: high
tags:
  - attack.lateral-movement
  - attack.t1021
---
title: NightShift Linux Memfd Loader and Zimbra Swatchrc Persistence
id: 6d48a7c2-8c1e-4e89-9b41-54a10f92c102
status: experimental
description: Detects Linux command lines combining anonymous memory execution (memfd_create) with systemd inhibit
lock files or modifying Zimbra swatchrc configuration files.
author: Odin by Brandefense
date: 2026-11-22
logsource:
  category: process_creation
  product: linux
detection:
  selection_memfd:
    CommandLine|contains: 'memfd_create'
  selection_lock:
    CommandLine|contains:
      - 'inhibit.lock'
      - 'github-c2-agent-dual'
```

```
  selection_zimbra:
    CommandLine|contains: '.swatchrc'
    User: 'zimbra'
  filter_patch_hosts:
    ComputerName:
      - 'zimbra-patch-01.corp.example'
  condition: ((selection_memfd and selection_lock) or selection_zimbra) and not filter_patch_hosts
falsepositives:
  - Authorized Zimbra upgrades modifying swatch monitoring rules during maintenance windows
level: high
tags:
  - attack.defense-evasion
  - attack.t1620
---
title: NightShift Windows Defender Tampering and Taskgmr Miner Staging
id: 6d48a7c2-8c1e-4e89-9b41-54a10f92c103
status: experimental
description: Detects Taskgmr, pool, or OSS command-line markers, or Defender tamper commands launched by w3wp.exe
or sqlservr.exe. It does not correlate these signals.
author: Odin by Brandefense
date: 2026-11-22
logsource:
  category: process_creation
  product: windows
detection:
  selection_miner:
    CommandLine|contains:
      - 'krxYMRN97D'
      - 'wa.theshyc.xyz'
      - 'imagefiles-backup.oss-ap-southeast-7.aliyuncs.com'
      - 'Taskgmr.exe'
  selection_defender_tamper:
    CommandLine|contains: 'DisableRealtimeMonitoring'
    ParentImage|endswith:
      - '\w3wp.exe'
      - '\sqlservr.exe'
  filter_admin_hosts:
    ComputerName:
      - 'win-edr-lab-01.corp.example'
  condition: (selection_miner or selection_defender_tamper) and not filter_admin_hosts
falsepositives:
  - Isolated lab imaging workflows that temporarily toggle antivirus settings
level: high
tags:
  - attack.impact
  - attack.t1496
  - attack.t1562.001
```

About Odin Research

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

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

Online edition, indicators and rules · brandefense.io/odin-research/reports/operation-nightshift-enterprise-middleware-intrusion-off-hours-mining-and-seo/
Short Read · brandefense.io/odin-research/blog/operation-nightshift-middleware-intrusion-mining-and-seo-abuse/
Defense Kit · brandefense.io/odin-research/defense-kit/