FULL REPORT · DELIVERY INFRASTRUCTURE · MONOGRAPH 71 / 70 · 22 MIN READ

Bulk-Mail Kit Staging: PowerMTA, MailWizz, and Suppression Databases

Defensive analysis of 144 staged entries across an open Apache bulk-mail workbench pairing patched PowerMTA v5 daemons, ESP archives and installers, DNS rotation modules, and suppression and schema files

BY
Odin by Brandefense

PUBLISHED
19 November 2026

READING TIME
22 min read

EDITION
Version 1.1 · TLP:CLEAR

SCOPE
Prepared November 2026

1. Executive Summary

IN SHORT

Recorded on 26 November 2026, Odin by Brandefense analyzed 144 staged files totaling 827.50 megabytes across 21 open Apache directories on a Japan-routed bulk-mail workbench. The server pairs license-patched PowerMTA v5 daemons with ESP panel archives, four installer scripts, DNS rotation scripts, and 213.30 megabytes of suppression and schema files. Enforce newly registered domain holds, DMARC reject rules, and cloud port-25 blocks.

Many email gateways still treat passing SPF, DKIM, and DMARC checks as a sign of sender safety. Turnkey bulk-mail kits weaken that trust on freshly rented virtual servers. These kits set up DNS records, virtual mail relays, and bounce filters in minutes. Operators can send authenticated lures from newly registered domains and swap blocked addresses fast.

Recorded on 26 November 2026, Odin by Brandefense examined an open Apache directory on TCP port 80 of a Japan-routed server (`Workbench A`). Across 21 directories, the deduplicated inventory holds 144 sized files totaling 827,500,373 bytes (827.50 megabytes) and zero unsized entries.

Initial directory files carried 4 to 9 August 2026 batch timestamps. The full `/downloads/` mirror and 38 endpoint and secret records were recorded on 26 November 2026. `Workbench A` is assessed consistently as an adversary bulk-mail staging workbench. Its IPv4 address, file SHA-256 digests, four script password records, and kit vendor domains are withheld.

1. **Patched PowerMTA v5 daemons and RPM packages form half of total workbench bytes.**
   Sixty-three entries totaling 414,333,861 bytes (50.07 percent) stage `PowerMTA5.0.rpm` (56.45 megabytes) in three paths. Two `/patch/usr/sbin/` trees hold patched `pmtad` (34.67 megabytes) and `pmtahttpd` (41.20 megabytes) binaries built to overwrite license checks.

2. **Two panel archives and four installer scripts pair with legacy PHP ionCube loaders.**
   Fifty-one entries totaling 234,495,804 bytes include MailWizz and Interspire panel archives plus four installer scripts; three measured installers span 3,869–3,959 lines. They sit beside Mumara and SparkMail scripts and PHP 5.3 and 5.6 `ionCube` shared objects.

3. **Five suppression and schema files under the install directory total 213.30 megabytes.**
   Three blacklist-named files under `/Install/dbs/` hold two raw SQL dumps (112.81 megabytes and 60.80 megabytes) and one 36.56-megabyte Mumara ZIP. Two baseline SQL schema dumps complete the five-file set; no email rows or imports were verified.

4. **Modular DNS and IP-rotation scripts automate rapid sender turnover.**
   Fifteen `/setupxmpta/` files and four rotation scripts configure SPF, DKIM, DMARC, proxy, and virtual-MTA bindings on rented servers.

Three Decisions for Security and Email Leaders

1. **Hold or sandbox mail from newly registered domains even when SPF, DKIM, and DMARC pass.** Gateways need domain-age checks and link rewriting because setup scripts align DNS authentication on throwaway domains fast.
2. **Enforce DMARC reject policies, MTA-STS, and cloud port-25 egress blocks.** Publish strict `p=reject` DMARC and MTA-STS rules on owned domains, and block unapproved ports 25, 465, 587, and 2525 in cloud VPCs.

---

3. **Hunt kit downloads, binary overwrites, and SQL blacklist imports across network and host logs.** Deploy HTTP proxy rules, Linux process checks, and bounded YARA rules for patched `pmtad` binaries, ESP installers, and suppression dumps.

2. Workbench A Inventory, Directory Zones, and Functional Clusters

Odin by Brandefense recorded all 21 Apache HTTP directories on `TCP 80` of `Workbench A` (`Japan-routed VPS`, IPv4 withheld) on `26 November 2026`. Earlier directory entries carried `4-9 August 2026` batch timestamps. The full `/downloads/` mirror and **38** endpoint and secret records were recorded on `26 November 2026`. Batch dates show when files were indexed, not when an operator ran them.

Throughout this report, `Workbench A` is classified consistently as an **adversary bulk-mail staging workbench** (`T1583.003`, `T1608.002`, `[REF-07]`, `[REF-08]`). It pairs license-bypass daemons (`/patch/usr/sbin/pmtad` and `pmtahttpd`) with two ESP panel archives, four installer scripts, IP swap scripts, and **213.30 MB** of suppression and schema files.

We withhold `Workbench A`'s IPv4 address so no third party can pull archives or SQL files from the server. All file SHA-256 digests, four script password records, and all kit reseller brand prefixes and promotional domains are also withheld. Figure 1 maps the five directory zones and OPSEC boundary.

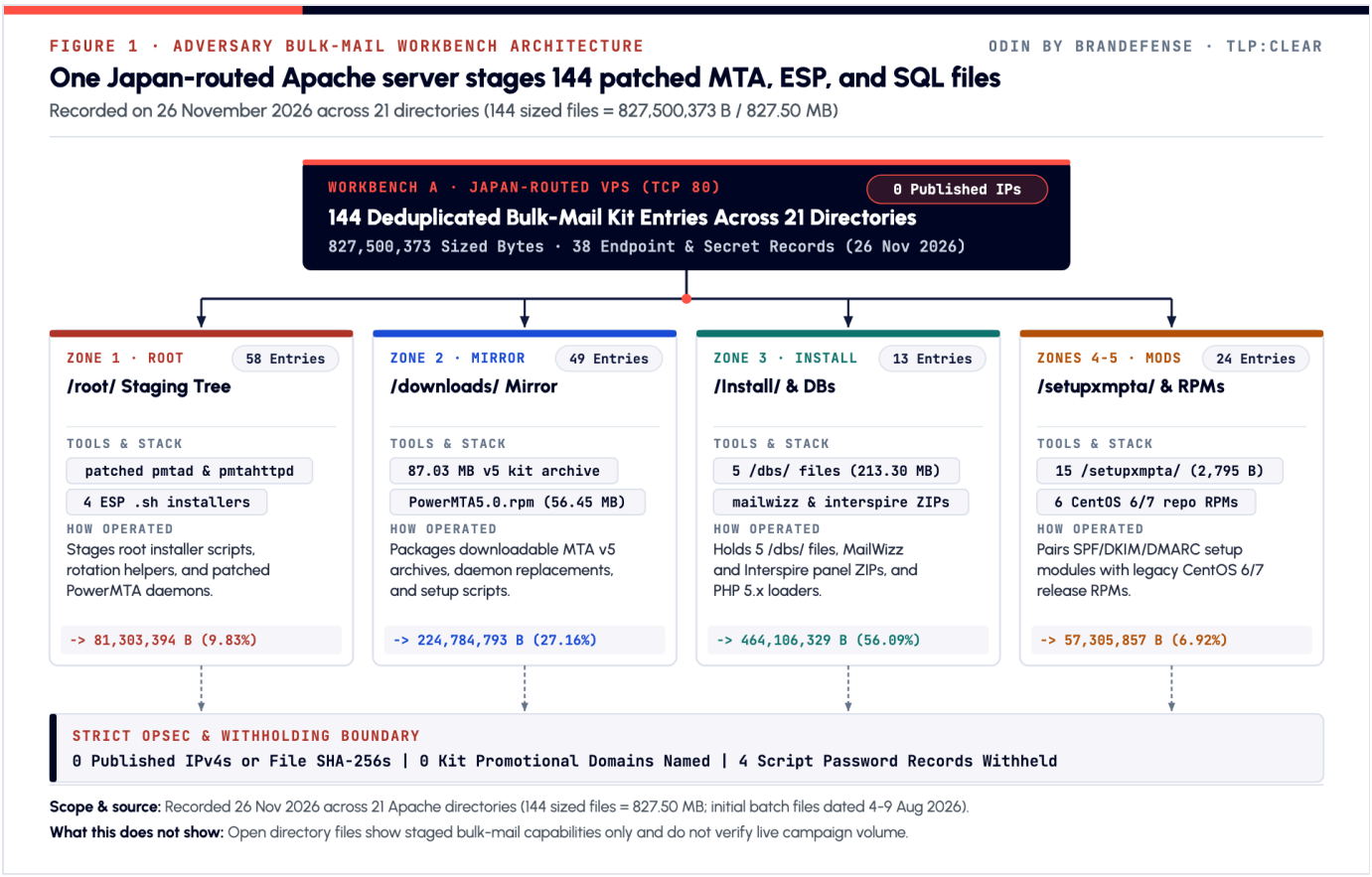

Figure 1: One Japan-routed Apache server stages 144 patched MTA, ESP, and SQL files

Five-Zone Directory Breakdown (`n = 144` Sized Files, 827,500,373 Bytes)

Across all **21** directories on `Workbench A`, the inventory holds **144 sized files** totaling **827,500,373 bytes (827.50 MB)** and **0 unsized entries**. Cloud teams can use external attack surface management to spot open Apache directory listings on rented virtual servers. Pairing those checks with cyber threat intelligence turns staged mail-kit paths into network and host rules. Table 1 reconciles all **144** entries across five zones.

Directory zone on `Workbench A`	Entries	Share (%)	Sized / Unsized	Sized bytes	Byte (%)	Primary staged contents
Operator Root Tree (`/root/`)	58	40.28 %	58 / 0	81,303,394	9.83%	Patched `pmtad` & `pmtahttpd`, 4 ESP `.sh` installers, 4 rotators, `languages.zip`, `clean.sh` + `.1` - `.3`.
Installer Mirror (`/downloads/`)	49	34.03 %	49 / 0	224,784,793	27.16 %	Bundled 87,031,808 B v5 ZIP (prefix withheld), `PowerMTA5.0.rpm`, patched daemons, `.sh` scripts.
DNS & Auth Modules (`/setupxmpta/`)	15	10.42 %	15 / 0	2,795	0.00 %	12 numbered DNS, IP, MTA, proxy, DMARC, DKIM, DB, and SPF modules plus 3 helper scripts.
DBs, ESPs & Loaders (`/Install/`)	13	9.03%	13 / 0	464,106,329	56.09%	5 `/dbs/` files (213.30 MB), 5 `/files/` ZIPs (191.83 MB), `PowerMTA5.0.rpm`, 2 `ionCube .so`.
CentOS RPMs & Root (`/osupdatex/`, `/images/` & root)	9	6.25%	9 / 0	57,303,062	6.92%	6 CentOS 6/7 repo RPMs (85,124 B), 2 JPEGs (763,934 B), root `/PowerMTA5.0.rpm` (56.45 MB).
Total (100.00% exact; 100.01% rounded)	**144**	**100.00 %**	**144 / 0**	**827,500,373**	**100.00 %**	**Complete 21-directory bulk-mail kit inventory (827.50 MB).**

Every file in `/Install/` (**13** files = **464,106,329** bytes) reconciles to the exact byte. It holds **5** `/Install/dbs/` files (**213,299,034** B), **5** `/Install/files/` ZIPs (**191,828,019** B), `PowerMTA5.0.rpm`

(**56,454,004** B), and **2** `ionCube` `.so` files (**2,525,272** B). Mirrored trees in `/root/` (**58** files) and `/downloads/` (**49** files) hold **74.31%** of entries.

File-Class and Six-Cluster Functional Breakdown

Table 2 splits the **144** sized files (**827,500,373** bytes) by file class. Shell scripts lead by count (**87** files, **60.42%**), spanning **84** `.sh` files and **3** `.1` - `.3` backup copies of `clean.sh`. Archives (**58.67%** of bytes), SQL dumps (**21.36%**), and binaries (**19.25%**) form **99.28%** of byte volume.

File class	Entries	Share (%)	Sized / Unsized	Sized bytes	Byte (%)	Extension & binary breakdown
Shell scripts (`script`)	87	60.42%	87 / 0	5,202,135	0.63%	**84** `.sh` scripts (**4** ESP installers, **4** rotators, `/setupxmpta/`, `clean.sh`) + **3** `.1` - `.3` backups.
Packages & ZIPs (`archive`)	30	20.83%	30 / 0	485,464,434	58.67%	**21** `.rpm` files (**3** `PowerMTA5.0.rpm` + CentOS RPMs) and **9** `.zip` ESP, kit, and blacklist bundles.
Metadata files (`text`)	11	7.64%	11 / 0	4,583	0.00%	**9** `.info` descriptor files and **2** extensionless text config markers (**< 0.01%** of bytes).
ELF & `.so` binaries (`exe`)	10	6.94%	10 / 0	159,331,080	19.25%	**4** patched ELF daemons (**2** `pmtahttpd` + **2** `pmtad`) and **6** `ionCube` `.so` loaders (**7,575,816** B).

File class	Entries	Share (%)	Sized / Unsized	Sized bytes	Byte (%)	Extension & binary breakdown
Raw SQL dumps (`data`)	4	2.78 %	4 / 0	176,734,207	21.36 %	`mw_email_blacklist.sql` (112.81 MB), `email_banned_emails.sql` (60.80 MB), and 2 panel SQL schemas.
Web images (`image`)	2	1.39%	2 / 0	763,934	0.09 %	`email-marketing-campaig33n.jpg` (691,285 B) and `applicationlogo.jpg` (72,649 B).
Total	**144**	**100.00 %**	**144 / 0**	**827,500,373**	**100.00 %**	**Exact parity with Table 1 (144 sized files = 827.50 MB).**

Table 3 and Figure 5 divide all **144** entries into six mutually exclusive clusters (`63 + 51 + 11 + 9 + 7 + 3 = 144`). Patched PowerMTA v5 files (**63** entries) and multi-ESP archives and installers (**51** entries) account for **79.17%** of files (**78.41%** of bytes).

All five `/Install/dbs/` files sum to **213,299,034** B (**213.30 MB**). Four raw `.sql` dumps total **176,734,207** B, and `mumara_email_blacklist.zip` adds **36,564,827** B. In Table 3, the suppression cluster pairs both raw SQL blacklists (**173,619,421** B) with `4dbintil.sh` (**133** B = **173,619,554** B). Meanwhile, the multi-ESP cluster groups `mumara_email_blacklist.zip` , `interspire-2015.sql` , and `mailwizz.sql` with their web panels.

Functional cluster	Entries	Share (%)	Sized / Unsized	Sized bytes	Byte (%)	Key staged files
Patched PowerMTA v5 Daemons & RPMs	63	43.75 %	63 / 0	414,333,861	50.07%	`PowerMTA5.0.rpm` (56.45 MB x 3), patched `pmtahttpd` & `pmtad`, 87.03 MB v5 archive.
Multi-ESP Frontends & Installers	51	35.42 %	51 / 0	234,495,804	28.34 %	`mailwizz.zip`, `interspire-2015.zip`, `mumara_email_blacklist.zip`, `addons.zip`, `phpMyAdmin`, 4 `.sh`.
Legacy CentOS Mirrors & ionCube	11	7.64%	11 / 0	2,610,811	0.32%	`ioncube_loader_lin_5.6.so` (1.48 MB) & `5.3.so` (1.04 MB), 6 CentOS 6/7 repo RPMs.
Maintenance, Backup & Cleanup	9	6.25%	9 / 0	2,439,332	0.29 %	`/Install/files/index.zip` (1.67 MB), 2 JPEGs (763,934 B), 5 `clean.sh` scripts and backups.
IP/Domain Rotation & SPF/DKIM/DMARC	7	4.86%	7 / 0	1,011	0.00 %	Seven `/setupxmpta/` DNS, IP, MTA, proxy, DMARC, DKIM, and SPF module scripts (141–149 B).
Blacklist-Named SQL & Init	3	2.08%	3 / 0	173,619,554	20.98 %	`mw_email_blacklist.sql` (112,814,881 B), `email_banned_emails.sql` (60,804,540 B), `4dbintil.sh` (133 B).

Functional cluster	Entries	Share (%)	Sized / Unsized	Sized bytes	Byte (%)	Key staged files
Combined inventory	144	100.00%	144 / 0	827,500,373	100.00%	Six mutually exclusive clusters across 21 Apache directories (827.50 MB).

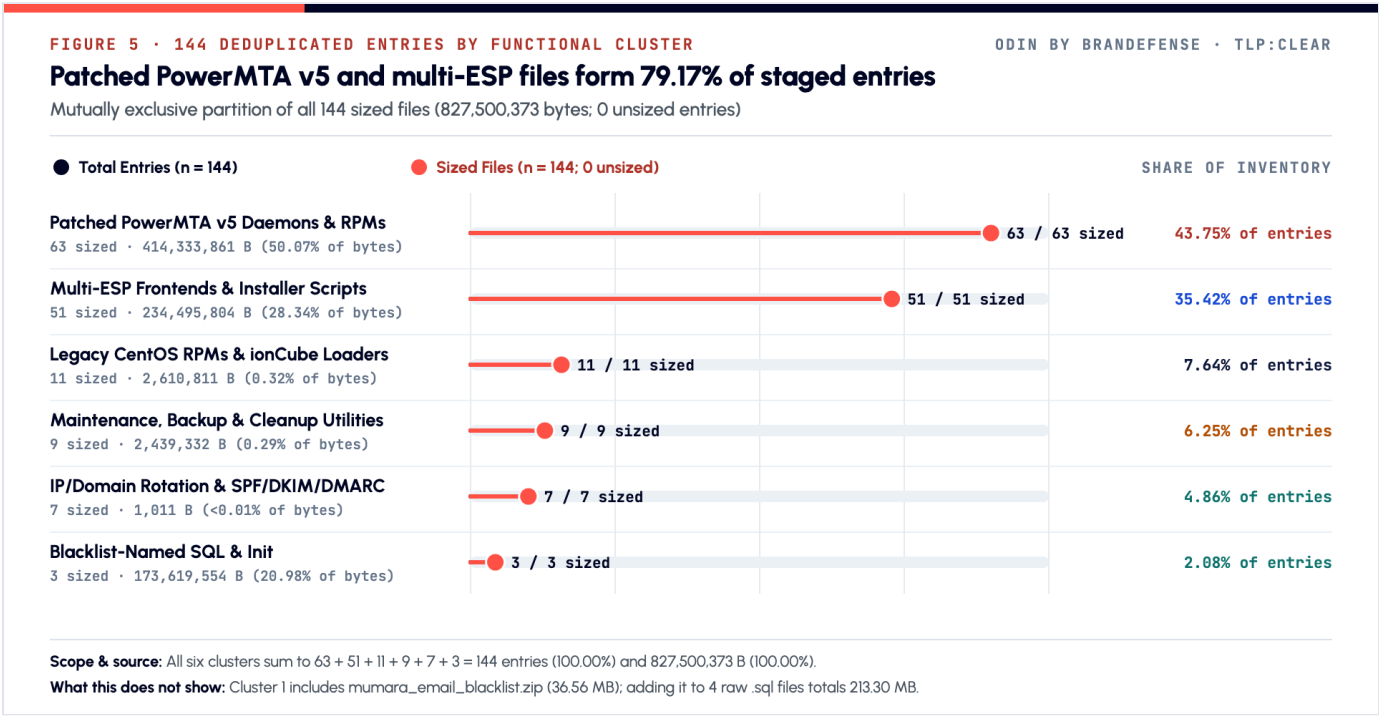

Figure 5: Patched PowerMTA v5 and multi-ESP files form 79.17% of staged entries

3. Patched PowerMTA v5 Daemons, ionCube Loaders, and ESP Installers

Commercial mail transfer agents enforce license checks, rate policies, and abuse contracts. Bulk-mail operators bypass those checks by pairing patched MTA binaries with PHP campaign panels on rented virtual servers (`T1583.003` , `T1608.002` , `[REF-07]` , `[REF-08]`). Figure 3 shows a dashed analytical model of how staged MTA patching, SQL imports, DNS modules, and IP rotation meet defender controls.

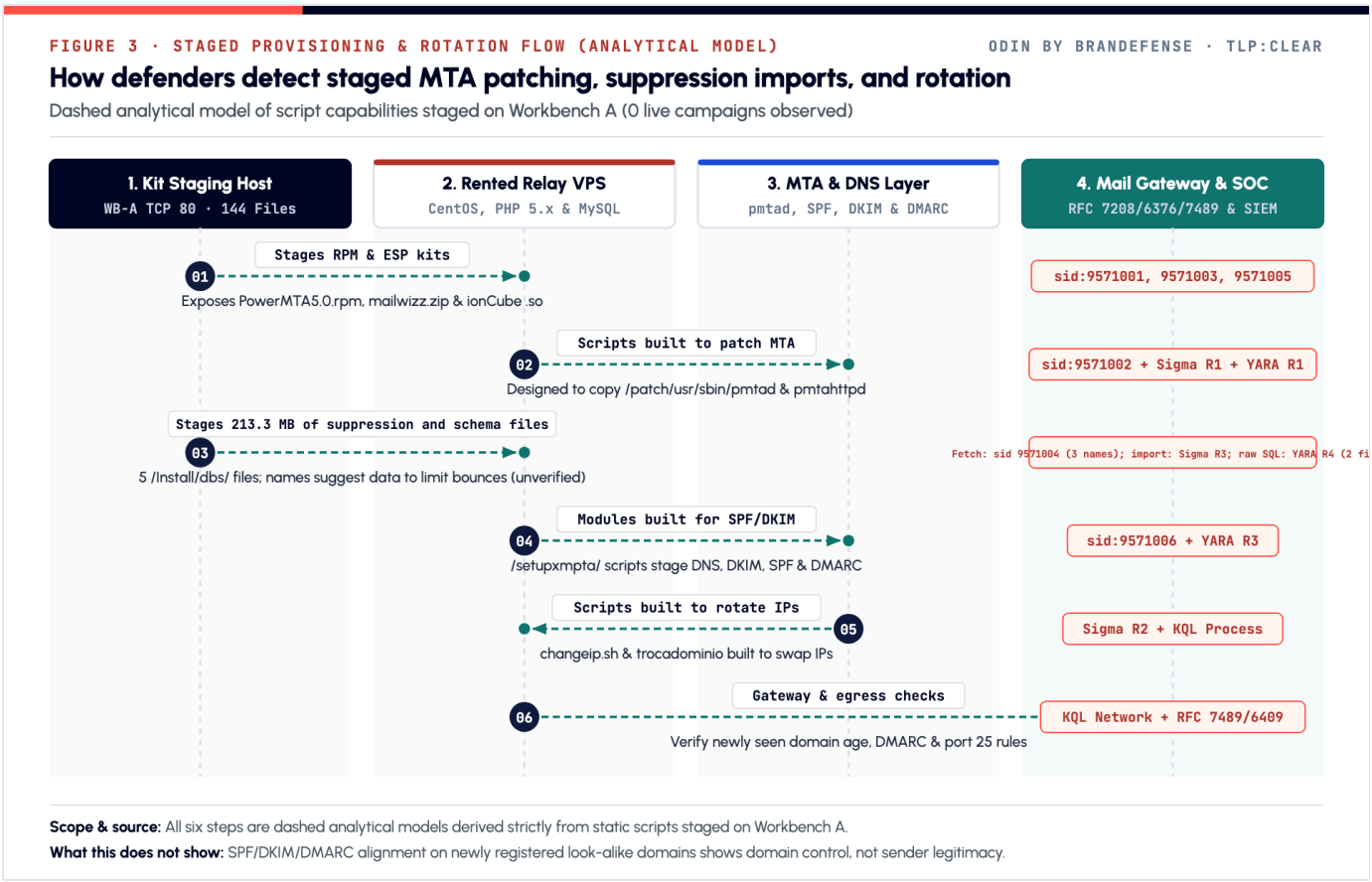

Figure 3: How defenders detect staged MTA patching, suppression imports, and rotation

License-Bypass Binary Overwrite (`PowerMTA5.0.rpm`, `pmtad`, and `pmtahttpd`)

Within the 63-entry PowerMTA cluster (**414,333,861** bytes), `Workbench A` stages a two-step installation and binary replacement workflow:

1. **Base RPM setup.** Three paths hold identical **56,454,004**-byte `PowerMTA5.0.rpm` packages beside an **87,031,808**-byte v5 kit ZIP. Installing the RPM creates `/etc/pmta/` configs, service scripts, and `/usr/sbin/` binary targets.
2. **Patched ELF overwrite.** Both `/root/` and `/downloads/` stage `/patch/usr/sbin/` folders holding `pmtad` (**34,673,216** B x **2**) and `pmtahttpd` (**41,204,416** B x **2**). Scripts copy them over `/usr/sbin/` to bypass license checks while keeping virtual-MTA (`vmta`) IP rotation.

Two Panel Archives, Four ESP Installers, `ionCube` Loaders, and Legacy CentOS RPMs

While `pmtad` manages raw SMTP queues, web ESP frontends are designed to manage target lists, HTML templates, tracking URLs, and bounce hooks. `Workbench A` stages panel archives for MailWizz and Interspire plus four installer scripts (three measured at **3,869–3,959** lines), PHP bytecode loaders, and legacy OS packages (Table 4).

Component group	Staged filename	Size (bytes)	Count / lines	Role in staged bulk-mail stack
MailWizz	`mailwizz.zip` / `mailwizzinstaller7.sh` / `mailwizz.sql`	105,906,176 / 155,121 / 540,981	3,869 lines	PHP panel (**105.91 MB**), CentOS 7 LAMP + MTA installer, and MySQL schema.
Interspire	`interspire-2015.zip` / `interspireinstaller6.sh` / `interspire-2015.sql`	41,148,584 / 159,236 / 2,573,805	3,959 lines	**2015** panel (**41.15 MB**), CentOS 6 installer, schema, and `addons.zip` (33,486,401 B).
Mumara	`mumarainstaller6.sh` / `mumara_email_blacklist.zip`	153,415 / 36,564,827	`.sh` + ZIP	Automated Mumara installer (line count unrecorded; no panel ZIP) paired with a **36.56 MB** blacklist archive.
SparkMail	`sparkmail.sh`	158,681	3,947 lines	Shell installer provisioning SparkMail frontend and mail relay packages (no panel ZIP staged).

Component group	Staged filename	Size (bytes)	Count / lines	Role in staged bulk-mail stack
ioncube	`ioncube_loader_lin_5.6.so` & `5.3.so`	1,483,032 & 1,042,240	3 paths each	Shared objects decoding PHP 5.3 and PHP 5.6 bytecode in older add-ons.
Legacy OS	6 `/osupdatex/` RPMs + `phpMyAdmin-4.2.1.zip`	85,124 + 9,618,356	6 RPMs + ZIP	`epel-release`, `remi-release`, and `rpmforge-release` for CentOS 6/7 plus `phpMyAdmin 4.2.1`.

Deploying `ioncube_loader_lin_5.3.so`, `ioncube_loader_lin_5.6.so`, `phpMyAdmin-4.2.1.zip`, and end-of-life CentOS 6/7 RPMs widens a server's attack surface on public cloud networks. Older **2015** PHP panels require discontinued PHP **5.3** and **5.6** packages, so `/osupdatex/` mirrors legacy repository RPMs directly.

4. Suppression SQL Databases, Domain Rotation Scripts, and DNS Modules

Two hurdles slow bulk lure delivery on a fresh VPS: **early bounce or spam-trap blocks** and **domain or IP blacklisting** once filters react. `Workbench A` addresses both hurdles through `/Install/dbs/`, four rotation scripts, and `/setupxmpta/`. Figure 4 reconciles all **144** files and **827.50 MB** across `Workbench A`.



Figure 4: How 827.50 MB of MTA binaries, ESP panels, and SQL lists split on TCP 80

Suppression and Schema Files (213,299,034 Bytes Across 5 Files)

Sending large mail waves to dead addresses (**550** hard bounces) or spam traps triggers rapid IP throttling at major mailbox providers (`[REF-05]`). Table 5 reconciles all five database dumps inside `/Install/dbs/` (**213,299,034** bytes = **213.30 MB**, or **25.78%** of workbench bytes).

Staged `/Install/dbs/` path	Size (bytes)	Share (%)	Class	Role in staged kit

`/Install/dbs/mw_email_blacklist.sql`	117,814,881	52.89%	`data`	Staged MailWizz blacklist SQL file (112.81 MB); file name suggests data intended to limit bounces (rows unverified).
`/Install/dbs/email_banned_emails.sql`	60,804,540	28.51%	`data`	Staged banned-address SQL file (60.80 MB); file name suggests data intended to limit bounces (no imports observed).
`/Install/dbs/mumara_email_blacklist.zip`	36,564,827	17.14%	`archive`	Compressed Mumara blacklist archive (36.56 MB) for `mumarainstaller6.sh` (contents unverified).
`/Install/dbs/interspire-2015.sql`	2,573,805	1.21%	`data`	Baseline SQL schema and seed tables (2.57 MB) for `interspire-2015.zip`.

`/Install/dbs/mailwizz.sql`	540,981	0.25%	`data`	Baseline SQL schema (540.98 KB) for `mailwizz.zip`.
Total (`/Install/dbs/` , 5 files)	**213,299,034**	**100.00%**	4 SQL + ZIP	176,734,207 B raw `.sql` + 36,564,827 B `.zip` = 213.30 MB.

Legitimate senders keep suppression lists for user opt-outs. On `Workbench A`, three blacklist-named files total **210,184,248 bytes (210.18 MB)** alongside two baseline panel schemas (**3,114,786** bytes). The file names suggest data intended to limit bounces; no email rows, imports, or sending outcomes were verified.

Automated Domain/IP Rotation and `/setupxmpta/` SPF/DKIM/DMARC Scripts

When a domain or IP hits blocklists, staged shell scripts swap sender identities without rebuilding the server. Table 6 summarizes the rotation, `/setupxmpta/`, and cleanup scripts staged on `Workbench A`.

Script group	Staged scripts & sizes	Operational purpose
Domain & IP rotators (4 files, 28,479 B)	`trocadominio-2015.sh` (8,051 B), `mwchangedomain.sh` (7,998 B), `iemchangedomain.sh` (7,965 B), `changeip.sh` (4,465 B).	Rewrite web vhosts, ESP URLs, and `/etc/pmta/` virtual-MTA IPv4 bindings.

Script group	Staged scripts & sizes	Operational purpose
DNS, IP & relay setup (`/setupxmpta/`)	`2dnsupdate.sh` (145 B), `4dbintil.sh` (133 B), `6ipconfig.sh` (145 B), `8mtamaster.sh` (145 B), `9proxysetup.sh` (141 B).	Configure DNS zones, DB init, multi-IP bindings, master relays, and proxies.
Email auth modules (`/setupxmpta/`)	`10dmarcsys.sh` (141 B, `[REF-01]`), `11dkimpuyr.sh` (145 B, `[REF-03]`), `12spfupdate.sh` (149 B, `[REF-02]`), plus 7 other entries (2,795 B total).	Format `DMARC` , `DKIM` , and `SPF` records across 12 numbered modules and 3 helpers.
Cleanup & assets (9 files, 2,439,332 B)	`/downloads/clean.sh` (1,415 B), `/root/clean.sh` + `.1` - `.3` (1,336 B x 4), `index.zip` (1.67 MB), 2 JPEGs (763,934 B).	Clear mail queues and logs while staging web root and marketing assets.

Figure 2 maps selected hunts across the six functional clusters on `Workbench A` to the detection rules in Chapter 7.

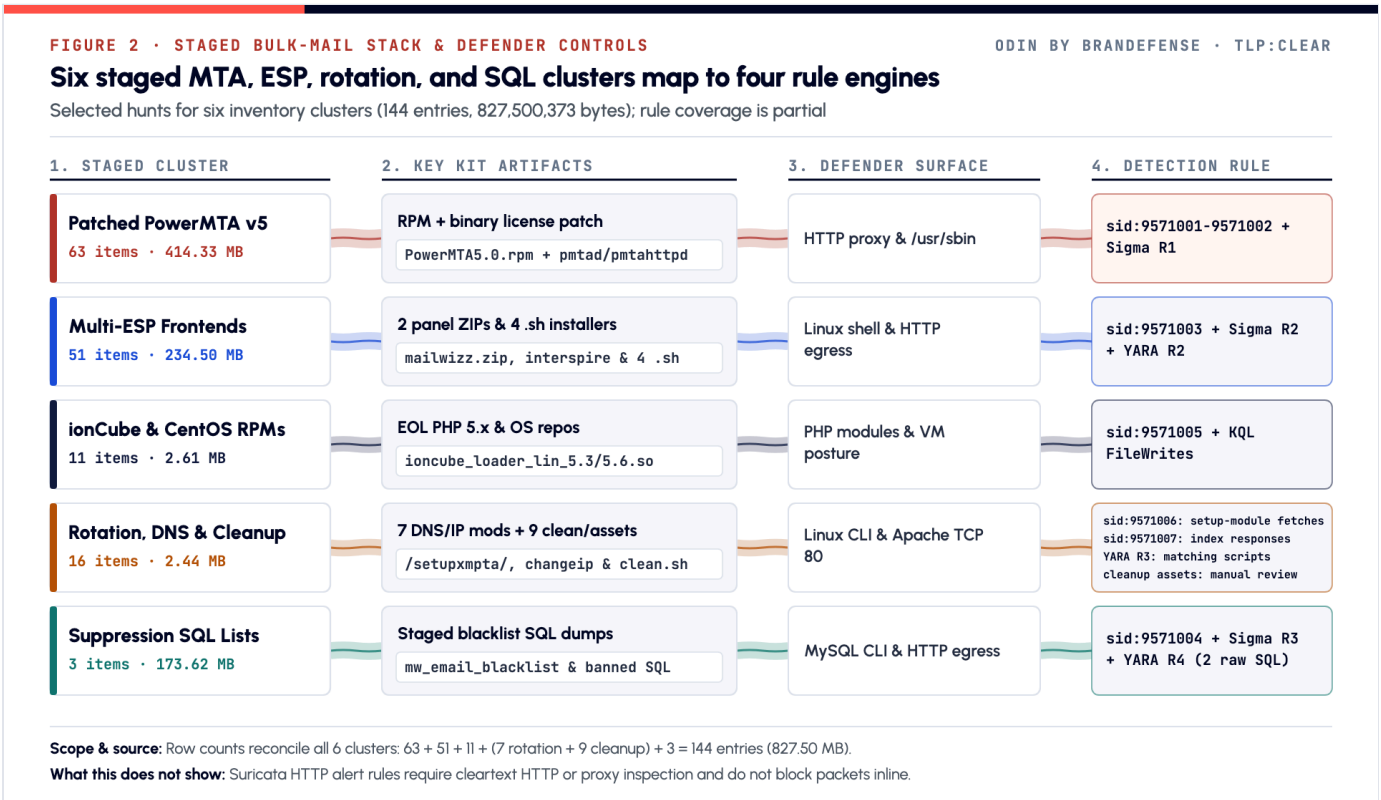

Figure 2: Six staged MTA, ESP, rotation, and SQL clusters map to four rule engines

5. Email Gateway, DNS, and Cloud Egress Exposure Analysis

Under SPF (RFC 7208 , [REF-02]), DKIM (RFC 6376 , [REF-03]), and DMARC (RFC 7489 , [REF-01]), passing email authentication confirms only that the sender controls the domain's DNS zone ([REF-05]). The staged /setupxmpta/ scripts could configure email authentication for a look-alike domain. No lure delivery or authentication-pass result was observed. Defenders should verify five controls across gateways, DNS zones, and cloud networks:

Exposure surface	Observed Workbench A evidence	Control to verify	Operational risk
Gateway trust in SPF / DKIM / DMARC	/setupxmpta/ stages 12spfupdate.sh , 11dkimpuyr.sh , 10dmarcsys.sh , and 2dnsupdate.sh .	Verify whether gateways hold mail from < 30-day domains even when SPF , DKIM , and DMARC pass ([REF-01] - [REF-03] , [REF-05]).	Staged DNS setup scripts could configure authentication on newly registered look-alike domains ([REF-05]).
Weak corporate DMARC & MTA-STS	trocadominio-2015.sh , mwchangedomain.sh , iemchangedomain.sh , and 8mtamaster.sh swap domains.	Verify whether corporate and parked domains enforce v=DMARC1; p=reject; ([REF-01]), -all SPF ([REF-02]), and MTA-STS ([REF-04]).	Domains left at p=none or ~all allow direct spoofing alongside look-alike lures ([REF-05]).
Open cloud TCP 25 / 587 egress	PowerMTA5.0.rpm (56.45 MB x 3), patched pmtad , changeip.sh , and 9proxysetup.sh .	Verify whether cloud VPCs block outbound TCP 25 from non-relay subnets and govern TCP 587 (RFC 6409 , [REF-06]).	An unmonitored cloud VM can become a high-rate pmtad relay in minutes (T1583.003).

Exposure surface	Observed `Workbench A` evidence	Control to verify	Operational risk
Staged suppression and schema files	5 `/Install/dbs/` files (213.30 MB), including 3 blacklist files (210.18 MB) and 2 panel schemas.	Verify whether gateways pair bounce telemetry with new-IP burst limits, URL sandboxing, and domain-age scoring.	Staged blacklist file names suggest data intended to limit bounces (no rows, imports, or sending outcomes verified).
Open HTTP trees & EOL PHP/CentOS	Apache `TCP 80` directory with 144 files (827.50 MB), 4 passwords, `phpMyAdmin-4.2.1.zip`, and CentOS RPMs.	Verify whether EASM checks close `Index of /` listings and ban EOL CentOS 6/7 or PHP 5.x VM images.	Open staging folders leak embedded passwords and expose unpatched web admin panels.

6. Alternative Hypotheses

Hypothesis	Evidence for	Evidence against	Assessment
Legitimate ESP mirror or licensed PowerMTA backup	Holds commercial ESP names (`MailWizz`, `Interspire`, `Mumara`), `SPF`/`DKIM` scripts, and suppression tables.	Pairs `PowerMTA5.0.rpm` with `/patch/usr/sbin/pmta*` license patches, 4 ESP installers, and IP/domain rotators on an open VPS.	**Refuted.** Classified consistently as an adversary bulk-mail workbench; IPv4 and vendor domains are withheld.
`Workbench A` **relayed live phishing waves on** `TCP 25`	Stages `pmtad`, `pmtahttpd`, 4 ESP installers, and 213.30 MB of suppression and schema files across `/root/` and `/Install/`.	Evidence comes strictly from passive HTTP `TCP 80` indexing; 0 outbound SMTP lure messages were captured from `Workbench A`.	**Unverified; framed as staged.** File presence never establishes live lure delivery or victim impact.

Hypothesis	Evidence for	Evidence against	Assessment
Shared kit filenames indicate one spam group	Directory layout mirrors a packaged v5 kit bundle alongside Portuguese (`trocadominio-2015.sh`) and English scripts.	Cracked PowerMTA + MailWizz/Interspire bundles circulate broadly across resellers and independent buyers.	**Unsupported.** Treat staged filenames as shared underground bulk-mail kits rather than one group.
The 4 script passwords grant live remote access	Static review recorded 38 endpoint and secret findings on `26 November 2026`, including 4 script passwords.	Passwords inside `.sh` installers are often default local MySQL setup strings, and 0 credentials were tested.	**Untested and withheld.** All 4 password values and host identifiers remain withheld.

7. Detection Rules for Patched MTA Kits, ESP Installers, and Suppression Imports

All host IPv4s, file SHA-256 digests, and kit reseller domains are withheld. Defenders should deploy **network URI signatures, Linux process and file hunts, and bounded YARA rules** that catch this toolkit on any host.

Each rule file underwent static verification before release. All seven Suricata **7.x** `alert http` rules (`sid:9571001`–**9571007**) passed the static Suricata linter with **0** problems. Sentinel KQL table

schemas, exact `in~` / `in` / `==` operators, Sigma `ComputerName` allowlists, and `filesize`-bounded YARA conditions were verified structurally. Native Suricata, Sentinel, Sigma, and YARA engines were not installed in this build environment, so validate alert volume in staging before rollout.

7.1 Suricata 7.x Network Signatures (`sid:9571001` -9571007)

Rules `sid:9571001`-**9571003** detect outbound HTTP `GET` fetches (`to_server`) for `PowerMTA5.0.rpm` , `/patch/usr/sbin/pmta*` binaries, and `/Install/files/` ESP archives. Rules `sid:9571004`-**9571006** detect fetches of suppression dumps, `ioncube_loader_lin_5.` modules, and `/setupxmpta/*.sh` scripts. Rule `sid:9571007` flags inbound HTTP responses (`to_client`) whose body lists both `Index of /` and `PowerMTA5.0.rpm`.

All seven HTTP signatures require cleartext HTTP traffic or a TLS-terminating proxy. Every rule uses `alert` mode and logs detections without dropping packets inline.

```
SURICATA

# Odin by Brandefense - Monograph 71 Suricata 7.x Ruleset
# Covers unlicensed PowerMTA5.0.rpm fetches, patched pmtad/pmtahttpd binaries, bundled
ESP archives, suppression SQL lists, legacy ionCube loaders, /setupxmpta/ modules, and
Apache directory listings.

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R71 Outbound Unlicensed Packag
e Fetch. PowerMTA5.0.rpm"; flow:established,to_server; http.method; content:"GET"; bsiz
e:3; http.uri; content:"PowerMTA5.0.rpm"; nocase; fast_pattern; classtype:policy-violat
ion; sid:9571001; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R71 Outbound Patched Daemon Fe
tch. Binary pmtad or pmtahttpd"; flow:established,to_server; http.method; content:"GE
T"; bsize:3; http.uri; content:"/patch/usr/sbin/pmta"; fast_pattern; pcre:"//patch/usr/
sbin/pmta(?:d|httpd)$/"; classtype:trojan-activity; sid:9571002; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R71 Outbound Bundled ESP Fetc
h. MailWizz or Interspire"; flow:established,to_server; http.method; content:"GET"; bsi
ze:3; http.uri; content:"/Install/files/"; fast_pattern; pcre:"//Install/files/(?:mailw
izz|interspire-2015|addons).zip$/i"; classtype:policy-violation; sid:9571003; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R71 Outbound Suppression Dump
Fetch. Email Blacklist"; flow:established,to_server; http.method; content:"GET"; bsize:
3; http.uri; content:"email_b"; nocase; fast_pattern; pcre:"/(?:mw_email_blacklist.sql|
email_banned_emails.sql|mumara_email_blacklist.zip)$/i"; classtype:trojan-activity; si
d:9571004; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R71 Outbound Legacy PHP Loader
Fetch. Module ionCube"; flow:established,to_server; http.method; content:"GET"; bsize:
3; http.uri; content:"ioncube_loader_lin_5."; fast_pattern; classtype:policy-violation;
sid:9571005; rev:1;)
```

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R71 Outbound Rotation Module F
etch. Script setupxmpta"; flow:established,to_server; http.method; content:"GET"; bsiz
e:3; http.uri; content:"/setupxmpta/"; fast_pattern; content:".sh"; distance:0; classty
pe:trojan-activity; sid:9571006; rev:1;)
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-R71 Inbound Apache Open Direct
ory. Exposes PowerMTA5.0.rpm"; flow:established,to_client; http.response_body; conten
t:"Index of /"; content:"PowerMTA5.0.rpm"; distance:0; fast_pattern; classtype:bad-unkn
own; sid:9571007; rev:1;)
```

7.2 Microsoft Sentinel KQL Hunt

This **7**-day query unions process, file, and network events, then summarizes hits by `DeviceName` and `AccountName`. Its network branch (`UnapprovedSmtpEgress`) checks outbound SMTP connections on exact ports **25**, **465**, **587**, and **2525** (`RFC 6409` , `[REF-06]`); inspect HTTP proxy logs for full download URLs. Replace `mta-relay-01.corp.example` and `esp-admin-01.corp.example` in `ApprovedMailRelayHosts` before scheduling.

```KQL
// Odin by Brandefense - Monograph 71
// Hunts patched PowerMTA daemon replacements, automated ESP installers, suppression SQ
L imports, and unapproved SMTP egress.
let Lookback = 7d;
let ApprovedMailRelayHosts = dynamic(["mta-relay-01.corp.example", "esp-admin-01.corp.e
xample"]);
let EspAndRotationScripts = dynamic([
    "mailwizzinstaller7.sh", "interspireinstaller6.sh", "mumarainstaller6.sh", "sparkma
il.sh",
    "trocadominio-2015.sh", "mwchangedomain.sh", "iemchangedomain.sh", "changeip.sh",
"/setupxmpta/"
]);
let PatchedMtaAndEspInstallerProcesses =
    DeviceProcessEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedMailRelayHosts))
    | where (
        (FileName in~ ("rpm", "yum", "dnf", "cp", "install", "mv", "chmod")
            and ProcessCommandLine has_any ("PowerMTA5.0.rpm", "/patch/usr/sbin/pmtad",
"/patch/usr/sbin/pmtahttpd"))
        or (FileName in~ ("bash", "sh") and ProcessCommandLine has_any (EspAndRotationS
cripts))
        or (FileName in~ ("mysql", "mariadb")
            and ProcessCommandLine has_any ("mw_email_blacklist.sql", "email_banned_ema
ils.sql", "mumara_email_blacklist"))
```

```
    )
    | project Timestamp, DeviceName, AccountName, SignalType = "PatchedMtaOrEspKitExe
c", Detail = ProcessCommandLine;
let PatchedDaemonAndLoaderFileWrites =
    DeviceFileEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedMailRelayHosts))
    | where ActionType in ("FileCreated", "FileModified", "FileRenamed")
    | where (
        (FolderPath == "/usr/sbin" and FileName in ("pmtad", "pmtahttpd"))
        or FileName in~ (
            "ioncube_loader_lin_5.6.so", "ioncube_loader_lin_5.3.so",
            "mw_email_blacklist.sql", "email_banned_emails.sql", "PowerMTA5.0.rpm"
        )
    )
    | project Timestamp, DeviceName, AccountName = InitiatingProcessAccountName,
        SignalType = "MtaDaemonOrSuppressionWrite",
        Detail = strcat(InitiatingProcessFileName, " -> ", FolderPath, "/", FileName);
let UnapprovedSmtpEgress =
    DeviceNetworkEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedMailRelayHosts))
    | where InitiatingProcessFileName in~ ("pmtad", "pmtahttpd", "php", "php-fpm", "cur
l", "wget")
    | where RemotePort in (25, 465, 587, 2525)
    | project Timestamp, DeviceName, AccountName = InitiatingProcessAccountName,
        SignalType = "UnapprovedSmtpEgress",
        Detail = strcat(InitiatingProcessFileName, " -> ", RemoteIP, ":", tostring(Remo
tePort));
union PatchedMtaAndEspInstallerProcesses, PatchedDaemonAndLoaderFileWrites, UnapprovedS
mtpEgress
| summarize FirstSeen = min(Timestamp), LastSeen = max(Timestamp), EventCount = count
(),
    Signals = make_set(SignalType, 6), SampleDetails = make_set(Detail, 5) by DeviceNam
e, AccountName
| order by LastSeen desc
```

7.3 Portable Linux Sigma Rules (3 Rules)

Rule 1 flags `rpm`, `yum`, `cp`, `install`, `mv`, or `chmod` commands referencing `PowerMTA5.0.rpm` or `/patch/usr/sbin/pmta*` outside `mta-relay-01.corp[.]example`. Rule 2 catches `bash` or `sh` running the four ESP installers, four domain/IP rotators, or `/setupxmpta/` outside `esp-admin-01.corp[.]example`. Rule 3 flags MySQL, MariaDB, or shell imports of the staged suppression lists.

```yaml
title: Patched PowerMTA Daemon Overwrite or Unmanaged RPM Installation
id: 71a9d420-5e31-4c28-9b11-71d20f59b301
status: experimental
description: Detects Linux package or file commands installing PowerMTA5.0.rpm or overw
riting /usr/sbin/pmtad and /usr/sbin/pmtahttpd from a staged /patch/usr/sbin/ director
y.
author: Odin by Brandefense
date: 2026-11-27
logsource:
  category: process_creation
  product: linux
detection:
  selection_bin:
    Image|endswith:
      - '/rpm'
      - '/yum'
      - '/cp'
      - '/install'
      - '/mv'
      - '/chmod'
  selection_mta_patch:
    CommandLine|contains:
      - 'PowerMTA5.0.rpm'
      - '/patch/usr/sbin/pmtad'
      - '/patch/usr/sbin/pmtahttpd'
  filter_relay_hosts:
    ComputerName:
      - 'mta-relay-01.corp.example'
  condition: (selection_bin and selection_mta_patch) and not filter_relay_hosts
falsepositives:
  - Authorized mail-transfer-agent maintenance on designated corporate relay servers
level: high
tags:
  - attack.resource-development
  - attack.t1608.002
  - attack.t1583.003
---
title: Bulk-Mail ESP Automated Installer or Domain and IP Rotation Script Execution
id: 71a9d420-5e31-4c28-9b11-71d20f59b302
status: experimental
description: Detects shell execution of turnkey MailWizz, Interspire, Mumara, or SparkM
ail installers alongside domain/IP rotation scripts and /setupxmpta/ DNS modules.
author: Odin by Brandefense
date: 2026-11-27
logsource:
```

```
  category: process_creation
  product: linux
detection:
  selection_shell:
    Image|endswith:
      - '/bash'
      - '/sh'
  selection_kit_scripts:
    CommandLine|contains:
      - 'mailwizzinstaller7.sh'
      - 'interspireinstaller6.sh'
      - 'mumarainstaller6.sh'
      - 'sparkmail.sh'
      - 'trocadominio-2015.sh'
      - 'mwchangedomain.sh'
      - 'iemchangedomain.sh'
      - 'changeip.sh'
      - '/setupxmpta/'
  filter_esp_hosts:
    ComputerName:
      - 'esp-admin-01.corp.example'
  condition: (selection_shell and selection_kit_scripts) and not filter_esp_hosts
falsepositives:
  - Isolated security lab VMs analyzing bulk-mail installer script behavior
level: high
tags:
  - attack.resource-development
  - attack.t1583.003
---
title: Blacklist-Named Bulk-Mail Suppression SQL Import
id: 71a9d420-5e31-4c28-9b11-71d20f59b303
status: experimental
description: Detects MySQL, MariaDB, or shell database initialization importing blackli
st-named suppression SQL dumps staged with bulk-mail kits.
author: Odin by Brandefense
date: 2026-11-27
logsource:
  category: process_creation
  product: linux
detection:
  selection_db_or_shell:
    Image|endswith:
      - '/mysql'
      - '/mariadb'
      - '/bash'
      - '/sh'
  selection_suppression_sql:
```

```
    CommandLine|contains:
      - 'mw_email_blacklist.sql'
      - 'email_banned_emails.sql'
      - 'mumara_email_blacklist'
      - '4dbintil.sh'
  filter_esp_hosts:
    ComputerName:
      - 'esp-admin-01.corp.example'
  condition: (selection_db_or_shell and selection_suppression_sql) and not filter_esp_h
osts
falsepositives:
  - Approved marketing database migrations on designated ESP administration hosts
level: medium
tags:
  - attack.resource-development
  - attack.initial-access
  - attack.t1608.002
```

7.4 Structural `filesize`-Bounded YARA Rules (4 Rules)

Four bounded YARA rules match PowerMTA license-patch scripts (**< 512KB**) and `ionCube` ESP installer scripts (**< 512KB**). Rules 3 and 4 match `SPF` / `DKIM` rotation scripts (**< 64KB**) and `mw_email_blacklist` or `email_banned_emails` SQL dumps (**< 120MB**). Scope Rule 4 to unapproved mail staging hosts rather than authorized marketing DB backups.

```
YARA
/*
   Odin by Brandefense - Monograph 71 YARA Suite
   4 filesize-bounded structural rules covering patched PowerMTA v5 installer scripts,
   multi-ESP ionCube setup scripts, domain/IP/SPF/DKIM rotation modules, and blacklist-
named suppression SQL dumps.
*/

rule ODIN_WB71_PowerMTA_Daemon_License_Patch_Installer
{
    meta:
        author = "Odin by Brandefense"
        monograph = "71"
        description = "Detects shell installer scripts pairing PowerMTA5.0.rpm with /pa
tch/usr/sbin/ pmtad or pmtahttpd daemon overwrites"
        date = "2026-11-27"
    strings:
        $rpm = "PowerMTA5.0.rpm" ascii nocase
```

```
        $patch = "/patch/usr/sbin/" ascii
        $d1 = "pmtad" ascii
        $d2 = "pmtahttpd" ascii
        $svc1 = "service pmta" ascii
        $svc2 = "systemctl" ascii
    condition:
        filesize < 512KB and $rpm and $patch and ($d1 or $d2) and ($svc1 or $svc2)
}

rule ODIN_WB71_MultiESP_IonCube_Installer_Script
{
    meta:
        author = "Odin by Brandefense"
        monograph = "71"
        description = "Detects turnkey bulk-mail ESP installer scripts combining legacy
ionCube PHP 5.x loaders with bundled MailWizz, Interspire, or Mumara archives"
        date = "2026-11-27"
    strings:
        $ic1 = "ioncube_loader_lin_5." ascii
        $ic2 = "zend_extension" ascii
        $esp1 = "mailwizz.zip" ascii nocase
        $esp2 = "interspire-2015.zip" ascii nocase
        $esp3 = "mumara_email_blacklist.zip" ascii nocase
        $esp4 = "phpMyAdmin-4.2.1.zip" ascii nocase
    condition:
        filesize < 512KB and $ic1 and $ic2 and ($esp1 or $esp2 or $esp3 or $esp4)
}

rule ODIN_WB71_Domain_IP_SPF_DKIM_Rotation_Script
{
    meta:
        author = "Odin by Brandefense"
        monograph = "71"
        description = "Detects shell scripts automating virtual-MTA IP/domain rotation
alongside SPF, DKIM, or DMARC record templates"
        date = "2026-11-27"
    strings:
        $auth1 = "v=spf1" ascii nocase
        $auth2 = "v=DMARC1" ascii nocase
        $auth3 = "opendkim" ascii nocase
        $mta1 = "vmta" ascii
        $mta2 = "/etc/pmta/config" ascii
        $mut1 = "sed -i" ascii
        $mut2 = "ip addr" ascii
    condition:
        filesize < 64KB and ($auth1 or $auth2 or $auth3) and ($mta1 or $mta2) and ($mut
1 or $mut2)
```

```
}

rule ODIN_WB71_BulkMail_Suppression_SQL_Dump_Header
{
    meta:
        author = "Odin by Brandefense"
        monograph = "71"
        description = "Detects blacklist-named SQL dump files defining mw_email_blackli
st or email_banned_emails suppression tables for analyst triage on mail staging hosts"
        date = "2026-11-27"
    strings:
        $sql1 = "CREATE TABLE" ascii nocase
        $sql2 = "INSERT INTO" ascii nocase
        $tbl1 = "mw_email_blacklist" ascii nocase
        $tbl2 = "email_banned_emails" ascii nocase
    condition:
        filesize < 120MB and ($sql1 or $sql2) and ($tbl1 or $tbl2)
}
```

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

The Indicators tab holds **0** published IPv4 addresses and **0** file SHA-256 digests. Defenders can hunt across web proxies, Linux EDR, MySQL logs, and VPC flow logs using the **10** behavioral and protocol markers below.

Marker category	Pattern / behavioral marker	Layer	Defensive hunt & control
PowerMTA RPM fetch	`GET /*PowerMTA5.0.rpm` (56.45 MB)	HTTP egress	Alert via `sid:9571001`, proxy logs, and Sigma Rule 1. Block unapproved `.rpm` fetches from raw IPs.

Marker category	Pattern / behavioral marker	Layer	Defensive hunt & control
Patched MTA daemons	`/patch/usr/sbin/pmtad` & `pmtahttpd`	HTTP / Host	Alert via `sid:9571002`, KQL `DeviceFileEvents`, Sigma Rule 1; use YARA Rule 1 on related installer scripts. Check `/usr/sbin/pmta*`.
Bundled ESP ZIPs	`GET /Install/files/mailwizz.zip`, `interspire-2015.zip`, `addons.zip`	HTTP egress	Alert via `sid:9571003`, outbound HTTP proxy logs; use YARA Rule 2 on related installer scripts.
Turnkey ESP `.sh`	`mailwizzinstaller7.sh`, `interspireinstaller6.sh`, `mumarainstaller6.sh`, `sparkmail.sh`	Linux CLI	Alert via Sentinel `DeviceProcessEvents`, Sigma Rule 2, and YARA Rule 2 on cloud Linux VMs.
Suppression SQL lists	`mw_email_blacklist.sql`, `email_banned_emails.sql`, `mumara_email_blacklist.zip`	HTTP / MySQL	Alert via `sid:9571004`, Sentinel KQL, Sigma Rule 3; use YARA Rule 4 on the two raw SQL files after extraction, not on the ZIP.
EOL `ionCube .so`	`ioncube_loader_lin_5.6.so` & `5.3.so`	HTTP / PHP	Alert via `sid:9571005` and KQL `DeviceFileEvents`. Ban EOL PHP 5.x runtimes in VM baselines.

Marker category	Pattern / behavioral marker	Layer	Defensive hunt & control
Domain & IP rotators	`trocadominio-2015.sh`, `mwchangedomain.sh`, `iemchangedomain.sh`, `changeip.sh`	Linux CLI	Alert via Sigma Rule 2, Sentinel KQL, and YARA Rule 3.
`/setupxmpta/` modules	12 numbered DNS, IP, MTA, proxy, DMARC, DKIM, and SPF `.sh` modules	HTTP / CLI	Alert via `sid:9571006`, Sigma Rule 2, Sentinel KQL, and YARA Rule 3.
EOL CentOS & DB UI	`/osupdatex/centos/6-7/` RPMs + `phpMyAdmin-4.2.1.zip`	Host / EASM	Audit cloud VMs for EOL CentOS 6/7 repos and exposed `phpMyAdmin` panels.
Open index & SMTP ports	`Index of /` + `PowerMTA5.0.rpm` & `TCP 25/465/587/2525`	HTTP / VPC	Alert via `sid:9571007` and KQL `UnapprovedSmtpEgress`. Block `TCP 25` egress in cloud VPCs (`[REF-06]`).

9. Hardening Priorities for Email Gateways, Domains, and Cloud VPCs

Email architects, cloud engineers, and SOC teams can close these bulk-mail and rotation gaps in five steps:

1. **Hold or sandbox mail from newly registered domains (`0-48 Hours`).** Because `/setupxmpta/` scripts align `SPF`, `DKIM`, and `DMARC` on fresh domains (`[REF-01]` - `[REF-03]`), never let passing auth skip phishing checks (`[REF-05]`). Quarantine or rewrite URLs in mail from **< 30**-day or first-seen domains (`[REF-05]`).

2. **Enforce `DMARC p=reject`, `-all` `SPF`, and `MTA-STS` (`0-72 Hours`).** Move active and parked domains to `v=DMARC1; p=reject;` (`[REF-01]`) and `-all` `SPF` (`[REF-02]`). Rotate **2048**-bit `DKIM` keys (`[REF-03]`) and publish `MTA-STS` in `enforce` mode (`[REF-04]`).
3. **Block direct cloud `TCP 25` relay and govern `TCP 587` (`Days 1-7`).** Deny outbound `TCP 25`, **465**, **587**, and **2525** across standard cloud subnets (`RFC 6409`, `[REF-06]`, `T1583.003`, `[REF-07]`). Restrict any configured PowerMTA web monitor with inbound access controls, and send approved app mail through allowlisted relays.
4. **Roll out proxy, EDR, and YARA rules for kit staging (`Days 7-14`).** Enable Suricata `sid:9571001`-**9571007** behind web proxies, schedule the Sentinel KQL and Sigma rules, and scan forensic images with YARA Rules 1-4 (`T1608.002`, `[REF-08]`).
5. **Close Apache directory indexes and ban EOL PHP/CentOS images (`Days 14-30`).** Set `Options -Indexes` on Apache hosts and block CentOS 6/7, PHP 5.x `ionCube`, and legacy `phpMyAdmin` packages in VM build policies.

10. Scope, Limits, and Sources

Odin by Brandefense passively analyzed an open Apache HTTP directory on `TCP 80` of `Workbench A` (`Japan-routed VPS`) recorded on `26 November 2026`. Initial directory files carried `4-9 August 2026` batch timestamps, while the `/downloads/` mirror and **38** endpoint and secret records were recorded on `26 November 2026`.

The inventory covers **21** indexed directories and **144** deduplicated sized files (**827,500,373** bytes / **827.50 MB**; **0** unsized entries). Those **144** entries reconcile across five directory zones (**58 + 49 + 15 + 13 + 9**). They also reconcile across six file classes (**87 + 30 + 11 + 10 + 4 + 2**) and six functional clusters (**63 + 51 + 11 + 9 + 7 + 3**).

Static directory listings document staged kits rather than verified outbound SMTP lure traffic. Zero binaries or scripts were run, zero passwords were tested, and zero email rows from `/Install/dbs/` were extracted. `Workbench A`'s IPv4 address, all file SHA-256 digests, **4** script password records, and all kit reseller brand prefixes and promotional domains are withheld.

1. `[REF-01]` IETF (`datatracker.ietf[.]org`), *RFC 7489 - Domain-based Message Authentication, Reporting, and Conformance (DMARC)* (verified on 27 November 2026).
2. `[REF-02]` IETF (`datatracker.ietf[.]org`), *RFC 7208 - Sender Policy Framework (SPF) for Authorizing Use of Domains in Email* (verified on 27 November 2026).

---

3. [REF-03] IETF (datatracker.ietf[.]org), *RFC 6376 - DomainKeys Identified Mail (DKIM) Signatures* (verified on 27 November 2026).
4. [REF-04] IETF (datatracker.ietf[.]org), *RFC 8461 - SMTP MTA Strict Transport Security (MTA-STS)* (verified on 27 November 2026).
5. [REF-05] NIST (csrc.nist[.]gov), *NIST SP 800-177 Rev. 1 - Trustworthy Email* (verified on 27 November 2026).
6. [REF-06] IETF (datatracker.ietf[.]org), *RFC 6409 - Message Submission for Mail (Separating Authenticated Port 587 Submission from Port 25 Relay)* (verified on 27 November 2026).
7. [REF-07] MITRE ATT&CK (attack.mitre[.]org), *Acquire Infrastructure: Virtual Private Server (T1583.003)* (verified on 27 November 2026).
8. [REF-08] MITRE ATT&CK (attack.mitre[.]org), *Stage Capabilities: Upload Tool (T1608.002)* (verified on 27 November 2026).

BRANDEFENSE CAPABILITIES RELATED TO THIS RESEARCH

Cyber Threat Intelligence

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

Phishing and Domain Abuse

Find the traffic gates and lookalike domains early.

Threat Search

Pivot on an indicator across the Brandefense dataset.

DEFENDER KIT

Indicators of compromise

Verified adversary infrastructure and tool hashes from this study. Every value below is also discussed in the report.

No network or file indicators are published for this study

The hosts in this report are exposed or unattributed systems rather than confirmed adversary infrastructure, so they stay anonymous. Use the detection rules below to find the same exposure in your own estate.

10 records from this study are not published in this table: candidate, suspected and dual-use hosts, victim-related values, and hashes of exposed secrets or files.

DEFENDER KIT

Detection rules

The rule files exactly as printed in the report. Test them in your own engine before deployment.

YARA **odin_patched_powermta_esp_and_suppression_kits.yar** 77 lines

```
/*
   Odin by Brandefense - Monograph 71 YARA Suite
   4 filesize-bounded structural rules covering patched PowerMTA v5 installer scripts,
   multi-ESP ionCube setup scripts, domain/IP/SPF/DKIM rotation modules, and blacklist
-named suppression SQL dumps.
*/

rule ODIN_WB71_PowerMTA_Daemon_License_Patch_Installer
{
    meta:
        author = "Odin by Brandefense"
        monograph = "71"
        description = "Detects shell installer scripts pairing PowerMTA5.0.rpm with /p
atch/usr/sbin/ pmtad or pmtahttpd daemon overwrites"
        date = "2026-11-27"
    strings:
        $rpm = "PowerMTA5.0.rpm" ascii nocase
        $patch = "/patch/usr/sbin/" ascii
        $d1 = "pmtad" ascii
        $d2 = "pmtahttpd" ascii
        $svc1 = "service pmta" ascii
        $svc2 = "systemctl" ascii
    condition:
        filesize < 512KB and $rpm and $patch and ($d1 or $d2) and ($svc1 or $svc2)
}

rule ODIN_WB71_MultiESP_IonCube_Installer_Script
{
    meta:
        author = "Odin by Brandefense"
        monograph = "71"
        description = "Detects turnkey bulk-mail ESP installer scripts combining legac
y ionCube PHP 5.x loaders with bundled MailWizz, Interspire, or Mumara archives"
        date = "2026-11-27"
    strings:
        $ic1 = "ioncube_loader_lin_5." ascii
        $ic2 = "zend_extension" ascii
        $esp1 = "mailwizz.zip" ascii nocase
        $esp2 = "interspire-2015.zip" ascii nocase
```

```
        $esp3 = "mumara_email_blacklist.zip" ascii nocase
        $esp4 = "phpMyAdmin-4.2.1.zip" ascii nocase
    condition:
        filesize < 512KB and $ic1 and $ic2 and ($esp1 or $esp2 or $esp3 or $esp4)
}

rule ODIN_WB71_Domain_IP_SPF_DKIM_Rotation_Script
{
    meta:
        author = "Odin by Brandefense"
        monograph = "71"
        description = "Detects shell scripts automating virtual-MTA IP/domain rotation
alongside SPF, DKIM, or DMARC record templates"
        date = "2026-11-27"
    strings:
        $auth1 = "v=spf1" ascii nocase
        $auth2 = "v=DMARC1" ascii nocase
        $auth3 = "opendkim" ascii nocase
        $mta1 = "vmta" ascii
        $mta2 = "/etc/pmta/config" ascii
        $mut1 = "sed -i" ascii
        $mut2 = "ip addr" ascii
    condition:
        filesize < 64KB and ($auth1 or $auth2 or $auth3) and ($mta1 or $mta2) and ($mu
t1 or $mut2)
}

rule ODIN_WB71_BulkMail_Suppression_SQL_Dump_Header
{
    meta:
        author = "Odin by Brandefense"
        monograph = "71"
        description = "Detects blacklist-named SQL dump files defining mw_email_blackl
ist or email_banned_emails suppression tables for analyst triage on mail staging host
s"
        date = "2026-11-27"
    strings:
        $sql1 = "CREATE TABLE" ascii nocase
        $sql2 = "INSERT INTO" ascii nocase
        $tbl1 = "mw_email_blacklist" ascii nocase
        $tbl2 = "email_banned_emails" ascii nocase
    condition:
        filesize < 120MB and ($sql1 or $sql2) and ($tbl1 or $tbl2)
}
```

Suricata `odin_patched_powermta_mailwizz_and_suppression_hunt.rules`

11 lines

```
# Odin by Brandefense - Monograph 71 Suricata 7.x Ruleset
# Covers unlicensed PowerMTA5.0.rpm fetches, patched pmtad/pmtahttpd binaries, bundled ESP archives, suppression SQL lists, legacy ionCube loaders, /setupxmpta/ modules, and Apache directory listings.

alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R71 Outbound Unlicensed Package Fetch. PowerMTA5.0.rpm"; flow:established,to_server; http.method; content:"GET"; bsize:3; http.uri; content:"PowerMTA5.0.rpm"; nocase; fast_pattern; classtype:policy-violation; sid:9571001; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R71 Outbound Patched Daemon Fetch. Binary pmtad or pmtahttpd"; flow:established,to_server; http.method; content:"GET"; bsize:3; http.uri; content:"/patch/usr/sbin/pmta"; fast_pattern; pcre:"/\/patch\/usr\/sbin\/pmta(?:d|httpd)$/"; classtype:trojan-activity; sid:9571002; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R71 Outbound Bundled ESP Fetch. MailWizz or Interspire"; flow:established,to_server; http.method; content:"GET"; bsize:3; http.uri; content:"/Install/files/"; fast_pattern; pcre:"/\/Install\/files\/(?:mailwizz|interspire-2015|addons)\.zip$/i"; classtype:policy-violation; sid:9571003; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R71 Outbound Suppression Dump Fetch. Email Blacklist"; flow:established,to_server; http.method; content:"GET"; bsize:3; http.uri; content:"email_b"; nocase; fast_pattern; pcre:"/(?:mw_email_blacklist\.sql|email_banned_emails\.sql|mumara_email_blacklist\.zip)$/i"; classtype:trojan-activity; sid:9571004; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R71 Outbound Legacy PHP Loader Fetch. Module ionCube"; flow:established,to_server; http.method; content:"GET"; bsize:3; http.uri; content:"ioncube_loader_lin_5."; fast_pattern; classtype:policy-violation; sid:9571005; rev:1;)
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ODIN-R71 Outbound Rotation Module Fetch. Script setupxmpta"; flow:established,to_server; http.method; content:"GET"; bsize:3; http.uri; content:"/setupxmpta/"; fast_pattern; content:".sh"; distance:0; classtype:trojan-activity; sid:9571006; rev:1;)
alert http $EXTERNAL_NET any -> $HOME_NET any (msg:"ODIN-R71 Inbound Apache Open Directory. Exposes PowerMTA5.0.rpm"; flow:established,to_client; http.response_body; content:"Index of /"; content:"PowerMTA5.0.rpm"; distance:0; fast_pattern; classtype:bad-unknown; sid:9571007; rev:1;)
```

Show full rule

Sentinel KQL **sentinel_patched_powermta_mailwizz_and_suppression_hunt.kql**

49 lines

```
// Odin by Brandefense - Monograph 71
// Hunts patched PowerMTA daemon replacements, automated ESP installers, suppression S
```

```
QL imports, and unapproved SMTP egress.
let Lookback = 7d;
let ApprovedMailRelayHosts = dynamic(["mta-relay-01.corp.example", "esp-admin-01.corp.
example"]);
let EspAndRotationScripts = dynamic([
    "mailwizzinstaller7.sh", "interspireinstaller6.sh", "mumarainstaller6.sh", "sparkm
ail.sh",
    "trocadominio-2015.sh", "mwchangedomain.sh", "iemchangedomain.sh", "changeip.sh",
"/setupxmpta/"
]);
let PatchedMtaAndEspInstallerProcesses =
    DeviceProcessEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedMailRelayHosts))
    | where (
        (FileName in~ ("rpm", "yum", "dnf", "cp", "install", "mv", "chmod")
            and ProcessCommandLine has_any ("PowerMTA5.0.rpm", "/patch/usr/sbin/pmta
d", "/patch/usr/sbin/pmtahttpd"))
        or (FileName in~ ("bash", "sh") and ProcessCommandLine has_any (EspAndRotation
Scripts))
        or (FileName in~ ("mysql", "mariadb")
            and ProcessCommandLine has_any ("mw_email_blacklist.sql", "email_banned_em
ails.sql", "mumara_email_blacklist"))
    )
    | project Timestamp, DeviceName, AccountName, SignalType = "PatchedMtaOrEspKitExe
c", Detail = ProcessCommandLine;
let PatchedDaemonAndLoaderFileWrites =
    DeviceFileEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedMailRelayHosts))
    | where ActionType in ("FileCreated", "FileModified", "FileRenamed")
    | where (
        (FolderPath == "/usr/sbin" and FileName in ("pmtad", "pmtahttpd"))
        or FileName in~ (
            "ioncube_loader_lin_5.6.so", "ioncube_loader_lin_5.3.so",
            "mw_email_blacklist.sql", "email_banned_emails.sql", "PowerMTA5.0.rpm"
        )
    )
    | project Timestamp, DeviceName, AccountName = InitiatingProcessAccountName,
        SignalType = "MtaDaemonOrSuppressionWrite",
        Detail = strcat(InitiatingProcessFileName, " -> ", FolderPath, "/", FileName);
let UnapprovedSmtpEgress =
    DeviceNetworkEvents
    | where Timestamp >= ago(Lookback)
    | where not(DeviceName in~ (ApprovedMailRelayHosts))
    | where InitiatingProcessFileName in~ ("pmtad", "pmtahttpd", "php", "php-fpm", "cu
rl", "wget")
```

```
    | where RemotePort in (25, 465, 587, 2525)
    | project Timestamp, DeviceName, AccountName = InitiatingProcessAccountName,
        SignalType = "UnapprovedSmtpEgress",
        Detail = strcat(InitiatingProcessFileName, " -> ", RemoteIP, ":", tostring(Rem
otePort));
union PatchedMtaAndEspInstallerProcesses, PatchedDaemonAndLoaderFileWrites, Unapproved
SmtpEgress
| summarize FirstSeen = min(Timestamp), LastSeen = max(Timestamp), EventCount = count
(),
    Signals = make_set(SignalType, 6), SampleDetails = make_set(Detail, 5) by DeviceNa
me, AccountName
| order by LastSeen desc
```

Sigma **sigma_patched_powermta_esp_installers_and_rotation.yml** 105 lines

```
title: Patched PowerMTA Daemon Overwrite or Unmanaged RPM Installation
id: 71a9d420-5e31-4c28-9b11-71d20f59b301
status: experimental
description: Detects Linux package or file commands installing PowerMTA5.0.rpm or over
writing /usr/sbin/pmtad and /usr/sbin/pmtahttpd from a staged /patch/usr/sbin/ directo
ry.
author: Odin by Brandefense
date: 2026-11-27
logsource:
  category: process_creation
  product: linux
detection:
  selection_bin:
    Image|endswith:
      - '/rpm'
      - '/yum'
      - '/cp'
      - '/install'
      - '/mv'
      - '/chmod'
  selection_mta_patch:
    CommandLine|contains:
      - 'PowerMTA5.0.rpm'
      - '/patch/usr/sbin/pmtad'
      - '/patch/usr/sbin/pmtahttpd'
  filter_relay_hosts:
    ComputerName:
      - 'mta-relay-01.corp.example'
  condition: (selection_bin and selection_mta_patch) and not filter_relay_hosts
falsepositives:
  - Authorized mail-transfer-agent maintenance on designated corporate relay servers
```

```
level: high
tags:
  - attack.resource-development
  - attack.t1608.002
  - attack.t1583.003
---
title: Bulk-Mail ESP Automated Installer or Domain and IP Rotation Script Execution
id: 71a9d420-5e31-4c28-9b11-71d20f59b302
status: experimental
description: Detects shell execution of turnkey MailWizz, Interspire, Mumara, or Spark
Mail installers alongside domain/IP rotation scripts and /setupxmpta/ DNS modules.
author: Odin by Brandefense
date: 2026-11-27
logsource:
  category: process_creation
  product: linux
detection:
  selection_shell:
    Image|endswith:
      - '/bash'
      - '/sh'
  selection_kit_scripts:
    CommandLine|contains:
      - 'mailwizzinstaller7.sh'
      - 'interspireinstaller6.sh'
      - 'mumarainstaller6.sh'
      - 'sparkmail.sh'
      - 'trocadominio-2015.sh'
      - 'mwchangedomain.sh'
      - 'iemchangedomain.sh'
      - 'changeip.sh'
      - '/setupxmpta/'
  filter_esp_hosts:
    ComputerName:
      - 'esp-admin-01.corp.example'
  condition: (selection_shell and selection_kit_scripts) and not filter_esp_hosts
falsepositives:
  - Isolated security lab VMs analyzing bulk-mail installer script behavior
level: high
tags:
  - attack.resource-development
  - attack.t1583.003
---
title: Blacklist-Named Bulk-Mail Suppression SQL Import
id: 71a9d420-5e31-4c28-9b11-71d20f59b303
status: experimental
description: Detects MySQL, MariaDB, or shell database initialization importing blackl
```

```
ist-named suppression SQL dumps staged with bulk-mail kits.
author: Odin by Brandefense
date: 2026-11-27
logsource:
  category: process_creation
  product: linux
detection:
  selection_db_or_shell:
    Image|endswith:
      - '/mysql'
      - '/mariadb'
      - '/bash'
      - '/sh'
  selection_suppression_sql:
    CommandLine|contains:
      - 'mw_email_blacklist.sql'
      - 'email_banned_emails.sql'
      - 'mumara_email_blacklist'
      - '4dbintil.sh'
  filter_esp_hosts:
    ComputerName:
      - 'esp-admin-01.corp.example'
  condition: (selection_db_or_shell and selection_suppression_sql) and not filter_esp_
hosts
falsepositives:
  - Approved marketing database migrations on designated ESP administration hosts
level: medium
tags:
  - attack.resource-development
  - attack.initial-access
  - attack.t1608.002
```

