Spam/Phishing Analysis Report

testspam analysis - run 2

2026-05-15

Spam/Phishing Analysis — 856 .eml in testspam/ (run 2)

Emails analyzed: **856** (was 506 in the previous run, +350) Confirmed phishing/scam: **~152 (17.8%)** Remainder: bulk-mailing / newsletters (commercial mass-mail, partly legitimate).

Mail server detected from headers: **SmarterMail** + Message Sniffer + GBUdb.

What changed since the previous run

1. **Botnet `103.176.192.0/24` extended to the twin `.193`**: new IPs in the `103.176.193.0/24` range (20 emails) with the same throwaway domains and exact same modus operandi (CVS/Walmart/Costco/Lowes/Omaha Steaks). Worth blacklisting the full `103.176.192.0/23` (= /23 covers both 192 and 193).
2. **Donation scam `192.93.19.27` (uha.fr)**: from 19 to **44 emails**, always the same Subject "Donazione di 2.500.000 euro", always Reply-To `jflore1942@gmail.com`. Stable pattern.
3. **New Costco campaign**: same botnet `103.176.193.x` started using the Costco brand ("Membership Ended - Costco Needs Renewal", "For Your Recent Costco Trip…"). Identical pattern to previous ones; I added `costco|cstc` to the `From-localpart` regex.
4. **Facebook badge phishing**: `support916@notifyfacebook-noreply.com` / `support164@notifyfacebook-noreply.com` — "[party]Congratulazioni! La tua pagina Facebook ha ricevuto un badge di verifica blu…". From **forged** IP headers (leading-zero values like `026.05.15.03`).
5. **Finance teaser**: new IP `159.92.157.11` with domain `news.getthefinnewsnow.com`. Subject "Silver at $309 soon?".

Italian /24s 93.174.70.0/24 and 62.97.141.0/24 are NOT phishing

They are **Italian email-marketing platforms** (mdrctr.com, MailRouter, etc.) used by dozens of distinct customers (Teamwork Events, Well Magazine, Material Preview, CAD Academy, Paysage, Sunebo, EdilSocial, Cubalatin Travel, etc.). Annoying mass-mail commercials, but legitimate; SPF/DKIM pass. **Don't blacklist the /24**: block the individual senders you're not interested in via **Blocked Senders**. Same goes for `199.244.75.99` (`turbomta@bounce.turbo-smtp.com`) — these are legitimate NDR notifications from TurboSMTP, not spam.

---

1) The 3 main phishing campaigns (90% of phishing)

A) Botnet `103.176.192.0/23` — US-brand phishing (93 of 856 emails)

Same modus operandi as the previous run, now with **range extended to `.192` and `.193`**:

1. **Sender IP** in `103.176.192.0/23` (50+ distinct IPs → botnet)
2. **From-localpart** with the brand name in clear: `cvspointsextra@…`, `harborfreighttoois@…`, `mahasteakspecial@…`, `welcomeacehardware@…`, `hellofromcvs@…`, `cstcperkperks@…`, `mahasteaksfresh@…`

3. **Sender domain** = 2 random English words, .com, unrelated to the brand
4. **English Subject** with leetspeak: `TooI`, `0maha`, `0nly`, `SampIer`, `1OO`, `5OO`, `K0BALT`, `T0day`, `Com-pIimentery`, `OnIy`, `MyL0wes`, `Walmart`, and new: `pIan` (capital I instead of l)
5. **Brands hit** (new vs before): Costco "Membership Ended", "Costco Trip"
6. **Reply-To** missing or equal to the fake From
7. **No X-Mailer**, HTML body with links to the same random sender domain

B) `192.93.19.27` (compromised uha.fr) — 419 donation scam (44 emails)

- Always the same subject: **"Donazione di 2.500.000 euro"** (Italian: "Donation of 2,500,000 euros") — doubled!
- From: rotation among compromised `@uha.fr` accounts
- **Return-Path / Reply-To: `jflore1942@gmail.com`** in all 44 emails (super-stable, perfect block target)
- Italian body: "medical diagnosis... incurable illness... donation... 2,500,000 euros"

C) `161.71.34.73-75` + `159.92.157.11` — finance/crypto teaser (8 emails)

- Subjects: **"Mark Cuban missed this one…"** (5x), **"Silver at $309 soon?"** (2x), **"Elon Warns: Exec Order 14024 Targets Dollar"** (1x)
- From: `contact@news.<random>.com` (radicaltechreveal.com, finfuturemedia.com, unicornbulletin.com, mizunoreport.com, raditentailnews.com, getthefinnewsnow.com, budgetsolutionspro.com)
- Reply-To: `reply-…@news.<random>.com` (typical fake-newsletter mismatch)

Minor campaigns (still phishing):

IP	Sender / Domain	Pattern
`52.101.52.111`	`isabel_shu_q3290@cgbedugt.onmicrosoft.com`	"Claim your Parkside 3-piece set opportunity"
`92.113.148.155`	`pointrdpwalmart@loveromantic.com`	"Walmart points are transforming to a 100 card"
`74.125.82.45-52`	`nibrash.ridge@gmail.com`	"Offer List for Crust Leather... Ridge International"
`216.24.226.93`	`contact@cldstylehouse.com`	"Re: TWO VIP BI-COASTAL EVENT PARTNERSHIPS" (fake reply)
`148.222.54.8`	`monika@eventattendlink2.shop`	"RE: 28,329 Client profiles" (fake reply)
`18037@kanu.ac.th`	reply-to `infopolice.etatlu@aol.com`	Luxembourg police scam
`dianamrsrudolf@gmail.com`	—	"HOW ARE YOU TODAY?" classic 419
`notifyfacebook-noreply.com`	`support916@…` / `support164@…`	Facebook verification badge scam

---

2) Content filter rules — ready for SmarterMail

2.1 Sender IP block (Received)

```
# Phishing botnet - block whole /23 (covers .192 and .193) - 93 emails
Received  =~  /\[103\.176\.19[23]\.\d{1,3}\]/   → DELETE
```

```
# Finance/crypto scam
Received  =~  /\[(161\.71\.34\.(73|74|75)|159\.92\.157\.11)\]/  → DELETE

# uha.fr donation scam (44 emails!)
Received  =~  /\[192\.93\.19\.27\]/             → DELETE

# Walmart/Parkside scam
Received  =~  /\[(92\.113\.148\.155|52\.101\.52\.111)\]/  → DELETE
```

In SmarterMail → **IP Address Blacklist** (Antispam → Blacklists / Blocked IP):

```
103.176.192.0/23   (= 103.176.192.0 + 103.176.193.0)
161.71.34.73
161.71.34.74
161.71.34.75
159.92.157.11
192.93.19.27
92.113.148.155
52.101.52.111
```

2.2 Sender domain block (Blocked Senders)

Botnet throwaway domains (43, updated for run 2):

```
airlinedrive.com       bidsstream.com         bankmeetings.com
booknovels.com         casemovies.com         cyclebytes.com
dragonegypt.com        expandnews.com         greathandle.com
insurearea.com         landtotal.com          laptopmind.com
lavishsport.com        letsbookmark.com       listcourse.com
logodays.com           loopcustom.com         marineleads.com
markethard.com         mattface.com           morecheaper.com
needylist.com          origamifun.com         partyteams.com
placesafety.com        playbudget.com         polkmusic.com
quotearmor.com         quotecapture.com       radiomine.com
ratebuilders.com       recipemore.com         researchbest.com
reviewhall.com         satbrowser.com         screamnews.com
sellingclick.com       soccerjacket.com       stagepreview.com
studiosilt.com         tocashback.com         webpagezone.com
webstudying.com
```

One-off campaign domains:

```
loveromantic.com           (Walmart scam)
news.finfuturemedia.com    (Elon scam)
news.mizunoreport.com
news.raditentailnews.com
news.getthefinnewsnow.com
news.budgetsolutionspro.com
radicaltechreveal.com
unicornbulletin.com
eventattendlink2.shop
cldstylehouse.com
notifyfacebook-noreply.com (Facebook badge scam)
```

Reply-To to blacklist:

```
jflore1942@gmail.com
infopolice.etatlu@aol.com
```

2.3 Subject regex — leetspeak (zero false positives, CASE-SENSITIVE)

```
\b(TooI|MaiI|SampIer|OnIy|WaImart|MyL0wes|K0BALT|T0day|Wa1mart|CompI[Ii]mentery|[1-
9]O{2,3}|0maha|0nly|pIan)\b
```

2.4 Subject regex — scam phrases (CASE-INSENSITIVE)

```
(?i)\b(donazione di [\d\.]+ euro|how are you today|hello (my )?dear|mark cuban missed|elon warns
```

2.5 From-localpart regex (CASE-INSENSITIVE)

```
(?i)^[a-z0-9._-]*(walmart|waimart|cvs|lowes|aceh?ardware|aaa[a-z]*|harborfreight|kobalt|chees
z0-9._-]*@
```

2.6 Body regex — recurring phrases

```
# Donation scam (uha.fr)
(?i)(malattia incurabile|diagnosi medica.{0,200}donazione|2\.500\.000 euro)
# Luxembourg police scam
(?i)(veuillez trouver ci-joint la convocation|Chef de police.{0,40}Luxembourg)
# US brand gift card scam
(?i)expire(s)?\s+today.{0,200}(gift card|reward|sampler|tool set|kit|points?)
# Facebook badge scam
(?i)pagina facebook.{0,30}badge.{0,30}verifica
```

---

3) NOT phishing — Italian bulk-mailing to handle differently

These sources are the bulk of the ~700 non-phishing messages. SPF/DKIM pass: they're never phishing, just **annoying commercial mass-mail**.

Source	Emails	What to do
`email.ramsesconsulting.it` (77.32.176.205)	65	Blocked Sender `*@email.ramsesconsulting.it`
`uha.fr` ← already in blacklist (donation scam, real phishing)	44	blocked above
`bounce.turbo-smtp.com` (199.244.75.99)	24	**Do NOT block** — these are legitimate NDRs
`nettowork.it`	23	Blocked Sender if not interested in recruiting
`news.teamworkevents.it` (on 93.174.70.x)	16	Blocked Sender (tourism events)
`bdmbanca.it`	12	**Do NOT block** — transactional banking, DKIM pass
`mail.pixartprinting.com`	12	Blocked Sender if not a customer
`news.wellmagazine.it` (on 93.174.70.x)	11	Blocked Sender
`pec.aruba.it`	10	**Do NOT block** — legitimate certified email

Source	Emails	What to do
email.mediaworld.it, insider.sky.it, business.facebook.com, email.ratehawk.com	<10 each	**Verify**: newsletters someone subscribed to

The entire **/24** **93.174.70.0/24** (62 emails) and **62.97.141.0/24** (20 emails) are Italian mass-mailing platforms (like MailRouter / mdrctr.com) used by many customers — **don't block the /24**, block the individual `from_domain` you're not interested in.

---

4) Compact list to paste into the mail server

4.1 IPs to blacklist (Firewall / IP Block List)

```
103.176.192.0/23
161.71.34.73
161.71.34.74
161.71.34.75
159.92.157.11
192.93.19.27
92.113.148.155
52.101.52.111
74.125.82.45
74.125.82.46
74.125.82.47
74.125.82.49
74.125.82.52
```

4.2 Domains to blacklist (Blocked Senders)

See §2.2 (43 botnet + 11 one-off campaigns + reply-to).

4.3 Subject regex (case-sensitive)

```
\b(TooI|MaiI|SampIer|OnIy|WaImart|MyL0wes|K0BALT|T0day|Wa1mart|CompI[Ii]mentery|[1-9]O{2,3}|0maha|0nly|pIan)\b
```

4.4 Subject regex (case-insensitive, scam phrases)

```
(?i)\b(donazione di [\d\.]+ euro|how are you today|hello (my )?dear|mark cuban missed|elon warns
```

4.5 From-localpart regex (case-insensitive)

```
(?i)^[a-z0-9._-]*(walmart|waimart|cvs|lowes|aceh?ardware|aaa[a-z]*|harborfreight|kobalt|chees
z0-9._-]*@
```

---

5) Estimated impact

Applying the rules above (IP + domain + Subject regex):

- **152 of 856 emails (~17.8%)** dropped immediately as confirmed phishing

- The remaining ~700 are mostly Italian commercial bulk-mail. For those:
  - raise `SmarterMail SpamAction` to `Delete` when `X-MessageSniffer-Scan-Result ≠ 0` (≈190 emails cut, no legitimate in the 856 observed)
  - add to Blocked Senders the `from_domain` listed in §3 that you don't care about

Expected false positives

Zero for: - Blacklist `103.176.192.0/23` (known Asian botnet) - Reply-To `jflore1942@gmail.com` (specific only to the donation scam) - Leetspeak regex (`TooI`, `0maha`, `100`, `SampIer`, `pIan`, etc.) — sequences impossible in legitimate mail - `From-localpart` brand-name regex (no legitimate sender uses `cvspoints@randomstuff.com`)

Sources: files analyzed in `D:\testspam\*.eml` (856 messages, run on 2026-05-15 17:13).