

FIELD NOTES FROM A PRESALES SOLUTIONS ARCHITECT

Why a Clean cPanel Mail Server Landed on Spamhaus XBL — Exim Sender Verify Callouts

A field story about a mail server that sent no spam and still landed on Spamhaus XBL — the Exim setting almost nobody checks — and the log line I now read before anyone says "we've been hacked".

Daanial Farrukh · 21 October 2026 · <https://quabin.com/spamhaus-xbl-clean-mail-server-exim-callouts/>

The alert came in at one in the morning. A blacklist monitor, one line:

Blacklists: before 1, now 4.

The server was a customer's cPanel box. Websites and mail for one company, one public IP, nothing exotic. The "1" was old news — a listing that covered the whole provider network, not this server. The jump to 4 was new.

I ran the lookups from my laptop. Two of the new listings were Spamhaus: **XBL** and **CSS**.

That is the bad one. XBL is the Exploits Blocklist. Spamhaus puts an IP there when it sees traffic that looks like malware, a botnet or an open proxy.

The Spamhaus page was blunt. The IP had been "classified as part of a proxy network". It showed one recent connection, with a timestamp and the HELO name the sender used.

The HELO was the server's own hostname. mail.example.com.

So the obvious conclusion wrote itself. "The server is compromised. Something on it is sending spam."

I didn't believe it yet. I wanted the log line first.

The Trap — A Server That Looks Guilty and Isn't

That's the trap. An XBL listing does not mean your server sent spam. It means something with your IP touched port 25 in a way that looks like a bot. Those are not the same thing.

A blacklist entry is a symptom, not a verdict.

Step One Was Proving the Server Clean

Before chasing exotic causes, I checked the boring ones. Every one of these is read-only.

The mail queue:

```
exim -bpc
```

It said 6. A server pushing spam has hundreds or thousands of messages stuck in the queue. Six is a normal night.

Live outbound connections to port 25:

```
ss -tnp state established '( dport = :25 )'
```

Empty. Nothing was talking to remote mail servers at that moment.

Who had sent mail, by authenticated user:

```
grep '<=' /var/log/exim_mainlog | grep -o 'A=dovecot_[a-z]*:[^']*' | sort | uniq -c | sort -rn  
| head -5
```

The top sender was cPanel's own notification service with 69 messages. Then real staff mailboxes with 8 to 15 each. No mailbox with thousands. No stolen password.

Then two things that kill the usual Spamhaus explanation.

Spamhaus says XBL is almost always an infected phone or a smart TV sharing the same public IP through NAT. So I checked where the IP lived:

```
ip -4 -br addr
```

The public IP was bound directly to the VM's network card. No office network behind it. No phones. Nothing else shares that address.

And cPanel's SMTP Restrictions were on:

```
whmapi1 get_tweaksetting key=smtpmailgidonly
```

value: '1'. With this on, only Exim, Mailman and root can open connections to remote port 25. A hacked WordPress plugin or a PHP script cannot reach port 25 on its own.

So the only things on this server that could have made that connection were Exim itself — or root-level malware.

The Log Line at the Exact Minute

Spamhaus gave me a time: 16:50 UTC. The server ran on local time, five hours ahead. So I read the Exim log for that window.

```
grep -E '^2026-10-20 21:(49|50|51)' /var/log/exim_mainlog
```

In those three minutes the server delivered exactly one email — a cPanel notification to a Gmail address. Normal.

But one line above it was the answer:

```
H=mail-xx.google.com sender verify defer for <random@n.spammer-domain.org>:  
Could not complete sender verify callout: n.spammer-domain.org [198.51.100.25] :  
SMTP timeout after initial connection
```

Spam had arrived through Google's servers, with a throwaway sender address. Before accepting it, Exim had **connected out on port 25 to the spammer's own mail server** to check whether that sender address

existed. The connection opened, nothing answered, and Exim gave up about a minute and a half later.

That connection was in progress at 16:50 UTC. With the server's HELO. To port 25.

I looked up who owned 198.51.100.25. It was a domain-parking provider — one IP hosting about 69,000 domains, no hostname, already flagged as abusive in public reputation databases. Not a mail server anyone runs on purpose.

How often had this happened?

```
grep -c 'Could not complete sender verify callout' /var/log/exim_mainlog
```

284 times in the current log. The same spammer domain alone had triggered it four more times that night.

What a Sender Verify Callout Actually Is

A sender verify callout is Exim pretending to deliver a reply to the sender, and hanging up before any mail is sent.

The flow looks like this:

Email arrives → Exim reads MAIL FROM: someone@sender-domain → Exim looks up the MX of sender-domain → Exim connects to that MX on port 25 → HELO mail.example.com → MAIL FROM:<> → RCPT TO:<someone@sender-domain> → reads the reply → QUIT

- Reply 250 — the address exists, Exim accepts the incoming mail.
- Reply 550 — no such user, Exim rejects the incoming mail.
- No reply or timeout — Exim defers, and the sender has to try again later.

Exim never sends DATA. No message leaves your server. But look at that conversation from the other side: an unknown server connects on port 25, says hello and asks "does this mailbox exist?" — then leaves.

That is exactly what a spambot harvesting addresses looks like.

Where callouts are common:

- Older cPanel servers where someone turned them on years ago to "fight spam" and never revisited it.
- Self-built Exim or Postfix setups copied from old tutorials.
- Servers migrated between panels, carrying old settings along.

Why Traps Count It as a Bot

Spammers love throwaway domains. Many of those domains end up parked, and their mail points at servers that have no real mailboxes at all.

A server with no mailboxes should never receive a legitimate SMTP connection. So operators of traps and sinkholes do the simple thing — they log every IP that connects on port 25 and share it with blocklists.

Here's the part that trips people up. Your server only calls out because spam arrived. The more spam you receive from throwaway domains, the more your server knocks on trap doors. **Receiving spam is what got this server listed.**

I want to be honest about what I could and could not prove. The log line, the timing, the HELO and the owner of the IP are facts. That this particular parking network feeds Spamhaus is my inference — the evidence fits, but I cannot see Spamhaus's sensor data. The real test is the next step: turn callouts off, request removal, and see whether the listing comes back.

How to Actually Fix This

Step 1: Confirm Callouts Are On

On cPanel, the Exim options live in one file.

```
grep -i callout /etc/exim.conf.localopts
```

If you see callouts=1, the server is calling out. In WHM it is Home > Service Configuration > Exim Configuration Manager > Basic Editor > ACL Options > **Sender Verification Callouts**.

Step 2: Back Up the Options File

This is the change step, so back up first.

```
cp -p /etc/exim.conf.localopts /etc/exim.conf.localopts.bak-$(date +%F)
```

Step 3: Turn Callouts Off

The easy path is the WHM toggle above: set Sender Verification Callouts to **Off** and save. WHM rebuilds the config and restarts Exim for you.

From the shell, the same change:

```
sed -i 's/^callouts=1$/callouts=0/' /etc/exim.conf.localopts
```

```
/scripts/buildeximconf
```

```
/scripts/restartsrv_exim
```

buildeximconf must say "Configuration file passes test!" before you restart. If it does not, restore the backup and stop.

Step 4: Verify

This step is where most tutorials stop and where mine starts.

```
grep -n callout /etc/exim.conf
```

What you want to see is only cache timers and comments — lines like callout_negative_expire = 1h.

What you do not want to see is any verify = sender/callout in the ACLs. If it is still there, the rebuild did not pick up your change.

Then confirm Exim is healthy and the queue is normal:

```
exim -bpc
```

Watch the main log for a few minutes. New "sender verify callout" lines should stop completely.

Step 5: Request Removal

Only now go to Spamhaus's IP check page, open the XBL entry and request removal. Removing it before the cause is gone just buys you a fresh listing tomorrow.

In this case the Spamhaus website showed the IP as clean within minutes of the request. The DNS zone that receiving mail servers actually query did not. So check the source, not a cache:

```
dig +short NS zen.spamhaus.org
```

```
dig +short 10.113.0.203.zen.spamhaus.org @a.gns.spamhaus.org
```

Reverse the IP octets for the query. An empty answer means delisted. 127.0.0.4 means XBL is still in the live zone. 127.0.0.3 is CSS. Note that Spamhaus refuses queries from big public resolvers such as 8.8.8.8, so always ask their own name servers or your own resolver.

This lag is not a bug. It is the verification.

What You Lose When Callouts Are Off

Very little. You lose one check: rejecting mail whose sender mailbox does not exist on the sender's own server.

Everything that does the real work stays on:

- 1 **Basic sender verification** — the sender domain must exist and have mail servers. This is a DNS lookup only, no outbound connection.
- 2 **RBL checks** on the connecting IP — Spamhaus, SpamCop and similar.
- 3 **SPF, DKIM and DMARC** — whether the sender is allowed to send for that domain at all.
- 4 **SpamAssassin** — content scoring, Bayes and rules.

And you gain two things. Inbound mail stops stalling — in this case a callout to a dead trap held a Gmail connection open for over a minute and a half. And your server stops knocking on doors that report you.

Also notice where this spam came from: Google's own servers. Gmail had already filtered it once. The callout added almost nothing.

A check that gets you blacklisted is not a security control.

The Bigger Lesson — Read the Listing Before Blaming the Box

When a mail server lands on XBL, this is the order I now work in:

- 1 **Which list, which code?** 127.0.0.4 is XBL, 127.0.0.3 is CSS. Different lists, different causes.
- 2 **What HELO and time did the list show?** If the HELO is your own hostname, the source may be your MTA itself.
- 3 **Is the queue normal?** `exim -bpc`
- 4 **Is the IP shared?** `ip -4 -br addr` — NAT is Spamhaus's number one cause.
- 5 **Can anything except the MTA reach port 25?** `whmapi1 get_tweaksetting key=smtpmailgidonly`

- 6 **What did the MTA do at that minute?** Read the log for the exact window, not the whole day.
- 7 **Are callouts on?** `grep -i callout /etc/exim.conf.localopts`

Only if all of these come back clean do you go hunting for rootkits.

What I Tell Every Customer Now

When a customer forwards me a blacklist alert, the first thing I ask is not "who hacked you?". It is:

"Does your mail server call out to the sender's mail server before accepting mail?"

If the answer is no, we look for real malware. If the answer is "what's a callout?", we're not done yet.

I write about the questions I ask in real customer rooms — the ones that change architectures and surface the problems no one else noticed. If you found this useful, drop your email below and I'll send the next one when it's ready.

FAQs

Does a Spamhaus XBL listing mean my server sent spam?

No. XBL means Spamhaus saw traffic from your IP that looks like malware, a botnet or a proxy, usually on port 25. That can be an infected device behind the same IP, real malware on the server, or your mail server's own sender verify callouts hitting spam traps. Prove which one with the queue, the IP layout and the Exim log before assuming a breach.

What is an Exim sender verify callout?

It is a check where Exim connects to the sender's mail server on port 25 and asks whether the sender's address exists, using `MAIL FROM:<>` and `RCPT TO`, then quits before sending any data. It was meant to reject forged senders, but to a trap server it looks exactly like a spambot testing addresses.

Is it safe to turn off Sender Verification Callouts in cPanel?

Yes for almost every server. Basic sender verification, RBL checks, SPF, DKIM, DMARC and SpamAssassin all keep working, and none of them make outbound connections to spammers. You lose only the rejection of mail from non-existent sender mailboxes, which SpamAssassin and the sender's own SPF and DMARC already cover.

Why does the Spamhaus website say clean while DNS still shows the listing?

The website reads the Spamhaus database directly, while mail servers query the DNS zone, which updates on its own schedule. Query Spamhaus's own name servers to see the live zone, and give it some hours. Public resolvers such as 8.8.8.8 are refused by Spamhaus, so they are not a reliable test.

How do I know callouts were the cause and not malware?

Match the Spamhaus timestamp and HELO against the Exim log for that exact minute, and confirm nothing else on the server can reach port 25. Then turn callouts off and request removal. If the IP stays clean for the following days, callouts were the cause; if it is listed again, start a proper compromise investigation.

Read online: <https://quabin.com/spamhaus-xbl-clean-mail-server-exim-callouts/>