

FIELD NOTES FROM A PRESALES SOLUTIONS ARCHITECT

All Three Servers Blacklisted on the Same Morning — When the Listing Is Your ASN, Not Your Server

A presales war story about a blacklist alert that hit every server at once — the sign that nothing is wrong with the servers — and the one DNS query I now run before anyone touches a mail config.

Daanial Farrukh · 24 October 2026 · <https://quabin.com/uceprotect-level-3-asn-blacklist-all-servers/>

The alert came in on a Saturday morning. Our blacklist monitor showed three servers going from 0 to 1. Three different servers, three different jobs, three different owners inside the company.

Within minutes the first message arrived in the team chat.

"All three are on a blacklist. We must be compromised."

It is a fair fear. A listing is usually what a hack looks like from the outside. I asked one question first.

"Did they go from clean to listed at different times, or all at once?"

Silence. Then: "All at once. Same check."

That was the answer. Three unrelated servers do not get hacked in the same minute. Something above the servers had changed.

The Trap, Named

That's the trap. When every server alerts together, the instinct is to open the servers. Check the logs. Check the mail queue. Reset passwords.

It all feels like work. **It is all work on the wrong layer.**

The listing was not about the servers. It was about the network they sit in.

What a UCEPROTECT Level 3 Listing Actually Is

UCEPROTECT runs a blacklist in three levels. The level tells you what is being listed:

- **Level 1** — one single IP address that sent spam to their trap.
- **Level 2** — a whole range of addresses of one provider.
- **Level 3** — a whole ASN. Every IP the network announces.

An ASN is the identity of a network on the internet. It is the number that says "this block of addresses belongs to this operator". A Level 3 listing says: **too many addresses inside this network behaved**

badly, so we list all of them.

Your server can be perfect and still be listed. It shares the number with everyone else in the network.

This is common in three places:

- A hosting provider or ISP with many customers on one ASN.
- A company with an old public range that mixes mail servers, VPN users and customer lines.
- Any network where nobody owns the question "who sends mail from this range?"

The listing page gave me the numbers. A spam score of 168.8. Six Level 1 abuser addresses seen in the last seven days. And a count of 54 "impacts" against an escalation limit of 50.

That last line is the whole mechanism. The limit was 50. The network sat at 54. Four impacts over, and the entire ASN was listed.

Why Nobody Sees It Coming

There are two reasons the usual checks miss this.

First, your own server tests show nothing. The server's own address is not listed at Level 1 or Level 2. A mail test tool that checks only the IP may show a clean result, or one confusing result among many.

Second, the cause is not on your servers at all. It is five or six addresses somewhere else in the same network, owned by people who never read your alerts.

Absence of a listing on your IP is not health. It only tells you the problem is above you.

How to Confirm It — and Fix the Right Layer

This is the part that takes ten minutes, and it saves a day of looking in the wrong place.

Step 1: Check the Level 3 list first. UCEPROTECT is queried by IP, with the octets reversed. For the address 192.0.2.10 the query is:

```
dig +short 10.2.0.192.dnsbl-3.uceprotect.net
```

If the answer is 127.0.0.2, the address is covered by a Level 3 listing. No answer means it is not. Run the same query for Level 1 and Level 2 on the same address:

```
dig +short 10.2.0.192.dnsbl-1.uceprotect.net
```

```
dig +short 10.2.0.192.dnsbl-2.uceprotect.net
```

In my case Level 3 answered and Level 1 and Level 2 did not. That combination is the proof: the server itself is not listed, its network is.

Step 2: Confirm which ASN you are in.

```
dig +short TXT 10.2.0.192.origin.asn.cymru.com
```

The first number in the answer is the ASN. Check that all three alerting servers show the same one. If they do, you are looking at the same listing three times, not three incidents.

Step 3: Find the abuser addresses. Level 3 appears when Level 1 hits pile up inside the ASN. So list every address your network announces, and ask the Level 1 list about each one. I took the prefixes from the public RIPEstat data, which gave 32,768 addresses, and ran the DNS query against all of them with asynchronous lookups, 256 at a time. It finished in a few minutes.

Five addresses were listed. Four of them were addresses nobody in the team recognised — one carried only the generic default reverse name of the provider. The fifth was a surprise.

It was the company's own mail server.

Nobody had been looking at it, because everyone assumed the problem was out there. A sixth abuser had already dropped off Level 1 by the time I scanned, which matches the six in the last-seven-days count.

Step 4: Fix it on the network side, not the server side. This is the step that is different from every other blacklist article. The people who can act are the network operations and abuse team. They can:

- Find out which customers own the listed addresses and stop the spam.
- Fix the company's own mail server, if it is on the list.
- Stop Level 1 hits from accumulating again.

Step 5: Let it expire. Level 3 listings clear on their own once the seven-day impact count falls under the limit. The listing page does not show a start date, so watch the count, not the calendar.

Never pay for express delisting. The paid removal clears the symptom and teaches the list that you will pay. The abusers are still in your network, and the count climbs again.

Plain takeaway: a Level 3 listing is fixed by cleaning five addresses, not by touching three servers.

The Bigger Lesson — Who Owns the Range?

The technical fix took one afternoon. The real gap was organisational, and it is the part I raise in the next architecture review.

Nobody owned the question "what sends mail from our address space?" The company's own mail server was on the list for a reason that nobody had looked at. Nobody could say which addresses in the range were allowed to send directly on port 25. Each team watched its own server and nobody watched the range.

Here is the short list I leave behind after a case like this:

- 1 **Know your ASN and your prefixes.** Write them down. Check them against the public registry data once a month.
- 2 **Monitor the range, not only the servers.** One scan of the whole range against the Level 1 list takes minutes. Run it on a schedule.
- 3 **Block outbound port 25 from customer lines.** Allow it only from the servers that are meant to send mail.
- 4 **Give every sending server a proper reverse name.** A generic default name is how an address ends up looking like a customer line.

- 5 **Alert on "same minute" patterns.** Several servers changing state together is a network event until proven otherwise.

Plain takeaway: a blacklist is a signal about behaviour you can see. Make sure someone is looking at all of it.

One Other Thing I Saw That Day

While checking, two other lists flagged the same servers. They looked like part of the same event. They were not.

- One list flags addresses when the registry record for the country domain has no owner email. That one is old and unrelated.
- One score service answered with 127.255.255.255. That is not a listing. It means "your query was refused", which happens when you send DNS queries through a large public resolver.

Both are noise. If you do not tell the noise from the real listing, you chase three problems and fix none.

What I Tell Every Customer Now

When more than one server alerts at the same time, I ask the team this before anyone logs in:

"Did the alerts start in the same minute?"

If the answer is yes, I run the Level 3 query on one address first. It takes ten seconds. It tells us if we should be looking at the servers or at the network.

If the answer is "different days", then it is probably the servers, and the normal checklist applies. If the answer is "same minute", we are not done until someone has looked at the ASN.

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

What is a UCEPROTECT Level 3 listing?

It is a blacklist entry that covers a whole ASN, which means every IP address a network announces. It appears when enough addresses inside that network have been listed at Level 1 within seven days. Your own server does not need to have sent any spam.

How do I know if my server is listed because of its own IP or its ASN?

Query the same address against the Level 1, Level 2 and Level 3 lists. If only Level 3 answers with 127.0.0.2, the listing is on the ASN. If Level 1 answers, the address itself is listed and you should look at that server.

How long does a Level 3 listing last?

It clears on its own once the number of Level 1 impacts in the last seven days falls under the escalation limit. In my case the limit was 50 and the network was at 54. The listing page does not show a start date, so watch the count.

Should I pay for express delisting?

No. Paying removes the entry but not the cause. The abusing addresses are still in your network, so the count rises again and the listing returns. Fix the addresses that caused the hits instead.

Does a Level 3 listing stop my email?

Only for receivers that use this list to reject mail. Many large providers do not. The risk is with smaller receivers and some corporate gateways, so watch for bounces that name the list and tell affected customers early.

Who can fix a Level 3 listing?

The network operator. The operations or abuse team can find the listed addresses, contact the customers behind them, and fix the operator's own mail servers. A single customer or server owner cannot clear it alone.

Read online: <https://quabin.com/uceprotect-level-3-asn-blacklist-all-servers/>