# Possible cache poisoning of mail-handling domains

Leigh Metcalf
Jonathan Spring

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM-0000864

# We’re here to discuss weirdness in the DNS

We’re not entirely sure what this is, but we have a good guess, and we’re pretty sure you should care.

What if your MX is not your MX?

This is not theory, this is what we observe on the wire.

# What we see

A NS providing an IP for a domain

A different NS providing a different IP *for the same domain*

You might say – that’s called a CDN stupid.

So filter those.

What’s left?  The ‘bad’ stuff.

# Who are these misbehaving NS?

Mostly seem to be out of shared-hosting environments, so it’s hard to say.

## What to do?

- DNSSEC would be the canonical answer
- The user is probably not going to be able to do much
- Enterprise, check (like we did) for NS-served domain relationship being sane (e.g., reputation services can probably do this)

# How has this gone unnoticed?

Unless you have big passive DNS collectors, no one organization can detect this because it’s distributed.

- You can’t notice a discrepancy between two values if you only ever get one value.

Data sharing! Yay data sharing!

## Probable causes?

- Compromised hosts pointed to maliciously-created NS
- Compromised legitimate NS
- We’re not sure yet.

# Questions/comments?