

# Emotet Stops Using 0.0.0.0 in Spambot Traffic - SANS ISC

By SANS Internet Storm Center

Archived: 2026-04-05 14:19:19 UTC

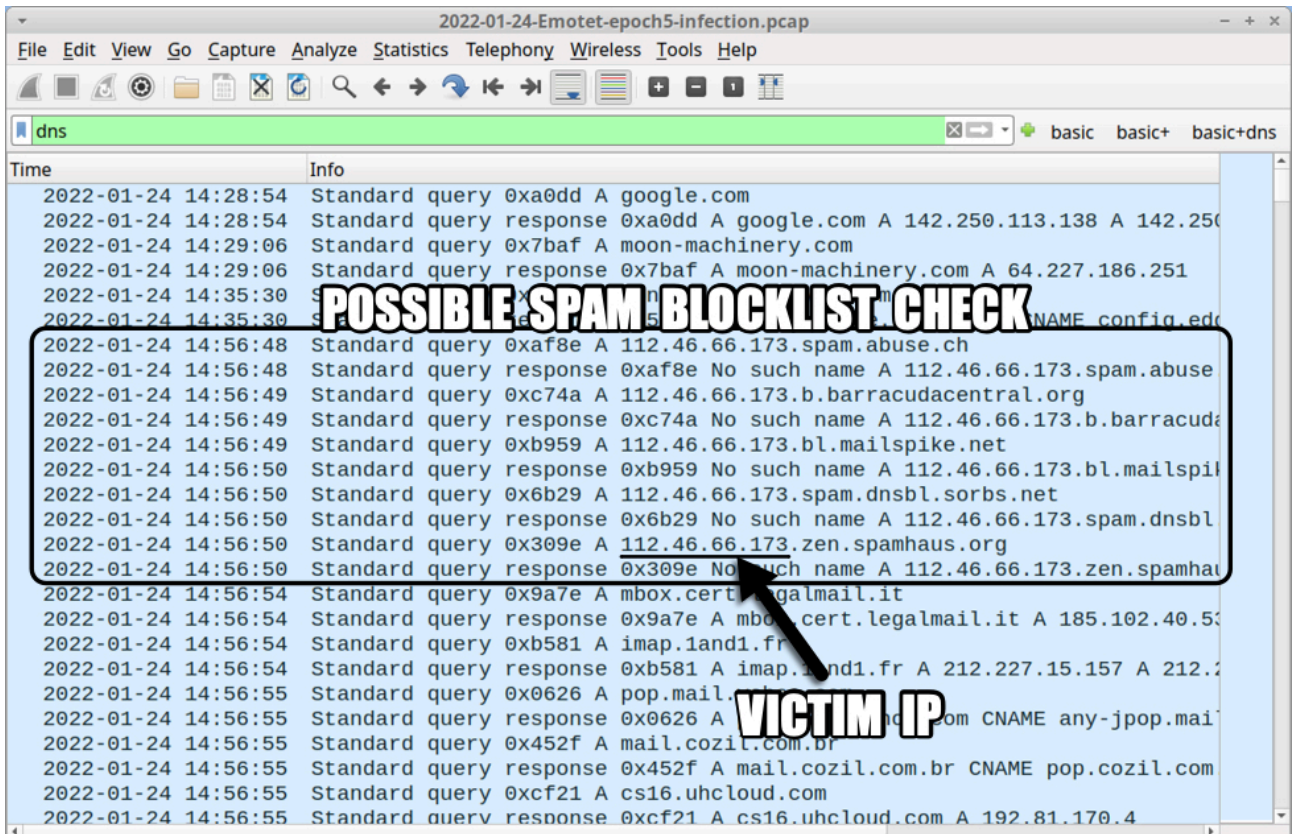
## Introduction

Last week, I wrote a diary about Emotet using **0.0.0.0** in its spambot traffic instead of the actual IP address of the infected Windows host ([link](#)).

Shortly after that diary, Emotet changed from using **0.0.0.0** to using the victim's IP address, but with the octet values listed in reverse order.

## Details

During a recent Emotet infection on Tuesday 2022-01-24, my infected Windows host was using **173.66.46.112** as its source IP. Note that my source IP has been edited for this diary to sanitize/disguise the actual IP address. See the image below for DNS traffic representing a possible spam blocklist check by my infected Windows host. In other malware families like Trickbot, the octet order is reversed. But order is not reversed for this Emotet infection.

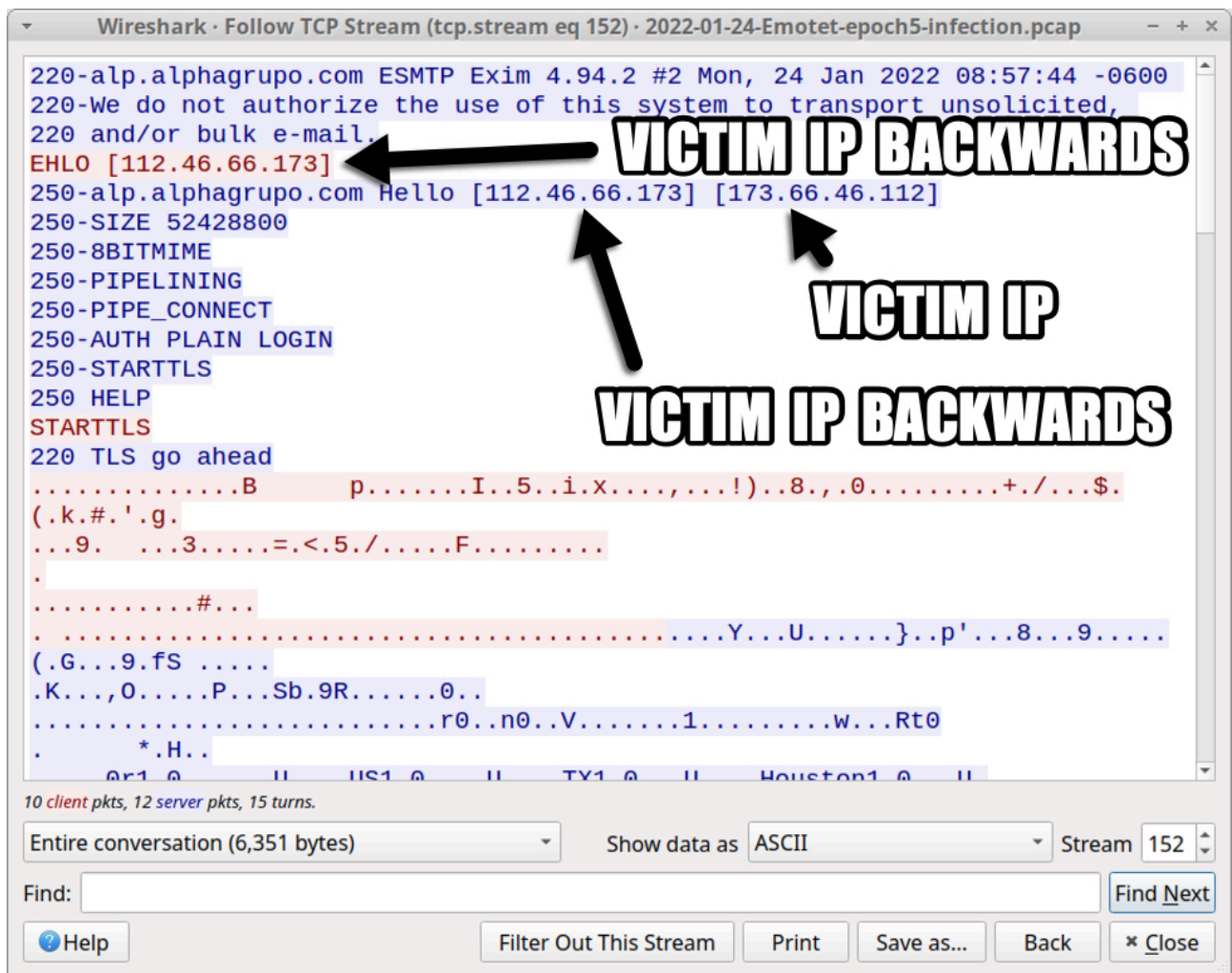


Shown above: Possibly spam blocklist check by my Emotet-infected host on Tuesday 2022-01-24.

As seen in the above image, the following DNS queries were made:

- 173.66.46.112spam.abuse.ch
- 173.66.46.112.b.barracudacentral.org
- 173.66.46.112.bl.mailspike.net
- 173.66.46.112.spam.dnsbl.sorbs.net
- 173.66.46.112.zen.spamhaus.org

Again, I normally see the octet order reversed with other malware like Trickbot. This reversed order also appeared during SMTP traffic with the command *ELHO [112.46.66.173]* as shown below.



Shown above: Victim IP address in Emotet spambot traffic on Tuesday 2022-01-24.

[Twitter discussion for last week's diary](#) indicates Emotet developers may have broken something in the spambot module to produce the previous *0.0.0.0* traffic. I'm not sure if this new traffic--the reversed order of the victim's IP address--is intentional or not.

### Final words

You can find up-to-date indicators for Emotet malware samples, URLs, and C2 IP addresses at:

- <https://urlhaus.abuse.ch/browse/tag/emotet/>
- <https://feodotracker.abuse.ch/browse/emotet/>

- <https://bazaar.abuse.ch/browse/tag/Emotet/>
- <https://threatfox.abuse.ch/browse/malware/win.emotet/>

---

Brad Duncan

brad [at] malware-traffic-analysis.net

---

Source: <https://isc.sans.edu/forums/diary/Emotet+Stops+Using+0000+in+Spambot+Traffic/28270/>