SANS ISC: Emotet Stops Using 0.0.0.0 in Spambot Traffic - SANS Internet Storm Center SANS Site Network Current Site SANS Internet Storm Center Other SANS Sites Help Graduate Degree Programs Security Training Security Certification Security Awareness Training Penetration Testing Industrial Control Systems Cyber Defense Foundations DFIR Software Security Government OnSite Training SANS ISC InfoSec Forums

isc.sans.edu/forums/diary/Emotet+Stops+Using+0000+in+Spambot+Traffic/28270/

Emotet Stops Using 0.0.0.0 in Spambot Traffic

Brad
433
Posts
ISC
Handler
Jan
25th
2022

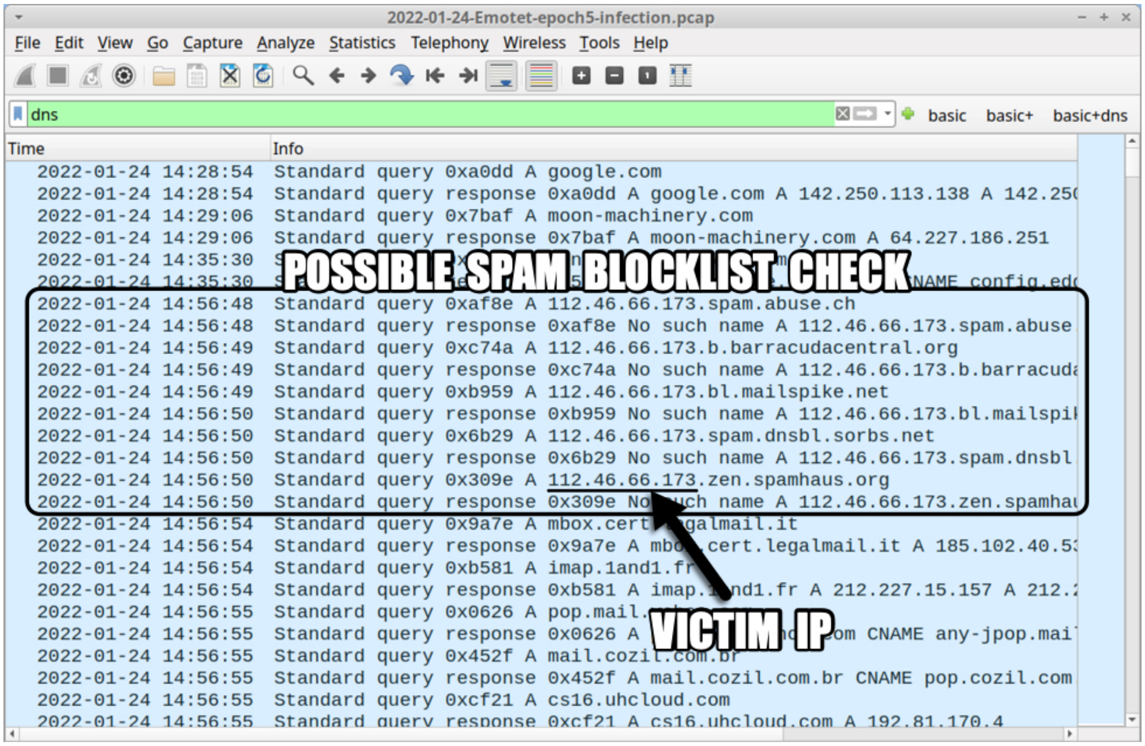
Introduction

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.


2022-01-24-Emotet-epoch5-infection.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
basic
basic+
basic+dns

POSSIBLE SPAM BLOCKLIST CHECK

VICTIM IP

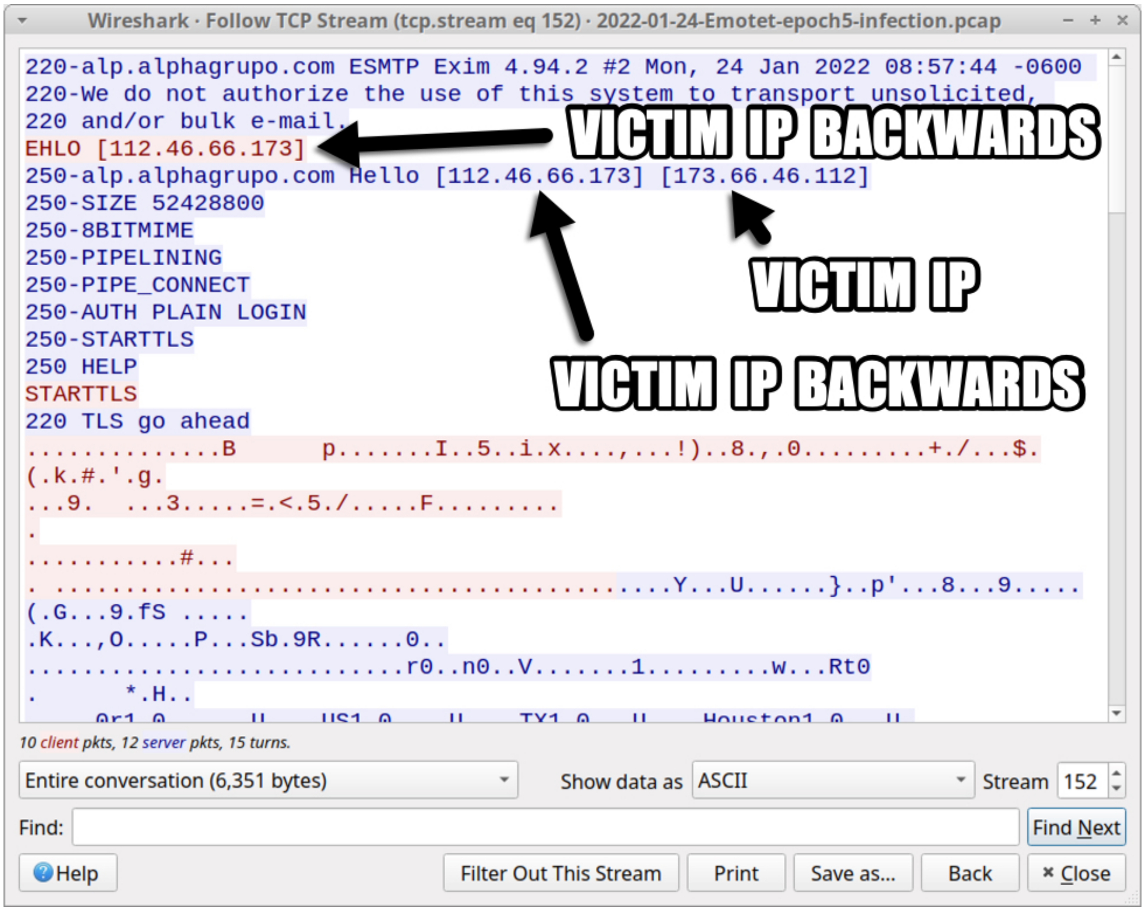
```
Time                 Info
  2022-01-24 14:28:54  Standard query 0xa0dd A google.com
  2022-01-24 14:28:54  Standard query response 0xa0dd A google.com A 142.250.113.138 A 142.250
  2022-01-24 14:29:06  Standard query 0x7baf A moon-machinery.com
  2022-01-24 14:29:06  Standard query response 0x7baf A moon-machinery.com A 64.227.186.251
  2022-01-24 14:35:30  S
  2022-01-24 14:35:30  S                                                NAME config.edc
  2022-01-24 14:56:48  Standard query 0xaf8e A 112.46.66.173.spam.abuse.ch
  2022-01-24 14:56:48  Standard query response 0xaf8e No such name A 112.46.66.173.spam.abuse
  2022-01-24 14:56:49  Standard query 0xc74a A 112.46.66.173.b.barracudacentral.org
  2022-01-24 14:56:49  Standard query response 0xc74a No such name A 112.46.66.173.b.barracuda
  2022-01-24 14:56:49  Standard query 0xb959 A 112.46.66.173.bl.mailspike.net
  2022-01-24 14:56:50  Standard query response 0xb959 No such name A 112.46.66.173.bl.mailspik
  2022-01-24 14:56:50  Standard query 0x6b29 A 112.46.66.173.spam.dnsbl.sorbs.net
  2022-01-24 14:56:50  Standard query response 0x6b29 No such name A 112.46.66.173.spam.dnsbl
  2022-01-24 14:56:50  Standard query 0x309e A 112.46.66.173.zen.spamhaus.org
  2022-01-24 14:56:50  Standard query response 0x309e No such name A 112.46.66.173.zen.spamhau
  2022-01-24 14:56:54  Standard query 0x9a7e A mbox.cert.legalmail.it
  2022-01-24 14:56:54  Standard query response 0x9a7e A mbox.cert.legalmail.it A 185.102.40.53
  2022-01-24 14:56:54  Standard query 0xb581 A imap.1and1.fr
  2022-01-24 14:56:54  Standard query response 0xb581 A imap.1and1.fr A 212.227.15.157 A 212.2
  2022-01-24 14:56:55  Standard query 0x0626 A pop.mail.
  2022-01-24 14:56:55  Standard query response 0x0626 A            om CNAME any-jpop.mai
  2022-01-24 14:56:55  Standard query 0x452f A mail.cozil.com.br
  2022-01-24 14:56:55  Standard query response 0x452f A mail.cozil.com.br CNAME pop.cozil.com
  2022-01-24 14:56:55  Standard query 0xcf21 A cs16.uhcloud.com
  2022-01-24 14:56:55  Standard query response 0xcf21 A cs16.uhcloud.com A 192.81.170.4
```

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.


Wireshark · Follow TCP Stream (tcp.stream eq 152) · 2022-01-24-Emotet-epoch5-infection.pcap
VICTIM IP BACKWARDS
VICTIM IP
VICTIM IP BACKWARDS

```
220-alp.alphagrupo.com ESMTP Exim 4.94.2 #2 Mon, 24 Jan 2022 08:57:44 -0600
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
EHLO [112.46.66.173]
250-alp.alphagrupo.com Hello [112.46.66.173] [173.66.46.112]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-PIPE_CONNECT
250-AUTH PLAIN LOGIN
250-STARTTLS
250 HELP
STARTTLS
220 TLS go ahead
..............B      p.......I..5..i.x....,...!)..8.,.0.........+./...$.
(.k.#.'.g.
...9.  ...3.....=.<.5./.....F.........
.
..........#...
. ........................................Y...U......}..p'...8...9.....
(.G...9.fS .....
.K...,O.....P...Sb.9R......0..
...........................r0..n0..V.......1.........w...Rt0
.       *.H..
     0r1.0      U    US1.0    U     TX1.0   U      Houston1.0   U
```

10 client pkts, 12 server pkts, 15 turns.

Entire conversation (6,351 bytes) Show data as ASCII Stream 152

Find: Find Next

Help Filter Out This Stream Print Save as… Back × Close

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