SANS ISC: InfoSec Handlers Diary Blog - 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 InfoSec Handlers Diary Blog

isc.sans.edu/diary/rss/28254

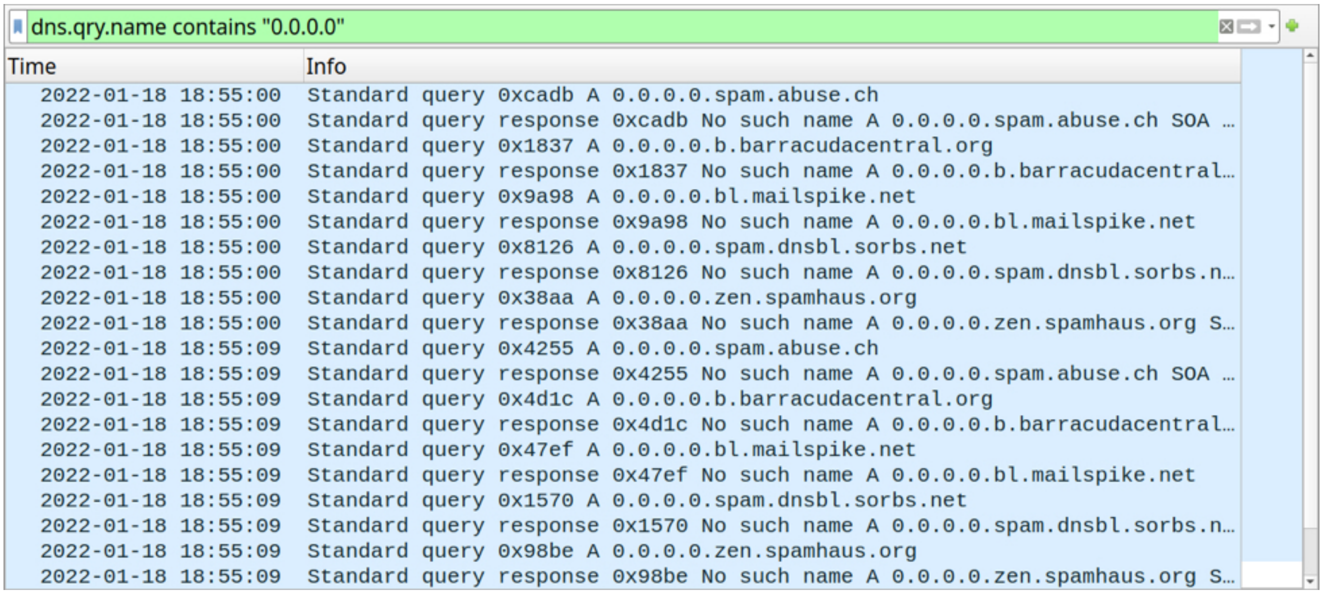
0.0.0.0 in Emotet Spambot Traffic

Published: 2022-01-19
Last Updated: 2022-01-19 03:39:21 UTC
by Brad Duncan (Version: 1)
0 comment(s)
Introduction

Emotet often uses information from emails and address books stolen from infected Windows hosts. Malicious spam (malspam) from Emotet spoofs legitimate senders to trick potential victims into running malicious files.

Additionally, Emotet uses IP address 0.0.0.0 in spambot traffic, possibly attempting to hide the actual IP address of an Emotet-infected host.

This ISC diary reviews the spoofed 0.0.0.0 address used in a recent Emotet infection from Tuesday 2022-01-18.



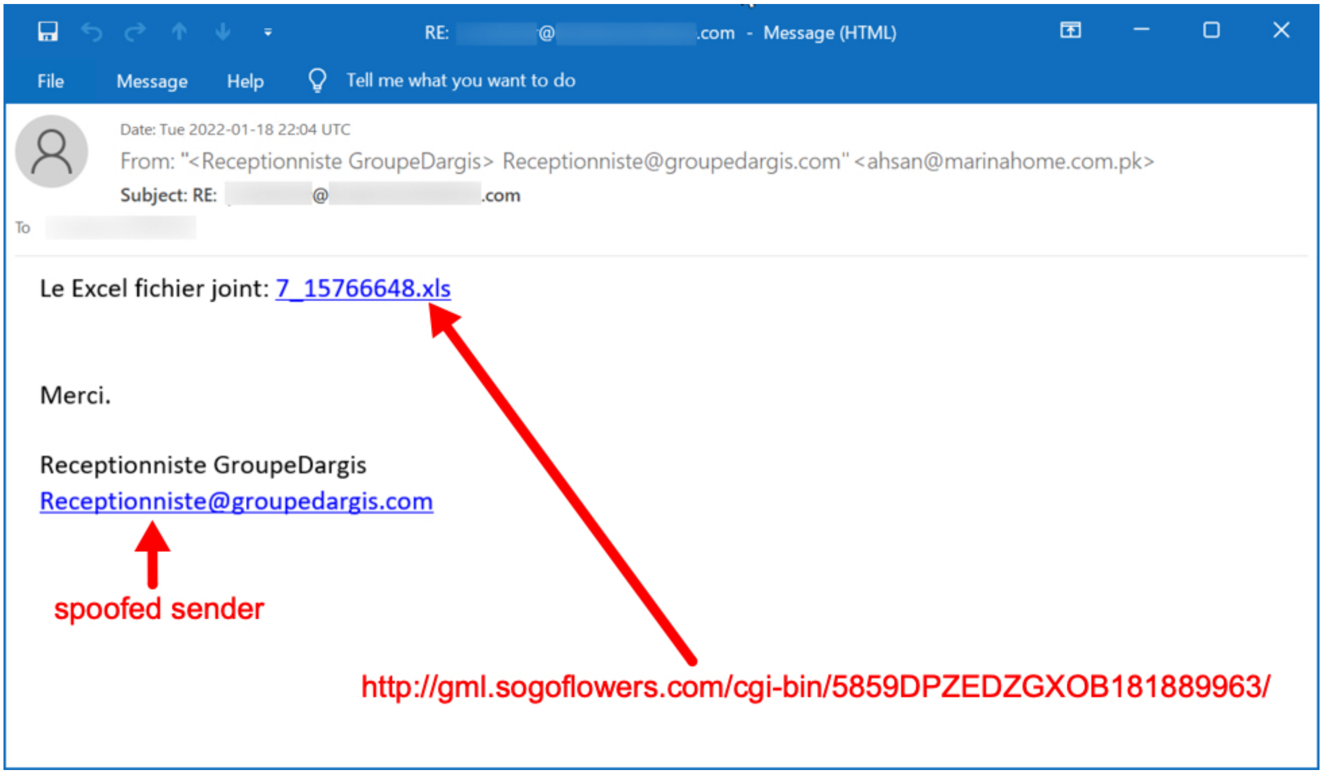
```
dns.qry.name contains "0.0.0.0"

Time                   Info
  2022-01-18 18:55:00  Standard query 0xcadb A 0.0.0.0.spam.abuse.ch
  2022-01-18 18:55:00  Standard query response 0xcadb No such name A 0.0.0.0.spam.abuse.ch SOA …
  2022-01-18 18:55:00  Standard query 0x1837 A 0.0.0.0.b.barracudacentral.org
  2022-01-18 18:55:00  Standard query response 0x1837 No such name A 0.0.0.0.b.barracudacentral…
  2022-01-18 18:55:00  Standard query 0x9a98 A 0.0.0.0.bl.mailspike.net
  2022-01-18 18:55:00  Standard query response 0x9a98 No such name A 0.0.0.0.bl.mailspike.net
  2022-01-18 18:55:00  Standard query 0x8126 A 0.0.0.0.spam.dnsbl.sorbs.net
  2022-01-18 18:55:00  Standard query response 0x8126 No such name A 0.0.0.0.spam.dnsbl.sorbs.n…
  2022-01-18 18:55:00  Standard query 0x38aa A 0.0.0.0.zen.spamhaus.org
  2022-01-18 18:55:00  Standard query response 0x38aa No such name A 0.0.0.0.zen.spamhaus.org S…
  2022-01-18 18:55:09  Standard query 0x4255 A 0.0.0.0.spam.abuse.ch
  2022-01-18 18:55:09  Standard query response 0x4255 No such name A 0.0.0.0.spam.abuse.ch SOA …
  2022-01-18 18:55:09  Standard query 0x4d1c A 0.0.0.0.b.barracudacentral.org
  2022-01-18 18:55:09  Standard query response 0x4d1c No such name A 0.0.0.0.b.barracudacentral…
  2022-01-18 18:55:09  Standard query 0x47ef A 0.0.0.0.bl.mailspike.net
  2022-01-18 18:55:09  Standard query response 0x47ef No such name A 0.0.0.0.bl.mailspike.net
  2022-01-18 18:55:09  Standard query 0x1570 A 0.0.0.0.spam.dnsbl.sorbs.net
  2022-01-18 18:55:09  Standard query response 0x1570 No such name A 0.0.0.0.spam.dnsbl.sorbs.n…
  2022-01-18 18:55:09  Standard query 0x98be A 0.0.0.0.zen.spamhaus.org
  2022-01-18 18:55:09  Standard query response 0x98be No such name A 0.0.0.0.zen.spamhaus.org S…
```

Shown above: 0.0.0.0 in DNS queries from an Emotet-infected host.

Scenes from an infection

Both Emotet botnets (dubbed by researchers as "epoch 4" and "epoch 5") resumed activity after the recent holiday season, and malicious spam started approximately one week ago on Tuesday 2022-01-11.

Most Windows hosts I've infected with Emotet in my lab will start spamming within an hour or less after the initial infection. Refer to the images below for activity from a recent Emotet infection on 2022-01-18.


RE: [redacted]@[redacted].com - Message (HTML)
File
Message
Help
Tell me what you want to do

Date: Tue 2022-01-18 22:04 UTC

From: "<Receptionniste GroupeDargis> Receptionniste@groupedargis.com" <ahsan@marinahome.com.pk>

Subject: RE: [redacted]@[redacted].com

To [redacted]

Le Excel fichier joint: 7_15766648.xls

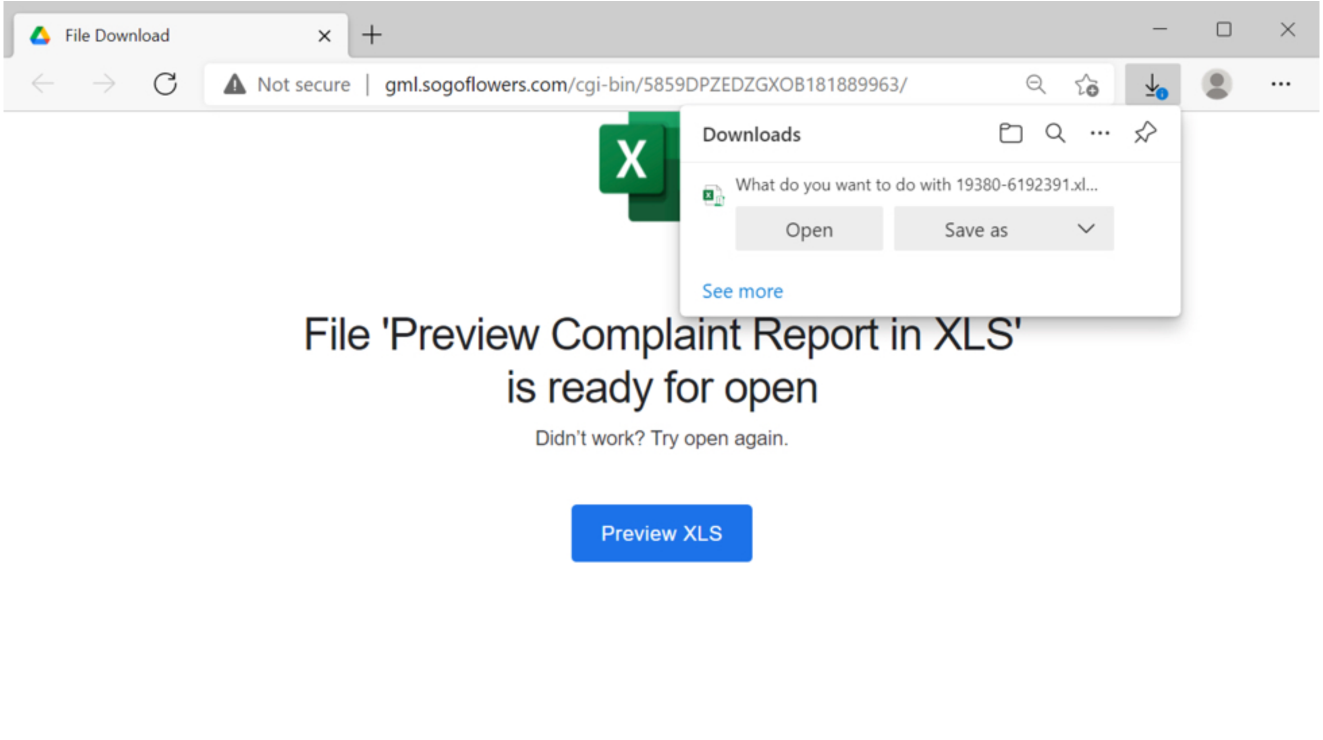
Merci.

Receptionniste GroupeDargis
Receptionniste@groupedargis.com

spoofed sender

http://gml.sogoflowers.com/cgi-bin/5859DPZEDZGXOB181889963/

Shown above: Screenshot from malspam pushing Emotet on Tuesday 2022-01-18.

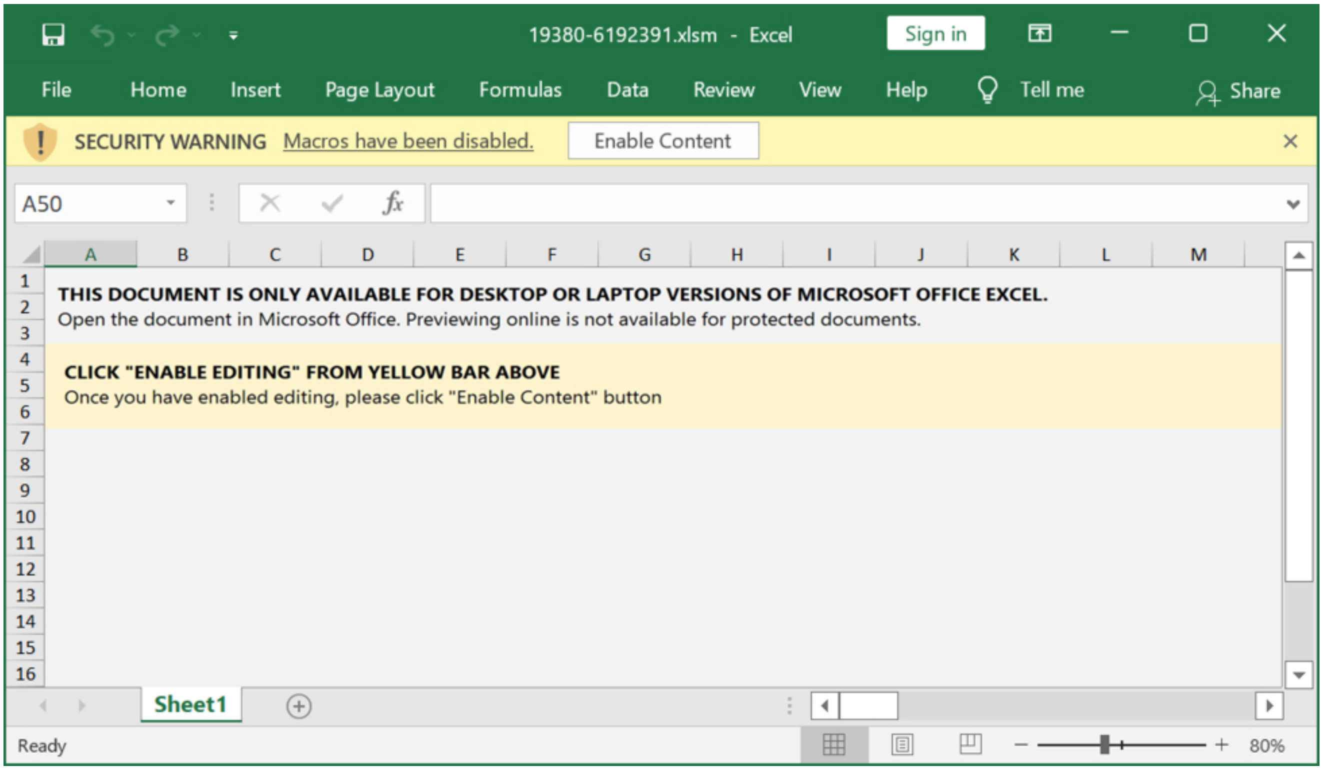


What do you want to do with 19380-6192391.xl...

File 'Preview Complaint Report in XLS' is ready for open

Didn't work? Try open again.

Shown above: Web page from link in the malspam.

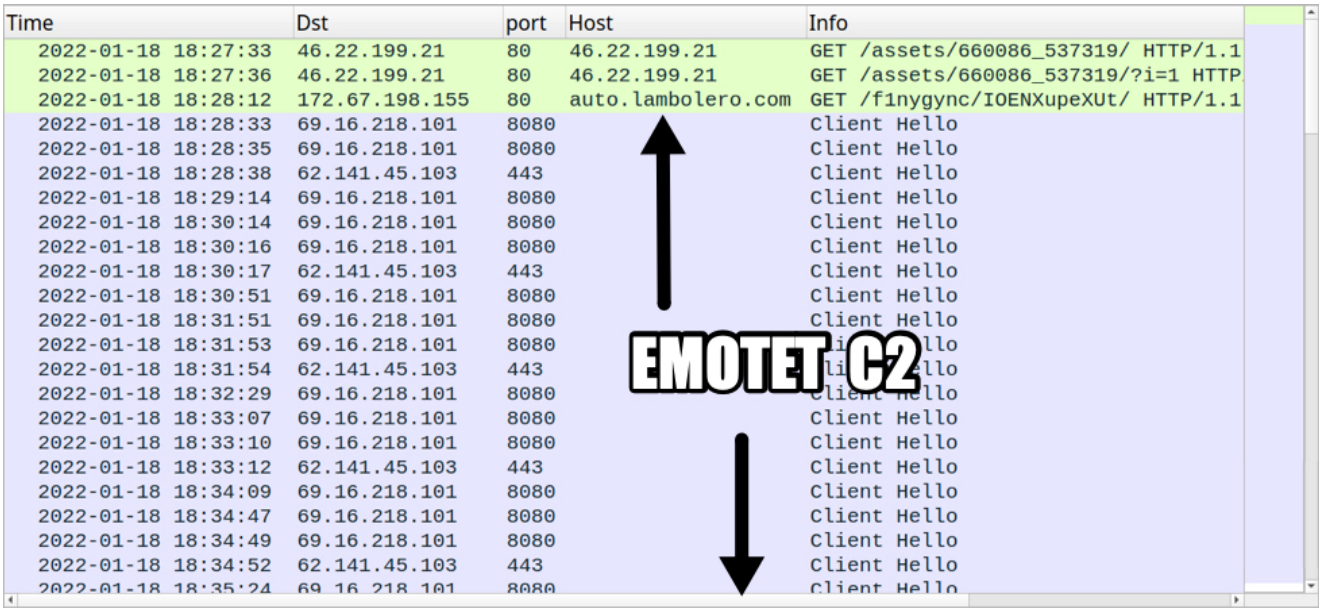


THIS DOCUMENT IS ONLY AVAILABLE FOR DESKTOP OR LAPTOP VERSIONS OF MICROSOFT OFFICE EXCEL.
Open the document in Microsoft Office. Previewing online is not available for protected documents.

CLICK "ENABLE EDITING" FROM YELLOW BAR ABOVE
Once you have enabled editing, please click "Enable Content" button

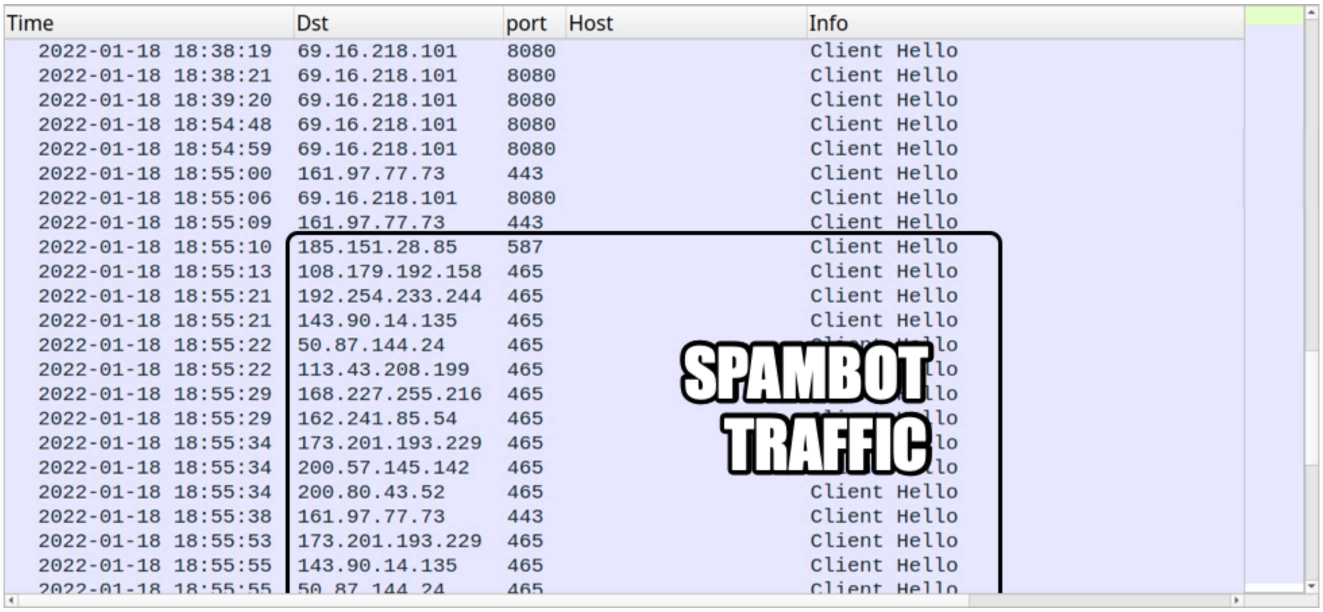
Shown above: Example of downloaded Excel spreadsheet for Emotet.

Enable macros in a downloaded spreadsheet, and they will infect a vulnerable Windows host. This is standard operating procedure for Emotet.



Time	Dst	port	Host	Info
2022-01-18 18:27:33	46.22.199.21	80	46.22.199.21	GET /assets/660086_537319/ HTTP/1.1
2022-01-18 18:27:36	46.22.199.21	80	46.22.199.21	GET /assets/660086_537319/?i=1 HTTP
2022-01-18 18:28:12	172.67.198.155	80	auto.lambolero.com	GET /f1nygync/IOENXupeXUt/ HTTP/1.1
2022-01-18 18:28:33	69.16.218.101	8080		Client Hello
2022-01-18 18:28:35	69.16.218.101	8080		Client Hello
2022-01-18 18:28:38	62.141.45.103	443		Client Hello
2022-01-18 18:29:14	69.16.218.101	8080		Client Hello
2022-01-18 18:30:14	69.16.218.101	8080		Client Hello
2022-01-18 18:30:16	69.16.218.101	8080		Client Hello
2022-01-18 18:30:17	62.141.45.103	443		Client Hello
2022-01-18 18:30:51	69.16.218.101	8080		Client Hello
2022-01-18 18:31:51	69.16.218.101	8080		Client Hello
2022-01-18 18:31:53	69.16.218.101	8080		Client Hello
2022-01-18 18:31:54	62.141.45.103	443		Client Hello
2022-01-18 18:32:29	69.16.218.101	8080		Client Hello
2022-01-18 18:33:07	69.16.218.101	8080		Client Hello
2022-01-18 18:33:10	69.16.218.101	8080		Client Hello
2022-01-18 18:33:12	62.141.45.103	443		Client Hello
2022-01-18 18:34:09	69.16.218.101	8080		Client Hello
2022-01-18 18:34:47	69.16.218.101	8080		Client Hello
2022-01-18 18:34:49	69.16.218.101	8080		Client Hello
2022-01-18 18:34:52	62.141.45.103	443		Client Hello
2022-01-18 18:35:24	69.16.218.101	8080		Client Hello

Shown above: Traffic from an infection filtered in Wireshark.



Time	Dst	port	Host	Info
2022-01-18 18:38:19	69.16.218.101	8080		Client Hello
2022-01-18 18:38:21	69.16.218.101	8080		Client Hello
2022-01-18 18:39:20	69.16.218.101	8080		Client Hello
2022-01-18 18:54:48	69.16.218.101	8080		Client Hello
2022-01-18 18:54:59	69.16.218.101	8080		Client Hello
2022-01-18 18:55:00	161.97.77.73	443		Client Hello
2022-01-18 18:55:06	69.16.218.101	8080		Client Hello
2022-01-18 18:55:09	161.97.77.73	443		Client Hello
2022-01-18 18:55:10	185.151.28.85	587		Client Hello
2022-01-18 18:55:13	108.179.192.158	465		Client Hello
2022-01-18 18:55:21	192.254.233.244	465		Client Hello
2022-01-18 18:55:21	143.90.14.135	465		Client Hello
2022-01-18 18:55:22	50.87.144.24	465		Client Hello
2022-01-18 18:55:22	113.43.208.199	465		Client Hello
2022-01-18 18:55:29	168.227.255.216	465		Client Hello
2022-01-18 18:55:29	162.241.85.54	465		Client Hello
2022-01-18 18:55:34	173.201.193.229	465		Client Hello
2022-01-18 18:55:34	200.57.145.142	465		Client Hello
2022-01-18 18:55:34	200.80.43.52	465		Client Hello
2022-01-18 18:55:38	161.97.77.73	443		Client Hello
2022-01-18 18:55:53	173.201.193.229	465		Client Hello
2022-01-18 18:55:55	143.90.14.135	465		Client Hello
2022-01-18 18:55:55	50.87.144.24	465		Client Hello

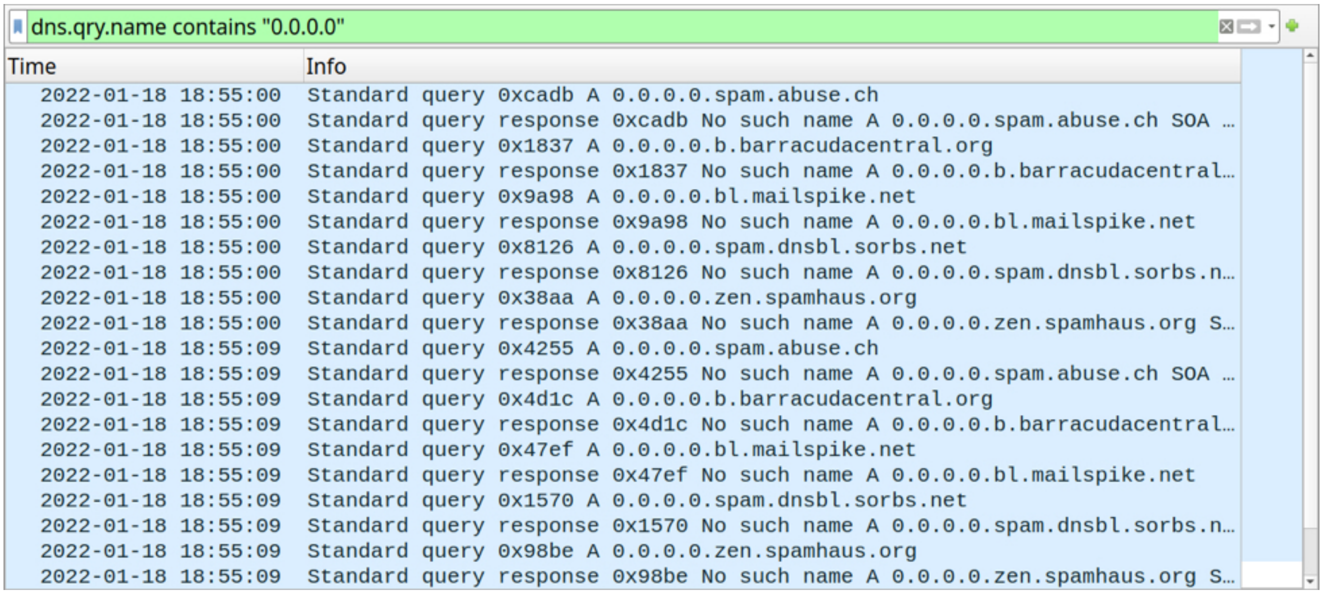
Shown above: Spambot activity started approximately 27 minutes after the initial infection.

Emotet spambot traffic using 0.0.0.0

Right as the spambot activity starts, the following DNS queries are made using domains related to spam filtering:

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

Similar DNS queries, but without the 0.0.0.0, are generated during Trickbot infections. However, Trickbot uses the infected host's public IP address data in the DNS query. Here is an example from analysis of a Trickbot sample (scroll down to the "Domains" list).

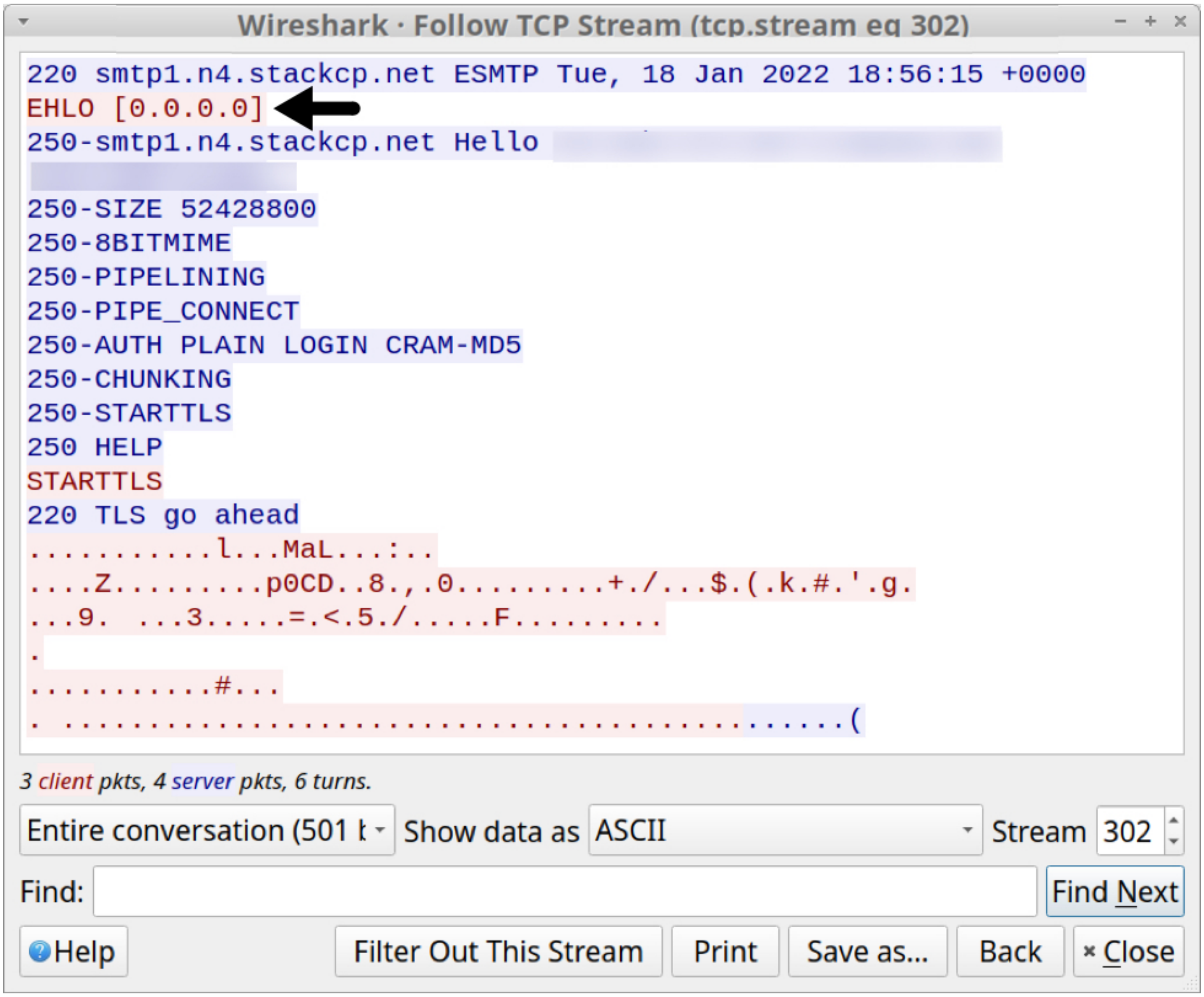


dns.qry.name contains "0.0.0.0"

```
Time                 Info
 2022-01-18 18:55:00  Standard query 0xcadb A 0.0.0.0.spam.abuse.ch
 2022-01-18 18:55:00  Standard query response 0xcadb No such name A 0.0.0.0.spam.abuse.ch SOA …
 2022-01-18 18:55:00  Standard query 0x1837 A 0.0.0.0.b.barracudacentral.org
 2022-01-18 18:55:00  Standard query response 0x1837 No such name A 0.0.0.0.b.barracudacentral…
 2022-01-18 18:55:00  Standard query 0x9a98 A 0.0.0.0.bl.mailspike.net
 2022-01-18 18:55:00  Standard query response 0x9a98 No such name A 0.0.0.0.bl.mailspike.net
 2022-01-18 18:55:00  Standard query 0x8126 A 0.0.0.0.spam.dnsbl.sorbs.net
 2022-01-18 18:55:00  Standard query response 0x8126 No such name A 0.0.0.0.spam.dnsbl.sorbs.n…
 2022-01-18 18:55:00  Standard query 0x38aa A 0.0.0.0.zen.spamhaus.org
 2022-01-18 18:55:00  Standard query response 0x38aa No such name A 0.0.0.0.zen.spamhaus.org S…
 2022-01-18 18:55:09  Standard query 0x4255 A 0.0.0.0.spam.abuse.ch
 2022-01-18 18:55:09  Standard query response 0x4255 No such name A 0.0.0.0.spam.abuse.ch SOA …
 2022-01-18 18:55:09  Standard query 0x4d1c A 0.0.0.0.b.barracudacentral.org
 2022-01-18 18:55:09  Standard query response 0x4d1c No such name A 0.0.0.0.b.barracudacentral…
 2022-01-18 18:55:09  Standard query 0x47ef A 0.0.0.0.bl.mailspike.net
 2022-01-18 18:55:09  Standard query response 0x47ef No such name A 0.0.0.0.bl.mailspike.net
 2022-01-18 18:55:09  Standard query 0x1570 A 0.0.0.0.spam.dnsbl.sorbs.net
 2022-01-18 18:55:09  Standard query response 0x1570 No such name A 0.0.0.0.spam.dnsbl.sorbs.n…
 2022-01-18 18:55:09  Standard query 0x98be A 0.0.0.0.zen.spamhaus.org
 2022-01-18 18:55:09  Standard query response 0x98be No such name A 0.0.0.0.zen.spamhaus.org S…
```

Shown above: 0.0.0.0-related DNS queries from an Emotet-infected host.

In addition to DNS queries, Emotet uses 0.0.0.0 during SMTP communications. This happens whenever an Emotet-infected host tries sending malspam to a targeted mailserver. The SMTP command is ***EHLO [0.0.0.0]***.



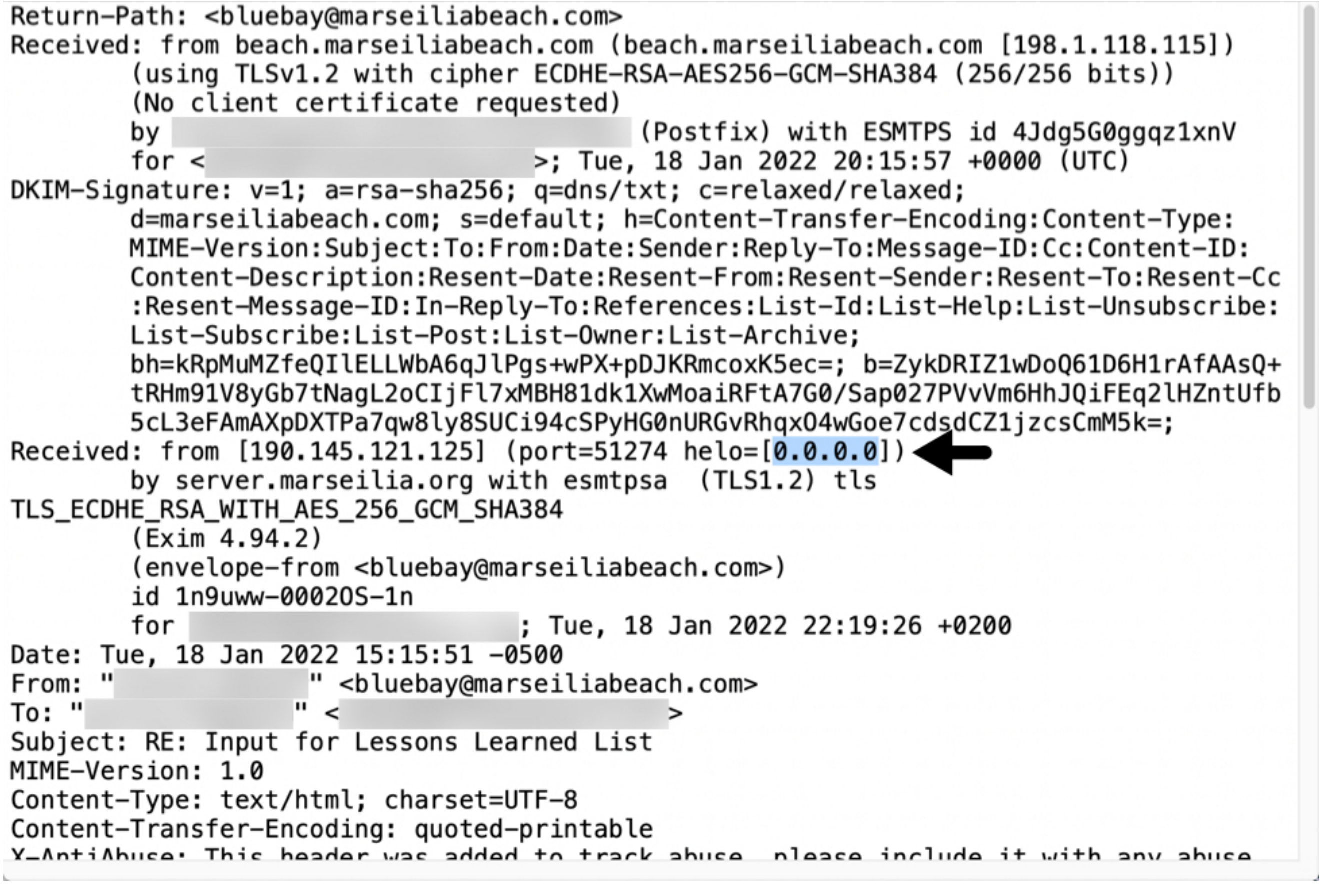
```
220 smtp1.n4.stackcp.net ESMTP Tue, 18 Jan 2022 18:56:15 +0000
EHLO [0.0.0.0]
250-smtp1.n4.stackcp.net Hello [redacted]
250-SIZE 52428800
250-8BITMIME
250-PIPELINING
250-PIPE_CONNECT
250-AUTH PLAIN LOGIN CRAM-MD5
250-CHUNKING
250-STARTTLS
250 HELP
STARTTLS
220 TLS go ahead
...........l...MaL...:..
....Z.........p0CD..8.,.0.........+./...$.(.k.#.'.g.
...9.  ...3.....=.<.5./.....F.........
.
...........#...
. ......................................(
```

3 client pkts, 4 server pkts, 6 turns.

Entire conversation (501 b Show data as ASCII Stream 302

Shown above: SMTP traffic using EHLO [0.0.0.0].

This attempt does not hide the actual IP address of an Emotet-infected host, because it still appears elsewhere in the SMTP traffic (blurred in the above image, for example). But 0.0.0.0 can be an indicator of emails pushing Emotet or other malware.



```
Return-Path: <bluebay@marseiliabeach.com>
Received: from beach.marseiliabeach.com (beach.marseiliabeach.com [198.1.118.115])
        (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits))
        (No client certificate requested)
        by [redacted] (Postfix) with ESMTPS id 4Jdg5G0ggqz1xnV
        for <[redacted]>; Tue, 18 Jan 2022 20:15:57 +0000 (UTC)
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed;
        d=marseiliabeach.com; s=default; h=Content-Transfer-Encoding:Content-Type:
        MIME-Version:Subject:To:From:Date:Sender:Reply-To:Message-ID:Cc:Content-ID:
        Content-Description:Resent-Date:Resent-From:Resent-Sender:Resent-To:Resent-Cc
        :Resent-Message-ID:In-Reply-To:References:List-Id:List-Help:List-Unsubscribe:
        List-Subscribe:List-Post:List-Owner:List-Archive;
        bh=kRpMuMZfeQIlELLWbA6qJlPgs+wPX+pDJKRmcoxK5ec=; b=ZykDRIZ1wDoQ61D6H1rAfAAsQ+
        tRHm91V8yGb7tNagL2oCIjFl7xMBH81dk1XwMoaiRFtA7G0/Sap027PVvVm6HhJQiFEq2lHZntUfb
        5cL3eFAmAXpDXTPa7qw8ly8SUCi94cSPyHG0nURGvRhqxO4wGoe7cdsdCZ1jzcsCmM5k=;
Received: from [190.145.121.125] (port=51274 helo=[0.0.0.0])
        by server.marseilia.org with esmtpsa  (TLS1.2) tls
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
        (Exim 4.94.2)
        (envelope-from <bluebay@marseiliabeach.com>)
        id 1n9uww-0002OS-1n
        for [redacted]; Tue, 18 Jan 2022 22:19:26 +0200
Date: Tue, 18 Jan 2022 15:15:51 -0500
From: "[redacted]" <bluebay@marseiliabeach.com>
To: "[redacted]" <[redacted]>
Subject: RE: Input for Lessons Learned List
MIME-Version: 1.0
Content-Type: text/html; charset=UTF-8
Content-Transfer-Encoding: quoted-printable
X-AntiAbuse: This header was added to track abuse, please include it with any abuse
```

Shown above: Example of Emotet malspam with 0.0.0.0 in the email headers.

Final words

While 0.0.0.0 is an indicator for Emotet or other malware, 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

Keywords: Emotet
0 comment(s)

Top of page

×

Diary Archives