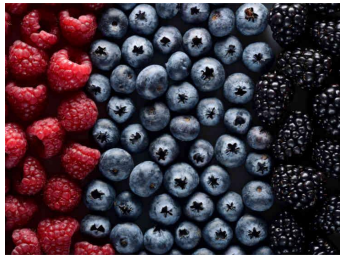
Email security auditing and alert triage with Zeek

Barry Weymes
Bro Workshop Europe 2019

Who is this guy!?



FUJITSU

SWIFT

FOX IT
part of nccgroup

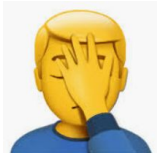
aramco

Security Engineer

‘The rules guy’ - Challenge accepted

Motivation / Background

- Zeek data -> Passive Audit first thing
- Contactor didnt turn on STARTTLS when installing server.

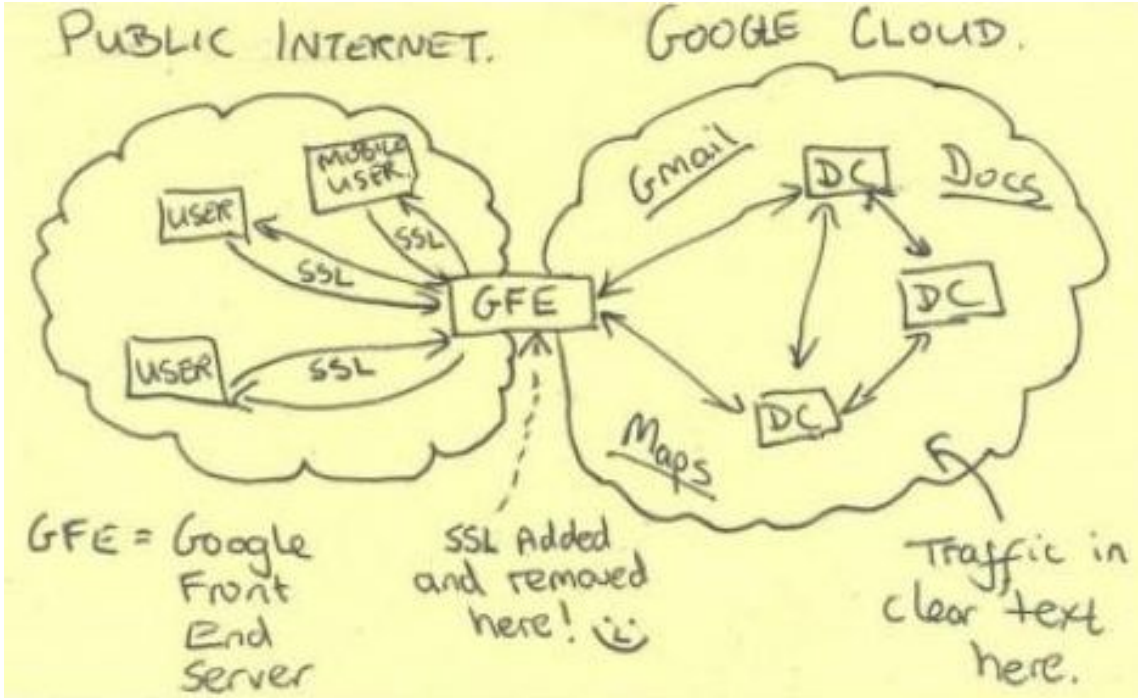


He probably didn't even know how, it's complicated…

- I blame Vendor, for its bad defaults for all SMTP over plain text!

- Year long threat hunt. Information being sent over unencrypted channels.
- The ´No email encryption´ issue is a two party problem.
  One side can have the best config in the world but fail to secure their data.

Motivation / Background



Overview

- STARTTLS, a brief overview, a battle
- The hunt, the results.

- Unique attacks over email. Just use CC!

- Challenges doing alert triage on these attacks.

STARTTLS, a brief overview, a battle

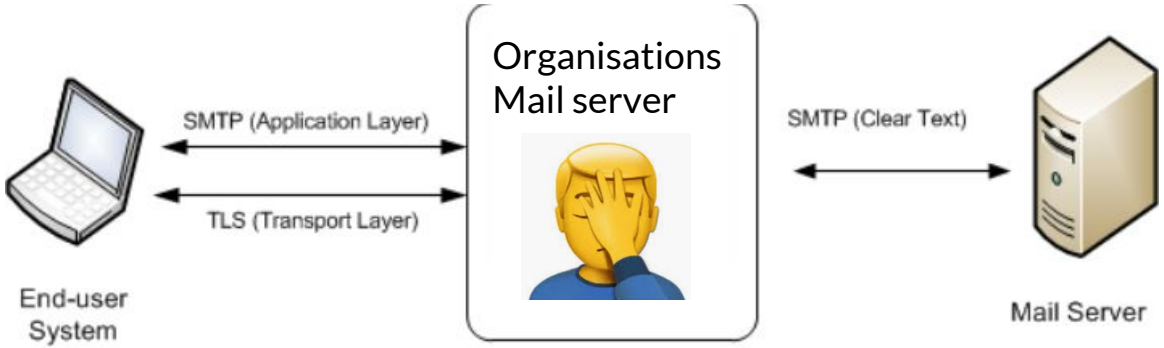
Opportunistic TLS (Transport Layer Security) refers to a way to upgrade a plain text connection to an encrypted (TLS or SSL) connection instead of using a separate port for encrypted communication.

It is primarily intended as a countermeasure to passive monitoring.

STARTTLS, a brief overview, a battle

Off, **Preferred** or **Enforced** encryption options.

Once its gone to the internet, it's in the clear sadly! For ´everyone´ to see



Good

ts	time	1400168396.898137
uid	string	Cso2UBv2cpQrcbq2
id.orig_h	addr	192.168.4.149
id.orig_p	port	54170
id.resp_h	addr	74.125.142.26
id.resp_p	port	25
trans_depth	count	1
helo	string	openssl.client.net
mailfrom	string	-
rcptto	set[string]	-
date	string	-
from	string	-
to	set[string]	-
cc	set[string]	-
reply_to	string	-
msg_id	string	-
in_reply_to	string	-
subject	string	-
x_originating_ip	addr	-
first_received	string	-
second_received	string	-
last_reply	string	220 2.0.0 Ready to start TLS
path	vector[addr]	74.125.142.26,192.168.4.149
user_agent	string	-
tls	bool	T
fuids	vector[string]	(empty)
is_webmail	bool	F

Bad

Field	Type	Value
ts	time	1254722768.219663
uid	string	CfpfJd2yA1vu6bcOB
id.orig_h	addr	10.10.1.4
id.orig_p	port	1470
id.resp_h	addr	74.53.140.153
id.resp_p	port	25
trans_depth	count	1
helo	string	GP
mailfrom	string	gurpartap@patriots.in
rcptto	set[string]	raj_deol2002in@yahoo.co.in
date	string	Mon, 5 Oct 2009 11:36:07 +0530
from	string	"Gurpartap Singh" <gurpartap@patriots.in>
to	set[string]	<raj_deol2002in@yahoo.co.in>
cc	set[string]	-
reply_to	string	-
msg_id	string	<000301ca4581$ef9e57f0$cedb07d0$@in>
in_reply_to	string	-
subject	string	SMTP
x_originating_ip	addr	-
first_received	string	-
second_received	string	-
last_reply	string	250 OK id=1Mugho-0003Dg-Un
path	vector[addr]	74.53.140.153,10.10.1.4
user_agent	string	Microsoft Office Outlook 12.0
tls	bool	F
fuids	vector[string]	FeI9gs4OtNEV6gUJZ5,Ft4M3f2yMvLlmwtbq9,FL9Y0d45OI4LpS6fmh
is_webmail	bool	F

Ironport logs

Here is an example of a successful TLS connection from the remote host (reception):

```
Tue Apr 17 00:57:53 2018 Info: New SMTP ICID 590125205 interface Data 1 (192.168.1.1) address 100.0.0.1 reverse dns host mail
Tue Apr 17 00:57:53 2018 Info: ICID 590125205 ACCEPT SG SUSPECTLIST match sbrs[-1.4:2.0] SBRS -1.1
Tue Apr 17 00:57:54 2018 Info: ICID 590125205 TLS success protocol TLSv1 cipher DHE-RSA-AES256-SHA
Tue Apr 17 00:57:55 2018 Info: Start MID 179701980 ICID 590125205
```

Here is an example of a successful TLS connection to the remote host (delivery):

```
Tue Apr 17 00:58:02 2018 Info: New SMTP DCID 41014367 interface 192.168.1.1 address 100.0.0.1 port 25
Tue Apr 17 00:58:02 2018 Info: DCID 41014367 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-SHA384
Tue Apr 17 00:58:03 2018 Info: Delivery start DCID 41014367 MID 179701982 to RID [0]
```

Comprehensive Setup Guide for TLS on ESA. Have fun reading all 10 pages!

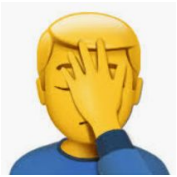
https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118844-technote-esa-00.html

The hunt starts

- Hunting in Bro/Zeek data is fun!
- Loads of early wins, and confused faces! ¨Surely...¨
- Securing the Aramco family first
- High value communication next
- Waiting for the obscure to pop onto the dashboard afterwards.

How to hunt

- I started with a Snort rule.
  Correlating all these alerts with SMTP.log. Bad idea.



- Made a Zeek script that enriched the logs with our data classification.
- Splunk dashboard. Top unencrypted domains by classification. Bingo!

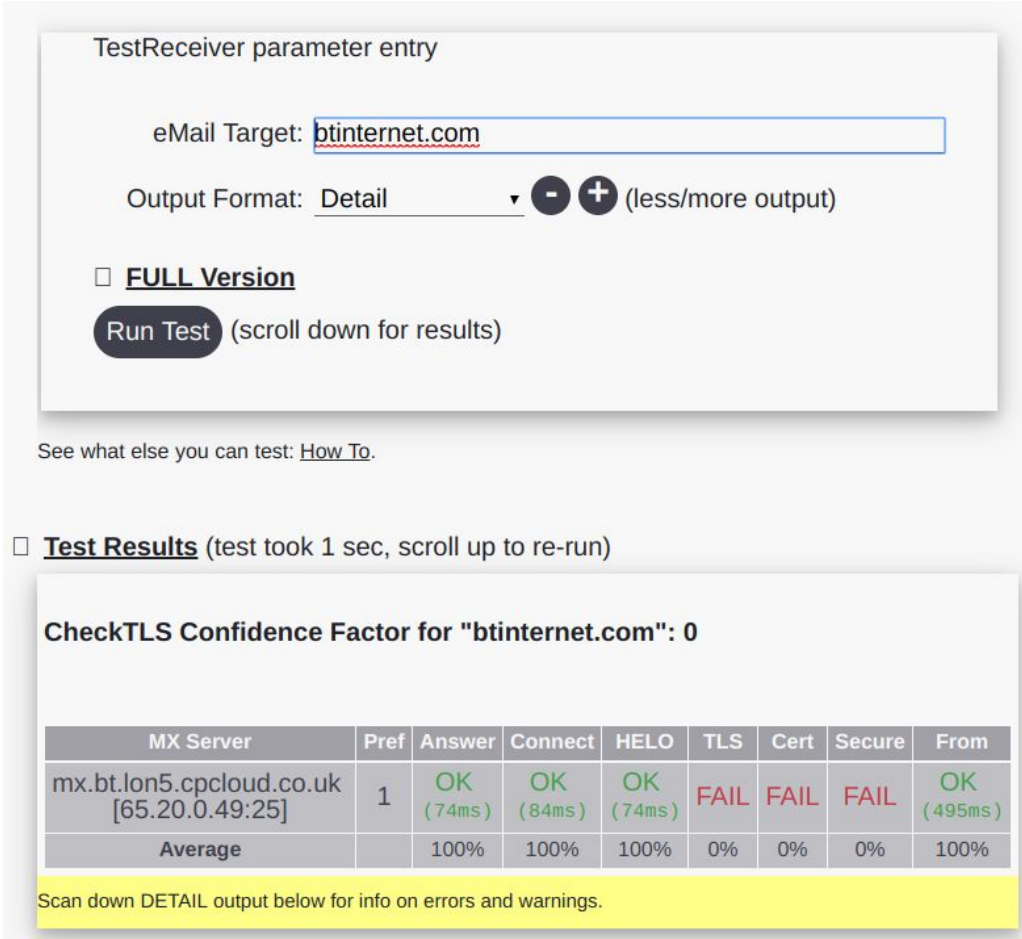
```
event smtp_data(c: connection, is_orig: bool, data: string)
    {

    if (data = ¨This email has been classified as Company Confidential by¨):
        Confidential = ¨Y¨

    }
```

This email has been classified as Company Confidential by **Weymes, Barry**

Double check

- I like **checktls.com**

- Some guys reaction:
  Block checktls.
  There are other options...



What I said!

- Email first, failing that a phone call.
  … Our (classified as) sensitive data has been over the clear.
  Please see attached Zeek log proof! 
- Please fix, thanks, Barry
- Unofficial warning - could be breaking security policy/contract

What I found!

- Global HR Firm
- Outbound issue only. Hybrid O365 setup
- Clearswift **secure** email gateway was the issue!

- It did not support STARTTLS 😱

What I found!

- Global Oil Firm
- Both directions in the clear, for everyone in the world

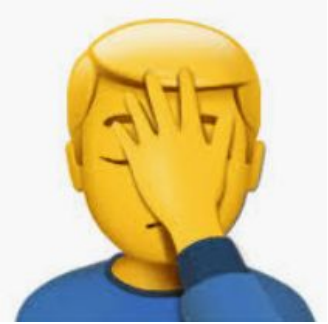
- Senior VP level emails in the clear 😱

What I found!

- ME Oil Firm
- Both directions in the clear, for everyone in the world

- Packet inspector prevented STARTTLS 😱

What I found!



- Global HR Firm
- Both directions in the clear, for everyone in the world

- Having serious trouble keeping issue fixed 😱

What I found!

- Global HR Firm
- Both directions in the clear, for everyone in the world
- Passports, financial data in the clear 😱
- Cold called the company, got COO. Took some convincing.

What I found!

- Global Law Firm
- Both directions in the clear, for everyone in the world
- Password resets, etc in the clear. 😱
- Most disappointing part was **they consult on Cyber-Security!**

What I found!

- European/Asian Industrial Firms
- Both directions in the clear, for everyone in the world

- Orders, Invoices, Shipping Details
  Schematics all gone out unencrypted 😱

What I got back!

- All positive reactions except for one. It was their 3rd party providers issue, they said. They they changed their mind quickly…
- Some changed and solved the issue instantly, others months. Afterwards we play email ping pong 🏓
- Most of people don't care until I say ´confidential data´ and proved proof! Zeek logs FTW

Lessons learnt

- Outbound from company to Aramco family is much harder to find/fix than inbound.
  It's not possible to use something like checktls.com.

- Visibility and expertise is the main problem. All had no clue!

- Zeek data is invaluable. Ironport and Exchange logs are useless!

Unique attacks over email. Just use CC!

- We have a serious attempted phishing incident via a vendor!
- ¨Hey Barry, I put that Nigerian guys email address into the data lake, I only get back your [expletive] bro logs.¨ - My boss. 

- That's strange, where's the Ironport or Exchange logs??

- Turns out they don't exist for CC addresses! 
- Go ahead, test it for yourself!

Challenges doing alert triage on these attacks.

- Doing alert triage is hard enough without log trusts issue like this!
- ¨Trust but verify¨
- Cross verification of facts can provide some interesting insights

- Fancy things like automated data extraction is not possible in Ironport/exchange logs
- So there's no way to alert on a gmail suddenly in the CC.

Challenges doing alert triage on these attacks.

- Vendors will continue to be breached and send us phishy emails.

- Bro logs give much more visibility, more than I initially realized before.

Questions?