Neither Snow Nor Rain Nor MITM...

An Empirical Analysis of Email Delivery Security

Nicolas Lidzborski, Elie Bursztein, Kurt Thomas, Vijay Eranti (*Google*)

Zakir Durumeric, David Adrian, Ariana Mirian, James Kasten, J. Alex Halderman (*University of Michigan*) Michael Bailey (*University of Illinois*)

Study’s goal: measuring the state of email delivery security

Agenda

Email encryption while in transit

Current deployment of SMTP TLS and attacks observed in the wild

Email authentication

How prevalent authentication technologies are

The future of email security

Overview of on-going efforts dedicated to improve email security

Datasets used in the study

Gmail longitudinal data

Longitudinal statistics based of what Gmail see

Alexa top 1M sites

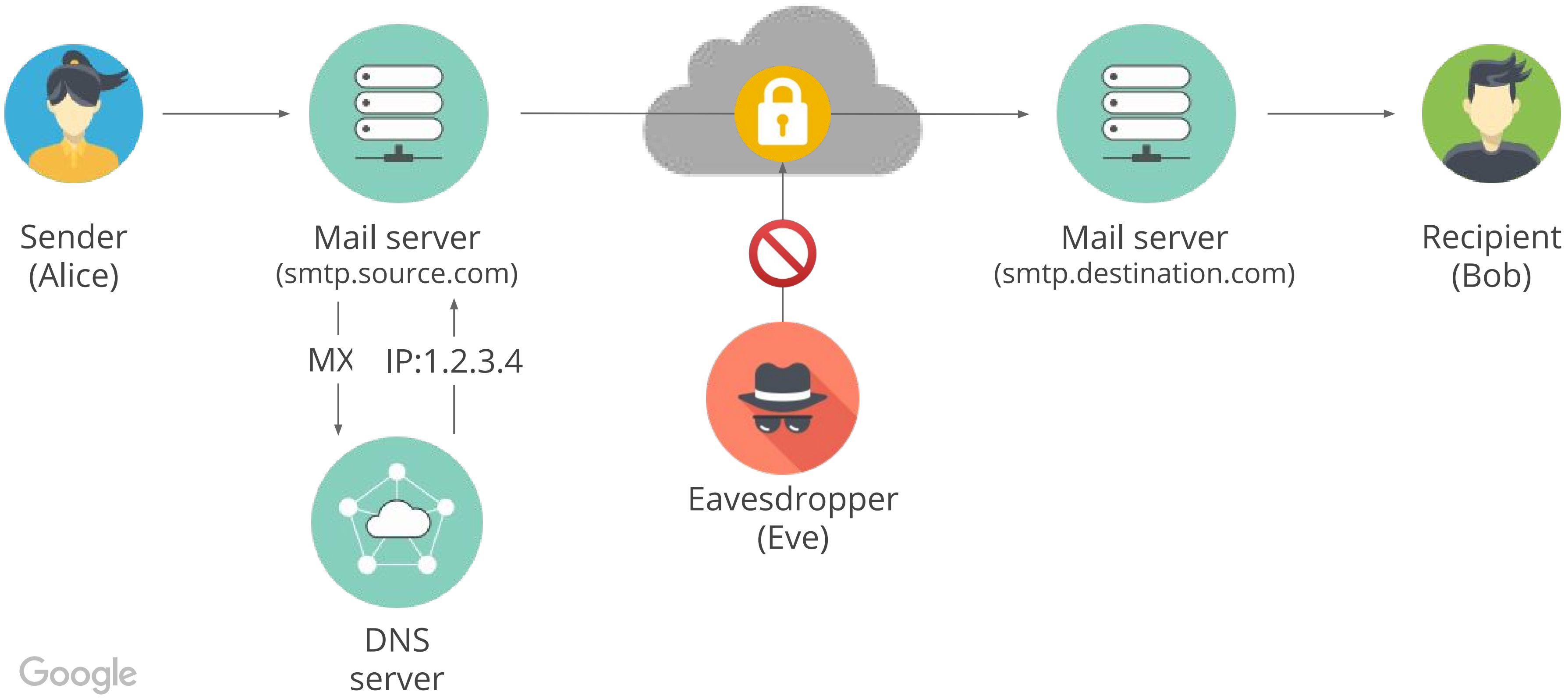
Zmap scanning of Alexa Top 1M sites SMTP servers

IPv4 public SMTP and DNS servers

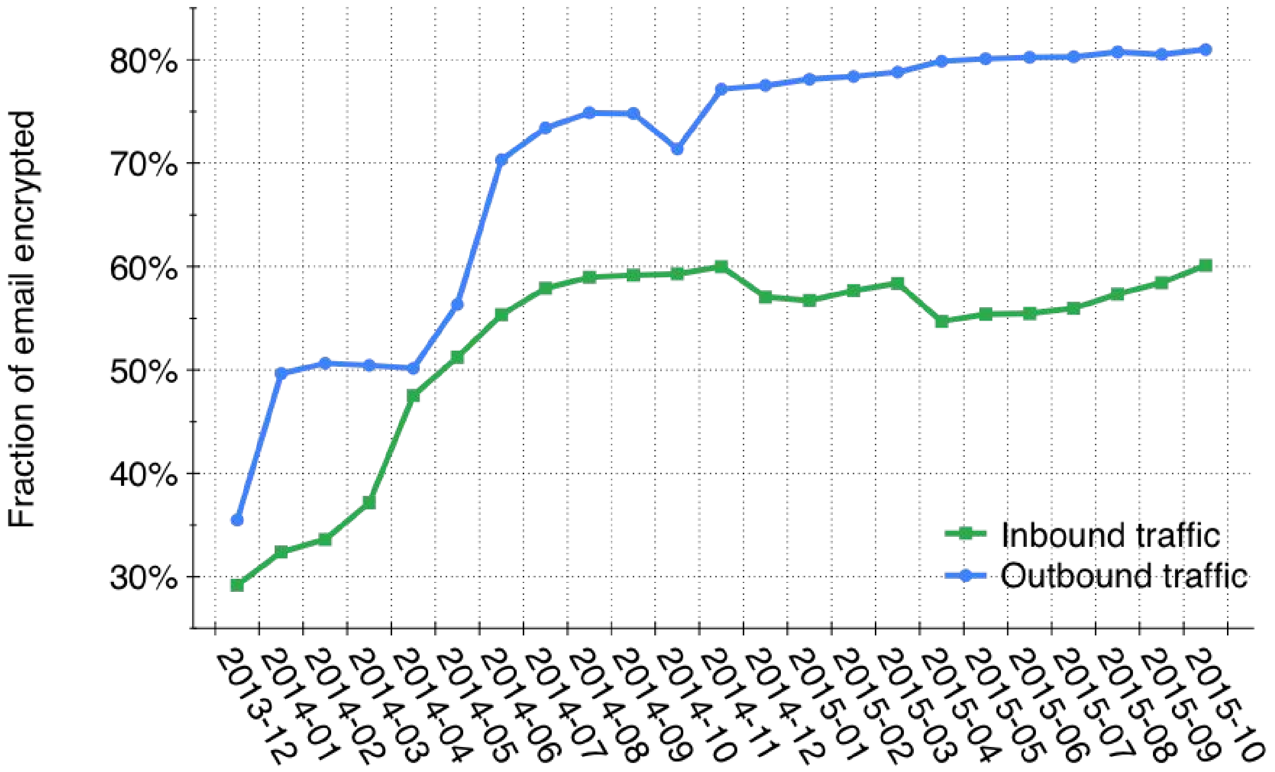
Zmap scanning for publicly reachable SMTP & DNS servers

1 SMTP encryption

SMTP encryption



Fraction of email encrypted as seen by Gmail

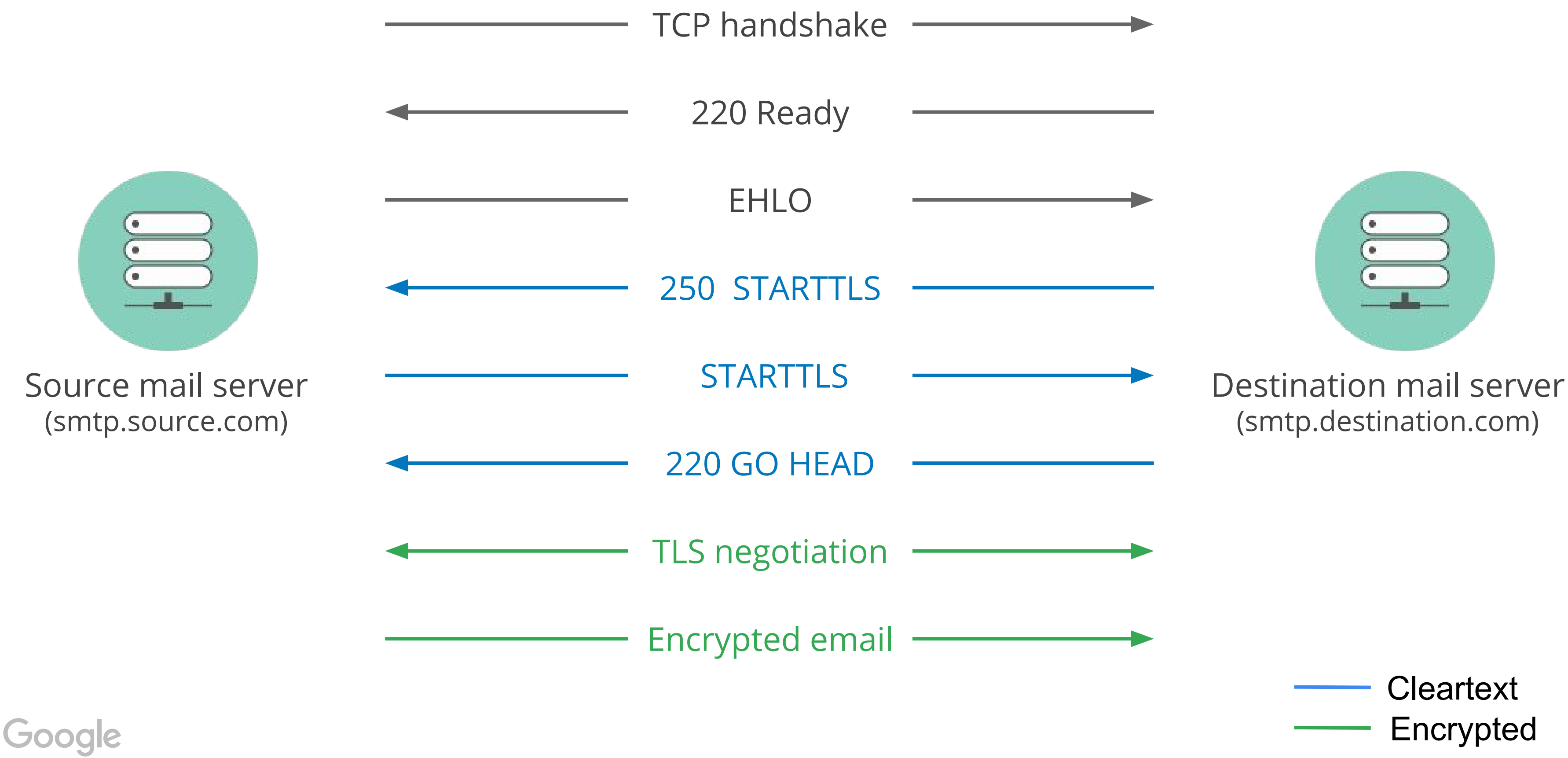


Google

Encryption quality

Provider	Incoming Key Exchange	Certificate name	Incoming ciphersuite	Outgoing key exchange	Outgoing ciphersuite
Gmail	ECDHE	match	AES128-GCM	ECDHE	AES128-GCM
Yahoo	ECDHE	match	AES128-GCM	ECDHE	RC4-128
Microsoft	ECDHE	match	AES256-CBC	ECDHE	AES256
Apple iCloud	ECDHE	match	AES128-GCM	DHE	AES128-GCM
Facebook mail	RSA	mismatch	AES128-CBC	ECDHE	AES128-CBC
Comcast	RSA	match	RC4-128	DHE	AES128-CBC
AT&T	ECDHE	match	AES128-GCM	ECDHE	RC4-128

STARTTLS



Source mail server
(smtp.source.com)

TCP handshake

220 Ready

EHLO

250 STARTTLS

STARTTLS

220 GO HEAD

TLS negotiation

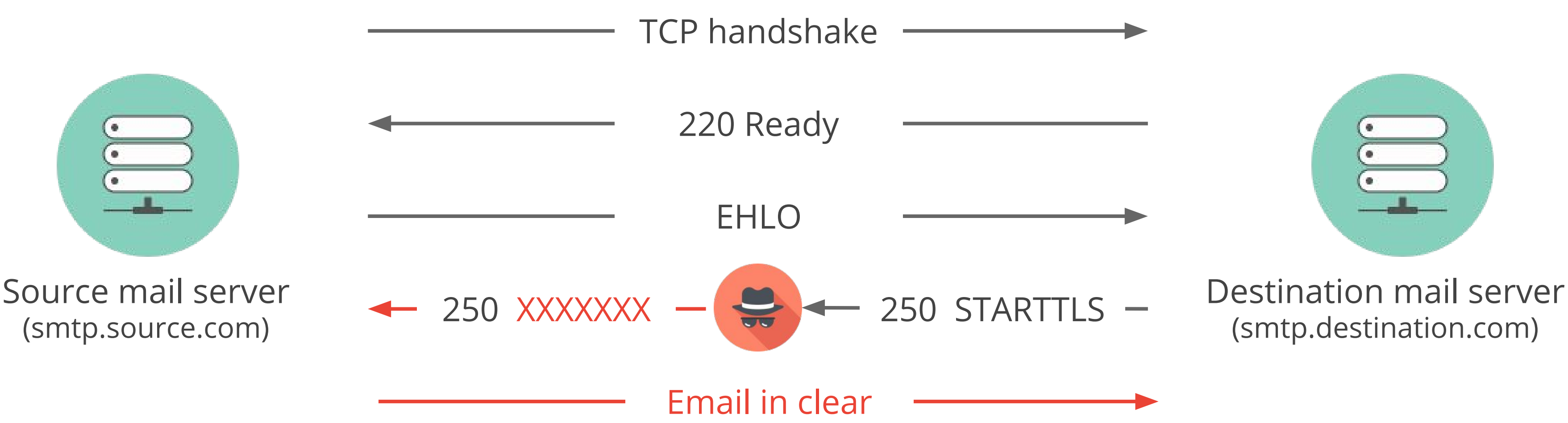
Encrypted email

Destination mail server
(smtp.destination.com)

Cleartext

Encrypted

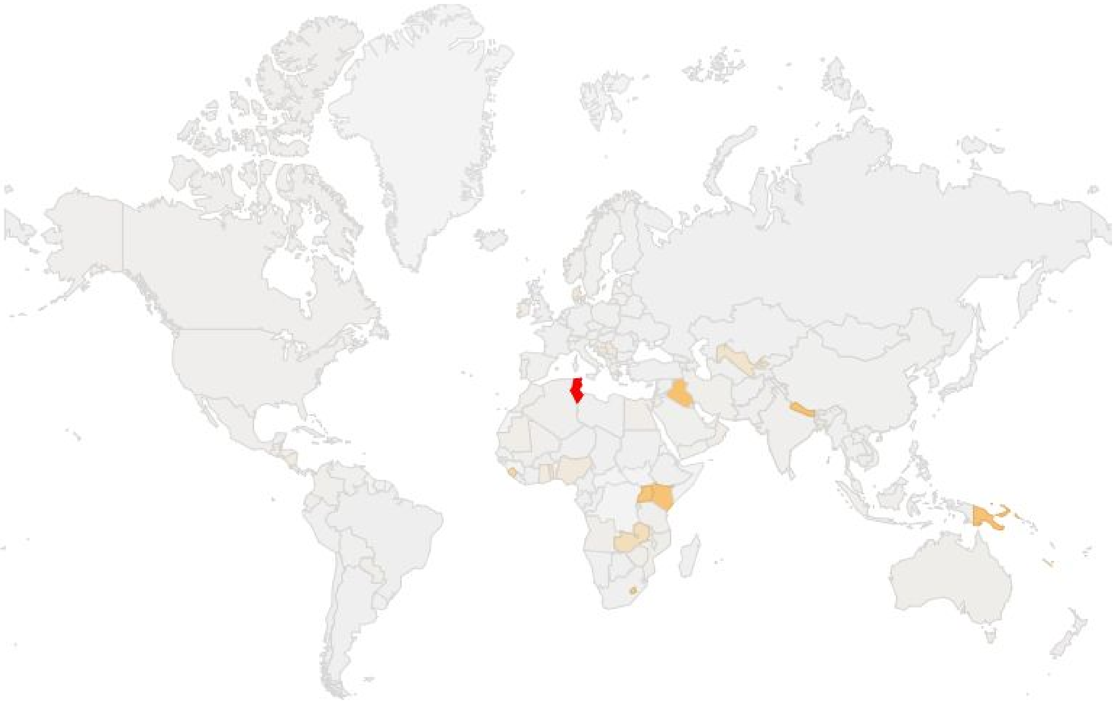
STARTTLS downgrade attack



STARTTLS downgrade by AS / organization

Organization Type	ASes
Corporation	43% (182)
ISP	17.5% (74)
Financial institutions	13.5% (57)
Academic institutions	8.3% (35)
Healthcare	3.3% (14)
Unknown	2.8% (12)
Airport	2.1% (9)
Hosting	1.7% (7)
NGO	0.7% (3)

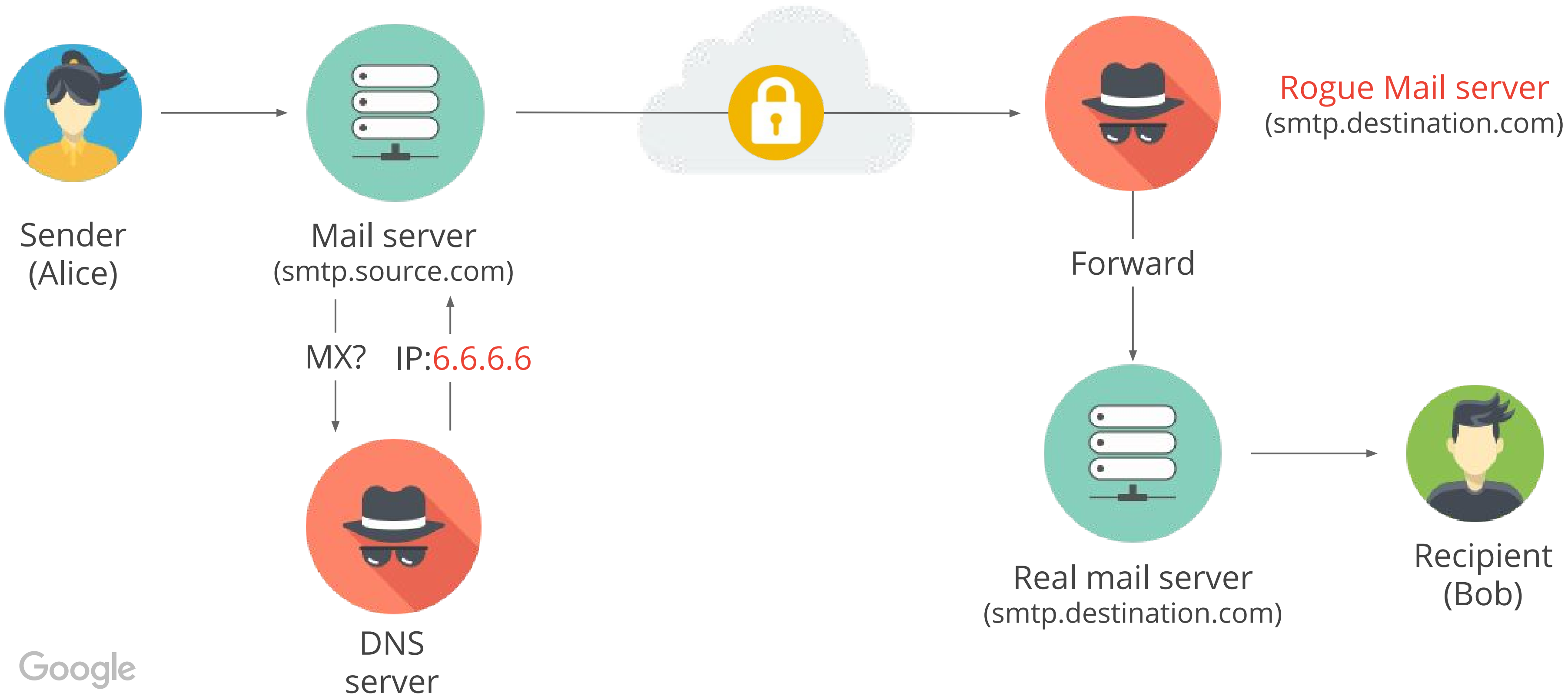
STARTTLS downgrading as seen by Gmail



country	% of inbound traffic
Tunisia	96.13%
Iraq	25.61%
Papua New Guinea	25.00%
Nepal	24.29%
Kenya	24.13%
Uganda	23.28%
Lesotho	20.25%
Sierra Leone	13.41%
New Caledonia	10.13%
Zambia	9.98%
Reunion	9.28%

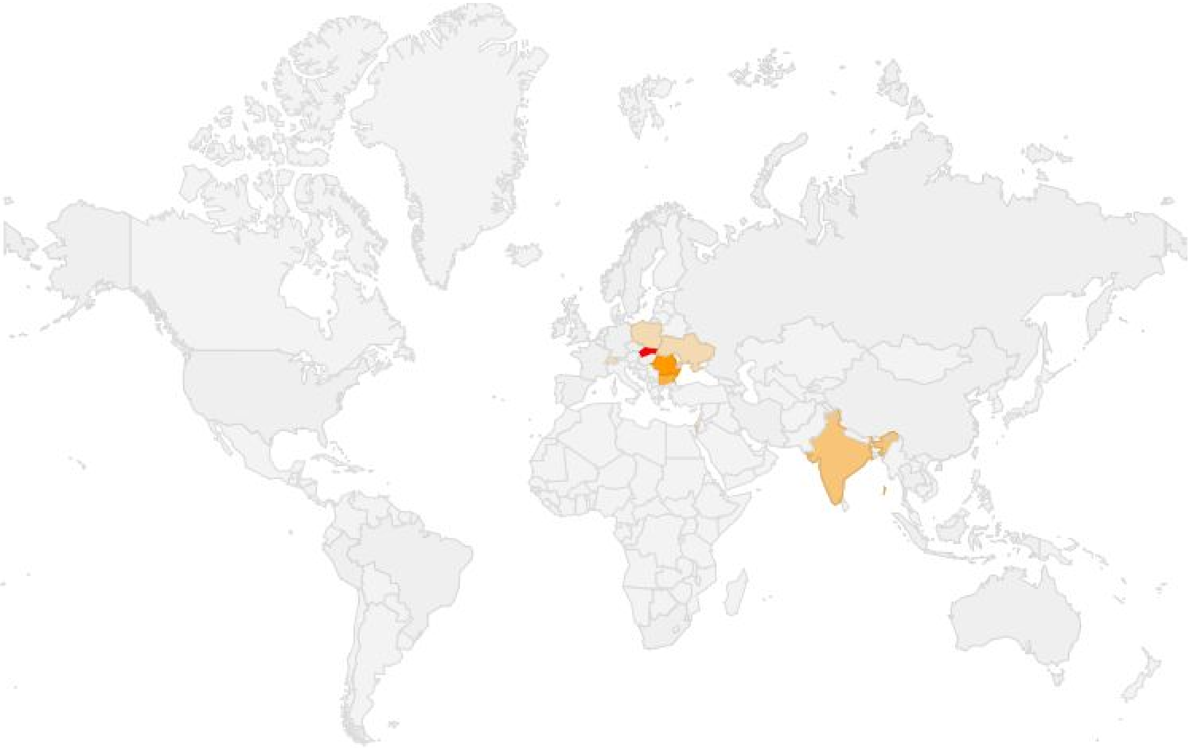
Google

MITM via DNS MX record hijacking



Google

DNS spoofing as seen by Gmail

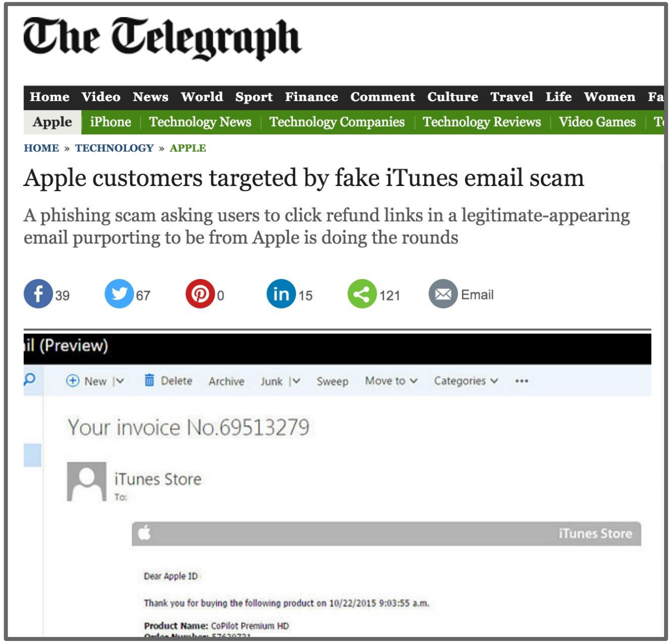


country	% of inbound traffic
Slovakia	0.08%
Romania	0.04%
Bulgaria	0.02%
India	0.01%
India	0.01%
Israel	0.01%
Poland	0.01%
Switzerland	0.01%
Ukraine	0.01%
Others	>0.01%

Google

2 Email authentication

Email authentication?


The Telegraph
Home Video News World Sport Finance Comment Culture Travel Life Women Fa
Apple iPhone Technology News Technology Companies Technology Reviews Video Games T
HOME » TECHNOLOGY » APPLE
39 67 0 15 121 Email
il (Preview)
New Delete Archive Junk Sweep Move to Categories

Apple customers targeted by fake iTunes email scam

A phishing scam asking users to click refund links in a legitimate-appearing email purporting to be from Apple is doing the rounds

Your invoice No.69513279

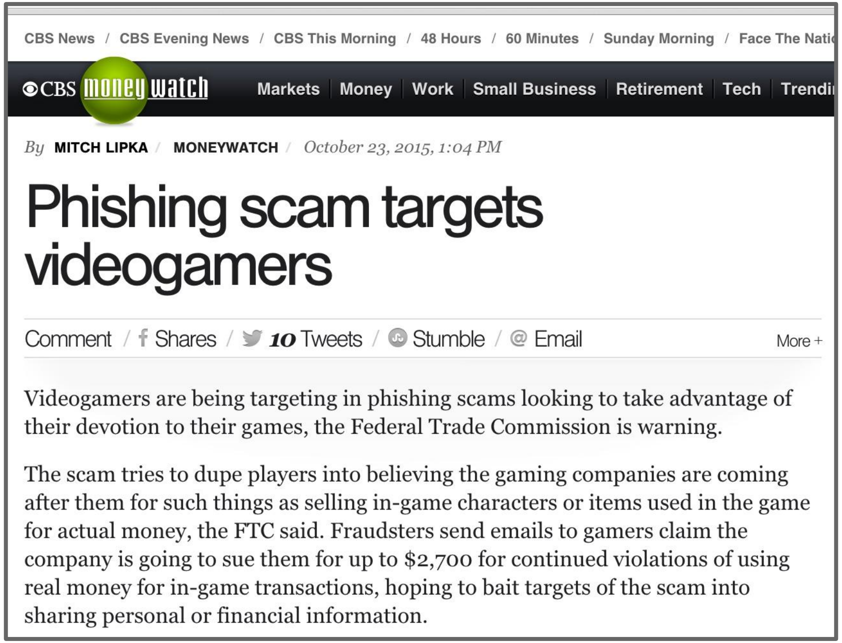
iTunes Store
To:

iTunes Store

Dear Apple ID

Thank you for buying the following product on 10/22/2015 9:03:55 a.m.

Product Name: CoPilot Premium HD


CBS News / CBS Evening News / CBS This Morning / 48 Hours / 60 Minutes / Sunday Morning / Face The Nati
CBS money watch
Markets Money Work Small Business Retirement Tech Trendi
Comment / Shares / 10 Tweets / Stumble / Email More +

By MITCH LIPKA / MONEYWATCH / *October 23, 2015, 1:04 PM*

Phishing scam targets videogamers

Videogamers are being targeting in phishing scams looking to take advantage of their devotion to their games, the Federal Trade Commission is warning.

The scam tries to dupe players into believing the gaming companies are coming after them for such things as selling in-game characters or items used in the game for actual money, the FTC said. Fraudsters send emails to gamers claim the company is going to sue them for up to $2,700 for continued violations of using real money for in-game transactions, hoping to bait targets of the scam into sharing personal or financial information.

Examples from October 2015

Email authentication technologies

SPF - Sender policy framework

Specify which IP addresses/prefix are allowed to send emails

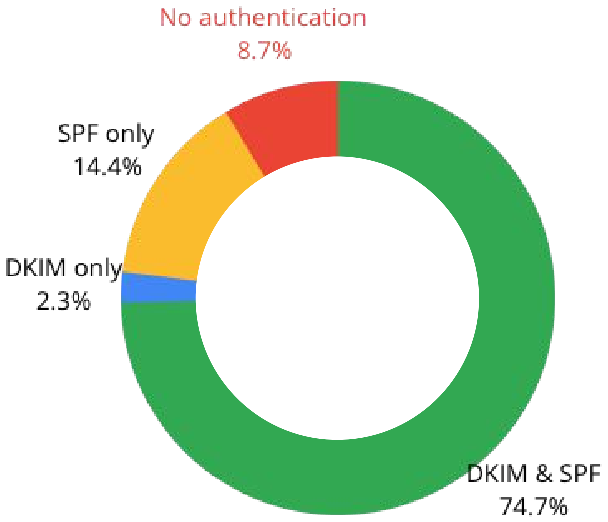
DKIM - Domain Key Identified Email

Use public key cryptography to sign the content of emails

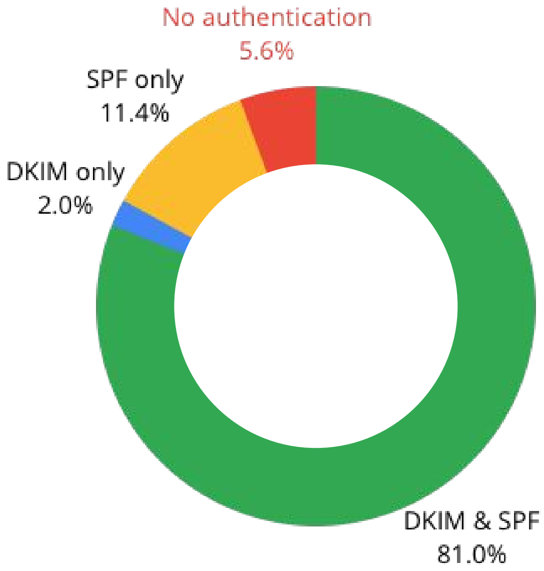
DMARC - Domain Message Authentication Reporting and Conformance

Specify what to do (reject, spam folder...) with non authenticated emails

Inbound authentication as seen by Gmail

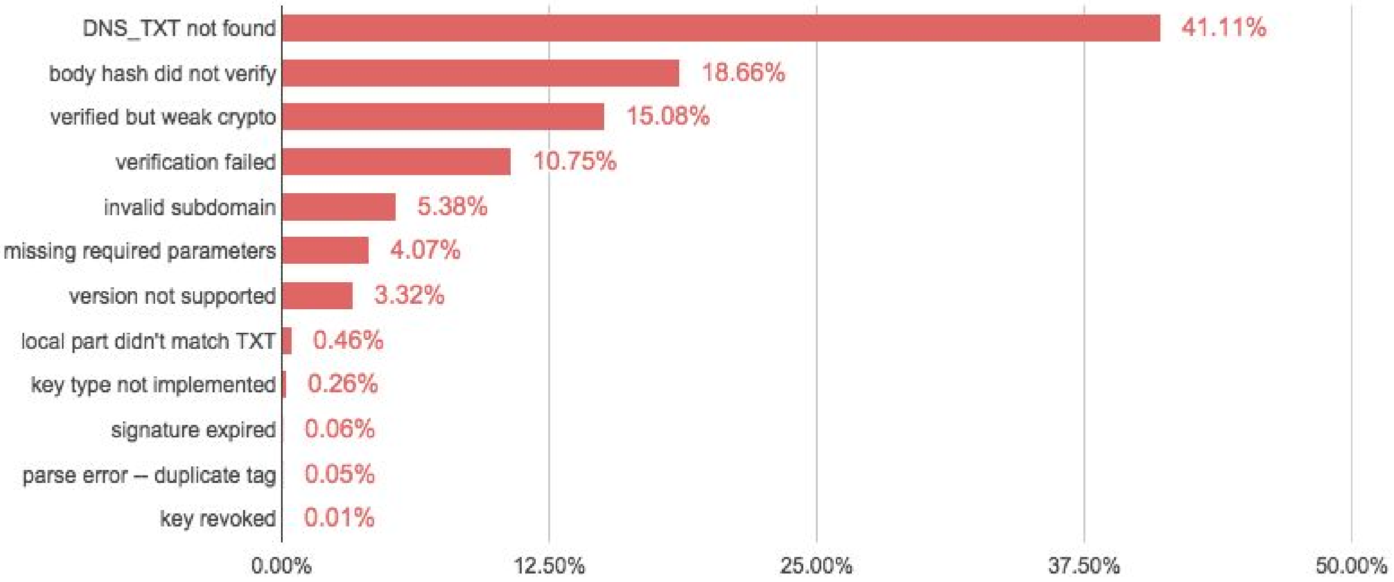


2013

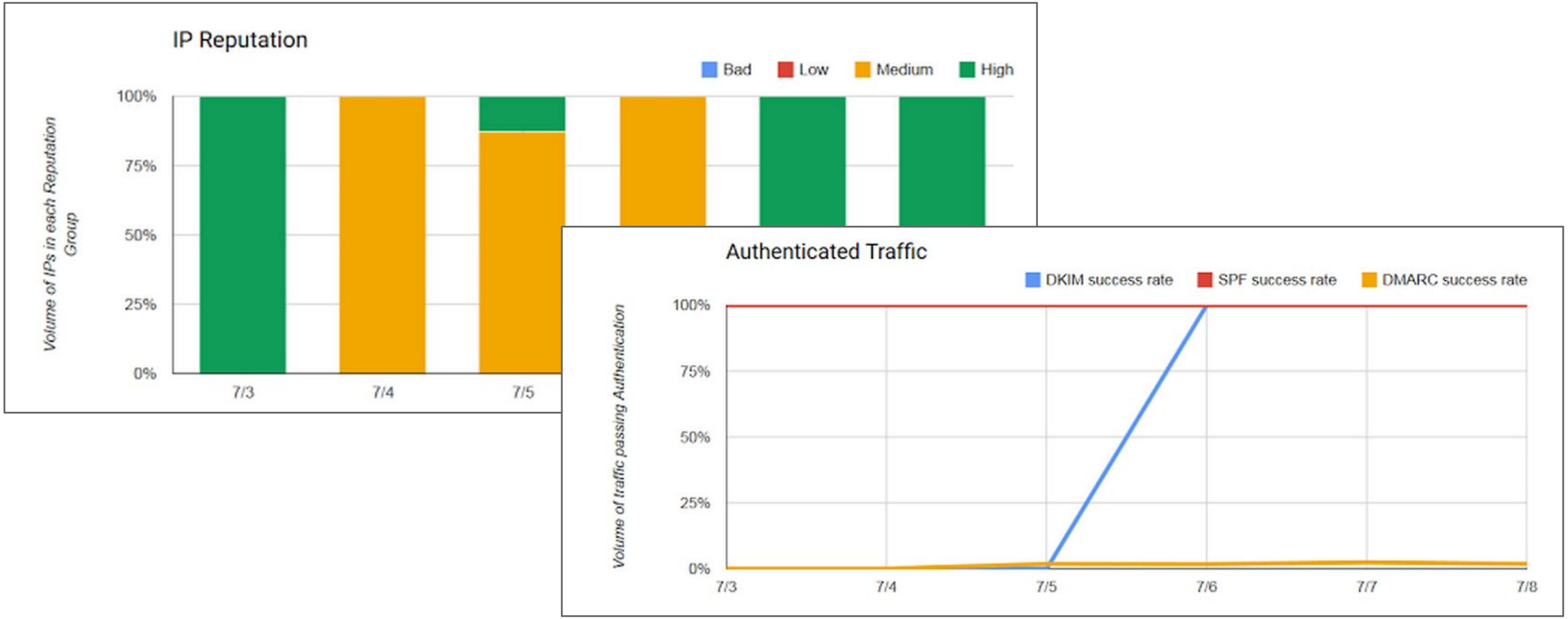


2015

Why DKIM fail?



Exposing data to Postmasters



3 Future

Missing encryption UI

SMTP Strict Transport Security and cert pinning

DMARC strict rejection enforcement and Auth Chain

Google

Thank you!