Clustering Disparate Attacks: Mapping The Activities of The Advanced Persistent Threat.

Martin Lee , Darren Lewis

Symantec.cloud

Context

32 000 customers

~ 10 million users

~500 000 email malware / day

~1:200 emails contains attached malware.

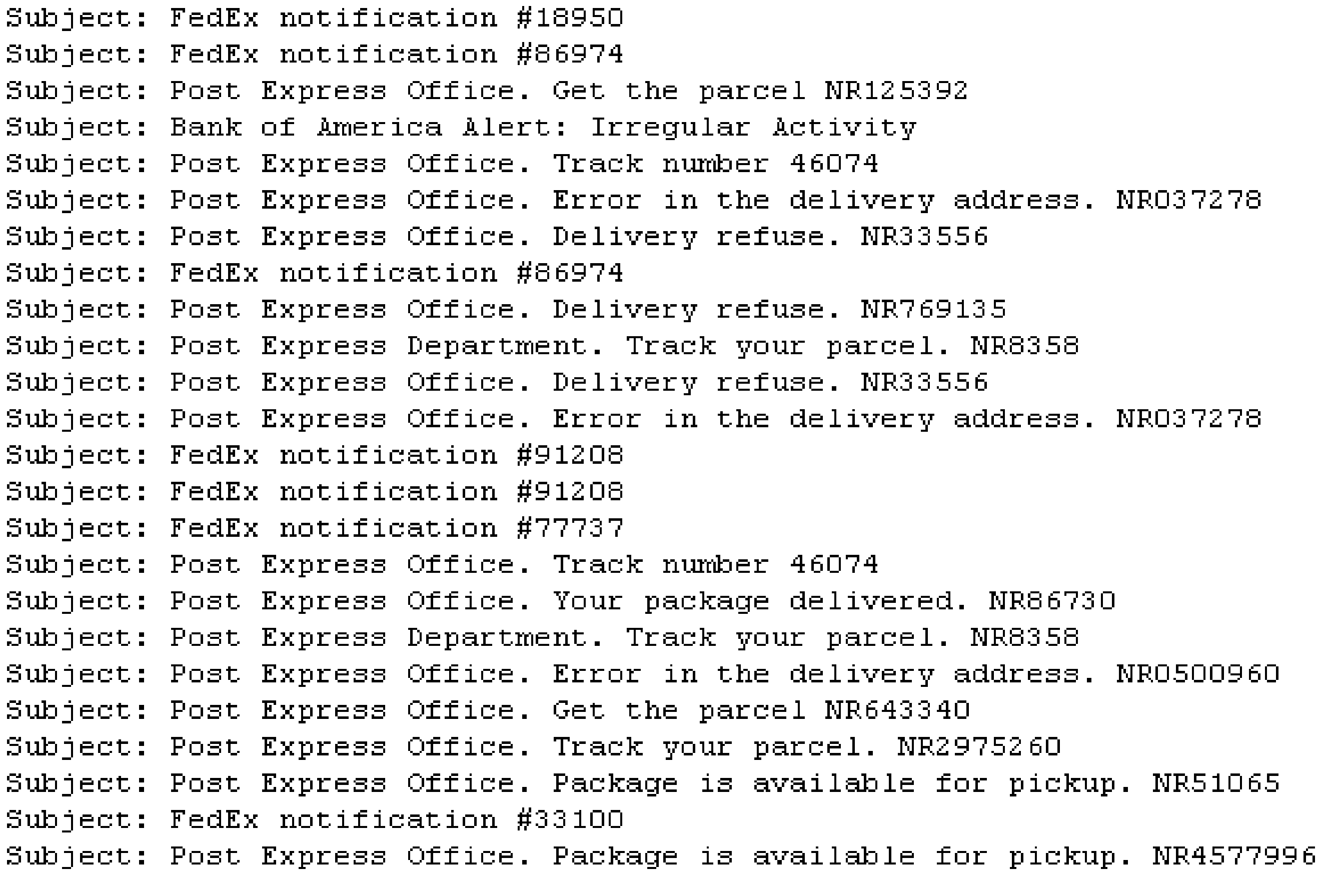
~1:5000 of these, is a targeted attack.

Characteristics of Targeted Attacks

Targeted	Non-Targeted
Attack relevant to interests of recipient	No regard to recipient
Low copy number	High copy number
Bespoke malware	Often kit based
Obscure business model	Clear revenue stream

How Do We Identify Them?

Remove the high copy number attacks.



```
Subject: FedEx notification #18950
Subject: FedEx notification #86974
Subject: Post Express Office. Get the parcel NR125392
Subject: Bank of America Alert: Irregular Activity
Subject: Post Express Office. Track number 46074
Subject: Post Express Office. Error in the delivery address. NR037278
Subject: Post Express Office. Delivery refuse. NR33556
Subject: FedEx notification #86974
Subject: Post Express Office. Delivery refuse. NR769135
Subject: Post Express Department. Track your parcel. NR8358
Subject: Post Express Office. Delivery refuse. NR33556
Subject: Post Express Office. Error in the delivery address. NR037278
Subject: FedEx notification #91208
Subject: FedEx notification #91208
Subject: FedEx notification #77737
Subject: Post Express Office. Track number 46074
Subject: Post Express Office. Your package delivered. NR86730
Subject: Post Express Department. Track your parcel. NR8358
Subject: Post Express Office. Error in the delivery address. NR0500960
Subject: Post Express Office. Get the parcel NR643340
Subject: Post Express Office. Track your parcel. NR2975260
Subject: Post Express Office. Package is available for pickup. NR51065
Subject: FedEx notification #33100
Subject: Post Express Office. Package is available for pickup. NR4577996
```

How Do We Identify Them?

Semi-manually analyse remainder:

False positives

Emailed executables

Tech support clients

‘Broken’ documents

Proof of concepts

Botnet prototypes

Script kiddies

Targeted attacks

Evidence of target selection

Sophistication

Context

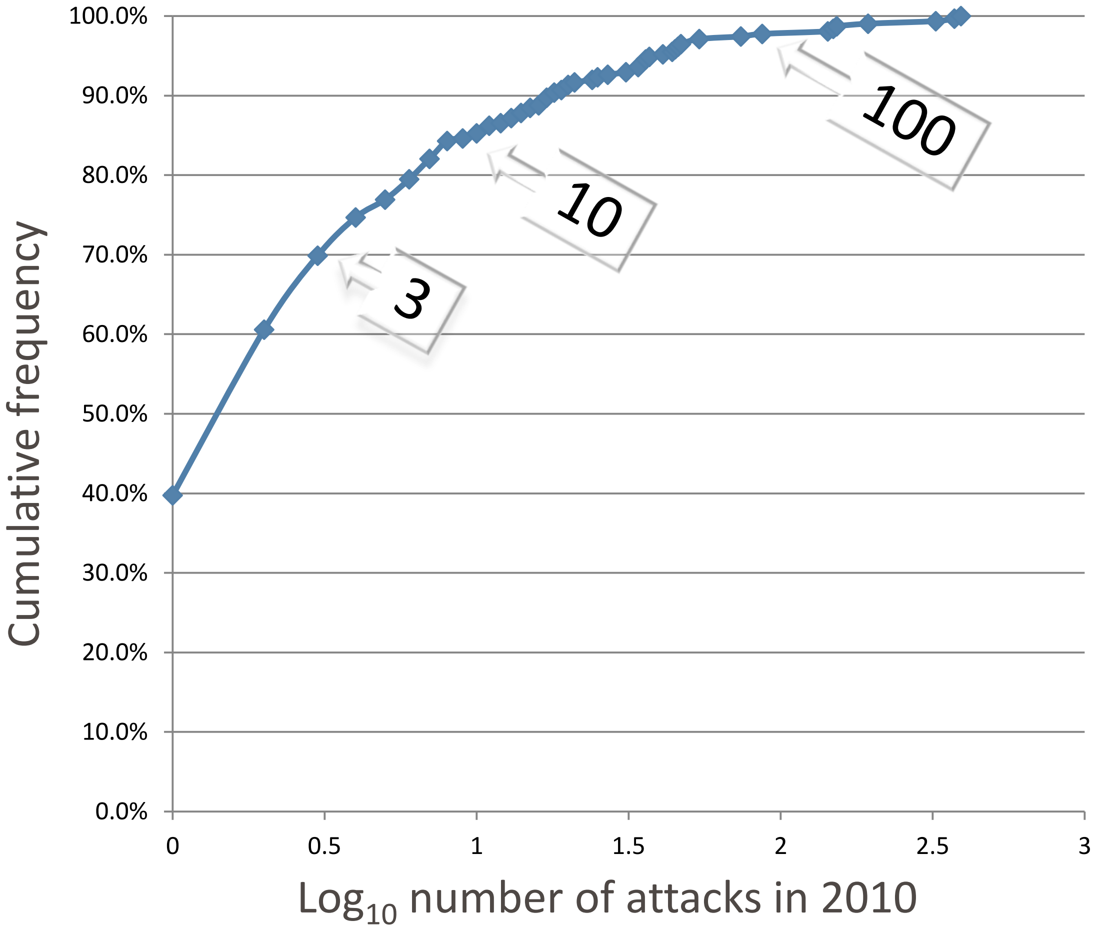
Since April 2008.

72500 targeted attack emails.

Sent to 28 300 email addresses.

Only 1:35 of customer base has been sent a targeted attack.

Frequency of attack against UK companies 2010



70% received no more than 3.

3% received more than 50.

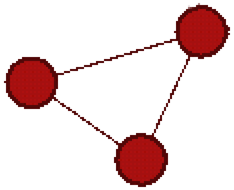
1 received 392 attacks.

Mapping Attacks

FW:Collection of Beautiful Sceneries

1 node = 1 email address

Edge = shared attack



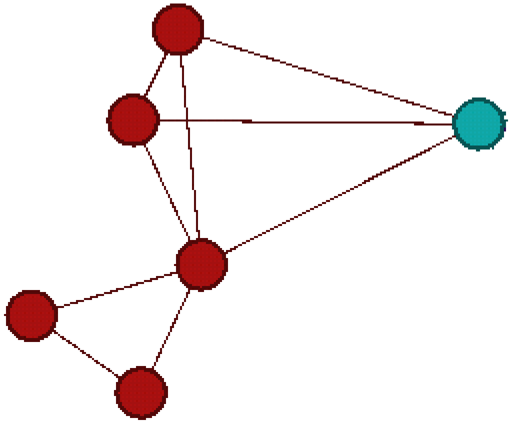
🟩 08 Manufacturing
🟥 19 Non-Profit
🟦 21 Gov/Public Sector
🟪 04 Prof Services

1 attack, 3 recipients

6 - 1 - 2011

Mapping Attacks

Haiti Sexual violence against women increasing

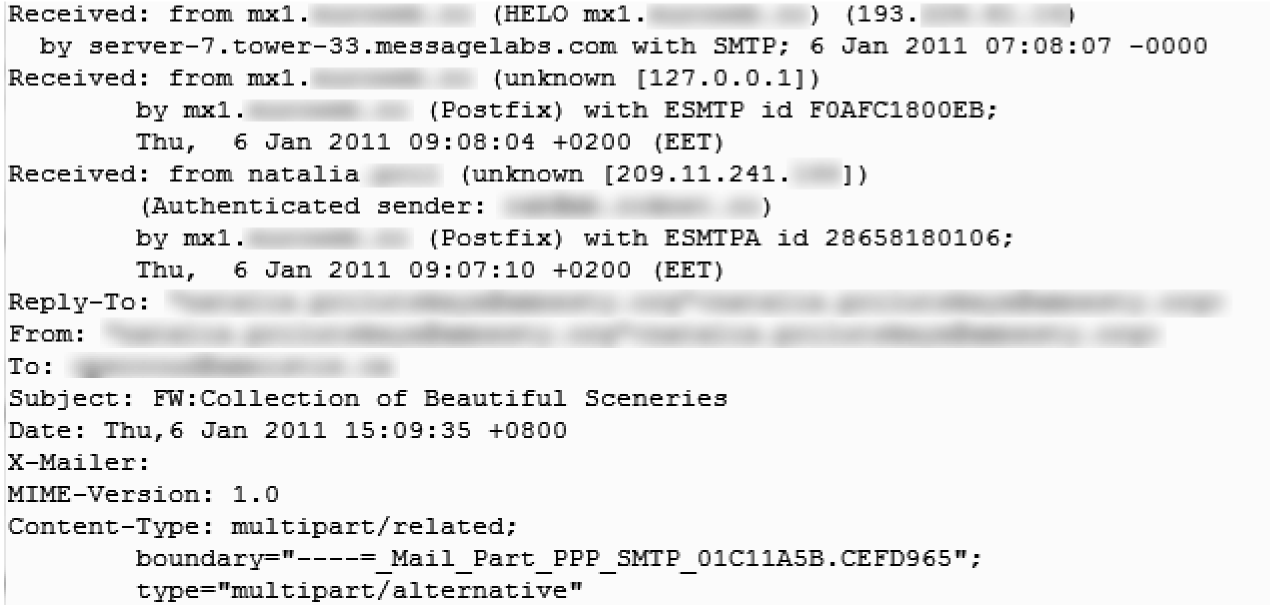


🟩 08 Manufacturing
🟥 19 Non-Profit
🟦 21 Gov/Public Sector
🟪 04 Prof Services

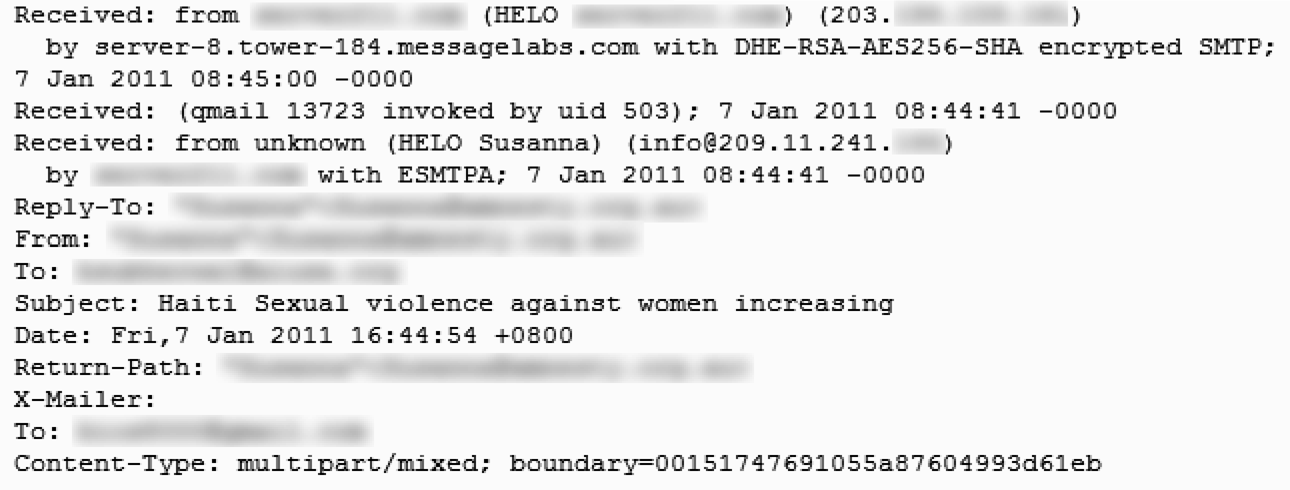
2 attacks, 6 recipients

7 - 1 - 2011

Searching for Similarities



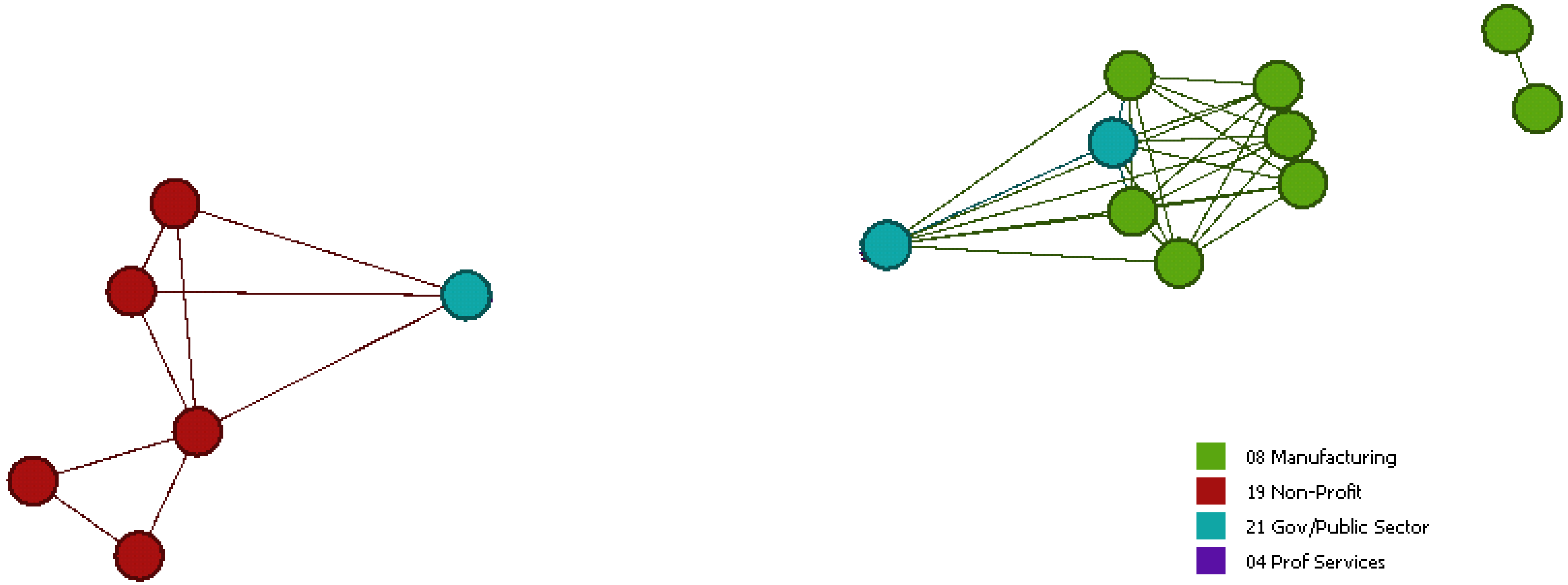
```
Received: from mx1.[redacted] (HELO mx1.[redacted]) (193.[redacted])
  by server-7.tower-33.messagelabs.com with SMTP; 6 Jan 2011 07:08:07 -0000
Received: from mx1.[redacted] (unknown [127.0.0.1])
        by mx1.[redacted] (Postfix) with ESMTP id F0AFC1800EB;
        Thu,  6 Jan 2011 09:08:04 +0200 (EET)
Received: from natalia[redacted] (unknown [209.11.241.[redacted]])
        (Authenticated sender: [redacted])
        by mx1.[redacted] (Postfix) with ESMTPA id 28658180106;
        Thu,  6 Jan 2011 09:07:10 +0200 (EET)
Reply-To: [redacted]
From: [redacted]
To: [redacted]
Subject: FW:Collection of Beautiful Sceneries
Date: Thu,6 Jan 2011 15:09:35 +0800
X-Mailer:
MIME-Version: 1.0
Content-Type: multipart/related;
        boundary="----=_Mail_Part_PPP_SMTP_01C11A5B.CEFD965";
        type="multipart/alternative"
X-MimeOLE: Produced By Microsoft Mime
X-Virus-Scanned: Yes
```



```
Received: from [redacted] (HELO [redacted]) (203.[redacted])
  by server-8.tower-184.messagelabs.com with DHE-RSA-AES256-SHA encrypted SMTP;
7 Jan 2011 08:45:00 -0000
Received: (qmail 13723 invoked by uid 503); 7 Jan 2011 08:44:41 -0000
Received: from unknown (HELO Susanna) (info@209.11.241.[redacted])
  by [redacted] with ESMTPA; 7 Jan 2011 08:44:41 -0000
Reply-To: [redacted]
From: [redacted]
To: [redacted]
Subject: Haiti Sexual violence against women increasing
Date: Fri,7 Jan 2011 16:44:54 +0800
Return-Path: [redacted]
X-Mailer:
To: [redacted]
Content-Type: multipart/mixed; boundary=00151747691055a87604993d61eb
```

CVE-2010-3333

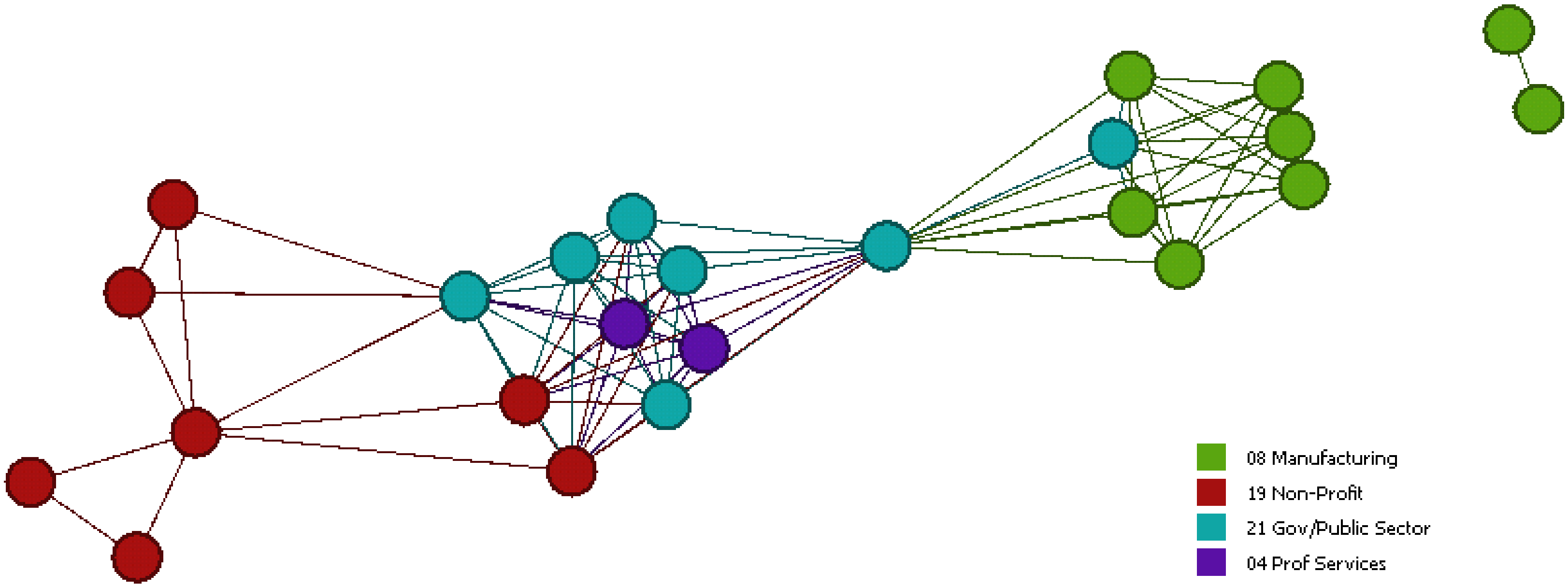
Mapping Attacks



21 - 2 - 2011

6 attacks, 16 recipients

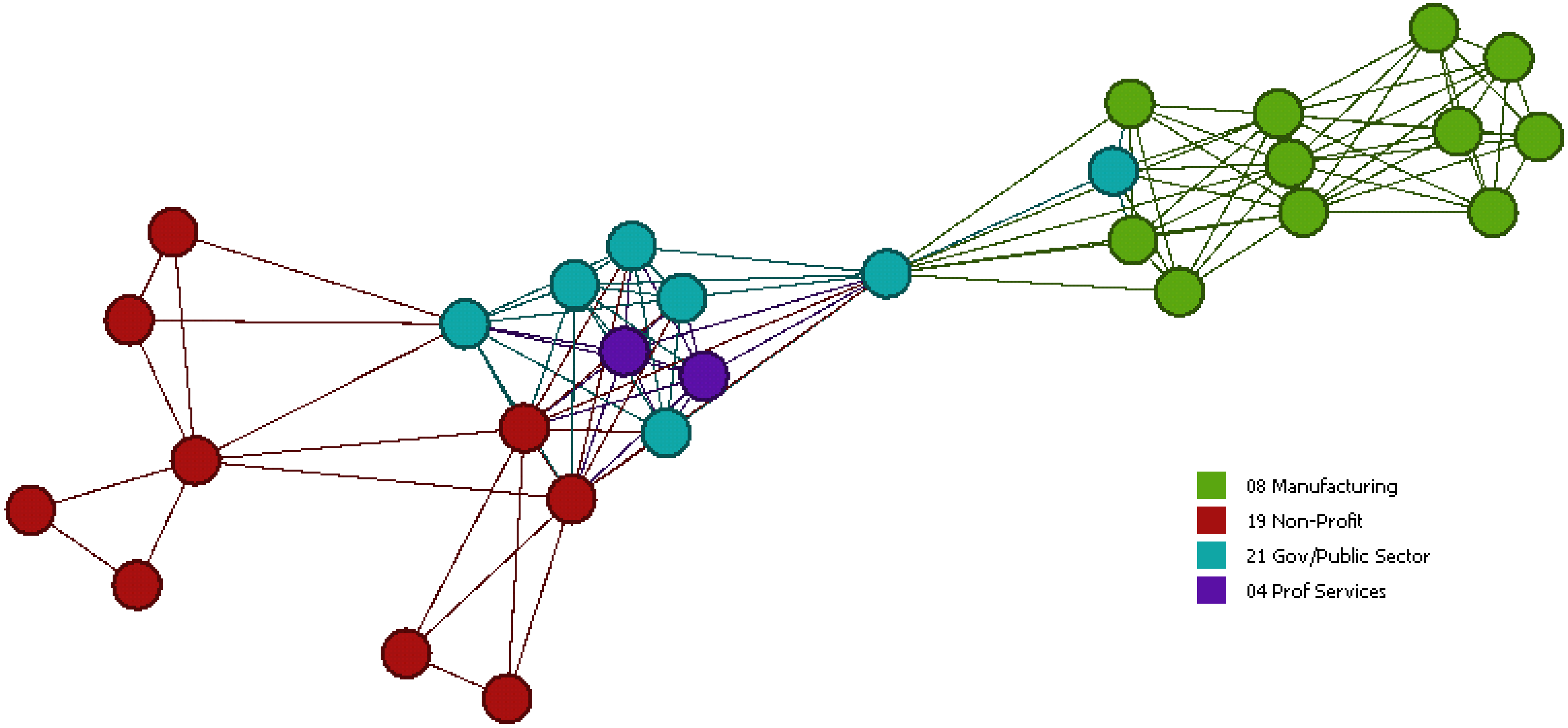
Mapping Attacks



7 attacks, 24 recipients

24 - 2 - 2011

Mapping Attacks



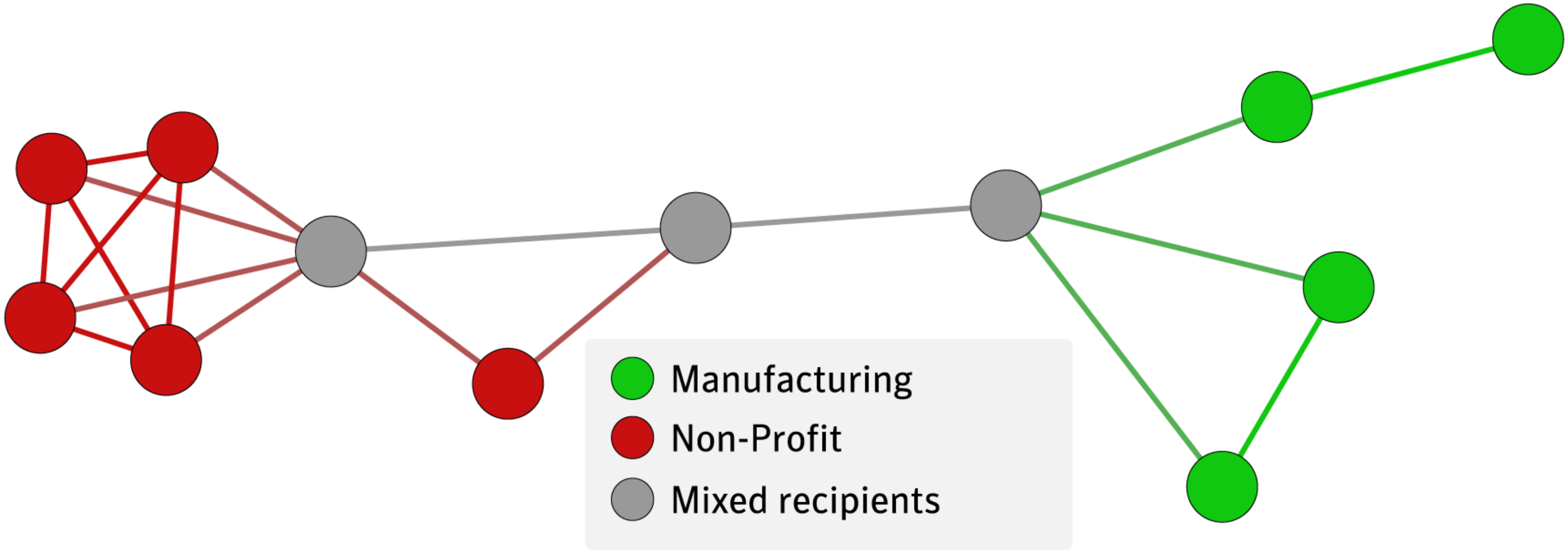
12 attacks, 29 recipients, 7 organisations

26 - 4 - 2011

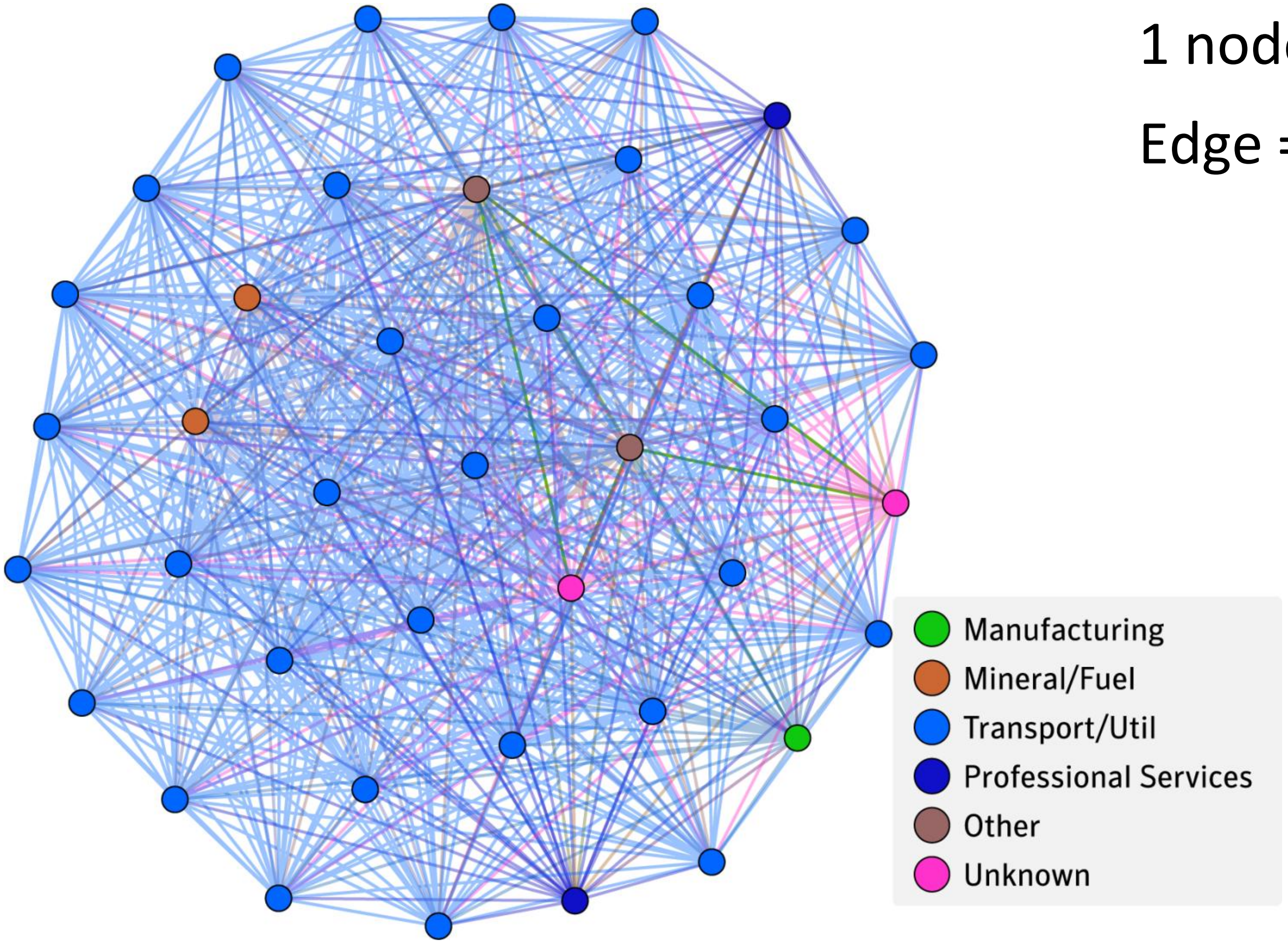
Simple Mapping

1 node = 1 attack

Edge = shared recipients



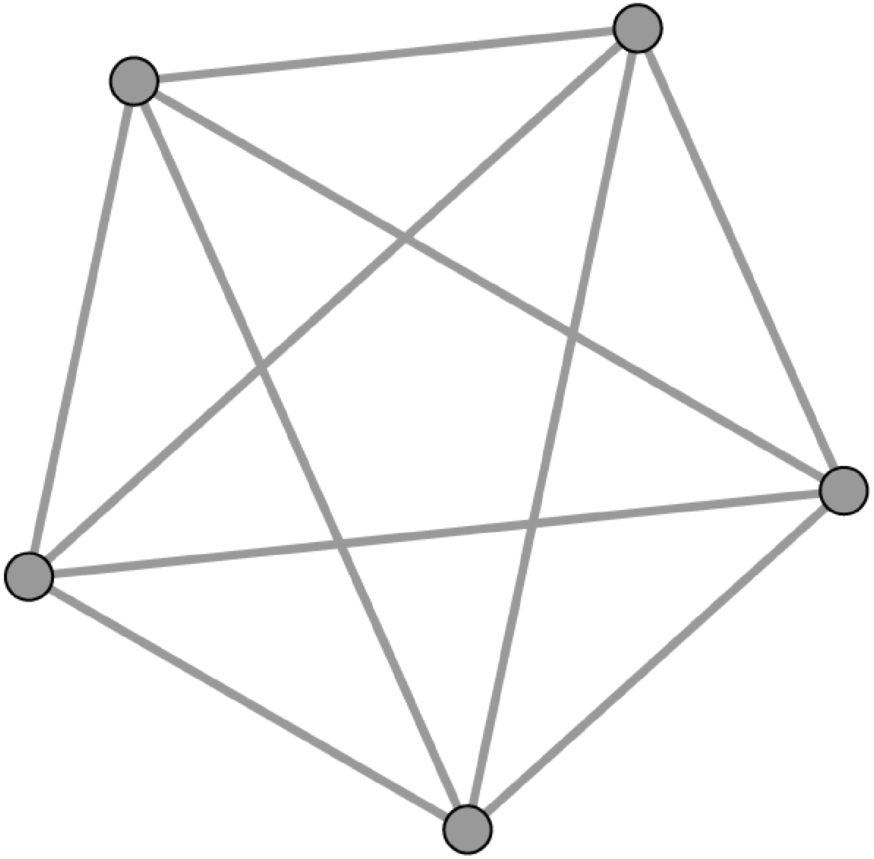
Too Much Information



1 node = 1 email address

Edge = shared attacks

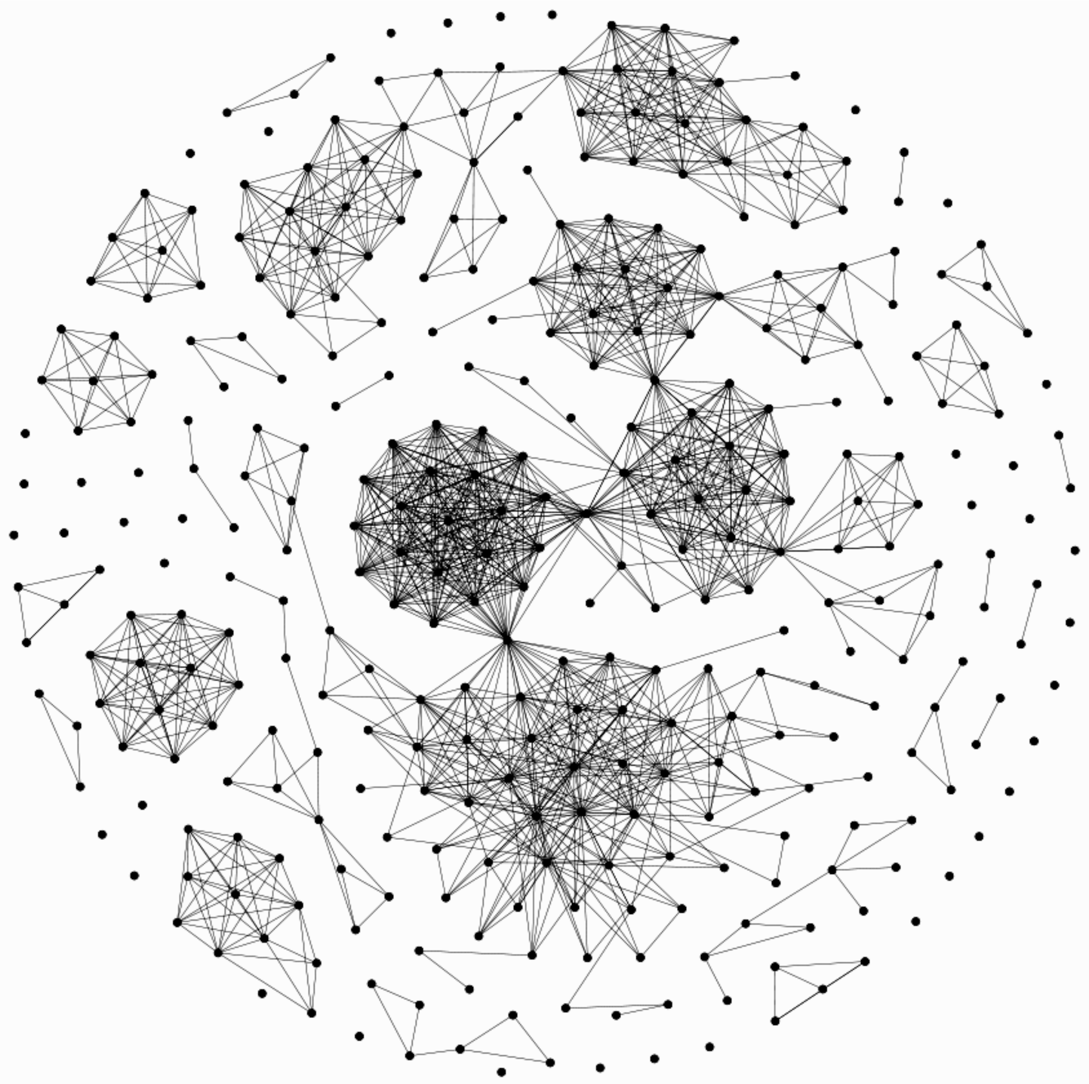
Too Much Information – Same Data



1 node = 1 attack

Edge = shared recipients

UK Private Sector Attacks During 2010



1 node = 1 attack

Edge = shared recipients

3 477 incidents

351 identified attacks

311 are linked

2 x large clusters of

149 & 53 linked attacks

Conclusions

Conclusions

Malware analysis -> similarities between malware -> what's next?

Recipient analysis -> similarities between recipients -> who's next?

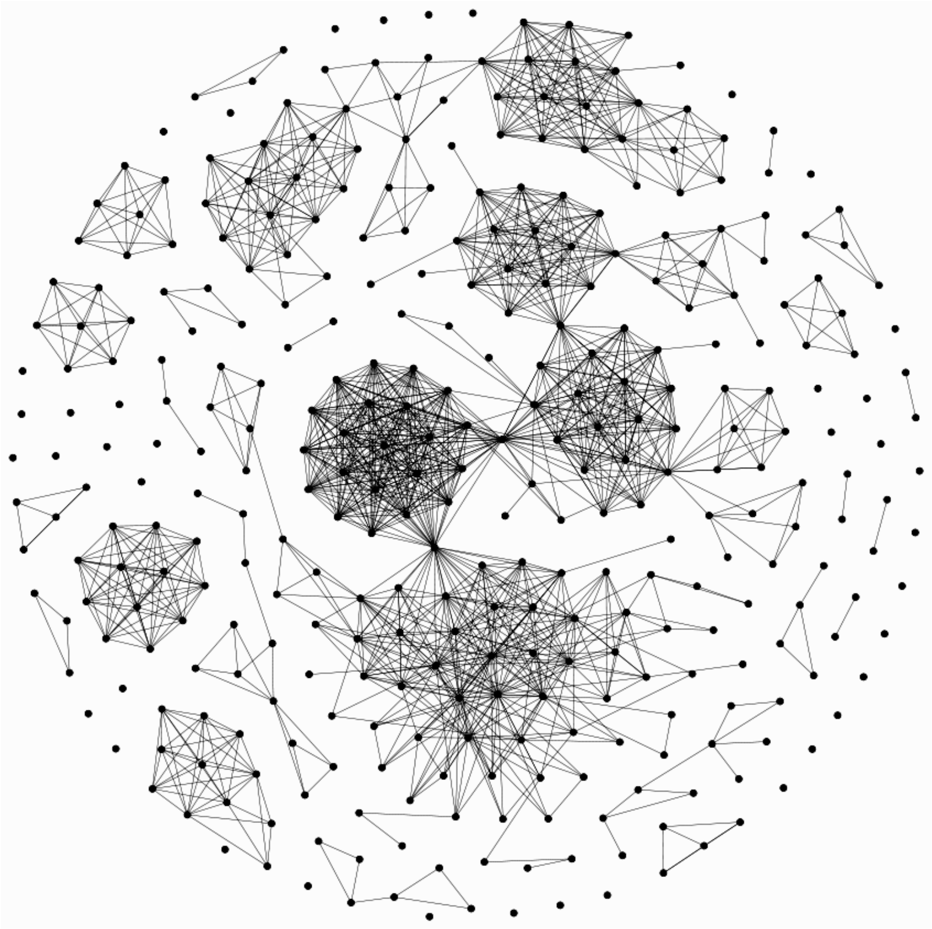
Conclusions

Single attacks make the press.

Collection of data + topological analysis shows size & nature of the issue.

Conclusions

Given enough data, maps can be constructed.



Maps show you where you are and how the landscape changes.

Symantec.cloud™

Thank you!

Martin Lee
martin_lee@symantec.com
+44 7775 823 278

Thanks: Tony Millington, Prashant Gupta, Steve White, Paul Stock, Polly Marshall.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.