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

<table>
<thead>
<tr>
<th>Targeted</th>
<th>Non-Targeted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack relevant to interests of recipient</td>
<td>No regard to recipient</td>
</tr>
<tr>
<td>Low copy number</td>
<td>High copy number</td>
</tr>
<tr>
<td>Bespoke malware</td>
<td>Often kit based</td>
</tr>
<tr>
<td>Obscure business model</td>
<td>Clear revenue stream</td>
</tr>
</tbody>
</table>
How Do We Identify Them?

Remove the high copy number attacks.
How Do We Identify Them?

Semi-manually analyse remainder:

<table>
<thead>
<tr>
<th>False positives</th>
<th>Proof of concepts</th>
<th>Targeted attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emailed executables</td>
<td>Botnet prototypes</td>
<td>Evidence of target selection</td>
</tr>
<tr>
<td>Tech support clients</td>
<td>Script kiddies</td>
<td>Sophistication</td>
</tr>
<tr>
<td>‘Broken’ documents</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 attack, 3 recipients

1 node = 1 email address
Edge = shared attack

6 - 1 - 2011
Mapping Attacks

Haiti Sexual violence against women increasing

2 attacks, 6 recipients

7 - 1 - 2011
Mapping Attacks

6 attacks, 16 recipients

21 - 2 - 2011
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.
Thank you!

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