Looking Back at Three Years of Targeted Attacks

Lessons Learned on the Attackers’ Behaviors and Victims’ Profiles

Olivier Thonnard
Principal Research Engineer
OUTLINE

1. Introduction
2. Targeted Attack Intelligence
3. Victims Profiles: Organizations and Individuals
4. Conclusions and Lessons Learned
Introduction

Targeted Attacks – Symantec TRIAGE methodology
Introduction

Characteristics of Targeted Attacks

**Targeted**
- Attack relevant to interests of recipient
- Low copy number
- Tailored malware, often embedded in weaponized documents
- Obscure business model

**Non-targeted**
- No regard to recipient
- High volume
- Common malware, often based on exploit kits
- Clear revenue stream

Cyberespionage
Privacy breach
IP theft

FIRST 2014 - Looking Back at Three Years of Targeted Attacks
Targeted Attacks – 2011-2013

Average Number of Spear-Phishing Attacks Per Day, 2011–2013

Source: Symantec
Data Set
Spear Phishing Emails

- **SKEPTIC** (and a combination of various filters/analyzers) used to block targeted attacks sent to Symantec.cloud customers
- Data set: over 100K attack emails blocked between 2011 → 2013
- Every email attachment was further analyzed:
  - AV Signatures from most common AV engines
  - Dynamic analysis: file and registry activities, network activity
- IP addresses of attackers mapped to geographical location
- Targeted recipients and domains mapped to industry sectors
  - Based on the SIC taxonomy

→ The enriched dataset was fed to TRIAGE for multi-dimensional clustering analysis and campaign/threat group identification
Email-targeted Spear-phishing Attacks Intelligence

Going from isolated attacks to coordinated campaigns (attribution)

Symantec TRIAGE technology: identifies attack campaigns performed by various threat groups
An Attack Campaign

A series of emails that:

- Show clear evidence that the subject and target has been deliberately selected.
- Contain at least 3 or 4 strong correlations to other emails, such as the topic, sender address, recipient domain, source IP address, etc.
- Are sent on the same day or across multiple days.

A Sykipot campaign (2011)
Typical Use case: Bottom-up Forensics Analysis

• Start from specific IOC’s:
  - **MD5**: 78c3d73e2e2bba6d8811c5dc39edd600
  - Zero-day exploit: **CVE-2012-0779**
  - **C&C**: 126.19.84.7

→ Any previously identified campaign associated to one of these IOC’s?
  - Find and visualize all related attacks (campaign analysis)
  - Quickly identify which “threat group” is likely behind these attacks

• Other way around:
  - **CommentCrew** is presumably linked to following IOC’s:
    - **MD5**: e1117ec1ea73b6da7f2c051464ad9197
    - **C&C**: 50.115.140.211
    - **Exploit**: CVE-2012-0754.B

→ Can we identify an attack campaign associated to these IOC’s?
Why TRIAGE Analytics?

Intelligence Extraction and Attack Investigation

- Identify groups of attacks related to the same campaign, likely orchestrated by a specific “threat group”

- Correlate indicators across data sets, enterprises, geographies, industry sectors, etc

- Determine the patterns and behaviors of the intruders, i.e., their tactics, techniques, and procedures (TTP’s)

- Find “how” they operate, rather than “what” they do

- Challenge: Intrusions sourced by the same attackers (group) may have varying degrees of correlation (md5, IP, from/to domains, attachments, etc)

FIRST 2014 - Looking Back at Three Years of Targeted Attacks
**Typical challenge addressed by TRIAGE**

**Identify Commonalities and Overlapping Indicators**

<table>
<thead>
<tr>
<th>Phase</th>
<th>Email feature</th>
<th>Intrusion 1</th>
<th>Intrusion 2</th>
<th>Intrusion 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconnaissance</td>
<td>Recipient</td>
<td>[user1]@org1.gov.uk</td>
<td>[user2]@org2.gov.uk</td>
<td>[user3]@org2.gov.uk</td>
</tr>
<tr>
<td>Weaponization</td>
<td>Attach_name</td>
<td>Global Pulse Project***.pdf</td>
<td>Agenda – G20***.pdf</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Attach MD5</td>
<td>dd2ed3f7dead4a[***]</td>
<td>2e36081dd7f62e[***]</td>
<td></td>
</tr>
<tr>
<td>Delivery</td>
<td>Date</td>
<td>2011-05-13</td>
<td>2011-05-14</td>
<td>2011-07-02</td>
</tr>
<tr>
<td></td>
<td>From addr.</td>
<td>[Att1]@gmail.com</td>
<td>[Att2]@gmail.com</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sender IP</td>
<td>74.125.83.***</td>
<td>74.125.82.***</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subject</td>
<td>FW:Project Document</td>
<td>Project Document</td>
<td>G20 Ds Finance Key Info – Paris July 2011</td>
</tr>
<tr>
<td></td>
<td>Email body</td>
<td>[body1]</td>
<td>[body2]</td>
<td></td>
</tr>
<tr>
<td>Exploitation</td>
<td>AV signature</td>
<td>CVE-2011-0611.C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Persistence</td>
<td>C&amp;C domains</td>
<td><a href="http://www.webserver">www.webserver</a>.***</td>
<td>[N/A]</td>
<td></td>
</tr>
</tbody>
</table>
Targeted Attack Intelligence
Targeted Attacks

Increase in targeted attack campaigns

+91%
Targeted Attack Campaigns

<table>
<thead>
<tr>
<th></th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email per Campaign</td>
<td>78</td>
<td>122</td>
<td>779</td>
</tr>
<tr>
<td>Recipients/Campaign</td>
<td>61</td>
<td>408</td>
<td>23</td>
</tr>
<tr>
<td>Campaigns</td>
<td>165</td>
<td>111</td>
<td>29</td>
</tr>
<tr>
<td>Duration of Campaign</td>
<td>4 days</td>
<td>3 days</td>
<td>8.3 days</td>
</tr>
</tbody>
</table>

FIRST 2014 - Looking Back at Three Years of Targeted Attacks
Focused versus Large-scale campaigns

- **Type 1**: More focused campaigns: 68%
- **Type 2**: Mass-scale (MOTA): 32%

**Target**
- Nr of Targeted companies
  - ≤ 5
  - > 5

**Sector**
- Type 1: Highly focused (≤ 5 sectors)
- Type 2: Mass-scale (> 5 sectors)

---

FIRST 2014 - Looking Back at Three Years of Targeted Attacks
“Targeted” campaign does not always mean small in size!

Elderwood Campaign – April 2012

- An Elderwood Campaign that used “gg880dd.com” accounts
- Over 1,800 attacks on **April 25, 2012**
- Exploits CVE-2012-0779 (**disclosed May 5, 2012**)
- Was targeting only 2 large Defense/Manufacturing industries
Doc types

<table>
<thead>
<tr>
<th>Executable type</th>
<th>2013</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>.exe</td>
<td>31.3%</td>
<td>39%</td>
</tr>
<tr>
<td>.scr</td>
<td>18.4%</td>
<td>2%</td>
</tr>
<tr>
<td>.doc</td>
<td>7.9%</td>
<td>34%</td>
</tr>
<tr>
<td>.pdf</td>
<td>5.3%</td>
<td>11%</td>
</tr>
<tr>
<td>.class</td>
<td>4.7%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>.jpg</td>
<td>3.8%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>.dmp</td>
<td>2.7%</td>
<td>1%</td>
</tr>
<tr>
<td>.dll</td>
<td>1.8%</td>
<td>1%</td>
</tr>
<tr>
<td>.au3</td>
<td>1.7%</td>
<td>&lt;1%</td>
</tr>
<tr>
<td>.xls</td>
<td>1.2%</td>
<td>5%</td>
</tr>
</tbody>
</table>

- More than **50 percent** of email attachments used in spear phishing attacks were executable files in 2013.
- **Microsoft Word and PDF documents** are both used regularly, making up 7.9 and 5.3 percent of attachments, respectively. However, these are both down from 2012.
- **Java .class files** also made up 4.7 percent of email attachments used in spear phishing attacks.
Email Topics Used in Targeted Attacks

- Most frequently occurring words used in targeted spear-phishing email attacks throughout 2013.
“Watering Hole” Attacks (2012-2013)

- Targeted Attacks predominantly start as spear phishing attacks
- In 2012, Watering Hole Attacks emerged (popularized by the Elderwood Gang)
Effectiveness of Watering Hole Attacks

- Watering Hole attacks are targeted at specific groups
- Can capture a large number of victims in a very short time

Watering Hole Attack in 2012

Infected 500 Companies

All Within 24 Hours
Example of Watering Hole Attack

- In 2013 this type of attack will become widely used
- Several high profile companies fell victim to just such an attack
There were a total of 23 zero-day vulnerabilities discovered in 2013. This is up from 14 in 2012.

There have been more zero-day vulnerabilities discovered in 2013 than in any year since Symantec began tracking them, and more than the past two years combined.
Relationship with Vulnerabilities

Scanned Websites With Vulnerabilities...

- 53% in 2012
- 78% in 2013 (an increase of 25%)

...% of Which Were Critical

- 24% in 2012
- 16% in 2013 (a decrease of 8%)

1 in 8 sites had critical unpatched vulnerabilities
Spear-phishing campaigns are becoming more aggressive ...

An employee of a multinational company receives an email referencing an INVOICE ...

Dear Employee,

Please take a moment to open the attached invoice:

Sincerely,
Sender

Invoice

The “Francophoned” attack campaign
(April 2013)
Spear-phishing campaigns are becoming more aggressive ... 

Minutes later, she receives a phone call ... 

Please process the invoice ... 

Attacker impersonates a high-ranked executive, requesting the victim to open immediately the attachment ...
Spear-phishing campaigns are becoming more aggressive ...
Targeted Attacks: Profiling Victims

Organizations and Individuals
Top 10 Industries Targeted in Spear-Phishing Attacks, 2013

- Public Administration (Gov.): 16%
- Services – Professional: 15%
- Services – Non-Traditional: 14%
- Manufacturing: 13%
- Finance, Insurance & Real Estate: 13%
- Transportation, Gas, Communications, Electric: 6%
- Wholesale: 5%
- Retail: 2%
- Mining: 1%
- Construction: 1%

Source: Symantec
Targeted Attacks by Industry in 2012

- Manufacturing: 24%
- Finance, Insurance & Real Estate: 19%
- Services – Non-Traditional: 17%
- Government: 12%
- Energy/Utilities: 10%
- Services – Professional: 8%
- Wholesale: 2%
- Retail: 2%
- Aerospace: 2%
- Transportation, Communications, Electric, Gas: 1%

- Manufacturing moved to top position in 2012
- But all industries are targeted
Spear Phishing Attacks by Size of Targeted Organization, 2011 – 2013

Source: Symantec

Organization size

<table>
<thead>
<tr>
<th>Year</th>
<th>1 to 250</th>
<th>251 to 500</th>
<th>501 to 1,000</th>
<th>1,001 to 1,500</th>
<th>1,501 to 2,500</th>
<th>2,501+ Employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>18%</td>
<td>50%</td>
<td>31%</td>
<td>50%</td>
<td>50%</td>
<td>100%</td>
</tr>
<tr>
<td>2012</td>
<td>30%</td>
<td>50%</td>
<td>50%</td>
<td>50%</td>
<td>50%</td>
<td>100%</td>
</tr>
<tr>
<td>2013</td>
<td>30%</td>
<td>50%</td>
<td>50%</td>
<td>50%</td>
<td>50%</td>
<td>100%</td>
</tr>
</tbody>
</table>
Risk Analysis
Epidemiology Concepts

Afflicted group

Identified “Factor”

- #subjects with factor
- #subjects without factor

Control group

Similar population

Goal: Compare likelihood of finding factor in afflicted (“diseased”) group with that of control group.
Odds Ratio (OR): Calculate strength of association of factor with “diseased” state by comparing probabilities.

<table>
<thead>
<tr>
<th></th>
<th>Diseased (afflicted)</th>
<th>Control (unafflicted)</th>
</tr>
</thead>
<tbody>
<tr>
<td>With risk factor</td>
<td>$p_{11}$</td>
<td>$p_{10}$</td>
</tr>
<tr>
<td>Without risk factor</td>
<td>$p_{01}$</td>
<td>$p_{00}$</td>
</tr>
</tbody>
</table>

$$OR = \frac{p_{11} \times p_{00}}{p_{10} \times p_{01}}$$

Odds ratio $> 1 \implies$ positive correlation

$< 1 \implies$ negative correlation
### Ratio of Organizations in an Industry Impacted by Targeted Attack Sent by Spear-Phishing Email

<table>
<thead>
<tr>
<th>Risk</th>
<th>1 IN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mining</td>
<td>2.7</td>
</tr>
<tr>
<td>Public Administration (Government)</td>
<td>3.1</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>3.2</td>
</tr>
<tr>
<td>Wholesale</td>
<td>3.4</td>
</tr>
<tr>
<td>Transportation, Communications, Electric, Gas &amp; Sanitary Services</td>
<td>3.9</td>
</tr>
<tr>
<td>Finance, Insurance &amp; Real Estate</td>
<td>4.8</td>
</tr>
<tr>
<td>Services — Non-Traditional</td>
<td>6.6</td>
</tr>
<tr>
<td>Construction</td>
<td>11.3</td>
</tr>
<tr>
<td>Agriculture, Forestry &amp; Fishing</td>
<td>12.0</td>
</tr>
</tbody>
</table>

Source: Symantec
### “At-Risk” Organizations by Size

<table>
<thead>
<tr>
<th>Risk</th>
<th>Ratio</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td></td>
</tr>
<tr>
<td>2,500+</td>
<td>2.3</td>
</tr>
<tr>
<td>1,501–2,500</td>
<td>2.9</td>
</tr>
<tr>
<td>1,001–1,500</td>
<td>2.9</td>
</tr>
<tr>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>501–1,000</td>
<td>3.8</td>
</tr>
<tr>
<td>251–500</td>
<td>4.3</td>
</tr>
<tr>
<td>1–250</td>
<td>5.2</td>
</tr>
</tbody>
</table>

*Ratio of Organizations Targeted by Industry Size Sent by Spear-Phishing Email

Source: Symantec

**FIRST 2014 - Looking Back at Three Years of Targeted Attacks**
**At-Risk** Individuals

Based on data collected from:

<table>
<thead>
<tr>
<th>Risk</th>
<th>Personal Assistant (Executive Assistant)</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Media</td>
</tr>
<tr>
<td>Medium</td>
<td>Senior Management</td>
</tr>
<tr>
<td></td>
<td>Sales</td>
</tr>
<tr>
<td></td>
<td>C-Level</td>
</tr>
<tr>
<td>Low</td>
<td>Recruitment</td>
</tr>
<tr>
<td></td>
<td>R&amp;D</td>
</tr>
</tbody>
</table>

Risk of Job Role Impact by Targeted Attack Sent by Spear-Phishing Email

Source: Symantec

FIRST 2014 - Looking Back at Three Years of Targeted Attacks
Most Likely To Be Targeted in 2013

Personal Assistant at a Large Mining company

To: JohnDoe@drillanddig.com
Subject: Re: Order Payment
From: Attacker

Please click on this executable to see your order information.
Targeted Attacks by Job Function in 2012

- R&D: 27%
- Senior: 12%
- C-Level: 17%
- Sales: 24%
- Shared Mailbox: 13%
- Recruitment: 4%
- Media: 3%
- PA: 1%

 Attacks may start with the ultimate target, but often look opportunistically for any entry into a company.
Conclusions – Lessons Learned
Targeted Attacks – Lessons Learned

• The Number of **Targeted Attacks has steadily increased** over the last few years

• Campaigns are becoming more **persistent**, more diverse and **widespread** (sometimes even automated), more **prevalent**

• Increases in zero-day vulnerabilities and unpatched web sites facilitate **move to watering hole style** targeted attacks

• **Most industries** are at elevated risk, in particular in favorable economic markets or government-related areas, and large organisations

• **Users continue to fall for social engineering tricks** and are not applying street smarts to online activity

• Urgent need for more **advanced intelligence capabilities** to better defend ourselves against such attacks (moving target)
## Thwarting Targeted Attacks

<table>
<thead>
<tr>
<th>Security Intelligence</th>
<th>• Human Intelligence regarding active and anticipated attack campaigns, targeted attacks, and emerging threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Holistic Security Monitoring</td>
<td>• Use full capabilities of monitoring solutions to provide full visibility into security posture and events across the entire enterprise footprint</td>
</tr>
<tr>
<td>Removable Media Device Control</td>
<td>• Restrict removable devices and functions to prevent malware infection</td>
</tr>
<tr>
<td>Email &amp; Web Gateway Filtering</td>
<td>• Scan and monitor inbound/outbound email and web traffic and block accordingly</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>• Discover data spills of confidential information that are targeted by attackers</td>
</tr>
<tr>
<td></td>
<td>• Detect and prevent exfiltration of confidential information that are targeted by attackers</td>
</tr>
<tr>
<td>Encryption</td>
<td>• Create and enforce security policies so all confidential information is encrypted</td>
</tr>
<tr>
<td>Incident Preparedness &amp; Response</td>
<td>• Ensure formal Incident Response capabilities are in place and fully tested</td>
</tr>
<tr>
<td></td>
<td>• Conduct periodic penetration tests and red-team exercises to evaluate defense and response capabilities from the perspective of an attacker</td>
</tr>
</tbody>
</table>
Thank you!

Olivier Thonnard
Olivier_Thonnard@symantec.com

2013 was the Year of the Mega Breach