A Broad View of the Ecosystem of Socially Engineered Exploit Documents

Stevens Le Blond, Cédric Gilbert, Utkarsh Upadhyay, Manuel Gomez Rodriguez and David Choffnes
Challenges with measuring targeted attacks

- **Low-volume, socially engineered** messages that convince **specific victims** to install malware
Challenges with measuring targeted attacks

• Low-volume, socially engineered messages that convince specific victims to install malware

• Three studies published at Usenix Security’14
  • Tibet (Hardy et al.), Middle East (Marczak et al.), and Uyghur (Le Blond et al.)
Challenges with measuring targeted attacks

- **Low-volume, socially engineered** messages that convince specific victims to install malware
- Three studies published at Usenix Security’14
  - Tibet (Hardy et al.), Middle East (Marczak et al.), and Uyghur (Le Blond et al.)
Challenges with measuring targeted attacks

- **Low-volume, socially engineered** messages that convince **specific** victims to install malware
- Three studies published at Usenix Security’14
  - Tibet (Hardy et al.), Middle East (Marczak et al.), and Uyghur (Le Blond et al.)
Challenges with measuring targeted attacks

- **Low-volume, socially engineered** messages that convince specific victims to install malware
- Three studies published at Usenix Security’14
  - Tibet (Hardy et al.), Middle East (Marczak et al.), and Uyghur (Le Blond et al.)

Measuring targeted attacks is a long and difficult process
Can Anti-Virus Aggregators (VirusTotal) help?
Can Anti-Virus Aggregators (VirusTotal) help?
Can Anti-Virus Aggregators (VirusTotal) help?
Can Anti-Virus Aggregators (VirusTotal) help?
VirusTotal Statistics (one week)
VirusTotal Statistics (one week)
VirusTotal Statistics (one week)
VirusTotal Statistics (one week)
VirusTotal Statistics (one week)
VirusTotal Statistics (one week)
VirusTotal as a vantage point to measure targeted attacks
VirusTotal as a vantage point to measure targeted attacks
VirusTotal as a vantage point to measure targeted attacks
VirusTotal as a vantage point to measure targeted attacks
Research questions

• Do targeted groups upload exploit documents to VirusTotal?

• Can we scale our analysis to hundreds of thousands of samples?

• How do attacks faced by different groups compare with each other?

• Is VirusTotal used by other actors such as attackers and researchers?
Outline

1) Methodology
2) Analysis of exploit documents
3) Future work
Exploit document infection process

1. Exploit document's delivery

Exploit  Decoy  Malware
Exploit document infection process

1. Exploit document's delivery
2. Reader exploitation
Exploit document infection process
Exploit document infection process
Data acquisition and processing workflow

1. Acquisition
   - VirusTotal
   - WUC

2. Detection
   - VirusTotal
   - WUC

3. Extraction
   - VirusTotal
   - WUC

4. Decoys analysis
   - Decoys

5. Malware analysis
   - Malware
Data acquisition and processing workflow
Can we scale our analysis to hundreds of thousands of samples? Acquisition
Can we scale our analysis to hundreds of thousands of samples? Acquisition
Can we scale our analysis to hundreds of thousands of samples? Acquisition

![Map of the world with icons and links to VirusTotal and EPFL logos.]

- VirusTotal
- EPFL

- 257,635
- 143
Data acquisition and processing workflow
Can we scale our analysis to hundreds of thousands of samples? Detection
Can we scale our analysis to hundreds of thousands of samples? Detection
Can we scale our analysis to hundreds of thousands of samples? Detection
Can we scale our analysis to hundreds of thousands of samples? Detection
How many versions of readers do we have to test?
How many versions of readers do we have to test?

Few exploits are portable across all reader versions.
Data acquisition and processing workflow
Can we scale our analysis to hundreds of thousands of samples? Extraction

257,635
143

-219,794
37,841

2003
2007
2010

Office w/ EMET
Acrobat w/ EMET

SP0 SP1 SP2 SP3
VIII IX X XI

0.0 1.0 2.0 3.0 4.0 5.0
Can we scale our analysis to hundreds of thousands of samples? Extraction
Can we scale our analysis to hundreds of thousands of samples? Extraction
Can we scale our analysis to hundreds of thousands of samples?

Extraction

Office w/ EMET

- 219,794
37,841

Acrobat w/ EMET

-29
114

Office w/ driver

-34,026
3,815

Acrobat w/ driver

-11
103
Data acquisition and processing workflow

1. Acquisition
   - VirusTotal 257,635
   - WUC 143

2. Detection
   - VirusTotal 37,841
   - WUC 114

3. Extraction
   - VirusTotal 3,815
   - WUC 103

4. Decoys analysis
   - Decoys

5. Malware analysis
   - Malware
Can we scale our analysis to hundreds of thousands of samples? Analysis

<table>
<thead>
<tr>
<th></th>
<th>Office w/ EMET</th>
<th>Acrobat w/ EMET</th>
<th>Office w/ driver</th>
<th>Acrobat w/ driver</th>
</tr>
</thead>
<tbody>
<tr>
<td>2003</td>
<td>-219,794</td>
<td>-34,026</td>
<td>-34,026</td>
<td>-11</td>
</tr>
<tr>
<td>2007</td>
<td>37,841</td>
<td></td>
<td>3,815</td>
<td></td>
</tr>
<tr>
<td>2010</td>
<td>143</td>
<td>114</td>
<td>103</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The numbers represent changes in some units, possibly samples or scores, over different years and software versions.
Can we scale our analysis to hundreds of thousands of samples? Analysis

<table>
<thead>
<tr>
<th></th>
<th>Office w/ EMET</th>
<th>Acrobat w/ EMET</th>
<th>Office w/ driver</th>
<th>Acrobat w/ driver</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SP0  SP1  SP2  SP3</td>
<td>0.0 1.0 2.0 3.0 4.0 5.0</td>
<td>SP0  SP1  SP2  SP3</td>
<td>0.0 1.0 2.0 3.0 4.0 5.0</td>
</tr>
<tr>
<td></td>
<td>2003</td>
<td>VIII</td>
<td>2003</td>
<td>VIII</td>
</tr>
<tr>
<td></td>
<td>2007</td>
<td>IX</td>
<td>2007</td>
<td>IX</td>
</tr>
<tr>
<td></td>
<td>2010</td>
<td>X</td>
<td>2010</td>
<td>X</td>
</tr>
<tr>
<td></td>
<td></td>
<td>XI</td>
<td></td>
<td>XI</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>257,635</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-219,794</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>37,841</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-34,026</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3,815</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Can we scale our analysis to hundreds of thousands of samples? Analysis

Office w/ EMET
2003
2007
2010
-219,794
37,841

Acrobat w/ EMET

2003
2007
2010

VIII
IX
X
XI

Acrobat w/ driver

2003
2007
2010

VIII
IX
X
XI

Office w/ driver

SP0
SP1
SP2
SP3

0.0
1.0
2.0
3.0
4.0
5.0

-34,026
3,815

Malware sandboxes

Translators

FireEye

37,841
416
3,815
439
Can we scale our analysis to hundreds of thousands of samples? Analysis

Office w/ EMET

Acrobat w/ EMET

Office w/ driver

Acrobat w/ driver

Translators

Malware sandboxes

- 219,794
37,841

-34,026
3,815

SP0 SP1 SP2 SP3
2003 2007 2010

SP0 SP1 SP2 SP3
2003 2007 2010

SP0 SP1 SP2 SP3
2003 2007 2010

- 219,794
37,841

-34,026
3,815
Can we scale our analysis to hundreds of thousands of samples? Analysis

<table>
<thead>
<tr>
<th></th>
<th>Office w/ EMET</th>
<th>Acrobat w/ EMET</th>
<th>Office w/ driver</th>
<th>Acrobat w/ driver</th>
<th>Translators</th>
<th>Malware sandboxes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SP0 SP1 SP2 SP3</td>
<td>SP0 SP1 SP2 SP3</td>
<td>SP0 SP1 SP2 SP3</td>
<td>SP0 SP1 SP2 SP3</td>
<td>SP0 SP1 SP2 SP3</td>
<td>SP0 SP1 SP2 SP3</td>
</tr>
<tr>
<td></td>
<td>0.0 1.0 2.0 3.0 4.0 5.0</td>
<td>0.0 1.0 2.0 3.0 4.0 5.0</td>
<td>0.0 1.0 2.0 3.0 4.0 5.0</td>
<td>0.0 1.0 2.0 3.0 4.0 5.0</td>
<td>0.0 1.0 2.0 3.0 4.0 5.0</td>
<td>0.0 1.0 2.0 3.0 4.0 5.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2,447</td>
<td>3,705</td>
<td>2,447</td>
<td>3,705</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>-219,794</td>
<td>37,841</td>
<td>-34,026</td>
<td>3,815</td>
<td></td>
<td>2,447</td>
</tr>
<tr>
<td></td>
<td>37,841</td>
<td></td>
<td>3,815</td>
<td></td>
<td></td>
<td>3,705</td>
</tr>
</tbody>
</table>
Outline

1) Methodology
2) Analysis of exploit documents
3) Future work
Do targeted groups upload exploit documents on VirusTotal? Likely targets (inferred from decoys)

<table>
<thead>
<tr>
<th>Group</th>
<th>Number</th>
<th>Fraction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uyghur</td>
<td>237</td>
<td>.16</td>
</tr>
<tr>
<td>Vietnam</td>
<td>145</td>
<td>.10</td>
</tr>
<tr>
<td>USA</td>
<td>118</td>
<td>.08</td>
</tr>
<tr>
<td>Tibet</td>
<td>115</td>
<td>.08</td>
</tr>
<tr>
<td>Taiwan</td>
<td>100</td>
<td>.06</td>
</tr>
<tr>
<td>India</td>
<td>72</td>
<td>.05</td>
</tr>
<tr>
<td>Russia</td>
<td>51</td>
<td>.03</td>
</tr>
<tr>
<td>Japan</td>
<td>50</td>
<td>.03</td>
</tr>
<tr>
<td>Philippines</td>
<td>38</td>
<td>.02</td>
</tr>
<tr>
<td>South Korea</td>
<td>19</td>
<td>.01</td>
</tr>
<tr>
<td>Myanmar</td>
<td>17</td>
<td>.01</td>
</tr>
<tr>
<td>Mongolia</td>
<td>14</td>
<td>&lt;.01</td>
</tr>
<tr>
<td>Thailand</td>
<td>9</td>
<td>&lt;.01</td>
</tr>
<tr>
<td>Indonesia</td>
<td>7</td>
<td>&lt;.01</td>
</tr>
<tr>
<td>Others</td>
<td>438</td>
<td>.30</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>1,430</td>
<td>1.00</td>
</tr>
</tbody>
</table>
Do targeted groups upload exploit documents on VirusTotal? Likely targets (inferred from decoys)

<table>
<thead>
<tr>
<th>Group</th>
<th>Number</th>
<th>Fraction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uyghur</td>
<td>237</td>
<td>0.16</td>
</tr>
<tr>
<td>Vietnam</td>
<td>145</td>
<td>0.10</td>
</tr>
<tr>
<td>USA</td>
<td>118</td>
<td>0.08</td>
</tr>
<tr>
<td>Tibet</td>
<td>115</td>
<td>0.08</td>
</tr>
<tr>
<td>Taiwan</td>
<td>100</td>
<td>0.06</td>
</tr>
<tr>
<td>India</td>
<td>72</td>
<td>0.05</td>
</tr>
<tr>
<td>Russia</td>
<td>51</td>
<td>0.03</td>
</tr>
<tr>
<td>Japan</td>
<td>50</td>
<td>0.03</td>
</tr>
<tr>
<td>Philippines</td>
<td>38</td>
<td>0.02</td>
</tr>
<tr>
<td>South Korea</td>
<td>19</td>
<td>0.01</td>
</tr>
<tr>
<td>Myanmar</td>
<td>17</td>
<td>0.01</td>
</tr>
<tr>
<td>Mongolia</td>
<td>14</td>
<td>&lt;.01</td>
</tr>
<tr>
<td>Thailand</td>
<td>9</td>
<td>&lt;.01</td>
</tr>
<tr>
<td>Indonesia</td>
<td>7</td>
<td>&lt;.01</td>
</tr>
<tr>
<td>Others</td>
<td>438</td>
<td>0.30</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>1,430</td>
<td>1.00</td>
</tr>
</tbody>
</table>
Do targeted groups upload exploit documents on VirusTotal? Likely targets (inferred from decoys)

<table>
<thead>
<tr>
<th>Group</th>
<th>Number</th>
<th>Fraction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uyghur</td>
<td>237</td>
<td>.16</td>
</tr>
<tr>
<td>Vietnam</td>
<td>145</td>
<td>.10</td>
</tr>
<tr>
<td>USA</td>
<td>118</td>
<td>.08</td>
</tr>
<tr>
<td>Tibet</td>
<td>115</td>
<td>.08</td>
</tr>
<tr>
<td>Taiwan</td>
<td>100</td>
<td>.06</td>
</tr>
<tr>
<td>India</td>
<td>72</td>
<td>.05</td>
</tr>
<tr>
<td>Russia</td>
<td>51</td>
<td>.03</td>
</tr>
<tr>
<td>Japan</td>
<td>50</td>
<td>.03</td>
</tr>
<tr>
<td>Philippines</td>
<td>38</td>
<td>.02</td>
</tr>
<tr>
<td>South Korea</td>
<td>19</td>
<td>.01</td>
</tr>
<tr>
<td>Myanmar</td>
<td>17</td>
<td>.01</td>
</tr>
<tr>
<td>Mongolia</td>
<td>14</td>
<td>&lt;.01</td>
</tr>
<tr>
<td>Thailand</td>
<td>9</td>
<td>&lt;.01</td>
</tr>
<tr>
<td>Indonesia</td>
<td>7</td>
<td>&lt;.01</td>
</tr>
<tr>
<td>Others</td>
<td>438</td>
<td>.30</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>1,430</strong></td>
<td><strong>1.00</strong></td>
</tr>
</tbody>
</table>
Do targeted groups upload exploit documents on VirusTotal? Likely targets (inferred from decoys)

<table>
<thead>
<tr>
<th>Group</th>
<th>Number</th>
<th>Fraction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uyghur</td>
<td>237</td>
<td>.16</td>
</tr>
<tr>
<td>Vietnam</td>
<td>145</td>
<td>.10</td>
</tr>
<tr>
<td>USA</td>
<td>118</td>
<td>.08</td>
</tr>
<tr>
<td>Tibet</td>
<td>115</td>
<td>.08</td>
</tr>
<tr>
<td>Taiwan</td>
<td>100</td>
<td>.06</td>
</tr>
<tr>
<td>India</td>
<td>72</td>
<td>.05</td>
</tr>
<tr>
<td>Russia</td>
<td>51</td>
<td>.03</td>
</tr>
<tr>
<td>Japan</td>
<td>50</td>
<td>.03</td>
</tr>
<tr>
<td>Philippines</td>
<td>38</td>
<td>.02</td>
</tr>
<tr>
<td>South Korea</td>
<td>19</td>
<td>.01</td>
</tr>
<tr>
<td>Myanmar</td>
<td>17</td>
<td>.01</td>
</tr>
<tr>
<td>Mongolia</td>
<td>14</td>
<td>&lt;.01</td>
</tr>
<tr>
<td>Thailand</td>
<td>9</td>
<td>&lt;.01</td>
</tr>
<tr>
<td>Indonesia</td>
<td>7</td>
<td>&lt;.01</td>
</tr>
<tr>
<td>Others</td>
<td>438</td>
<td>.30</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>1,430</td>
<td>1.00</td>
</tr>
</tbody>
</table>

VirusTotal gives visibility into attacks targeting numerous groups
How attacks faced by different groups compare with each other? Languages of decoys
How attacks faced by different groups compare with each other? Languages of decoys
How attacks faced by different groups compare with each other? Languages of decoys
How attacks faced by different groups compare with each other? Languages of decoys
How attacks faced by different groups compare with each other? Languages of decoys

Decoys tend to use the official language of the groups they target
How attacks faced by different groups compare with each other? Malware targeting
How attacks faced by different groups compare with each other? Malware targeting
How attacks faced by different groups compare with each other? Malware targeting
How attacks faced by different groups compare with each other? Malware targeting
How attacks faced by different groups compare with each other? Malware targeting

From our dataset, malware families tend to target one or two countries.
Targeted regions

• Chinese influence: Tibet, Uyghur, Taiwan

• Asia Pacific: Myanmar, the Philippines, Thailand, and Vietnam

• Asia Pacific, G20: India, Indonesia, Japan, and South Korea

• Russia and USA
How do attacks faced by different groups compare with each other? Malware targeting (cont.)
How do attacks faced by different groups compare with each other? Malware targeting (cont.)
How do attacks faced by different groups compare with each other? Malware targeting (cont.)
How do attacks faced by different groups compare with each other? Malware targeting (cont.)
How do attacks faced by different groups compare with each other? Malware targeting (cont.)

Malware found in multiple countries tend to target a confined region.
Outline

1) Methodology
2) Analysis of exploit documents
3) Future work
Future work

• Monitoring operator behavior of targeted malware

• Analysis of evasions techniques, attackers operations, and other attack vectors

• Deploy on-premises and cloud-based services for analysis of email attachments
Take home messages

• Complementary methodology to measure targeted attacks at scale

• At-risk groups upload exploit documents to VirusTotal

• Groups tend to be targeted with tailored decoys and malware families

• Preliminary impact
  • Service deployed at email provider with 100,000+ users
  • Dataset and academic service available at https://slingshot.dedis.ch
Frequently Asked Questions

• What are the observational biases of using VirusTotal?

• What are the common types of malicious documents that you filtered out?

• Why did you focus on exploit documents?

• What precautions did you take to reduce false negatives?

• Did you find indications of successful compromises?
What are the observational biases of using VirusTotal?

• Coverage of targeted attacks is limited to those users and organizations who upload suspicious files

• VirusTotal’s visibility is likely skewed towards users who work with non-classified material

• VirusTotal dataset offers a partial coverage of attacks where individuals and NGOs are likely over-represented
What are the most common malicious documents that you filtered out?

<table>
<thead>
<tr>
<th>Steps</th>
<th>Filtered categories</th>
<th># documents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detection</td>
<td>Office macros</td>
<td>-129,532</td>
</tr>
<tr>
<td></td>
<td>Cannot open</td>
<td>-17,177</td>
</tr>
<tr>
<td></td>
<td>Crashes</td>
<td>-3,370</td>
</tr>
<tr>
<td></td>
<td>Passwords</td>
<td>-1,001</td>
</tr>
<tr>
<td></td>
<td>False positives</td>
<td>-45,342</td>
</tr>
<tr>
<td></td>
<td>Neutralized</td>
<td>-5,574</td>
</tr>
<tr>
<td></td>
<td>Others</td>
<td>-17,798</td>
</tr>
<tr>
<td>Extraction</td>
<td>Downloads</td>
<td>-32,387</td>
</tr>
<tr>
<td></td>
<td>No executable or decoy</td>
<td>-1,639</td>
</tr>
<tr>
<td>Analysis</td>
<td></td>
<td>3,815</td>
</tr>
</tbody>
</table>
Why did you focus on exploit documents?

- Exploit documents are the most common vector of targeted attacks identified by related work.

- Macros require additional user approval and can be forcibly disabled by system administrators.

- Used against a range of targets including NGOs, news agencies, and military, governmental and intelligence agencies.
What precautions did you take to reduce false negatives?

- Reducing detection FNs
  - Cross validated EMET detection results with ground truth from the WUC dataset
  - 29/143 WUC documents were not detected by EMET, none of them FNs (16 Mac OS X, 9 wrong reader version, 2 password, and 2 without exploit)

- Reducing extraction FNs
  - Manually inspected EMET detections that didn’t write files to disk
  - 29/4,259 documents detected by EMET did not write any files to disk, none of them FNs (6 crashes, 4 experimental, and 19 dysfunctional)

- None of our analyses depends on the lack of evasion techniques in the malware embedded in exploit documents
Did you find indication of successful compromises?

• Coded decoys based on their languages, the countries they refer to, ethnic groups and dates, and whether they targeted specific individuals or organizations

• Native speakers independently coded the documents written in Russian, Traditional Chinese, Uyghur, and Vietnamese

• Identified documents likely exfiltrated from compromised systems and used as decoys in exploit documents targeting new, related victims
Did you find indication of successful compromises (cont.)?
Did you find indication of successful compromises (cont.)?

Most groups were targeted with replayed decoys.
Did you find evidence of zero-day vulnerabilities?

• We collaborated with a large AV vendor to determine the CVE tags of the exploited reader vulnerabilities

• The vendor scanned all the exploit documents that we detected and compared the resulting CVE with the majority of VirusTotal tags
  • If the two CVEs matched, no further action was taken
  • Otherwise, the sample was analyzed manually

• Samples for which the CVE release date was after the date of upload on VirusTotal were examined manually to determine the CVE’s correctness

• Based on this methodology, we didn’t find evidence of zero-day vulnerabilities
Can you estimate the dates of the decoys?

• We coded decoys according to their languages, the countries they refer to, ethnic groups and dates, and whether they targeted specific individuals or organizations.

• Native speakers independently coded the documents written in Russian, Traditional Chinese, Uyghur, and Vietnamese.
Can you estimate the dates of the decoys (cont.)?
Can you estimate the dates of the decoys (cont.)?

All groups exhibited decoys referring to at least one year in 2013-2015