TARGETED CAMPAIGN ANALYSIS AND TRACKING

ARE YOU AT THE TIP OF THE SPEAR OR THE BACK OF THE BUS?

Christopher Witter, Sr. Strategic Intrusion Analyst
About Me:

• Sr. Strategic Intrusion Analyst @ CrowdStrike
• IR Experience
  – Defense
  – Banking
  – Service Providers
• Lifetime InfoSec professional
• Outdoor Enthusiast
Introduction

- Types of Phishing
- Message Analysis
- Web Link Analysis
- Attachment Analysis
- Campaign Tracking Analysis
The Trifecta of Campaign Analysis...

- Message Analysis
- Web link Analysis
- Attachment Analysis
Message Analysis: Email Header Analysis

- Subject
- Sender
- Date\Time:
- Recipient
- Sending IP
- Attachment Name
Message Analysis: More Email Header...

• X-mailer
• Return-path
• In-reply-to
• User-agent
• References
• Sender display name
Message Analysis: Email Example

x-rocket-received: from [10.0.0.16] (JimBob@123.456.789.123 with xymcookie [66.196.81.168]) by smtp228.mail.gq1.yahoo.com with SMTP; 06 Apr 2014 13:41:19 +0000 UTC

references: <1725641872-1378324123-cardhu_decombobulator_blackberry.rim.net-772162753-@b28.c7.bise6.blackberry>

mime-version: 1.0 (1.0)
in-reply-to: <1725641872-1378324123-cardhu_decombobulator_blackberry.rim.net-772162753-@b28.c7.bise6.blackberry>

content-type: text/plain; charset=us-ascii
content-transfer-encoding: quoted-printable
message-id: <FA750D23-4D3F-496F-9D72-A350CEC975B5@yahoo.com>
x-mailer: iPhone Mail (11B511)
Message Analysis: Email Example

x-rocket-received: from [10.0.0.16] (JimBob@123.456.789.123 with xymcookie [66.196.81.168]) by smtp228.mail.gq1.yahoo.com with SMTP; 06 Apr 2014 13:41:19 +0000 UTC

references: <1725641872-1378324123-cardhu_decombobulator_blackberry.rim.net-772162753-@b28.c7.bise6.blackberry>

mime-version: 1.0 (1.0)

in-reply-to: <1725641872-1378324123-cardhu_decombobulator_blackberry.rim.net-772162753-@b28.c7.bise6.blackberry>

content-type: text/plain; charset=us-ascii

content-transfer-encoding: quoted-printable

message-id: <FA750D23-4D3F-496F-9D72-A350CEC975B5@yahoo.com>

x-mailer: iPhone Mail (11B511)
Message Analysis: Email Body Analysis

- Social Cues
- Social Media Analysis
- User Interview
- Links
- Attachments
• Drag and Drop Suspicious Emails into a folder/USB
• Strings:
  – strings xyzfilename.msg (ASCII Files)
  – strings –el xyzfilename.msg (UniCode Files)
• Extracting attachment from msg files
  – uudeview –i –p xyzfilename.msg
• Automatic:
  – Virustotal.com
  – Urlquery.net
  – Custom Sandbox (Cuckoo, Norman, JoeBox, etc…)

• Manual
  – Wget & curl
  – Thug
Wicked Web: Automatic Analysis tradeoffs...

- OPSEC
- Staffing
- Budget
- Convenience
Wicked Web: Manual Analysis tradeoffs...

- Infrastructure
- Processes \ Procedure
- Staffing
• Mirror your environment closely
  – Use the proxy if you have one (X-forwarded-for)
  – set the proper Referer
  – Use an appropriate User agent (custom to match your workstations)

• Thug
  – Mimic software configurations as closely as possible
  – Use delays (people think)
  – Use events (people move)
Attachment Analysis:

- AV \ YARA
- Malwr.com \ Virustotal.com
- Custom Sandbox (Cuckoo, Norman, JoeBox, etc…)
- In house reverse engineer\malware analyst
- ExifTool
Attachment Analysis: Metadata Analysis

• **ExifTool:**
  – Supports a ton of file formats (PE, Word, PPT, Excel, PDF…)
  – Extracts more than just GPS coords 😊
    • Total Edit Time
    • Words
    • Paragraphs
    • Slides
Attachment Analysis: Metadata Example PPTX

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Edit Time</td>
<td>17.8 days</td>
</tr>
<tr>
<td>Words</td>
<td>2608</td>
</tr>
<tr>
<td>Application</td>
<td>Microsoft Macintosh PowerPoint</td>
</tr>
<tr>
<td>Presentation Format</td>
<td>Custom</td>
</tr>
<tr>
<td>Paragraphs</td>
<td>790</td>
</tr>
<tr>
<td>Slides</td>
<td>60</td>
</tr>
<tr>
<td>Notes</td>
<td>21</td>
</tr>
<tr>
<td>Hidden Slides</td>
<td>6</td>
</tr>
<tr>
<td>MM Clips</td>
<td>0</td>
</tr>
<tr>
<td>Scale Crop</td>
<td>No</td>
</tr>
<tr>
<td>Heading Pairs</td>
<td>Theme, 1, Slide Titles, 60</td>
</tr>
<tr>
<td>Titles Of Parts</td>
<td>Office Theme, PowerPoint Presentation, About Me, PowerPoint Presentation, Today's Headlines, PowerPoint Presentation, PowerPoint Presentation, The Adversary has Evolved</td>
</tr>
</tbody>
</table>
Attachment Analysis: Metadata Example PDF
# Attachment Analysis: Good or Evil

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creator</td>
<td>user</td>
</tr>
<tr>
<td>Last Modified By</td>
<td>ASUS</td>
</tr>
<tr>
<td>Revision Number</td>
<td>2</td>
</tr>
<tr>
<td>Create Date</td>
<td>2013:08:25 20:02:00Z</td>
</tr>
<tr>
<td>Modify Date</td>
<td>2013:08:25 20:02:00Z</td>
</tr>
<tr>
<td>Template</td>
<td>Normal</td>
</tr>
<tr>
<td>Total Edit Time</td>
<td>2 minutes</td>
</tr>
<tr>
<td>Pages</td>
<td>1</td>
</tr>
<tr>
<td>Words</td>
<td>2</td>
</tr>
<tr>
<td>Characters</td>
<td>18</td>
</tr>
<tr>
<td>Application</td>
<td>Microsoft Office Word</td>
</tr>
<tr>
<td>Doc Security</td>
<td>None</td>
</tr>
<tr>
<td>Lines</td>
<td>1</td>
</tr>
<tr>
<td>Paragraphs</td>
<td>1</td>
</tr>
<tr>
<td>Scale Crop</td>
<td>No</td>
</tr>
<tr>
<td>Company</td>
<td></td>
</tr>
<tr>
<td>Links Up To Date</td>
<td>No</td>
</tr>
<tr>
<td>Characters With Spaces</td>
<td>19</td>
</tr>
<tr>
<td>Shared Doc</td>
<td>No</td>
</tr>
<tr>
<td>Hyperlinks Changed</td>
<td>No</td>
</tr>
<tr>
<td>App Version</td>
<td>12.0000</td>
</tr>
<tr>
<td>File Type</td>
<td>PDF</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------</td>
</tr>
<tr>
<td>MIME Type</td>
<td>application/pdf</td>
</tr>
<tr>
<td>PDF Version</td>
<td>1.5</td>
</tr>
<tr>
<td>Linearized</td>
<td>No</td>
</tr>
<tr>
<td>Page Count</td>
<td>2</td>
</tr>
<tr>
<td>Language</td>
<td>zh-CN</td>
</tr>
<tr>
<td>Tagged PDF</td>
<td>Yes</td>
</tr>
<tr>
<td>Author</td>
<td>user</td>
</tr>
<tr>
<td>Creator</td>
<td>Microsoft® Word 2010</td>
</tr>
<tr>
<td>Create Date</td>
<td>2013-06-18 15:12:56+08:00</td>
</tr>
<tr>
<td>Modify Date</td>
<td>2013-06-18 15:12:56+08:00</td>
</tr>
<tr>
<td>Producer</td>
<td>Microsoft® Word 2010</td>
</tr>
</tbody>
</table>
Attachment Analysis: Good or Evil

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comments</td>
<td>kLyKroiV</td>
</tr>
<tr>
<td>Company Name</td>
<td>PHgfEJYN</td>
</tr>
<tr>
<td>File Description</td>
<td>dayJWvvG</td>
</tr>
<tr>
<td>File Version</td>
<td>1.0.0.0</td>
</tr>
<tr>
<td>Internal Name</td>
<td>autoit.exe</td>
</tr>
<tr>
<td>Legal Copyright</td>
<td>nSEiIlgj</td>
</tr>
<tr>
<td>Legal Trademarks</td>
<td>gkvWzsvVM</td>
</tr>
<tr>
<td>Original Filename</td>
<td>autoit.exe</td>
</tr>
<tr>
<td>Product Name</td>
<td>IXWQvPor</td>
</tr>
<tr>
<td>Product Version</td>
<td>1.0.0.0</td>
</tr>
</tbody>
</table>
Campaign Tracking

• Why track
• What to track
• How to track
Campaign Tracking: Why track?

- PO59782.rar
- Product attention needs.rar
- payment slip.zip
- pdf.ex_
- po_1320.rar
- quote.rar
- Marketing Copy.pdf
- funds release.zip
- product sample and invoice.rar
- Orders.scr
Campaign Tracking: Why track?
• Simple characteristics
  – Hashes
  – Filename
  – VT Detections
  – C2 Domains \ IPs
  – X-Mailer
  – Carrier File type
  – Sender \ Recipient
  – Theme
  – Associated Threat
• Advanced characteristics
  – Exploits used
  – Droppers
  – RAT
  – Interesting Strings
  – Interesting Routines
  – Persistence mechanisms
  – Domain registry information
Campaign Analysis:

• How did it happen
• Goal of the Campaign
• Detection \ Prevention
Campaign Analysis: How did it happen...

- User interview
- Social Media Analysis
- Log Analysis
Campaign Analysis: Goal of the Campaign...

• Trends
• Method of Targeting
• Context of the message
This Page Left Intentional Blank
CONTACT ME

EMAIL: Christopher.Witter@crowdstrike.com

TWITTER: mr_cwitter
Thank You!

For additional information, please visit: response.crowdstrike.com/services