CROWDSTRIKE

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

SPAM
Luncheon Meat
Hormel Foods

Image: http://www.freepasswordmanager.com/wp-content/uploads/2013/10/phishing-attack.png

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

Message Analysis: Email Analysis Tricks

- 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

Wicked Web: Web Link Analysis

- 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…

- Infrastucture
- Processes \ Procedure
- Staffing

Wicked Web: Manual Analysis Tips…

- 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)

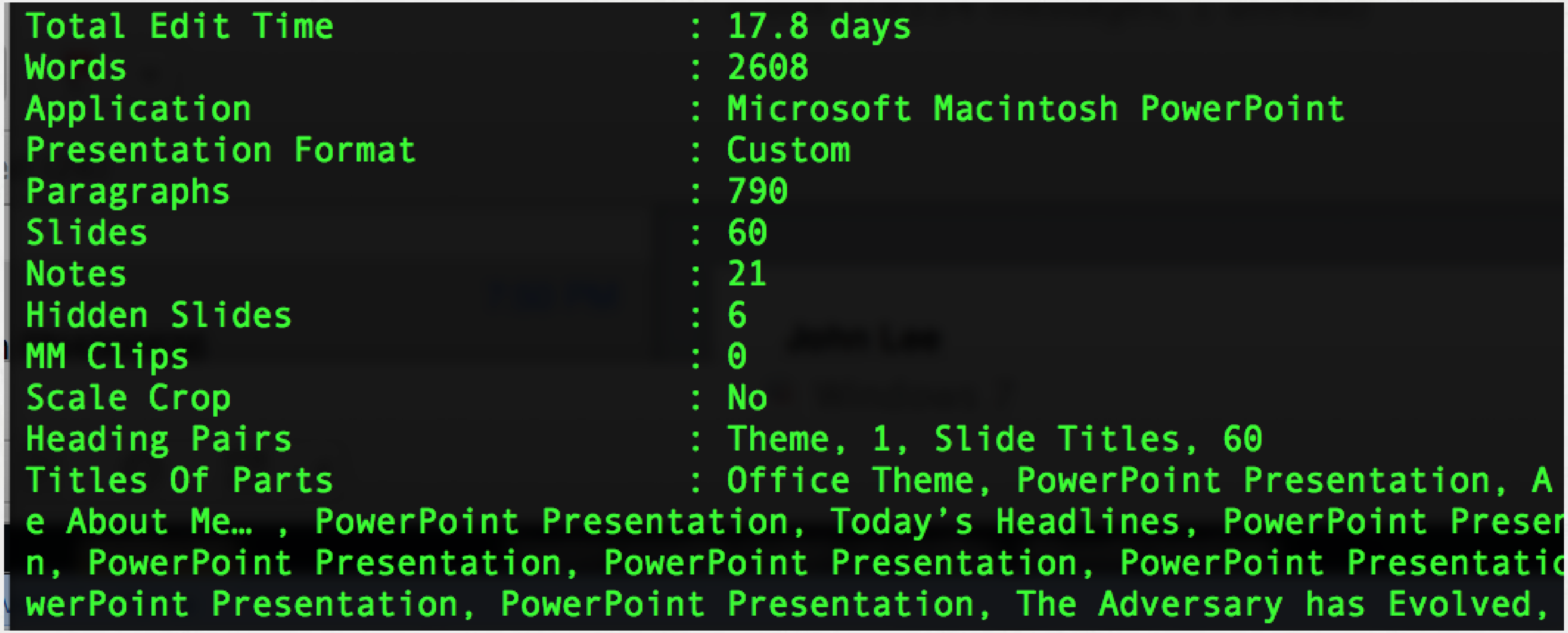
Attachment Analysis:

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

Attachment Analysis: Metadata Analysis

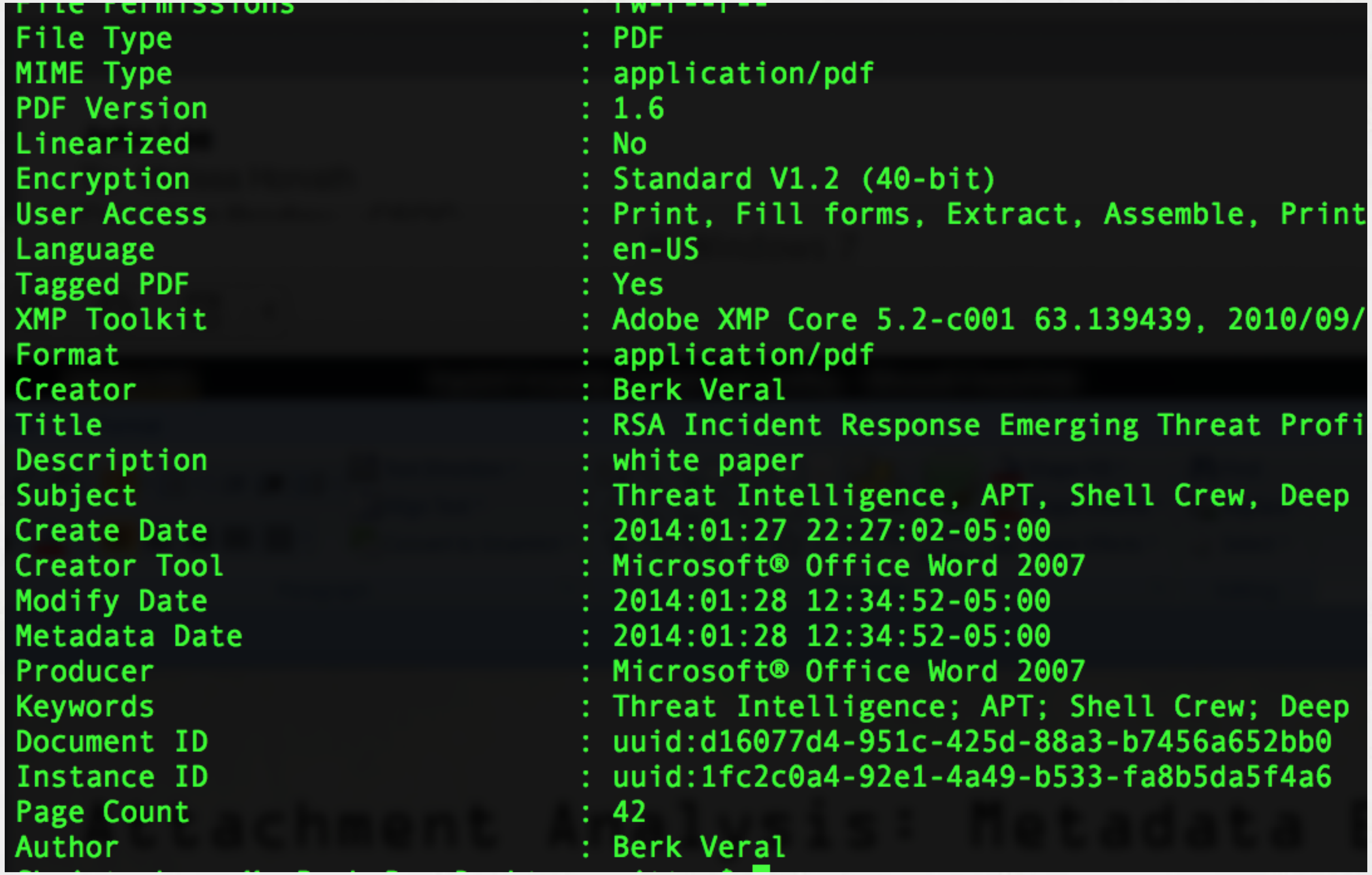
- ExifTool:
  - Supports a ton of file formats (PE, Word, PPT, Excel, PDF…)
  - Extracts more than just GPS coords ☺
    - Total Edit Time
    - Words
    - Paragraphs
    - Slides

Attachment Analysis: Metadata Example PPTX



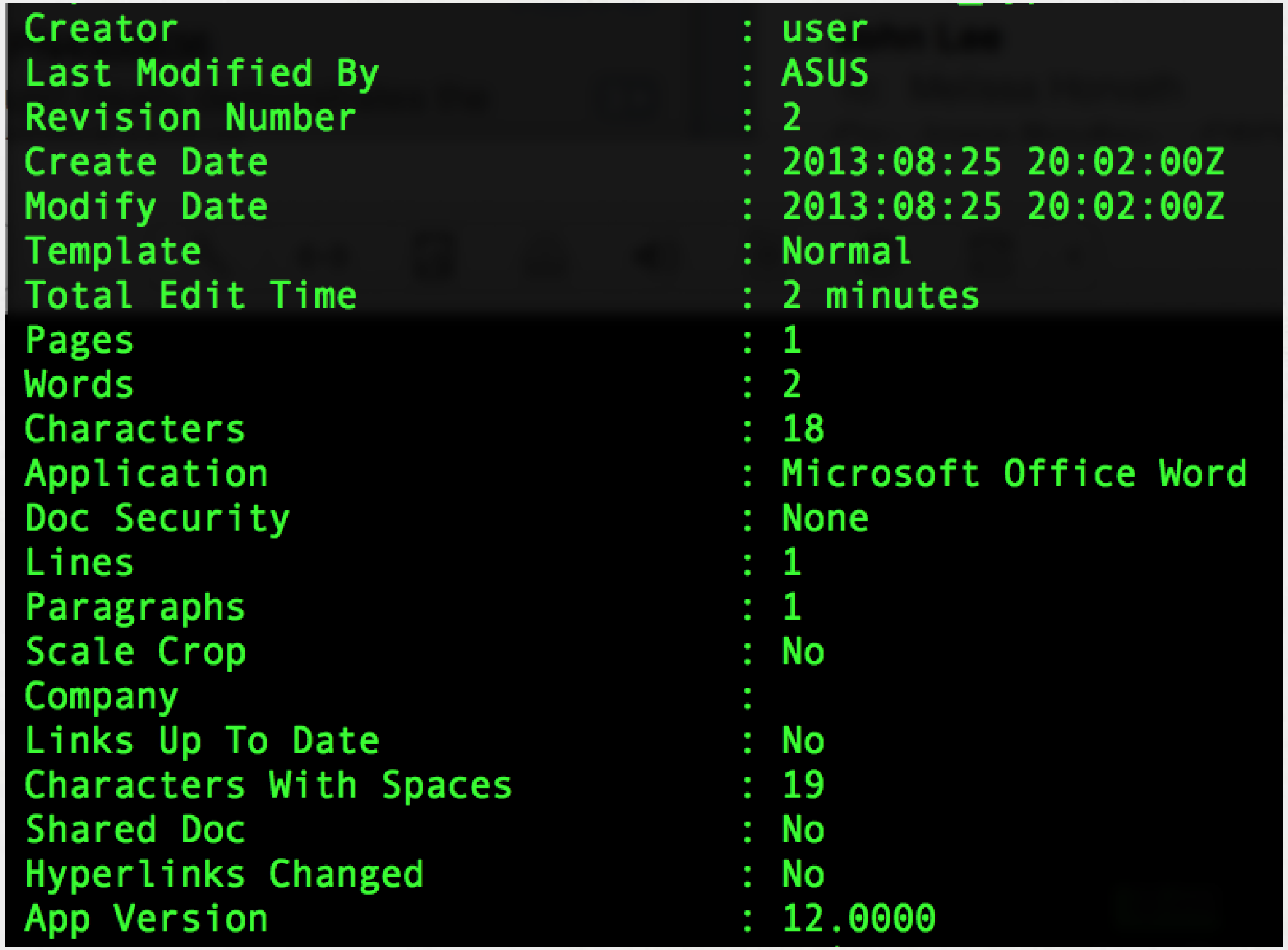
```
Total Edit Time                 : 17.8 days
Words                           : 2608
Application                     : Microsoft Macintosh PowerPoint
Presentation Format             : Custom
Paragraphs                      : 790
Slides                          : 60
Notes                           : 21
Hidden Slides                   : 6
MM Clips                        : 0
Scale Crop                      : No
Heading Pairs                   : Theme, 1, Slide Titles, 60
Titles Of Parts                 : Office Theme, PowerPoint Presentation, A
e About Me… , PowerPoint Presentation, Today’s Headlines, PowerPoint Preser
n, PowerPoint Presentation, PowerPoint Presentation, PowerPoint Presentatic
werPoint Presentation, PowerPoint Presentation, The Adversary has Evolved,
```

Attachment Analysis: Metadata Example PDF



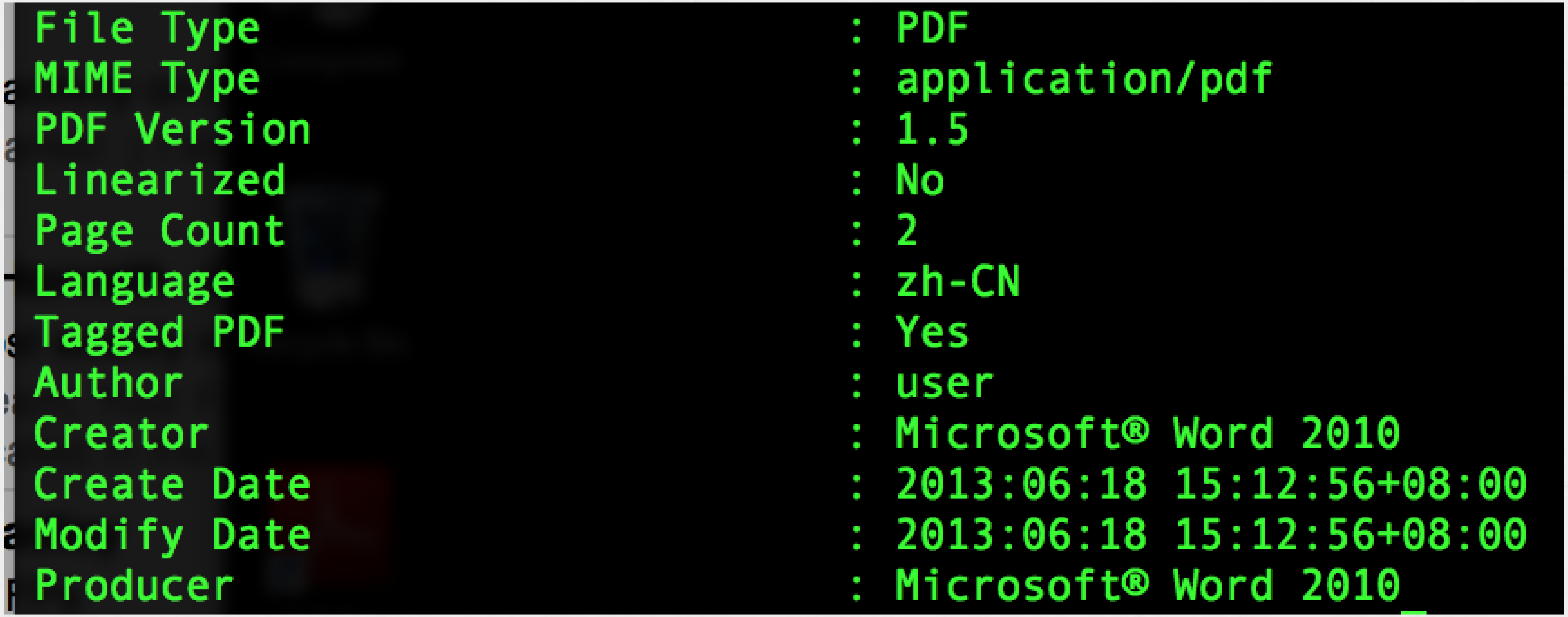
```
File Permissions                : rw-r--r--
File Type                       : PDF
MIME Type                       : application/pdf
PDF Version                     : 1.6
Linearized                      : No
Encryption                      : Standard V1.2 (40-bit)
User Access                     : Print, Fill forms, Extract, Assemble, Print
Language                        : en-US
Tagged PDF                      : Yes
XMP Toolkit                     : Adobe XMP Core 5.2-c001 63.139439, 2010/09/
Format                          : application/pdf
Creator                         : Berk Veral
Title                           : RSA Incident Response Emerging Threat Profi
Description                     : white paper
Subject                         : Threat Intelligence, APT, Shell Crew, Deep
Create Date                     : 2014:01:27 22:27:02-05:00
Creator Tool                    : Microsoft® Office Word 2007
Modify Date                     : 2014:01:28 12:34:52-05:00
Metadata Date                   : 2014:01:28 12:34:52-05:00
Producer                        : Microsoft® Office Word 2007
Keywords                        : Threat Intelligence; APT; Shell Crew; Deep
Document ID                     : uuid:d16077d4-951c-425d-88a3-b7456a652bb0
Instance ID                     : uuid:1fc2c0a4-92e1-4a49-b533-fa8b5da5f4a6
Page Count                      : 42
Author                          : Berk Veral
```

Attachment Analysis: Good or Evil



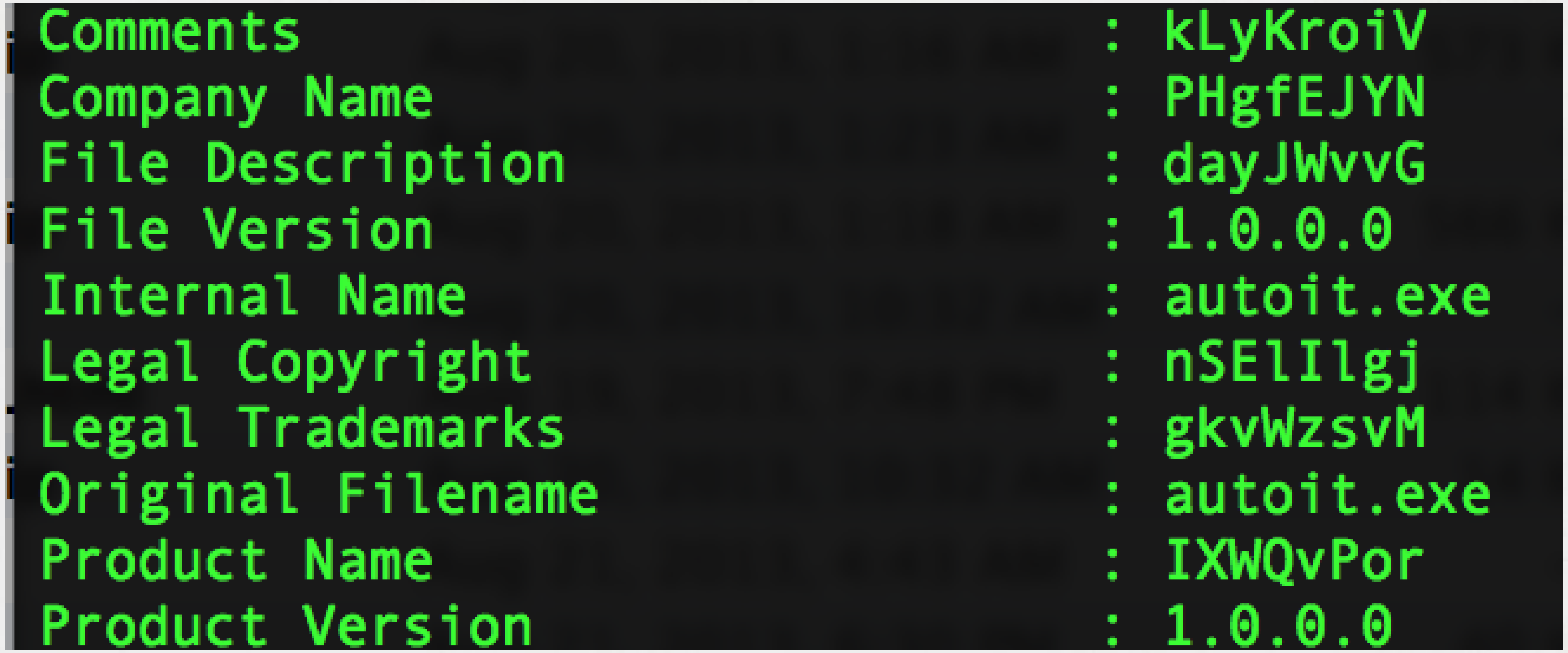
```
Creator                         : user
Last Modified By                : ASUS
Revision Number                 : 2
Create Date                     : 2013:08:25 20:02:00Z
Modify Date                     : 2013:08:25 20:02:00Z
Template                        : Normal
Total Edit Time                 : 2 minutes
Pages                           : 1
Words                           : 2
Characters                      : 18
Application                     : Microsoft Office Word
Doc Security                    : None
Lines                           : 1
Paragraphs                      : 1
Scale Crop                      : No
Company                         :
Links Up To Date                : No
Characters With Spaces          : 19
Shared Doc                      : No
Hyperlinks Changed              : No
App Version                     : 12.0000
```

Attachment Analysis: Good or Evil



```
File Type                       : PDF
MIME Type                       : application/pdf
PDF Version                     : 1.5
Linearized                      : No
Page Count                      : 2
Language                        : zh-CN
Tagged PDF                      : Yes
Author                          : user
Creator                         : Microsoft® Word 2010
Create Date                     : 2013:06:18 15:12:56+08:00
Modify Date                     : 2013:06:18 15:12:56+08:00
Producer                        : Microsoft® Word 2010
```

Attachment Analysis: Good or Evil

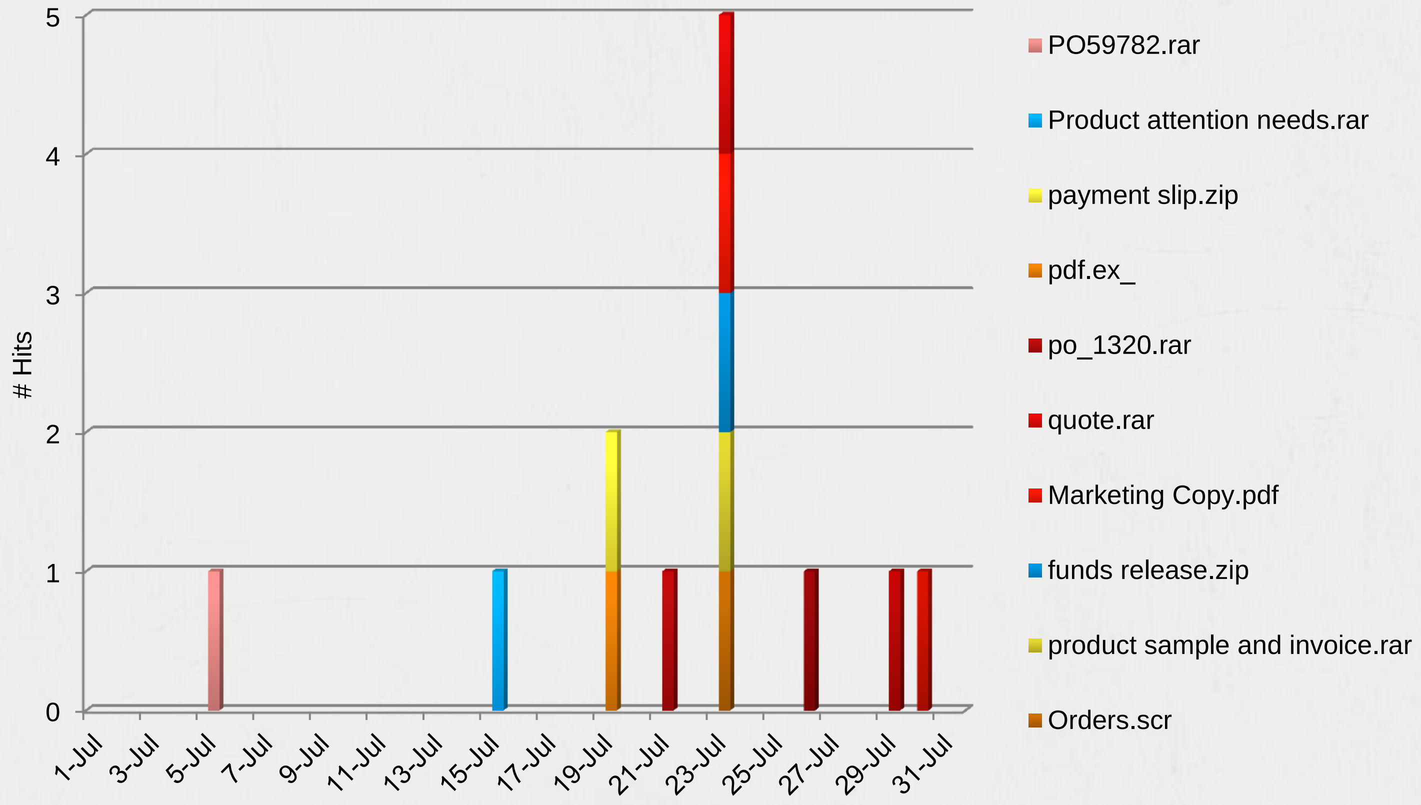


```
Comments                              : kLyKroiV
Company Name                          : PHgfEJYN
File Description                      : dayJWvvG
File Version                          : 1.0.0.0
Internal Name                         : autoit.exe
Legal Copyright                       : nSElIlgj
Legal Trademarks                      : gkvWzsvM
Original Filename                     : autoit.exe
Product Name                          : IXWQvPor
Product Version                       : 1.0.0.0
```

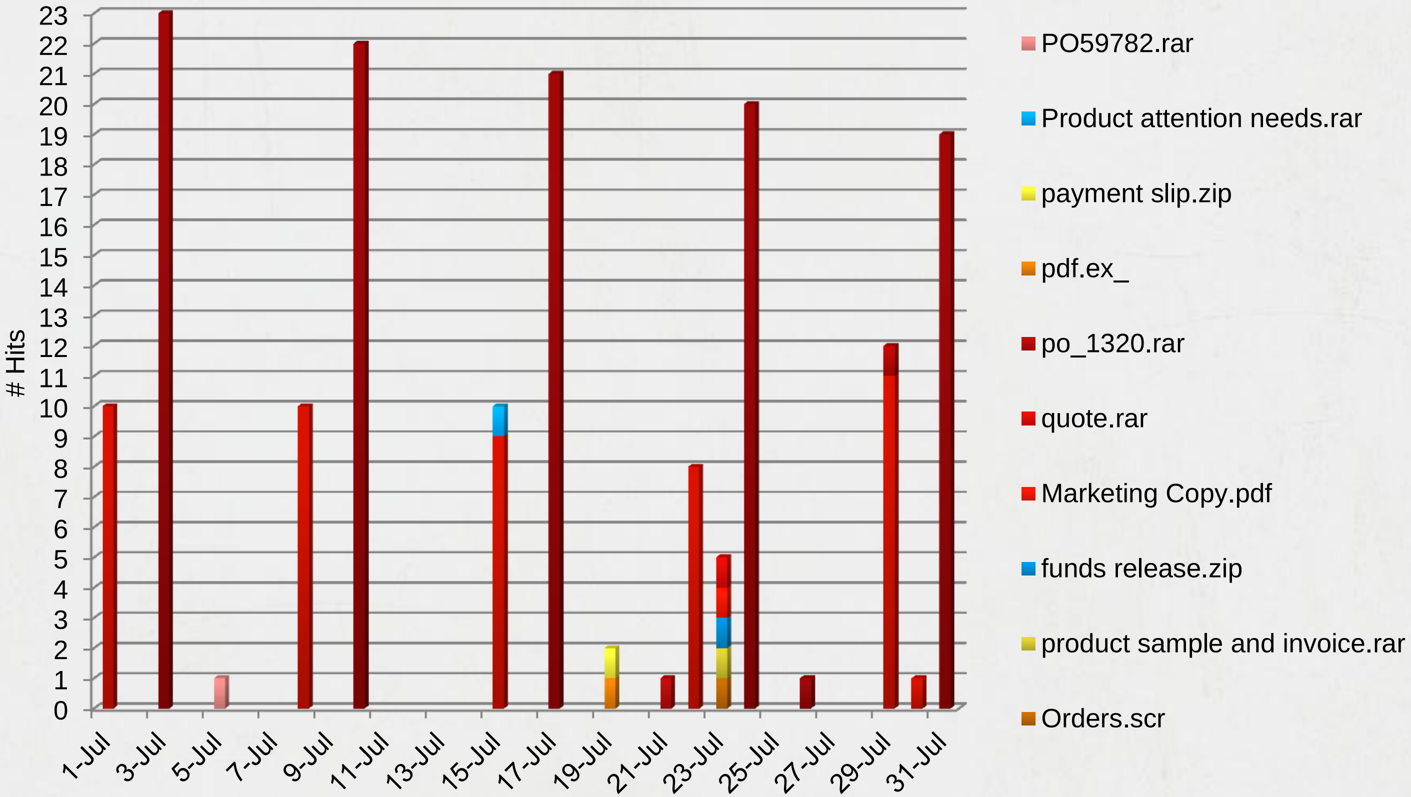
Campaign Tracking

- Why track
- What to track
- How to track

Campaign Tracking: Why track?



Campaign Tracking: Why track?



Campaign Tracking: What to Track v1.0:

- Simple characteristics
  - Hashes
  - Filename
  - VT Detections
  - C2 Domains \ IPs
  - X-Mailer
  - Carrier File type
  - Sender \ Recipient
  - Theme
  - Associated Threat

What to Track: What to Track v2.0:

- 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

Campaign Analysis: Detection \ Prevention

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**

CROWDSTRIKE