Document Malware

PDF Malware

Origins of Portable Document File (PDF)

- Adobe Systems, 1993
  - Initially proprietary standard
  - Released as open standard (ISO 32000-1:2008) in 2008
- Derived from PostScript language
- Representation of document file (text, fonts, vector graphics, raster images) that is independent of applications and operating systems

Engineers deliver "Computer Paper", v1.0

Marketing Department takes over…

Can I embed Flash animations?
(We should enhance *synergy* between our products)

Our customers should be able to fill out a form in a PDF and hit a submit button to send it somewhere

The documents should be able to run scripts when launched to prepare or validate the forms. JavaScript?

Wouldn't it be great if I can click a button in the PDF and Internet Explorer launched? (Why not make it *any* program?)

Exploiting PDFs

- Extremely common to open PDF files during normal business operations
  - Some workers might even need to open *unsolicited* PDFs! (e.g. accounts payable department)
- The complexity of PDF viewers and the ubiquity of the files provides great potential for malware authors to use as a delivery method
  - Not necessarily the *entire* malware, but enough for the first stage of an infection
  - Dropper – Save *internal* malware file to disk
  - Downloader – Download *external* malware file to disk

Distribution

- Mass emails (spam) to myriad recipients with attachment
- Targeted emails to specific recipients
  - Provides great opportunities to tailor email & attachment to appear legitimate
- Drive-by downloads (web browsers can download & render PDFs)

Exploiting PDFs – Methods of Attack

1. **Abuse a feature** of the PDF viewer to do something *evil* automatically when viewed
   - Run JavaScript
   - Run ActionScript in Flash
   - Run an external program
   - *PDF viewers have closed off the most obvious lines of attack with more secure default settings*
2. **Exploit a code vulnerability** within PDF viewer to run arbitrary code when PDF file is rendered
   - Example: Malformed TIFF vulnerability
   - *Always more bugs to discover! Aided by software complexity*
3. **Trick the user** into enabling feature of PDF viewer that can be abused
   - "To view bank information click ENABLE to continue"

Exploiting PDFs – Evasion Techniques

- Pad PDF files with bogus data to evade antivirus scanners
- Crash PDF viewer (after launching malware behind the scenes)
- Obfuscation obfuscation obfuscation
  - Encode data / Compress data
  - Spaghetti code / logic
  - Split code across multiple separate objects (combined when file is processed)

PDF Structure

Header	Version of PDF, e.g. `%pdf-1.x`

Body	Object
	Object
	Object, e.g.
	`objectNum verNum obj`
	`<< Contents>>`
	`endobj`

Xref	Cross Reference Table List all objects and file offset in bytes
Trailer	End of file. Specifies offset of Xref table, number of objects, and first object

PDF Structure

Object Number

Version Number

```
1 0 obj
Type: /Page
<<
  /AA /O 43 0 R
>>
endobj
```

Beginning

Automatic Action

When Opened

Object 43 0

End

PDF Structure

```
83 0 obj
<<
    /Filter
      [/FlateDecode]
    /Length 925
>>
stream
    Contents
endstream
endobj
```

Decoding method for bytes
(zlib/deflate)

Sequence of Bytes
(Could be fonts, pictures, text)

PDF Keywords

Tag	Purpose
`/JS`	JavaScript
`/JavaScript`	
`/XFA`	XML Forms Architecture
`/RichMedia`	Flash
`/Launch`	Launch external program
`/EmbeddedFiles`	Embedded Files
`/AA`	Automatic Action
`/OpenAction`	Run when document viewed

Resources

- https://www.dst.defence.gov.au/sites/default/files/publications/documents/DSTO-TR-2730.pdf
  - Threat Modelling Adobe PDF (2012)
- https://studylib.net/doc/18609162/the-rise-of-pdf-malware
  - The Rise of PDF Malware (2010) – Symantec
- https://www.sans.org/reading-room/whitepapers/malicious/owned-malicious-pdf-analysis-33443
  - Getting Owned By Malicious PDF – Analysis (2010)
- *Note that PDF threats peaked in early 2010's, although they are still used as a deployment method today*

Microsoft Office Malware

Exploiting ~~PDFs~~ MS Office Documents

Notice a similarity here?

- Extremely common to open ~~PDF~~ Office files during normal business operations
  - Some workers might even need to open *unsolicited* ~~PDFs~~ Office docs! (e.g. accounts payable department)
- The complexity of ~~PDF viewers~~ MS Office and the ubiquity of the files provides great potential for malware authors to use as a delivery method
  - Not necessarily the *entire* malware, but enough for the first stage of an infection (dropper, downloader)

Visual Basic for Applications (VBA)

- Macros in Microsoft Office support many features that are attractive to malware authors
  - Download files
  - Create files
  - Execute programs
  - Run automatically when document is opened (if permitted)
- Like PDFs, Office documents can be used as a downloader or dropper for subsequent malware stages

MS Office File Types

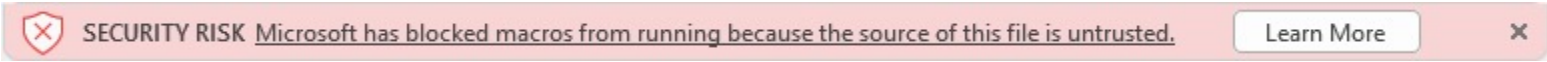
- Object Linking and Embedding (OLE2)
  - Legacy format
  - Essentially a binary dump of application memory to disk
    - Fast to load but indecipherable
  - File extensions: `.doc`, `.xls`, `.ppt`, …
- XML
  - Modern format (Office 2007+)
  - File is a ZIP archive of many component parts
  - File extensions:
    - `.docx`, `.xlsx`, `.pptx` – Macros *ignored*
    - `.docm`, `.xlsm`, `.pptm` – Macros (potentially) enabled

Tools and Techniques

- Native tools – Put a copy of MS Office i*nside your sandbox*
  - Behavioral analysis – Detonate malware and watch what happens
  - Use Office VBA debugger to inspect macro (either statically or at runtime)
    - Very useful to watch it de-obfuscate script at runtime
- Just unzip the document and look around
  - Might find images
  - Might find VBA files you could decode or search for strings
- Utilities in REMnux
  - **oledump.py** – Explore contents & structure
  - **olevba.py** – Extract VBA macros, provides summary table of threats
  - olebrowse.py
  - olecfinfo.py
  - oledir.py
  - *Don't be alarmed about the OLE names – these support newer XML documents too*

Update – February 2022

- Breaking news from Microsoft!
- New default setting for Microsoft Office apps that run macros…
  - **VBA macros obtained from the internet will now be blocked by default**
  - **There is no "run it anyway" button for users to click**



- Finally!!!!! *Only took how many years?*

https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/ba-p/3071805

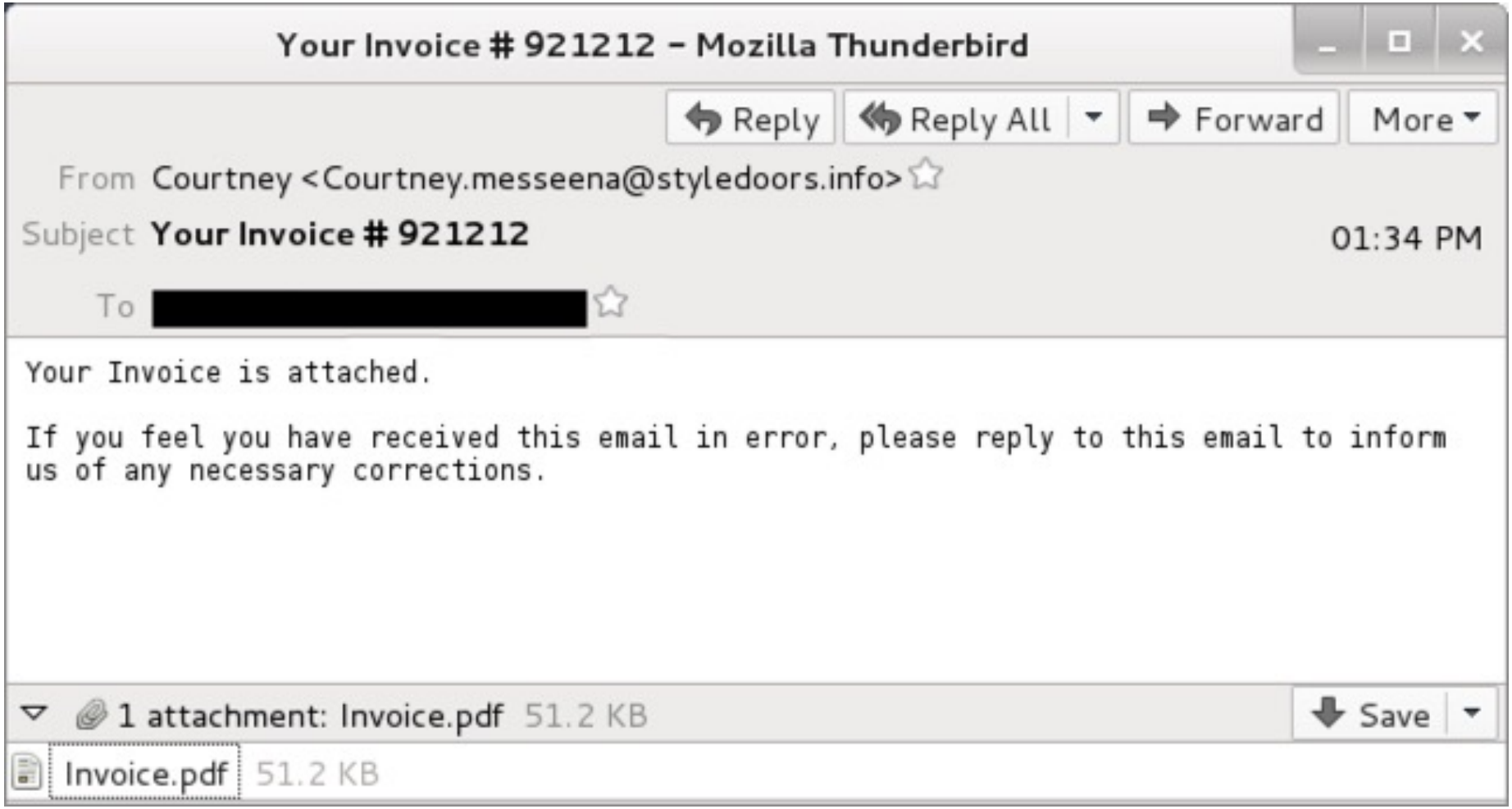
Malware

Jaff Ransomware

- **Just to be clear:**
  <u>Jaff</u> ransomware, not Jeff ransomware
- Release: May 2017
- Searches all drives and network shares for long list of valid file types
- Encrypts first 512kB of each file using 256-bit AES encryption
- Appends .jaff extension to end of file name
- Demands bitcoin

Distribution

- Step 1: Spam emails with PDF attachment containing embedded JavaScript
- Example subject:
  Invoice(00-5523) -- Attachment name: 68-5182.pdf
- Example sender:
  FREDRIC RALLI <FREDRIC.RALLI@RVAGROCERYSHOPPER.COM>

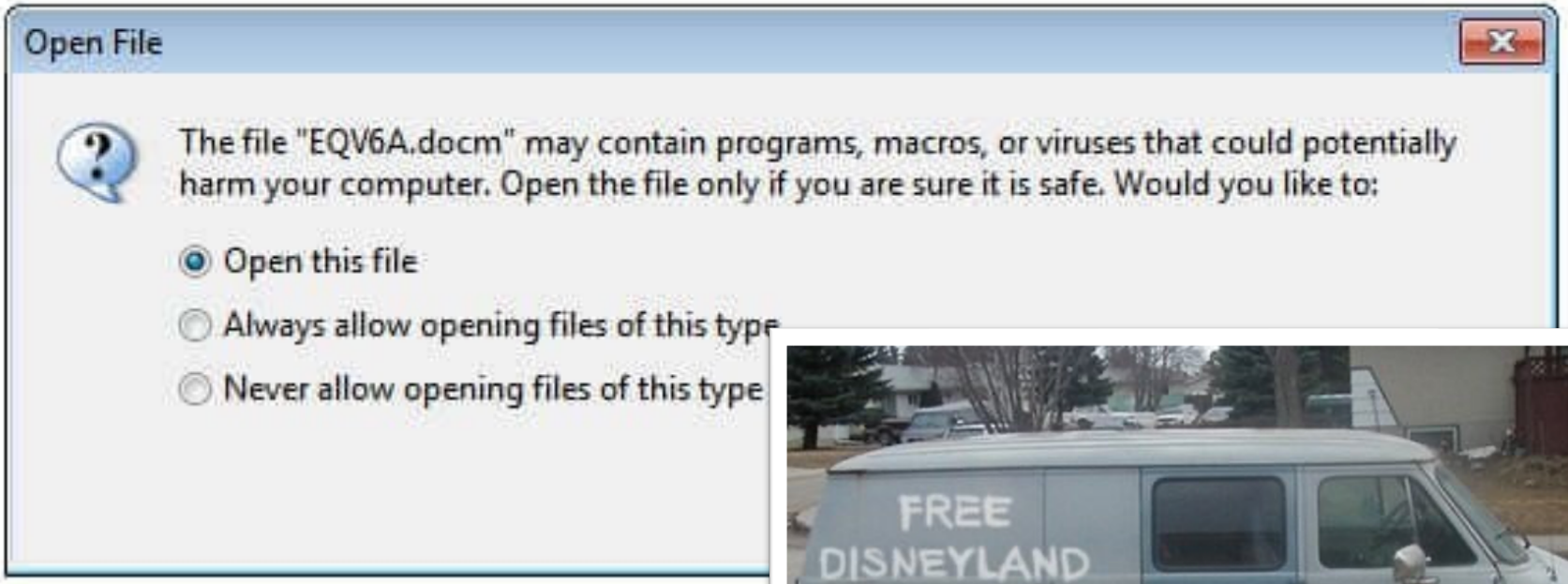

Your Invoice # 921212 - Mozilla Thunderbird
Reply
Reply All
Forward
More
From Courtney <Courtney.messeena@styledoors.info>
Subject Your Invoice # 921212
01:34 PM
To [redacted]
Your Invoice is attached.
If you feel you have received this email in error, please reply to this email to inform us of any necessary corrections.
1 attachment: Invoice.pdf 51.2 KB
Save
Invoice.pdf 51.2 KB

nm.pdf - Adobe Reader

File Edit View Document Tools Window Help

1 / 1 151% Find

Please open attached EQV6A.docm file



Distribution

- Step 2: User prompted to allow launch of external program when PDF is viewed – *Social Engineering*
  - Any modern PDF viewer should *not* automatically launch
  - Consent also allows JavaScript to save the embedded .docm file to a temporary file on disk
- Step 3: Word launches and loads .docm file

EQV6A [Read-Only] [Compatibility Mode] - Microsoft Word

File Home Insert Page Layout References Mailings Review View

Paste Cut Copy Format Painter Clipboard

Times New Rom 12 Font

Paragraph

¶ Normal ¶ No Spaci... Heading 1 Heading 2 Title Subtitle Subtle Em... Emphasis Styles

Change Styles

Find Replace Select Editing

This Document is protected!

1 Open the document in Microsoft Office. Previewing offline is not available for protected documents.

2 If this document was downloaded from your email, please click "Enable editing" from the yellow bar above.

3 Once you have enabled editing, please click "Enable content" on the yellow bar above.

Words: 0

Distribution

- Step 4: User prompted to allow office macros – *Social Engineering*
- Step 5: Visual Basic macro starts and downloads executable from hxxp://babil117.com/f87346b
  - Generates new child process pitupi20.exe
  - Profit!

jaff decryptor system - Windows Internet Explorer

Favorites | Web Slice Gallery

jaff decryptor system

Page | Safety | Tools

jaff decryptor system

Files are encrypted!

To decrypt flies you need to obtain the private key.
The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet

❶ You must install Tor Browser:
https://www.torproject.org/download/download-easy.html.en

❷ After instalation, run the Tor Browser and enter address:
http://rktazuzi7hbln7sy.onion/

Follow the instruction on the web-site.

Your decrypt ID: 2770906685

Done | Computer | Protected Mode: Off | 100%

Jaff Ransomware

- https://www.vmray.com/blog/jaff-ransomware-hiding-in-a-pdf-document/
- https://blog.emsisoft.com/en/27262/jaff-ransomware-the-new-locky/
- https://isc.sans.edu/forums/diary/Jaff+ransomware+gets+a+makeover/22446/
- https://www.malware-traffic-analysis.net/2017/05/16/index.html
  - Samples!

Jaff Malware Demo!