

Infecting files on-the-fly

Leonardo Nve

leonardo.nve@gmail.com

@leonardonve

About me

Red Team Leader

Hacking techniques trainer

Security researcher **Offensive Security**

From **Spain & Equatorial Guinea**



Why this talk?

```
Index of /pub/videolan/vlc/3.0.4/win32/  
  
..  
vlc-3.0.4-win32-debugsym.7z  
vlc-3.0.4-win32.7z  
vlc-3.0.4-win32.7z.asc  
vlc-3.0.4-win32.7z.md5  
vlc-3.0.4-win32.7z.sha1  
vlc-3.0.4-win32.7z.sha256  
vlc-3.0.4-win32.exe  
vlc-3.0.4-win32.exe.asc  
vlc-3.0.4-win32.exe.md5  
vlc-3.0.4-win32.exe.sha1  
vlc-3.0.4-win32.exe.sha256  
vlc-3.0.4-win32.msi  
vlc-3.0.4-win32.msi.asc  
vlc-3.0.4-win32.msi.md5  
vlc-3.0.4-win32.msi.sha1  
vlc-3.0.4-win32.msi.sha256  
vlc-3.0.4-win32.zip  
vlc-3.0.4-win32.zip.asc  
vlc-3.0.4-win32.zip.md5  
vlc-3.0.4-win32.zip.sha1  
vlc-3.0.4-win32.zip.sha256  
09-Aug-2018 16:06  
09-Aug-2018 16:06  
31-Aug-2018 14:33  
31-Aug-2018 14:33  
31-Aug-2018 14:33  
31-Aug-2018 14:33  
31-Aug-2018 14:33  
31-Aug-2018 14:33  
09-Aug-2018 16:06  
31-Aug-2018 14:33  
31-Aug-2018 14:33  
31-Aug-2018 14:33  
31-Aug-2018 14:33  
31-Aug-2018 14:33  
09-Aug-2018 16:06  
31-Aug-2018 14:33  
31-Aug-2018 14:33  
31-Aug-2018 14:33  
31-Aug-2018 14:33  
31-Aug-2018 14:33  
09-Aug-2018 16:06  
31-Aug-2018 14:33  
31-Aug-2018 14:33  
31-Aug-2018 14:33  
31-Aug-2018 14:33
```

VideoLAN, a project and a **non-profit organization**.

Downloading VLC 2.2.6 for Windows 64 bits

Thanks! Your download will start in few seconds...
If not, [click here](#). [Display checksum](#).

softlibre.unizar.es/videolan/vlc/2.2.6/win64/vlc-2.2.6-win64.exe

www.nvidia.es/download/driverResults.aspx/127042/es

/IDIA.

PLATAFORMAS ▾ DESARROLLADORES ▾ COMUNIDAD ▾ COMPRAR CONTROLADORES SOPORTE ACERCA DE N

Comparar y compra - GeForce
NVIDIA 3D Vision
PhyX
CUDA
Juegos de PC

Versión: 388.31 WHQL
Fecha de publicación: 2017.11.15
Sistema operativo: Windows 10 64-bit
Idioma: Español (España)
Tamaño: Temporarily unavailable

DESCARGAR AHORA

SURGIRÁN NUEVAS LEYENDAS
DURANTE UN TIEMPO LIMITADO,
COMpra UNA GEFORCE® GTX Y
LLEVATE DESTINY 2.
"Destiny 2 para PC. Promoción sujetos a condicionamiento de derechos."

ASPECTOS DESTACADOS DE LA VERSIÓN PRODUCTOS SOPORTADOS MÁS INFORMACIÓN

As part of the [NVIDIA Notebook Driver Program](#), this is a reference driver that can be installed on supported NVIDIA notebook GPUs. However, please note that your notebook original equipment manufacturer (OEM) provides certified drivers for your specific notebook on their website. NVIDIA recommends that you check with your notebook OEM about recommended software updates for your notebook. OEMs may not provide technical support for issues that arise from the use of this driver.

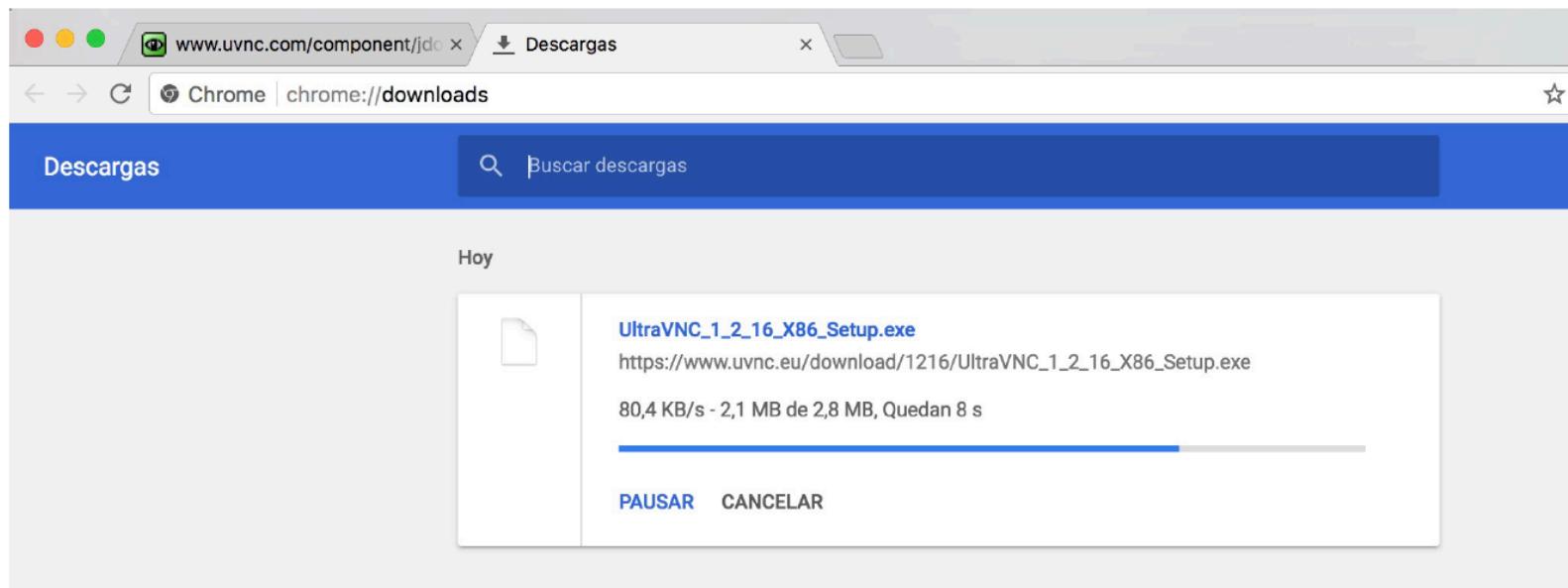
Before downloading this driver:

- It is recommended that you backup your current system configuration. [Click here for instructions](#).

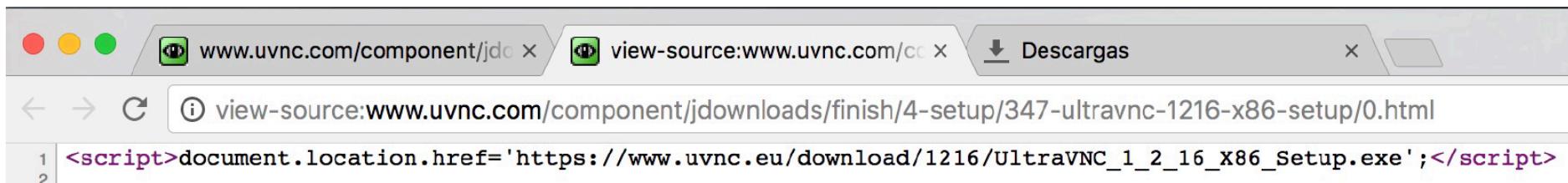
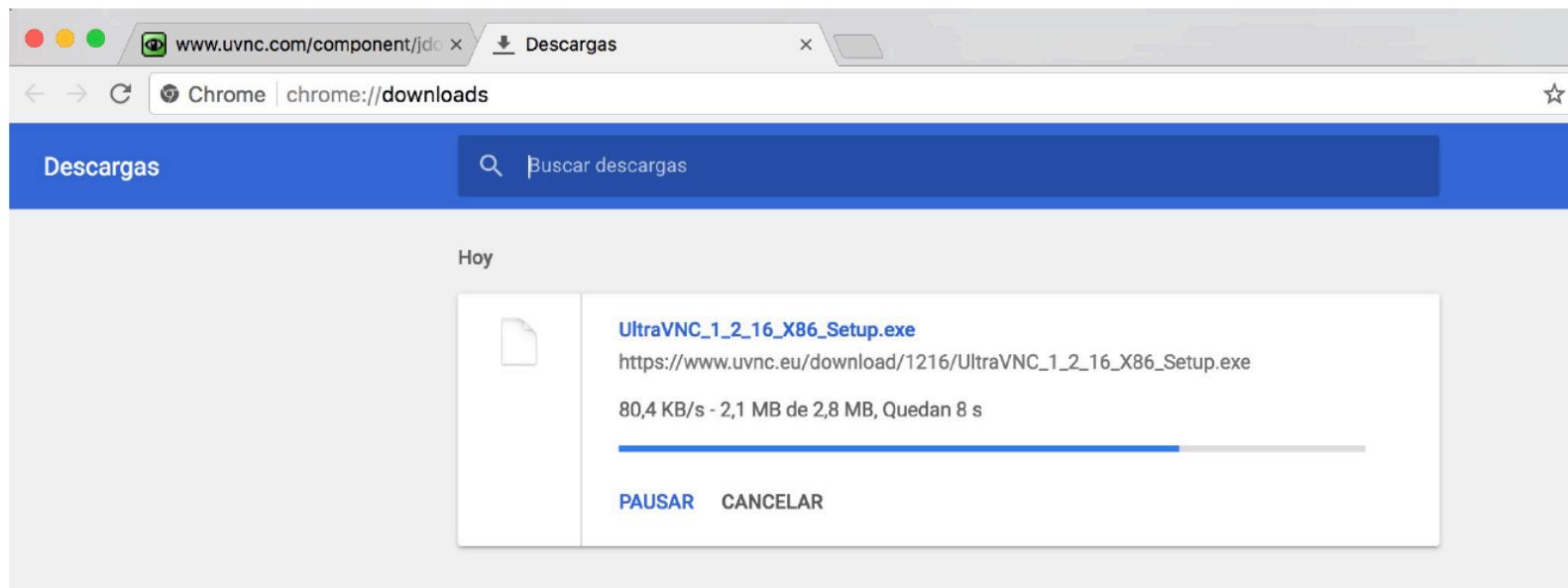
Game Ready Drivers provide the best possible gaming experience for all major new releases, including Virtual Reality

www.nvidia.es/content/DriverDownload-March2009/confirmation.php?url=/Windows/388.31/388.31-notebook-win10-64bit-international-whql.exe&lang=es&type=geforce

Why this talk?



Why this talk?



Why this talk?



Why this talk? – Not all is PE

The screenshot shows the official WinZip website for Mac. At the top, there's a navigation bar with links to PaintShop, VideoStudio, WinDVD, Aftershot, Roxio, Pinnacle, WinZip, CorelDRAW, and Painter. Below this is a main menu with links to Products, Buy Now, Download, Learn, Support, and Enterprise. The central part of the page features a large image of the WinZip Mac software box. To its right, the text "WinZip® Mac" is displayed with a "NEW VERSION!" badge. A brief description follows: "WinZip is the world's #1 choice when working with large files – zip, unzip, protect, share and more." Below this are three bullet points: "Zip and unzip files instantly", "Protect files with banking-level AES encryption", and "Share directly to iCloud Drive, Dropbox, Google Drive and ZipShare, from within WinZip". Two buttons are present: "DOWNLOAD TRIAL" (with the note "It's free, go for it") and "BUY NOW" (with the note "Starts at €35.64"). At the bottom of the page, a search bar contains the query "filetype:docx", and a link to "download.winzip.com/winzipmacedition60.dmg".

The screenshot shows a web browser window with two tabs. The active tab is titled "Maq. ENFOQUES-IMPAR" and displays a PDF document from "www.rediris.es/difusion/publicaciones/boletin/90/ponencia9.A.pdf". The content of the PDF is visible, including the title "TOUM: Tablón Oficial de la Universidad de Murcia" and some names. Below this tab, another tab is visible with the title "Android USB Driver for Windows" and the URL "chrome://downloads". The main content area of this tab shows a download progress bar for a file named "SAMSUNG_USB_Driver_for_Mobile_Phones.zip". The progress bar indicates "585 KB/s - 12,2 MB de 15,3 MB, Quedan 5 s". There are "PAUSAR" and "CANCELAR" buttons at the bottom of the download panel.

Gamma explain what I'm going to talk about

<https://www.youtube.com/watch?v=AWmpNWsWbYc>

Commercial Tools



FINFISHER™
EXCELLENCE IN
IT INVESTIGATION

FinFly LAN

Some of the major challenges law enforcement agencies are facing are mobile targets that don't allow any physical access to their computers and do not open any unknown files they receive. Security-aware targets are almost impossible to monitor as they keep their systems up-to-date and successfully resist common exploits or intrusion techniques.

FinFly LAN covertly deploys remote monitoring solutions on target systems in Local Area Networks (Wired and Wireless). It patches files that are downloaded by the target on-the-fly, sends fake software updates or deploys the monitoring solution into visited websites.

Capabilities

- » Deploys remote monitoring solutions on target systems in LAN environments

]Hacking Team[

▼	RCS 9.6 (stable)	11 Jul 2015 02:48	--	Folder
►	Documentation	11 Jul 2015 02:48	--	Folder
▼	Product	11 Jul 2015 02:49	--	Folder
►	Console	11 Jul 2015 02:48	--	Folder
▼	Injector	11 Jul 2015 02:48	--	Folder
	networkinjector-9.6.0.iso	08 Jul 2015 11:56	1,11 GB	ISO Disk Image
►	Server	11 Jul 2015 02:49	--	Folder
☒	Remote Control System 9.6 - Readme.pdf	06 Jul 2015 22:32	43 KB	Adobe...cument

Free Tools

Peinjector <https://github.com/JonDoNym/peinjector>

Provides different ways to infect these files with custom payloads without changing the original functionality. It creates patches, which are then applied seamlessly during file transfer. It is very performant, lightweight, modular and can be operated on embedded hardware.

Features

- Full x86 and x64 PE file support.
- Open Source
- Fully working on Windows and Linux, including automated installation scripts.
- Can be operated on embedded hardware, tested on a Raspberry Pi 2.
- On Linux, all servers will be automatically integrated as service, no manual configuration required.
- Plain C, no external libraries required (peinjector).
- MITM integration is available in C, Python and Java. A sample Python MITM implementation is included.
- Foolproof, mobile-ready web interface. Anyone who can configure a home router can configure the injector server.
- Easy to use integrated shellcode factory, including reverse shells, meterpreter, ... or own shellcode. Everything is available in 32 and 64 bit with optional automated encryption. Custom shellcode can be injected directly or as a new thread.

Free Tools

Backdoor Factory Proxy <https://github.com/secretsquirrel/BDFProxy>

Patch Binaries via MITM: BackdoorFactory + mitmProxy.

Features

- Full x86 and x64 PE file support.
- ELF and Mach-O
- Open Source

<https://www.youtube.com/watch?v=YzeGxlurQy8>

Modifying Tools issues

- Resources / icons?
- Antivirus?
- Executable signatures?
- The original code is executed?
- Executables auto-integrity checks
- UAC?
- Other not executable file formats:
 - ZIP
 - RAR
 - PDF
 - MS Office
 - ETC

Modifying Tools issues

What do you think on-the-fly means?

Download a file vs Download a file through a proxy

The screenshot shows a Mac OS X desktop environment. At the top is the Dock with various icons. Above the Dock is the system menu bar with options like QuickTime Player, Archivo, Edición, Visualización, Ventana, and Ayuda. The battery icon shows 76% remaining. The date and time are Sáb 3:42. Below the menu bar is the Dock again, featuring icons for Finder, Mail, Safari, and other applications.

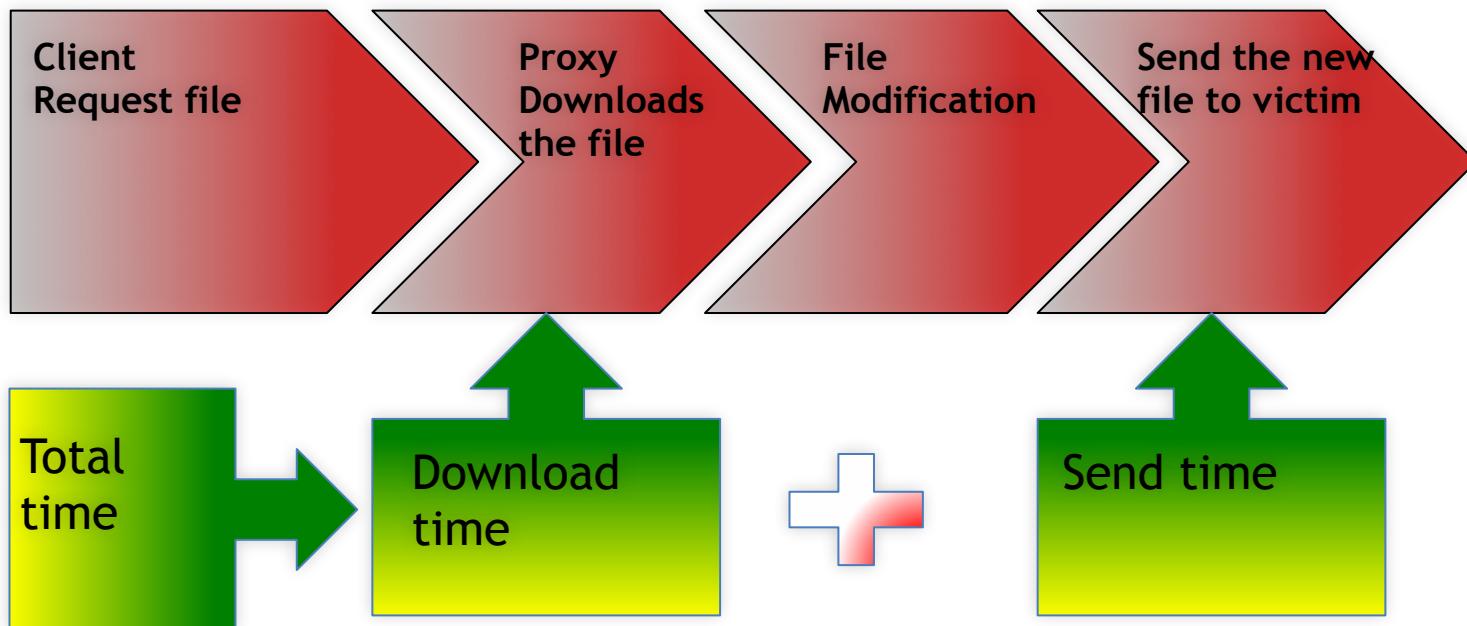
The main window is a web browser (Safari) showing an Apache directory listing for the URL softlibre.unizar.es/videolan/vlc/last/win64/. The title bar shows "Index of /videolan/vlc/last/win64". The page content is a table listing files in the directory:

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
vlc-2.2.6-win64.7z	2017-05-24 15:09	28M	
vlc-2.2.6-win64.7z.asc	2017-05-24 15:09	195	
vlc-2.2.6-win64.7z.md5	2017-05-24 15:09	53	
vlc-2.2.6-win64.7z.sha1	2017-05-24 15:09	61	
vlc-2.2.6-win64.7z.sha256	2017-05-24 15:09	85	
vlc-2.2.6-win64.exe	2017-05-24 15:09	31M	
vlc-2.2.6-win64.exe.asc	2017-05-24 15:09	195	
vlc-2.2.6-win64.exe.md5	2017-05-24 15:09	54	
vlc-2.2.6-win64.exe.sha1	2017-05-24 15:09	62	
vlc-2.2.6-win64.exe.sha256	2017-05-25 12:57	86	
vlc-2.2.6-win64.xpi	2017-05-26 13:40	32M	
vlc-2.2.6-win64.xpi.asc	2017-05-26 13:40	195	
vlc-2.2.6-win64.xpi.md5	2017-05-26 13:40	54	
vlc-2.2.6-win64.xpi.sha1	2017-05-26 13:40	62	
vlc-2.2.6-win64.xpi.sha256	2017-05-26 13:40	86	
vlc-2.2.6-win64.zip	2017-05-26 13:40	51M	
vlc-2.2.6-win64.zip.asc	2017-05-26 13:40	195	
vlc-2.2.6-win64.zip.md5	2017-05-26 13:40	54	
vlc-2.2.6-win64.zip.sha1	2017-05-26 13:40	62	
vlc-2.2.6-win64.zip.sha256	2017-05-26 13:40	86	

At the bottom of the browser window, there is a footer bar with the text "Apache/2.4.10 (Debian) Server at softlibre.unizar.es Port 80".

Files Modification on-the-fly

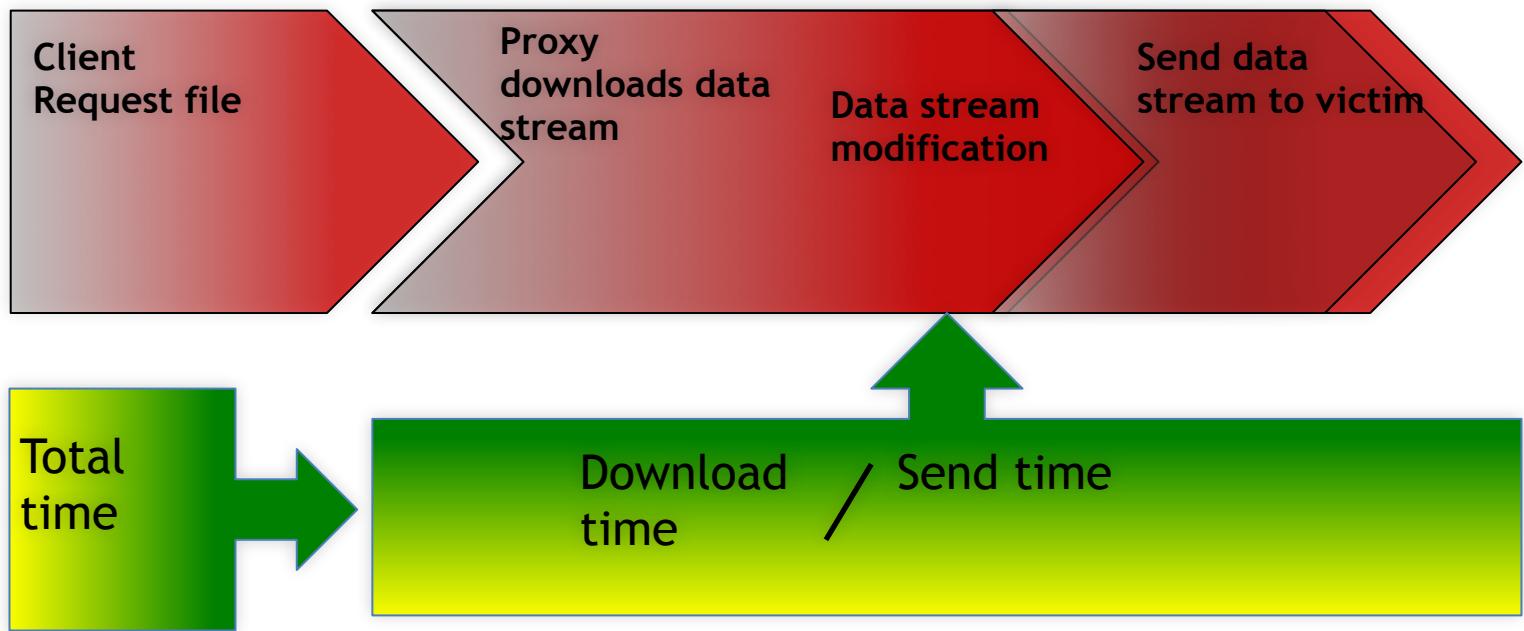
(option 1)



- Dependency of connection speed.
- Dependency of file size.
- Dependency of file format.

File Modification on-the-fly

(option 2)



- (IN)dependency of connection speed.
- (IN)dependency of file size.
- Dependency of file format.

File Modification on-the-fly (option 2)

- Know the file format to guess the future modification.
- From the beginning we know the original file size (original Content-Length).
- Resulting file size? (New Content-Length)
- File format with CRC?
- Headers of modified file?
- A study of all file formats is needed.
- Thanks to Ange Albertini ([@angealbertini](#)) it is easy with most common filetypes.

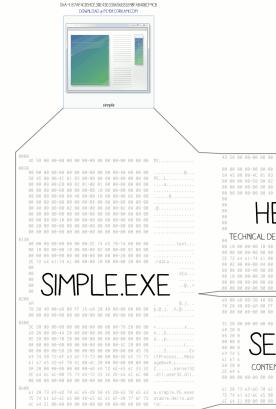
PE Infection

PE Format

PE¹⁰¹ a windows executable walkthrough

ANGE ALBERTINI
CORKAMI.COM

DISSECTED PE



HEADER

TECHNICAL DETAILS ABOUT THE EXECUTABLE

SECTIONS

CONTENTS OF THE EXECUTABLE

LOADING PROCESS

1 HEADERS

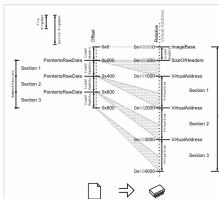
THE DOS HEADER IS PARSSED.
THE PE HEADER IS PARSED.
(OPTIONAL HEADER IS PARSED)
THE OPTIONAL HEADER IS PARSED.
(IT OVERRIDES THE PE HEADER)

2 SECTION TABLE

SECTION TABLE IS PARSED.
IT IS LOCATED AT OFFSET OPTIONAL HEADER - 40H (POINT TO PE HEADER).
IT CONTAINS NUMBER OF SECTIONS ELEMENTS.
IT IS CHECKED FOR VALIDITY WITH ALIGNMENTS.

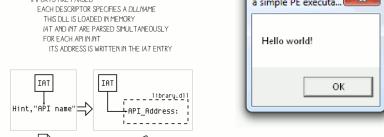
3 MAPPING

THE FILE IS MAPPED IN MEMORY ACCORDING TO:
THE IMAGEBASE
THE SECTION ADDRESSES
THE SECTION TABLE



4 IMPORTS

DATASECTION ARE PARSED.
THEY FOLLOW THE OPTIONALHEADER.
THEY ARE INDEXED BY ADDRESS.
IMPORTS ARE ALWAYS #2.
IMPORTS ARE PARSED.
EACH IMPORT SPECIFIES A COLUMN.
THIS COLUMN IS LOADED IN MEMORY.
INT ARE PARSED SIMULTANEOUSLY.
FOR EACH IMPORT
ITS ADDRESS IS WRITTEN IN THE INT ENTRY



5 EXECUTION

CODE IS CALLED AT THE ENTRYPOINT.
THE CALLS OF THE CODE GO VIA THE INT TO THE API.



FIELDS	VALUES	EXPLANATION
e_magic	"MZ" 0x40	CONSTANT SIGNATURE OFFSET OF THE PE HEADER 1
Signature	"PE", 0, 0 0x14c [intel 386]	CONSTANT SIGNATURE PROCESSOR ARCHITECTURE, NUMBER OF SECTIONS 2
Machine	0x14c [intel 386]	RELATIVE OFFSET OF THE SECTION TABLE 2
NumberofSections	3	
SizeofOptionalHeader	0x0	
Characteristics	0x102 [32b EXE]	EXFOLIUM.
Magic	0x10b [32b]	32BITS64BITS
AddressofEntryPoint	0x1000	WHERE EXECUTION STARTS 5
ImageBase	0x000000	ADDRESS WHERE THE FILE SHOULD BE MAPPED IN MEMORY 3
SectionAlignment	0x200	WHERE SECTIONS SHOULD START IN MEMORY 2
FileAlignment	0x200	REQUIRED VERSION OF WINDOWS
MajorSubSystemVersion	4 [NT 4 or Later]	TOTAL SIZE OF THE IMAGE 3
SizeOfImage	0x200	DRIVER/GRAFIQUE/COMMAND LINE
SectionHeaders	0x20	NUMBER OF DATA DIRECTORIES 4
Subsystem	2 [GUI]	
NumberofRvaAndSizes	16	
ImportsVA	0x2000	RVA OF THE IMPORTS 4
DATA DIRECTORIES		
CODE		
DATA		
IMPORTS		
SECTIONS TABLE		
X86 ASSEMBLY		
EQUIVALENT C CODE		
CONSEQUENCES		
STRINGS		
a simple PE executable Hello world!		

THIS IS THE WHOLE FILE, HOWEVER MOST PE FILES CONTAIN MORE ELEMENTS.
EXPLANATIONS ARE SIMPLIFIED FOR CONCERNCE

NOTES

MZ HEADER AND FOLLOWS
START WITH NT INITIAL MARK, ZINHOK0X1000 DOS DEVELOPER

PE HEADER AKA PAGE, FILE, HEADERS / COFF PE HEADER
STARTS WITH PE PORTABLE EXECUTABLE

OPTIONAL HEADER AKA PAGE, OPTIONAL HEADER

OPTIONAL HEADER IS NOT A PE BUT REQUIRED FOR EXECUTABLES

RELATIVE VIRTUAL ADDRESS

ADDRESS RELATIVE TO PAGEBASE, INT IMAGEBASE RVA + 0

ALMOST ALL ADDRESSES OF THE HEADERS ARE RVA

IN CODE, ADDRESSES ARE NOT RELATIVE.

INT IMPORT NAME TABLE

NULL-TERMINATED LIST OF POINTERS

FILE IF IT IS A COPY OF THE INT

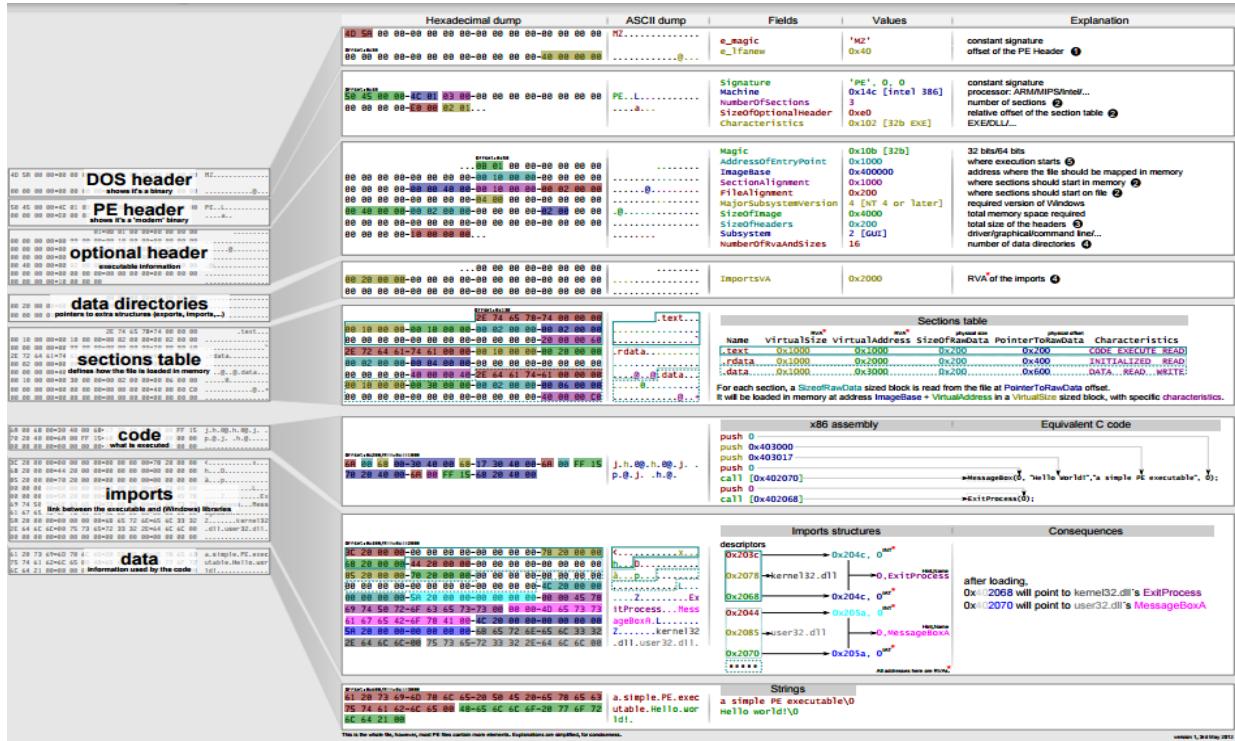
AFTER LOADING, IT POINTS TO THE IMPORTED ARS

INT

INDEX IN THE EXPORTS TABLE OF A DLL TO BE IMPORTED

NOT REQUIRED BUT PROVIDES A SPEED-UP BY REDUCING LOOK-UP

PE Format



Normal Setsions

.text : executable code

.data : global initialized data

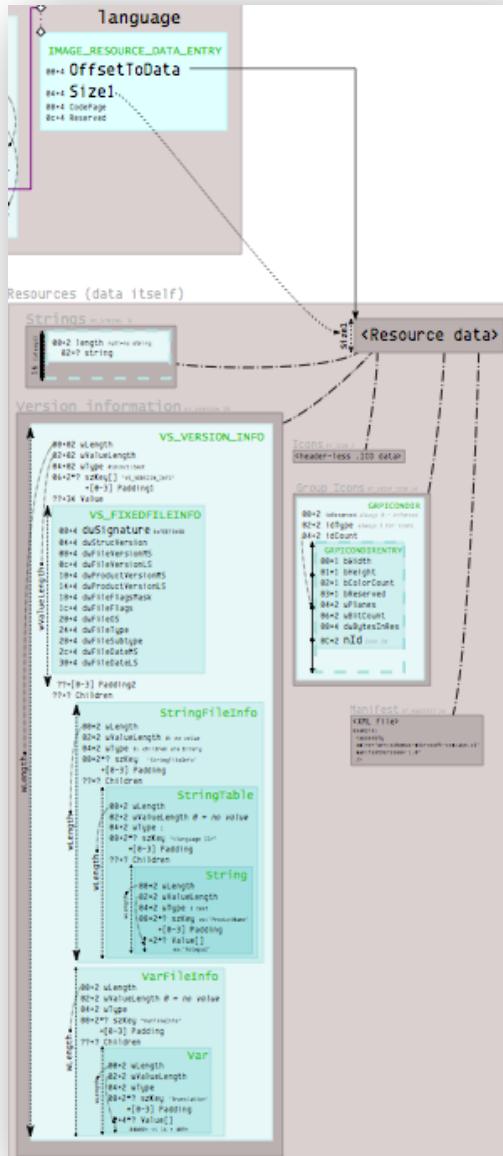
.rdata : global read-only data

.edata: export tables

.idata : import tables

- | | |
|------------|---|
| .pdata | : exception handling information |
| .xdata | : exception information, free format |
| .reloc | : information for relocation of library files |
| .rsrc | : resources of the executable |
| .directive | : linker options |
| .bss | : uninitialized data, free format |

PE Resource Structure



- Structure very unclear even in the specification.
- Usage of virtual relative addresses from uncertain PE points.
- Hard analysis and hard construction.
- Have to consider the alignment inside file space.

EXE Infection

- EXE = executable PE.
- The original EXE must be executed as expected while other process is executed (payload).
- The process must be transparent to the user.
- Protections:
 - File name (reputation)
 - Digital signature (S.O. Level)
 - Integrity check (code level)

EXE Infection

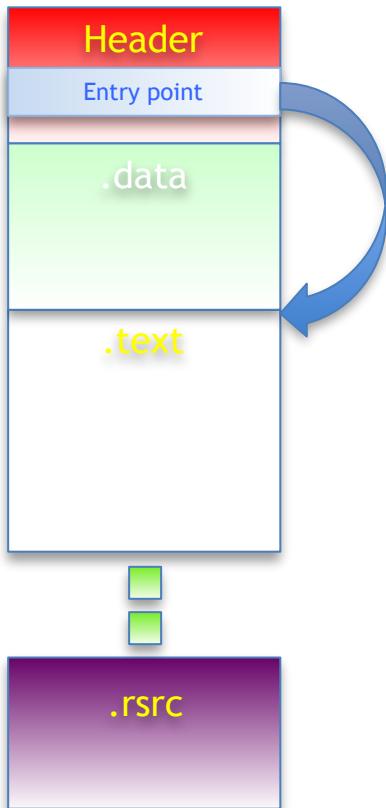
(Option 1)

- Add new code at the end of the file.
- Change Entry Point.
- Remove digital signature.
- The new code is executed and calls later to the original code.

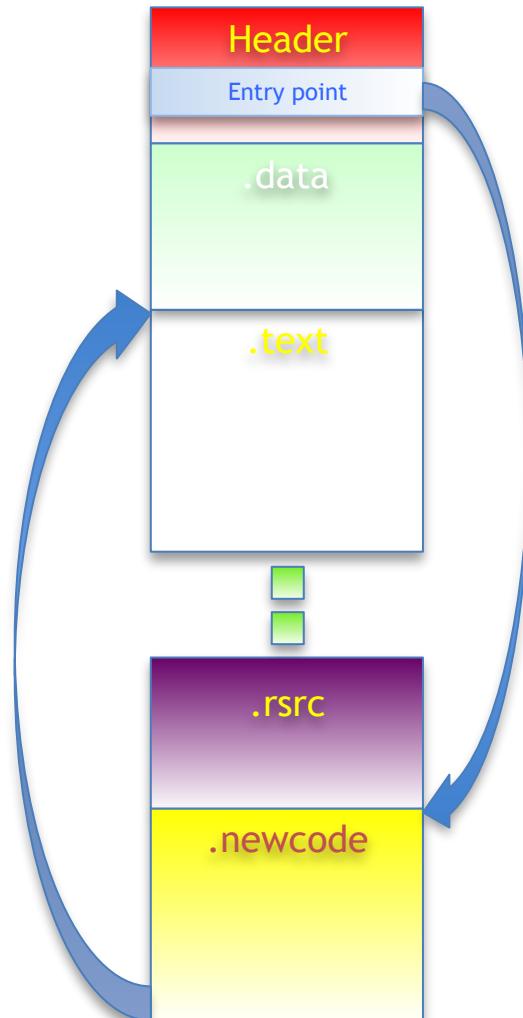
EXE Infection

(Opción 1)

Original EXE



Infected EXE



EXE Infected

(Option 1)

- The executable may be signed a posteriori if you have a certificate.
- The auto-integrity check fails.
- Well known method by AVs
- New size = original +new code
- The resource section is preserved so the ICON is not modified

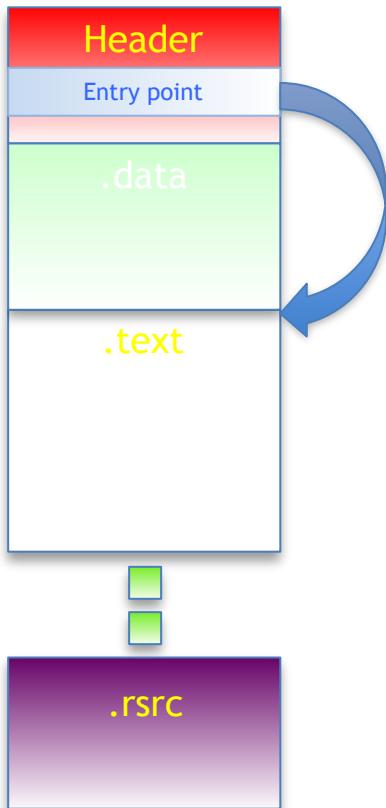
EXE Infection

(Option 2)

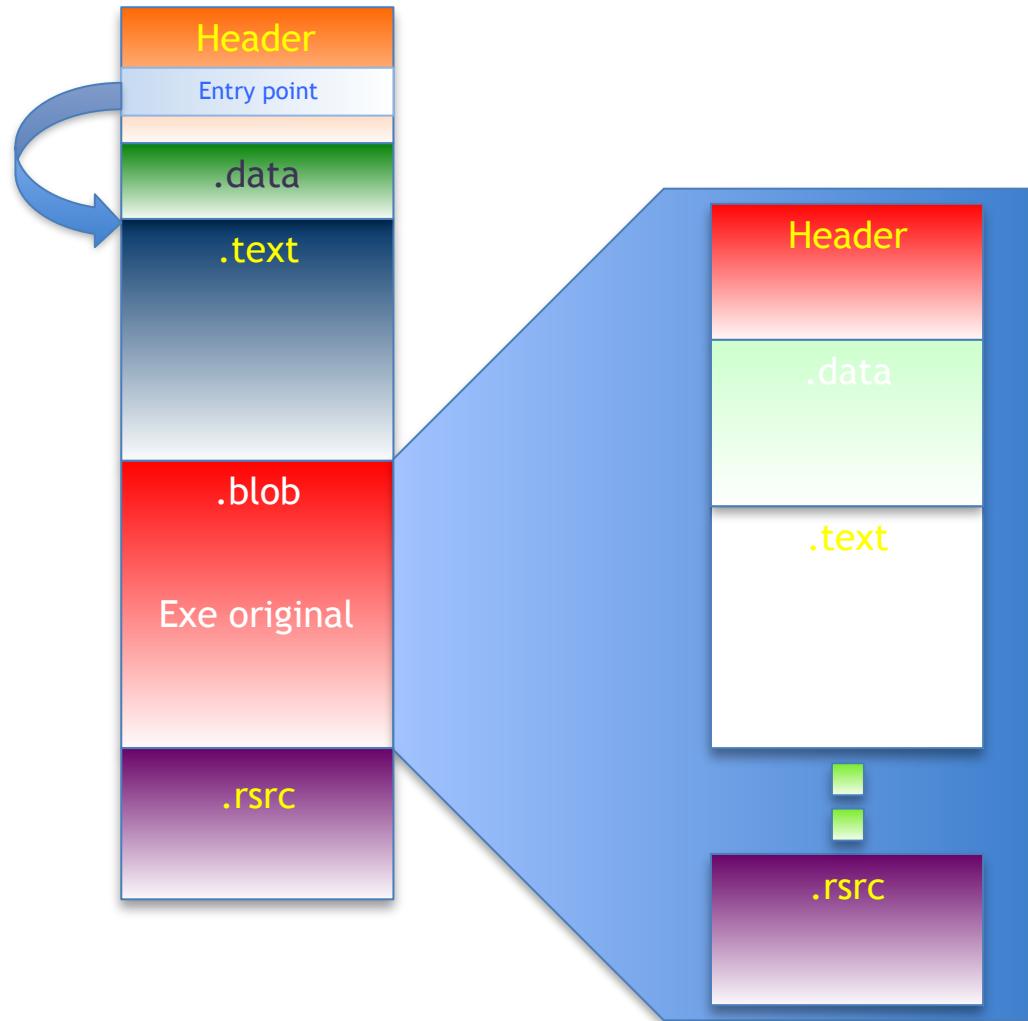
- Add original EXE to a section of the new malware.
- The new EXE executes its magic, copies the section to another file and runs it.

EXE Infection (Option 2)

EXE Original



Malware + original



EXE Infection

(Option 2)

- The executable may be signed a posteriori if you have a valid certificate.
- The resource section is preserved so the ICON is not modified
- Size = original + malware + original resources section+ alignment

Encimadelamosca (EDM)

EXE Infection

- Analyzes original EXE's header (1st stream).
- Modifies the new EXE's header.
 - Add data section.
 - Sizes
 - Add resources section.
- Sends the new EXE
- Sends the original EXE
- Sends the resources section
- Content-type:

File type	Content-types
.exe	application/x-msdownload application/octet-stream

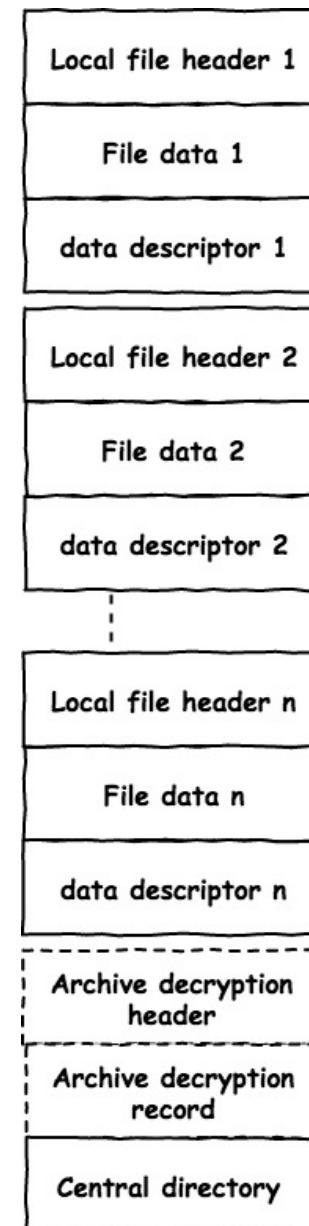
Demo:

Infecting an EXE using EDM

ZIP files infection

PKWare ZIP Format

- General structure of non encrypted ZIP file. (simplified)



PKWare ZIP Format

- Local file header

	0x0	0x1	0x2	0x3	0x4	0x5	0x6	0x7	0x8	0x9	0xa	0xb	0xc	0xd	0xe	0xf
0x0000		Signature		Version		Flags		Compression		Mod time		Mode date		Crc-32		
0x0010	Crc-32		Compressed size		Uncompressed size			File name len		Extra field len						
0x0020					File name (variable size)											
0x0030					Extra field (variable size)											

0x0030

size field (size)

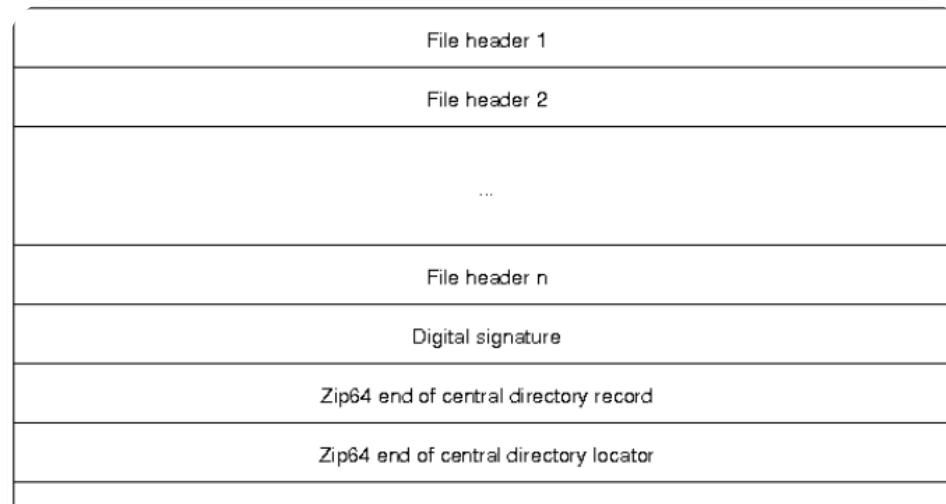
PKWare ZIP Format

- Data descriptor

0x0000	0x0 0x1 0x2 0x3 0x4 0x5 0x6 0x7 0x8 0x9 0xa 0xb	Crc-32	Compressed size	Uncompressed size
--------	---	--------	-----------------	-------------------

PKWare ZIP Format

- **Central directory:** Contains metadata about the files in the file, including the data about the files encryption. Beside the ZIP files divided in multiple files.



<https://www.pkware.com/documents/casestudies/APPNOTE.TXT>

PKWare ZIP Format

- Central directory file header

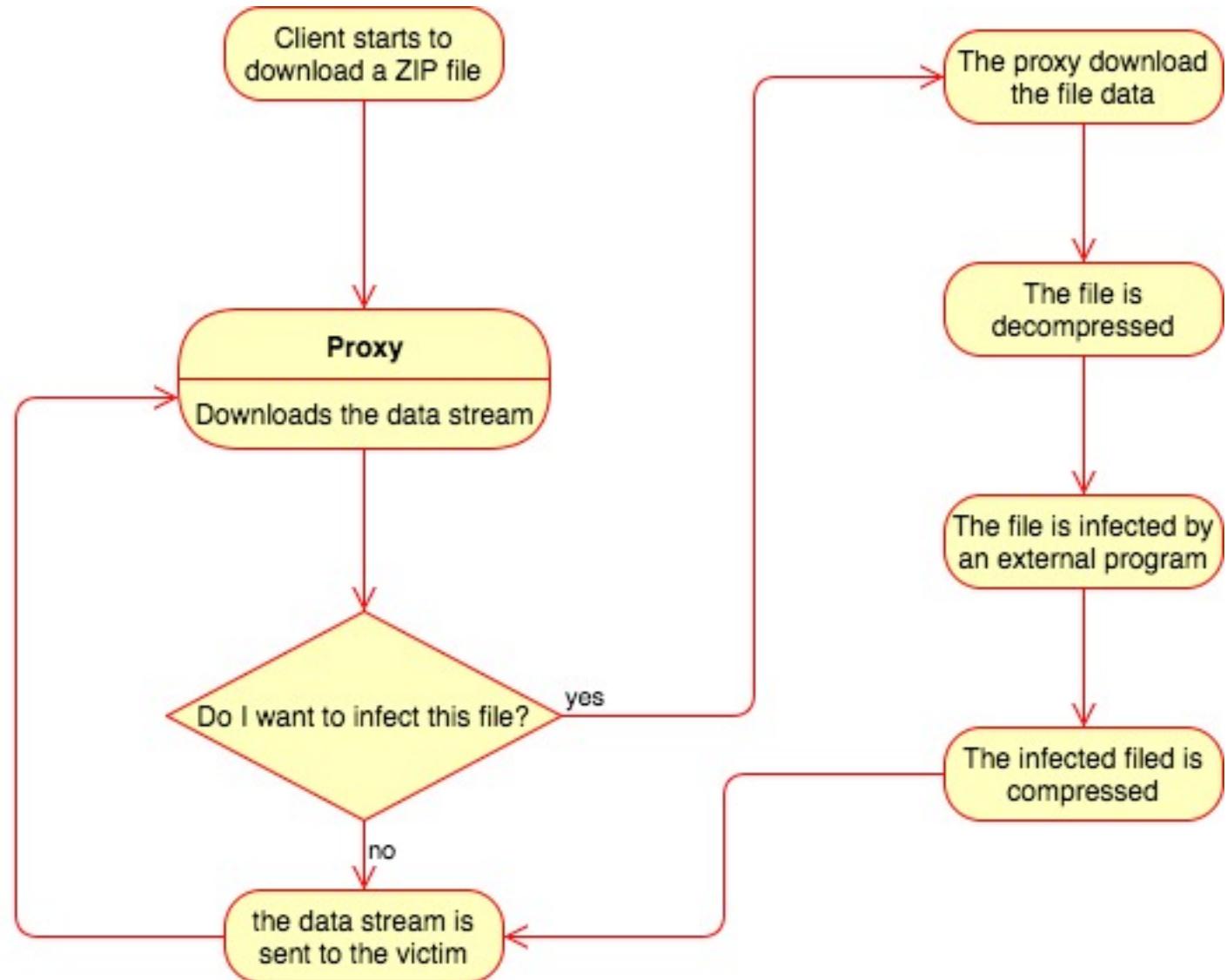
	0x0 0x1 0x2 0x3 0x4 0x5 0x6 0x7 0x8 0x9 0xa 0xb 0xc 0xd 0xe 0xf							
0x0000	Signature	Version	Vers. needed	Flags	Compression	Mod:time	Mod:date	
0x0010	Crc-32	Compressed size			Uncompressed size	File name len	Extra field len	
0x0020	File comm. len	Disk # start	Internal attr.	External attr.	Offset of local header			
0x0030				File name (variable)				
0x0040				Extra field (variable)				
0x0050				File comment (variable)				

	0x0 0x1 0x2 0x3 0x4 0x5 0x6 0x7 0x8 0x9 0xa 0xb 0xc 0xd 0xe 0xf					
0x0000	Signature	Disk number	Disk # w/od	Disk entries	Total entries	Central directory size
0x0010	Offset of cd w/ starting disk	Comment len			ZIP file comment (variable)	

- End

Encimadelamosca

ZIP files infection(beta)



Encimadelamosca

ZIP file infection

- Delays with big compressed files.
- Encrypted ZIP files (Being resolved).
- Size = file size + infected data + padding.
- Capability of adding files on-the-fly.
- Content-type:

File type	Content-types
.zip	application/zip application/octet-stream

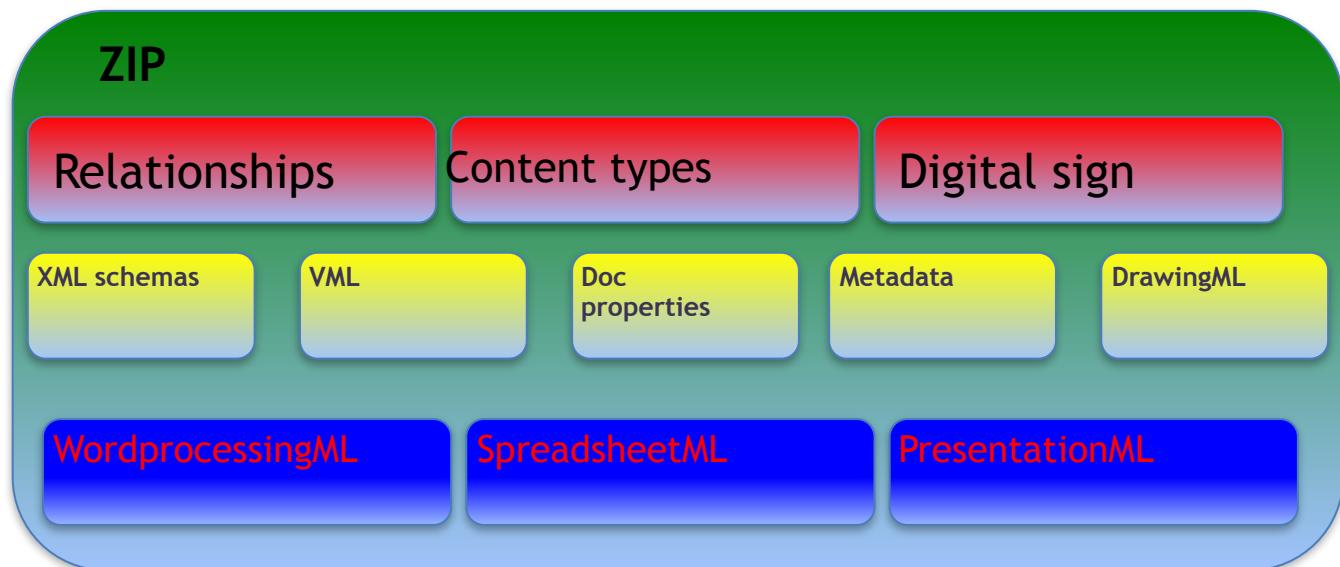
DEMO:

Infecting an ZIP using EDM

OOXML Infection

OOXML Format

- Office Open XML is a standard file format which most common extensions are .docx, .xlsx, .pptx y .ppsx.
- International standard ISO/IEC 29500:2008, Information technology - Office Open XML formats.



OOXML Format

Identifies the content type in the document, such as the document's main body, styles, configuration, and file properties.

Contains information about the files relationships (XML)

```
Arhem:Documents leonardonve$ unzip WinDbg\  
CheatSheet.docx  
Archive: WinDbg CheatSheet.docx  
inflating: [Content_Types].xml  
inflating: _rels/.rels  
inflating: word/_rels/document.xml.rels  
inflating: word/document.xml  
inflating: word/theme/theme1.xml  
extracting: docProps/thumbnail.jpeg  
inflating: word/settings.xml  
inflating: word/webSettings.xml  
inflating: word/stylesWithEffects.xml  
inflating: docProps/core.xml  
inflating: word/styles.xml  
inflating: word/fontTable.xml  
inflating: docProps/app.xml
```

Defines the relationships between the directory tree files and the document.

Document in xml format

Document properties

Files properties

OOXML Format

```
[Dinamics:hitb Leonardo$ unzip document.docx
Archive: document.docx
    inflating: [Content_Types].xml
    inflating: _rels/.rels
    inflating: word/_rels/document.xml.rels
    inflating: word/document.xml
    inflating: word/theme/theme1.xml
    extracting: word/media/image1.png
    extracting: word/media/image2.png
    inflating: word/settings.xml
    inflating: word/webSettings.xml
    inflating: word/styles.xml
    inflating: word/numbering.xml
    inflating: docProps/core.xml
    inflating: word/fontTable.xml
    inflating: docProps/app.xml
Dinamics:hitb Leonardo$ ]
```

Encimadelamosca

OOXML Infection

- Similar to ZIP file

- Content-types:

File type	Content-types
.docx	application/vnd.openxmlformats-officedocument.wordprocessingml.document application/octet-stream application/msword
.xlsx	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet application/octet-stream
.pptx	application/vnd.openxmlformats-officedocument.presentationml.presentation application/octet-stream
.ppsx	application/vnd.openxmlformats-officedocument.presentationml.slideshow application/octet-stream

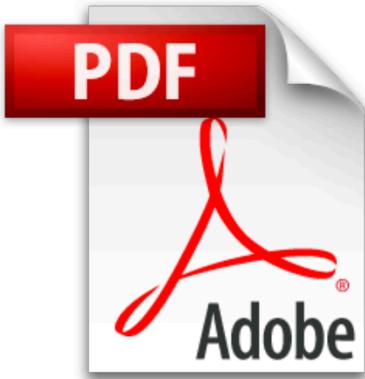
DEMO:

Infecting an OOXML using EDM

Other files type Infection??

TODO

- **PDF** - How to infect on the paper, just need to code it
- **RAR** - How to infect on the paper, just need to code it
- **TGZ** - TAR + GZ - How to infect on the paper, just need to code it
- **APK** - It is just a ZIP - same technique



TODO

- **Torrent**
- Mac OS X Disk Image **DMG**
- Mac OS X Installer Package **PKG**
- Java **CLASS** (it exists inside JARs which are ZIP files too)



BitTorrent™



TODO

- C-code porting for embedded devices and HA
- New techniques of infection OTF
- PE signature implementation

EDM

EDM available on Git:

<https://b1b.es/edm>

The End...