Antivirus (In)Security

Chaos Communication Camp 2007

Sergio '**shadown**' Alvarez +

nruns...
network · technology · security · consulting

Acknowledgments

- My wife Maureen,my son Ulises and my daughter Eileen
- Without their unconditional support this wouldn't be possible.

Who Am I

- Sergio 'shadown' Alvarez
- Security Researcher
- Argentinian
- Live in Germany since July 2005
- Work for n.runs AG

Agenda

- Introduction
- The Myths
- The Facts
- Common Problems
- Hunting Bugs
- Demo
- Final Comments
- Q&A

Antivirus (In)Security

First things first...

- How many of you are currently using antivirus software in your boxes?

INTRODUCTION

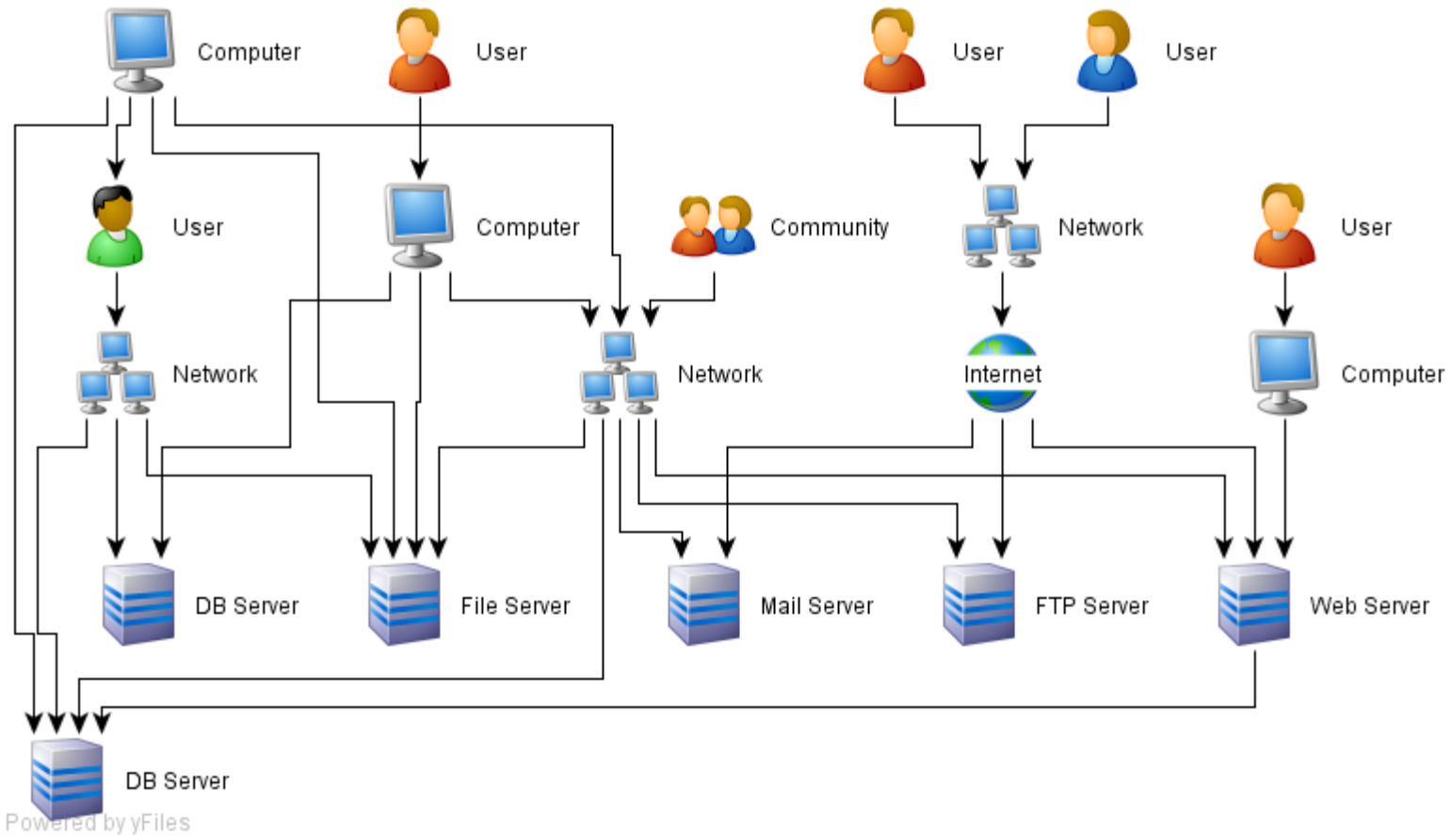
Antivirus (In)Security

Introduction

- What is an Antivirus?
  - Antivirus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software. (From Wikipedia)
- Where is Antivirus software located?
  - Commonly installed
    - Mail Servers, Web Browsers, Web Servers, FTP Servers, File Servers, DataBase Servers, Files R/W, IM software, Gateways, Appliances
  - Scanning Approaches
    - Memory, Files Formats, Packers, Contents (Exploits, etc)
    - Detection by Heuristic, Patterns and suspicious behaviours

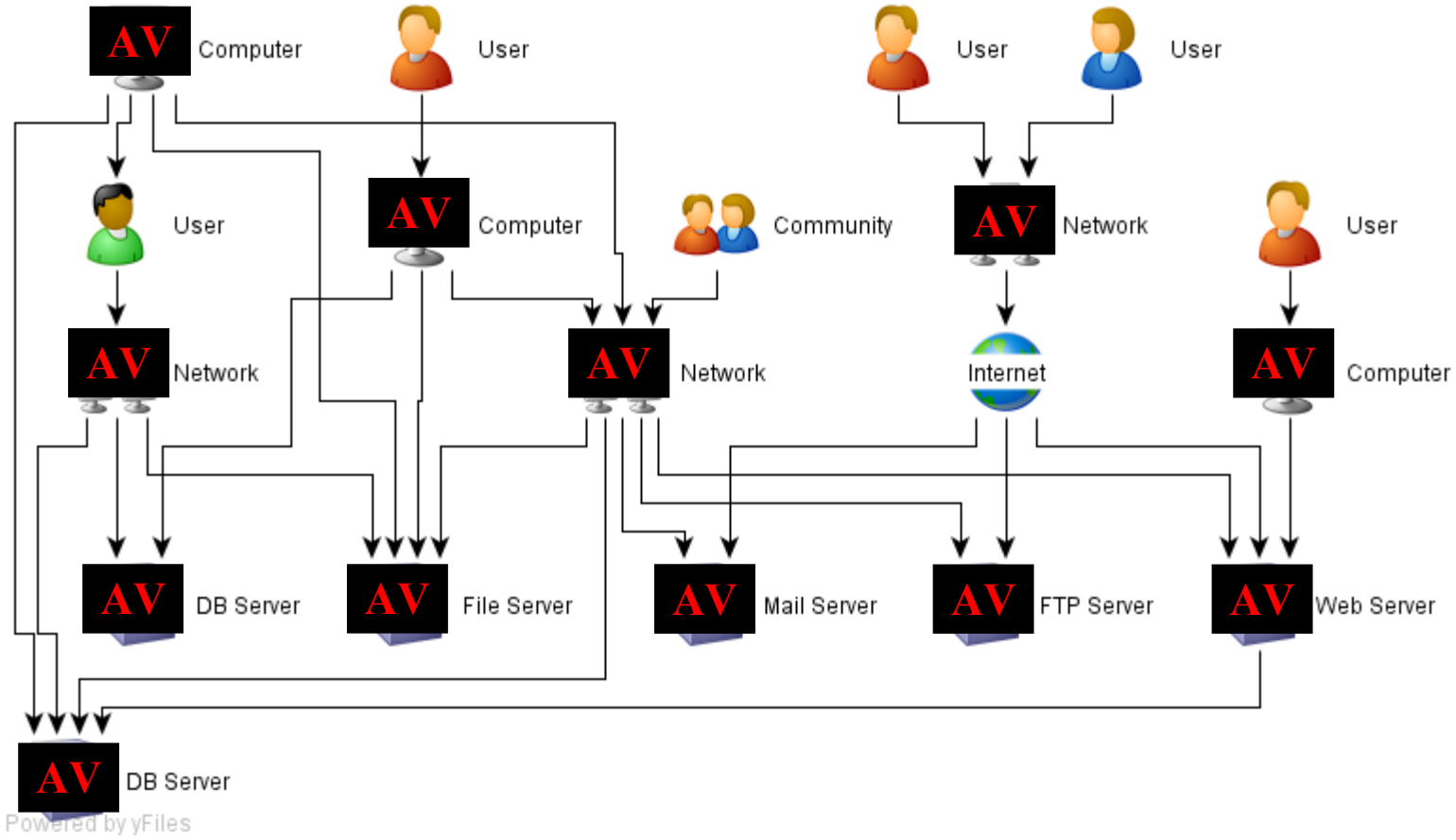
Antivirus (In)Security

Introduction



Antivirus (In)Security

Introduction



Introduction

- Who could be affected by AV vulnerabilities?
  - +90% of computers (workstations, servers, laptops)
  - Appliances
  - PDAs
  - Even phones

Antivirus (In)Security

THE MYTHS AND THE FACTS

Antivirus (In)Security

The Myths (or common asupmtions)

- Antivirus Security
  - Antivirus Software is secure
  - Makes our network and systems more secure
- Antivirus Developers
  - Are developed by security experts
- Antivirus Detection
  - I use Antivirus, I will not get infected
  - My Antivirus detects even unknown viruses

Antivirus (In)Security

The Facts

- Antivirus Security
  - We'll discuss how secure AV software is in this talk
- Antivirus Developers
  - Are developed by **programmers** as any other software
- Antivirus Detection
  - Very old viruses tend to not be detected
  - Not all packers are detected by all AVs
  - Each AV is able to handle a limited number of archiving formats, all AV has the more common ones.
  - **Someone has to suffer first**

Antivirus (In)Security

The Facts

- **Antivirus Software is a *must have***

Antivirus (In)Security

COMMON PROBLEMS

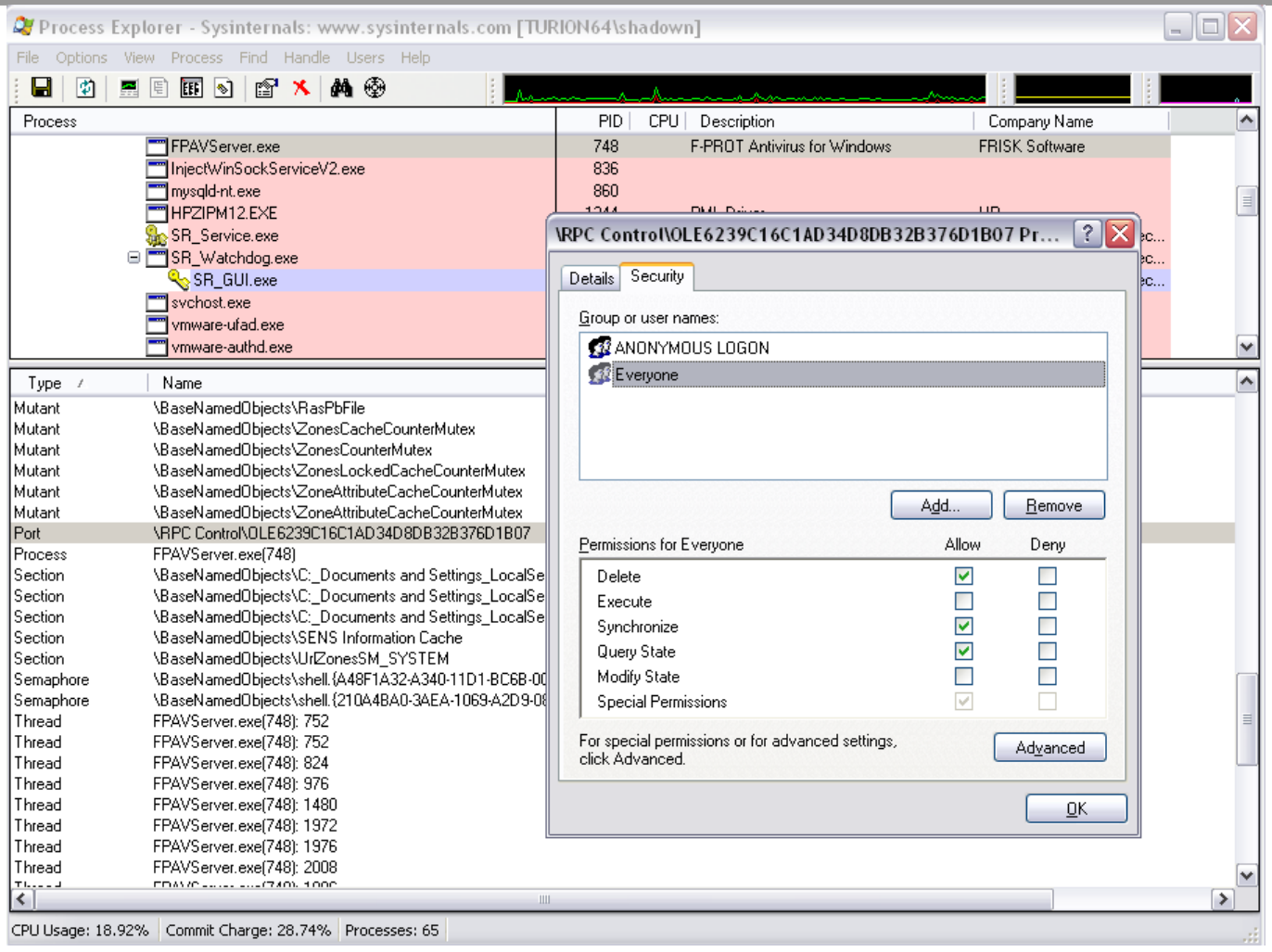
Antivirus (In)Security

Common Problems

- Communication Protocols Security by Obscurity
  - Hardcoded passwords in the binaries
- UnProper Password Handling
  - Storing the password of the Administration console also in the clients config file. (TrendMicro some time ago, 'encrypted' with a char depending on possition mutation algorithm.)
- Client Listeners standard Security Issues
- NULL DACLs
  - Registry for Settings
  - Config files
  - Handles

Antivirus (In)Security

Common Problems



Antivirus (In)Security

Common Problems

- Very bad input validation
  - Plenty of interger issues
    - Reading sizes from the headers
    - Signed integers to deal with sizes and lengths
- Don't Implement all filetype features
  - i.e: gzip concatenation
- Don't know how to deal with big files (>2GB)
- Are not aligned with massively used software
- They really think they know about security

Common Problems

- Parsing Vulnerabilities
  - Antivirus have to deal with so many file formats that the chances to have more than one security flaw in their parsers are very high
  - Zip, Zip SFX, ARJ, ARJ, SFX, TAR, GZ, ZOO, UUEncode, TNEF, MIME, BINHEX, MSCompress, CAB, CAB SFX, LZH, LZH SFX, LHA, RAR, RAR SFX, JAR, BZ2, Base64, MacBinary, ASPack, CHM, DOC, EML, EXE, FSG, HLP, PDF, Yoda, ELF, PPT, OPD, and much more.
  - If the creators of this filetypes have problems themself parsing them, what are the chances for the antivirus against them all? (scary isn't it?)

Antivirus (In)Security

Common Problems

- 25.07.2007 CA eTrust - Denial of Service Advisory [CHM]
- 23.07.2007 Norman Antivirus - Denial of Service Advisory [DOC]
- 23.07.2007 Norman Antivirus - Detection Bypass Advisory [DOC]
- 23.07.2007 Norman Antivirus - Arbitrary Code Execution Advisory [LZH]
- 23.07.2007 Norman Antivirus - Arbitrary Code Execution Advisory [ACE]
- 20.07.2007 Panda Antivirus - Arbitrary Code Execution [EXE]
- 20.07.2007 ESET NOD32 - Denial of Service [ASPACK+FSG]
- 20.07.2007 ESET NOD32 - Denial of Service [ASPACK]
- 20.07.2007 ESET NOD32 - Arbitrary Code Execution [CAB]
- 04.06.2007 F-Secure Denial of Service [FSG]
- 04.06.2007 F-Secure Denial of Service [ARJ]
- 01.06.2007 F-Secure Remote Code Execution [LZH]
- 30.05.2007 Avira Antivir Infinite Loop [TAR]
- 29.05.2007 Avira Antivir Divide By Zero [UPX]
- 28.05.2007 Avira Antivir Abritary Remote Code Execution [LZH]
- 25.05.2007 Avast! Heap Overflow [SIS]
- 24.04.2007 Avast! Heap Overflow [CAB]

+80 Vunerabilities Reported just by me @30 fixed

Common Problems

- Dangers
  - They mostly reuse their engines in their IPS/IDS
    - This is good though
- Impact
  - Bypass Detection
  - Settings Modificacion
  - DoS
  - Elevation of Privilege
  - Remote Code Execution
  - Whole Network Environment Compromize

Antivirus (In)Security

Common Problems

Common Problems

- Dealing with antivirus companies is not easy
- After the research I've disabled my antivirus, ok, during the research. ;)

Antivirus (In)Security

HUNTING BUGS

Hunting Bugs

- Attack Vectors
  - Any of the previous mentioned
  - Most profitable from the attacker PoV
    - E-Mail embedded files
    - WebSites
    - FTP
    - Instant Message
    - Gateway/Network Traffic (GW/IPS/IDS)
    - Shared Resources
    - USB Storage Devices
    - CD/DVD
    - MemSticks

Hunting Bugs

- Attack Vectors Testing
  - Entry Points Runtime Analysis
    - Wireshark
    - Cdb
    - OllyDbg
    - Dum(b)ug
    - Paimei (win32)
    - vtrace (multiplatform debugging framework)
    - Fuzzer-Framework v1.0, Sysinernals tools, etc
  - Parsers Analysis (idem above – ~~Wireshark~~ + IDA)
  - Fuzzing
    - Peach, Fuzzer-Framework v1.0 (private though)

Hunting Bugs

- Fuzzer-Framework v1.0
  - Fuzzing Engine
    - Customizable structures
    - Support structure recursions
    - Add customized structures on the fly (responses)
    - Function Calls Interception (script on the top of vtrace)
      - Arguments/Return values manipulation in runtime
      - Allows to fuzz virtually (almost) anything
    - Lorcon Interface, and more...
  - Runtime tracing (customed scripts on top of vtrace)
    - Automated tracing
    - Function Calls Hijacking

Antivirus (In)Security

Hunting Bugs

A. Local file header:	
local file header signature	4 bytes (0x04034b50)
version needed to extract	2 bytes
general purpose bit flag	2 bytes
compression method	2 bytes
last mod file time	2 bytes
last mod file date	2 bytes
crc-32	4 bytes
compressed size	4 bytes
uncompressed size	4 bytes
filename length	2 bytes
extra field length	2 bytes
filename	(variable size)
extra field	(variable size)
B. Data descriptor:	
crc-32	4 bytes
compressed size	4 bytes
uncompressed size	4 bytes
C. Central directory structure:	
central file header signature	4 bytes (0x02014b50)
version made by	2 bytes
version needed to extract	2 bytes
general purpose bit flag	2 bytes
compression method	2 bytes
last mod file time	2 bytes
last mod file date	2 bytes
crc-32	4 bytes
compressed size	4 bytes
uncompressed size	4 bytes
filename length	2 bytes
extra field length	2 bytes
file comment length	2 bytes
disk number start	2 bytes
internal file attributes	2 bytes
external file attributes	4 bytes
relative offset of local header	4 bytes
filename	(variable size)
extra field	(variable size)
file comment	(variable size)
end of central dir signature	4 bytes (0x06054b50)
number of this disk	2 bytes
number of the disk with the start of the central directory	2 bytes
total number of entries in the central dir on this disk	2 bytes
total number of entries in the central dir	2 bytes
size of the central directory	4 bytes
offset of start of central directory with respect to the starting disk number	4 bytes
zipfile comment length	2 bytes
zipfile comment	(variable size)

- ZIP (from Pkware)

Antivirus (In)Security

Hunting Bugs

fdt_zip.py (C:\ROOT\In-Progress\fuzzer_framework\fuzzgenerator\datatypes) - GVIM

File Edit Tools Syntax Buffers Window Help

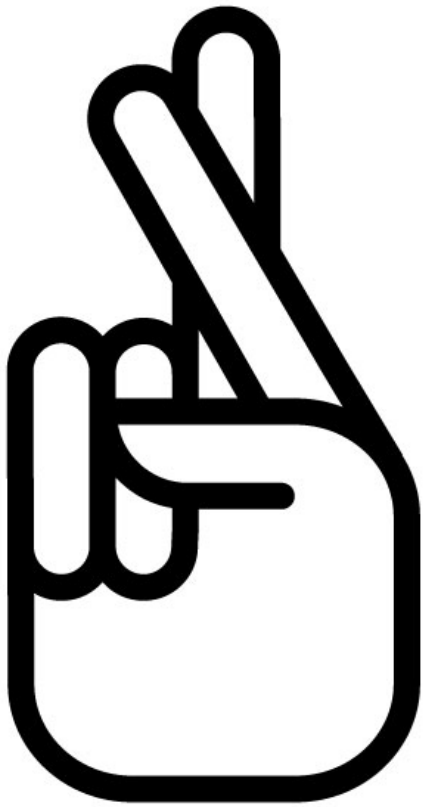
```
# declaracion de datatype 'ZIP'
dtype = [
        # Zip File Header
        ( 'datatype'  : None        , 'default' : b2s('50 4B 03 04')          ,'comments' : 'u4 signature'                },
        ( 'datatype'  : 'int16'     , 'default' : b2s('0A 00')                ,'comments' : 'u2 version'                  },
        ( 'datatype'  : 'int16'     , 'default' : b2s('00 00')                ,'comments' : 'u2 flag'                     },
        ( 'datatype'  : 'int16'     , 'default' : b2s('00 00')                ,'comments' : 'u2 comp method'              },
        ( 'datatype'  : 'int16'     , 'default' : b2s('30 8D')                ,'comments' : 'u2 last mod time'            },
        ( 'datatype'  : 'int16'     , 'default' : b2s('6A 34')                ,'comments' : 'u2 last mod date'            },
        ( 'datatype'  : 'int32'     , 'default' : b2s('DD 7D  D6 B6')         ,'comments' : 'u4 crc-32'                   },
        ( 'datatype'  : 'int32'     , 'default' : b2s('14 00 00 00')          ,'comments' : 'u4 compressed size'          },
        ( 'datatype'  : 'int32'     , 'default' : b2s('14 00 00 00')          ,'comments' : 'u4 uncompressed size'        },
        ( 'datatype'  : 'int16'     , 'default' : b2s('0A 00')                ,'comments' : 'u2 filename lenght'          },
        ( 'datatype'  : 'int16'     , 'default' : b2s('00 00')                ,'comments' : 'u2 extra field length'       },
        # Filename y estra field
        ( 'datatype'  : 'string'    , 'default' : 'prueba.txt'                ,'comments' : 'filename (tama#o variable'   },
        ( 'datatype'  : 'string'    , 'default' : 'esto es una prueba\x0d\x0a' ,'comments' : 'filename (tama#o variable'   },
        # Central directory structure
        ( 'datatype'  : None        , 'default' : b2s('50 4B 01 02')          ,'comments' : 'u4 file signature'           },
        ( 'datatype'  : 'int16'     , 'default' : b2s('14 00')                ,'comments' : 'u2 version'                  },
        ( 'datatype'  : 'int16'     , 'default' : b2s('0A 00')                ,'comments' : 'u2 version needed to extract'},
        ( 'datatype'  : 'int16'     , 'default' : b2s('00 00')                ,'comments' : 'u2 flag'                     },
        ( 'datatype'  : 'int16'     , 'default' : b2s('00 00')                ,'comments' : 'u2 method'                   },
        ( 'datatype'  : 'int16'     , 'default' : b2s('30 8D')                ,'comments' : 'u2 last mod time'            },
        ( 'datatype'  : 'int16'     , 'default' : b2s('6A 34')                ,'comments' : 'u2 last mod date'            },
        ( 'datatype'  : 'int32'     , 'default' : b2s('DD 7D D6 B6')          ,'comments' : 'u4 crc-32'                   },
        ( 'datatype'  : 'int32'     , 'default' : b2s('14 00 00 00')          ,'comments' : 'u4 compressed size'          },
        ( 'datatype'  : 'int32'     , 'default' : b2s('14 00 00 00')          ,'comments' : 'u4 uncompress size'          },
        ( 'datatype'  : 'int16'     , 'default' : b2s('0A 00')                ,'comments' : 'u2 filename length'          },
        ( 'datatype'  : 'int16'     , 'default' : b2s('00 00')                ,'comments' : 'u2 extra field length'       },
        ( 'datatype'  : 'int16'     , 'default' : b2s('00 00')                ,'comments' : 'u2 file comment length'      },
        ( 'datatype'  : 'int16'     , 'default' : b2s('00 00')                ,'comments' : 'u2 disk number start'        },
        ( 'datatype'  : 'int16'     , 'default' : b2s('01 00')                ,'comments' : 'u2 internal file attrib'     },
        ( 'datatype'  : 'int32'     , 'default' : b2s('00 00  00 00')         ,'comments' : 'u4 external file attrib'     },
        ( 'datatype'  : 'int32'     , 'default' : b2s('00 00  00 00')         ,'comments' : 'u4 relative offset of local header' },
        # Filename
        ( 'datatype'  : 'string'    , 'default' : 'prueba.txt'                ,'comments' : 'filename (tama#o variable'   },
        # End of central dir record
        ( 'datatype'  : None        , 'default' : b2s('50 4B 05 06')          ,'comments' : 'u4 end signature'            },
        ( 'datatype'  : 'int16'     , 'default' : b2s('00 00')                ,'comments' : 'u2 number of disk'           },
        ( 'datatype'  : 'int16'     , 'default' : b2s('00 00')                ,'comments' : 'u2 nro of disk of dir'       },
        ( 'datatype'  : 'int16'     , 'default' : b2s('01 00')                ,'comments' : 'u2 total number of entries in disk' },
        ( 'datatype'  : 'int16'     , 'default' : b2s('01 00')                ,'comments' : 'u2 total number of entries in dir' },
        ( 'datatype'  : 'int32'     , 'default' : b2s('38 00 00 00')          ,'comments' : 'u4 size of central dir'      },
        ( 'datatype'  : 'int32'     , 'default' : b2s('3C 00 00 00')          ,'comments' : 'u4 offset of start of central dir' },
        ( 'datatype'  : 'int16'     , 'default' : b2s('FF 00')                ,'comments' : 'u2 zipfile comment length'   },
        ( 'datatype'  : 'string'    , 'default' : 'A'*255                     ,'comments' : 'zipfile comment (tama#o variable)' },
        ( 'datatype'  : ''          , 'default' : ''                          ,'comments' : ''                            )
        ]
```

100,97-132 Bot

Antivirus (In)Security

Demo

- Demos tend to fail

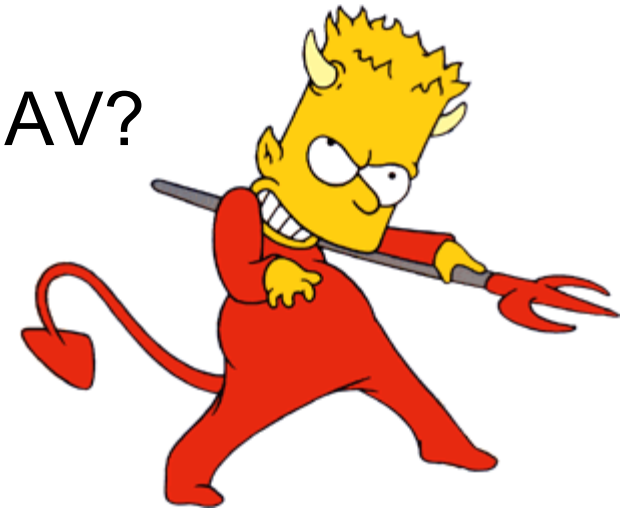


FINAL WORDS

Antivirus (In)Security

A moment of meditation...

- Most Antivirus lack of an Secure Dev Livecycle
  - They need to follow Microsoft steps.
- Worm + BIOS rootkit + PCI rootkits + Firmware rootkits + Virtualization Rootkits ...bad, very bad.
- Are you safe turning on your AV?
- I don't think so..., seriously ;)



Antivirus (In)Security

A moment of meditation...

- This is just the top of the iceberg
  - IPSs/IDSs deal with +100 protocols
- Paradox
  - “The more you Secure yourself the more chances an attacker has to get in”

Antivirus (In)Security

Some Recommendations

- Block Attachments
  - Let the AV scan ONLY the necesary ones
- Apply domain policies to change wrong permitions when possible
  - Registry, Filesystem, etc
- Hear what vendors tell you about their products, but don't believe them
- Conduct a security evaluation before selecting

AV Security Testing Paper

- I'm preparing a WhitePaper with a detailed methodology and tools needed to test the security of AV products that will be released soon

Q/A

Preguntas?

Antivirus (In)Security

Thanks for your time!

Sergio 'shadown' Alvarez
shadown[at]gmail[dot]com
sergio.alvarez[at]nruns[dot]com

References

- Vtrace
  - http://kenshoto.com/vtrace
- Paimei
  - http://paimei.openrce.org
- n.bug
  - http://www.nruns.com/security_tools.php
- Peach Fuzzing Framework
  - http://peachfuzz.sourceforge.net
- SysInternals Tools
  - http://www.sysinternals.com

References

- Dum(b)ug
  - http://www.phenoelit-us.org/fr/tools.html
- Wireshark
  - http://www.wireshark.org
- Windows Debugging Tools
  - www.microsoft.com/whdc/devtools/debugging
- IDA Pro
  - http://www.datarescue.com
- OllyDbg
  - http://www.ollydbg.de