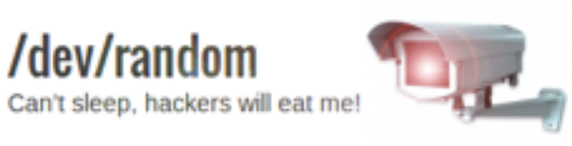
Automatic MIME Attachments Triage

Botconf 2015 - Lightning Talk

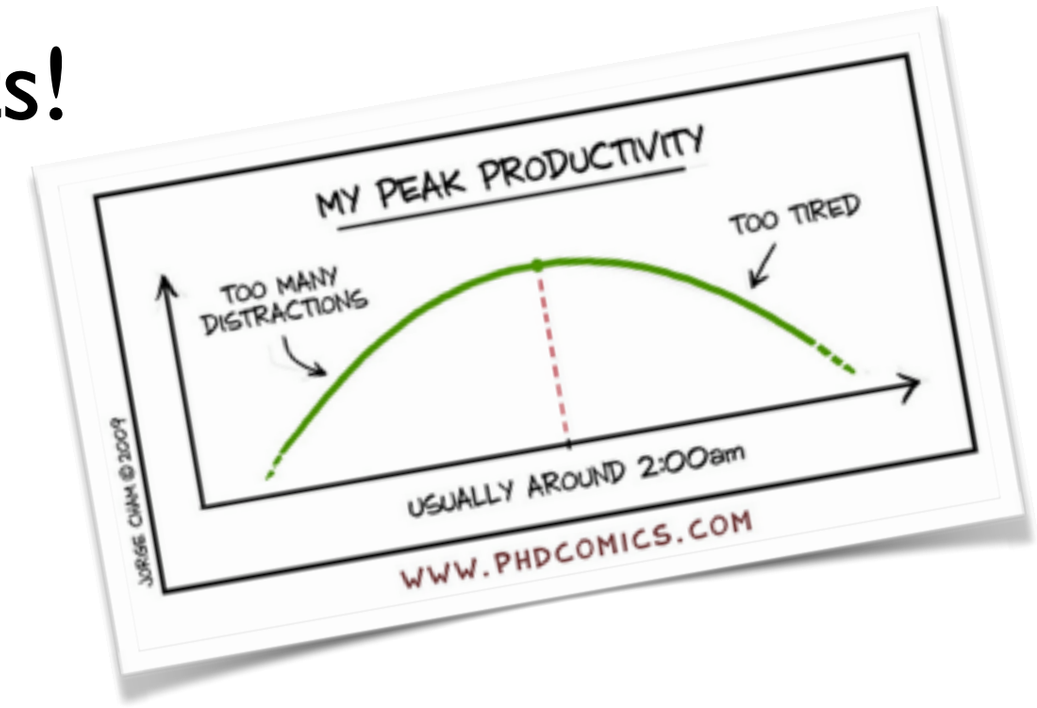
$ cat ~/whoami.xml

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



$ cat ~/.profile

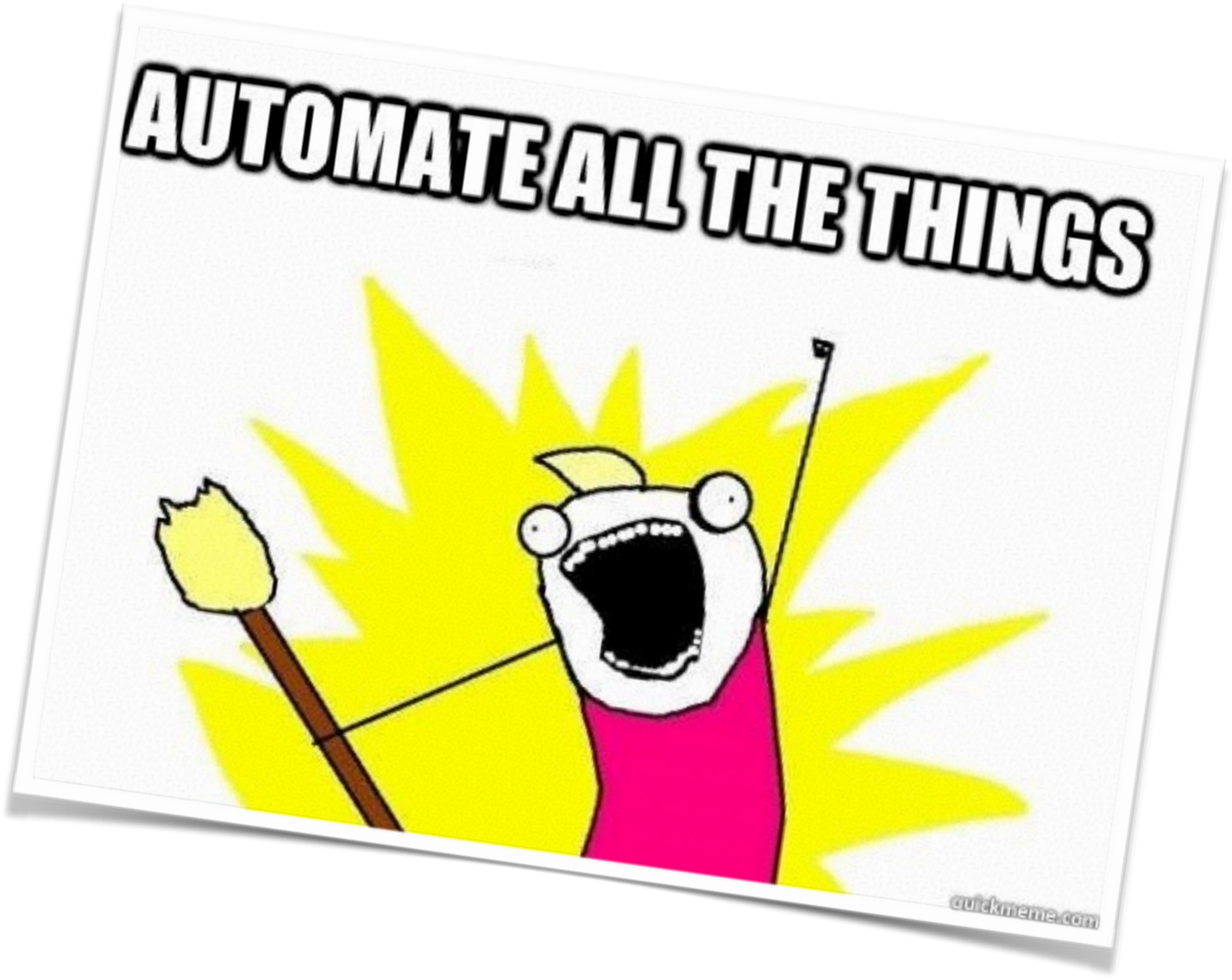
- I like (your) data
- Playing "Active Defense"
- I prefer t-shirts than ties
- I like to play with gadgets!



Problem

- Computers are compromised to join botnets
- Main infection vectors remains:
  - HTTP
  - SMTP
- Huge amount of data to process
- Infosec people needs knowledge
- Infosec people are lazy / don't have time

Solution



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

(*) http://www.decalage.info/python/olevba

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

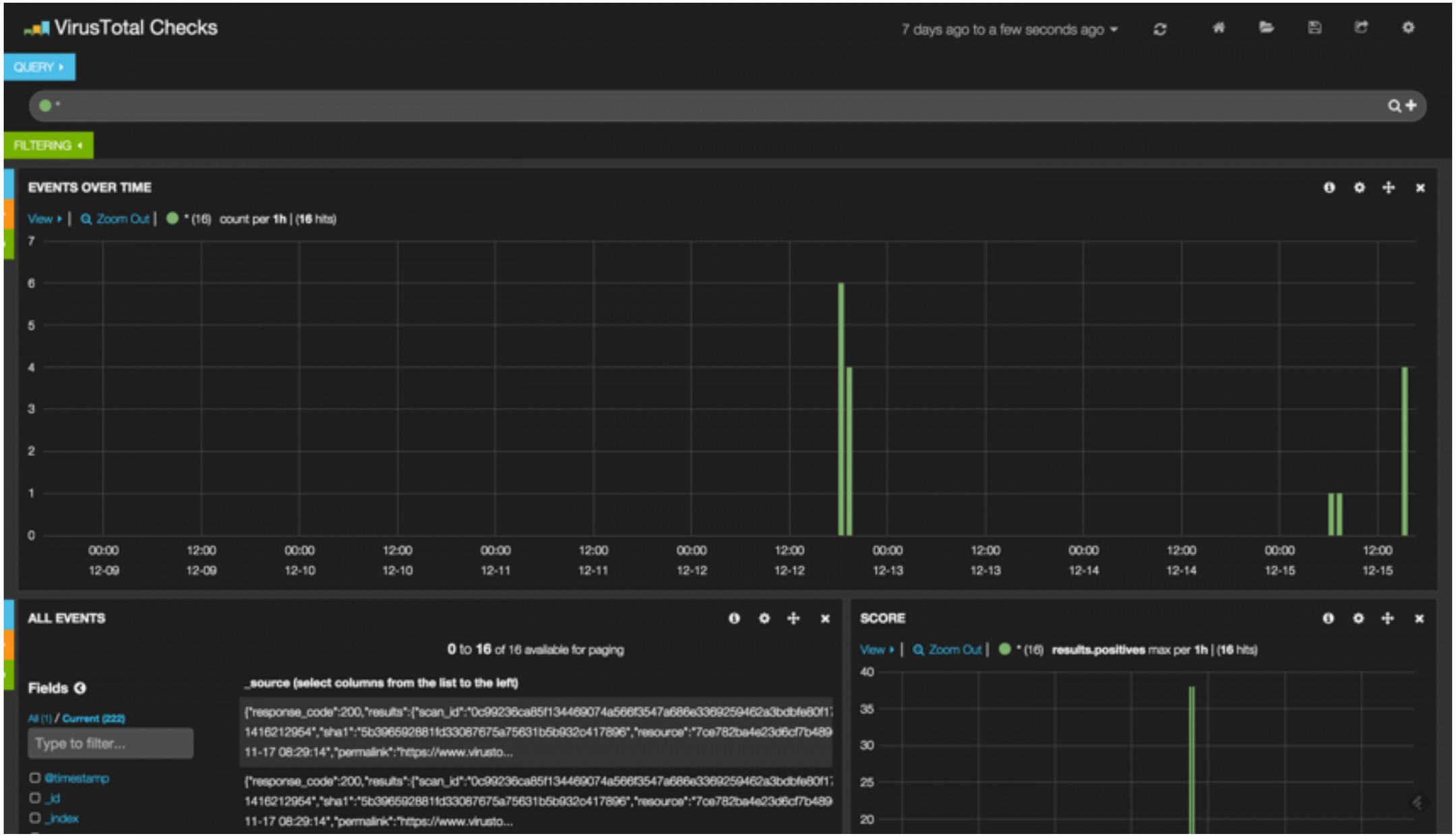
```
$ cat /etc/mime2vt.conf
[virustotal]
apikey: <redacted>
exclude: image/png,image/gif,image/jpeg,image/bmp,text/plain,text/html,text/
english,application/pgp-signature

[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
}
```

Bonus


VirusTotal Checks
7 days ago to a few seconds ago
QUERY
FILTERING
EVENTS OVER TIME
View | Zoom Out | * (16) count per 1h | (16 hits)
7
6
5
4
3
2
1
0
00:00 12-09
12:00 12-09
00:00 12-10
12:00 12-10
00:00 12-11
12:00 12-11
00:00 12-12
12:00 12-12
00:00 12-13
12:00 12-13
00:00 12-14
12:00 12-14
00:00 12-15
12:00 12-15
ALL EVENTS
0 to 16 of 16 available for paging
Fields
All (1) / Current (222)
Type to filter...
@timestamp
_id
_index
_source (select columns from the list to the left)
{"response_code":200,"results":{"scan_id":"0c99236ca85f134469074a566f3547a686e3369259462a3bdbfe80f1
1416212954","sha1":"5b3965928811fd33087675a75631b5b932c417896","resource":"7ce782ba4e23d6cf7b489
11-17 08:29:14","permalink":"https://www.virusto...
{"response_code":200,"results":{"scan_id":"0c99236ca85f134469074a566f3547a686e3369259462a3bdbfe80f1
1416212954","sha1":"5b3965928811fd33087675a75631b5b932c417896","resource":"7ce782ba4e23d6cf7b489
11-17 08:29:14","permalink":"https://www.virusto...
SCORE
View | Zoom Out | * (16) results.positives max per 1h | (16 hits)
40
35
30
25
20

Wanna Play?

https://github.com/xme/mime2vt

Thank you!

@xme

xavier@truesec.be

https://blog.rootshell.be

https://www.truesec.be