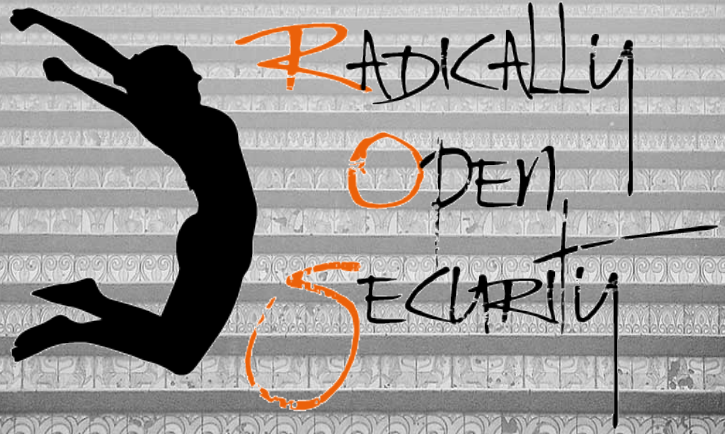
Digitally Aware

Developed by:

Brenno de Winter

Tim Blazytko

Ganesh Rajagopalan



Program

1) Attackers and Attacks
2) Our weaknesses
3) Attacking the systems
4) Reducing risks
5) Round-up

- With hack and solution demo's

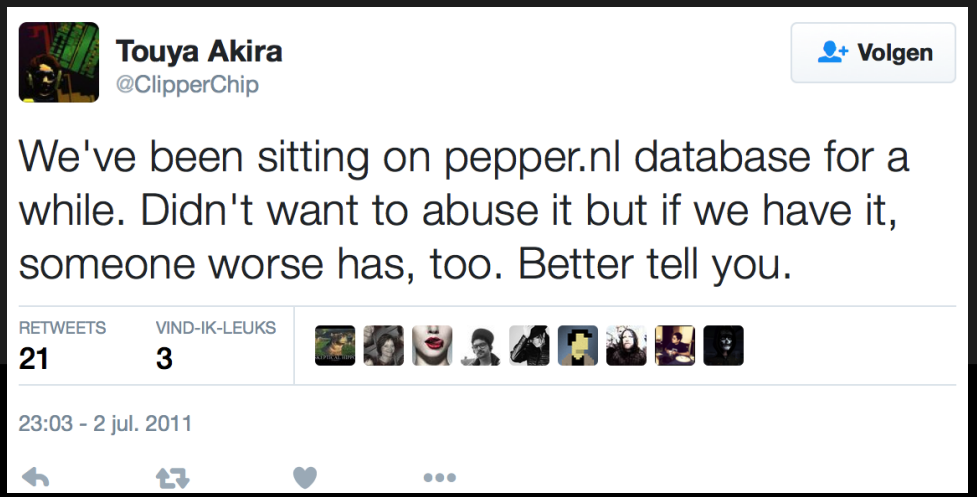
Program

1) **Attackers and Attacks**
2) Our weaknesses
3) Attacking the systems
4) Reducing risks
5) Round-up

- With hack and solution demo's

Pepper.nl

- Information of 54,000 people obtained through hack
- Website is a dating website
- Hacked by AnonymousIRC and placed online
- Many people used work e-mail
- Passwords stolen and tried on other services



E-mail addresses are money

Morocco	11568	Email Addresses	$50 USD
Mozambique	4226	Email Addresses	$50 USD
Myanmar	2540	Email Addresses	$50 USD
Namibia	8514	Email Addresses	$50 USD
Nauru	2393	Email Addresses	$50 USD
Nepal	10602	Email Addresses	$50 USD
Netherlands	932295	Email Addresses	$400 USD
Netherlands Antilles	5654	Email Addresses	$50 USD
New Caledonia	3611	Email Addresses	$50 USD
New Zealand	398340	Email Addresses	$300 USD
Nicaragua	9246	Email Addresses	$50 USD
Niger	12728	Email Addresses	$50 USD
Nigeria	4795	Email Addresses	$50 USD
Niue	51504	Email Addresses	$100 USD
Norfolk Island	1467	Email Addresses	$50 USD
Northern Mariana Islands	5304	Email Addresses	$50
Norway	488707	Email Addresses	$400 USD
Oman	9867	Email Addresses	$50 USD

Forbidden dating

Don't automatically trust companies

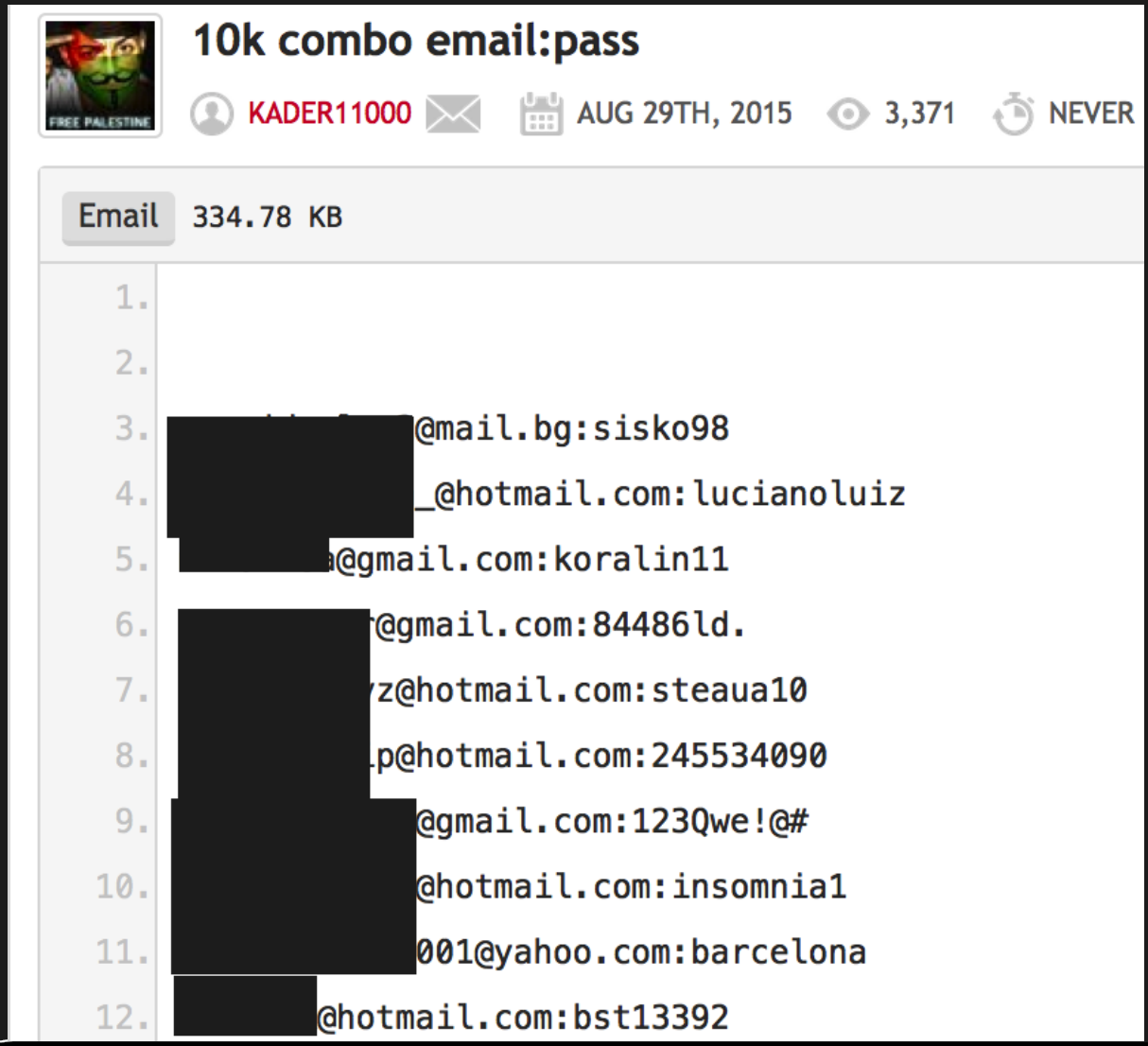
"At this time, we have been able to secure our sites, and close the unauthorized access points. We are working with law enforcement agencies, which are investigating this criminal act. Any and all parties responsible for this act of cyber-terrorism will be held responsible. Using the Digital Millennium Copyright Act (DMCA), our team has now successfully removed the posts related to this incident as well as all Personally Identifiable Information (PII) about our users published online."

Same mistakes again and again

- 'Life is Short, Have an Affair' – Ashley Madison
- 60Gb of company data placed online
- Over 15,000 people use government e-mail address
- 11 million accounts (and passwords!)
- Several people commit suicide

Two ways of disclosing stolen data

- Using:
  - Make it public (Pepper)
  - Place it on the darkweb (Ashley Madison)



Darkweb

- An network within the internet
- Highly anonymous
- With all sorts of services
- Reuse stolen credentials

Email addresses for sale

150K COLORADO US BUSINESS EMAILS FOR **EMAIL** MARKETING

pwoah7foa6au2pul.onion/listing.php?id=91578 **Alphabay**

150K COLORADO US BUSINESS EMAILS FOR **EMAIL** MARKETING BULK **EMAIL** MAILING CPA MARKETING AFFILIATE MARKETING INSTANT DELIVERY

Vendor joseph44trader (0) **Price** ฿0.02393815 **Location** Worldwide

1 MILLION CALIFORNIA US BUSINESS EMAILS FOR **EMAIL** MARKETING

pwoah7foa6au2pul.onion/listing.php?id=91577 **Alphabay**

1 MILLION CALIFORNIA US BUSINESS EMAILS FOR **EMAIL** MARKETING BULK **EMAIL** MAILING CPA MARKETING AFFILIATE MARKETING INSTANT DELIVERY

Vendor joseph44trader (0) **Price** ฿0.07195851 **Location** Worldwide

Accounts for sale

High quality Google **Email** account Gmail Not hacked accept wholesale

pwoah7foa6au2pul.onion/listing.php?id=50321 **Alphabay**

They are not hacked They are fresh and legit Account format **email** password recovery phone number recovery **email** every account is alive I check before sale No policy so far like or replacement

Vendor cashteam (0) **Price** ฿0.00360846 **Location** Worldwide

Hacked UK Amazon Accounts **Email** Access

pwoah7foa6au2pul.onion/listing.php?id=3958 **Alphabay**

This listing is for 1 x unchecked hacked uk amazon account with there **email** access Format of account Amazon Live p m thomas7 gmail com hdle21 CRE 196 **Email** Live p m thomas7 gmail com hdle21 CRE 196 There is no guarantee with these account as of items or content they contain they are picked at random live and none checked I will not replace due to security restricted accounts or any other problems...

Vendor stackcash (416) **Price** ฿0.01202559 **Location** Worldwide

10 x NETFLIX ACCOUNTS **EMAIL** AND PASSWORDS LOGIN PREMIUM LIFETIME

pwoah7foa6au2pul.onion/listing.php?id=114331 **Alphabay**

10 X Netflix login **email** and paswords

Vendor lfullz **Price** ฿0.00473296 **Location** Worldwide

RADICALLY OPEN SECURITY

You can buy anything

Home / Fraud Related / Documents & Data / Dutch ID

Dutch ID

USD 3,328.25

฿ 8.0394

119 in stock

Shipping options

Express Shipping [7 days] [+ USD 50.00]

Quantity: 1

Buy Now

Fake Illinois driver **license** best quality all security features 100

pwoah7foa6au2pul.onion/listing.php?id=73775 **Alphabay**

Fake Illinois driver **license** best quality all security features 100 If you want duplicate copy it is for 50 extra We ship from usa Production and shipping time is 2 days Please send driver **license** details in the order With a link to your photo and a link to your signature You can use postimg And The shipping address you want to recieve your id to All encrypted or in a privnote for security reasons

Vendor EuroBX (328) **Price** ฿0.24010757 **Location** United States

Description

EU - Dutch physical ID.

Or better

FAKE ID NETHERLNDS DRIVING LICENCE

abraxasdegupusel.onion/listing/u59DcF2G1u **Abraxas**

READ THIS ENTIRE LISTING AND OUR PROFILE VERY CAREFULLY BEFORE ORDERING Please be aware that FE Pre Payment is required to order from us and we are a verified vendor here on Abraxas that is allowed to request early finalization This is based upon our previous sales histories on other markets Escrow is not available All prices terms and conditions are absolutely and strictly non negotiable If you are...

Vendor flawlessfakeids (495) **Price** ฿1.6033356 **Location** EU

FAKE ID NETHERLANDS NATIONAL ID PERFECT REPLICA UV AND HOLOGRAM

abraxasdegupusel.onion/listing/Kq29bHPOLQ **Abraxas**

READ THIS ENTIRE LISTING AND OUR PROFILE VERY CAREFULLY BEFORE ORDERING Please be aware that FE Pre Payment is required to order from us and we are a verified vendor here on Abraxas that is allowed to request early finalization This is based upon our previous sales histories on other markets Escrow is not available All prices terms and conditions are absolutely and strictly non negotiable If you are...

Vendor flawlessfakeids (495) **Price** ฿1.6033356 **Location** EU

Full Identity

Complete Australian Identity

nucleuspf3izq7o6.onion...d7e3b3c2bddb403ff177e1b **Nucleus**

This is a complete and functional Australian new identity. It comes with Drivers license Medicare Card Anonymous Sim Card with the same details as identity Activated Fully linked and functional bank card A real and fresh Commonwealth Bank Account with a debit card Fully functional . Payslips and proof of employment Digital book on implementing your new identity. These are all custom made to you and...

Vendor JackOfAllTrades **Price** ฿8 **Location** WW

Walther PPK, Kal.7,65

New and unused!

Product	Price	Quantity
Walther PPK, Kal.7,65	600 EUR = 1.573 ฿	1 X Buy now
Ammo, 50 Rounds	40 EUR = 0.105 ฿	1 X Buy now

Hitman Network - Hire real killers with bitcoin, the only true hitman site on the deep web

Products FAQs Register Login

Hitman Network

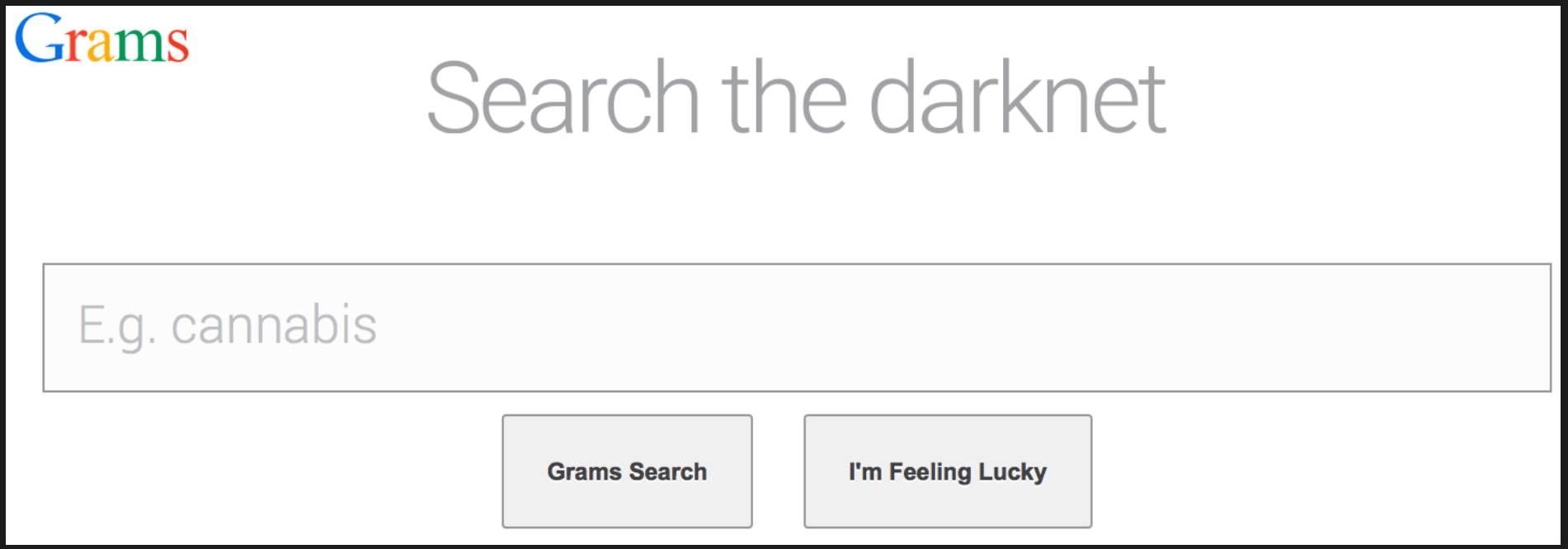
We are a team of 3 contract killers working in the US (+Canada) and in the EU.
Once you made a "purchase" we will reply to you within 1-2 days, contract will be completed within 1-3 weeks depending on target.

Only rules: no children under 16 and no top 10 politicians.

Product	Price	Quantity
We kill your target in the USA/Canada	16.392 ฿	1 X Buy now
We kill your target in the European Union	19.671 ฿	1 X Buy now

RADICALLY OPEN SECURITY

Searching the darknet



10G Ketamine 83 The Best From The Dutch

pwoah7foa6au2pul.onion/listing.php?id=113241 **Alphabay**

Pure Ketamine labtested 83 **dutch** made strong stuff so use with care

Vendor GlobalStore **Price** ฿0.59312748 **Location** Netherlands

5g Dutch Speed

pwoah7foa6au2pul.onion/listing.php?id=94750 **Alphabay**

Top quality **Dutch** Speed Product is dried powder Free Express Shipping

Vendor AngelTech (44) **Price** ฿0.15683814 **Location** Australia

NEW PROMO MDMA Dutch primo 1 gram

pwoah7foa6au2pul.onion/listing.php?id=66918 **Alphabay**

Dutch MDMA just as you know it High quality big stones as you can see in the picture

Vendor VivaLaResistance **Price** ฿0.03872842 **Location** Netherlands

(0)

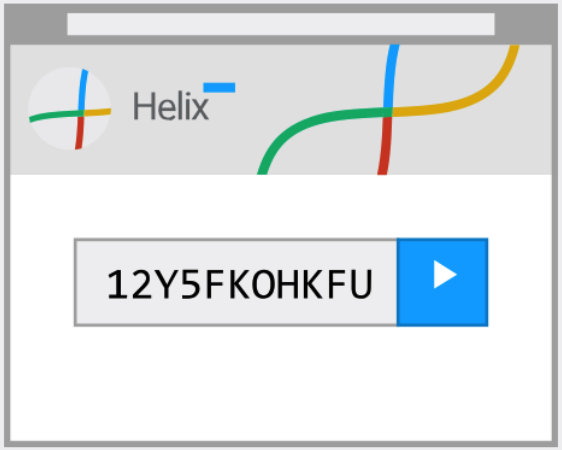
Clearing money

How Helix light works

Enter your Bitcoin address in the box above

Send your dirty coins to the Helix address

New, clean coins sent to your Bitcoin address



DigiNotar

- Digital Certificate Provider
  - Certifies the certificates with HTTPS
  - Prob. Iranian attack against NL
- Important

WHO

Who will do this?

- Those that seize the opportunity
  - People that stumble across an error and exploit it
  - Automated hacking tools for known weaknesses
  - People that read a trick and try it out

Who will do this?

- Those that attack professionally
  - Standard tools for standard leaks
  - Automated hacking tools for known weaknesses
  - Attackers that write their own hacking tools
  - Attackers that make an hack a serious project

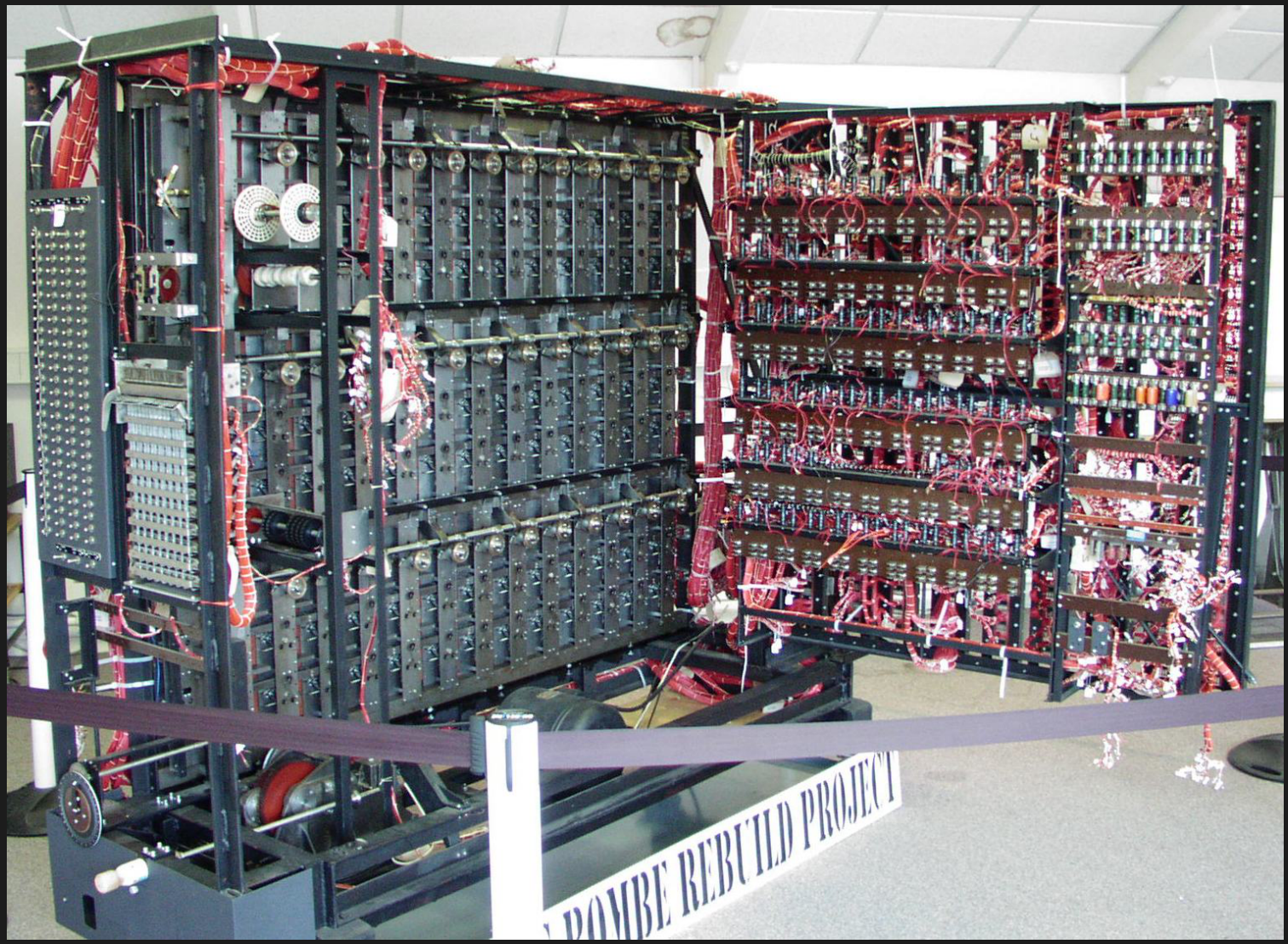
Types of attackers

Attacker	Description	Investment in attacking
Script kiddies	Use standard tools for hacking and sometimes are unaware of the consequences. Low skills.	Little
Cybercriminal	Make a living from digital crime. Lowly skilled to very knowledgeable and professional attackers.	Little to High
Scammers	Trying to lure people in (often financial) scams. Focus mainly on social engineering	Little to average
(H)Acitivists	Attacking for a (political) cause. Lowly skilled to very skilled.	Sometimes little to huge
Corporate spies	Attacking for financial gain (economic espionage). Often with huge funds and very skilled	High
Intelligence Agencies	Attacking for national interests (fighting terror, crime and economical reasons). Very skilled en very well equipped. Often have a lot of time	Very high
Malicious Insider	Helping outside attackers obtain what they want. If working in the right position little knowledge is needed only the right attributions	Relatively little

Not all hackers are evil

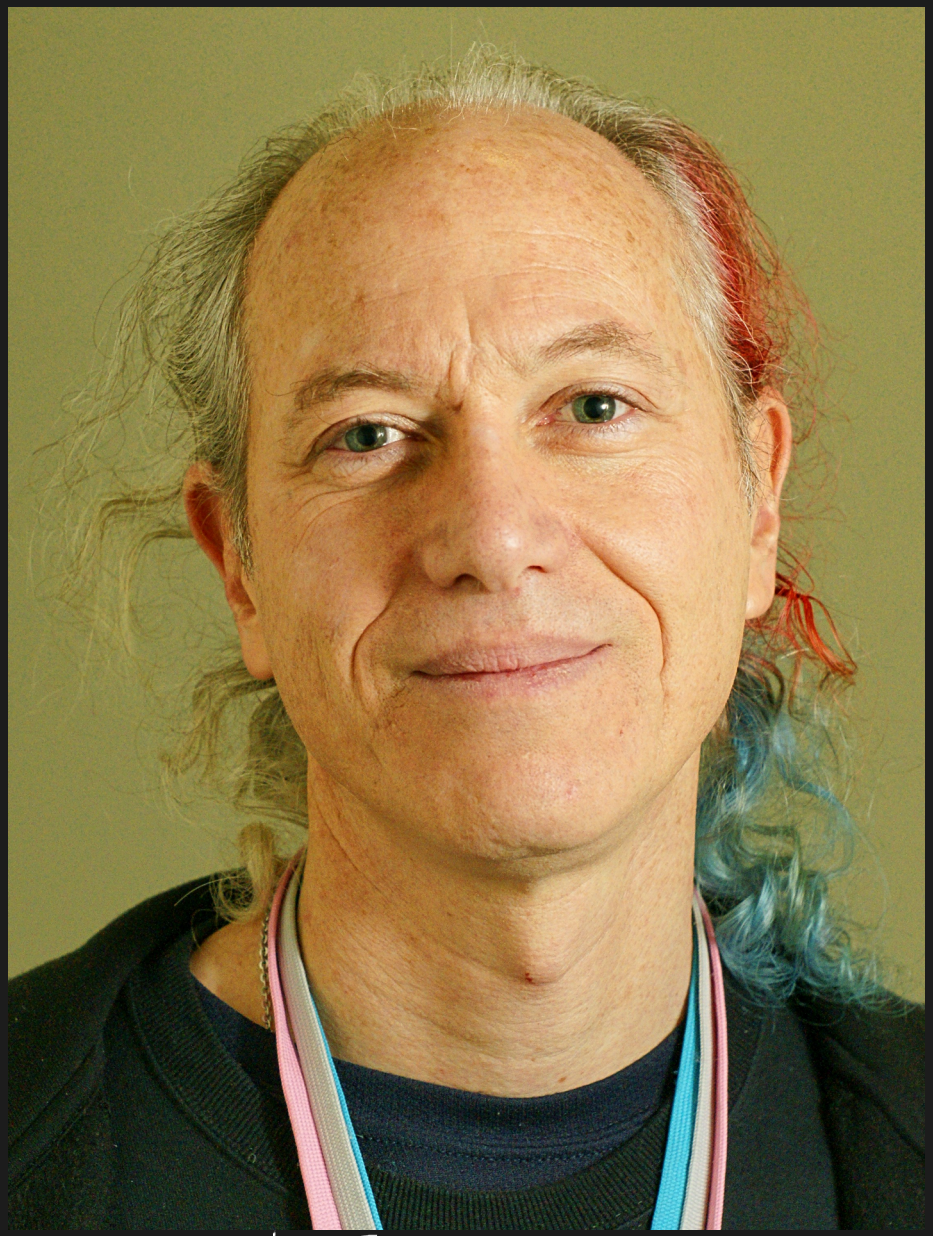
- Many of them build cool software
- Crack codes and save lives
- Just discover the functioning of systems
- Give out important warnings

Alan Turing



Jon Lech Johansen

Mitch Altman



WHY

Motives – 'Fun'

- Hacking is fun
  - The thrill of finding flaws and being 'grey'
  - The fun of making systems better, social involvement
  - The excitement of understanding systems
  - The thrill of 'being' cool
  - Trolling

Motives – Fun - fake

OV-chipkaartdiscounter.nl

The Lack Rack

Culture

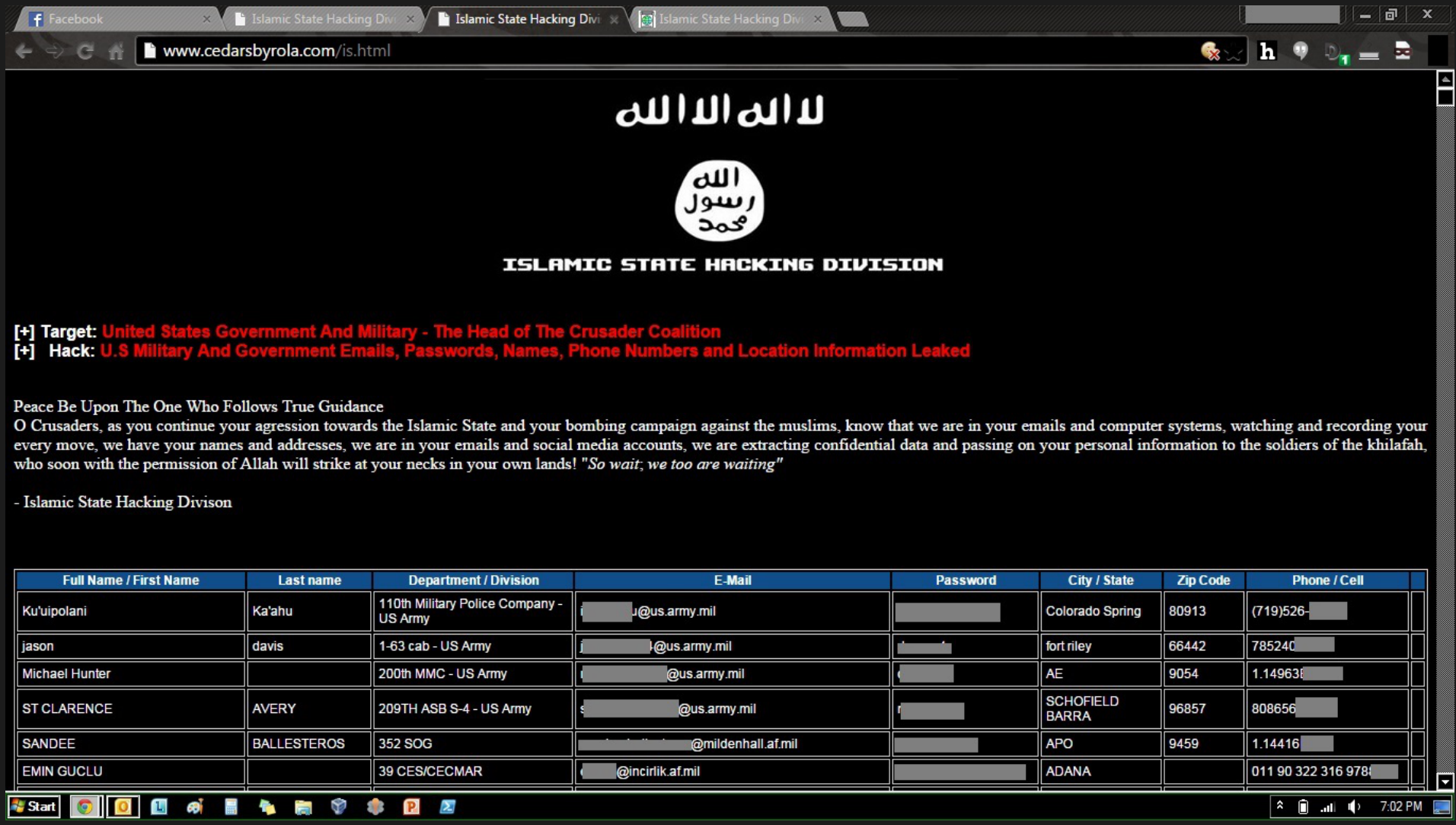

DER PRICKELNDE MATE-EISTEE
CLUB-MATE
Fischer-Pschorr
DER PRICKELNDE MATE-EISTEE
CLUB-MATE
Fischer-Pschorr


CLUB-MATE

Motives - Conviction

Nationaal Archief

Motives - conviction



لا اله الا الله

ISLAMIC STATE HACKING DIVISION

[+] Target: United States Government And Military - The Head of The Crusader Coalition
[+] Hack: U.S Military And Government Emails, Passwords, Names, Phone Numbers and Location Information Leaked

Peace Be Upon The One Who Follows True Guidance
O Crusaders, as you continue your agression towards the Islamic State and your bombing campaign against the muslims, know that we are in your emails and computer systems, watching and recording your every move, we have your names and addresses, we are in your emails and social media accounts, we are extracting confidential data and passing on your personal information to the soldiers of the khilafah, who soon with the permission of Allah will strike at your necks in your own lands! "*So wait; we too are waiting*"

- Islamic State Hacking Divison

Full Name / First Name	Last name	Department / Division	E-Mail	Password	City / State	Zip Code	Phone / Cell
Ku'uipolani	Ka'ahu	110th Military Police Company - US Army	[redacted]@us.army.mil	[redacted]	Colorado Spring	80913	(719)526-[redacted]
jason	davis	1-63 cab - US Army	[redacted]@us.army.mil	[redacted]	fort riley	66442	785240[redacted]
Michael Hunter		200th MMC - US Army	[redacted]@us.army.mil	[redacted]	AE	9054	1.14963[redacted]
ST CLARENCE	AVERY	209TH ASB S-4 - US Army	[redacted]@us.army.mil	[redacted]	SCHOFIELD BARRA	96857	808656[redacted]
SANDEE	BALLESTEROS	352 SOG	[redacted]@mildenhall.af.mil	[redacted]	APO	9459	1.14416[redacted]
EMIN GUCLU		39 CES/CECMAR	[redacted]@incirlik.af.mil	[redacted]	ADANA		011 90 322 316 978[redacted]

Start 7:02 PM

RADICALLY OPEN SECURITY

Wiki Commons

Motives - Finance

ICS VISA MasterCard
INTERNATIONAL CARD SERVICES

Rabobank
Aan: [redacted]
Antwoord aan: rabo@diensten.nl
Uw betaalpas wordt over 2 weken geblokkeerd

Uw rekeningoverzicht bekijken en betalen

Geachte kaarthouder,

Uw rekeningoverzicht van de ICS Card van de afgelopen maand is weer beschikbaar. U kunt dit overzicht bekijken en uw rekening betalen via Mijn Account op https://www.icscards.nl/ics/login.

De ICS Card-rekening betalen

- U hebt 21 dagen de tijd om uw rekening te betalen (gerekend vanaf de datum op het rekeningoverzicht).
- U kunt uw rekening betalen via Mijn Account. Betaalt u uw rekening per automatische incasso, dan hoeft u uiteraard niets te doen.
- Wanneer u ingelogd bent op Mijn Account ziet u in het tabblad 'Rekeningen' wanneer u het minimaal te betalen bedrag uiterlijk dient te voldoen.

Betaal op tijd, zo voorkomt u een betalingsachterstand en extra kosten.

Direct inloggen op Mijn Account

Met vriendelijke groet,

International Card Services BV
Postbus 23225, 1100 DS Diemen
KvK Amsterdam nr. 33.200.596

Motives - Finance

EFF

Hello,

I am pleased to inform you that that based on your professional background that you have been invited apply for inclusion into the International Society of Business Leaders network. Our research department nominates potential candidates based on a variety of factors such as your current professional standing, recent accomplishments, honors/awards, published articles, as well as information present on authoritative media outlets, social networks, and professional directories.

I believe that you would make a fitting addition to our premier network of leading professionals, and therefore encourage you to apply for inclusion by completing your application here, or by clicking the button below. There is no cost to apply or to be included.

APPLY NOW TO JOIN THE ISoBL

Sincerely,

The ISoBL
Managing Director, Research & Selection Department

Motives - Finance

MICROSOFTX CORPORATION

Antwoord aan: microsoftclaim2016@163.com

Winning No: MSFT/5975/107/2016

MICROSOFT® CORPORATION
Cardinal Place
80-100 Victoria Street
London,SW1E 5JL
United Kingdom

Winning No: MSFT/5975/107/2016
Ticket No: MSFT/3081/039/2016

MICROSOFT YEARLY ANNIVERSARY WINNING NOTIFICATIO

VERIFICATION AND FUNDS RELEASE FORM

(1) Your Contact Address/Private Email Address:
(2) Your Tel/Fax Numbers:
(3) Your Nationality/Country:
(4) Your Full Name:
(5) Occupation/Company:
(6) Age/Gender:
(7) Ever Won An Online Lottery?
(8) Comments about Microsoft:

Philippa Snare
Chief Marketing Officer, Microsoft UK
E-mail: microsoftclaim2016@163.com
Fax No: +44 8447 749 891

RADICALLY OPEN SECURITY

Motives - Warfare

Program

1)Attackers and Attacks

2)Our weaknesses

3)Attacking the systems

4)Reducing risks

5)Round-up

Human weakness

- We have human weaknesses:
  - We're generally nice, helpful people
  - We hate complexity so:
    we're bad in passwords
  - We see the physical world as digitally irrelevant
- This problem can be fixed with different behavior

Your immediate response is needed

JAMES B. COMEY
FBI DIRECTOR

Social Engineering

- Using the weakest link: us with psychology
  - Going after curiosity
  - Going after sympathy
  - Greed
  - Scaring people

United Nations

Antwoord aan: pamelayoughzenith@gmail.com

YOUR CONTRACT/INHERITANCE FUND

OFFICE OF THE PRESIDENT
FEDERAL REPUBLIC OF NIGERIA
FROM THE DESK OF: DR REUBEN ABATI
(PRESIDENTIAL SPOKESMAN)
OUR REF NO: 000991/FRN/7535/2014 REF: FRN/OHG/OXD2/2014
TEL DIRECT: +234-814-982-2801

ATTENTION: BENEFICIARY

RADICALLY OPEN SECURITY

Many forms and shapes

- Pretexting / Quid Pro Quo
- Phishing / IVR Phone phishing
- Baiting
- Tailgaiting

Using a fake ID-card for everything

VIDEO

Often advanced

- Use paper, e-mailadresses or phonenumbers that check out
- Using knowledge of organizations
- Some stories sound very consistent

Passwords

- Worst passwords in 2015, Top 15: 123456, password, 12345678, qwerty, 12345, 123456789, football, 1234, 1234567, baseball, welcome, 1234567890, abc123, 111111
- Internet of Things with default or no password
- Automated tests for passwords

Passwords

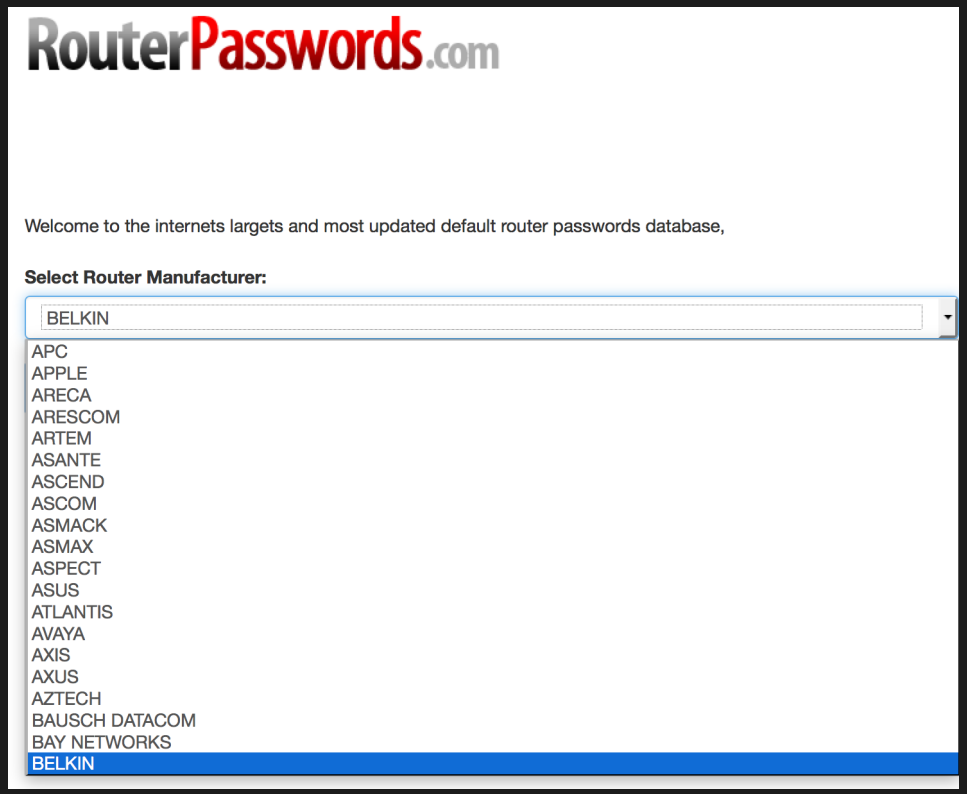
- All 11,000,000 passwords of Ashley Madison were hacked
- '123456' and 'password' were most popular

Psyomjesus

Automated password crackers

```
$john passwd
Created directory /home/ros/.join
Loaded 5 password hashed with 5 different salts (Traditional DES [64/64 BS MMX])
12345          (root)
password       (noot)
P@ssw0rd       (mies)
secret         (aap)
```

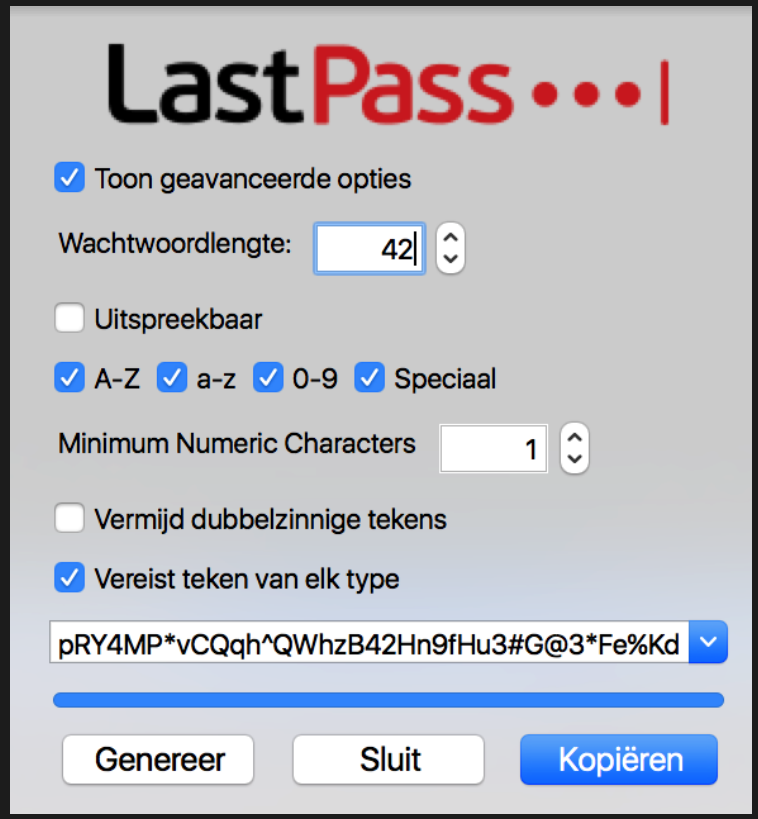
Online lists of default passwords...



admin	admin
admin	admin
307565	fxyNblIQCKRMF
admin	rainbow
PHANTOM	
DS	
DSA	
DESQUETOP	
ADMN	admn
GEN1	gen1
GEN2	gen2
NiLmXyno	RIIKHvAXQKoxoQyR
Wpgbdneq	KCcFcOKaWt
none	sysadm
n/a	sysadm
admin	hello
Admin	admin1
admin	changeme
admin	changeme

What helps

- Different passwords everywhere
  - Twitter, Facebook, Google
  - Government logins
  - Banks
- Better, stronger passwords
  - Use password vaults
  - Use longer texts

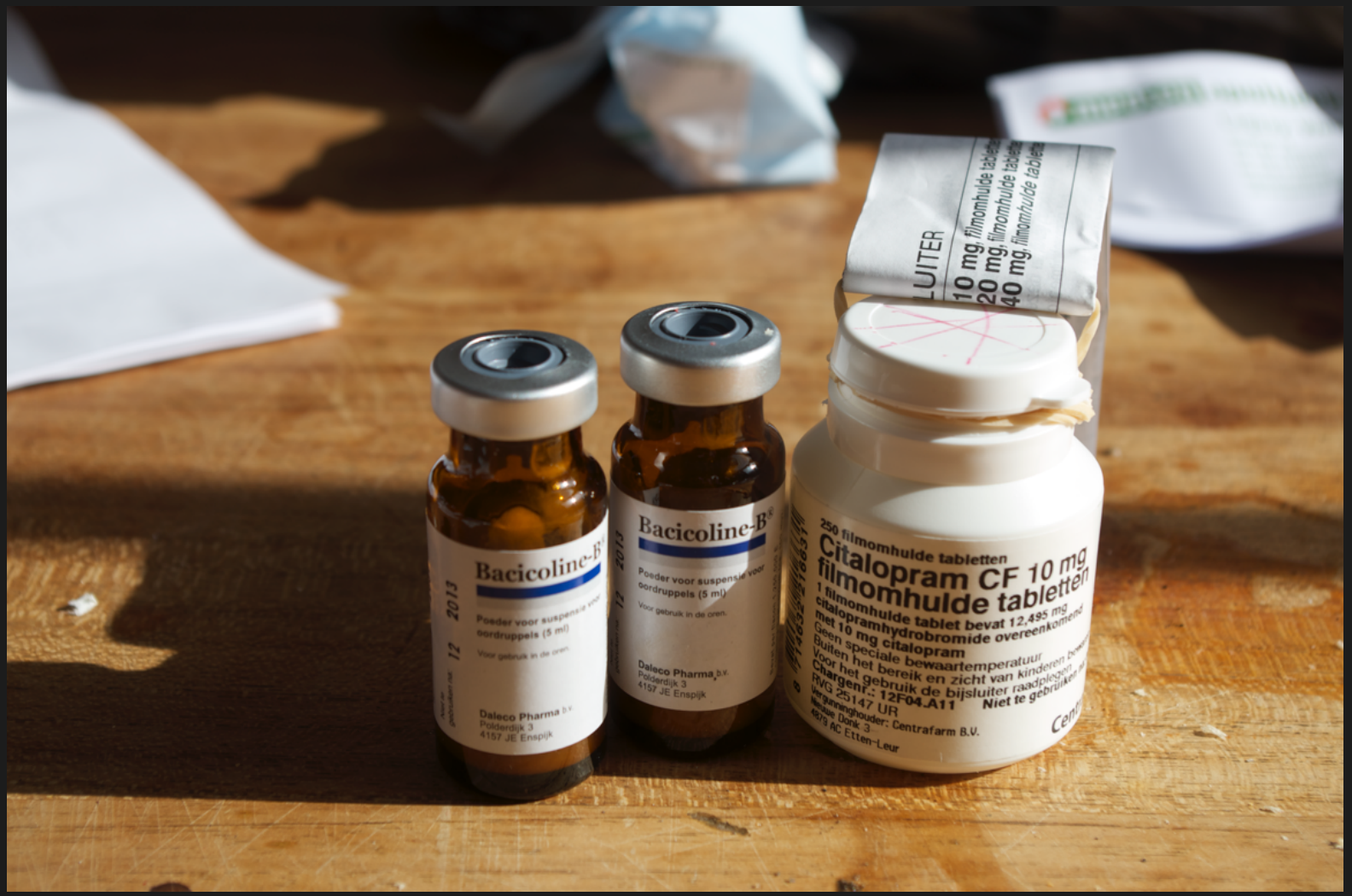


RADICALLY OPEN SECURITY

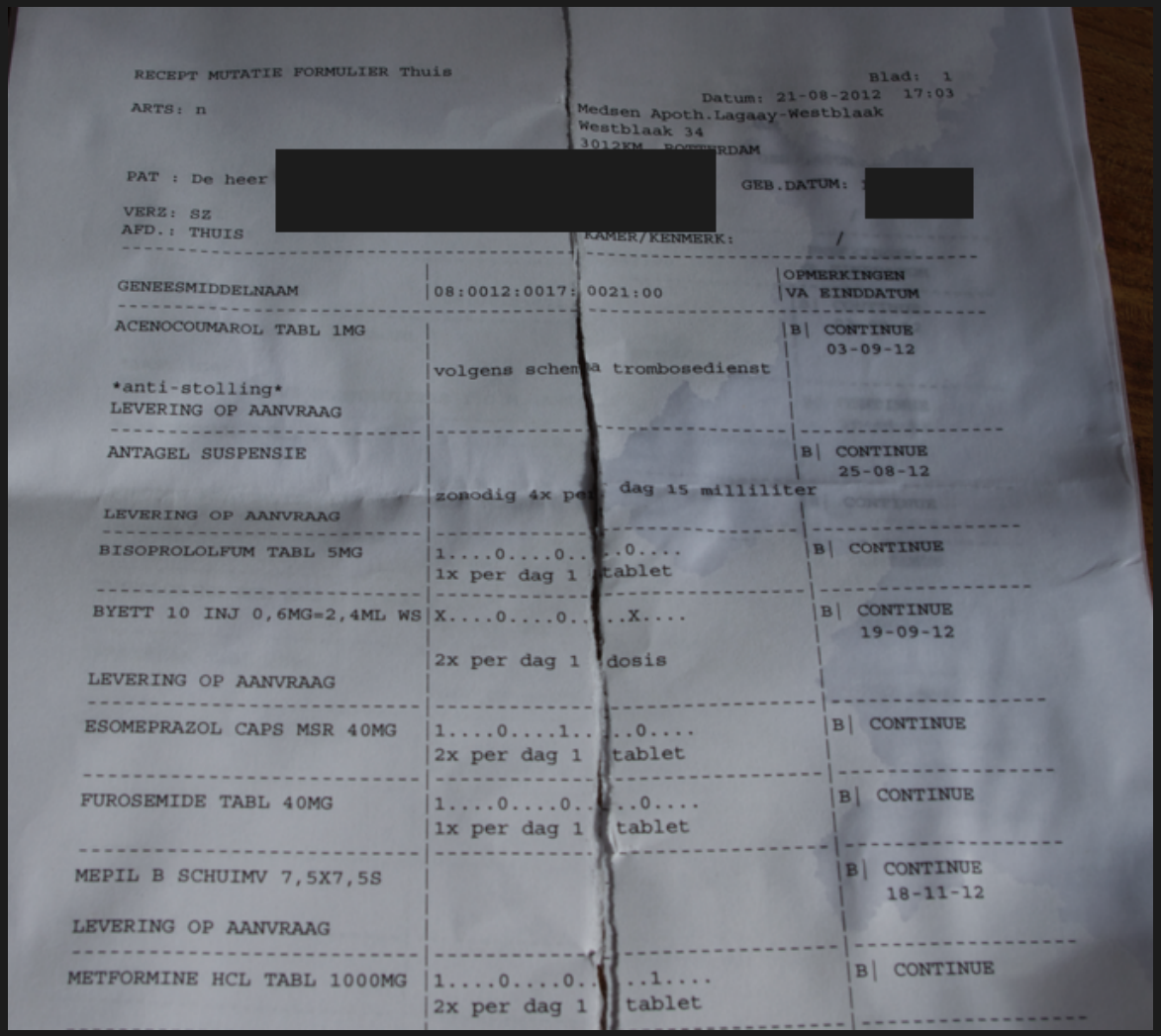
Dumpster diving

Throw away the party

Those returned medicine



And the medication list...



RECEPT MUTATIE FORMULIER Thuis

Blad: 1

ARTS: n

Datum: 21-08-2012 17:03

Medsen Apoth.Lagaay-Westblaak
Westblaak 34
3012KM ROTTERDAM

PAT : De heer [redacted] GEB.DATUM: [redacted]

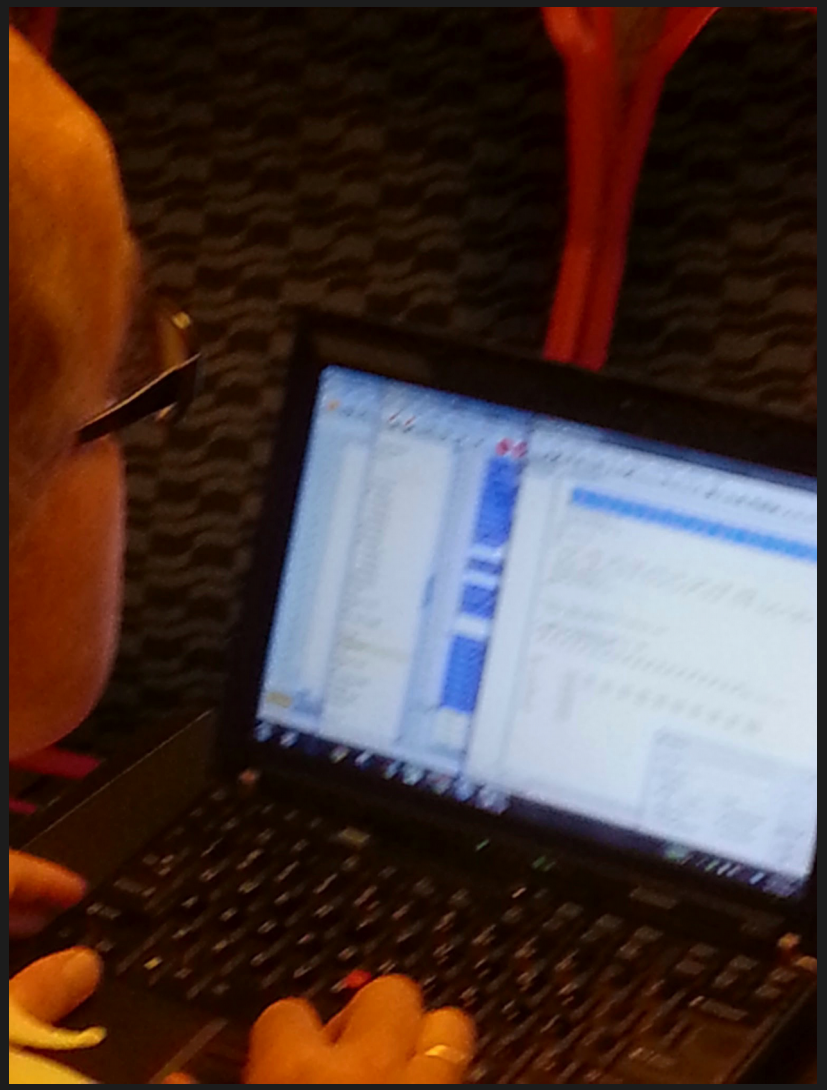
VERZ: SZ
AFD.: THUIS

KAMER/KENMERK: /

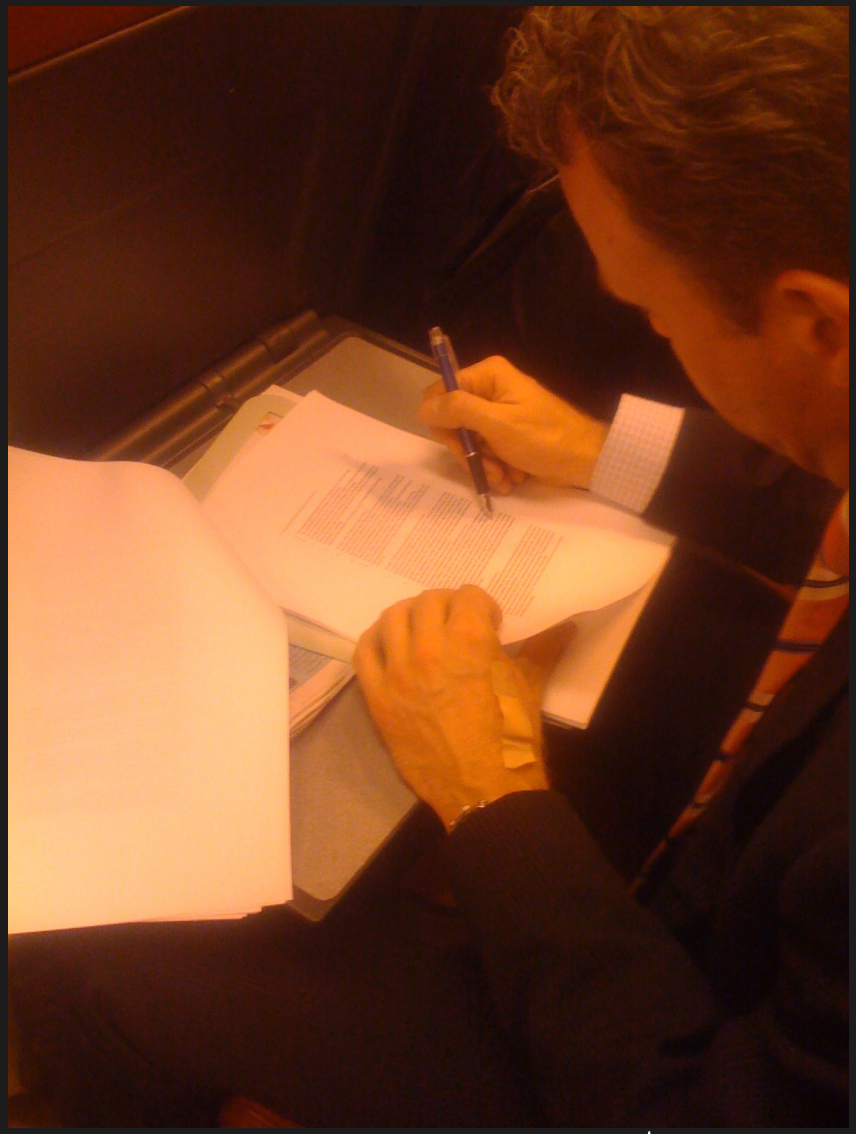
GENEESMIDDELNAAM	08:0012:0017:	0021:00	OPMERKINGEN VA EINDDATUM
ACENOCOUMAROL TABL 1MG *anti-stolling* LEVERING OP AANVRAAG	volgens schem	a trombosedienst	B CONTINUE 03-09-12
ANTAGEL SUSPENSIE LEVERING OP AANVRAAG	zonodig 4x pe	dag 15 milliliter	B CONTINUE 25-08-12
BISOPROLOLFUM TABL 5MG	1....0....0.. 1x per dag 1	..0.... tablet	B CONTINUE
BYETT 10 INJ 0,6MG=2,4ML WS LEVERING OP AANVRAAG	X....0....0.. 2x per dag 1	..X.... dosis	B CONTINUE 19-09-12
ESOMEPRAZOL CAPS MSR 40MG	1....0....1.. 2x per dag 1	..0.... tablet	B CONTINUE
FUROSEMIDE TABL 40MG	1....0....0.. 1x per dag 1	..0.... tablet	B CONTINUE
MEPIL B SCHUIMV 7,5X7,5S LEVERING OP AANVRAAG			B CONTINUE 18-11-12
METFORMINE HCL TABL 1000MG	1....0....0.. 2x per dag 1	..1.... tablet	B CONTINUE

Physical Risks

- Showing off sensitive documents
- Showing off sensitive sessions on laptops
- Having loud telephone conversations in public

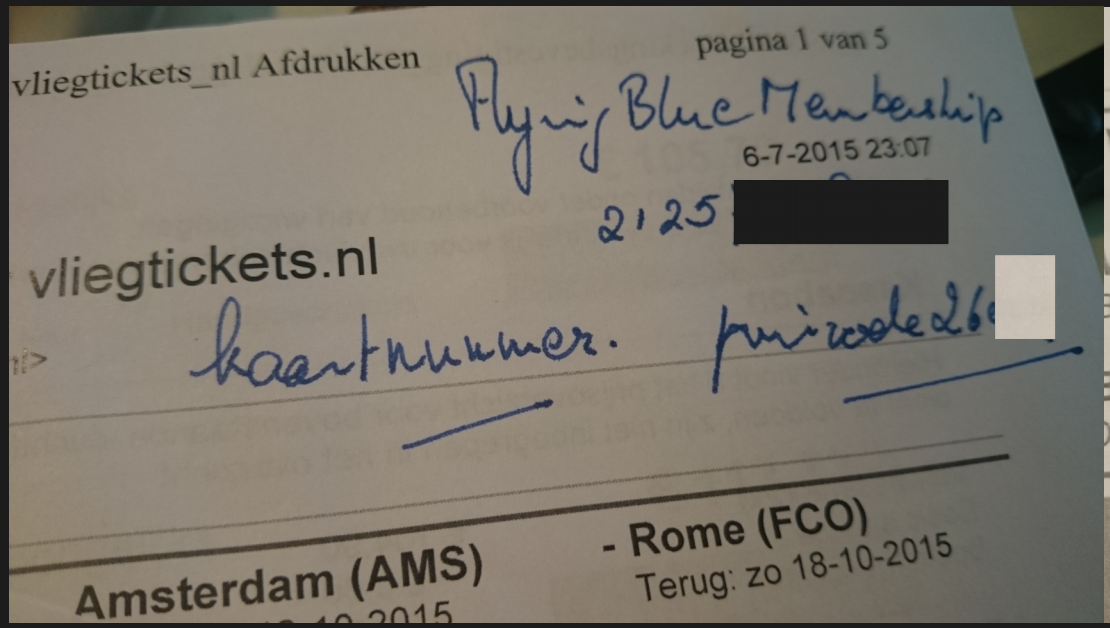


Physical Risks



- Using public computers for sensitive work
- Connecting cell phones to untrusted sources
- Abuse of physical documents – dumpster diving

Leaving some travell documents...



Free Powerrr!

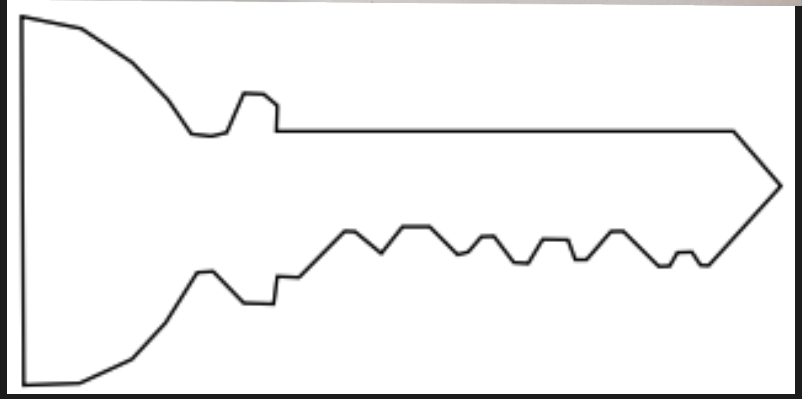
NEVER LEAVE YOUR PHONE OR TABLET UNATTENDED IN A STRANGE PLACE!

EVER!

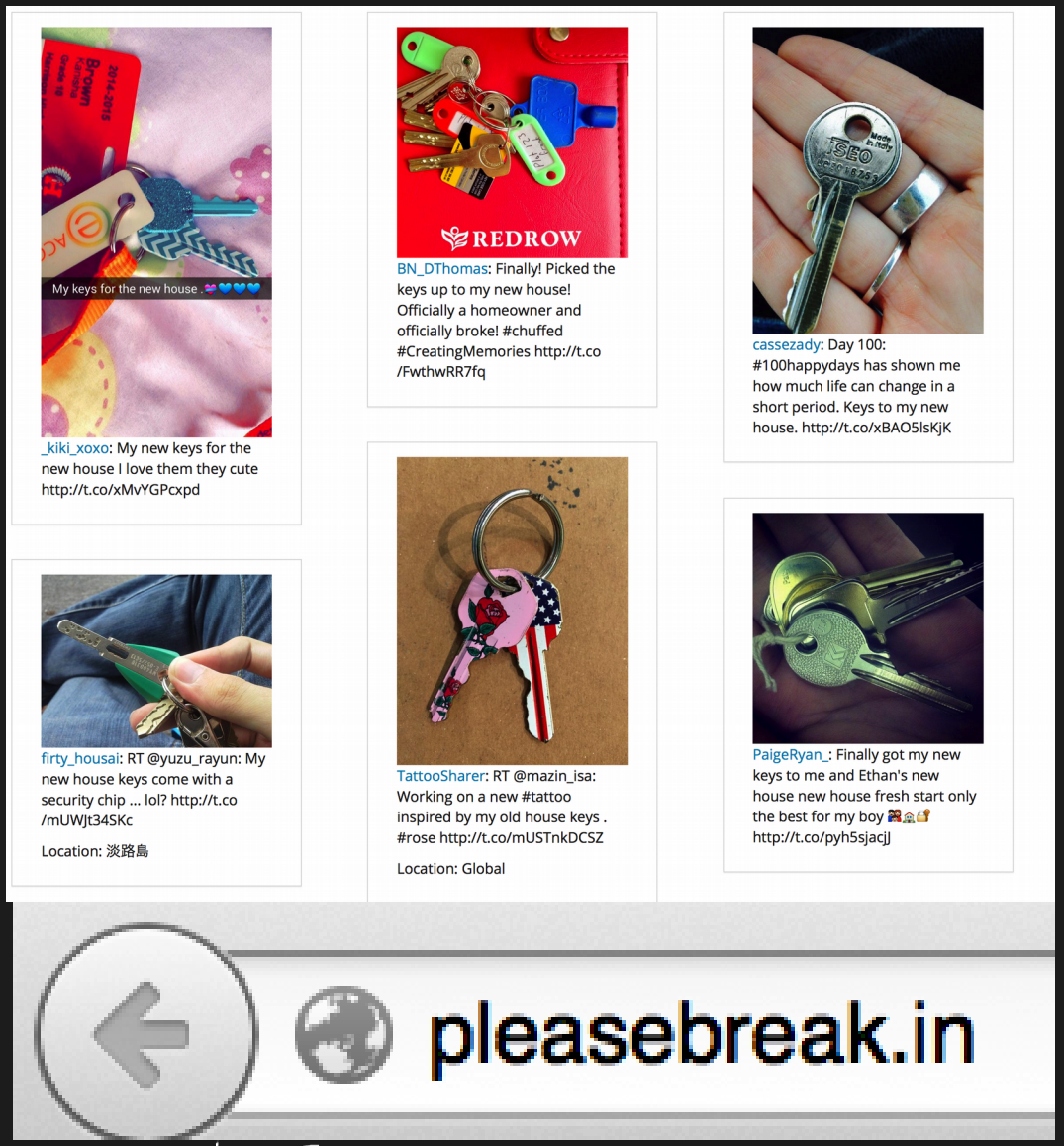
RADICALLY OPEN SECURITY

Free & Safe Powerrr!

Pictures of keys are fun!



Pictures of keys are fun!



_kiki_xoxo: My new keys for the new house I love them they cute http://t.co/xMvYGPcxpd

BN_DThomas: Finally! Picked the keys up to my new house! Officially a homeowner and officially broke! #chuffed #CreatingMemories http://t.co/FwthwRR7fq

cassezady: Day 100: #100happydays has shown me how much life can change in a short period. Keys to my new house. http://t.co/xBAO5lsKjK

firty_housai: RT @yuzu_rayun: My new house keys come with a security chip ... lol? http://t.co/mUWJt34SKc

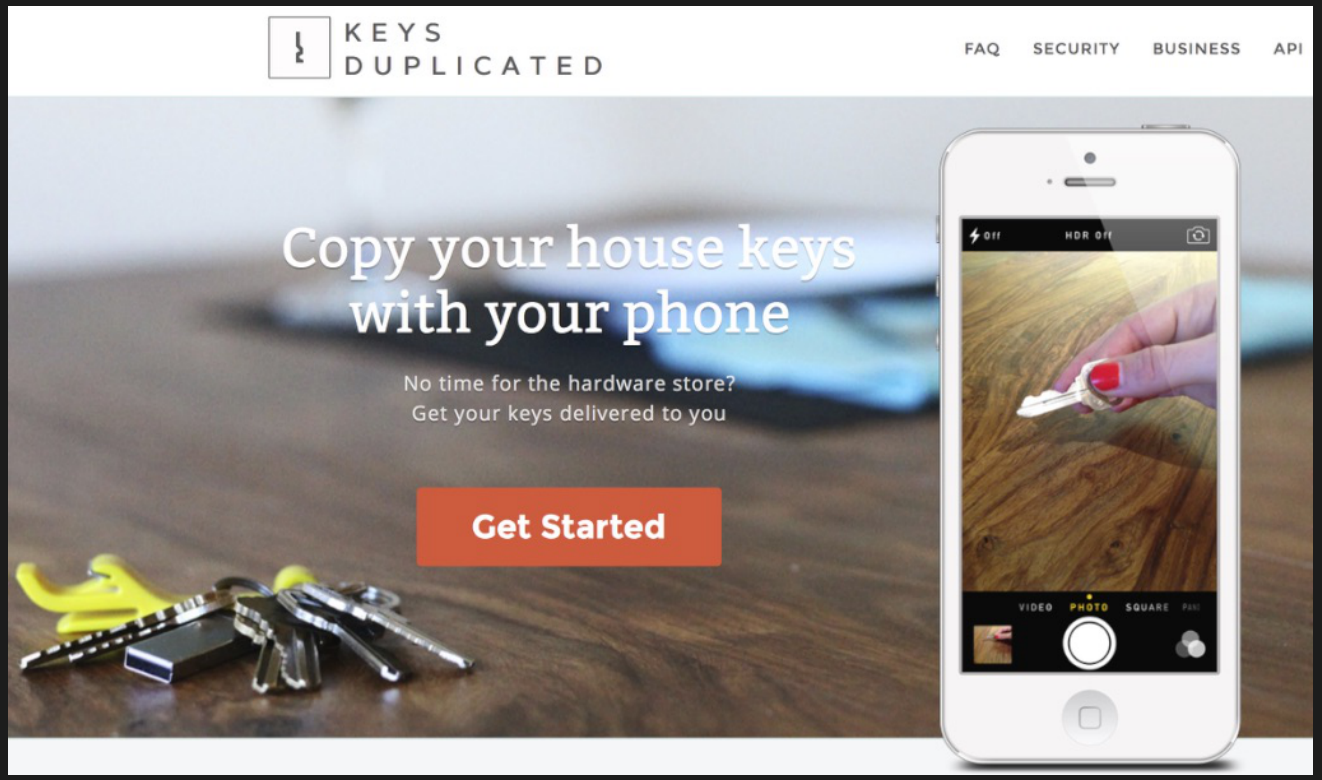
Location: 淡路島

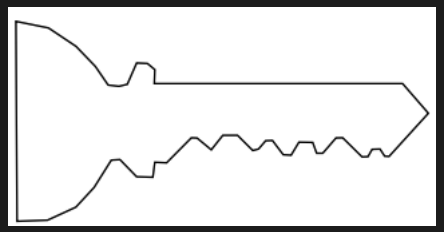
TattooSharer: RT @mazin_isa: Working on a new #tattoo inspired by my old house keys . #rose http://t.co/mUSTnkDCSZ

Location: Global

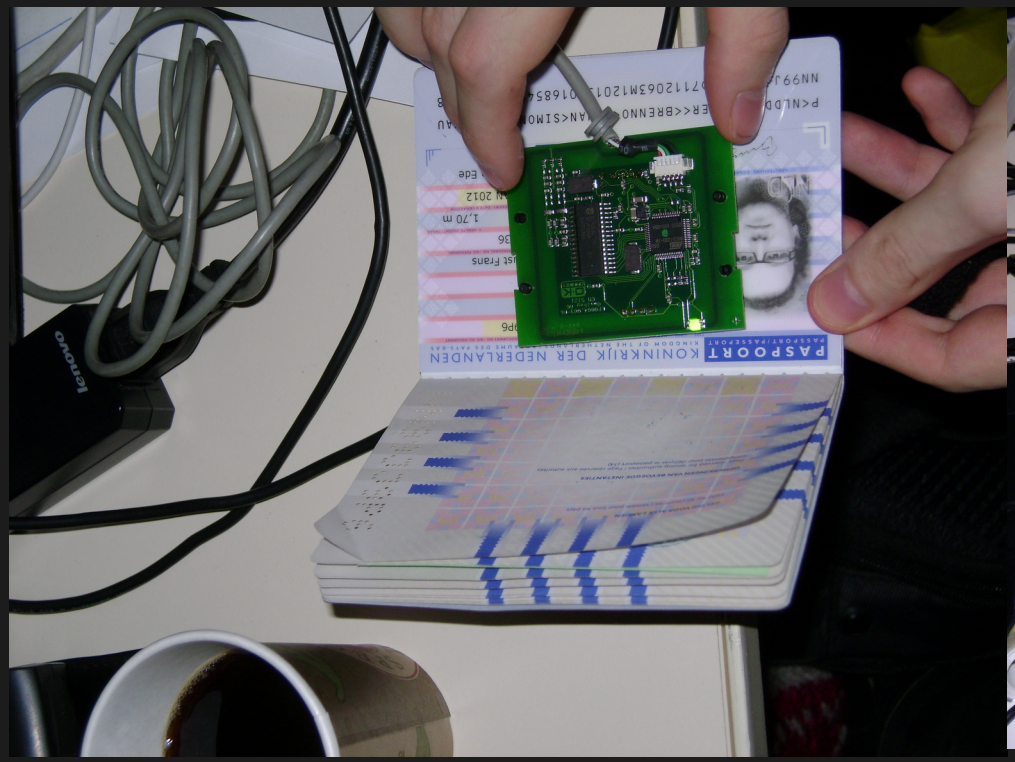
PaigeRyan_: Finally got my new keys to me and Ethan's new house new house fresh start only the best for my boy http://t.co/pyh5sjacjJ

Pictures of keys are fun!





Just hand out your passport briefly



Again: there's an app for that

Program

1)Attackers and Attacks

2)Our weaknesses

3)Attacking the systems

4)Reducing risks

5)Round-up

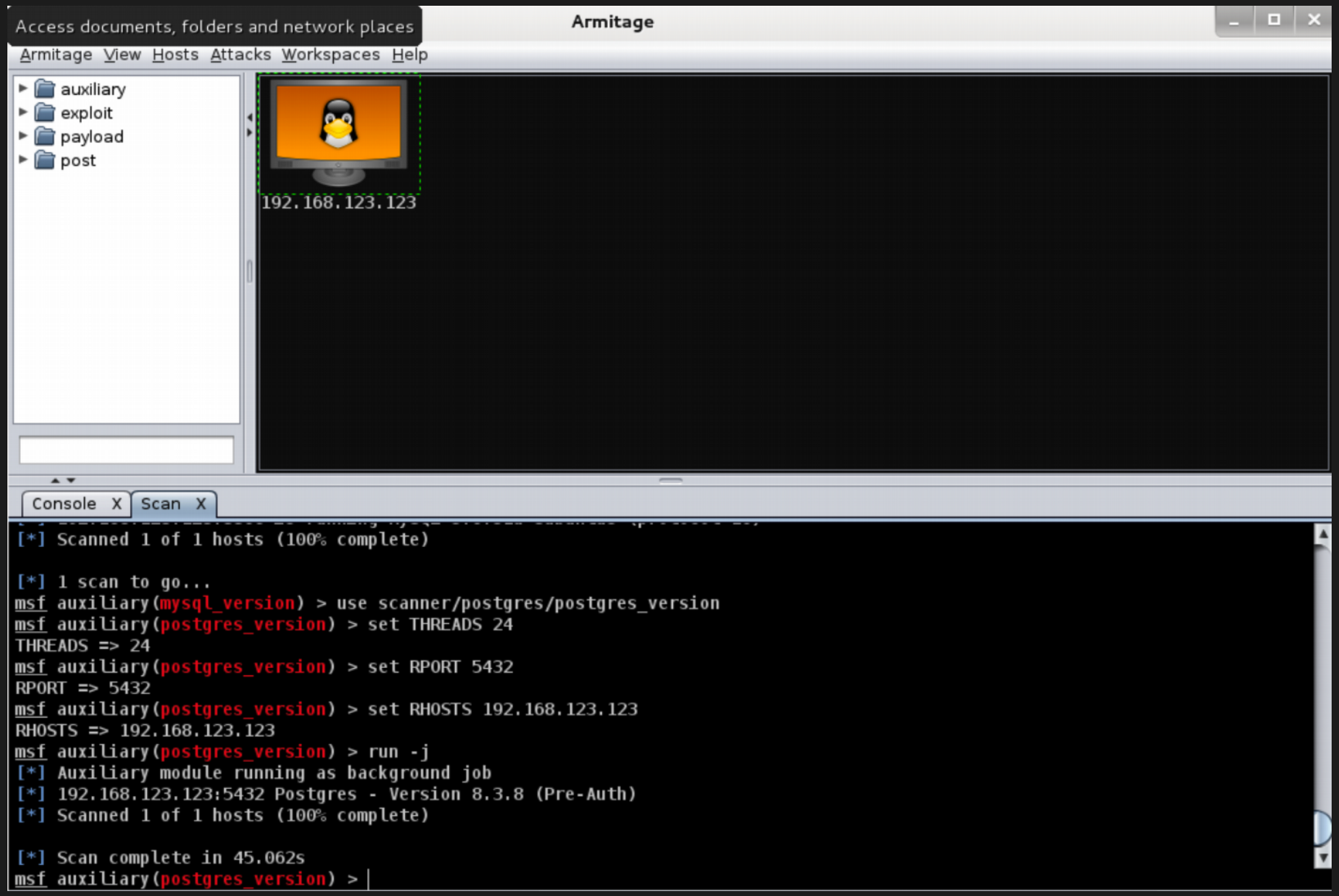
Hacking is simple

- >99% of major hacks in 2014
  - Took less than 10 minutes to execute
  - Exploited a flaw more than one year known
  - Can be done completely automated

Fully hacking a server is simple

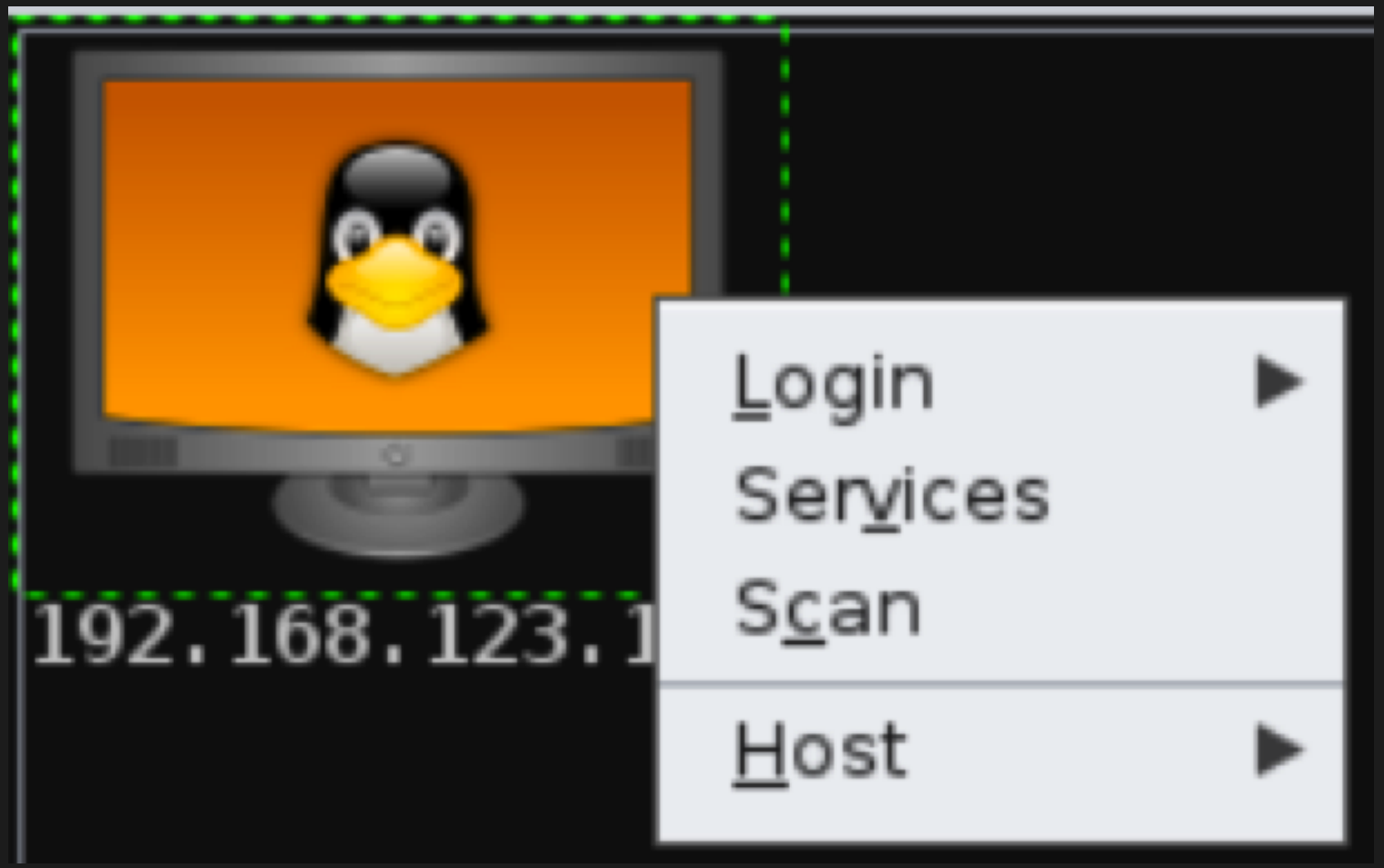
VIDEO

Hacking a system – step 1

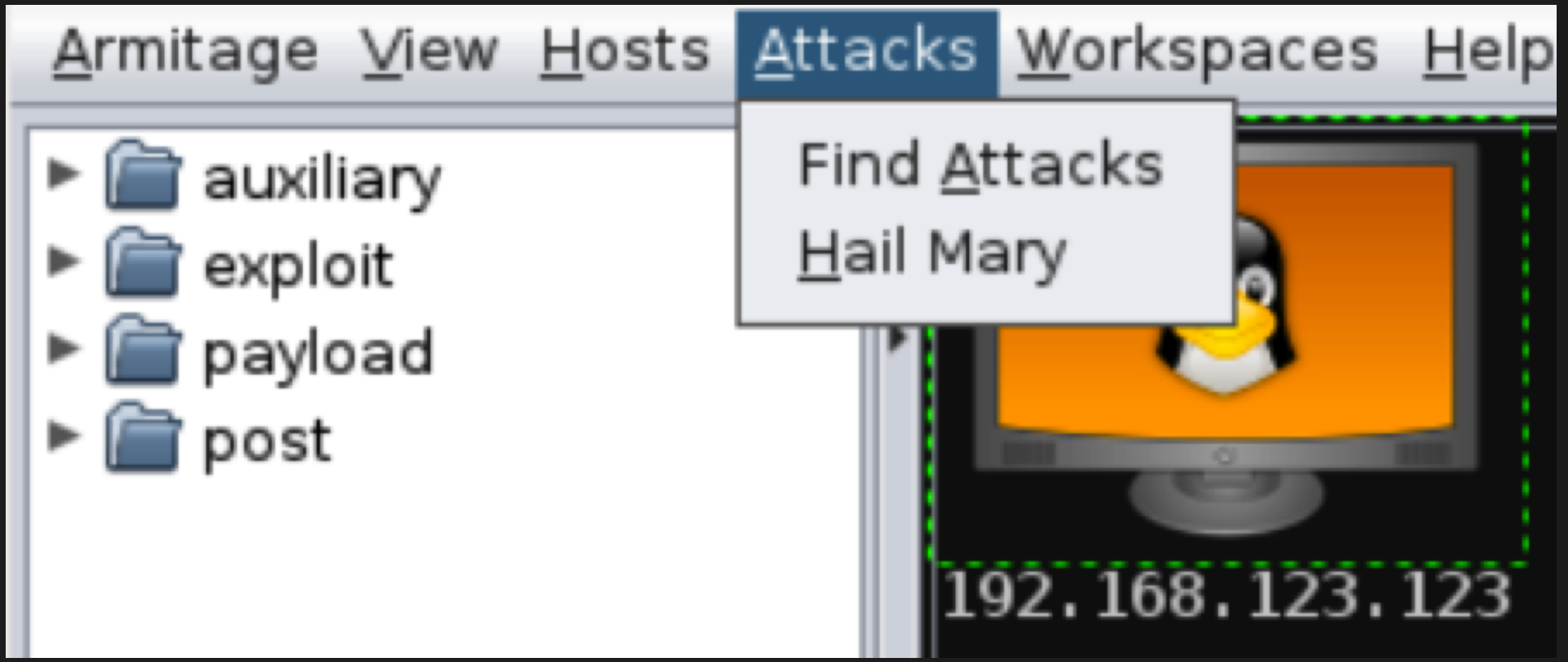


RADICALLY OPEN SECURITY

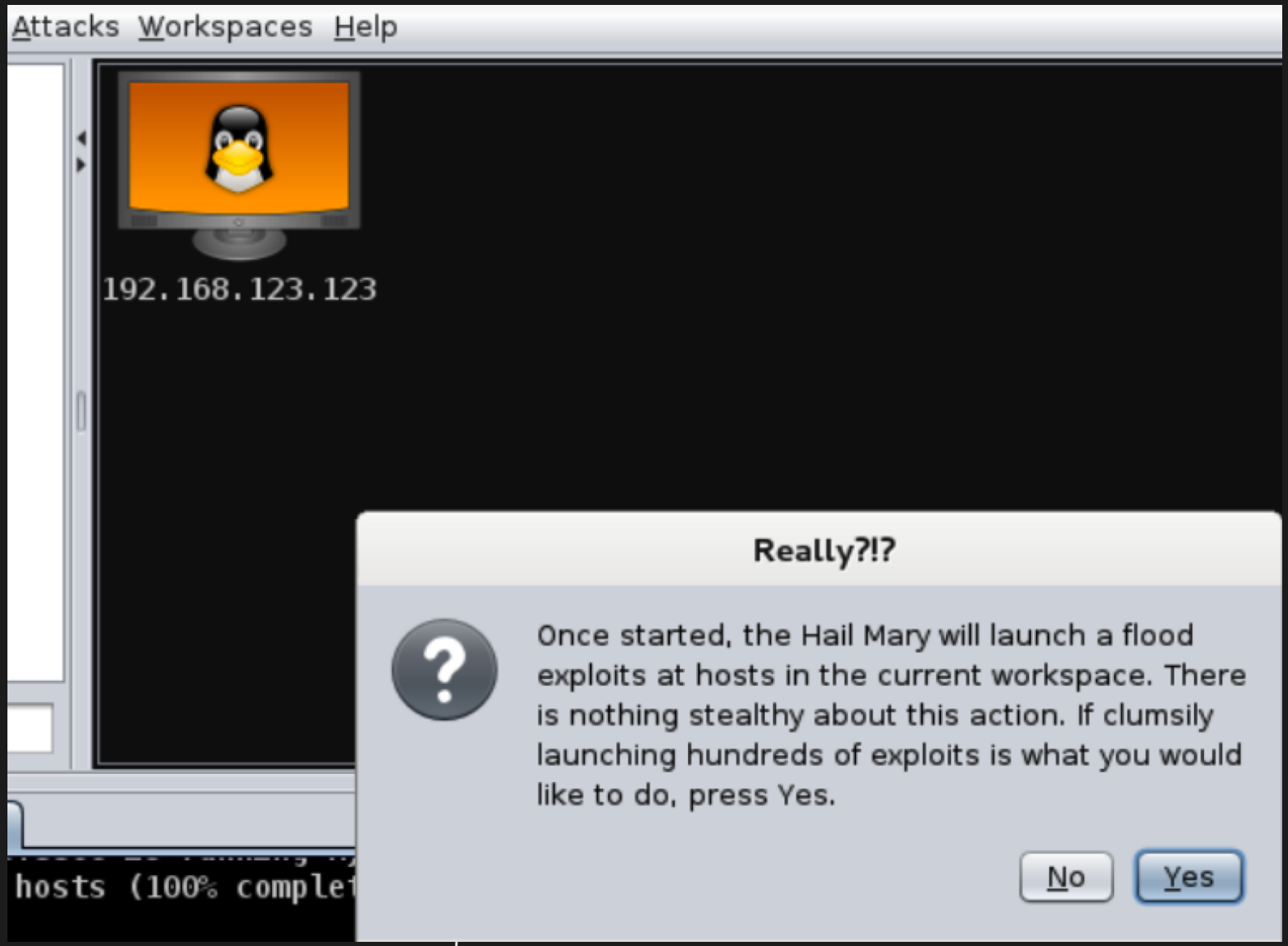
Hacking a system – step 2



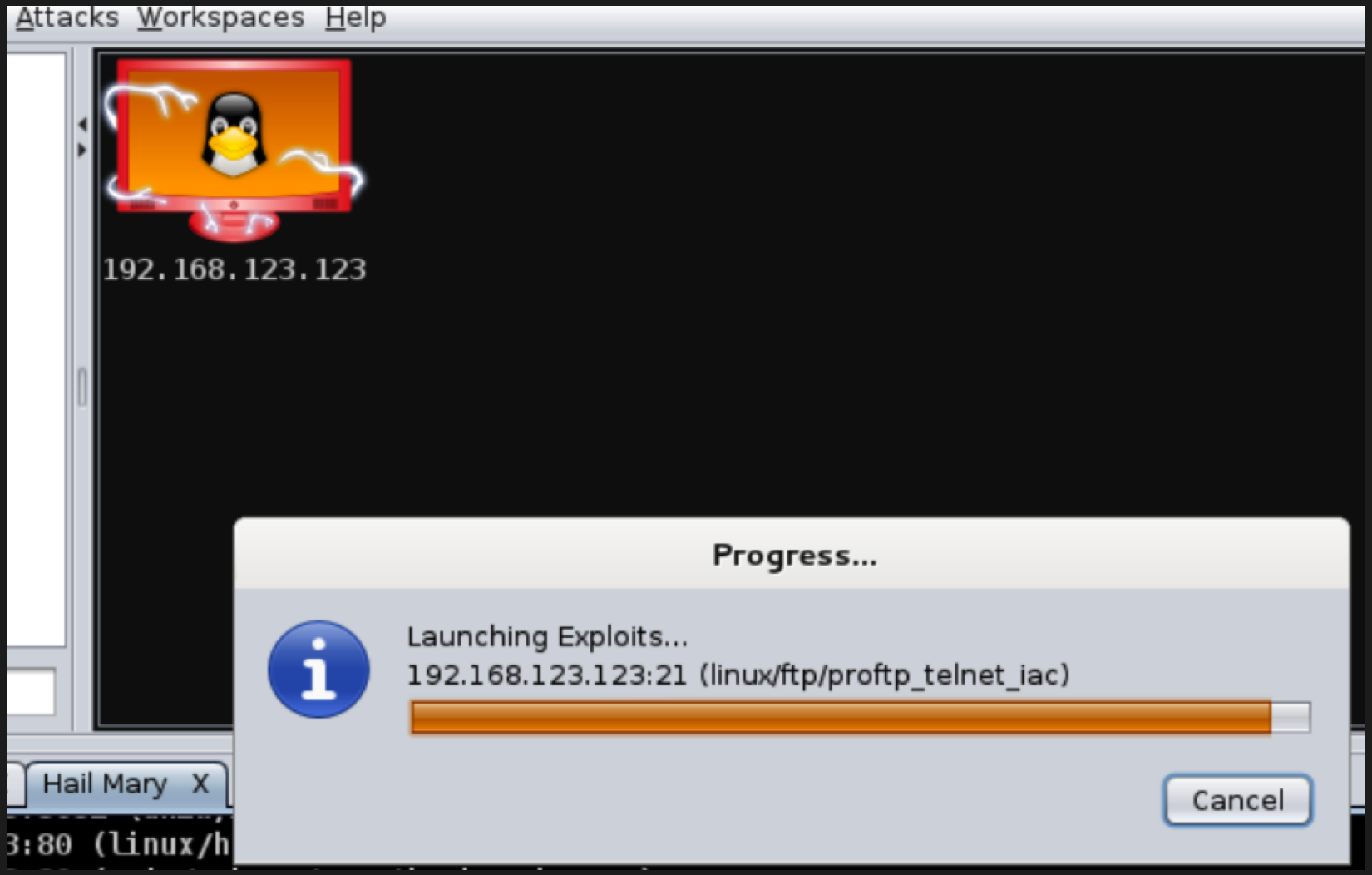
Hacking a system – step 3



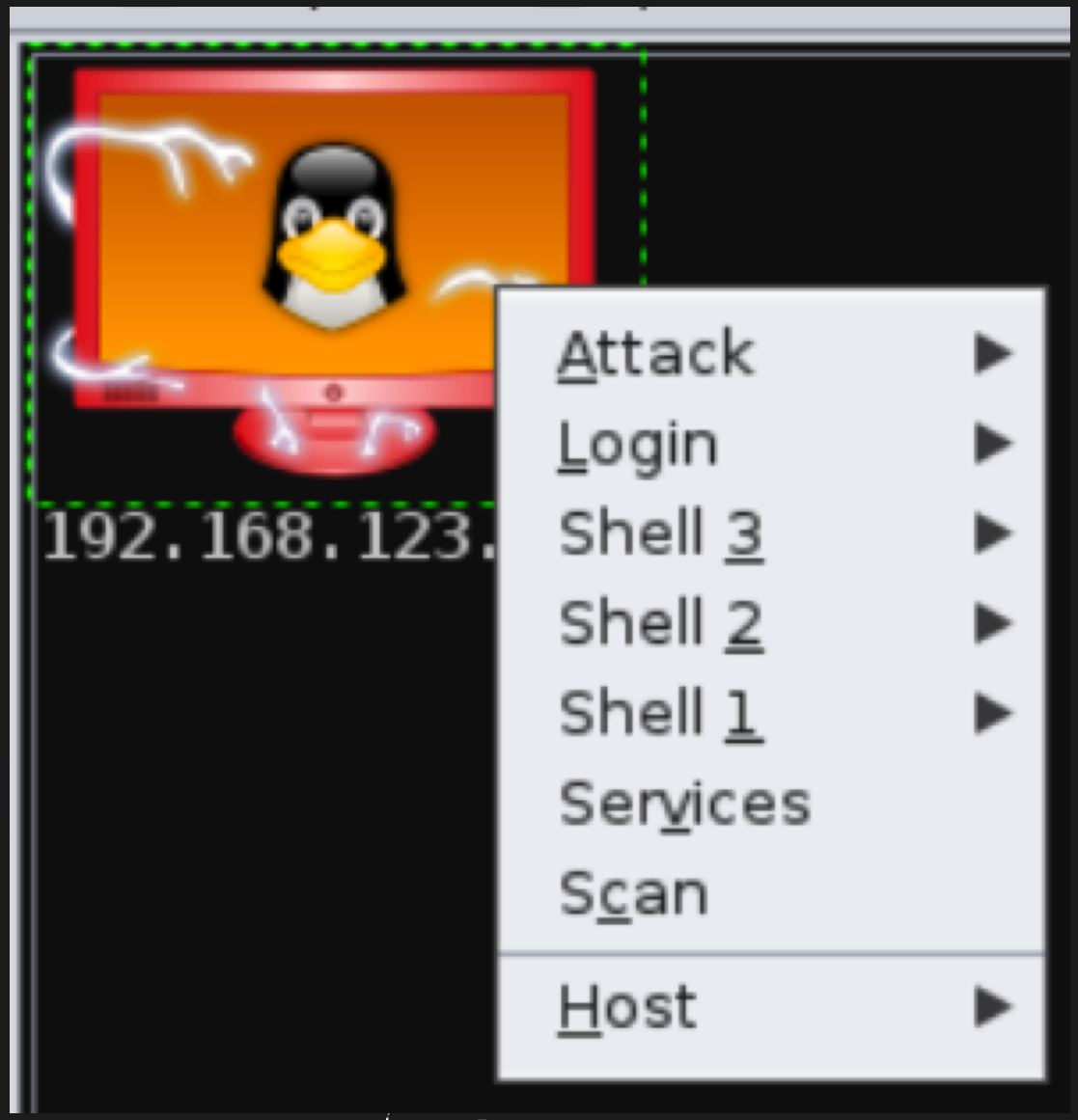
Hacking a system – step 4



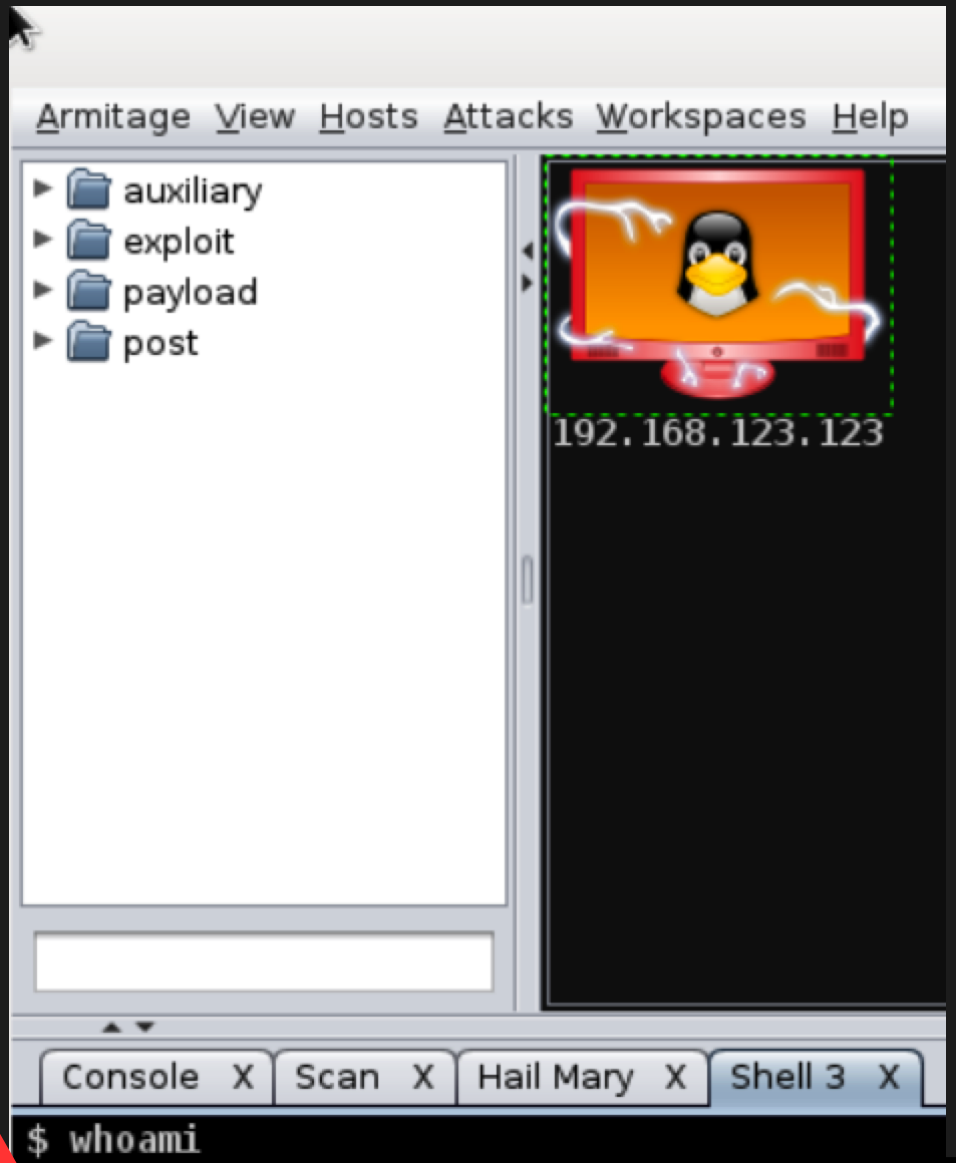
Hacking a system – step 5



Hacking a system – step 6



Total control



One simple solution in many cases:
Update your systems!

Why hack a server if you want data

- Don't trust companies automatically
- Often sites leak data with ease
- Attackers obtain that automatically

One simple solution in many cases:
Update your systems!

Take just the database

VIDEO

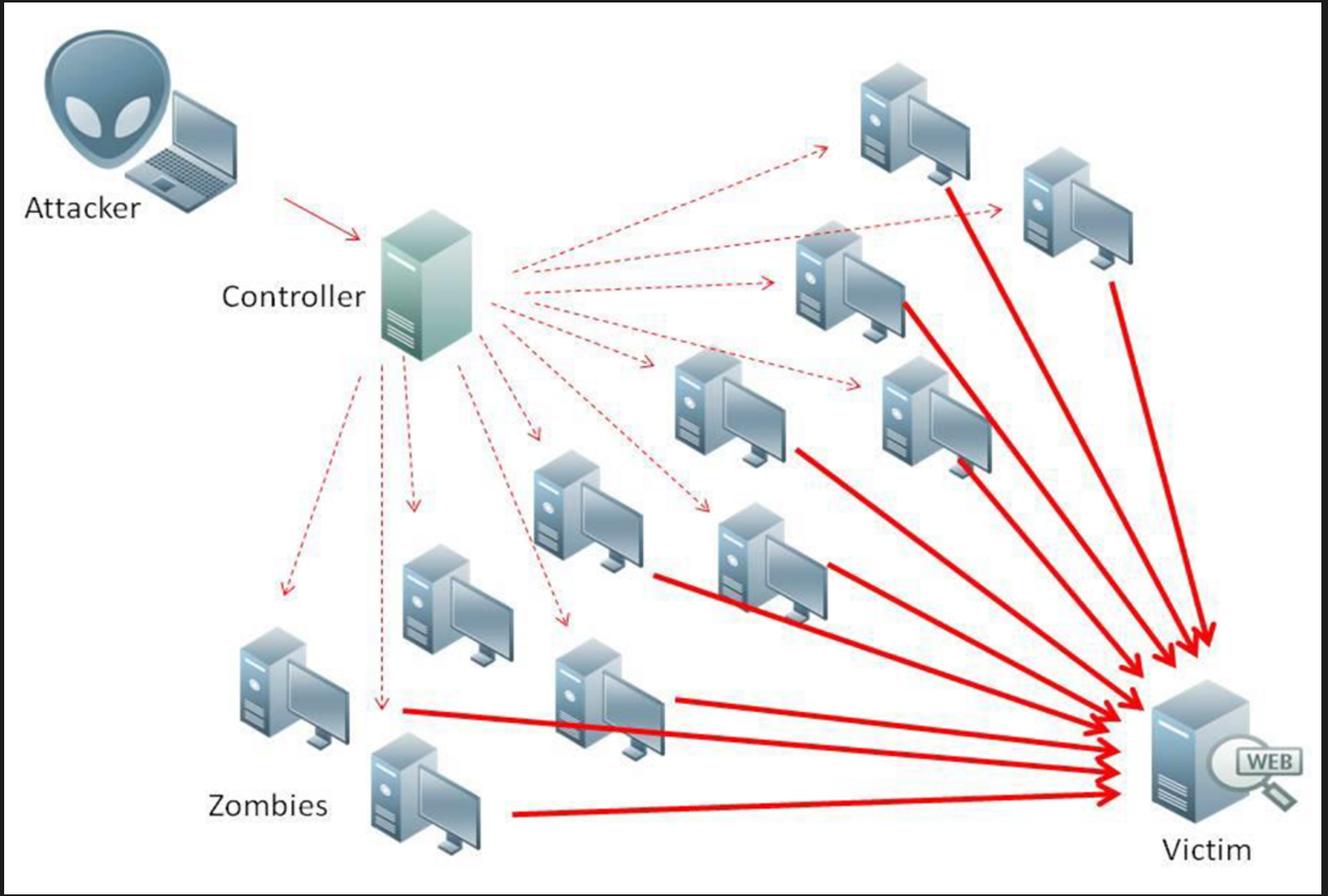
Take just the database

VIDEO

Another attack: (D)DoS

- Denial of Service
- This attack shuts down a service – like blocking the entry of a building
- Easy to execute
- One computer can do a lot (Denial of Service)
- Several computers can do the trick (Distributed Denial of Service)

DDOS: Schematic



Nasanbuyn

Again it's simple

1. Select target

Host victim.net Get

URL Get

2. Ready

Attack!

Selected target

72.52.4.120

3. Attack options

Timeout 9.000

HTTP Subsite /

Random

TCP/UDP Message U dun goofed

Random

80 Port

TCP Method

10 Threads

Wait for reply

0 Delay [ms]

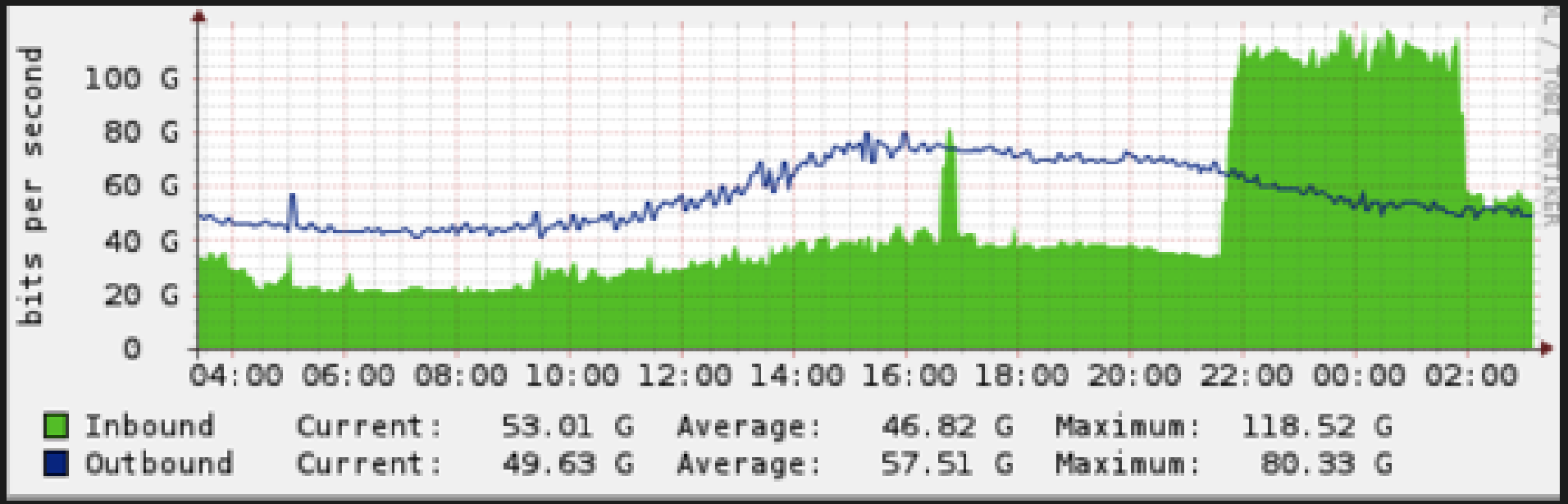
Socks proxy 127.0.0.1

Port 8.080

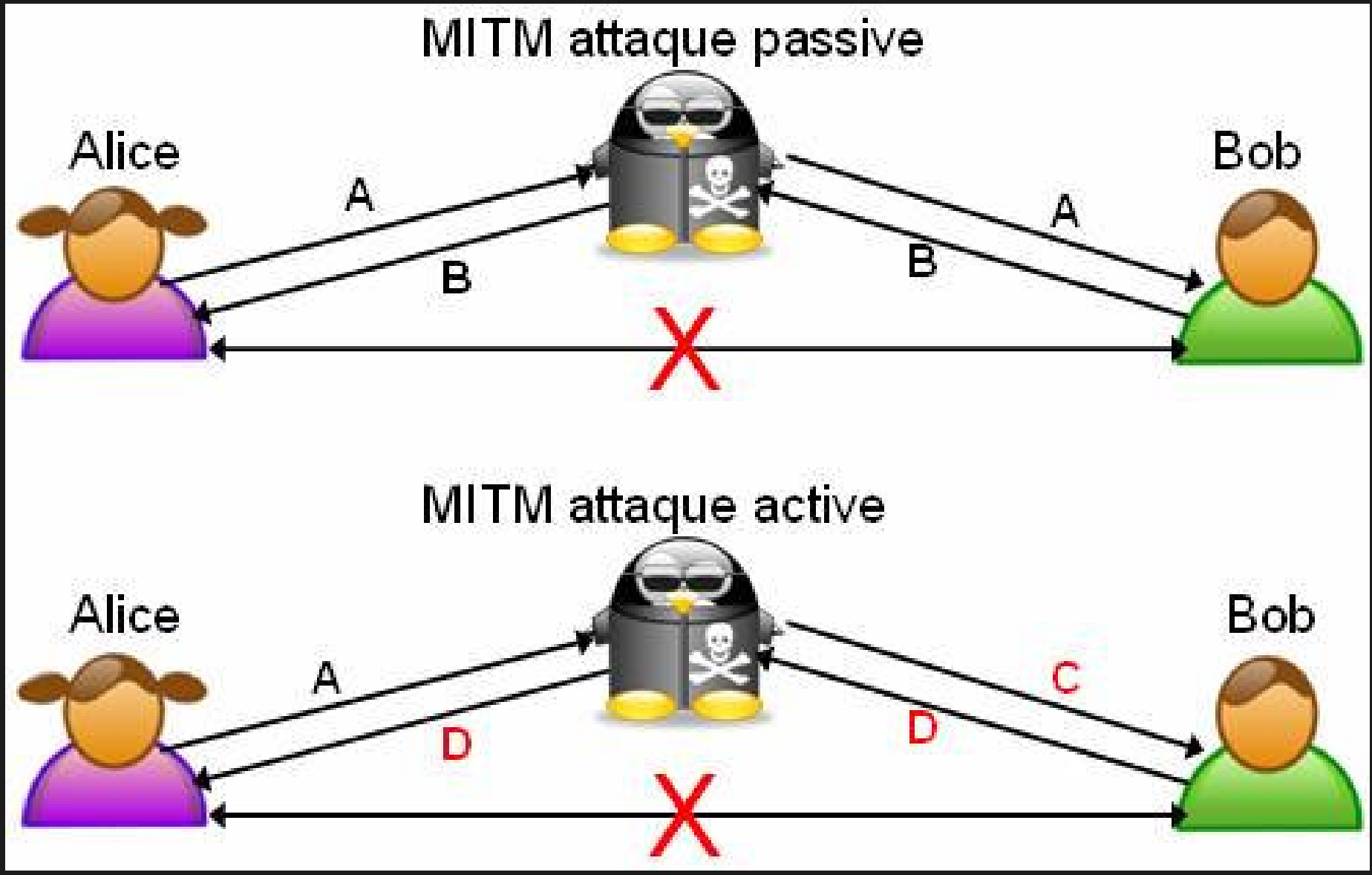
0,0 b/s

Cloudflare Spamhaus Cyberbunker

- 'The attack that almost broke the internet'
- Huge attack on Spamhaus and thus more sites



The Man in the Middle



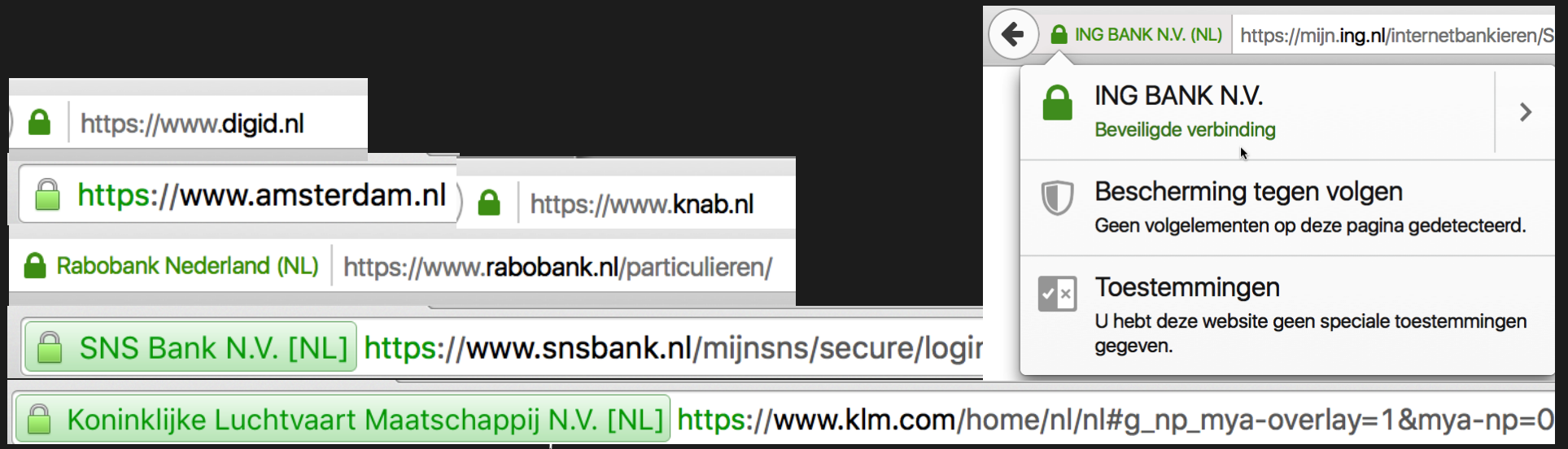
Martial Régereau

Doing a Man in the Middle

- Using your computer
- A Wifi Pineapple

Solutions

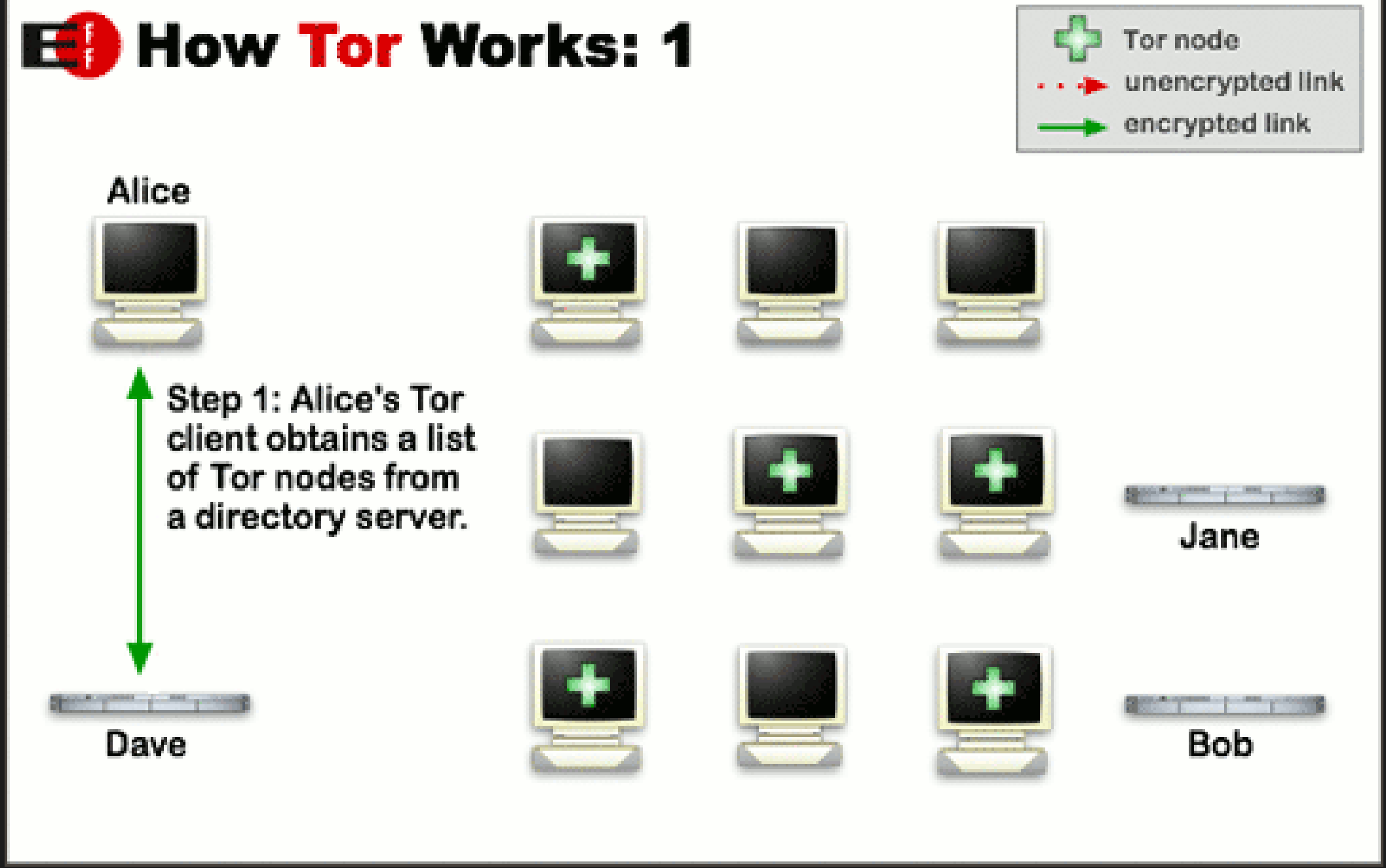
- Use encryption – check for HTTPS
- Check certificates on websites
- Use a VPN on untrusted networks



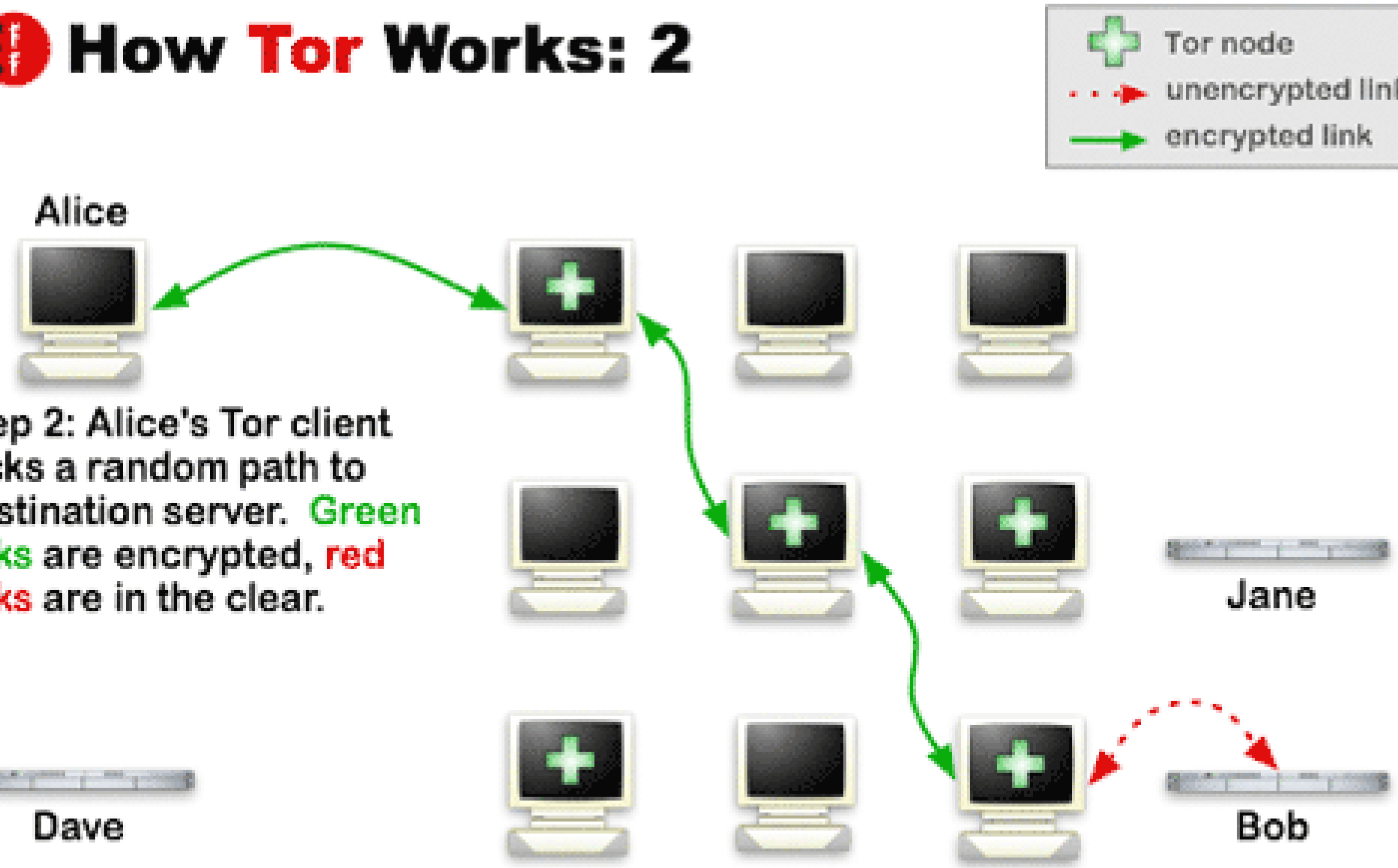
Tor

- Anonymizing network traffic
- Hide in the masses
- Afterwards 212.47.227.xxx
- One minute later 23.46.yyy.23

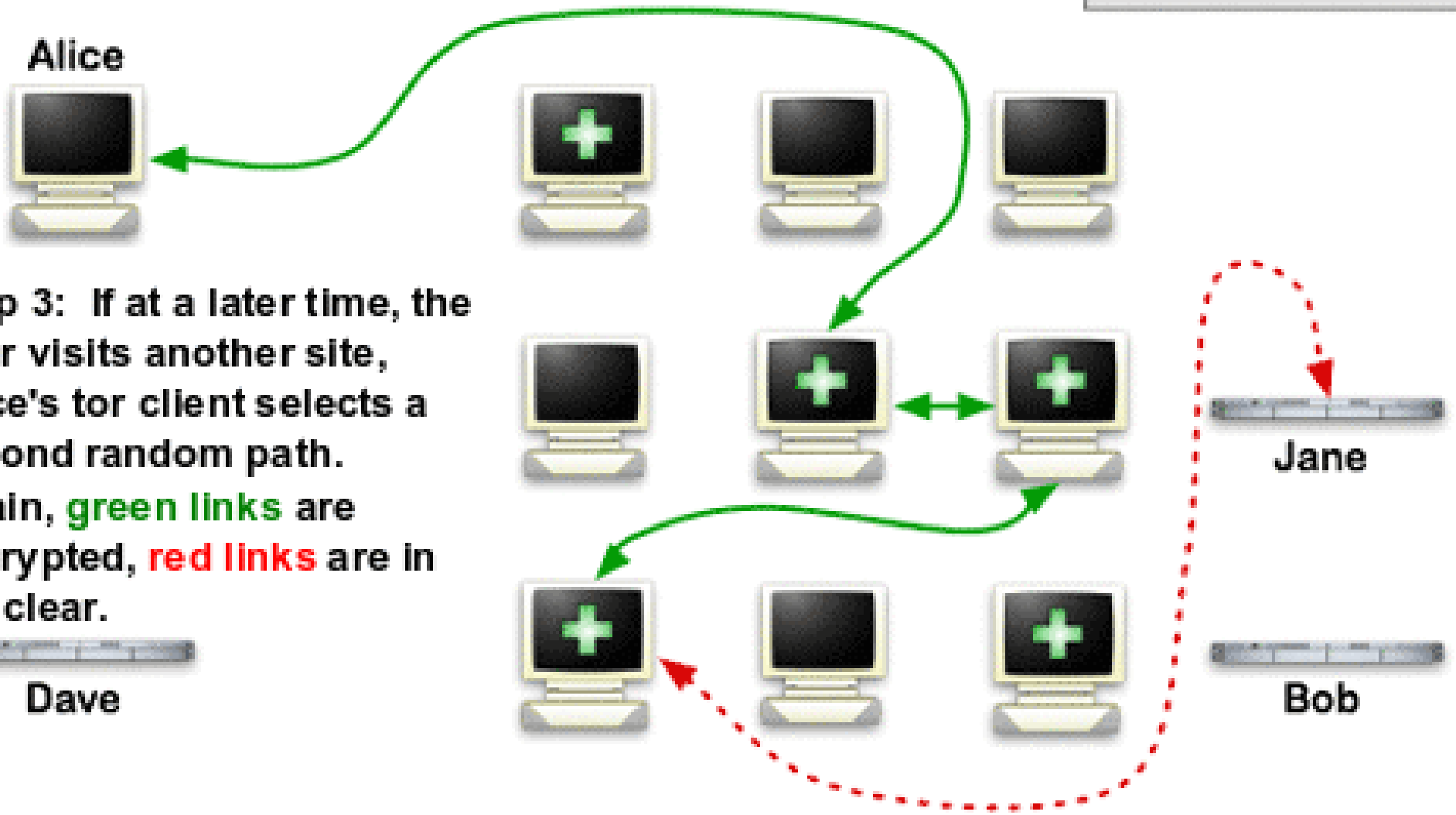
How Tor Works: 1



How Tor Works: 2



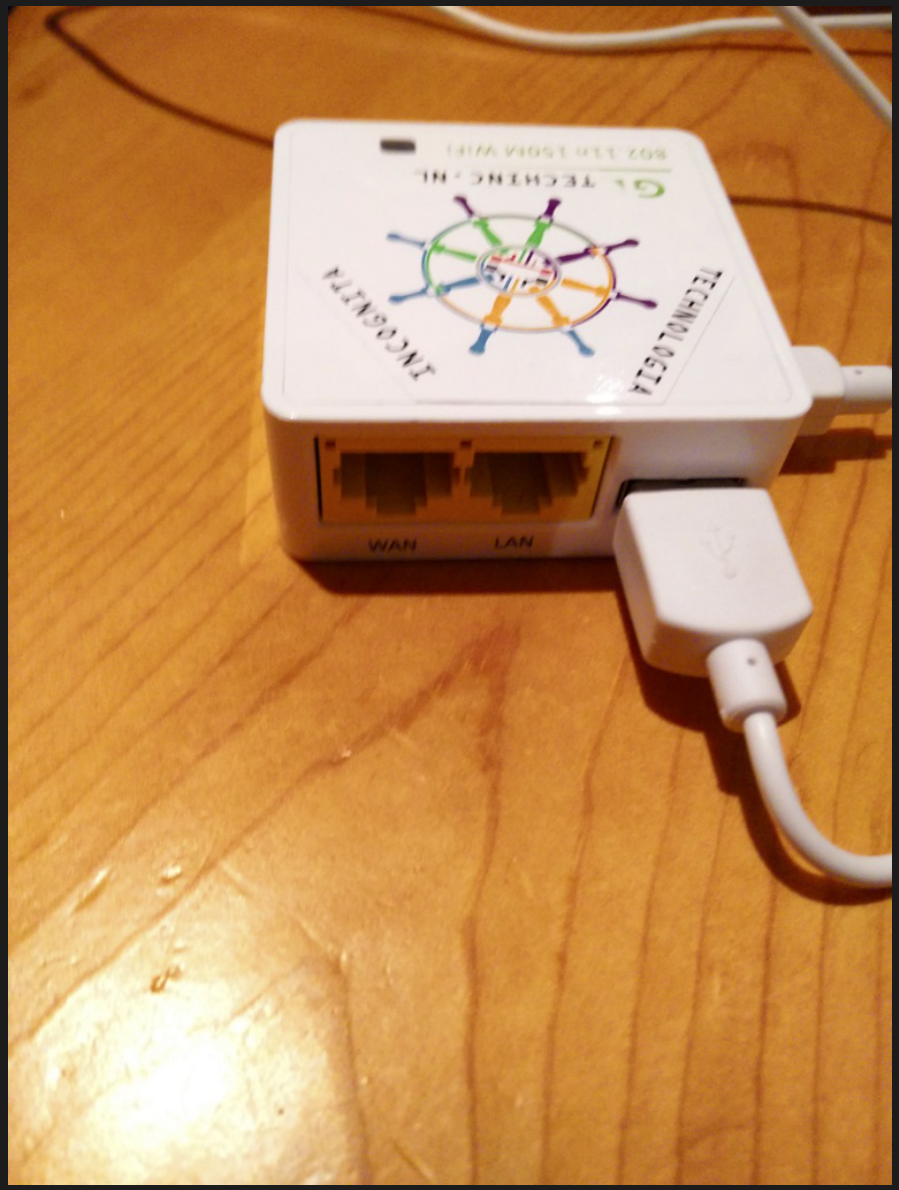
How Tor Works: 3



Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path.

Again, green links are encrypted, red links are in the clear.

Make it simple



Program

1)Attackers and Attacks

2)Our weaknesses

3)Attacking the systems

4)Reducing risks

5)Round-up

Simple prudent steps

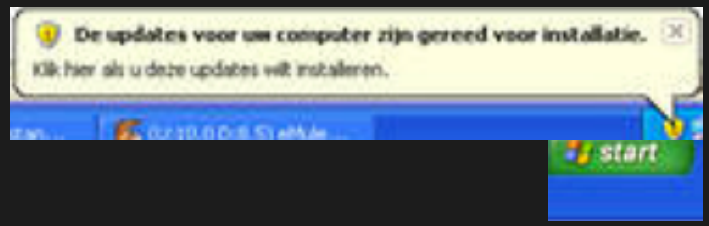
1) Update systems regularly
2) Have an up-to-date scanner for malware
3) Have a functioning firewall
4) Make regular back-ups
5) Don't be click-happy
6) If the service is free, you're the product
7) Be exemplary in behavior

Simple prudent steps

1) **Update systems regularly**
2) Have an up-to-date scanner for malware
3) Have a functioning firewall
4) Make regular back-ups
5) Don't be click-happy
6) If the service is free, you're the product
7) Be exemplary in behavior

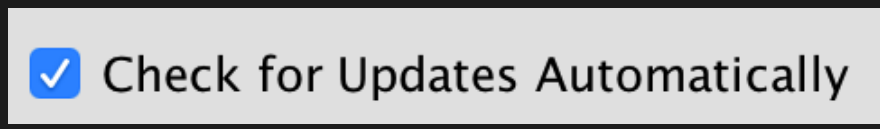
How?

- Never ignore update warnings
- Update automatically when possible
- Check your devices yourself
- Computer, tablet, phone and equipment
- Stop using unsupported software



Why?

- 99% of all hacks use leaks known for over a year
- Lower risks for malware
- Changes for hacks reduce dramatically
- Better functioning software
- It improves your system!



Really everything is connected

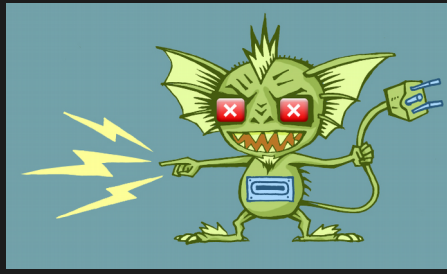
- Internet of Things
  - Fridge
  - Pick-up player
  - Television
  - Thermostats, Lights
  - Phones, Smartwatches
  - Video/Photo Camera's
  - Digital Television Boxes
  - Cars

Really everything is connected

Simple prudent steps

1) Update systems regularly
2) **Have an up-to-date scanner for malware**
3) Have a functioning firewall
4) Make regular back-ups
5) Don't be click-happy
6) If the service is free, you're the product
7) Be exemplary in behavior

Recognize malware



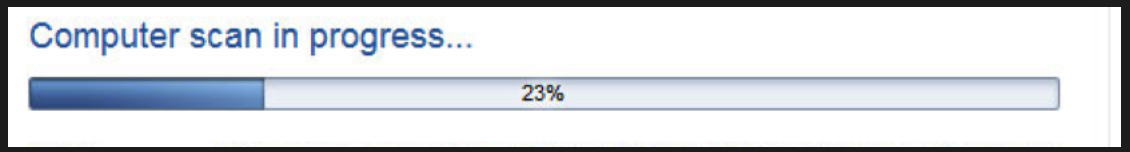
- Some common symptoms:
  - Your machine is slower than should be
  - You have a 'strange' default' homepage
  - Your browser favorites have altered
  - You keep getting strange popups
  - Strange links on the desktop workspace

How?

- Get software that protects against viruses and malware
- Be aware where malware can reside
- Have it always running
- Real-live detection
- Don't ignore warnings

Why?

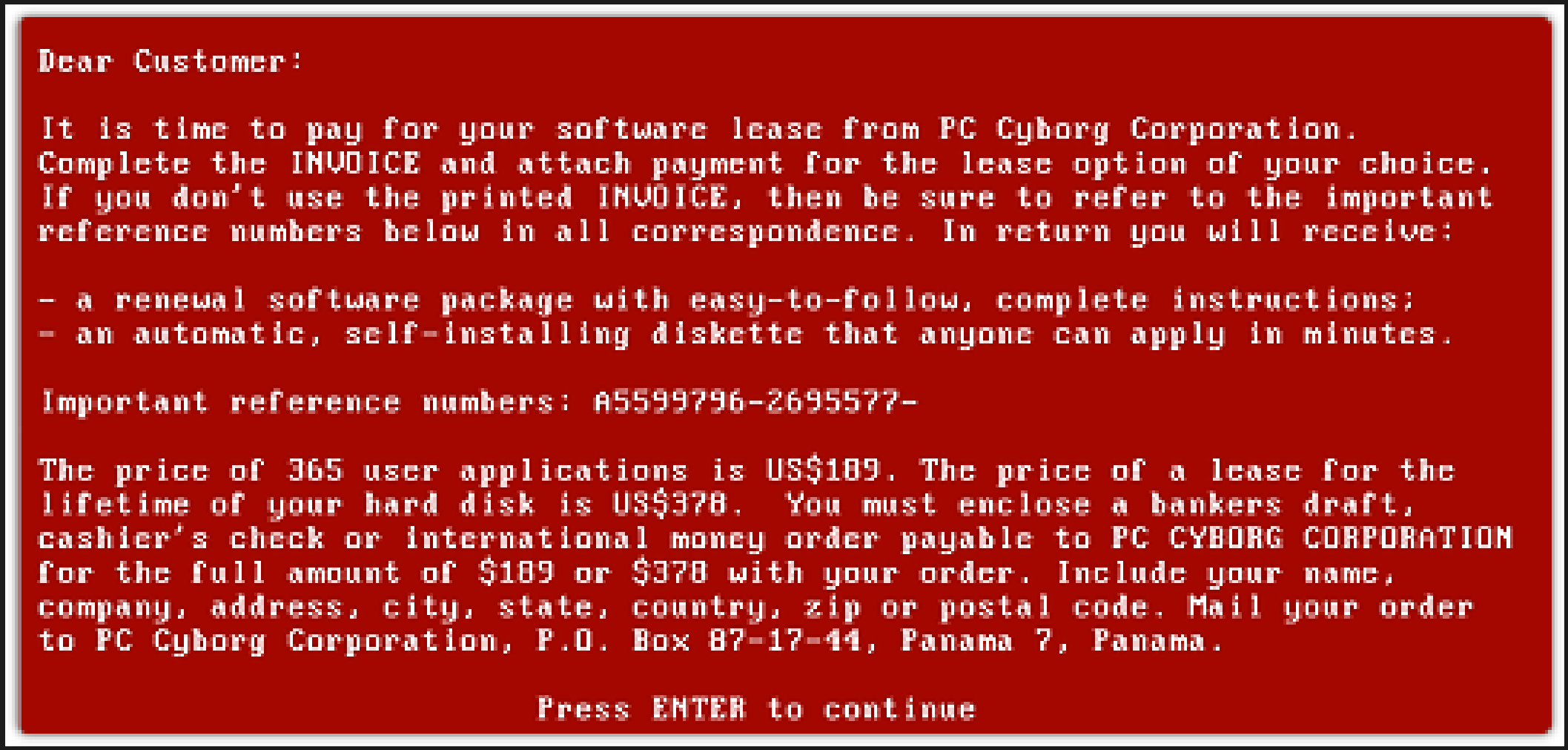
- Reduced risks for infections with malware, cryptolocker, virusses
- Warnings for potentially dangerous sites, files
- Solutions if malware hits you



Ransomware


POLITIE
Korps Landelijke Politiediensten
Openbaar Ministerie
CYBERCRIME POLITIE NEDERLAND
IP:
Land: Netherlands
Regio:
City:
ATTENTIE! Uw webbrowser wordt geblokkeerd om veiligheidsoverwegingen
wegens de hieronder aangegeven redenen.
Alle activiteiten van deze computer zijn opgenomen.
Al uw bestanden worden versleuteld.
paysafecard
Ukash
PIN-Code
Waarde
Typ uw code
100
1 2 3 4 5 6 7 8 9 0
Clear
Betalen PaySafeCard
Betalen Ukash
Waar kan ik een geldvoucher PaySafeCard aanschaffen?

Extortion not new – f.i. 1989



Joseph L. Popp, AIDS DOS Information Trojan author

Simple prudent steps

1) Update systems regularly
2) Have an up-to-date scanner for malware
3) **Have a functioning firewall**
4) Make regular back-ups
5) Don't be click-happy
6) If the service is free, you're the product
7) Be exemplary in behavior

How?

- Most operating systems offer this already
- Just turn it on or install one that sometimes comes with anti-malware
- Have it always running
- Take it warnings serious

Why?

- Less chance of attacks on your system
- Unneeded network connections can be prevented
- Some abnormal behavior can be stopped

Simple prudent steps

1) Update systems regularly
2) Have an up-to-date scanner for malware
3) Have a functioning firewall
4) **Make regular back-ups**
5) Don't be click-happy
6) If the service is free, you're the product
7) Be exemplary in behavior

How?

- Using Apple Timemachine, Windows Backup, Cloud solutions, NAS
- Have more than one backup
- Store in several locations
- Do it regularly

And store them properly

RADICALLY OPEN SECURITY

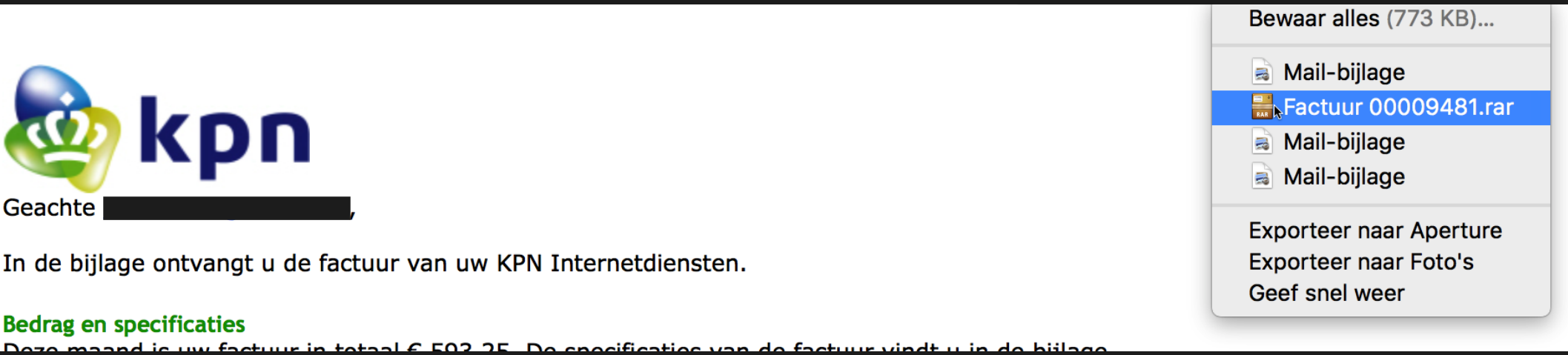
Why?

- Way to quickly recover when disaster strikes
- Resilience against cryptolocker
- Be resilient against simple mistakes

Simple prudent steps

1) Update systems regularly
2) Have an up-to-date scanner for malware
3) Have a functioning firewall
4) Make regular back-ups
5) **Don't be click-happy**
6) If the service is free, you're the product
7) Be exemplary in behavior

Install software with a simple click



Check, check, double check

Payment

Antwoord aan: Payment

Invoice #12664081 for your Order

Greetings, respectful client!
We have just shipped your order at you local post office.
You can find the listing of your shipment in the attachment. Please check.
Take care.

Order/Invoice number:
12664081

Order/Invoice date:
01.03.2016

Accounts Department
Wavenet Group
Incorporating - Titan Technology, Centralcom and S1 Network Services
Tel 0844588539

Simple prudent steps

1) Update systems regularly
2) Have an up-to-date scanner for malware
3) Have a functioning firewall
4) Make regularly back-ups
5) Don't be click-happy
6) **If the service is free, you're the product**
7) Be exemplary in behavior

You're the product

- Your profile is worth serious money
- Many companies store loads of information on you
- You leave many traces:
  - Telling information about yourself in forms
  - Uploading too much information
  - Secretly giving away details through: browser, ip-address, behavioral information

Simple prudent steps

1) Update systems regularly
2) Have an up-to-date scanner for malware
3) Have a functioning firewall
4) Make regularly back-ups
5) Don't be click-happy
6) If the service is free, you're the product
7) **Be exemplary in behavior**

Be alert for fraudsters

Facebook estimates that between 5.5% and 11.2% of accounts are fake

Mr Q Liu 2nd

Head of Operations at Bank of America

Hemel Hempstead, United Kingdom | Banking

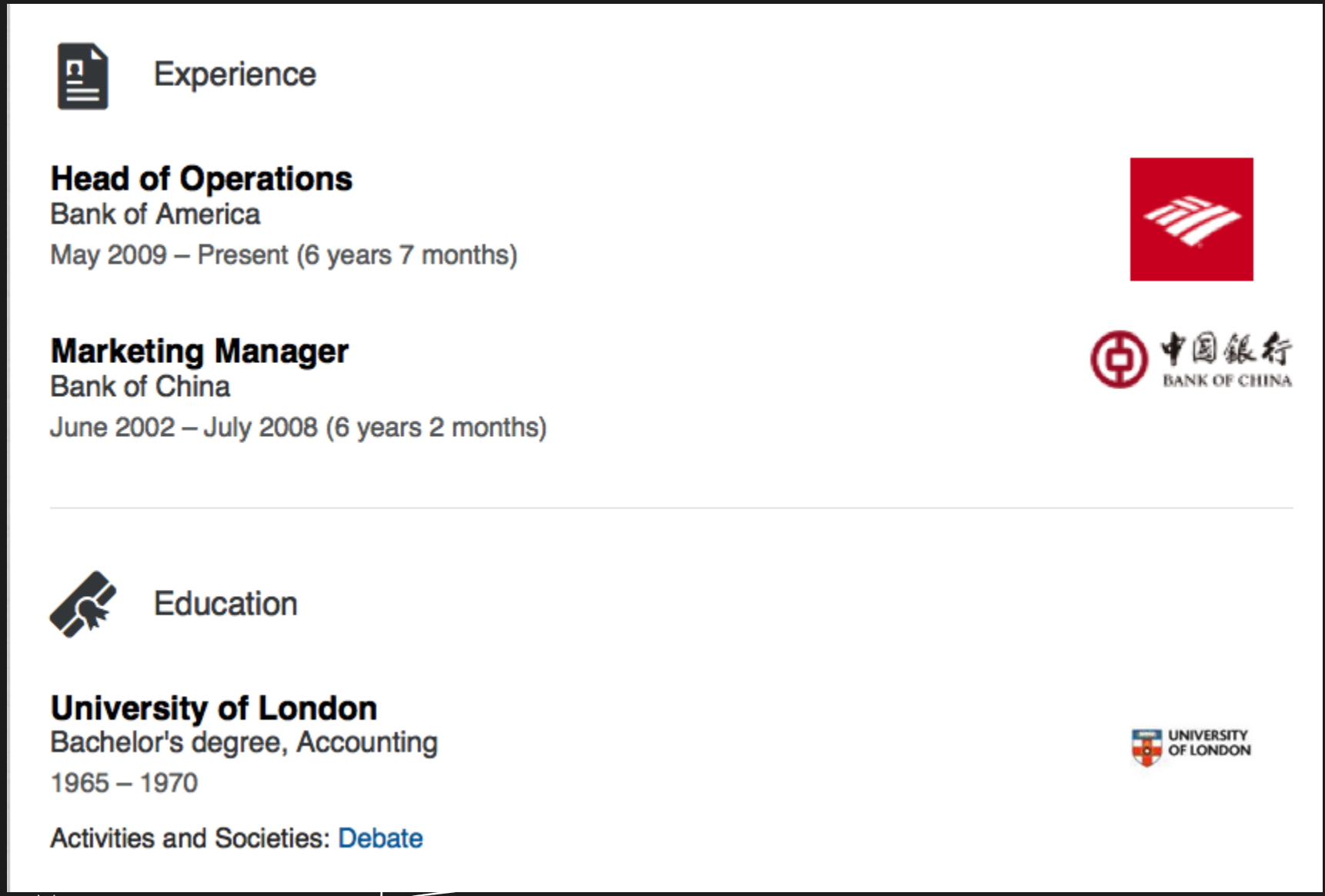
Previous Bank of China

Education University of London

Accept invitation | Send Mr Q InMail | 83 connections

Sometimes they're an easy catch

That's all?



Be smart

- Don't advertise security solutions you use on social media, employment adds
- When making a mistake:
  - Don't be a shamed
  - Apologize if needed
  - Seek help
- Don't put sensitive data on untrusted media
- In doubt abort any action

Don't leave printed papers for days

We all got have something of value

Hans de Raad

Yesterday at 3:10pm · Edited ·

"You shouldn't rate or assess your need for security based on your own companies size but to the size/scale of your possible adversary and their toolkit."

My own paraphrase of a statement done by Chris Ensor (UK gov CESG) but I feel this makes a lot of sense! Just because you're an SME or freelancer doesn't mean your ideas and data aren't worth stealing!

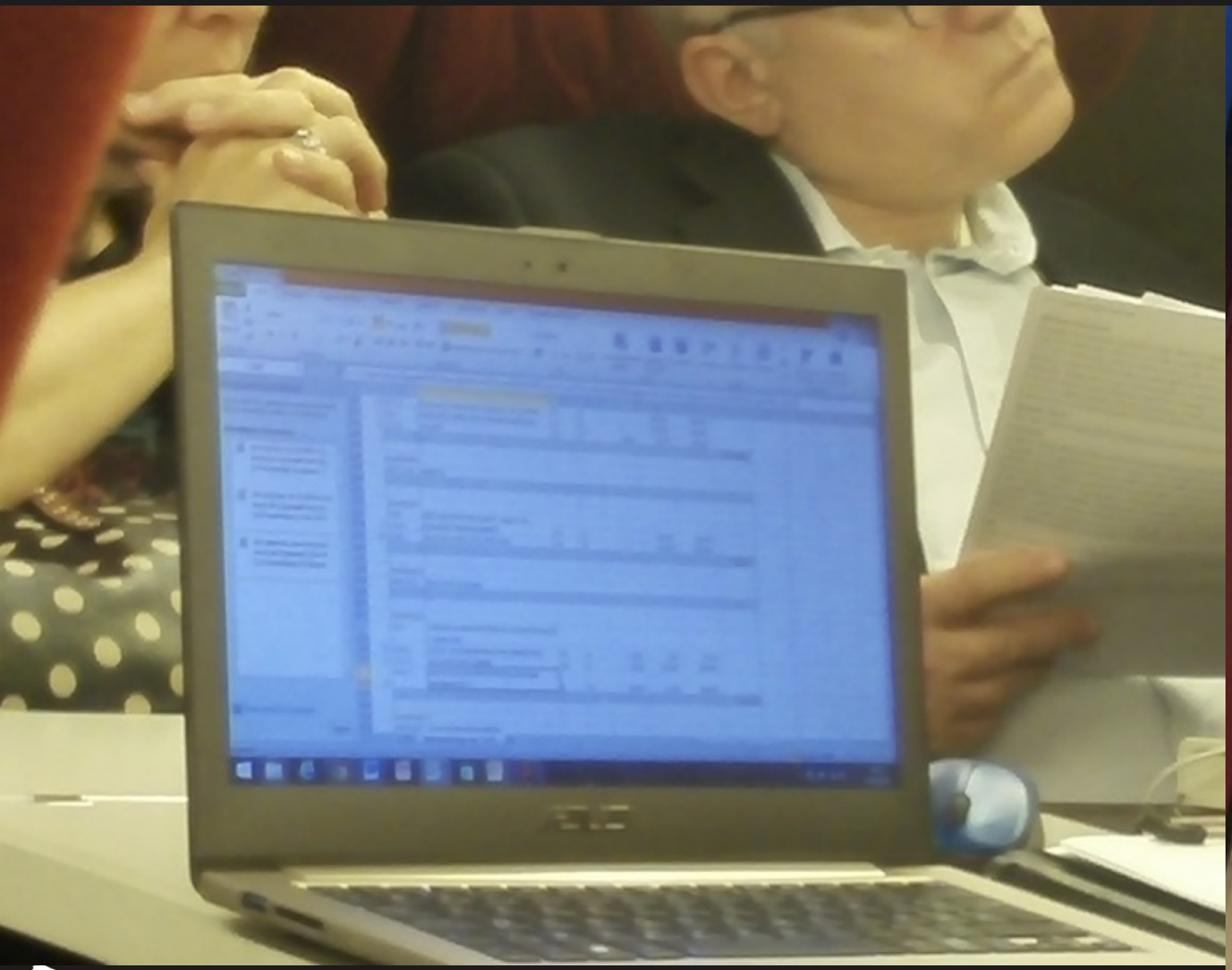
Unlike · Comment · Share

You like this.

Filter information for vendors

- They are not always trustworthy
- They also have attackers compromizing them
- Give them information on a real 'need to know basis'

Always be alert



Simple prudent steps

1)Update systems regularly

2)Have an up-to-date scanner for malware

3)Have a functioning firewall

4)Make regularly back-ups

5)Don't be click-happy

6)If the service is free, you're the product

7)Be exemplary in behavior

Program

- Attackers and Attacks
- Our weaknesses
- Attacking the systems
- Reducing risks
- **Round-up**

Round-up

?