

Digitaal Alert

Developed by:

Brenno de Winter

Tim Blazytko

Ganesh Rajagopalan



Programma

- 1) Aanvallen en hun Aanvallers
- 2) Onze Zakheden
- 3) Systemen aanvallen
- 4) Risico's verkleinen
- 5) Afronding/Vragen



Programma

- 1) Aanvallen en hun Aanvallers**
- 2) Onze Zakheden**
- 3) Systemen aanvallen**
- 4) Risico's verkleinen**
- 5) Afronding/Vragen**



Pepper.nl

- Dating website
- Gegevens van 54.000 verkregen via hack
- Gehacked door AnonymousIRC
- Online gezet
- Wachtwoorden elders geprobeerd
- Veel werk e-mails

Touya Akira
@ClipperChip

We've been sitting on pepper.nl database for a while. Didn't want to abuse it but if we have it, someone worse has, too. Better tell you.

RETWEETS VIND-IK-LEUKS
21 3

23:03 - 2 jul. 2011



E-mailadressen zijn geld waard

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 USD
Norway	488707	Email Addresses	\$400 USD
Oman	9867	Email Addresses	\$50 USD

Verboden dating



Vertrouw bedrijven niet automatisch

"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."



Zelfde fouten blijven herhalen

- 'Life is Short, Have an Affair' - Ashley Madison
- 60Gb bedrijfsgegevens online gezet
- 15,000 mensen gebruikten VS-overheids mail
- 11 miljoen accounts (e-mails, wachtwoorden)
- Diverse mensen plegen zelfmoord

Gegevens openbaren

- Twee opties:
 - Publiek maken
(Pepper.nl)
 - Via het darkweb
(Ashley Madison)

The screenshot shows a post on a dark web forum. The title of the post is "10k combo email:pass". The post was made by a user named "KADER11000" on August 29th, 2015, and has received 3,371 views. The post contains a list of 12 email addresses followed by their corresponding passwords. The first few entries are: 1. [REDACTED], 2. [REDACTED], 3. [REDACTED]@mail.bg:sisko98, 4. [REDACTED]_hotmail.com:lucianoluiz, 5. [REDACTED]@gmail.com:koralin11, 6. [REDACTED]@gmail.com:84486ld., 7. [REDACTED]z@hotmail.com:steaua10, 8. [REDACTED]p@hotmail.com:245534090, 9. [REDACTED]@gmail.com:123Qwe!@#, 10. [REDACTED]@hotmail.com:insomnia1, 11. [REDACTED]001@yahoo.com:barcelona, 12. [REDACTED]@hotmail.com:bst13392.

Rank	Email	Password
1.	[REDACTED]	
2.	[REDACTED]	
3.	[REDACTED]@mail.bg:sisko98	
4.	[REDACTED]_hotmail.com:lucianoluiz	
5.	[REDACTED]@gmail.com:koralin11	
6.	[REDACTED]@gmail.com:84486ld.	
7.	[REDACTED]z@hotmail.com:steaua10	
8.	[REDACTED]p@hotmail.com:245534090	
9.	[REDACTED]@gmail.com:123Qwe!@#	
10.	[REDACTED]@hotmail.com:insomnia1	
11.	[REDACTED]001@yahoo.com:barcelona	
12.	[REDACTED]@hotmail.com:bst13392	

Darkweb

- Een netwerk binnen het internet
- Hoge mate van anonimiteit
- Allerlei diensten/producten verkrijgbaar
- Bijv. gestolen identiteitsgegevens

E-mails te koop



150K COLORADO US BUSINESS EMAILS FOR EMAIL MARKETING

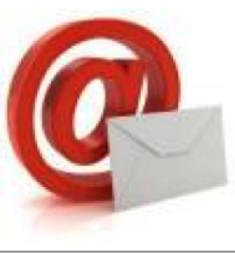
pwoah7foa6au2pul.onion/listing.php?id=91578 **Alphabay**

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



RADICALLY OPEN SECURITY

Inloggegevens te koop



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



RADIKALLY OPEN SECURITY

Werkelijk van alles te koop

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 receive your id to All encrypted or in a privnote for security reasons

Vendor EuroRX (328)

Price ₩ 24010757

Location United States

Description

EU - Dutch physical ID.



RADIKALLY OPEN SECURITY

Of beter



FAKE ID NETHERLINDS 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



RADIKALLY OPEN SECURITY

Complete identiteit



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



RADICALLY OPEN SECURITY

Walther PPK, Kal.7,65



New and unused!

Product	Price	Quantity	
Walther PPK, Kal.7,65	600 EUR = 1.573 ₩	<input type="text" value="1"/> X	Buy now
Ammo, 50 Rounds	40 EUR = 0.105 ₩	<input type="text" value="1"/> X	Buy now



RADICALLY OPEN SECURITY

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 ₿	<input type="button" value="1"/> X	Buy now
We kill your target in the European Union	19.671 ₿	<input type="button" value="1"/> X	Buy now



RADIKALLY OPEN SECURITY

Doorzoek het darknet

Grams

Search the darknet

E.g. cannabis

Grams Search

I'm Feeling Lucky



RADICALLY OPEN SECURITY



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
(0)

Price ₣0.03872842

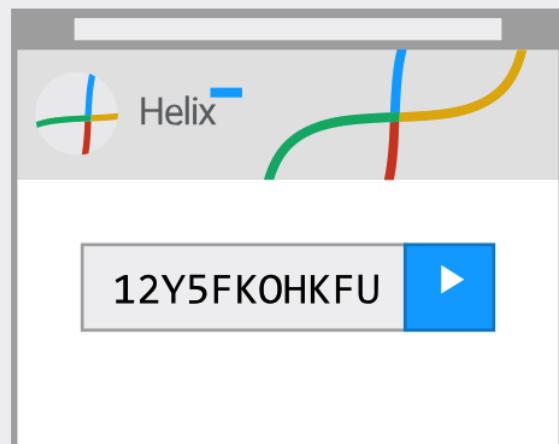
Location Netherlands



Geld witwassen

How Helix^{light} works

Enter your Bitcoin address in the box above



Send your dirty coins to the Helix address



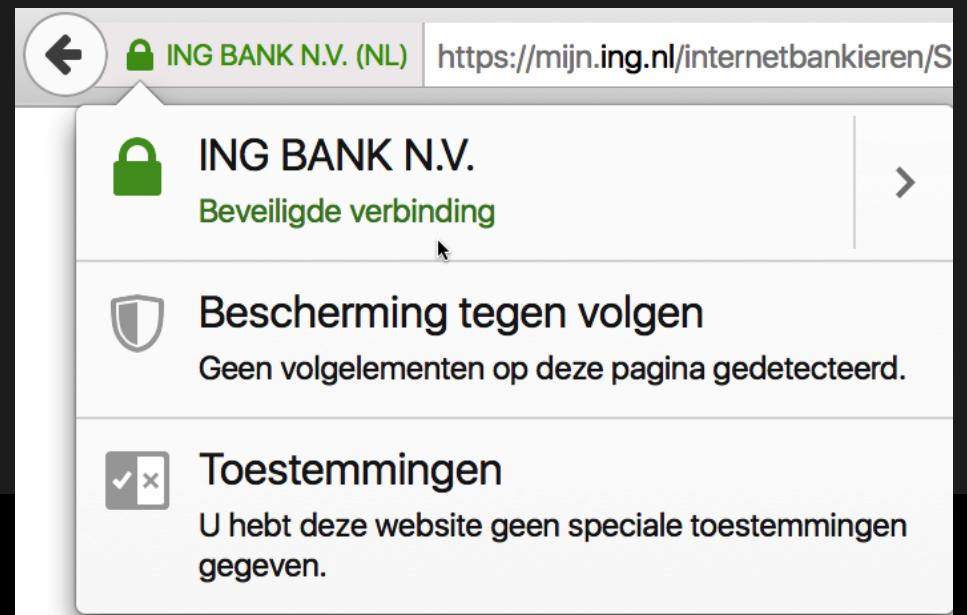
New, clean coins sent to your Bitcoin address



RADICALLY OPEN SECURITY

DigiNotar

- Uitgever en waарmerker digitale certificaten
 - Gebruikt voor veilige sites
 - Waarschijnlijk aanval vanuit Iran op Nederland
- Belangrijke infrastructuur



WIE DOEN DAT ALLEMAAL?

Wie doet zo iets?

- Mensen die een kans grijpen
 - Misbruik van een fout die je ziet
 - Geautomatiseerde programma's om te hacken
 - Iemand die leest over een truc



Wie doet dit?



- Professionele aanvallers
 - Standaard programmatuur voor aanvallen
 - Zelfs tools schrijven
 - Aanvallers die een serieus (langdurig) project maken van een aanval

Soorten aanvallers

Aanvaller	Beschrijving	Investering in aanval
Script kiddies	Gebruiken standaard hulpmiddelen, zijn vaak niet bewust van mogelijke gevolgen.	Weinig
Crimineel	Leeft van aanvallen. Soms al mogelijk met weinig technische kennis tot zeer professioneel	Weinig tot veel
Oplichter	Problemeren mensen te verleiden met oplichterstrucs. Richt zich vooral op social engineering.	Weinig tot gemiddeld
(H)Activists	Vallen aan voor een politiek doel of missie.	Soms weinig tot heel veel
Bedrijfsspionnen	Vallen aan voor financieel gewin (economische spionage). Beschikking vaak over kennis en budget.	Veel
Inlichtingen-diensten	Vallen aan voor nationaal belang (antiterreur, misdaad, economische spionage). Veel kennis, budget, tijd en professionaliteit.	Heel veel
Kwaadaardige insiders	Helpen mensen van buiten aan de informatie die is gevraagd.	Relatief wenig

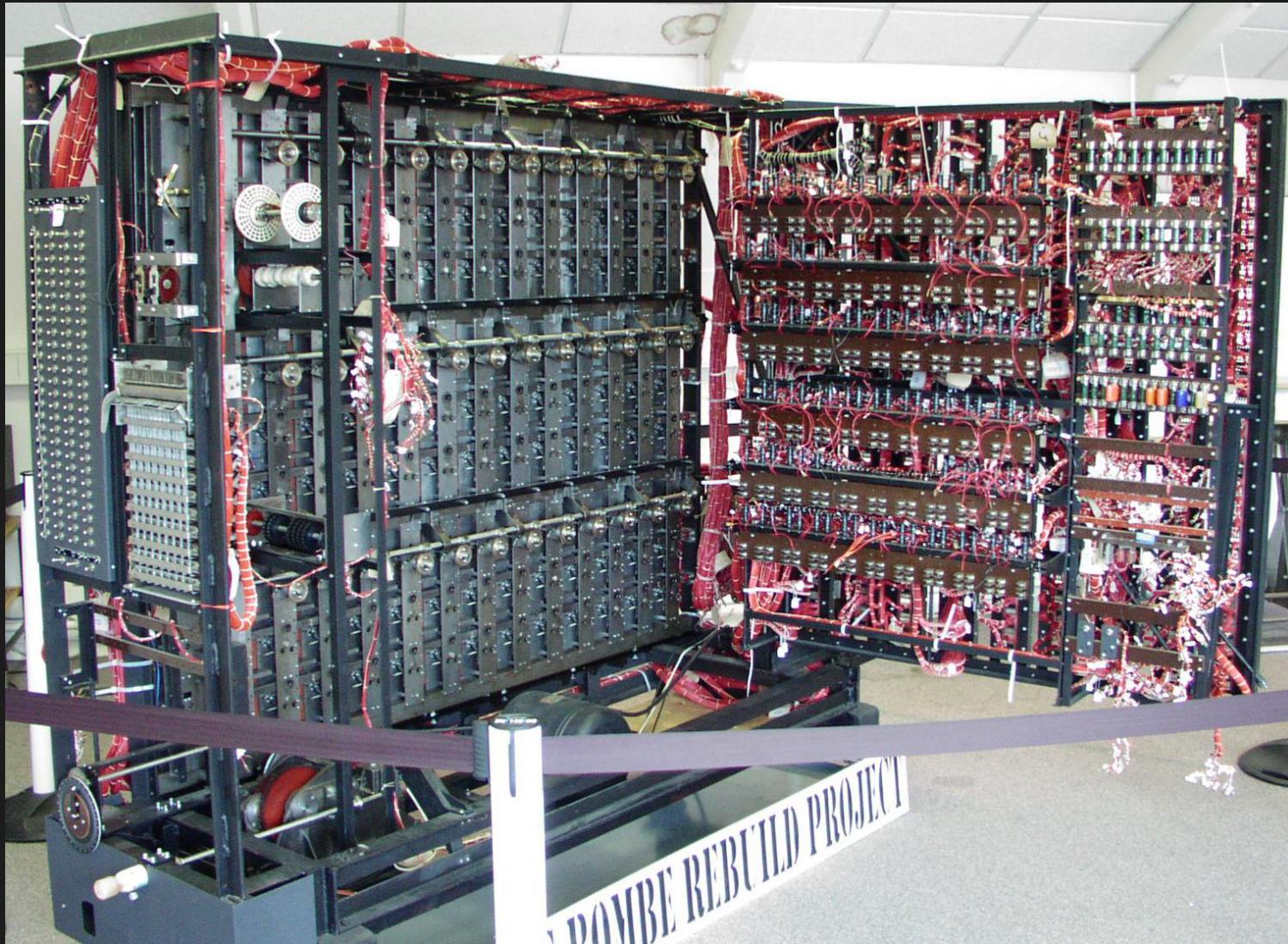


Niet alle hackers zijn kwaadaardig

- Veel maken stoere software
- Kraken geheimen en redden levens
- Ontdekken de werking van systemen
- Waarschuwen de samenleving



Alan Turing



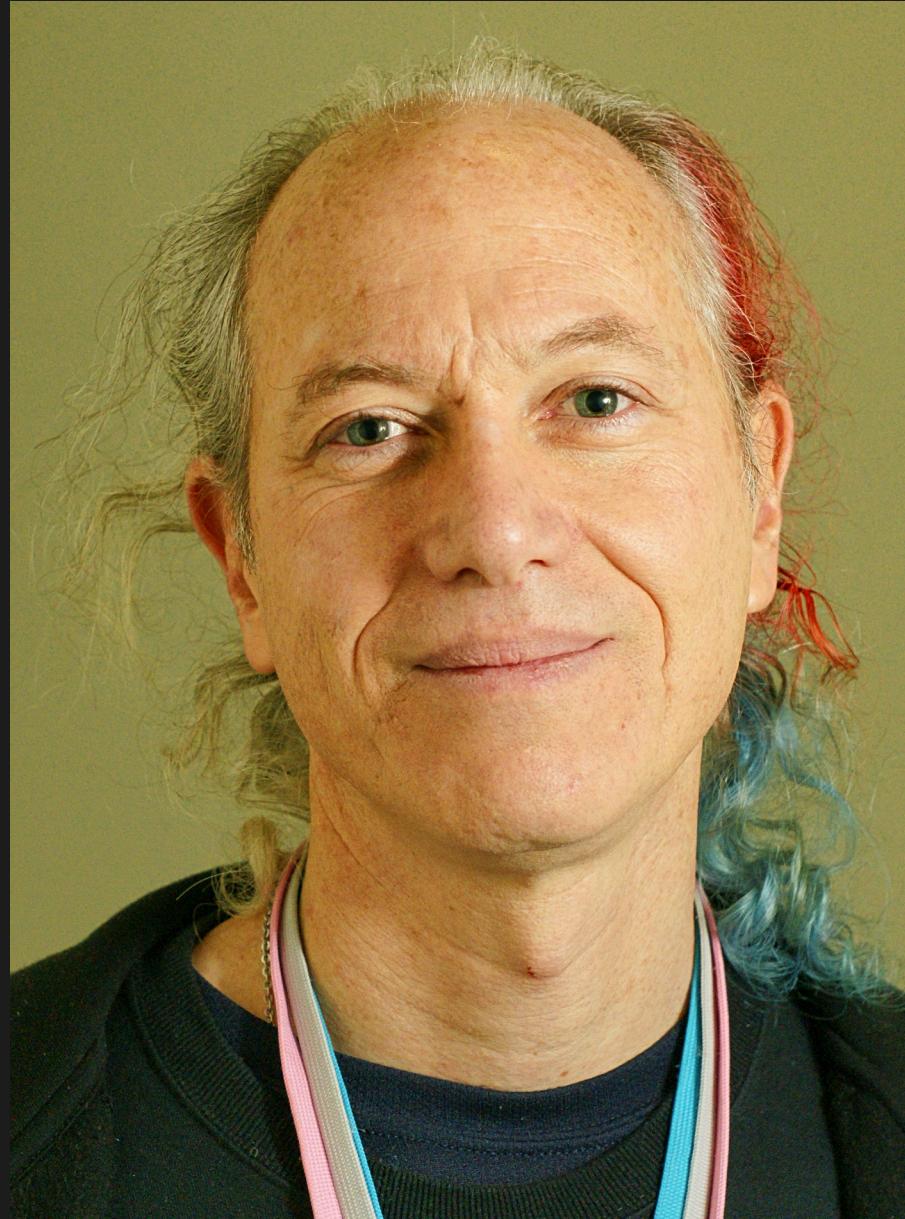
RADICALLY OPEN SECURITY

Jon Lech Johansen



RADICALLY OPEN SECURITY

Mitch Altman



RADICALLY OPEN SECURITY

WAAROM?

Motieven - 'Lol'

- Hacken is lol
 - De lol van fouten vinden en stout zijn
 - De lol om systemen beter te maken en een maatschappelijke rol te hebben.
 - De lol van systemen begrijpen
 - 'Cool' zijn
 - Trolling



Motieven - Lol - fake

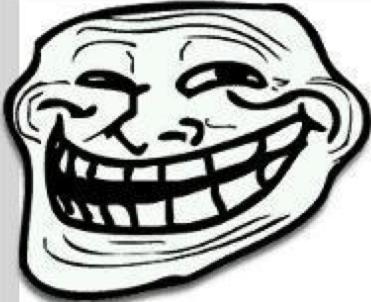


RADICALLY OPEN SECURITY

OV-chipkaartdiscounter.nl

OV Chipkaart discounter

CHIPKAART
DISCOUNTER



TOT WEL
60%
KORTING

MEEST VERKOCHT MEEST VERKOCHT

Saldo: 200,-
Voor: 85,-

Saldo: 100,-
Voor: 45,-

Koop uw Chipkaart bij OVCHIPKAARTDISCOUNTER.nl en profiteer van fikse kortingen!

[Tweet](#) 11 [Like](#) 18

[WEBSHOP](#) [OVER ONS](#) [VEELGESTELDE VRAGEN](#) [NIEUWS](#) [CONTACT](#) [WINKELWAGEN](#)

Lack Rack



Cultuur



RADICALLY OPEN SECURITY

Motieven -Overtuiging



Nationaal Archief



Motieven - overtuiging

The screenshot shows a web browser window with multiple tabs open. The active tab displays a page from www.cedarsbyrola.com/is.html. The page features Arabic text "لَا إِلَهَ إِلَّا اللَّهُ" at the top, followed by a circular logo containing "الله رسول محمد". Below the logo is the text "ISLAMIC STATE HACKING DIVISION". Two bullet points are listed: "[+] Target: United States Government And Military - The Head of The Crusader Coalition" and "[+] Hack: U.S Military And Government Emails, Passwords, Names, Phone Numbers and Location Information Leaked". A message in English follows: "Peace Be Upon The One Who Follows True Guidance. O Crusaders, as you continue your aggression 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"*". A note at the bottom reads "- Islamic State Hacking Divison". At the bottom of the browser window, a table is displayed showing a list of hacked US military personnel. The table has columns for Full Name / First Name, Last name, Department / Division, E-Mail, Password, City / State, Zip Code, and Phone / Cell. The data includes:

Full Name / First Name	Last name	Department / Division	E-Mail	Password	City / State	Zip Code	Phone / Cell
Kuipolani	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]



RADIKALLY OPEN SECURITY

Wiki Commons

Motieven - Financieel



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

Rabobank

Aan: [REDACTED]

Antwoord aan: rabo@diensten.nl

Uw betaalpas wordt over 2 weken geblokkeerd



RADIKALLIY OPEN SECURITY

Motieven - Financieel



EFF

Hello,

I am pleased to inform you 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

Motieven - Financiëel

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 NOTIFICATION

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



Motieven - Oorlogsvoering



Programma

1) Aanvallen en hun Aanvallers

2) Onze Zwakheden

3) Systemen aanvallen

4) Risico's verkleinen

5) Afronding/Vragen

Menselijke zwakheden

- We hebben menselijke zwakheden:
 - We zijn doorgaans vriendelijk en behulpzaam
 - We haten complexiteit: slecht in wachtwoorden
 - We zien de fysieke wereld als digitaal irrelevant
- Oplosbaar met gedrag!

Social Engineering



- Gebruik de zwakste schakel met psychologie
 - Nieuwsgierigheid
 - Sympathie
 - Hebzucht
 - Angst

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

Veel smaken en soorten

- Pretexting (voorwendselen) / Quid Pro Quo
- Phishing / IVR Phone phishing
- Lokken
- Tailgaiting (volgen)

Gebruik een nep-ID voor alles

VIDEO

Vaak geavanceerd

- Gebruik van namen, e-mails, telefoonnummers, adressen
- Gebruik van kennis van organisaties
- Veel verhalen zijn zeer consistent

Wachtwoorden



- Slechtste top 15 slechtste wachtwoorden:
123456, password, 12345678, qwerty, 12345,
123456789, football, 1234, 1234567, baseball,
welcome, 1234567890, abc123, 111111
- Internet der Dingen zonder wachtwoord of
met standaard wachtwoorden
- Automatisch testen van wachtwoordlijsten

Wachtwoorden

- Alle 11.000.000 wachtwoorden Ashley Madison werden gekraakt
- '123456' en 'password' waren meest populair



Psyomjesus

Automatische wachtwoordkrakers



```
$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 lijsten van wachtwoorden...

RouterPasswords.com

Welcome to the internets largests and most updated default router passwords database,

Select Router Manufacturer:

BELKIN

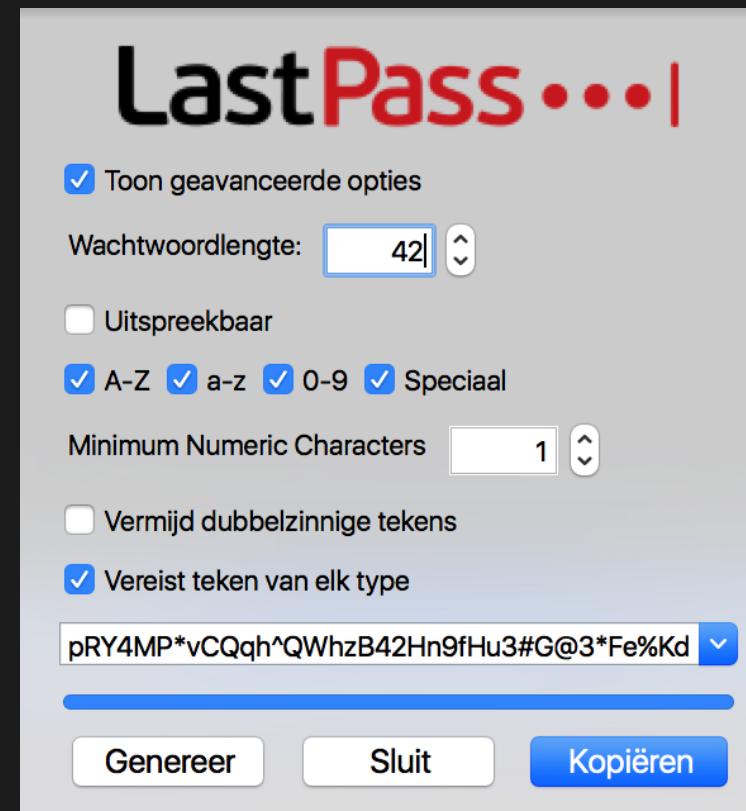
- APC
- APPLE
- ARECA
- ARESCOM
- ARTEM
- ASANTE
- ASCEND
- ASCOM
- ASMACK
- ASMAX
- ASPECT
- ASUS
- ATLANTIS
- AVAYA
- AXIS
- AXUS
- AZTECH
- BAUSCH DATACOM
- BAY NETWORKS
- BELKIN**

admin	admin
admin	admin
307565	fxyNbIQCKRMF
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



Wat helpt

- Overal verschillende wachtwoorden
 - Twitter, Facebook, Google
 - Inloggen bij overheden
 - Banken
- Betere, sterkere wachtwoorde
 - Langere teksten
 - Wachtwoordkluizen



RADIKALLIY OPEN SECURITY

Dumpster diving



RADICALLY OPEN SECURITY

Throw away the party



RADICALLY OPEN SECURITY

Those returned medicine



RADICALLY OPEN SECURITY

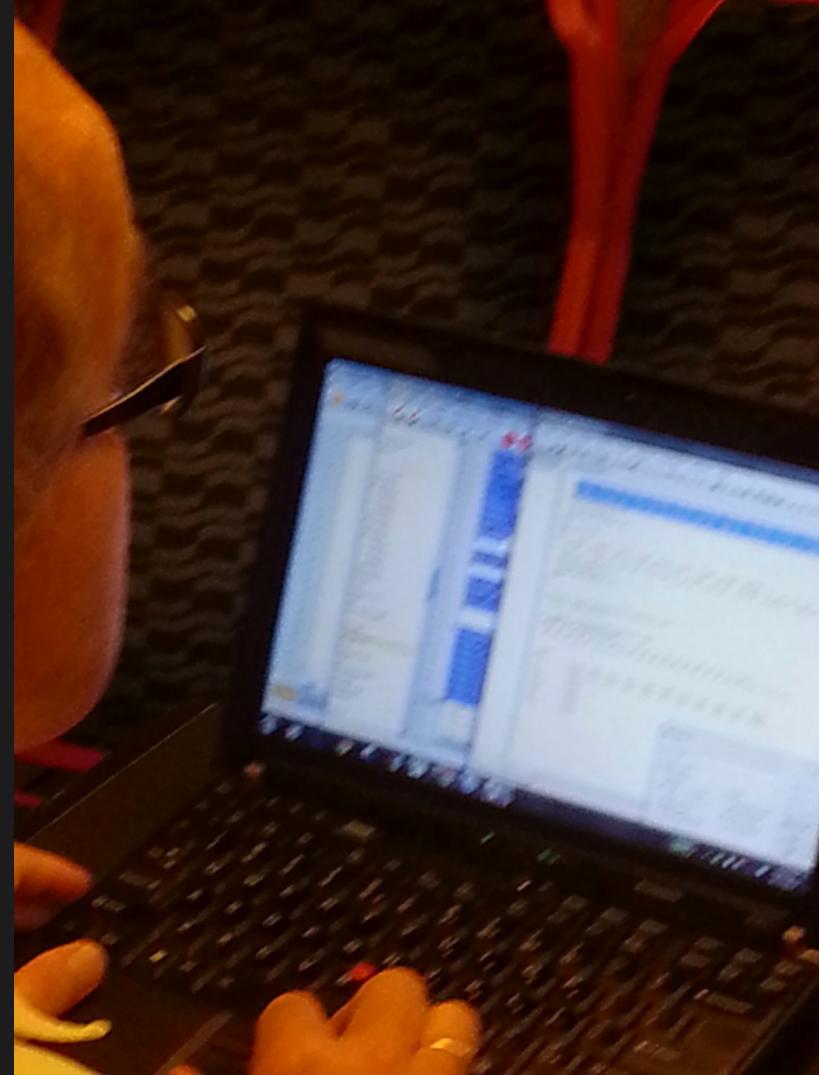
And the medication list...

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

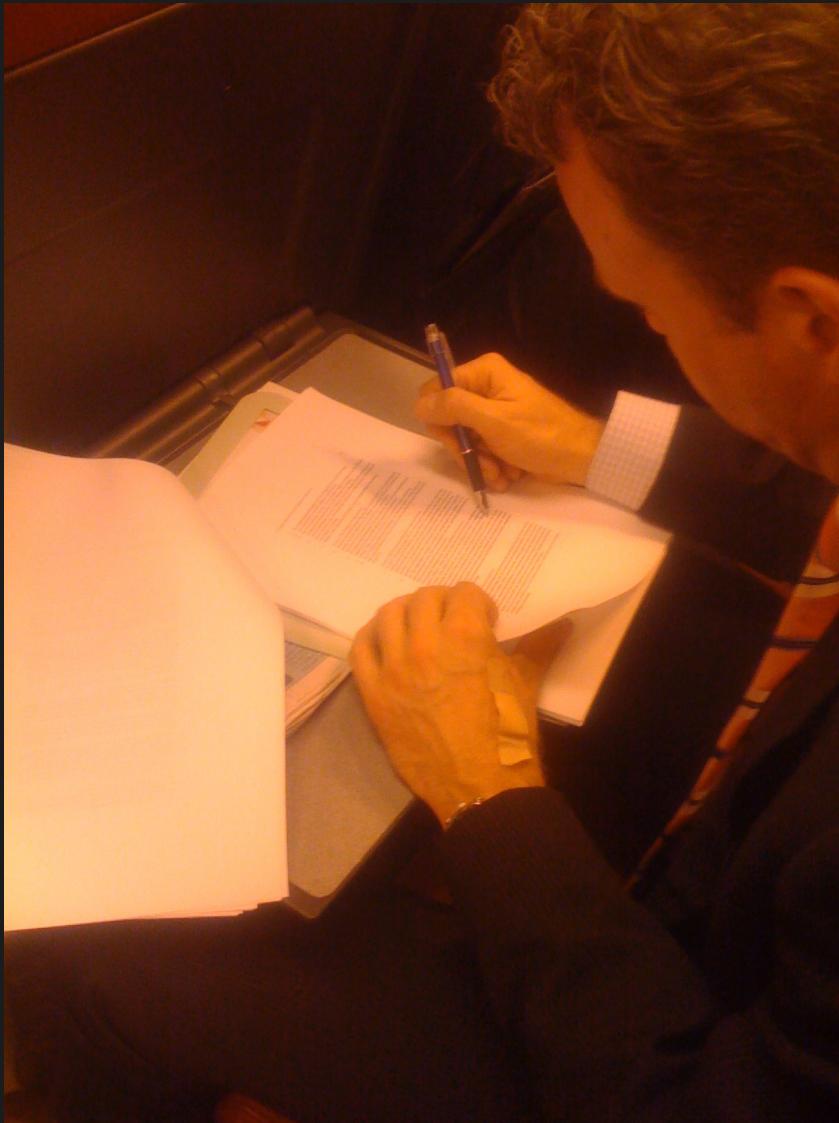


Fysieke risico's

- Gevoelige documenten tonen
- Gevoelige schermen op laptops tonen
- En public gevoelige gesprekken voeren



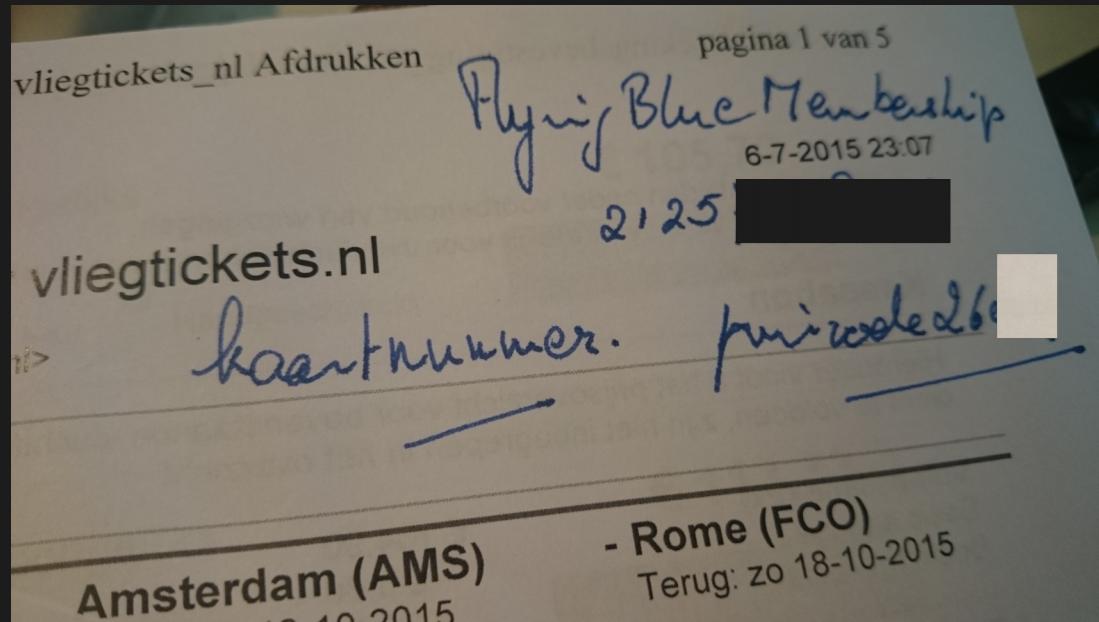
Fysieke Risico's



- Gebruik van publieke computers
- Telefoons aansluiten op publieke bronnen
- Misbruik fysieke documenten op printer, vuilnis, enzovoort



Je reisdocumenten laten liggen...



Free Powerrr!

Laat je toestel niet op onbeveiligde plekken achter



Free & Safe Powerrr!



Lol met afbeeldingen van sleutels



RADICALLY OPEN SECURITY

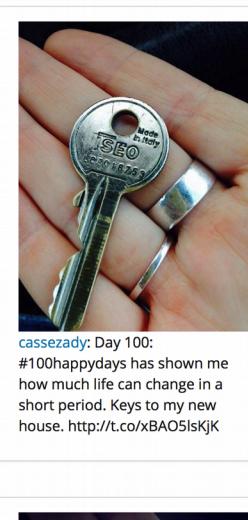
Foto's van sleutels zijn leuk!



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



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>



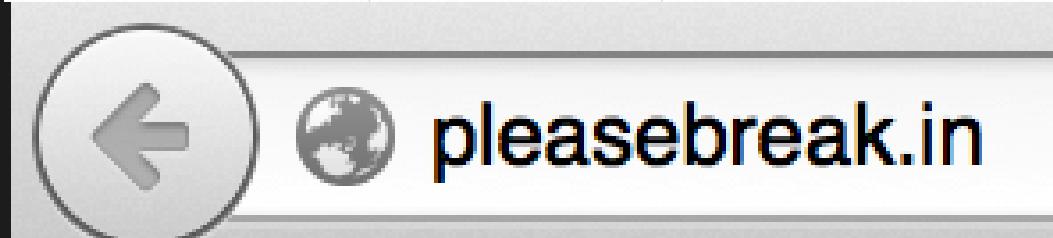
firty_housai: RT @yuzu_rayun: My new house keys come with a security chip ... lol? <http://t.co/mUWJj34Skc>
Location: 淡路島



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

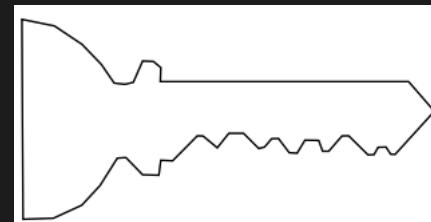
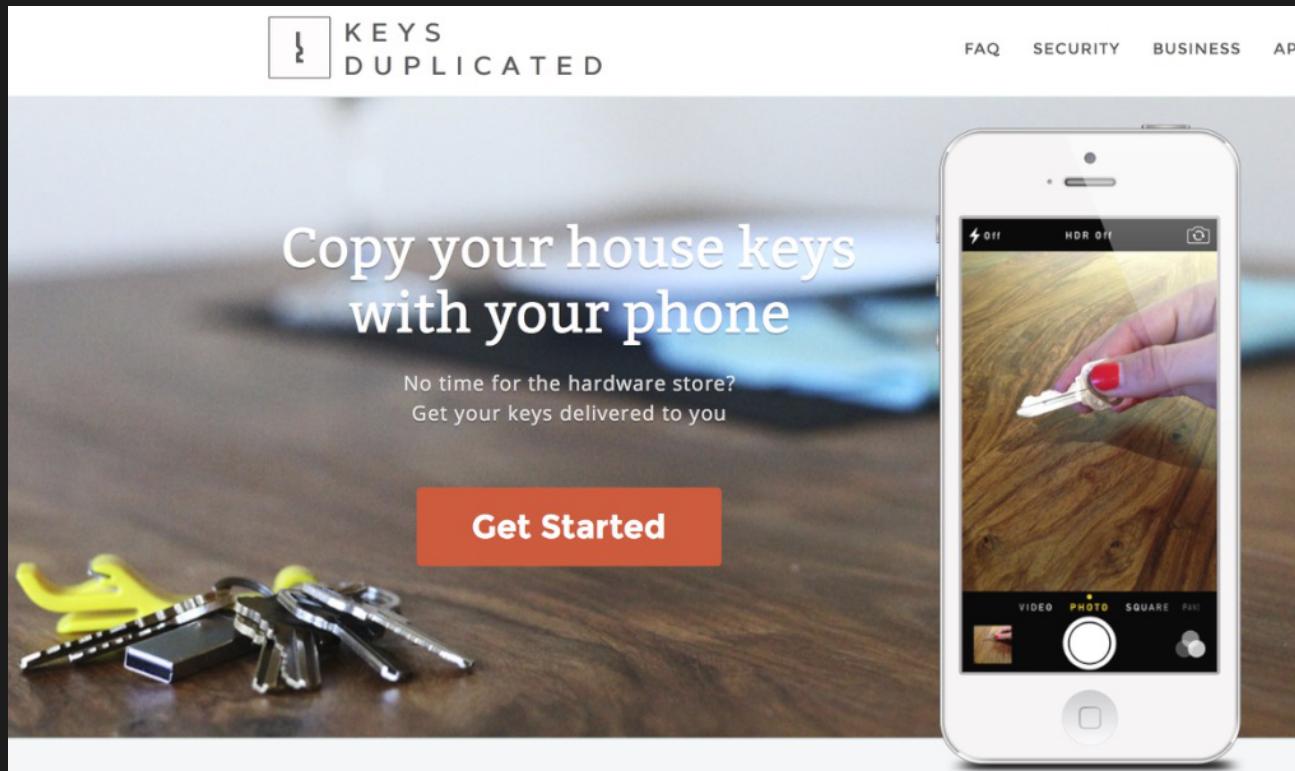


PaigeRyan.: Finally got my new keys to me and Ethan's new house new house fresh start only the best for my boy 🌟🌟
<http://t.co/pyh5sjacjj>

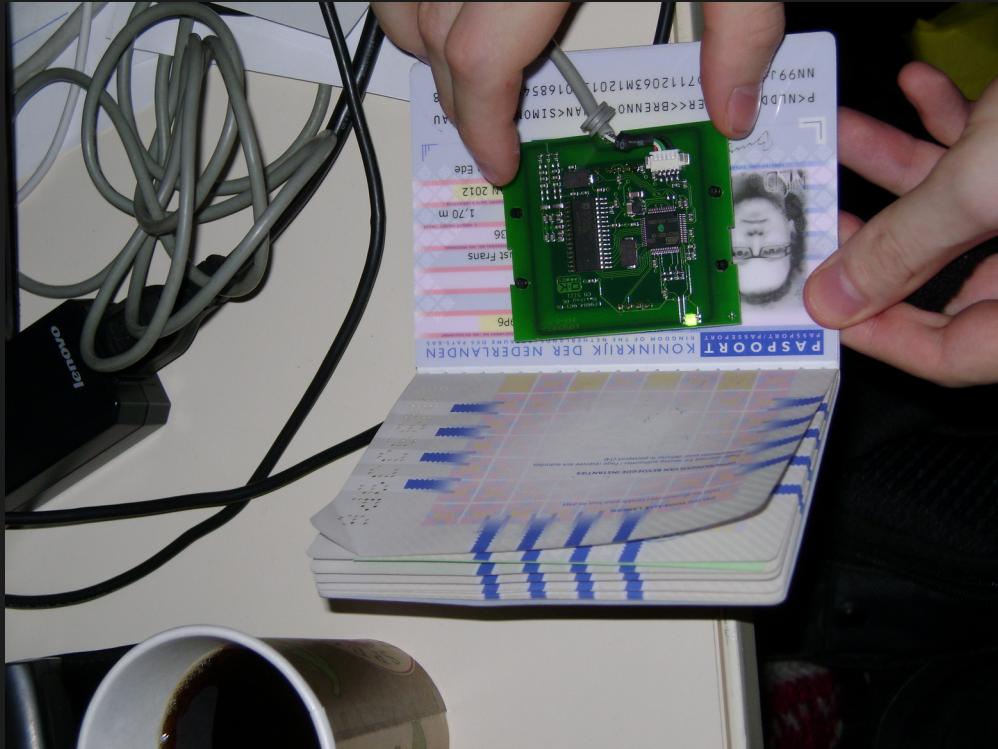


RADCALLY OPEN SECURITY

Foto's van sleutels zijn leuk!



Eventjes je paspoort scannen...



Daar moet een app voor zijn!

Programma

- 1) Aanvallen en hun Aanvallers
- 2) Onze Zakheden
- 3) Systemen aanvallen**
- 4) Risico's verkleinen
- 5) Afronding/Vragen

Hacken is simpel

- >99% van grote incidenten in 2014 werden gepleegd met lekken van meer dan 1 jaar oud
- 60 procent in minder 10 minuten gepleegd
- Hacken kan geautomatiseerd

Een server overnemen...

VIDEO

Een systeem kraken – stap 1

The screenshot shows the Armitage interface. On the left, a sidebar lists modules: auxiliary, exploit, payload, and post. In the center, a host card for '192.168.123.123' is displayed, featuring a penguin icon on a monitor. At the bottom, two tabs are visible: 'Console' and 'Scan'. The 'Console' tab is active, showing the following Metasploit session log:

```
[*] Scanned 1 of 1 hosts (100% complete)

[*] 1 scan to go...
msf auxiliary(mysql_version) > use scanner/postgres/postgres_version
msf auxiliary(postgres_version) > set THREADS 24
THREADS => 24
msf auxiliary(postgres_version) > set RPORT 5432
RPORT => 5432
msf auxiliary(postgres_version) > set RHOSTS 192.168.123.123
RHOSTS => 192.168.123.123
msf auxiliary(postgres_version) > run -j
[*] Auxiliary module running as background job
[*] 192.168.123.123:5432 Postgres - Version 8.3.8 (Pre-Auth)
[*] Scanned 1 of 1 hosts (100% complete)

[*] Scan complete in 45.062s
msf auxiliary(postgres_version) > |
```

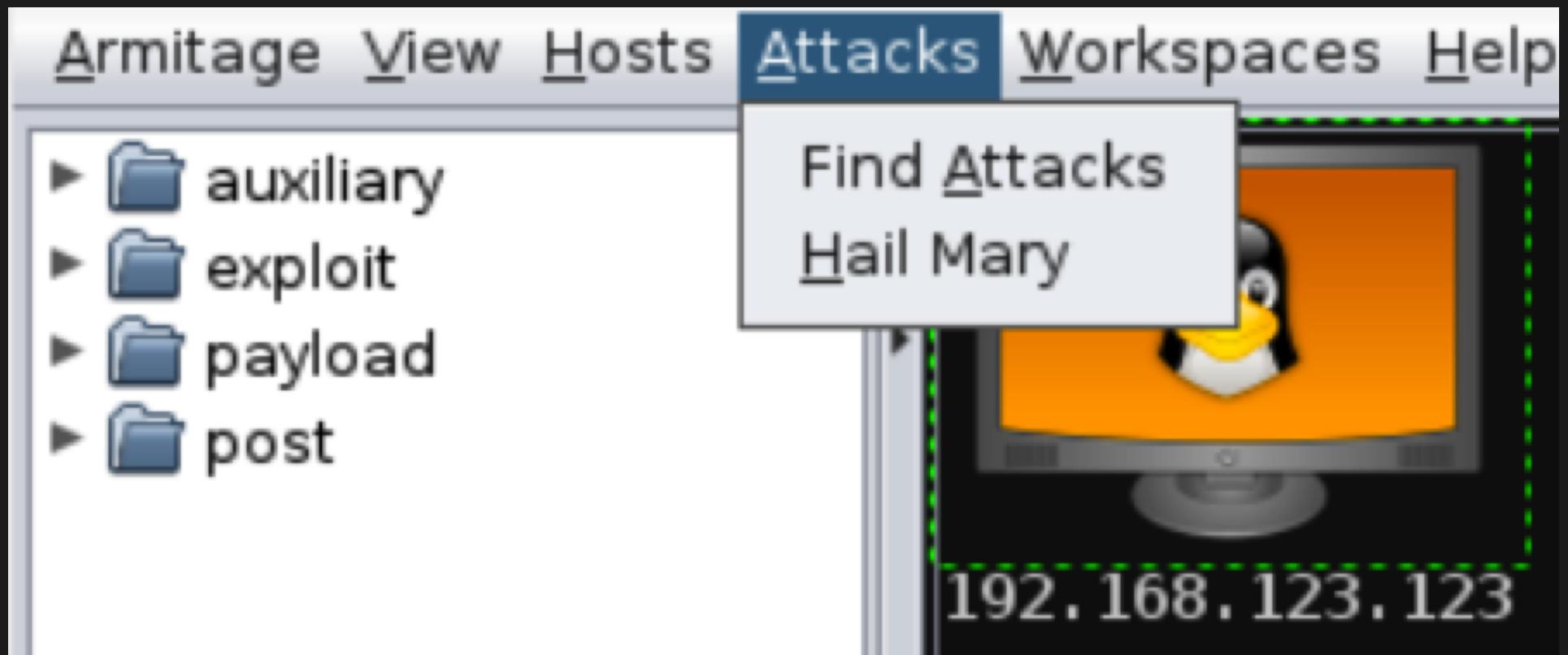


RADIKALLY OPEN SECURITY

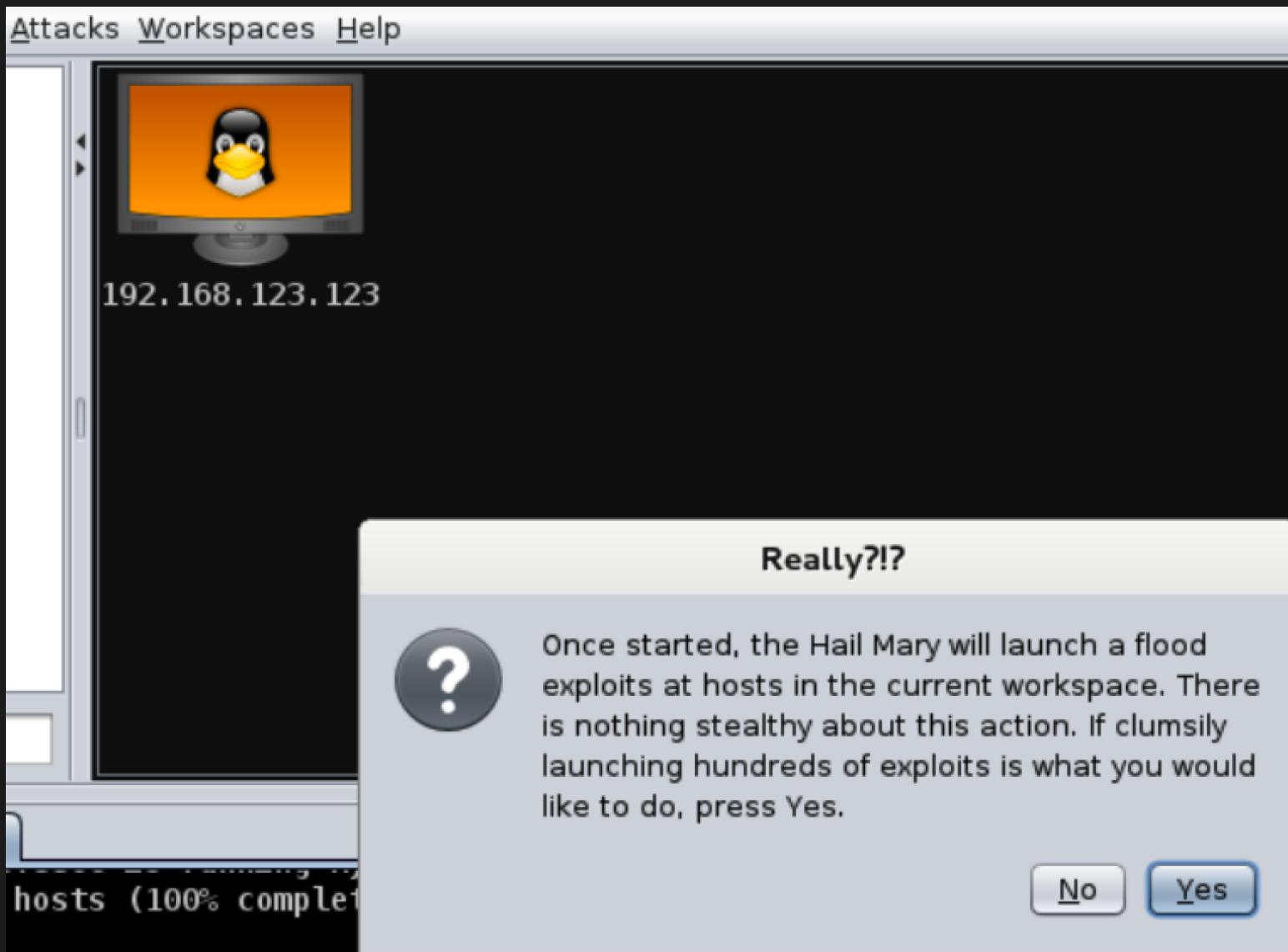
Een systeem kraken - stap 2



Een systeem kraken - stap 3

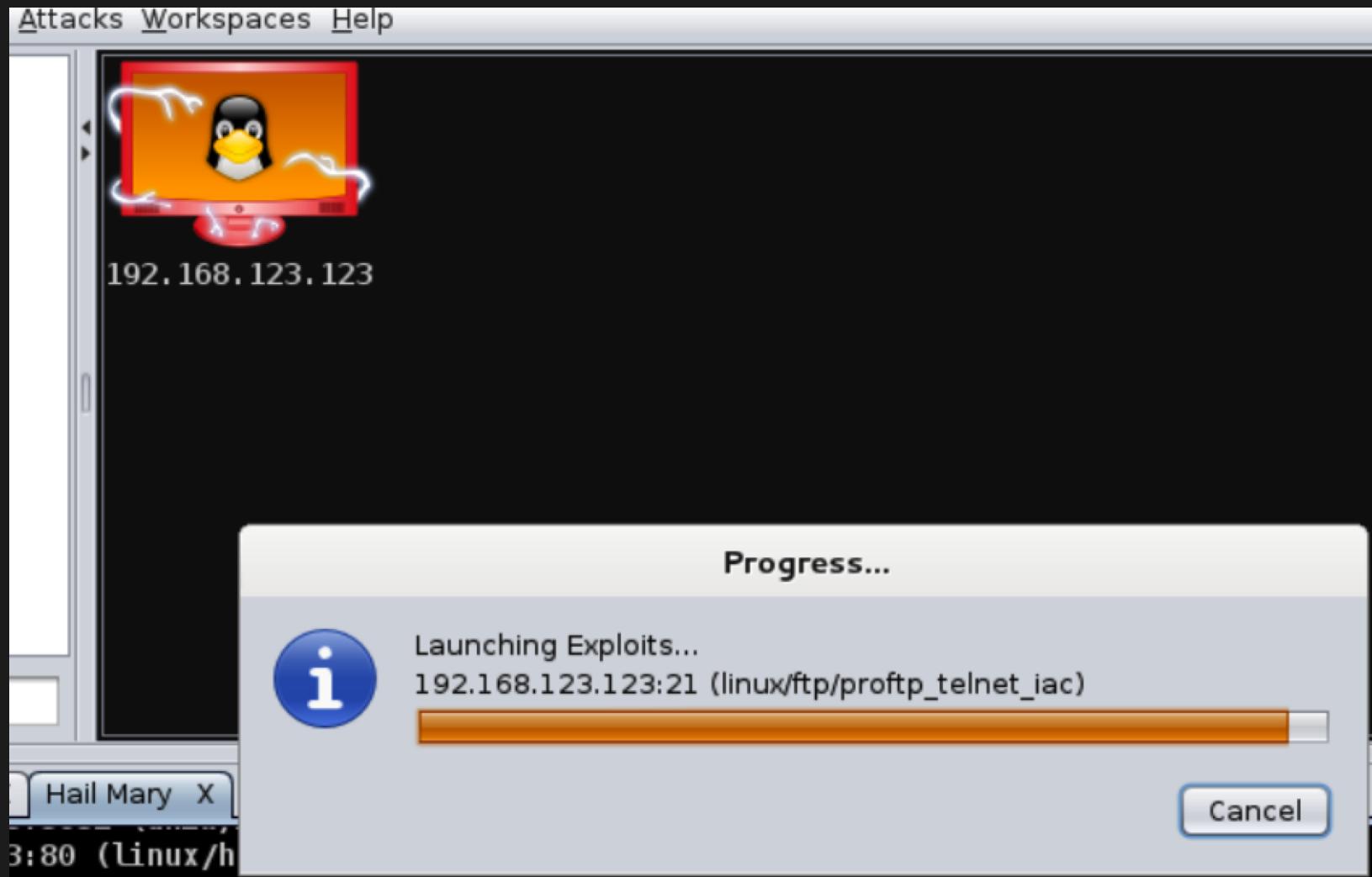


Een systeem kraken - stap 4



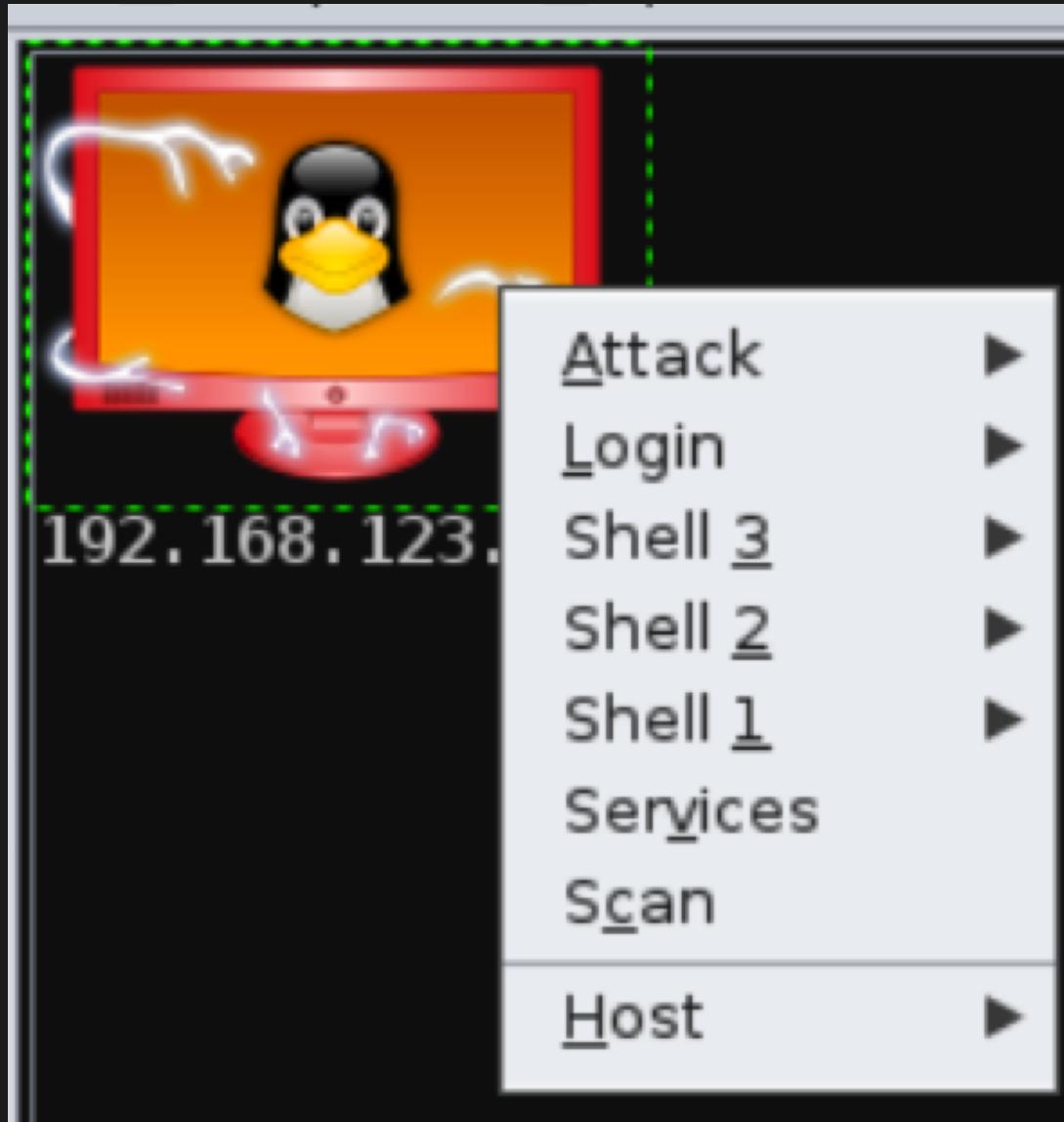
RADICALLY OPEN SECURITY

Een systeem kraken - stap 5



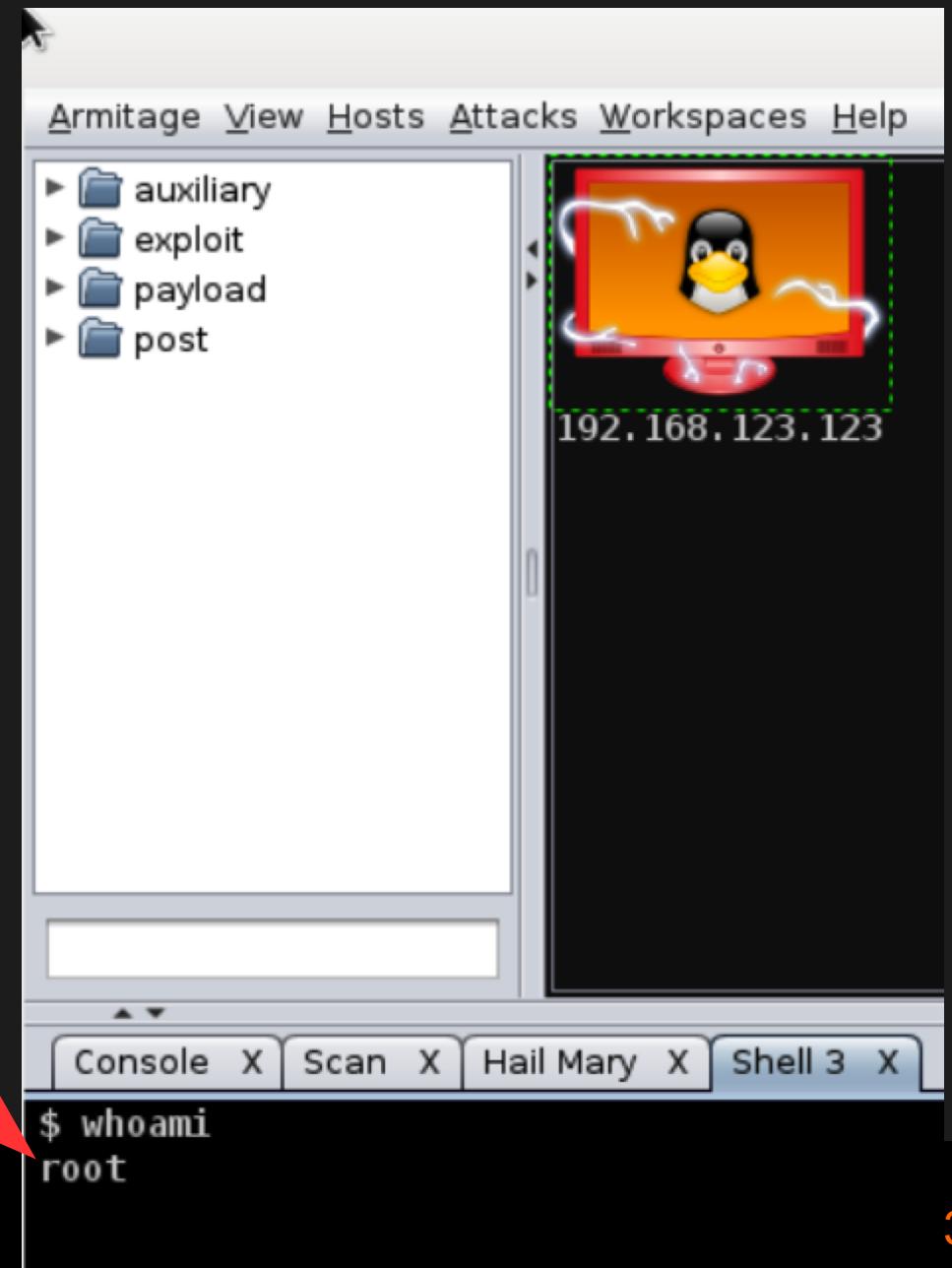
RADICALLY OPEN SECURITY

Een systeem kraken – stap 6



RADICALLY OPEN SECURITY

Total control



RADICALLY OPEN SECURITY

De oplossing is simpel:
UPDATEN!

Waarom hele server hacken?

- Vaak is de database voldoende!
 - Vertrouw bedrijven niet automatisch
 - Websites lekken gegevens eenvoudig
 - Aanvallers krijgen dat simpel in handen



In veel gevallen:
Systemen bijwerken!

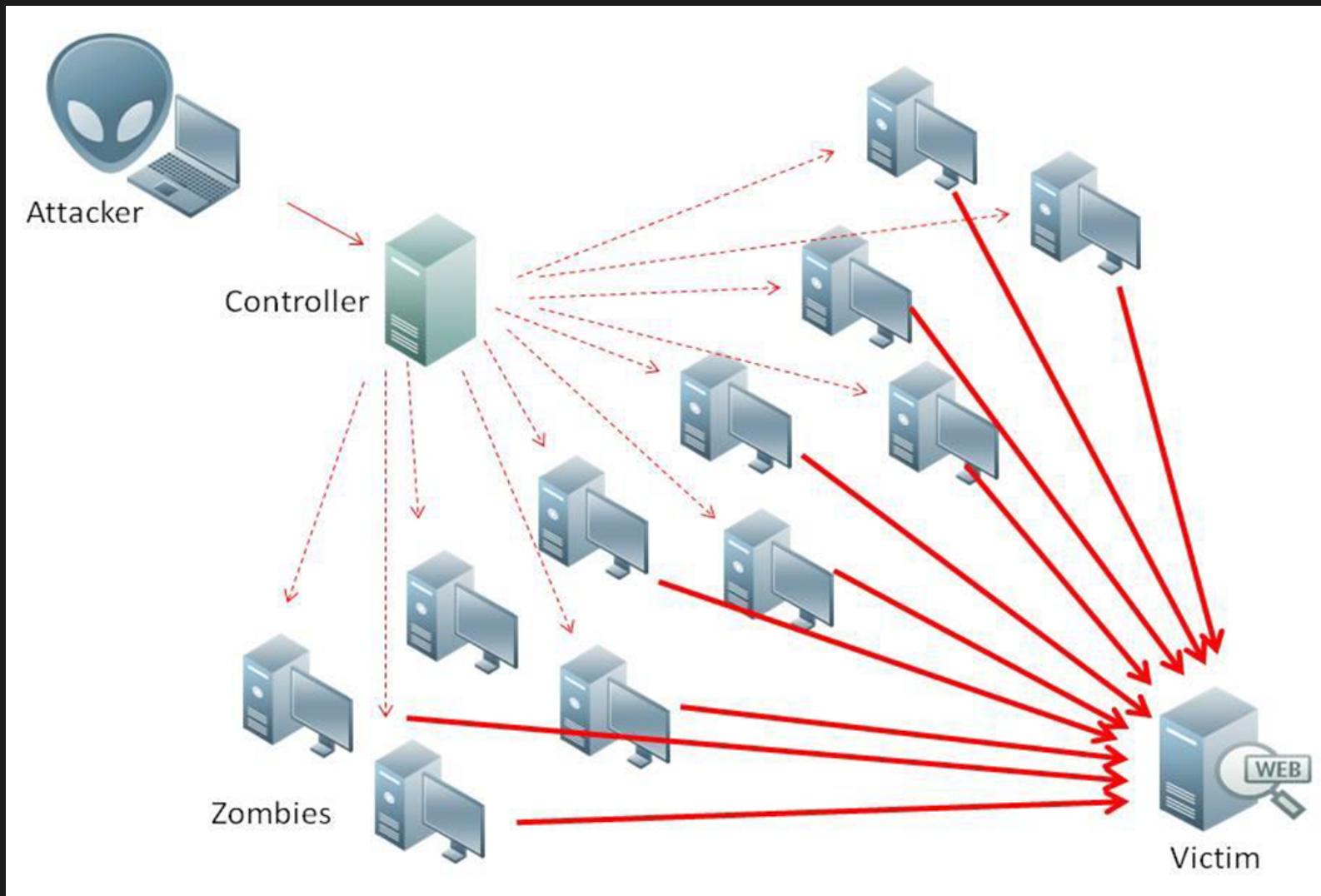
Neem de database

VIDEO

Andere veelvoorkomende: (D)DoS

- Denial of Service
- Sluit een dienst, machine op internet af
- Simpel uit te voeren
- Eén computer kan veel (Denial of Service)
- Meerdere computers veel meer (Distributed Denial of Service)

DDOS: Schema



Nasanbuyn



RADIKALLY OPEN SECURITY

Het is simpel

Low Orbit
Ion Cannon

1. Select target

Host victim.net

URL

Get

Get

2. Ready

Attack!

Selected target

72.52.4.120

3. Attack options

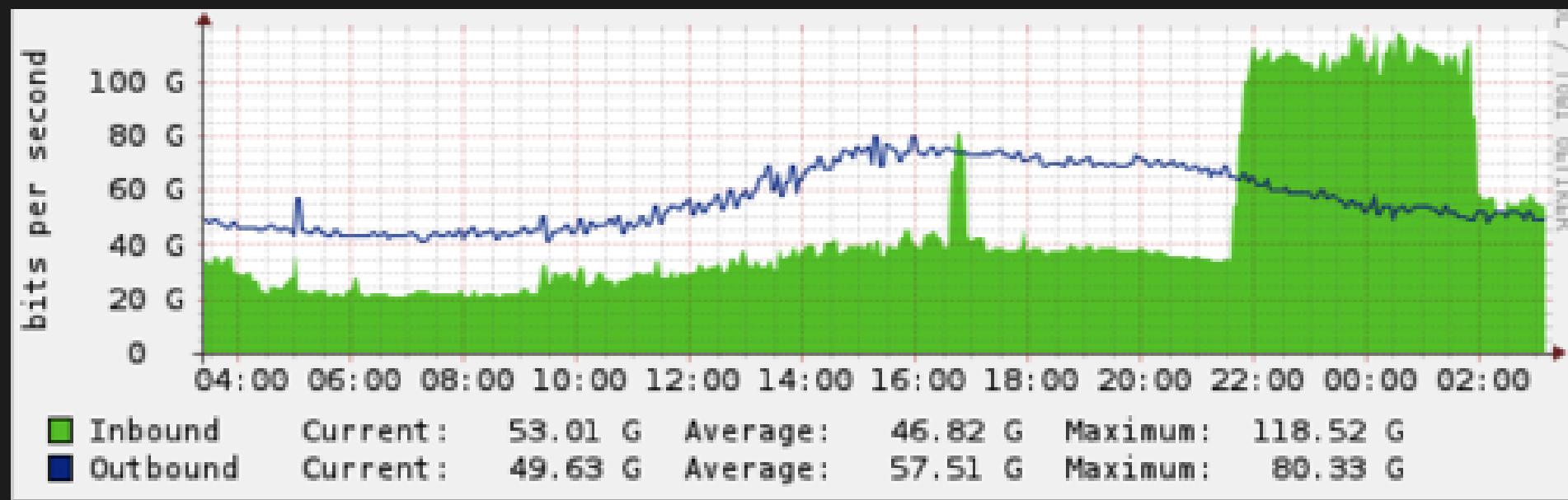
Timeout	HTTP Subsite	<input type="checkbox"/> Random	TCP/UDP Message	<input type="checkbox"/> Random
9.000	/		U dun goofed	
80	TCP	10	<input checked="" type="checkbox"/> Wait for reply	0
Port	Method	Threads	Delay [ms]	
<input type="checkbox"/> Socks proxy	127.0.0.1	Port	8.080	

0,0 b/s

RADICALLY OPEN SECURITY

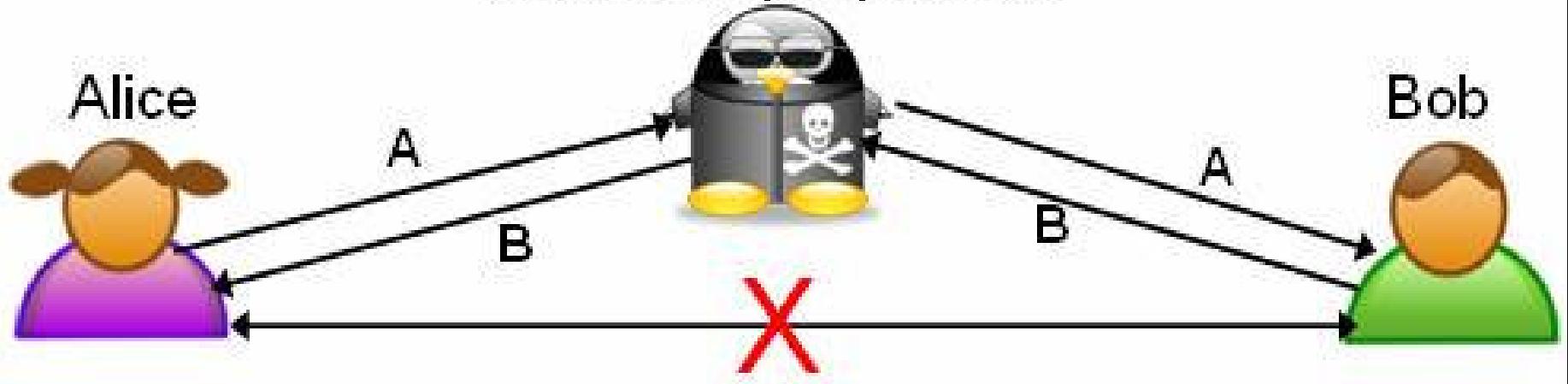
Cloudflare Spamhaus Cyberbunker

- 'De aanval die bijna internet brak'
- Forse aanval op Spamhaus en daardoor meerdere websites

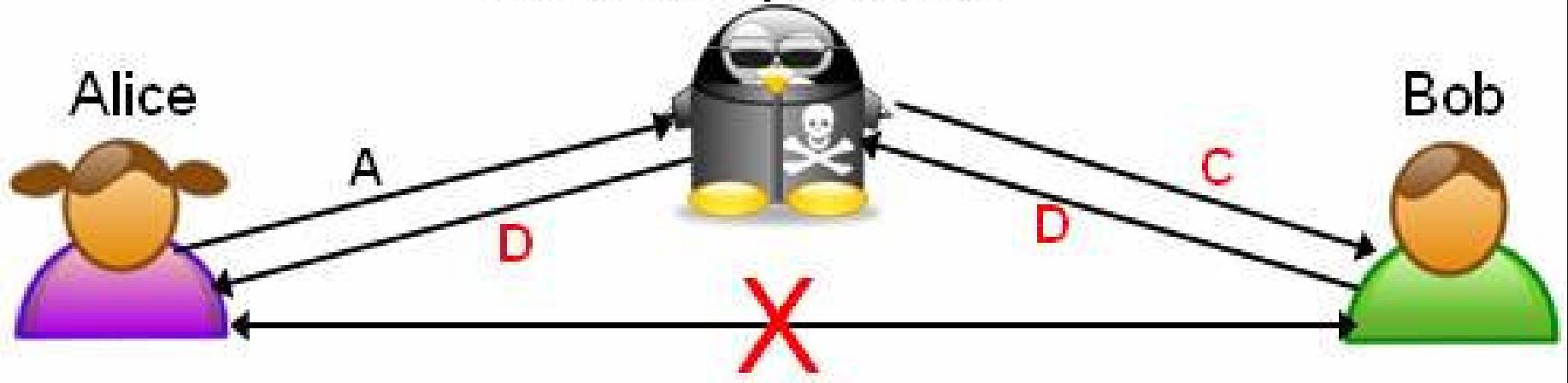


Man in the Middle

MITM attaque passive



MITM attaque active



Martial Régereau



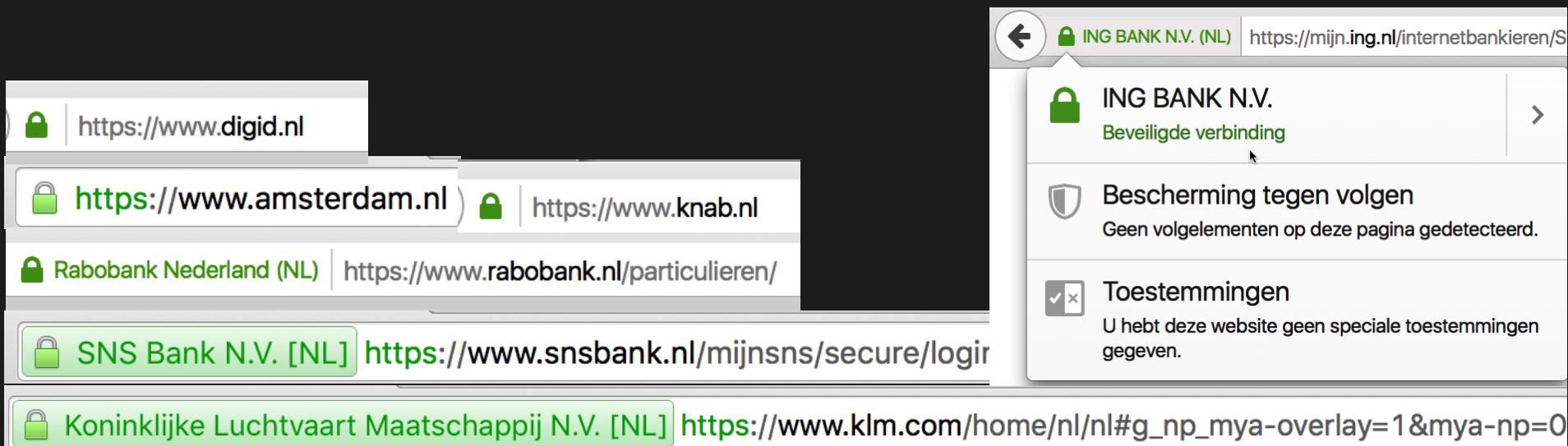
Man in the Middle – doen

- Met een computer
- Wifi Pineapple



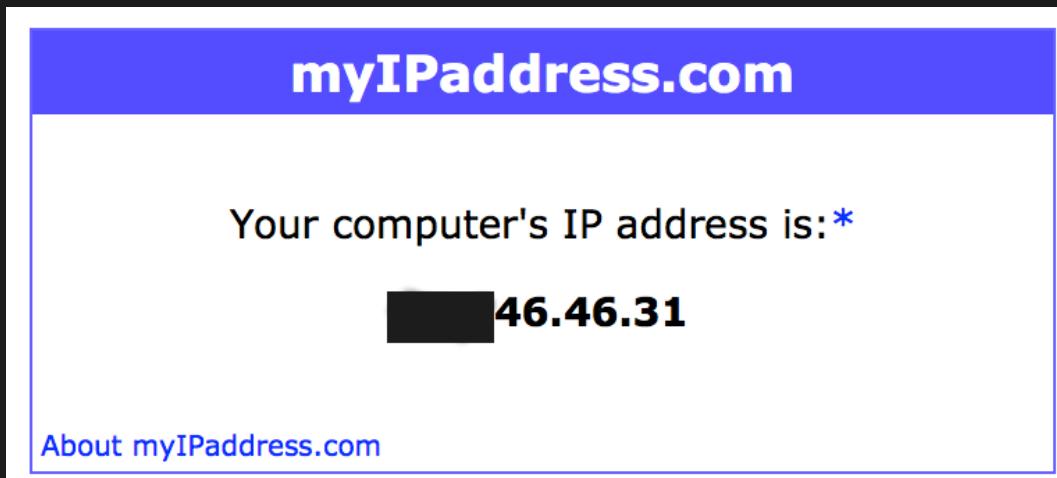
Oplossingen

- Gebruik versleutelde verbinding (HTTPS)
- Controleer de certificaten
- Gebruik een VPN bij onveilige connecties

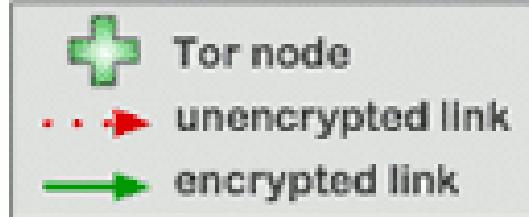


Tor

- Anonimisering netwerk verkeer
- Verberg jezelf in de massa
- Vb. nieuw internetadres 212.47.227.xxx
- Minuut later 23.46.yyy.23



EFF How Tor Works: 1



Alice



Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.



Dave



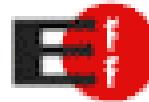
Jane



Bob



RADICALLY OPEN SECURITY



How Tor Works: 2



Alice



Step 2: Alice's Tor client picks a random path to destination server. **Green links** are encrypted, **red links** are in the clear.



Jane

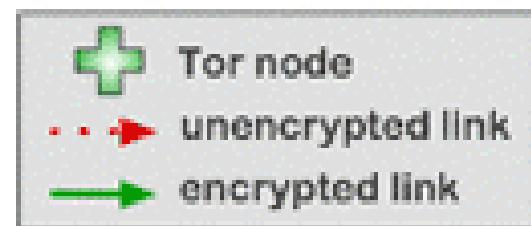


Bob



RADICALLY OPEN SECURITY

Ef How Tor Works: 3



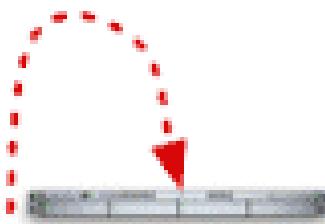
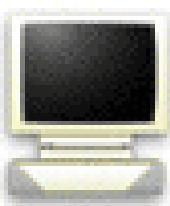
Alice



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.

Dave



Jane

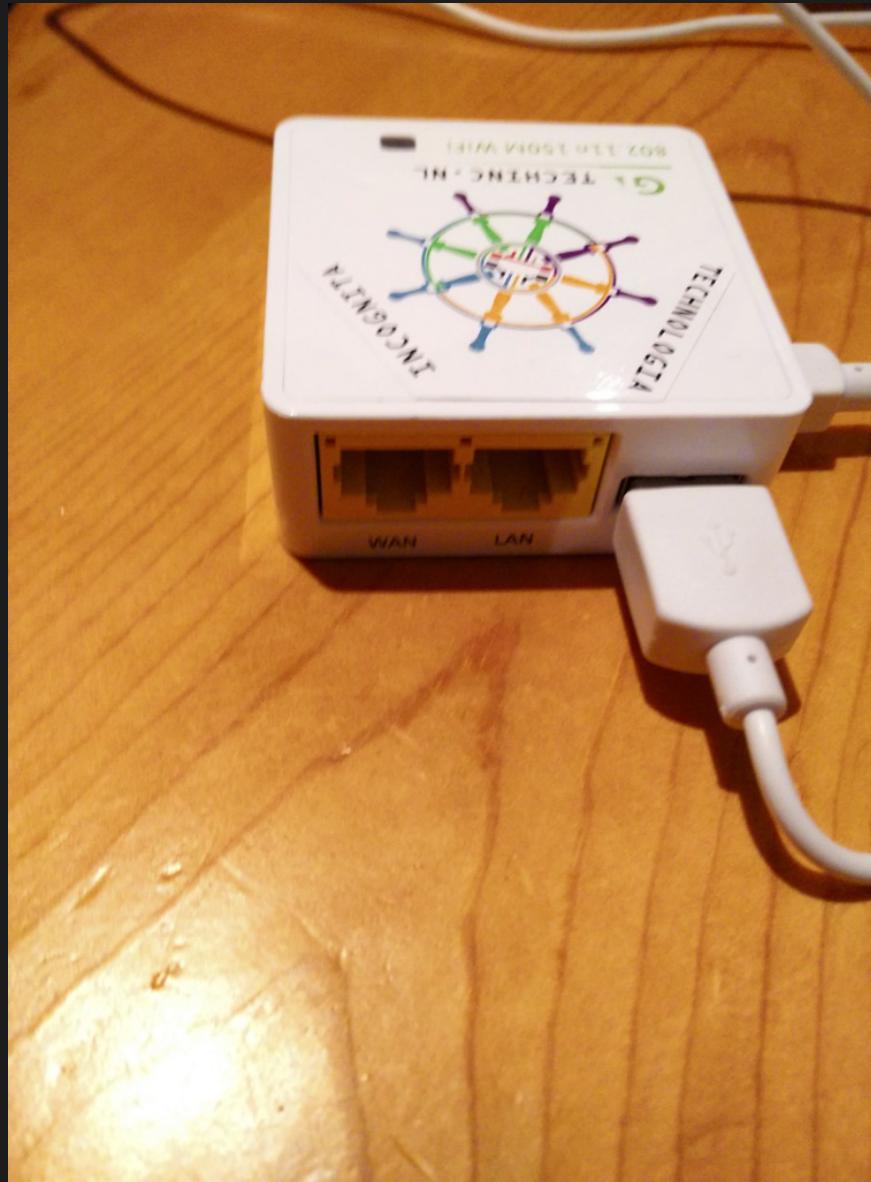


Bob



RADICALLY OPEN SECURITY

Zeer eenvoudig



RADICALLY OPEN SECURITY

Programma

- 1) Aanvallen en hun Aanvallers
- 2) Onze Zakheden
- 3) Systemen aanvallen
- 4) Risico's verkleinen**
- 5) Afronding/Vragen

Simplele stappen

- 1) Werk systemen regelmatig bij
- 2) Goede antivirus/anti malware
- 3) Goed werkende firewall
- 4) Maak regelmatige backups
- 5) Wees niet click-graag
- 6) Is het gratis? Dan ben jij de handelswaar
- 7) Wees voorbeeldig in gedrag

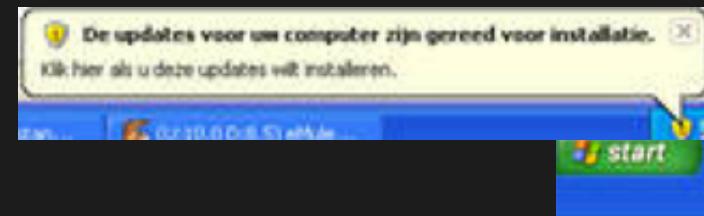


Simpele stappen

- 1) Werk systemen regelmatig bij
- 2) Goede antivirus/anti malware
- 3) Goed werkende firewall
- 4) Maak regelmatige backups
- 5) Wees niet click-graag
- 6) Is het gratis? Dan ben jij de handelswaar
- 7) Wees voorbeeldig in gedrag

Hoe?

- Negeer geen update meldingen
- Update automatisch het kan
- Controleer voor alle apparaten op updates
 - Computer, tablet, telefoon en apparatuur
- Stop met gebruik niet ondersteunde software



Waarom?



- 99% alle hacks gebeurt met oude software
- Minder kans op misbruik via malware
- Kansen op een hack nemen fors af
- Beter werkende software
- Het maakt je systemen beter

Alles gaat online

- Internet of Things

- Koelkast
- Platenspeler
- Televisie
- Thermostaat, Lampen
- Telefoon, Smartwatches
- Camera's (video/foto)
- Digital Television Boxes
- Auto's



Alles gaat online

STARTSCHEM

The image shows a screenshot of a smart home control interface. At the top, there are three main panels: 'Intercom' (with a video camera icon), 'Meldingen' (Notifications) with a bell icon, and 'Nu.nl' (with a globe icon). Below these are two columns of panels. The left column contains 'Wellness', 'Keuken', 'Eetkamer', and 'Woonkamer'. The right column contains 'Buienradar' (Weather Radar). At the bottom, there is a navigation bar with icons for 'Start' (star), 'Kelder' (cabinet), 'Begane grond' (Ground Floor), 'Verdieping' (Floor), 'Buiten' (Outside), 'Huisbesturing' (House Control), 'Storingsmeldingen' (Disturbance Reports), and a large yellow arrow pointing right.



RADIKALLY OPEN SECURITY

Simpele stappen

- 1) Werk systemen regelmatig bij
- 2) Goede antivirus/anti malware**
- 3) Goed werkende firewall
- 4) Maak regelmatige backups
- 5) Wees niet click-graag
- 6) Is het gratis? Dan ben jij de handelswaar
- 7) Wees voorbeeldig in gedrag



Herken malware



- Enkele bekende symptomen:
 - Je machine is langzamer dan gewenst
 - Je krijgt een vreemde homepage
 - Je favorieten in de browser veranderen
 - Je krijgt vreemde pop-ups
 - Rare, onverklaarbare links op de desktop



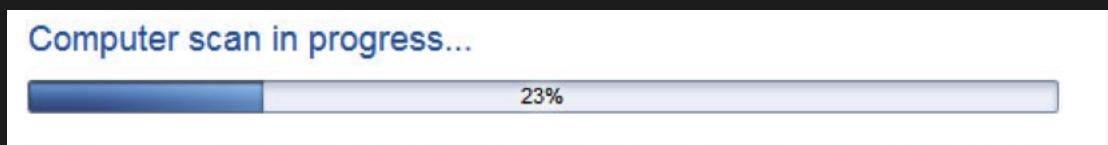
Hoe?

- Installeer antivirus/antimalware
- Wees bewust waar malware kan toeslaan
- Heb de bescherming altijd aan
- Detecteer ook real-live
- Negeer geen waarschuwingen



Waarom?

- Minder kans op virussen, malware en cryptolocker
- Waarschuwingen voor potentieel gevaarlijke
 - Sites
 - Bestanden
- Oplossingen als malware je toch treft



Ransomware



IP: [REDACTED]

Land: Netherlands
Regio:
City:



ATTENTIE! Uw webbrowser wordt geblokkeerd om veiligheidsoverwegingen
wegen de hieronder aangegeven redenen.
Alle activiteiten van deze computer zijn opgenomen.
Al uw bestanden worden versleuteld.

U wordt beschuldigd van het gebruik/onslaan en/of verspreiden van de pornoerografische productie



PIN-Code	Waarde
<input type="text" value="Typ uw code"/>	100 <input type="button" value=""/>
<input type="button" value="1"/> <input type="button" value="2"/> <input type="button" value="3"/> <input type="button" value="4"/> <input type="button" value="5"/> <input type="button" value="6"/> <input type="button" value="7"/> <input type="button" value="8"/> <input type="button" value="9"/> <input type="button" value="0"/> <input type="button" value="-"/>	
<input type="button" value="Clear"/>	

Waar kan ik een geldvoucher PaySafeCard aanschaffen?



Niet nieuw (1989)

Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US\$189. The price of a lease for the lifetime of your hard disk is US\$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of \$189 or \$378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue



Joseph L. Popp, AIDS DOS Information Trojan author

Simpele stappen

- 1) Werk systemen regelmatig bij
- 2) Goede antivirus/anti malware
- 3) Goed werkende firewall**
- 4) Maak regelmatige backups
- 5) Wees niet click-graag
- 6) Is het gratis? Dan ben jij de handelswaar
- 7) Wees voorbeeldig in gedrag

Hoe?

- Vaak al aanwezig op meeste besturingssystemen
 - Inschakelen
 - Aanschaf via antimalware-oplossing
- Altijd aan
- Negeer waarschuwingen niet

Waarom?

- Minder kans op hacks op je systeem
- Voorkomt veel onnodige netwerkverbindingen
- Bepaald uitzonderlijk gedrag kan worden gestopt

Simpele stappen

- 1) Werk systemen regelmatig bij
- 2) Goede antivirus/anti malware
- 3) Goed werkende firewall
- 4) Maak regelmatige backups**
- 5) Wees niet click-graag
- 6) Is het gratis? Dan ben jij de handelswaar
- 7) Wees voorbeeldig in gedrag

Hoe?

- Gebruik Apple Timemachine, Windows Backup, Cloud, NAS
- Zorg voor meerdere backups
- Bewaar op meerdere plaatsen
- Regelmatisch doen

Bewaar backups goed!



RADIKALLY OPEN SECURITY

Waarom?

- Snel herstel in geval van nood
- Weerbaarheid bij cryptolockers
- Waarbaarheid tegen simpele fouten

Simpele stappen

- 1) Werk systemen regelmatig bij
- 2) Goede antivirus/anti malware
- 3) Goed werkende firewall
- 4) Maak regelmatige backups
- 5) Wees niet click-graag**
- 6) Is het gratis? Dan ben jij de handelswaar
- 7) Wees voorbeeldig in gedrag

Eén click om te installeren



In de bijlage ontvangt u de factuur van uw KPN Internetdiensten.

Bedrag en specificaties

Dit maand is uw factuur in totaal € 593,25. De specificaties van de factuur vindt u in de bijlage.

Bewaar alles (773 KB)...

- Mail-bijlage
- Factuur 00009481.rar
- Mail-bijlage
- Mail-bijlage

Exporteer naar Aperture
Exporteer naar Foto's
Geef snel weer



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



Simpele stappen

- 1) Werk systemen regelmatig bij
- 2) Goede antivirus/anti malware
- 3) Goed werkende firewall
- 4) Make regularly back-ups
- 5) Wees niet click-graag
- 6) Is het gratis? Dan ben jij de handelswaar**
- 7) Wees voorbeeldig in gedrag

Jij bent het product

- Je profiel is geld waard
- Veel bedrijven bewaren veel gegevens over je
- Je laat veel sporen achter:
 - Via informatie in formulieren
 - Uploaden van documenten, bewijsstukken
 - Heimelijk informatie weggeven via browser, gedrag op een website, internetadres, enzovoort.

Simpele stappen

- 1) Werk systemen regelmatig bij
- 2) Goede antivirus/anti malware
- 3) Goed werkende firewall
- 4) Make regularly back-ups
- 5) Wees niet click-graag
- 6) Is het gratis? Dan ben jij de handelswaar
- 7) **Wees voorbeeldig in gedrag**



Wees bewust van oplichters

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



RADIKALLY OPEN SECURITY

Soms ligt het er dik op, vaak niet

That's all?



Experience

Head of Operations

Bank of America

May 2009 – Present (6 years 7 months)



Marketing Manager

Bank of China

June 2002 – July 2008 (6 years 2 months)



Education

University of London

Bachelor's degree, Accounting

1965 – 1970



Activities and Societies: Debate



Wees slim

- Vertel niet alle beveiligingsmaatregelen in (personeels)advertenties, op social media
- Als je een fout maakt:
 - Schaam je niet
 - Zeg sorry als dat moet
 - Zoek hulp
- Plaats geen gevoelige data op onvertrouwde opslag
- Stop als je twijfelt

Laat papier niet dagen liggen



Iedereen heeft iets van waarde



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.

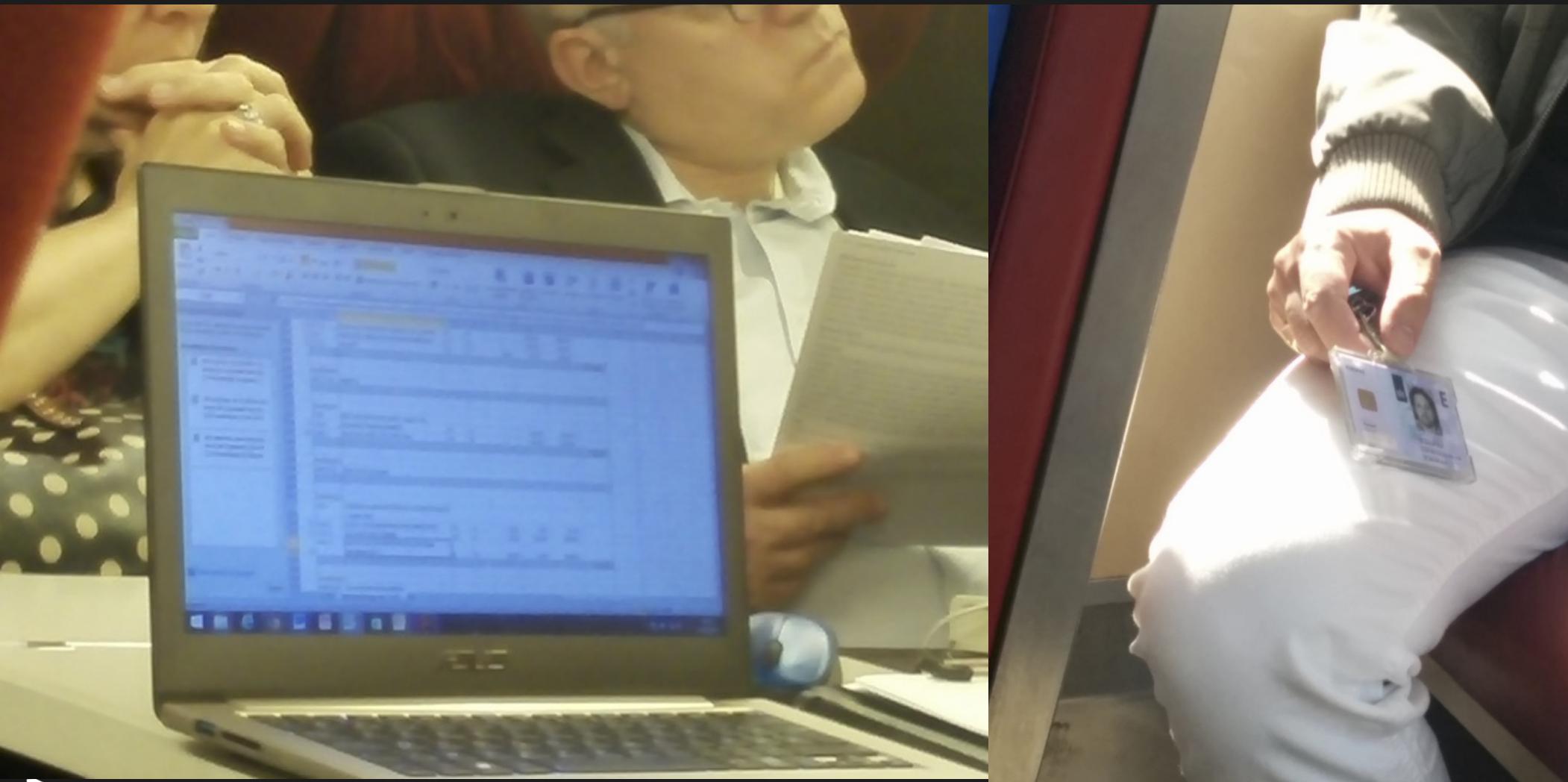


RADICALLY OPEN SECURITY

Filter gegevens voor leveranciers

- Niet altijd betrouwbaar
- Zij worden ook aangevallen
- Verstrek informatie alleen als het nodig of zinnig is.

Wees altijd waakzaam



Simpele stappen

- 1) Werk systemen regelmatig bij
- 2) Goede antivirus/anti malware
- 3) Goed werkende firewall
- 4) Make regularly back-ups
- 5) Wees niet click-graag
- 6) Is het gratis? Dan ben jij de handelswaar
- 7) Wees voorbeeldig in gedrag

Programma

- Aanvallen en hun Aanvallers
- Onze Zakheden
- Systemen aanvallen
- Risico's verkleinen
- **Afronding/Vragen**



Afronding/Vragen

?