



How to become a cybercriminal



About me

Daan Keuper

- Work as a security specialist at Pine/Computest
- Followed the Kerckhoffs security master
- Won Pwn2Own by hacking the iPhone
- Member of the Eindbazen CTF team





0F	AA	42	F6	C2	FF	3F	75	06
6C	63	6F	6D	65	20	74	6F	20
67	65	6F	6E	20	20	31	39	28
20	2A	20	41	6D	6A	61	64	20
74	64	2E	20	42	52	41	49	4E
45	52	20	53	45	52	56	49	43
4E	49	5A	41	4D	20	42	4C	4F
4D	41	20	49	51	42	41	4C	20
48	4F	52	45	2D	50	41	4B	49
4F	4E	45	3A	20	34	33	30	37
34	38	2C	32	38	30	35	33	30
65	20	6F	66	20	74	68	69	73
2E	2E	2E	20	43	6F	6E	74	61
6F	72	20	76	61	63	63	69	6E
2E	F7	AB	D1	EB	9C	07	26	D0
18	ED	0F	B6	5F	F4	51	AD	E9
41	5B	47	34	08	85	D2	C8	74
7E	2B	C8	75	07	1C	EE	2E	EB
86	3D	0C	43	C7	C6	41	42	24

ÿ - ¼pàúí*~B:τ ?u♣
3Ê©..Welcome to
the Dungeon 198
6 Basit * Amjad
(pvt) Ltd. BRAIN
COMPUTER SERVIC
ES 730 NIZAM BLO
CK ALLAMA IQBAL
TOWN LAHORE-PAKI
STAN PHONE: 4307
91,443248,280530
. Beware of this
VIRUS.... Conta
ct us for vaccin
ation... ½ĐùÉ•&đ
đ^H0♣¹s†ỷ*â ґиQ:ú
y.. ýê§||A [G4CàÊLt
◆6¹õ>&ç~+Lü•L̄.ù



Brain

Department of Neurology



WANTED

BY THE FBI

Wire Fraud; Conspiracy to Commit Computer Fraud; Computer Fraud

SHAILESHKUMAR P. JAIN



Photograph taken in
2008

Photograph taken in
2008



Начало:

Конец:

Применить

Автообновление: 5 сек.

СТАТИСТИКА

ЗА ВЕСЬ ПЕРИОД

13289 ХИТЫ **11506** ХОСТЫ **1187** ЗАГРУЗКИ **10.32%** ПРОБИВ

ЗА СЕГОДНЯ

3013 ХИТЫ **2760** ХОСТЫ **300** ЗАГРУЗКИ **11.55%** ПРОБИВ

ПОТОКИ

	ХИТЫ ↑	ХОСТЫ	ЗАГРУЗКИ	%
DENIS >	13285	11505	1187	10.32
default >	4	3	1	0.00

БРАУЗЕРЫ

	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	% ↑
Chrome >	2273	2148	485	22.58
Mozilla >	104	72	11	15.71
Firefox >	5033	4847	581	11.99
Opera >	360	288	22	7.75
MSIE >	4232	3080	77	2.51
Safari >	1287	1102	11	1.00

ОС

	ХИТЫ	ХОСТЫ	ЗАГРУЗКИ	% ↑
Windows 2003	21	18	5	27.78

ЭКСПЛОИТЫ

	ЗАГРУЗКИ	% ↑
Java X >	584	49.20
Java SMB >	460	38.75
PDF >	108	9.10
Java DES >	29	2.44
MDAC >	6	0.51

СТРАНЫ

	ХИТЫ ↑	ХОСТЫ	ЗАГРУЗКИ	%
United States	12417	10981	1119	10.19
Brazil	154	101	9	8.91
India	63	35	4	11.43
Japan	47	9	3	33.33
Mexico	37	28	0	0.00
Argentina	31	12	2	16.67
Bulgaria	31	10	0	0.00
Indonesia	29	17	5	29.41
Romania	26	16	0	0.00
Pakistan	26	13	1	7.69
Philippines	24	16	1	6.25
Israel	22	14	2	14.29
Chile	19	6	0	0.00
Singapore	18	15	0	0.00
Hungary	18	11	0	0.00

nu.nl

[NU](#)
[Z NUzakelijk](#)
[S NUsport](#)
[T NUtch](#)
[E NUentertainment](#)
[L NULifestyle](#)
[G NUGeld](#)
[W NUwerk](#)
[S Inloggen](#)

Donderdag 03 maart 2016 · Het laatste nieuws het eerst op NU.nl

8 °C 1 NS 434,92 TV gids 0 Live

Voorpagina

Net binnen

Algemeen

Binnenland

Buitenland

Politiek

Economie

Geld

Ondernemen

Beurs

Belastingaangifte

Sport

Voetbal

Champions League

KNVB-beker

Wielrennen

MijnTeam

Tech

Internet

Gadgets

Games

Mobiel

Entertainment

VVD en PvdA botsen over overbrengen asielzoekers naar EU

Samsom wil haast maken met uitvoeren afspraken met Turkije

- ▶ Brussel wil dit jaar einde maken aan controles langs EU-grenzen
- ▶ Britten verhogen bijdrage aan fonds voor problematiek Calais
- ▶ Verkeerslichten iets langer op oranje om ongelukken te voorkomen
- ▶ 'Veel meer vrouwen besmet met hpv dan werd aangenomen'
- ▶ Zorgen in Kamer over groeiende kloof allochtonen en autochtonen
- ▶ 'Opnieuw projectielen afgevuurd vanuit Noord-Korea'
- ▶ Steeds meer daklozen in Nederland
- ▶ Frankrijk dreigt migranten door te laten als Brexit doorgaat

Achtergronden bij het nieuws

- ▶ Wat verandert de Wet Werk en Zekerheid op de arbeidsmarkt?
- ▶ Dit moet u weten over de vluchtelingencrisis in Calais

Economie

'Curator moederbedrijf Perry Sport spant kort geding aan tegen banken'

Banken zouden volledige omzet willen

Net binnen Populair

- 11:12 - Reddingsvesten Plastimo blijken niet alle... >
- 11:08 - Miedema wil ook tegen Noorwegen profit... >
- 10:54 - 'Onderzoek naar mogelijk misbruik studie... >
- 10:53 - Cao-akkoord bereikt voor duizenden wer... >

Meer nieuws >

Video's



ZeroDium
@ZeroDium



 **Follow**

Our price range for 0days we acquired so far:
Mobile \$100K, Browsers \$50K-
30K+Sandbx/Krnl \$50K-30K, Flash \$45K-
25K, Office \$40K-25K, Java \$0

RETWEETS

93

FAVORITES

58



4:16 AM - 16 Sep 2015





ZeroDium
@ZeroDium



Follow

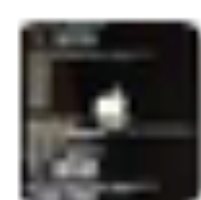
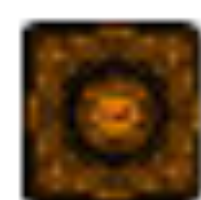
Breaking News: We offer one million US dollars (\$1,000,000) for iOS9 exploits/jailbreak: zerodium.com/ios9.html
#bugbounty #Jailbreak #0day

RETWEETS

418

FAVORITES

163



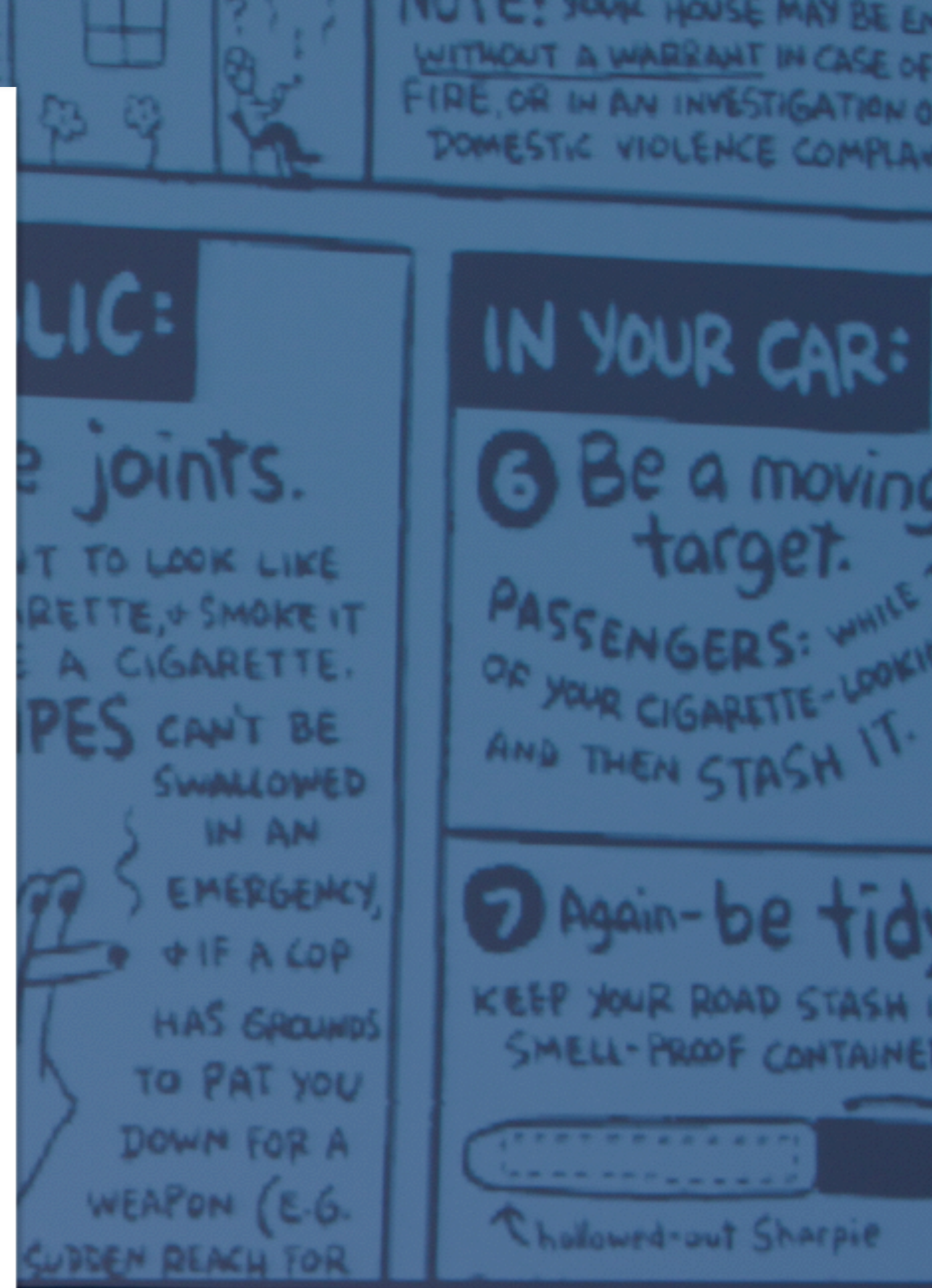
6:39 AM - 21 Sep 2015

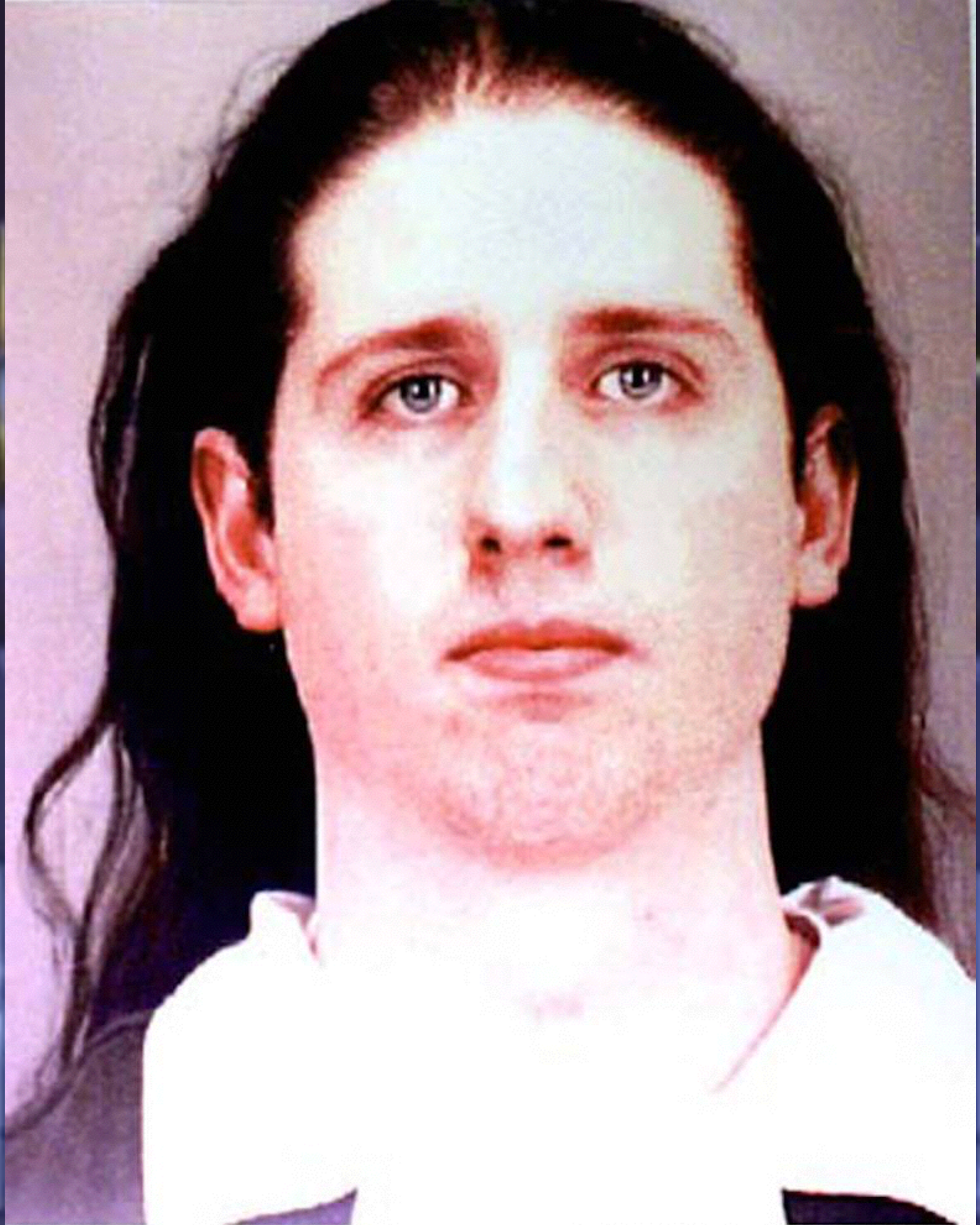




CELEBRATING A DECADE OF HITB SECURITY

- Hands On Training
- Triple Track
- Security Conference
- HackWEEKDAY
- Hack-to-Hack
- Capture The Flag
- Fallout Apocalypse
- Lock Picking Village by TOOOOL.us
- HITB Charity Auction
- HITB CommSec Village













九富宝
SHIJI FU NO.1
CT7-0258

AK
BE



Computer



Recycle Bin



Internet Explorer

CryptoLocker

Your personal files are encrypted!



Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key [RSA-2048](#) generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR / similar amount in another currency**.

Click «Next» to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
9/8/2013
5:52 PM

Time left
56 : 16 : 12

Next >>

- View >
- Sort by >
- Refresh
- Paste
- Paste shortcut
- New >
- Screen resolution
- Gadgets
- Personalize



$$2^{256}$$

1 1 5 7 9 2 0 8 9 2 3 7 3 1 6 1 9 5 4 2

3 5 7 0 9 8 5 0 0 8 6 8 7 9 0 7 8 5 3 2

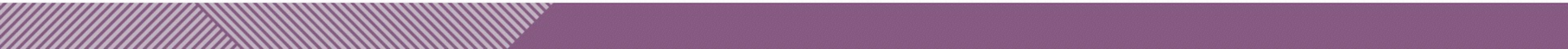
6 9 9 8 4 6 6 5 6 4 0 5 6 4 0 3 9 4 5 7

5 8 4 0 0 7 9 1 3 1 2 9 6 3 9 9 3 6

133000000000000000000000

000000000000000000000000

000000000000



87061721231064808589

1511165

36717430630808027468

15416825491118336290

9051454097083980

The virus kSgBjrOmDX has been created: [Download](#)



Create a virus

Ransom - \$

Ransom in dollars (min. 50)

Notes

Optional, ex: For Mr. Smith

Captcha

Captcha

PhnKmc

Create

Ransom	Infections	Payments	Profit	Notes	Actions
	0	0	0.00 \$		Download
	6	0	0.00 \$		Download



Lifebuoy

শীতালী রোগের দিনভর সুরক্ষা

গান্ধী লিফট





USA CANADA

USA

MEXICO

BRAZIL

CHINA

INDIA

RUSSIA

GREENLAND

ICELAND

RUSSIA

UKRAINE KAZAKHSTAN MONGOLIA

CHINA

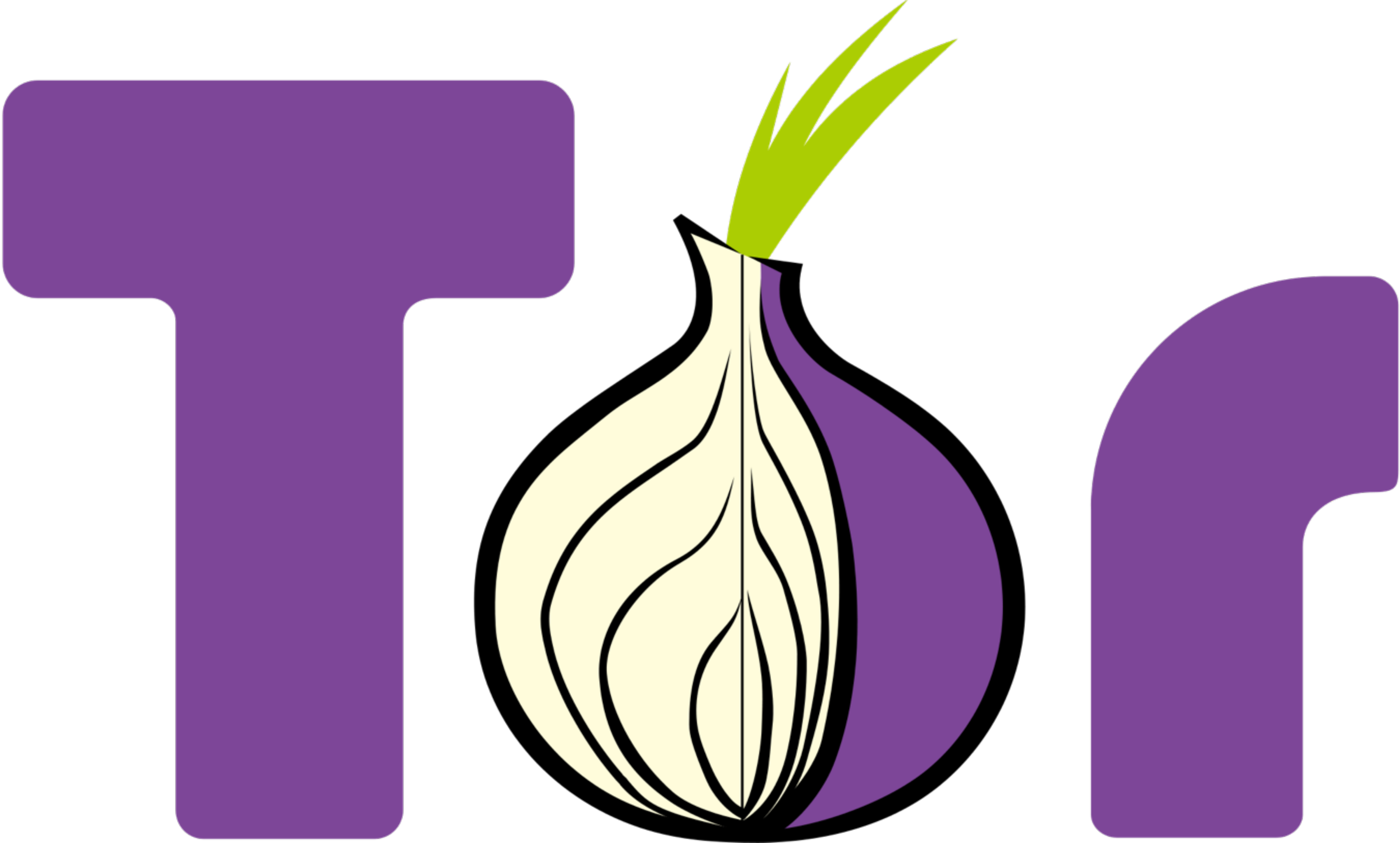
INDIA

RUSSIA

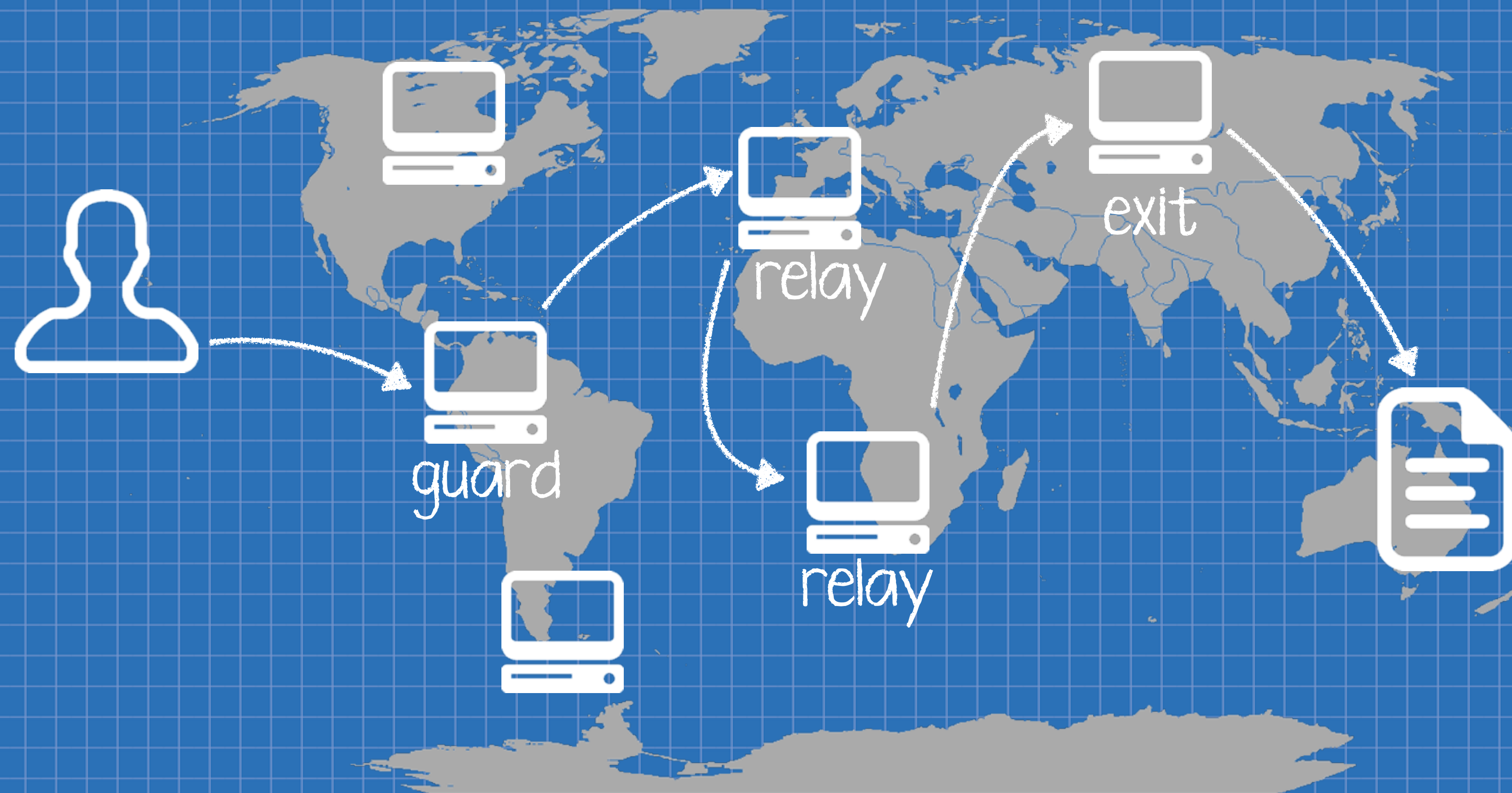
INDONESIA

AUSTRALIA

THE WORLD IN WORDS



The Onion Router (TOR)





Add to Favorites

Map

Satellite

Reception details



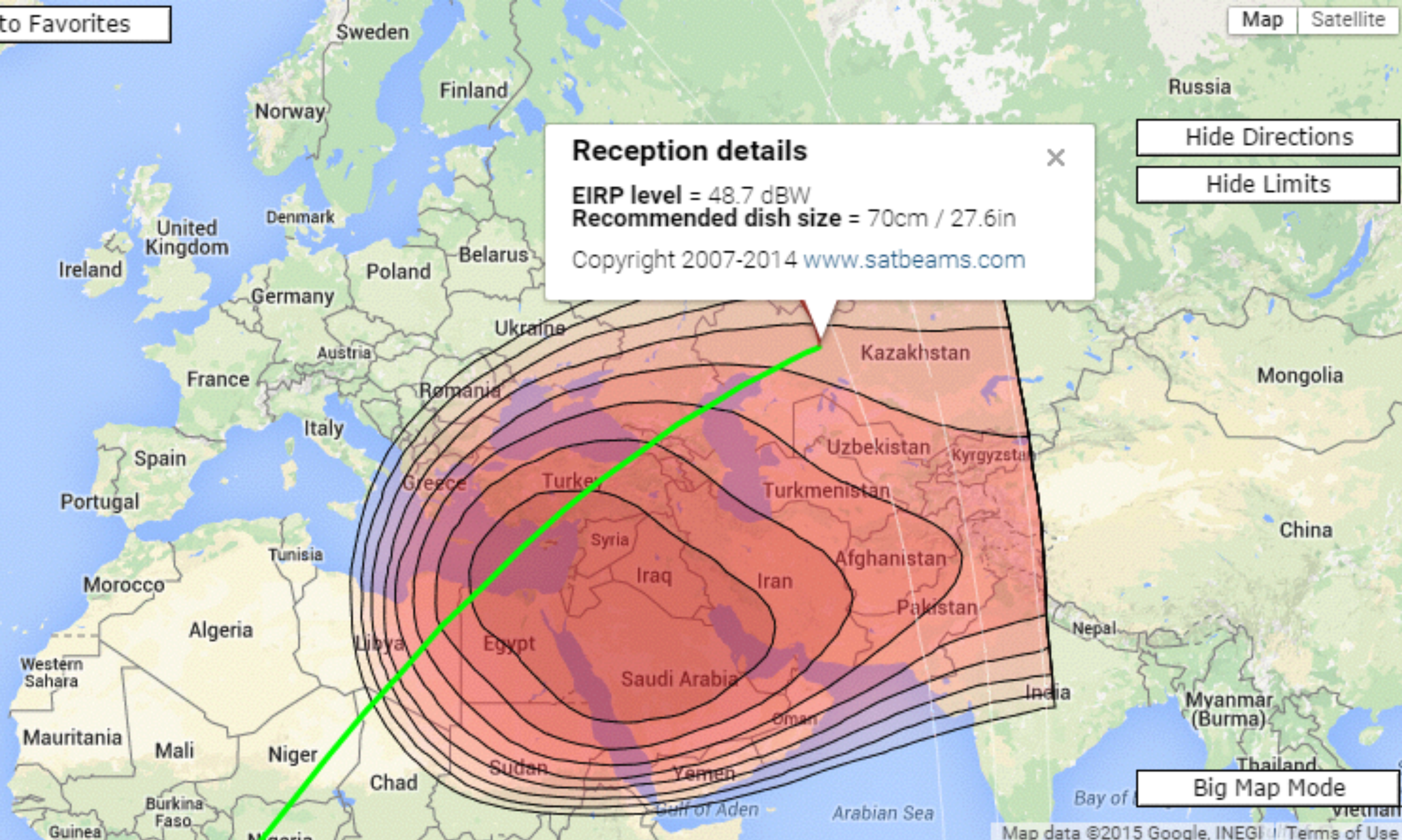
EIRP level = 48.7 dBW

Recommended dish size = 70cm / 27.6in

Copyright 2007-2014 www.satbeams.com

Hide Directions

Hide Limits



Big Map Mode



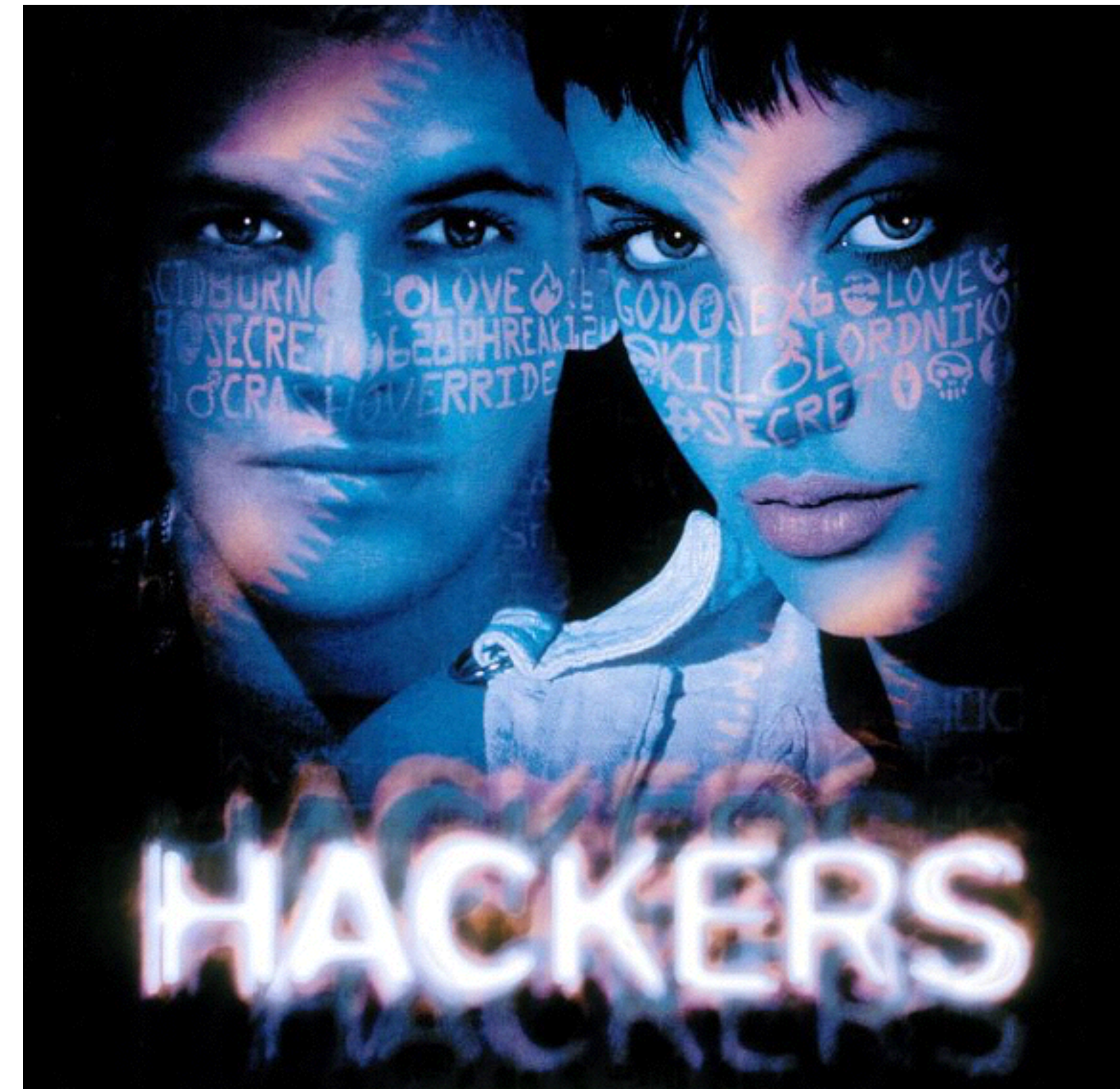
WiFi

- 449 SSID's captured
- ~45 people: I know your employer
- ~35 people: I know where you live
- 9 people I now know by name
- 1 just changed his snow tires
- 1 just visited Paris and one has just returned from Dublin



Summary

- This is happening on a daily basis
- Know where your data is
- Keep your systems up to date
- Use strong and unique passwords



Thank you for listening



dkeuper@computest.nl