

Fraud

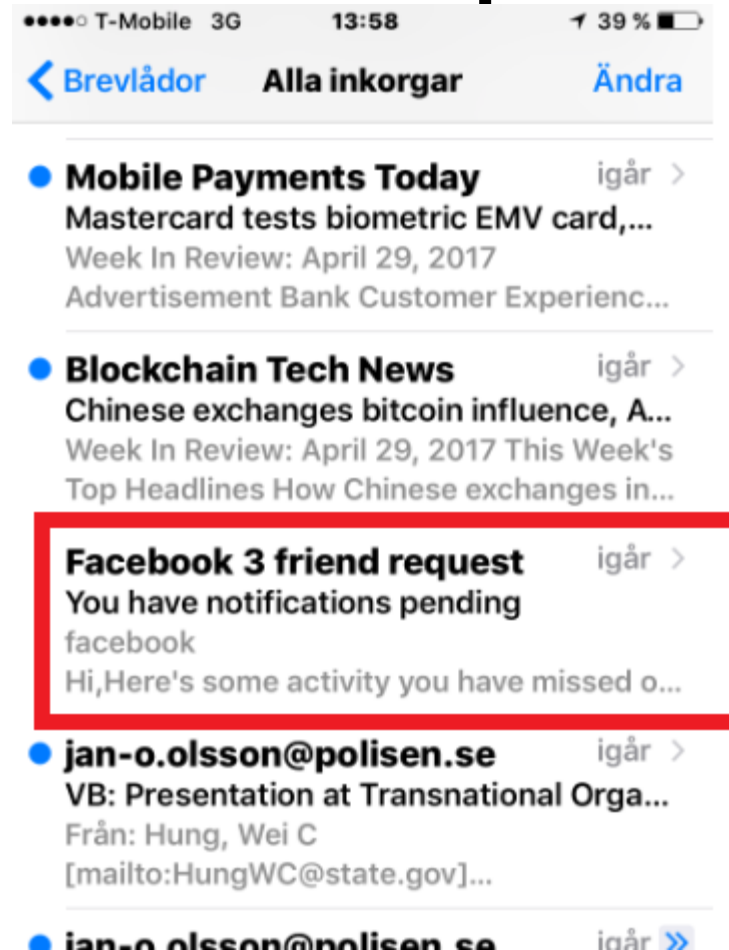
The evolution of fraud - a threat to Society



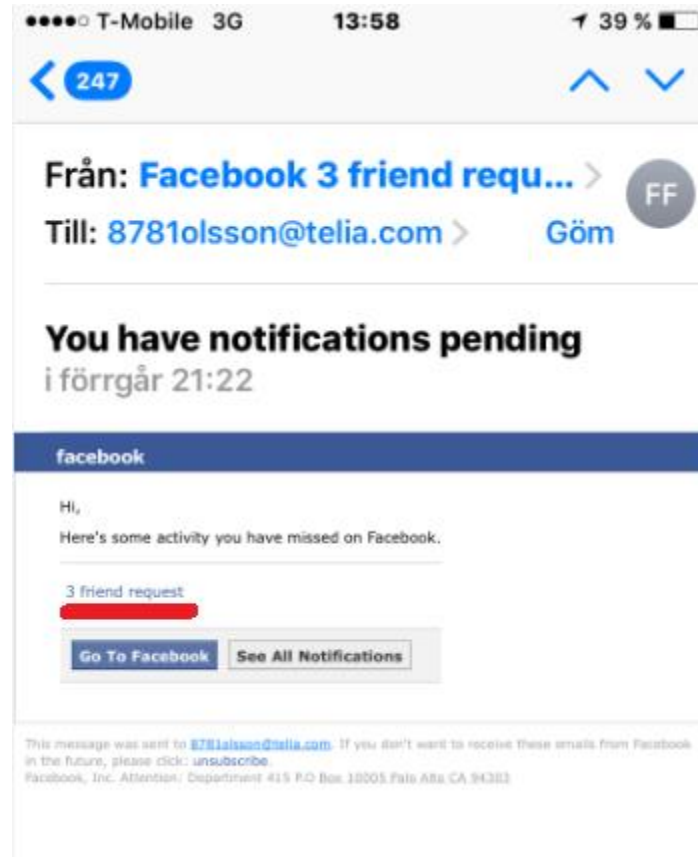
National Fraud Center (NBC)
Swedish Police
Jan Olsson



Fun in the phone



I seem to be popular, at last



What the f.....



Fraud, is that a problem?

I have not found any Swedish calculations, but:

- Annual Fraud Indicator 2016. The United Kingdom Fraud Costs Measurement Committee (UKFCMC)**

2.156.000.000.000 Sek (245 biljon \$ 2015)

Corresponds to 33.169 Sek / inhabitant

(or 3.782 \$ / inhabitant)

A not too scientific comparison but:

- The same conditions regarding computer density, the number of Internet connections per inhabitant, E-commerce tendencies and so on...**
- Criminal Propensity / naivety?**
- Sweden 9 920 881 inhabitants**
 - 33.169 Sek per capita**

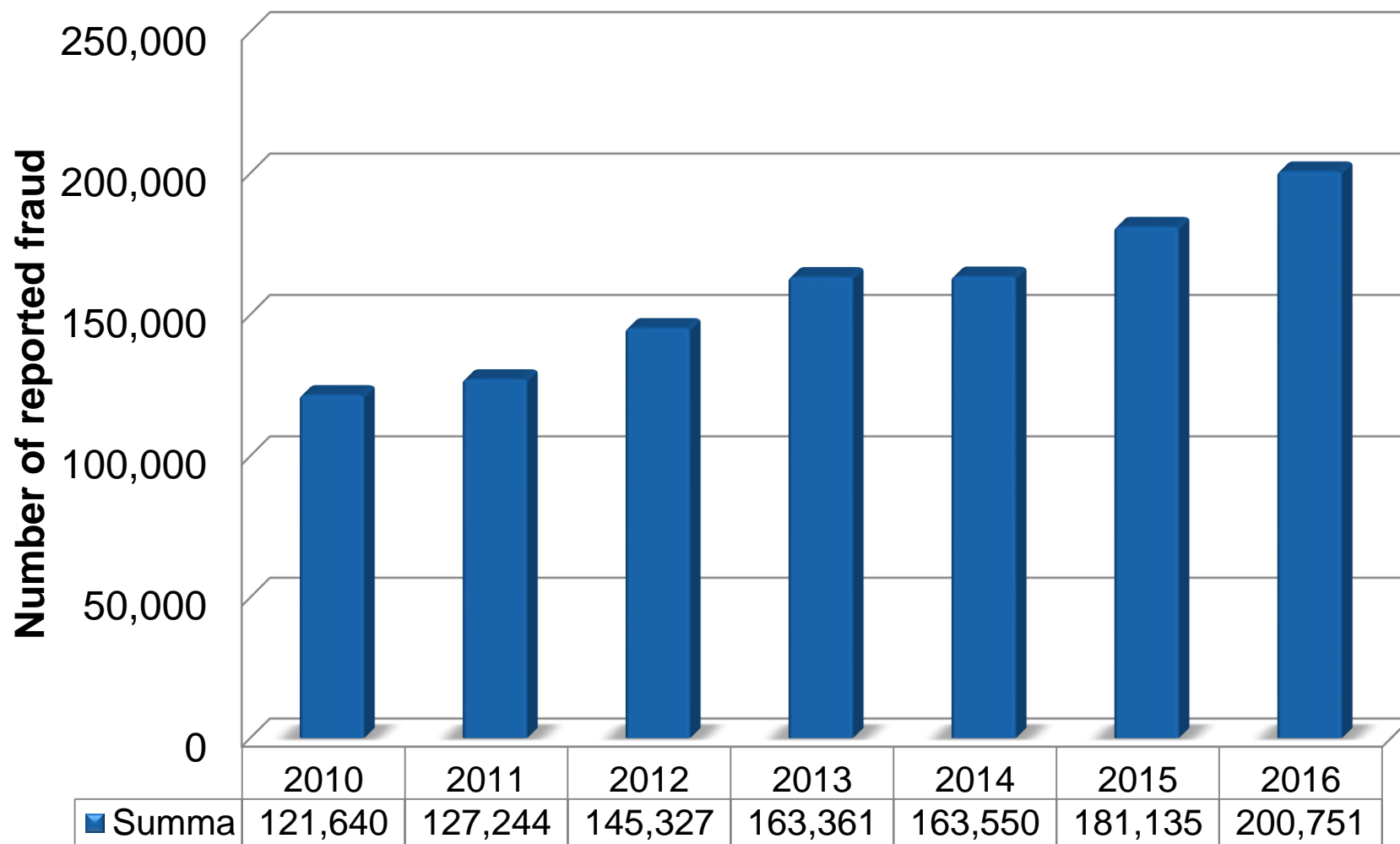
329.065.701.889 Sek

(Or 37.521.744.799 \$)

What does the amount represent?

- 5 x as much as Healthcare / Social Care (2015)**
- 7 x as much as the defense & crisis budget (2015)**
- 10.140 kr / sec (Or 1.156 \$ / sec)**

Development of fraud reported to the Swedish police



Card not present

Stay secure when buying online

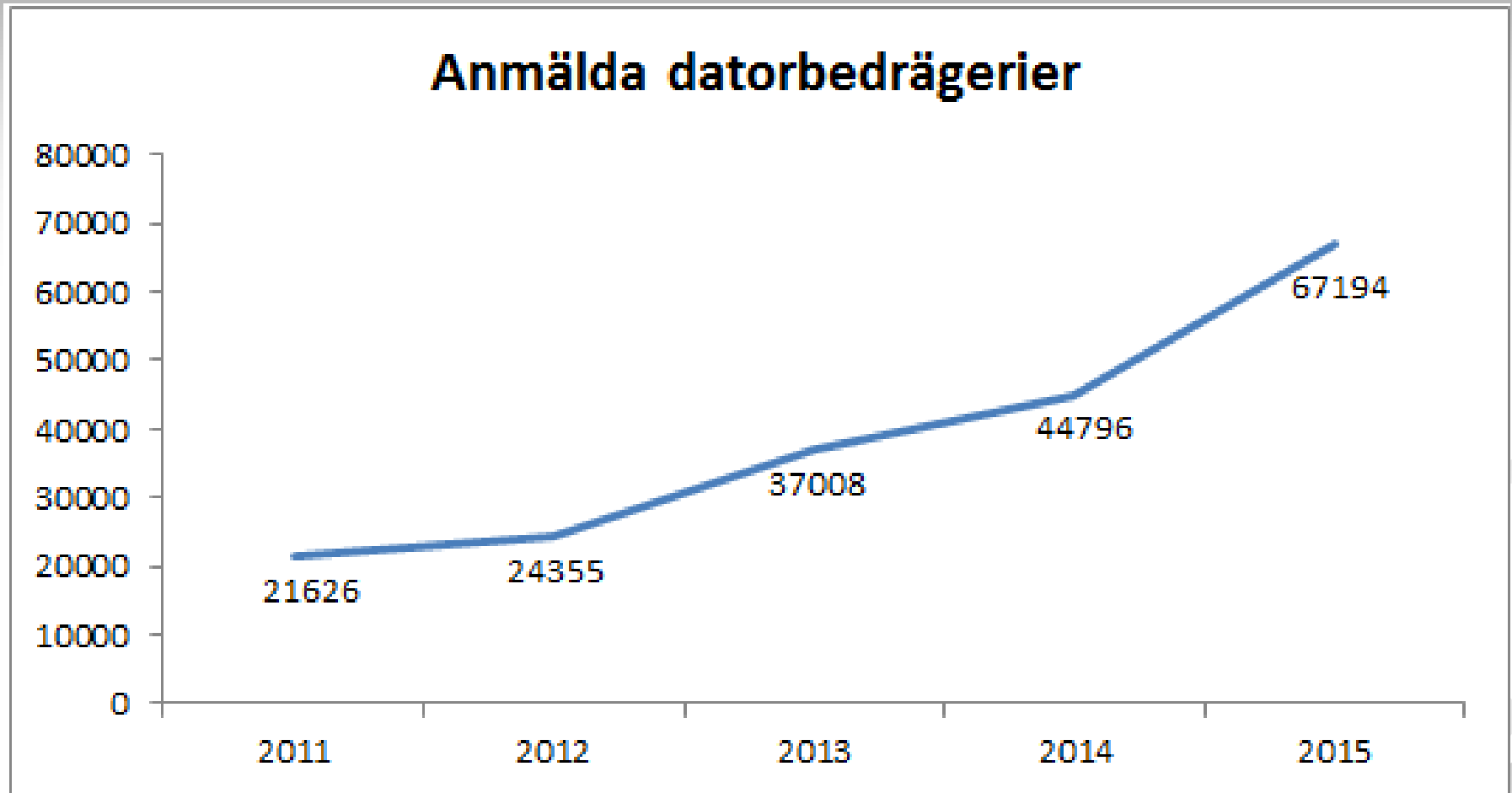


3D Secure

Verified by
VISA

MasterCard.
SecureCode

CNP trends in Sweden



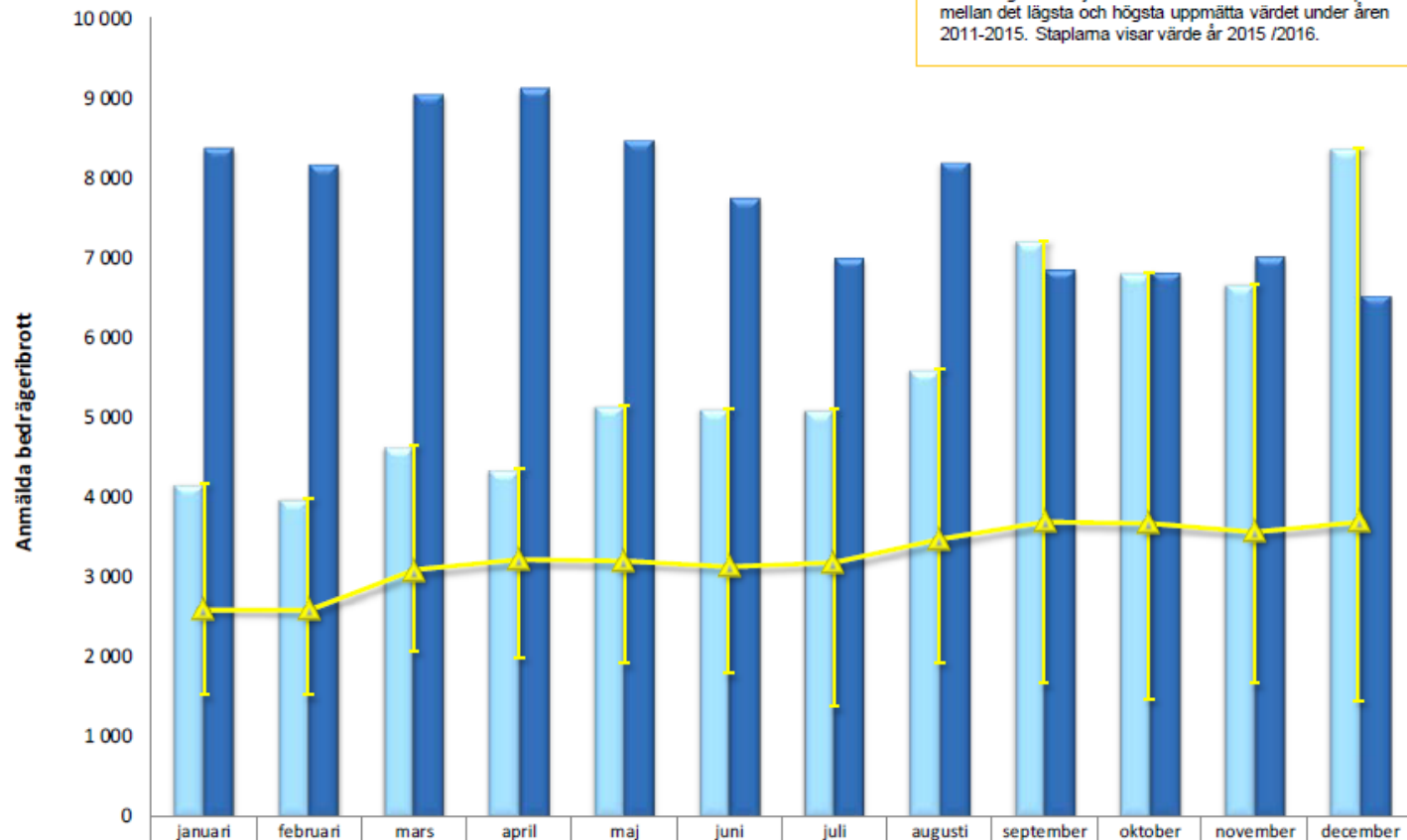
CNP 2016

Tillbaka till meny

Datorbedrägeri - Brottskod 0901

Läsanvisning till diagrammen

Linjen är medelvärde under åren 2011-2015. Det tunna strecket genom linjen som visar medelvärde är det spann mellan det lägsta och högsta uppmätta värdet under åren 2011-2015. Staplarna visar värde år 2015 /2016.



Card information ?

- Data Breach
- Pos Malware
- Keylogger internt/externt
- Phishing

Data Breaches

Zappos	24,000,000	web	hacked
Sony Online Entertainment	24,600,000	gaming	hacked
UK Revenue & Customs	25,000,000	government	lost / stolen media
U.S. Department of Veteran Affairs	26,500,000	government, military	lost / stolen computer
Tianya Club	28,000,000	web	hacked
Taringa	28,722,877	web	hacked
Ashley Madison	32,000,000	web	hacked
RockYou!	32,000,000	web, gaming	hacked
Steam	35,000,000	web	hacked
CardSystems Solutions Inc. (MasterCard, Visa, Discover Financial Services and American Express)	40,000,000	financial	hacked
Weebly	43,430,316	web	hacked
Evernote	50,000,000	web	hacked
Living Social	50,000,000	web	hacked
Commission on Elections	55,000,000	government	hacked
Home Depot	56,000,000	retail	hacked
Tumblr	65,469,298	web	hacked
Target Corporation	70,000,000	retail	hacked
JP Morgan Chase	76,000,000	financial	hacked
National Archives and Records Administration (U.S. military veterans' records)	76,000,000	military	lost / stolen media
Sony PlayStation Network	77,000,000	gaming	hacked
Anthem Inc.	80,000,000	healthcare	hacked
AOL	92,000,000	web	inside job, hacked
TK / TJ Maxx	94,000,000	retail	hacked
Rambler.ru	98,167,935	web	hacked
Heartland	130,000,000	financial	hacked
Equifax	143,000,000	financial, credit reporting	hacked
eBay	145,000,000	web	hacked
Adobe Systems	152,000,000	tech	hacked
Massive American business hack including 7-Eleven and Nasdaq	160,000,000	financial	hacked
Friend Finder Networks	412,214,295	web	poor security / hacked
Yahoo	500,000,000	web	hacked
Yahoo	3 000 000 000	web	hacked

Equifax - Interesting Breach

summer 2017

- **Equifax Inc.** is a consumer credit reporting agency in the US
- collects and aggregates information on over 800 million individual consumers and more than 88 million businesses worldwide.
- cybercriminals accessed approximately 145.5 million U.S. Equifax consumers' personal data, including their full names, Social Security numbers, birth dates, addresses, and, in some cases, driver license numbers.
- at least 209,000 consumers' credit card credentials were taken in the attack.
- Residents in the United Kingdom and Canada were also impacted
- Any Swedes ??

Magnitude / Vulnerability

Trustwawe Spiderlabs

- 81% didn't discovered it themselves
- 98% of the surveyed companies had weaknesses
 - 95% mobile apps had weaknesses

The criminal's return was staggering 1425%

IBM

- 256 days for discovery
 - 158 days to delete
- Average cost per company about 50 million sek (530.000 Euro)
 - Cost per data record 1.400 sek (150 Euro)

HP

- Of 200 companies with more than 1,000 employees, 100% were exposed to data breach, of which 67% in the past year

(Centric and Ponemon Institute 2015)

Can the private sector prevent CNP?

- Monitorising (ecommerce kyc)
- Amex Safekey – Dynamic Password
- Gemalto, Oberthur – Dynamic CVV
- PSD2/GDPR
- Internet barrier / Geoblocking

CEO/BEC-Fraud

Abstract wavy lines in shades of gray, flowing from the bottom right towards the center of the slide.



International Headlines

Ubiquiti Networks scammed out of \$46.7 million

Autozulieferer Leoni um 40 Millionen Euro betrogen

Austrian Aeronautics Company Loses Over €42 Million to BEC Scam

Bedragere lurte ansatt til å utbetale en halv milliard kroner

Belgian bank Crelan loses €75 million to BEC scammers



Swedish Headlines

Betala två fakturor på totalt 35 000 euro

Bedragare lurade av KTH en halv miljon Sek

Billerud Korsnäs har utsatts för bedrägeri

Lurats på 50 miljoner kronor

Lyckats förmå dotterbolaget att göra
oberättigade betalningar uppgående till
totalt 17,2 millioner euro.



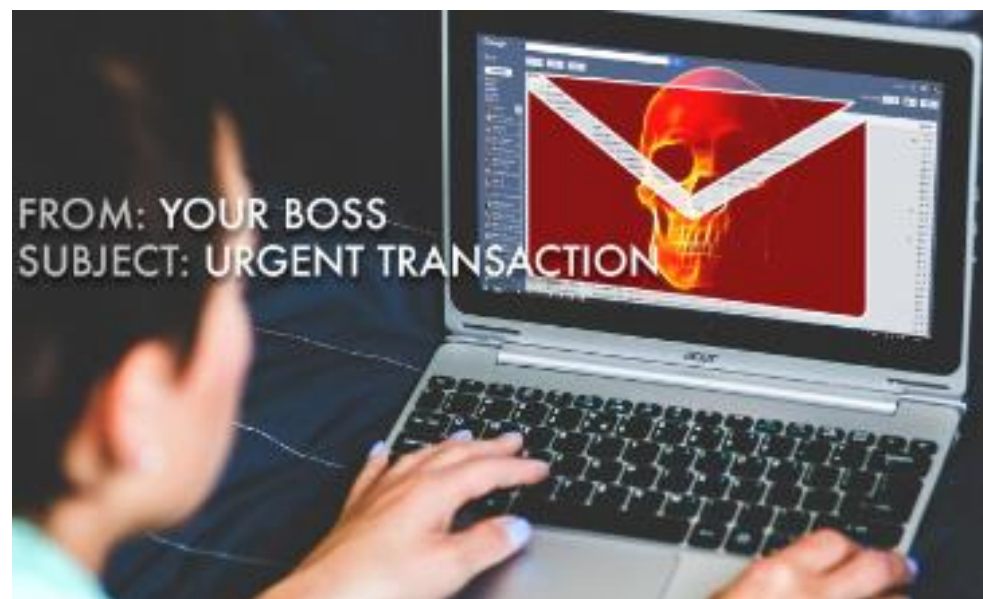
Three different Modus Operandi

- The French Original
- Simple email correspondance
- Trojans



The French original

Gilbert Chikli Fake CEO Scam Artist
'Is Unstoppable





Simple email correspondance

- Email Spoofing
- Similar domain addresses
- Other top level domain



Spoofing, Authentic Case

Från: Maria Broman [<mailto:maria.broman@visitskelleftea.se>]

Skickat: den 7 september 2016 13:31

Till: Jan Palm

Ämne: Hej

Jan

Jag skulle vilja veta om du kan bearbeta internationell överföring till idag? om det är möjligt så skickar jag bankuppgifterna för överföringen

MVH

Maria Broman

Spoofing, Authentic Case

Från: Maria Broman [maria.broman@visitskelleftea.se]

Svara avsändaren

Till: Maria Broman [cfo@execu.cba.pl]

Similar Domain Address, Misspelled Name..

Från: bjon.somnas@besgab.se [<mailto:bjon.somnas@besgab.se>]

Skickat: den 12 maj 2016 11:56

Till: Yvonne Swartling

Ämne: Re: Faktura

Hej Yvonne,

Anette behöver bifogad faktura betalas idag. Uppskatta om du kan göra en betalning så snart som möjligt och skicka överföringsinformation när du är klar för mig

Anette via följande e-post nedan certifierad och godkänd räkning och betalning. Jag ska förmedla mer information och dokumentation för transaktionen till dig när jag får den från Anette.

Huvudsaken är att fakturan är betald så snart som möjligt och behagar göra betalningen som "express". Tack.

Björn

Skickat från min iPhone

Similar Domain Address, Misspelled Name

The fraudster has registered a domain name that is confusingly similar to the real one

Real: arne.andersson@firma.se

New: arne.andersson@firman.se

Other top level domain

The fraudster has registered the same name on another top-level domain.

Real: arne.andersson@firma.se

New: arne.andersson@firma.com
arne.andersson@firma.org



Trojans

Access to :

- mail server
- personal information/Agendas
- PBXs
- billing/invoice program
- accounting software

Access to ...



Ransomware (Cryptolocker)

Then, Now and Tomorrow



Ransomware 3-4 years ago..



POLISEN ENHETEN FÖR DATABROTT

OBS!

Datorn är blockerad!

Din IP-adress: [REDACTED]
Din värd Namn: [REDACTED]
Din plats är fast

Detta operativsystem är blockerad på grund av brott mot svensk lag. Fastställt följande brott:

Med denna IP-adress var besökta webbplatser som innehåller pornografi, barnpornografi, tidelag, och våld mot barn. Videofter som innehåller pornografi, våld inslag av barnpornografi har installerats på dator! Dessutom skickades e-postmeddelanden i form av spam, som innehåller terrorist motiv från din epost adress.

Datorn har blockerats för att stoppa din olaglig verksamhet.

För att låsa upp datorn, du måste betala böter på 100 euro. Du kan betala en straffavgift på två sätt:

- 1) Betalning via ett system Ukash:

För att göra detta måste du ange i betalningsform 19-siffrig kod och trycka OK (Om du har flera koder, bör de införas en efter en, och klicka sedan på OK).

- 2) Betalning via ett system Paysafecard:

För att göra detta måste du ange i betalningsform 16-siffrig kod (Om nödvändigt, skriv in ett lösenord) och tryck OK (Om du har flera koder, bör de införas en efter en, och klicka sedan på OK).

Ukash Var kan jag köpa Ukash?

Du kan få Ukash från hundratals globala platser, på nätet, från pånböcker, från kiosker och uttagsautomater.

- Pressbyrån - Ukash finns nu från över 300 Pressbyrån kiosker över hela Sverige.
- 7Eleven - Få Ukash från över 200 grenar av 7Eleven finns i Shell bensinstationer.
- Payzone - Ukash tillgängliga Payzone terminaler runt om i Sverige.

paysafecard Var kan jag köpa Paysafecard?

I Sverige kan du köpa dina paysafecard vid 7-Eleven, Shell 7-Eleven, Direkten, Timebutiker, Pressbyrån, bensinstationer och tobaksaffärer.

Pressbyrån 7-Eleven Direkten time

Ange 100 EURO
Paysafecard och Ukash kod:

Ange koden eller Ukash Paysafetsard

SKICKA



Phishing mail from Postnord, Now



Du har lösta paket

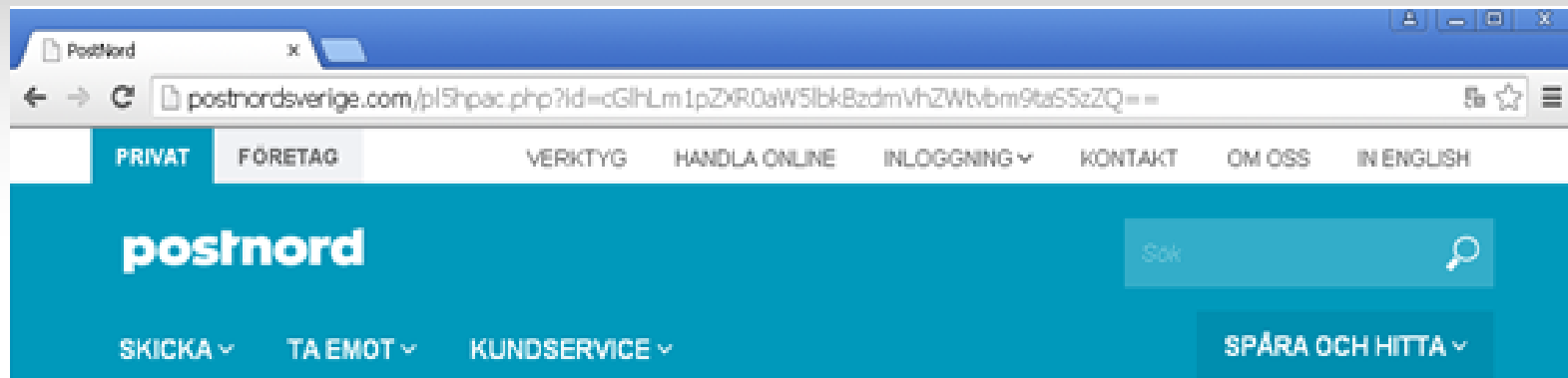
Vi har fått ditt paket **CT4194654352SE** på **2015/09/14**. Courier kunde inte leverera det här paketet till dig.

Få och skriva ut fraktsedel, och visa den på närmaste postkontor för att få det här paketet.

Om paketet inte tas emot inom 20 arbetsdagar, kommer Postnord ha rätt att kräva **Få fraktsedel** ersättning från dig - 60 kronor för varje dag för paketet lagring. Du kan hitta information om förfarandet och villkoren för paketet lagring i närmaste Postnord kontoret.

Detta är ett automatiskt meddelande. Klicka här för att avregistrera

If they clicked on the link in the mail...



Ladda ner och skriva ut fraktsedel



Ladda ner och skriva ut fraktsedel och visa den på närmaste postkontor för att få paketet.

764674

HÄMTA FRAKTSEDEL

And these two files get unpacked



Fill in the numbers and click "Download shipping slip" to download the following compressed file into your computer.



The screen locks for a while and then the instructions shows on the screen..



```
HOW_TO_RECOVER_FILES.txt - Notepad
File Edit Format View Help
1

=====
!!! WE HAVE ENCRYPTED YOUR FILES WITH CryptOL0cker VIRUS !!!
=====

Your important files (including those on the network disks, USB, etc): photos,
videos, documents, etc. were encrypted with our CryptOL0cker virus. The only
way to get your files back is to pay us. Otherwise, your files will be lost.

use this link to pay for files recovery:
http://3xo7axbmkttd4qlx.torprovider.cc/byr4ca.php?user_code=1b4r0r&user_pass=8236

-----

[=] what happened to my files?

Your important files: photos, videos, documents etc. were encrypted with our
CryptOL0cker virus. This virus uses very strong encryption
algorithm - RSA-2048. Breaking of RSA-2048 encryption algorithm is impossible
without special decryption key.

[=] How can I get my files back?

Your files are now unusable and unreadable, you can verify it by trying to
open them. The only way to restore them to a normal condition is to use our
special decryption software. You can buy this decryption software on
our website (http://3xo7axbmkttd4qlx.torprovider.cc/byr4ca.php?user_code=1b4r0r&user_pass=8236).

[=] what should I do next?

You should visit our website (http://3xo7axbmkttd4qlx.torprovider.cc/byr4ca.php?user_code=1b4r0r&user_pass=8236)
and buy decryption for your PC.

[=] I can not access to your website, what should I do?

our website should be accessible from one of these links:
http://3xo7axbmkttd4qlx.torprovider.cc/byr4ca.php?user_code=1b4r0r&user_pass=8236
http://3xo7axbmkttd4qlx.onion.to/byr4ca.php?user_code=1b4r0r&user_pass=8236
http://3xo7axbmkttd4qlx.onion.city/byr4ca.php?user_code=1b4r0r&user_pass=8236
http://3xo7axbmkttd4qlx.onion/byr4ca.php?user_code=1b4r0r&user_pass=8236 (using TOR browser)
```

All mail traced back to..

```
host XN--80AQEBIDA1BNH.XN--P1AI
xn--80aqebida1bnh.xn--p1ai has address 37.140.192.174
XN--80AQEBIDA1BNH.XN--P1AI mail is handled by 20 mx2.hosting.reg.ru.
XN--80AQEBIDA1BNH.XN--P1AI mail is handled by 10 mx1.hosting.reg.ru.

domain name pointer for 37.140.192.174 is server90.hosting.reg.ru.
```

```
AS 197695 (Domain names registrar REG.RU, Ltd)
```

Hosting provider:

inetnum: 37.140.192.0 - 37.140.195.255

Netname: REGRU-NETWORK

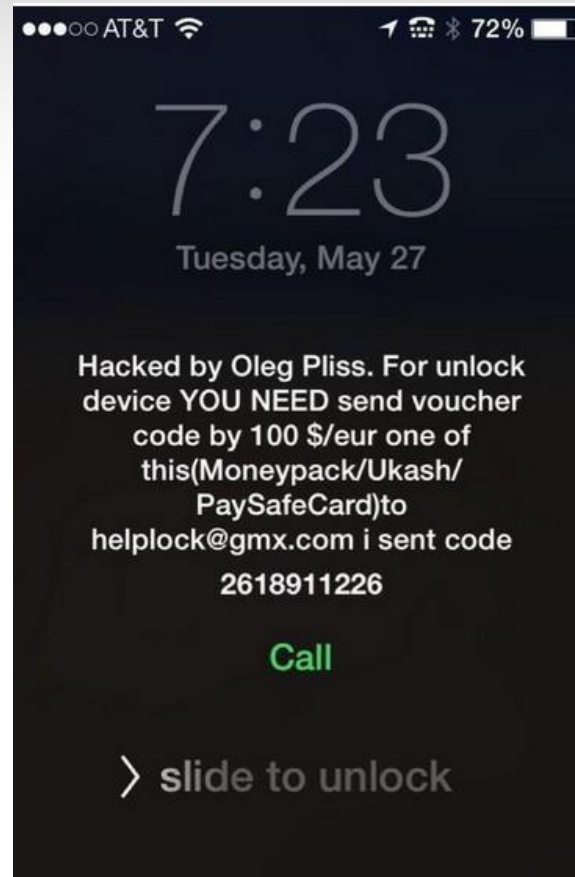
Descr: Reg.Ru Hosting

Country Code: RU

Country: Russian Federation

Person: Pavel Arbuzov

Why not the mobile phone or ■ ■ ■



Banktrojan Retefe (Rovnix)



geographical coverage



The Phishingmail

Siv

Från: "CDON.COM" <order@cdon-faktura.org>
Till: <sivan17@telia.com>
Skickat: den 18 maj 2015 18:05
Bifoga: Faktura_____18.05.2015.zip
Ämne: Din order fran CDON 149886534
Hej!

Här kommer din beställning.

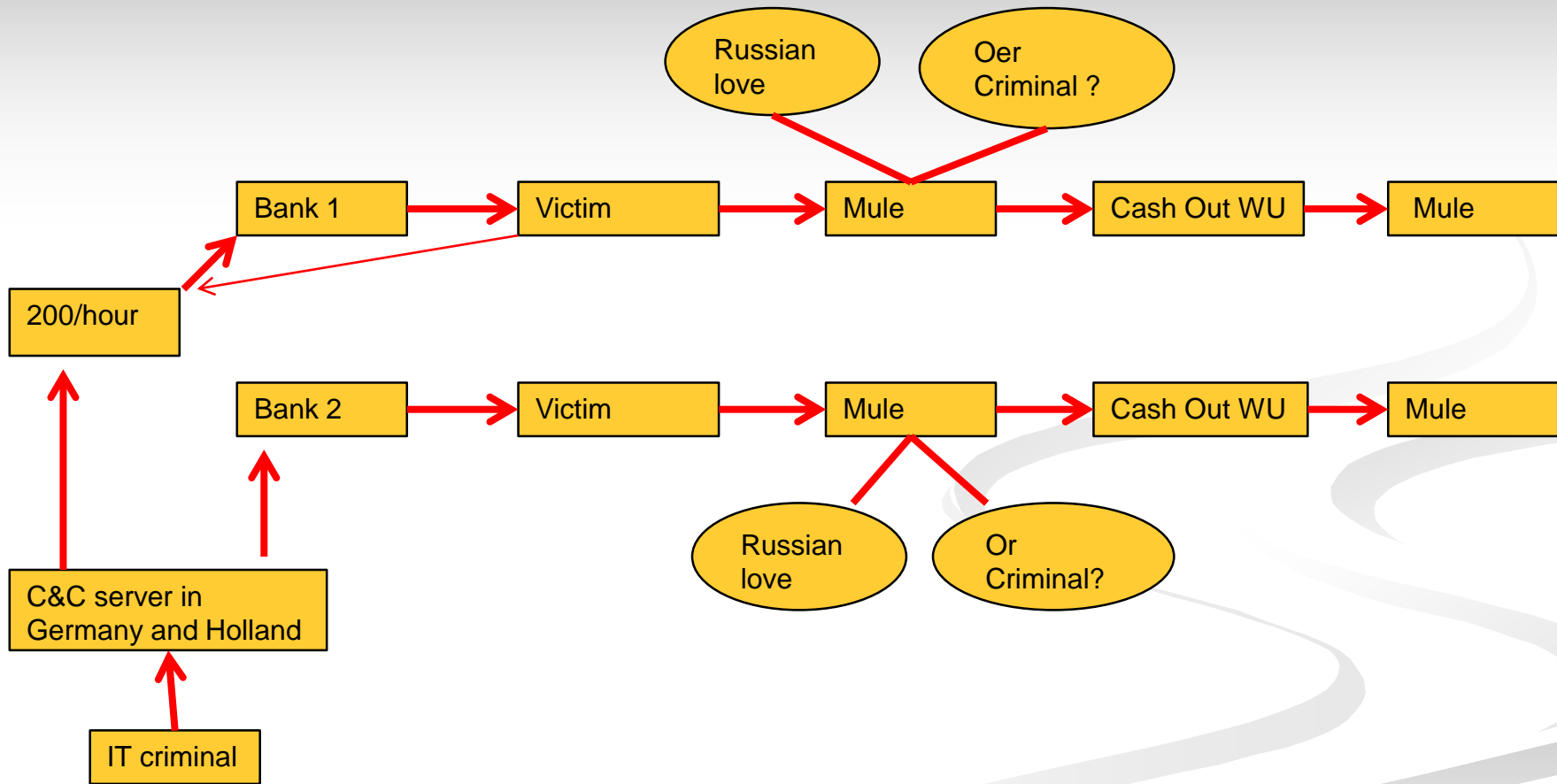
Orderspec.:
Betaling: Visa
Leveranssätt: UPS
Totalt inklusive moms: 12.441,14 sek

Du får ett e-postmeddelande när ordern skickas från vårt lager. Din beställning kommer at levereras till den adress som du angett/anger till oss.

Vi välkomnar dig som en kund!

Med vänliga hälsningar,
CDON.COM.

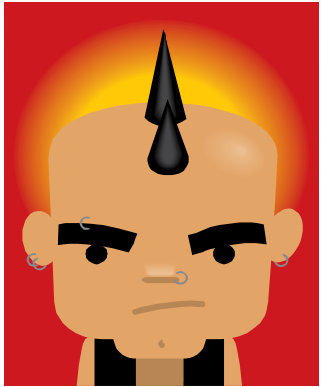
Flow Chart - Unusual



Spear phishing, social engineering, Crime-as-a-service and more...

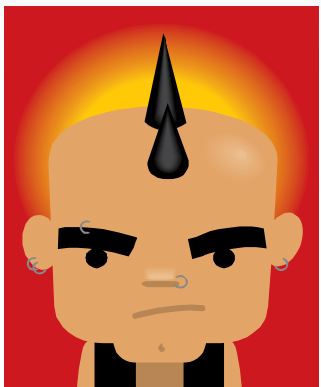
A case study





Bad guy

*Hijacking a
facebook account*



mapping "friends"

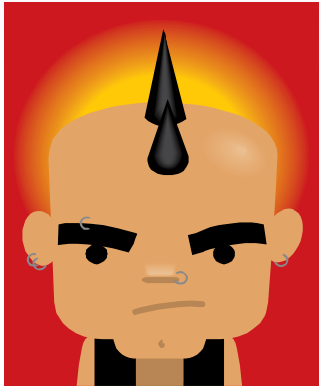
Lisa

John

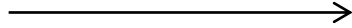
Stina

Anna

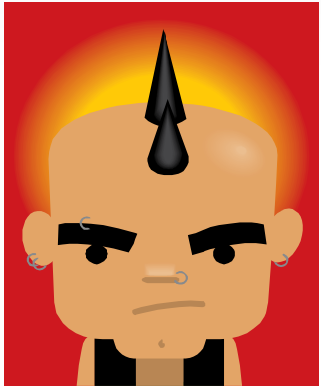
Sven



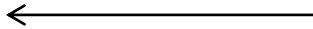
Everyday communication...



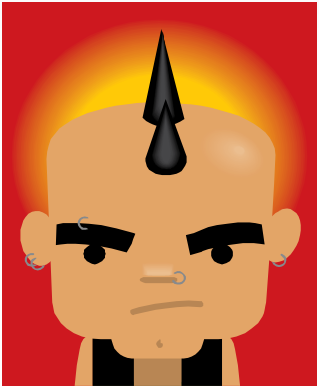
"friend"



*The friend hands over her login
(digipass) details to the internet
bank...*



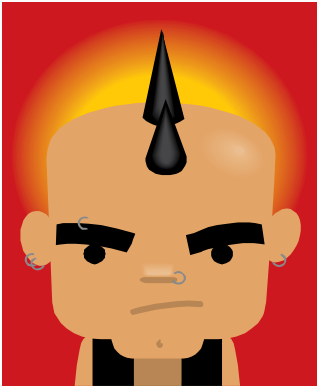
Access to
her
internetbank
account



Access to
her
internetbank
account



Swedbank Account
belonging to Trustly (3:e
party PSP)



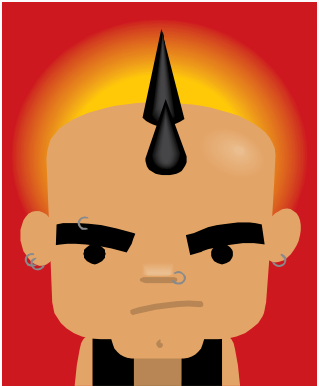
Access to
her
internetbank
account

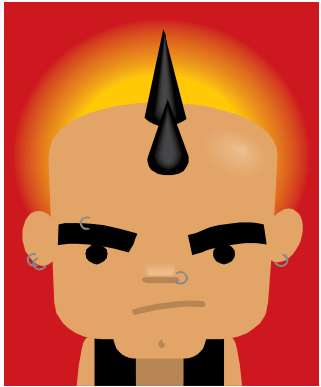


Swedbank Account
belonging to Trustly (3:e
party PSP)



Skrill account (Digital wallet)





Access to
her
internetbank
account



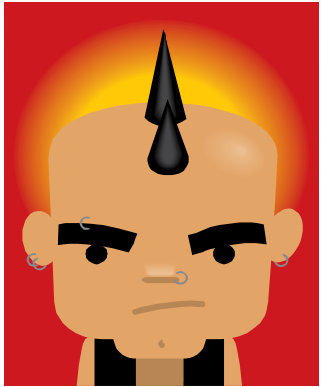
Swedbank Account
belonging to Trustly (3:e
party PSP)



Skrill account (Digital wallet)



Another skril account



Access to
her
internetbank
account



Swedbank Account
belonging to Trustly (3:e
party PSP)



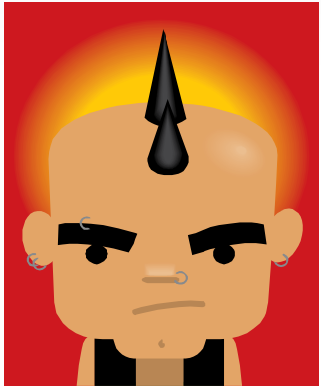
Skrill account (Digital wallet)



Another skrill account



Skrill prepaid
mastercard



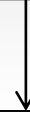
Access to
her
internetbank
account



Swedbank Account
belonging to Trustly (3:e
party PSP)



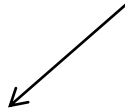
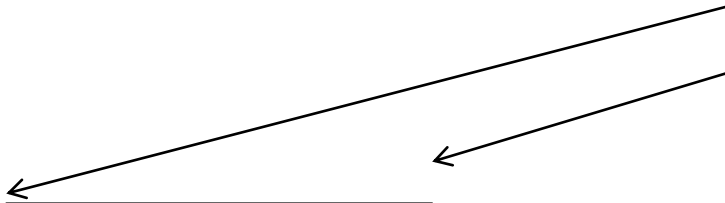
Skrill account (Digital wallet)



Another skroll account



Skrill prepaid Mastercard



Cash out ATM
Venezuela

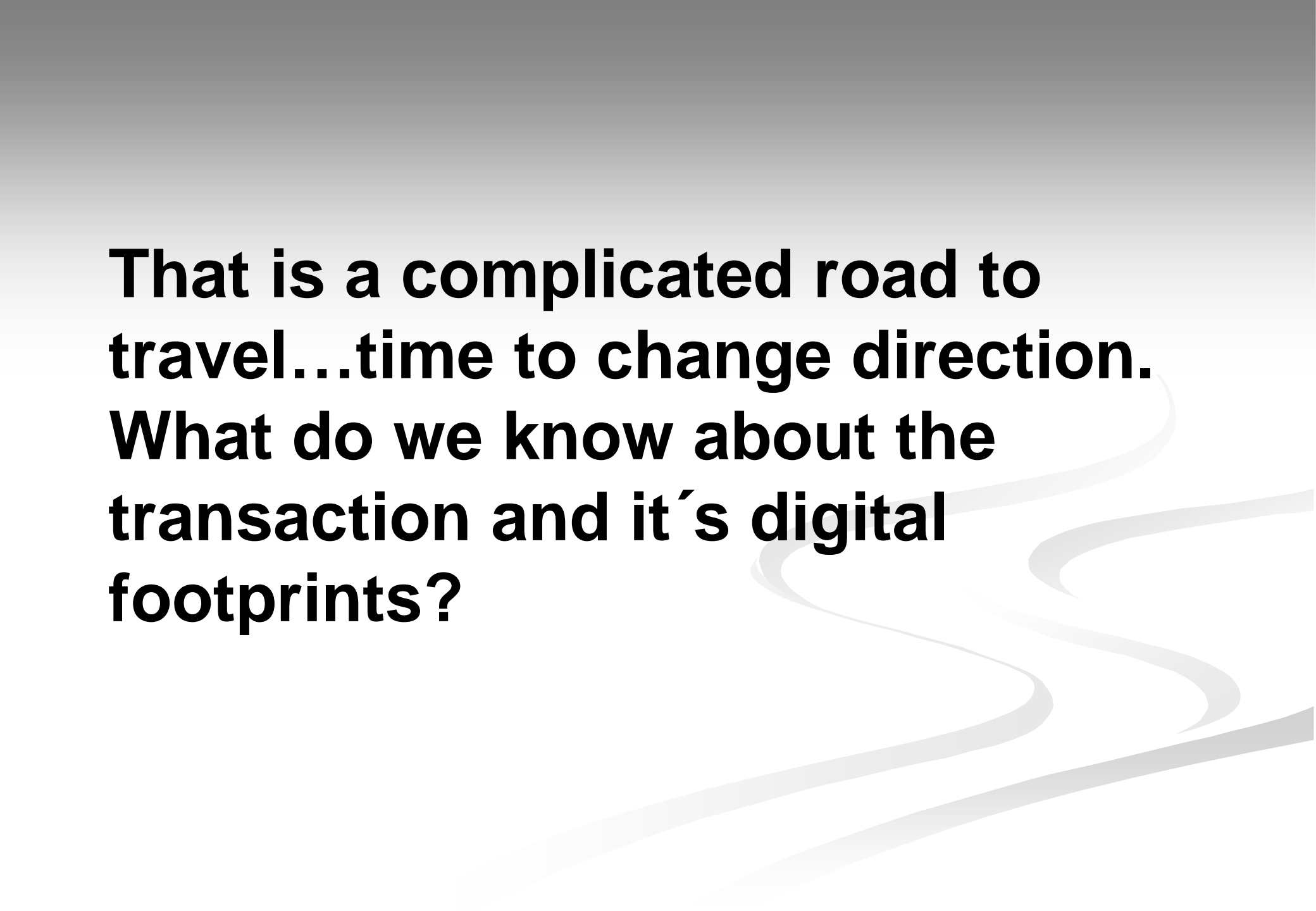
Cash out ATM
Frankrike

Cash out ATM
Serbien

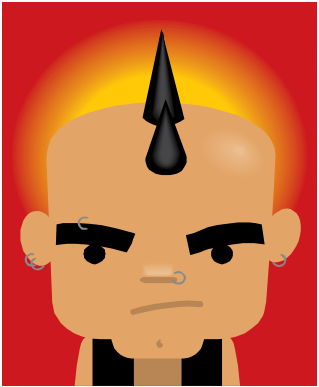
Cash out ATM
Lettland

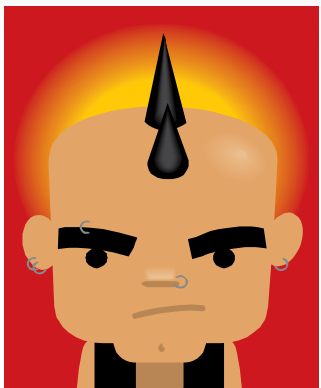
Cash out ATM
Slovenien

That is a complicated road to travel...time to change direction. What do we know about the transaction and it's digital footprints?

The background of the slide features a series of light gray, wavy, horizontal lines that sweep across the lower half of the image, creating a sense of movement and depth. The lines vary in thickness and curve, resembling stylized waves or a winding path.

Anonymus cashcard
dongle for Internet access

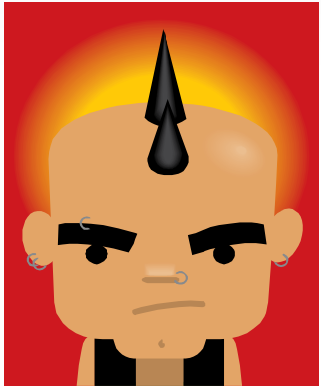




Anonymus cashcard dongle
for Internet access



Anonymity service (VPN)



Anonymus cashcard dongle for
Internet access

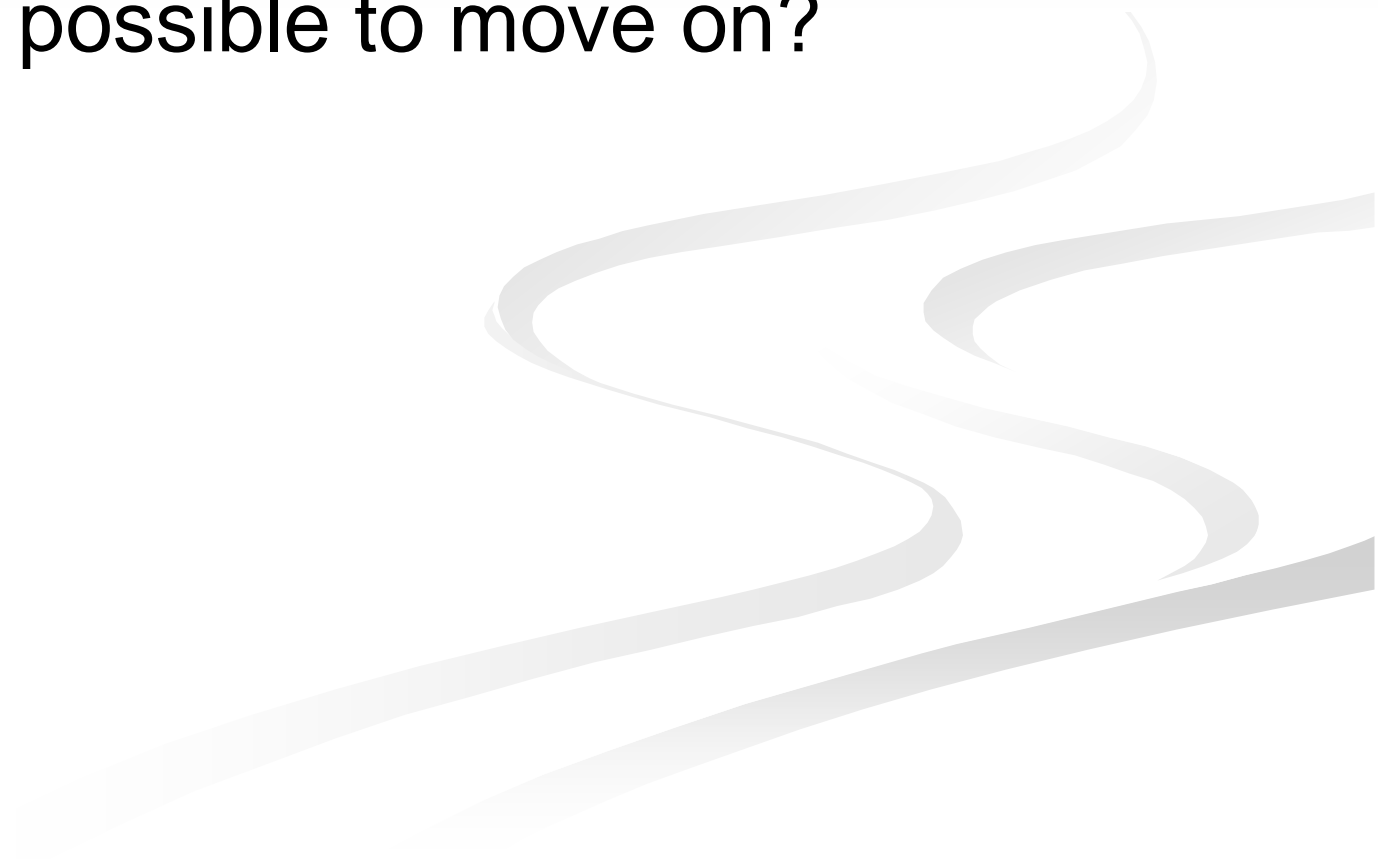


Anonymity service (VPN)



Botnet VIP72, outside Moscow)

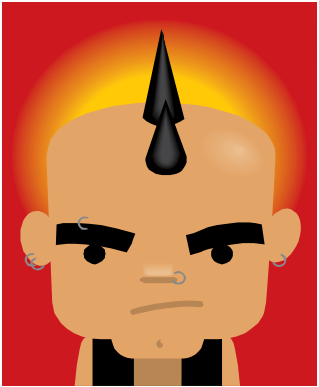
Is it even possible to move on?

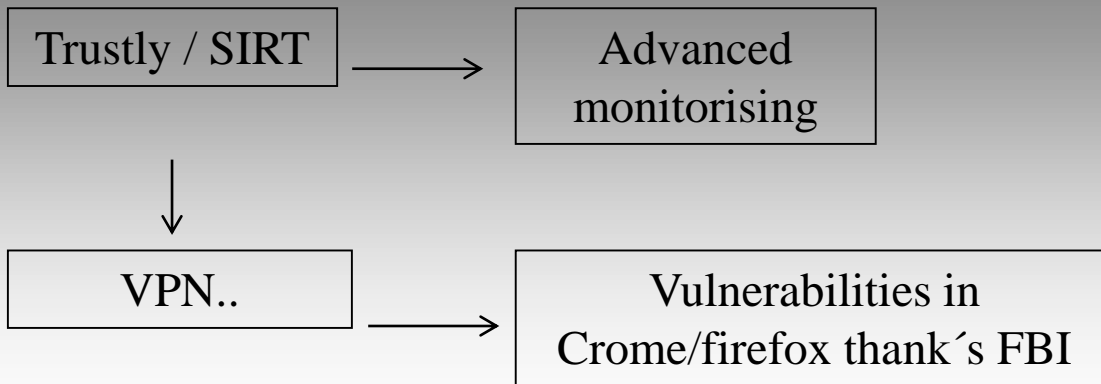
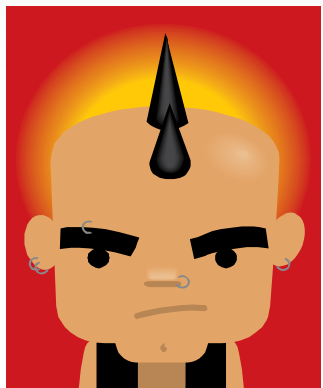


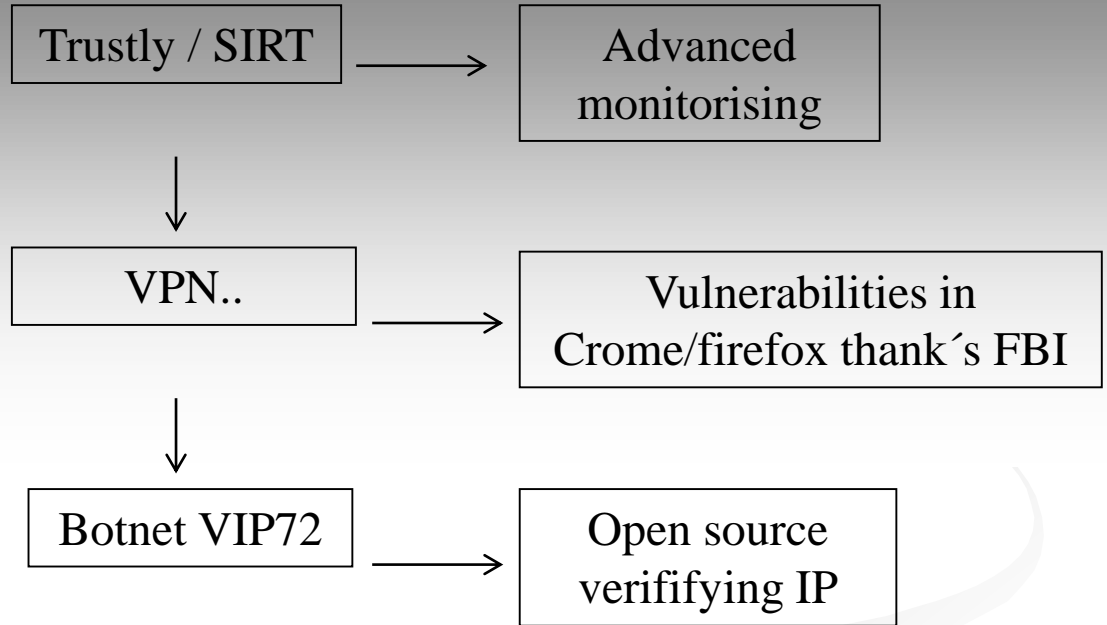
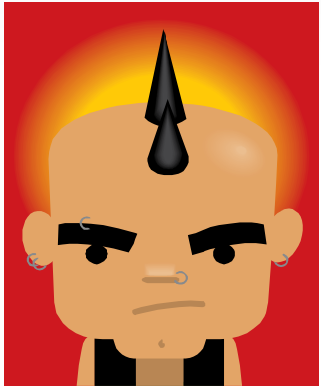
Trustly / SIRT

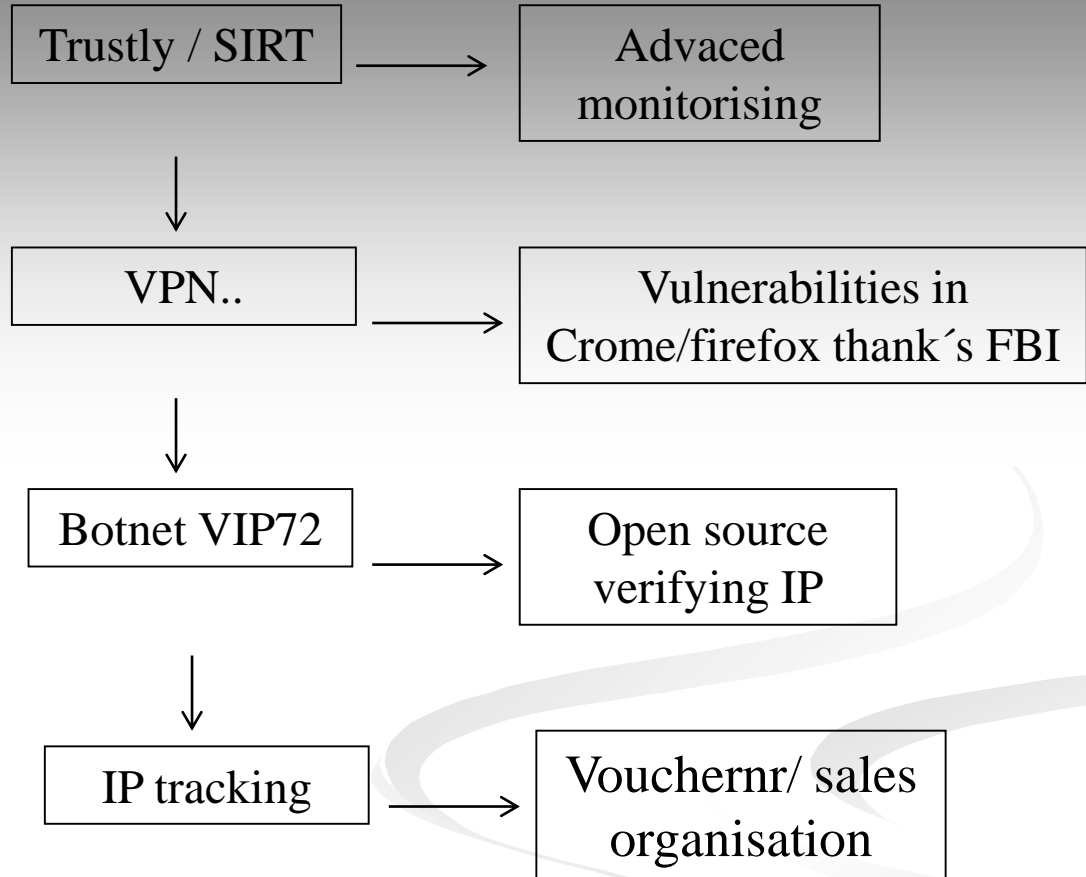
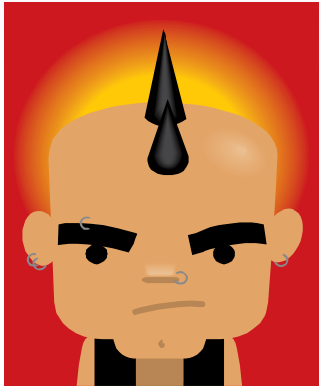


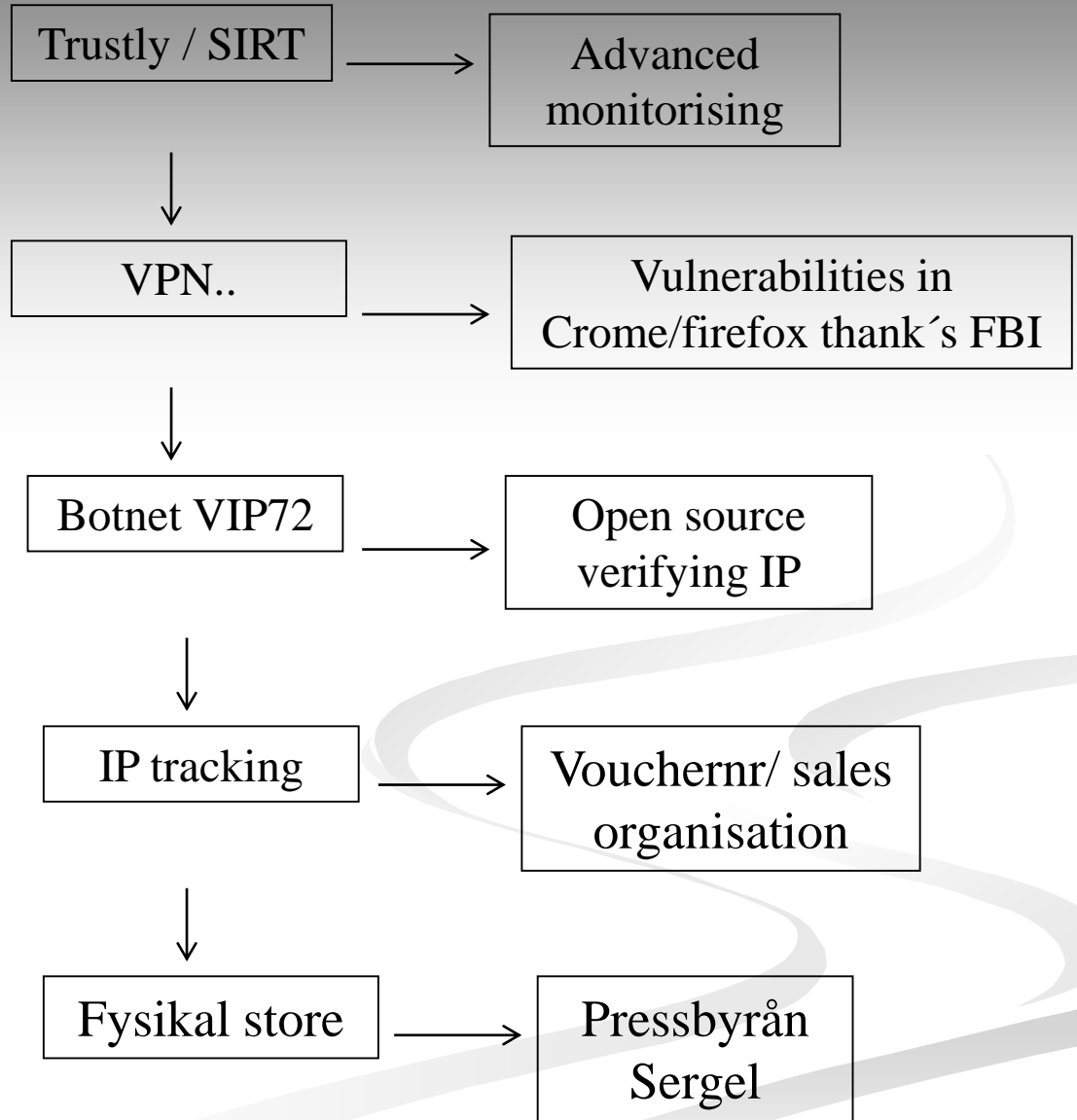
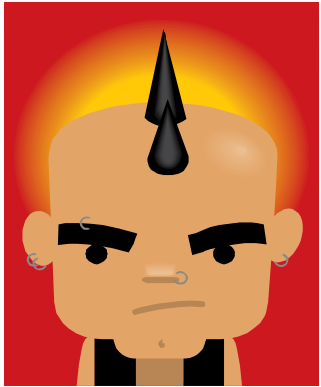
Advanced
monitoring







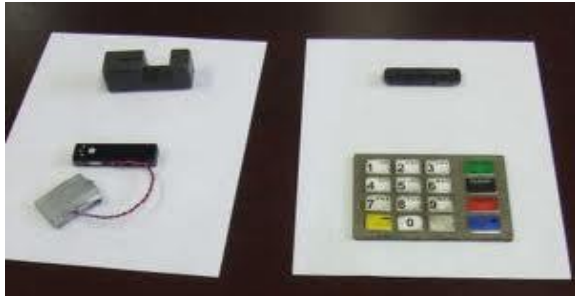




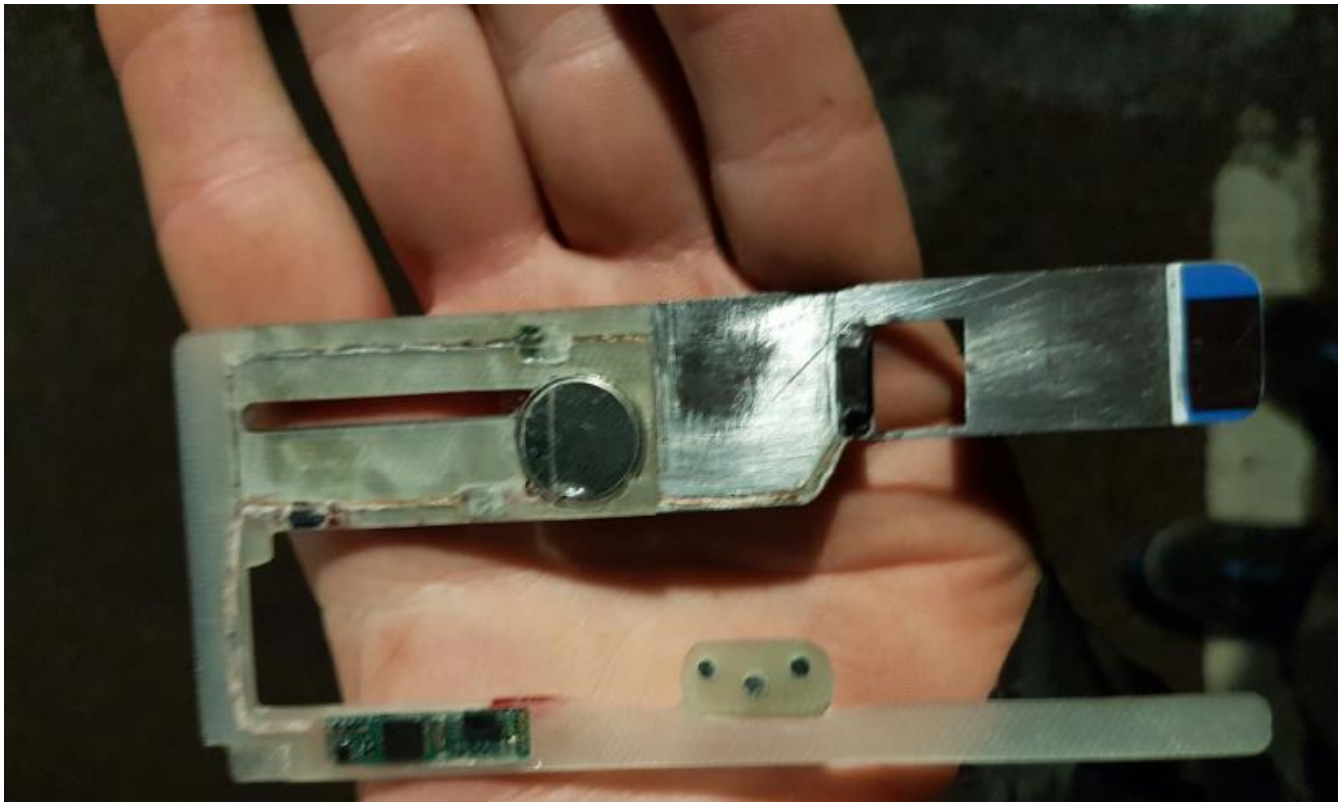
Got you !
Nothing is impossible, or is it?



Skimming



Deep Insert Skimming



Organized Crime?

1.4 Billion Yen Stolen from Japanese ATMs in less than 3 Hours

May 23, 2016



Over 1.4 billion Yen was reportedly stolen in a span of **two and a half hours** across automated teller machines (ATMs) found in over 1,400 convenience stores in Japan this month. According to the local police, the simultaneous theft occurred on March 15 where money was illegally withdrawn from ATMS located in Tokyo and 16 other locations including Kanagawa, Aichi, Osaka, and Fukuoka.

Law enforcement officials believe that the extraction was conducted by a group of more than 100 criminals between 5am to 8am using fraudulent credit cards containing information leaked by a bank in South Africa. It was reported that there were more than 14,000 transactions made. With each transaction extracting 100,000 Yen (or \$900 USD)—the maximum credit card withdrawal limit used in the said machines—the operation successfully amassed an amount equivalent to US\$13 million.

Authorities are currently looking into how the theft was stealthily coordinated and carried out. It is believed that the group behind the operation strategically withdrew money outside the nation where the **1,600** credit cards containing leaked data (by way of hacking or other method) originated from. Authorities are currently devising ways to identify and analyze images recorded from security cameras. Also, investigations on the cybersecurity front will be conducted with the help of South African law enforcement agencies via the Interpol to determine how data was mined from the South African bank.



ATM Malware



ATM Trix – Now in Sweden

Jackpotting



ATM Trix – Not as neat

Blackboxing



Skimming POS-terminaler

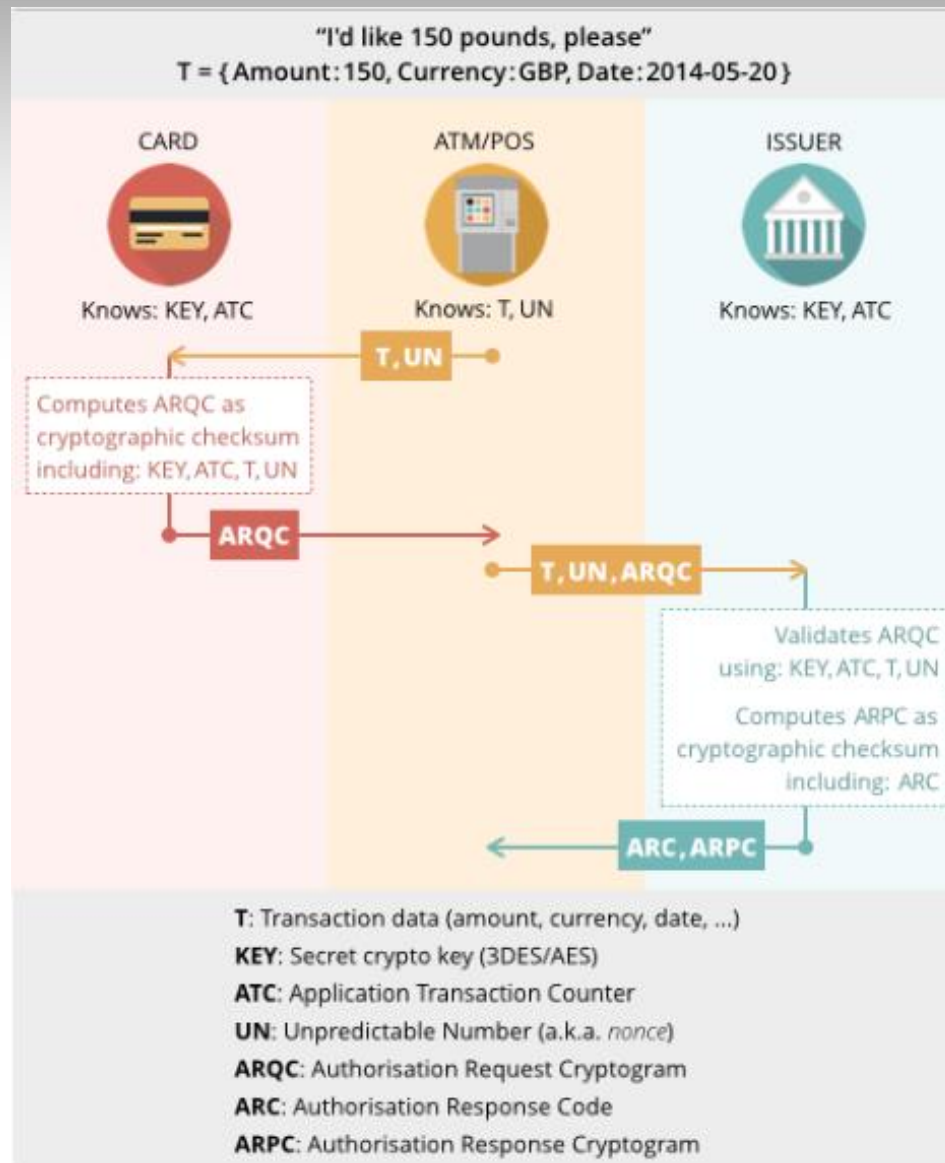


IoT

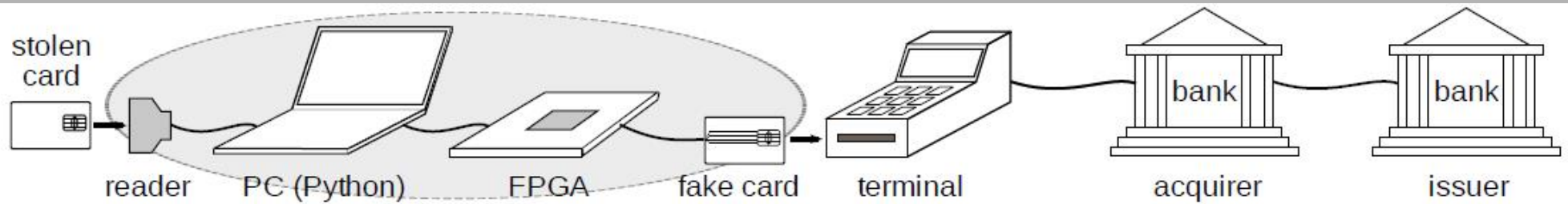
**Are we up to date with the
criminals within the technological
evolution?**

Abstract, light gray, wavy lines that flow from the bottom right towards the center of the slide, creating a sense of movement and depth.

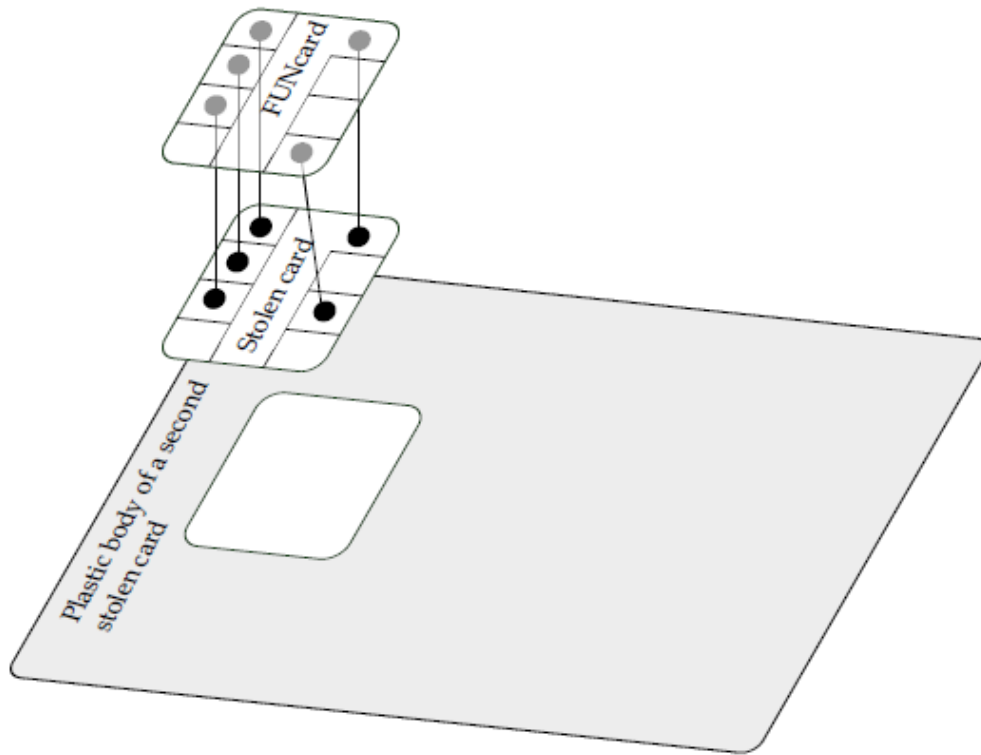
Cambridge report, a man-in-the-middle attack.



Equipment and flowchart



At the same time in the criminal world.....



40 cards total loss 680.000 dollar.

Impact of the fraud situation

- A treath to the monitary system**
- A treath to society**

But:

- Too much losses increase the propensity of change**
- The politicians act...**
- PSD2/GDPR**

Jan Olsson, NBC
National Fraud Coordinator
Head of unit

jan-o.olsson@polisen.se

+46(0)10-564 03 72

+46(0)70-736 49 32