Societal impact of Cybercrime

Jan Olsson

Cybercrime vs. Drugs (Global cost per year)

$6,000,000,000,000

$4,000,000,000,000

Crowe

UNIVERSITY OF PORTSMOUTH

The financial cost of fraud 2021

The latest data from around the world

Jim Gee and Professor Mark Button

UK stats

For the UK, Fraud losses equate to **£137 billion** each year.

Due to COVID-19 there has been a **19.8%** increase in fraud in England and Wales.

Office for National Statistics

Reducing losses by 40% would free up almost **£55 billion** each year. This sum is greater than what the UK government have spent on defence (£50.6 billion) in 2019 to 2020.

Fraud and error losses in any organisation should currently be expected to be at least **3%**, probably almost **6.5%** and possibly more than **10%**.

There has been an increase in average losses from 4.57% to **8.58%** for the period of 2019 to 2020.

88%

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?

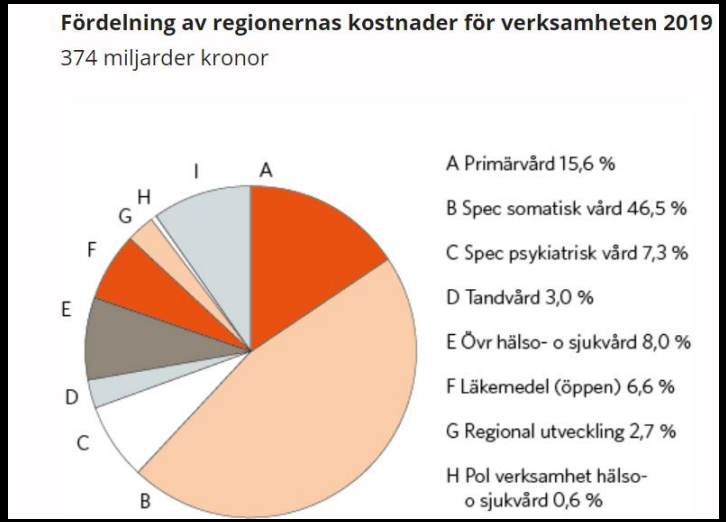
- Sweden 10.465.326 inhabitants dec 2021
- € 2.454 / Inhabitant

The Swedish loss :

€ 25.641.000.000 !

(Ca 265.000.000.000 Skr)

What does the amount represent?



5.5 % of GDP/BNP (2021)

EU Responded

GDPR (General Data Protection Regulation)

PSD2(Payment Service Directiv 2)

CNP(Card-Not-Present))

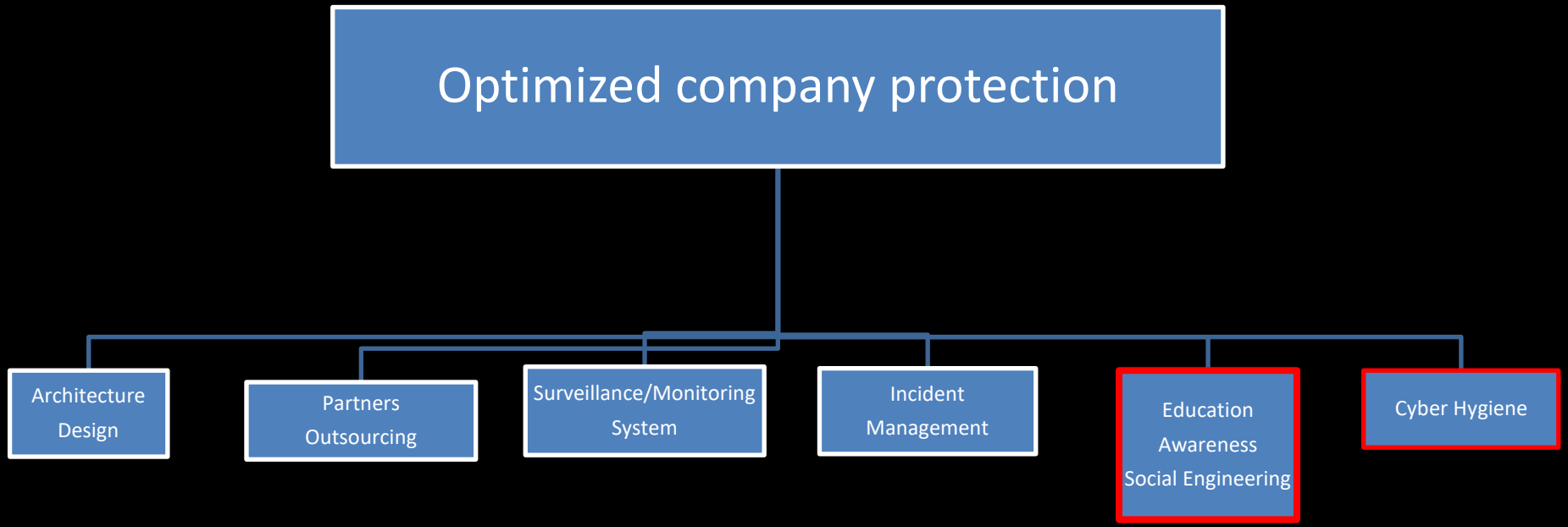
Data Breaches

Ransomware BEC/CEO-fraud (r)DDOS DDOS BankTrojans Fraud RAT

All evil after World War II

"There are only two types of companies:
those that have been hacked,
and those that will be."

Robert Mueller
FBI Director, 2012


Optimized company protection
Architecture Design
Partners Outsourcing
Surveillance/Monitoring System
Incident Management
Education Awareness Social Engineering
Cyber Hygiene

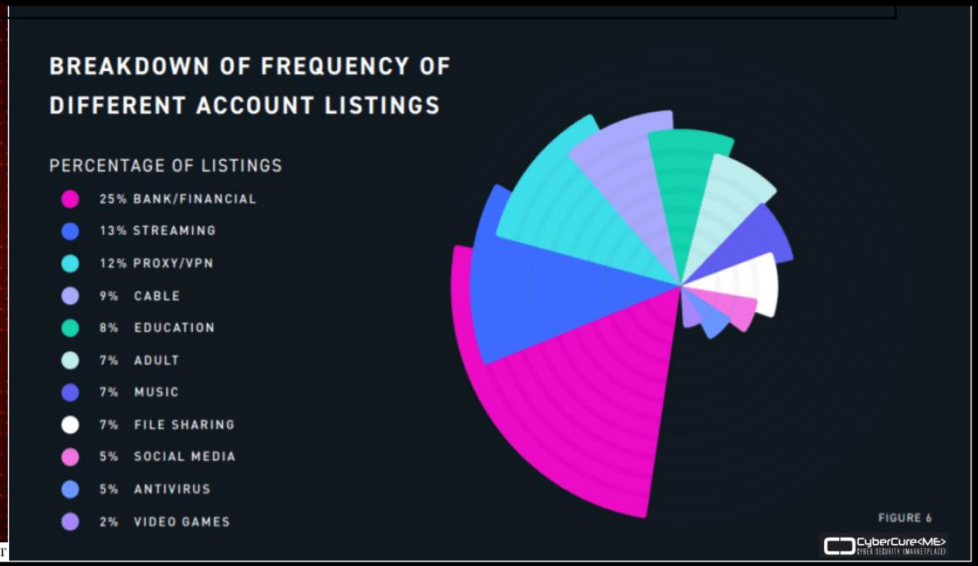
Password, the utlimate protection..

Do we use strong passwords ?

Industry	Total Exposed Credentials
Technology	5,071,144
Financials	4,915,553
Health Care	1,923,340
Industrials	1,898,434
Energy	1,745,283
Telecommunications	1,329,882
Retail	682,408
Transportation	602,003
Motor Vehicles & Parts	575,046
Aerospace & Defense	549,073

Industry	Top 5 Passwords	Industry	Top 5 Passwords
Technology	passw0rd 1qaz2wsx career121 abc123 password1	Telecommunications	cheer! welcome password 6693645 5 password1
Financials	456a33 student old123ma welcome 123456	Retail	111111 soccer1 123456789 abc123 password
Health Care	Exigent password pass1 000000 123456	Transportation	pass1 123456789 cheezy aaaaaa 112233
Industrials	12345678 1qaz1qaz passer condy password	Motor Vehicles & Parts	password 111111 penispenis 123456 3154061
Energy	password 123456 snowman old123ma 789_234	Aerospace & Defense	password1 opensesame carrier password 123456

So, are we secured ?

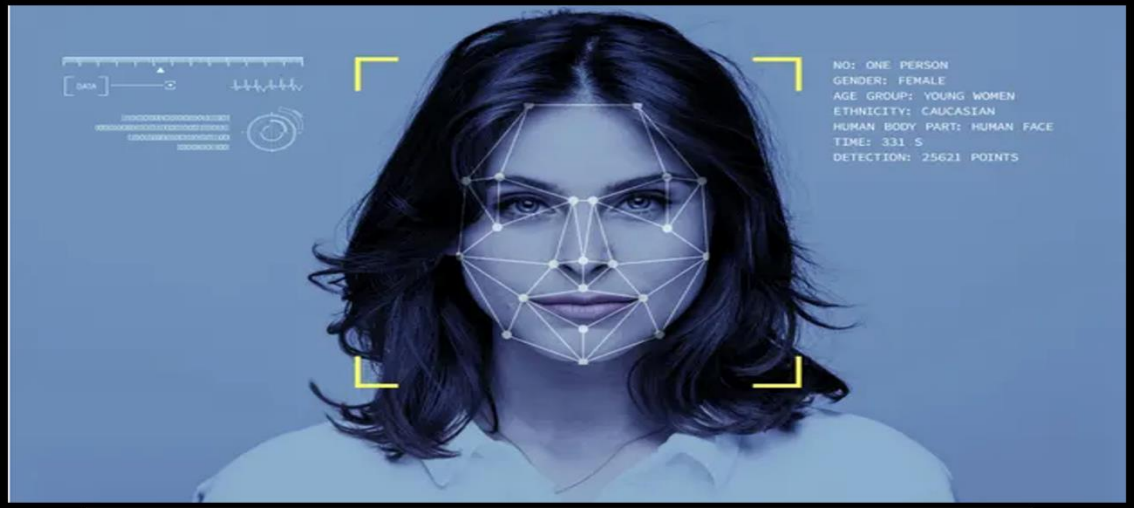


Ok, let´s go biotechnical..

Omfattningen av intrånget hos den amerikanska personalmyndigheten OPM fortsätter att växa. Nu meddelar myndigheten att 5,6 miljoner fingeravtryck stals i hackerattacken i våras, skriver IDG News.

A database containing the fingerprints of 1 million people, along with facial recognition and login data, was publicly available, researchers from the Israeli cybersecurity firm vpnmentor discovered last week

Major breach found in biometrics system used by banks, UK police and defence firms (28 million records)



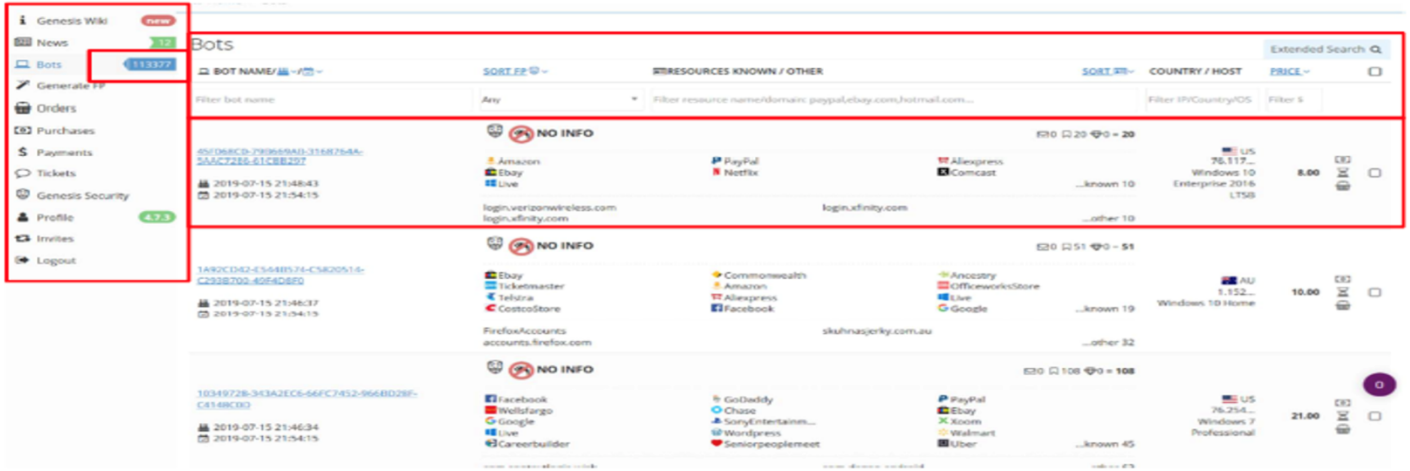
Fingerprints, facial recognition and other personal information from Biostar 2 discovered on publicly accessible database

Genesis marketplace

Specialized in selling digital fingerprints (bots)

genesis

- Genesis store an online cybercriminal marketplace for **stolen digital fingerprints**
- Bots from 5 to 200 USD searchable via panel



Multifactor Authentication

Something you have

Something you are

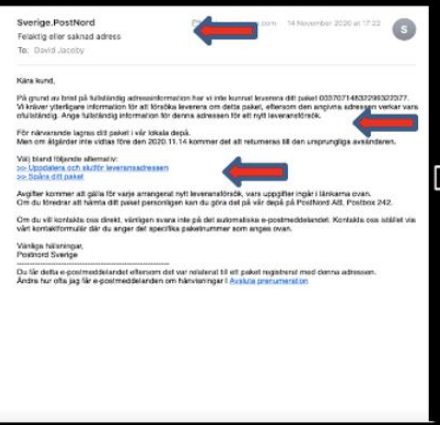
Something only you know

Consequence of digitalization

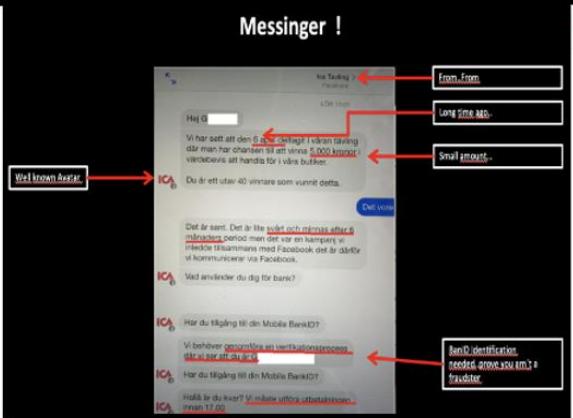
Why is safe unsafe?

Attack Vectors
Who's Who?

Phishing



Messinger !



Smishing
(Sms phishing)

Vishing
(Voice Phishing)

Uncool facts: Q3 2020 572.000 phishingsites, 367.00 unique, 1/3 is opend

Microsoft

Special Report: Ukraine

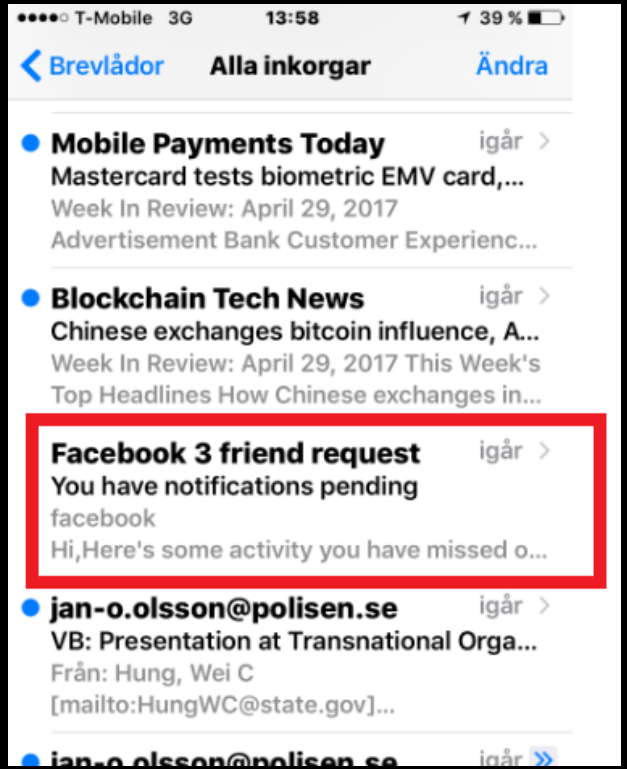
An overview of Russia's cyberattack activity in Ukraine

Recommendations

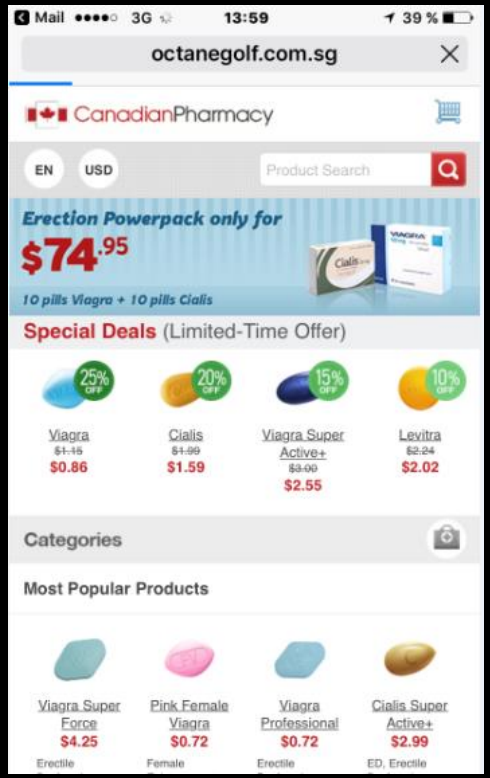
Microsoft has observed throughout our engagement that Russia-aligned cyber operations use several common tactics, techniques, and procedures to execute their intrusions. We have been able to turn these observations into actionable guidance for network defenders and security teams. Some of the most common intrusion techniques include:

- Exploitation of public facing applications or spear-phishing with attachments/links for initial access.

Phishing, who is stupid enough….?


T-Mobile 3G 13:58 39 %
Brevlådor
Alla inkorgar
Ändra
Mobile Payments Today
igår
Mastercard tests biometric EMV card,...
Week In Review: April 29, 2017
Advertisement Bank Customer Experienc...
Blockchain Tech News
igår
Chinese exchanges bitcoin influence, A...
Week In Review: April 29, 2017 This Week's
Top Headlines How Chinese exchanges in...
Facebook 3 friend request
igår
You have notifications pending
facebook
Hi,Here's some activity you have missed o...
jan-o.olsson@polisen.se
igår
VB: Presentation at Transnational Orga...
Från: Hung, Wei C
[mailto:HungWC@state.gov]...

What the .....


Mail 3G 13:59 39 %
octanegolf.com.sg
CanadianPharmacy
EN
USD
Product Search
Erection Powerpack only for
$74.95
10 pills Viagra + 10 pills Cialis
Special Deals (Limited-Time Offer)
25% OFF
Viagra
$1.15
$0.86
20% OFF
Cialis
$1.99
$1.59
15% OFF
Viagra Super Active+
$3.00
$2.55
10% OFF
Levitra
$2.24
$2.02
Categories
Most Popular Products
Viagra Super Force
$4.25
Erectile
Pink Female Viagra
$0.72
Female
Viagra Professional
$0.72
Erectile
Cialis Super Active+
$2.99
ED, Erectile

Ransomware

(1989 Dr Joseph Popp)

ATTENTION:

I have been elected to inform you that throughout your process of collecting and executing files, you have accdientally ¶HUCKΣ▶ yourself over: again, that's PHUCKED yourself over. No, it cannot be; YES, it CAN be, a ĴĪTûs has infected your system. Now what do you have to say about that? HAHAHAHA. Have ¶HÜÑ with this one and rememember, there is NO cure for

AIDS

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

2014, whole of europe was affected

Ransomware

The Phishing mail

postnord

Du har lösta paket

Vi har fått ditt paket **CT429586028SE** på [redacted]. 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.

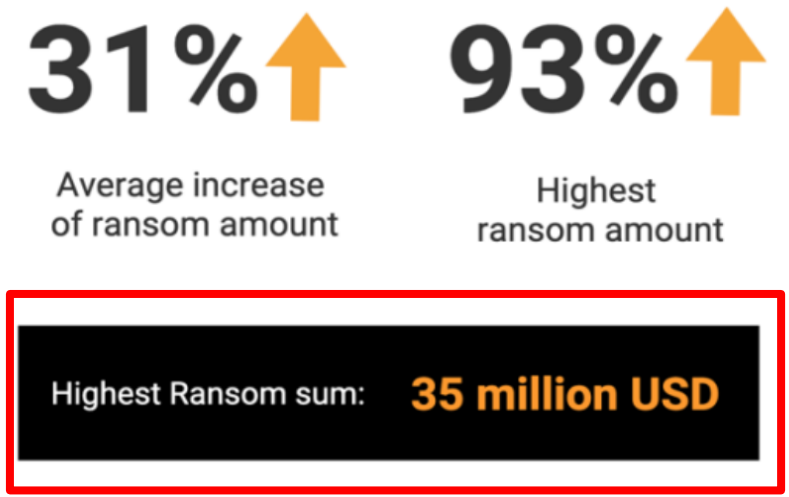
Få fraktsedel

Om paketet inte tas emot inom 20 arbetsdagar, kommer Postnord har rätt att kräva 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


Stora
coop
Uttag
agar 7-22

economical consequences



The ransom demands are calculated to be the highest value that is still affordable by the victim and are typically based on the turnover of the victim organization. The highest amount demanded has increased dramatically to over 290 million SEK in some cases, which is up 93% compared to 2019.

An important driver in the increase in the rise of ransom attacks is unregulated cryptocurrencies, like Bitcoin. The lack of regulation of Bitcoin allows cybercriminals to acquire extortion money without trace.

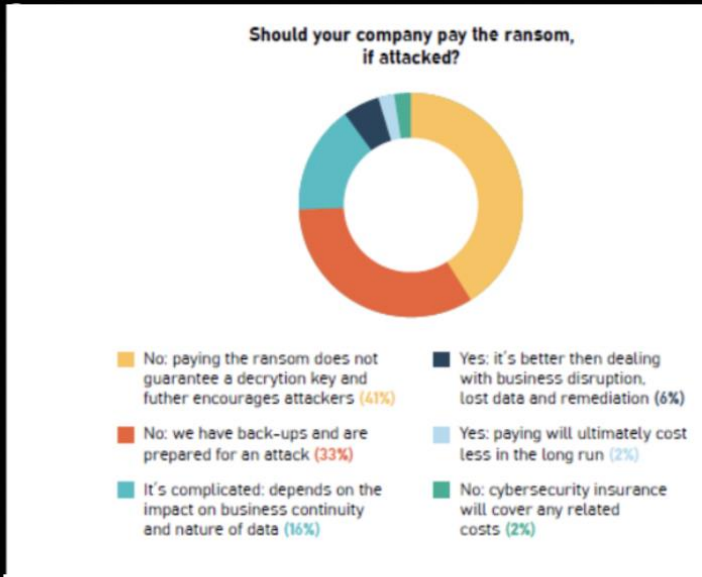
The success of ransomware attacks has also led to an increase in the number of smaller groups involved in various forms of Ransomware-as-a-Service schemes, as well as other ransom attacks. This means that the increase in average ransom demand has not risen much, as the less sophisticated attacks typically involve much lower ransom sums. Together these trends mean that the total number of ransom attacks has skyrocketed and is estimated to have increased in 2020 to around 300%, compared to 2019.

Easy peasy - just identify and captivate…or?

- State-prohibited
- State-prohibit-but-inadequate
- State-ignored
- State-encouraged
- State-shaped
- State-coordinated
- State-ordered
- State-rogue-conducted
- State-executed
- State-integrated

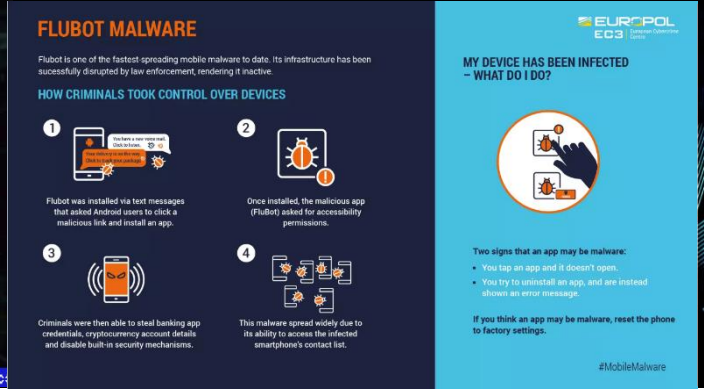
In what reality do we live in?

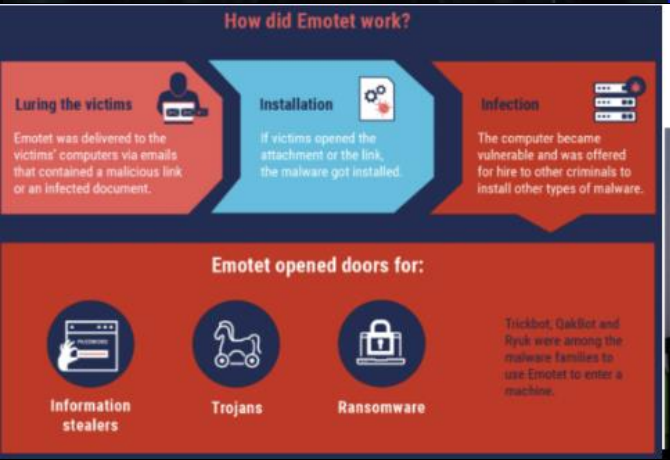
74% will definitely not pay?



But reality kicks back…

- Approx. all companies have been subjected to attempted ransomware attacks via phishingmail/social engineering
- 30% of all companies have been subjected to more qualitative attacks (Veritas)
- **60% of organizations didn´t have proper backup (Truesec)**
- **86% of companies choose to pay (Veritas)**
- 92% of organizations don't get all their data back (Forbes)
- 80% of those who payed got hit again (Threat Post)
- **3% choose to make police reports….(**Veritas)
- In 2020 the number of Ransomware attacks increased 300%
- Svensk Handel: 10% angripna 2020





*Participant countries: Australia, Belgium, Canada, France, Germany, the Netherlands, Luxembourg, Norway, Philippines, Poland, Romania, South Korea, **Sweden**, Switzerland, Kuwait, the United Kingdom, the United States and McAfee Enterprices, KPN, Bitdefender……

NoMoreRansom.org

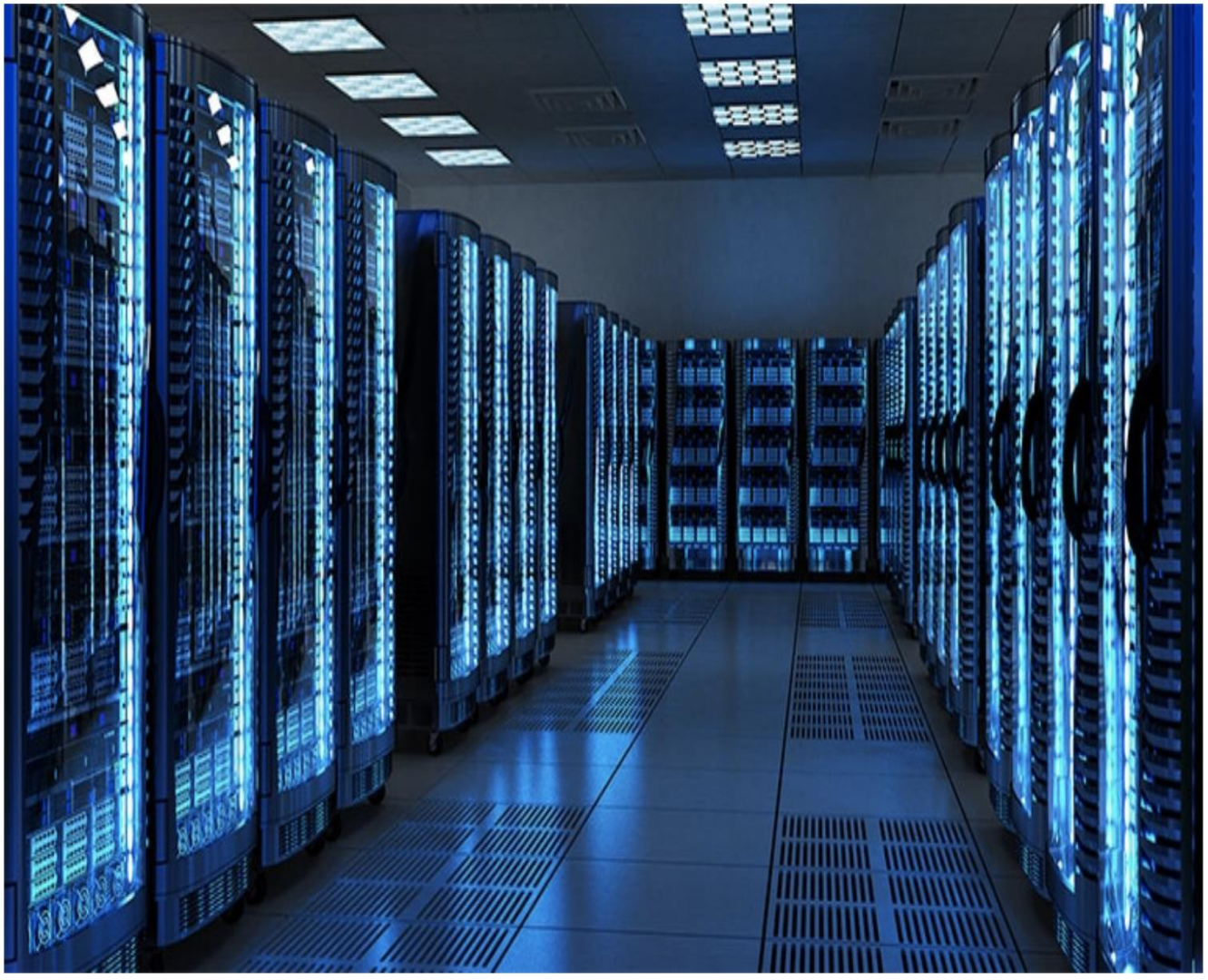
- A non profit organization, get help for free !
- 170 partners behind it: Europol, Law Enforcement organizations, IT/Cybersecurity companies
- 151 Ransomware families can be decrypted
- 121 tools, free to use
- Have saved more then € 800.000.000

IoT

The first digital murder?

DHS says it remotely hacked a Boeing 757 sitting on a runway

The future is already here!

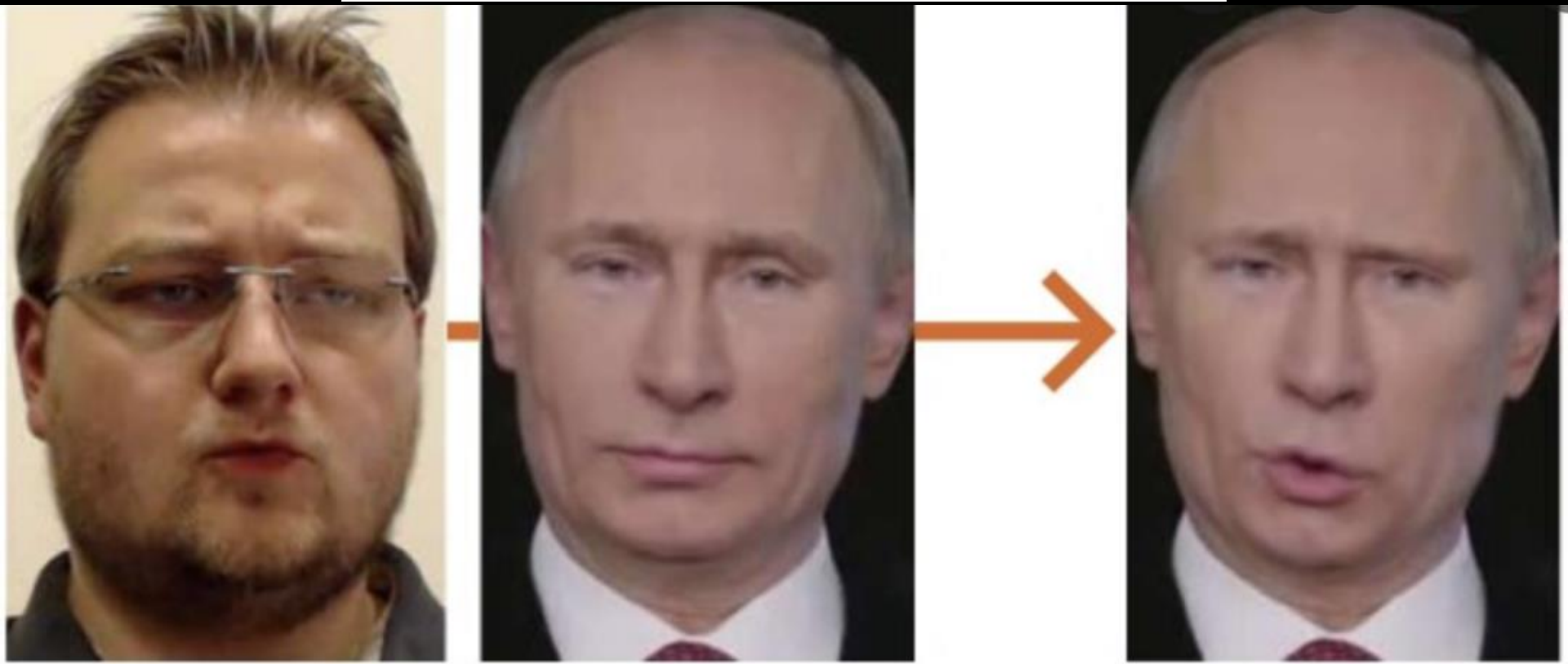


"58 procent av bolagen räknar med fler attacker mot molntjänster under 2022, men bara 37 procent har skaffat sig tillräckliga kunskaper om den egna situationen genom bedömningar av verksamheten."

Anders Carlsson, ansvarig Cyber Security, PwC Sverige

TODAY

‘Deep fakes’ are becoming more realistic thanks to new technology



Thank’s

If you need more, contact me….

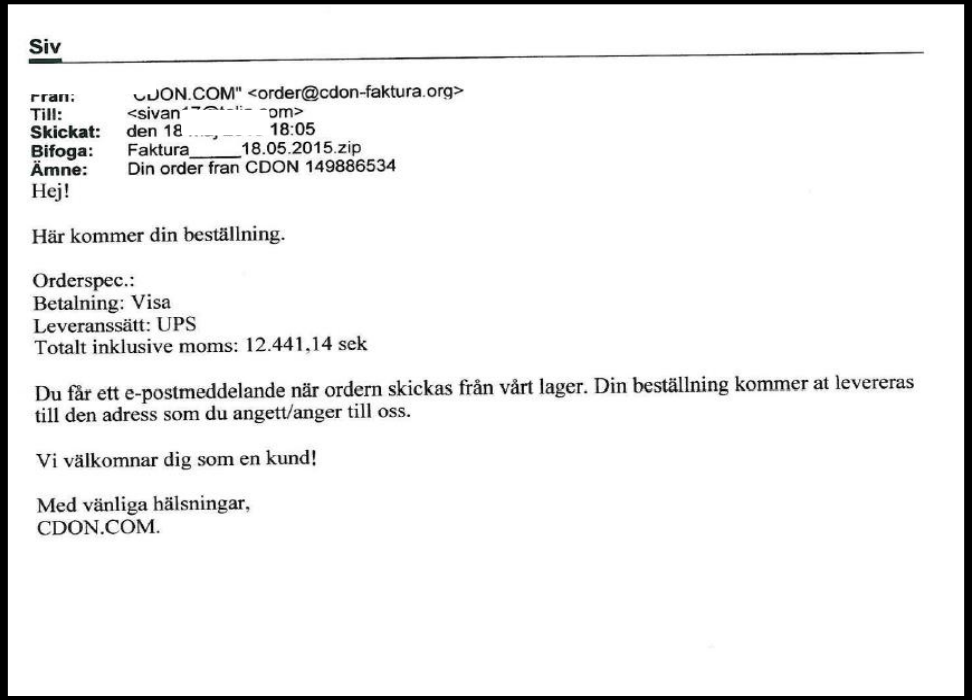
Jan Olsson
+46 (0)70-736 49 32

Investigation - Easy peacy

Follow the money it´s give you the honey, not!

Banktrojan Retefe (Rovnix)

The Phishingmail



Siv

Från: CDON.COM" <order@cdon-faktura.org>
Till: <sivan[illegible]om>
Skickat: den 18 [illegible] 18:05
Bifoga: Faktura_____18.05.2015.zip
Ämne: Din order fran CDON 149886534

Hej!

Här kommer din beställning.

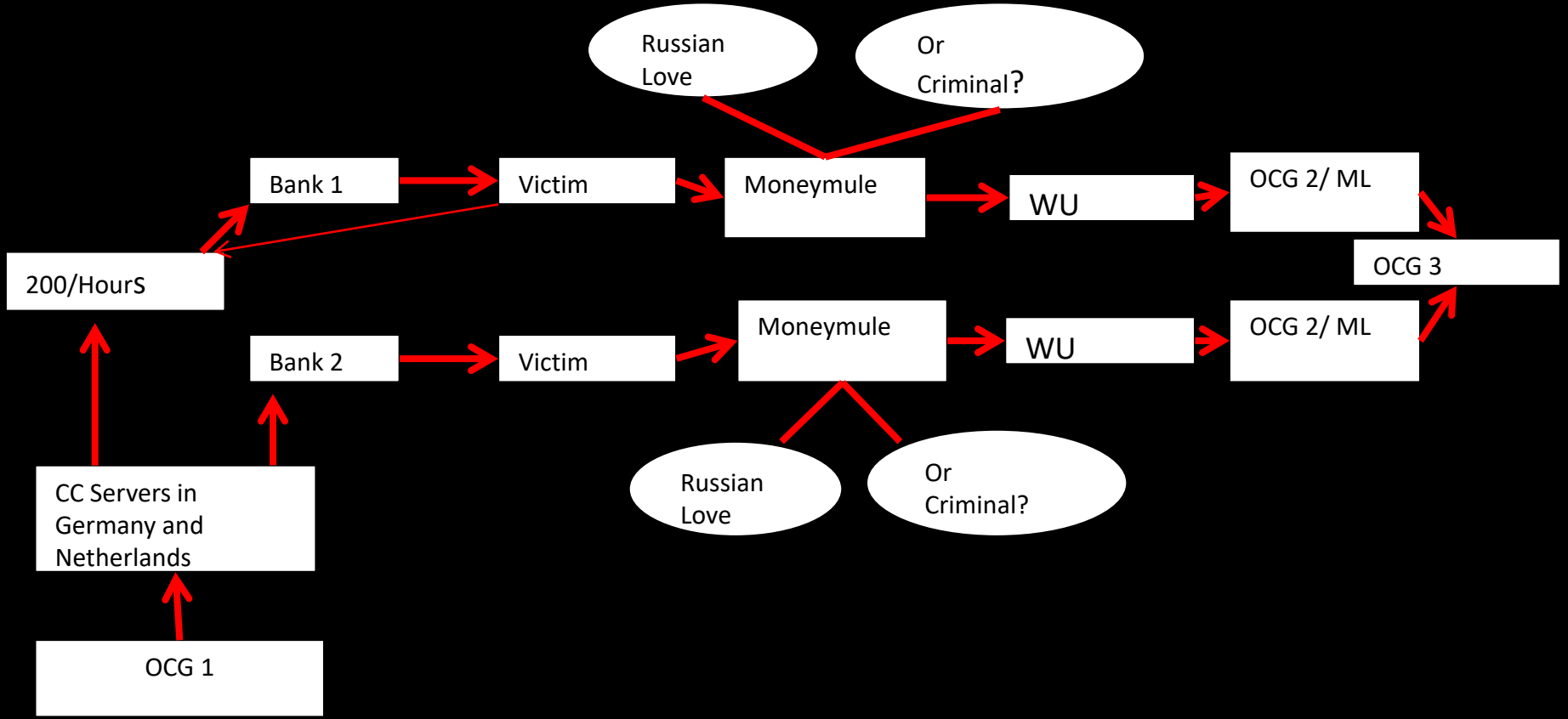
Orderspec.:
Betalning: Visa
Leveranssätt: UPS
Totalt inklusive moms: 12.441,14 sek

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


Russian Love
Or Criminal?
Bank 1
Victim
Moneymule
WU
OCG 2/ ML
OCG 3
200/HourS
Bank 2
Victim
Moneymule
WU
OCG 2/ ML
Russian Love
Or Criminal?
CC Servers in Germany and Netherlands
OCG 1

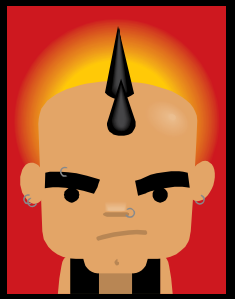
Thank’s

If you need more, contact me….

Jan Olsson
+46 (0)70-736 49 32

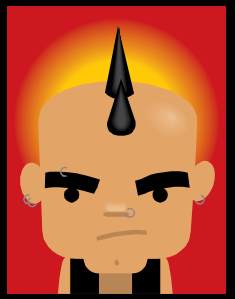
Investigate the simpliest kind of fraud today – is that simple?

Spear phishing, social engineering, Crime-as-a-service
and more…
A case study



Bad guy

Hijacking a facebook account



mapping ”friends”

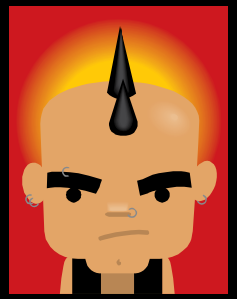
Lisa

John

Stina

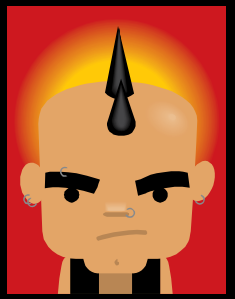
Anna

Sven



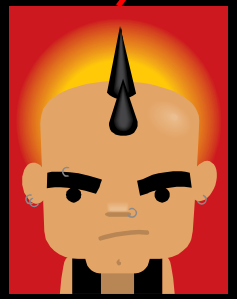
Everyday communication…

”friend”



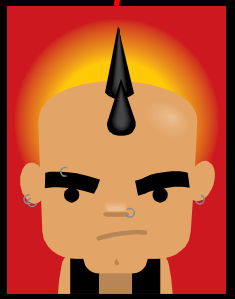
The friend hands over her login (digipass) details to the internet bank…

Access to her internet bankaccount



Access to her internetbank account

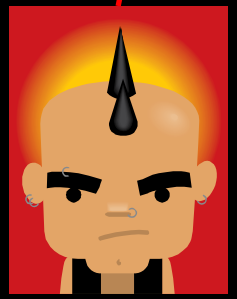
Swedbank Account belonging to Trustly (3:e party PSP)

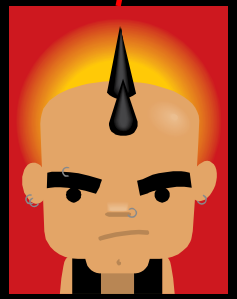


Access to her internet bankaccount

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

Skrill account (Digital wallet)





Access to her internet bankaccount

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

Skrill account (Digital wallet)

Another skrill account

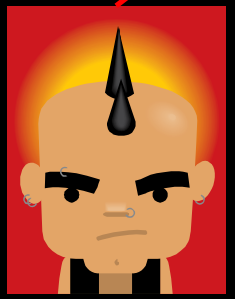
Access to her internet bankaccount

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

Skrill account (Digital wallet)

Another skrill account

Skrill prepayed Mastercard

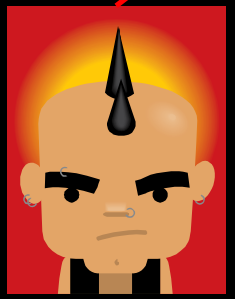


Access to her internet bankaccount

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

Skrill account (Digital wallet)

Another skrill account



Skrill prepayed Mastercard

Cash out ATM Venezuela

Cash out ATM Frankrike

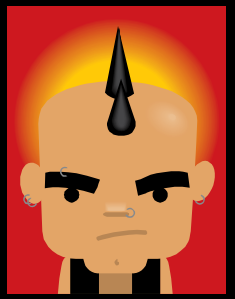
Cash out ATM Serbien

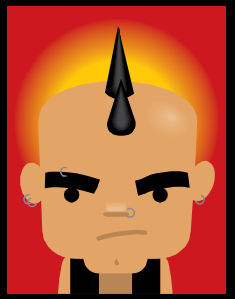
Cash out ATM Lettland

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?

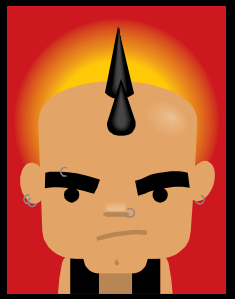
Anonymus cashcard
dongle for Internet access





Anonymus prepayed cashcard dongle for Internet access

Anonymity service (VPN)



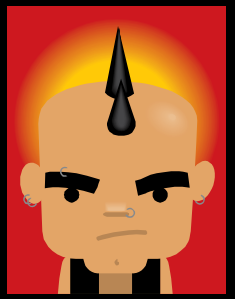
Anonymus cashcard dongle for Internet access

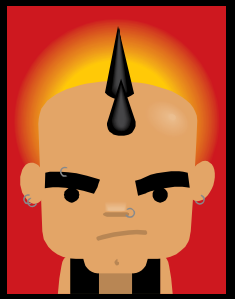
Anonymity service (VPN)

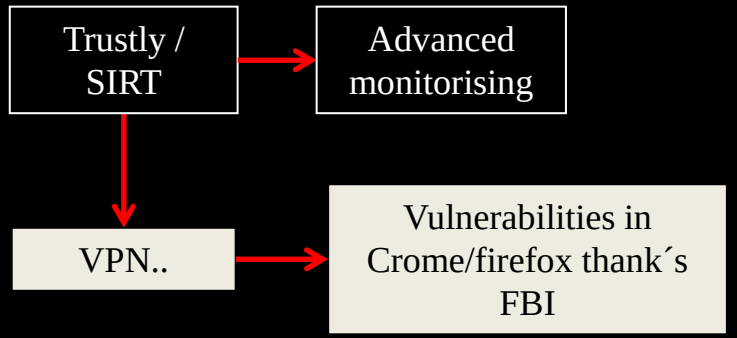
Botnet VIP72 (outside Moscow)

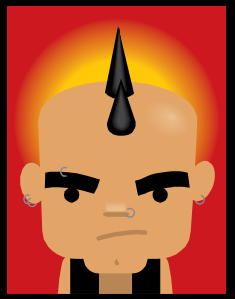
Is it even possible to move on?

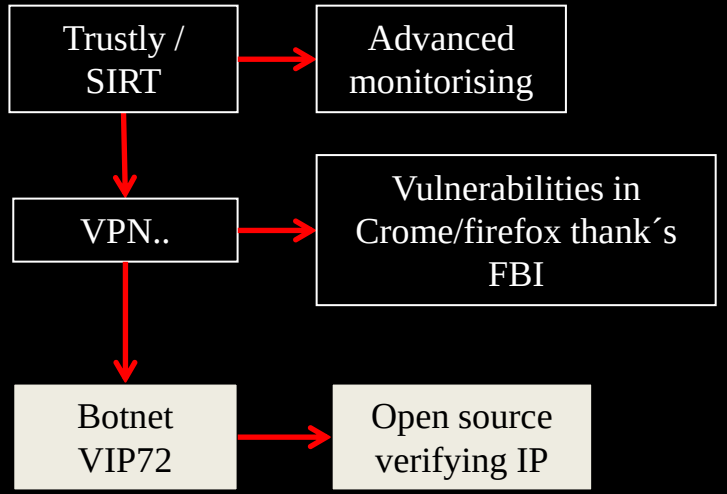
Trustly / SIRT → Advanced monitorising

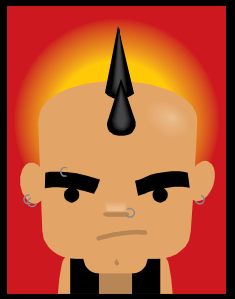


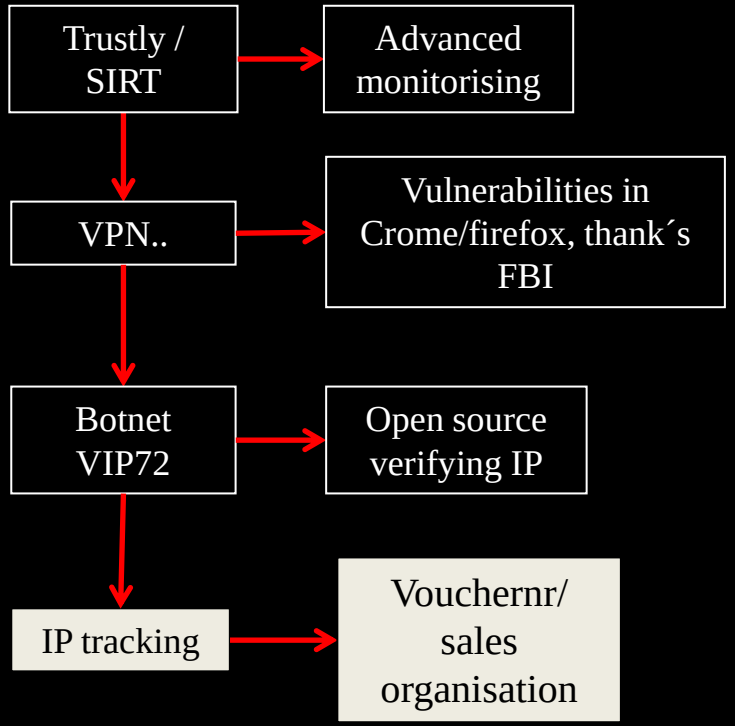


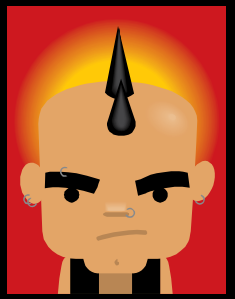

Trustly / SIRT
Advanced monitorising
VPN..
Vulnerabilities in Crome/firefox thank´s FBI




Trustly / SIRT
Advanced monitorising
VPN..
Vulnerabilities in Crome/firefox thank´s FBI
Botnet VIP72
Open source verifying IP




Trustly / SIRT
Advanced monitorising
VPN..
Vulnerabilities in Crome/firefox, thank´s FBI
Botnet VIP72
Open source verifying IP
IP tracking
Vouchernr/ sales organisation



Trustly / SIRT → Advanced monitorising

VPN.. → Vulnerabilities in Crome/firefox thank´s FBI

Botnet VIP72 → Open source verifying IP

IP tracking → Vouchernr/ sales organisation

Fysikal store → Pressbyrån Sergel

Got you !
Nothing is impossible, or ??

Thank’s

If you need more, contact me….

Jan Olsson
+46 (0)70-736 49 32