

Societal impact of Cybercrime



Jan Olsson



Cybercrime vs. Drugs (Global cost per year)



\$6,000,000,000,000

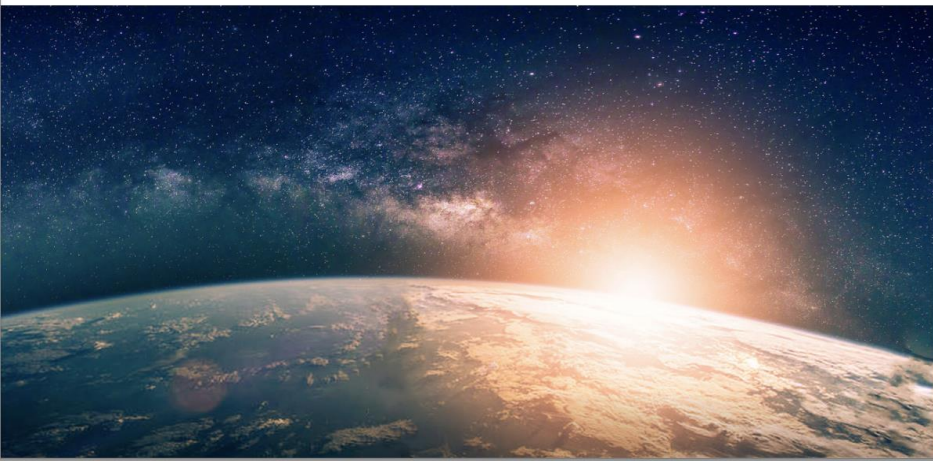


\$4,000,000,000,000

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:

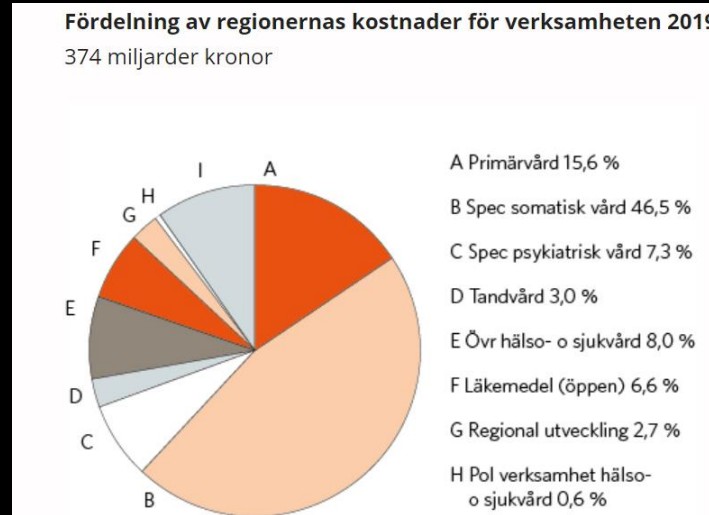
- The same conditions regarding computer density, the number of Internet connections per inhabitant, E-commerce tendencies and so on...
 - Criminal Propensity / naivety?
 - Sweden 10.465.326 inhabitants dec 2021
 - € 2.454 / Inhabitant

The Swedish loss :

€ 25.641.000.000 !

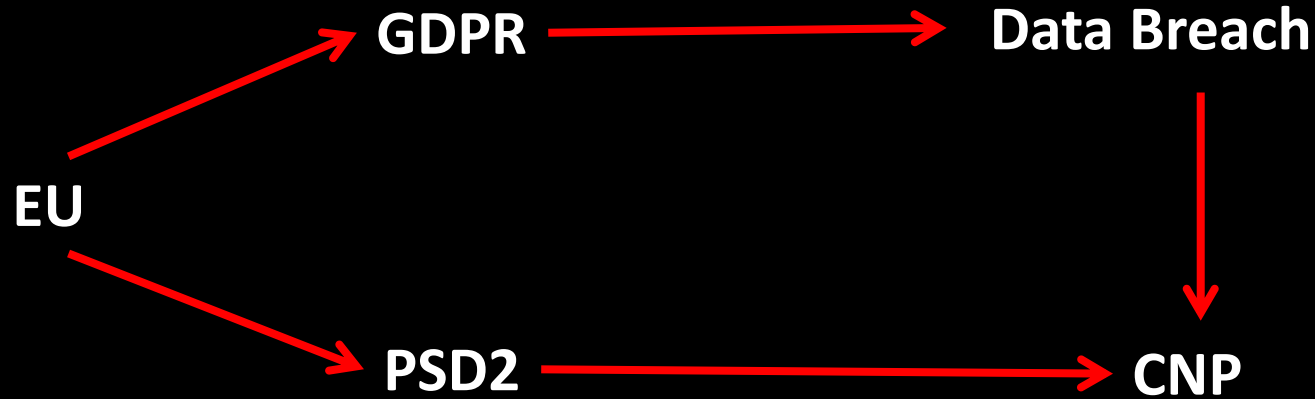
(Ca 265.000.000.000 Skr)

What does the amount represent?



5.5 % of GDP/BNP (2021)

EU Responded



GDPR (General Data Protection Regulation)

PSD2 (Payment Service Directive 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

```
graph TD; A[Optimized company protection] --- B[Architecture Design]; A --- C[Partners Outsourcing]; A --- D[Surveillance/Monitoring System]; A --- E[Incident Management]; A --- F[Education Awareness Social Engineering]; A --- G[Cyber Hygiene];
```

Architecture
Design

Partners
Outsourcing

Surveillance/Monitoring
System

Incident
Management

Education
Awareness
Social Engineering

Cyber Hygiene

Password, the ultimate 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	password lqaz!@wsx career121 abc123 password1	Telecommunications	cheer1 welcome password 66936455 password1
Financials	456a33 student old123ma welcome 123456	Retail	11111 soccer1 123456789 abc123 password
Health Care	Exigent password pass1 000000 123456	Transportation	pass1 123456789 cheezy aaaaa 112233
Industrials	12345678 lqaz!qaz passer comdy password	Motor Vehicles & Parts	password 11111 penispenis 123456 3154061
Energy	password 123456 snowman old123ma 789_234	Aerospace & Defense	password1 opensesame carrier password 123456

So, are we secured ?

Dark web researchers discovered 15 billion passwords and usernames circulating on criminal forums (Getty Images/Stockphoto)

15 BILLION STOLEN PASSWORDS ON SALE ON THE DARK WEB, RESEARCH REVEALS

INDEPENDENT

BREAKDOWN OF FREQUENCY OF DIFFERENT ACCOUNT LISTINGS

PERCENTAGE OF LISTINGS

- 25% BANK/FINANCIAL
- 13% STREAMING
- 12% PROXY/VPN
- 9% CABLE
- 8% EDUCATION
- 7% ADULT
- 7% MUSIC
- 7% FILE SHARING
- 5% SOCIAL MEDIA
- 5% ANTIVIRUS
- 2% VIDEO GAMES



FIGURE 4

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

The screenshot shows the Genesis marketplace interface. On the left is a navigation sidebar with items like 'Genesis Wiki', 'News', 'Bots', 'Orders', 'Purchases', 'Payments', 'Tickets', 'Genesis Security', 'Profile', 'Invites', and 'Logout'. The 'Bots' section is highlighted with a red box and shows a count of 113377. The main content area displays a list of bots for sale, each with a unique ID, a list of associated resources, and a price. The first bot is highlighted with a red box.

BOT NAME / ID	RESOURCES KNOWN / OTHER	COUNTRY / HOST	PRICE
401D86C3-79365941-31587684-2A5C7256-61C8E227	Amazon, eBay, Live, PayPal, Netflix	US 76.117 - Windows 10 Enterprise 2016 L758	8.00
1A82CD42-E548B574-C3620516-C2328702-40F4D8F0	Commonwealth, Amazon, Alexapress, Facebook, Ebay, Ticketmaster, Telstra, CostcoStore	AU 3.52 - Windows 10 Home	10.00
10349728-343A2EC6-66FC7852-5668D28F-C4349C92	Facebook, Wellsfargo, Google, Live, Careerbuilder, GoDaddy, Chase, SonyEntertainm..., Wordpress, Seniorpeoplemeet	US 76.254 - Windows 7 Professional	21.00

Multifactor Authentication

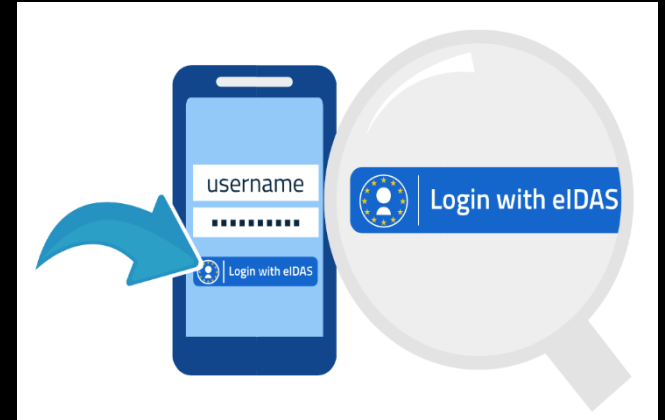
Something
you have



Something you are



Something only you know

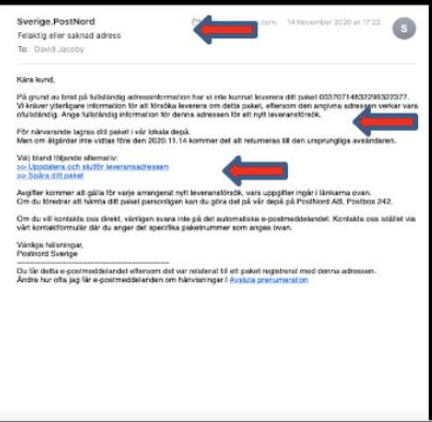


Consequence of digitalization

Why is safe unsafe?

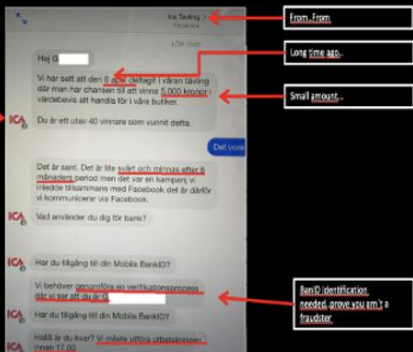
Attack Vectors Who's Who?

Phishing



Well known email

Messenger !



Smishing (Sms phishing)



Vishing (Voice Phishing)



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



Recommendations

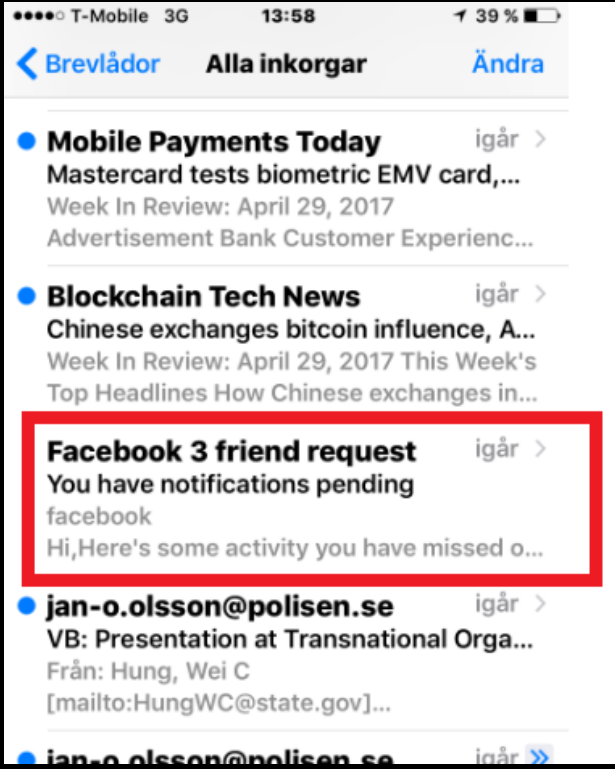
Microsoft has observed throughout our engagement that Russia-aligned cyber operations use several common tactics, techniques, and procedures to execute their intrusions. We have been able to turn these observations into actionable guidance for network defenders and security teams. Some of the most common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

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

Special Report: Ukraine

An overview of Russia's cyberattack activity in Ukraine

Phishing, who is stupid enough....?



T-Mobile 3G 13:58 39%

Brevlådar 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]...

● **jan-o.olsson@polisen.se** igår >>

What the

The screenshot shows a mobile browser view of the CanadianPharmacy website. The address bar displays 'octanegolf.com.sg'. The page features a navigation bar with 'EN' and 'USD' options, a 'Product Search' field, and a shopping cart icon. A prominent banner advertises an 'Erection Powerpack only for \$74.95', which includes '10 pills Viagra + 10 pills Cialis'. Below this, a 'Special Deals (Limited-Time Offer)' section lists four products with their respective discounts:

Product	Original Price	Discount	Current Price
Viagra	\$1.16	25% OFF	\$0.86
Cialis	\$1.99	20% OFF	\$1.59
Viagra Super Active+	\$3.00	15% OFF	\$2.55
Levitra	\$2.24	10% OFF	\$2.02

Below the special deals, there is a 'Categories' section and a 'Most Popular Products' section. The most popular products are:

Product	Price	Category
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 accidentally THUCKED
yourself over: again, that's PHUCKED yourself over. No, it cannot
be: YES, it CAN be, a Jitū has infected your system. Now what do
you have to say about that? HAHAAAA. Have THUN with this one and
remember, there is NO cure for

A I O S
```

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



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. Videofiler som innehåller pornografi, våld mot barn. Videofiler som innehåller pornografi, våld mot barn. 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 hundratentals globala platser, på nätet, från pålabböcker, 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, Timebutliker, Pressbyrån, bensinstationer och tobaksaffärer.

Ange 100 EURO Paysafecard och Ukash kod:

Ransomware

The Phishing mail

postnord

Du har lösta paket

Vi har fått ditt paket **CT429586028SE** på 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 ha 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

Öppettid
agar 7-22

10:-

10:-

30:-

49:-



10:-

15:-

10:-

economical consequences



Joakim Folstad • 1:a

Channel Account Manager på Sophos

1 mån • Redigerad •

Kostnaden för att återhämta sig från gisslanangrepp kostar en organisation i genomsnitt 7,5 miljoner kronor. I Sverige - som betalar mest för återhämtningen av gisslanprogram - är den siffran 26 miljoner kronor(!).

Lär dig 5 saker att hålla ett öga på för att undvika att det händer er eller era kunder:

[#gisslanprogram](#) [#ransomware](#)



31% ↑

Average increase
of ransom amount

93% ↑

Highest
ransom amount

Highest Ransom sum: **35 million USD**

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...

Should your company pay the ransom, if attacked?



- No: paying the ransom does not guarantee a decryption key and further encourages attackers (41%)
- No: we have back-ups and are prepared for an attack (33%)
- It's complicated: depends on the impact on business continuity and nature of data (16%)
- Yes: it's better then dealing with business disruption, lost data and remediation (6%)
- Yes: paying will ultimately cost less in the long run (2%)
- No: cybersecurity insurance will cover any related costs (2%)

- 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

THIS DOMAIN HAS BEEN SEIZED

The domain for
RAID-FORUMS

has been seized by the Federal Bureau of Investigation, the United States Secret Service, and the Department of Justice in accordance with a seizure warrant issued pursuant to 18 U.S.C. §§ 981, 982, inter alia, by the United States District Court for the Eastern District of Virginia as part of law enforcement action taken in parallel with Europol's Joint Cybercrime Action Task Force, the United Kingdom's National Crime Agency, the Swedish Police Authority, the Romanian National Police, the Internal Revenue Service Criminal Investigation and other international law enforcement partners.



NCA
National Crime Agency



Polisen
Swedish Police

FLUBOT MALWARE

Flubot is one of the fastest-spreading mobile malware to date. Its infrastructure has been successfully disrupted by law enforcement, rendering it inactive.

HOW CRIMINALS TOOK CONTROL OVER DEVICES

- Flubot was installed via text messages that asked Android users to click a malicious link and install an app.
- Once installed, the malicious app (Flubot) asked for accessibility permissions.
- Criminals were then able to steal banking app credentials, cryptocurrency account details and disable built-in security mechanisms.
- This malware spread widely due to its ability to access the infected smartphone's contact list.

MY DEVICE HAS BEEN INFECTED - WHAT DO I DO?



- Two signs that an app may be malware:
- You tap an app and it doesn't open.
 - You try to uninstall an app, and are instead shown an error message.

If you think an app may be malware, reset the phone to factory settings.

#MobileMalware



How did Emotet work?

Luring the victims



Emotet was delivered to the victims' computers via emails that contained a malicious link or an infected document.

Installation



If victims opened the attachment or the link, the malware got installed.

Infection



The computer became vulnerable and was offered for hire to other criminals to install other types of malware.

Emotet opened doors for:



Information stealers



Trojans



Ransomware

Trickbot, Qakbot and Ryuk were among the malware families to use Emotet to enter a machine.

Cyberattackererna mot Sverige

Hackergruppen utslagen av FBI: "Blev riktigt sura"



The New York Times



During a meeting in Geneva on June 16, President Biden pressured Russia's president, Vladimir V. Putin, to take action against cybercriminals who are attacking American targets. In starker terms, Mr. Biden demanded that Mr. Putin take action in a call last week. Doug Mills/The New York Times



*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 Enterprises, 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!



Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

9 February 2021

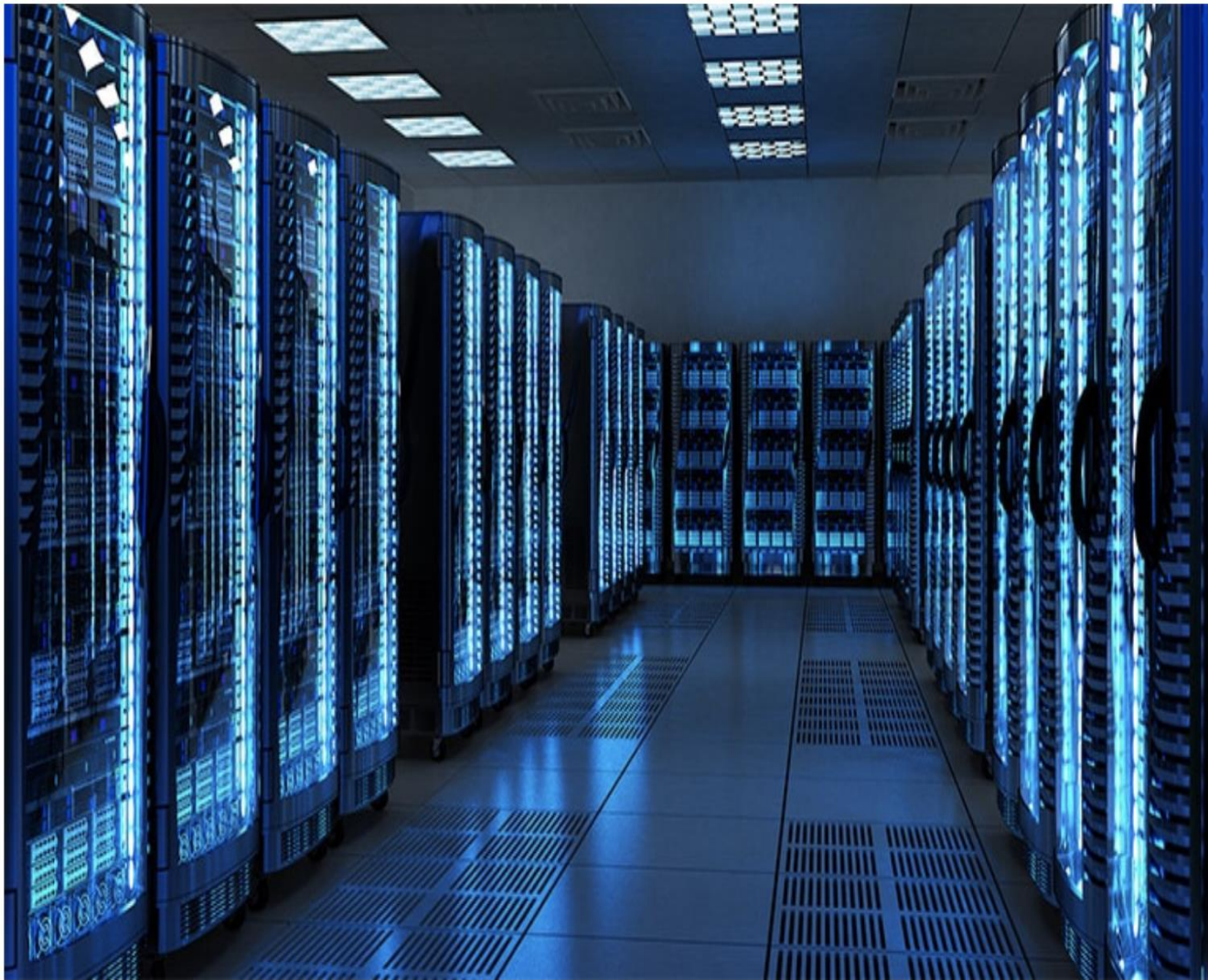
PIN Number
20210209-001

Cyber Actors Compromise US Water Treatment Facility



Confirmed: North Korean malware found on Indian nuclear plant's network

Two days after rumors of a malware infection at the Kudankulam Nuclear Power Plant surfaced on Twitter, the plant's parent company confirms the security breach.
By Gideon Coppenher for Zero Day | October 26, 2020 - 12:08 GMT (02:08 PDT) | Topic: Security

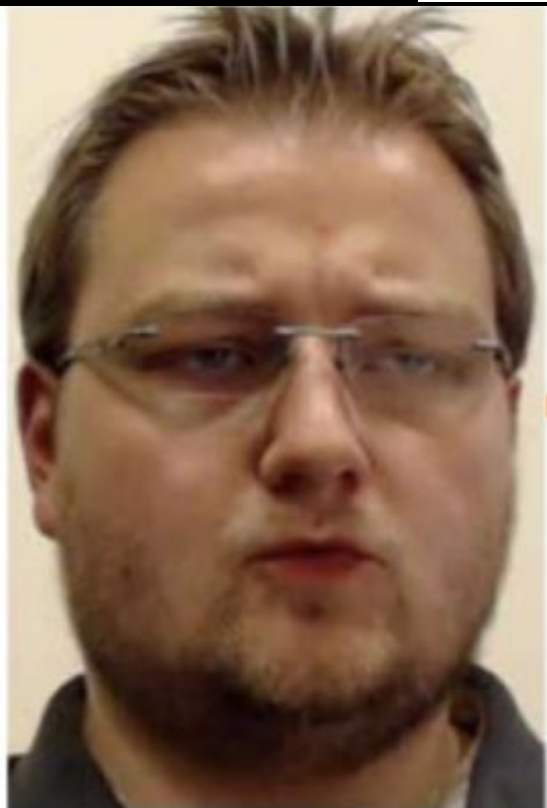


"58 procent av bolagen räknar med fler attacker mot molntjänster under 2022, men bara 37 procent har skaffat sig tillräckliga kunskaper om den egna situationen genom bedömningar av verksamheten."

Anders Carlsson, ansvarig Cyber Security, PwC Sverige

TODAY

'Deep fakes' are becoming more realistic thanks to new technology



The background of the slide is a dark green field filled with vertical columns of glowing green characters, resembling the 'Matrix' digital rain effect. The characters are mostly alphanumeric and symbols, appearing to fall from the top of the frame.

Thank's
If you need more, contact me....

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

Investigation - Easy peasy

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@retefe.com>
Skickat: den 18.05.2015 18:05
Bifoga: Faktura_18.05.2015.zip
Ämne: Din order från CDON 149886534
Hej!

Här kommer din beställning.

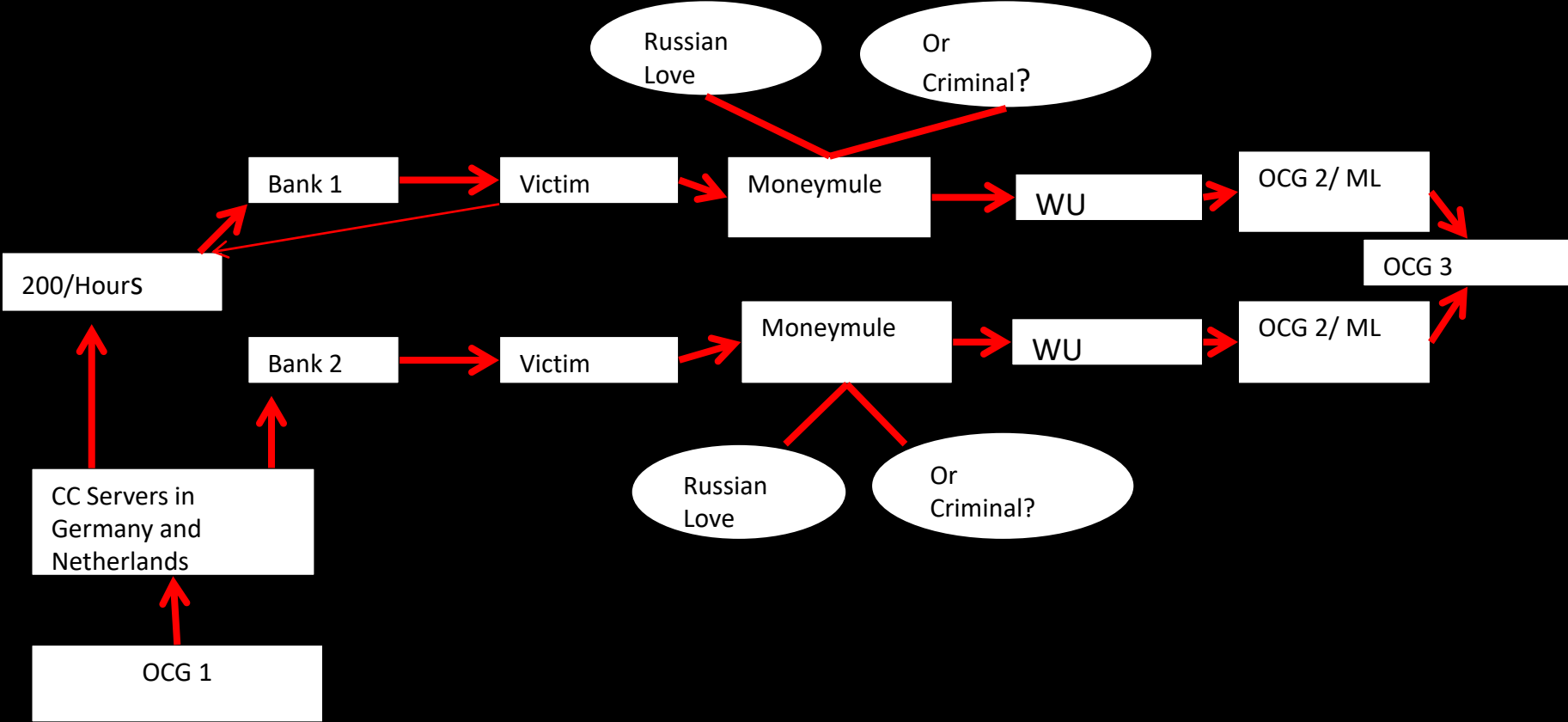
Orderspec.:
Betalning: Visa
Leveranssätt: UPS
Totalt inklusive moms: 12.441,14 sek

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



The background of the slide is a dark green field filled with vertical columns of glowing green characters, resembling the 'Matrix' digital rain effect. The characters are mostly alphanumeric and symbols, appearing to fall from the top of the frame.

Thank's
If you need more, contact me....

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

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

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

A case study





*Hijacking a facebook
account*

Bad guy



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



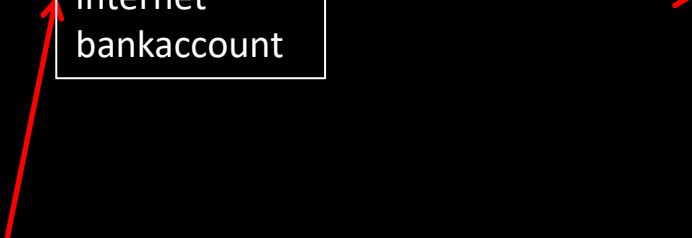
Swedbank Account belonging to Trustly (3:e party PSP)



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





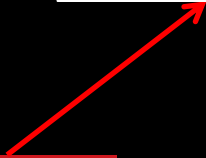
Access to her
internet
bankaccount

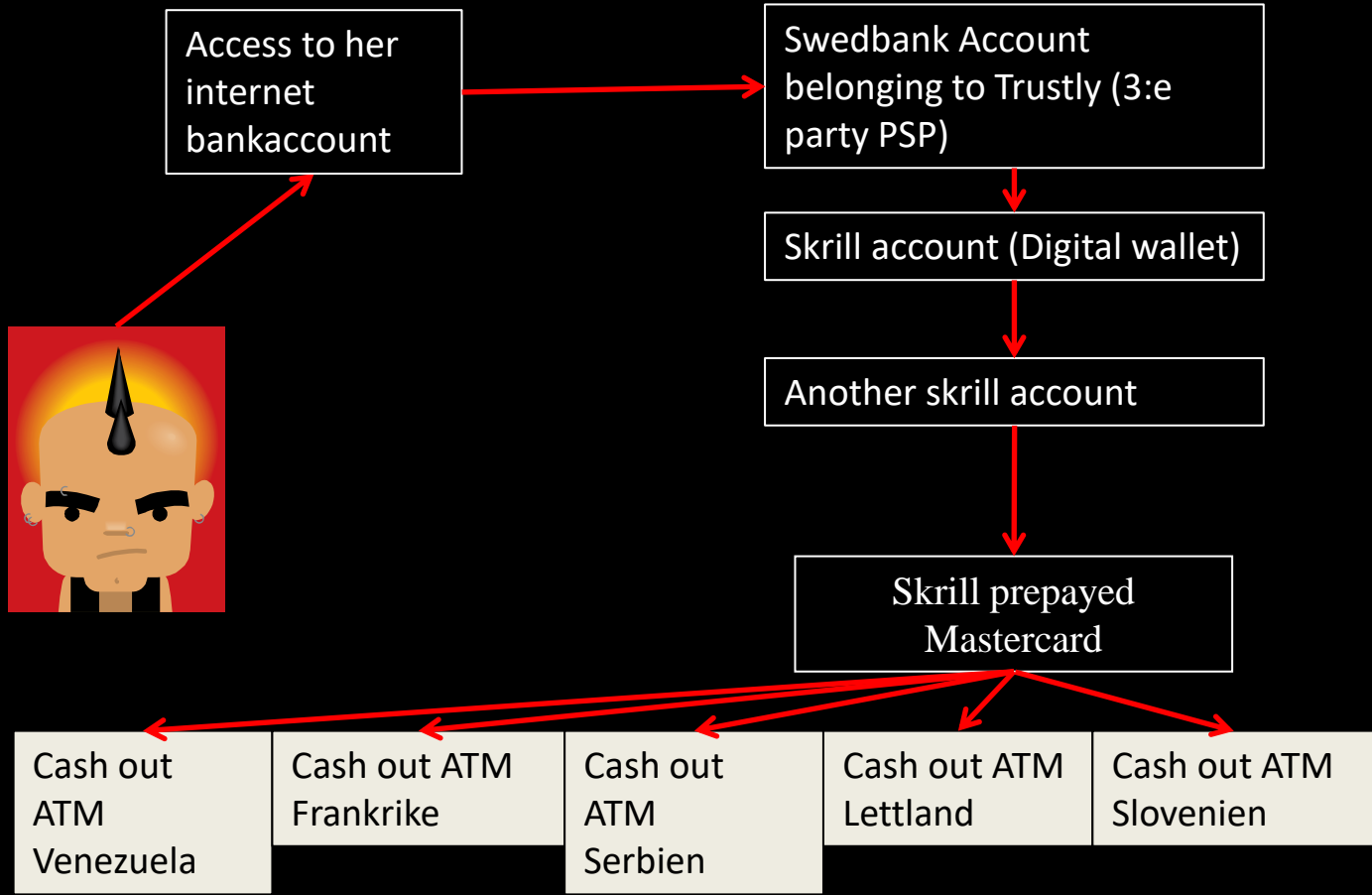
Swedbank Account
belonging to Trustly (3:e
party PSP)

Skrill account (Digital wallet)

Another skrill account

Skrill prepayed
Mastercard





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

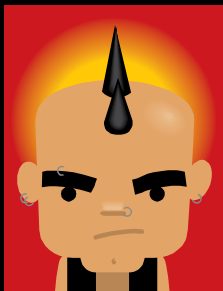




Anonymus prepaid cashcard
dongle for Internet access



Anonymity service (VPN)



Anonymus cashcard dongle for
Internet access

Anonymity service (VPN)

Botnet VIP72 (outside Moscow)

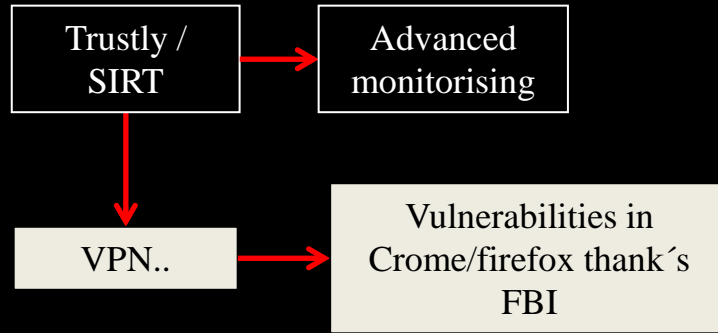
Is it even possible to move on?

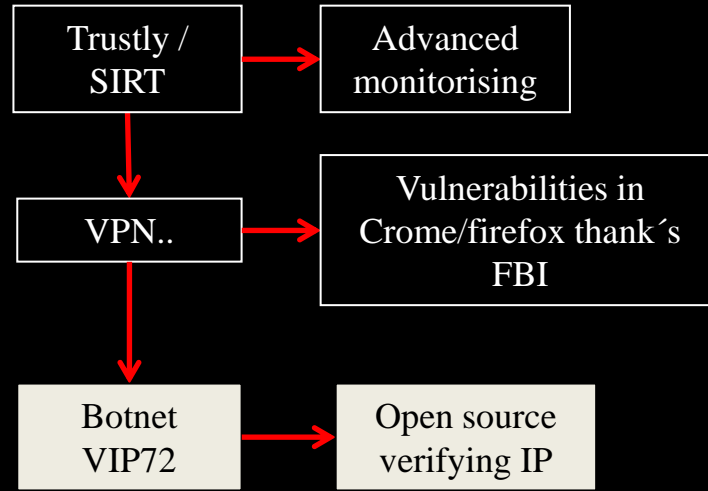
Trustly /
SIRT

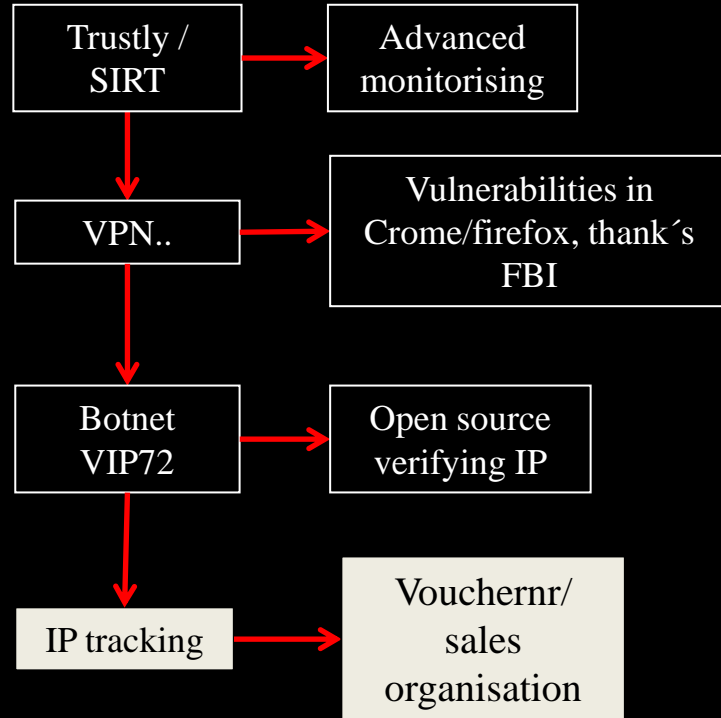


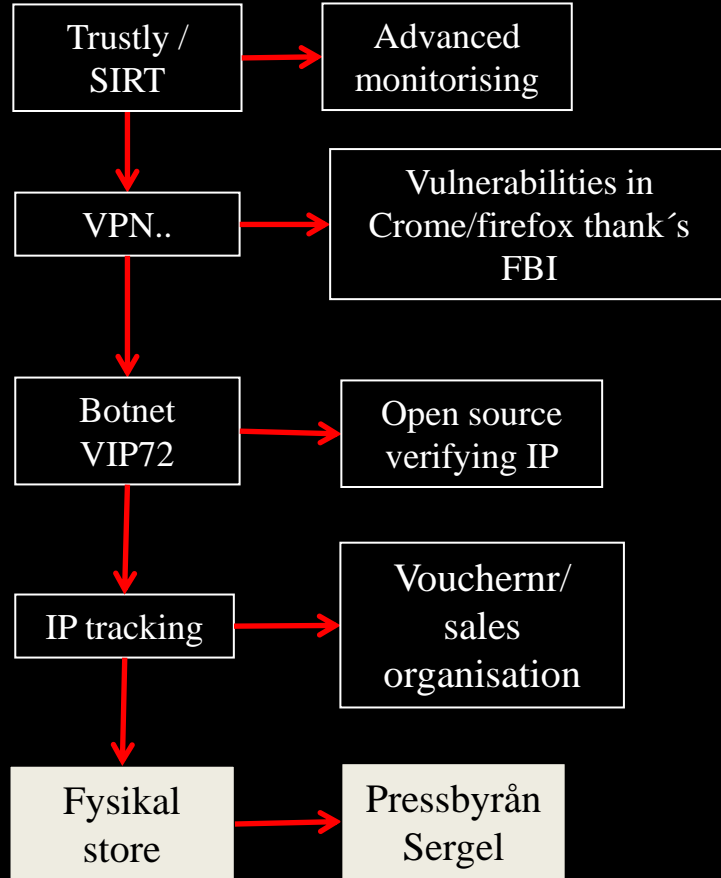
Advanced
monitoring











Got you !
Nothing is impossible, or ??



The background of the slide is a dark green field filled with vertical columns of glowing green characters, resembling the 'Matrix' digital rain effect. The characters are mostly alphanumeric and symbols, appearing to fall from the top of the frame.

Thank's
If you need more, contact me....

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