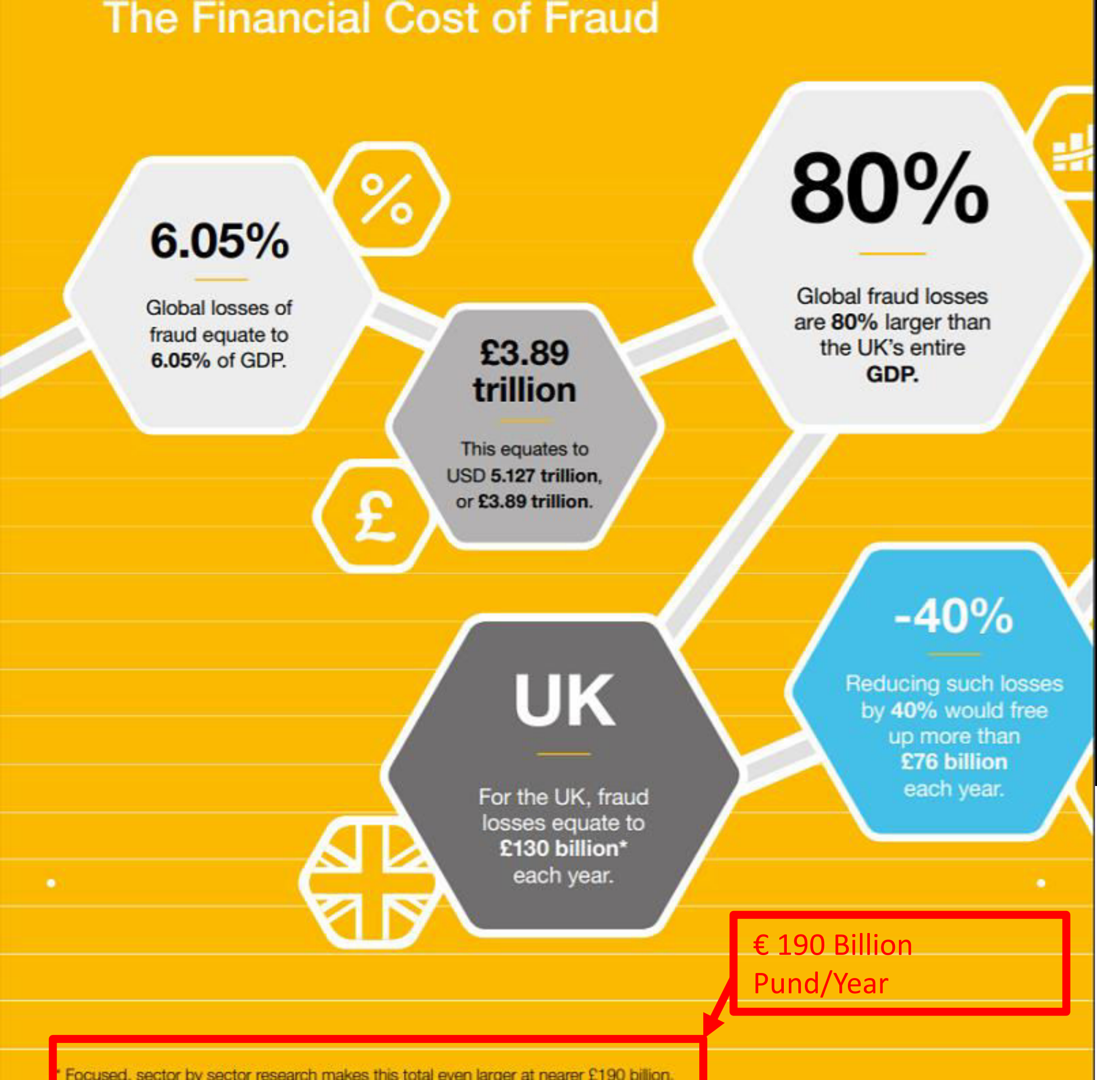
Inyett

Cybercrime – What´s the fuzz?

Jan Olsson



The Financial Cost of Fraud

6.05%

Global losses of fraud equate to **6.05%** of GDP.

£3.89 trillion

This equates to USD **5.127 trillion**, or **£3.89 trillion**.

80%

Global fraud losses are **80%** larger than the UK's entire **GDP.**

UK

For the UK, fraud losses equate to **£130 billion*** each year.

-40%

Reducing such losses by **40%** would free up more than **£76 billion** each year.

€ 190 Billion
Pund/Year

* Focused, sector by sector research makes this total even larger at nearer £190 billion.

Crowe

UNIVERSITY OF PORTSMOUTH

The Financial Cost of Fraud 2019

The latest data from around the world

Jim Gee and Professor Mark Button

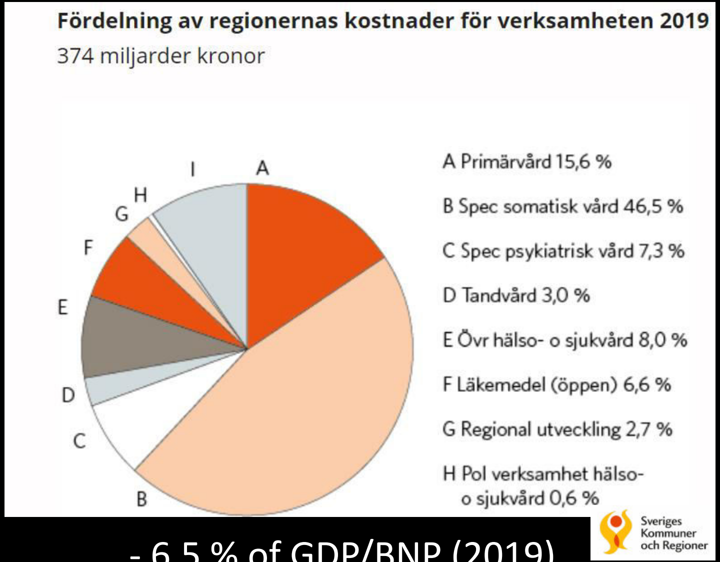
The Swedish losses:

349.989.000.000 Sek !

Aprox SEK 350 billion or € 36.31 billion

Norway   € 18.66 billion
Denmark € 20.41 billion
Finland   € 19.53 billion

What does the amount represent?



Fördelning av regionernas kostnader för verksamheten 2019

374 miljarder kronor

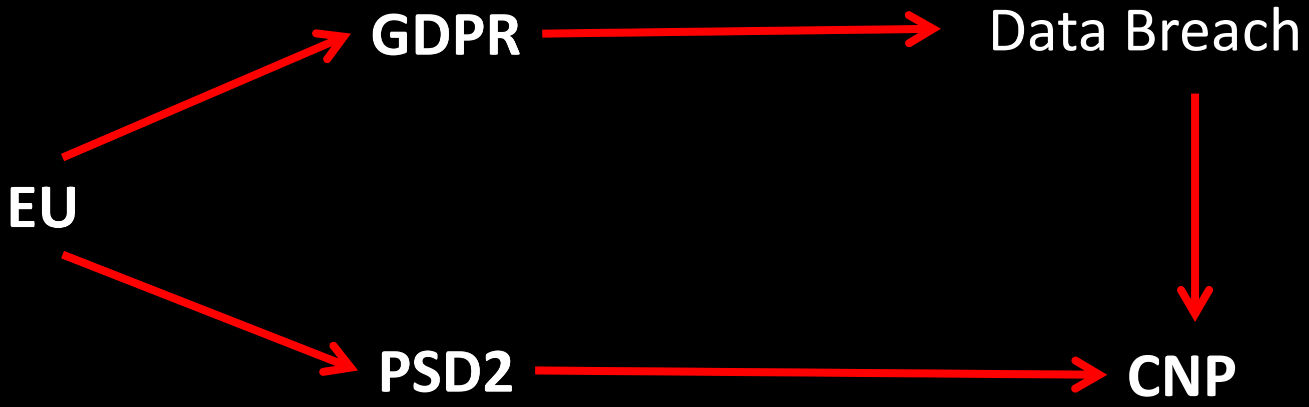
- 6.5 % of GDP/BNP (2019)
- 11.090 Skr/ sec.

Global Remarks

4.700.000.000.000 Euro = The global costs of Fraud (UKFCMC)

5.500.000.000.000 Euro = The global costs for companies due to

EU Responded



EU

GDPR

PSD2

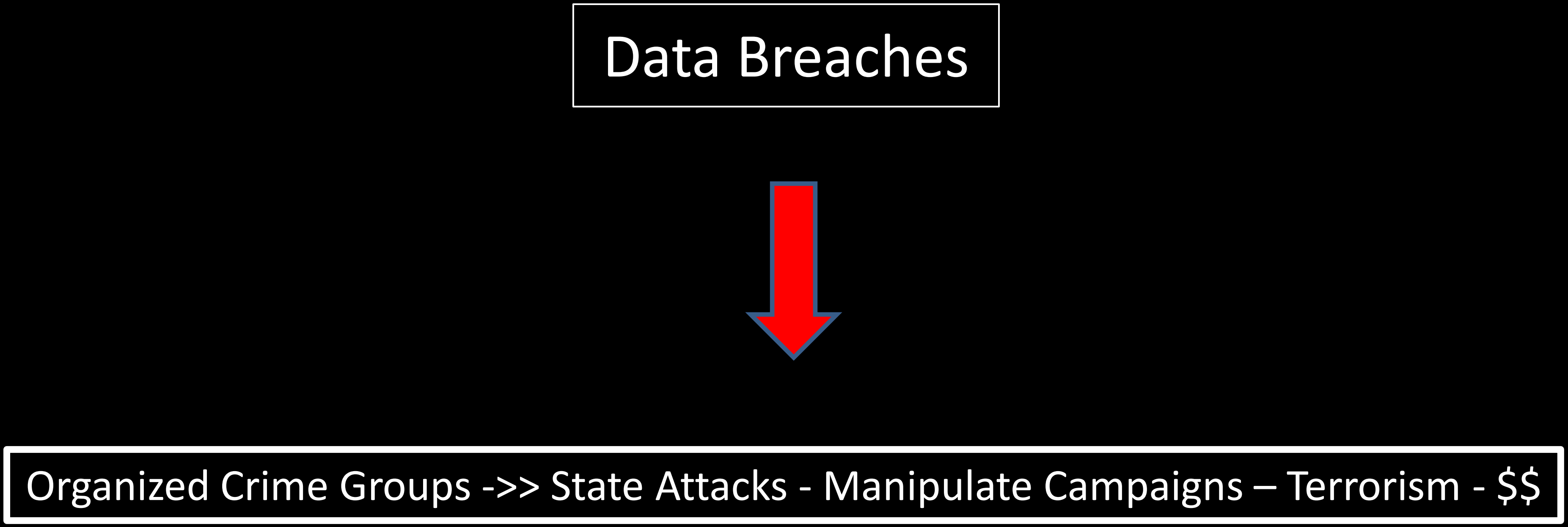
Data Breach

CNP

GDPR (General Data Protection Regulation)

PSD2(Payment Service Directiv 2)

CNP(Card-Not-Present))



Data Breaches

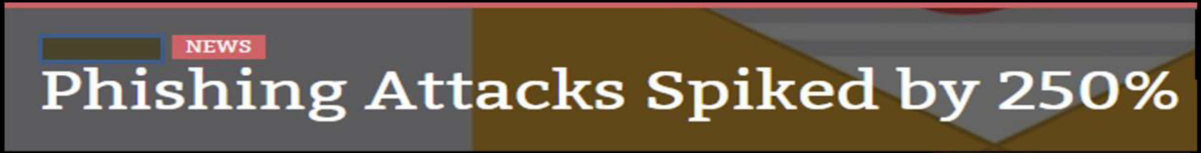
Organized Crime Groups ->> State Attacks - Manipulate Campaigns – Terrorism - $$

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



[redacted] NEWS

Phishing Attacks Spiked by 250%

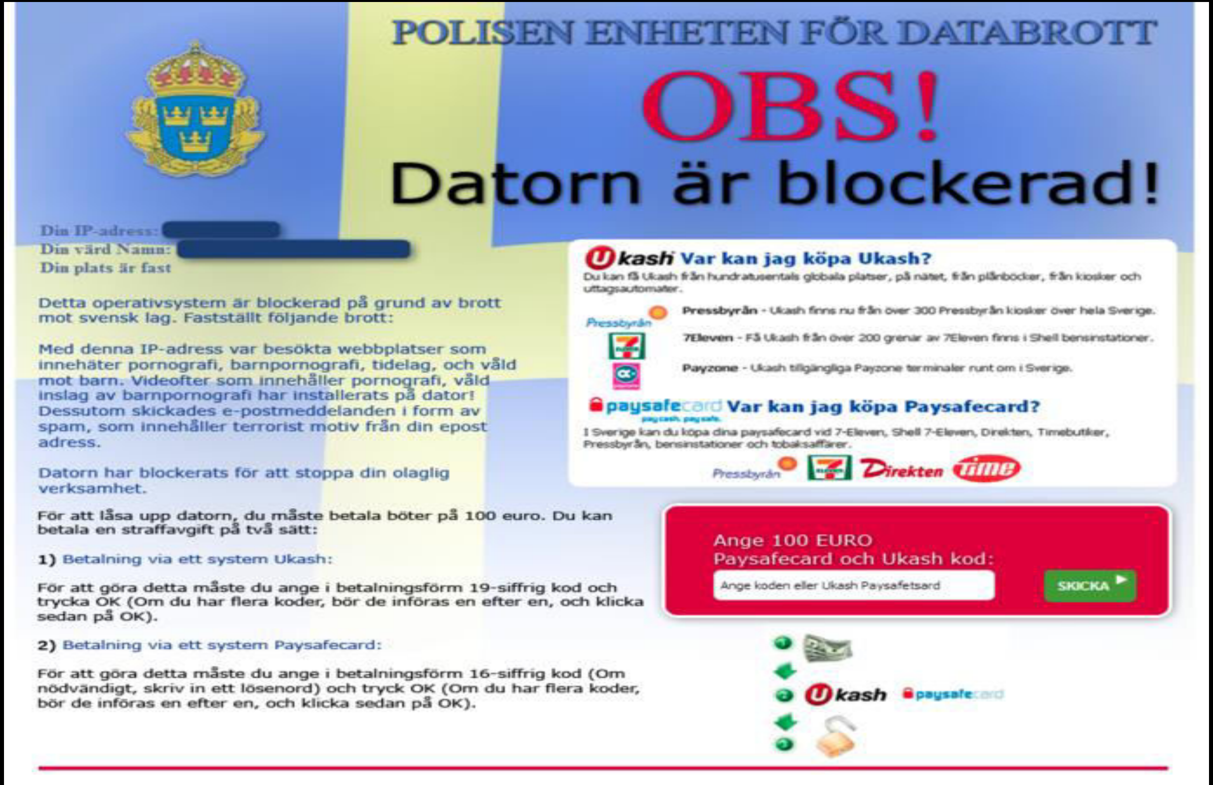
info security

STRATEGY I INSIGHT I TECHNOLOGY

COMB: largest breach of all time leaked online with 3.2 billion records

contains more than 3.2 billion unique pairs of cleartext emails and passwords

2014, the 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 innehäter 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 betalningsförm 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 betalningsförm 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 hundratusentals globala platser, på nätet, från plånböcker, 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.

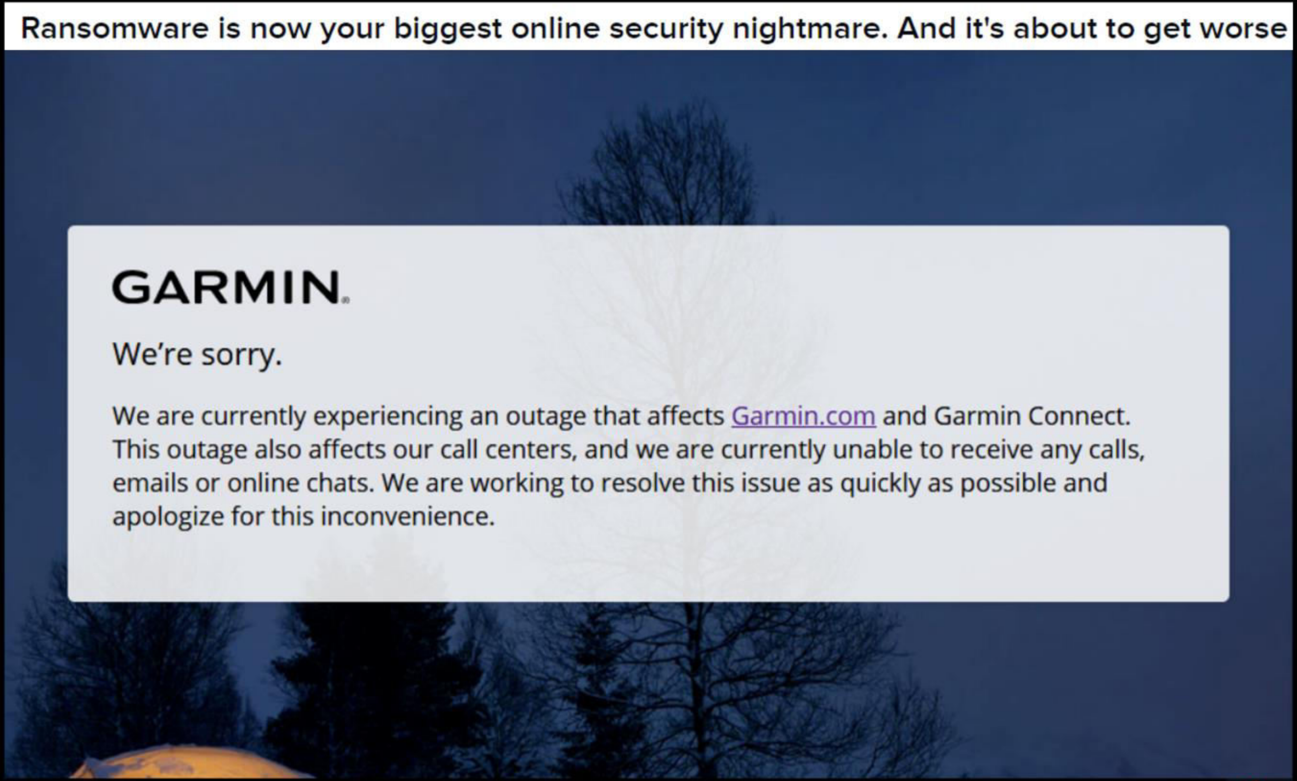
Payzone - Ukash tillgängliga Payzone terminaler runt om i Sverige.

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.

Ange 100 EURO
Paysafecard och Ukash kod:

To Day



Ransomware is now your biggest online security nightmare. And it's about to get worse

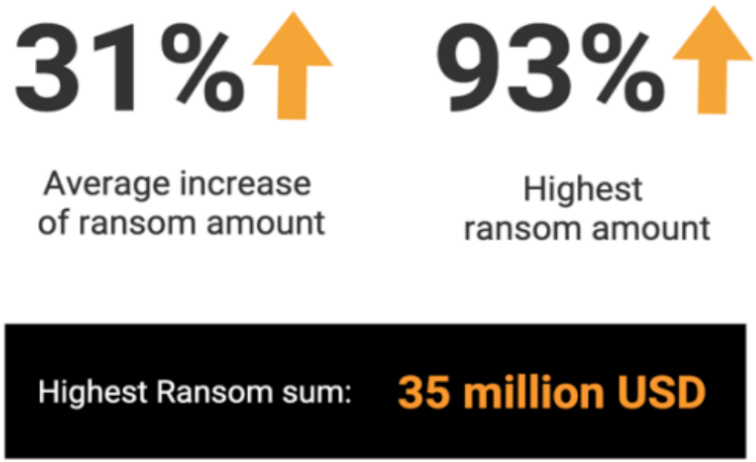
GARMIN.

We're sorry.

We are currently experiencing an outage that affects Garmin.com and Garmin Connect. This outage also affects our call centers, and we are currently unable to receive any calls, emails or online chats. We are working to resolve this issue as quickly as possible and apologize for this inconvenience.

Ransom € 10.000.000

ZDNet



31% ↑

Average increase of ransom amount

93% ↑

Highest ransom amount

Highest Ransom sum: 35 million USD

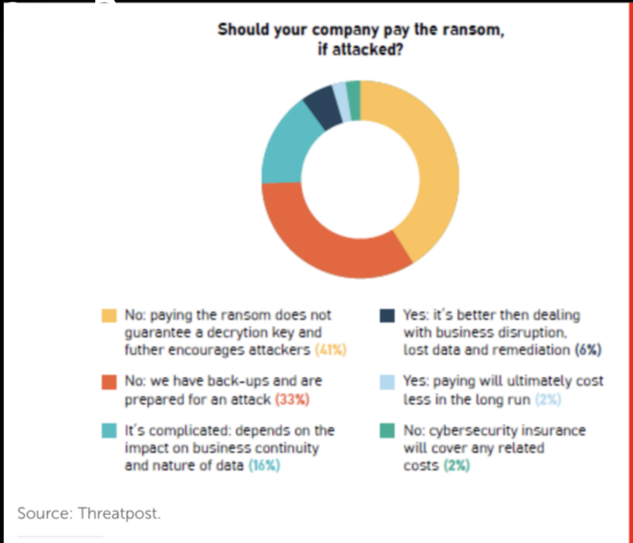
The ransom demands are calculated to be the highest value that is still affordable by the victim and are typically based on the turnover of the victim organization. The highest amount demanded has increased dramatically to over 290 million SEK in some cases, which is up 93% compared to 2019.

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.

In what reality do we live in?

74% will definitely not



Source: Threatpost.

But reality kicks back...

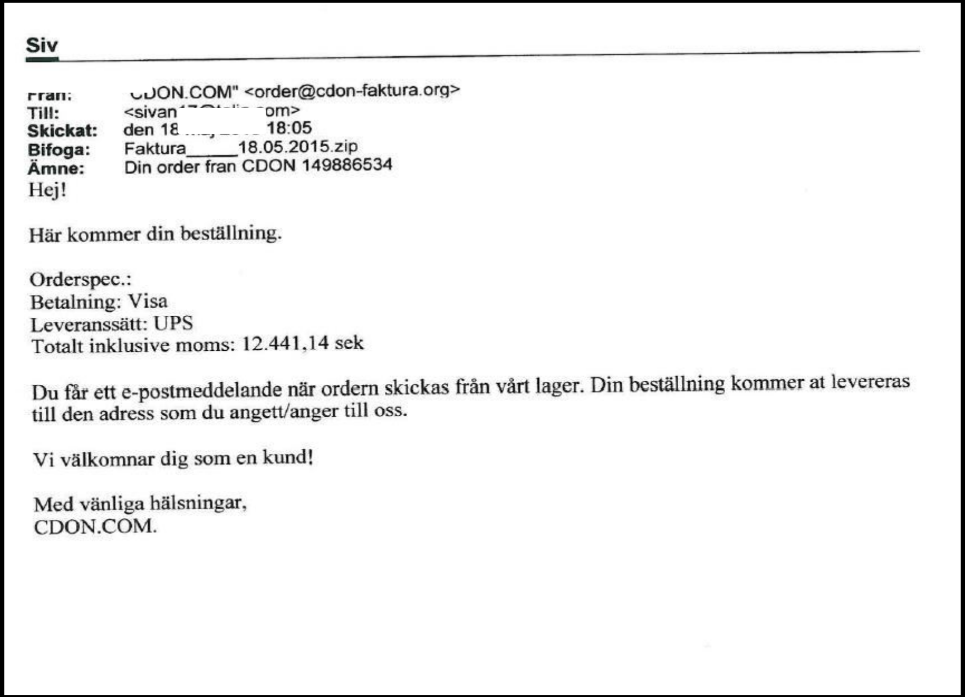
- Approx. all companies have been subjected to attempted ransomware attacks via phishingmail/social engineering
- 30% of all companies have been subjected to more qualitative attacks (Veritas)
- **60% of organizations didn´t have proper backup (Truesec)**
- **86% of companies choose to pay (Veritas)**
- 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% (Truesec)

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

Banktrojan Retefe (Rovnix)

The Phishingmail



Siv

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

Hej!

Här kommer din beställning.

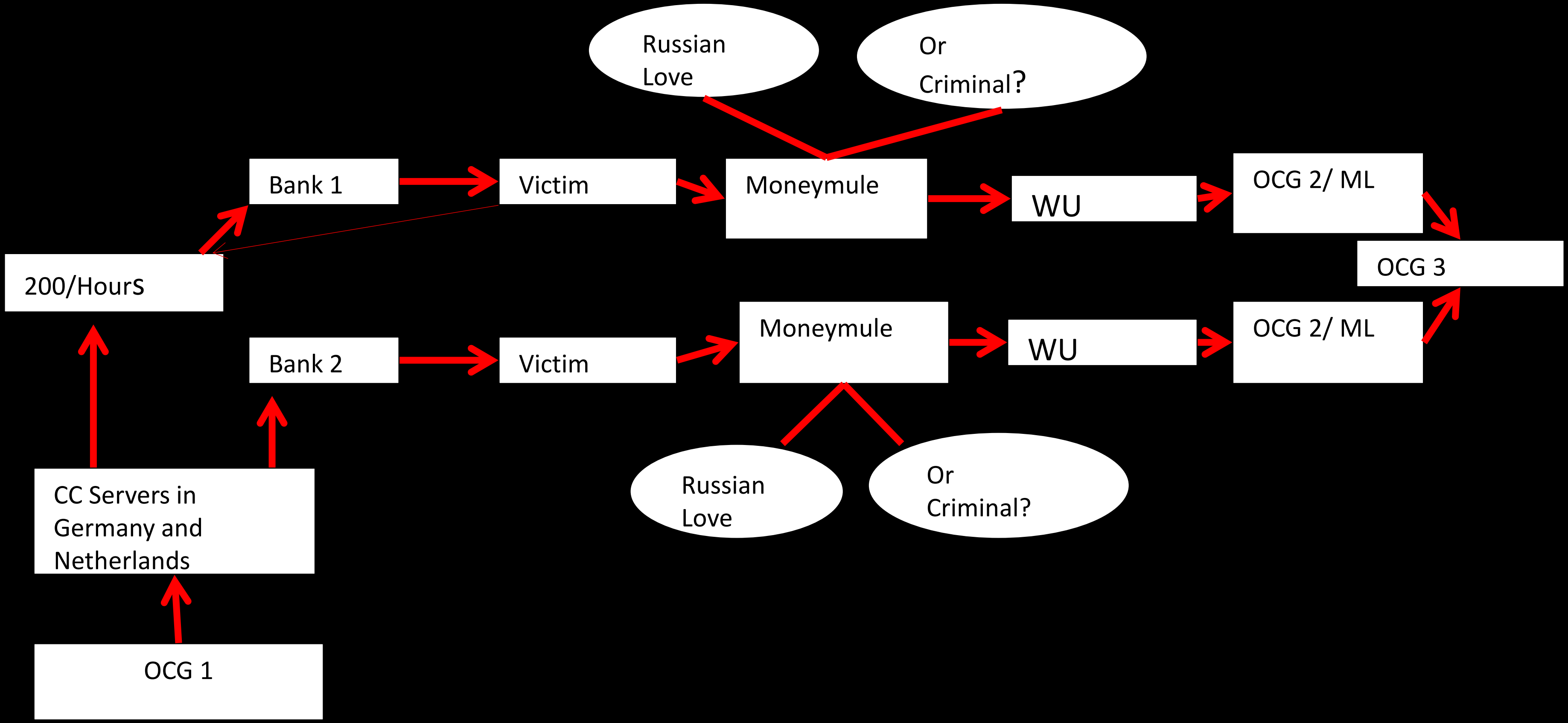
Orderspec.:
Betalning: Visa
Leveranssätt: UPS
Totalt inklusive moms: 12.441,14 sek

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!

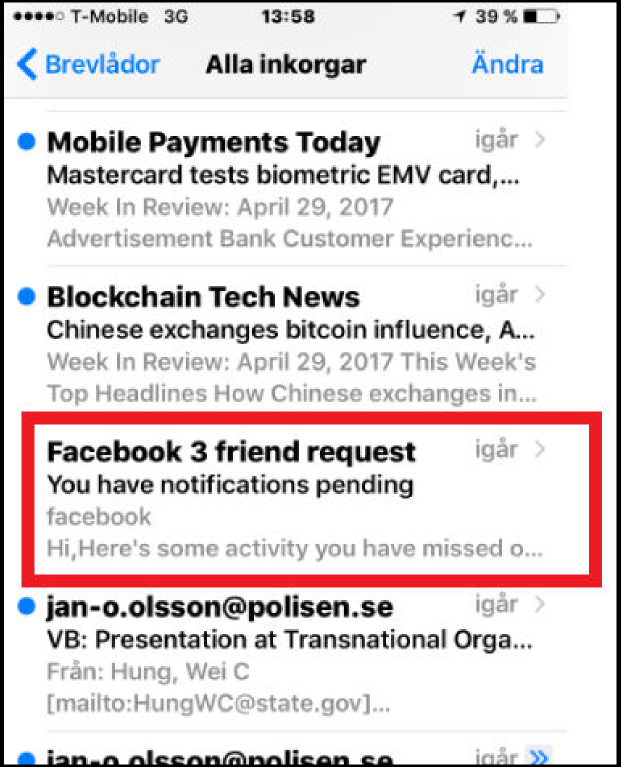
Med vänliga hälsningar,
CDON.COM.

Flow chart



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

Phishing, who is stupid enough….?



Mobile Payments Today igår
Mastercard tests biometric EMV card,...
Week In Review: April 29, 2017
Advertisement Bank Customer Experienc...

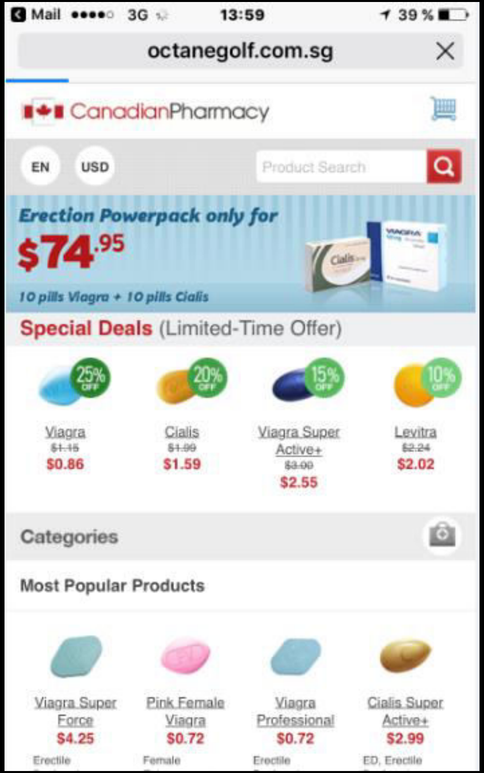
Blockchain Tech News igår
Chinese exchanges bitcoin influence, A...
Week In Review: April 29, 2017 This Week's
Top Headlines How Chinese exchanges in...

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 …..



octanegolf.com.sg

CanadianPharmacy

Erection Powerpack only for

$74.95

10 pills Viagra + 10 pills Cialis

Special Deals (Limited-Time Offer)

25% OFF	20% OFF	15% OFF	10% OFF
Viagra	Cialis	Viagra Super Active+	Levitra
~~$1.15~~	~~$1.99~~	~~$3.00~~	~~$2.24~~
$0.86	$1.59	$2.55	$2.02

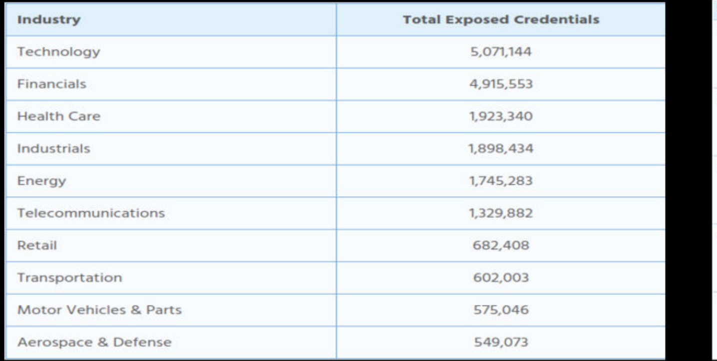
Categories

Most Popular Products

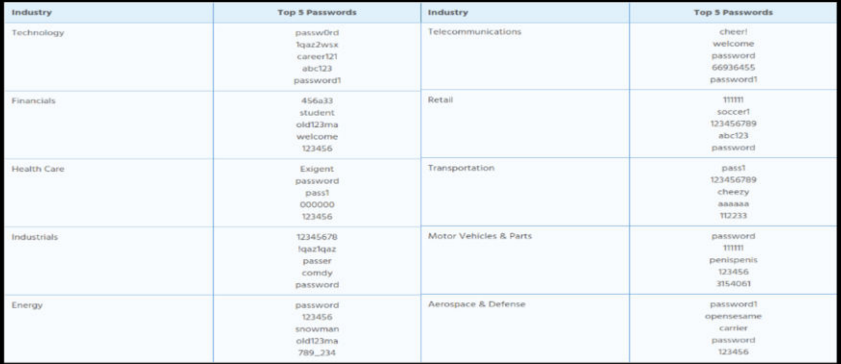
Viagra Super Force	Pink Female Viagra	Viagra Professional	Cialis Super Active+
$4.25	$0.72	$0.72	$2.99
Erectile	Female	Erectile	ED, Erectile

Password, the utlimate protection..

Do we use strong passwords ?

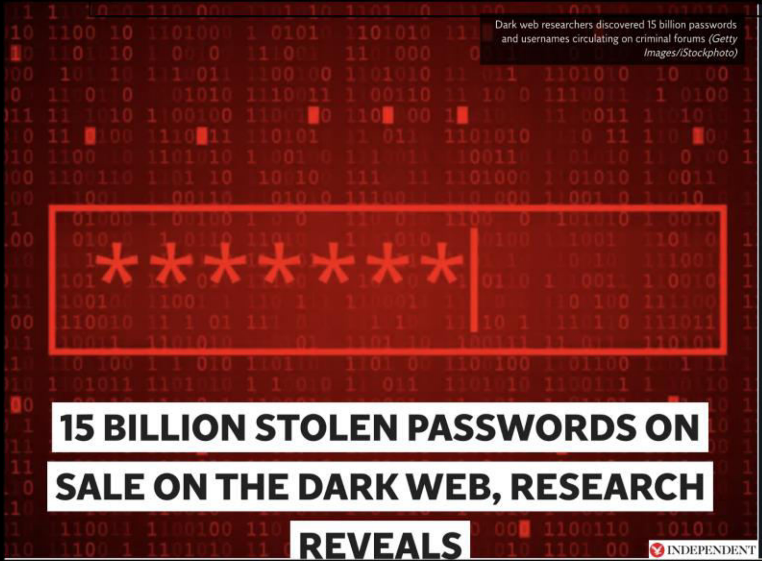


Industry	Total Exposed Credentials
Technology	5,071,144
Financials	4,915,553
Health Care	1,923,340
Industrials	1,898,434
Energy	1,745,283
Telecommunications	1,329,882
Retail	682,408
Transportation	602,003
Motor Vehicles & Parts	575,046
Aerospace & Defense	549,073



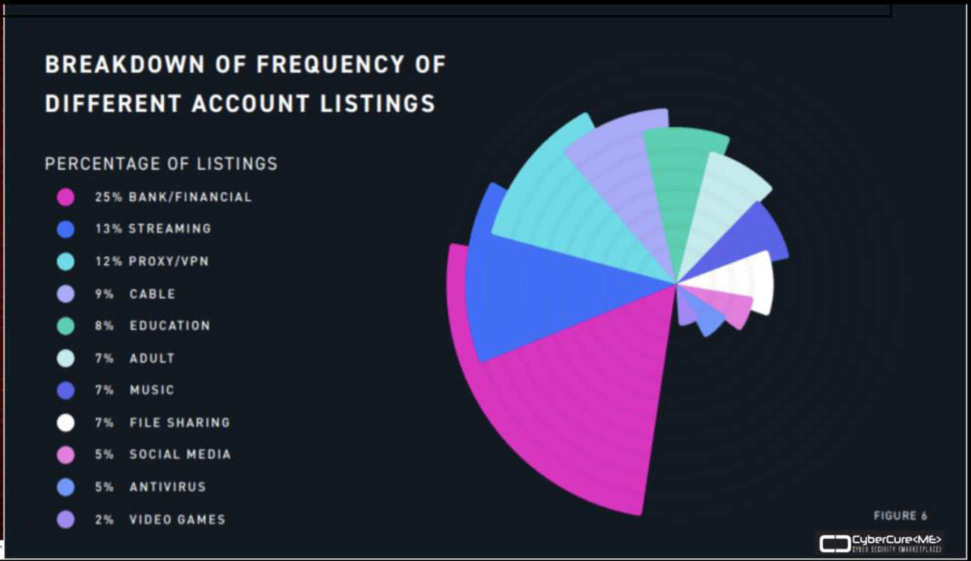
Industry	Top 5 Passwords	Industry	Top 5 Passwords
Technology	passw0rd 1qaz2wsx career121 abc123 password1	Telecommunications	cheer! welcome password 66936455 password1
Financials	456a33 student old123ma welcome 123456	Retail	111111 soccer1 123456789 abc123 password
Health Care	Exigent password pass1 000000 123456	Transportation	pass1 123456789 cheezy aaaaaa 112233
Industrials	12345678 !qaz1qaz passer comdy 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 ?



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

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



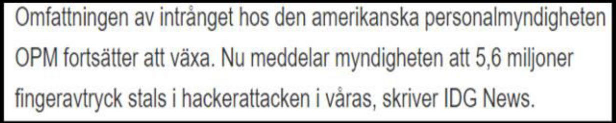
BREAKDOWN OF FREQUENCY OF DIFFERENT ACCOUNT LISTINGS

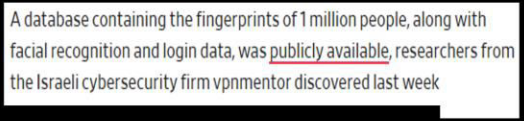
PERCENTAGE OF LISTINGS

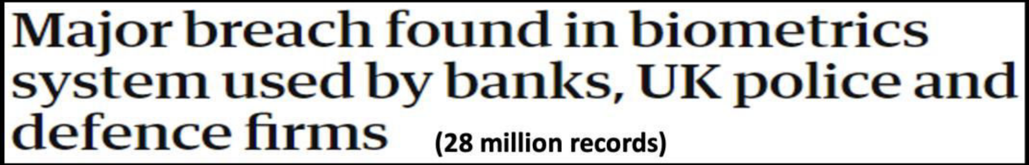
- ● 25% BANK/FINANCIAL
- ● 13% STREAMING
- ● 12% PROXY/VPN
- ● 9% CABLE
- ● 8% EDUCATION
- ● 7% ADULT
- ● 7% MUSIC
- ● 7% FILE SHARING
- ● 5% SOCIAL MEDIA
- ● 5% ANTIVIRUS
- ● 2% VIDEO GAMES

FIGURE 6

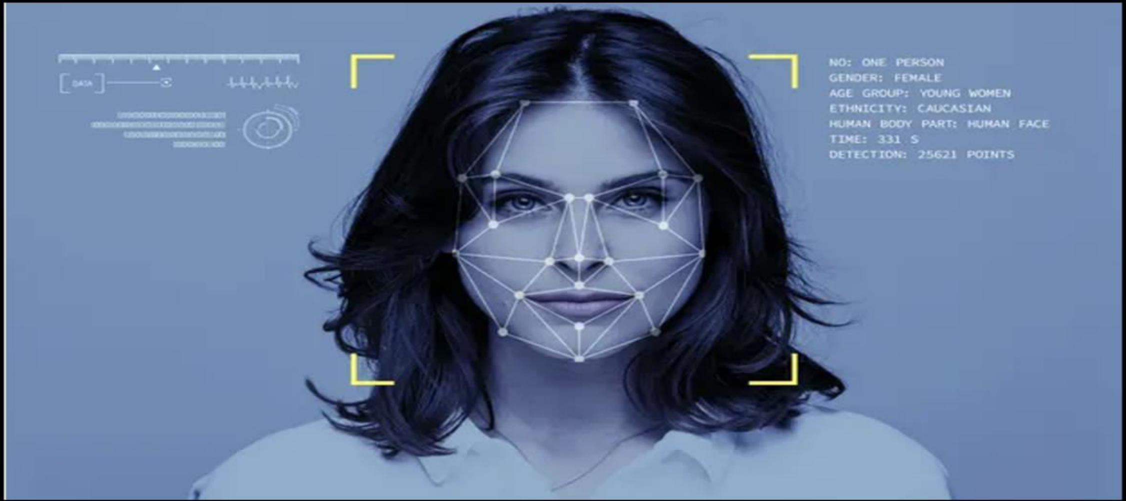
Ok, let´s go biotechnical..

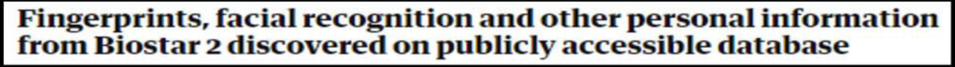

Omfattningen av intrånget hos den amerikanska personalmyndigheten OPM fortsätter att växa. Nu meddelar myndigheten att 5,6 miljoner fingeravtryck stals i hackerattacken i våras, skriver IDG News.


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)





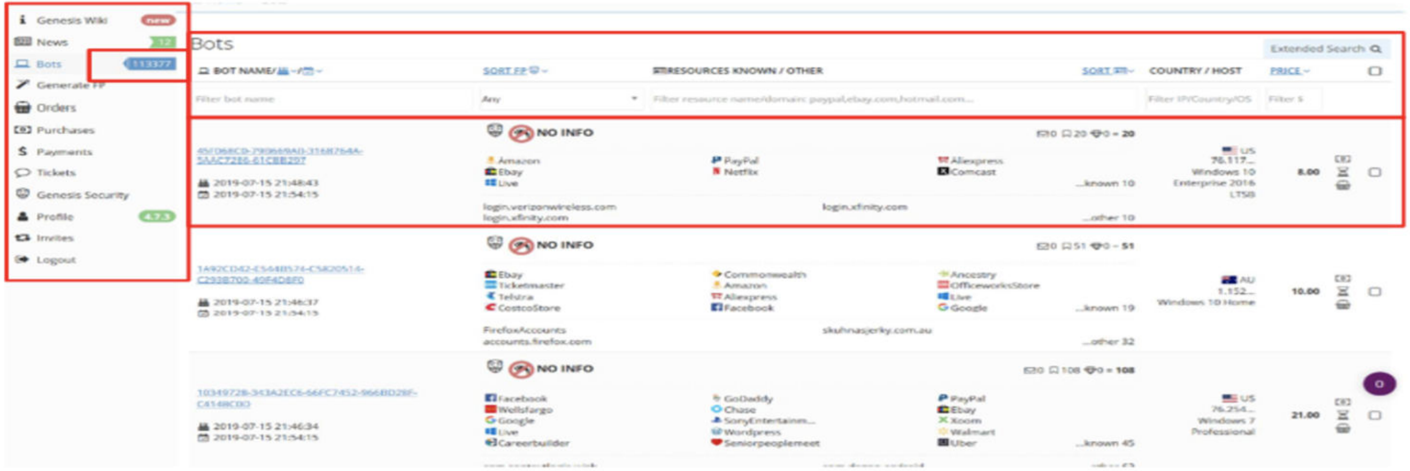
Fingerprints, facial recognition and other personal information from Biostar 2 discovered on publicly accessible database

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



Bots

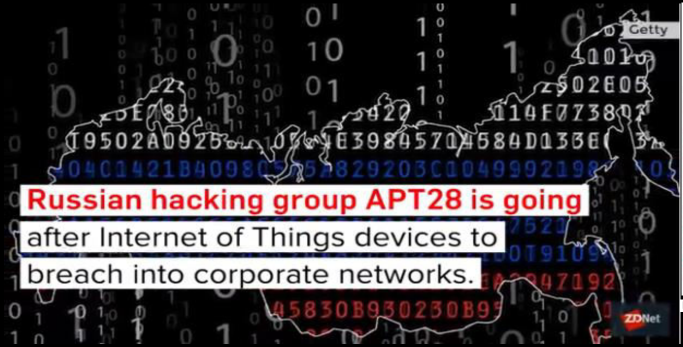
BOT NAME/	SORT FP	RESOURCES KNOWN / OTHER			SORT	COUNTRY / HOST	PRICE	□
Filter bot name	Any	Filter resource name/domain: paypal,ebay.com,hotmail.com...				Filter IP/Country/OS	Filter $	
45F068CD-79066 9A0-3168764A-5AAC7286-61CBB297 2019-07-15 21:48:43 2019-07-15 21:54:15	NO INFO	Amazon Ebay Live login.verizonwireless.com login.xfinity.com	PayPal Netflix login.xfinity.com	Aliexpress Comcast	0 20 0 = 20 ...known 10 ...other 10	US 76.117... Windows 10 Enterprise 2016 LTSB	8.00	□
1A92CD42-E5448574-C5820514-C293B700-40F4D8F0 2019-07-15 21:46:37 2019-07-15 21:54:15	NO INFO	Ebay Ticketmaster Telstra CostcoStore FirefoxAccounts accounts.firefox.com	Commonwealth Amazon Aliexpress Facebook skuhnasjerky.com.au	Ancestry OfficeworksStore Live Google	0 51 0 = 51 ...known 19 ...other 32	AU 1.152... Windows 10 Home	10.00	□
10349728-343A2EC6-66FC7452-966BD28F-C4148C00 2019-07-15 21:46:34 2019-07-15 21:54:15	NO INFO	Facebook Wellsfargo Google Live Careerbuilder	GoDaddy Chase SonyEntertainm... Wordpress Seniorpeoplemeet	PayPal Ebay Xoom Walmart Uber	0 108 0 = 108 ...known 45	US 76.254... Windows 7 Professional	21.00	□

IoT

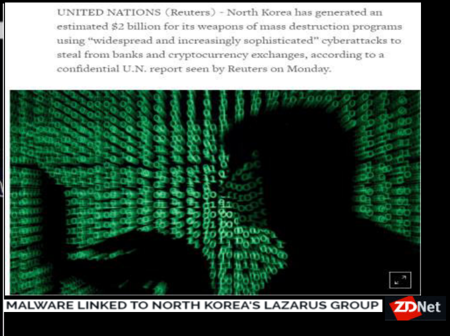
The first digital murder?

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

The future is already here!

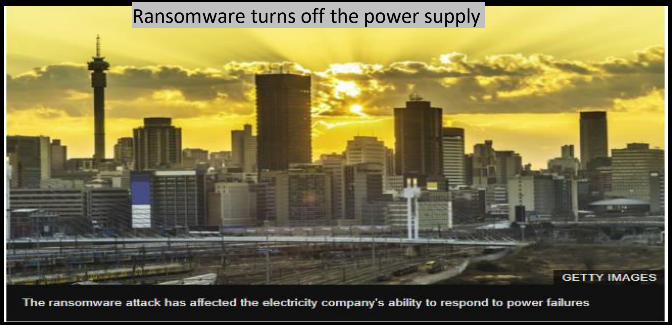


Russian hacking group APT28 is going after Internet of Things devices to breach into corporate networks.



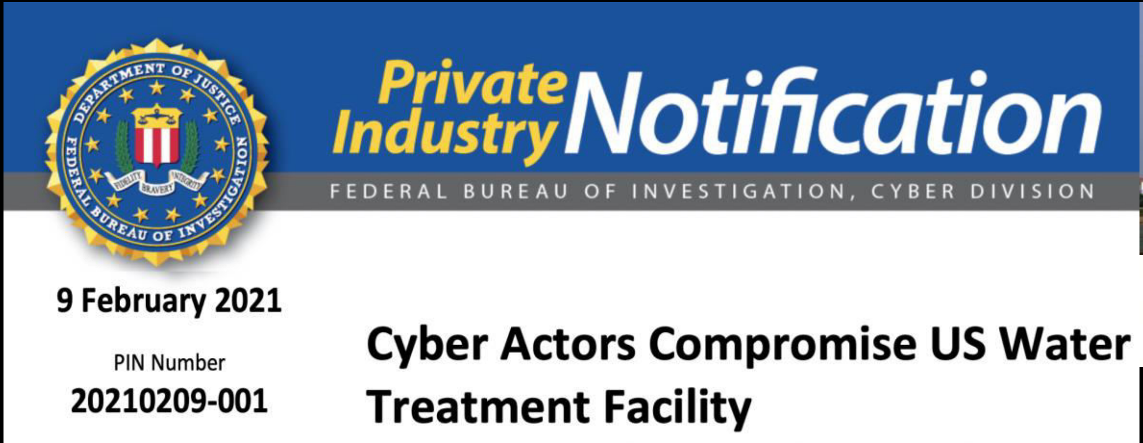
UNITED NATIONS (Reuters) - North Korea has generated an estimated $2 billion for its weapons of mass destruction programs using "widespread and increasingly sophisticated" cyberattacks to steal from banks and cryptocurrency exchanges, according to a confidential U.N. report seen by Reuters on Monday.

MALWARE LINKED TO NORTH KOREA'S LAZARUS GROUP



Ransomware turns off the power supply

The ransomware attack has affected the electricity company's ability to respond to power failures



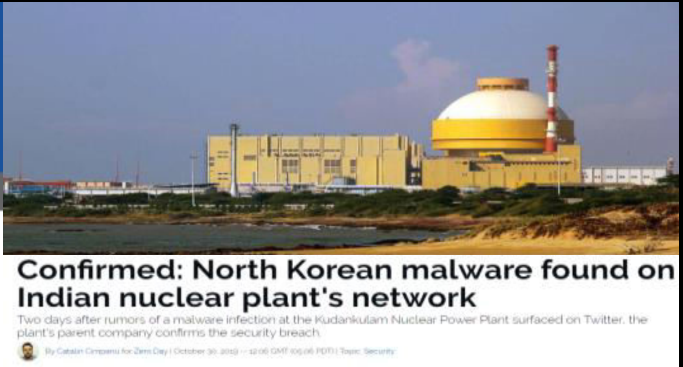
Private Industry Notification

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 Catalin Cimpanu for Zero Day | October 30, 2019 -- 12:06 GMT (05:06 PDT) | Topic: Security

The way forward - and it has started…

- The most important thing: prevention and then prevention...
- Incident planning

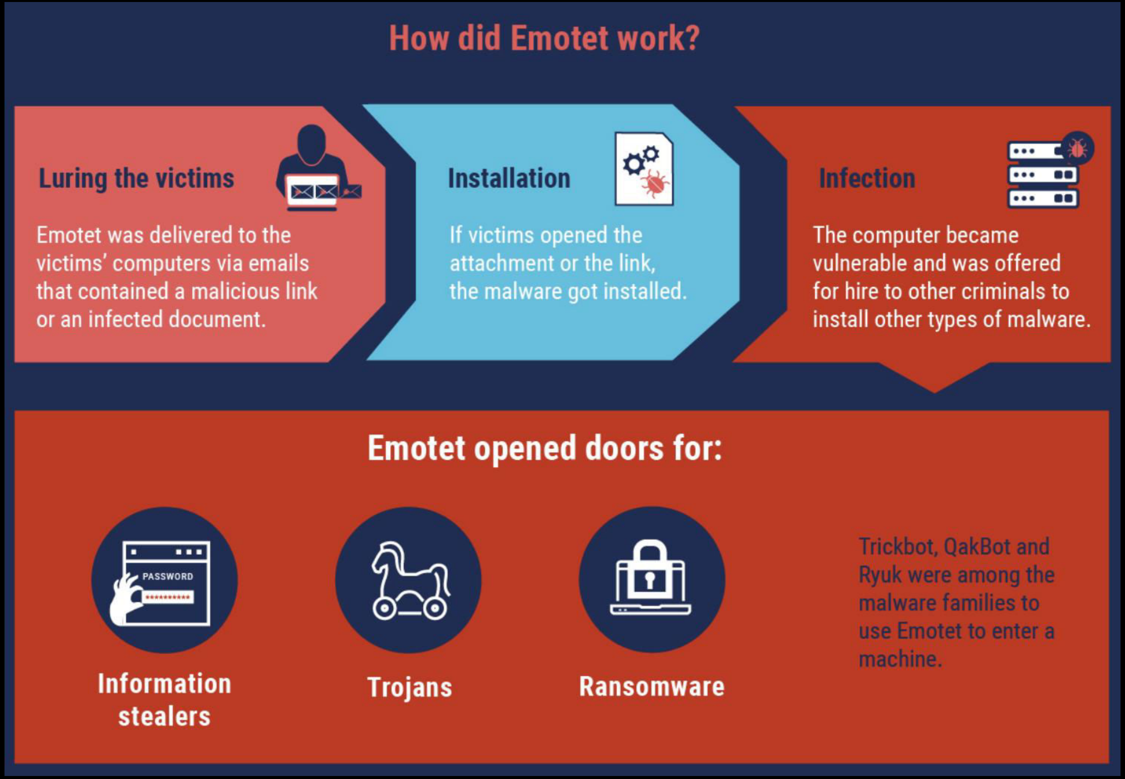
But except from that:

- Report to the Police

- Increase and accelerate national and global cooperations between authorities

- Build Private-Public-Partnership (P3) organisations
  - Ransomware Task Force (US)
  - NoMoreRansom.org
  - ECCFI
  - NCFTA
  - NN-organizations

JIT – Joint Investiogation Teams



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.

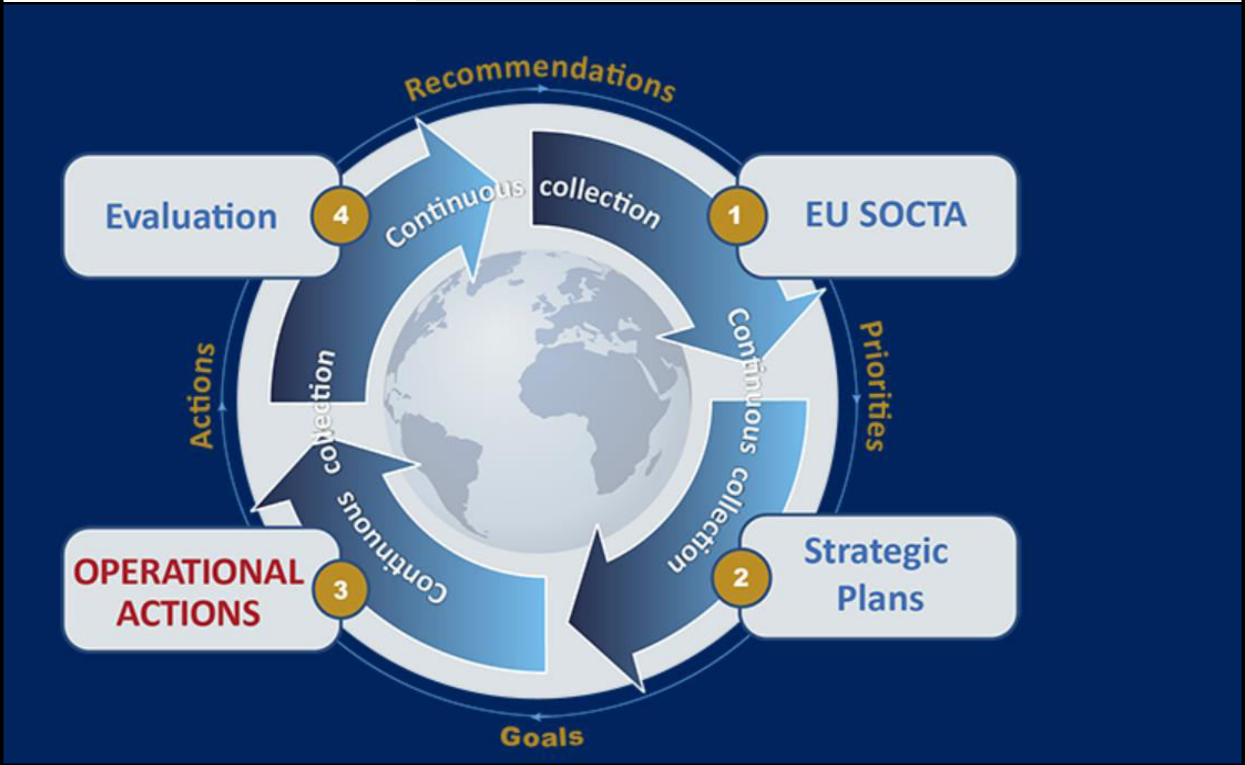
Emotet opened doors for:

- Information stealers
- Trojans
- Ransomware

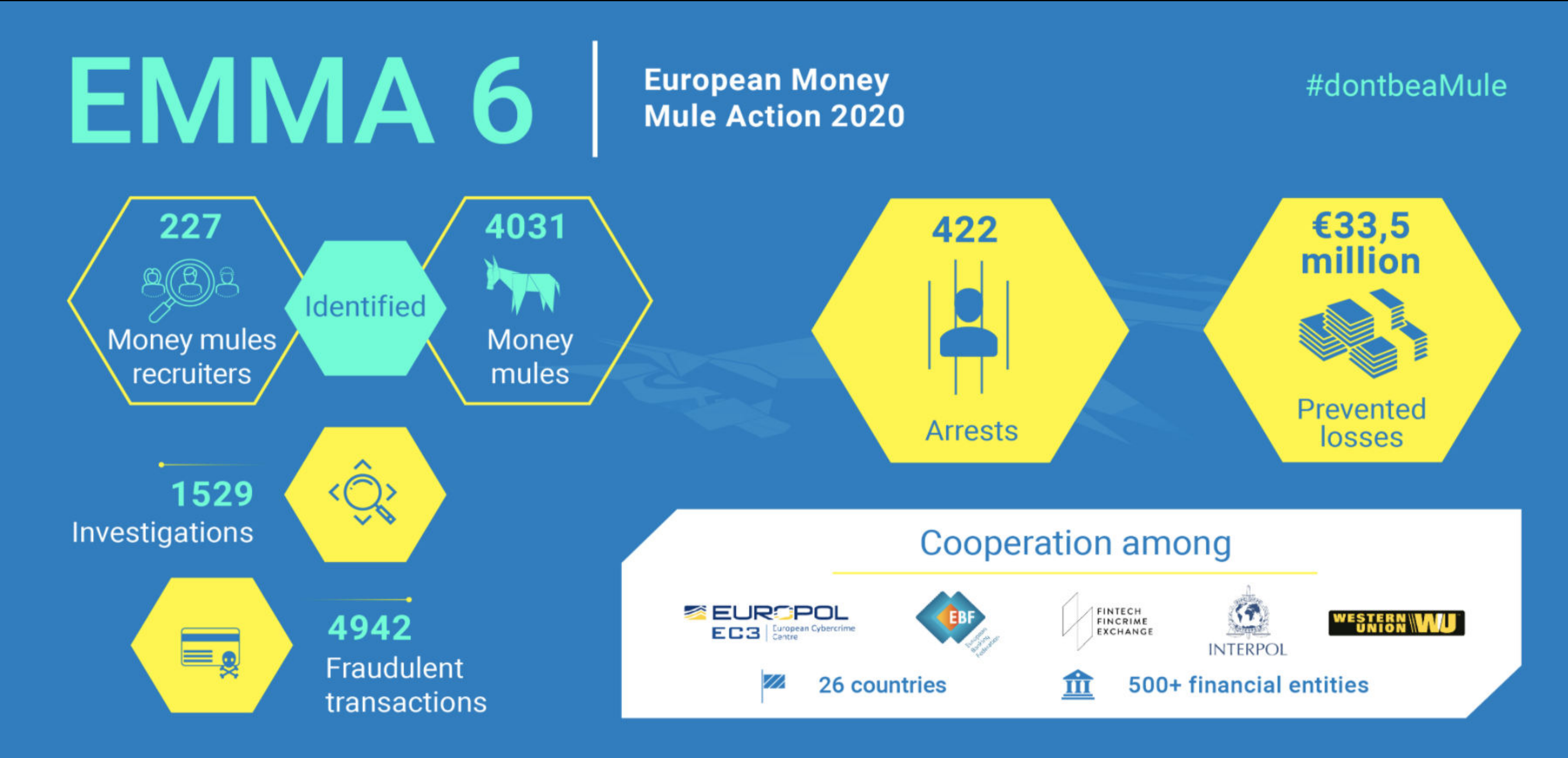
Trickbot, QakBot and Ryuk were among the malware families to use Emotet to enter a machine.

EMPACT

EUROPOL Europeiska unionens byrå för samarbete om brottsbekämpning - **Att göra Europa säkrare**



422 ARRESTED AND 4 031 MONEY MULES IDENTIFIED IN GLOBAL CRACKDOWN ON MONEY LAUNDERING



EMMA 6

European Money Mule Action 2020

#dontbeaMule

Identified

227 Money mules recruiters

4031 Money mules

422 Arrests

€33,5 million Prevented losses

1529 Investigations

4942 Fraudulent transactions

Cooperation among

EUROPOL
EC3 European Cybercrime Centre
EBF European Banking Federation
FINTECH FINCRIME EXCHANGE
INTERPOL
WESTERN UNION WU

26 countries

500+ financial entities

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

NN – When LEA gets the information..

Genrebild. **Foto: Gustav Sjöholm/TT**

Omfattande it-attack mot flera svenska storföretag

More ?

Jan Olsson

+46 (0)70-736 49 32