CORA
CONNECTING
REMOTE
AREAS

Interreg
North Sea Region
CORA
European Regional Development Fund

EUROPEAN UNION

Understanding Cyber Risk

Jens Myrup Pedersen, Professor, Aalborg Universitet

CORA Workshop 2022

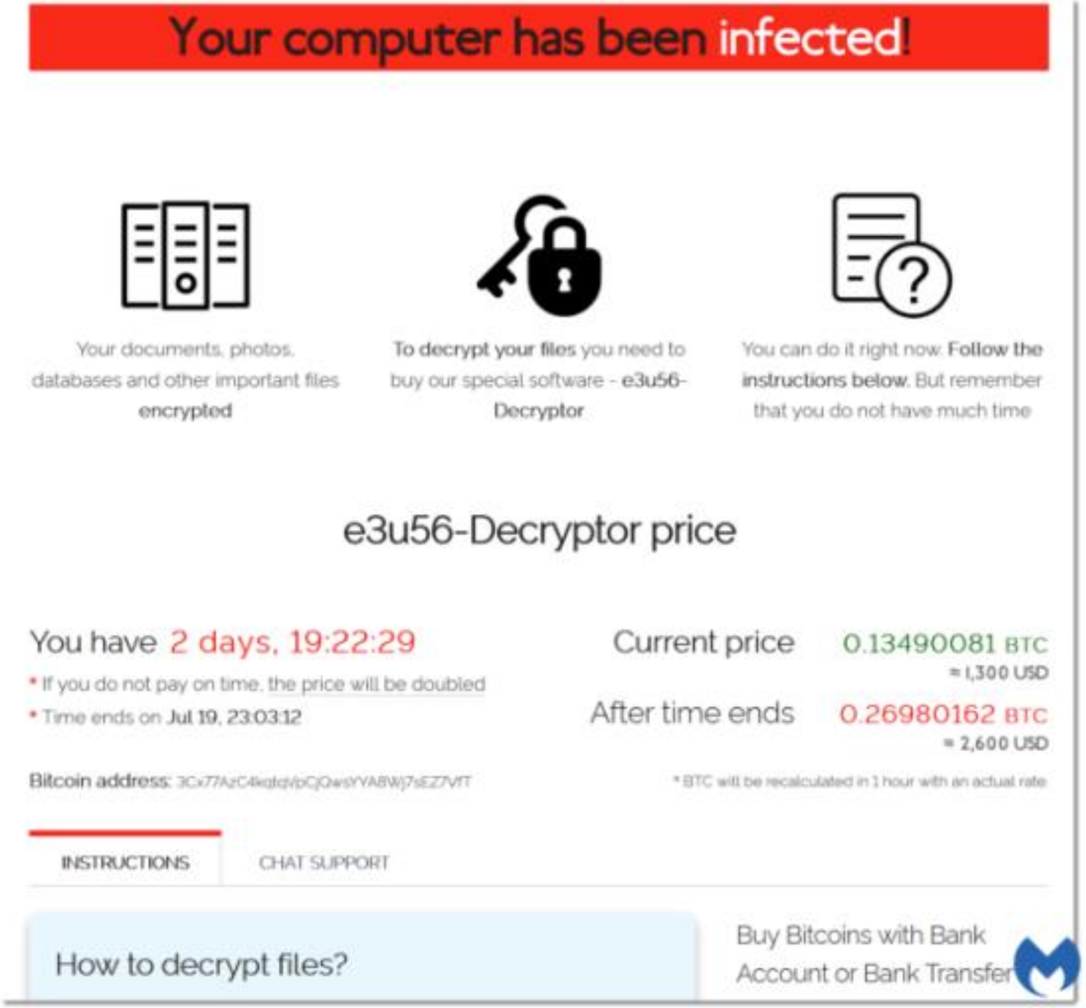
AALBORG UNIVERSITY
DENMARK

Cyber security is all about risks

The cyber threat is for real

7-Eleven Denmark confirms ransomware attack behind store closures

By **Lawrence Abrams** August 10, 2022 06:21 PM 1



Your computer has been infected!

Your documents, photos, databases and other important files **encrypted**

To decrypt your files you need to buy our special software - **e3u56-Decryptor**

You can do it right now. **Follow the instructions below.** But remember that you do not have much time

e3u56-Decryptor price

You have 2 days, 19:22:29

* If you do not pay on time, the price will be doubled
* Time ends on **Jul 19, 23:03:12**

Current price 0.13490081 BTC ≈ 1,300 USD

After time ends 0.26980162 BTC ≈ 2,600 USD

Bitcoin address: 3Cx77AzC4kqtqVpCjQwsYYA8Wj7sEZ7VfT

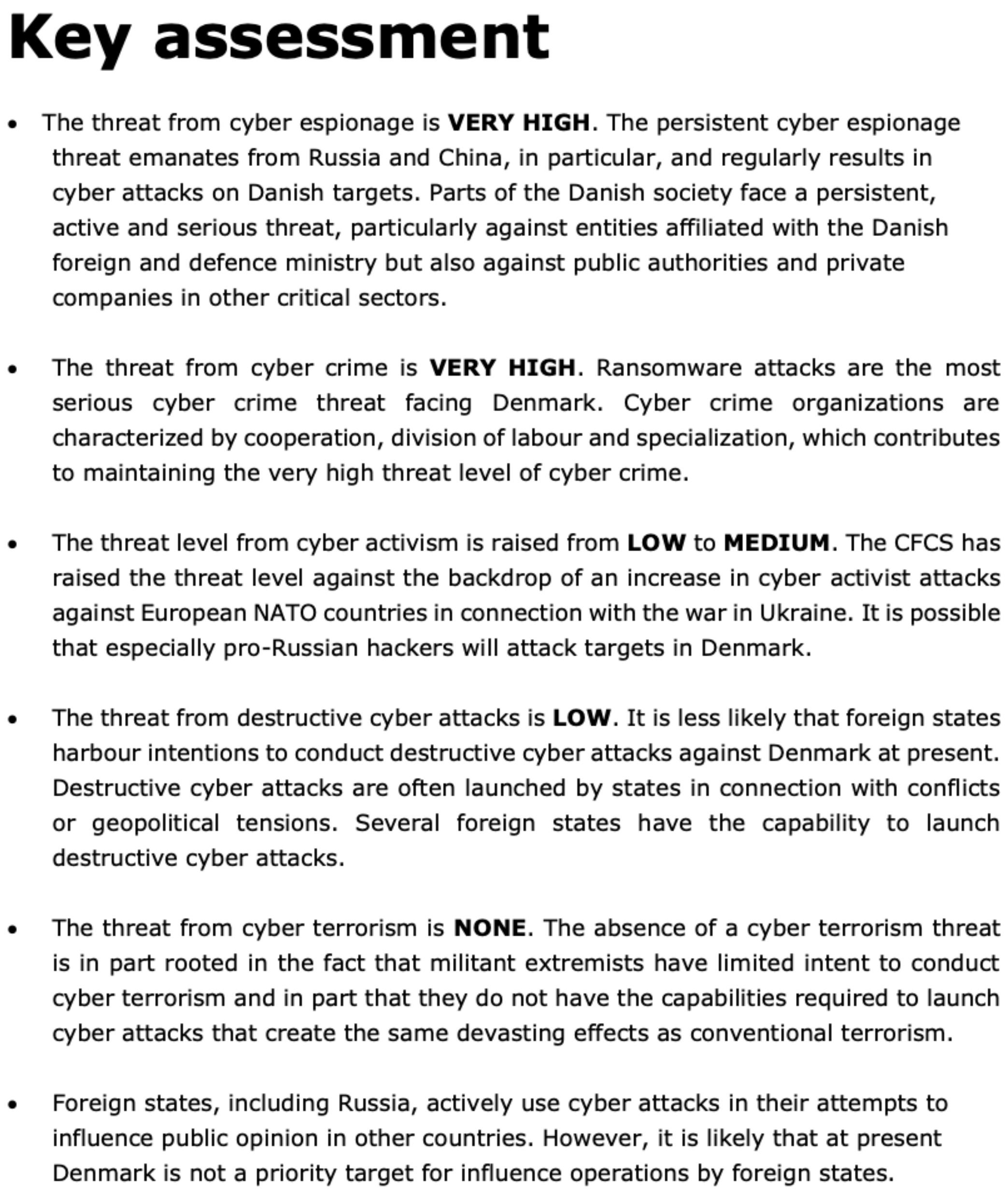
* BTC will be recalculated in 1 hour with an actual rate

How to decrypt files?

Buy Bitcoins with Bank Account or Bank Transfer

Threat is more than a number (CFCS Assessment 2022)

- The threat from cyber espionage is VERY HIGH.
- The Threat from cyber crime is VERY HIGH.
- The threat from cyber activities is MEDIUM (up from low due to the war in Ukraine).
- The treat from destructive cyber attacks is LOW.
- The threat from cyber terror is NONE.



Key assessment

- The threat from cyber espionage is **VERY HIGH**. The persistent cyber espionage threat emanates from Russia and China, in particular, and regularly results in cyber attacks on Danish targets. Parts of the Danish society face a persistent, active and serious threat, particularly against entities affiliated with the Danish foreign and defence ministry but also against public authorities and private companies in other critical sectors.

- The threat from cyber crime is **VERY HIGH**. Ransomware attacks are the most serious cyber crime threat facing Denmark. Cyber crime organizations are characterized by cooperation, division of labour and specialization, which contributes to maintaining the very high threat level of cyber crime.

- The threat level from cyber activism is raised from **LOW** to **MEDIUM**. The CFCS has raised the threat level against the backdrop of an increase in cyber activist attacks against European NATO countries in connection with the war in Ukraine. It is possible that especially pro-Russian hackers will attack targets in Denmark.

- The threat from destructive cyber attacks is **LOW**. It is less likely that foreign states harbour intentions to conduct destructive cyber attacks against Denmark at present. Destructive cyber attacks are often launched by states in connection with conflicts or geopolitical tensions. Several foreign states have the capability to launch destructive cyber attacks.

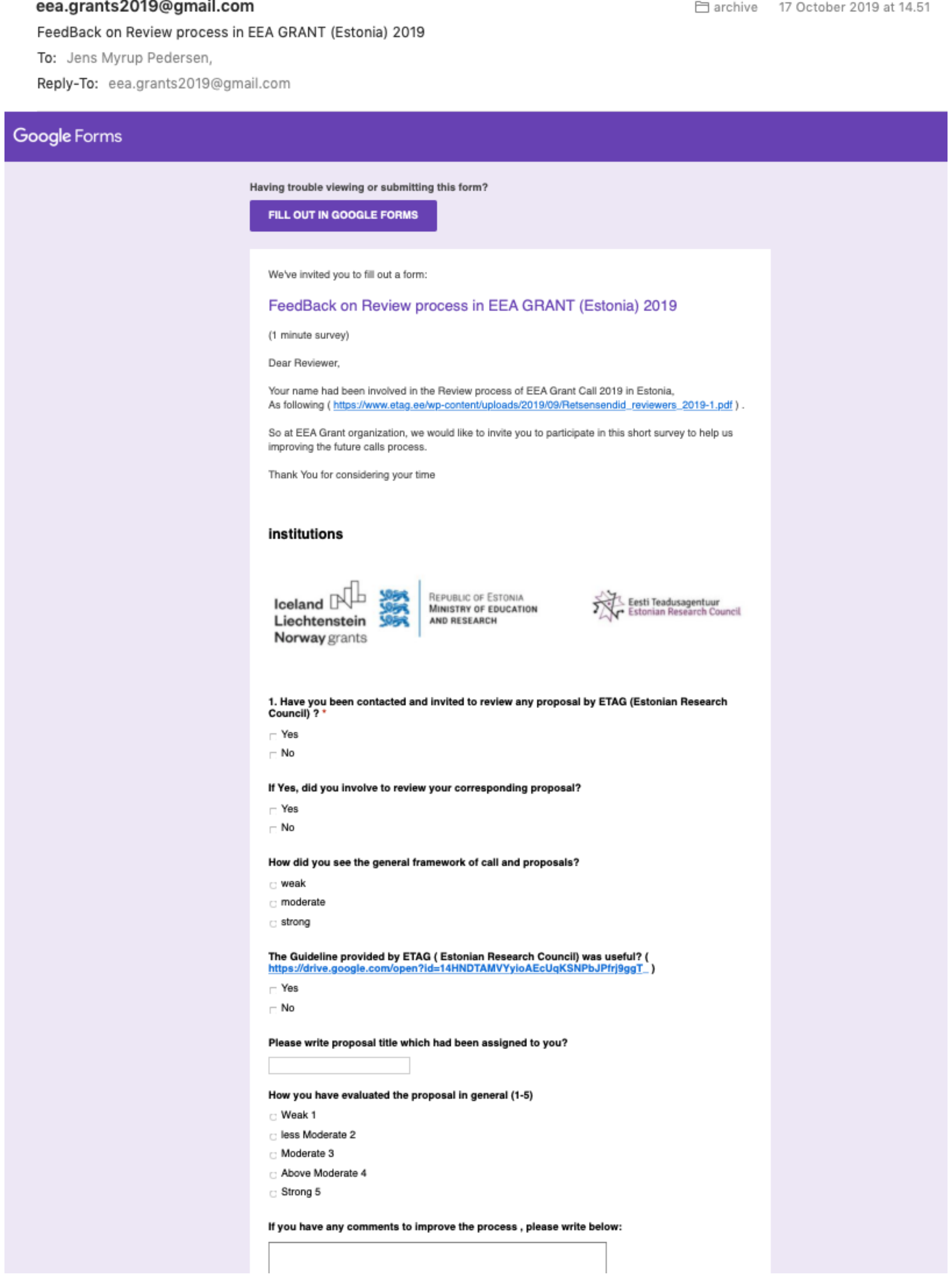
- The threat from cyber terrorism is **NONE**. The absence of a cyber terrorism threat is in part rooted in the fact that militant extremists have limited intent to conduct cyber terrorism and in part that they do not have the capabilities required to launch cyber attacks that create the same devasting effects as conventional terrorism.

- Foreign states, including Russia, actively use cyber attacks in their attempts to influence public opinion in other countries. However, it is likely that at present Denmark is not a priority target for influence operations by foreign states.

Important to understand

- Different groups
  - Motivations
  - Resources
  - Capabilities

- And to differentiate between
  - Cyber criminals (profit)
  - Nation Stateus (strategy)
  - Insiders
  - Greyhats, hacktivists, script kiddies...



eea.grants2019@gmail.com

FeedBack on Review process in EEA GRANT (Estonia) 2019

To: Jens Myrup Pedersen,

Reply-To: eea.grants2019@gmail.com

Having trouble viewing or submitting this form?

We've invited you to fill out a form:

FeedBack on Review process in EEA GRANT (Estonia) 2019

(1 minute survey)

Dear Reviewer,

Your name had been involved in the Review process of EEA Grant Call 2019 in Estonia,
As following (https://www.etag.ee/wp-content/uploads/2019/09/Retsensendid_reviewers_2019-1.pdf) .

So at EEA Grant organization, we would like to invite you to participate in this short survey to help us improving the future calls process.

Thank You for considering your time

institutions

1. Have you been contacted and invited to review any proposal by ETAG (Estonian Research Council) ? *

□ Yes
□ No

If Yes, did you involve to review your corresponding proposal?

□ Yes
□ No

How did you see the general framework of call and proposals?

○ weak
○ moderate
○ strong

The Guideline provided by ETAG (Estonian Research Council) was useful? (https://drive.google.com/open?id=14HNDTAMVYyioAEcUqKSNPbJPfrj9ggT_)

□ Yes
□ No

Please write proposal title which had been assigned to you?

How you have evaluated the proposal in general (1-5)

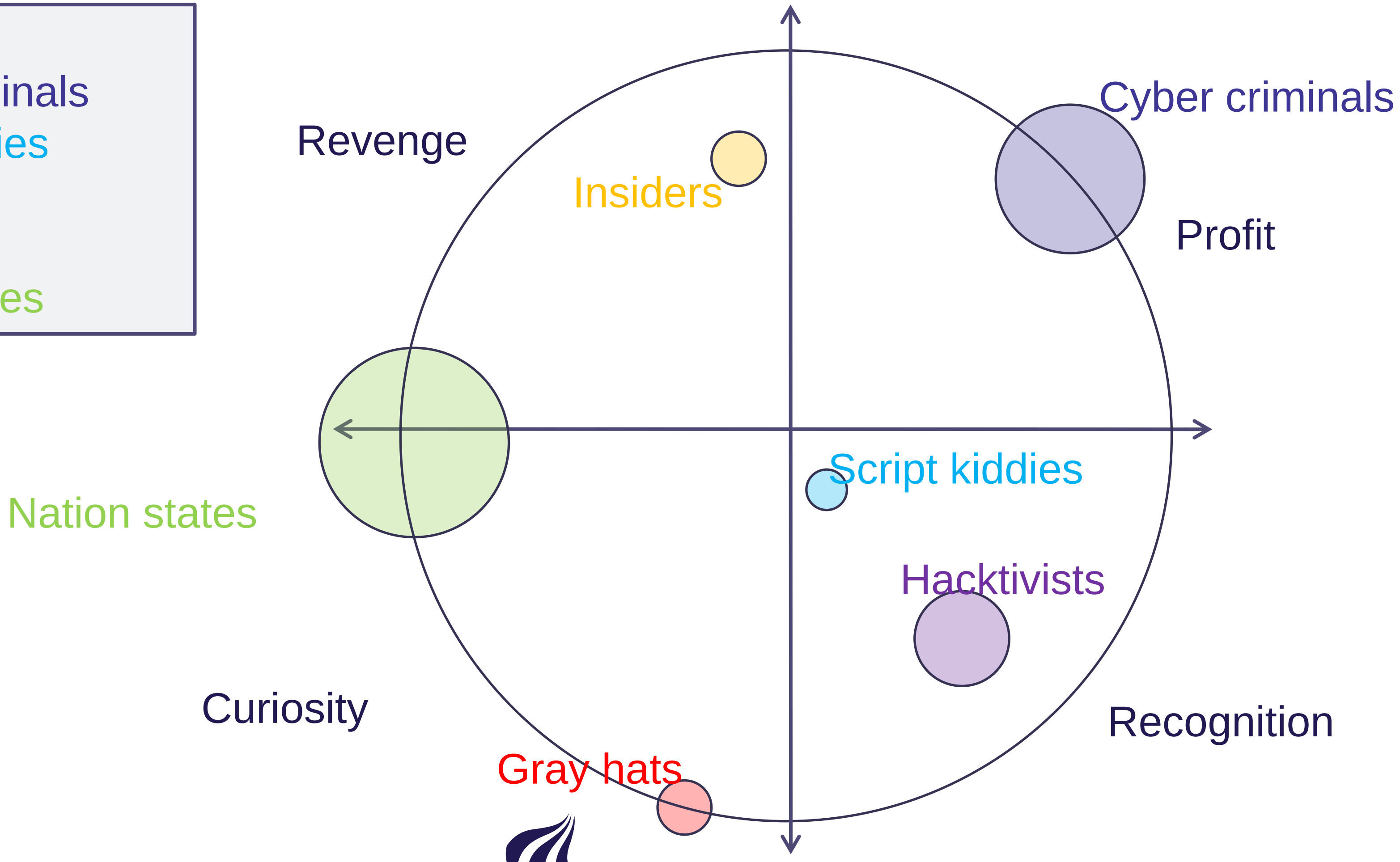
○ Weak 1
○ less Moderate 2
○ Moderate 3
○ Above Moderate 4
○ Strong 5

If you have any comments to improve the process , please write below:

AALBORG UNIVERSITET

Overview: Circumplex taxonomy

Insiders
Cyber criminals
Script kiddies
Gray hats
Hacktivists
Nation states



AALBORG UNIVERSITY
DENMARK

Cyber criminals – for €€€

University of Utah Pays $457K After Ransomware Attack

KRIMI

Tidligere terrordømte hackede sig til millioner på biblioteker

1. feb. 2019, 11:50
Opd. 1. feb. 2019, 13:05

Herlev Bibliotek, Skanderborg Bibliotek og Middelfart Bibliotek var blandt de biblioteker, hvis computere blev hacket af brødrene. Foto: Morten Germund / Scanpix Denmark

MEST SETE PÅ TV2.DK

UDLAND
Kinesisk virus har bredt sig til Europa

EM HÅNDBOLD
Dybt skuffet Sagosen: - Vi havde en drøm og et mål

DAGENS OVERBLIK
Dagens overblik: De største stjerner hylder Wozniacki

EM HÅNDBOLD
Nu starter udskudt semifinale i kølvandet på

Cybersecurity

Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom

By William Turton, Michael Riley, and Jennifer Jacobs

13 May 2021, 16:15 CEST

Updated on 14 May 2021, 01:01 CEST

- Payment came shortly after attack got underway last week
- FBI discourages organizations from paying ransom to hackers

Damn fine TV
Twin Peaks returns
Exclusive Kyle MacLachlan interview
The original cast: what happened next

Delicious spring veg recipes
cook and weekend

How to be a dad by Tim Dowling (and sons)
weekend

Write that novel! The 13 steps to success
review

£1.60 for subscribers page 24 →

theguardian

NHS targeted in global cyber-attack

- Hack appears to exploit US spy agency leak
- Major incident declared as 16 NHS trusts hit
- Similar strikes reported across Europe and Asia

[illegible]

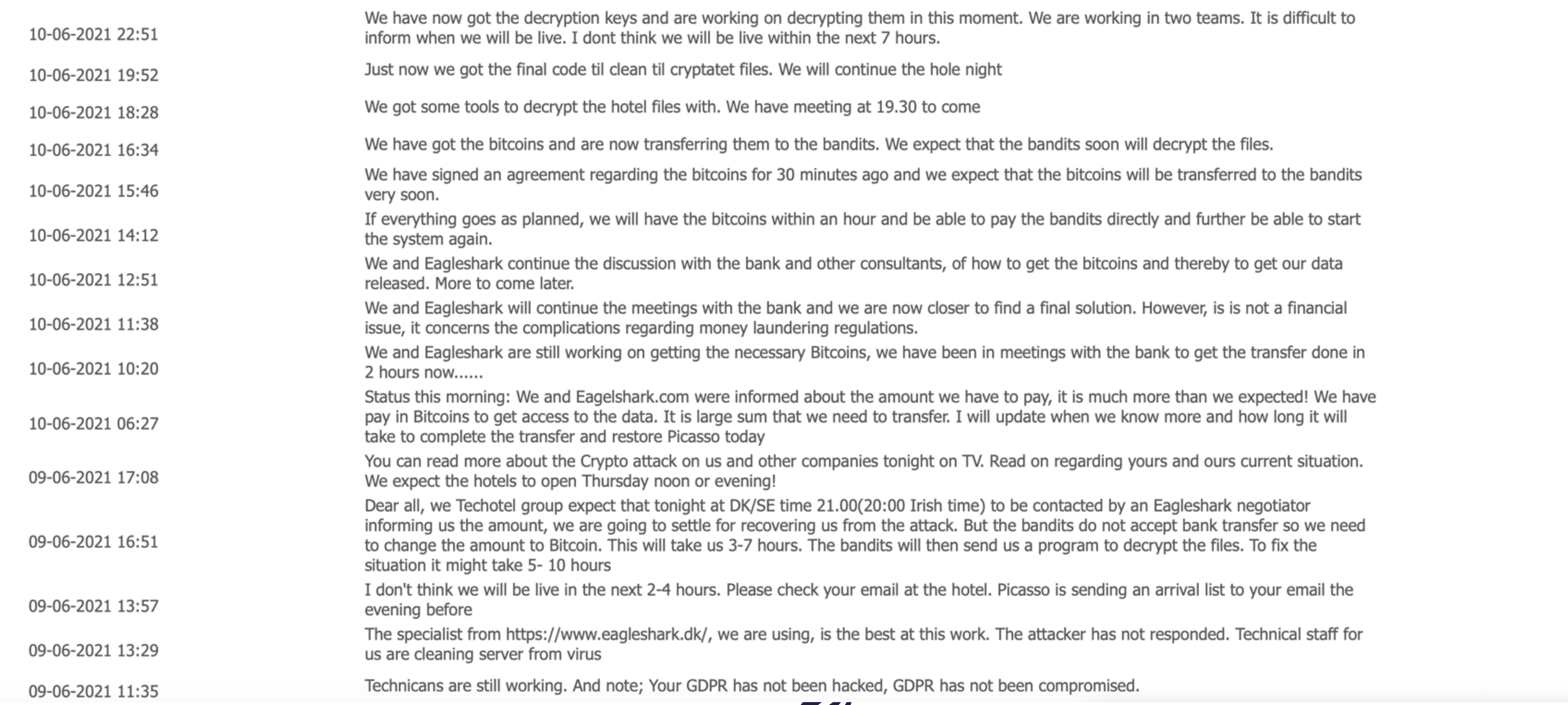
He's looking for the C-word ... it's on the door

Don't turn May into Thatcher, warns Tom Watson

[illegible]

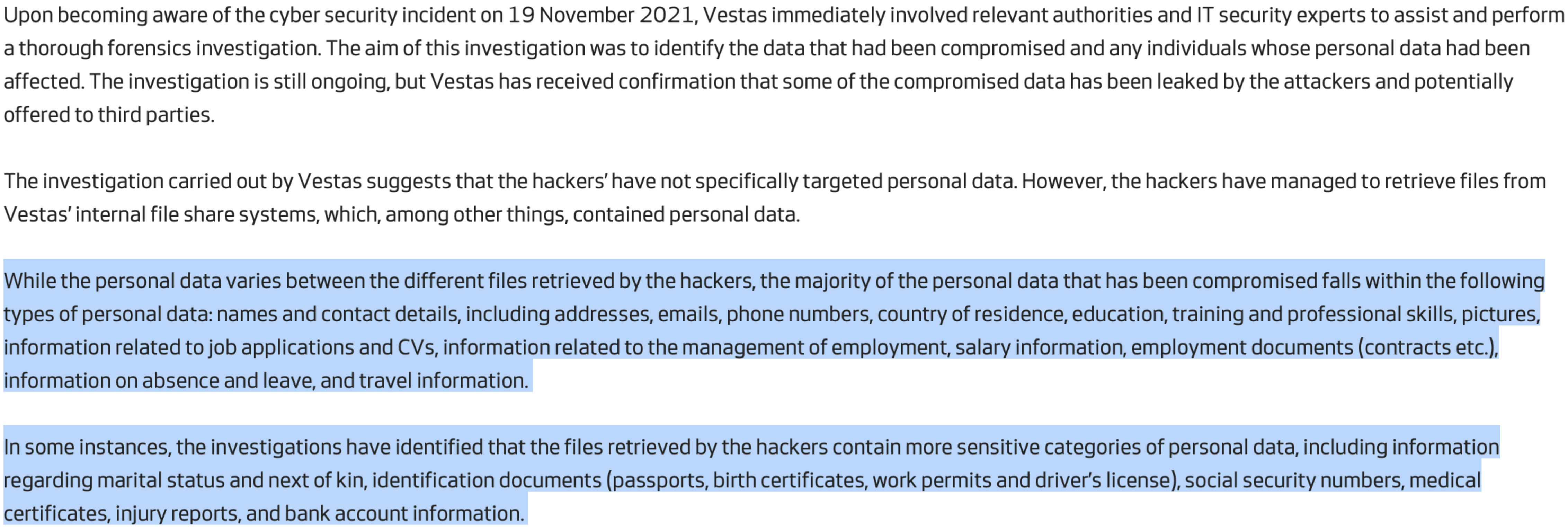
First it was a lettuce shortage, then a courgette crisis. Now there is trouble looming in the avocado aisle...

A Danish company in 2021 – AK Techotel



10-06-2021 22:51	We have now got the decryption keys and are working on decrypting them in this moment. We are working in two teams. It is difficult to inform when we will be live. I dont think we will be live within the next 7 hours.
10-06-2021 19:52	Just now we got the final code til clean til cryptatet files. We will continue the hole night
10-06-2021 18:28	We got some tools to decrypt the hotel files with. We have meeting at 19.30 to come
10-06-2021 16:34	We have got the bitcoins and are now transferring them to the bandits. We expect that the bandits soon will decrypt the files.
10-06-2021 15:46	We have signed an agreement regarding the bitcoins for 30 minutes ago and we expect that the bitcoins will be transferred to the bandits very soon.
10-06-2021 14:12	If everything goes as planned, we will have the bitcoins within an hour and be able to pay the bandits directly and further be able to start the system again.
10-06-2021 12:51	We and Eagleshark continue the discussion with the bank and other consultants, of how to get the bitcoins and thereby to get our data released. More to come later.
10-06-2021 11:38	We and Eagleshark will continue the meetings with the bank and we are now closer to find a final solution. However, is is not a financial issue, it concerns the complications regarding money laundering regulations.
10-06-2021 10:20	We and Eagleshark are still working on getting the necessary Bitcoins, we have been in meetings with the bank to get the transfer done in 2 hours now......
10-06-2021 06:27	Status this morning: We and Eagelshark.com were informed about the amount we have to pay, it is much more than we expected! We have pay in Bitcoins to get access to the data. It is large sum that we need to transfer. I will update when we know more and how long it will take to complete the transfer and restore Picasso today
09-06-2021 17:08	You can read more about the Crypto attack on us and other companies tonight on TV. Read on regarding yours and ours current situation. We expect the hotels to open Thursday noon or evening!
09-06-2021 16:51	Dear all, we Techotel group expect that tonight at DK/SE time 21.00(20:00 Irish time) to be contacted by an Eagleshark negotiator informing us the amount, we are going to settle for recovering us from the attack. But the bandits do not accept bank transfer so we need to change the amount to Bitcoin. This will take us 3-7 hours. The bandits will then send us a program to decrypt the files. To fix the situation it might take 5- 10 hours
09-06-2021 13:57	I don't think we will be live in the next 2-4 hours. Please check your email at the hotel. Picasso is sending an arrival list to your email the evening before
09-06-2021 13:29	The specialist from https://www.eagleshark.dk/, we are using, is the best at this work. The attacker has not responded. Technical staff for us are cleaning server from virus
09-06-2021 11:35	Technicans are still working. And note; Your GDPR has not been hacked, GDPR has not been compromised.

Vestas also hit in 2021 – data leaked



Upon becoming aware of the cyber security incident on 19 November 2021, Vestas immediately involved relevant authorities and IT security experts to assist and perform a thorough forensics investigation. The aim of this investigation was to identify the data that had been compromised and any individuals whose personal data had been affected. The investigation is still ongoing, but Vestas has received confirmation that some of the compromised data has been leaked by the attackers and potentially offered to third parties.

The investigation carried out by Vestas suggests that the hackers' have not specifically targeted personal data. However, the hackers have managed to retrieve files from Vestas' internal file share systems, which, among other things, contained personal data.

While the personal data varies between the different files retrieved by the hackers, the majority of the personal data that has been compromised falls within the following types of personal data: names and contact details, including addresses, emails, phone numbers, country of residence, education, training and professional skills, pictures, information related to job applications and CVs, information related to the management of employment, salary information, employment documents (contracts etc.), information on absence and leave, and travel information.

In some instances, the investigations have identified that the files retrieved by the hackers contain more sensitive categories of personal data, including information regarding marital status and next of kin, identification documents (passports, birth certificates, work permits and driver's license), social security numbers, medical certificates, injury reports, and bank account information.

Conti Leaks (and a bit on Ukraine)

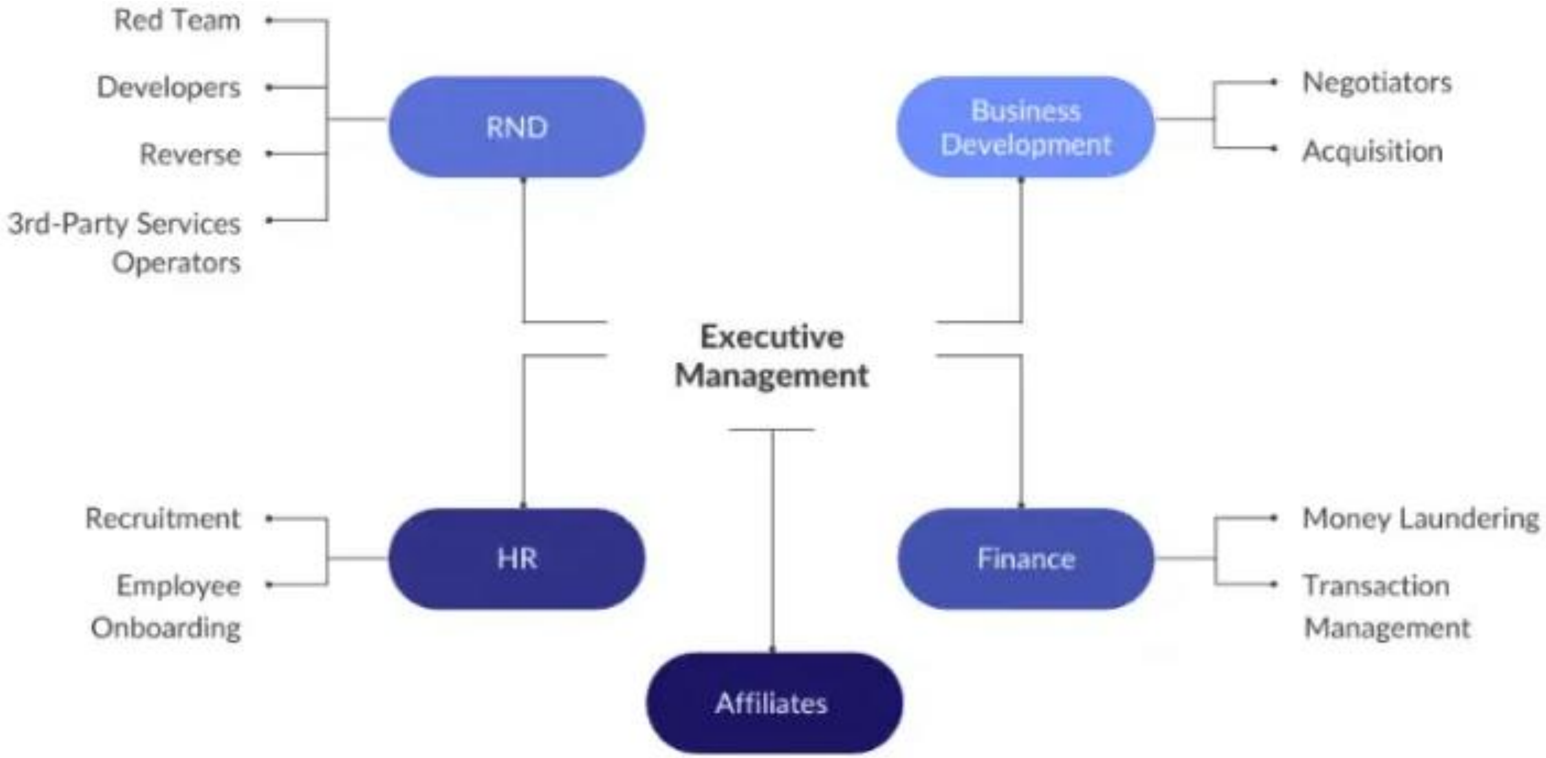
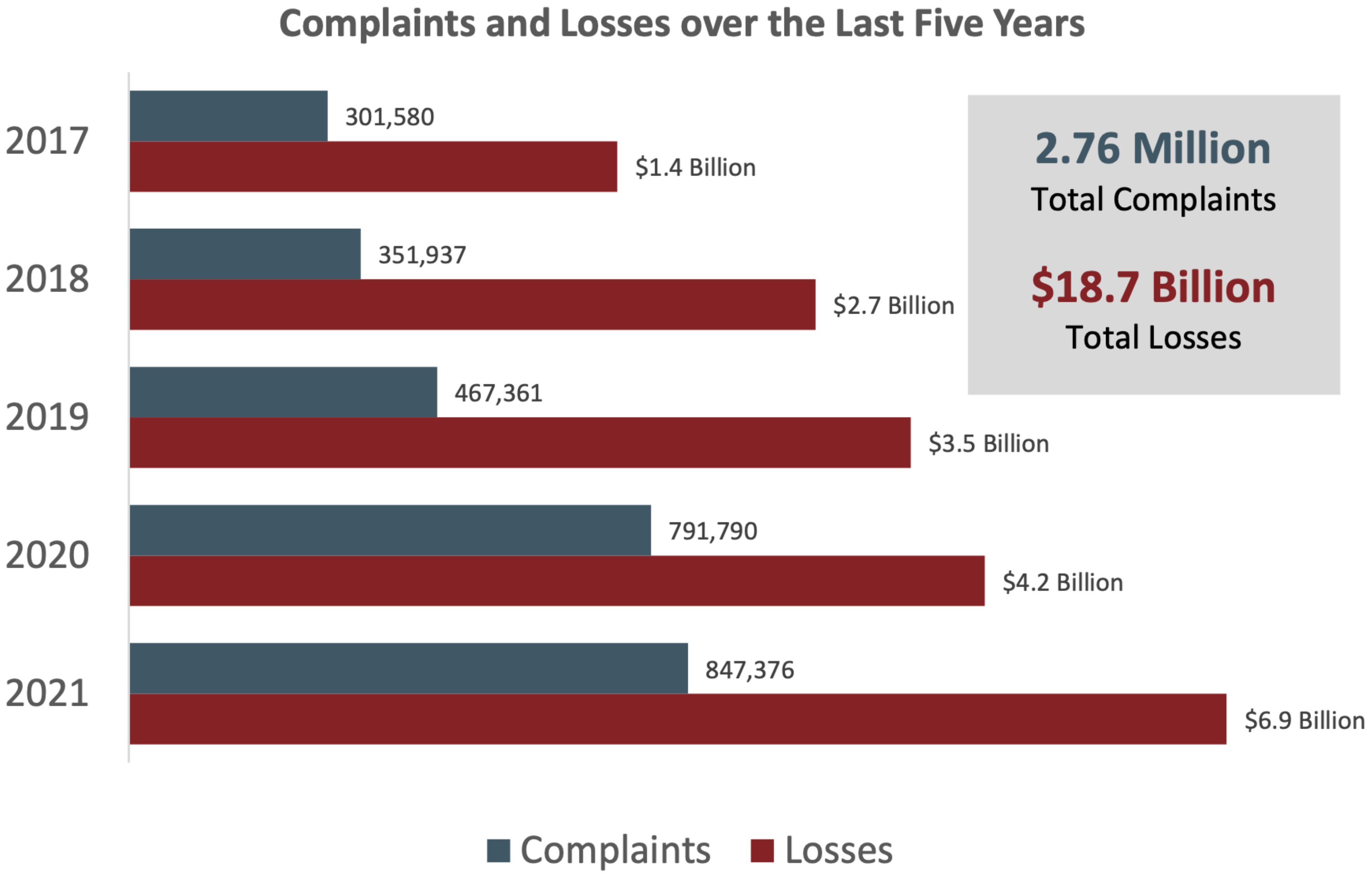


Figure 8: Conti's organization chart concluded from the leaks

Source: Cyberint

Losses according to Internet Crime Complaint Center (FBI)



Complaints and Losses over the Last Five Years

2.76 Million
Total Complaints

$18.7 Billion
Total Losses

2021 was the year for supply chain attacks

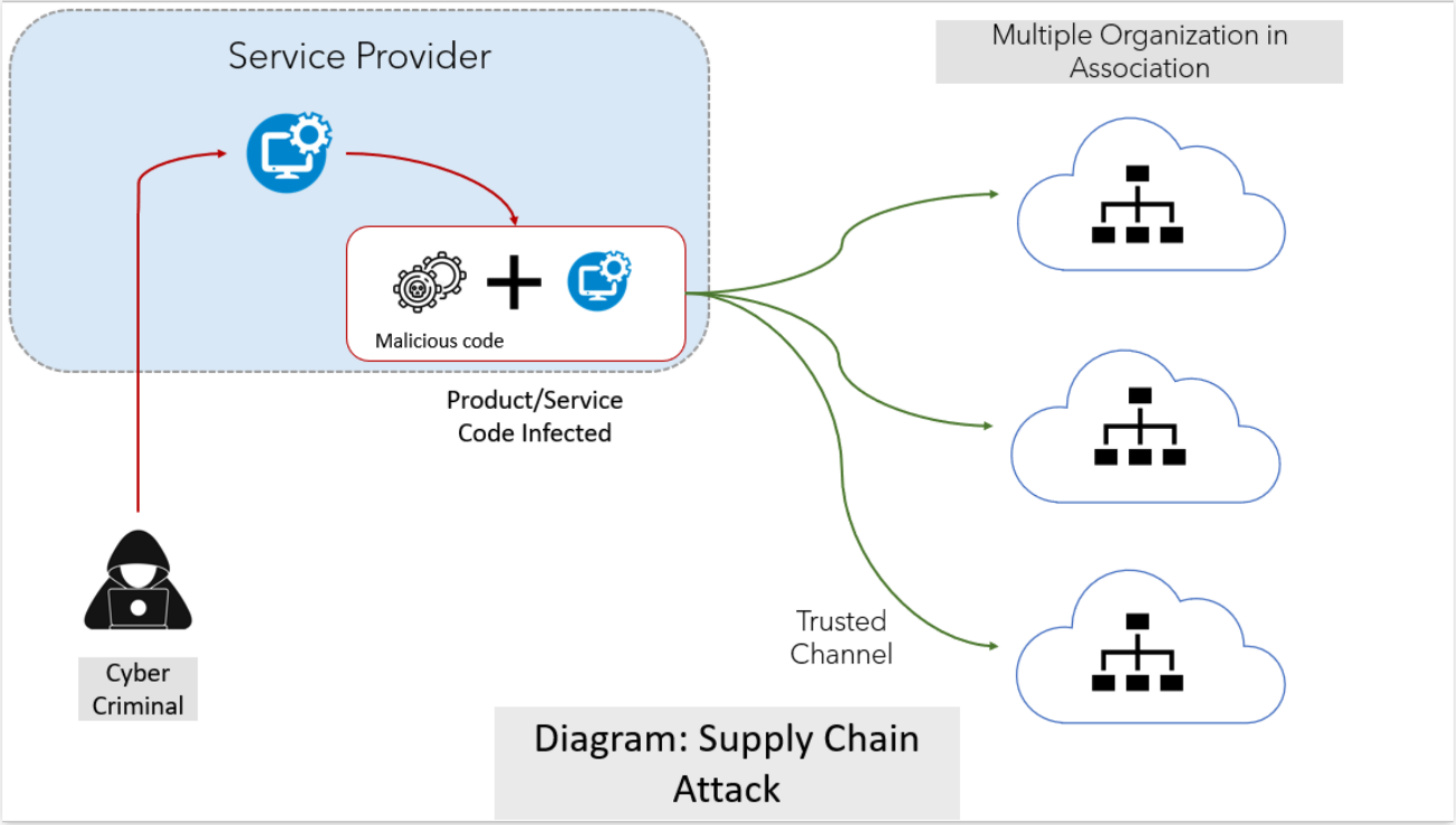
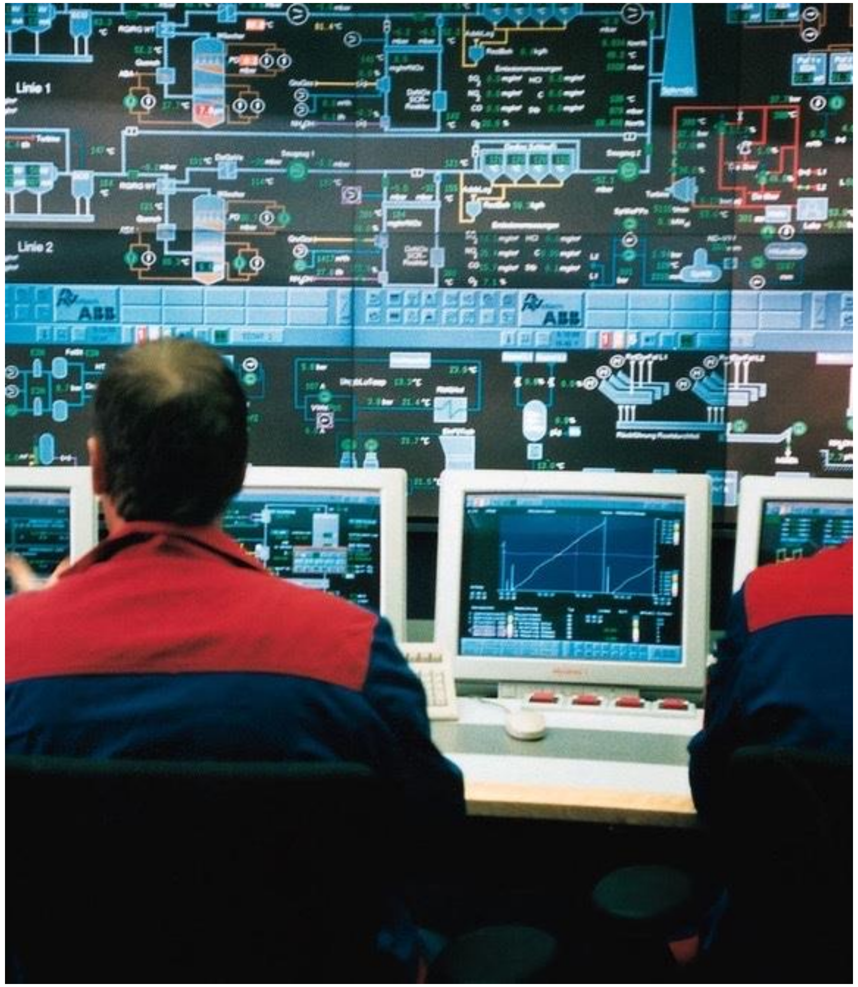

Service Provider
Multiple Organization in Association
Malicious code
Product/Service Code Infected
Trusted Channel
Cyber Criminal

Diagram: Supply Chain Attack

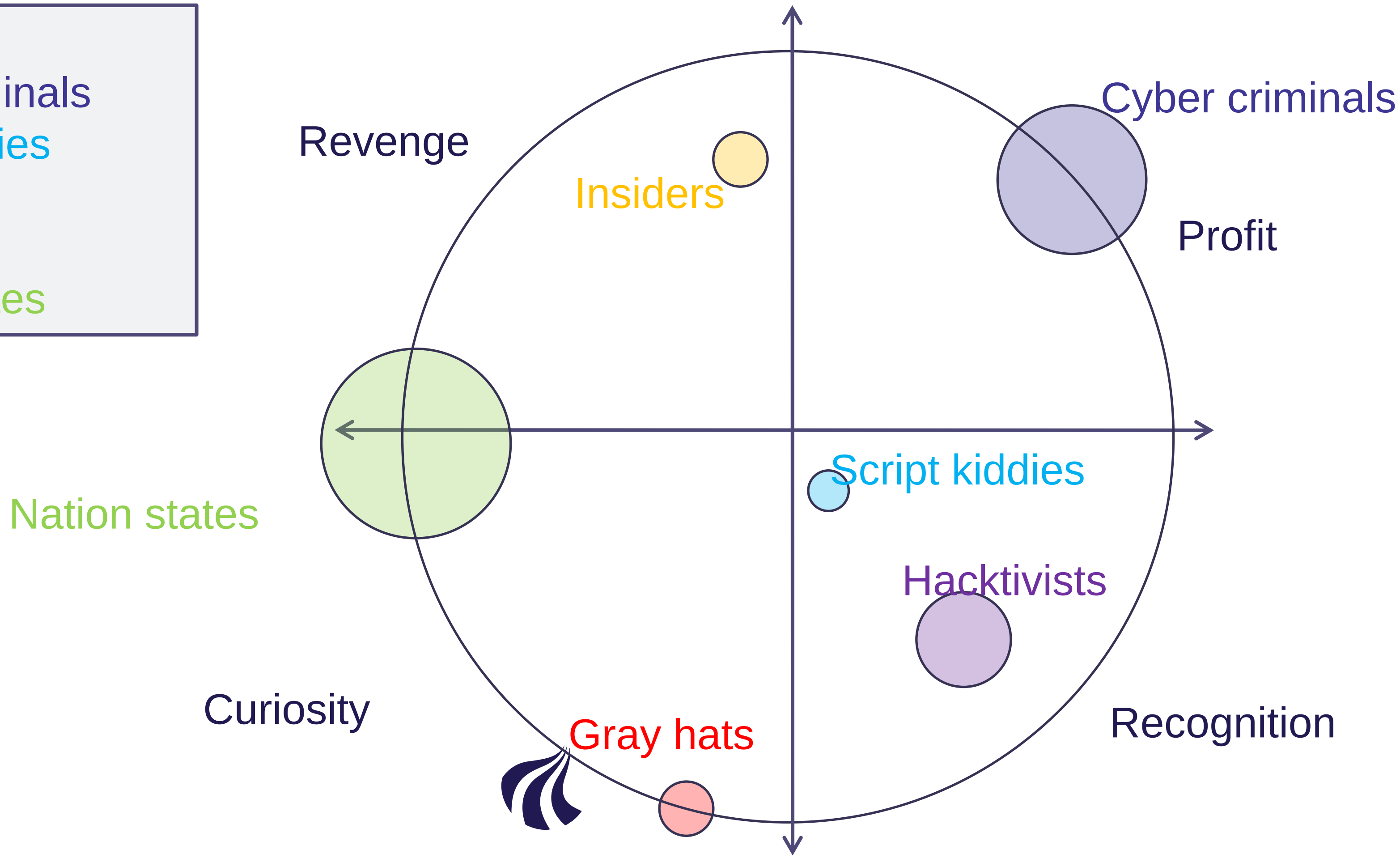
SoloriGate/Sunburst: SolarWinds Supply Chain Attack

Nation states



How are these groups connected? And why is this important?

Insiders
Cyber criminals
Script kiddies
Gray hats
Hacktivists
Nation states



AALBORG UNIVERSITY
DENMARK

What to do according to NIST

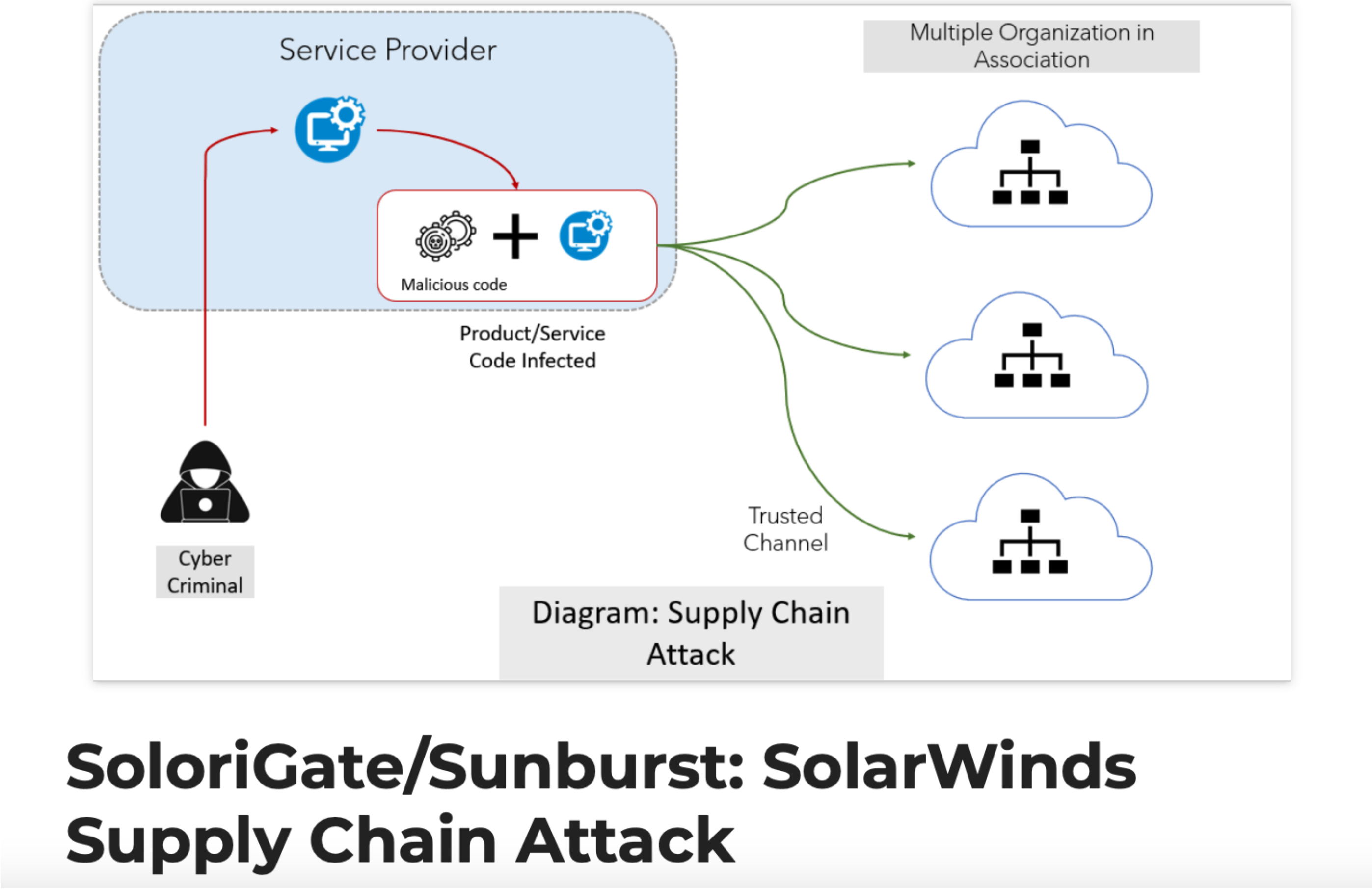
The Five Functions of NIST

- Identify
- Protect
- Detect
- Respond
- Recover

Don’t forget it’s all about risk ☺

Trends (1)

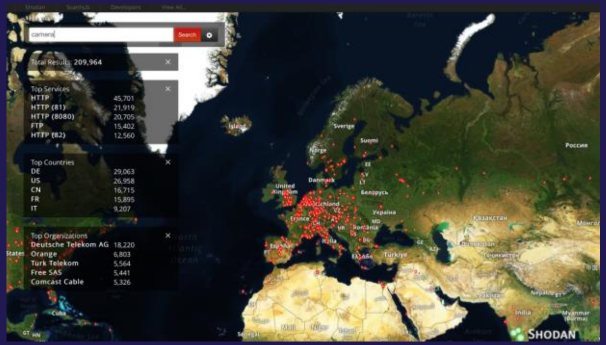
- More sophisticated attacks, larger targets, and at the same time lots of opportunistic attacks. Supply chain attacks are here to stay, and appears very challenging to address.


Service Provider
Multiple Organization in Association
Malicious code
Product/Service Code Infected
Cyber Criminal
Trusted Channel
Diagram: Supply Chain Attack

SoloriGate/Sunburst: SolarWinds Supply Chain Attack

Trends? (2)

- More sophisticated attacks, larger targets, and at the same time lots of opportunistic attacks. Supply chain attacks are here to stay, and appears very challenging to address.
- The number of Internet connected devices keeps increasing. It is hard to know what to trust – and if it is flawed, it is already found.

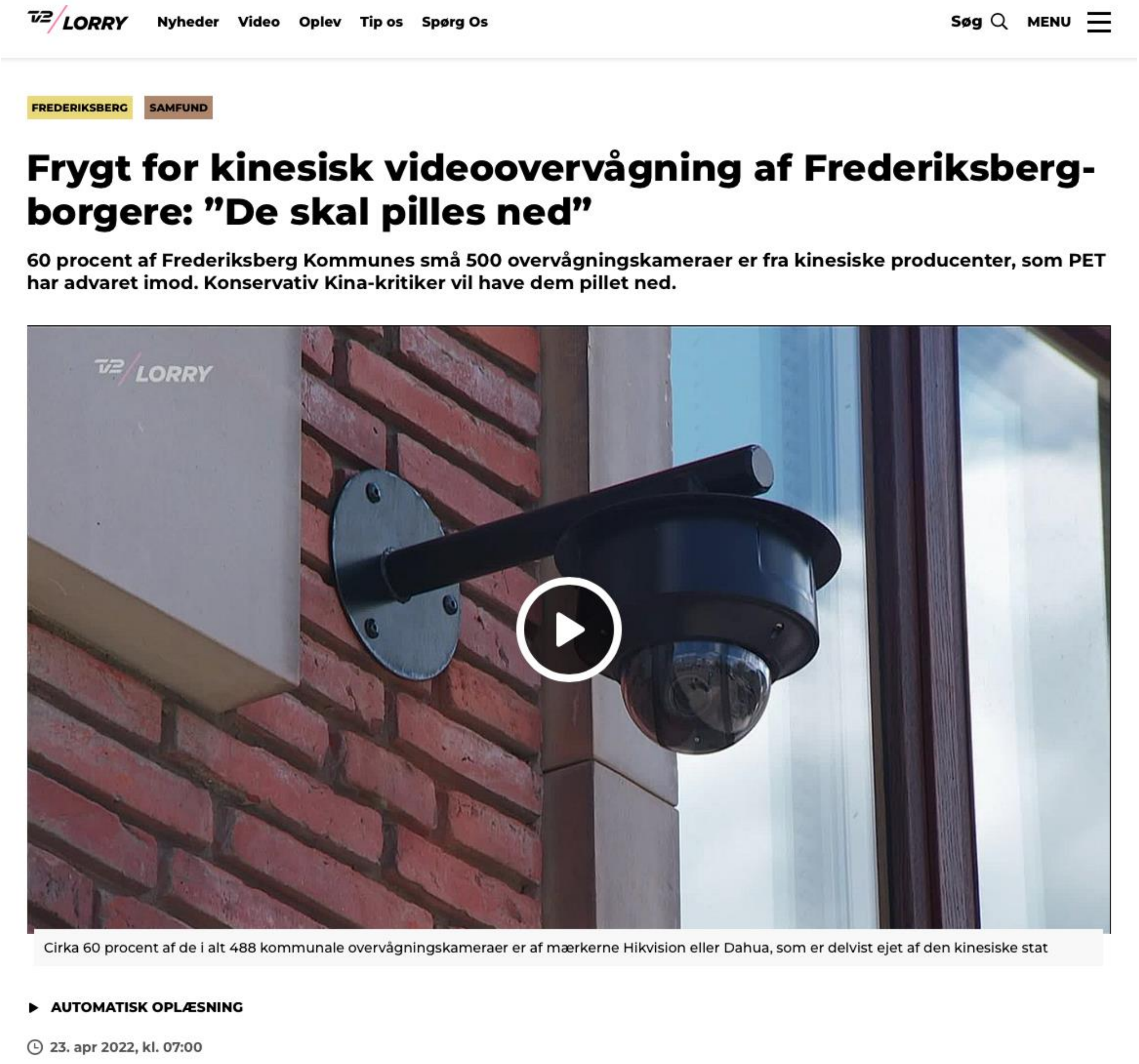


Total Results: 209,964

Top Services	
HTTP	45,701
HTTP (81)	21,919
HTTP (8080)	20,705
FTP	15,402
HTTP (82)	12,560

Top Countries	
DE	29,063
US	26,958
CN	16,715
FR	15,895
IT	9,207

Top Organizations	
Deutsche Telekom AG	18,220
Orange	6,803
Turk Telekom	5,564
Free SAS	5,441
Comcast Cable	5,326



Frygt for kinesisk videoovervågning af Frederiksberg-borgere: ”De skal pilles ned”

60 procent af Frederiksberg Kommunes små 500 overvågningskameraer er fra kinesiske producenter, som PET har advaret imod. Konservativ Kina-kritiker vil have dem pillet ned.

Cirka 60 procent af de i alt 488 kommunale overvågningskameraer er af mærkerne Hikvision eller Dahua, som er delvist ejet af den kinesiske stat

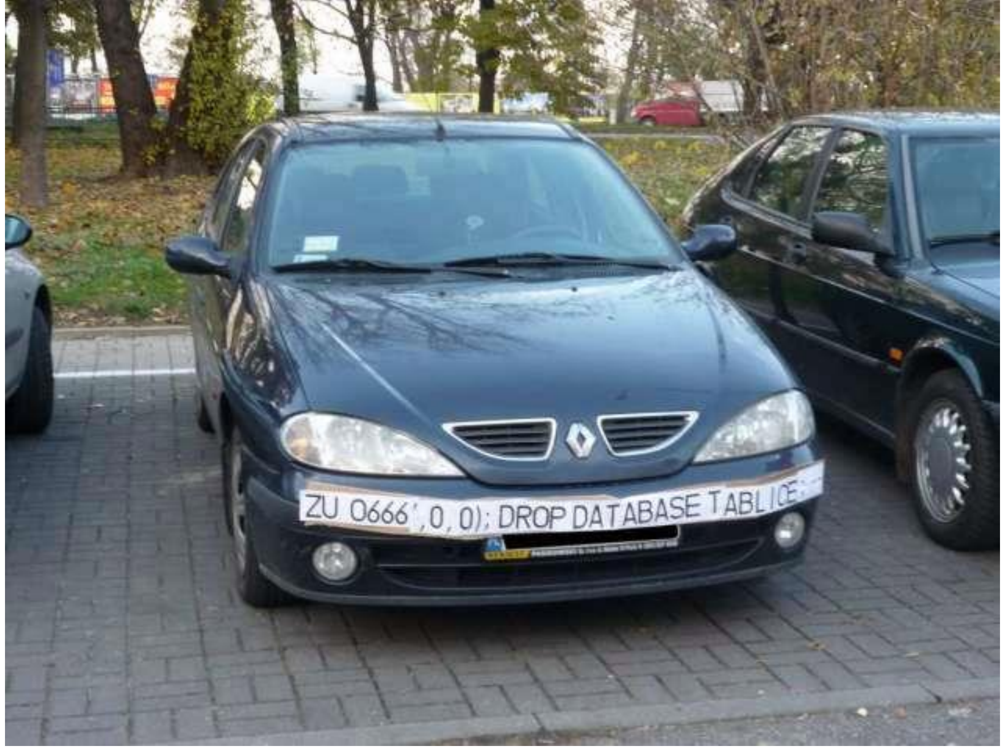
▶ AUTOMATISK OPLÆSNING

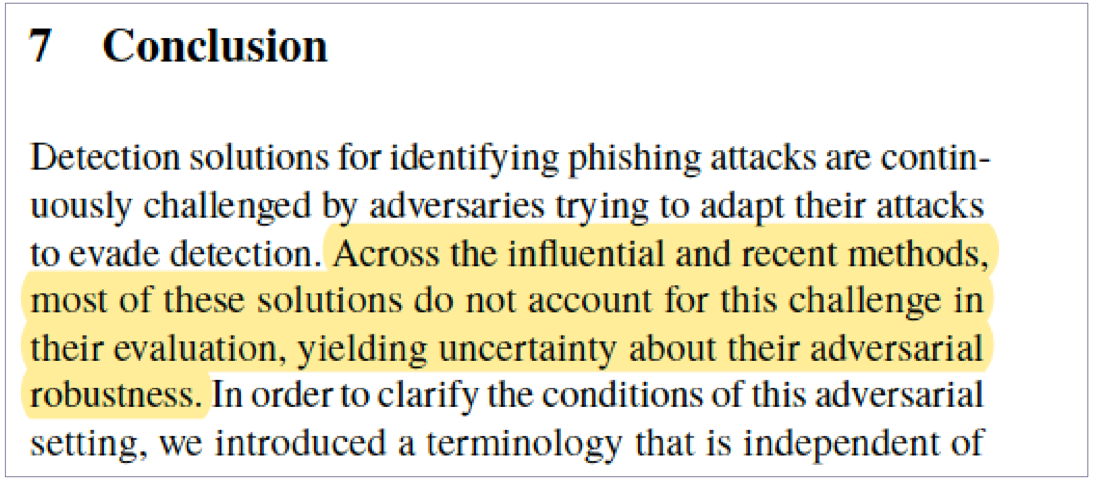
23. apr 2022, kl. 07:00

AALBORG UNIVERSITET

Trends (3)

- More sophisticated attacks, larger targets, and at the same time lots of opportunistic attacks. Supply chain attacks are here to stay, and appears very challenging to address.
- The number of Internet connected devices keeps increasing. It is hard to know what to trust – and if it is flawed, it is already found.
- We see a lot of artificial intelligence and machine learning, but do we understand how it works and how it can be attacked?





7 Conclusion

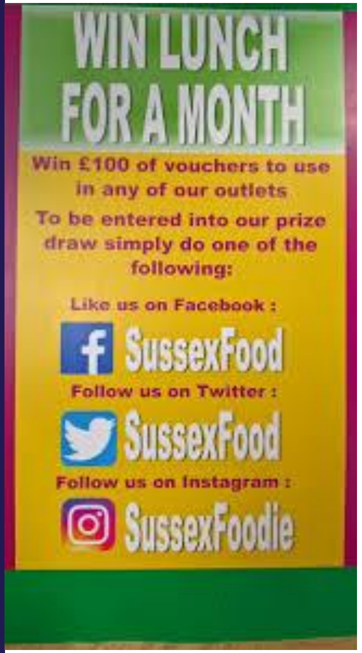
Detection solutions for identifying phishing attacks are continuously challenged by adversaries trying to adapt their attacks to evade detection. Across the influential and recent methods, most of these solutions do not account for this challenge in their evaluation, yielding uncertainty about their adversarial robustness. In order to clarify the conditions of this adversarial setting, we introduced a terminology that is independent of

AALBORG UNIVERSITET

Panum, T. K., Hageman, K., Hansen, R. R., & Pedersen, J. M. (2020). Towards Adversarial Phishing Detection. I 13th USENIX Workshop on Cyber Security Experimentation and Test USENIX - The Advanced Computing Systems Association. https://www.usenix.org/system/files/cset20-paper-panum.pdf

Trends? (4)

- More sophisticated attacks, larger targets, and at the same time lots of opportunistic attacks. Supply chain attacks are here to stay, and appears very challenging to address.
- The number of Internet connected devices keeps increasing. It is hard to know what to trust – and if it is flawed, it is already found.
- We see a lot of artificial intelligence and machine learning, but do we understand how it works and how it can be attacked?
- We need a holistic view on cyber security, including the users – and we need to understand that cyber security is part of a context.



WIN LUNCH FOR A MONTH

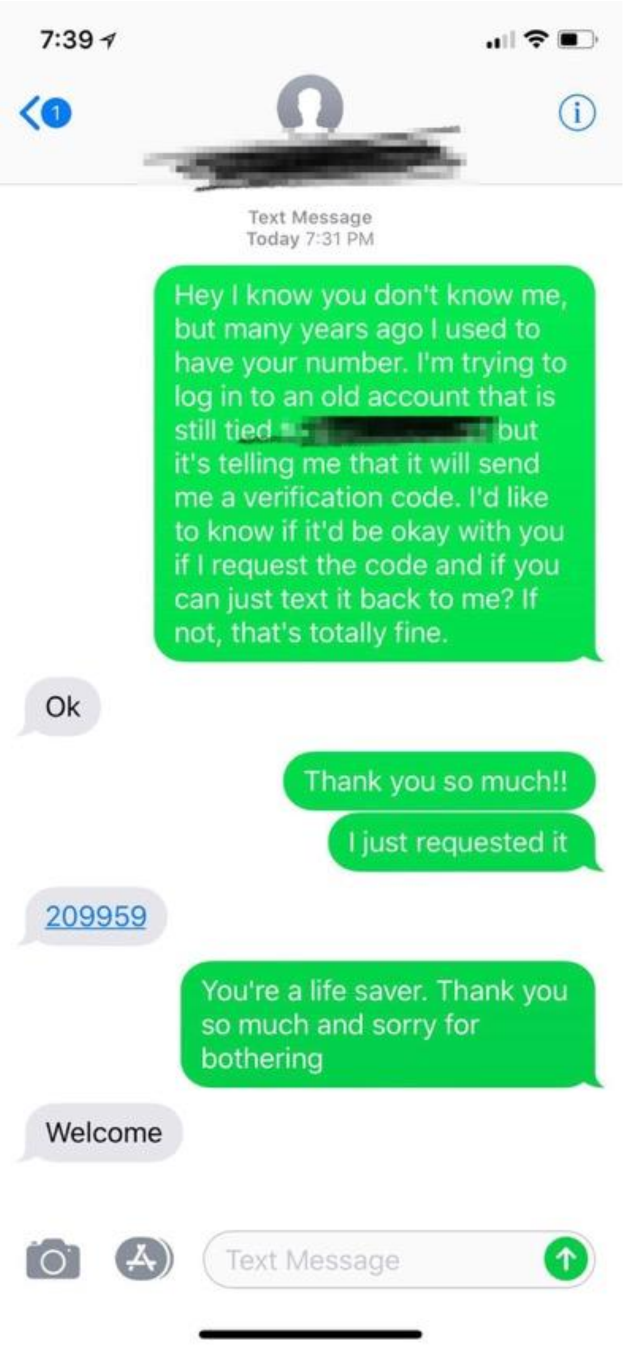
Win £100 of vouchers to use in any of our outlets

To be entered into our prize draw simply do one of the following:

Like us on Facebook : SussexFood

Follow us on Twitter : SussexFood

Follow us on Instagram : SussexFoodie



Hey I know you don't know me, but many years ago I used to have your number. I'm trying to log in to an old account that is still tied [redacted] but it's telling me that it will send me a verification code. I'd like to know if it'd be okay with you if I request the code and if you can just text it back to me? If not, that's totally fine.

Ok

Thank you so much!!

I just requested it

209959

You're a life saver. Thank you so much and sorry for bothering

Welcome

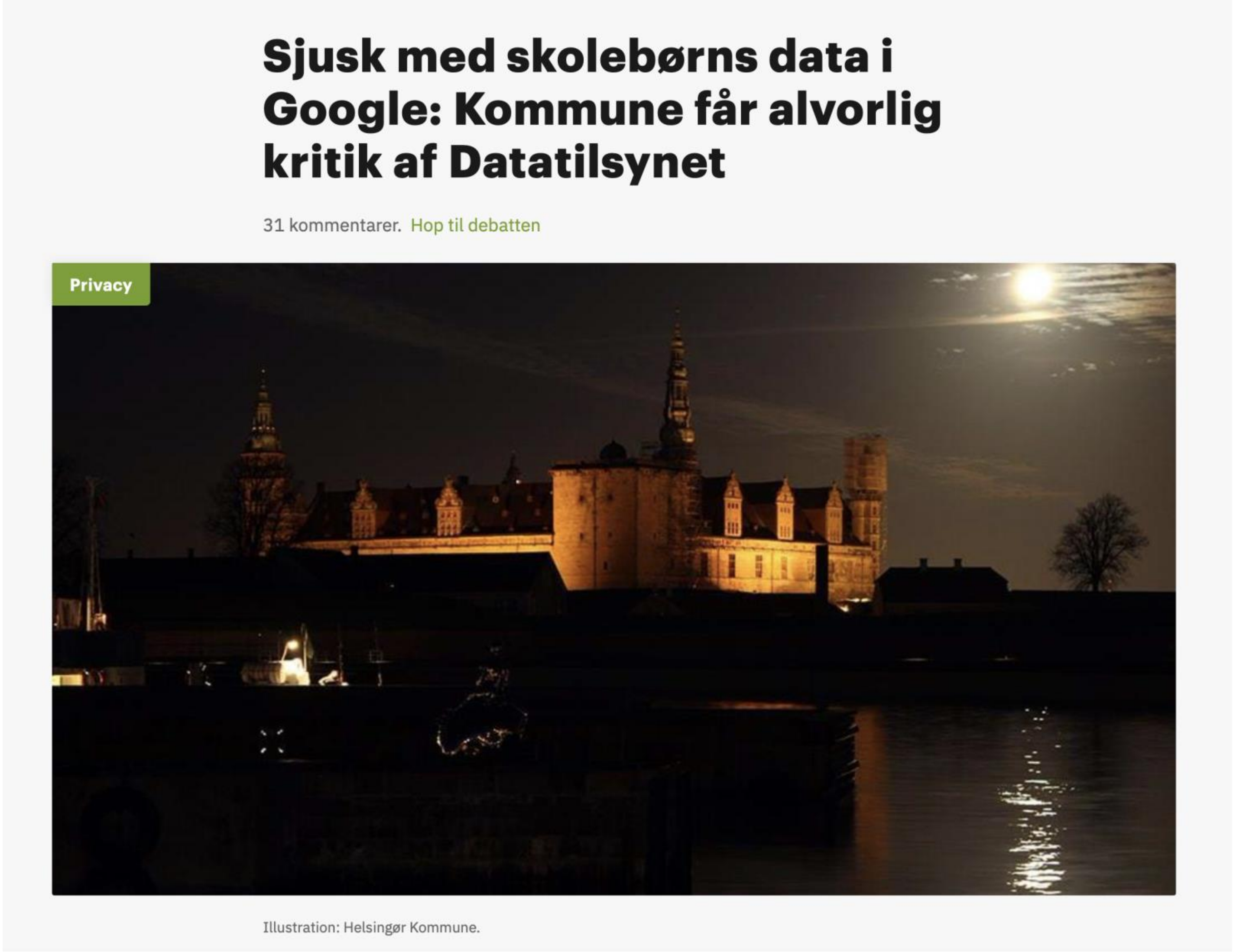
Her er det gratis trådløst internett

Nett: Gjovik_Free_Wifi

GJØVIK KOMMUNE

Trends? (5)

- More sophisticated attacks, larger targets, and at the same time lots of opportunistic attacks. Supply chain attacks are here to stay, and appears very challenging to address.
- The number of Internet connected devices keeps increasing. It is hard to know what to trust – and if it is flawed, it is already found.
- We see a lot of artificial intelligence and machine learning, but do we understand how it works and how it can be attacked?
- We need a holistic view on cyber security, including the users – and we need to understand that cyber security is part of a context.
- Increasing regulation e.g. NIS2 – higher requirements for companies and suppliers.



Sjusk med skolebørns data i Google: Kommune får alvorlig kritik af Datatilsynet

31 kommentarer. Hop til debatten

Privacy

Illustration: Helsingør Kommune.

AALBORG UNIVERSITET

Cyber security is all about risks

Keep calm and ...

ASIV Case!

- In this case, you need to come up with a plan on how to handle cyber attacks: How to prevent attacks, how to detect attacks, and most importantly: What to do in case of an attack?
- You have until 15.15 to work in the groups
- During the session, there might be updates. These are distributed in the chat of the main room (so we will close the breakout rooms whenever there is an update).
- Good advice: Keep cool. Organise yourself.