Denn Wissen hat Wert.

www.kapitalmarktconsult.at

Feindbild „Cybercrime“ Die wachsende Bedrohung im Netz

Dr. Philipp Amann, MSc
Head of Strategy
European Cybercrime Centre
Europol

Europol's Mandate

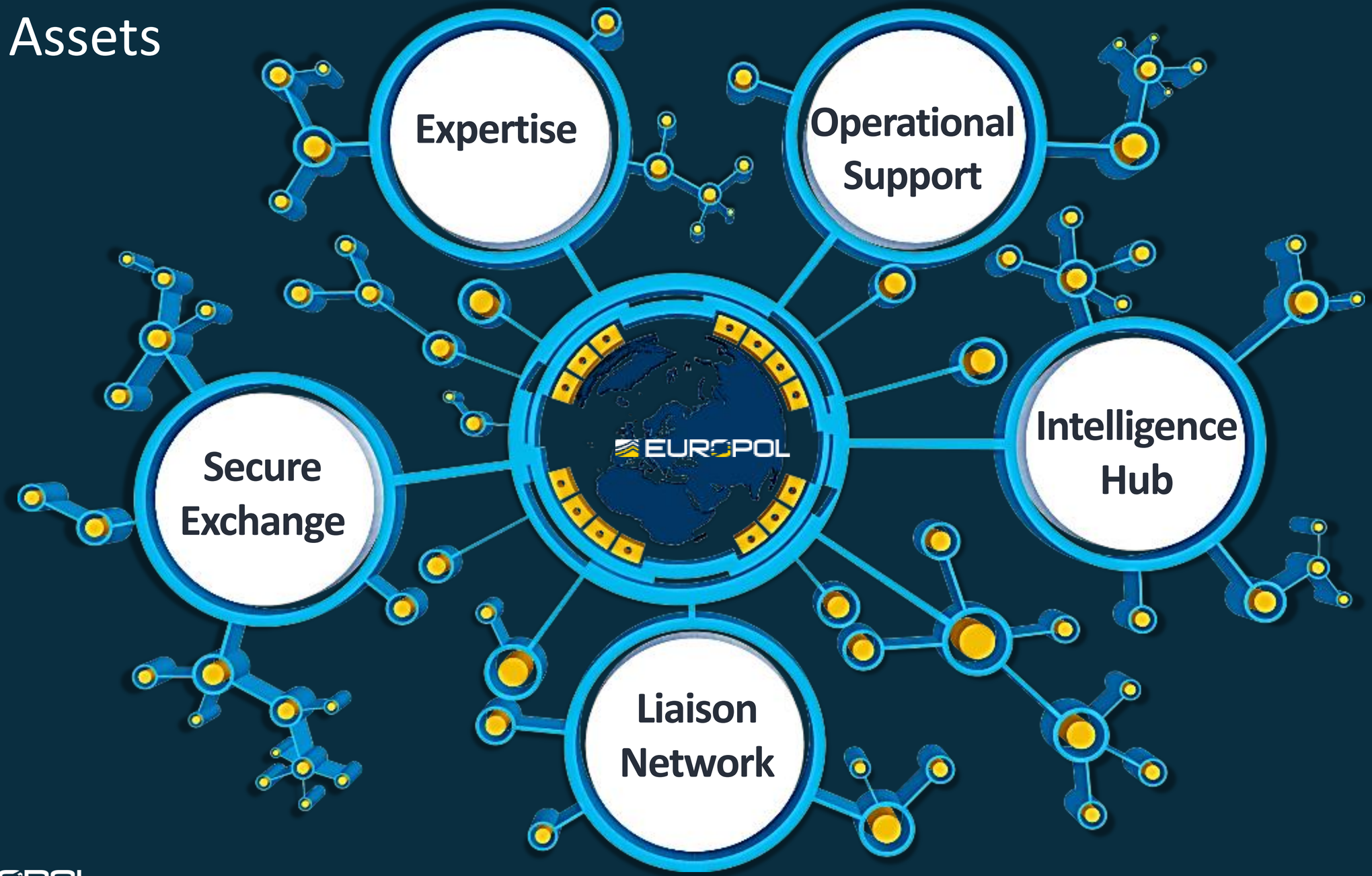
EUROPOL

The Hague, Netherlands

"Europol shall support and strengthen action by the competent authorities of the Member States and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy"

(Europol Regulation)

Key Assets



Public-Private-Partnerships – Advisory Groups

Communication Providers

Financial Services

Internet Security

Europol Unclassified - Basic Protection Level

Highlights 2020

OPERATIONAL COOPERATION

35+ cross-border operations supported

Contributions to COVID-19 related crime monitoring

Disruption of EMOTET

CAPACITY-BUILDING

1 New tool created to support law enforcement investigations

200 vouchers distributed to LE to get RIPE certified

INFORMATION & INTELLIGENCE SHARING

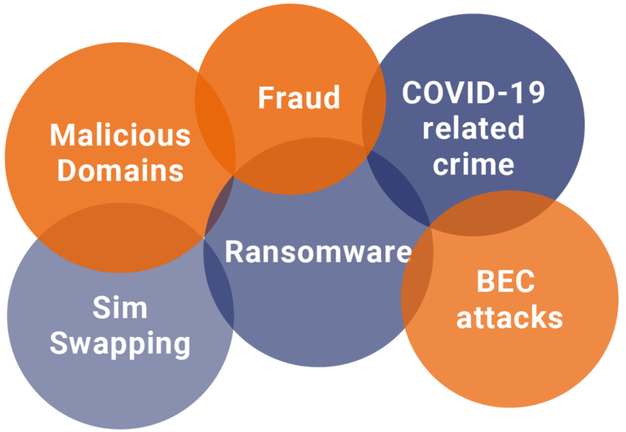
9 Meetings

15 Presentations

16 Members interviewed for the IOCTA 2020

2 Members supported Foresight Exercises

Continuous intelligence notifications, including COVID-19 themed threats



3 Thematic sessions
- SIM Swapping
- Malicious Domains
- DNS over Https

PREVENTION AND AWARENESS

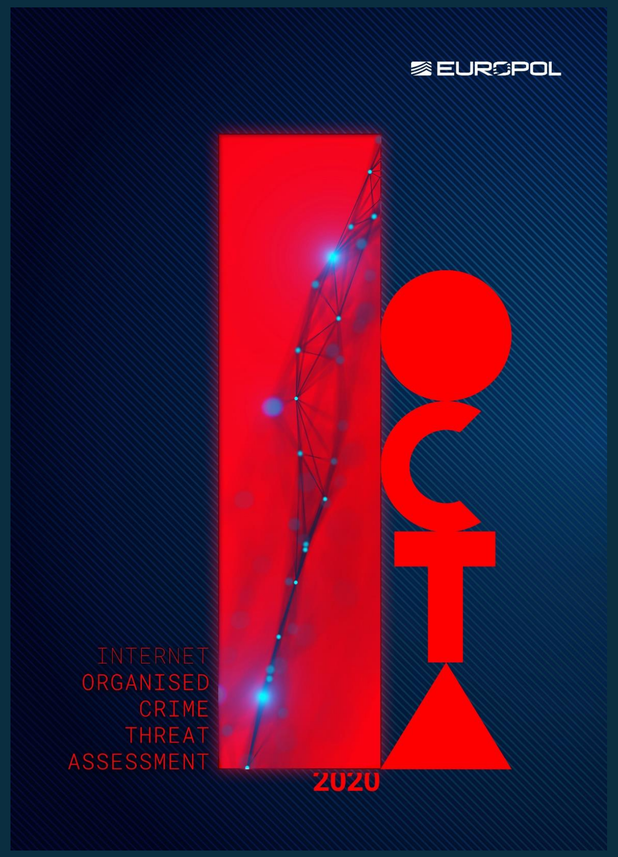
6 Prevention & awareness projects supported

Joint Report on malicious use of AI

EUROPOL EC3 European Cybercrime Centre

Information Position

IOCTA 2020: Key Threats



- Social engineering, malware and ransomware remain top threats
- Cryptocurrencies continue to facilitate payments for various forms of cybercrime
- Reporting challenges hinder the ability to create an accurate overview of crime
- Criminals take advantage of the COVID-19 crisis

The 2020 cyber threat landscape

Cybercrime evolution:

- Fundamentals firmly rooted
- Cybercriminals refine their artisanship
- CaaS raises capability among threat actors

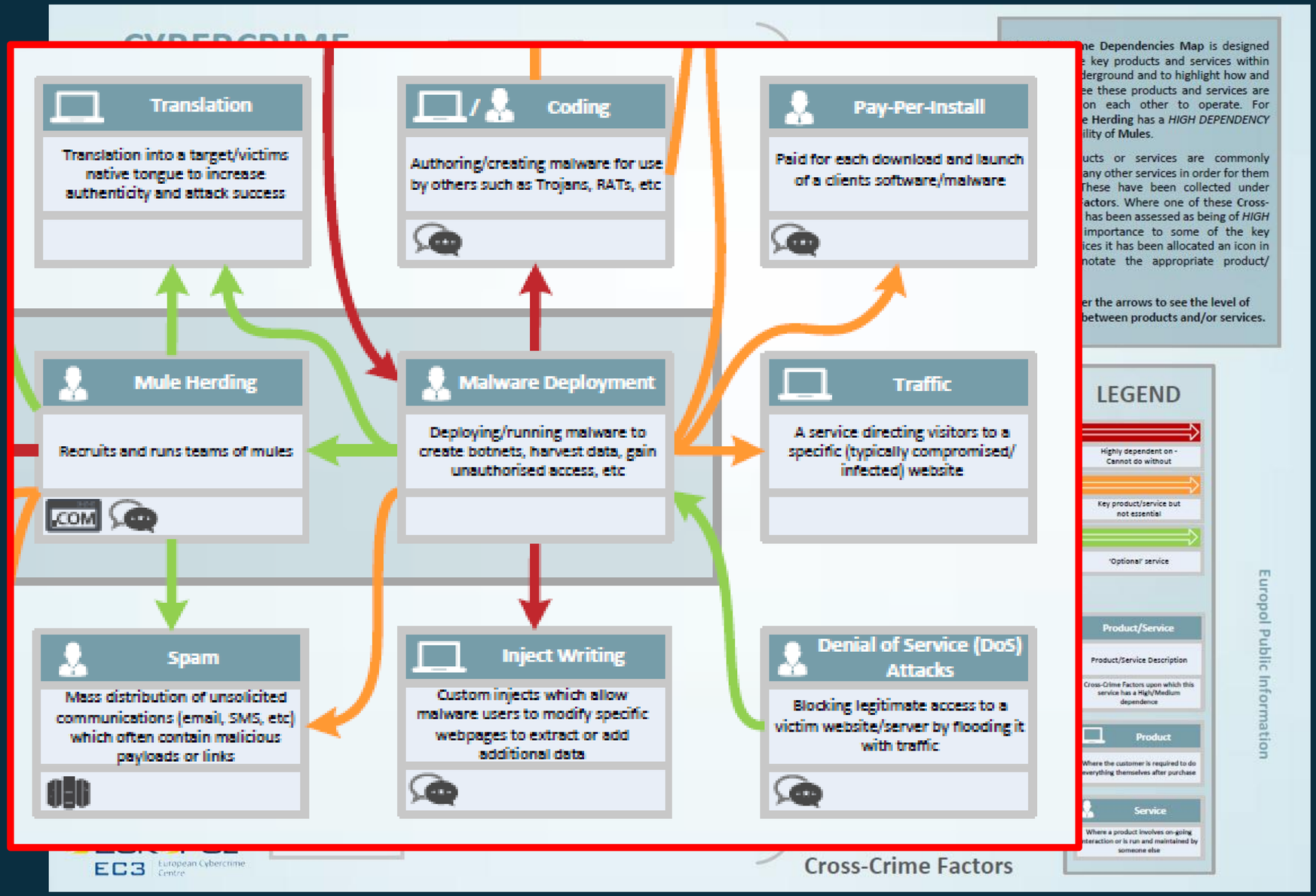
Criminals drive enterprise mindsets in their approach:

- Improving crime methodologies and odds of success
- The cyber-element infiltrates almost all areas of crime

Threat actors abused the COVID-19 pandemic crisis narrative in criminal activities.

- Crisis amplified existing problems with people working from home and spending time online, particularly seen in Child Sexual Exploitation/CSAM

Cybercrime Dependencies Map



Highlights

Payment Fraud

- **Increase in (E-)SIM swapping and SMishing**
- **BEC growing concern**
- Online investment fraud with victims all over Europe
- Card-not-present fraud continues to increase

Phishing Attacks

- **Faster and more automated**
- Criminals adopting a holistic strategy
- More authentic-looking messages and sites
- **Situational awareness: COVID-19 narrative**

Ransomware

- **Targets organisations rather than persons**
- **GDPR fines used as added leverage**
- **Fear of re-victimization: reluctant to report crime**
- **Ransom demand negotiating**

Malware

- **Advanced modular Malware**
- **Mobile malware**
- Commodity malware lowering barriers to entry into cybercrime

Threat Actors

- **CaaS model fully established**
- More operational security
- Hide tracks:
  - PETs
  - Bulletproof hosting
  - Cryptocurrencies

Reporting challenges

- Broad and static crime registration systems
- Difficult to quantify resource requests
- **Insufficient cybercrime awareness among the public and local police**

Tackling the Threat

Hackers behind Colonial Pipeline attack reportedly received $90 mill in bitcoin before shu

PUBLISHED TUE, MAY 18 2021•9:04 AM EDT | UPDATED T

Ryan Browne
@RYAN_BROWNE_

KEY POINTS

- DarkSide, the h received $90 r blockchain sleu
- The cybercrimi servers and as
- Elliptic said Da the digital curr

Cyber attac giant JBS

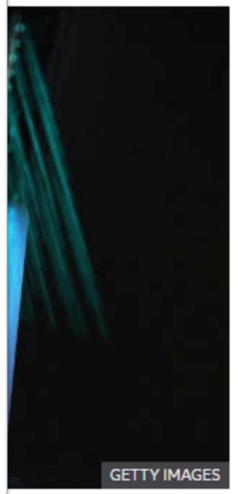
ABC Radio Brisbane / By Edwi
Posted Yesterday at 4:43am, u

A union says there could be a

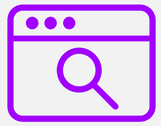
Cyber attack 'most significant on

The ransomware plague cost the world over $1 billion

Group-IB has presented a report which examines key shifts in the cybercrime world internationally between H2 2019 and H1 2020 and gives forecasts for the coming year. The most severe financial damage has occurred as a result of ransomware activity.



The ransomware ‘kill chain’







Recon

- Most dominant threat - increasingly targeted
- Victim reconnaissance plays significant role
- Attacks against local governments, healthcare, education, manufacturing, finance, energy, and transport industries
- COVID-19 – increased attack surface
- Reported attacks on shipping and logistics firms tripled between 2019 and 2020
- RaaS – affiliate programme, steps covered by different actors

Dev/ Test

Sales/ Resales

Infra Setup & Ops

Pre-Event

Initial Access

- Triple extortion - increased pressure by threatening publication /auctioning/ wiping of data (GDPR fines, cold-calling victims, attacks against insurance companies)
- Significant risks to other organisations in the supply chain and critical infrastructure

Ransomware Live

Event

Recovery

- Victimisation goes beyond the primary target
- Cryptocurrencies key facilitator
- Impact beyond financial damage

Post-Event

US fuel pipeline hackers 'didn't mean to create problems'

By Mary-Ann Russon
Business reporter, BBC News

10 May

Complete Mission

- Data exfiltration via rclone or WinSCP
- Data theft extortion
- DARKSIDE ransomware deployment (generally via PsExec)

Emotet Takedown

Taking control

Innovative approach to disrupt and gain control of the infrastructure from the inside

International collaboration

Netherlands, France, Germany, Ukraine, United Kingdom, Lithuania, Canada, United States, and Europol EC3

EUROPOL EC3 European Cybercrime Centre

Attacks for hire

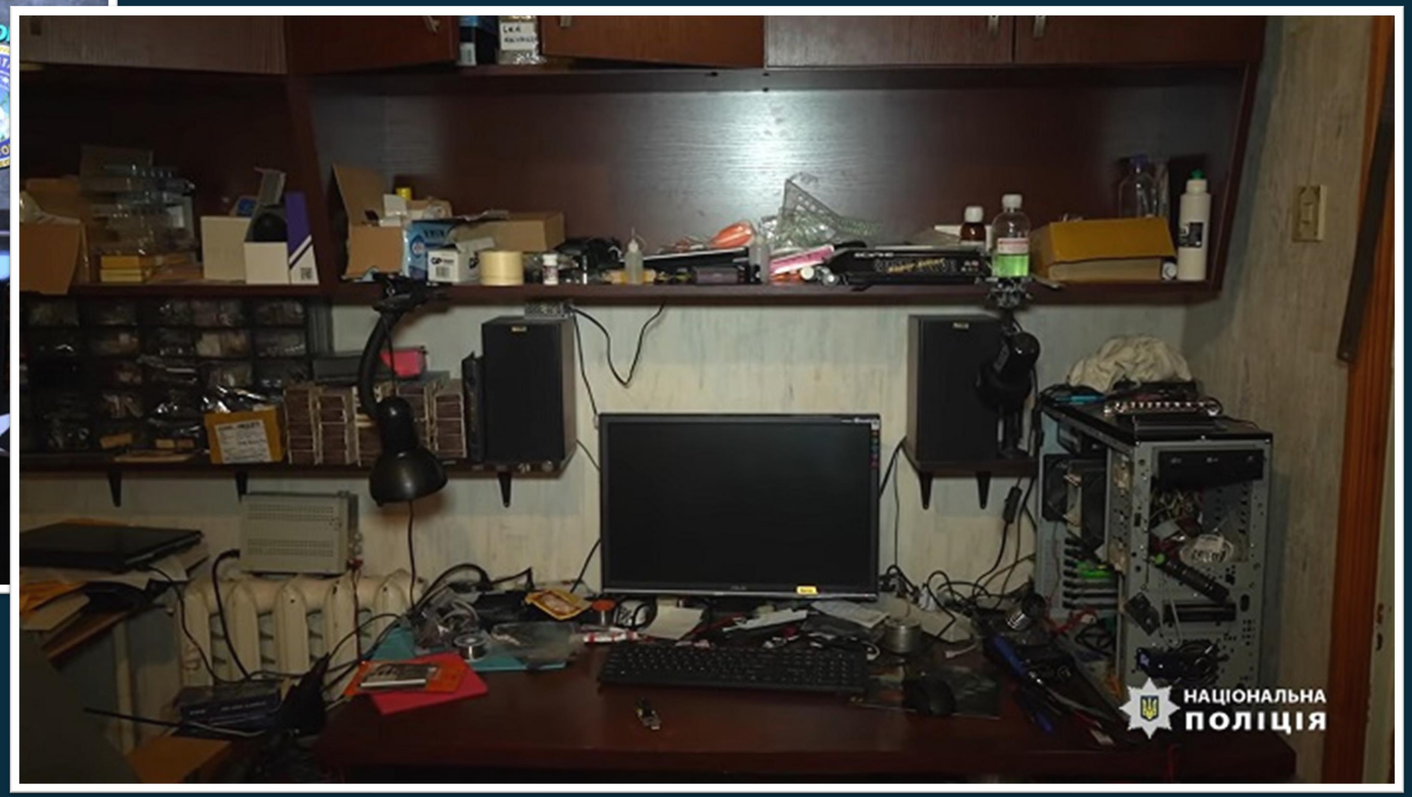
For information stealers, Trojans, ransomware, …
60% in 2019

Global criminal infrastructure

Several hundreds of servers across the world with different functionalities

EUROPOL

Emotet: Expectation vs. Reality

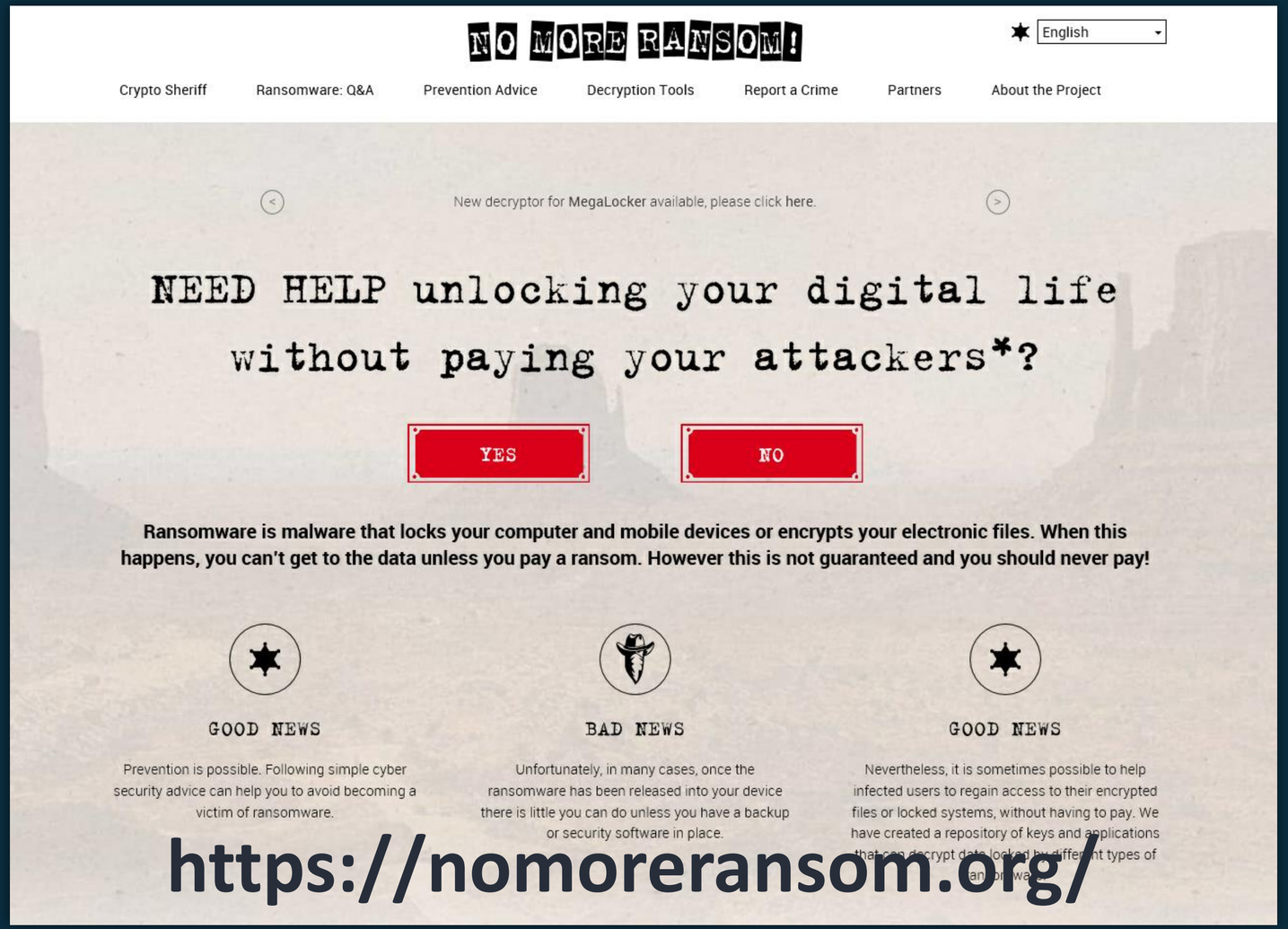


To pay or not to pay…

- You are dealing with criminals
- No guarantees that you will get back your data
- You will finance ransomware and other forms of criminality
- You are likely to become a target again
- Business continuity
- Costs of outage >> ransom
- Insurance

#DONTPAY

Public-private partnership: No More Ransom

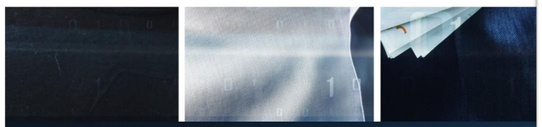


https://nomoreransom.org/

- **+170 partners**
- **Website available in 37 languages**
- **+100 tools capable of decrypting +135 ransomware families**
- **$ 632 million in ransom payments stopped**

European Money Mule Action

"I thought it was pa



MONEY MULING HELPS P

IGNORANCE IS NO EXCUSE

Criminals
victims into
behalf by m
legitimate a

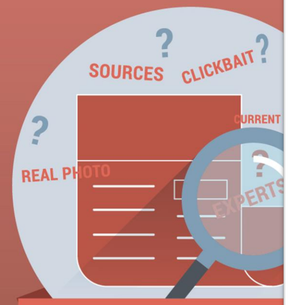
Be wary o
written wit
spelling mis

#dontbeaMule

EUROPOL EC3 European Cybercrime Centre

FAKE NEWS

COVID-19 DISINFORMATION CAN ENDANGER PEOPLE'S LIVES



SPOT THE FA

BARGAIN or DEALBREAKER?

The golden rules of online shopping

BUY FROM TRUSTED SOURCES

Use brands and shops that you are familiar with.

CHECK REVIEWS AND RATINGS

Especially of unknown stores and individual sellers.

CONTROL RECURRING CHARGES

Before providing your card details to pay for a continuous service over the internet, find out how you can stop that service.

MAKE SURE THE DATA TRANSFER IS SECURE

Use HTTPS and SSL protocols when browsing the internet. Remember: the padlock symbol alone doesn't make a website legitimate.

THINK TWICE BEFORE PURCHASING

Make sure you understand the risks of buying online.

USE CREDIT CARDS WHEN PURCHASING THINGS ONLINE

Most credit cards have a strong customer protection policy. If you don't get what you ordered, the card issuer will refund you.

SAVE ALL DOCUMENTS RELATED TO YOUR ONLINE PURCHASES

They may be needed to establish the terms and conditions of the sale or to prove that you have paid for the goods.

DON'T SEND MONEY TO SOMEONE YOU DON'T KNOW

If you wouldn't give money to a random person on the street, don't do it on the internet. If possible, reserve the right to receive the goods first.

NEVER SEND YOUR CARD DETAILS BY EMAIL

Never send a copy of your card, your card number, PIN or any other card information to anyone by email.

NOT BUYING? DON'T LEAVE YOUR CARD BEHIND

If you are not buying anything, don't submit or save your card details.

CHECK THE WEBSITE PAYMENT SECURITY

Only do your online shopping on websites that use full authentication systems (such as Verified by Visa / MasterCard Secure Code).

EUROPOL EC3 European Cybercrime Centre

MRC

#BuySafePaySafe

EUROPOL

Looking ahead

CEO Fraud – using AI?

STEP 6

The employ
to an accou
the fraudst
re-transferr
multiple jur

STEP 5

Instructions
proceed are
third-person

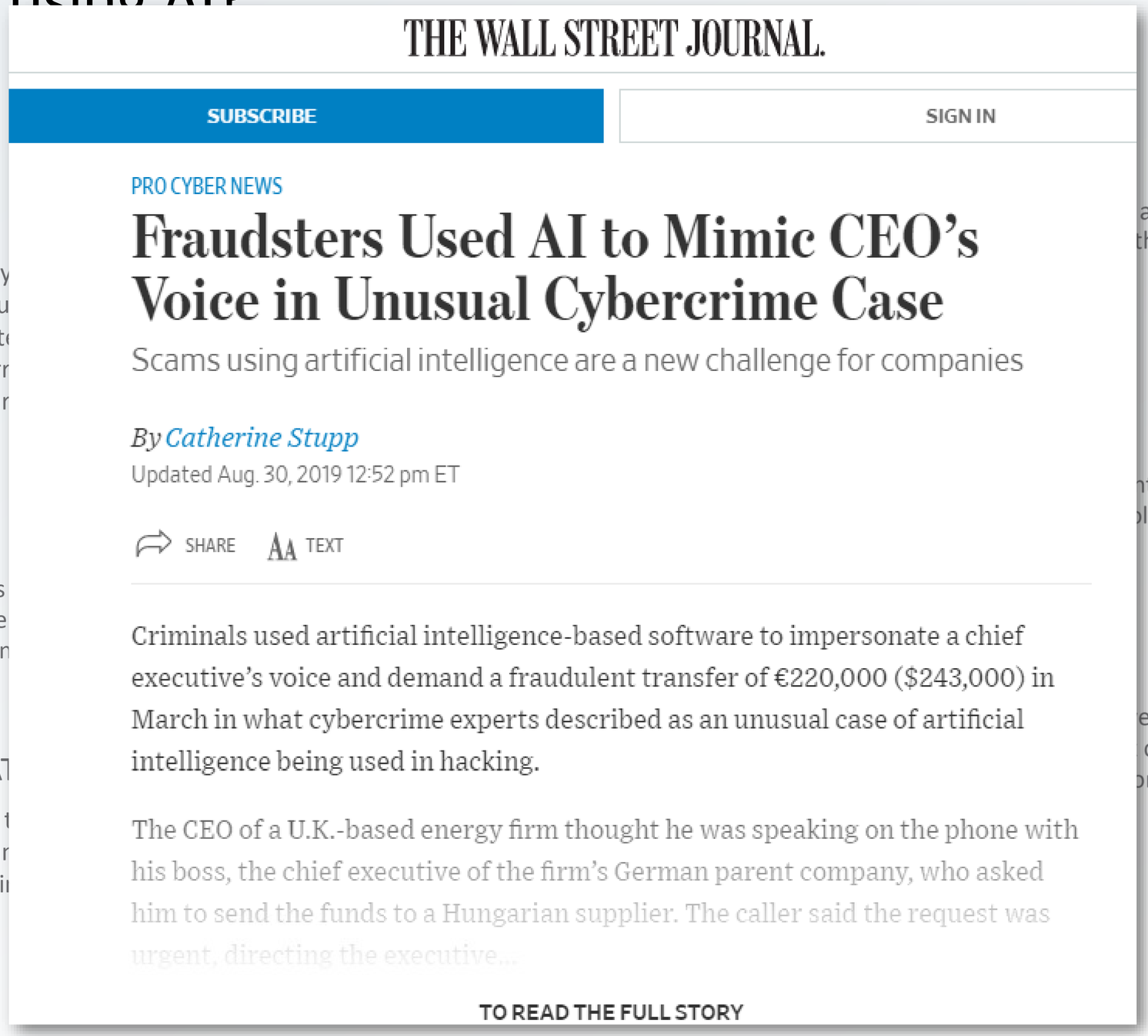
ALTERNAT

- Requests t
  (e.g. all ur
- Uses the i
  clients

as
the

nt transfer
olute

e
control;
on)



THE WALL STREET JOURNAL.

SUBSCRIBE SIGN IN

PRO CYBER NEWS

Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case

Scams using artificial intelligence are a new challenge for companies

By Catherine Stupp

Updated Aug. 30, 2019 12:52 pm ET

SHARE TEXT

Criminals used artificial intelligence-based software to impersonate a chief executive's voice and demand a fraudulent transfer of €220,000 ($243,000) in March in what cybercrime experts described as an unusual case of artificial intelligence being used in hacking.

The CEO of a U.K.-based energy firm thought he was speaking on the phone with his boss, the chief executive of the firm's German parent company, who asked him to send the funds to a Hungarian supplier. The caller said the request was urgent, directing the executive...

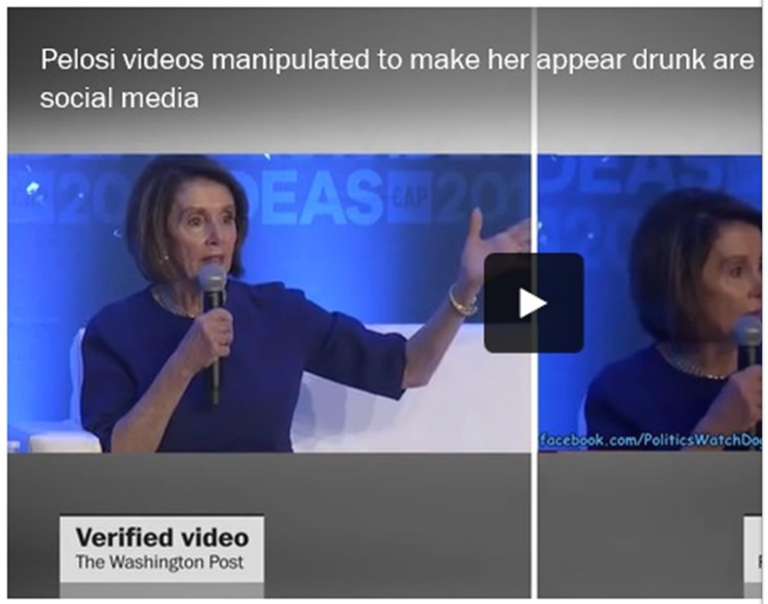
TO READ THE FULL STORY

Deep Fakes

Support The Guardian | Search jobs | Sign in | Search | The | International edition

Technology

Faked Pelosi videos, slowed to make her appear drunk, spread across social media



Altered videos of House Speaker Nancy Pelosi (D-Calif.), slowed down to
and slurred, are spreading across social media. (Blair Guild, Elyse Samu

People are Googling Rihanna and their birthday in a Twitter challenge
Monday 2:13 PM

Here are all of the Fortnite earthquake cracks thus far
Monday 1:21 PM

New Apex Legends characters leaked by data miners
Monday 12:36 PM

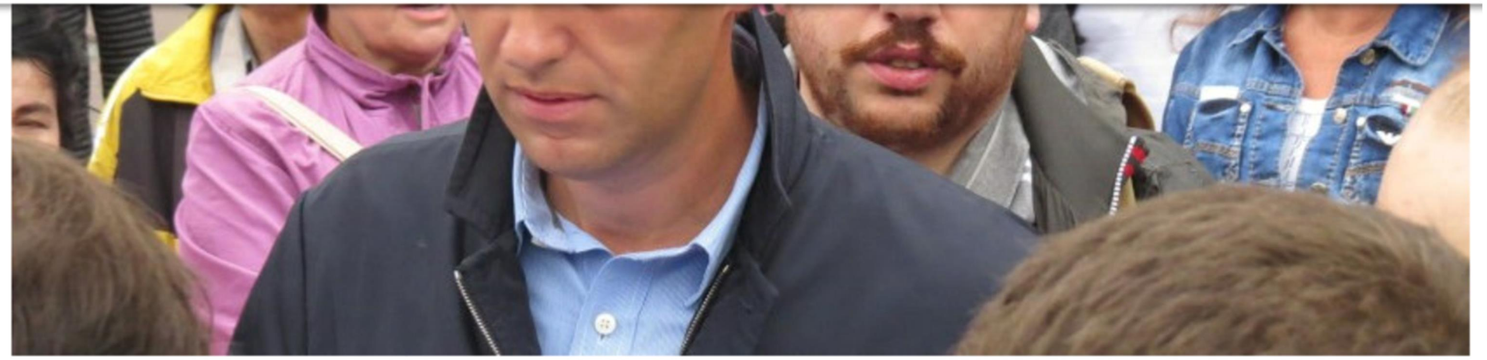
A new website that utilizes artifi
generate the faces of people who

Email | Subscribe Now! | ×

PAGES | Search site

NL#TIMES

TOP STORIES HEALTH CRIME POLITICS BUSINESS TE



Leonid Volkov with Alexei Navalny - Source: putnik at Wikimedia Commons

POLITICS TECH INNOVATION LEONID VOLKOV ALEXEI NAVALNY DEEPFAKE
» MORE TAGS

SHARE THIS:

SATURDAY, APRIL 24, 2021 - 09:36

Dutch MPs in video conference with deep fake imitation of Navalny's Chief of Staff

Dutch parliamentarians, like their British and Baltic colleagues, had a conversation via Zoom with a deep fake imitation of the chief of staff of the Russian opposition leader Alexei Navalny on Wednesday.

Fake Identities

www.whichfaceisreal.com

Fake Identities

www.whichfaceisreal.com

Artificial Intelligence: friend or foe?

- Automated and enhanced recon
- KYC and identity management
- Bypassing of (AI-based) defence mechanisms (e.g. Spam filters)
- Mis- and disinformation

Summary


Always has been.
Wait, it was just a lack
of basic IT-security measures?!
imgflip.com

Main Takeaway Points

- **Industrialisation and agility of Cybercrime – Crime-as-a-Service model firmly established (COVID-19, AIforCrime-as-a-Service, …)**
- **Expanding attack surface (IoT, shadow IT, supply chain) and need to manage increasing complexity and risks**
- **Ransomware one of the main threats – worrying aspects are attacks on critical infrastructure, convergence of actors and triple-dip attacks**
- **Social engineering, including phishing, remains one of the main attack vectors**

Main Takeaway Points

- **Cover the basics – cyber hygiene including steps that are relatively easy to implement (e.g. password policy – MFA, monitoring of privileged accounts, blocking remote access/ports, AV software, blocked lists, …)**
- **Be prepared – regular training and awareness raising, technical measures and governance (penetration testing, batch & vulnerability management, backup strategies, ...) and incident response**
- **Know your enemy - information position and risk management (risks specific to your industry, darkweb offerings, data leaks, technology watch function, …)**

Main Takeaway Points

- **Cyber threats and cybercrime at scale require a networked response, including prevention and awareness – joint responsibility (#SafetyTech)**

- **Cooperation is key (e.g. NMR, improved situational awareness) – involve law enforcement!**

How high can you build your walls in cyberspace…?

Rechtliche Hinweise

Die Kapitalmarkt Consult KCU GmbH (KCU) ist eine im Firmenbuch des Handelsgerichts Wien zu FN 449855 b eingetragene Gesellschaft mit beschränkter Haftung.

KCU wie auch der Vortragende übernehmen keine wie immer geartete Haftung für die Richtigkeit, Vollständigkeit und Aktualität der in dieser Präsentation enthaltenen Informationen sowie der im Rahmen des Vortrags seitens des Vortragenden getätigten Aussagen. Die Inhalte stellen lediglich eine Themenauswahl dar. Auch die in der Präsentation aufgezeigten Gefahren- bzw. Haftungspotenziale stellen lediglich eine Auswahl möglicher solcher Potenziale dar. Irrtümer vorbehalten.

Thank you!

www.europol.europa.eu

Denn Wissen hat Wert.

www.kapitalmarktconsult.at