Kaspersky Industrial Cybersecurity Conference 2024

TOP Cyberthreats to Operational Technology

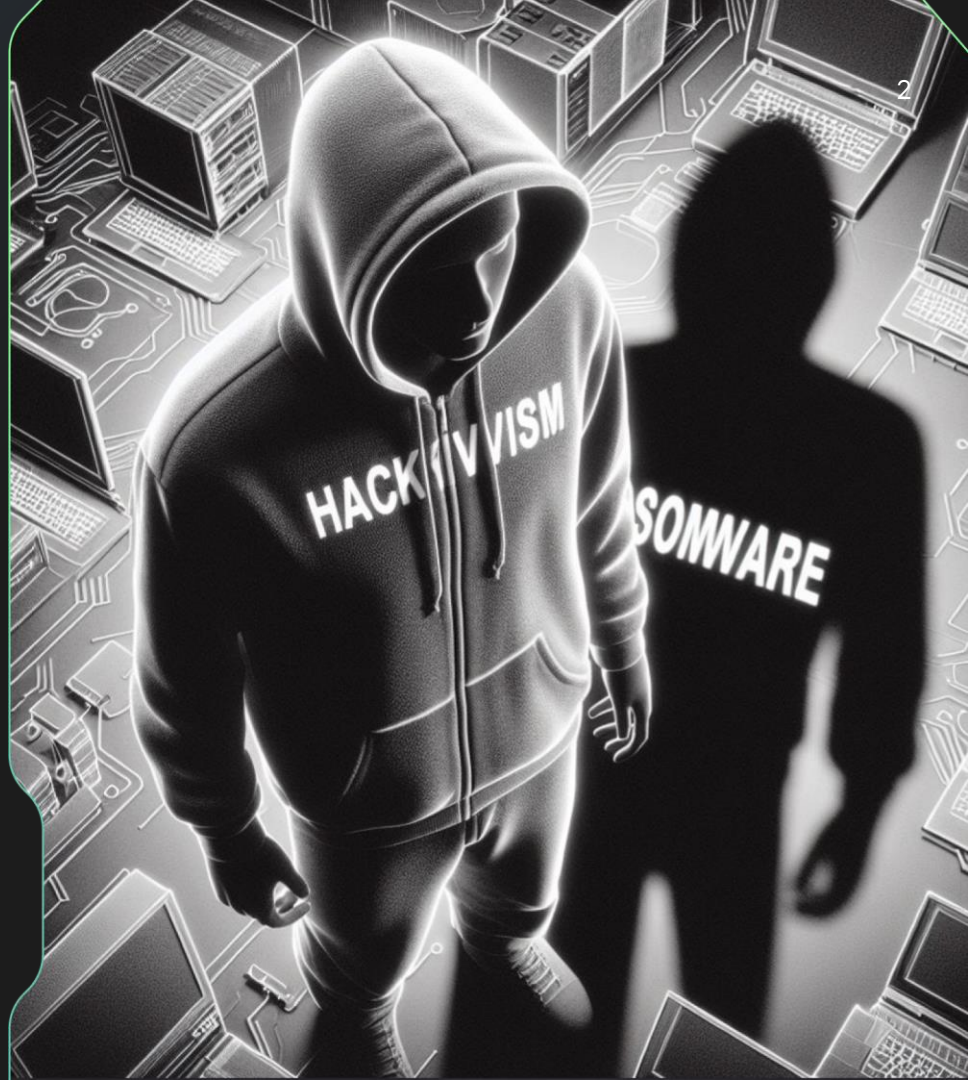
What we see now
and what to expect

kaspersky

Main Cyber Threat

for Industrial enterprises & OT environments –

> … a “traditional” **ransom attack on IT infrastructure**
>
> …or **hacktivism**?



Hacktivism

- political motives
- commodity tools
- ransomware as a part of toolsets
- it may involve insiders and utilize supply chain / trusted partner attack vectors

Example #1

Attack on Unitronics (rebranded) HMI/PLC (all in one)

160

households cut from water supply in Drum/Binghamstown area of Erris, Ireland.

Example #2

A devastating cyber attack scenario?
The Reality..

70%

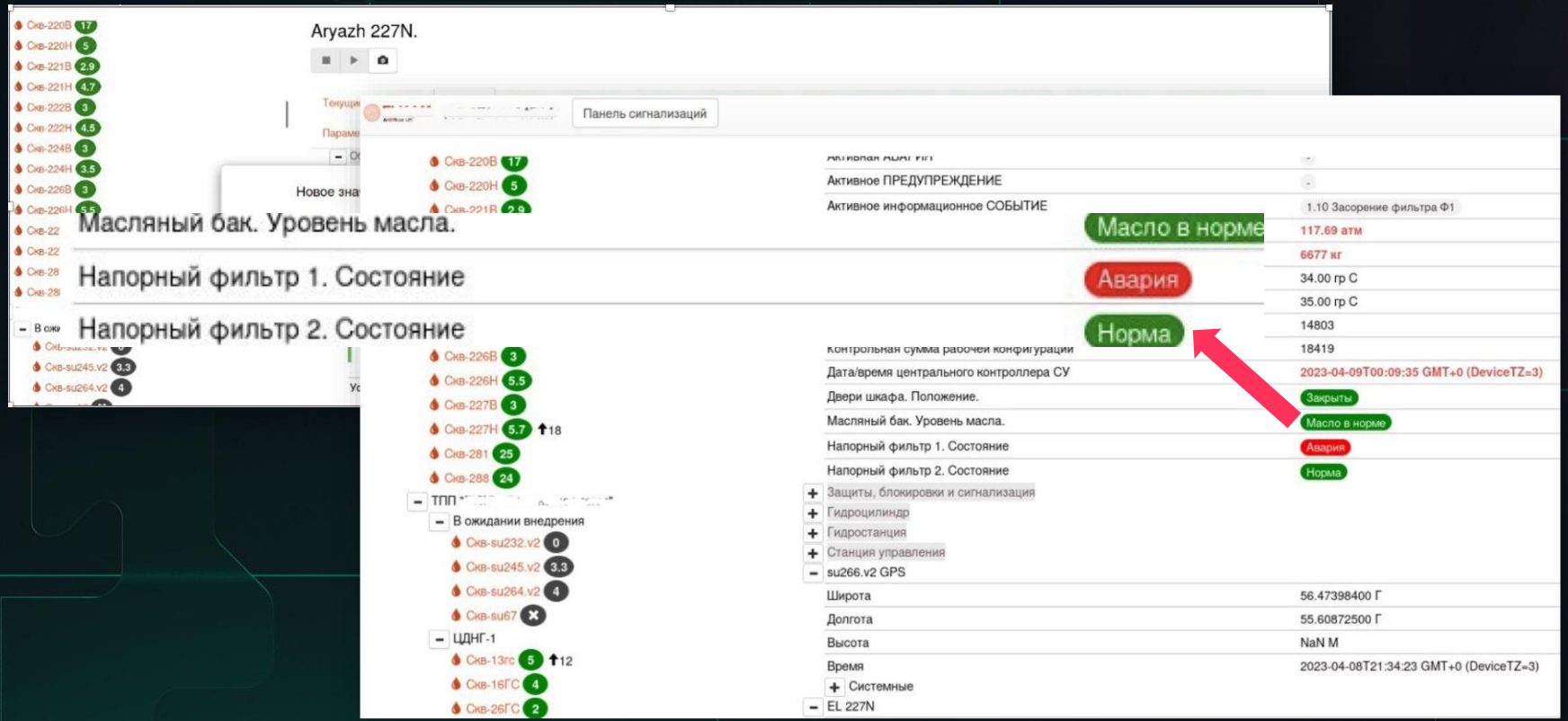
of Iranian gas stations out of service

Example #3

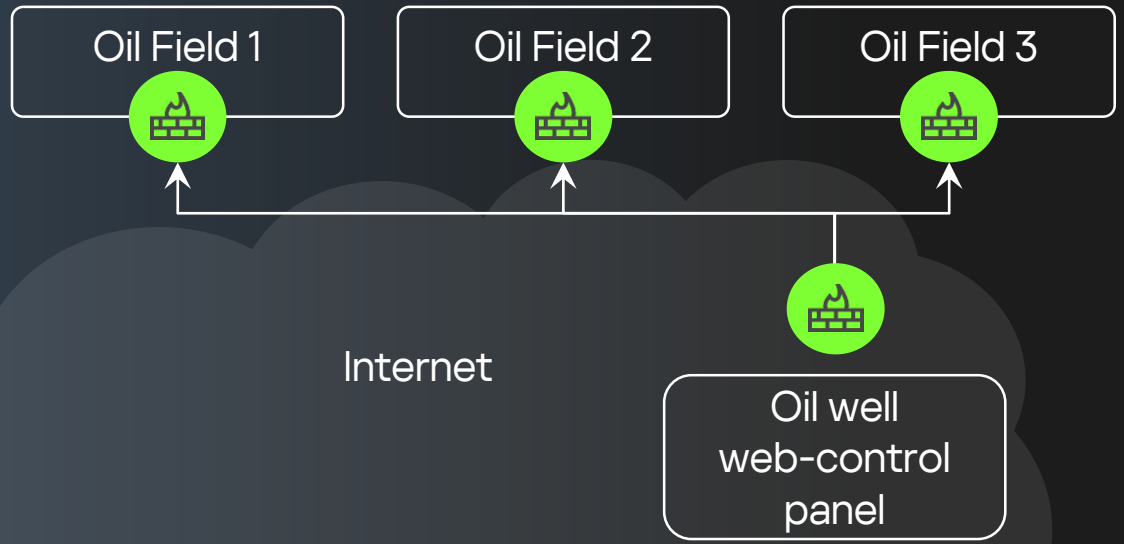
Attack on Oil & Gas vendor / service provider ..

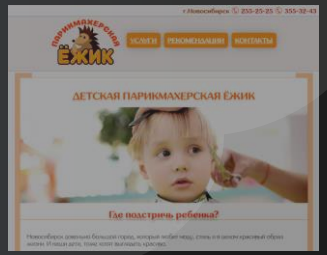
Pumps stopped at multiple oil fields operated by several oil and gas companies

What happened?



What happened?





The pannel was hosted at a public hosting,

...sharing infrastructure with consumer-oriented srvices

26 SQL Injection 0-day vulnerabilities.

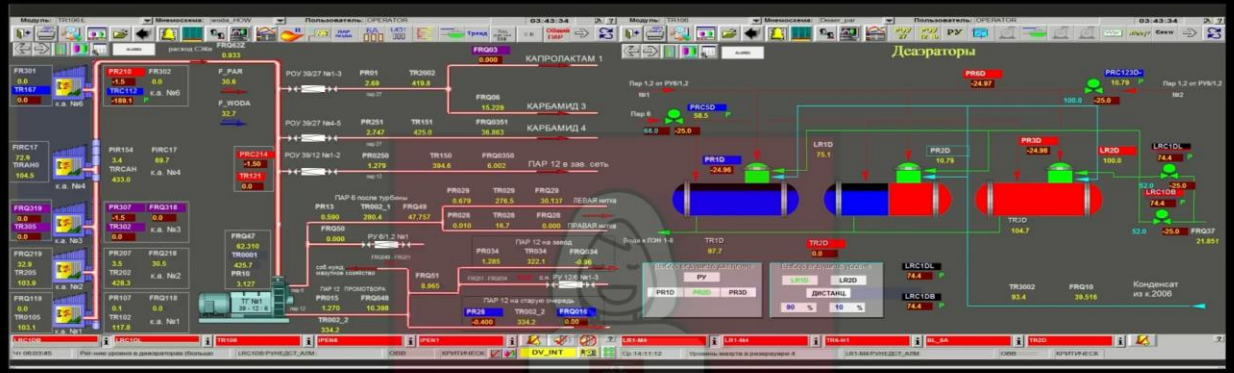
One of wich lead to the pannel full compromise

Example #4

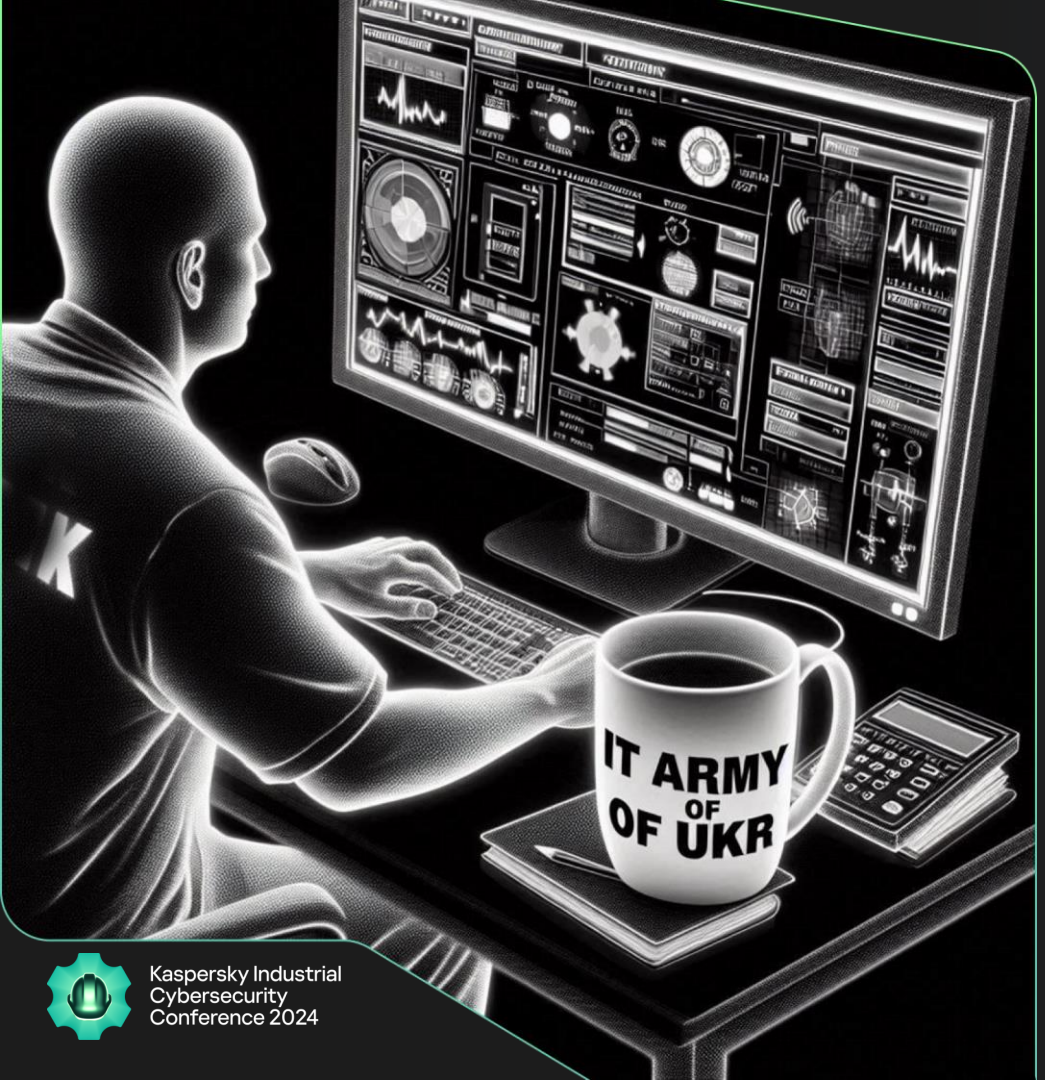
Attack on fertilizers production

Attackers accessed SCADA at the boiler control room and switched the boilers off

What happened?



Управляем котельным цехом



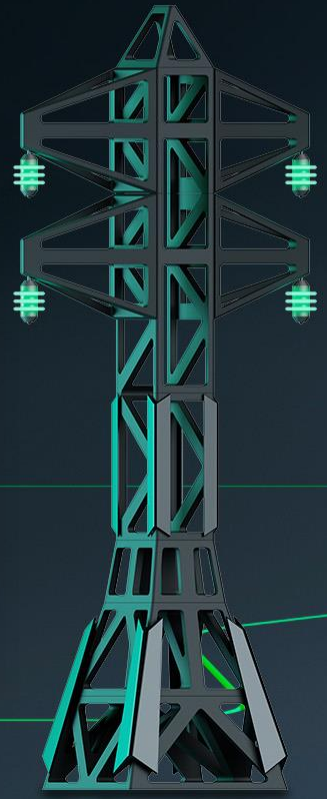
Example #5

Attack on metal production facility

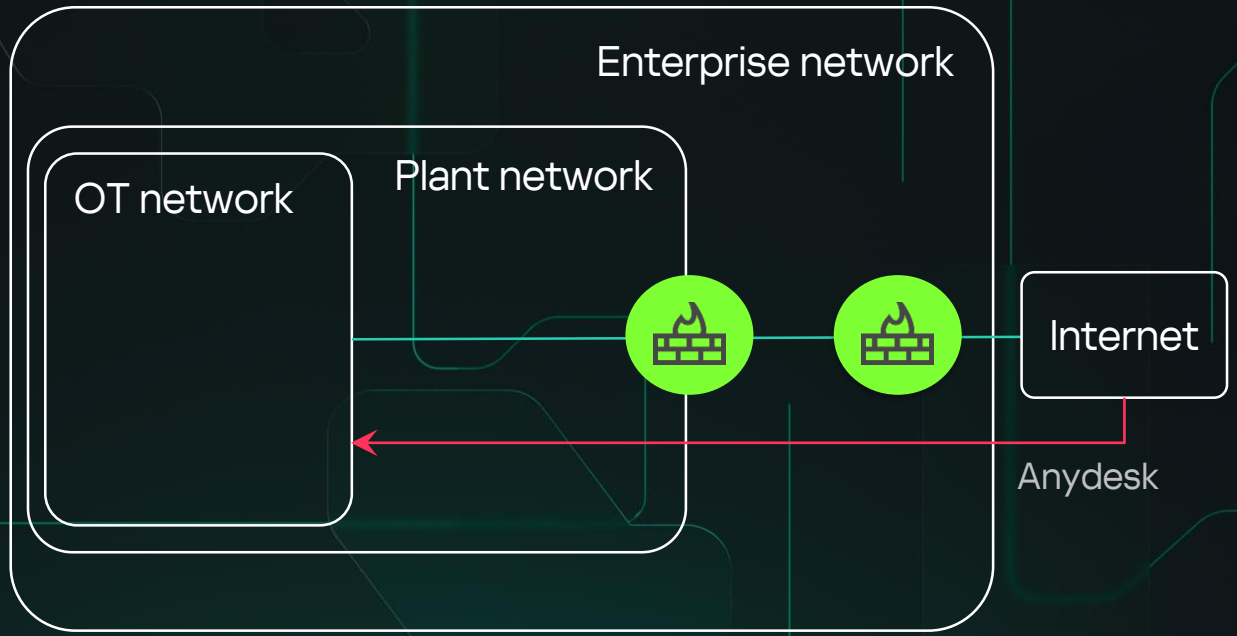
Insider on the supplier side accessed SCADA at the gas piston powerplant and started changing the setpoints in attempt sabotage

What happened?

IT Security team of the enterprise detected abnormal amounts of outbound traffic from the gas piston power plant supplying electricity to one of the enterprise facilities

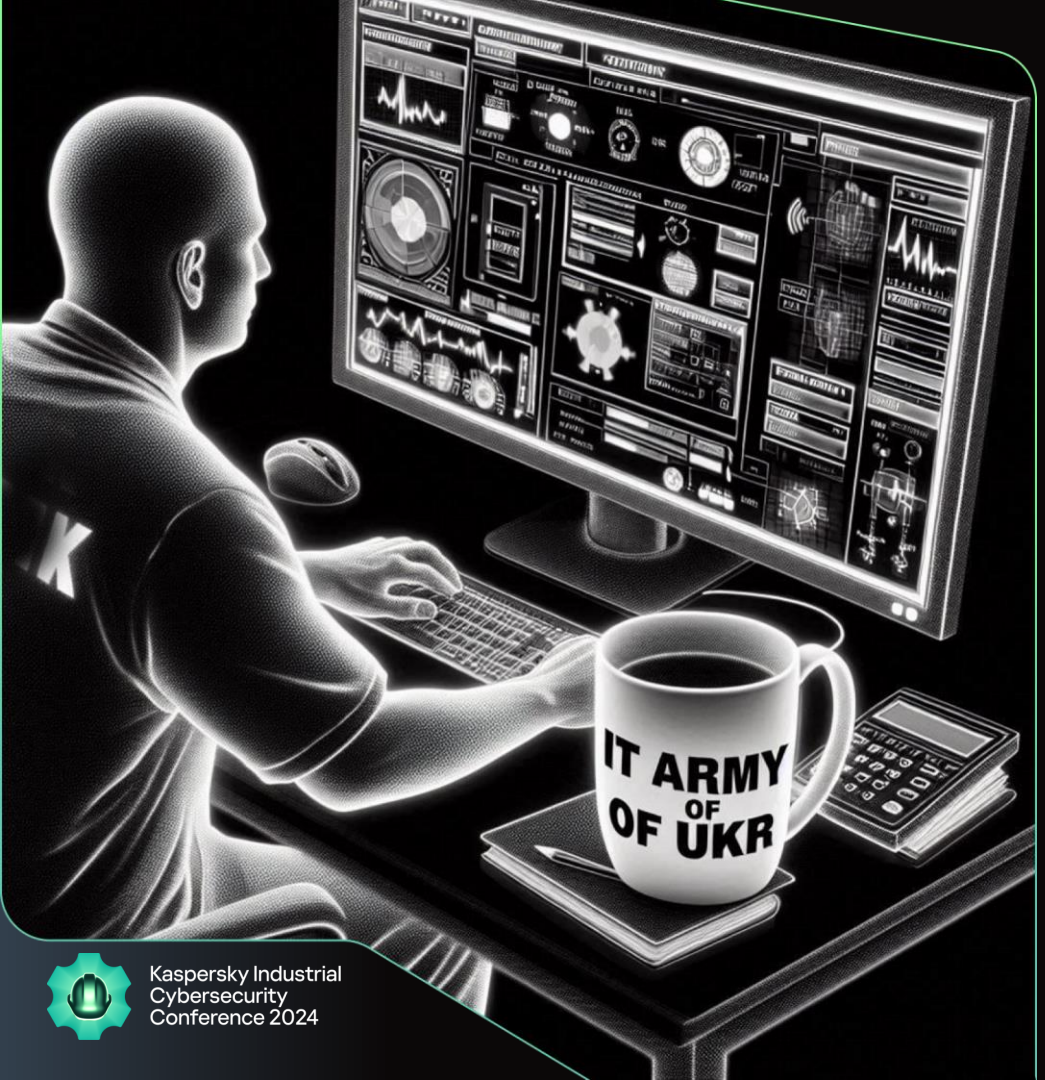


What happened?



Insider at the trusted partner side used remote access to infect SCADA server with malware for DDoSing governmet-relatyed resources

When detected he connected the server in a sabotage attempt



...An important note on cybersecurity implications of AI...

Ransomware

- cosmopolitical cyber-crime
- balanced ecosystem
- growing market

Example #1

A devastating cyber attack scenario?

40%

of Australian container shipment blocked

30 000

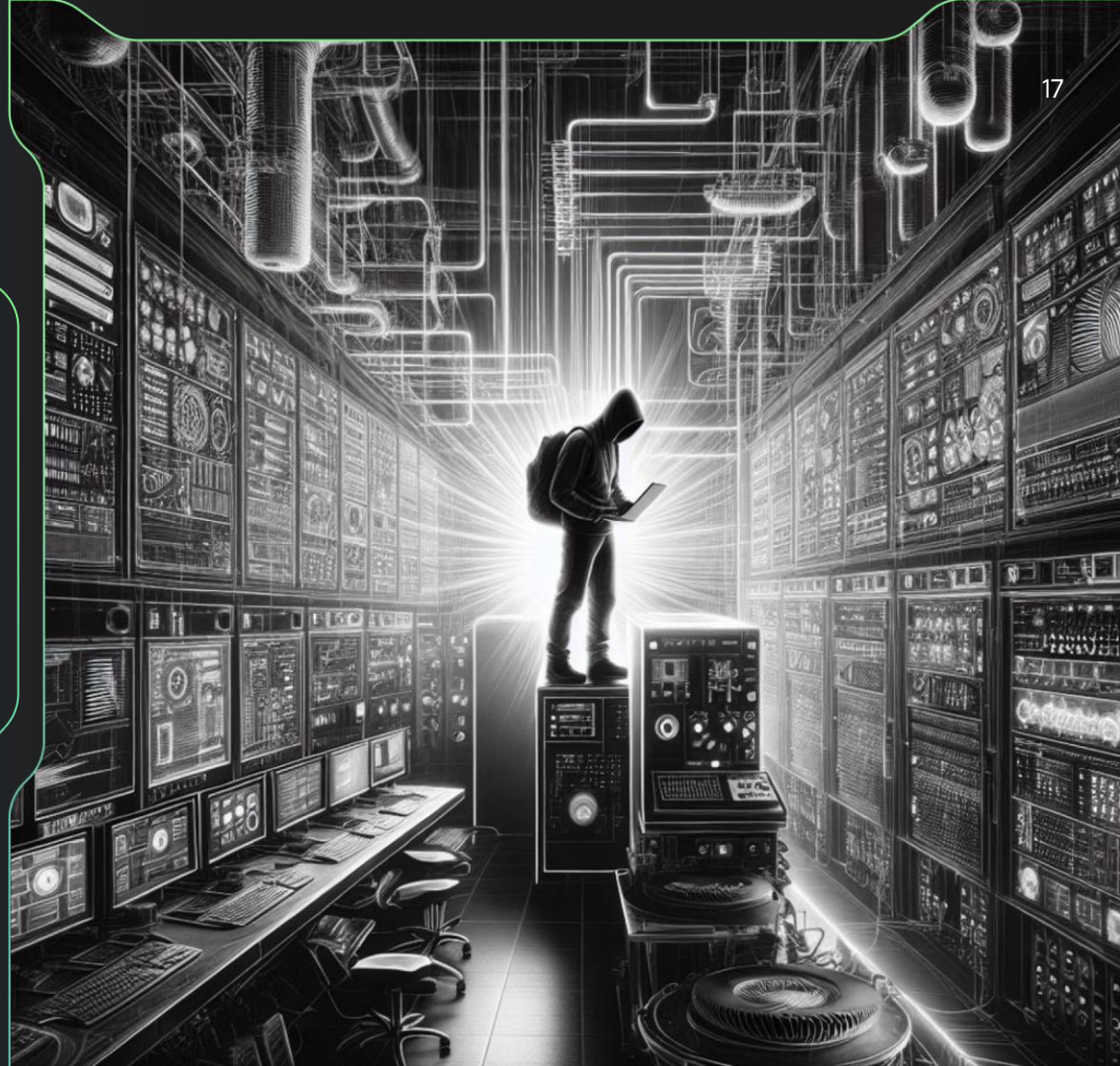
containers got stuck in 4 main ports

Example #2

Attack on Jonson Controls (HVAC equipment producer)

$27M

estimated loss

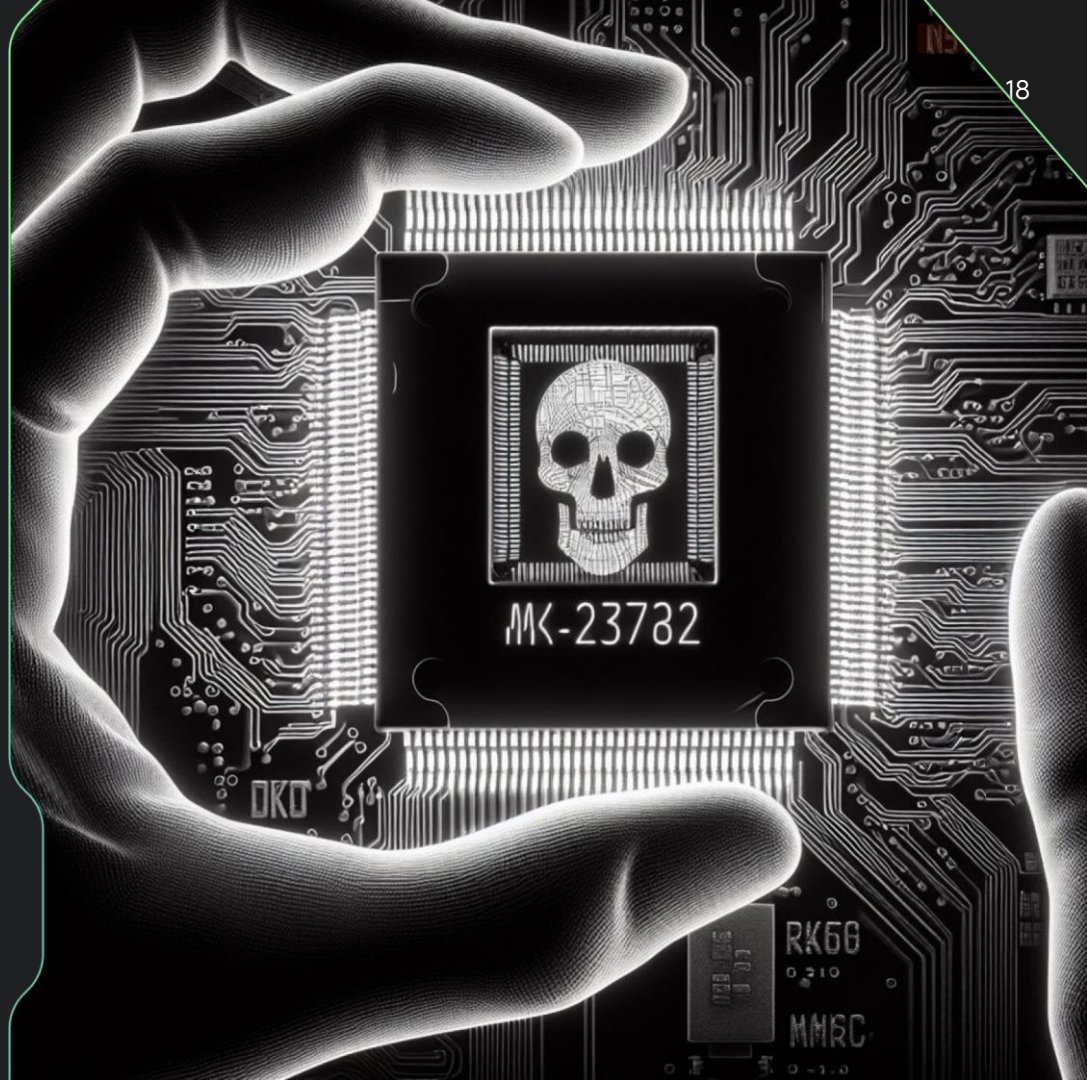


Example #3

Attack on MKS Instruments (chip maker)

$200M

estimated loss



Example #4

Attack on Clorox (chemicals)

$356M

estimated loss

Ransomware

Example #2

Attack on CDK Global
(SaaS for car dealerships)

$1.02B

estimated direct losses

Ransomware

Example #2

Attack on CDK Global
(SaaS for car dealerships)

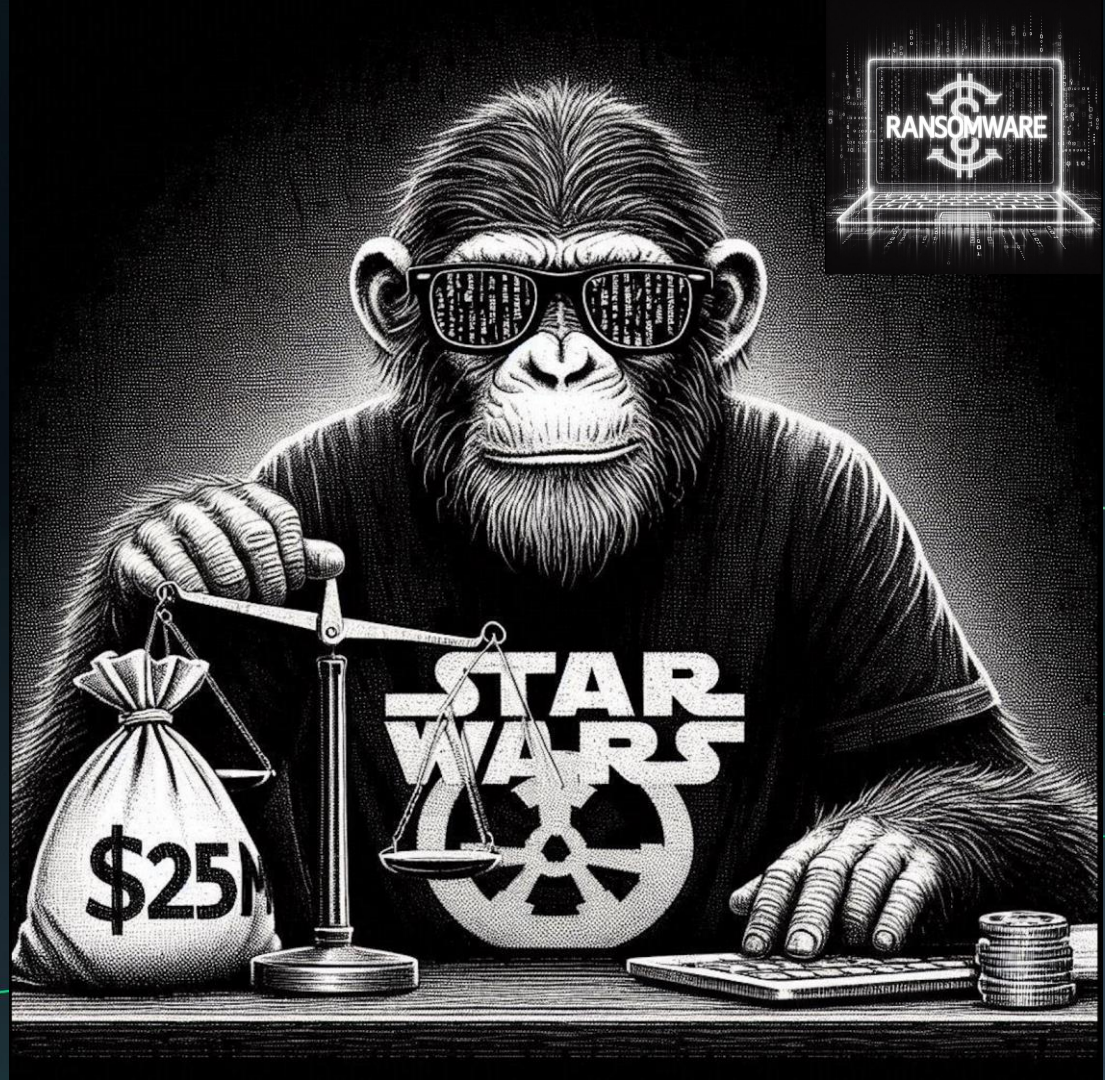
15K dealerships halted

56K cars not sold

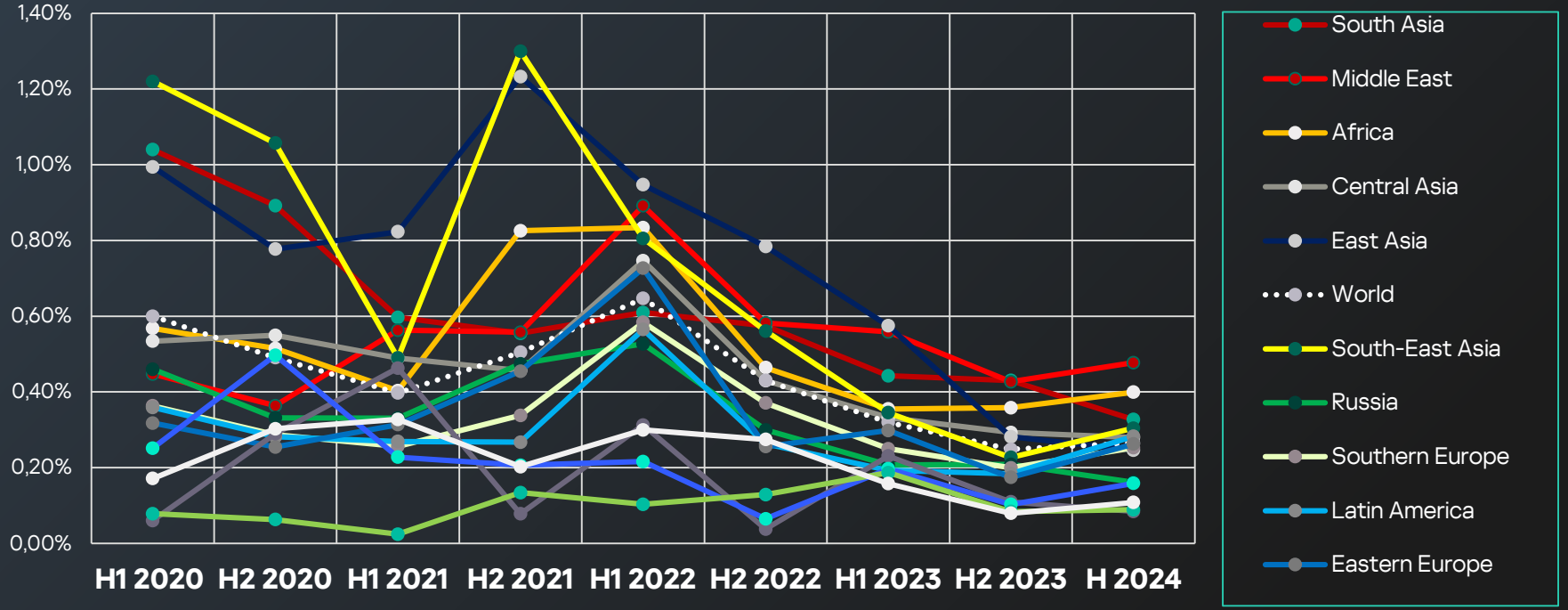
Ransom attack efficiency?

Unproportional and poorly controlled damage

$25M ransom for $1B damage

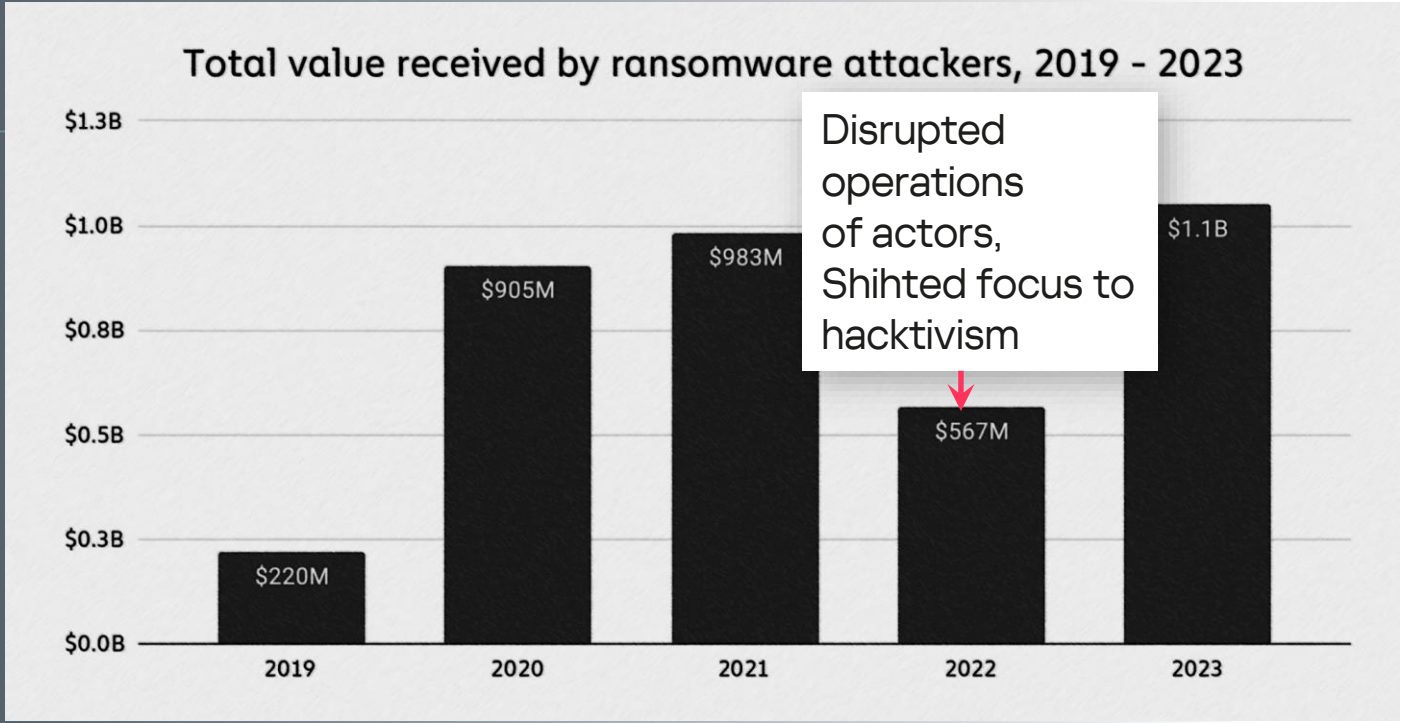


Exposure of OT infrastructures to the ransomware threat for the Worlds' regions goes generally down

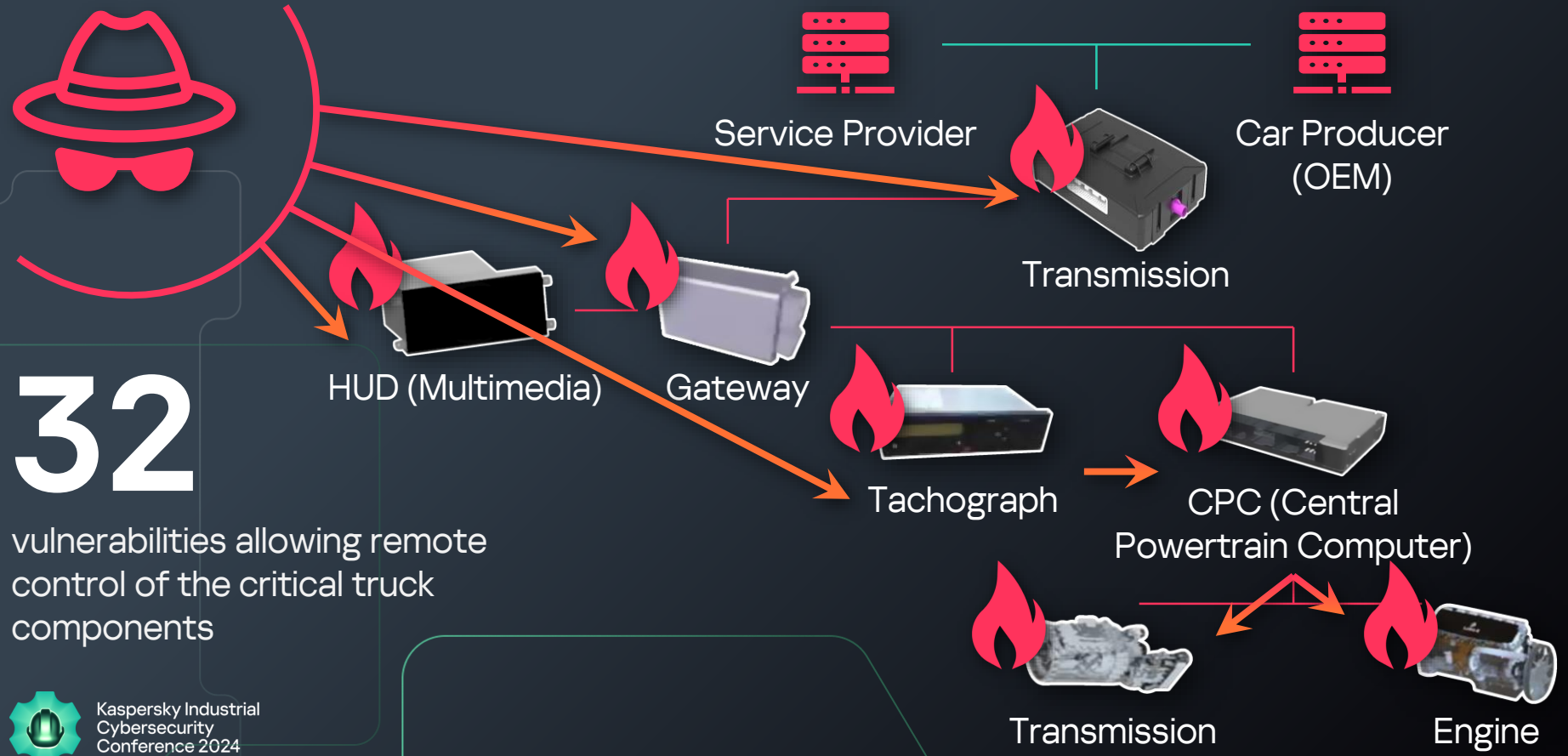


Ransomware market: highly dependent on geopolitical situation and on law enforcement activities, may reach its plateau or experience drop down in 2024-2025

chainalysis.com/blog/ransomware-2024/



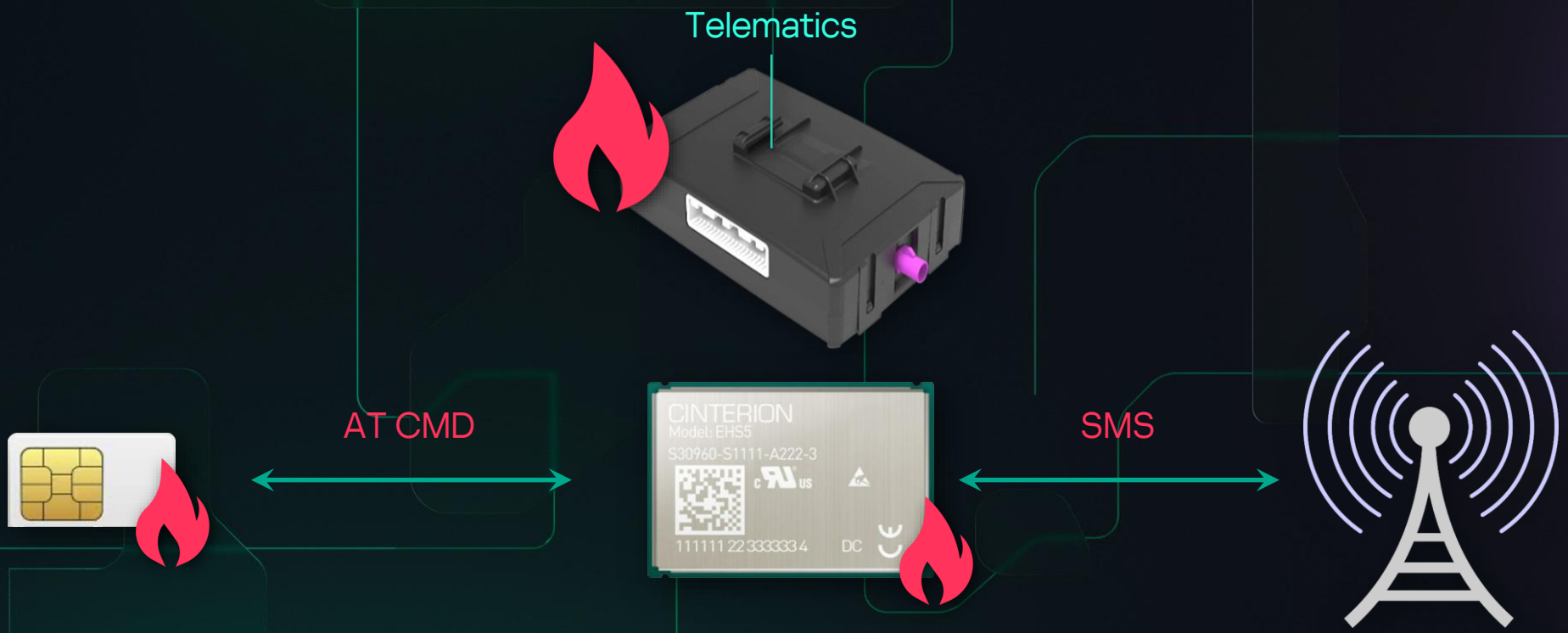
...and is a ”die-hard-4” cyberattack scenario just a matter of time...?



32

vulnerabilities allowing remote control of the critical truck components

...and all because of a vulnerability...



https://ics-cert.kaspersky.com/publications/reports/2024/06/13/cinterion-ehs5-3g-umts-hspa-module-research/

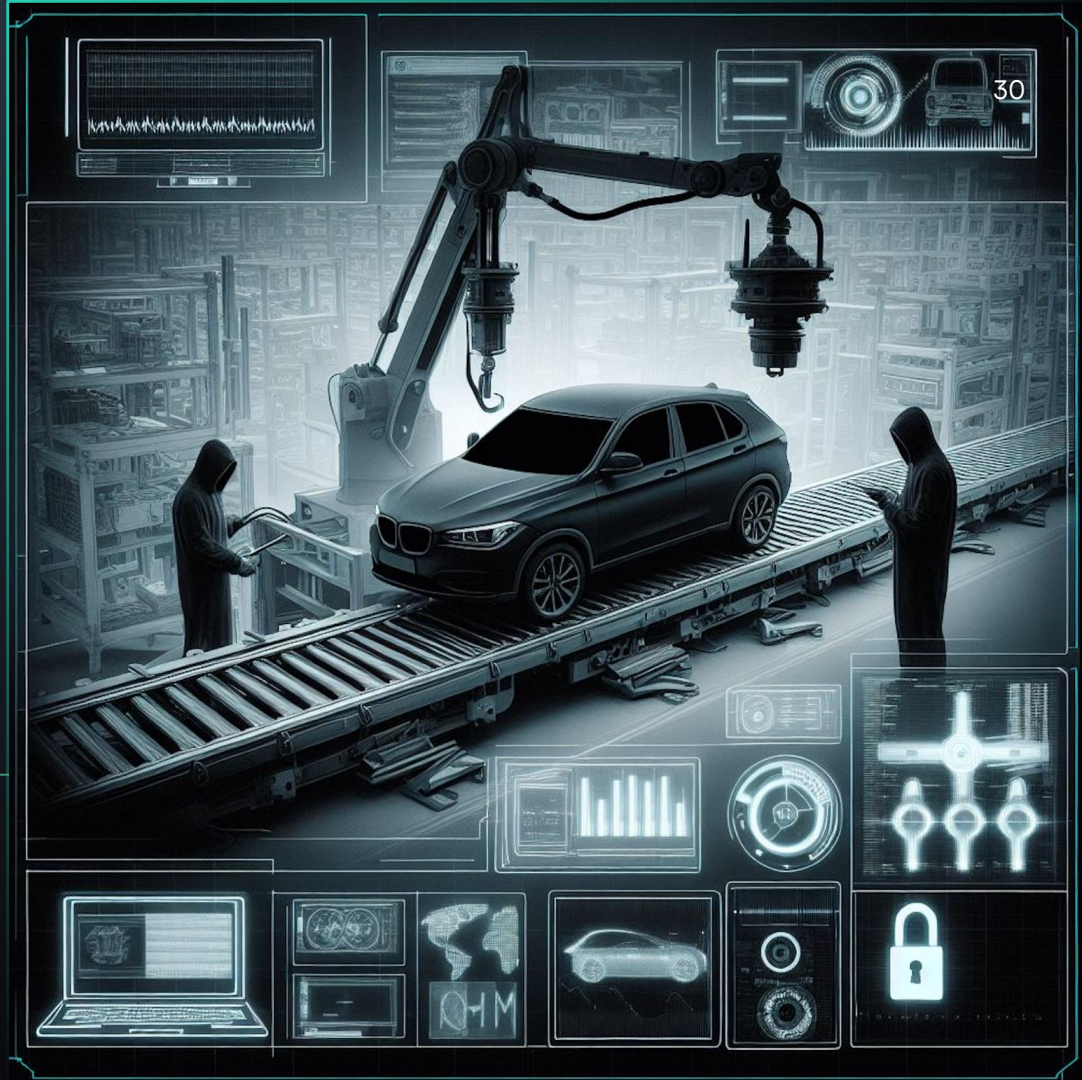
...voila... We are now in full remote control of the truck...

And, if we know their SIM card IDs, of all other vehicles of this kind

...cyberattacks locking vehicles, ships and parts of remote OT infrastructure

...so what to expect?

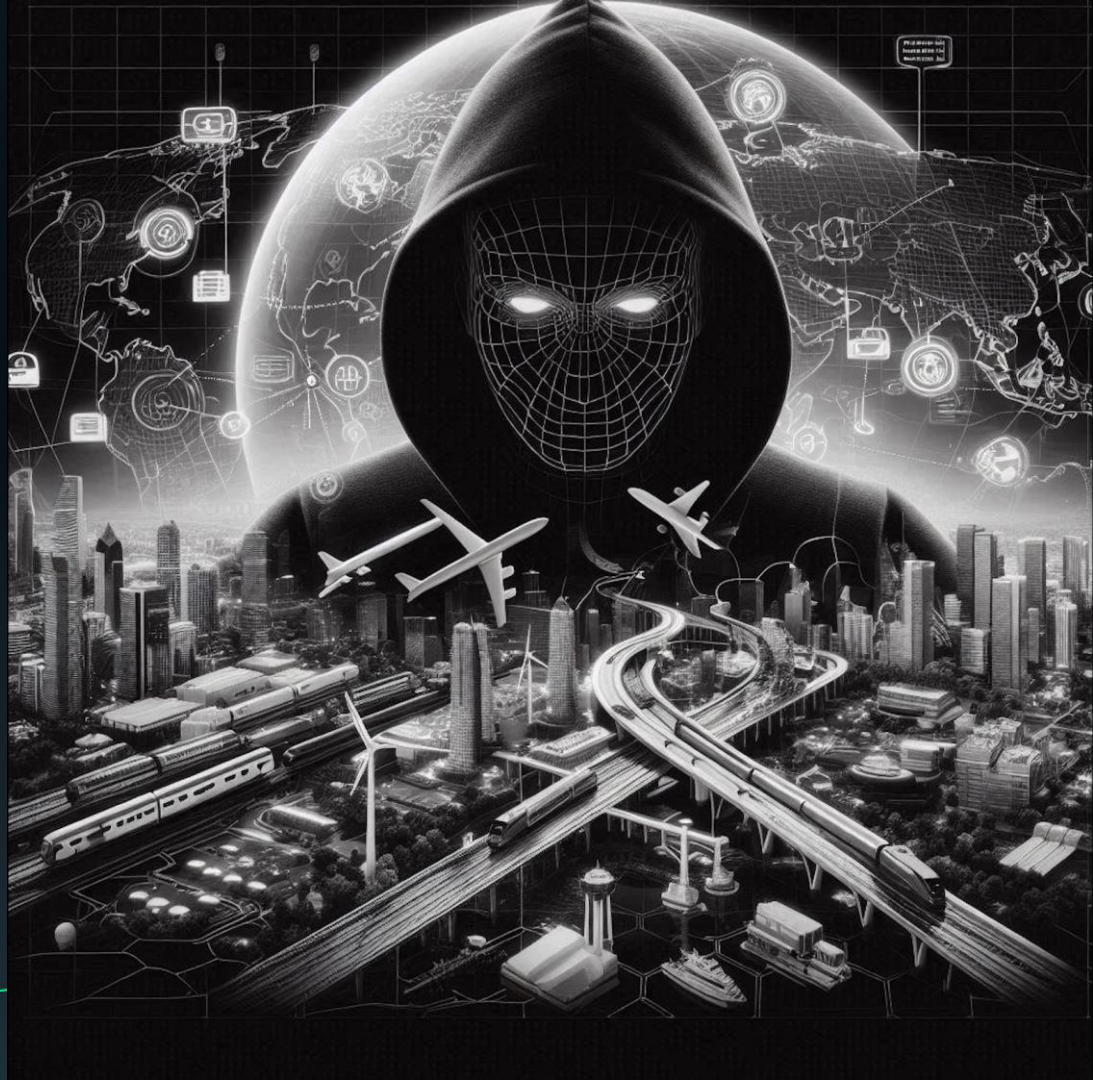
...increased likelihood of physical consequences of traditional attack scenarios



...greater intertwining of cyber- and traditional crime

APT

- Insiders, firmware 0-days, hardware implants and MITM on telecom side
- Maintain stealthy persistence in all CI sectors
- Propagate to peer organizations
- Spy
- Rare or no cyber-physical operations



Thank you!

Evgeny Goncharov

Head of Kaspersky ICS CERT

ics-cert.kaspersky.com

kaspersky