Cyber Security and Society: a pre-war reality check

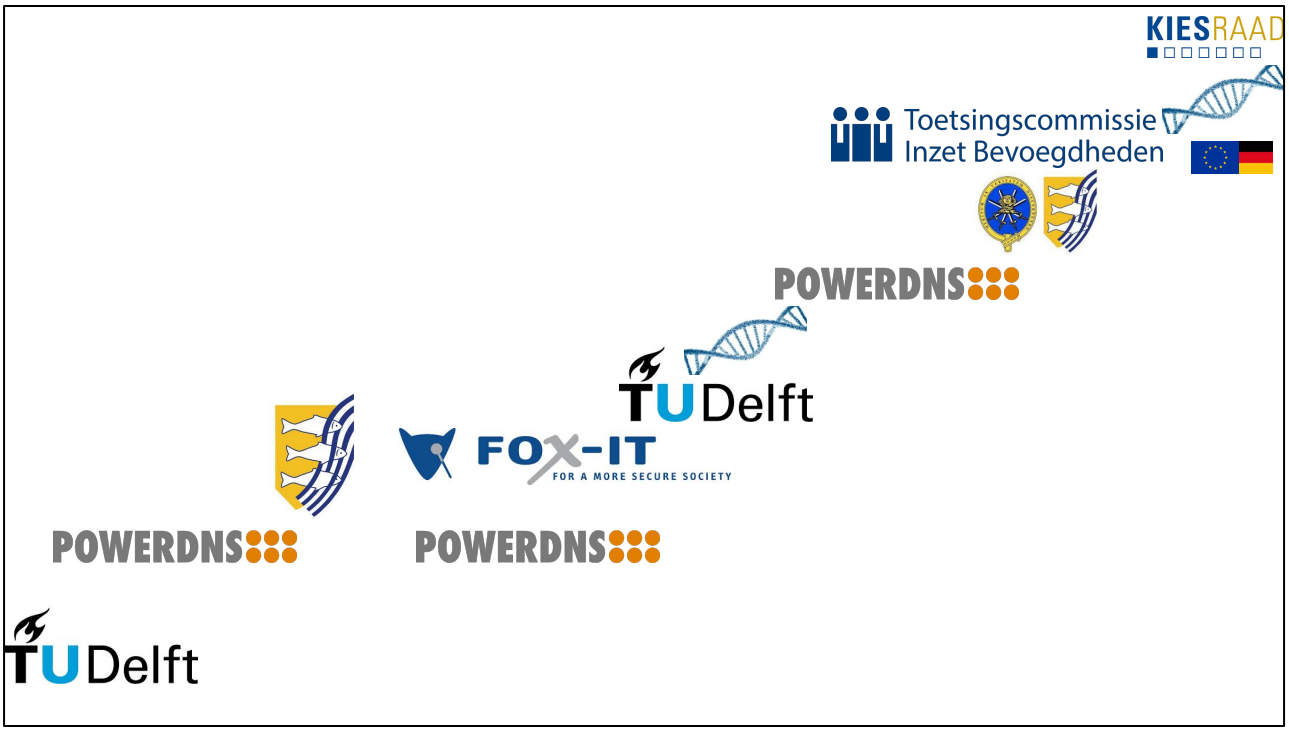
Bert Hubert / bert@hubertnet.nl
https://berthub.eu/prewar

First some important words from Donald T.

“I know it sounds devastating but we have to get used to the fact that **a new era has begun: the pre-war era**.”

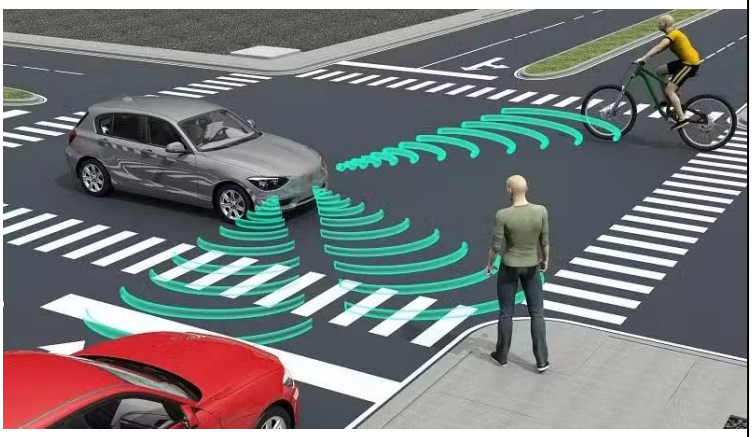
“When **Donald Tusk** was Polish prime minister for the first time, from 2007 to 2014, he said few other European leaders beyond **Poland and the Baltic states** realised Russia was a potential threat.”

https://edition.cnn.com/2024/03/29/europe/poland-tusk-europe-pre-war-russia-ukraine-intl/index.html



Things I have done - only interesting to put my (strong) claims on later pages in context. I failed in my studies of physics, launched an unsuccessful startup (PowerDNS), and when that did not go well joined Dutch intelligence & security agency AIVD. From there I went on to develop software for police and intelligence agencies, while PowerDNS went on. After Fox-IT I did DNA research in Delft again, and then focused on PowerDNS again. After that, I became a regulator of Dutch intelligence services for 2 years. During this time I managed to get my DNA paper published in Nat. Scientific Data.
https://www.nature.com/articles/s41597-022-01179-8

This committee that regulates the Dutch intelligence and security agencies is/was unique in that it employs technical specialists at the heart of a place that in most countries only features lawyers. If you work at a department that studies policy and technology, this should warm your heart!
https://www.politico.eu/article/intelligence-watchdog-bert-hubert-netherlands-hacking-cyber-law/ has some stuff on this committee.

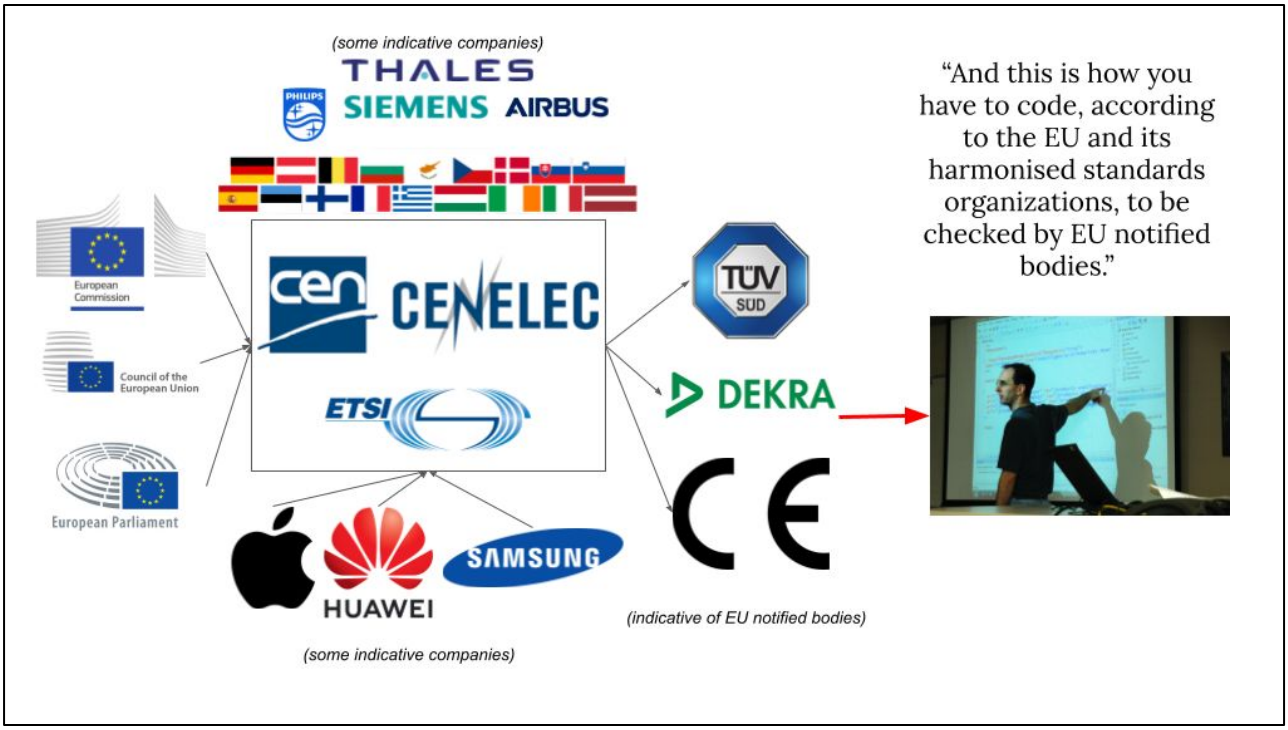


https://www.drive.com.au/news/tesla-hit-and-run-driver-to-stand-trial-for-crash-blamed-on-autopilot/

In this book, Brenno argued that we will not take cyber security serious until we get a really big disaster. Before the Titanic, everyone could build a ship. For a “Titanic” event, Brenno suggested self driving cars being reprogrammed to not avoid pedestrians but drive over them

- Cyber Security Act
- Cyber Resilience Act
- Cyber Solidarity Act
- Digital Operational Resilience Act (DORA)
- NIS2 Directive
- Product Liability Directive
- .. and they aren't done yet

https://berthub.eu/articles/posts/eu-cra-secure-coding-solution/ - Brenno was not entirely right, we are now getting legislation with bite



Brief ad, if you can contribute to standardisation of cyber, do contact CEN/CENELEC or your local branch (NEN etc)

Stuxnet

On 24 February, a cyber-attack against Viasat began approximately 1 hour before Russia launched its major invasion of Ukraine. Although the primary target is believed to have been the Ukrainian military, other customers were affected, including personal and commercial internet users. Wind farms in central Europe and internet users were also affected.

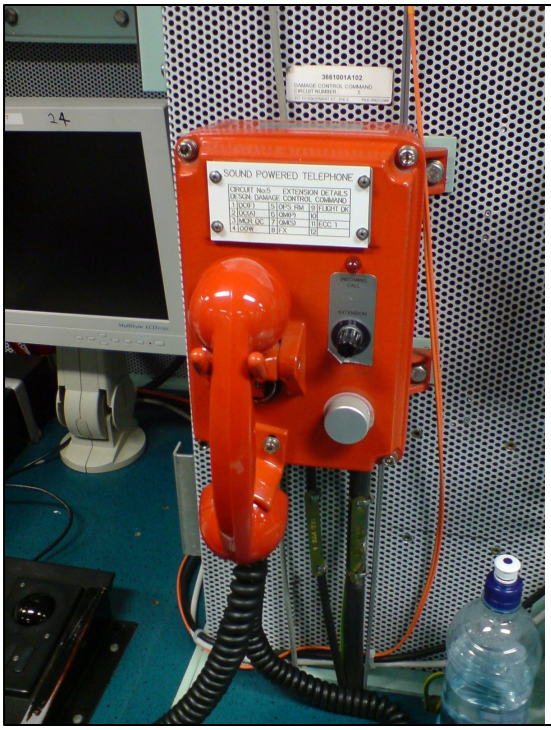
Viasat has said that "**tens of thousands of terminals have been damaged, made inoperable and cannot be repaired.**"

https://en.wikipedia.org/wiki/Viasat_hack

When times are bad, you are (much more) on your own!

- ROBUST: **Does not fall over by itself**
- LIMITED/KNOWN DEPENDENCIES: **Does not need too much unknown stuff too far away**
- OWNERSHIP/UNDERSTANDING: **If things break, you can improvise or fix things**

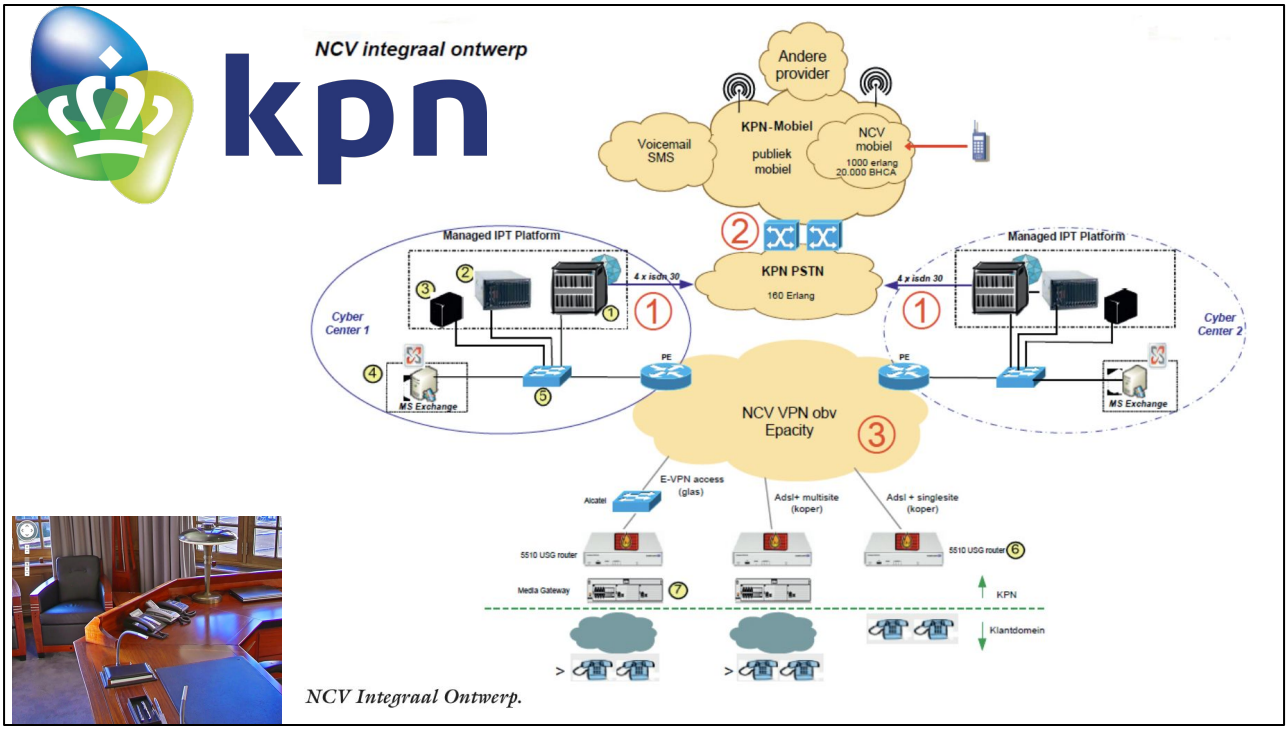
The Key Things



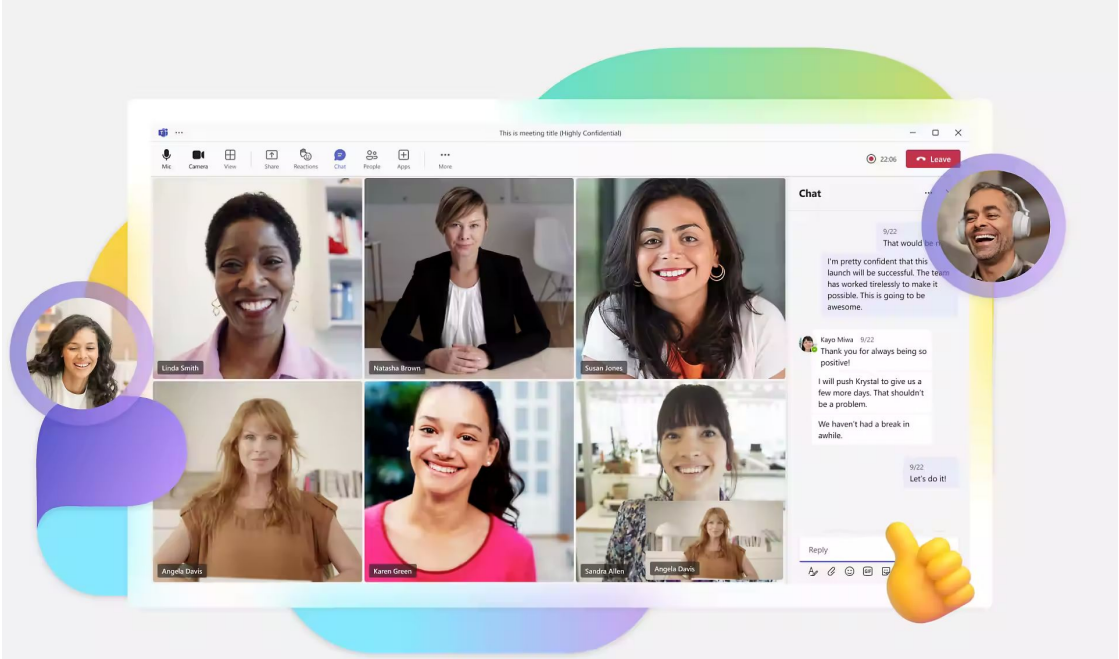
“Many different types of equipment have attempted, **but have largely failed**, to replace the incredibly simple sound-powered telephones on ships. Due to the rugged, reliable and **power-free** nature of this equipment, it remains in use on all US military vessels.”

https://en.wikipedia.org/wiki/Sound-powered_telephone - ALWAYS works. Can do 50 kilometer distance.

https://www.gld.nl/nieuws/8135427/kijken-mag-nu-want-geheime-atoombunker-voldoet-alleen-nog-als-erfgoed

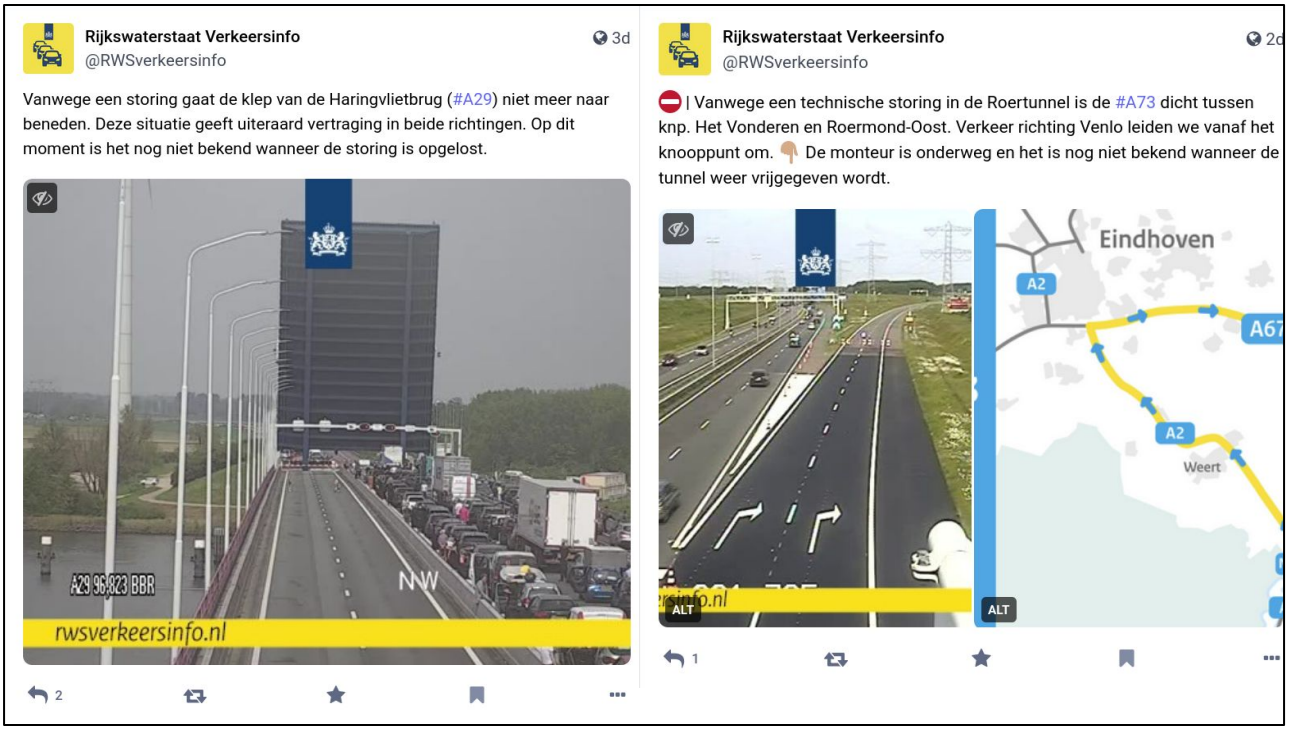


https://vovklict.nl/intercom/2013/1/38__41.pdf -
https://www.nctv.nl/binaries/nctv/documenten/publicaties/2023/03/20/koepelnotitie-crisiscommunicatie-bij-uitval-van-elektriciteit/Koepelnotitie+comm.+elektra.pdf



More like Microsoft M364

The actual government emergency communication platform



What if you can’t call “the engineer”

NOS Nieuws • Vrijdag 14 april 2023, 15:57 • Aangepast vrijdag 14 april 2023, 17:01

Vodafone: storing lijkt opgelost, bellen met 112 weer mogelijk

De landelijke storing bij Vodafone lijkt opgelost. Klanten kunnen volgens de telecomprovider weer mobiel bellen en gebeld worden. Ook 112 is weer te bereiken.

Software Apps

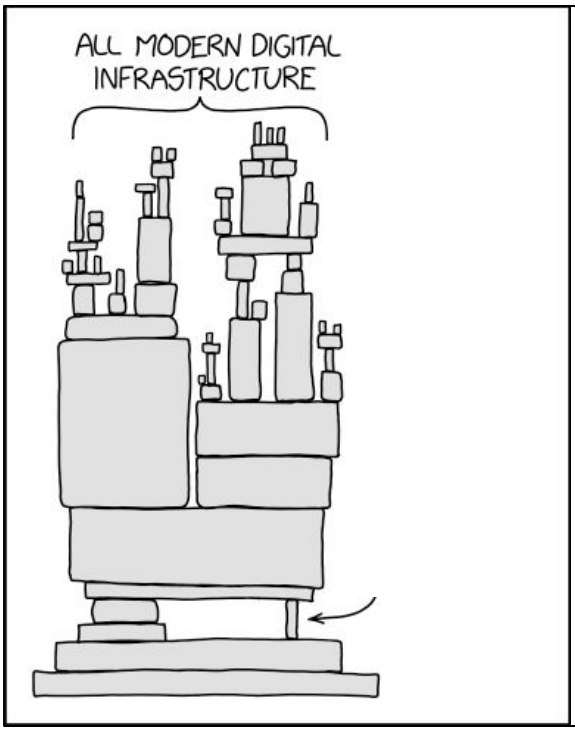
Microsoft 365 was down, stopping people from opening Office, Outlook, and OneDrive (Update)

News By Sean Endicott published September 6, 2023

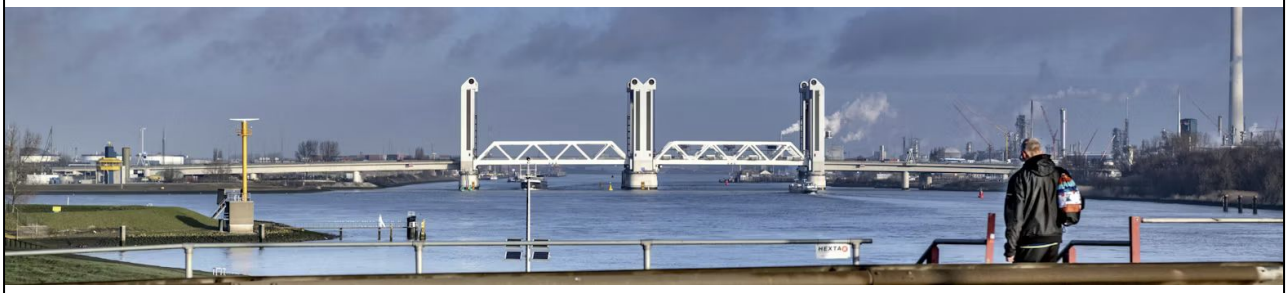
A Microsoft 365 outage could cause a stressful start to your workday.

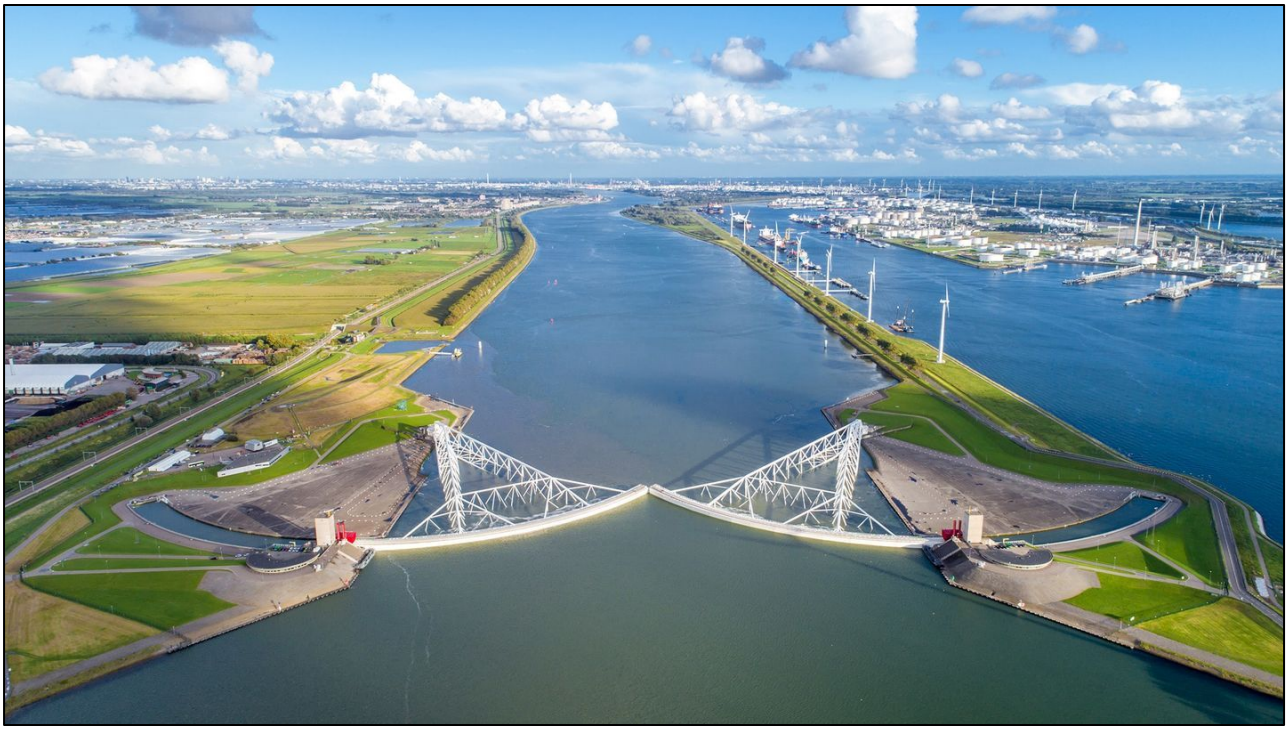
Comments (0)

More like M364



The stack is too high!


HEXTAG



So where are we?

Also see: berthub.eu

5G: The outsourced elephant in the room

Jan 20 2020

> *This article is part of a series on (European) innovation and capabilities.*

In a break from the usual GPS/Galileo, DNA and C++ posts, here is a bit on 5G and national security. It turns out that through PowerDNS and its parent company Open-Xchange, we know a lot about how large scale European communication service providers work - most of whom are our customers in some way.

In addition, in a previous life I worked in national security and because of that I have relevant knowledge of how governments (your own and foreign ones) "interact" with telecommunication providers. So what follows is based on lived experience.

Note: this article is mostly about Europe. Considerations and conditions in the US and the rest of the world are very different.

Telecommunication is what makes the world go round, and with everything moving to the cloud, any breakdown would severely disrupt our economy and safety. So it makes sense to think hard about this vital service to our society.

https://berthub.eu/articles/posts/5g-elephant-in-the-room/

‘Any worries about “the Chinese” being able to disrupt our communications through backdoors ignore the fact that all they’d need to do to disrupt our communications.. **is to stop maintaining our networks for us!**’ (2020)

https://berthub.eu/articles/posts/5g-elephant-in-the-room/


Google
aws


Google
aws
HUAWEI
Infosys
TECH
mahindra
wipro
Kalaallit Nunaat
Canada
Ísland
Føroyar
Norge
Eesti
Danmark
Nederland
Luxembourg
France
Andorra
Malta
Algérie
Cabo Verde
Niger
Ghana
Guinea Ecuatorial
Saint Helena, Ascension and Tristan da Cunha
Angola
Burundi
Malawi
Zimbabwe
Namibia
South Africa
Seychelles
Mauritius
Россия
Беларусь
Қазақстан
Монгол
Cambodia
Malaysia
Indonesia
Guam
Belau
Papua New Guinea
Marshall Islands
Nauru
Solomon Islands
Vanuatu
Australia
Norfolk Island
New Zealand
México
Cuba
Haiti
Guatemala
Aruba
Panama
Colombia
Ecuador
Perú
Brasil
Bolivia
Paraguay
Chile
Argentina
Pitcairn Islands
Falkland Islands (Malvinas)
South Georgia and South Sandwich Islands


Nunaat
Ísland
Norge
Suomi / Finland
Sverige
Россия
United Kingdom
Беларусь
Deutschland
Україна
Қазақстан
France
România
Italia
España
Ελλάς
Türkiye
Türkmenistan
O'zbekiston
العراق
ایران
افغانستان
پاکستان
Algérie
الجزائر
ليبيا
مصر
السعودية

NOS

NOS Nieuws • Zondag 11 februari, 18:04

Tienduizenden computersystemen kwetsbaar voor inbraak

Joost Schellevis
redacteur Tech

Vele tienduizenden computersystemen wereldwijd, en duizenden in Nederland, zijn kwetsbaar voor cybercriminelen en inlichtingendiensten. Dat blijkt uit een inventarisatie van de NOS. Het gaat hierbij om computersystemen waarvan bekend is dat ze onveilig zijn, maar die niet worden voorzien van een oplossing.

Waarom moet JOOST dit doen?? Dit is heel laaghangend fruit. Te vinden als bijbaan. En toch blijft het maar zo.

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Nieuwe malware benadrukt aanhoudende interesse in edge devices

Nieuwsbericht | 06-02-2024 | 15:45

Tijdens een incident response onderzoek, door de Militaire Inlichtingen en Veiligheidsdienst (MIVD) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), is er op een aantal FortiGate-apparaten nieuwe malware aangetroffen. Dit benadrukt een trend waar interesse wordt getoond in publiek benaderbare edge devices. In de publicatie bieden de MIVD en AIVD inzicht in deze malware. Tevens bieden wij in dit bericht handelingsperspectief om de risico's van deze malware te beperken.

Een van de zeldzame gevallen waarin de Nederlandse overheid bekende gehackt te zijn. Wel goed dat ze dit deden, en ook de leverancier bekend maakten.

toegang verkrijgen tot systemen maar om toegang te behouden. De aanvankelijke toegang was te verkrijgen door de kwetsbaarheid in FortiGate met het kenmerk CVE-2022-42475 te misbruiken. Het NCSC heeft deze kwetsbaarheid in december 2022 ingeschaald als hoge kans en hoge impact.

Duiding

De MIVD en AIVD stellen dat deze aanval past binnen een bredere trend. Zowel het NCSC als partnerorganisaties zien een trend in het misbruik van kwetsbaarheden in publiek benaderbare *edge devices* zoals firewalls, VPN-servers, en e-mailservers. Edge devices vormen een interessant doelwit omdat deze componenten zich aan de rand van het netwerk bevinden en geregeld een directe verbinding hebben met het internet. Edge devices worden vaak niet ondersteund door Endpoint Detection and Response (EDR) oplossingen. Dit maakt dat malafide of afwijkend gedrag moeilijk te detecteren is. In eerdere publicaties over verhoogde scanactiviteiten, Fortigate VPN, Pulse Secure en recentelijk Ivanti Connect Secure, wordt hier dieper op ingegaan.

Men noemt hier diverse andere leveranciers waar je mee op moet passen. Zijn klinkende namen.

NOS

Overheden worden permanent gehackt en dat weten ze, maar daar zeggen ze meestal niet zoveel over.

— Bert Hubert, ex-toezichthouder inlichtingendiensten

Al vaak lek

Hubert noemt het "wel gek" dat Defensie nog steeds gebruikmaakt van het product van het bedrijf Fortinet, waarover het gaat in het rapport. "Dat is een bedrijf dat al zo vaak lek is gebleken: in 2023 180 keer. Dat is heel raar, want die producten zijn juist bedoeld om je te beschermen tegen aanvallen."

Hij vindt het dus vreemd dat de overheid nog vertrouwen heeft in Fortinet. "Het is alsof je een slot op je fiets plaatst dat er juist voor zorgt dat 'ie gestolen zal worden."

Vreemd genoeg blijft iedereen deze lekke spullen kopen.

Description

A Critical Patch Update is a collection of patches for multiple security vulnerabilities. These patches address vulnerabilities in Oracle code and in third party components included in Oracle products. These patches are usually cumulative, but each advisory describes only the security patches added since the previous Critical Patch Update Advisory. Thus, prior Critical Patch Update advisories should be reviewed for information regarding earlier published security patches. Refer to "Critical Patch Updates, Security Alerts and Bulletins" for information about Oracle Security advisories.

Oracle continues to periodically receive reports of attempts to maliciously exploit vulnerabilities for which Oracle has already released security patches. In some instances, it has been reported that attackers have been successful because targeted customers had failed to apply available Oracle patches. Oracle therefore strongly recommends that customers remain on actively-supported versions and apply Critical Patch Update security patches without delay.

This Critical Patch Update contains 441 new security patches across the product families listed below. Please note that an MOS note summarizing the content of this Critical Patch Update and other Oracle Software Security Assurance activities is located at April 2024 Critical Patch Update: Executive Summary and Analysis.

CERT-EU

Security Advisory 2024-034

Multiple Vulnerabilities in Microsoft Products

April 10, 2024 — v1.0

TLP:CLEAR

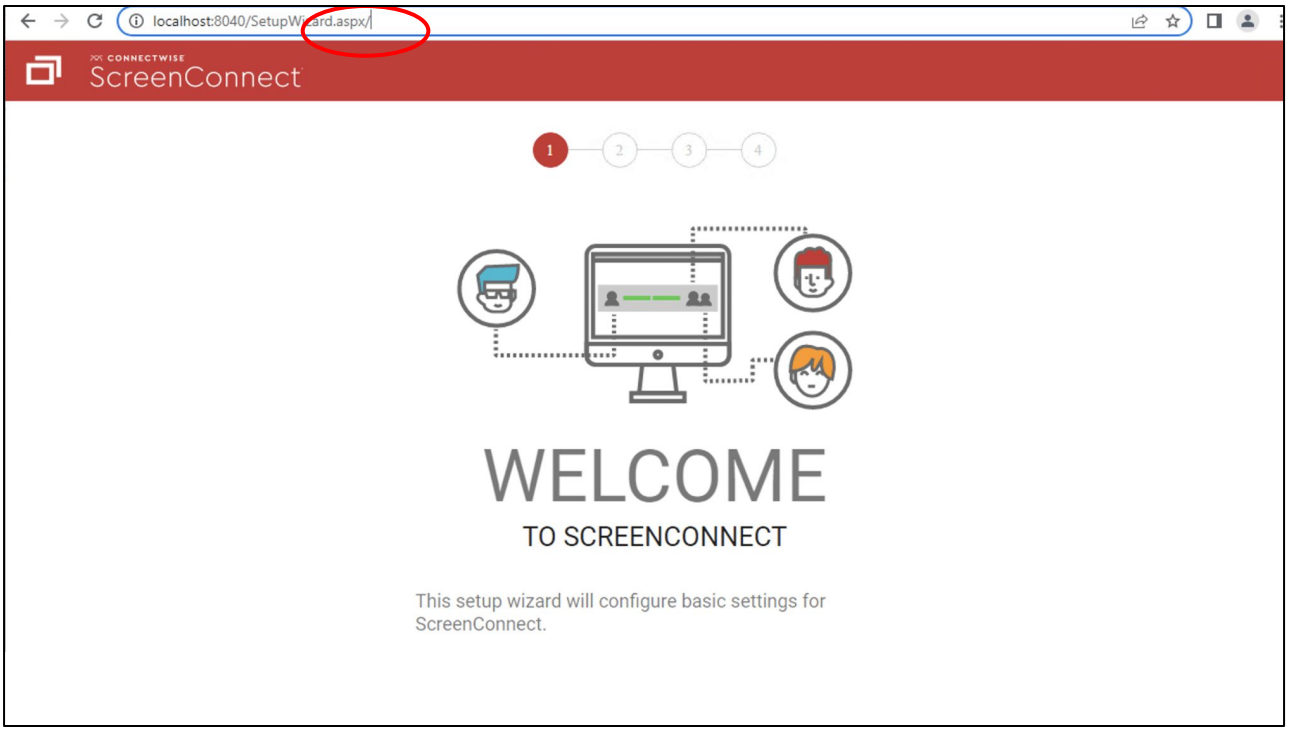
History:

- *10/04/2024 — v1.0 – Initial publication*

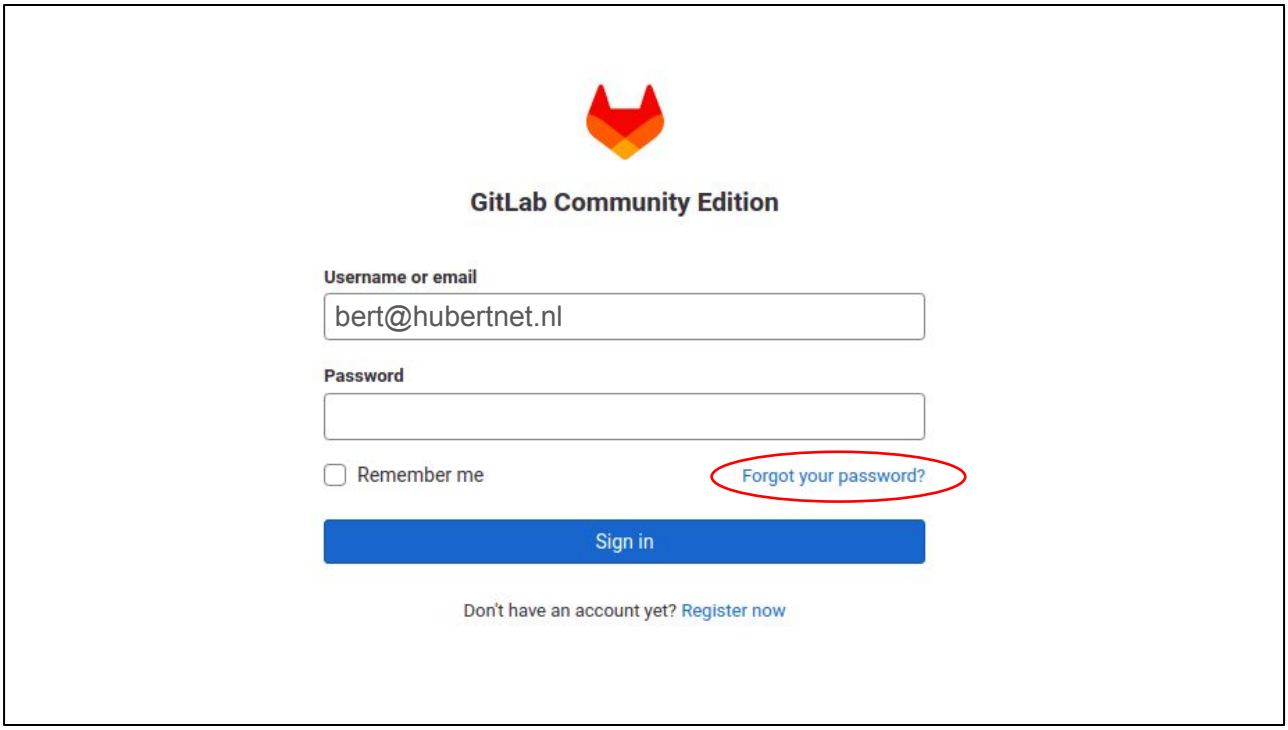
Summary

On April 9, 2024, Microsoft addressed 150 vulnerabilities in its April 2024 Patch Tuesday update [1], including 67 remote code execution (RCE) vulnerabilities and 2 zero-days exploited in malware attacks [2].

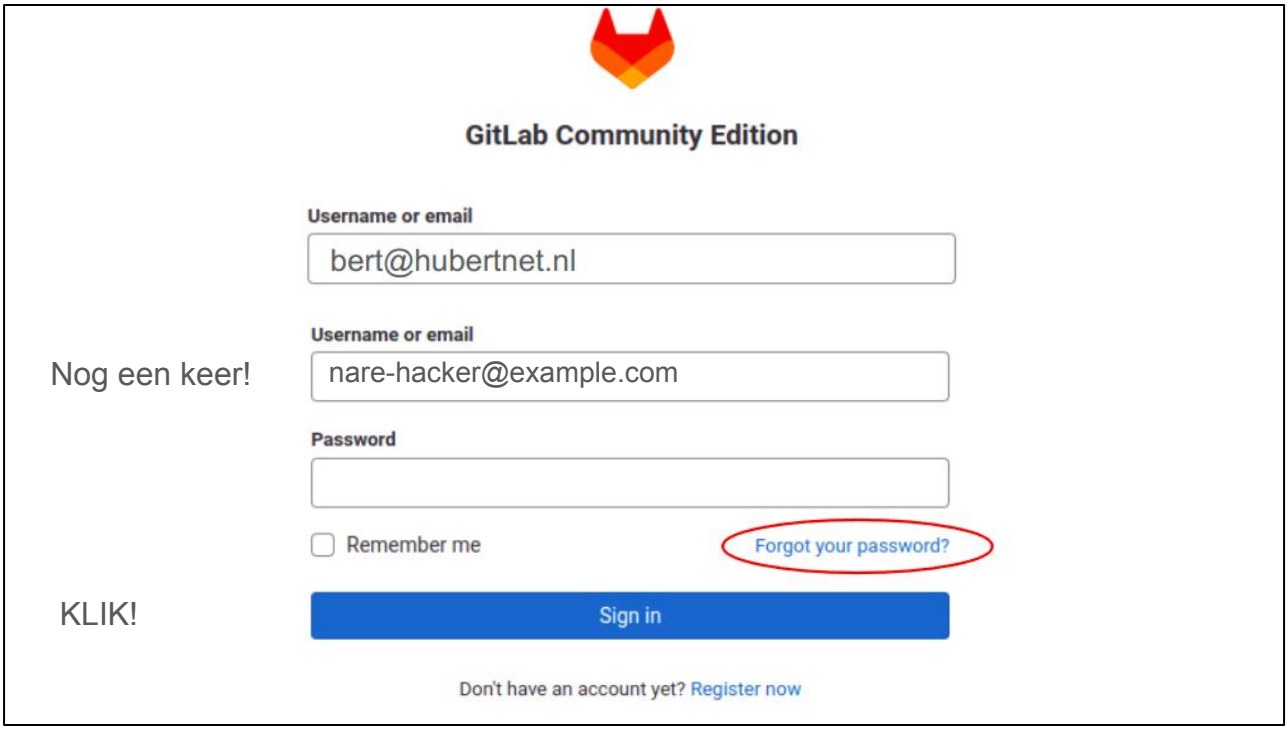
It is recommended applying updates as soon as possible on affected products.



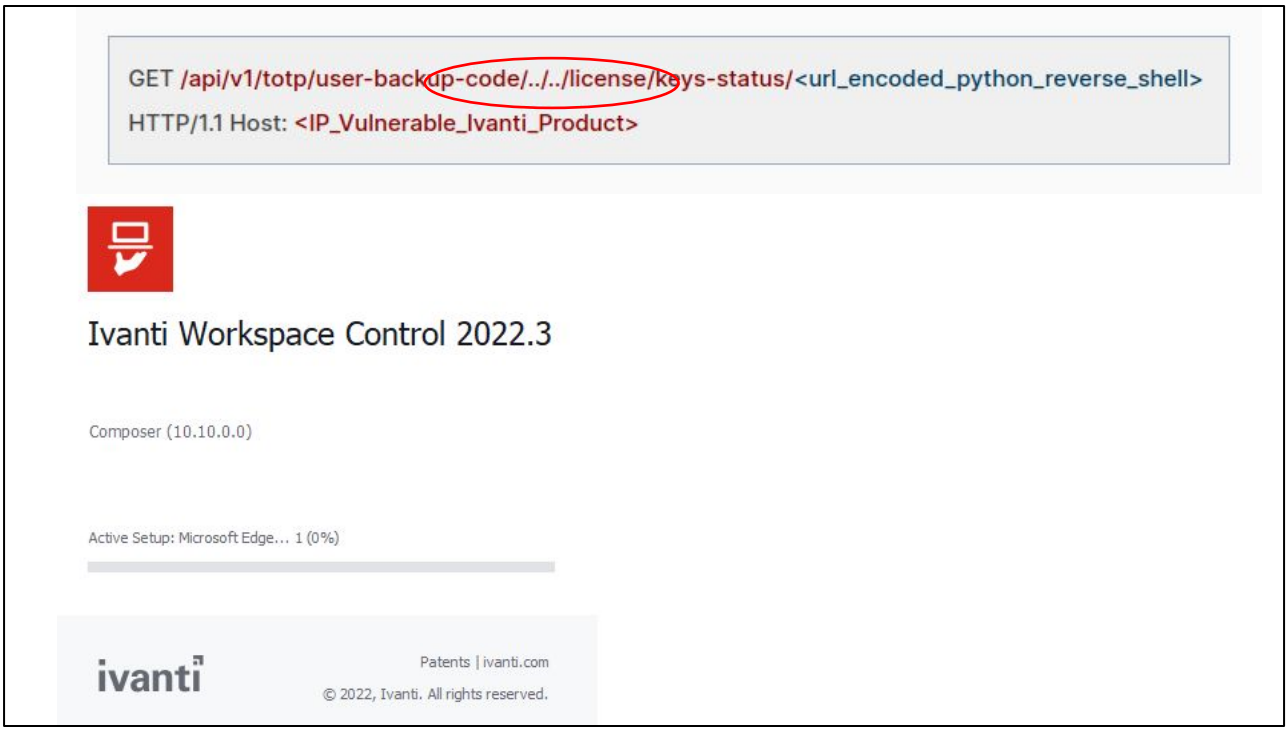
Deze software wordt gebruikt door helpdesks om computers op afstand mee over te nemen. Het bleek dat als je een “/” toevoegde bovenin je het wachtwoord mocht veranderen. En zo kan je een heel bedrijf overnemen. En een / toevoegen is geen heel bijzondere hacktechniek.



In GitLab bewaren bedrijven en overheden de broncode van applicaties. Als je je wachtwoord vergeten bent kan je hier een link opvragen om een nieuw wachtwoord in te stellen. Maar..



Maar bleek dat als je TWEE email adressen opgaf het systeem het eerste email adres controleerde of het de goeie was. En daarna stuurde hij de “reset je wachtwoord link” naar het tweede email adres. Wat dan van een hacker kan zijn. Super spannende hack techniek.

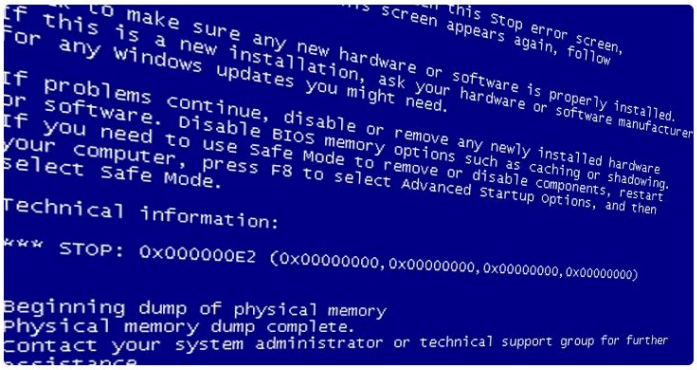


https://www.picussecurity.com/resource/blog/ivanti-cve-2023-46805-and-cve-2024-21887-zero-day-vulnerabilities - inmiddels verboden door de US overheid, maar wij gaan er mee door.
https://www.cisa.gov/news-events/news/cisa-issues-emergency-directive-requiring-federal-agencies-mitigate-ivanti-connect-secure-and-policy - je komt pas bij Ivanti als je al 1 wachtwoord ingevuld hebt, maar daarna is het prijsschieten.

Perhaps move to the cloud then?

Outlook Hack: Microsoft Reveals How a Crash Dump Led to a Major Security Breach

Sep 07, 2023 Newsroom Cyber Attack / Email Hacking



Microsoft on Wednesday revealed that a China-based threat actor known as **Storm-0558** acquired the inactive consumer signing key to forge tokens and access Outlook by compromising an engineer's corporate account.

This enabled the adversary to access a debugging environment that contained information pertaining to a crash of the consumer signing system and steal the key. The system crash took place in April 2021.

Trending News

Oeps. Microsoft vertelde hier dat hackers met een super geavanceerde truc binnengekomen waren, via een “crash dump”.

Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard

MSRC / By MSRC / March 08, 2024 / 2 min read

This blog provides an update on the nation-state attack that was detected by the Microsoft Security Team on January 12, 2024. As we shared, on January 19, the security team detected this attack on our corporate email systems and immediately activated our response process. The Microsoft Threat Intelligence investigation identified the threat actor as Midnight Blizzard, the Russian state-sponsored actor also known as NOBELIUM.

As we said at that time, our investigation was ongoing, and we would provide additional details as appropriate.

In recent weeks, we have seen evidence that Midnight Blizzard is using information initially exfiltrated from our corporate email systems to gain, or attempt to gain, unauthorized access. This has included access to some of the company's source code repositories and internal systems. To date we have found no evidence that Microsoft-hosted customer-facing systems have been compromised.

It is apparent that Midnight Blizzard is attempting to use secrets of different types it has found. Some of these secrets were shared between customers and Microsoft in email, and as we discover them in our exfiltrated email, we have been and are reaching out to these customers to assist them in taking mitigating measures. Midnight Blizzard has increased the volume of some aspects of the attack, such as password sprays, by as much as 10-fold in February, compared to the already large volume we saw in January 2024.

Midnight Blizzard's ongoing attack is characterized by a sustained, significant commitment of the threat actor's resources, coordination, and focus. It may be using the information it has obtained to accumulate a picture of areas to attack and enhance its ability to do so. This reflects what has become more broadly an unprecedented global threat landscape, especially in terms of sophisticated nation-state attacks.

Across Microsoft, we have increased our security investments, cross-enterprise coordination and mobilization, and have enhanced our ability to defend ourselves and secure and harden our environment against this advanced persistent threat. We have and will continue to put in place additional enhanced security controls, detections, and monitoring.

Our active investigations of Midnight Blizzard activities are ongoing, and findings of our investigations will continue to evolve. We remain committed to sharing what we learn.

Microsoft confirms they are still hacked

Microsoft faulted for ‘cascade’ of failures in Chinese hack

The independent Cyber Safety Review Board’s report knocks the tech giant for shoddy cybersecurity practices, lax corporate culture and a deliberate lack of transparency

By Ellen Nakashima and Joseph Menn

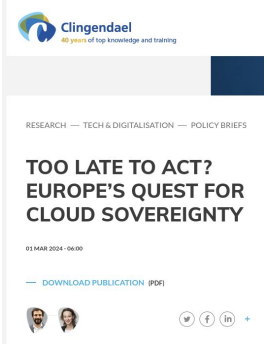
Updated April 2, 2024 at 6:18 p.m. EDT | Published April 2, 2024 at 4:00 p.m. EDT

https://www.washingtonpost.com/national-security/2024/04/02/microsoft-cyber-china-hack-report/ a must read

Cloud Naïve: Europe and the 'Bijenkorf' Megascaler

Apr 28 2024

Lately there's been some confusion: places like SIDN (Dutch national operator of all internet names that end on .NL) claim that nobody in Europe can deliver their computer needs, and that they therefore must outsource their operations to American cloud providers.



https://www.clingendael.org/publication/too-late-act-europes-quest-cloud-sovereignty
https://berthub.eu/articles/posts/cloud-naive-europe-and-the-megascaler/

Your tech or my tech: make up your mind quickly

Mar 02 2024

There's no need to do everything yourself by the way. Source: Wikimedia

"You end up in a situation where everyone who loves IT has left, and as an employer you have also become very unattractive to people who have actual skills."

https://berthub.eu/articles/posts/your-tech-my-tech/

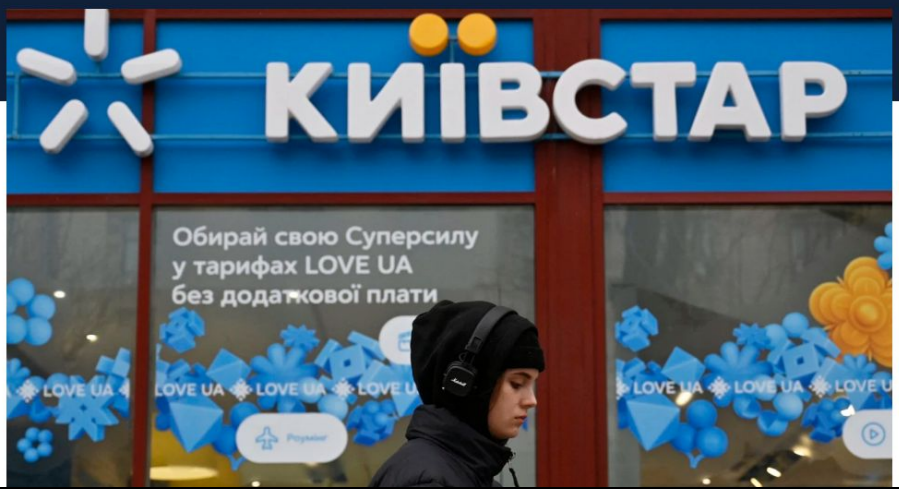
Why is this happening?

https://berthub.eu/articles/posts/how-tech-loses-out/

We can’t go on like this!

Ukraine faces second day of huge phone and internet outage after suspected Russian cyberattack

Ukrainian authorities accused Russia's military intelligence unit of being responsible.



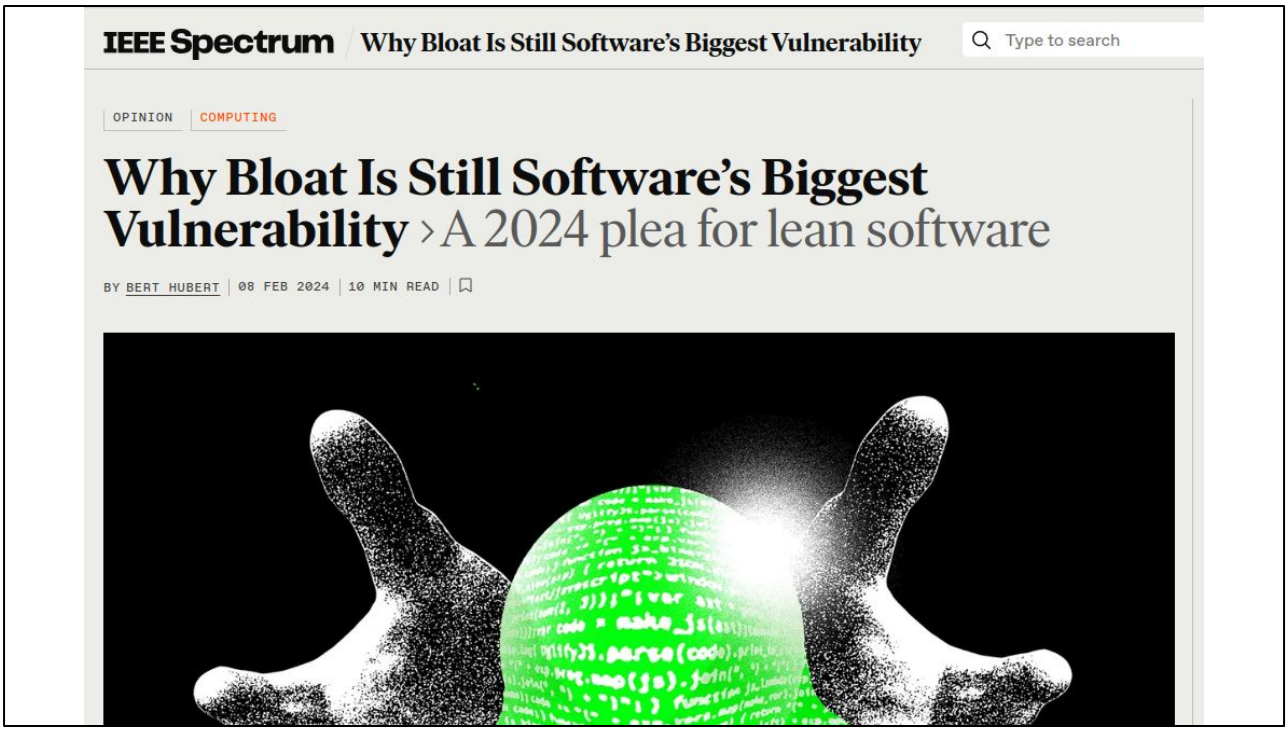
December 2023

When times are bad, you are (much more) on your own!
(no one has time for you!)

- ROBUST: **Does not fall over by itself**
- LIMITED/KNOWN DEPENDENCIES: **Does not need too much unknown stuff too far away**
- OWNERSHIP/UNDERSTANDING: **If things break, you can improvise or fix things**

Is there a way back?

https://berthub.eu/articles/posts/european-innovation-and-capabilities/



https://berthub.eu/articles/posts/a-2024-plea-for-lean-software/

Summary

- The systems that support our daily lives are way way too complex & fragile
  - And getting more complex
- Maintenance is moving ever further away from us
  - As is understanding
- Our own skills are wilting, we are **no longer able to control our infrastructure**
- Now imagine a war where you need help from everyone else

- **We get this because non-technical people make economic choices**
- I don't know how we can fix this

https://berthub.eu/articles/posts/nerdfluisteraar/

Cyber Security and Society: a pre-war reality check

Bert Hubert / bert@hubertnet.nl
https://berthub.eu/prewar