
HELPENDE HACKERS
CYBERELLENDE
WAS NOG NOOIT ZO LEUK
Onthullende verhalen uit de wereld van informatiebeveiligers en hackers
Chris van 't Hof
TEK
TOK
HACK
TALK
DIVD

Ons bedrijf

Werkt voor jou

ONS TEAM

Bart de baas

Cor de compagnon

Christel de CFO

Lotte Hoofd Legal

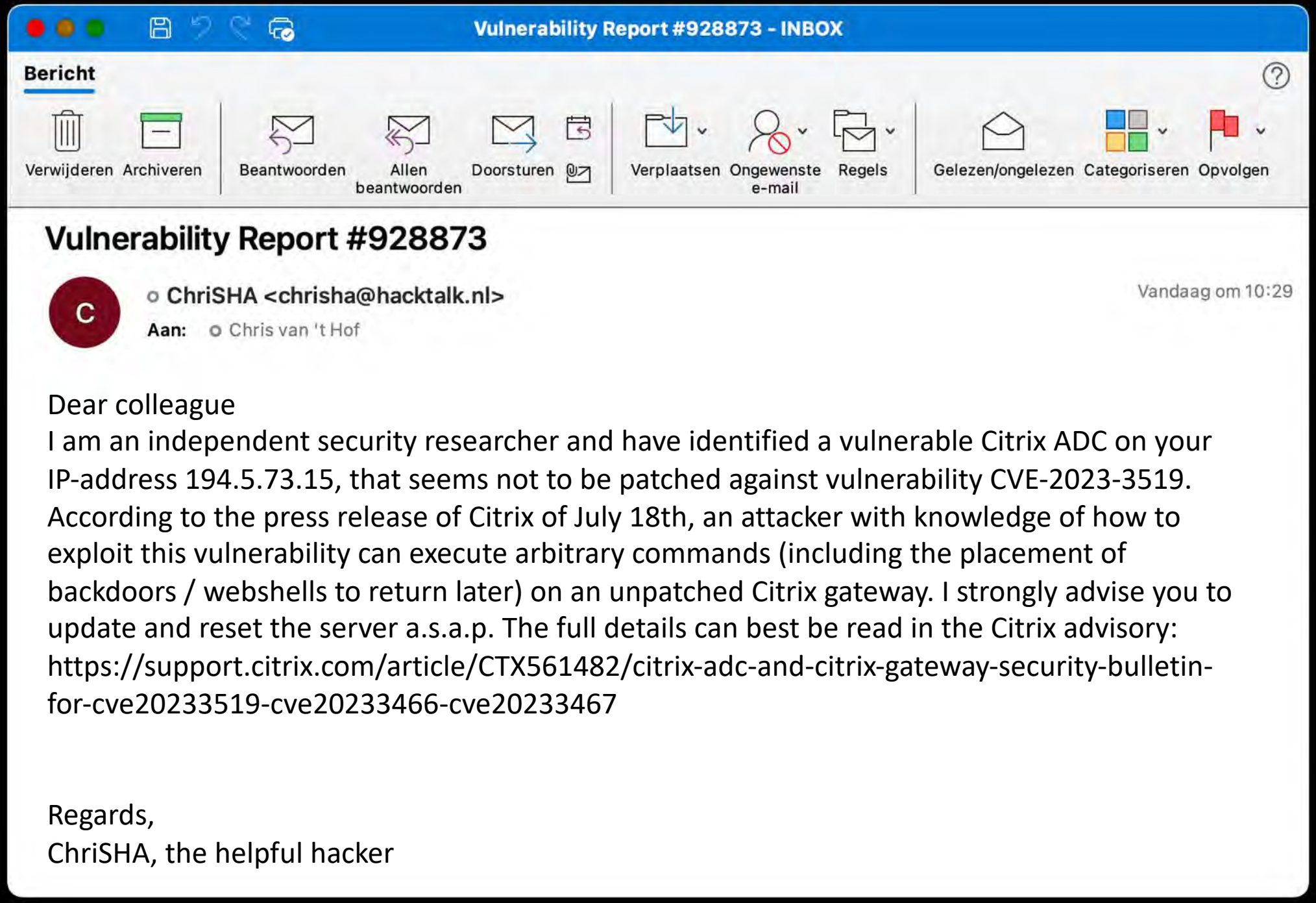
Ineke Hoofd ICT

Babs

Francine de FG

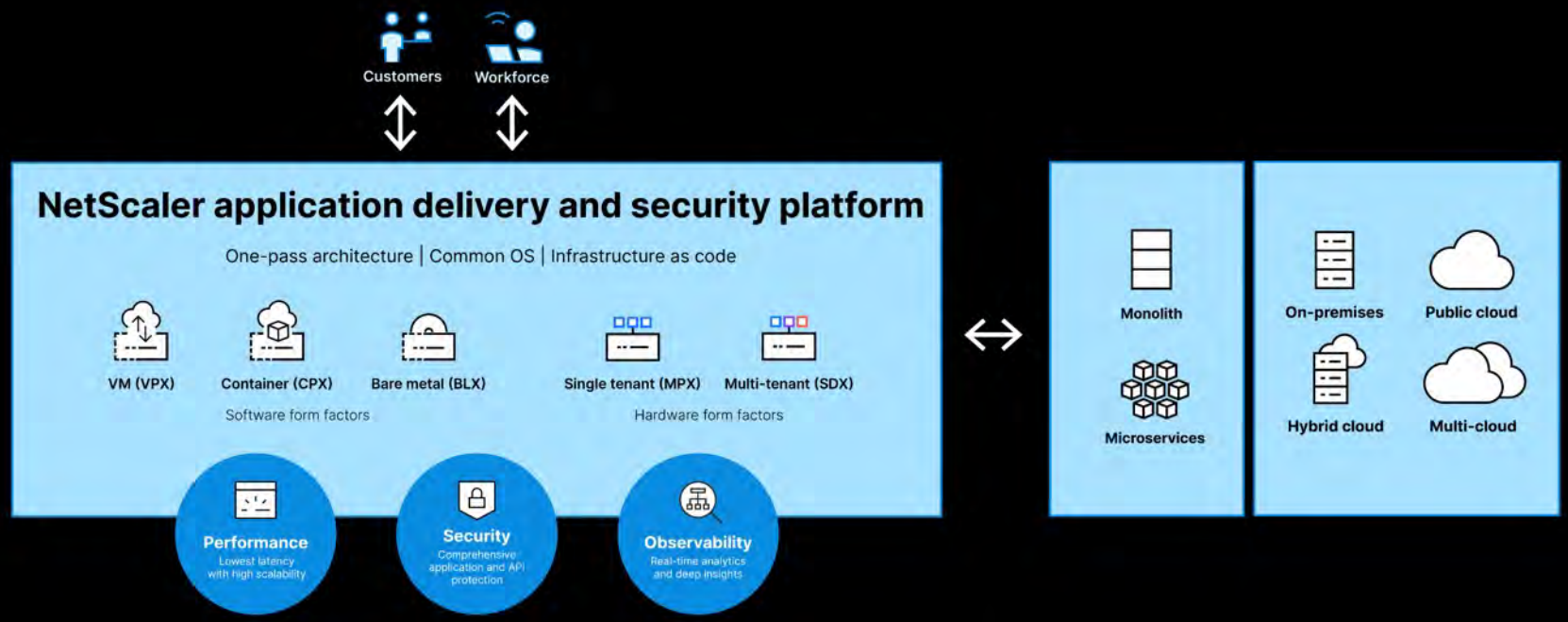
Karin Hoofd CRM

Wekelijkse vergadering


Vulnerability Report #928873 - INBOX
Bericht
Verwijderen
Archiveren
Beantwoorden
Allen beantwoorden
Doorsturen
Verplaatsen
Ongewenste e-mail
Regels
Gelezen/ongelezen
Categoriseren
Opvolgen
Vulnerability Report #928873
C
ChriSHA <chrisha@hacktalk.nl>
Aan: Chris van 't Hof
Vandaag om 10:29
Dear colleague
I am an independent security researcher and have identified a vulnerable Citrix ADC on your IP-address 194.5.73.15, that seems not to be patched against vulnerability CVE-2023-3519. According to the press release of Citrix of July 18th, an attacker with knowledge of how to exploit this vulnerability can execute arbitrary commands (including the placement of backdoors / webshells to return later) on an unpatched Citrix gateway. I strongly advise you to update and reset the server a.s.a.p. The full details can best be read in the Citrix advisory: https://support.citrix.com/article/CTX561482/citrix-adc-and-citrix-gateway-security-bulletin-for-cve20233519-cve20233466-cve20233467
Regards,
ChriSHA, the helpful hacker

One platform for hybrid cloud application delivery and security

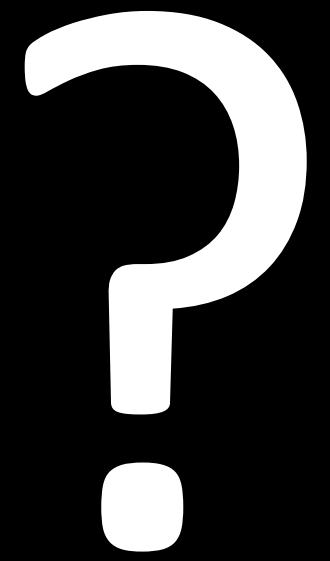
NetScaler is the only application delivery and security platform where you can manage all of your ADC operations in one place.



Environment agnostic. Intent based. API driven.
Application delivery for a multi-cloud world

Wat doen we?

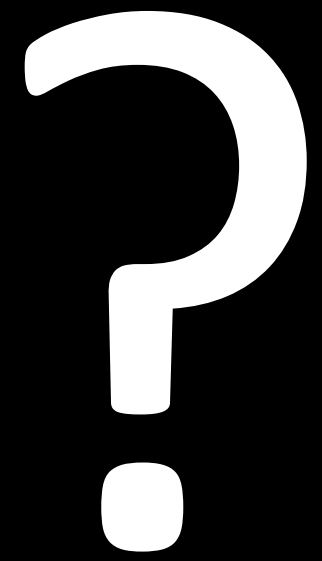
A. Vragen om uitleg
B. Niks, zal wel spam zijn
C. Doorsturen naar ICT
D. Externe expert vragen
E. Anders, nm: …

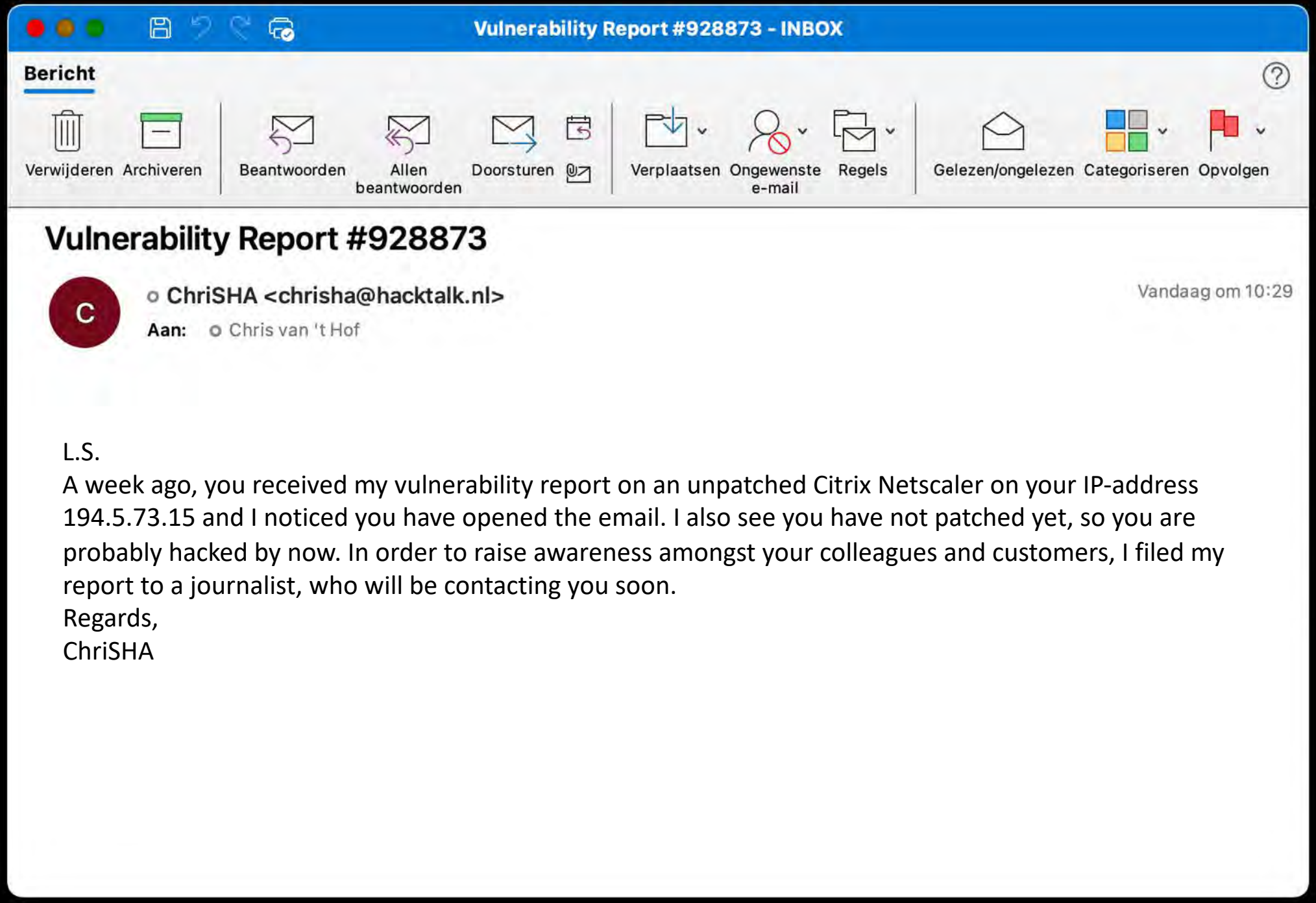



distance ahead, but we
can see plenty there that
needs to be done."
Alan Turing

Wat doen we?

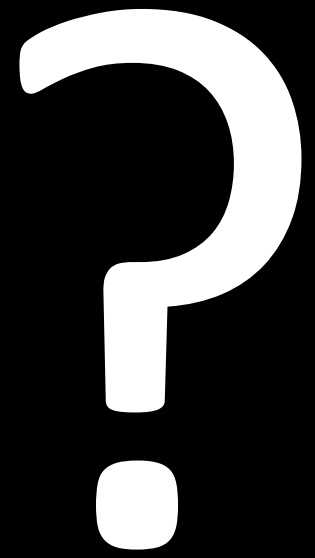
A. Melder vragen om hulp
B. Onze ICT moet het oplossen
C. Aansprakelijkheid uitzoeken
D. Externe expert vragen
E. Netscaler uitzetten
F. Anders, nm: …




Vulnerability Report #928873 - INBOX
Bericht
Verwijderen
Archiveren
Beantwoorden
Allen beantwoorden
Doorsturen
Verplaatsen
Ongewenste e-mail
Regels
Gelezen/ongelezen
Categoriseren
Opvolgen
Vulnerability Report #928873
C
ChriSHA <chrisha@hacktalk.nl>
Aan: Chris van 't Hof
Vandaag om 10:29
L.S.
A week ago, you received my vulnerability report on an unpatched Citrix Netscaler on your IP-address 194.5.73.15 and I noticed you have opened the email. I also see you have not patched yet, so you are probably hacked by now. In order to raise awareness amongst your colleagues and customers, I filed my report to a journalist, who will be contacting you soon.
Regards,
ChriSHA

Wat doen we?

A. Melder vragen journalist af te bellen
B. Aangifte doen
C. Aansprakelijkheid uitzoeken
D. Externe expert vragen
E. Persbericht opstellen
F. Anders, nm: …



Data breach notification obligation

News message / 4 January 2016

Since 1 January 2016, the data breach notification obligation has entered into force. This obligation means that organisations (companies as well as governments) must immediately notify the Dutch Data Protection Authority as soon as they experience a serious data breach. And in some cases, they must also report the data breach to the data subjects (the

Publicaties

Beleidsregels / 8 December 2015

Policy rules data breach notification obligation

DOWNLOAD

LOSS OF DATA - INBOX

Bericht

Verwijderen Archiveren Beantwoorden Allen beantwoorden Doorsturen Verplaatsen Ongewenste e-mail Regels Gelezen/ongelezen Categoriseren Opvolgen

LOSS OF DATA

CW

Cyberwatchers

Aan: Chris van 't Hof

Vandaag om 11:11

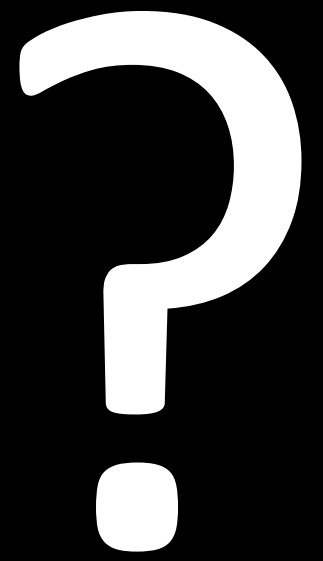
Hi Company,
You may be wondering what happened to your database. Well, it appeared to be unpatched and wide open for criminals. But don’t worry, we made a back-up of all your files, wiped the server clean and patched it ourselves.

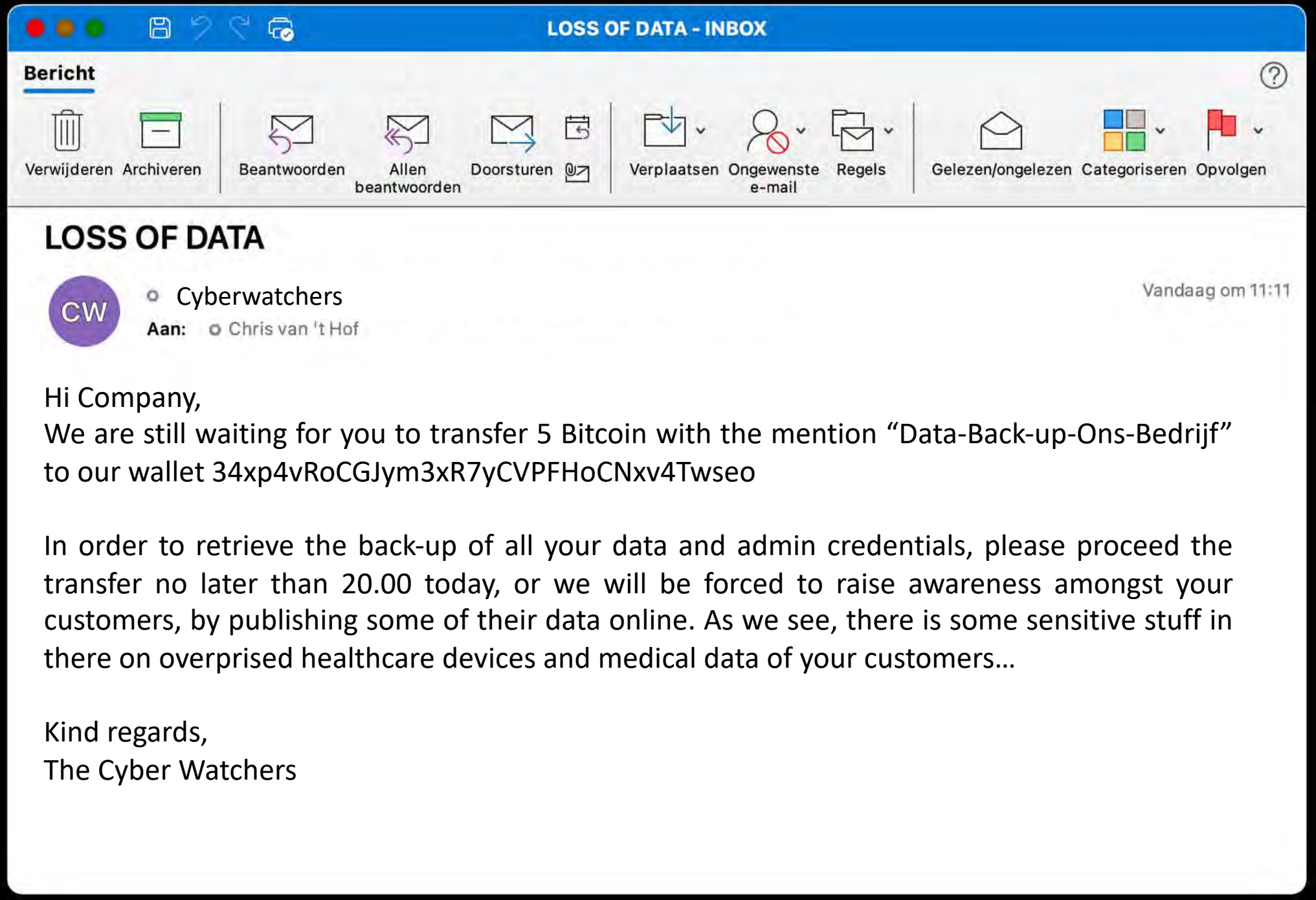
In order to retrieve your back-up and admin credentials, we kindly ask you to transfer 5 Bitcoin to our wallet 34xp4vRoCGJym3xR7yCVPFHoCNxv4Tws1o with the mention “Data-Back-up-Ons-Bedrijf”. We can also help you with this transfer. Just reply to this email.

Kind regards,
The Cyber Watchers

Wat doen we?

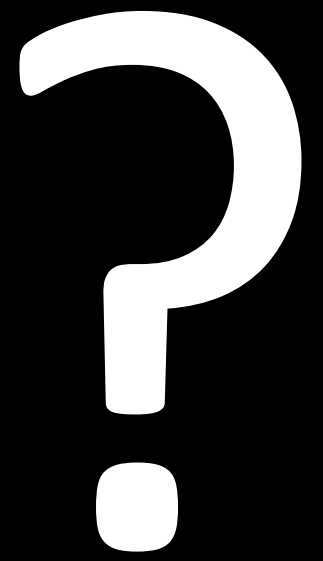
A. Betalen
B. Onderhandelen
C. Aangifte doen
D. Verzekering raadplegen
E. Externe experts inhuren
F. Niets
G. Anders, nm: …




LOSS OF DATA - INBOX
Bericht
Verwijderen
Archiveren
Beantwoorden
Allen beantwoorden
Doorsturen
Verplaatsen
Ongewenste e-mail
Regels
Gelezen/ongelezen
Categoriseren
Opvolgen
LOSS OF DATA
CW
Cyberwatchers
Aan: Chris van 't Hof
Vandaag om 11:11
Hi Company,
We are still waiting for you to transfer 5 Bitcoin with the mention “Data-Back-up-Ons-Bedrijf” to our wallet 34xp4vRoCGJym3xR7yCVPFHoCNxv4Twseo
In order to retrieve the back-up of all your data and admin credentials, please proceed the transfer no later than 20.00 today, or we will be forced to raise awareness amongst your customers, by publishing some of their data online. As we see, there is some sensitive stuff in there on overprised healthcare devices and medical data of your customers…
Kind regards,
The Cyber Watchers

Wat doen we?

A. Betalen
B. Onderhandelen
C. Aangifte doen
D. Verzekering raadplegen
E. Externe experts inhuren
F. Niets
G. Anders, nm: …



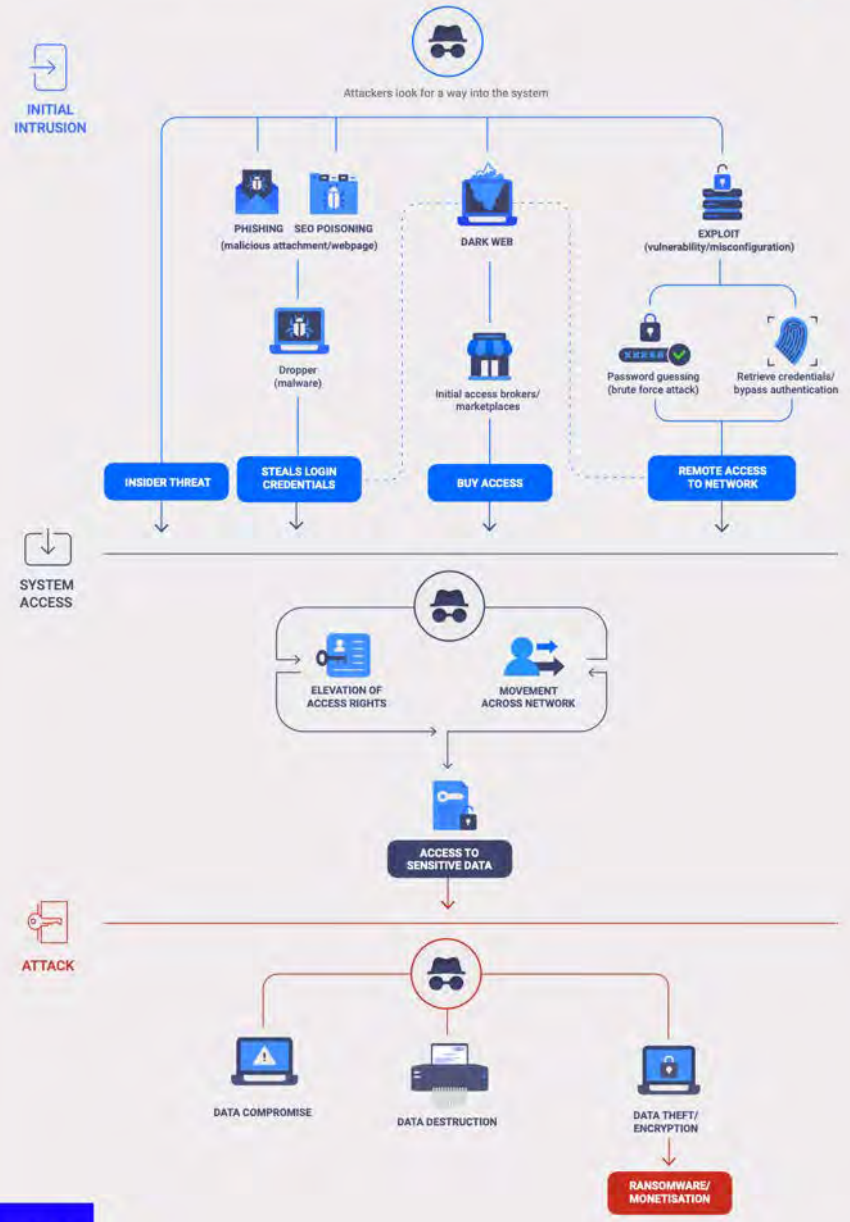

The End

EUROPOL

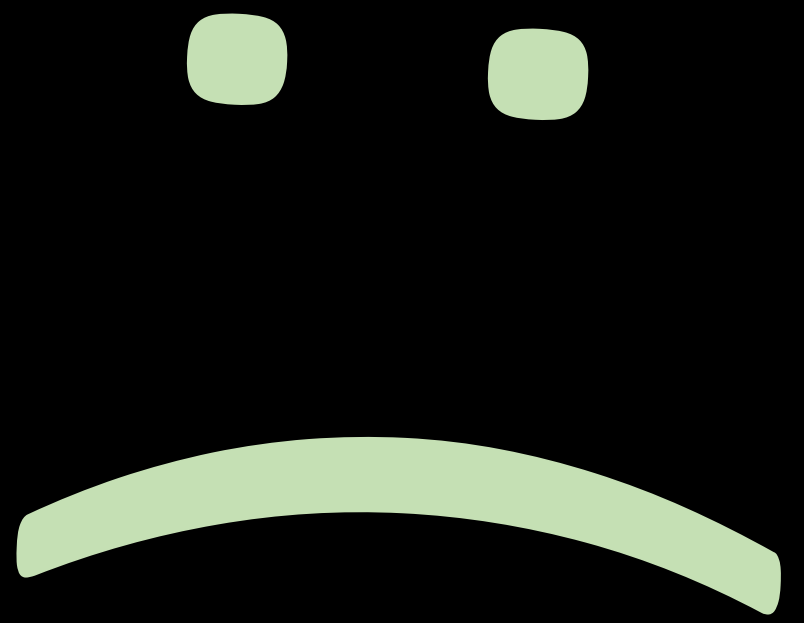
IOCTA

EUROPOL SPOTLIGHT

CYBER-ATTACKS: THE APEX OF CRIME-AS-A-SERVICE



Cyber ellende



Cyber elende

Was nog nooit zo leuk

1. Cyberellende zo oud als de Oudheid
2. Hackers kunnen helpen
3. Informatiebeveiliging open wereld
4. Meest waardevolle kennis is gratis
5. Nerds organiseren de beste feestjes
6. Je bent pas veilig als je gehackt bent
7. Taart voor iedereen


κυβερνήτης

Kamasutra Cipher

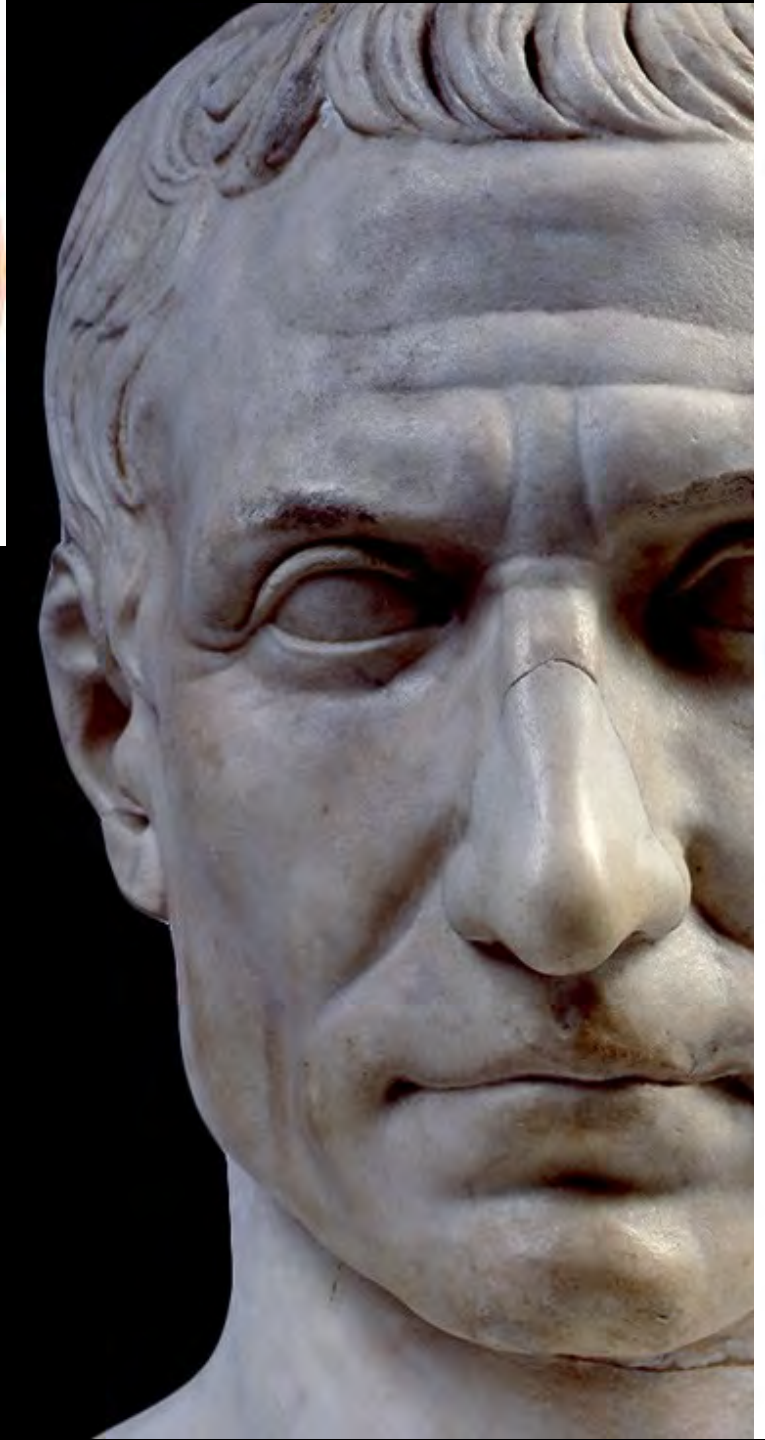
- The Kamasutra cipher is one of the earliest known substitution methods.
- The purpose was to teach women how to hide secret messages from prying eyes.

Principle

The key is the permutation of the alphabet. The plaintext and the ciphertext alphabet are the same. The alphabet is divided in two halves to pair the letters:

F Y M Q G V O P D J R A K
C I E U B X T S Z W N L H

The letter “F” becomes the letter “C” and “B” is replaced by “G”. The word "EXAMPLE" would be encoded by: "MVLESAM".



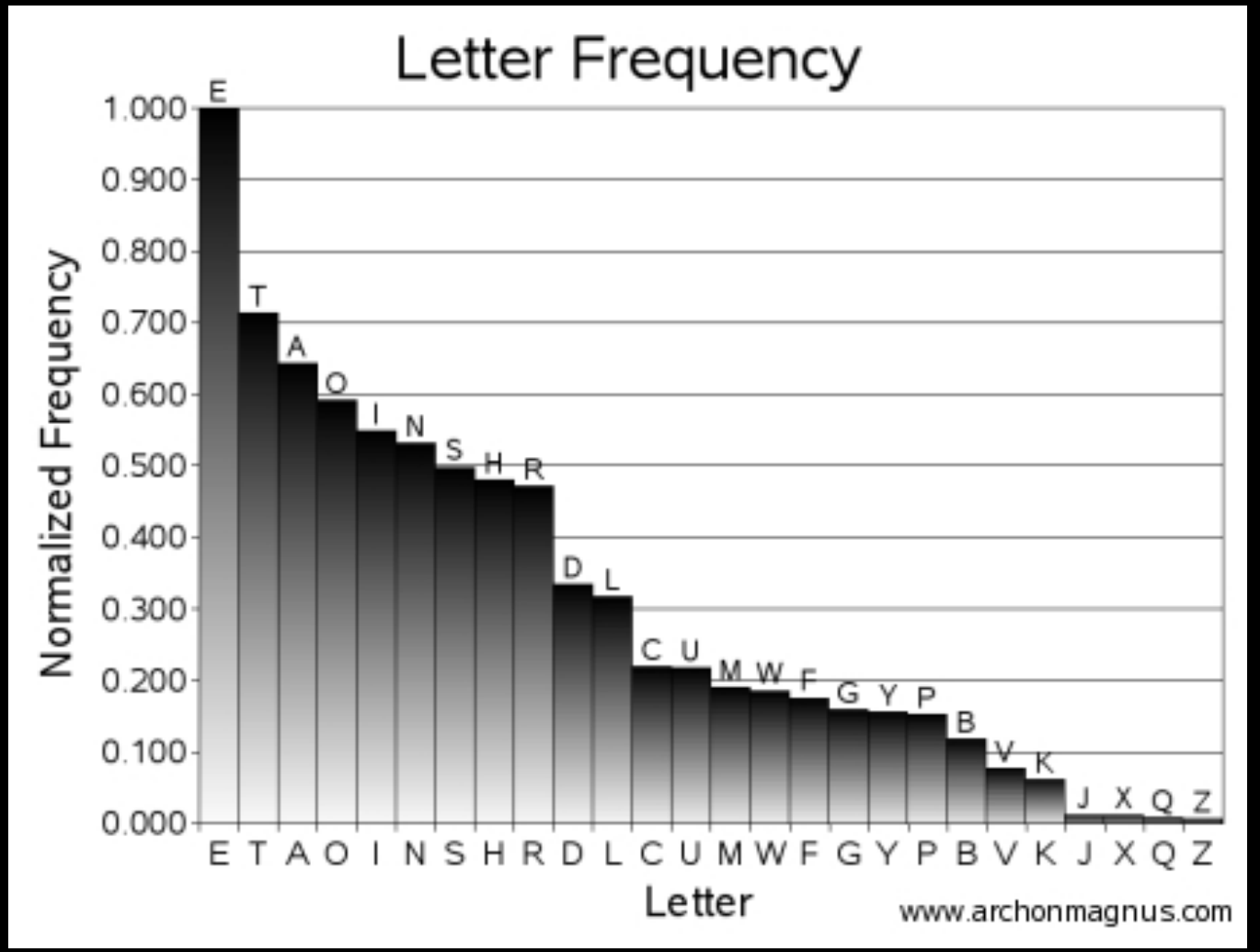
▲ © Reuters

Nederlander hackt Twitteraccount Donald Trump: 'Ik dacht 'oh god' toen ik was ingelogd'

Een Nederlander heeft het twitteraccount @realDonaldTrump van de Amerikaanse president Donald Trump voor de tweede keer gehackt. Trump gebruikte het wachtwoord 'maga2020!' (*Make america great again*) en zou geen extra beveiliging hebben ingesteld, meldt *Vrij Nederland*. Ook werd ongeveer hetzelfde wachtwoord gebruikt voor het wifi-netwerk op grote Trump-bijeenkomsten. Het Witte Huis ontkent dat de president gehackt is.

Binnenlandredactie 22-10-20, 15:55 Laatste update: 23-10-20, 11:57


SYRIA
الجمهورية العربية السورية
10
1994
POSTAGE


Letter Frequency
Normalized Frequency
1.000
0.900
0.800
0.700
0.600
0.500
0.400
0.300
0.200
0.100
0.000
E T A O I N S H R D L C U M W F G Y P B V K J X Q Z
Letter
www.archonmagnus.com

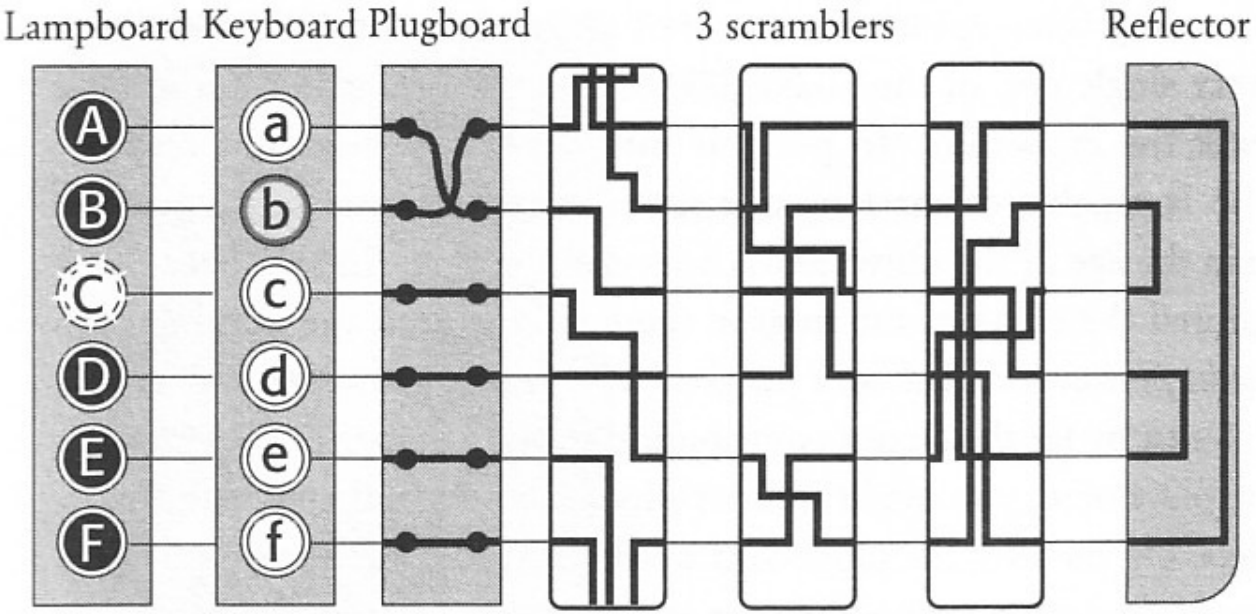
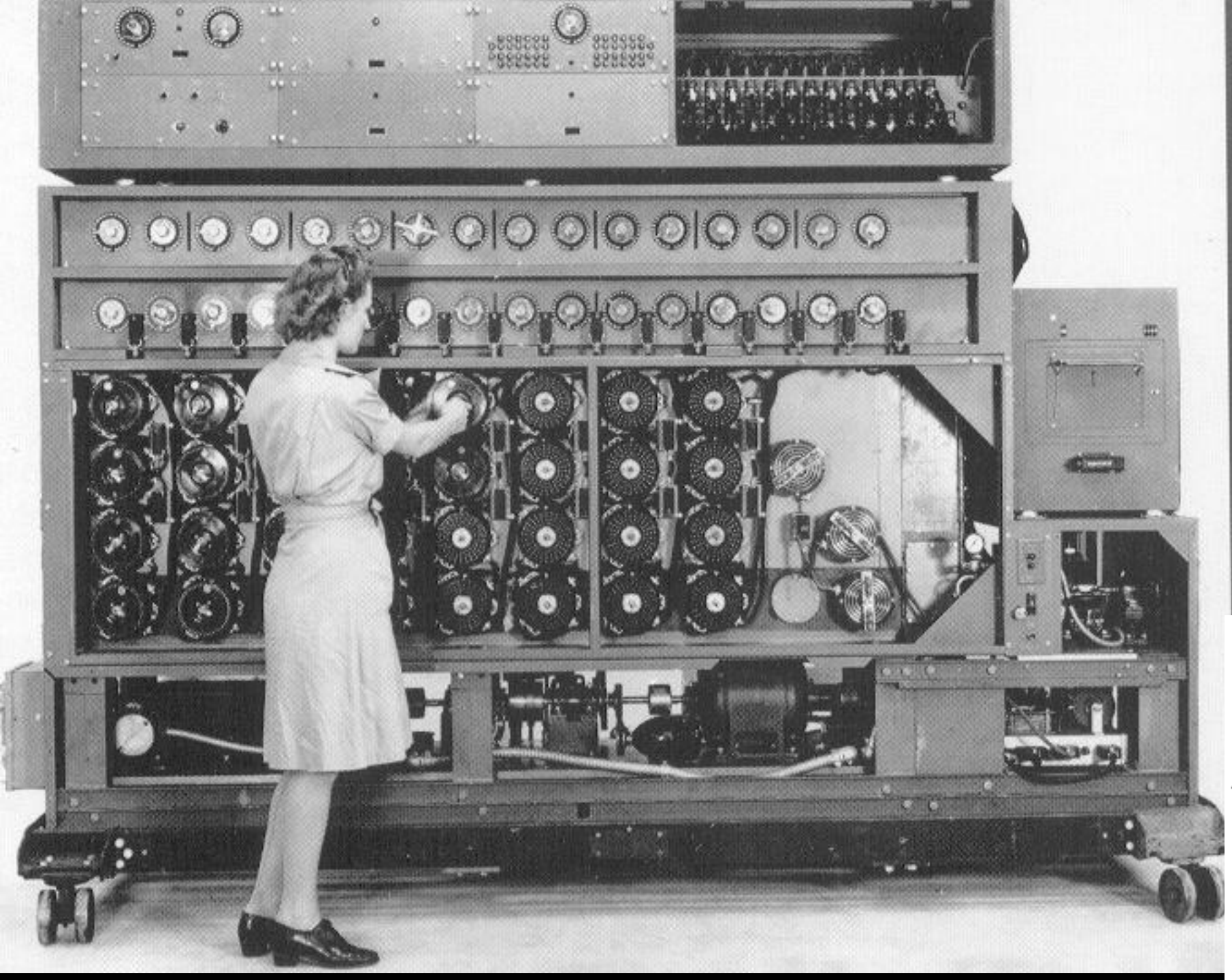
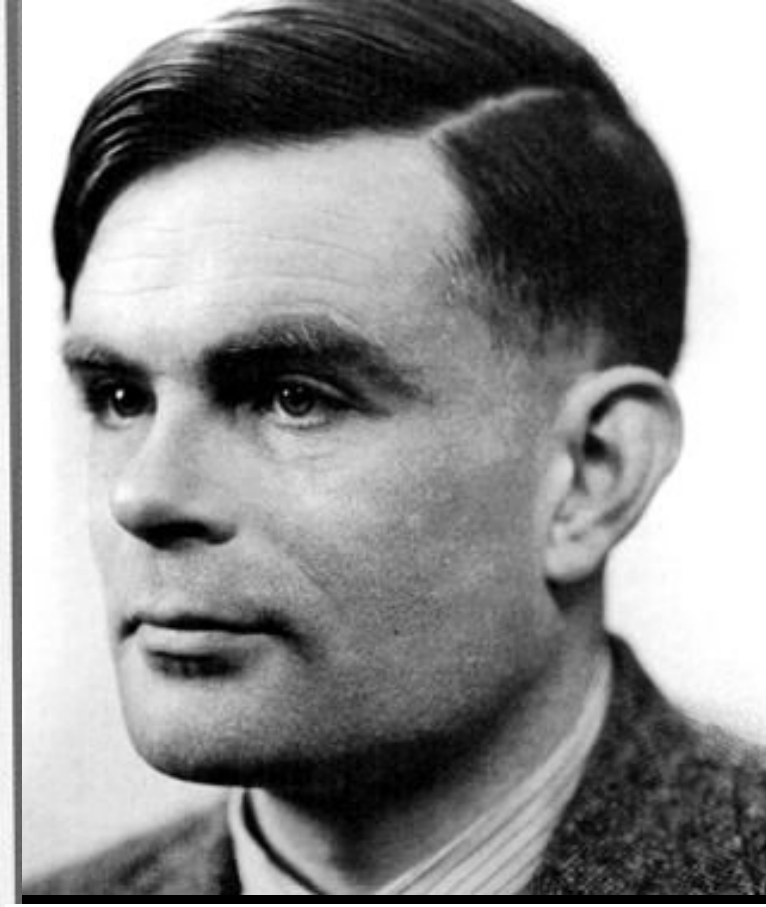


Figure 37 The plugboard sits between the keyboard and the first scrambler. By inserting cables it is possible to swap pairs of letters, so that, in this case, b is swapped with a. Now, b is encrypted by following the path previously associated with the encryption of a. In the real 26-letter Enigma, the user would have six cables for swapping six pairs of letters.





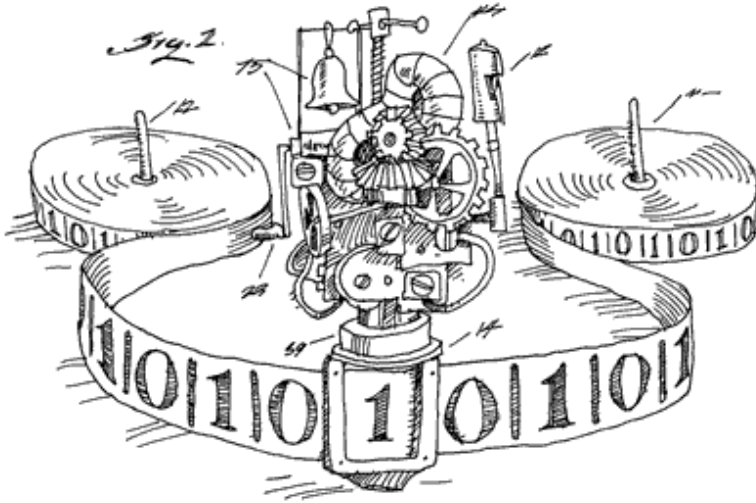
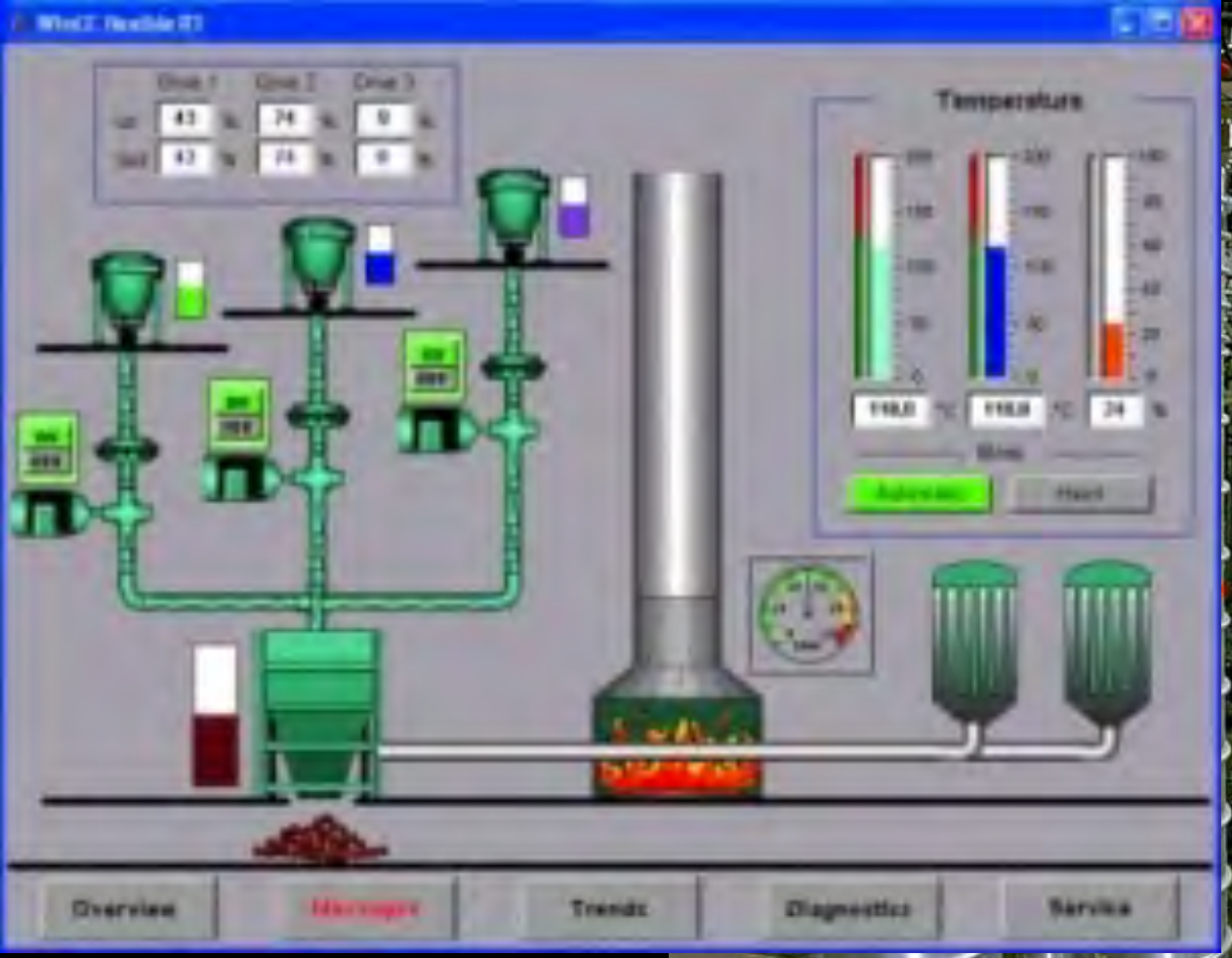
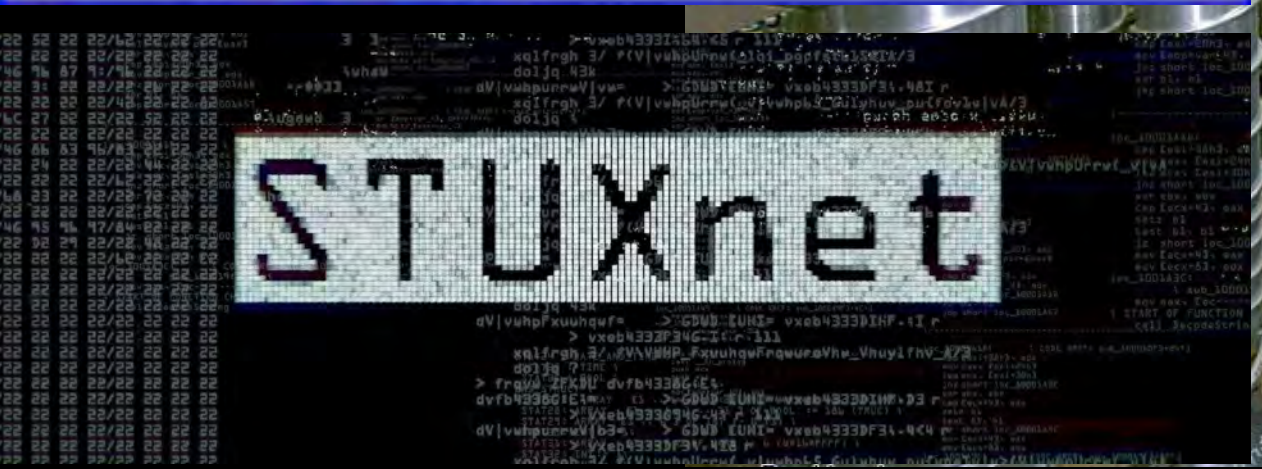


Fig. 1.
1 0 1 1 0 1 1 0 1 1



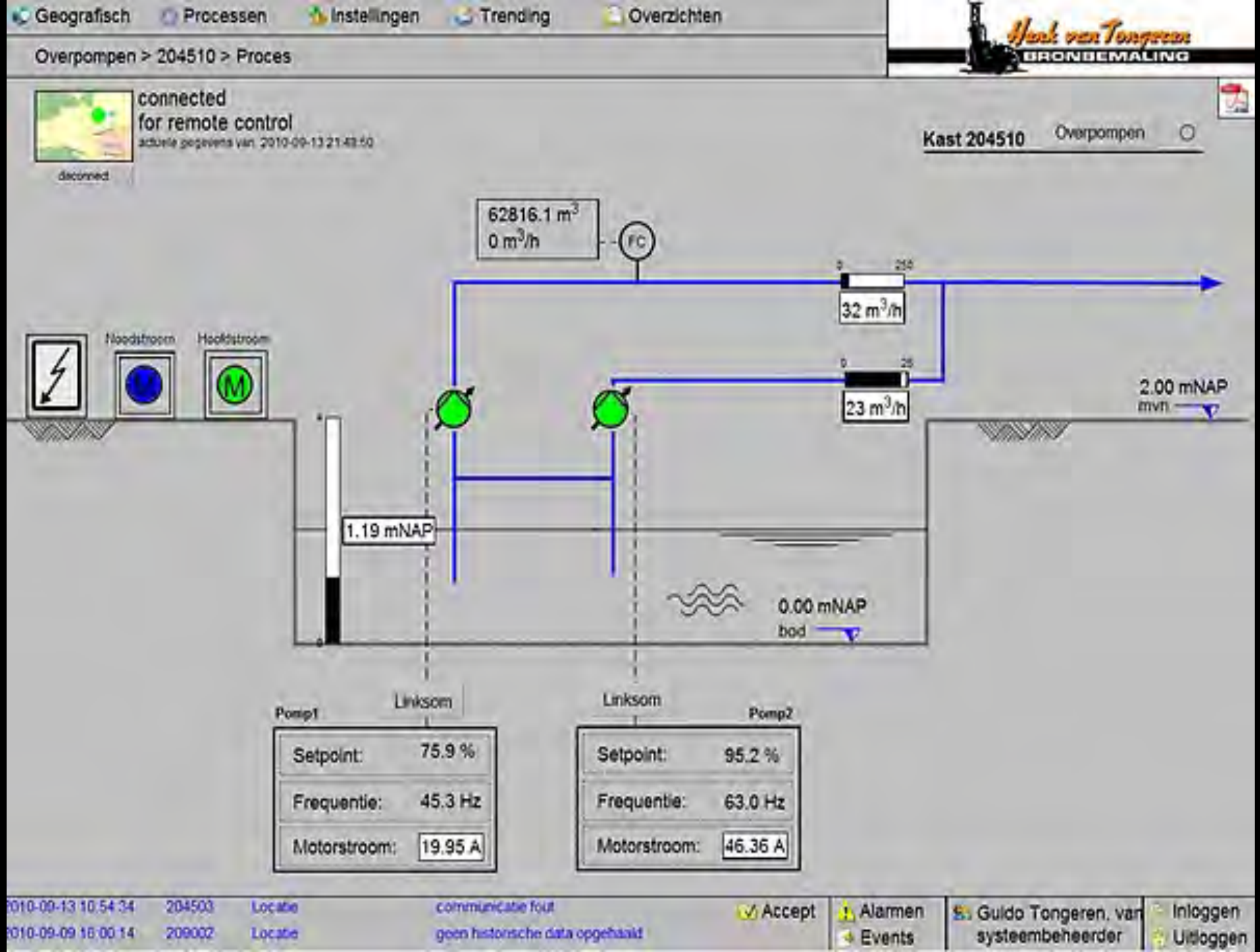


HET IS OORLOG

MAAR NIEMAND DIE HET ZIET

PODIUM

HUIB MODDERKOLK


Geografisch
Processen
Instellingen
Trending
Overzichten
Overpompen > 204510 > Proces
Henk van Tongeren
BRONBEMALING
connected
for remote control
actuele gegevens van: 2010-09-13 21:49:50
deconnect
Kast 204510
Overpompen
62816.1 m3
0 m3/h
FC
32 m3/h
23 m3/h
Noodstroom
Hoofdstroom
2.00 mNAP
mvn
1.19 mNAP
0.00 mNAP
bod
Linksom
Linksom
Pomp1
Pomp2
Setpoint: 75.9 %
Frequentie: 45.3 Hz
Motorstroom: 19.95 A
Setpoint: 95.2 %
Frequentie: 63.0 Hz
Motorstroom: 46.36 A
2010-09-13 10:54:34 204503 Locatie communicatie fout
2010-09-09 16:00:14 209002 Locatie geen historische data opgehaald
Accept
Alarmen
Events
Guido Tongeren, van
systeembeheerder
Inloggen
Uitloggen

SHODAN scada Explore Enterprise Access Contact Us

New to Shodan? Login or

Exploits Maps

TOTAL RESULTS

470

TOP COUNTRIES

Belgium	73
United States	61
Norway	47
Spain	44
Bulgaria	39

TOP SERVICES

HTTP	202
FTP	74
8081	30
NetBIOS	20
Modbus	17

TOP ORGANIZATIONS

RELATED TAGS: scada

166.148.161.245

245.sub-166-148-161.myvzw.com

Verizon Wireless

Added on 2017-06-12 17:53:34 GMT

United States

Details

ics

```
Unit ID: 0
-- Device Identification: Schneider Electric 171 CBU 98090 v01.00
-- CPU module: 171 CBU 98090
-- Project information: Hackberry - V8.1   SCADA-LT
-- Project revision: 0.0.135
-- Project last modified: 2016-08-09 13:17:03

Unit ID: 1
-- Device Identification: Schneider Electric 171 CB...
```

78.134.21.32

78-134-21-32.v4.ngi.it

NGI SpA

Added on 2017-06-12 17:28:32 GMT

Italy, Monteu Roero

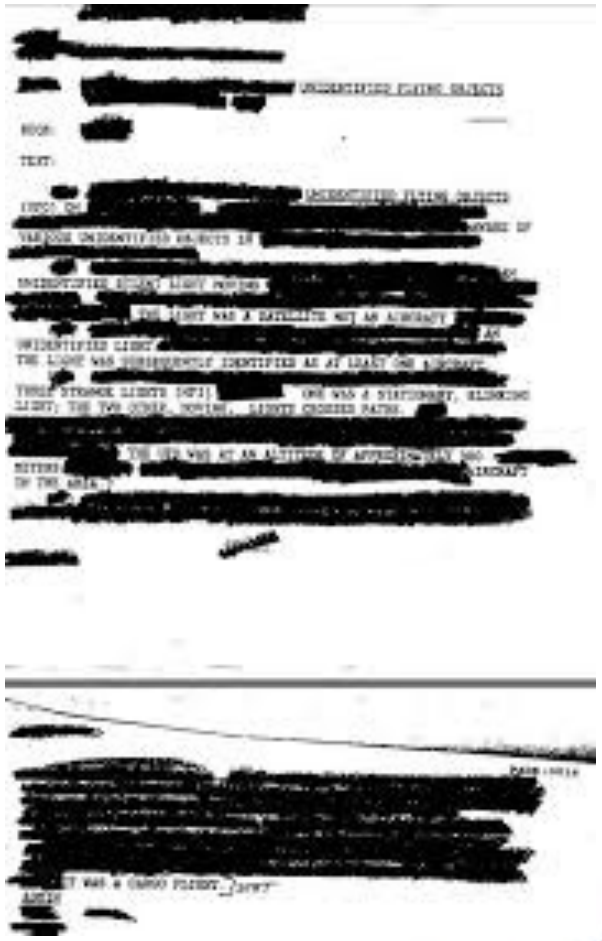
Details

```
HTTP/1.0 200 OK
Expires: Thu, 27 Jan 2009 16:00:00 GMT
Set-Cookie: ID=4706A78EAF66; path=/

<html>
  <head>
    <meta http-equiv="content-type" content="text/html;charset=windows-1252">
```


Afgelopen 7 dagen
Omroepen
Regio
Pop-out
Beeld vergroten

Hackers kunnen helpen



DIAGNOSTIEK VOOR U


Maatschappelijk belang?
Proportionaliteit?
Subsidiariteit?

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Coordinated Vulnerability Disclosure: de Leidraad


One
Conference
2018


LYB


RESPONSIBLE
DISCLOSURE


Informatie
beveiliging
open
Wereld

Victor Gevers

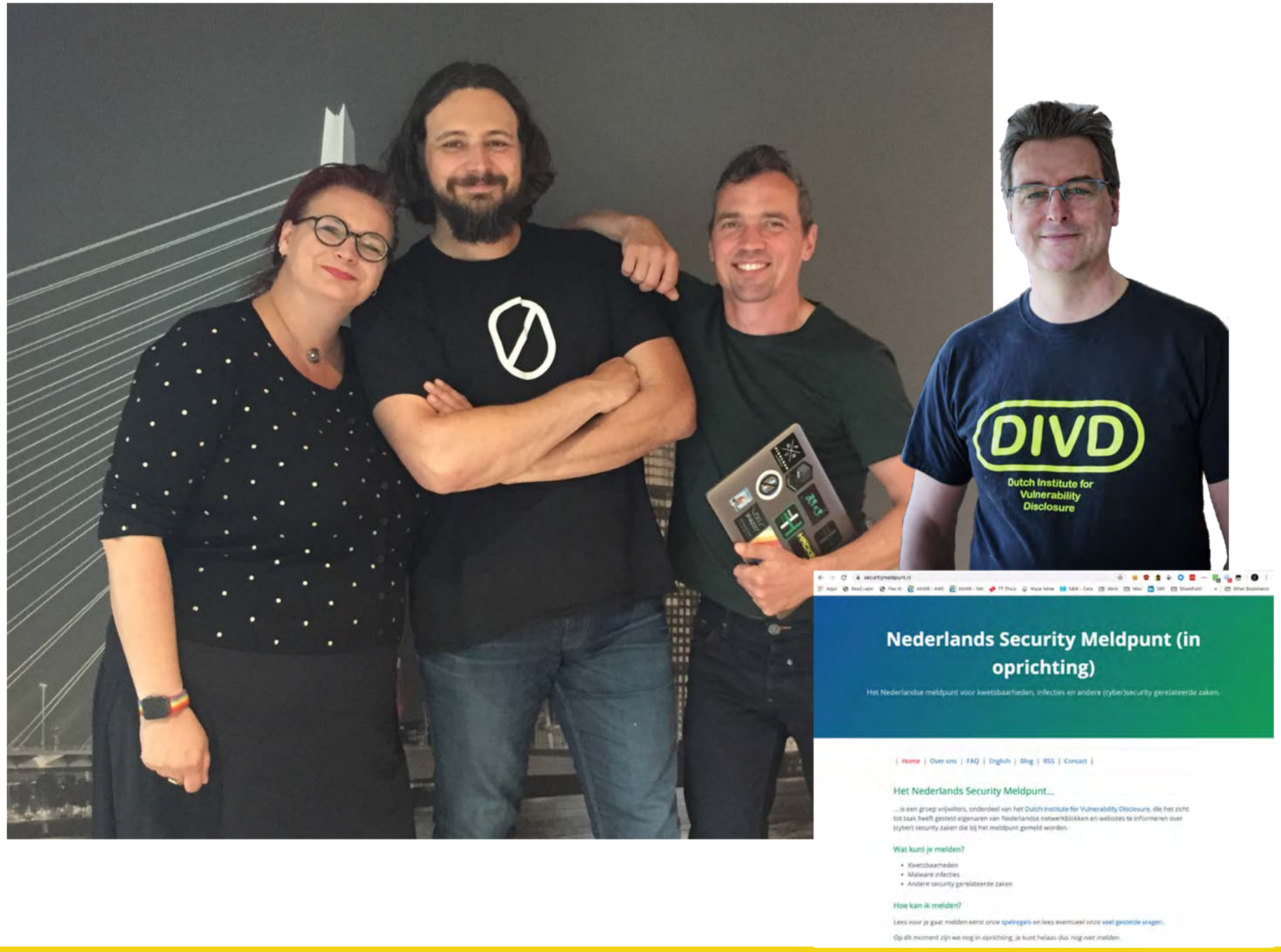
@0xDUDE Follows you

Hacker. 5,499 Responsible Disclosures / Coordinated Vulnerability Disclosures. Researcher @ GDI.foundation / Known as 维克多 葛弗斯 in China.

gdi.foundation

DIVD

26 September 2019



DIVD

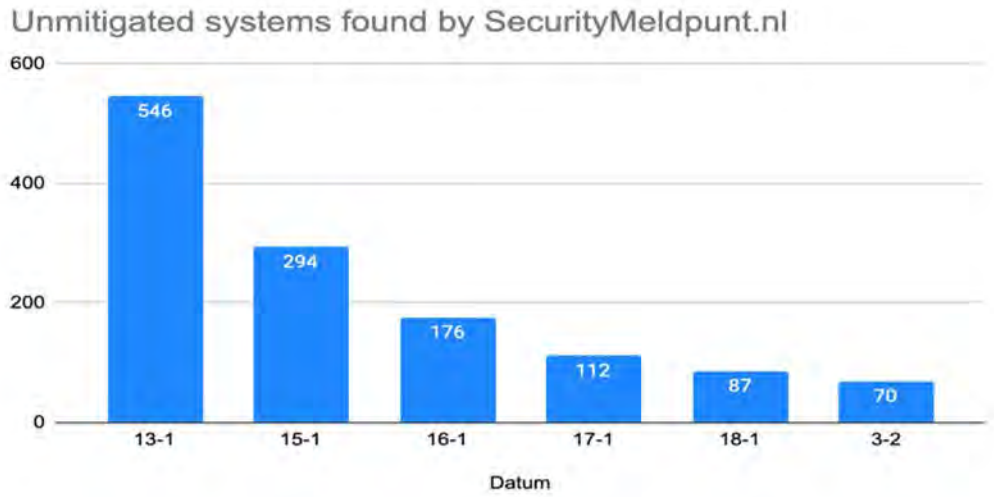
Citrix ADC 2020

20 januari 2020 05:05
Laatste update: 20 januari 2020 11:08

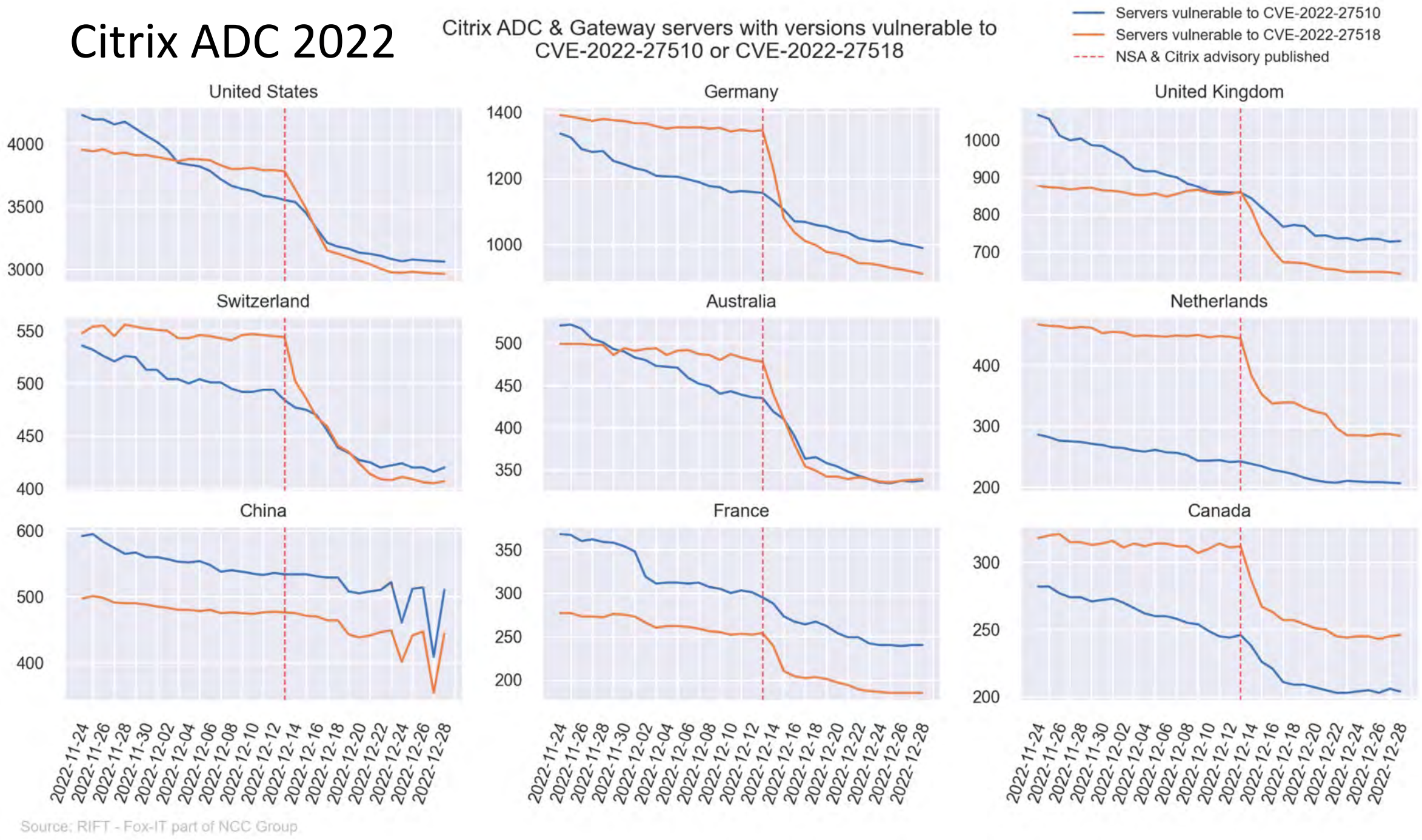
26

Het verkeer moest maandagochtend rekening houden met een drukkere spits vanwege de kans op gladheid en dichte dat files vanwege de Citrix-problemen bovei gebruikelijk. Dat gold met name voor de Rai

De meeste Nederlandse ministeries haalden vr offline vanwege een beveiligingslek, waardoor kunnen werken. Hierdoor verwachtte de ANWE Overheidsmedewerkers gebruiken Citrix norm interne netwerk van ministeries.



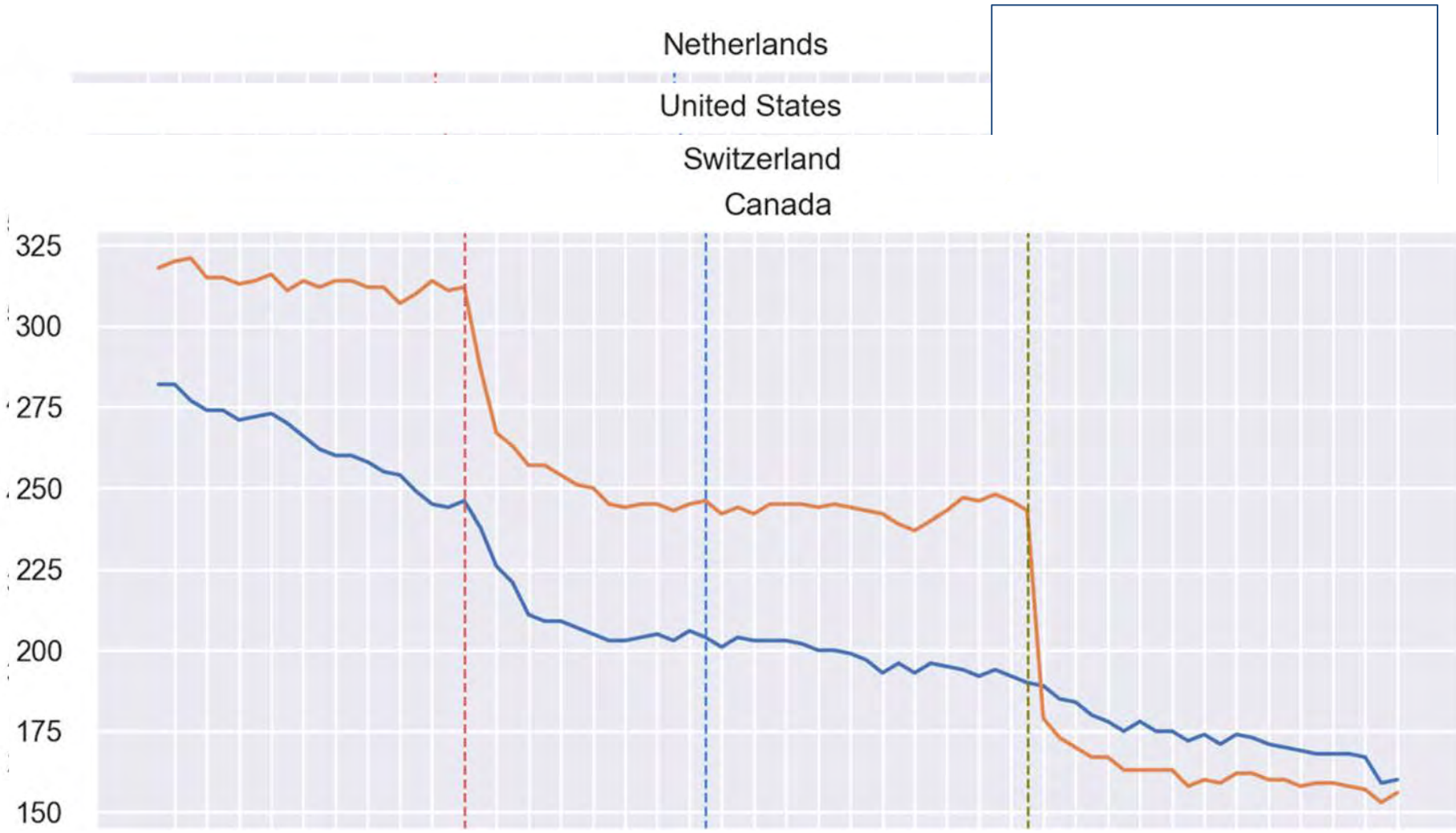
Citrix ADC 2022



DIVD

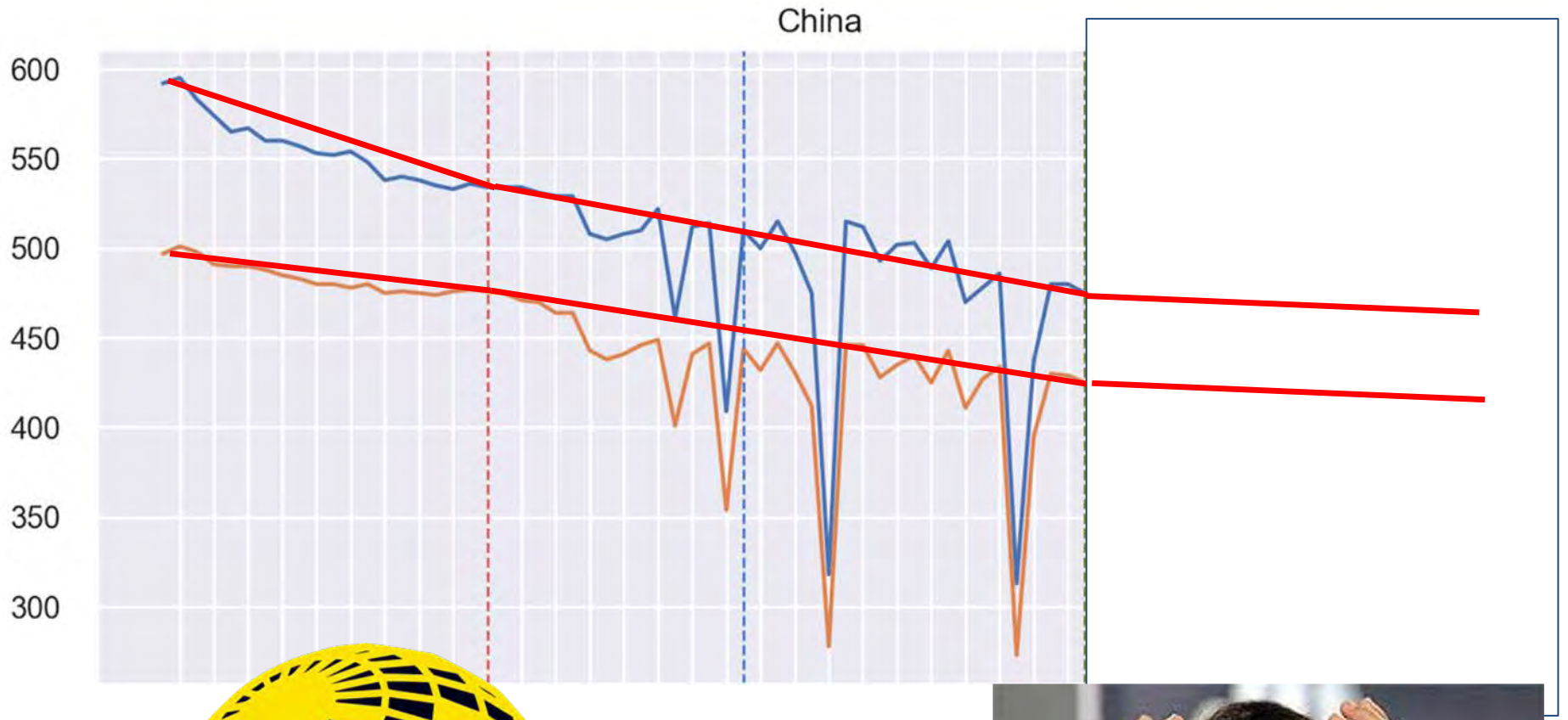
FOX IT
part of nccgroup

Citrix ADC 2022

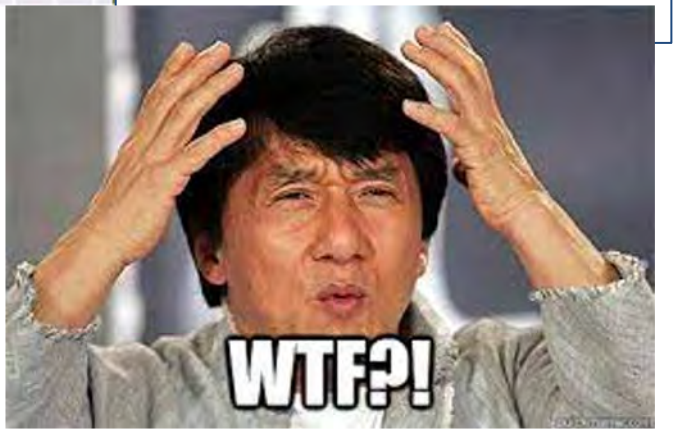


DIVD

DIVD



CSIRT.global
POWERED BY DIVD



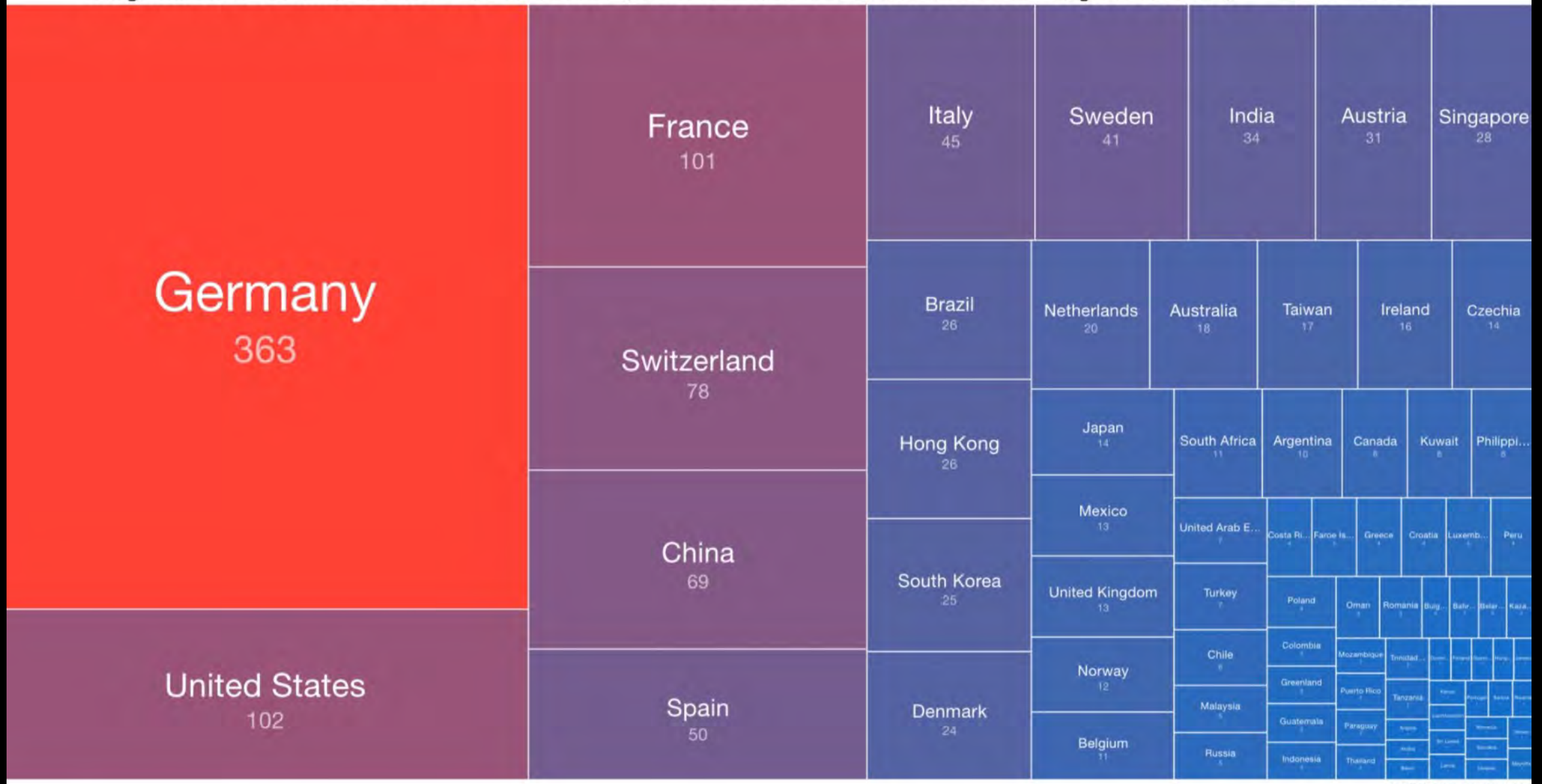
DIVD

Citrix ADC 2023

SHADOWSERVER

FOX IT part of nccgroup

Compromised Citrix NetScaler devices (as a result of CVE-2023-3519 exploitation) - 2023-10-07



Kwetsbaar door software - Lessen naar aanleiding van beveiligingslekken door software van Citrix

december 2019

Startdatum onderzoek
02.07.2020

Publicatiedatum rapport
16.12.2021

Status
Afgerond

Delen

Bekijk het rapport

Yes we (s)can!

Minister Yeşilgöz van
Justitie & Veiligheid
26 Sept 2022:

DIVD

“Het DIVD doet echt uitzonderlijk goed werk en daar zijn wij ontzettend blij mee. Het Nationaal Cyber Security Centrum werkt op dit moment waar mogelijk ook al heel veel samen en zal dit in het nieuwe stelsel ook blijven doen. …

Het DIVD kan op dit moment, in beginsel, door scannen binnendringen in een geautomatiseerd netwerk zonder dat daartegen een strafrechtelijk onderzoek wordt ingesteld. Het moet zich dan wel houden aan de richtlijn van het Openbaar Ministerie met betrekking tot Coordinated Vulnerability Disclosure. Rijksoverheidsorganisaties moeten een wettelijke grondslag hebben of toestemming krijgen van de betrokken organisatie om binnen te mogen treden in geautomatiseerde netwerken, anders is er sprake van strafbaar handelen. Dat is dus best wel een verschil….

Er is dus al een goede samenwerking. Wat ons betreft zullen we altijd blijven zoeken naar een betere samenwerking, want ze hebben natuurlijk wel een hele belangrijke functie.”


Waardevolle
kennis
is gratis

Welcome to the new CVE Beta website! CVE Records have a new and enhanced format. View records in the new format using the CVE ID lookup above or download them on the Downloads page. CVE List keyword search will be temporarily hosted on the legacy cve.mitre.org website until the transition is complete.

CVE® Program Mission

Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

Currently, there are **213,562** CVE Records accessible via Download or Search

The CVE Program partners with community members worldwide to grow CVE content and expand its usage. Click below to learn more about the role of CVE Numbering Authorities (CNAs) and Roots.

Learn More | Become a Partner

Access

- List of Partners
- CNA Rules
- CVE Record Lifecycle
- CVEProject on GitHub for Development
- Idea tracker

Learn

- About CVE
- Process
- Program Organization
- Related Efforts
- Terminology
- CVE Services for CNAs

Report/Request

- Report vulnerability/Request CVE ID
- Request CVE Record be published/updated
- Report the use of a reserved CVE ID

Access Resources Based on Role

CVE Numbering Authority (CNA) | Working Group | Vulnerability Researcher

News

- Legacy CVE Download Formats Will Be Phased Out Beginning January 1, 2024
- Keeper Security Added as CVE Numbering Authority (CNA)
- Lexmark Added as CVE Numbering Authority (CNA)
- 1E Added as CVE Numbering Authority (CNA)

NEWS ICONS

MORE NEWS

Events

- Strategic Planning Working Group (SPWG) Meeting
  Every Wednesday | Virtual
- CNA Coordination Working Group (CNACWG) Meeting
  Every Other Wednesday | Virtual
- CVE Board Meeting
  Every Other Wednesday | Virtual
- CVE Outreach and Communications Working Group

TOTAL RESULTS

3,317

TOP COUNTRIES

United States	1,364
Germany	247
Poland	195
United Kingdom	153
Russian Federation	150

TOP SERVICES

HTTPS	1,582
HTTP	556
8081	360
ntop	134
SIP	62

TOP ORGANIZATIONS

Microsoft Corporation	364
Amazon Technologies Inc.	327
DigitalOcean, LLC	233
Amazon.com, Inc.	227
Amazon Data Services NoVa	88

TOP OPERATING SYSTEMS

Debian	3
QTS	2
Ubuntu	2

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

婚約指輪完全ランキング | ブライダル専門店に特化!

153.120.92.171
ring.how-to-inc.com
SAKURA Internet Inc.
Added on 2021-05-05 13:45:15 GMT
Japan, Tokyo
Technologies:
Cart Functionality
jQuery Migrate

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 05 May 2021 13:45:14 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-Powered-By: PHP/7.0.11
Link: <https://how-to-inc.com/engagement-ring/wp-json/>; rel="https://api.w.org/"
Stri...
```

185.44.0.40

Amayama network
Added on 2021-05-05 13:52:53 GMT
Russian Federation, Moscow
Technologies:

```
HTTP/1.1 200 OK
Server: nginx
Date: Wed, 05 May 2021 13:52:53 GMT
Content-Type: text/html; charset=windows-1251
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: ring=4b1a00eTu0LNa9P%2FF1VMEcN1DLEvg0a9; expires=Thu, 05-May-2022 13:52:53 GMT; Max-Age=31536000;
```

20.190.157.31

Microsoft Corporation
Added on 2021-05-05 13:38:46 GMT
United States, San Antonio

cloud

SSL Certificate

Issued By:
|- Common Name: **Microsoft Azure TLS Issuing CA 01**
|- Organization: **Microsoft Corporation**
Issued To:
|- Common Name: **graph.microsoft.com**
|- Organization: **Microsoft Corporation**

Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2

```
HTTP/1.1 301 Moved Permanently
Date: Wed, 05 May 2021 13:38:44 GMT
Transfer-Encoding: chunked
Location: https://developer.microsoft.com/graph
Strict-Transport-Security: max-age=31536000
request-id: 23da360b-f281-4e9c-b0f4-52fc3556dbf5
client-request-id: 23da360b-f281-4e9c-b0f4-52fc3556dbf5
...
```

censys.io

censys | IPv4 Hosts | Search | Register | Sign In

Relational Database Exposure Dashboard

Quick Glance Numbers

Database Servers	MySQL Servers	MSSQL Servers	Postgres Servers	Oracle Servers
5.7M	4.8M	635.8K	605.0K	92.6K

MySQL Exposure

	Autonomous System (AS)	MySQL Servers
1.	OVH	217.9K
2.	EGIHOSTING - EGIHosting	178.8K
3.	UNIFIEDLAYER-AS-1 - Unified Layer	174.2K
4.	AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC	166.2K
5.	HOMEPL-AS	164.3K
6.	AMAZON-02 - Amazon.com, Inc.	144.4K
7.	ENZUINC-US - Enzu Inc	104.1K
8.	DIGITALOCEAN-ASN - DigitalOcean, LLC	90.9K
9.	HETZNER-AS	78.8K
10.	CNNIC-TENCENT-NET-AP Shenzhen Tencent Computer S...	76.2K
	Grand total	**4.8M**

1 - 10 / 21670

Home Notify me Domain search Who's been pwned Passwords API About Donate

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

rob.bertholee@aivd.nl pwned?

Oh no — pwned!

Pwned on 4 breached sites and found no pastes (subscribe to search sensitive breaches)

Internet.nl
IS YOUR INTERNET UP TO DATE?

English Nederlands

Home Nieuws Kennisbank Hall of Fame Over Internet.nl

Moderne Internetstandaarden zorgen voor meer betrouwbaarheid en verdere groei van het Internet.
Gebruik jij ze al?

Test je website

Modern adres? Beveiligde verbinding? Beveiligingsopties? Route-autorisatie?

over de test ›

Jouw website-domeinnaam:

www.example.nl

Start test

Test je e-mail

Modern adres? Anti-phishing? Beveiligd transport? Route-autorisatie?

over de test ›

Jouw e-mailadres:

@ example.nl

Start test

Test je verbinding

Moderne adressen bereikbaar? Domein-handtekeningen gecontroleerd?

over de test ›

Start test

Nieuws

- Verbeterde testen voor CSP en security.txt op Internet.nl ›
- Universal Acceptance Day - #Internet4all ›
- Internet.nl voegt test voor security.txt toe ›
- Nieuwe release van Internet.nl met RPKI-test ›
- Onderhouds- en bugfixrelease van Internet.nl ›
- Platform Internetstandaarden: "Aandacht voor verdere adoptie IPv6 ›

Hall of Fame

3782 domeinen met 2 x 100%
Laatste toevoeging: 10-10-2023

- ✓ forumstandaardisatie.nl
- ✓ floorlabel.nl
- ✓ verbindingstoernooi.rwsduurzamespelen.nl
- ✓ rfa.cz
- ✓ www.rijksapplicaties.nl
- ✓ www.blgwonen.nl
- ✓ zuiderzeeland.nl
- ✓ alu.hr
- ✓ zwn24.nl
- ✓ xolx.nl

Tests in cijfers

579883 unieke web-domeinen

✓ 100%:	31266
× 0-99%:	548617

253169 unieke mail-domeinen

✓ 100%:	12074
× 0-99%:	241095

25337 unieke verbindingen

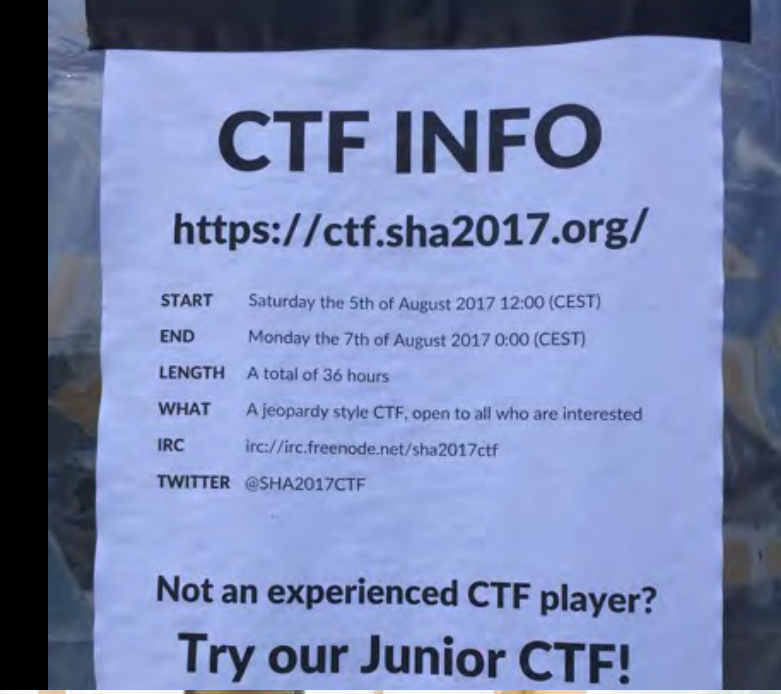
✓ 100%:	9230
× 0-99%:	16107


Volledig scherm
Risico's
DNS beveiliging (DNSSEC)
Transport Layer Security (TLS)
Ontbreken van versleuteling
Strict-Transport-Security Header (HSTS)
X-Frame-Options Header (clickjacking)
X-XSS-Protection Header
X-Content-Type-Options Header
Moment
2018 week 22
<<< -1 week
+1 week >>>
De basisbeveiliging is:
Perfect
Goed
Matig
Slecht
Onbekend
Url
Sealand
Brussels
Belgium
Lille
Goed
Matig
Slecht
Onbekend
HACK
TALK

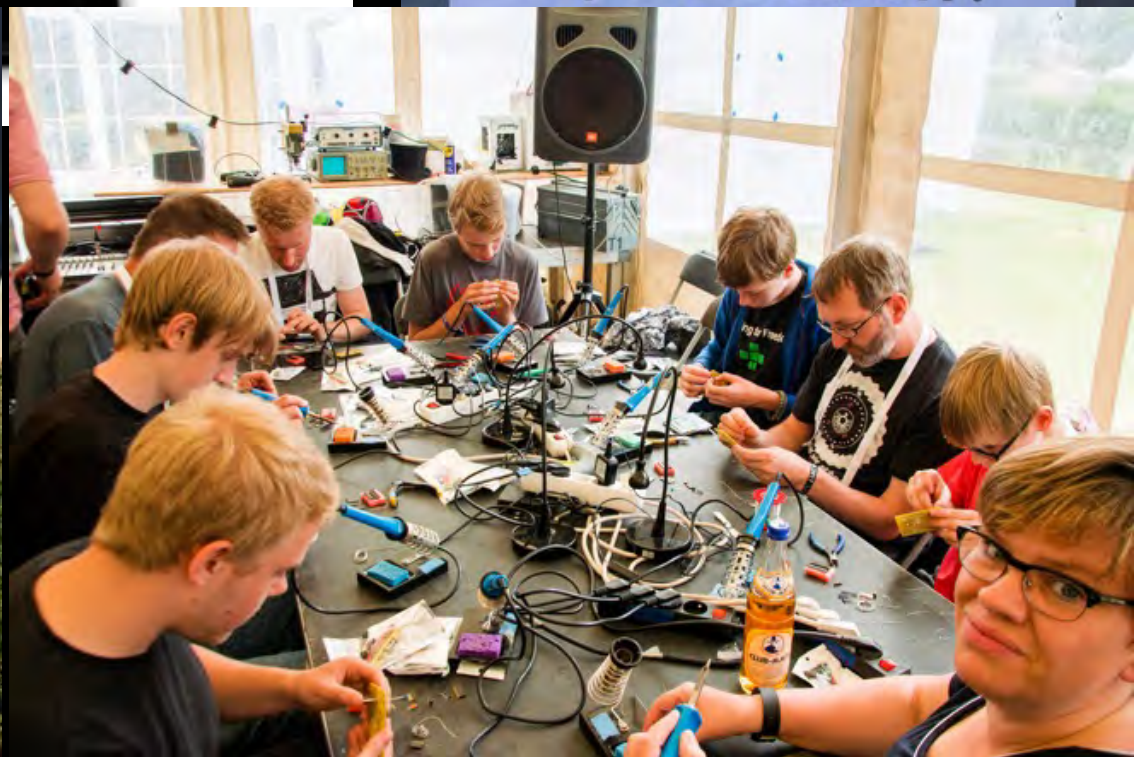

SHIA2017


Datacenters
3 datacentres spread over thee sites with existing telco rack
30kw of cooling capacity
Colocation hosting for
NOC (2 flightcases)
Sysadmin (2 flightcases)
POC (3 huge flightcases)
VOC/AV/Productiehuis (1 flightcase)


CRYPTOGRAPHIC
HASH FUNCTIONS
WORLD TOUR
1989 MD2 BROKEN, STILL CRITICAL
1990 SNEFRU MORE LIKE SNAFU
1990 MD4 SEVERELY COMPROMISED
1992 MD5 RAINBOWS EVERYWHERE
1992 RIPEMD RIP IN PIECES MD
1992 HAVAL-128 IS IE KAPOT?!
1993 SHA-0 NOT IN YOUR LIBRARY
1995 SHA-1 FOR DECORATION ONLY
1996 RIPEMD-160 STILL GOING STRONG
2001 SHA-2 COMPANY UPGRADE
2015 SHA-3 BREAKING RESEARCH
2017 SHA-2017 STILL HACKING ANYWAY


CTF INFO
https://ctf.sha2017.org/
START Saturday the 5th of August 2017 12:00 (CEST)
END Monday the 7th of August 2017 0:00 (CEST)
LENGTH A total of 36 hours
WHAT A jeopardy style CTF, open to all who are interested
IRC irc://irc.freenode.net/sha2017ctf
TWITTER @SHA2017CTF
Not an experienced CTF player?
Try our Junior CTF!

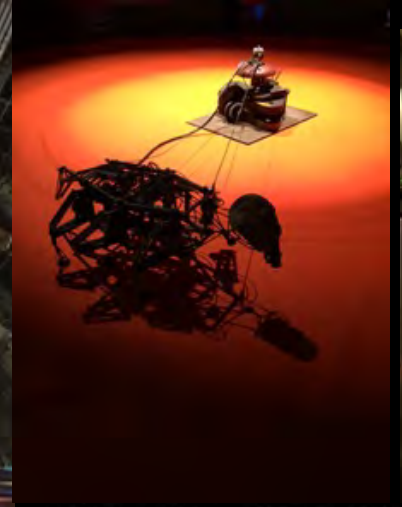

ZUM ANEUFEN:
Kurbel einmal drehen
ZUM SPEECHEN:
Knopf im Hörer drücken

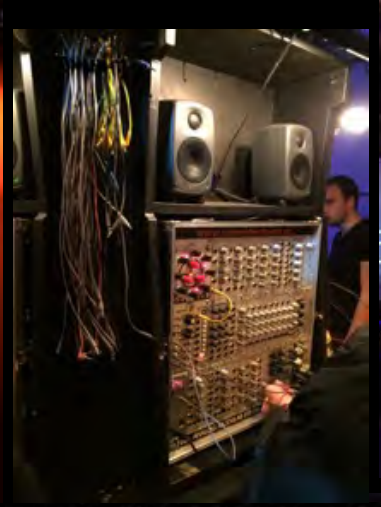



Mass Surveillanc
William Binney
Former Technical Director
SA


leaseweb
reliable hosting


Nerds hebben
de beste
feestjes





34. Chaos Communication Congress

27. - 30. Dezember 2017

Leipzig, Messegelände

rOwaR!

CHOOSE A NETWORK...

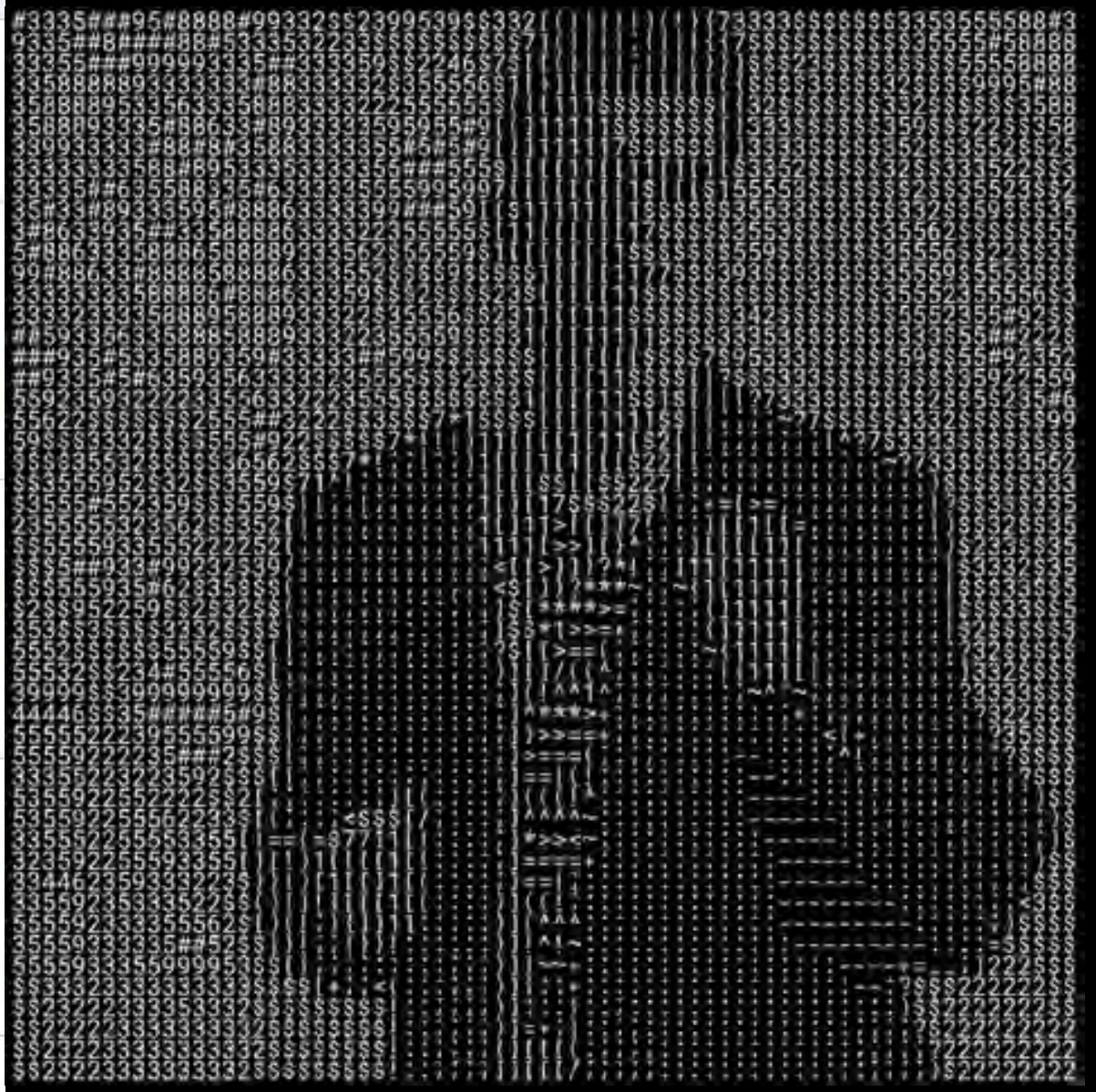
01 Never gonna give y...

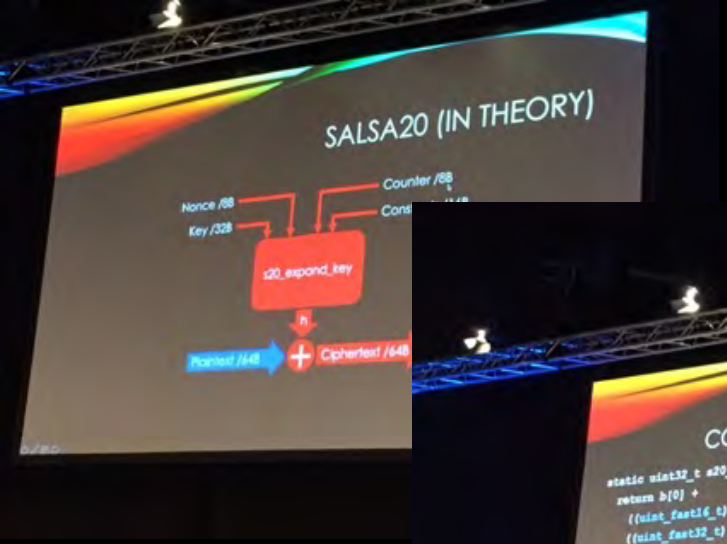
02 Never gonna let you down

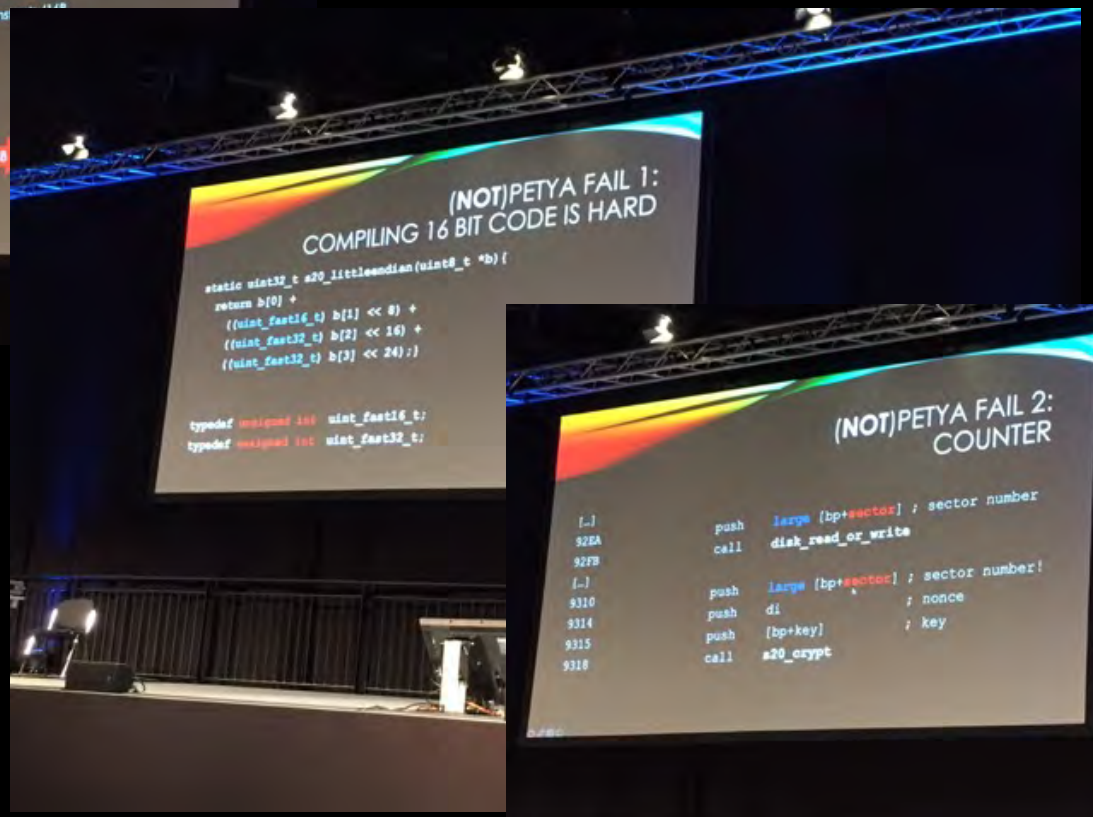
03 Never gonna run around

04 Never gonna make you cry

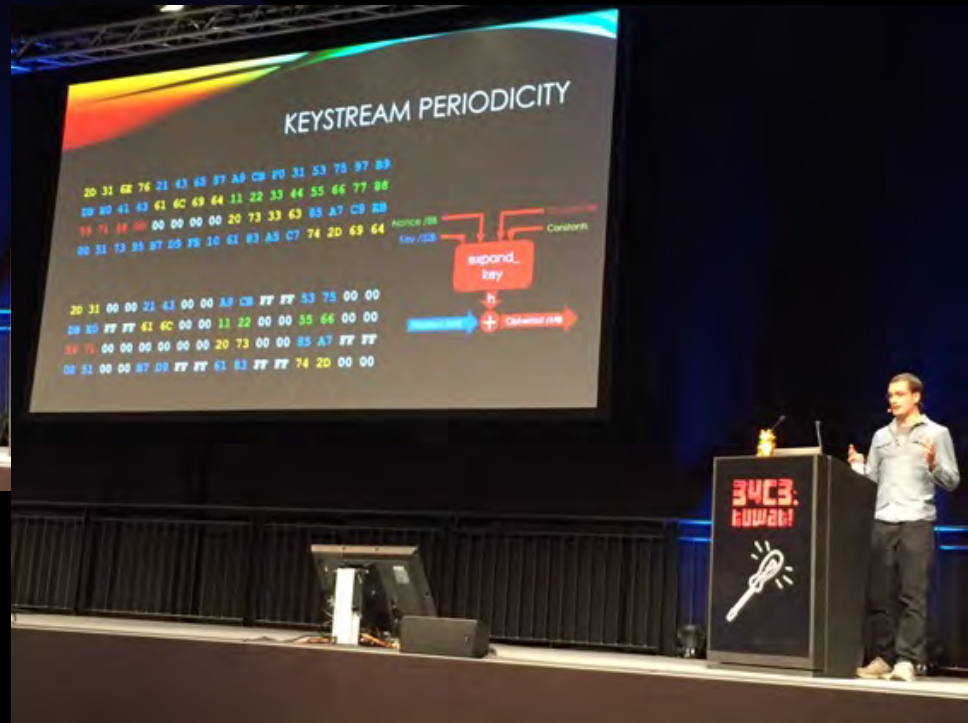
05 Never gonna say




SALSA20 (IN THEORY)
Nonce /88
Counter /88
Key /328
s20_expand_key
h
Plaintext /648
Ciphertext /648


(NOT)PETYA FAIL 1:
COMPILING 16 BIT CODE IS HARD
static uint32_t s20_littleendian(uint8_t *b){
return b[0] +
((uint_fast16_t) b[1] << 8) +
((uint_fast32_t) b[2] << 16) +
((uint_fast32_t) b[3] << 24);}
typedef unsigned int uint_fast16_t;
typedef unsigned int uint_fast32_t;

(NOT)PETYA FAIL 2:
COUNTER
[...]
92EA
92FB
[...]
9310
9314
9315
9318
push large [bp+sector] ; sector number
call disk_read_or_write
push large [bp+sector] ; sector number!
push di ; nonce
push [bp+key] ; key
call s20_crypt


KEYSTREAM PERIODICITY
expand_
key
h
Nonce /88
Key /328
Constants
Plaintext /648
Ciphertext /648
34C3:
tuwat!

Aanval met NotPetya-malware kost Maersk tot 256 miljoen euro

Logistiekbedrijf Maersk zegt dat de malwareaanval waar het eind juni door getroffen werd, een financiële impact heeft van 200 tot 300 miljoen dollar, omgerekend zo'n 171 tot 256 miljoen euro. De exacte schade zal in het volgende kwartaal duidelijk worden.

Maersk maakt de schatting bekend in een tussentijds rapport over de cijfers van het tweede kwartaal. Het bedrijf zegt dat de financiële impact van de malwareaanval grotendeels pas in het volgende kwartaal zichtbaar zal zijn, door misgelopen inkomsten en 'buitengewone' it-kosten. Het Deense bedrijf heeft voor nu alleen een schatting gegeven. Mogelijk maakt het bij de presentatie van de cijfers over het derde kwartaal specifieker bekend wat de misgelopen inkomsten zijn en hoeveel is uitgegeven aan beveiligingsmaatregelen.

NO MORE RANSOM

Aangifte doen

Crypto-sheriff

Vul het onderstaande formulier in om ons te helpen identificeren door welk type ransomware uw apparaat is geïnfecteerd. Hiermee kunnen wij nagaan of er een oplossing beschikbaar is. Als dit het geval is, sturen wij u een link waarmee u de ontsleutelingsoplossing kunt downloaden.

Door bestanden te versturen ter beoordeling, ga ik akkoord met de VOORWAARDEN VOOR GEGEVENSVERSTREKKING.

Versleutelde bestanden hier uploaden (mag niet groter zijn dan 1 MB)

Eerste bestand selecteren

Tweede bestand selecteren

Vul hieronder alle e-mailadressen, website-URL's, onion- en/of bitcoinadressen in die u ziet in het LOSGELDBERICHT. Let op: zorg ervoor dat u de exacte spelling van deze adressen overneemt.

Of upload het door de criminelen verstuurde bestand (.txt or .html) met het losgeldbericht

02 oktober 2023 // Updates

Dit was Hâck The Hague 2023

Vandaag zijn de digitale systemen van de gemeente Den Haag getest door 116 ethische hackers. Tijdens de zes uur durende hackwedstrijd zijn 65 unieke meldingen van kwetsbaarheden ingediend. Zes meldingen waren kwetsbaarheden met een hoog risico. Nog eens zes meldingen zijn tijdens de dag zelf opgelost. Er kwamen vooral veel meldingen binnen die te maken hadden met een fout in de beveiliging van een webapplicatie.


Cylock®
The electromechanical key system


PARTNERS
TREND MICRO
BDO
kpn
DARKTRACE
mnemonic
zerocopter
National Cyber Security Centre
Ministry of Justice and Security
TARGETS
ARS T&TT
axiell
ANOIGO
ComBus
ultimate IoT connectivity
expoints
share experiences
FORTES
intus
sensus
process management
recourse
centric
connect.engage.succeed.
TOPdesk
abf
The Hague


MOST SOPHISTICATED HACK - 1ST PRIZE
€ 2.500,-
HÂCK
THE HAGUE
2023 5TH EDITION


Pas veilig als
je gehackt
bent

1. Cyberellende zo oud als de Oudheid
2. Hackers kunnen helpen
3. Informatiebeveiliging open wereld
4. Meest waardevolle kennis is gratis
5. Nerds organiseren de beste feestjes
6. Je bent pas veilig als je gehackt bent
7. ?


Gratis
taart
voor iedereen

Hackers zien dingen anders dan anderen

H4CK3R$ z13N D1Ng3N
4Nd3R$ d4N 4Nd3R3N

H4CK3R$

z13N

D1Ng3N

4Nd3R$

d4N

4Nd3R3N

H4CK3R$

z13N

D1Ng3N

4Nd3R$

d4N

4Nd3R3N

H4CK3R$

z13N

D1Ng3N

4Nd3R$

d4N

4Nd3R3N

WARNING!

A fatal exception just occurred in your brain. All currently running biases towards hackers will be terminated.
To continue, download and install a free update at www.cyberellende.nl
You don’t have to press any key to continu, just read _