Cybersecurity threats | in de huid van een hacker

13 september 2022 - Dag van de Domeinnaam

+31 (0)20-7881030

info@networking4all.com

https://www.networking4all.com

NETWORKING4ALL

LEADING IN CYBERSECURITY SOLUTIONS

MEET THE **ETHICAL** HACKERS

Cybersecurity threats | Agenda

MEET THE **HACKERS**

CYBERSECURITY THREATS | AGENDA

BEROEPS CRIMINEEL

CRIMINELE ORGANISATIE

OVERHEID

VRAAG: **Hoeveel Nederlanders waren volgens het CBS slachtoffer van online criminaliteit, in 2021**

A. 748.000

B. 1.500.000

C. 2.500.000

Geregistreerde “normale” misdrijven 2021: 754.000

HACKTIVIST

Anoniem actie voeren...

- Ideologisch of politiek doel
- Data publiekelijk maken, cyberaanvallen
- Een bekende groep is Anonymous.

CYBERVANDAAL

Alias: Script Kiddie

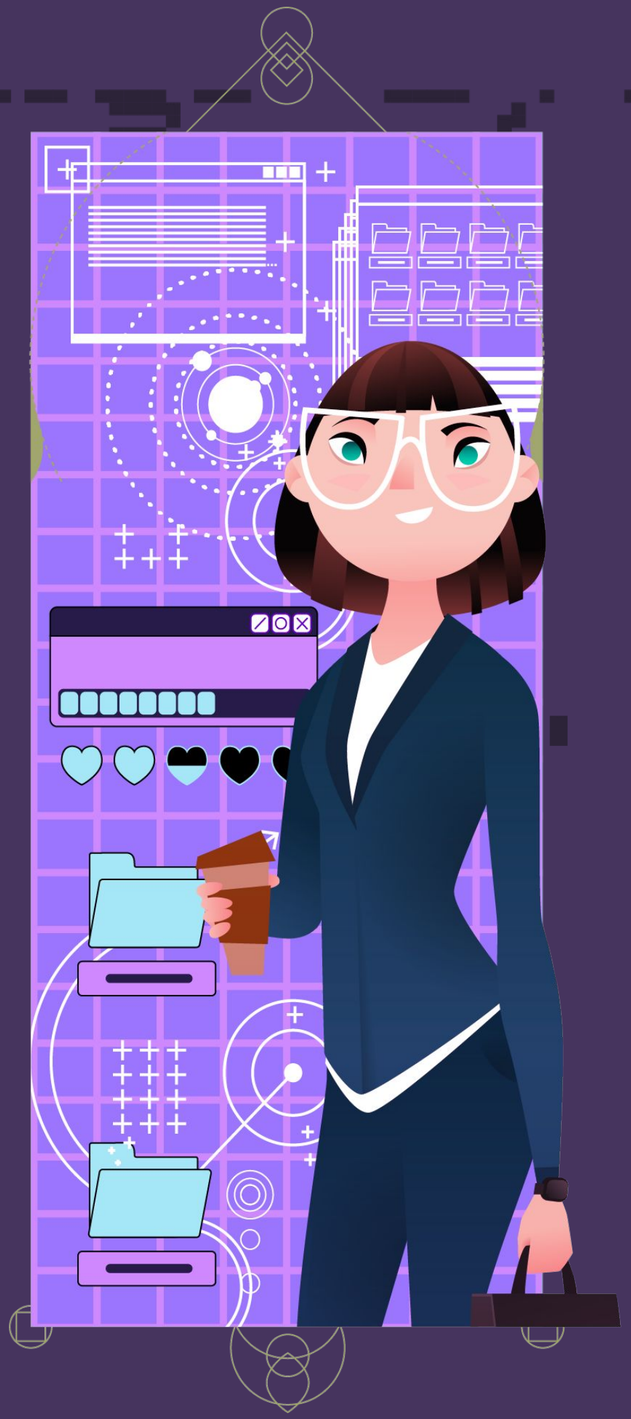
- Hoe ver kan ik komen?
- Niet bewust van de gevolgen
- Vaak erg jong, gebruiken veel standaard scripts en diensten

FBI laat Leidse tiener oppakken voor uitvoeren DDoS-aanvallen

Politie arresteert tiener die overheidssite platlegde

Mijnoverheid.nl en Overheid.nl lagen uren plat na DDoS-aanval

Verdachte DDoS-aanvallen: banken moeten het op orde hebben



GEMOTIVEERDE INDIVIDUEN

Voor mij was het alsof het een game was

- Motivatie soms financieel
- Status
- Uitdaging

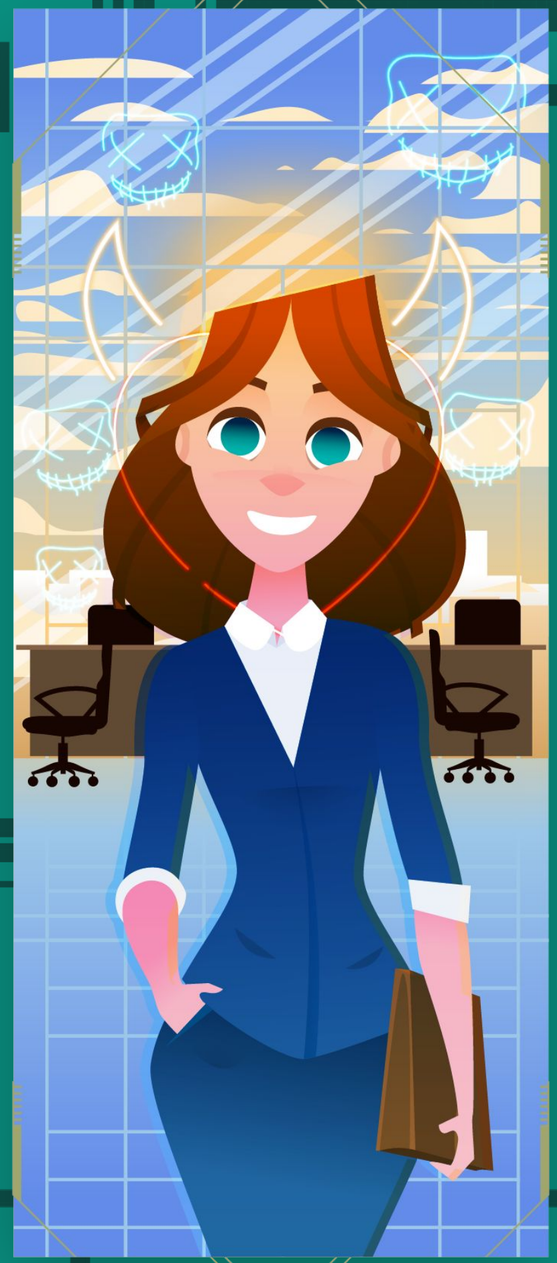
16- en 17-jarige jongens vast voor KPN-hack

26 maart 2012 17:00
Aangepast: 26 maart 2012 17:30

INSIDER

Ik kon wel wat extra geld gebruiken...

- Informatie voor concurrentie
- 83% nog altijd toegang bij ex-werkgever
- Broncode software



DE GOED GEORGANISEERDE CRIMINELE ORGANISATIE

Wij persen eerlijk af

- Bankfraude
- Afpersing
- Malware & ransomware

TERRORIST

Aanvallen zonder te hoeven reizen.

- Ontwrichting
- Virtueel als Fysiek
- Goedkoper dan traditioneel terrorisme

OVERHEID

Alles in het belang voor de veiligheid van de burger

- 0-days
- intellectuele eigendom, handel's informatie, afluisteren van gesprekken en belangrijke documenten.
- Doel heiligt vaak de middelen

BEROEPS CRIMINEEL

Hard werken: het domste dat je kunt doen

- Phishing
- Identiteitsfraude
- Uitbuiten van kwetsbaarheden


admin password: password
admin password: password
admin password: p@ssword
admin password: !Password
admin password: p4ssw0rd
admin password: p455w0rd
admin password: password!
admin password: password1
admin password: password2
admin password: password3
admin password: 1234
admin password: 1111
admin password: 0000
admin password: admin
admin password: Admin
admin password: !Admin
admin password: 1980
admin password: admin1980
admin password: !admin1980
PATCHING

IPV4 COLLECTING

102.129.242.124

102.129.242.125

102.129.242.126

In kaart brengen van ip4-nummers (CDIR)

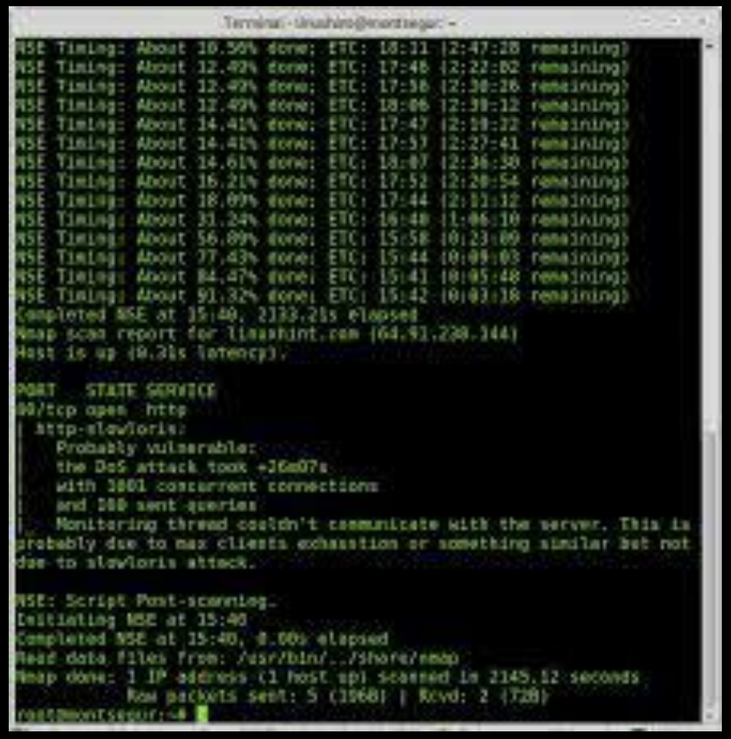
RIPE DATABASE

Querying the RIPE Database

```
role:           RIPE NCC Registration Services Department
address:        RIPE Network Coordination Centre (NCC)
address:        P.O. Box 10096
address:        1001 EB Amsterdam
address:        The Netherlands
phone:          +31 20 535 4444
fax-no:         +31 20 535 4445
nic-hdl:        CREW-RIPE
mnt-by:         RIPE-NCC-HM-MNT
created:        2002-09-23T10:13:06Z
last-modified:  2020-01-10T13:08:46Z
source:         RIPE
```

Domeinnamen gekoppeld aan ip-nr’s

IP4 SCANNING



- Poorten
- Software
- Automatiseren
- Logging

CVE-2022-36917	
CVE-2021-43298	The code that performs password matching when using 'Basic' HTTP authentication does not use a constant-time memcmp and has no rate-limiting. This means that an unauthenticated network attacker can brute-force the HTTP basic password, byte-by-byte, by recording the webserver's response time until the unauthorized (401) response.
CVE-2022-2578	
CVE-2022-28796	
CVE-2022-24514	
CVE-2022-2768	
CVE-2022-253	
CVE-2022-976	
CVE-2022-324	

AANMAKEN **DATABASE** MET **ALLE** RECENTE **CVE'S**

(kwetsbaarheden)

CVE
KOPPELING

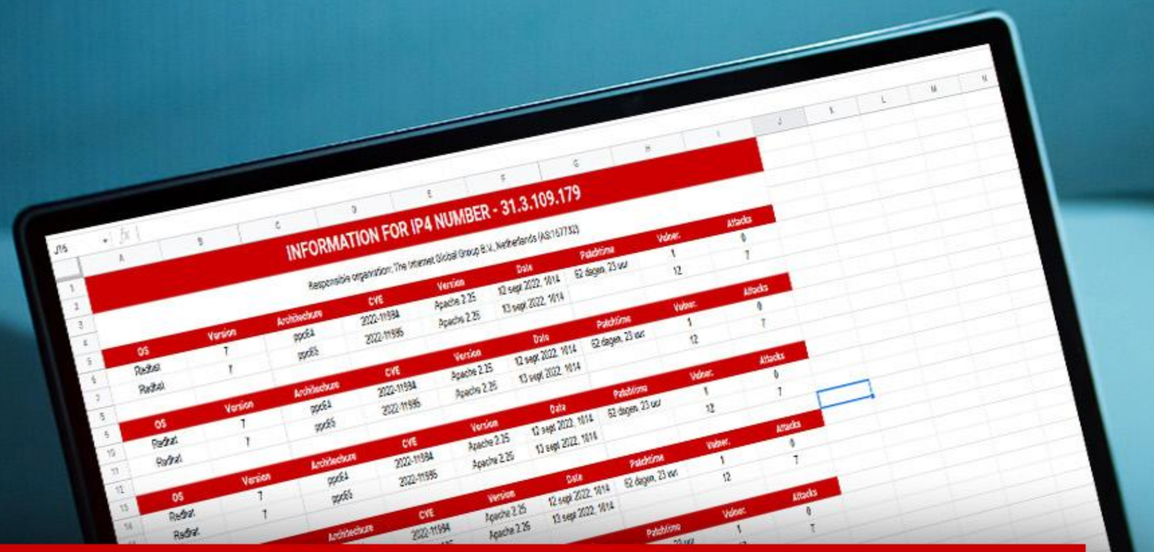
CVE Data
Alle bekende vulnerabilities

Eigen Data
Info welk bedrijf op welke versie zit

Auto_Hack.php
Misbruik kwetsbaarheid hack binnen 15 min

HISTORY

AVERAGE PATCH TIME **89 DAYS**



INFORMATION FOR IP4 NUMBER - 31.3.109.179

Responsible organistion: The Internet Global Group B.V., Netherlands (AS:167732)

OS	Version	Architechure	CVE	Version	Date	Patchtime	Vulner.	Attacks
Redhat	7	ppc64	2022-11994	Apache 2.25	12 sept 2022, 1014	62 dagen, 23 uur	1	0
Redhat	7	ppc65	2022-11995	Apache 2.22	13 sept 2022, 1014		12	7

SNEL PATCHEN **IS BELANGRIJK**

Hackers scan for vulnerabilities within 15 minutes of disclosure

By **Bill Toulas** July 26, 2022 03:44 PM 2

27 July 2022

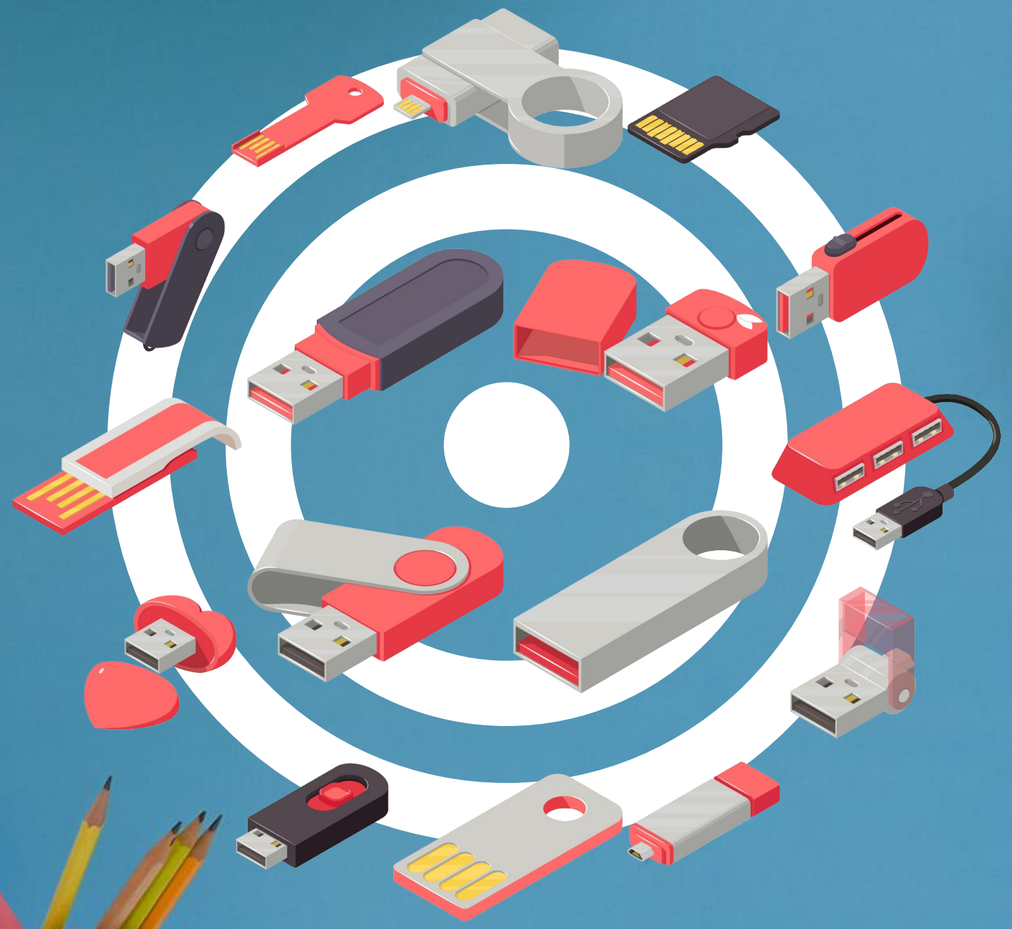
Threat actors start scanning for vulnerabilities within 15 minutes of a CVE public disclosure

Hackers now exploit new vulnerabilities in just 15 minutes

DE GOED GEORGANISEERDE CRIMINELE ORGANISATIE

Betalen is nog de enige mogelijkheid

- Uitbuiten kwetsbaarheden
- Ransomware
- Social engineering



USB DUCK HUNTING

USB AANVAL

RUBBER DUCKY IN EEN POWERBANK

THE GIVEAWAY THAT GIVES YOU(R DATA) AWAY

VERENIGING VAN REGISTRARS

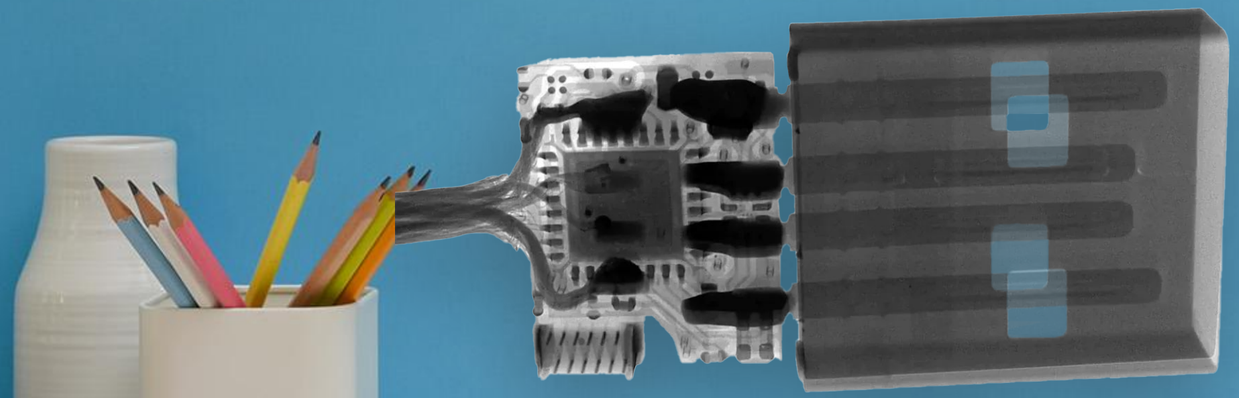
Privacy statement

Copyright © VvR 2022

Ontwikkeld door Web Whales

OMG! CABLE


O.MG
SYSLOG
KEYLOG
PAYLOAD
1 DUCKY_LANG US
2 REM simple hello world script
3 STRING Hello,
4 WRITE World!
ERROR: Unrecognized command:
'WRITE'. Did you mean 'STRING'?
5 ENTER
SAVE
LOAD
RUN




PWR
CABLE
ACT
O.MG

REAL OR DUCK


Microsoft
Office
Professional Plus
1 PC
2021
PRODUCT KEY INSIDE-NO DISC


OFFICE 2021 PRO PLUS
X22-62826


HOTEL

PHISHING &SOCIALS

DAAR **TRAP IK** **NIET** MEER **IN**

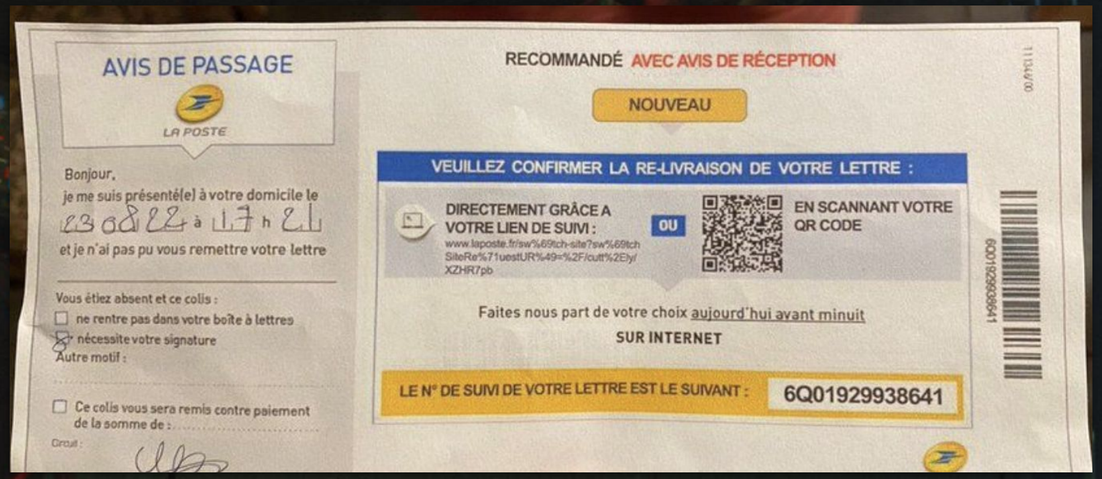
CONTACT

VERTROUWEN

BEDRIJFSNETWERK

Linkedin post

QRCODE


AVIS DE PASSAGE

LA POSTE

Bonjour,
je me suis présenté(e) à votre domicile le
[illegible] à 17 h 21
et je n'ai pas pu vous remettre votre lettre

Vous étiez absent et ce colis :
☐ ne rentre pas dans votre boîte à lettres
☒ nécessite votre signature
Autre motif :

☐ Ce colis vous sera remis contre paiement de la somme de :

Circuit :

RECOMMANDÉ AVEC AVIS DE RÉCEPTION

NOUVEAU

VEUILLEZ CONFIRMER LA RE-LIVRAISON DE VOTRE LETTRE :

DIRECTEMENT GRÂCE A VOTRE LIEN DE SUIVI :
www.laposte.fr/sw%69tch-site?sw%69tchSiteRe%71uestUR%49=%2Fcutt%2Ely/XZHR7pb

OU

EN SCANNANT VOTRE QR CODE

Faites nous part de votre choix aujourd'hui avant minuit
SUR INTERNET

LE N° DE SUIVI DE VOTRE LETTRE EST LE SUIVANT : 6Q01929938641

6Q01929938641

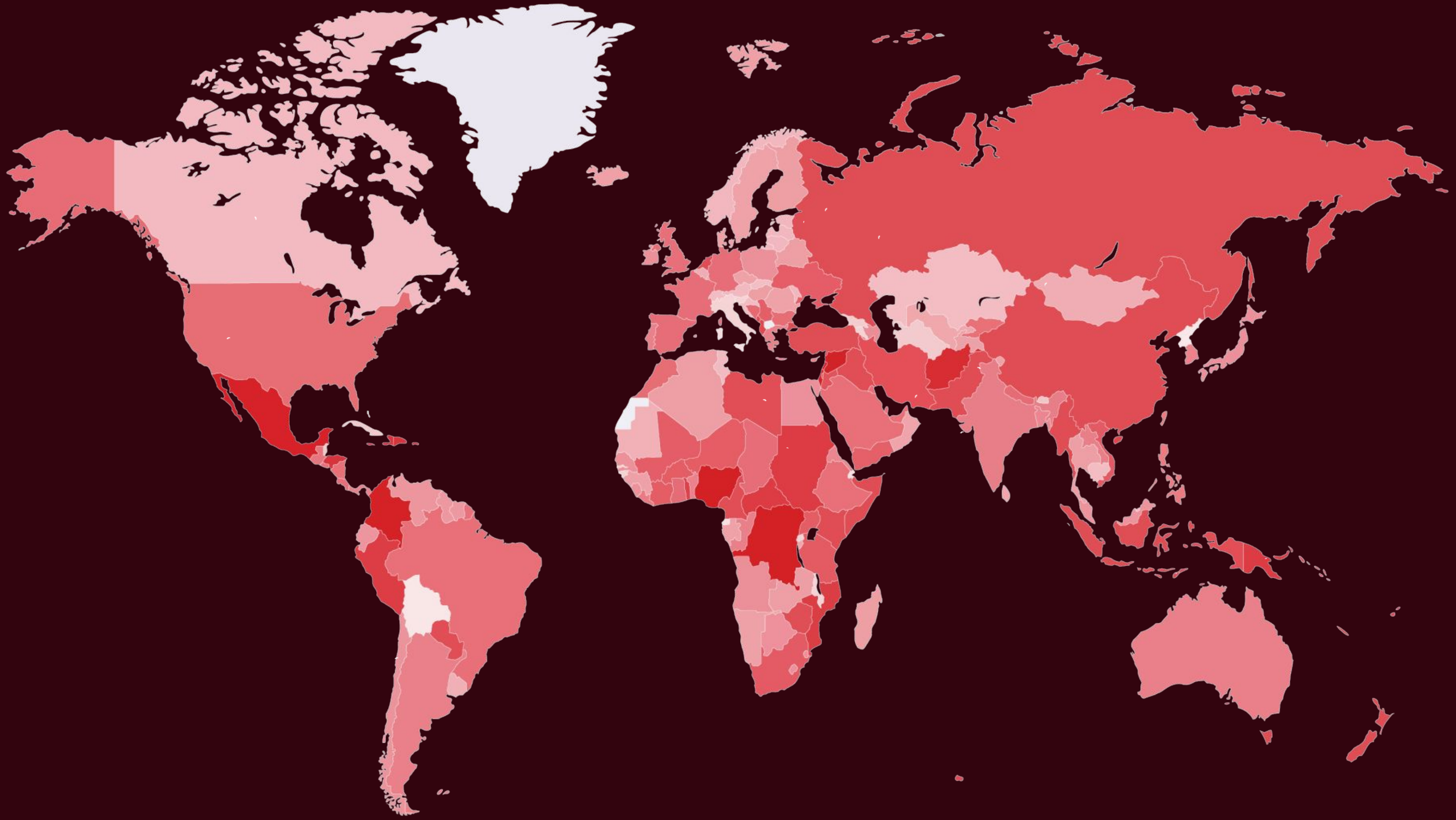
GitHub

Google Play

OVERHEID

Er zijn geen grenzen...

- 0-days
- Grijs gebied
- Doel heiligt de middelen



ZERODAYS

TECHNOLOGY > CYBERSECURITY | August 25, 2022 | updated 26 Aug 2022 4:27am

Apple zero day vulnerability on the market for €8 million

A 12 month warranty – in case the flaw gets patched – and a cloud-based code injection are also on offer as part of the package.

By Ryan Morrison

pple's mobile operating system iOS that allows for remote
n advertised for sale for €8m, according to leaked

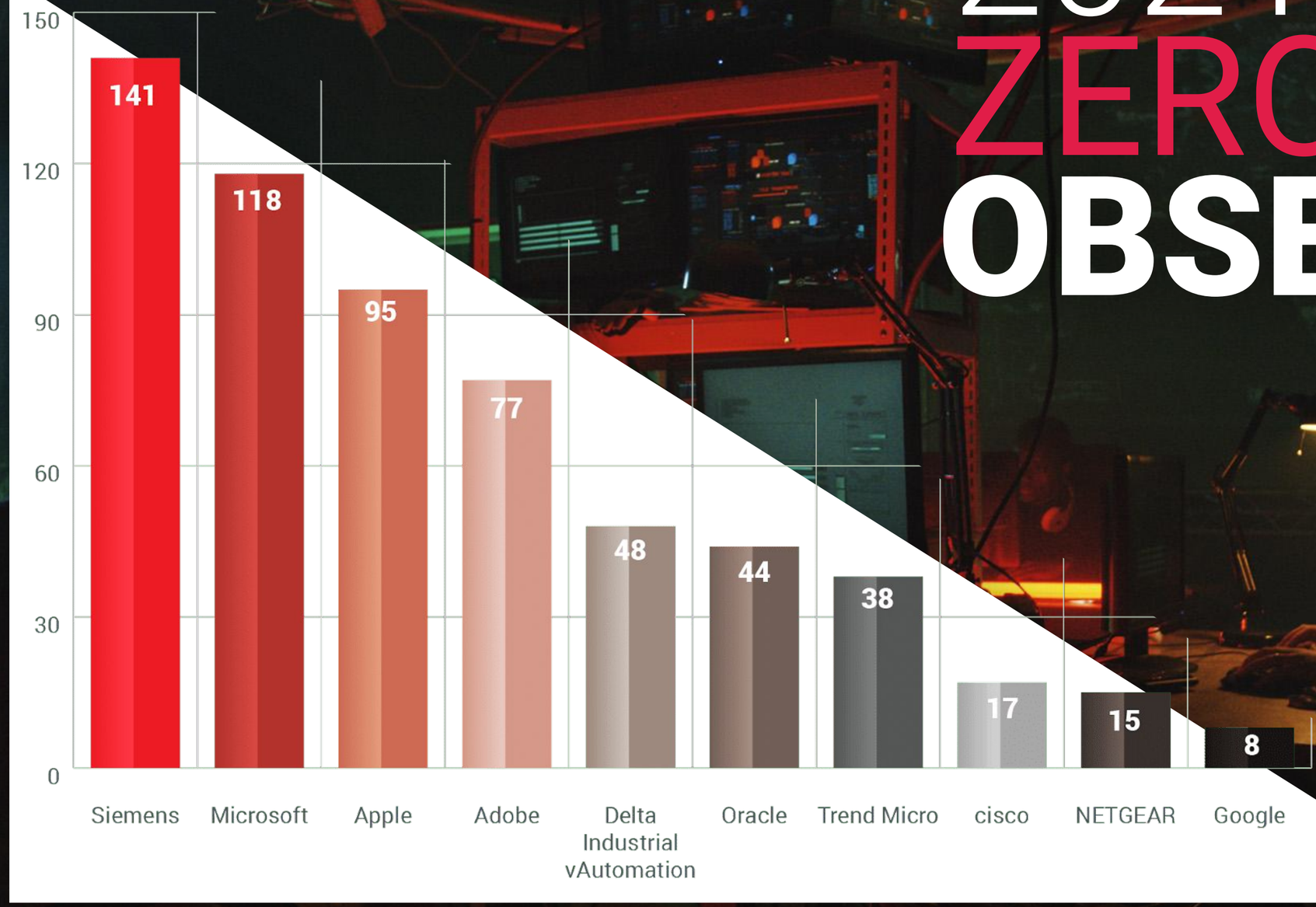
Threat actors offer millions for zero-days, developers talk of exploit-as-a-service

November 17, 2021 03:33 AM 0

By Ionut Ilascu

ZEROCLICKS

2021 MOST ZERO DAYS OBSERVED



ZERO DAYS

QNAP

Nieuws

Ransomware versleutelt ruim 11.000 QNAP-apparaten via zerodaylek

maandag 12 september 2022, 12:33 door **Redactie**, 2 **reacties**

De criminelen achter de DeadBolt-ransomware hebben begin deze maand ruim 11.000 NAS-apparaten van fabrikant QNAP via een zerodaylek weten te versleutelen, zo stelt securitybedrijf **Censys**. Sinds het begin van dit jaar zijn QNAP-systemen het doelwit van de DeadBolt-ransomware, waarbij vaak bekende kwetsbaarheden worden gebruikt. Begin september wisten de aanvallers NAS-systemen via een **zerodaylek** in de Photo Station-software aan te vallen.

12 SEPT 2022
APPLE FIXES 8 ZERODAYS

Apple patches zero-day holes – even in the brand new iOS 16

12 SEP 2022 0

Apple iOS OS X Vulnerability

12 SEP 2022 0

Apple fixes eighth zero-day used to hack iPhones and Macs this year

By Sergiu Gatlan

September 12, 2022 02:20 PM 0

The issue, assigned the identifier CVE-2022-32917, is rooted in the Kernel component and could enable a malicious app to execute arbitrary code with kernel privileges. "**Apple is aware** of a report that t**his issue may have been actively exploited,**" the iPhone maker acknowledged in a brief statement, adding it resolved the bug with improved bound checks.

incorporating a new Lockdown Mode that's designed to make zero-click attacks harder.

VRAGEN?

NETWORKING4ALL
LEADING IN CYBERSECURITY SOLUTIONS

PRIVACYBOX