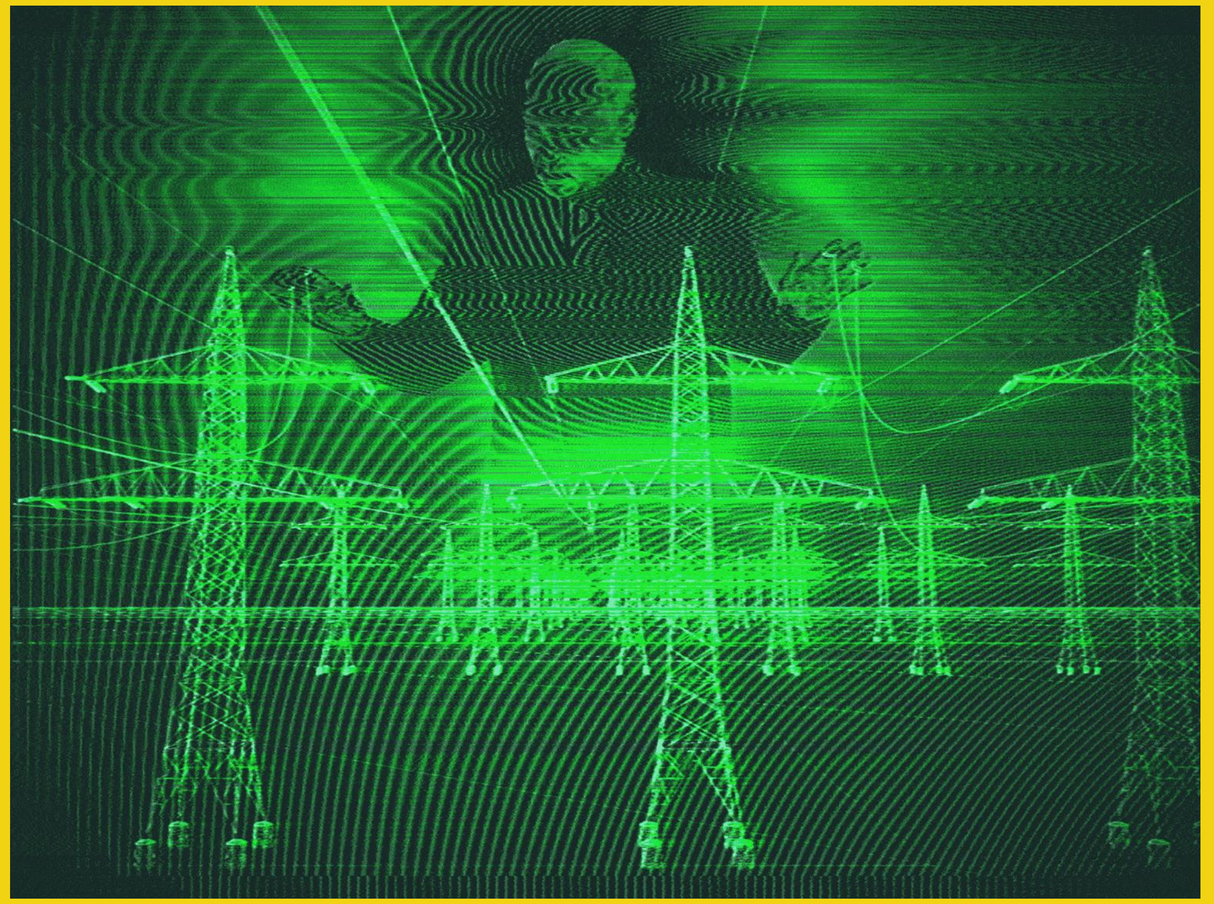
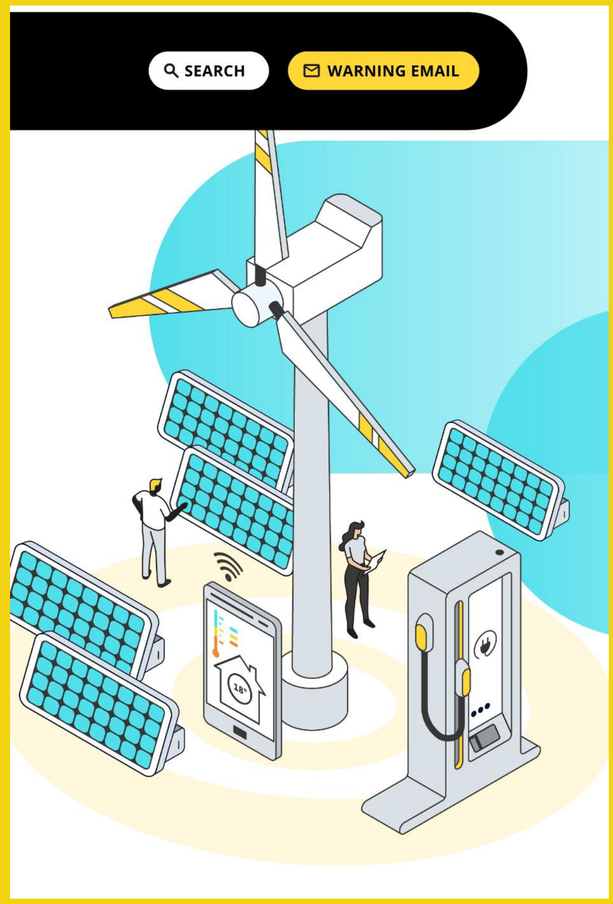
DIVD





Hoe cybercriminelen ons elektriciteitsnet kunnen verstoren (en wij helpen dat te voorkomen)

Chris van ‘t Hof, 16 april 2025

DIVD

1 13

Uit de Kom @UitDeKom · Dec 14, 2024
#nietmijnoorlog #bankrun

5 23 3.7K

Zappa-IsTheBest ⚓ @ZappaforPotus · Dec 15, 2024
Wie stopt deze oorlogshitser. #nietmijnoorlog

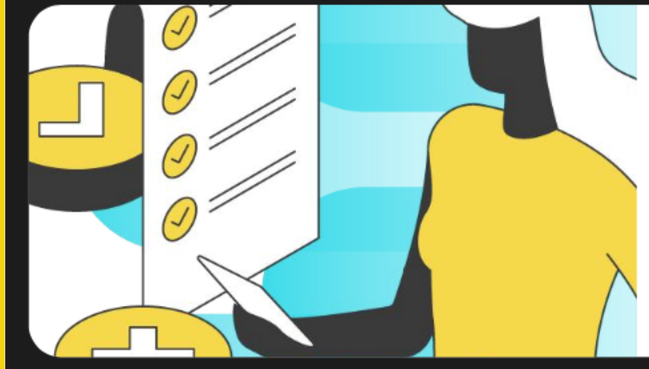
Wie wij zijn

DIVD

189
MEMBERS

163
TOTAL CASES

1.338.459
VULNERABLE IPS NOTIFIED



Ethics at the base of everything we do

We aim to make the digital world safer by reporting vulnerabilities we find in digital systems to the people who can fix them. We have a global reach, but do it Dutch style: open, honest, collaborative and for free.

CODE OF CONDUCT

Code of Conduct Art.4

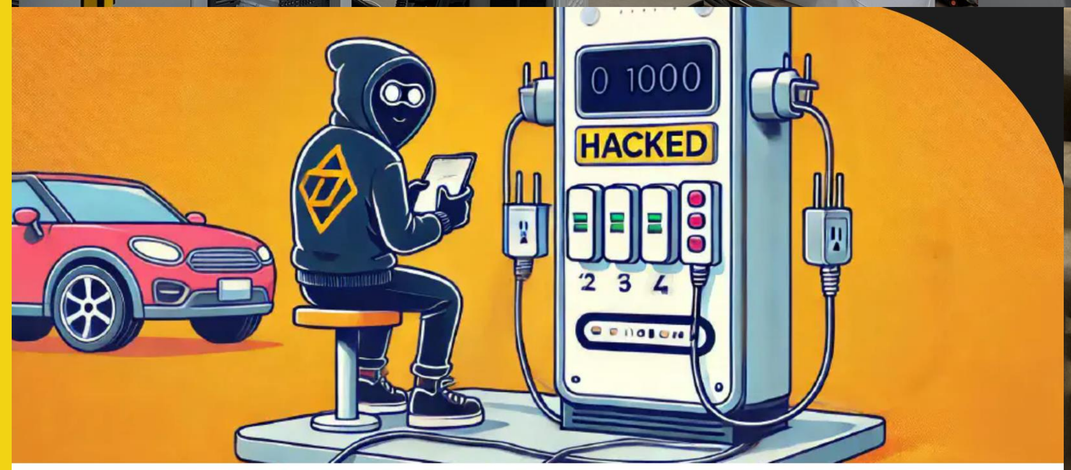
Societal need: we do vulnerability disclosure to prevent online damage to as many internet users as possible and don’t serve any particular financial, political or individual interests.

Principle of Proportionality: we serve this need with appropriate means. Our research should increase and not decrease the integrity and availability of online systems.

Principle of Subsidiarity: if several means are available to meet the need, we opt for the one which has the least impact.

DIVD

Hacker Harm



Press release: Research unveils 17 new zero-days in EV Chargers

In our most recent research into the security of EV chargers, 17 new vulnerabilities (zero days) were discovered in chargers manufactured by iocharger. These vulnerabilities were present in all AC-models of iocharger. The research was conducted by external researcher Wilco van Beijnum and DIVD researcher Harm van den Brink.

Case lead
Frank Breedijk

Researchers
Harm van den Brink
Wilco van Beijnum

DIVD-2024-00035

Hacker Wietse

DIVD

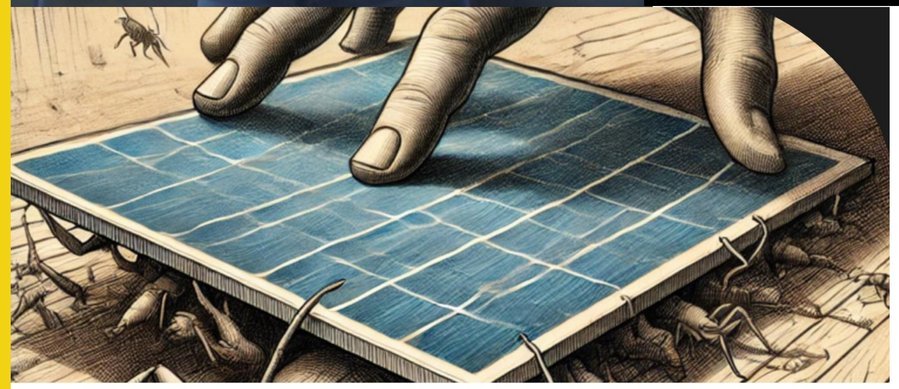
Why is it vulnerable?

```
def get_locale(use_qp=true)
   requested_locale = ""

   requested_locale = @cm.params['locale'][0].to_s if @cm.params.has_key?('locale')
   short_locale = requested_locale.slice(0,2)

   return requested_locale if @locales.has_key?(short_locale)
   return short_locale if @locales.has_key?(short_locale)
   return @@locale unless @@locale.empty?
   return get_emu_default_locale()[0]
end
```

HACKER HOTEL



DIVD responsibly discloses six new zero-day vulnerabilities to vendor

The Hague, Netherlands – Aug 12, 2024
by Serena de Pater and Marieke Smits

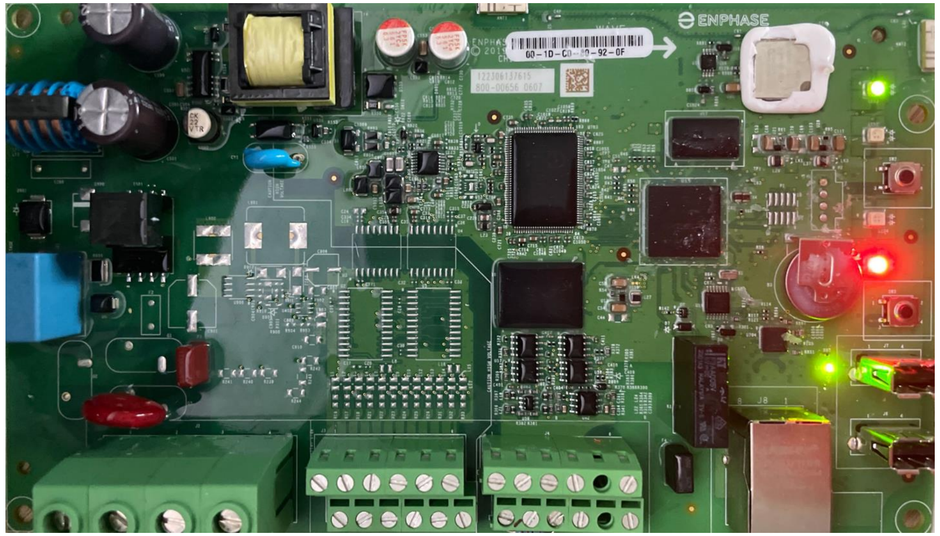
Case lead
Frank Breedijk

Researchers
Wietse Boonstra
Hidde Smit
Max van der Horst
Frank Breedijk

DIVD-2024-00011

About the case

DIVD researchers have discovered and, in collaboration with the vendor, disclosed **six new zero-day vulnerabilities** in Enphase IQ Gateway devices. This investigation was conducted by Wietse Boonstra and Hidde Smit, both researchers at DIVD, under case DIVD-2024-00011.



A CVE is a hackers best CV

“

- CVE-2021-30116 - A credentials leak and business logic flaw
- CVE-2021-30117 - An SQL injection vulnerability
- CVE-2021-30118 - A Remote Code Execution vulnerability
- CVE-2021-30119 - A Cross Site Scripting vulnerability
- CVE-2021-30120 - 2FA bypass
- CVE-2021-30121 - A Local File Inclusion vulnerability
- CVE-2021-30201 - A XML External Entity vulnerability

DIVD

DIVD

Macht Samenleving Economie Cultuur Leven Klimaat

Korte update zondag 4 juli

Nederlandse hackers probeerden aanval met gijzelsoftware te voorkomen

Een Nederlandse groep vrijwilligers heeft de afgelopen maanden getracht samen met het getroffen bedrijf Kaseya de lekken in hun software te dichten. De aanval van de Russische cyberbende REvil kwam daags te vroeg, zo blijkt uit onderzoek van Vrij Nederland.

Gerard Janssen
Foto: ANP/ Hollandse Hoogte/ Richard Brocken

THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Books & Arts Real Estate Life & Work WSJ Magazine Sports

WSJ NEWS EXCLUSIVE | TECH

Software Firm at Center of Ransomware Attack Was Warned of Cyber Flaw in April

President Biden is meeting officials to discuss recent attacks, including latest affecting hundreds of organizations around the world

Ransomware attacks are increasing in frequency, victim losses are skyrocketing, and hackers are shifting their targets. WSJ's Dustin Volz explains why these attacks are on the rise and what the U.S. can do to fight them. Photo illustration: Laura Kammermann

UPCOMING EVENTS

Oct 5 2021 — 12:00 PM - 5:00 PM EDT — WSJ Jobs Summit

Oct 6 — 12:30 PM - 2:00 PM EDT — The Future Of Health

DIVD

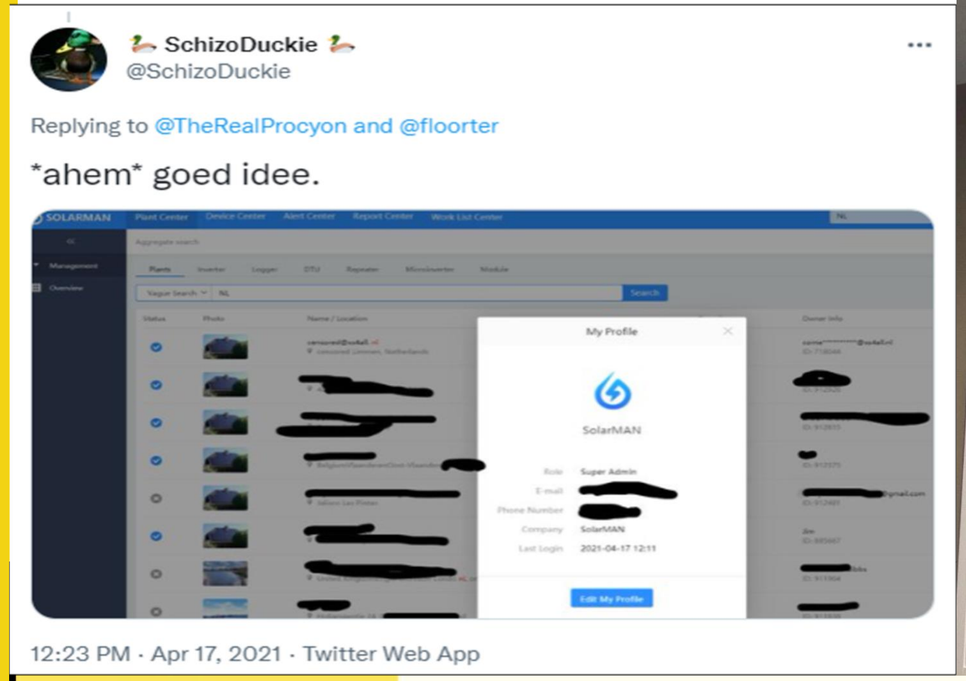
DIVD


ONDERZOEKSRAAD VOOR VEILIGHEID
Voorval melden
Blijf op de hoogte
Contact
EN | NL
Onderzoeken
Werkwijze
Over de Raad
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

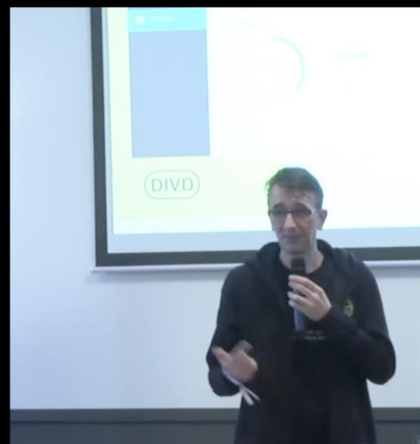
DIVD

~~Hacker~~ Vinder Jelle

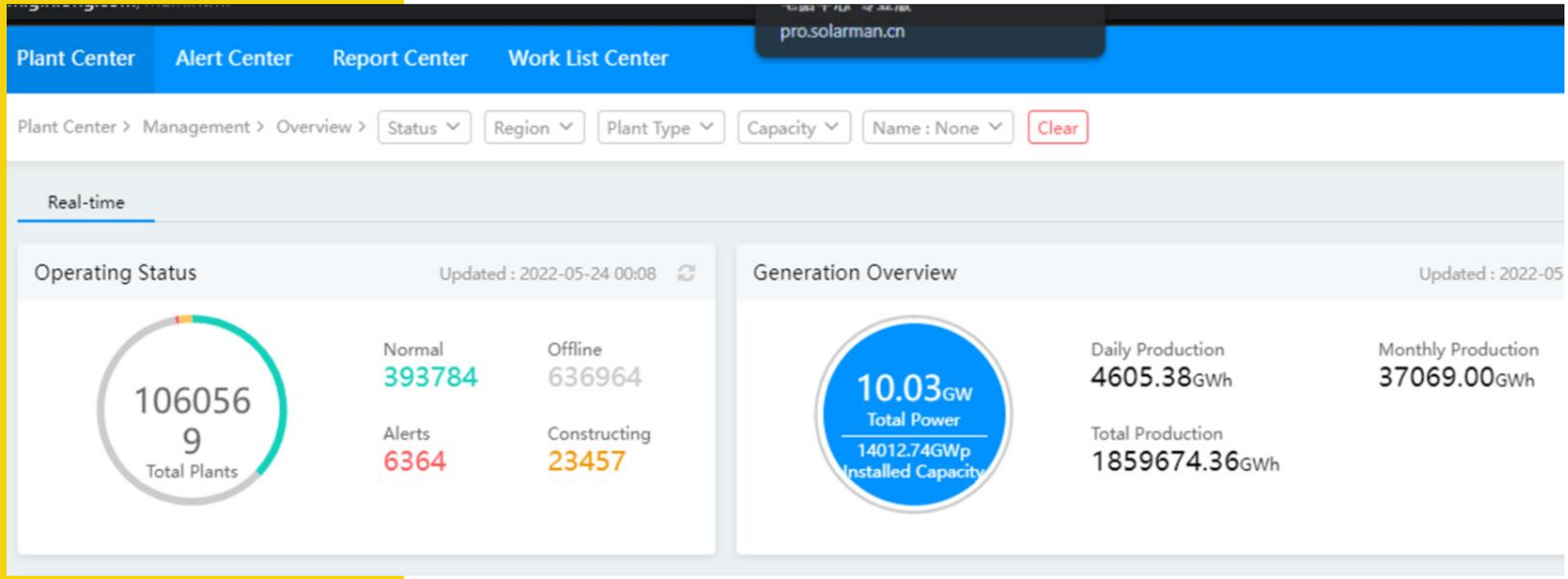
DIVD



DIVD



Wat zou een kwaadwillende kunnen met 10GW?



DIVD

Hack-out

Uitschakelen of brandgevaar

Hacker kon tienduizenden zonnepanelen saboteren door rondslingerend wachtwoord

Door Stan Hulsen · 24 juli 2022 · Aangepast: 25 juli 2022

RTL Nieuws

Tienduizenden zonnepaneelinstallaties in Nederland en een miljoen wereldwijd waren kwetsbaar voor sabotage. Een Chinees bedrijf dat monitoringssoftware voor omvormers levert, liet een wachtwoord voor een online-controlepaneel rondslingeren op het internet. Kwaadwillenden hadden de apparaten kunnen uitschakelen of de software kunnen aanpassen, waardoor brandgevaar zou ontstaan.

Beantwoording Kamervragen naar aanleiding van het artikel ‘Hacker ontdekt dat Chinese zonnepanelen een bedreiging zijn voor ons stroomnet’

Kamerstuk | 02-09-2022

Minister Jetten (Klimaat en Energie) beantwoordt vragen naar aanleiding van het artikel ‘Hacker ontdekt dat Chinese zonnepanelen een bedreiging zijn voor ons stroomnet’. De vragen zijn gesteld door de Kamerleden Rajkowski en Erkens (beide VVD).

↗ Beantwoording Kamervragen naar aanleiding van het artikel ‘Hacker ontdekt dat Chinese zonnepanelen een bedreiging zijn voor ons stroomnet’ (PDF | 9 pagina's | 419 kB)

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat

Rapport Rijksinspectie Digitale Infrastructuur

Onderzoek storingsproblematiek en cyberveiligheid omvormers voor zonnepanelen

Samen voor een digitaal veilige energiesector

Met onze nieuwe onderzoekslijn versterken we de digitale weerbaarheid van het steeds kwetsbaarder wordende energiesysteem.

DIVD

Organisatorisch landschap digitale veiligheid energie

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

digital trust center.

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Ministerie van Klimaat en Groene Groei

Autoriteit Consument & Markt

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

topsector energie

mffbas

Security organizations

ENCS

DIVD

INTERNET CLEANUP FOUNDATION

Netbeheer Nederland

Holland Solar

ENERGIE NEDERLAND

ISACs and working groups

Elaad nl

ENERGY STORAGE NL

NedZero
Branchevereniging voor windenergie

EDSN
energiedata voor iedereen

NIS2, CRA...

Implementatie...

DIVD

Divd.nl/energie

Samen voor een digitaal veilige energiesector

Met onze nieuwe onderzoekslijn versterken we de digitale weerbaarheid van het steeds kwetsbaarder wordende energiesysteem.

DOWNLOAD PARTNERDECK

Een slimme, duurzame, maar kwetsbare energiesector

Waarom veiligheid cruciaal is

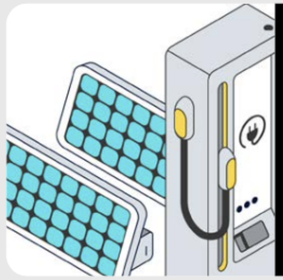
Het Europese elektriciteitsnetwerk is nu een ‘smart grid’, waarin consumenten zowel energie gebruiken als produceren. Slimme online verbonden apparaten stemmen vraag en aanbod beter op elkaar af, wat verduurzaming en innovatie stimuleert. Tegelijkertijd maakt dit ons energiesysteem kwetsbaar voor digitale aanvallen. Hoewel losse apparaten weinig impact hebben, kan grootschalige manipulatie door cybercriminelen leiden tot ernstige stroomstoringen en zelfs een (inter)nationale black-out.

DIVD

Divd.nl/energie

Wat gaan we precies doen?

Met het project CVD in de energiesector starten we een nieuwe onderzoekslijn om de digitale weerbaarheid van het steeds kwetsbaarder wordende energiesysteem te versterken. We richten ons op kennisontwikkeling, samenwerking en bewustwording binnen de sector en onderzoeken daarbij specifiek kwetsbaarheden in randapparatuur, zoals laadpalen, omvormers, thuisbatterijen en energiebeheersystemen. Eerdere bevindingen leidden al tot Kamervragen en acties van autoriteiten zoals de Rijksinspectie Digitale Infrastructuur (RDI).
In 2025 zetten we hierin de volgende stappen:



IoT Hacking Lab

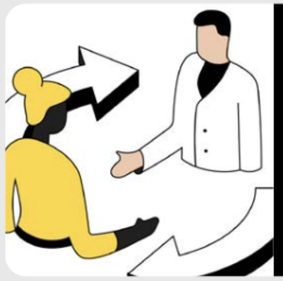
We zetten een IoT Hacking Lab op om onder andere randapparatuur zoals laadpalen, thuisbatterijen, omvormers e.d. te onderzoeken en testen. Daarnaast werken we samen met andere labs.

Onderzoek

We doen en publiceren onderzoek om hiermee autoriteiten en partners te ondersteunen bij handhaving en het implementeren van verbeteringen binnen de energiesector.

Educatie

We leiden nieuwe experts op met **DIVD. Academy** door lesmateriaal, trainingen en workshops te ontwikkelen voor studenten, de installatiebranche en onderwijsinstellingen in de energiesector.



Samenwerken

We werken samen met netbeheerders, overheden, leveranciers, fabrikanten, etc. om bewustzijn binnen de sector te vergroten en kwetsbaarheden te vinden en op te lossen.

DIVD

Divd.nl/energie

Zo kun je helpen

Financiën

Hoewel DIVD wordt gerund door bijna 200 Nederlandse vrijwilligers, hebben we financiële middelen nodig om ons werk effectief te blijven doen. Om continuïteit te waarborgen en te groeien, hebben we een stabiele financiering van minimaal €200.000 per jaar nodig. Dit stelt ons in staat te investeren in professionele ondersteuning, essentiële diensten, tools en medewerkers.

We zijn hierbij volledig afhankelijk van sponsoren en donateurs. Daarom zoeken we organisaties en individuen die ons willen steunen met terugkerende jaarlijkse donaties vanaf €5.000 per jaar.

Direct doneren, ga naar: **divd.nl/donate**

Materialen

Onze organisatie is sterk afhankelijk van IT. Gelukkig krijgen we al veel steun van leveranciers in de vorm van gratis licenties, tools en diensten.
Hoewel we geen productaanbevelingen doen – om onze ANBI-status en onafhankelijkheid te waarborgen – erkennen we graag een bijdrage op onze partnerpagina.

Daarnaast ondersteunen veel partners ons niet alleen op IT-gebied, maar ook met juridische, communicatieve en organisatorische expertise.

Mensen

Organisaties kunnen ons ondersteunen met de meest waardevolle hulpbron: mensen. Door medewerkers structureel een aantal uur per week de ruimte te geven om zich voor een langere periode in te zetten als vrijwilliger bij DIVD, dragen zij direct bij aan onze missie.

Dit draagt niet alleen bij aan hun persoonlijke ontwikkeling, maar laat ook zien dat hun werkgever onze missie ondersteunt en actief invulling geeft aan maatschappelijk verantwoord ondernemen.

Security researchers binnen de energiesector zijn meer dan welkom om zich als vrijwilliger bij DIVD aan te sluiten.

SIDN fonds

topsector energie

THE GREEN VILLAGE

Elaadnl

ENCS

Nationaal Coördinator Terrorismebestrijding en Veiligheid
Ministerie van Justitie en Veiligheid

eset

vmware

A2B Internet

bit internet technology

DIVD

people.divd.nl/careers

SENIOR SECURITY RESEARCHER ENERGY SYSTEMS

Senior Security Researcher Energy Systems

Department: Research & Development

Voluntary work, 4-8 hrs/week

Help out to protect the energy grid

DIVD is the voluntary fire brigade of the Internet. At the Dutch Institute for Vulnerability Disclosure we aim to make the digital world safer by reporting vulnerabilities we find in digital systems to the people who can fix them. We operate on a global level, but do it Dutch style: open, honest, collaborative, and for free.

<insert happy end here>

DIVD

<insert happy end here>

Hoeveel MW leveren Jullie?

DIVD

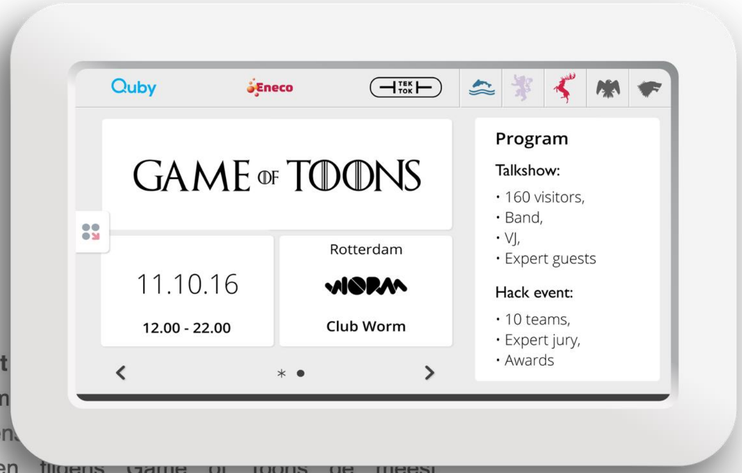
Net binnen Algemeen Economie Sport Media en Cultuur Achterklap Shop Meer

Maandag 7 april 2025 | Het laatste nieuws het eerst op NU.nl

<insert happy end here>

THE GREEN VILLAGE

DIVD



Most

Team

Foren

wisten tijdens Game of Toons de meest technisch geavanceerde hack te plegen op Toon van Eneco. Jurylid Michiel en juryvoorzitter Hans V vertellen waarom.

Wierdest hack

Team Sesamstraat wist tijde de meeste bijzondere hack Glenn ten Cate (Security Philis) en juryvoorzitter Han vertellen waarom. Tot de uit anoniem. Toen Patricia Cybersecurity bij NCTV, de nam was dat een bijzondere

Most dangerous hack

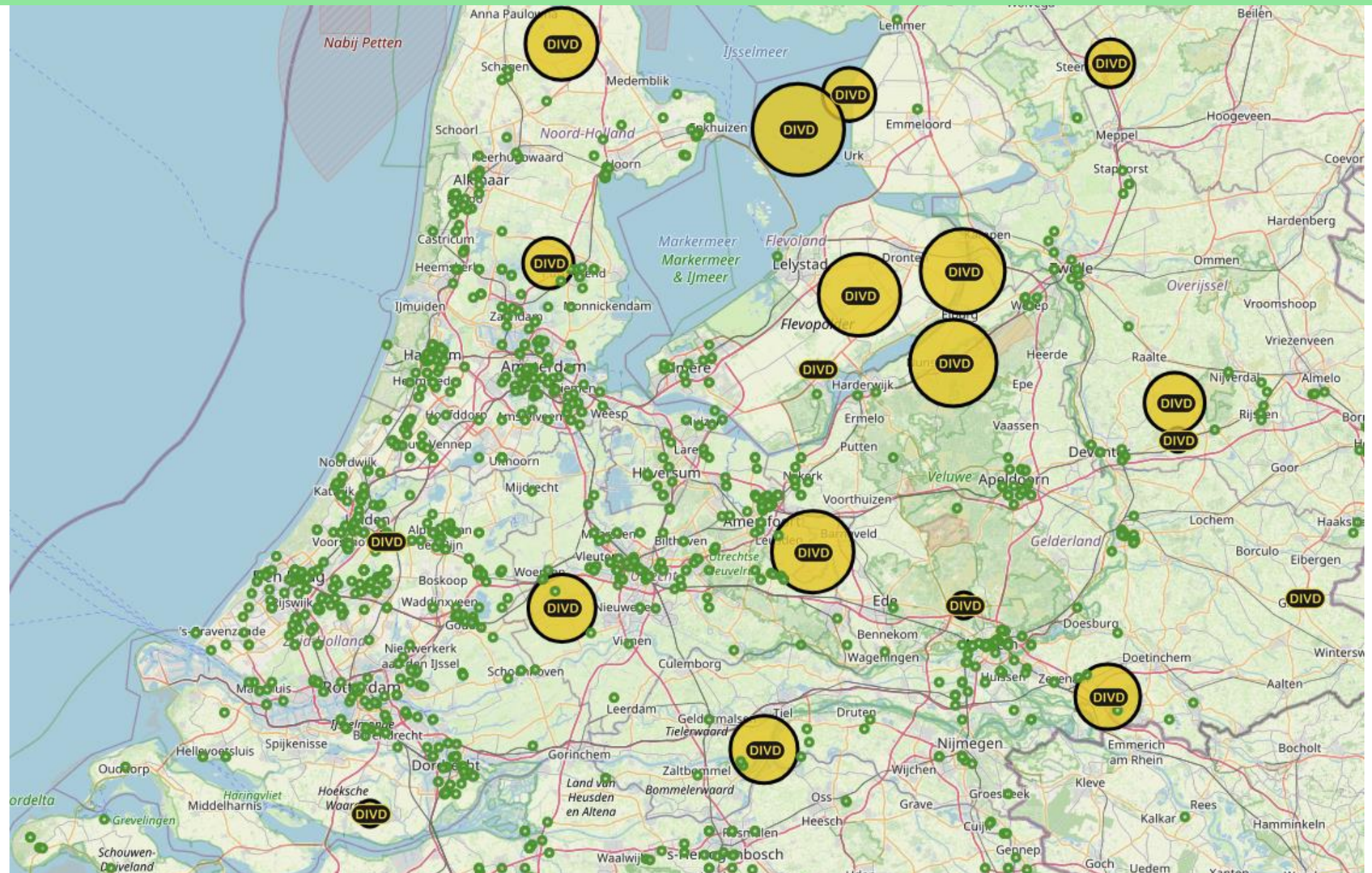
Team LooneyToons van De Game of Toons de gevaarlij op Toon van Eneco. Juryli (Security Advisor Zerocopte Hans Valk, (CEO Quby) vert

MESHTASTIC

An open source, off-grid, decentralized, mesh network built to run on affordable, low-power devices

<insert happy end here>

DIVD



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

DIVD

chris@divd.nl

Q&A

www.divd.nl/energie