NB408: JOUW ODIDO GEGEVENS ZIJN NU EEN WAPEN

Deze week bereikte het Odido datalek zijn definitieve omvang van 6,1 miljoen getroffen klanten, inclusief paspoortnummers en BSN nummers van zzp'ers. We leggen uit hoe criminelen deze gegevens combineren met eerdere datalekken tot complete digitale profielen die op het darkweb worden verhandeld. Een autonome AI bot voerde een weekenlange aanval uit op Microsoft en DataDog via GitHub, terwijl de politie "Check je hack" lanceerde zodat miljoenen gedupeerden hun gegevens kunnen controleren. Uit onderzoek van Follow the Money bleek dat ook medewerkers van ProRail, TenneT, ASML en de politie zijn getroffen. Tot slot zoekt de politie een vrouw na bankhelpdeskfraude bij een 70-jarige man in Breda. Lees alle details in de vijf artikelen van deze week.

DATAVERRIJKING: WAAROM HET ODIDO LEK GEVAARLIJKER IS DAN JE DENKT

Het Odido lek is pas het begin. Criminelen combineren gestolen gegevens met eerdere datalekken tot complete digitale profielen, zogenaamde "fullz", die op het darkweb worden verhandeld voor 20 tot 130 dollar per stuk. Hoe dit proces van dataverrijking precies werkt en wat jij er nu tegen kunt doen, ontdek je in dit artikel.

Lees hoe criminelen jouw gegevens uit meerdere lekken samenvoegen »

ODIDO FINALE: 6,1 MILJOEN OP STRAAT, OVERHEID KWETSBAAR

De volledige dataset van 6,1 miljoen Odido klanten staat nu op het darkweb, inclusief paspoortnummers en BSN nummers van zzp'ers. Tegelijk werd de Dienst Justitiële Inrichtingen vijf maanden bespioneerd via een kwetsbaarheid in Ivanti en onthulde IBM dat een kwart van alle cyberaanvallen op Europa is gericht. Waarom juist die BSN nummers het datalek zoveel gevaarlijker maken, lees je in het journaal.

Ontdek waarom BSN nummers van zzp'ers dit lek zoveel ernstiger maken »

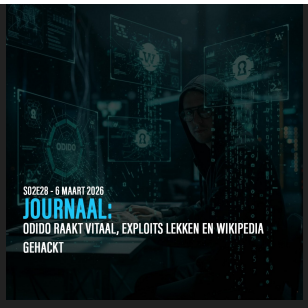
AI BOT HACKT GITHUB, NEDERLAND GRIJPT IN EN CYBEROORLOG IRAN

Een autonome bot genaamd hackerbot-claw voerde een weekenlange aanval uit op Microsoft en DataDog via GitHub en wist in vier repositories op afstand code uit te voeren. Ondertussen lanceerde de politie "Check je hack" zodat miljoenen gedupeerden van het Odido lek kunnen controleren of hun gegevens zijn gestolen. Hoe een AI bot zelfstandig techgiganten aanvalt en wat de Tweede Kamer debatteert over digitale veiligheid, lees je in het journaal.

Bekijk hoe een AI bot zelfstandig techgiganten aanviel »

ODIDO RAAKT VITAAL, EXPLOITS LEKKEN EN WIKIPEDIA GEHACKT

Uit onderzoek van Follow the Money blijkt dat ruim 16.300 medewerkers van vitale bedrijven als ProRail, TenneT, ASML en de politie zijn getroffen door het Odido lek. Tegelijk onthulde Google hoe een geavanceerde exploit kit voor



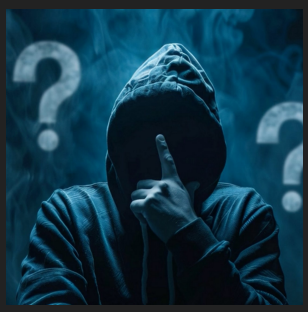
iPhones van overheden naar criminelen is doorgesijpeld en werd Wikipedia in 23 minuten gehackt door een zelfverspreidende worm. Welke vitale sectoren precies zijn geraakt, lees je in het volledige journaal.

Zie welke vitale bedrijven zijn getroffen door het Odido lek »

VROUW GEZOCHT NA BANKHELPDESKFRAUDE IN BREDA

Een 70-jarige man uit Breda werd in januari slachtoffer van bankhelpdeskfraude nadat een beller zich voordeed als medewerker van de fraudeafdeling. Kort daarna verscheen een jonge vrouw aan zijn deur die zijn bankpassen, telefoon en pincodes meenam en meerdere transacties deed. De politie heeft camerabeelden en zoekt deze vrouw, herken jij haar?

Bekijk de camerabeelden en help de politie »



CYBERCRIME QUIZ WEEK 10 - TEST JE KENNIS!

Weet jij hoeveel klanten van Odido zijn getroffen? Welke gebeds-app werd als cyberwapen ingezet tegen Iran? En hoeveel zero-days werden in 2025 uitgebuit? Van AkzoNobel en Anubis ransomware tot 94 procent botverkeer bij inlogpogingen. Test in 20 vragen of jij alles hebt meegekregen!

Test in 20 vragen of jij alles hebt meegekregen!

Liever luisteren of kijken?

Geen tijd om te lezen? Blijf op de hoogte via uw favoriete platform. Kies voor de snelle update, de diepgaande analyse of de visuele presentatie.

Spotify Audio »
DAGELIJKS JOURNAAL (3 min)
DIEPTE ANALYSE (15 min)

YouTube Video »
VISUELE PRESENTATIE (5 min)

STRATEGISCHE DREIGINGSANALYSE VAN DIGIWEERBAAR

Dit wekelijkse rapport biedt een strategische dreigingsanalyse van actuele cyber en geopolitieke ontwikkelingen die de digitale autonomie en vitale infrastructuur van Nederland raken. Het geeft inzicht in afhankelijkheden, kwetsbaarheden en het veranderende dreigingslandschap, met focus op overheid, zorg en kritieke sectoren. Het rapport ondersteunt besluitvorming door risico's en trends helder en samenhangend te duiden.

NU 30 DAGEN GRATIS »

Help Cybercrimeinfo in de lucht te houden

Onze tools, journalen en waarschuwingen zijn gratis voor iedereen. Maar onderzoek en hosting kosten geld. Waardeert u onze intelligence? Help ons dan met een eenmalige donatie. Elke bijdrage maakt de digitale wereld een stukje veiliger.

Ik wil graag steunen »

Bedankt voor het lezen! Deel deze nieuwsbrief gerust met vrienden, familie en collega's, samen maken we Nederland en België digitaal weerbaarder.

Tot volgende week,
Cybercrimeinfo