Cybercrimeinfo (ccinfo.nl)

Het onzichtbare zichtbaar maken

Nieuwsbrief 361

Reading in another language

Analyse van kwetsbaarheden op het gebied van cyberbeveiliging maart 2025

In maart 2025 werden er opnieuw ernstige kwetsbaarheden ontdekt die het digitale landschap onveilig maken voor zowel bedrijven als consumenten. Van zwakke plekken in populaire netwerkapparatuur zoals VMware ESXi tot kritieke beveiligingslekken in software zoals WordPress, de risico's zijn aanzienlijk. In dit artikel belichten we de meest zorgwekkende kwetsbaarheden van de afgelopen maand en bieden we praktische tips om systemen te beschermen tegen aanvallen. Het is cruciaal om snel te reageren op updates en maatregelen te nemen om de veiligheid van jouw digitale omgeving te waarborgen. Lees verder voor gedetailleerde analyses en waardevolle adviezen.

Lees verder

Reading in another language

Politie cyber nieuws 2025 maart

In maart 2025 werden belangrijke stappen gezet in de wereldwijde strijd tegen cybercriminaliteit, met succesvolle operaties en arrestaties in zowel Nederland als daarbuiten. Van phishingaanvallen tot grootschalige identiteitsfraude en internationale samenwerking tegen cybercriminelen, de politie zet zich in om digitale misdrijven te bestrijden en de daders achter de tralies te krijgen. In dit artikel krijg je een overzicht van de meest opvallende gevallen en operaties van de afgelopen maand, inclusief de nieuwste ontwikkelingen en de cruciale rol van opsporingsinstanties wereldwijd. Lees verder om te ontdekken hoe de strijd tegen digitale misdaad zich blijft intensiveren.

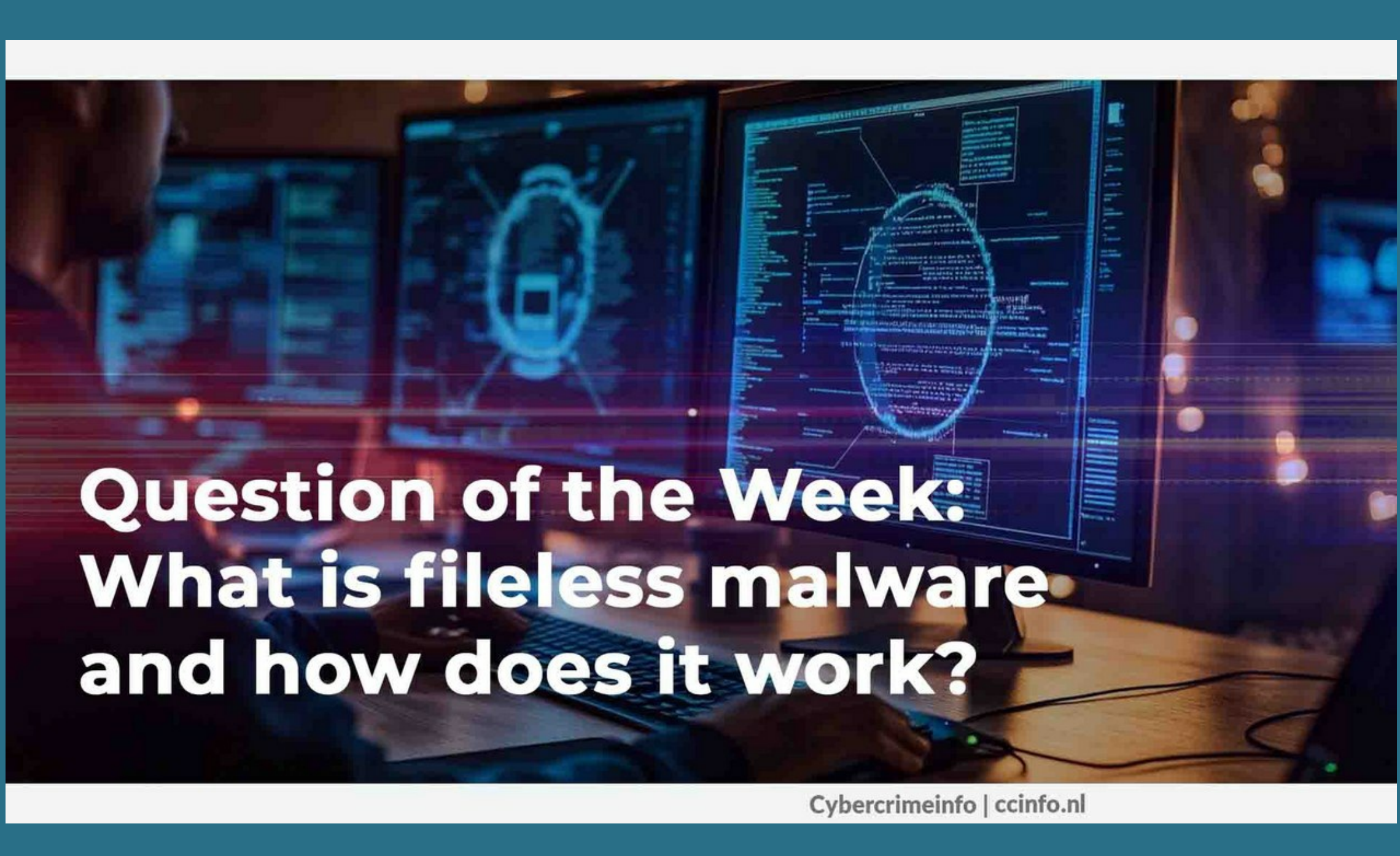
Lees verder

Reading in another language

Ransomware in 2025, een groeiende dreiging: trends en ontwikkelingen

Ransomware blijft een van de grootste dreigingen voor bedrijven en overheden wereldwijd, en in 2025 neemt de situatie een verontrustende wending. Het aantal aanvallen stijgt snel, met een alarmwekkende toename van 45% in vergelijking met het vorige jaar. Dit artikel biedt een diepgaande blik op de nieuwste trends, de sectoren die het vaakst getroffen worden, en de opkomst van nieuwe ransomware-groepen. Daarnaast bespreken we welke maatregelen bedrijven kunnen nemen om zich beter te beschermen tegen deze steeds geavanceerdere aanvallen. Ontdek hoe je je organisatie weerbaarder kunt maken tegen deze groeiende dreiging.

Lees verder



Reading in another language

Vraag van de week: Wat is fileless malware en hoe werkt het?

Fileless malware is een van de meest gevorderde en moeilijk te detecteren vormen van cyberdreiging die bedrijven en organisaties steeds vaker treffen. Deze malware laat geen fysieke bestanden achter en maakt gebruik van legitieme systeemtools om zijn kwaadaardige activiteiten uit te voeren. Hierdoor ontsnapt het vaak aan traditionele beveiligingssoftware. Maar hoe werkt deze vorm van malware precies en hoe kun je jezelf ertegen beschermen? In dit artikel duiken we dieper in op de gevaren van fileless malware en bieden we praktische tips om jezelf en je organisatie te beschermen tegen deze onzichtbare dreiging.

Lees verder

Reading in another language

FBI rolt $24 miljoen darkweb crypto witwasoperatie op

De FBI heeft recent een omvangrijke operatie uitgevoerd waarbij een internationaal crypto-witwasnetwerk, goed voor 24 miljoen dollar, werd opgerold. Deze actie onthult niet alleen de kracht van de crypto-industrie voor criminele activiteiten, maar ook de geavanceerde technieken die wetshandhavers inzetten om deze dreigingen te bestrijden. In dit artikel duiken we in de wereld van crypto-witwassen op het darkweb, de rol van de FBI en de bredere impact van deze misdaad.

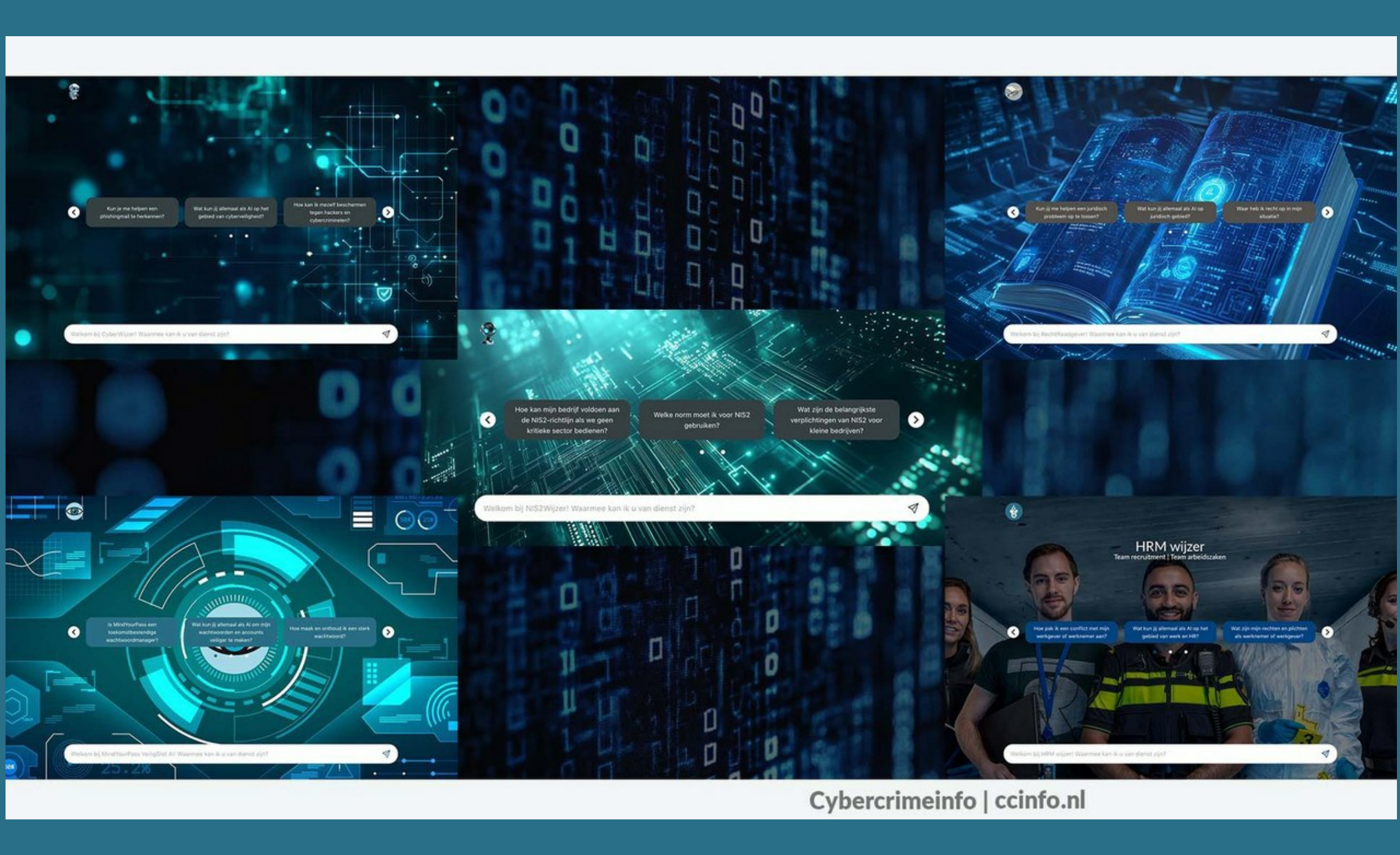
Lees verder

Reading in another language

Den Haag - Nepagent

In Den Haag werd een 81-jarige man het slachtoffer van een geraffineerde babbeltruc, waarbij een oplichter zich voordeed als politieagent. Deze vorm van oplichting, bekend als 'nepagentschap', is helaas niet uniek. Het gebruik van autoriteit om vertrouwen te winnen is een veelvoorkomende tactiek onder cybercriminelen. Hoe herken je zo'n nepagent en wat kun je doen om jezelf te beschermen tegen deze vorm van fraude? Lees verder voor cruciale tips en inzichten.

Lees verder



AI Chatbots Cybercrimeinfo

AI Chatbots | Ontdek **CyberWijzer**, **RechtRaadgever** en **NIS2Wijzer**, 24/7 beschikbaar voor hulp bij cybercriminaliteit, strafrecht en NIS2-wetgeving. Als je hulp nodig hebt bij het installeren of gebruiken van MindYourPass, gebruik dan AI Gids **VeiligSlot**. De AI **HRMWijzer** bevindt zich momenteel in de testfase van ontwikkeling en biedt richtlijnen en informatie over verschillende aspecten van HRM binnen de politie.

Reading in another language

Waarom jouw donatie aan Cybercrimeinfo essentieel is

Beste lezer,
In een wereld waarin digitale dreigingen steeds geavanceerder en talrijker worden, speelt Cybercrimeinfo een cruciale rol in de strijd tegen cybercriminaliteit. Als onafhankelijke organisatie, volledig gedreven door vrijwilligers, zetten wij ons in om het publiek te informeren en beschermen tegen de gevaren van het digitale tijdperk.

Jouw donatie maakt het verschil. Dit is waarom:

- **Een onafhankelijke en betrouwbare bron van informatie**
  Cybercrimeinfo is geen onderdeel van de Nederlandse Politie. Wij bieden een onpartijdige en toegankelijke bron van actuele informatie over cyberdreigingen, oplichtingstechnieken en preventiemethoden.
- **Bewustwording en preventie mogelijk maken**
  Met jouw donatie help je ons om kennis en bewustzijn over cybercriminaliteit te vergroten. Onze artikelen, nieuwsupdates en praktische tips dragen direct bij aan het voorkomen van digitale misdrijven.
- **Ondersteuning van operationele kosten**
  Donaties worden direct gebruikt voor het hosten van onze website en het up-to-date houden van technologische middelen. Hierdoor kunnen we cybercriminelen blijven volgen en jullie informeren over de nieuwste digitale dreigingen.

Elke bijdrage, groot of klein, is van onschatbare waarde in onze strijd tegen cybercriminaliteit. Met jouw steun kunnen we blijven werken aan een veiliger digitaal landschap voor iedereen.

Doneer nu via onze doneerpagina (kies zelf het bedrag dat je wilt doneren) of gebruik de onderstaande QR-code.

We waarderen je steun enorm en bedanken je alvast voor je bijdrage aan deze belangrijke zaak.

Met vriendelijke groet,
Het team van Cybercrimeinfo

Doneer | Cybercrimeinfo.nl (ccinfo.nl)

Doneer pagina

Geen budget? Geen probleem!

Help ons de zichtbaarheid van Cybercrimeinfo te vergroten met jouw Google review!

Laat jouw stem horen: Steun ons met een Google review!

Wij streven er voortdurend naar om de zichtbaarheid en bereikbaarheid van Cybercrimeinfo te verbeteren. Een fantastische manier waarop jij ons hierbij kunt helpen, is door een review achter te laten op Google. Jouw feedback is onmisbaar voor ons en helpt anderen om ons makkelijker te vinden.
Het plaatsen van een recensie is simpel en kost slechts een minuutje van je tijd. Klik op de volgende link om jouw ervaringen te delen: **Schrijf een review.**
Elke review draagt bij aan onze missie om iedereen beter te informeren over cyberveiligheid. Jouw steun is voor ons ontzettend waardevol!
Hartelijk dank voor je betrokkenheid.

Non-profit team Cybercrimeinfo (ccinfo)

Schrijf een review
