Cybercrimeinfo (ccinfo.nl)

Het onzichtbare zichtbaar maken

Nieuwsbrief 377

Podcast

Podcast

Reading in another language

De stille pandemie van 2025, ransomware explodeert wereldwijd en blijft onzichtbaar

Ransomware heeft in 2025 zijn intrede gemaakt als een stille pandemie, met een explosieve stijging van 63% in het aantal wereldwijde aanvallen in het tweede kwartaal. Wat nog verontrustender is, is het feit dat veel van deze aanvallen onzichtbaar blijven voor het publiek. Niet alleen grote organisaties worden getroffen, maar ook kwetsbare sectoren zoals zorg en retail worden steeds vaker doelwit. In dit artikel duiken we dieper in de oorzaken, de onzichtbare dreiging en de nieuwe tactieken die cybercriminelen gebruiken om organisaties wereldwijd te gijzelen en data te stelen. Lees verder en ontdek waarom de traditionele verdedigingen niet langer voldoende zijn in de strijd tegen deze toenemende cyberdreiging.

Lees verder

Reading in another language

AI en de toekomst: de onzichtbare kracht die alles verandert

Kunstmatige intelligentie (AI) is niet langer een toekomstvisie, maar een alomtegenwoordige technologie die steeds dieper in ons dagelijks leven doordringt. In dit artikel duiken we in de visie van Eric Schmidt, voormalig CEO van Google, over de verborgen kracht van AI en de technologische revolutie die de wereld voorgoed verandert. Terwijl de publieke discussie vaak draait om chatbots zoals ChatGPT, wijzen Schmidt en anderen erop dat de werkelijke impact van AI veel verder gaat. Ontdek de uitdagingen en ethische dilemma's die gepaard gaan met autonome systemen, evenals de enorme kansen die AI biedt voor de toekomst.

Lees verder

Reading in another language

Raspberry Pi, 4G modem en een bankoverval: De geheime strategie van UNC2891

De wereld van cybercriminaliteit wordt steeds geavanceerder, en de aanval van de groep UNC2891 is een schoolvoorbeeld van hoe innovatief cybercriminelen kunnen zijn. Deze groep gebruikte een onwaarschijnlijke combinatie van een Raspberry Pi, een 4G-modem en geavanceerde

malware om een bank te overvallen. Door fysieke toegang te combineren met digitale manipulatie wisten ze beveiligingssystemen te omzeilen en kritieke infrastructuur aan te vallen. Ontdek in dit artikel hoe deze aanval werd uitgevoerd, welke technieken werden gebruikt en wat dit betekent voor de toekomst van bankbeveiliging.

Lees verder

Reading in another language

Lovense, het speeltje dat terugkijkt

Lovense, de fabrikant van op afstand bestuurbare seksspeeltjes, staat zwaar onder druk door ernstige beveiligingslekken die jarenlang onopgemerkt bleven. Meer dan 11 miljoen gebruikers, waaronder cammodellen en sekswerkers, werden blootgesteld aan aanzienlijke privacyrisico's door de zwakke infrastructuur van het bedrijf. Dit artikel duikt dieper in de onthullingen van ethische hackers en de impact van deze kwetsbaarheden op de gebruikersveiligheid. Wat betekent dit voor de toekomst van de sekstechnologie en de verantwoordelijkheid van bedrijven in een digitale wereld? Lees verder voor een gedetailleerd overzicht van de situatie en de dringende noodzaak voor verandering.

Lees verder

Reading in another language

Internationaal offensief op het darkweb, BlackSuit onderuitgehaald

Internationale wetshandhavingsinstanties hebben recentelijk een

belangrijke slag geslagen in de strijd tegen cybercriminaliteit. De beruchte ransomwaregroep BlackSuit, beter bekend als Royal, is in een gecoördineerde operatie zwaar getroffen. Het in beslag nemen van hun technische infrastructuur markeert een doorbraak in de bestrijding van deze gevaarlijke groep die wereldwijd miljoenen dollars eiste van bedrijven en overheidsinstellingen. Maar terwijl deze operatie een overwinning lijkt, blijft de dreiging van ransomware groot. De opkomst van een nieuwe groep, Chaos, toont aan hoe snel cybercriminelen zich aanpassen. Wat betekent deze ontwikkeling voor de toekomst van cybercriminaliteit en hoe kunnen we ons beschermen? Lees verder om meer te ontdekken.

Lees verder

Reading in another language

Bladel - Nepagent

In Bladel heeft een 80-jarige vrouw recentelijk het slachtoffer geworden van een geraffineerde oplichtingstruc, uitgevoerd door nepagenten. Deze oplichters maakten misbruik van haar vertrouwen door zich voor te doen als politieagenten. Het slachtoffer werd telefonisch benaderd en overtuigt om waardevolle sieraden ter waarde van duizenden euro's af te staan. Het incident benadrukt de groeiende dreiging van nepagenten, die vaak gebruik maken van autoriteit en geloofwaardigheid om hun slachtoffers te misleiden. Lees verder om meer te leren over deze oplichters, hun werkwijze en hoe je jezelf kunt beschermen tegen dergelijke scams.

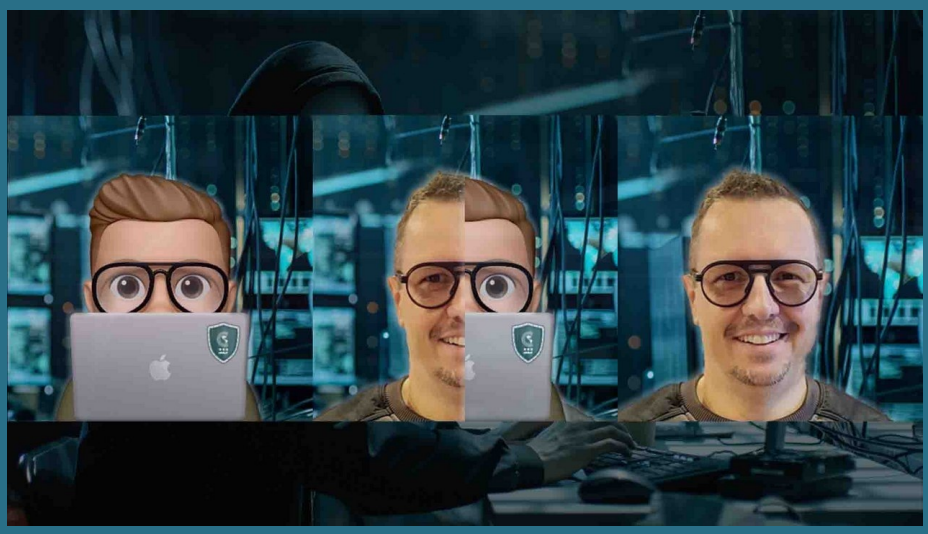
Lees verder

De Cybercrime Podcast van Cybercrimeinfo

Wil je altijd op de hoogte blijven van het laatste cybernieuws? Abonneer je dan op **De Cybercrime Podcast**. Je ontvangt dagelijks een korte update met betrouwbare informatie over actuele dreigingen, trends en praktische adviezen. De inhoud is zorgvuldig samengesteld door Cybercrimeinfo en eenvoudig te volgen via AI-gegenereerde Nederlandse stemmen. Luister waar en wanneer je wilt via **YouTube** of **Spotify** en versterk je digitale weerbaarheid. Abonneren is gratis en zo geregeld.

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.

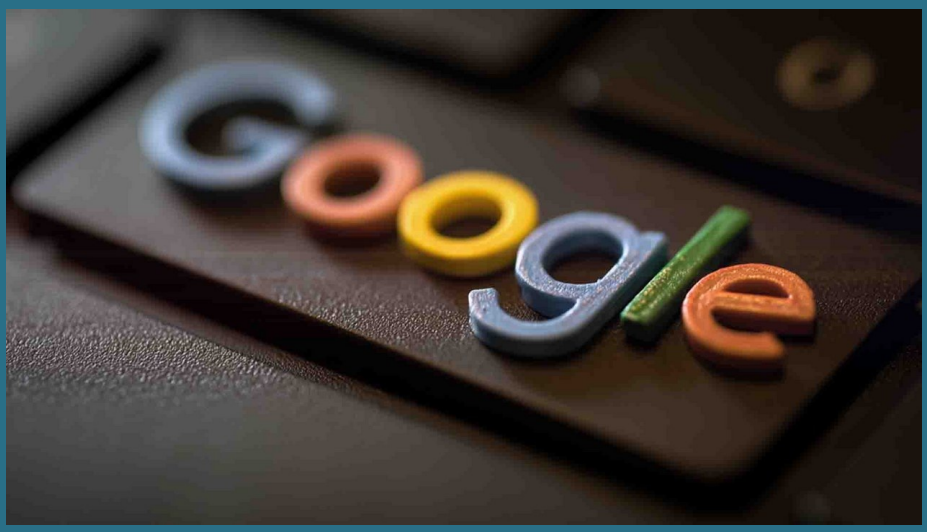
Met vriendelijke groet,
Het team van Cybercrimeinfo

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