



Cybercrimeinfo (ccinfo.nl)
Het onzichtbare zichtbaar maken

Nieuwsbrief 375



[Reading in another language](#)

Kwetsbaarheden in 2025: Hoe bedrijven de digitale dreigingen van morgen kunnen overleven

De digitale dreigingen van morgen vormen een steeds grotere uitdaging voor bedrijven die hun systemen veilig willen houden. In 2025 worden er dagelijks tal van nieuwe kwetsbaarheden ontdekt, die door cybercriminelen snel kunnen worden uitgebuit. Hoe kunnen bedrijven zich hiertegen wapenen? In dit artikel bespreken we de snelheid van kwetsbaarheden, het belang van effectief patchbeheer en de regionale risico's voor bedrijven in België en Nederland. Lees verder om te ontdekken hoe jouw bedrijf zich kan voorbereiden op de digitale dreigingen van de toekomst.

[Lees verder](#)



NoName057(16): De schimmige wereld van pro-Russische cyberoorlog en de strijd om deze digitale dreiging te stoppen

NoName057(16): The shadowy world of pro-Russian cyberwarfare and the struggle to stop this digital threat

[Reading in another language](#)

NoName057(16): De schimmige wereld van pro-Russische cyberoorlog en de strijd om deze digitale dreiging te stoppen

De digitale strijd speelt zich steeds vaker af in de wereld van cyberoorlog, waar groepen als NoName057(16) de grenzen van online dreigingen verleggen. Deze pro-Russische hacktivistische groep richt zich met grootschalige DDoS-aanvallen tegen landen die Oekraïne steunen. In dit artikel duiken we diep in de werking van NoName057(16), de internationale reactie via Operatie Eastwood, en de bredere implicaties van deze cyberdreiging. Ontdek wat deze dreigingen betekenen voor de toekomst van cyberbeveiliging en geopolitieke spanningen.

[Lees verder](#)



De verborgen dreigingen: hoe de veranderende wereldorde Nederland kwetsbaar maakt

The hidden threats: how the changing world order makes the Netherlands vulnerable

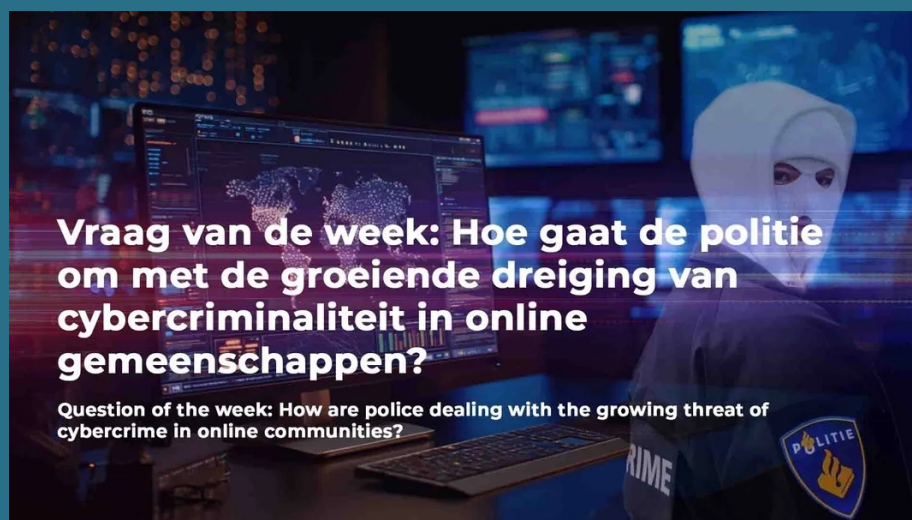
[Reading in another language](#)

De verborgen dreigingen: hoe de veranderende wereldorde Nederland kwetsbaar maakt

De wereldorde verandert snel en daarmee ook de dreigingen voor landen wereldwijd. Nederland is niet alleen een belangrijk knooppunt in Europa, maar ook steeds meer het doelwit van digitale aanvallen door landen als

Rusland, China en Iran. Dit artikel onderzoekt hoe geopolitieke verschuivingen Nederland kwetsbaar maken voor deze verborgen digitale dreigingen. Wat zijn de gevolgen voor onze nationale veiligheid en economie? En hoe kan Nederland zich wapenen tegen deze nieuwe vormen van cyberoorlog? Ontdek meer over de impact van deze veranderingen op de veiligheid van ons land.

[Lees verder](#)



Vraag van de week: Hoe gaat de politie om met de groeiende dreiging van cybercriminaliteit in online gemeenschappen?

Question of the week: How are police dealing with the growing threat of cybercrime in online communities?

[Reading in another language](#)

Vraag van de week: Hoe gaat de politie om met de groeiende dreiging van cybercriminaliteit in online gemeenschappen?

Cybercriminaliteit in online gemeenschappen neemt snel toe, wat vraagt om een proactieve aanpak van de politie. Hoe speelt de wetshandhaving in op deze digitale dreigingen en wat doet Europol om de veiligheid op sociale media en andere platforms te verbeteren? In dit artikel duiken we dieper in de strategieën die Europese landen ontwikkelen om cybercriminaliteit effectiever te bestrijden. Van online patrouilles tot samenwerking met internationale partners, ontdek hoe politie-instanties zich aanpassen aan de virtuele wereld en welke lessen we kunnen trekken voor de toekomst van digitale opsporing.

[Lees verder](#)



Het duistere einde van Abacus Market: exit scam op het darkweb onthuld

The dark end of Abacus Market: exit scam on the dark web revealed

[Reading in another language](#)

Het duistere einde van Abacus Market: exit scam op het darkweb onthuld

Abacus Market, ooit een van de grootste darkweb marktplaatsen, is recent abrupt offline gegaan. Wat leek op een technische storing, blijkt waarschijnlijk een exit scam te zijn, waarbij beheerders met de fondsen van gebruikers zijn verdwenen. Dit incident heeft niet alleen geleid tot enorme verliezen voor betrokkenen, maar ook de bredere instabiliteit van het darkweb verder aangewakkerd. In dit artikel onderzoeken we de signalen die wezen op de scam, de impact op gebruikers, en de bredere gevolgen voor de darkweb economie.

[Lees verder](#)



[Reading in another language](#)

Beverwijk - Helpdesk fraude

Op 29 april 2025 werd een 84-jarige vrouw in Beverwijk het slachtoffer van bankhelpdeskfraude, een oplichtingstechniek die steeds vaker voorkomt. De vrouw werd gebeld door een oplichter die zich voordeed als bankmedewerker en haar naar haar pincode vroeg. Later die dag werd er geld van haar rekening gehaald. Dit geval is slechts één voorbeeld van hoe criminelen misbruik maken van vertrouwen. In dit artikel leer je niet alleen hoe je deze vorm van fraude kunt herkennen, maar ook hoe je jezelf kunt beschermen tegen deze en andere cyberdreigingen zoals vishing en smishing.

[Lees verder](#)

**Blijf alert,
luister
DE CYBERCRIME
PODCAST**

Abonneer je op
onze podcast via

 YouTube

 Spotify



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.

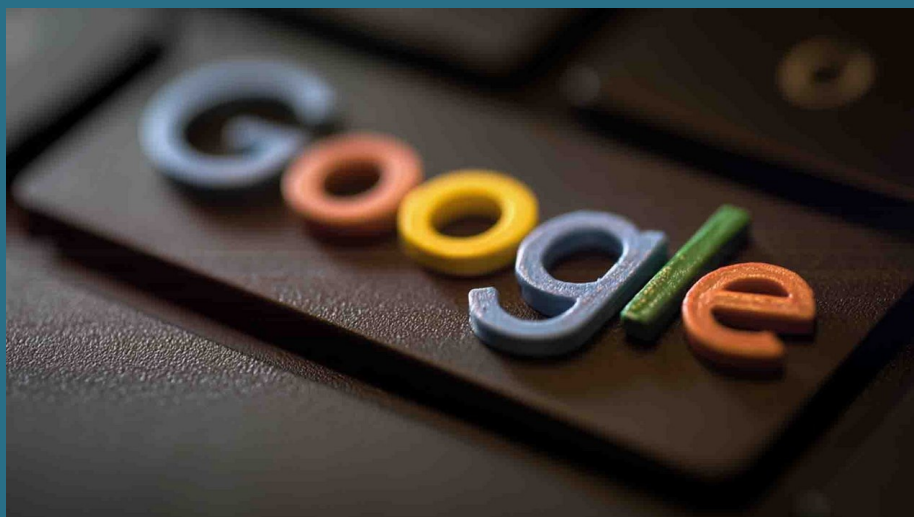
Met vriendelijke groet,
Het team van Cybercrimeinfo



Doneer 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



Share



Tweet



Share



Pinterest



Bluesky



Mastodon

Deze e-mail is verstuurd aan {{email}}.

Als u geen nieuwsbrief meer wilt ontvangen, kunt u zich [hier afmelden](#).

U kunt ook uw gegevens [inzien](#) en [wijzigen](#).

Voor een goede ontvangst voegt u info@cybercrimeinfo.nl toe aan uw adresboek.