Cybercrimeinfo (ccinfo.nl)

Het onzichtbare zichtbaar maken

NB380

Podcast

Podcast

Reading in another language

Toename cybercriminaliteit, DDoS-aanvallen, datalek bij Eurofins & Nederland's rol

Op 23 augustus 2025 werden er verschillende incidenten gemeld die de groeiende dreiging van cybercriminaliteit onderstrepen. Een van de meest impactvolle was de aanval op Eurofins, waarbij persoonlijke en medische gegevens van meer dan een half miljoen mensen werden gestolen. Dit benadrukt de kwetsbaarheid van de zorgsector, die dringend maatregelen nodig heeft om dataveiligheid te verbeteren. Tegelijkertijd voerde de cybergroep NoName DDoS-aanvallen uit op belangrijke Belgische websites, wat opnieuw de kwetsbaarheid van vitale infrastructuren toont. Daarnaast groeit de dreiging van jeugdgedreven cybercrime, waarbij hackercollectieven zoals Scattered Spider steeds professioneler worden. Deze groepen richten zich op bedrijven zoals KLM en MGM Resorts, gebruikmakend van social engineering technieken om gevoelige gegevens te stelen en te verkopen op het dark web. Nederland speelt een sleutelrol in de internationale bestrijding van cybercriminaliteit, zoals blijkt uit de operatie Serengeti 2.0, die leidde tot honderden arrestaties van cybercriminelen wereldwijd.

Lees verder

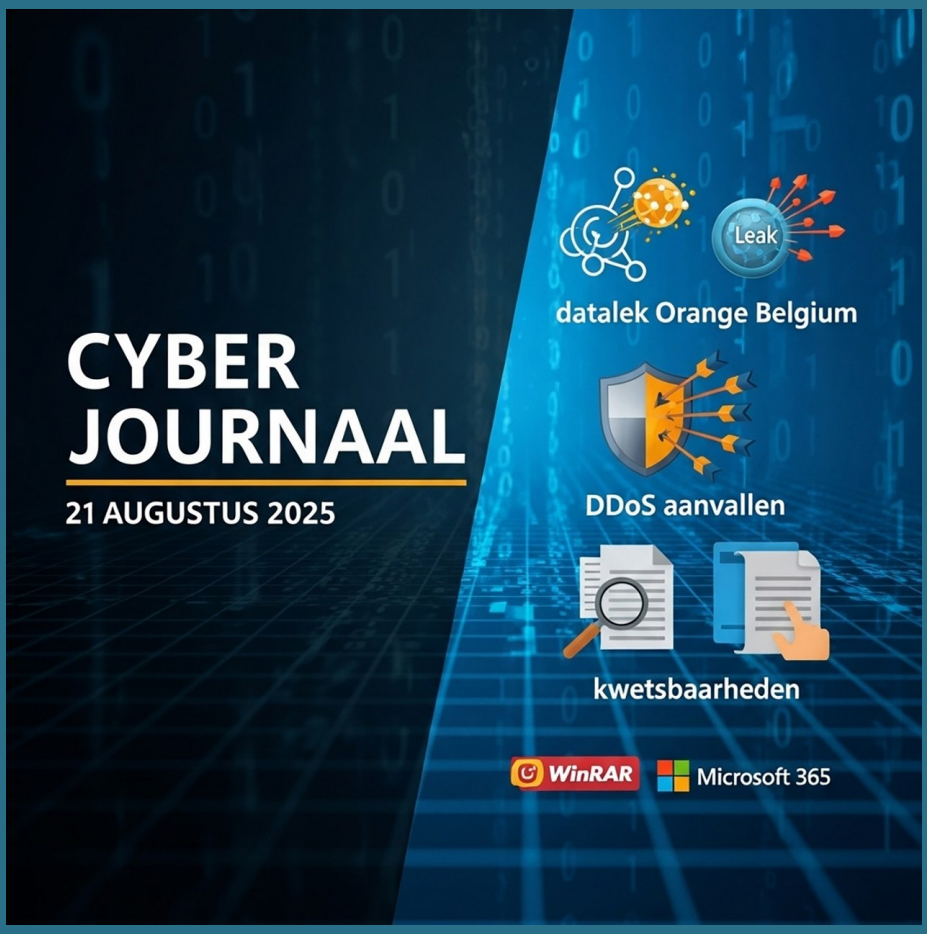
Reading in another language

Ransomware-aanvallen op Seabridge en Fluxys, DDoS-aanvallen op Belgische gemeenten en Apple-kwetsbaarheid

Op 22 augustus 2025 werden verschillende belangrijke cyberincidenten gerapporteerd. Het Belgische bedrijf Seabridge werd getroffen door een ransomware-aanval van de Qilin-groep, wat leidde tot verstoringen in hun bedrijfsvoering. Ook de Belgische gasnetbeheerder Fluxys werd het doelwit van een DDoS-aanval door de Z-ALLIANCE-groep, wat resulteerde in tijdelijke onbereikbaarheid van hun website. Verschillende Belgische gemeentelijke websites, waaronder die van Waimes en Kelmis, werden eveneens getroffen door een DDoS-aanval van de hacker-groep NoName. Daarnaast werd een kritieke kwetsbaarheid in Apple-software ontdekt, die

werd misbruikt voor remote code execution. Apple bracht spoedupdates uit om deze kwetsbaarheid te verhelpen. Er werd ook een ernstige kwetsbaarheid gevonden in Apache Tika, waardoor aanvallers toegang kregen tot gevoelige gegevens via gemanipuleerde PDF-bestanden. Ook werd de ManualFinder Trojan, een gevaarlijke malware die zich voordoet als een PDF-editor, ontdekt, die onder andere cryptomining kan uitvoeren.

Lees verder



Reading in another language

Datalek Orange Belgium, DDoS-aanvallen en kwetsbaarheden in WinRAR en Microsoft 365

Op 21 augustus 2025 kwamen er verschillende belangrijke cyberdreigingen aan het licht. Orange Belgium werd getroffen door een datalek waarbij de persoonlijke gegevens van 850.000 klanten werden gestolen, waaronder telefoonnummers en PUK-codes, wat risico's voor simswapping-aanvallen met zich meebrengt. Tegelijkertijd voerde de NoName-hackersgroep DDoS-aanvallen uit op websites van grote Belgische bedrijven. In Nederland werd een man veroordeeld voor phishing, gericht op ouderen. Daarnaast werden kritieke kwetsbaarheden ontdekt in veelgebruikte software zoals WinRAR en Microsoft 365, waardoor hackers vertrouwelijke gegevens konden stelen. Er werd ook een zero-day kwetsbaarheid ontdekt in WinRAR, misbruikt door cybercriminelen om malware te verspreiden. Bovendien werden beveiligingsrisico's geïdentificeerd in wachtwoordmanagers en 2FA-systemen, wat de noodzaak benadrukt om digitale beveiligingsmaatregelen voortdurend bij te werken. De geopolitieke spanningen in cyberspace werden ook versterkt door misbruik van een kwetsbaarheid in Cisco-apparatuur, waarbij statelijke actoren betrokken waren.

Lees verder

Reading in another language

20 augustus 2025 | Journaal: DDoS-aanvallen op Belgische infrastructuur, kwetsbaarheden in SAP, Salesforce en Telegram-bots

Op 20 augustus 2025 werd België getroffen door meerdere cyberdreigingen, waaronder DDoS-aanvallen van de groepen Z-ALLIANCE en NoName057(16), die verschillende kritieke systemen verstoorden. De haven van Luik werd tijdelijk offline gehaald, wat de strategische impact van de aanval benadrukt. Ook andere Belgische organisaties zoals Vivaqua en Belfius Bank werden getroffen door de hacktivisten. Verder werden ernstige kwetsbaarheden ontdekt in Santesoft en SAP NetWeaver, die potentieel misbruikt kunnen worden voor datalekken en remote code-executie. Beveiligingslekken in Salesforce en Atlassian werden ook blootgelegd door de manier waarop beveiligingsscanners onbedoeld gevoelige informatie lekten naar publieke databases. Een nieuwe dreiging werd geïdentificeerd in de vorm van de GodRAT, die zich richt op financiële instellingen in Nederland en België, terwijl Telegram steeds vaker wordt ingezet door cybercriminelen voor datadiefstal. Tot slot werden geopolitieke risico's benadrukt door Russische cyberaanvallen op een Poolse waterkrachtcentrale, wat de bredere dreigingen voor Europa laat zien.

Lees verder

Reading in another language

19 augustus 2025 | Journaal: NAVO-datalek, DDoS-aanvallen en kwetsbaarheden vergroten cyberdreigingen in België en Nederland

Op 19 augustus 2025 werden verschillende belangrijke cyberdreigingen in België en Nederland gerapporteerd. Een datalek op het darkweb beweerde gevoelige NAVO-gegevens te bevatten, waaronder militaire en strategische informatie. Als dit klopt, heeft dit ernstige gevolgen voor de nationale veiligheid van NAVO-lidstaten zoals België en Nederland. Daarnaast vonden er DDoS-aanvallen plaats op luchthavens in Nederland en vitale instellingen in België, waaronder ENGIE Electrabel en de Rijksdienst voor Sociale Zekerheid. Tevens werden kwetsbaarheden ontdekt in N-Central en Trend Micro Apex One software, die actief misbruikt werden door cybercriminelen, wat het risico op aanvallen vergrootte. Geopolitieke dreigingen, zoals het NAVO-datalek, en ransomware-financiering via cryptocurrency blijven de regio beïnvloeden. Het artikel benadrukt de dringende noodzaak voor bedrijven en overheden om snel te reageren op kwetsbaarheden en de impact van geopolitieke cyberdreigingen serieus te nemen.

Lees verder

Reading in another language

18 augustus 2025 | Journaal: Ransomware-aanvallen, datalekken bij Eurofins, en kwetsbaarheden in Fortinet

Op 18 augustus 2025 werd er melding gemaakt van verschillende cyberdreigingen. Eurofins, een bedrijf in de gezondheidszorg, werd getroffen door een datalek, waarbij vertrouwelijke gegevens werden gestolen. De cybercriminelen dreigen deze gegevens openbaar te maken tenzij een betaling wordt gedaan. Töller, een Belgisch timmerbedrijf, werd getroffen door een ransomware-aanval, waarbij gevoelige bedrijfsinformatie werd buitgemaakt. Er werd ook gewaarschuwd voor geavanceerde phishingaanvallen gericht op effectenmakelaars, waarbij fraudeurs aandelen manipuleren. Verder blijft de Russische groep EncryptHub misbruik maken van kwetsbaarheden in Microsoft Windows om stealer-malware te verspreiden, en is er een kwetsbaarheid in de FortiWeb-webapplicatiewall van Fortinet ontdekt, die bedrijven in België en Nederland bedreigt. Gamers en PayPal-gebruikers worden gewaarschuwd voor malware en datalekken die via piratensites en gestolen inloggegevens verspreid worden. Tenslotte werden Chinese hackers in verband gebracht met cyberaanvallen op webinfrastructuren in Taiwan, wat ook een bedreiging vormt voor Belgische en Nederlandse organisaties.

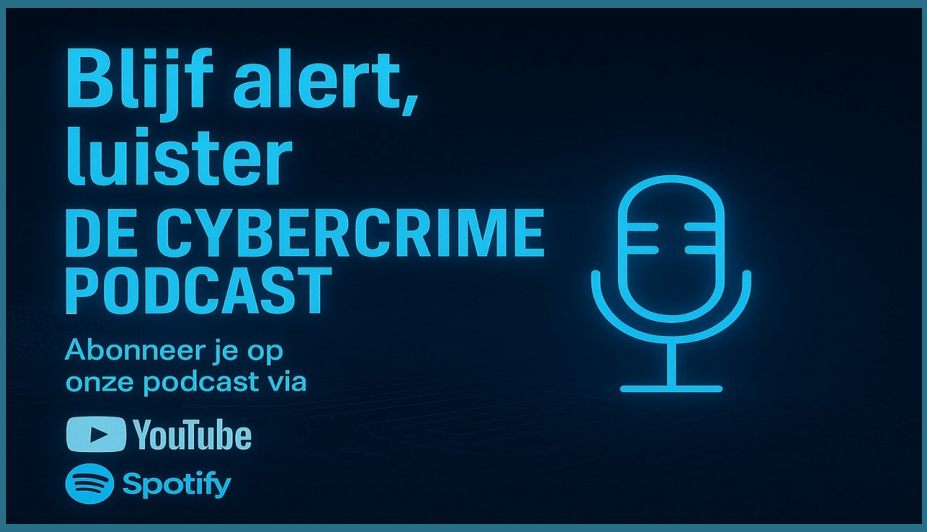
Lees verder

Reading in another language

Utrecht, nepagent oplichting: vrouw verliest 1400 euro door valse politieagent

Op 16 mei 2025 werd een vrouw in Utrecht het slachtoffer van een oplichtingsactie door een nepagent. De man, die zich voordeed als politieagent "Bas Brouwer", belde de vrouw en waarschuwde haar dat haar waardevolle spullen in gevaar waren. Onder het voorwendsel haar bankpassen te blokkeren om diefstal te voorkomen, vroeg de nepagent haar om pincodes en geld. Na meerdere telefoongesprekken met een tweede nepagent gaf de vrouw uiteindelijk 800 euro contant geld en haar pinpassen af. Later werd ontdekt dat met de gestolen passen 1400 euro werd opgenomen. De verdachte, die mogelijk minderjarig is, werd op camerabeelden vastgelegd, maar zijn gezicht is geblurd. De politie roept getuigen op zich te melden en benadrukt het belang van waakzaamheid tegen nepagenten, die gebruik maken van de autoriteit van de politie om slachtoffers te misleiden.

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.

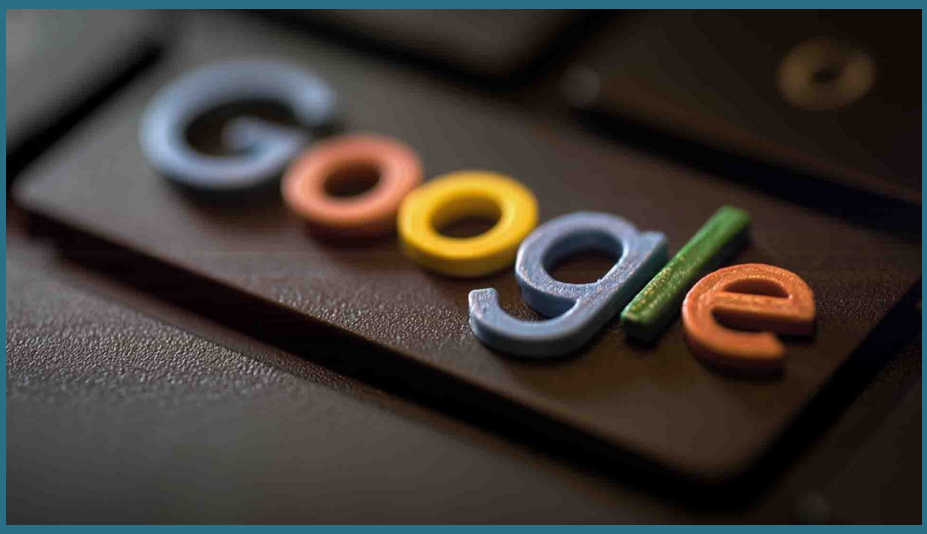
Met vriendelijke groet,
Het team van Cybercrimeinfo

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

Share Tweet Share Pinterest Bluesky Mastodon