Cybercrimeinfo

"Omdat wat waardevol is, beschermd moet worden"

Nieuwsbrief 397

Bent u nog digitaal weerbaar in de laatste weken van 2025?

Terwijl het jaar ten einde loopt, blijkt de digitale wereld onverminderd turbulent. Week 51 bracht verontrustend nieuws over statelijke actoren, Duitsland wijst direct naar de Russische militaire inlichtingendienst voor aanvallen op kritieke infrastructuur, en ook in Nederland scherpt de MIVD de strategie voor 2026 aan. Maar de dreiging komt niet alleen van spionnen. Wist u dat een populair e-book uw apparaat kan overnemen, of dat hackersgroep ShinyHunters claims legt op de gegevens van 1,5 miljoen Nederlanders? En wat betekent de recente overname van iDIN door het Belgische itsme voor uw digitale identiteit?
Van ransomware op hypervisors tot datalekken via ChatGPT.

QUIZ 51-2025

Strategisch Dreigingsrapport Cyberveiligheid week 51-2025

Het moderne cyberdreigingslandschap bevindt zich op een kritiek kantelpunt waarbij de grens tussen de digitale en fysieke wereld definitief is vervaagd, wat resulteert in tastbare maatschappelijke ontwrichting door sabotage van kritieke infrastructuren en economische beïnvloeding. Deze dreiging wordt gevoed door een convergentie van geopolitieke spanningen, de verregaande professionalisering van cybermisdaad en wijdverspreide technologische kwetsbaarheden, wat een geïntegreerde strategische benadering van beleidsmakers en organisaties noodzakelijk maakt.

Natiestaten zetten code steeds vaker in als strategisch wapen voor hybride oorlogsvoering, waarbij zowel directe aanvallen op vitale systemen als geraffineerde desinformatiecampagnes met deepfakes worden gebruikt om democratische processen te ondermijnen. Concrete incidenten tonen aan dat de Benelux direct in de vuurlinie ligt, wat onder meer blijkt uit gecoördineerde DDoS aanvallen op Belgische overheidsdiensten en de overname van IoT-gestuurde infrastructuren in Nederlandse steden door buitenlandse actoren. Geavanceerde dreigingsgroepen innoveren voortdurend door misbruik te maken van legitieme clouddiensten en vertrouwde systeemmechanismen, waardoor hun activiteiten uiterst moeilijk te detecteren zijn met traditionele beveiligingsinstrumenten.

Parallel aan statelijke acties is de cybercriminaliteit getransformeerd tot een geïndustrialiseerde sector met een volwaardige toeleveringsketen en gespecialiseerde diensten zoals Ransomware as a Service en Phishing as a Service. Deze ontwikkeling verlaagt de drempel voor kwaadwillenden aanzienlijk, aangezien complexe aanvalstools nu voor relatief lage prijzen toegankelijk zijn via platforms als Telegram en het dark web. De economische impact van deze professionalisering is aanzienlijk, aangezien meer dan de helft van de getroffen bedrijven verliezen lijdt die de grens van tweehonderdvijftigduizend dollar overschrijden, wat de urgentie voor een proactieve en weerbare defensiestrategie onderstreept.

RAPPORT 51-2025

Vraag van de week: Waarom de digitale euro zoveel vragen oproept en waarom die vragen terecht zijn

De digitale euro is een geplande digitale vorm van publiek geld binnen de eurozone, beheerd door de Europese Centrale Bank. In tegenstelling tot commercieel bankgeld fungeert dit als een digitaal alternatief voor contant geld. Hoewel het stabiliteit en onafhankelijkheid van private partijen nastreeft, roept het project belangrijke vragen op over privacy, macht en controle. Het debat richt zich vooral op de waarborgen tegen misbruik, de beveiliging tegen cybercrime en de noodzaak van een publieke digitale betaalinfrastructuur.

LEES VERDER

Live transcriptie van Epstein dossiers via github, een revolutie in open source intelligence

De vrijgave van nieuwe Epstein-dossiers door de Amerikaanse overheid heeft geleid tot een technologische revolutie binnen open source intelligence. Via een uniek GitHub-project wordt de enorme stroom aan juridische documenten realtime verwerkt met geavanceerde AI technologie. Deze software zet scans onmiddellijk om in doorzoekbare tekst en identificeert automatisch relevante personen en organisaties. Hierdoor kunnen onderzoekers en journalisten razendsnel complexe data analyseren zonder te wachten op handmatige transcripties, wat de transparantie en democratische controle aanzienlijk versterkt.

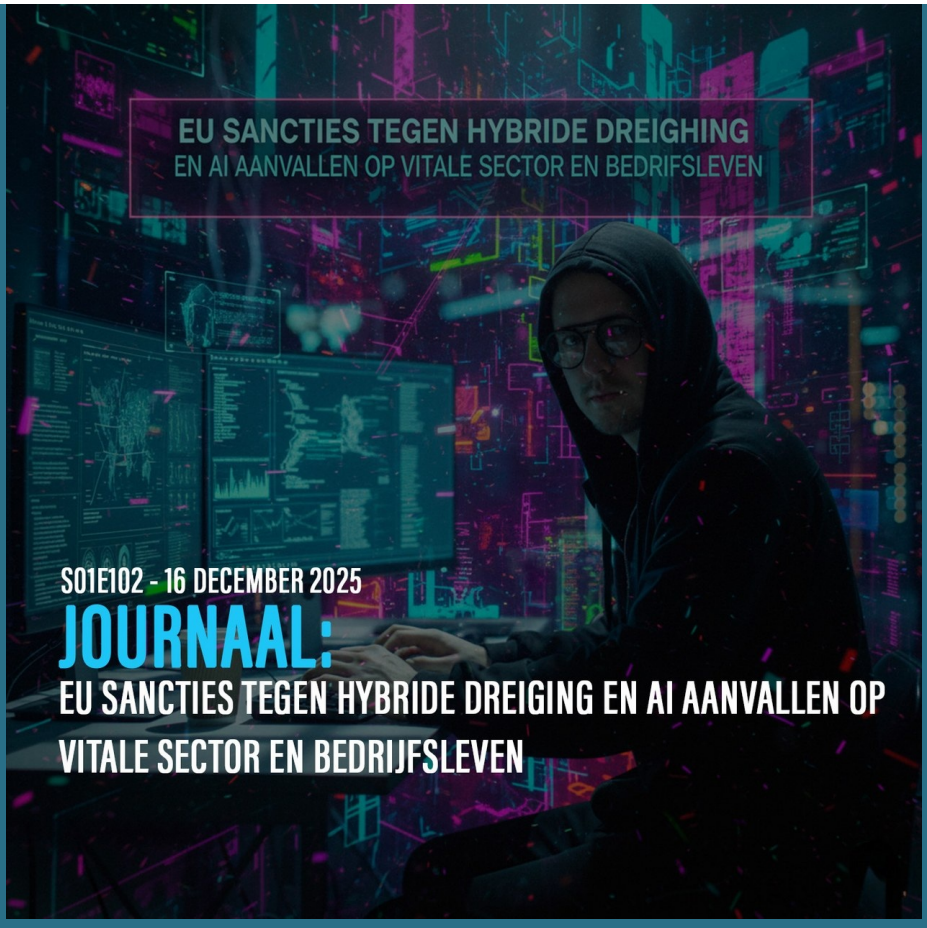
LEES VERDER

Russische sabotage van luchtverkeer en digitale belegering van lokale besturen

Dit artikel beschrijft een toename van hybride oorlogsvoering en cybercriminaliteit, waarbij Russische actoren en hacktivisten vitale infrastructuren en overheden in Nederland, België en Duitsland bestoken. Naast politiek gemotiveerde sabotage, zoals aanvallen op de luchtverkeersleiding en lokale besturen, vormen verouderde software in voertuigen en slimme apparaten grote beveiligingsrisico's. Ook geavanceerde malwarecampagnes en grootschalige datalekken zetten de digitale veiligheid onder druk. Overheden reageren hierop door plannen te ontwikkelen die de nationale digitale soevereiniteit moeten versterken.

LEES VERDER

Weten hoe kwetsbaar jouw organisatie is?
Plan een gratis adviesgesprek



EU sancties tegen hybride dreiging en AI aanvallen op vitale sector en bedrijfsleven

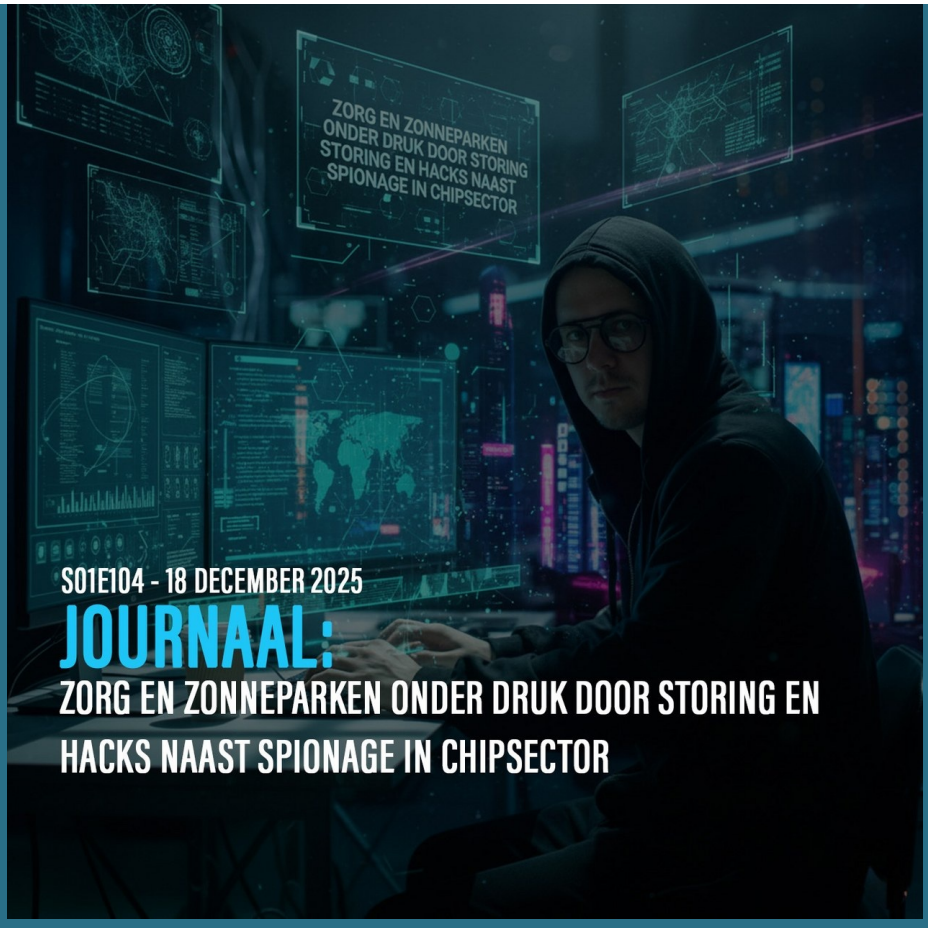
De Europese Unie intensiveert de strijd tegen hybride oorlogsvoering door sancties op te leggen aan actoren die Russische desinformatie en cyberaanvallen steunen. Ondertussen neemt de digitale dreiging toe door gecoördineerde aanvallen op de vitale infrastructuur, waaronder de Belgische energiesector. Cybercriminelen gebruiken steeds vaker geavanceerde technieken zoals kunstmatige intelligentie en sociale engineering om data te stelen en systemen te ontregelen. Ondanks deze groeiende risico's boeken opsporingsdiensten successen met arrestaties in grote fraudezaken en strenger toezicht op privacy.

LEES VERDER

Datalekken en droneaanvallen teisteren vitale sectoren onder dreiging van AI spionage

Recente incidenten tonen een zorgwekkende vermenging van fysieke en digitale dreigingen. Terwijl innovatieve droneaanvallen de maritieme oorlogsvoering veranderen, worden wereldwijd vitale sectoren en streamingdiensten getroffen door grootschalige datalekken. Cybercriminelen misbruiken razendsnel nieuwe kwetsbaarheden in beheersoftware en voertuigen, terwijl spionage via browser-extensies en AI toepassingen toeneemt. Ondanks internationale politieacties tegen fraudenetwerken, waarschuwen experts voor een toekomst waarin autonome kunstmatige intelligentie cyberaanvallen uitvoert met een snelheid die menselijk ingrijpen onmogelijk maakt.

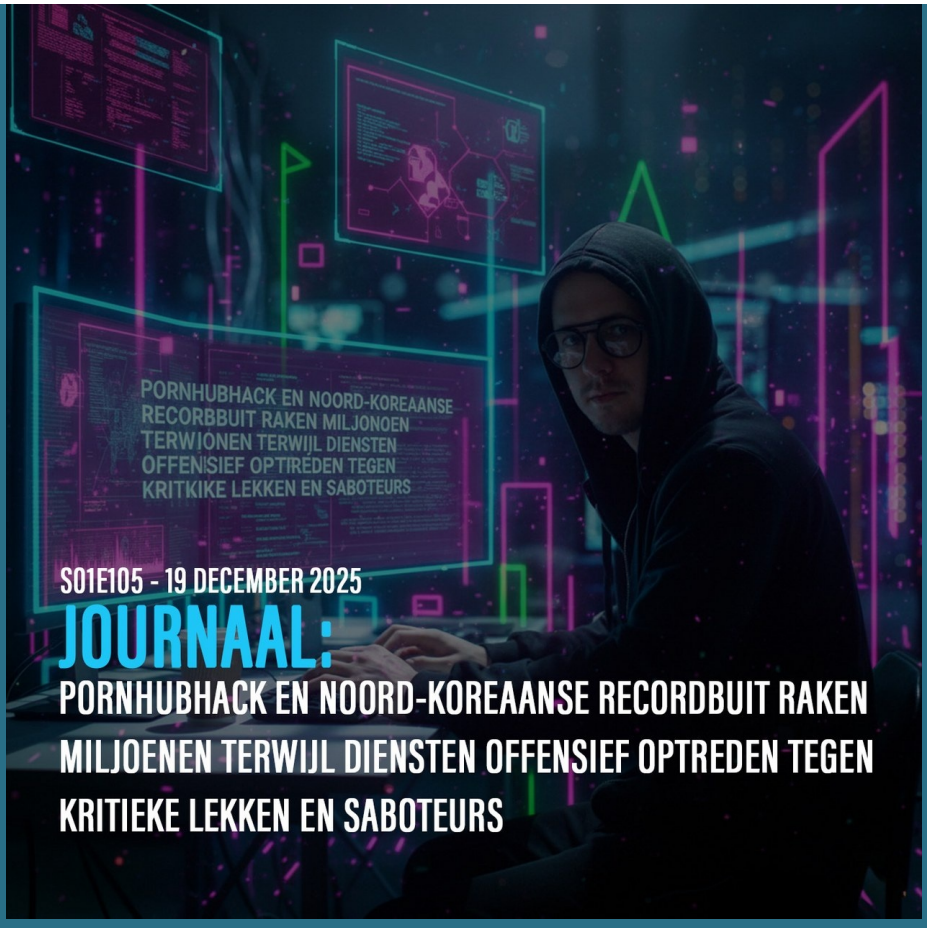
LEES VERDER



Zorg en zonneparken onder druk door storing en hacks naast spionage in chipsector

De digitale veiligheid staat breed onder druk door een combinatie van technische storingen, spionage en geavanceerde cyberaanvallen. In de zorgsector leidden softwareproblemen tot uitgestelde operaties, terwijl de energiesector kwetsbaar blijkt voor sabotage van zonneparken. Ondertussen verharden geopolitieke spanningen door Chinese spionage in de chipsector en Russische hybride oorlogsvoering. Innovatieve malware en misbruik van AI maken datadiefstal en fraude steeds complexer. Toezichthouders reageren hierop met miljoenenboetes en arrestaties om nalatigheid en criminaliteit effectiever te bestrijden.

LEES VERDER



Pornhubhack en Noord-Koreaanse recordbuit raken miljoenen terwijl diensten offensief optreden tegen kritieke lekken en saboteurs

Miljoenen burgers zijn getroffen door grootschalige datalekken, waaronder een diefstal bij Pornhub waarbij privégegevens van anderhalf miljoen Nederlanders zijn buitgemaakt. Daarnaast zorgen kritieke beveiligingslekken in netwerkapparatuur en beheersoftware voor grote risico's. Terwijl criminelen records breken met cryptoroof en spionage, treden internationale opsporingsdiensten offensief op. Zo werd een belangrijk witwasplatform ontmanteld en zijn verdachten van sabotage opgepakt. Beheerders en gebruikers moeten alert blijven op aanhoudende dreigingen in de cloud en via malafide software.

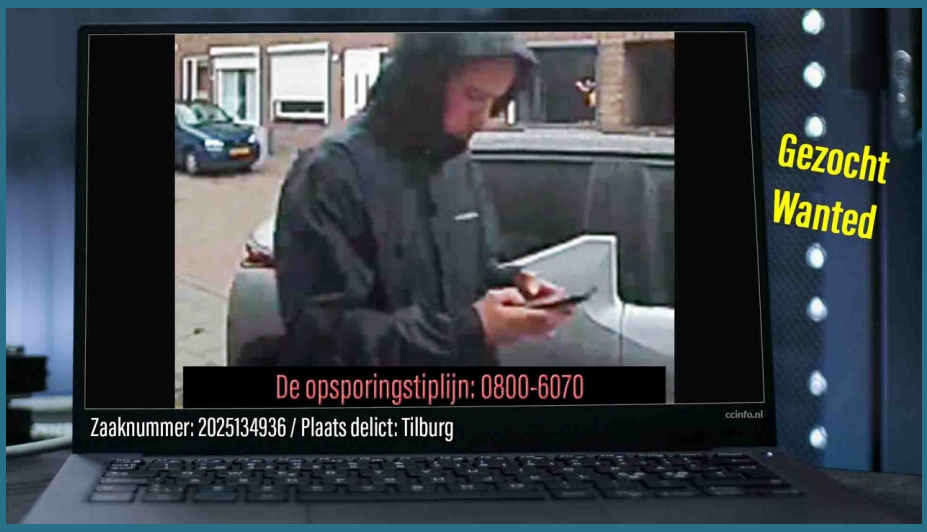
LEES VERDER

Dagelijks inzicht in actuele cyberdreigingen
Abonneer u op het cyberdreigingsrapport

Ransomware bij Rconcept en AI datalek gemeente Eindhoven naast sabotage van waterleidingen en spionage

Diverse organisaties zijn recent getroffen door ernstige cyberincidenten. Zo kampt de gemeente Eindhoven met een groot datalek door onveilig gebruik van AI tools en is het Belgische Rconcept slachtoffer van ransomware. Daarnaast vormen kritieke kwetsbaarheden in firewalls en moederborden een acuut risico. Wereldwijd neemt de dreiging toe door actieve spionagegroepen en sabotage van vitale infrastructuur, zoals een waterleidingbedrijf in Denemarken. Gelukkig zijn er ook successen geboekt met de arrestatie van enkele cybercriminelen en corrupte beveiligers.

LEES VERDER



Bent u nog digitaal weerbaar in de laatste weken van 2025?

In Tilburg zijn slachtoffers misleid door geraffineerde bankhelpdeskfraude. Criminelen gebruiken een combinatie van sms-berichten, langdurige

telefoongesprekken en fysieke bezoeken van koeriers om vertrouwen te winnen. Door psychologische manipulatie worden slachtoffers geïsoleerd en gedwongen om limieten te verhogen en bankpassen af te geven. De politie benadrukt dat banken nooit aan de deur komen of om pincodes vragen. Bij verdachte situaties is het essentieel om direct op te hangen en zelf contact op te nemen met de bank.

LEES VERDER

Luister naar de discussiepodcast over het nieuws van de afgelopen week.

Luister de podcast nu op Youtube

Luister de podcast nu op Spotify

Meer leren over cybercrime? Ontdek de verschillende vormen en begrippen

In de Cybercrimeinfo Bibliotheek vind je een uitgebreide verzameling van termen en verschillende vormen van cybercriminaliteit. Van phishing en malware tot ransomware en andere digitale dreigingen, we leggen elke vorm duidelijk uit. Zo krijg je inzicht in wat deze aanvallen inhouden, hoe ze werken en welke risico's ze met zich meebrengen.

Of je nu op zoek bent naar uitleg over specifieke cybercrime termen of meer wilt leren over de verschillende soorten digitale bedreigingen, onze bibliotheek biedt de kennis die je nodig hebt om jezelf beter te beschermen.

Verdiep je in de wereld van cybercrime en vergroot je digitale weerbaarheid.

BEKIJK DE BIBLIOTHEEK

Beantwoorde vragen en tips voor digitale weerbaarheid

Op deze pagina vind je antwoorden op veelgestelde vragen, nuttige tips en praktische hulpmiddelen om je digitale veiligheid te verbeteren. Of je nu meer wilt weten over bescherming tegen cyberdreigingen of jezelf beter wilt wapenen tegen online gevaren, wij bieden de informatie die je nodig hebt.

BEKIJK DE TIPS

Veelgestelde vragen over digitale veiligheid en cybercrime

Op Cybercrimeinfo vind je antwoorden op de meest gestelde vragen over cybersecurity en cybercrime. Leer hoe je jezelf en je organisatie kunt beschermen tegen digitale dreigingen, van phishing en malware tot ransomware en DDoS-aanvallen. We bieden duidelijke uitleg en praktische tips om je digitale veiligheid te versterken.

ONTDEK DE ANTWOORDEN

Vergroot je kennis en vaardigheden

Wil je je kennis over cybersecurity en het darkweb uitbreiden? Bij de Leerplek van Cybercrimeinfo vind je een breed aanbod van cursussen, tutorials en quizzen die je helpen up-to-date te blijven met de nieuwste technieken en dreigingen. Of je nu net begint of al een expert bent, onze interactieve leeromgeving biedt de uitdaging die je nodig hebt om jezelf verder te ontwikkelen.
Test je kennis met uitdagende quizzen en verdien toegang tot de exclusieve Perfecte Score Club. Voor opsporingsambtenaren bieden we binnenkort speciaal op maat gemaakte quizzen aan.

TEST JE KENNIS

Contact met Cybercrimeinfo

Heb je een vraag of probleem? Vul het formulier in en stel je vraag. We reageren zo snel mogelijk, maar houd er rekening mee dat het door de hoge aantallen vragen soms enkele dagen kan duren.

STEL JE VRAAG

Steun Cybercrimeinfo en help de strijd tegen cybercriminaliteit

Elke dag zetten wij ons in om je op de hoogte te houden van de laatste cyberdreigingen en trends. Onze missie is om jou en anderen te beschermen tegen de groeiende risico's in de digitale wereld. Maar we kunnen dit niet alleen. Jouw steun maakt het verschil.
Door te doneren help je ons waardevolle informatie te blijven leveren, nieuwe tools te ontwikkelen en de bewustwording over cybercriminaliteit te vergroten. Elke bijdrage, groot of klein, draagt bij aan de bescherming van digitale veiligheid.
Wil je ons steunen?

Samen maken we de online wereld een stukje veiliger.
Bedankt voor je steun!

❤ STEUN ONS NU

Dagelijks cyber journaal van Cybercrimeinfo

Het Dagelijks Cyber Journaal biedt dagelijkse updates over de belangrijkste cyberdreigingen en incidenten in België en Nederland. Dit is bedoeld voor mensen die de ontwikkelingen in cybercrime willen volgen, maar geen tijd hebben om alles bij te houden. Het biedt een efficiënte manier om snel up-to-date te blijven zonder uren te spenderen aan het zoeken naar relevante informatie. De updates zijn beschikbaar in zowel tekst als via een dagelijkse podcast op Spotify en YouTube.

Ontvang dagelijks het cyber journaal tussen 12:00 en 14:00 (behalve zondag).
Schrijf je in en ontvang het automatisch in je mailbox.

E-mailadres *

Voornaam

Achternaam

Inschrijven

Inschrijven

Ontvang dagelijks het cyber journaal tussen 12:00 en 14:00 (behalve zondag). Schrijf je in en ontvang het automatisch in je mailbox.

INSCHRIJVEN

Share Tweet Share Pinterest Bluesky Mastodon