Cybercrimeinfo.nl
Het onzichtbare zichtbaar maken

Nieuwsbrief 356

Reading in another language

Slachtofferanalyse en trends België en Nederland februari 2025

Ransomware, datalekken en DDoS aanvallen blijven ook in februari 2025 een serieuze dreiging vormen voor bedrijven, overheden en onderwijsinstellingen in Nederland en België. Van gemeenten en productiebedrijven tot ICT dienstverleners en reisorganisaties, geen enkele sector bleef gespaard. Cybercriminelen verfijnen hun tactieken en maken steeds vaker gebruik van geavanceerde methoden om gegevens te stelen of systemen te saboteren.
In dit maandelijkse overzicht brengen we de belangrijkste cyberincidenten in kaart, analyseren we trends en geven we concrete aanbevelingen om toekomstige aanvallen te voorkomen. Hoe ernstig is de impact van deze aanvallen? Welke organisaties werden getroffen?

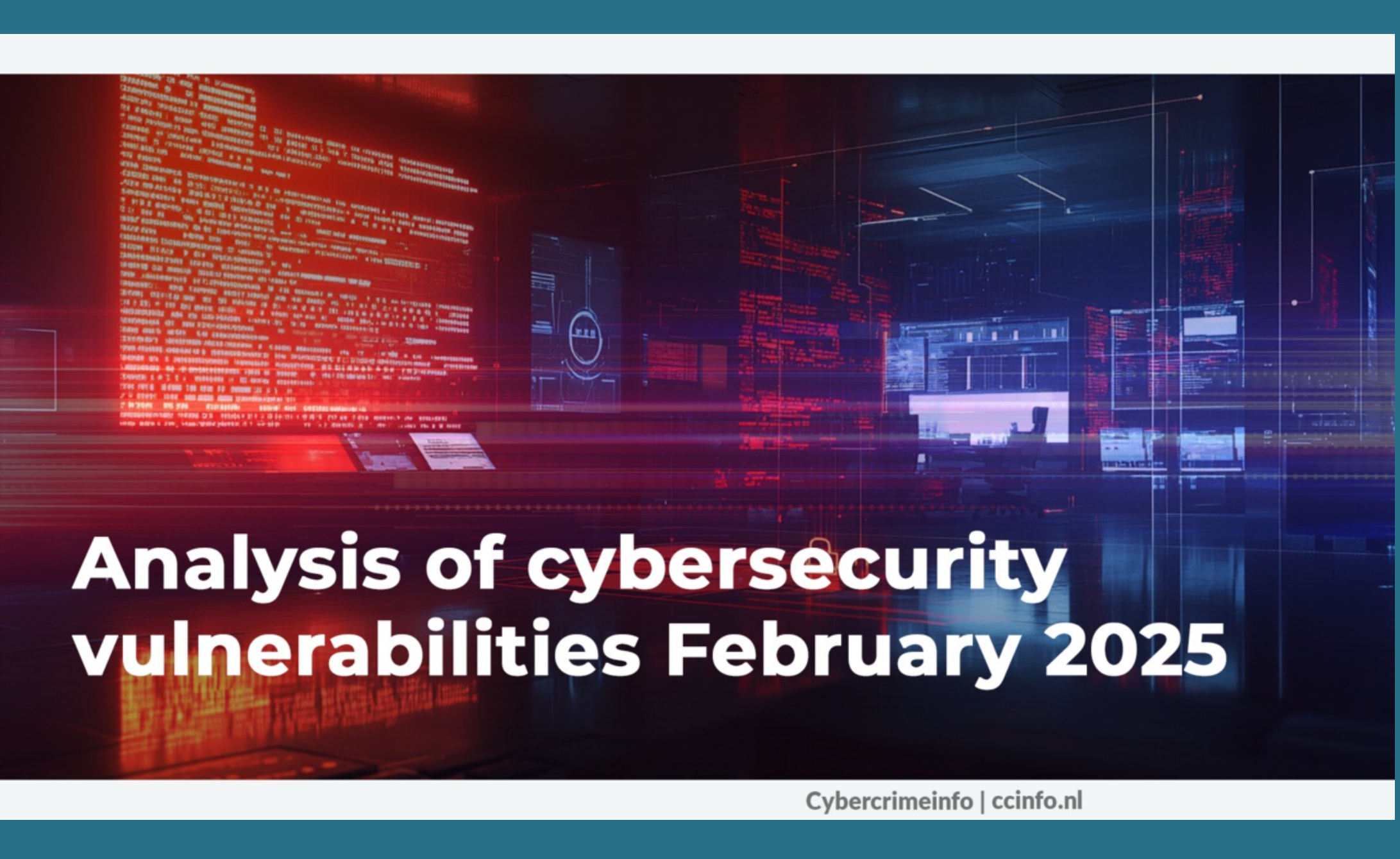
Lees verder

Reading in another language

Cyberoorlog nieuws 2025 februari

Februari 2025 werd gekenmerkt door een golf aan cyberaanvallen die de kwetsbaarheid van Europa's digitale infrastructuren blootlegden. Van de gerichte inzet van Paragon spyware tegen Nederlandse WhatsApp gebruikers tot een dreigende aanval op het Belgische elektriciteitsnet kwamen cybercriminelen en staatshackers steeds nadrukkelijker in beeld. Ondertussen waarschuwde De Nederlandsche Bank voor de groeiende risico's binnen de financiële sector terwijl Russische en Chinese hackers zich richtten op overheidsinstellingen en kritieke systemen. Hoe beïnvloeden deze aanvallen onze digitale veiligheid en welke maatregelen zijn noodzakelijk om de cyberdreiging het hoofd te bieden? Lees verder en ontdek de meest verontrustende ontwikkelingen in de wereld van cyberoorlog.

Lees verder



Reading in another language

Analyse van kwetsbaarheden op het gebied van cyberbeveiliging februari 2025

Elke maand worden nieuwe kwetsbaarheden ontdekt die hackers een kans geven om in te breken in systemen en gevoelige gegevens te stelen. In februari 2025 waren het vooral Apple-chips, Zimbra, NVIDIA en verschillende industriële systemen die in de schijnwerpers stonden. Van speculatieve aanvallen op Apple-processors tot kritieke kwetsbaarheden in veelgebruikte software, de risico's nemen toe. Dit artikel biedt een diepgaand overzicht van de meest urgente beveiligingslekken en laat zien welke maatregelen je kunt nemen om je systemen te beschermen tegen dreigingen die steeds geavanceerder worden.

Lees verder

Reading in another language

Politie cyber nieuws 2025 februari

Cybercriminelen worden steeds slimmer en gewetenlozer, maar politie en justitie zitten niet stil. In februari 2025 wisten opsporingsdiensten meerdere cybercriminelen in de kraag te vatten, van bankhelpdeskfraudeurs en Snapchat-afpersers tot internationale hackers. Dankzij alertheid van slachtoffers en gecoördineerde politieacties konden meerdere misdrijven worden verijdeld en verdachten gearresteerd. Tegelijkertijd roepen nieuwe dreigingen vragen op over de bescherming van vertrouwelijke gegevens en het verschoningsrecht. In dit artikel lees je hoe de politie cybercrime te lijf gaat, welke trends opvallen en wat jij kunt doen om jezelf te beschermen tegen digitale oplichting.

Lees verder

Reading in another language

De ondergang van Incognito Market hoe een darkwebkoning ten val kwam

Incognito Market leek onaantastbaar een gigantische marktplaats op het darkweb waar anonieme handelaren miljoenen verdienden. Maar zelfs in de digitale onderwereld kan één misstap fataal zijn. De jonge Taiwanese programmeur achter het platform bouwde een imperium met geavanceerde beveiligingstechnieken, maar maakte cruciale fouten die uiteindelijk zijn eigen ondergang inluidden. Hoe wisten opsporingsdiensten en hackers hem op te sporen en waarom stortte zijn marktplaats als een kaartenhuis in elkaar? Ontdek het fascinerende verhaal achter de val van een darkwebkoning.

Lees verder

Reading in another language

Helmond - Helpdesk fraude

Een inwoner van Helmond is recent slachtoffer geworden van een geraffineerde vorm van bankhelpdeskfraude. Oplichters deden zich telefonisch voor als medewerkers van ABN AMRO en overtuigden het slachtoffer om zijn bankpas en pincode af te geven aan een nepkoerier. Kort daarna werd er tweemaal €900 opgenomen met de gestolen pas. De politie heeft camerabeelden van een verdachte en roept het publiek op om mee te helpen bij de opsporing. Herken jij deze persoon of heb je tips? Lees verder en ontdek hoe deze vorm van fraude werkt en hoe je jezelf kunt beschermen tegen dit type oplichting.

Lees verder

AI-gids CyberWijzer: Kunstmatige intelligentie voor cyberveiligheid

De AI-gids CyberWijzer biedt een overzicht van hoe kunstmatige intelligentie (AI) kan helpen bij het verbeteren van cyberveiligheid. De gids bevat praktische tips en tools om AI effectief in te zetten tegen digitale dreigingen. Met de opkomst van cybercriminaliteit wordt AI steeds vaker gebruikt om aanvallen sneller te detecteren en te bestrijden. CyberWijzer helpt gebruikers om AI op een veilige en verantwoorde manier toe te passen, zowel voor bedrijven als particulieren. De gids behandelt onder andere het herkennen van verdachte activiteiten, het verbeteren van wachtwoordbeheer en het veilig omgaan met online data. Daarnaast is CyberWijzer zeer handig bij de implementatie van de NIS2-richtlijn, die strengere eisen stelt aan cybersecurity binnen bedrijven en organisaties. Door AI op de juiste manier te benutten, kunnen organisaties en individuen zich beter wapenen tegen cyberdreigingen.

AI CyberWijzer

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