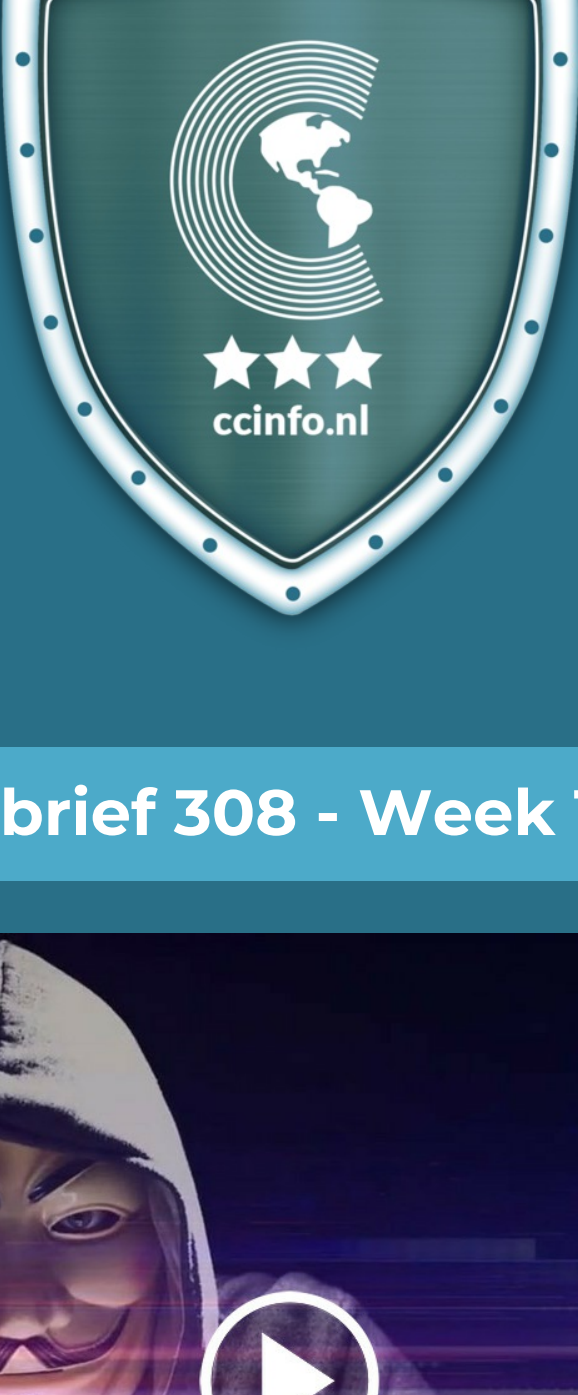




Nieuwsbrief 308 - Week 14-2024



De afgebeelde personen in de foto's en video's zijn gecreëerd met AI en bestaan niet echt.

Nieuwsbrief



Digitale Oorlogsvoering in 2024: Escalerende Cyberaanvallen en Hun Impact op Wereldwijde Veiligheid

In de schaduwen van het digitale tijdperk voeren cybercriminelen en staten een onzichtbare oorlog, waarbij de grenzen tussen recht en onrecht, beveiliging en kwetsbaarheid, steeds verder vervagen. Recentelijk hebben we een escalatie gezien in cyberaanvallen die zowel nationale overheden als kritieke infrastructuur over de hele wereld treffen. Deze aanvallen variëren van gerichte phishing-campagnes tot grootschalige DDoS-aanvallen, die de groeiende dreiging van cybercriminaliteit voor onze samenleving onderstrepen. Ontdek meer over hoe deze cyberdreigingen onze veiligheid en democratie beïnvloeden door verder te lezen op onze website.

[Lees verder](#)



Kritieke Cyberdreigingen in Maart 2024: Een Diepgaande Analyse van Recent Ontdekte Kwetsbaarheden

In maart 2024 kwamen diverse kritieke cybersecuritykwetsbaarheden aan het licht die zowel individuen als organisaties wereldwijd raken. Opmerkelijk is de ontdekking van een achterdeur in XZ Tools, die veel gebruikt wordt binnen Linux distributies. Deze kwetsbaarheid, geïdentificeerd als CVE-2024-3094, maakt het mogelijk voor onbevoegden om op afstand code uit te voeren. Daarnaast zijn er ernstige lekken ontdekt in Google Chrome en Microsoft Exchange, die snelle actie vereisen om potentiële schade te beperken. Voor een gedetailleerde analyse van deze en andere recente kwetsbaarheden, en tips over hoe je je systemen kunt beschermen, lees verder op onze website.

[Lees verder](#)



Grensoverschrijdende doorbraken in de maart-editie van politie cyber nieuws 2024

Ontdek de nieuwste wereldwijde inspanningen tegen cybercriminaliteit in ons uitgebreide verslag van politie cyber nieuws van maart 2024. We belichten belangrijke doorbraken, waaronder de aanpak van bankhelpdeskfraude en de succesvolle ontmanteling van duistere netwerken op het darkweb. De complexiteit van cybercriminaliteit komt aan het licht door diverse internationale operaties, zoals de recente actie tegen de beruchte Blackcat-ransomware, waarbij de Amerikaanse overheid een beloning van 10 miljoen dollar uitloofde voor cruciale informatie. Lees meer over hoe samenwerkende autoriteiten wereldwijd stappen zetten om onze digitale wereld veiliger te maken. Klik om het volledige artikel te lezen.

[Lees verder](#)



Slachtofferanalyses en Trendontwikkelingen van Week 13-2024

Verken de laatste ontwikkelingen in cybercriminaliteit met onze analyse van slachtoffergevallen en trends uit week 13-2024. Deze editie belicht de toename van DinodasRAT Malware, gericht op Linux servers, en onthult belangrijke inzichten in een groot datalek bij AT&T, dat 73 miljoen klanten heeft getroffen. Ontdek hoe deze en andere recente incidenten invloed hebben op diverse sectoren, van de financiële wereld tot de detailhandel, en krijg praktische adviezen voor het verbeteren van je digitale beveiliging. Voor een uitgebreid verslag van onze bevindingen, klik op verder lezen op onze website.

[Lees verder](#)



De Verborgen Gevaren: Cyberveiligheid en Aansprakelijkheid in Supply Chains

Ontdek hoe cyberincidenten binnen supply chains ernstige verstoringen kunnen veroorzaken in bedrijfsoperaties en de complexe juridische vraagstukken die hierbij komen kijken. In ons nieuwste artikel verkennen we de impact van deze digitale bedreigingen, belichten we de uitdagingen en bieden we praktische tips voor preventie en bescherming. Zorg dat je voorbereid bent op mogelijke cyberdreigingen en leer hoe je effectieve samenwerking en communicatie binnen de supply chain kunt bevorderen om je risico's te minimaliseren. Lees het volledige artikel voor gedetailleerde inzichten en deskundige adviezen over het beheren van cyberveiligheid in een verbonden wereld.

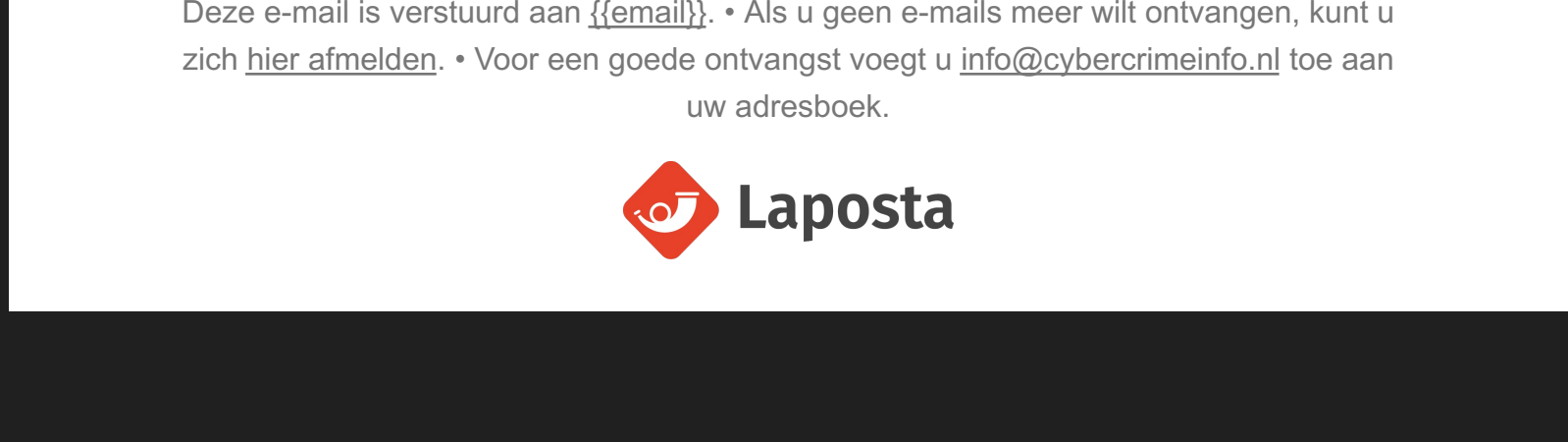
[Lees verder](#)



Alert in Den Haag: Hoe Bankhelpdeskfraude Slachtoffers Misleidt

In augustus 2023 viel een inwoner van Den Haag ten prooi aan bankhelpdeskfraude. De oplichters deden zich voor als bankmedewerkers en beweerden dat er problemen waren met zijn bankrekening. Ze meldden dat een medewerker de pinpas zou ophalen om de problemen op te lossen. Niet veel later werd de pinpas gebruikt om geld te pinnen. De politie heeft camerabeelden vrijgegeven en zoekt naar getuigen om de verdachte te identificeren. Ontdek meer over deze vorm van fraude en hoe je deze kunt herkennen en voorkomen.

[Lees verder](#)



Ontdek en verbeter je cybersecurity kennis met quizen

CyberCrimelInfo biedt een unieke kans voor iedereen met interesse in cybersecurity om hun kennis te testen en te verbeteren via een reeks boeiende quizen. Het platform is erop gericht om zowel beginners als gevorderden te voorzien van diepgaande inzichten in digitale veiligheid, met een sterke nadruk op privacy. Door simpelweg je naam en e-mailadres in te vullen, ontvang je binnen 24 uur een unieke toegangscode. Wees gerust, deze persoonlijke informatie wordt strikt gebruikt om de deelname aan de quizen mogelijk te maken en wordt niet voor reclamedoeleinden ingezet.

Deze toegangscode opent de deur naar diverse quizen, waar je kunt ontdekken hoevel je weet en wat er nog te leren valt over cruciale cybersecurityonderwerpen. Na het indienen van je antwoorden krijg je vaak binnen 48 uur gedetailleerde feedback, wat een rijke leerervaring garandeert. Voor degenen die uitblinken, is er de 'Perfect Score Club'; een perfecte score levert niet alleen een plek op de topperslijst op maar geeft ook erkenning binnen de CyberCrimelInfo gemeenschap. Dit initiatief onderstreept het belang van voortdurende educatie en het bijblijven met de nieuwste ontwikkelingen in de strijd tegen digitale criminaliteit, alles in een veilige en reclamevrije omgeving.

Nieuwe Uitdaging Alert: Darkweb Quizen Zijn Hier!

We zijn verheugd om te delen dat onze nieuwste serie quizen over het Darkweb nu live is, verstrekt over drie uitdagende niveaus! Voor de cybersecurity-enthousiastelingen onder ons biedt dit een unieke kans om dieper in de mysterieuze wereld van het darkweb te duiken.

Maar dat is nog niet alles: behaal een perfecte score van 10/10 op elk niveau en verdien tot 6 extra punten richting jouw totaalscore. Deze punten zijn niet alleen een bewijs van je deskundigheid, maar brengen je ook dichterbij de top van onze prestigieuze Perfecte Score Club. Wie zal de nieuwe nummer 1 worden?

Dit is jouw kans om te schitteren en te bewijzen dat jij tot de elite van cybersecurity behoort. De strijd om de topospositie is geopend. Zijn jij en je collega's klaar voor deze uitdaging?

Neem deel aan de quizen, verken de diepten van het darkweb, en misschien is het jouw naam die straks bovenaan onze leiderstabel pronkt.

[Naar quizen](#)

De Perfecte Score Club!

Topscore		
Johan	10	16-maart-2024
Maxim	9	16-maart-2024
Phillip Savaete	9	17-maart-2024
Kenan	7	30-maart-2024

[Totaal overzicht](#)

AI Gids CyberWijzer

De **AI Gids CyberWijzer** is een geavanceerde AI Chatbot, aangeboden door Cybercrimeinfo. Deze chatbot gebruikt een aangepaste versie van ChatGPT-4 om betrouwbare en actuele informatie te verstrekken over cybercriminaliteit, het darkweb en cybersecurity. CyberWijzer is exclusief verbonden met de Cybercrimeinfo-database, waardoor het een veelzijdige bron is voor een breed scala aan doelgroepen. Deze omvatten beginners, gevorderden, cybersecurity experts, CISO's, ondernemers, burgers, kinderen, IT professionals, studenten, juridische professionals, beleidsmakers, ontwikkelaars, malware analisten, en ICS en OT beheerders. Het biedt informatie over onderwerpen zoals cyberveiligheid, financiële fraude, ransomware, netwerkbeveiliging, en meer.

CyberWijzer is ontworpen om intuïtief en veilig te zijn, met eenvoudige navigatie en heldere uitleg. Het waarborgt privacy en veiligheid door geavanceerde encryptie en naleving van privacyregulering.

[Download QR code](#)

AI Gids RechtRaadgever

De **AI Gids RechtRaadgever** is een chatbot ontwikkeld voor gebruik in het gebied van strafrecht en strafvordering. Het is ontworpen om efficiënte, snelle en nauwkeurige antwoorden te bieden in het steeds veranderende digitale landschap. Deze chatbot dient als een essentiële bron voor opsporingsambtenaren, hulpofficieren en iedereen die geïnteresseerd is in strafrecht. De expertisegebieden van RechtRaadgever omvatten:

- Strafrecht en Strafvordering:** Het biedt diepgaande informatie over een breed scala aan onderwerpen binnen deze gebieden.
- Proces-verbaal en Bewijsrecht:** De chatbot geeft duidelijke en accurate antwoorden met betrekking tot proces-verbaal en bewijsrecht.
- Wetteksten:** RechtRaadgever helpt gebruikers om eenvoudig door complexe juridische materie te navigeren.

RechtRaadgever is 24/7 beschikbaar en maakt gebruik van AI-technologie die continu leert en verbetert. Het biedt gebruikstips zoals het formuleren van duidelijke, specifieke vragen en het vertrouwen op exclusieve, betrouwbare bronnen. De chatbot garandeert een vertrouwelijke omgeving met privacybescherming, en moedigt gebruikers aan om te experimenteren met verschillende vragen om de capaciteiten van de chatbot te leren kennen.

De chatbot is gebruiksvriendelijk en veilig, met gemakkelijke navigatie, duidelijke antwoorden, geavanceerde encryptie en privacybescherming.

[Download QR code](#)

Waarom jouw donatie aan Cybercrimeinfo essentieel is

Beste lezer, In een wereld waar digitale dreigingen steeds geavanceerder en talrijker worden, speelt Cybercrimeinfo een cruciale rol in de strijd tegen cybercriminaliteit. Wij zijn een onafhankelijke organisatie, gedreven door vrijwilligers, die zich inzet voor het informeren en beschermen van het publiek tegen de gevaren van het digitale tijdperk. Jouw donatie maakt het verschil. Hier is waarom:

- Onafhankelijke en Belangrijke 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.
- Bijdragen aan Bewustwording en Preventie:** Door te doneren help je ons in de missie om kennis en bewustzijn over cybercriminaliteit te vergroten. Onze artikelen, nieuwsupdates en praktische tips dragen bij aan het voorkomen van digitale misdrijven.
- Ondersteuning van Onze Operationele Kosten:** Donaties worden direct gebruikt voor het hosten van de website en het vernieuwen van onze technologische middelen. Dit stelt ons in staat om op de voet te volgen hoe cybercriminelen opereren en jullie te informeren over de nieuwste digitale gevaren.

Elke bijdrage, hoe klein ook, is van onschatbare waarde in onze continue strijd tegen cybercriminaliteit. Met jouw steun kunnen we blijven werken aan een veiliger digitaal landschap voor iedereen. We waarderen je steun enorm en bedanken je alvast voor je bijdrage aan deze belangrijke zaak.

Doneren kan via de [WhyDonate pagina](#) of via onderstaande QR code.

Met vriendelijke groet,
Het team van Cybercrimeinfo

[Download QR code](#)

[Share](#) [Tweet](#) [Share](#) [Pinterest](#)

Deze e-mail is verzonden aan [\[email\]](#). • Als u geen e-mails meer wilt ontvangen, kunt u zich [hier afmelden](#). • Voor een goede ontvangst voegt u [info@cybercrimeinfo.nl](#) toe aan uw adresboek.

