Nieuwsbrief 333

Hacktivist group Twelve: The invisible front line of cyber warfare
Cybercrimeinfo | ccinfo.nl

Reading in ▯▯ or another language

Hacktivistengroep Twelve: De onzichtbare frontlinie van de cyberoorlog

Hacktivistengroep Twelve speelt een hoofdrol in de cyberoorlog tegen Rusland. Deze groep gebruikt verwoestende cyberaanvallen om Russische doelwitten te saboteren en het land te destabiliseren. In dit artikel ontdek je hoe Twelve opereert, welke methoden ze inzetten en welke impact ze hebben op de moderne cyberoorlog. Hacktivisme, een samensmelting van hacken en activisme, evolueert snel en wordt steeds geavanceerder. Twelve staat bekend om hun brute tactieken en het gebruik van wiper-malware, waarmee ze onherstelbare schade aanrichten. Benieuwd naar de volledige analyse van hun methoden en invloed?

Lees verder

The alarming rise in ransomware attacks: a 73% increase
Cybercrimeinfo | ccinfo.nl

Reading in ▯▯ or another language

De alarmerende stijging van ransomware-aanvallen: een toename van 73%

Ransomware-aanvallen zijn in 2023 met maar liefst 73% gestegen, waarbij groepen zoals CL0P en LockBit voor veel van deze aanvallen verantwoordelijk zijn. Deze explosieve toename benadrukt de groeiende dreiging van cybercriminaliteit voor bedrijven en overheden wereldwijd. In ons artikel bespreken we de trends, de doelwitten van deze aanvallen en hoe organisaties zich effectief kunnen beschermen tegen ransomware. Wil je meer weten over de recente ontwikkelingen en praktische tips om jouw bedrijf te beveiligen? Lees verder op onze website en ontdek hoe je jouw organisatie kunt beschermen tegen deze gevaarlijke aanvallen.

Lees verder

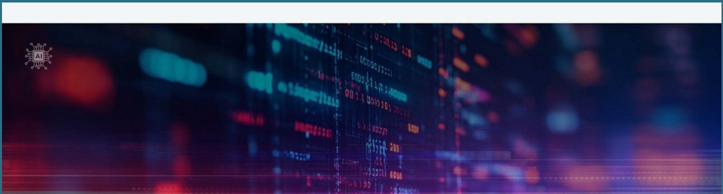
Data on the darkweb:
making the invisible visible
Cybercrimeinfo | ccinfo.nl

Reading in □□ or another language

Data op het darkweb: het onzichtbare zichtbaar maken

Wist je dat jouw persoonlijke gegevens zomaar op het darkweb kunnen belanden zonder dat je het weet? Of het nu gaat om een datalek bij een bedrijf of een hack van je eigen accounts, criminelen kunnen deze informatie verkopen aan de hoogste bieder. In ons nieuwste artikel duiken we in hoe deze gegevens op het darkweb terechtkomen, welke risico’s dit met zich meebrengt en, het allerbelangrijkst, hoe je jezelf kunt beschermen tegen deze dreiging. Ontdek hoe jij je online veiligheid kunt waarborgen en blijf een stap voor op cybercriminelen

Lees verder



Victim analysis and trends from Week 38-2024
Cybercrimeinfo | ccinfo.nl

Reading in □□ or another language

Slachtofferanalyse en Trends van Week 38-2024

In week 38 van 2024 zagen we een zorgwekkende toename van cyberaanvallen, waarbij bedrijven, onderwijsinstellingen en zelfs kritieke infrastructuren zoals luchthavens werden getroffen. Uit de analyse blijkt dat ransomware en datalekken de belangrijkste bedreigingen blijven. Zo werden gevoelige klantgegevens gestolen bij een Belgische modeketen, en eiste een aanval op een Amerikaanse school miljoenen aan losgeld. Deze trends benadrukken de noodzaak voor bedrijven en individuen om hun beveiligingsmaatregelen te versterken. Wilt u meer weten over de specifieke aanvallen en hoe u zichzelf kunt beschermen? Lees het volledige artikel op onze website.

Lees verder

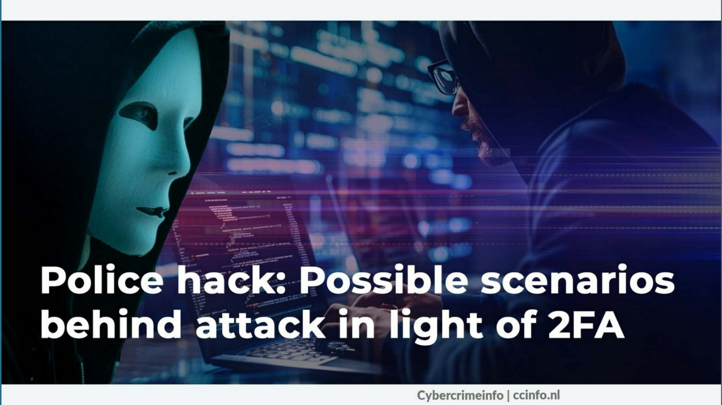
Police data breach:
what do you need to know and how do you protect yourself?
Cybercrimeinfo | ccinfo.nl

Reading in □□ or another language

Datalek bij de Politie: wat moet je weten en hoe bescherm je jezelf?

Recentelijk is er een datalek geweest bij de politie waarbij de namen en werkgerelateerde gegevens van medewerkers zijn gestolen. Hoewel er geen privégegevens zijn gelekt, blijven de risico's groot. Criminelen kunnen deze gegevens gebruiken voor phishing-aanvallen of zelfs impersonatiepogingen, waarbij ze zich voordoen als politieagenten om gevoelige informatie te bemachtigen. Wil je weten hoe je jezelf en je gegevens kunt beschermen tegen de gevolgen van dit lek? Lees ons uitgebreide artikel voor praktische tips en actiepunten om verdere schade te voorkomen.

Lees verder

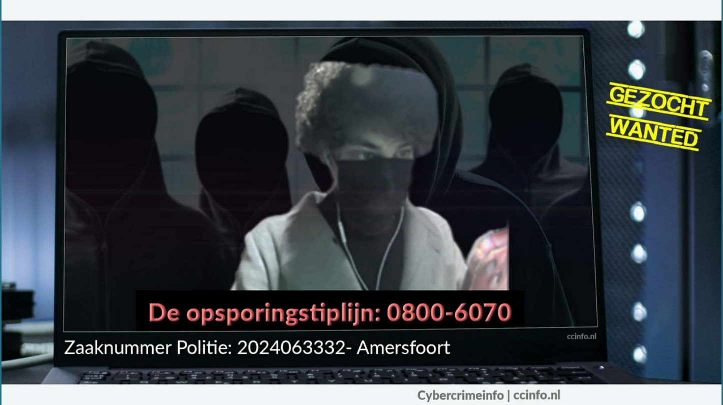

Police hack: Possible scenarios behind attack in light of 2FA
Cybercrimeinfo | ccinfo.nl

Reading in □□ or another language

Politiehack: Mogelijke scenario's achter de aanval in het licht van 2FA

Een recente hack bij de politie roept vragen op over hoe dit kon gebeuren ondanks het gebruik van tweefactorauthenticatie (2FA). In dit artikel onderzoeken we mogelijke scenario's die geleid kunnen hebben tot de aanval. Denk hierbij aan phishing gecombineerd met sessiekaping, misbruik van externe dienstverleners, of zelfs insider threats. Hoewel 2FA een sterke beveiliging biedt, weten geavanceerde cybercriminelen toch manieren te vinden om deze beveiligingslaag te omzeilen. Benieuwd naar de details en hoe je jezelf hiertegen kunt beschermen? Lees verder om meer te ontdekken over deze aanvalstechnieken en de oplossingen.

Lees verder

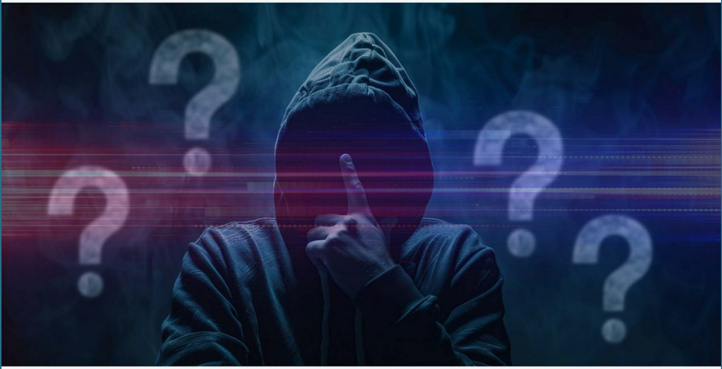

GEZOCHT
WANTED
De opsporingstiplijn: 0800-6070
Zaaknummer Politie: 2024063332- Amersfoort
ccinfo.nl
Cybercrimeinfo | ccinfo.nl

Reading in ▯▯ or another language

Amersfoort - Helpdesk fraude

De politie is op zoek naar een verdachte van een helpdeskfraudezaak in Amersfoort. Een 73-jarige man werd op 27 februari 2024 het slachtoffer toen de oplichter zich voordeed als een bankmedewerker. Het slachtoffer gaf zijn bankpas en pincode af, waarna grote geldbedragen werden opgenomen. Dezelfde dader wordt ook gelinkt aan vergelijkbare oplichtingen in Vught en Rotterdam. Herkent u de verdachte of heeft u informatie die kan helpen bij deze zaak? Meld het dan via de opsporingstiplijn of anoniem.

Lees verder



Cybercrimeinfo | ccinfo.nl

Reading in □□ or another language

Verbeter je cyberveiligheid: Test je kennis met onze interactieve quizzen

Verken de wereld van cybersecurity en het darkweb met onze interactieve quizzen op CyberCrimeInfo. Of je nu een beginner bent of een doorgewinterde expert, onze quizzen bieden een leuke en uitdagende manier om je kennis uit te breiden.

Wat kun je verwachten?

- **Leer in je eigen tempo:** Ontdek en test je vaardigheden wanneer het jou het beste uitkomt.
- **Ontvang feedback:** Krijg gedetailleerde feedback na elke quiz, zodat je precies weet waar je staat en waar je nog kunt verbeteren.
- **Verdien speciale erkenning:** Behaal een perfecte score en ontvang speciale erkenning voor je prestaties.

Ben je klaar om je kennis te testen en jezelf te meten met anderen? Begin vandaag nog aan je leerreis en vraag je toegangscode aan!

Naar quizzen

De Perfecte Score Club!

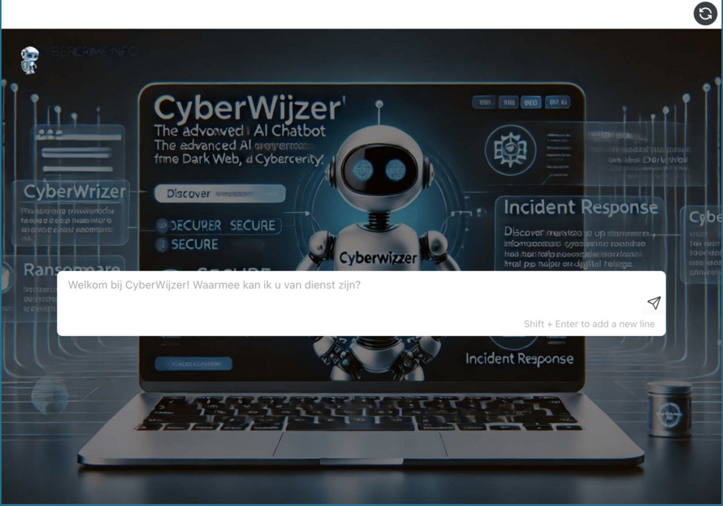
Topscorer	Punten	Wanneer
Joost W.	10	04-08-2024

Jasper	10	23-05-2024
Johan	10	16-03-2024
Philip S.	9	17-03-2024
Maxim	9	16-03-2024
Aart	7	21-06-2024
Thijs	7	09-04-2024
Kenan	7	30-03-2024

NIEUW TOEGEVOEGD

Maximaal te behalen **punten: 20**
Aantal deelnemers tot nu toe: 894

Totaal overzicht De Perfecte Score Club!



Welkom bij CyberWijzer! Waarmee kan ik u van dienst zijn?

Shift + Enter to add a new line

Reading in □□ or another language

AI Gids CyberWijzer

Wat is CyberWijzer?
CyberWijzer, aangeboden door Cybercrimeinfo, is een geavanceerde AI-chatbot die gebruikmaakt van een aangepaste versie van ChatGPT-S. Deze chatbot levert betrouwbare en actuele informatie over

cybercriminaliteit, het darkweb en cybersecurity. Dankzij de exclusieve koppeling met de Cybercrimeinfo-database fungeert CyberWijzer als een veelzijdige en onmisbare informatiebron.

Voor Wie is CyberWijzer?

CyberWijzer is ontworpen voor een breed scala aan gebruikers, waaronder:

- **Beginners en gevorderden:** Zowel nieuwkomers als ervaren gebruikers vinden hier waardevolle informatie.
- **Cybercrime-experts en CISO's:** Specialistische kennis en inzichten voor professionals.
- **Ondernemers en burgers:** Praktische tips om persoonlijke en zakelijke gegevens te beschermen.
- **Kinderen en IT-professionals:** Beveiligingsadvies op maat voor jong en oud.
- **Studenten en juridische professionals:** Ondersteuning bij studie en juridische vraagstukken.
- **Beleidsmakers en ontwikkelaars:** Informatie voor het creëren van veilige beleid en software.
- **Malware-analisten en ICS/OT-beheerders:** Diepgaande analyses en beveiligingsstrategieën.

Uitgebreide Onderwerpen

CyberWijzer biedt gedetailleerde informatie over een breed scala aan onderwerpen, zoals:

- Cyberveiligheid
- Financiële fraude
- Ransomware
- Netwerkbeveiliging
- En veel meer

Gebruiksvriendelijk en Veilig

CyberWijzer is ontwikkeld met de gebruiker in gedachten:

- **Intuïtieve interface:** Gemakkelijk te navigeren en te gebruiken.
- **Heldere uitleg:** Begrijpelijke en duidelijke informatie.
- **Privacy en veiligheid:** Geavanceerde encryptie en strikte naleving van privacyregelgeving zorgen voor uw bescherming.

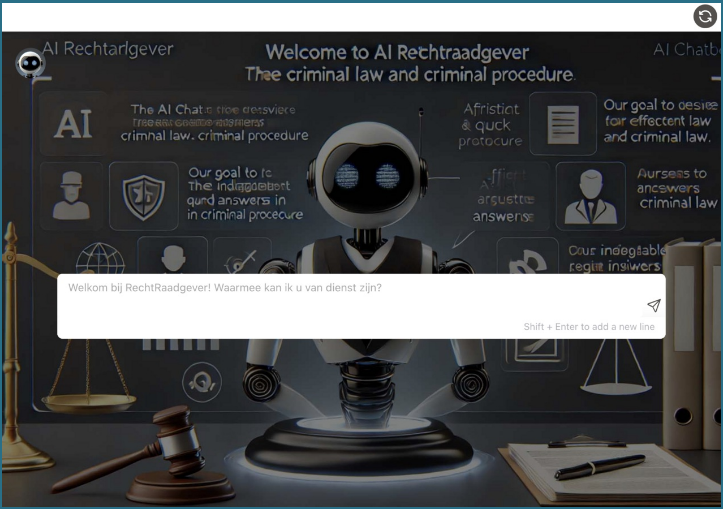
Waarom Kiezen voor CyberWijzer?

CyberWijzer is uw betrouwbare partner in het beschermen tegen cyberdreigingen en het bevorderen van cyberveiligheid. Met een schat aan informatie en een gebruiksvriendelijke benadering, staat CyberWijzer klaar om u te ondersteunen bij al uw vragen en uitdagingen op het gebied van cyberveiligheid.

Download QR code

Naar CyberWijzer

We hebben jouw hulp nodig om onze **AI gratis beschikbaar te houden**. Met een **donatie**, ongeacht het bedrag, kun je ons helpen onze missie voort te zetten. Elke bijdrage, groot of klein, maakt een groot verschil. Bedankt voor je steun!


AI Rechtarlgever
Welcome to AI Rechtraadgever
Thee criminal law and criminal procedure
AI Chatb
AI
crimnal law. criminal procedure
Our goal to desire for effectent law and criminal law.
Afristict & quck protocure
Our goal to tc The indigpoobert qurd answers in in criminal procecure
Aursens to ancswers criminal law

Welkom bij RechtRaadgever! Waarmee kan ik u van dienst zijn?

Shift + Enter to add a new line

Reading in □□ or another language

AI Gids RechtRaadgever

RechtRaadgever is een geavanceerde AI-chatbot, speciaal ontwikkeld om professionals en geïnteresseerden in strafrecht en strafvordering te ondersteunen. In het dynamische digitale tijdperk biedt deze chatbot snelle, nauwkeurige en efficiënte antwoorden.

Expertisegebieden

Strafrecht en Strafvordering: Ontvang diepgaande informatie over diverse onderwerpen binnen deze vakgebieden.
Proces-verbaal en Bewijsrecht: Krijg heldere en nauwkeurige antwoorden op vragen over proces-verbaal en bewijsrecht.
Wetteksten: Met RechtRaadgever wordt het navigeren door complexe juridische materie eenvoudig.

Voordelen en Functionaliteiten

- **Altijd Beschikbaar:** RechtRaadgever is 24/7 bereikbaar, zodat u op elk moment kunt rekenen op deskundig advies.
- **Continu Leren en Verbeteren:** De AI-technologie blijft zichzelf ontwikkelen, waardoor u altijd de meest actuele en nauwkeurige informatie ontvangt.
- **Gebruiksvriendelijk:** Dankzij de intuïtieve interface en eenvoudige navigatie vindt u snel wat u zoekt.
- **Veiligheid en Privacy:** Geavanceerde encryptie en strikte privacybescherming zorgen voor een veilige en vertrouwelijke omgeving.

Tips voor Optimaal Gebruik

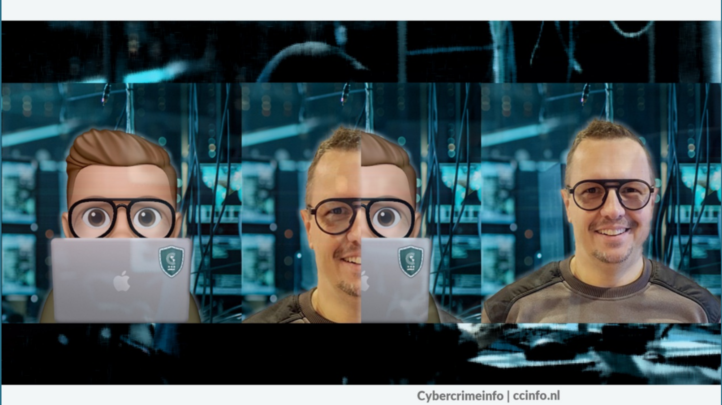
Formuleer duidelijke en specifieke vragen voor de beste resultaten. Vertrouw op betrouwbare bronnen en experimenteer met verschillende vraagstellingen om de volledige potentie van RechtRaadgever te benutten.

RechtRaadgever

Download QR code

Naar RechtRaadgever

We hebben jouw hulp nodig om onze **AI gratis beschikbaar te houden**. Met een **donatie**, ongeacht het bedrag, kun je ons helpen onze missie voort te zetten. Elke bijdrage, groot of klein, maakt een groot verschil. Bedankt voor je steun!



Cybercrimeinfo | ccinfo.nl

Reading in ▯▯ or another language

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:

1. **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.
2. **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.

3. **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 **doneer pagina** (Kies nu zelf het bedrag dat je wilt doneren!) of via onderstaande QR code.

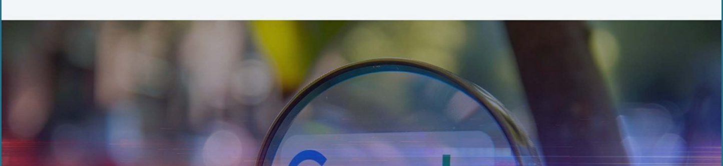
Met vriendelijke groet,
Het team van Cybercrimeinfo

Doneer | Cybercrimeinfo.nl (ccinfo.nl)

Doneer pagina

Geen budget? Geen probleem!

Help ons de zichtbaarheid van Cybercrimeinfo te vergroten met jouw Google review!



Google
Cybercrimeinfo | ccinfo.nl

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

Share Tweet Share Pinterest

Deze e-mail is verstuurd 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.

Laposta