Nieuwsbrief 349

Reading in another language

Hoe onwetendheid in het Westen de oorlog met Rusland voedt via cyberfraude

In een wereld waarin technologie ons steeds verder verbindt, blijkt onze onwetendheid een krachtig wapen te zijn voor kwaadwillenden. Dit artikel onthult de zorgwekkende manier waarop cyberfraude in het Westen niet alleen individuen financieel verwoest, maar ook geopolitieke conflicten zoals de oorlog tegen Rusland voedt. Cybercriminelen, vaak gelinkt aan staatsgerelateerde groepen, benutten technieken zoals investerings- en cryptofraude om illegale inkomsten te genereren. Deze inkomsten zouden wel eens kunnen worden ingezet voor staatsactiviteiten die ons allemaal treffen. Dit artikel biedt niet alleen inzicht in de complexe mechanismen achter deze frauduleuze praktijken, maar reikt ook middelen aan om jezelf te beschermen. Ontdek hoe iets ogenschijnlijk lokaals een cruciaal tandwiel in een wereldwijde machine van bedreiging en macht kan vormen. Lees verder om te begrijpen hoe onwetendheid een gevaarlijk spel speelt en hoe je jezelf kunt wapenen tegen deze sluipende vijand.

Lees verder

Reading in another language

De opkomst van nieuwe cyberdreigingen: misbruik van reCAPTCHA en verborgen malware

In de dynamische wereld van cyberbeveiliging onthullen we een verontrustende verschuiving in de methoden van cyberaanvallen. Het artikel "De opkomst van nieuwe cyberdreigingen: misbruik van reCAPTCHA en verborgen malware" beschrijft hoe cybercriminelen een bekende beveiligingstechniek, reCAPTCHA, omvormen tot een valstrik. Door slim gebruik te maken van social engineering en malware die zich verstopt achter ogenschijnlijk onschuldige elementen, weten deze aanvallen gebruikers te misleiden op een manier die moeilijk te detecteren is. Ontdek hoe deze innovatieve strategieën werken en leer effectieve methoden om uzelf te beschermen tegen deze doortrapte dreigingen.

Lees verder

Reading in another language

Mysteryland ontmaskerd: de verborgen wereld van een darkweb-dealer

In een wereld waar anonimiteit als een schild wordt gezien, heeft 'Mysteryland', een toonaangevende darkweb-drugshandelaar, dit idee radicaal op de proef gesteld. Het artikel "Mysteryland ontmaskerd: de verborgen wereld van een darkweb-dealer" werpt een onthullend licht op de complexe netwerken en geavanceerde technieken achter de grootste darkweb-operaties. Door internationale samenwerking en cutting-edge opsporingstechnieken hebben autoriteiten erin geslaagd dit illusoire netwerk bloot te leggen en een grote slag toe te brengen aan de digitale onderwereld. Wat begon als een ongrijpbaar spel van vraag en aanbod, transformeerde in een meeslepend verhaal van verraad en gerechtigheid. Ontdek hoe deze moderne Sherlock Holmes-zaak zich ontplooide en welke lessen dit trekt voor de toekomst van cybercriminaliteit. Bent u klaar om de schijnwerper te richten op een wereld die meestal in het donker blijft? Lees verder en ontdek de geheimen van 'Mysteryland'.

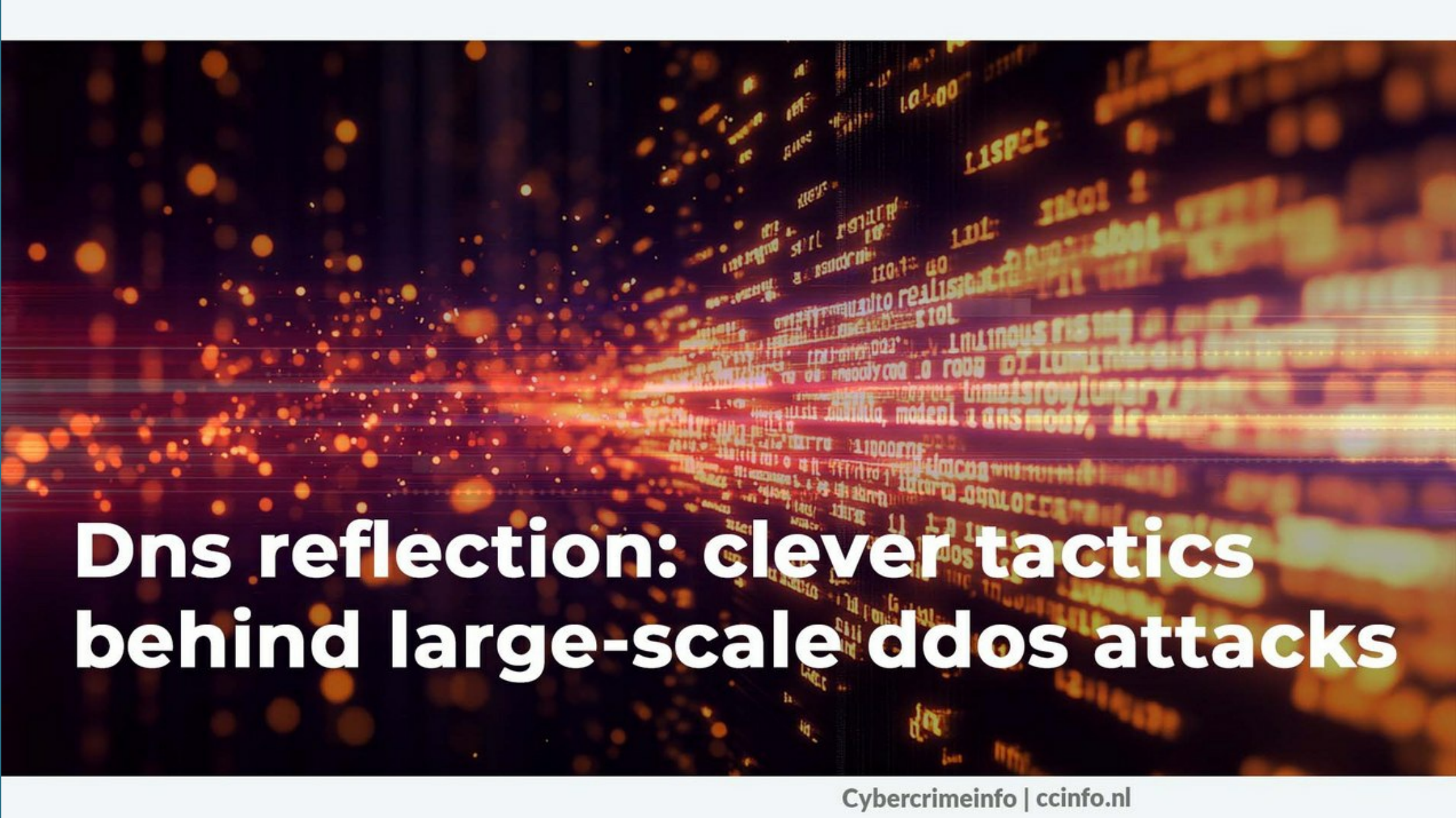
Lees verder

Reading in another language

Slachtofferanalyse en Trends van Week 02-2025

De tweede week van 2025 heeft de kwetsbaarheid van digitale systemen opnieuw pijnlijk blootgelegd. In heel Nederland en België zijn diverse bedrijven getroffen door een reeks geavanceerde cyberaanvallen, met name ransomware en datalekken, die hun gegevens en bedrijfsprocessen zwaar hebben beschadigd. In dit artikel maken we een diepgaande analyse van de recente ontwikkelingen in de wereld van cybercrime, waarbij we specifieke aandacht besteden aan de meest getroffen bedrijven en de opkomende trends binnen deze sinistere sector. Ontdek welke tactieken cybercriminelen gebruiken en hoe bedrijven wereldwijd zich wapenen tegen deze steeds groeiende dreiging. De complexiteit en omvang van de huidige dreigingen zijn groter dan ooit; een reden te meer om verder te lezen en uzelf te informeren over de nieuwste ontwikkelingen in cyberveiligheid.

Lees verder



Reading in another language

Dns-reflectie: slimme tactiek achter grootschalige ddos-aanvallen

In de wereld van cyberaanvallen behoort de Distributed Denial-of-Service (DDoS)-aanval tot de meest gevreesde en destructieve vormen van cybercriminaliteit. Binnen deze categorie is de DNS-reflectieaanval een geavanceerde tactiek die kwaadwillenden in staat stelt om met relatief gemak systemen te verlammen zonder zelf direct naar voren te treden. In dit artikel duiken we dieper in de slimme mechanismses achter DNS-reflectieaanvallen, die verder gaan dan traditionele methoden zoals eenvoudige flood-aanvallen. We onderzoeken hoe deze geavanceerde techniek onderwijs- en zorgsectoren raakt, organisaties die steeds vaker doelwit zijn door de openheid van hun digitale ecosystemen. Benieuwd hoe deze onzichtbare vijand werkt en welke gevolgen het heeft voor de kwetsbare digitale infrastructuren? Lees verder en ontdek de strategieën en dreigingen die uw cyberveiligheid op de proef stellen.

Lees verder

Reading in another language

Spaarndam - Helpdesk fraude

Op 25 april 2024 viel een 72-jarige inwoner van Spaarndam ten prooi aan bankhelpdeskfraude, een steeds vaker voorkomende vorm van oplichting in Nederland. De dader, die zich voordeed als bankmedewerker, slaagde erin persoonlijke gegevens te bemachtigen en geld op te nemen bij een geldautomaat in de Molenwijk, Amsterdam. De verdachte is vastgelegd op camerabeelden, en de politie roept de hulp van het publiek in om deze persoon te identificeren. Bent u in staat om deze verdachte te herkennen of heeft u andere bruikbare informatie? Deel uw tips anoniem via Meld Misdaad Anoniem. Lees verder om te ontdekken hoe u zich kunt beschermen tegen dit soort misdrijven.

Lees verder

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