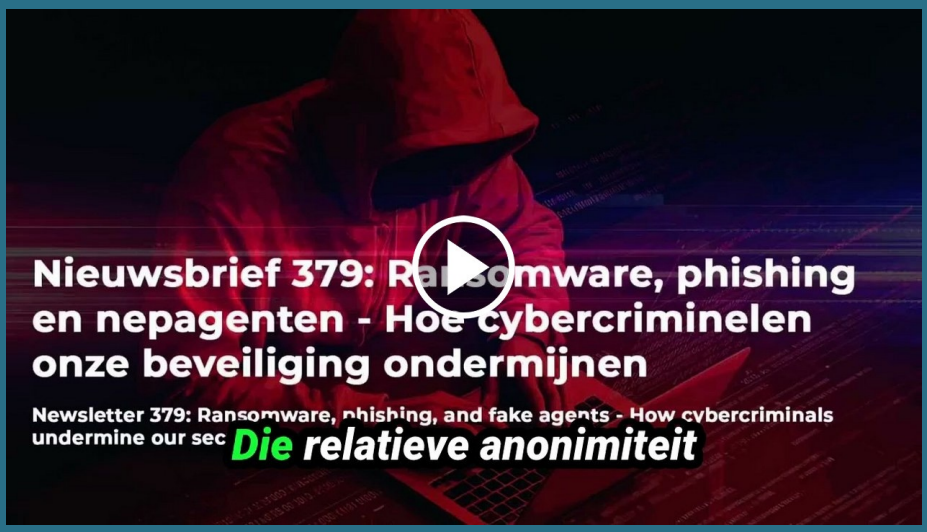
Cybercrimeinfo (ccinfo.nl)

Het onzichtbare zichtbaar maken

Nieuwsbrief 379 en Cyberjournaal



Podcast

Podcast

Reading in another language

Dagelijks Cyber Journaal van Cybercrimeinfo: Altijd op de hoogte van de laatste cyberdreigingen in België en Nederland

In de dynamische wereld van cyberdreigingen is het essentieel om altijd up-to-date te blijven. Elke dag brengen nieuwe aanvallen, kwetsbaarheden en geopolitieke ontwikkelingen nieuwe risico's voor bedrijven, overheden en individuen in België en Nederland. Het Dagelijks Cyber Journaal van Cybercrimeinfo biedt jou de kans om snel de belangrijkste gebeurtenissen van de afgelopen dag te volgen, met een focus op de regio. Dit journaal verschijnt **dagelijks tussen 12:00 en 14:00**

uur, behalve op zondag. Of je nu een professional bent die zijn beveiliging wil versterken of gewoon geïnteresseerd bent in de laatste trends, met dit journaal ben je altijd goed geïnformeerd. Ontdek het nu en blijf voorbereid op alles wat de digitale wereld te bieden heeft.

Lees verder

Reading in another language

Cyberaanvallen juli 2025: Van ransomware tot overheidshacks, wat betekent het voor België en Nederland?

In juli 2025 werden wereldwijd verschillende ernstige kwetsbaarheden ontdekt, waaronder zero-daylekken in Microsoft SharePoint en Citrix NetScaler, die actief werden misbruikt. Deze kwetsbaarheden vormden een ernstige dreiging voor organisaties, waaronder overheidsinstellingen. Ook werden kritieke lekken aangetroffen in netwerkapparatuur, zoals Cisco's Identity Services Engine en SonicWall's SMA 100-serie, die aanvallers de mogelijkheid gaven volledige controle over systemen te krijgen. Daarnaast bleken alledaagse apparaten zoals wifi-thermostaten en beveiligingscamera's kwetsbaar voor aanvallen, wat wijst op de toenemende inzet van hackers op IoT-apparaten. Cybercriminelen richtten zich ook op webapplicaties en cloudtoepassingen, zoals de populaire WordPress-plugin Post SMTP. De incidenten benadrukken het belang van een robuuste patchstrategie en voortdurende monitoring om systemen te beschermen tegen de snel evoluerende digitale dreigingen.

Lees verder

Reading in another language

Juli 2025: De strijd tegen cybercriminaliteit - Aanhoudingen, ransomware en de nieuwe technologieën die cybercriminelen gebruiken

In juli 2025 werden belangrijke stappen gezet in de strijd tegen cybercriminaliteit in Nederland en België. De politie voerde verschillende operaties uit, waaronder de arrestatie van cybercriminelen die betrokken waren bij phishing en ransomware-aanvallen. In Spanje werden twee hackers gearresteerd voor gegevensdiefstal, terwijl in Italië een Chinese hacker werd opgepakt voor cyberespionage. In Nederland leidde de opkomst van phishing via QR-codes tot de aanhouding van vijf jongeren in Hellevoetsluis. Daarnaast werd een groep oplichters die zich voordeden als nepagenten in de regio Den Haag gearresteerd. Op internationaal niveau werden aanzienlijke maatregelen genomen, waaronder de inbeslagname van ransomware-websites van de BlackSuit-groep door Amerikaanse autoriteiten. Nieuwe technologieën, zoals het gebruik van cryptocurrencies, blijven zorgen voor extra uitdagingen in de bestrijding van cybercriminaliteit. In juli werd ook een groeiende zorg geuit over de rol van cryptocurrencies in criminele netwerken, wat het voor opsporingsdiensten steeds moeilijker maakt om verdachte financiële transacties te traceren.

Lees verder

Reading in another language

13 augustus 2025 | Journaal

Op 12 augustus 2025 werden in Nederland en België verschillende ernstige cyberdreigingen gerapporteerd, waaronder ransomware-aanvallen, datadiefstallen en kwetsbaarheden in kritieke systemen. Een belangrijke aanval was gericht op het Nederlandse bedrijf Agrofair, waar de Qilin ransomwaregroep aanzienlijke schade veroorzaakte. In België werd bankfraude gerapporteerd, waarbij oplichters kloosters misleidden via telefonische gesprekken om geld van bankrekeningen te stelen.

Daarnaast werd het datalek bij Clinical Diagnostics gemeld, waarbij gevoelige gegevens van 485.000 vrouwen werden gestolen. Verder bleken de Citrix- en VMware-systemen kwetsbaar, wat miljoenen systemen wereldwijd bedreigde. De geopolitieke situatie, met name de censuur in Rusland, beïnvloedt ook de cyberveiligheid, terwijl de dreiging van ransomware en malwarecampagnes blijft groeien. Deze incidenten benadrukken de voortdurende risico's voor bedrijven en overheden, wat de noodzaak van investering in cybersecurity onderstreept.

Lees verder

Reading in another language

14 augustus 2025 | Journaal

Op 13 augustus 2025 werden verschillende incidenten in cyberspace gemeld, waaronder een grote cyberaanval op Clinical Diagnostics LCPL, waarbij medische gegevens van gedetineerden en vrouwen op het darkweb werden gelekt. De Nova ransomwaregroep was verantwoordelijk voor het datalek, waarbij een deel van de gestolen gegevens al openbaar was, ondanks betaling van losgeld. Daarnaast werden ernstige kwetsbaarheden ontdekt in systemen zoals XZ-Utils en Fortinet-producten, die een bedreiging vormen voor bedrijven in België en Nederland. Verder werd er een toename van ransomware- en brute-force-aanvallen opgemerkt, evenals geopolitieke spanningen die hun weerslag hadden in cyberspionage, zoals een hack bij het Openbaar Ministerie in Nederland. Deze incidenten benadrukken de toenemende complexiteit van cyberdreigingen en de noodzaak voor snel handelen om systemen te beveiligen.

Lees verder

Reading in another language

15 augustus 2025 | Journaal

Op 14 augustus 2025 werden er diverse belangrijke cyberincidenten geregistreerd. Er werd een kwetsbaarheid in remote access software N-Central geïdentificeerd, die bedrijven in Nederland en België bedreigde. Een phishingaanval op Booking.com maakte gebruik van visuele verwarring via Japanse tekens om slachtoffers naar malafide websites te leiden. Verder werd een aanval op FIDO-authenticatie vastgesteld, die bedrijven in Nederland en België blootstelt aan phishing en sessiehijacking. Ook een nieuwe Android malware genaamd PhantomCard vormt een groeiende dreiging voor mobiele betalingen. Tot slot werden er meer dan 300 miljoen dollar aan cryptocurrency in beslag genomen door internationale wetshandhavers in de strijd tegen cybercriminaliteit. Deze incidenten benadrukken de noodzaak voor bedrijven en consumenten om alert te blijven op de laatste dreigingen.

Lees verder

Reading in another language

16 augustus 2025 | Journaal

Colt Telecom werd getroffen door een ransomware-aanval, waarbij meer dan een miljoen documenten werden gestolen, waaronder klantgegevens. De aanval werd uitgevoerd door de WarLock ransomwaregroep, wat de beveiliging van telecomdiensten ernstig bedreigt. Ook werden kwetsbaarheden ontdekt in Cisco's Secure Firewall Management Center en in veelgebruikte VPN-apps, die duizenden gebruikers wereldwijd in gevaar brengen. Ten slotte werden er geavanceerde ransomware-aanvallen gemeld, gericht op grote Europese organisaties, evenals phishingcampagnes die werkzoekenden in Nederland en België targetten. Deze gebeurtenissen benadrukken de groeiende dreigingen in cyberspace en de noodzaak voor verbeterde digitale veiligheid.

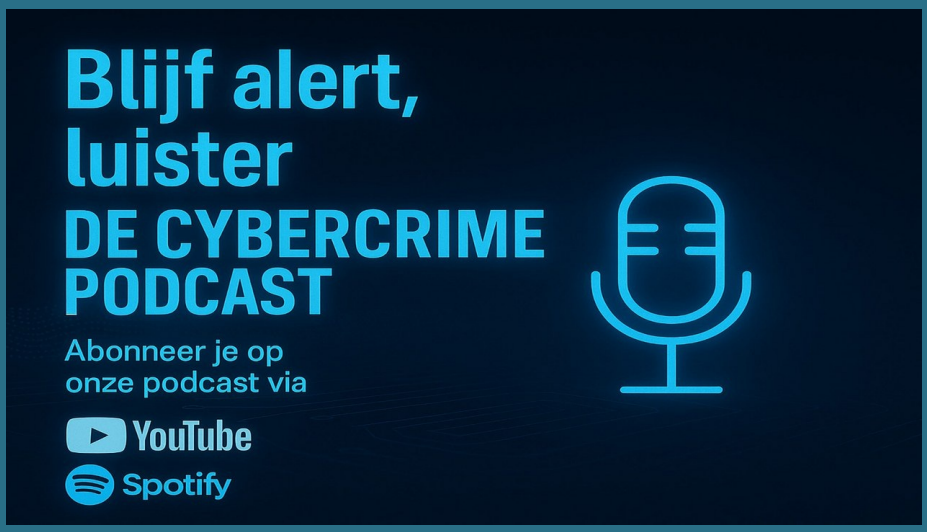
Lees verder

Reading in another language

Zandvoort - Nepagent

Op 26 juni 2025 werd een 76-jarig slachtoffer uit Zandvoort opgelicht door een man die zich voordeed als politieagent. De verdachte beweerde dat hij € 20.000 moest "veiligstellen" en verdween met het geld. Het slachtoffer zag het geld nooit meer terug. De verdachte wordt omschreven als een man van 20-30 jaar, met zwart krullend haar en een baard. Hij droeg een beige poloshirt, een broek en zwarte schoenen met een witte zool. De politie heeft beelden van de verdachte vrijgegeven en roept getuigen op zich te melden via het opsporingsnummer of online. Nepagenten maken gebruik van de geloofwaardigheid van autoriteiten om slachtoffers te misleiden, zowel telefonisch, fysiek als online. Het is belangrijk om altijd legitimatie te vragen en bij twijfel de politie te bellen.

Lees verder



De Cybercrime Podcast van Cybercrimeinfo

Wil je altijd op de hoogte blijven van het laatste cybernieuws? Abonneer je dan op **De Cybercrime Podcast**. Je ontvangt dagelijks een korte update met betrouwbare informatie over actuele dreigingen, trends en praktische adviezen. De inhoud is zorgvuldig samengesteld door Cybercrimeinfo en eenvoudig te volgen via AI-gegenereerde Nederlandse stemmen. Luister waar en wanneer je wilt via **YouTube** of **Spotify** en versterk je digitale weerbaarheid. Abonneren is gratis en zo geregeld.

AI Chatbots Cybercrimeinfo

AI Chatbots | Ontdek **CyberWijzer**, **RechtRaadgever** en **NIS2Wijzer**, 24/7 beschikbaar voor hulp bij cybercriminaliteit, strafrecht en NIS2-wetgeving. Als je hulp nodig hebt bij het installeren of gebruiken van MindYourPass, gebruik dan AI Gids **VeiligSlot**. De AI **HRMWijzer** bevindt zich momenteel in de testfase van ontwikkeling en biedt richtlijnen en informatie over

verschillende aspecten van HRM binnen de politie.

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.

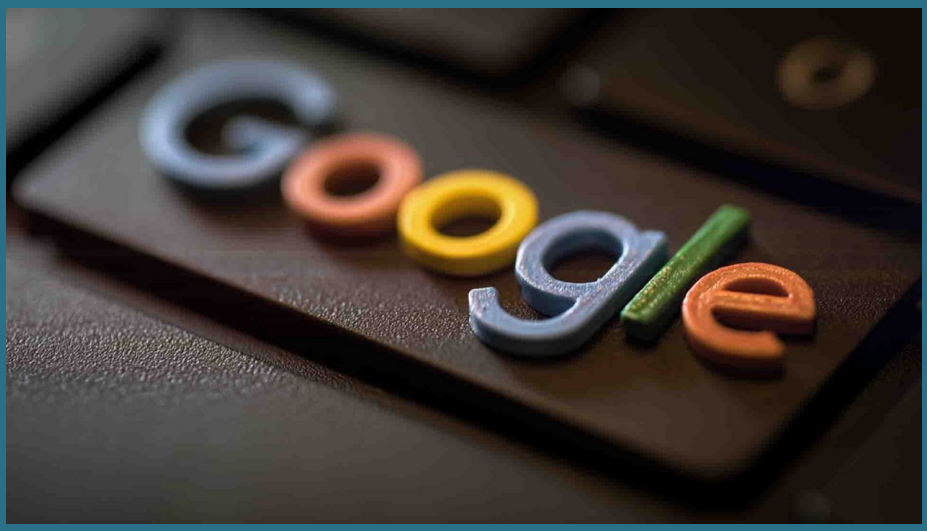
Met vriendelijke groet,
Het team van Cybercrimeinfo

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