



Nieuwsbrief 352

Victim Analysis and Trends in Belgium and the Netherlands January 2025

Cybercrimeinfo | ccinfo.nl

[Reading in another language](#)

Slachtofferanalyse en trends België en Nederland januari 2025

Het nieuwe jaar begon schijnbaar rustig, maar al snel volgde een storm van cyberaanvallen, datalekken en ransomware-incidenten in Nederland en België. Bedrijven, overheidsinstanties en zelfs onderwijsinstellingen werden hard geraakt door cybercriminelen die data stalen en te koop aanboden op het darkweb. Van lokale gemeenten tot grote IT-bedrijven: niemand bleek immuun. Wat zeggen deze ontwikkelingen over de digitale dreigingen van vandaag? En welke lessen kunnen we trekken voor de toekomst? In dit artikel analyseren we de belangrijkste trends, getroffen organisaties en de gevolgen voor digitale veiligheid.

[Lees verder](#)

Cryptovaluta: betaalmiddel voor Poetin om westerse sancties te omzeilen

Cybercrimeinfo | ccinfo.nl

[Reading in another language](#)

Cryptovaluta: betaalmiddel voor Poetin om westerse sancties te omzeilen

Terwijl de wereld toekijkt hoe Rusland onder zware sancties gebukt gaat, lijkt Poetin een alternatieve strategie te hanteren: cryptovaluta. Met digitale munten zoals bitcoin omzeilt het Kremlin financiële blokkades en houdt het de economie draaiende. Maar hoe effectief is deze aanpak? En welke rol spelen Russische hackers, mining-operaties en verborgen handelsroutes hierin? In dit artikel duiken we dieper in de opkomst van crypto als geopolitiek wapen en de verborgen geldstromen die sancties ondermijnen. Lees verder en ontdek hoe digitaal geld een sleutelrol speelt in deze mondiale machtsstrijd.

[Lees verder](#)

Cyberoorlog nieuws Januari 2025

Cybercrimeinfo | ccinfo.nl

[Reading in another language](#)

Cyberoorlog nieuws 2025 januari

De eerste maand van 2025 liet opnieuw zien hoe intens en veelzijdig cyberdreigingen zijn geworden. Van gerichte ransomware-aanvallen op vitale infrastructuur tot geopolitieke spionage en grootschalige desinformatiecampagnes – overheden, bedrijven en burgers wereldwijd werden geconfronteerd met digitale dreiging op ongekende schaal. Russische en Chinese hackersgroepen voerden gerichte operaties uit, terwijl nieuwe samenwerkingen, zoals die tussen de TU Eindhoven en Defensie, een tegenoffensief proberen te vormen. In dit artikel duiken we dieper in de cyberaanvallen die januari 2025 bepaalden. Wat zijn de nieuwste tactieken van cybercriminelen en statelijke actoren? Welke impact hebben deze aanvallen op de internationale veiligheid? En hoe bereiden landen zich voor op een steeds digitaal slagveld? Ontdek de laatste ontwikkelingen en de strijd om digitale weerbaarheid.

[Lees verder](#)

Analyse van kwetsbaarheden op het gebied van cyberbeveiliging januari 2025

Cybercrimeinfo | ccinfo.nl

[Reading in another language](#)

Analyse van kwetsbaarheden op het gebied van cyberbeveiliging januari 2025

De eerste maand van 2025 heeft opnieuw laten zien hoe kwetsbaar onze digitale wereld is. Van ernstige beveiligingslekken in routers en IoT-apparaten tot kritieke zwakheden in Microsoft- en cloudsystemen: cybercriminelen zaten niet stil. In dit overzicht analyseren we de belangrijkste kwetsbaarheden van januari, inclusief de impact van Microsoft Patch Tuesday en zero-day exploits die actief werden misbruikt. Welke risico's lopen bedrijven en particulieren, en welke maatregelen zijn essentieel om veilig te blijven? Lees verder en ontdek hoe jij je digitale omgeving optimaal kunt beschermen.

[Lees verder](#)

Het verscholen gevaar: Hoe MKB bedrijven doelwit worden op het darkweb

Cybercrimeinfo | ccinfo.nl

[Reading in another language](#)

Het verscholen gevaar: Hoe MKB bedrijven doelwit worden op het darkweb

Cybercriminelen verleggen hun focus steeds vaker naar het mkb, en het darkweb speelt hierin een cruciale rol. Gevoelige bedrijfsdata, gestolen inloggegevens en zelfs complete ransomware-aanvallen worden op deze verborgen marktplaats verhandeld. Veel ondernemers denken dat ze te klein zijn om interessant te zijn voor hackers, maar niets is minder waar. Het gebrek aan geavanceerde beveiliging maakt kleinere bedrijven juist een gewild doelwit. In dit artikel ontdek je hoe cybercriminelen via het darkweb te werk gaan en welke stappen je kunt nemen om jouw bedrijf te beschermen tegen deze groeiende dreiging.

[Lees verder](#)


De opsporingstlijn: 0800-6070

Zaaknummer Politie: 2024040667 - Vinkeveen

[Reading in another language](#)

Vinkeveen - Helpdesk fraude

Een 83-jarige man uit Vinkeveen is slachtoffer geworden van een sluwe vorm van helpdeskfraude. Oplichters deden zich voor als medewerkers van ING en een nep-rechercheur, waardoor de man duizenden euro's en waardevolle bezittingen kwijtraakte. De politie heeft camerabeelden van een vrouwelijke verdachte en roept het publiek op om mee te helpen bij de identificatie. Weet jij wie zij is? Bekijk de beelden en deel je tips!

[Lees verder](#)

Waarom jouw donatie aan Cybercrimeinfo essentieel is

Beste lezer, In een wereld waarin digitale dreigingen steeds geavanceerder en spraakwer 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

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.

Laposta