Cybercrimeinfo

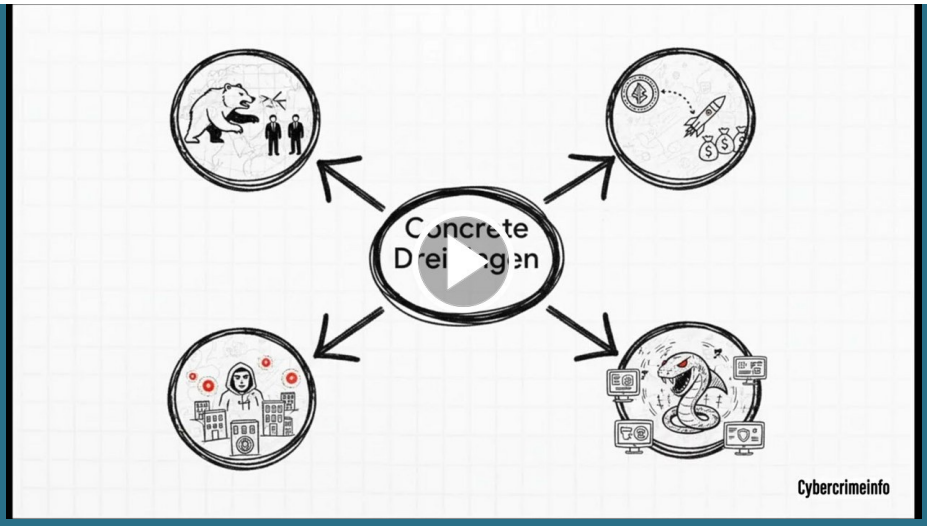
"Omdat wat waardevol is, beschermd moet worden"

NB389

Luister naar de discussiepodcast over het nieuws van de afgelopen week.

Luister de podcast nu op Youtube

Luister de podcast nu op Spotify



Vraag van de week: Cybersecuritybeleid en cyberweerbaarheid in de verkiezingsprogramma's van 2025

De Tweede Kamerverkiezingen van 2025 besteden ook aandacht aan digitale veiligheid en cyberweerbaarheid. Politieke partijen benadrukken het belang van het versterken van de digitale infrastructuur en het beschermen tegen cyberdreigingen. Partijen zoals de VVD pleiten voor meer Europese samenwerking, terwijl GroenLinks en PVDA digitale autonomie binnen Europa voorstellen. De ChristenUnie richt zich op de bescherming van kwetsbare groepen, en Volt pleit voor ethiek in technologie. D66 wil privacy beschermen en technologische innovatie bevorderen, terwijl het CDA digitale soevereiniteit benadrukt. De SP en JA21 willen meer verantwoordelijkheid van de overheid op digitaal gebied. De PVV legt de focus op nationale veiligheid.

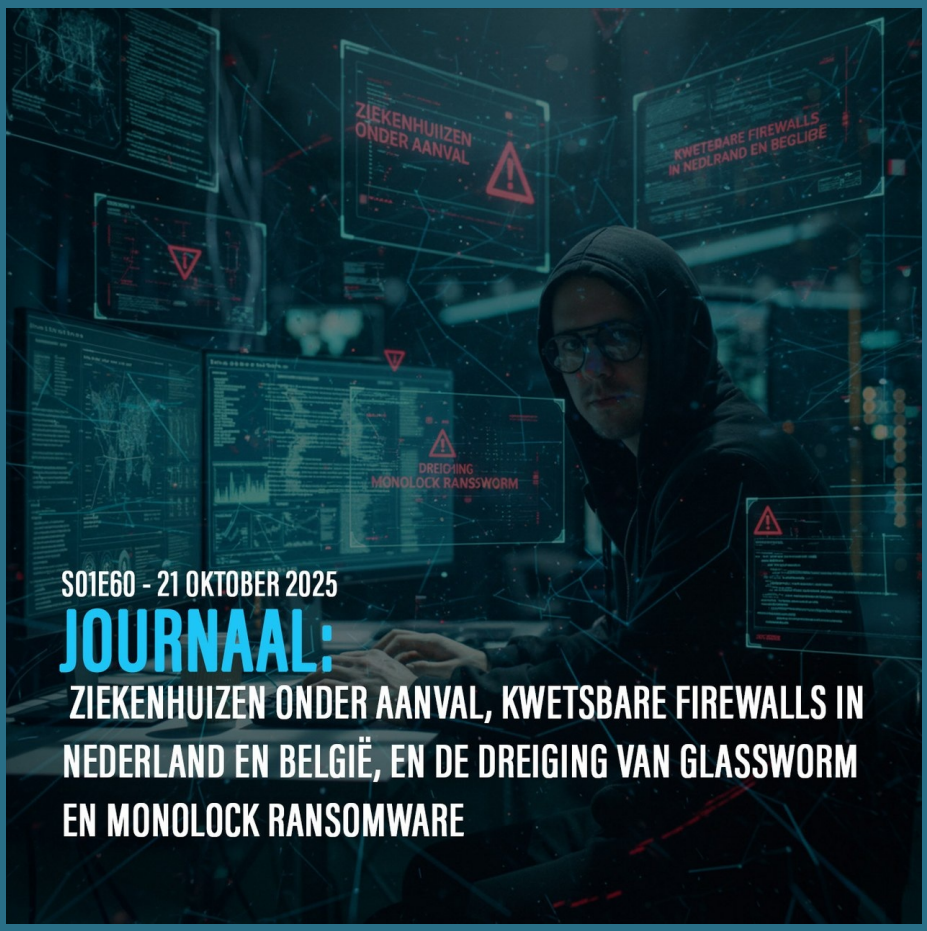
LEES VERDER

Noord-Korea en Rusland richten cyberaanvallen op

Europa en verspreiden nieuwe malware via kwetsbaarheden in software

Noord-Korea en Rusland zijn verantwoordelijk voor cyberaanvallen op Europese bedrijven, waarbij ze nieuwe malware verspreiden via kwetsbaarheden in software zoals ASP.NET en Redis. De aanvallen richten zich op vitale sectoren zoals defensie en energie, en worden uitgevoerd via phishing en ransomware. Daarnaast zijn er kwetsbaarheden ontdekt in software zoals ConnectWise Automate en de Windows Disk Cleanup Tool, die aanvallers in staat stellen om gegevens te stelen of systemen te manipuleren. Organisaties wordt geadviseerd om updates snel te installeren om schade te voorkomen.

LEES VERDER



Ziekenhuizen onder aanval, kwetsbare firewalls in Nederland en België, en de dreiging van GlassWorm en Monolock ransomware

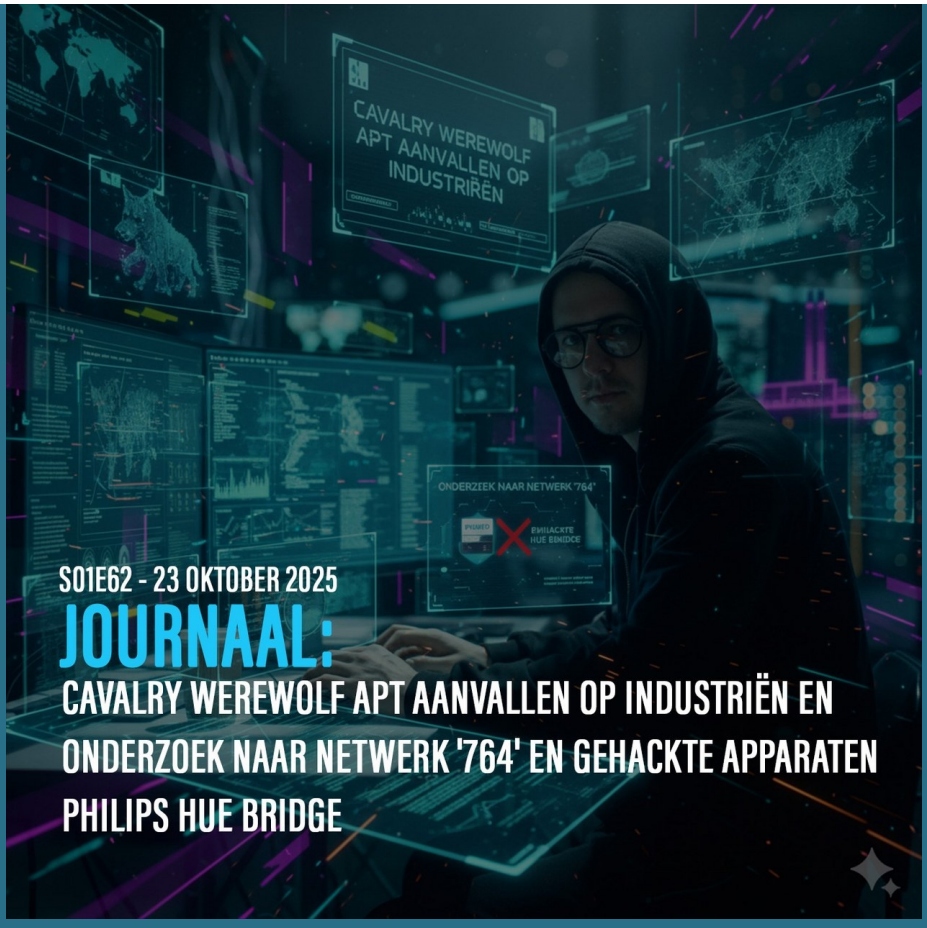
Ziekenhuizen in Europa, zoals het Centre hospitalier intercommunal de Haute-Comté in Frankrijk, worden getroffen door cyberaanvallen die medische systemen platleggen en losgeld eisen voor de decryptie van gegevens. In Nederland en België zijn kwetsbare firewalls ontdekt die door cybercriminelen misbruikt kunnen worden, wat grote risico's voor systemen met zich meebrengt. Ook zijn er nieuwe dreigingen, zoals GlassWorm malware die zich via ontwikkelaarsplatformen verspreidt, en Monolock ransomware die systemen vergrendelt en losgeld eist. Bedrijven en gebruikers moeten hun systemen up-to-date houden om aanvallen te voorkomen.

LEES VERDER

Waarschuwing van Autoriteit Persoonsgegevens over AI chatbots en de verkoop van gedecentraliseerde botnet malware op het darkweb

De Autoriteit Persoonsgegevens (AP) heeft een waarschuwing uitgebracht over het gebruik van AI-chatbots voor het geven van stemadvies. De chatbots kunnen vertekende informatie verstrekken, wat de verkiezingsresultaten zou kunnen beïnvloeden. Daarnaast is er zorg over de verkoop van gedecentraliseerde botnet malware op het darkweb, die gebruikt kan worden voor DDoS-aanvallen en andere cyberaanvallen. De AP benadrukt de noodzaak van strengere regels voor AI in de politiek en waarschuwt bedrijven en overheden om zich beter te wapenen tegen deze opkomende dreigingen.

LEES VERDER



Cavalry Werewolf APT aanvallen op industrieën en onderzoek naar netwerk '764' en gehackte apparaten Philips Hue Bridge

Cavalry Werewolf APT richt zich op vitale sectoren zoals energie en mijnbouw met geavanceerde malware, waaronder FoalShell en StallionRAT. Tegelijkertijd wordt netwerk '764' in Nederland onderzocht, waar jongeren gedwongen werden tot gewelddadige en seksueel misbruikende handelingen. Onderzoekers ontdekten kwetsbaarheden in de Philips Hue Bridge en Samsung Galaxy S25, die hackers kunnen misbruiken voor remote code execution. De dreigingen van malware zoals SnakeStealer en Lumma Stealer blijven toenemen, wat de beveiliging van zowel bedrijven als consumenten blijft ondermijnen.

LEES VERDER

Omrin nog steeds geraakt door cyberaanval en gegevens van Albert Heijn medewerkers gelekt

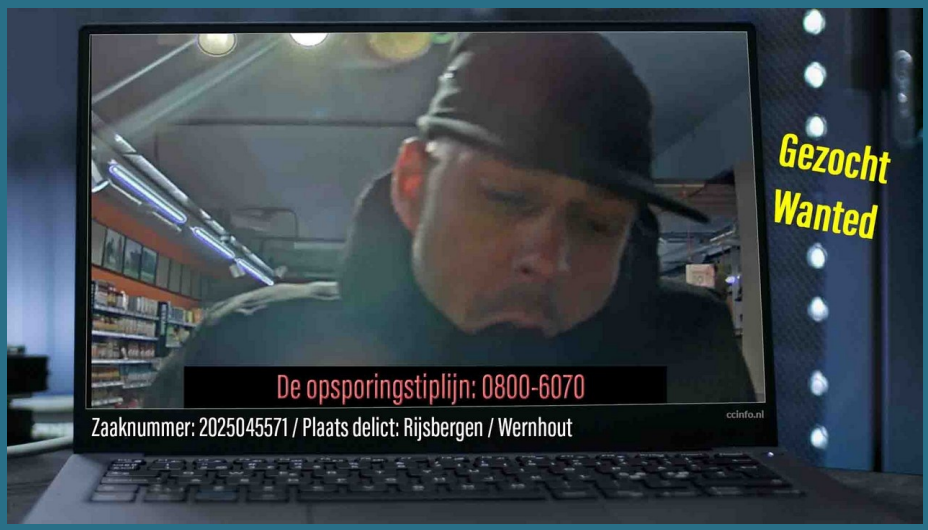
Omrin ondervindt nog steeds de gevolgen van een cyberaanval die in oktober begon, met tijdelijke storingen in hun afvalapp en kringloopwinkels. Er werd een datalek ontdekt, waarbij persoonlijke gegevens van klanten mogelijk zijn gelekt. Ook Bun, een grote Albert Heijn-franchisenemer, werd getroffen door een ransomwareaanval, waarbij duizenden medewerkersgegevens werden gestolen en op het darkweb gepubliceerd. De aanval werd uitgevoerd door de ransomwaregroep ThreeAM. Ondertussen worden kwetsbaarheden in Adobe Commerce en Lanscope aangepakt, en is er een waarschuwing voor oplichting met thuisbatterijen.

LEES VERDER

Albert Heijn franchisenemer Bun bevestigt ransomware aanval en KBC klanten doelwit van social engineering aanval

Albert Heijn franchisenemer Bun bevestigde dat het bedrijf slachtoffer werd van een ransomware-aanval, waarbij persoonlijke gegevens van medewerkers, zoals paspoorten en salarisinformatie, werden gestolen. De aanvallers, ThreeAM, hebben een deel van de gegevens gepubliceerd en dreigen meer vrij te geven als er geen betaling wordt gedaan. Ook werden klanten van de Belgische bank KBC doelwit van een social engineering-aanval, waarbij oplichters zich voordeden als medewerkers van Proximus en via een kwaadaardige app controle over de telefoons van slachtoffers kregen om fraude te plegen.

LEES VERDER



Rijsbergen / Wernhout - Bankhelpdeskfraude

Op 7 februari 2025 werd een inwoner van Rijsbergen slachtoffer van bankhelpdeskfraude. De oplichters belden het slachtoffer met een valse melding over een ongevraagd overboekingstransactie naar België. Na meerdere

telefoongesprekken wisten ze het slachtoffer ervan te overtuigen dat zijn bankrekening was gehackt. Uiteindelijk werd er duizenden euro's overgemaakt. De politie heeft beelden van de verdachte die het geld opnam bij een geldautomaat. De verdachte wordt omschreven als een man van 35-45 jaar met een blanke huidskleur en een North Face jas.

LEES VERDER

Meer leren over cybercrime? Ontdek de verschillende vormen en begrippen

In de Cybercrimeinfo Bibliotheek vind je een uitgebreide verzameling van termen en verschillende vormen van cybercriminaliteit. Van phishing en malware tot ransomware en andere digitale dreigingen, we leggen elke vorm duidelijk uit. Zo krijg je inzicht in wat deze aanvallen inhouden, hoe ze werken en welke risico's ze met zich meebrengen.

Of je nu op zoek bent naar uitleg over specifieke cybercrime termen of meer wilt leren over de verschillende soorten digitale bedreigingen, onze bibliotheek biedt de kennis die je nodig hebt om jezelf beter te beschermen.

Verdiep je in de wereld van cybercrime en vergroot je digitale weerbaarheid.

BEKIJK DE BIBLIOTHEEK

Beantwoorde vragen en tips voor digitale weerbaarheid

Op deze pagina vind je antwoorden op veelgestelde vragen, nuttige tips en praktische hulpmiddelen om je digitale veiligheid te verbeteren. Of je nu meer wilt weten over bescherming tegen cyberdreigingen of jezelf beter wilt wapenen tegen online gevaren, wij bieden de informatie die je nodig hebt.

BEKIJK DE TIPS

Veelgestelde vragen over digitale veiligheid en cybercrime

Op Cybercrimeinfo vind je antwoorden op de meest gestelde vragen over cybersecurity en cybercrime. Leer hoe je jezelf en je organisatie kunt beschermen tegen digitale dreigingen, van phishing en malware tot ransomware en DDoS-aanvallen. We bieden duidelijke uitleg en praktische tips om je digitale veiligheid te versterken.

ONTDEK DE ANTWOORDEN

Vergroot je kennis en vaardigheden

Wil je je kennis over cybersecurity en het darkweb uitbreiden? Bij de Leerplek van Cybercrimeinfo vind je een breed aanbod van cursussen, tutorials en quizzen die je helpen up-to-date te blijven met de nieuwste technieken en dreigingen. Of je nu net begint of al een expert bent, onze interactieve leeromgeving biedt de uitdaging die je nodig hebt om jezelf verder te

ontwikkelen.
Test je kennis met uitdagende quizzen en verdien toegang tot de exclusieve Perfecte Score Club. Voor opsporingsambtenaren bieden we binnenkort speciaal op maat gemaakte quizzen aan.

TEST JE KENNIS

Contact met Cybercrimeinfo

Heb je een vraag of probleem? Vul het formulier in en stel je vraag. We reageren zo snel mogelijk, maar houd er rekening mee dat het door de hoge aantallen vragen soms enkele dagen kan duren.

STEL JE VRAAG

Steun Cybercrimeinfo en help de strijd tegen cybercriminaliteit

Elke dag zetten wij ons in om je op de hoogte te houden van de laatste cyberdreigingen en trends. Onze missie is om jou en anderen te beschermen tegen de groeiende risico's in de digitale wereld. Maar we kunnen dit niet alleen. Jouw steun maakt het verschil.
Door te doneren help je ons waardevolle informatie te blijven leveren, nieuwe tools te ontwikkelen en de bewustwording over cybercriminaliteit te vergroten. Elke bijdrage, groot of klein, draagt bij aan de bescherming van digitale veiligheid.
Wil je ons steunen?

Samen maken we de online wereld een stukje veiliger.
Bedankt voor je steun!

STEUN ONS NU

Dagelijks cyber journaal van Cybercrimeinfo

Het Dagelijks Cyber Journaal biedt dagelijkse updates over de belangrijkste cyberdreigingen en incidenten in België en Nederland. Dit is bedoeld voor mensen die de ontwikkelingen in cybercrime willen volgen, maar geen tijd hebben om alles bij te houden. Het biedt een efficiënte manier om snel up-to-date te blijven zonder uren te spenderen aan het zoeken naar relevante informatie. De updates zijn beschikbaar in zowel tekst als via een dagelijkse podcast op Spotify en YouTube.

Ontvang dagelijks het cyber journaal tussen 12:00 en 14:00 (behalve zondag).
Schrijf je in en ontvang het automatisch in je mailbox.

E-mailadres *

Voornaam

Achternaam

Inschrijven

Inschrijven

Ontvang dagelijks het cyber journaal tussen 12:00 en 14:00 (behalve zondag). Schrijf je in en ontvang het automatisch in je mailbox.

INSCHRIJVEN

Share Tweet Share Pinterest Bluesky Mastodon