Cybercrimeinfo

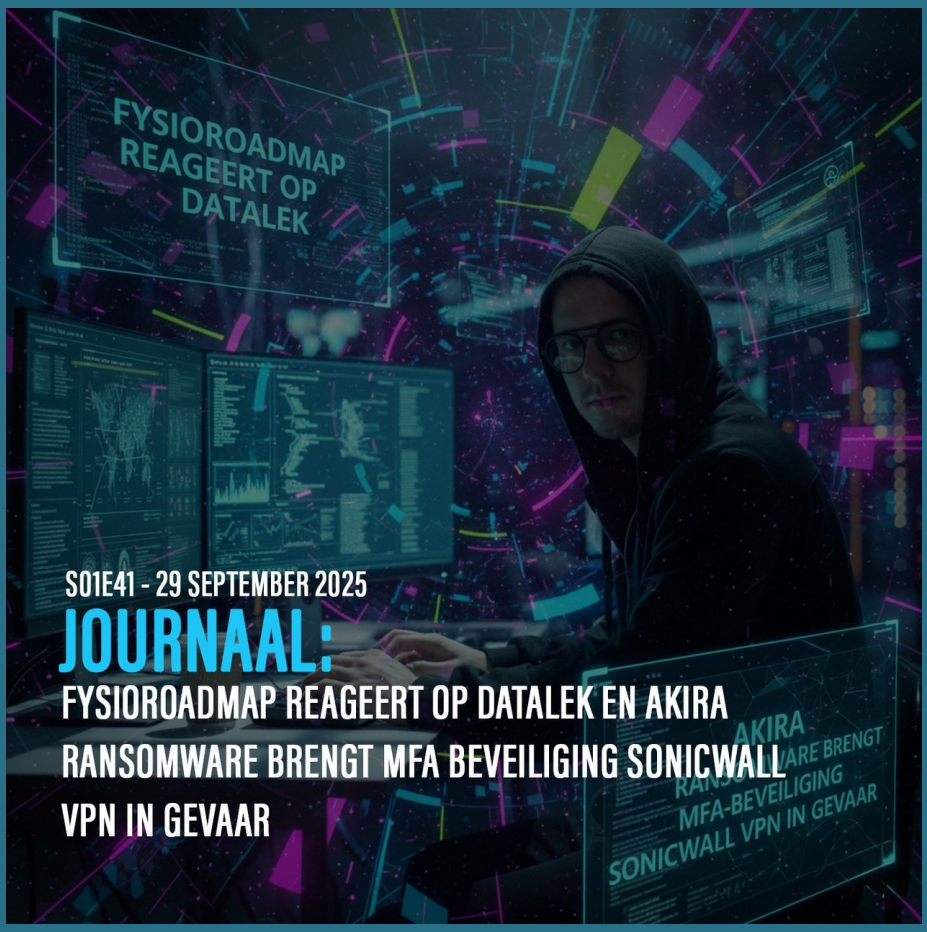
"Omdat wat waardevol is, beschermd moet worden"

NB386

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

Luister de podcast nu op Youtube

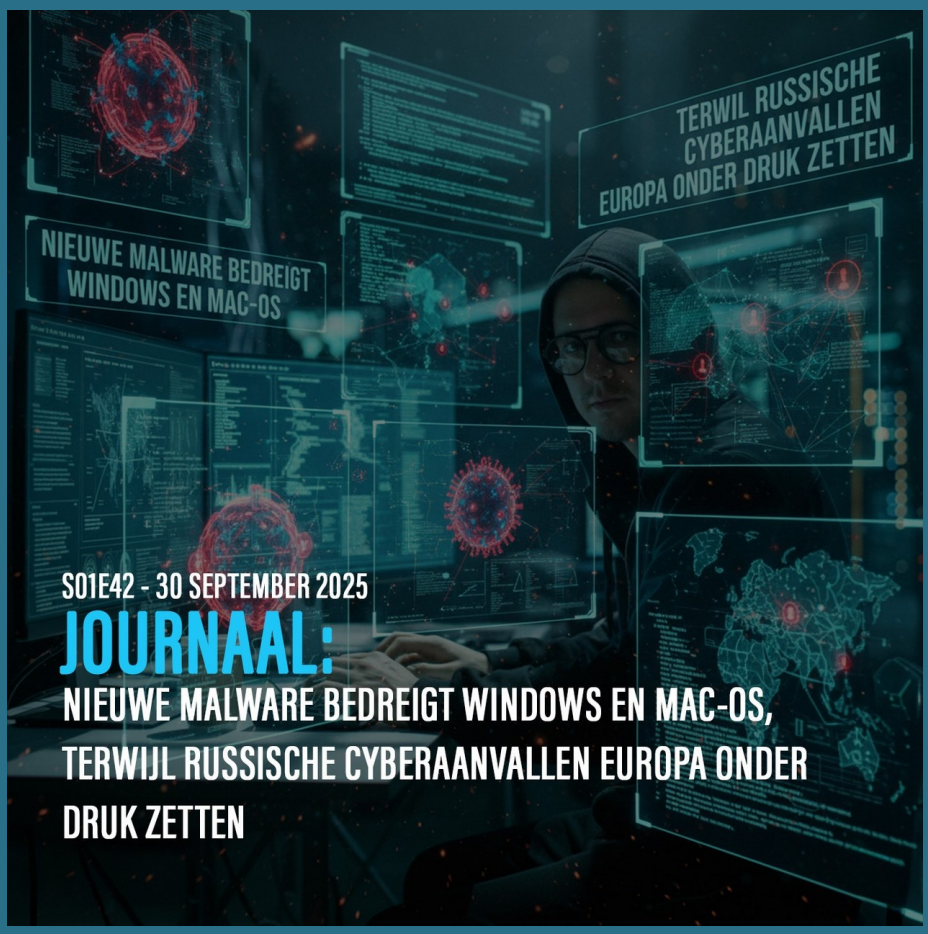
Luister de podcast nu op Spotify



FysioRoadmap reageert op datalek en Akira ransomware breekt MFA beveiliging van SonicWall VPN

FysioRoadmap, een softwareleverancier voor fysiotherapeuten in Nederland, werd getroffen door een cyberaanval waarbij gevoelige patiëntgegevens werden gestolen. Het bedrijf heeft de situatie gecontroleerd en werkt met experts om verdere schade te voorkomen. Er werd ook een kwetsbaarheid ontdekt in Apache Airflow, die gevoelige gegevens blootstelt, en een andere in SonicWall VPN, waarbij de Akira ransomware MFA-beveiliging omzeilde. Dit benadrukt de noodzaak van regelmatige beveiligingsupdates. Daarnaast blijft de dreiging van AI-gedreven malware en botnets toenemen, wat organisaties dwingt extra waakzaam te blijven.

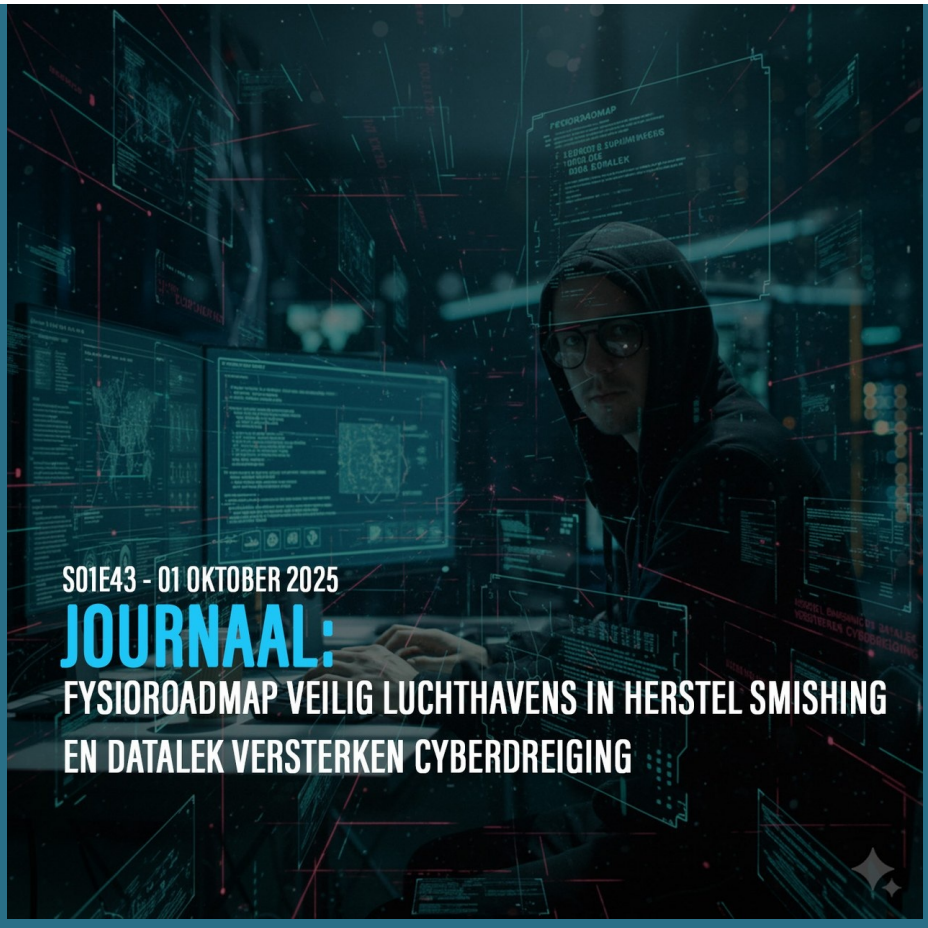
Lees verder



Nieuwe malware bedreigt Windows en macOS, terwijl Russische cyberaanvallen Europa onder druk zetten

Nieuwe malware bedreigt zowel Windows als macOS door persoonlijke gegevens te stelen, waaronder wachtwoorden en bankinformatie. Hackers maken gebruik van populaire software om deze malware te verspreiden, terwijl phishingtechnieken zich voordoen als betrouwbare software-updates. De Russische cyberaanvallen blijven Europa onder druk zetten, met focus op politieke destabilisatie, bijvoorbeeld in Moldavië. Daarnaast blijft de dreiging van datalekken groeien, zoals bij de Britse winkelketen Harrods, waar gegevens van 430.000 klanten zijn gelekt. Er is een toenemende behoefte aan verbeterde digitale beveiliging.

Lees verder



Cyberaanvallen vergroten dreigingen in luchtvaart cryptosector en gaming en versterken geopolitieke spanningen

FysioRoadmap is niet gehackt, maar een individuele praktijk werd getroffen door misbruik van inloggegevens via RDP. Het platform ondersteunt de herstelmaatregelen samen met Z-CERT. In de luchtvaart ondervinden luchthavens vertraging door een leveranciersaanval, terwijl Brussels Airport een nieuw check-in systeem invoert. Belangrijke beveiligingsupdates zijn uitgebracht voor Apple, VMware en Cisco vanwege kwetsbaarheden die actief worden misbruikt. Criminelen gebruiken 4G/5G routers voor smishing-aanvallen, en er zijn nieuwe bedreigingen gericht op ouderen via valse apps. Datalekken en hybride dreigingen zoals spionage en hacktivisme nemen toe.

Lees verder

Beveiliging zorgsector aangescherpt na datalek, kwetsbaarheden in AI tools en nieuwe cyberaanvallen op schepen en overheidsplatforms

De beveiliging in de zorgsector is aangescherpt na een datalek bij Bevolkingsonderzoek Nederland, waarbij gegevens van 850.000 patiënten werden gestolen. Z-CERT monitort de systemen continu om nieuwe risico's te vermijden. Daarnaast werden kwetsbaarheden ontdekt in AI-tools en platforms zoals OneLogin, die organisaties wereldwijd bedreigen. Cyberaanvallen op schepen, zoals de Sumud Flotilla, en overheidsplatforms, zoals KodexGlobal, benadrukken de kwetsbaarheid van kritieke infrastructuren. Er is ook een stijging van fraude via telefoontjes en sms'jes, waarbij cybercriminelen 13 miljoen euro wisten te stelen.

Lees verder

Nieuwe phishingaanval via ZIP bestanden, fraude met QR codes en Europese standpunten tegen Rusland

Een nieuwe phishingaanval maakt gebruik van ZIP-bestanden waarin kwaadaardige snelkoppelingen zijn verstopt, die gebruikers naar schadelijke software leiden. Daarnaast wordt er fraude gepleegd met QR-codes die naar nepwebsites leiden, waar persoonlijke gegevens worden gestolen. Geopolitieke spanningen, zoals de situatie tussen Rusland en Europa, versterken de digitale dreigingen, waarbij Europese landen waarschuwen voor de toename van cyberaanvallen. Hacktivistische groepen en ransomware blijven ernstige risico's vormen voor zowel bedrijven als overheden wereldwijd.

Lees verder

Defensie wil cyberwapens inzetten tegen Rusland, Europol waarschuwt over datatoegang

Defensie overweegt cyberwapens in te zetten tegen Rusland, terwijl Europol waarschuwt voor de groeiende dreigingen van ransomware, malware en phishing. Hackers hebben bedrijven zoals Oracle en AndSoft aangevallen, waarbij gevoelige gegevens werden gestolen. Europol benadrukt het belang van samenwerking om deze bedreigingen te bestrijden, aangezien criminelen steeds vaker versleuteling en andere technologieën gebruiken om het werk van wetshandhavers te bemoeilijken. Daarnaast blijven cybercriminelen geavanceerde technieken gebruiken, zoals de GhostSocks malware en phishingaanvallen via WhatsApp, die de veiligheid van zowel bedrijven als individuen onder druk zetten.

Lees verder

Bankhelpdeskfraude Zevenbergen Fijnaart: Onderzoek naar verdachten

In Zevenbergen werd een vrouw slachtoffer van bankhelpdeskfraude. Ze werd meerdere keren gebeld door zogenaamde bankmedewerkers, die haar verzochten

haar limieten te verhogen. Nadat haar bankpas werd opgehaald, werd deze gebruikt in verschillende steden, waaronder Fijnaart, Amsterdam en Haarlem. De politie heeft beelden van de verdachte, die onder andere een zwarte helm en een Prada tas droeg. De verdachten proberen hun identiteit te verbergen door hun gezicht te bedekken. De politie roept getuigen op zich te melden.

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