Cybercrimeinfo

"Omdat wat waardevol is, beschermd moet worden"

NB385

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

Luister de podcast nu op Youtube

Luister de podcast nu op Spotify

FysioRoadMap getroffen door Nova ransomware aanval - Nederlandse fysiotherapeuten slachtoffer van datalek

FysioRoadMap, een softwareleverancier voor fysiotherapiepraktijken, werd getroffen door een ransomware-aanval van de Nova-groep, waarbij gevoelige patiëntgegevens, waaronder BSN-nummers en medische resultaten, werden gestolen. De hackers lieten een "readme"-bestand achter met instructies voor het herstellen van de gegevens, wat hen onder druk zet om losgeld te betalen. Dit incident heeft ernstige gevolgen voor zowel de betrokken praktijken als patiënten, met verhoogd risico op identiteitsdiefstal. Het is nog onduidelijk hoe FysioRoadMap het herstel zal aanpakken, maar het informeren van getroffen patiënten is essentieel.

Lees verder

Luchthavens en systemen onder druk door cyberdreigingen van cybercriminelen, hacktivisten en statelijke actoren

Luchthavens wereldwijd, zoals Brussels Airport, staan onder druk door cyberdreigingen van cybercriminelen, hacktivisten en statelijke actoren. Recent werd Brussels Airport getroffen door een aanval die de vluchtprocedures verstoorde, met 35.000 passagiers als gevolg. Daarnaast zijn er nieuwe kwetsbaarheden ontdekt in populaire systemen, waardoor persoonlijke gegevens gevaar lopen. Hacktivistische groepen bundelen krachten, terwijl Rusland Estland blijft aanvallen. Ook de opkomst van AI-ondersteunde malware en de groei van zeroday kwetsbaarheden versterken de zorgen over digitale veiligheid wereldwijd.

Lees verder

Ransomware aanvallen en cyberdreigingen bedreigen multinationals en vitale systemen, terwijl ABN AMRO klanten gewaarschuwd worden voor phishing

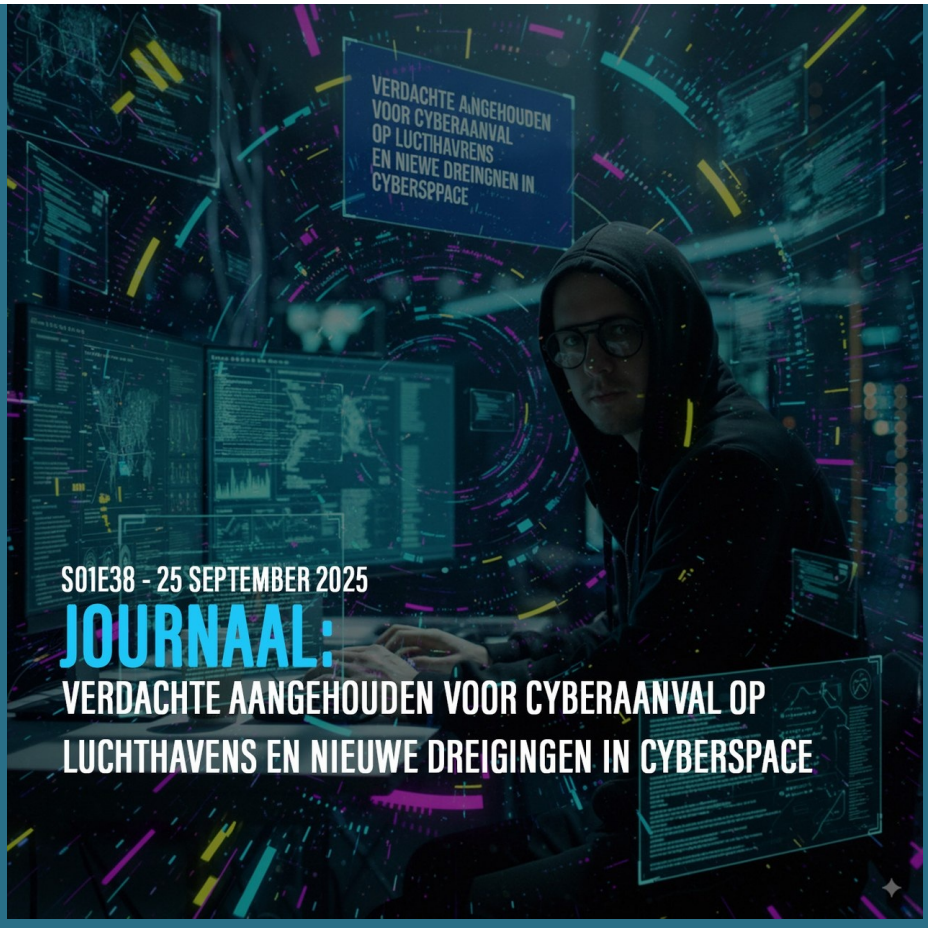
Ransomware-aanvallen bedreigen multinationals, vitale systemen en luchthavens wereldwijd. ABN AMRO waarschuwt klanten voor phishing-aanvallen waarbij valse noodnummers worden verstrekt. Kwetsbaarheden in Microsoft Entra ID en Google Chrome vergroten de risico's van malware en ransomware. Nieuwe dreigingen komen van de groepen Nimbus Manticore en Kawa4096, die zich richten op strategische sectoren en bedrijven wereldwijd. Hacktivistische allianties, zoals die tussen Inteid en Eye of Sauron, verhogen het risico voor overheids- en bedrijfsnetwerken. Ondernemers moeten zich voorbereiden op phishing en malware-aanvallen via SVG-bestanden.

Lees verder

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

Cyberdreigingen nemen toe in de luchtvaart, cryptosector en gaming, met malware-aanvallen, softwarekwetsbaarheden en oplichtingspraktijken die een groeiende zorg vormen. Luchthavens zoals Brussels Airport ondervonden verstoringen door ransomware, terwijl de game BlockBlasters werd getroffen door malware die persoonlijke gegevens van spelers steelt. Ook werd een platform in de cryptosector gehackt, waardoor miljoenen verloren gingen. Ondertussen bleken er kwetsbaarheden in populaire software zoals Web Help Desk en Oracle te bestaan, die hackers toegang gaven tot gevoelige gegevens. Geopolitieke spanningen, waaronder Russische inmenging, verergeren de situatie verder.

Lees verder



Verdachte aangehouden voor cyberaanval op luchthavens en nieuwe dreigingen in cyberspace

Een verdachte is aangehouden in het Verenigd Koninkrijk na een cyberaanval op verschillende luchthavens, waaronder Brussels Airport. De aanval, vermoedelijk uitgevoerd met ransomware, veroorzaakte verstoringen in de luchtvaartsector. Internationale samenwerking bleek cruciaal bij het terugvorderen van 439 miljoen dollar aan gestolen geld en activa in een wereldwijde operatie. Daarnaast werd er wereldwijd nieuwe malware gedetecteerd, terwijl kwetsbaarheden in populaire software zoals Salesforce en OnePlus de digitale veiligheid in gevaar brengen. Verdere samenwerking en beveiligingsmaatregelen zijn noodzakelijk om deze dreigingen tegen te gaan.

Lees verder

Openbaar Ministerie herstelt systemen na cyberinbraak Rust malware steelt crypto sleutels en man veroordeeld

Het Openbaar Ministerie in Nederland heeft zijn systemen hersteld na een cyberinbraak in juli 2025, veroorzaakt door een kwetsbaarheid in het Citrix-systeem. Ondertussen werd de Rust malware ontdekt, die crypto wallets aanvalt door private sleutels te stelen, wat de veiligheid van digitale valuta bedreigt. In Europa waren er diverse kwetsbaarheden in populaire systemen zoals die van Cisco en Supermicro, die hackers in staat stelden volledige controle te verkrijgen. Ook werd een ransomwaregroep, Miga, ontdekt, die grote netwerken aanvalt.

Lees verder

Nederlandse tieners gearresteerd voor spionage en Roblox gebruikers in gevaar door cheattools

Twee 17-jarige jongens uit Nederland werden gearresteerd wegens verdacht spionagegedrag voor een Russische inlichtingendienst. Ze probeerden geheime informatie te verzamelen met speciale apparatuur in Den Haag. Daarnaast werd een internationale kinderopvangorganisatie, Kido, getroffen door een ransomware-aanval waarbij gegevens van 8.000 kinderen werden gestolen. Er werd ook gewaarschuwd voor de risico's van cheattools op het platform Roblox, die kunnen leiden tot verlies van persoonlijke gegevens en accounts. Tot slot werden kwetsbaarheden ontdekt in Cisco-systemen, die organisaties in Nederland en België moeten patchen.

Lees verder

Bankhelpdeskfraude in Prinsenbeek (Breda) 82 jarige vrouw opgelicht

Een 82-jarige vrouw uit Prinsenbeek werd slachtoffer van bankhelpdeskfraude. Ze werd gebeld door iemand die zich voordeed als een bankmedewerker en haar angst

aanjoeg met het verhaal van een internetvirus. De vrouw werd onder druk gezet om haar bankpassen en waardevolle spullen over te dragen aan een zogenaamde collega die langs zou komen. Kort daarna verscheen er een man die de spullen meenam, waarna de passen meteen werden gebruikt. De politie zoekt de verdachte, die wordt omschreven als een man van 20-30 jaar, gekleed in een zwart Nike-trainingsjack en een zwarte pet.

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