Cybercrimeinfo

"Omdat wat waardevol is, beschermd moet worden"

Nieuwsbrief 398

De wekelijkse digitale weerbaarheid quiz: Week 52-2025

Terwijl 2025 op zijn einde loopt, blijkt de digitale wapenstilstand ver te zoeken. In week 52 zien we een zorgwekkende mix van nieuwe kritieke kwetsbaarheden en de nasleep van geopolitieke spanningen. Bent u op de hoogte van de laatste incidenten die de feestdagen verstoorden, en heeft u de strategische verschuivingen van het afgelopen jaar scherp op het netvlies?
In deze editie testen we uw kennis over actuele dreigingen, zoals de 1.760 WatchGuard firewalls die in Nederland nog altijd openstaan voor misbruik en de recente ransomware aanval op Victoria Benelux door een beruchte hackersgroep. Daarnaast duiken we de diepte in met complexe casussen:

- Weet u welke legitieme Windows functie (BitLocker) werd misbruikt bij de aanval op de Roemeense waterbeheerautoriteit?
- Bent u bekend met de 'Sleeping Bouncer' hardware kwetsbaarheid die DMA beveiliging bij het opstarten omzeilt?
- En heeft u meegekregen dat Anna’s Archive claimt maar liefst 300 terabyte aan data bij Spotify te hebben buitgemaakt?

Van de alliantie tussen Qilin, DragonForce en LockBit tot de adviezen rondom dumbphones voor kinderen: deze 20 vragen scheiden de security experts van de nieuws scanners.

QUIZ 52-2025

Strategisch Dreigingsrapport Cyberveiligheid week 52-2025

Het strategisch rapport over week 52 van 2025 schetst een zorgwekkend beeld van de digitale veiligheid, waarbij de grens tussen statelijke actoren en criminele syndicaten steeds verder vervaagt. Deze ontwikkeling kenmerkt zich door een verschuiving naar hybride operaties, waarbij zowel digitale systemen als fysieke infrastructuren, zoals onderwaterkabels en energieverbindingen, het doelwit vormen. De inzet van kunstmatige intelligentie en geavanceerde samenwerkingsverbanden tussen hackersgroepen versterkt deze dreiging, wat een integrale aanpak van nationale cybersecurity noodzakelijk maakt.

In de laatste periode van 2025 is een sterke toename van disruptieve aanvallen op vitale diensten waargenomen, zoals de grootschalige DDoS aanvallen op de Franse bankensector en de Belgische energiesector tijdens de kerstperiode. Deze acties, vaak uitgevoerd door groepen zoals DDoSia, lijken sterk verbonden met geopolitieke spanningen rondom Europese besluitvorming. Daarnaast blijft ransomware een kritiek risico voor de bedrijfscontinuïteit, waarbij groepen zoals Qilin gebruikmaken van voorbereidende diefstal van inloggegevens om systemen methodisch te gijzelen.

De actoren achter deze dreigingen tonen een hoge mate van specialisatie en professionalisering, variërend van de Russische spionagecampagnes gericht op cognitieve oorlogsvoering tot de geraffineerde Iraanse malware ontwikkeling. Opvallend is ook de Noord-Koreaanse strategie om via valse identiteiten en IT functies op afstand valuta te genereren voor nationale programma's. Terwijl de winstgevendheid van individuele ransomware aanvallen onder druk staat door strengere wetshandhaving, reageert het criminele ecosysteem door strategische allianties te vormen tussen groepen zoals LockBit en DragonForce om hun slagkracht te behouden.

RAPPORT 52-2025

Nieuwe ransomware allianties en sabotage in Benelux verharden wereldwijde hybride dreiging

De digitale dreiging in de Benelux verhardt door nieuwe allianties tussen ransomwaregroepen en gerichte aanvallen op vitale infrastructuur, zoals de energiesector. De grens tussen digitale verstoring en fysieke sabotage vervaagt, waarbij ook maritieme verbindingen onder druk staan. Kwetsbaarheden in consumentenelektronica en zakelijke software blijven grote risico's vormen voor de privacy. Ondanks internationale successen tegen fraude, waarschuwen instanties voor de inzet van AI en psychologische oorlogsvoering om de maatschappij strategisch te ontwrichten.

LEES VERDER

Dagelijks inzicht in actuele cyberdreigingen
Abonneer u op het cyberdreigingsrapport

Roemeense waterdienst gegijzeld en duizenden firewalls in Benelux kwetsbaar

Een grootschalige ransomware aanval heeft de systemen van een Roemeense waterdienst platgelegd, terwijl in de Benelux duizenden firewalls acuut gevaar lopen door een kritiek lek. Wereldwijd kampen organisaties zoals NASA met datadiefstal en groeit de zorg over AI gegenereerde deepfakes op scholen. Tegenover deze dreigingen staan internationale politiesuccessen, waarbij fraudenetwerken zijn opgerold en een ontvoering is verijdeld. Ondertussen waarschuwen privacyvoorvechters voor toenemende Europese massasurveillance en pleit de overheid voor digitale weerbaarheid bij jongeren.

LEES VERDER

Enorme datadiefstal bij Spotify en Franse kerstdrukte verstoord door cyberaanval

Diverse digitale verstoringen hebben recent grote impact gehad op vitale diensten en bedrijven. In Frankrijk zorgden DDoS aanvallen voor chaos bij postdiensten en banken, terwijl een datalek bij softwareleverancier Red Hat onder meer ING heeft getroffen. Daarnaast claimen hackers honderden terabytes aan data bij Spotify te hebben buitgemaakt. Experts waarschuwen tevens voor kritieke kwetsbaarheden in veelgebruikte bedrijfssoftware en nieuwe malwarevarianten, terwijl techbedrijven actief maatregelen nemen tegen spionagepogingen van staatshackers.

LEES VERDER

Weten hoe kwetsbaar jouw organisatie is?
Plan een gratis adviesgesprek

Rijen / Breda - Bankhelpdeskfraude

Geraffineerde bankhelpdeskfraude in Rijen en Breda laat zien hoe oplichters slachtoffers manipuleren door extreme tijdsdruk en paniek te creëren. Criminelen doen zich voor als bankmedewerkers en overtuigen mensen hun bankpas door te knippen, terwijl de cruciale chip intact blijft. Hierdoor lijkt de pas onbruikbaar, maar kunnen daders er alsnog grote bedragen mee pinnen. Het fysiek ophalen van de pas aan de deur vergroot de geloofwaardigheid van deze geraffineerde psychologische aanval aanzienlijk.

LEES VERDER

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

Luister de podcast nu op Youtube

Luister de podcast nu op Spotify

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

Het Cyber Journaal

Het Cyber Journaal biedt meerdere keren per week een overzicht van de belangrijkste cyberdreigingen en incidenten in België en Nederland. Het is bedoeld voor mensen die de ontwikkelingen in cybercrime willen volgen, maar niet de tijd hebben om alle bronnen zelf bij te houden. Het journaal maakt het mogelijk om efficiënt en snel inzicht te krijgen in relevante informatie zonder langdurig te hoeven zoeken. De updates zijn beschikbaar in tekstvorm en gelijktijdig als podcast via Spotify en YouTube.

Het Cyber Journaal verschijnt meerdere keren per week, doorgaans tussen 12:00 en 14:00 uur. Schrijf je in en ontvang het automatisch in je mailbox.

E-mailadres *

Voornaam

Inschrijven

Inschrijven

Ontvang meerdere keren per week het Cyber Journaal met actuele ontwikkelingen en dreigingen in de digitale wereld. Het journaal verschijnt doorgaans tussen 12:00 en 14:00 uur en wordt automatisch per e-mail toegestuurd. Gelijktijdig verschijnt ook de bijbehorende podcast.

INSCHRIJVEN

Share Tweet Share Pinterest Bluesky Mastodon