Cybercrimeinfo

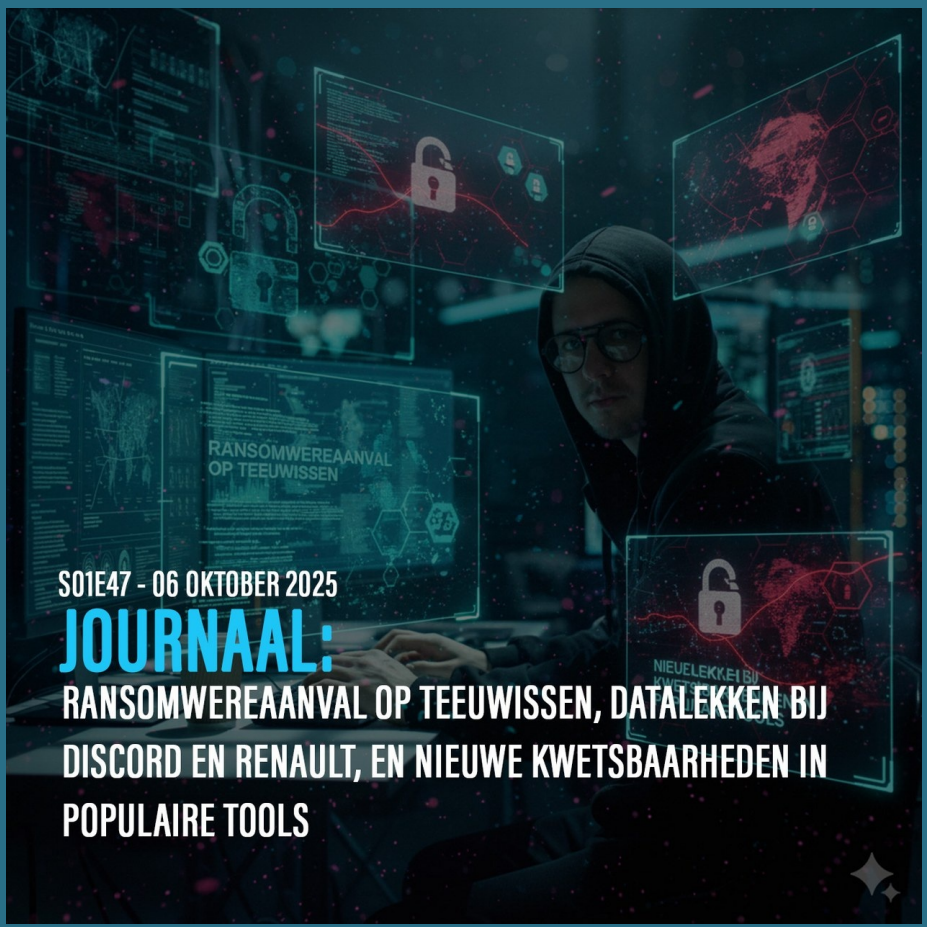
"Omdat wat waardevol is, beschermd moet worden"

NB387

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

Luister de podcast nu op Youtube

Luister de podcast nu op Spotify



Ransomwareaanval op Teeuwissen, datalekken bij Discord en Renault, en nieuwe kwetsbaarheden in populaire tools

Teeuwissen Rioolreiniging werd getroffen door een ransomwareaanval, waarbij $370.000 werd geëist voor de vrijgave van gestolen gegevens. Ook Discord meldde dat identiteitsbewijzen van gebruikers werden gestolen door een externe partij, en Renault UK bevestigde dat klantgegevens werden buitgemaakt bij een aanval op een leverancier. Nieuwe kwetsbaarheden in Unity, OneDrive en Zimbra bedreigen de veiligheid van gebruikers. Bovendien werd een toename van verdachte activiteiten bij beveiligingsbedrijven waargenomen, en werden er zorgen geuit over de groeiende cyberdreigingen in Europa.

Lees verder

Sunweb datalek en nieuwe fraudepraktijken bedreigen consumenten terwijl XWorm malware en Kyber Onion ransomware wereldwijd toeslaan

Sunweb werd getroffen door een datalek waarbij klantgegevens werden gestolen, waarna phishingmails werden verzonden met verzoeken om persoonlijke informatie of betalingen. Tegelijkertijd nam fraude toe, met oplichters die zich voordoen als gerechtsdeurwaarders of incassobureaus. Nieuwe dreigingen zoals de XWorm malware en Kyber Onion ransomware blijven wereldwijd slachtoffers maken. XWorm, verspreid via phishing, kan zowel gegevens stelen als losgeld eisen, terwijl Kyber Onion organisaties wereldwijd bedreigt met encryptie-aanvallen. Bedrijven worden aangespoord om hun beveiligingsmaatregelen te verbeteren.

Lees verder

Nederland start proef met steunpunten tegen cyberaanvallen terwijl Sunweb phishing slachtoffers afwijst

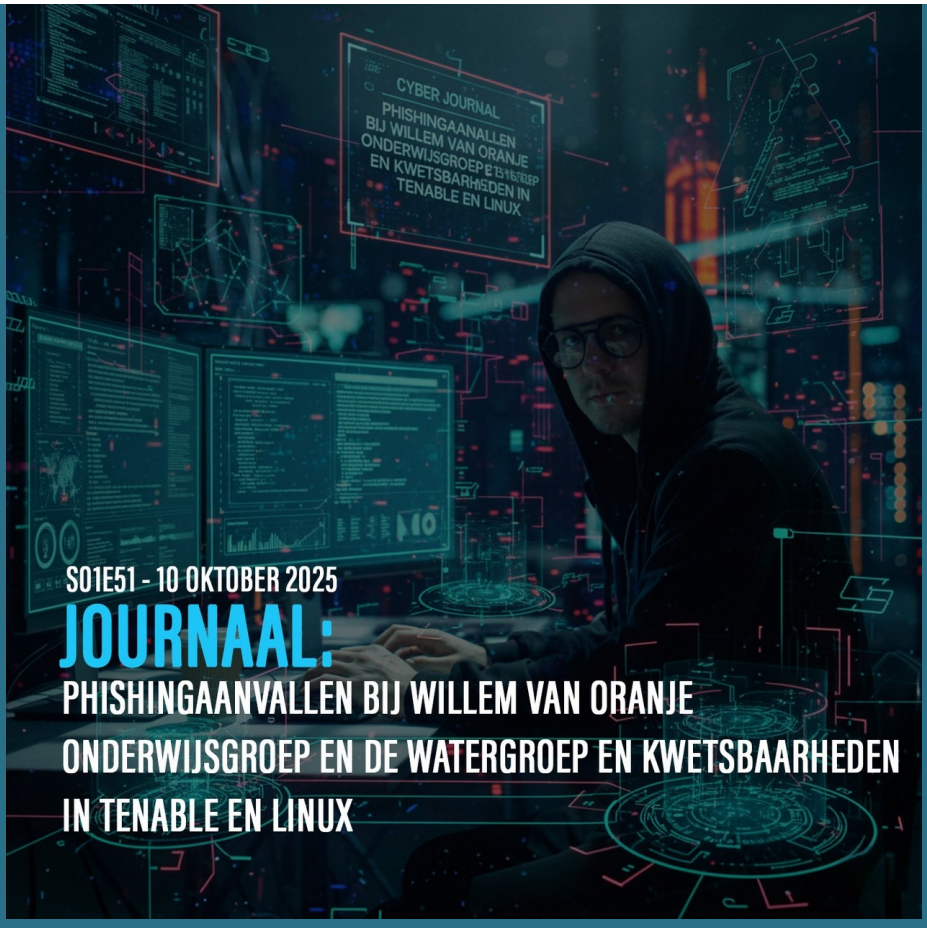
Sunweb heeft besloten geen compensatie te bieden aan klanten die slachtoffer werden van phishingaanvallen, ondanks dat klantgegevens zijn gestolen. Er wordt onderzocht of Sunweb verantwoordelijk is voor de schade vanwege onvoldoende gegevensbeveiliging. In Nederland wordt een proef gestart met noodsteunpunten voor crises, waaronder cyberaanvallen. Deze steunpunten, die in alle veiligheidsregio's komen, bieden hulp bij digitale en natuurrampen. Daarnaast zijn er nieuwe kwetsbaarheden ontdekt in software die bedrijven kunnen blootstellen aan aanvallen, waardoor snelle updates noodzakelijk zijn.

Lees verder

Ransomware aanval in Volendam, recorddiefstal van cryptocurrency en kritieke kwetsbaarheden in populaire software

Een ransomware-aanval heeft meerdere bedrijven in Volendam getroffen, waardoor systemen zijn geblokkeerd en losgeld wordt geëist. Tegelijkertijd stalen Noord-Koreaanse hackers meer dan $2 miljard aan cryptocurrency, vermoedelijk voor nucleaire wapens. Er werden kritieke kwetsbaarheden ontdekt in populaire software zoals WordPress, Google Chrome, Figma en AWS, die gebruikers dringend oproepen tot updates. De dreiging van cyberaanvallen blijft toenemen, met zowel ransomware als geopolitieke aanvallen, waaronder hacktivistische acties en sextortion, die de wereldwijde cyberbeveiliging onder druk zetten.

Lees verder



Phishingaanvallen bij Willem van Oranje Onderwijsgroep en De Watergroep en kwetsbaarheden in Tenable en Linux

Phishingaanvallen hebben plaatsgevonden bij de Willem van Oranje Onderwijsgroep en De Watergroep, waarbij valse e-mails medewerkers naar nepwebsites lokten. Bij de Onderwijsgroep leidde dit tot het uitlekken van 450 e-mailadressen. Ook werden kwetsbaarheden ontdekt in Tenable Security Center, Linux-systemen en de Nothing Phone, die risico's vormen voor gevoelige data en systemen. Cybercriminelen kunnen deze kwetsbaarheden misbruiken om systemen te compromitteren. Gebruikers wordt geadviseerd om de laatste beveiligingsupdates snel door te voeren om zich tegen deze dreigingen te beschermen.

Lees verder

Malwareaanvallen op telecomklanten en spionage binnen de EU vergroten de digitale dreigingen

Malwareaanvallen op telecomklanten en spionage binnen de EU vormen een groeiende digitale dreiging. Cybercriminelen richten zich steeds vaker op telecombedrijven en hun klanten met schadelijke software, die kan leiden tot het stelen van gevoelige informatie zoals bankgegevens. Daarnaast is er bezorgdheid over spionageactiviteiten binnen de EU, waarbij landen als Hongarije beschuldigd worden van het verzamelen van inlichtingen. De situatie wordt verder gecompliceerd door de ontdekking van geavanceerde malware en ransomwaregroepen die zich op bedrijven richten, wat de noodzaak voor betere bescherming tegen deze dreigingen benadrukt.

Lees verder

Bankhelpdeskfraude op Damrak in Amsterdam

Twee verdachten worden gezocht voor bankhelpdeskfraude in Amsterdam, waarbij een vrouw uit Hoofddorp 18.000 euro verloor. De vrouw werd telefonisch benaderd door een oplichter die zich als bankmedewerker voordeed en haar vroeg om haar

bankpas en pincode af te geven. Na de oplichting werd het gestolen geld opgenomen bij verschillende pinautomaten in Amsterdam. De verdachten zijn een mogelijk minderjarig persoon met krullend zwart haar en donkere kleding, en een meerderjarige man met een baard in een grijs joggingspak. De politie vraagt getuigen 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