Cybercrimeinfo

"Omdat wat waardevol is, beschermd moet worden"

Nieuwsbrief 392

Test je digitale weerbaarheid met de wekelijkse pro quiz van Cybercrimeinfo

Cybercrimeinfo daagt je elke week uit met een pro quiz, speciaal ontworpen om jouw kennis van cyberveiligheid te versterken.
Ransomware, phishing, zwakke plekken in systemen, deze quiz houdt je scherp en up-to-date met de laatste digitale dreigingen.

Je leert niet alleen bij, maar traint ook actief je digitale weerbaarheid. Zo ben je beter voorbereid op de slimmigheidjes van cybercriminelen.

Kortom: een slimme, snelle en serieuze manier om je cybersecurity skills te verbeteren. Doe mee met de quiz en blijf de cyberboeven een stap voor!

QUIZ 46-2025

DDoS aanvallen via Cisco, runC kwetsbaarheden en de opkomst van GlassWorm en Whisper Leak versterken cyberdreigingen

DDoS-aanvallen hebben recent belangrijke Belgische websites getroffen, uitgevoerd door hackercollectieven zoals HEZI RASH en NoName. Deze aanvallen overbelasten systemen, waardoor ze tijdelijk onbereikbaar zijn. Er zijn ook kwetsbaarheden ontdekt in populaire software, zoals Cisco's firewalls en WordPress-plugins, die hackers kunnen misbruiken om toegang tot gevoelige gegevens te verkrijgen. Nieuwe malware zoals GlassWorm en Whisper Leak bedreigen verdere veiligheid, waarbij GlassWorm via ontwikkelaarsplatforms gegevens steelt en Whisper Leak versleuteld verkeer kan analyseren. AI en drones versterken de dreiging van cyberaanvallen.

LEES VERDER

Chinese cyberwapens en doelwitlijsten, APT aanvallen op de bouwsector, AI misbruik en cryptofraude

Een recente aanval op de Chinese cybersecurityfirma Knownsec heeft duizenden documenten onthuld, waaronder informatie over staatsgesponsorde cyberaanvallen, en doelwitten wereldwijd. Ook de bouwsector wordt steeds vaker getroffen door APT-aanvallen, waarbij hackers via phishing inloggegevens proberen te verkrijgen. Daarnaast werd een kwetsbaarheid in de JavaScript-bibliotheek expr-eval ontdekt, die misbruikt kan worden voor schadelijke code-executie. Verder neemt cryptofraude in 2025 explosief toe, met al 29 miljoen euro verloren door digitale oplichting. Nieuwe ransomware, zoals Kazu Onion, blijft een serieuze dreiging vormen voor bedrijven wereldwijd.

LEES VERDER

Everest valt AGFA (B) aan, Microsoft verhelpt zeroday kwetsbaarheden en AI gedreven supply chain aanvallen nemen toe

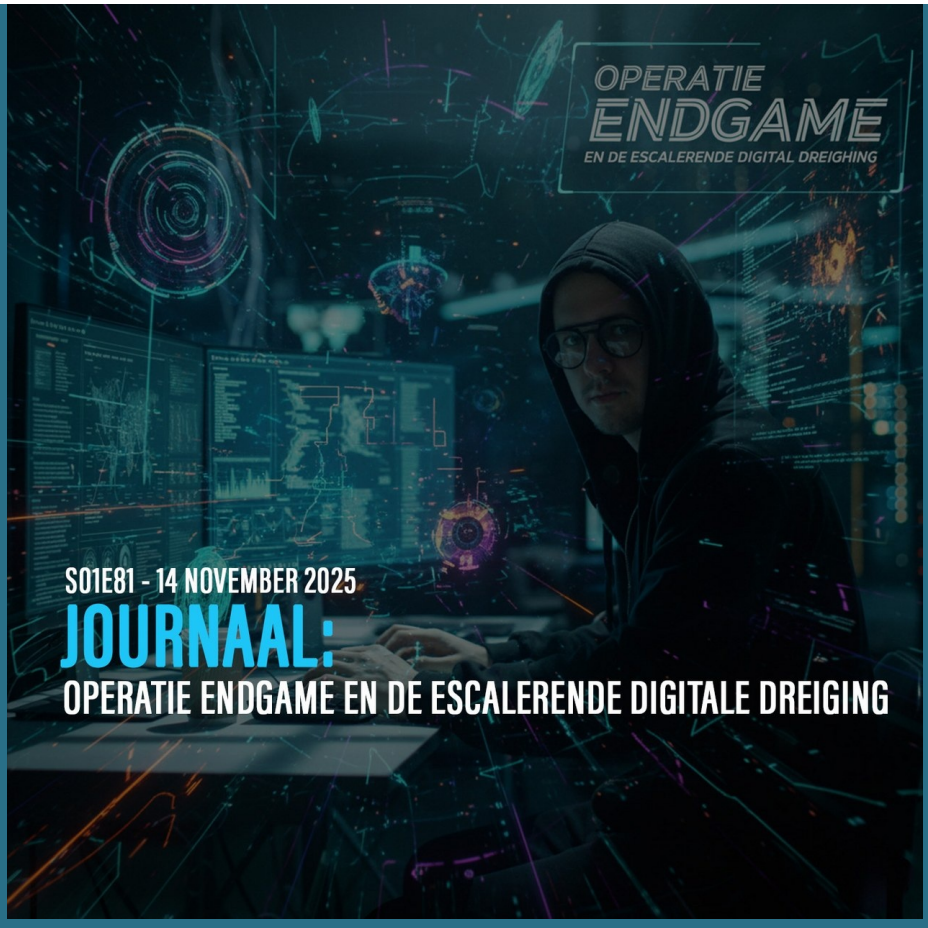
Everest ransomware heeft het Belgische AGFA aangevallen, maar de omvang van de schade is nog onbekend. Tegelijkertijd heeft Microsoft kwetsbaarheden in zijn systemen gepatcht, waaronder zero-day kwetsbaarheden in Zoom en Samsung-apparaten. De dreiging van AI-gedreven supply chain-aanvallen neemt wereldwijd toe, wat de effectiviteit van traditionele beveiligingsmaatregelen ondermijnt. Daarnaast is er een toename van phishingcampagnes die zich richten op Microsoft 365-gebruikers. Bedrijven wordt aangeraden om snel beveiligingsupdates door te voeren om zich te beschermen tegen deze geavanceerde dreigingen.

LEES VERDER

Phishing via Meta, Facebook malware op macOS en beveiligingsplannen voor Belgische havens

Grootschalige phishingaanvallen via Meta Business Suite en Facebookmail richten zich op MKB-gebruikers wereldwijd, waarbij inloggegevens van slachtoffers worden gestolen. Daarnaast neemt de dreiging van macOS-infostealers toe, die vertrouwelijke gegevens zoals inloggegevens en cryptowallets stelen. In België worden nieuwe beveiligingsmaatregelen getroffen voor havens, met een focus op het beschermen tegen zowel cyberaanvallen als fysieke dreigingen, waaronder drones en schepen. De verhoogde hybride dreiging benadrukt de noodzaak van versterkte beveiliging van kritieke infrastructuur in de regio.

LEES VERDER



Operatie Endgame en de escalerende digitale dreiging

Operatie Endgame heeft aanzienlijke vooruitgang geboekt in de strijd tegen cybercriminelen, waarbij 1025 servers werden uitgeschakeld, waarvan 83 in Nederland. Tegelijkertijd blijven kwetsbaarheden in technologie, zoals in firewalls en AI-systemen, digitale veiligheid ernstig bedreigen. Malware zoals MastaStealer en de geavanceerde Safery Ethereum Wallet richten zich op gebruikers van digitale wallets en cryptocurrencies. Internationale samenwerking, waaronder Europol en Eurojust, blijft cruciaal in de bestrijding van cybercriminaliteit. De dreiging van digitale aanvallen neemt toe door automatisering en de opkomst van AI, die de snelheid van aanvallen vergroot.

LEES VERDER

Cybergolven: van lokale aanvallen tot mondiale AI oorlogsvoering

Er is een datalek gemeld bij Eurofiber, waarbij zowel een volledige database als onderdelen van het interne IT-systeem zouden zijn buitgemaakt. RTV Noord werd getroffen door een ransomware-aanval, maar weigerde het geëiste losgeld te betalen. Er werden verschillende kritieke kwetsbaarheden ontdekt, waaronder in ImunifyAV en ASUS DSL-routers. Nieuwe ransomware-aanvallen zoals Kraken en Akira richten zich op grote organisaties wereldwijd. In Nederland werden 250 fysieke servers in beslag genomen in een actie tegen een bulletproof hoster, en er werden wereldwijde inspanningen geleverd tegen Chinese cryptofraudenetwerken. AI-gestuurde cyberaanvallen krijgen steeds meer aandacht, met een groeiende rol van kunstmatige intelligentie in geopolitieke cyberdreigingen.

LEES VERDER

Tilburg - Oplichter doet zich voor als FIOD agent en steelt geld en sieraden

In Tilburg heeft een oplichter zich voorgedaan als een FIOD-agent en heeft een

man opgelicht door geld en sieraden af te nemen. De verdachte belde het slachtoffer en vroeg hem om waardevolle spullen over te dragen. Vervolgens overtuigde de oplichter het slachtoffer om een programma te installeren om een zogenaamd virus te verwijderen, waarna er geld naar een andere rekening werd overgemaakt. De politie zoekt de verdachte, die op camerabeelden te zien is, en roept getuigen op zich te melden.

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

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