Cybercrimeinfo

"Omdat wat waardevol is, beschermd moet worden"

Nieuwsbrief 393

Bent u op de hoogte van de digitale dreigingen van Week 47, 2025?

De wereld van cybersecurity staat nooit stil en de afgelopen week was daar het perfecte bewijs van. Van grootschalige infrastructurele storingen tot geavanceerde spionagepraktijken: de impact op onze digitale veiligheid was groot. We zagen hoe een ogenschijnlijke cyberaanval op Cloudflare uiteindelijk te herleiden was naar een ‘latente bug’ na een configuratie-aanpassing, terwijl Jaguar Land Rover wel degelijk slachtoffer werd van de Scattered Lapsus$ Hunters, met een schadepost van ruim $220 miljoen tot gevolg.

Maar hoe veilig is uw data dichter bij huis? In Nederland ontstond politieke onrust over de veiligheid van DigiD en MijnOverheid na de overname van Solvinity door het Amerikaanse Kyndryl, en werden bij een datalek bij Clinical Diagnostics de gegevens van bijna een miljoen mensen geraakt. Tegelijkertijd vervaagt de grens tussen fysieke en digitale oorlogvoering: van Noord-Koreaanse spionnen die via ‘laptop-farms’ Amerikaanse bedrijven infiltreren tot sabotage aan het Poolse spoor in opdracht van Russische inlichtingendiensten.

Daarnaast rukt de rol van Artificial Intelligence in de cybercriminaliteit op. Weet u hoe tools als Xanthorox worden betaald, of hoe AI wordt ingezet om pig-butchering fraude te automatiseren? En bent u alert op technische kwetsbaarheden, zoals het misbruik van het stokoude ‘Finger’-protocol op poort 79 of de risico’s van VPN’s zonder multi-factor authenticatie bij Akira-ransomware?

Test uw kennis van het actuele dreigingslandschap, vitale infrastructuur en de nieuwste aanvalstechnieken in De Wekelijkse Digitale Weerbaarheid Quiz.

QUIZ 47-2025

Cybercrimeinfo’s Strategisch Dreigingsrapport Cyberveiligheid

Het geopolitieke cyberdreigingslandschap vertoont een toenemende convergentie van digitale en fysieke conflicten. Statelijke actoren gebruiken cyberaanvallen steeds vaker als onderdeel van hybride strategieën, met tastbare fysieke gevolgen zoals sabotage en militaire aanvallen. Dit rapport analyseert de gebruikte tactieken van deze actoren, waaronder de exploitatie van softwarekwetsbaarheden en vertrouwen in digitale systemen. Zero-day kwetsbaarheden en geavanceerde technieken zoals DLL sideloading worden steeds meer ingezet om defensieve maatregelen te omzeilen. Daarnaast speelt kunstmatige intelligentie een grotere rol in het verhogen van de schaal en effectiviteit van cybercriminaliteit, van geautomatiseerde social engineering tot desinformatiecampagnes.
De profielen van landen zoals Noord-Korea, China, Rusland en Iran tonen aan hoe cyberoperaties hun strategische doelen ondersteunen, van financiële winst tot spionage en militaire operaties. Hybride oorlogsvoering, waarbij digitale en fysieke dreigingen geïntegreerd worden ingezet, vormt een groeiende bedreiging voor de nationale veiligheid en vitale infrastructuren wereldwijd. Deze ontwikkelingen benadrukken de noodzaak van een integrale, proactieve benadering van cyberveiligheid, met versterkte samenwerking tussen publieke en private sectoren en de waarborging van digitale soevereiniteit.

Rapport 47-2025

De digitale oorlog voortgezet met AI en oude protocollen

De digitale oorlog blijft intensiveren, gedreven door de opkomst van AI-gedreven dreigingen en het misbruik van verouderde protocollen. Onlangs werden kwetsbaarheden in systemen zoals Cisco, XWiki en het 'Finger' protocol uitgelegd, die aangevallen werden door diverse cybercriminelen. Tevens werd de dreiging van Noord-Koreaanse spionage en geavanceerde malware zoals Lumma Stealer en Akira ransomware besproken. Cyberaanvallen richten zich steeds vaker op kritieke infrastructuur, terwijl de inzet van AI in cyberaanvallen nieuwe risico's voor digitale veiligheid creëert.

LEES VERDER

De digitale frontlinies een wereldwijde strijd om data en stabiliteit

De digitale strijd om data en stabiliteit wordt steeds intensiever, met recente incidenten die de kwetsbaarheid van systemen onderstrepen. Zo werden persoonlijke gegevens gestolen via een kwetsbaarheid in een ticketplatform van Eurofiber. Tegelijkertijd duiken er steeds meer veilingen op voor gestolen identiteiten en toegangspunten tot netwerken. Hackers maken gebruik van geavanceerde technieken zoals phishing en malware om gevoelige informatie te stelen. De druk op Europese landen neemt toe, zowel door digitale aanvallen als hybride dreigingen die fysieke infrastructuren destabiliseren. Europese samenwerking wordt essentieel voor het versterken van de verdediging tegen deze dreigingen.

LEES VERDER

Cloudflare storing, kwetsbaarheden in Chrome en ransomware uitdagingen vergroten digitale dreigingen in Europa

Een wereldwijde storing bij Cloudflare veroorzaakte de uitval van meerdere websites, waaronder die van Nederlandse media en platforms zoals X en ChatGPT. Tegelijkertijd kampten providers als Odido en Ziggo met technische storingen, die ook de zorgsector troffen. In Europa nam de dreiging van ransomware en andere cyberaanvallen toe, waarbij nieuwe kwetsbaarheden in Chrome en misbruik van e-mailspoofing werden aangewend voor phishingaanvallen. Verschillende hackergroepen, zoals Lazarus en UNC1549, richten zich op gevoelige sectoren, terwijl AI-tools in criminele netwerken de drempel voor aanvallen verlagen.

LEES VERDER

Fysieke sabotage en digitale spionage zetten Europese infrastructuur onder druk

Fysieke sabotage en digitale spionage hebben de Europese infrastructuur onder druk gezet, met zorginstellingen en bedrijven als doelwit. Een datalek bij Clinical Diagnostics heeft de gegevens van 850.000 vrouwen blootgesteld, terwijl ook ziekenhuizen en vervoersbedrijven werden getroffen door hackers. Cloudflare ondervond een storing die wereldwijd diensten verstoorde, terwijl beveiligingslekken in software en verouderde hardware zoals routers ernstige risico's met zich meebrengen. Nieuwe cyberaanvallen maken gebruik van AI en steganografie om malware onzichtbaar te verbergen, wat de dreiging vergroot. Internationale politieacties hebben geleid tot het neerhalen van hostingnetwerken die door cybercriminelen werden gebruikt.

LEES VERDER

Miljardenclaim in routeroorlog en massaal misbruik van Amazon S3

TP-Link heeft een rechtszaak aangespannen tegen Netgear en eist miljarden schadevergoeding vanwege een vermeende smaadcampagne die de indruk wekte dat TP-Link routers door Chinese hackers waren gecompromitteerd. Dit heeft geleid tot aanzienlijke schade. Tegelijkertijd wordt er massaal misbruik gemaakt van Amazon S3-buckets, waarbij criminelen misconfiguraties en klantbeheerde versleuteling gebruiken om gegevens te gijzelen met nieuwe ransomware-varianten. Deze aanvallen wijzen op een groeiende dreiging van gerichte cyberaanvallen en misbruik van cloudopslag door kwaadwillenden.

LEES VERDER

Digitale belegering en de stille opmars van onzichtbare dreigingen

Het dreigingslandschap wordt steeds complexer met gerichte aanvallen op detailhandel, industrie en vitale infrastructuren. Ransomwarebendes richten zich op e-commerce en verkooppunten, terwijl in Italië documenten van de spoorwegen op het darkweb terechtkwamen. Cybercriminelen misbruiken AI voor malware, en er ontstaan nieuwe spionagecampagnes zoals die van APT24. Ook kwetsbaarheden in populaire software zoals Windows Server Update Services en Vue.js worden actief misbruikt. Politieke zorgen over de digitale soevereiniteit nemen toe, met grote focus op het beheer van kritieke overheidsgegevens.

LEES VERDER

Wormer / Amsterdam - Bankhelpdeskfraude

In Wormer en Amsterdam werd een complexe vorm van bankhelpdeskfraude gepleegd waarbij criminelen psychologische manipulatie toepasten om bankpassen te stelen. Het begon met een sms-bericht waarin het slachtoffer werd gevraagd de bank te bellen. Na een gesprek met een zogenaamd bankmedewerker, stond een

koerier met een 'geheime code' voor de deur om de pas en pincode op te halen. De criminelen gebruikten deze gegevens om onmiddellijk €18.000 te besteden in een warenhuis. Deze hybride aanval combineert digitale en fysieke fraudetechnieken.

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