Cybercrimeinfo

"Omdat wat waardevol is, beschermd moet worden"

Nieuwsbrief 396

Ben jij op de hoogte van de digitale frontlinie van week 50? Doe de test!

De afgelopen week heeft opnieuw bewezen dat het digitale landschap razendsnel verandert, waarbij geopolitiek conflict en cybercriminaliteit dwars door elkaar lopen. Terwijl de Oekraïense inlichtingendienst een verwoestende slag toebrengt aan de Russische logistieke reus Eltrans+ (waarbij 700 servers sneuvelden), zien we dichter bij huis hoe de groep NoName Belgische instellingen zoals de KU Leuven en Stad Antwerpen bestookt.

Maar de dreiging is niet alleen militair. Weet jij welke risico's er schuilen in moderne ontwikkelomgevingen nu de 'IDEsaster' kwetsbaarheden in AI tools zijn blootgelegd en hackers de VS Code Marketplace overspoelen met malafide extensies? Ook onze privacy staat onder druk: van de zorgen rondom de Cloud Act nu Kyndryl het beheer van DigiD overneemt, tot de VS die socialemediaprofielen wil eisen voor een ESTA aanvraag.

Beschik jij over de technische kennis om te begrijpen hoe Makop ransomware legitieme drivers misbruikt, of waarom MITRE Cross-site scripting (XSS) heeft uitgeroepen tot het grootste gevaar van 2025? Test of jij weet hoe de Britse marine internetkabels beschermt met 'Atlantic Bastion' en of je op de hoogte bent van de React2Shell kwetsbaarheid die nog honderden Nederlandse IP-adressen raakt. Duik in de details, van EtherRAT tot Amazon fraude, en ontdek hoe weerbaar jij bent in deze Wekelijkse Digitale Weerbaarheid Quiz.

QUIZ 50-2025

Strategisch Dreigingsrapport Cyberveiligheid week 50-2025

Het cyberdreigingslandschap is geëvolueerd naar een intens verhard digitaal slagveld, waar de scheidslijn tussen financieel gemotiveerde cybercriminaliteit en staatssponsoring steeds vager wordt. Deze convergentie creëert een gevaarlijke mix van ransomware en sabotage die vitale sectoren en logistieke ketens treft, met verstrekkende maatschappelijke gevolgen. Cyberaanvallen zijn inmiddels integraal onderdeel van geopolitieke conflicten, waarbij landen zoals Nederland en België direct worden beïnvloed.

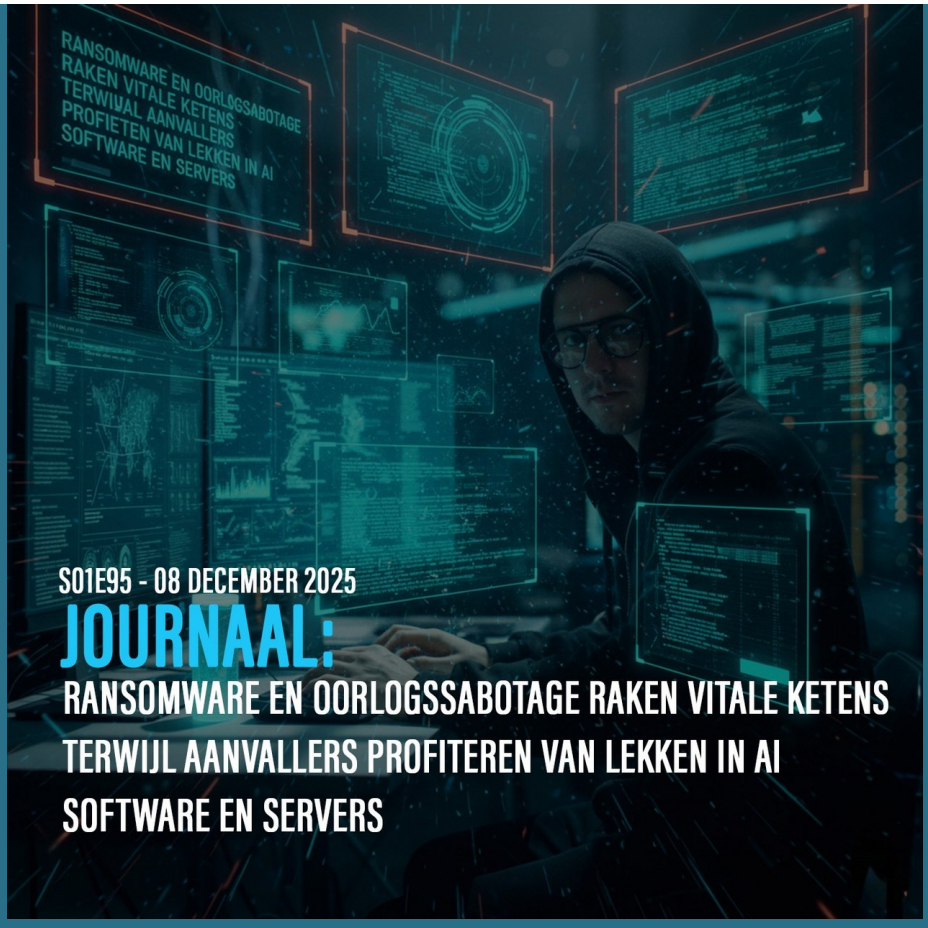
In de geopolitieke dimensie van cyberdreigingen wordt cyberspace steeds meer ingezet als wapen in staatsconflicten. Het Oekraïneconflict illustreert hoe cyberaanvallen gecombineerd worden met fysieke operaties om de soevereiniteit van landen te ondermijnen. Statelijke actoren zoals Noord-Korea, Rusland, China en Iran gebruiken cyberoperaties voor spionage en destabilisatie van geopolitieke rivalen. In de strijd om vitale infrastructuur, zoals onderzeese internetkabels en spoorwegen, worden geavanceerde defensieprogramma's zoals het "Atlantic Bastion" opgezet om sabotage te voorkomen.

De trend van ransomware en de exploitatie van softwarekwetsbaarheden vormt een groeiend risico. Groeperingen zoals Qilin en Clop misbruiken kwetsbaarheden in systemen, met name in de zorg- en financiële sector, wat leidt tot aanzienlijke economische schade. Daarnaast maken aanvallers gebruik van steeds geavanceerdere technieken om detectie te omzeilen en diep in systemen door te dringen.

Cybercriminaliteit heeft inmiddels niet alleen financiële en operationele gevolgen, maar heeft ook directe fysieke impact op burgers, bijvoorbeeld in de vorm van fraude en geweld. De recente DDoS-aanvallen in België onderstrepen de intentie van groepen als NoName om de publieke infrastructuur van landen te verstoren.

Als antwoord op deze bedreigingen is het van essentieel belang om digitale weerbaarheid als nationale veiligheidsprioriteit te behandelen. Dit vraagt om een geïntegreerde aanpak, waarbij samenwerking tussen overheden, inlichtingendiensten en de private sector cruciaal is. De noodzaak voor digitale soevereiniteit en proactieve investeringen in technologie, kennisontwikkeling en internationale samenwerking zijn essentieel om de digitale veiligheid in een steeds complexer wordende wereld te waarborgen.

RAPPORT 50-2025



Ransomware en oorlogssabotage raken vitale ketens terwijl aanvallers profiteren van lekken in AI software en servers

Het digitale dreigingslandschap wordt momenteel getekend door een intensivering van zowel criminele ransomware campagnes als geopolitieke cybersabotage. Groeperingen zoals Clop en Qilin richten zich agressief op vitale sectoren, waarbij gevoelige gegevens worden buitgemaakt en systemen wereldwijd worden versleuteld. Daarnaast vormen ernstige kwetsbaarheden in veelgebruikte AI ontwikkeltools en serversoftware een acuut risico voor organisaties, waarbij specifiek in de Benelux honderden systemen gevaar lopen door ongepatchte lekken. Deze dreiging wordt versterkt door de verkoop van geautomatiseerde aanvalstools en grootschalige inlogpogingen op VPN netwerken.
Een opmerkelijke wending in het criminele circuit is het lekken van de echte IP adressen van diverse darkweb markten naar het openbare internet, wat hun anonimiteit opheft. Op het vlak van hybride oorlogsvoering zijn logistieke ketens het doelwit van destructieve hacks, terwijl academische instellingen in Rusland blijken bij te dragen aan militaire technologie en fraude. De situatie wordt verder gecompliceerd door oplopende spanningen tussen grote techplatformen en Europese toezichthouders, evenals de uitdagingen voor Europa om strategisch onafhankelijk te worden op het gebied van kritieke grondstoffen en technologische kennis.

LEES VERDER

Fysieke sabotage van spoorlijnen en digitale ontwrichting vormen explosieve cocktail

De grens tussen fysieke sabotage en digitale oorlogsvoering vervaagt steeds meer, wat leidt tot een verhoogde dreiging voor vitale infrastructuren in Nederland en België. Dit werd recent zichtbaar door grootschalige DDoS aanvallen op Belgische overheidsdiensten en de aanhoudende wereldwijde financiële schade door ransomware en beleggingsfraude. Technologisch vernuft speelt een sleutelrol bij deze dreigingen; zo maken spywareleveranciers gebruik van onbekende kwetsbaarheden in mobiele telefoons en worden cloudomgevingen en softwareontwikkeltools steeds vaker gecompromitteerd door hackers. Daarnaast manifesteren statelijke actoren en criminele groepen zich via geavanceerde spionagecampagnes en de inzet van drones als vliegende computers.
Op juridisch en militair vlak wordt hard teruggeslagen tegen deze hybride dreigingen. Er is een internationaal verzoek ingediend voor de opsporing van saboteurs van spoorlijnen en er is succes geboekt in de aanpak van criminele netwerken die geweld als dienst aanbieden. Tevens zet de Britse marine in op autonome systemen en kunstmatige intelligentie om kwetsbare internetkabels op de zeebodem te beschermen tegen buitenlandse spionage. Op het gebied van privacy en digitalisering worden stappen gezet met de aanstaande introductie van een volledige digitale identiteitskaart in België en strengere Europese eisen die techplatforms dwingen gebruikers meer controle te geven over hun dataverzameling.

LEES VERDER

Digitale sabotage in havens en universiteiten naast diplomatieke spanningen

De afgelopen periode werd gekenmerkt door een reeks digitale verstoringen die vitale infrastructuren in de Benelux en daarbuiten raakten, variërend van DDoS aanvallen op Belgische instellingen tot grootschalige datalekken in Azië. Tegelijkertijd maken statelijke actoren misbruik van kritieke kwetsbaarheden in veelgebruikte bedrijfssoftware om geavanceerde malware te verspreiden en netwerken te infiltreren. Het criminele landschap evolueert met nieuwe tactieken zoals misleiding via legitieme ontwikkelaarstools en gerichte aanvallen op de maritieme sector, terwijl opsporingsdiensten terugslaan met fysieke arrestaties en innovatieve wervingscampagnes. De verwevenheid van digitale dreigingen met geopolitieke conflicten wordt zichtbaar in zowel de fysieke oorlogsvoering als de toenemende online radicalisering. Op beleidsniveau trachten overheden grip te krijgen op deze ontwikkelingen door middel van privacyhandhaving, regulering van technologie en juridische procedures tegen dominante techbedrijven.

LEES VERDER

Wereldwijde spionagecampagnes en kritieke lekken in vitale software domineren het nieuws

Het actuele cyberlandschap wordt gekenmerkt door een mix van inventieve fraude, kritieke kwetsbaarheden in software en aanhoudende geopolitieke spanningen. Criminelen wisten via manipulatie van logistieke systemen aanzienlijke bedragen buit te maken bij een groot e-commercebedrijf, terwijl consumenten en zakelijke gebruikers doelwit waren van geavanceerde phishingcampagnes en datalekken door systeemfouten. IT afdelingen staan onder druk door een grote hoeveelheid noodzakelijke beveiligingsupdates voor veelgebruikte software en hardware, waarbij diverse ernstige lekken al actief worden misbruikt door aanvallers.
De financiële sector en vitale infrastructuur worden bedreigd door steeds complexere malware en ransomware die specifiek ontworpen zijn om detectie te ontwijken en authenticatieprocessen te omzeilen. Tegenover deze digitale dreigingen staan successen van opsporingsdiensten, waaronder arrestaties en strafeisen in zaken rondom helpdeskfraude, ddos aanvallen op alarmnummers en de diefstal van persoonsgegevens. Op internationaal niveau blijven statelijke actoren zich roeren met digitale spionage gericht op de persvrijheid en pogingen om westerse sancties te ontduiken ten behoeve van militaire productie. Binnen de overheid en wetenschap wordt intussen gedebatteerd over digitale soevereiniteit, waarbij de balans wordt gezocht tussen innovatie, zoals digitale identiteitswallets en kwantumtechnologie, en de risico's van afhankelijkheid van buitenlandse techbedrijven.

LEES VERDER

Digitale soevereiniteit onder druk door spionagecampagnes en falende beveiliging

Het digitale landschap wordt momenteel gedomineerd door een combinatie van toenemende cybercriminaliteit, technische kwetsbaarheden en geopolitieke spanningen. Burgers en organisaties ondervinden directe schade door geraffineerde emailhacks en datalekken bij grote dienstverleners zoals LastPass, terwijl privacyzorgen toenemen door de overgang van het DigiD beheer naar een Amerikaans bedrijf en strengere eisen voor reizigers naar de Verenigde Staten. Tegelijkertijd kampen ontwikkelaars met ernstige beveiligingslekken in essentiële software zoals Notepad++, Docker en Google Chrome, die actief worden misbruikt door kwaadwillenden.

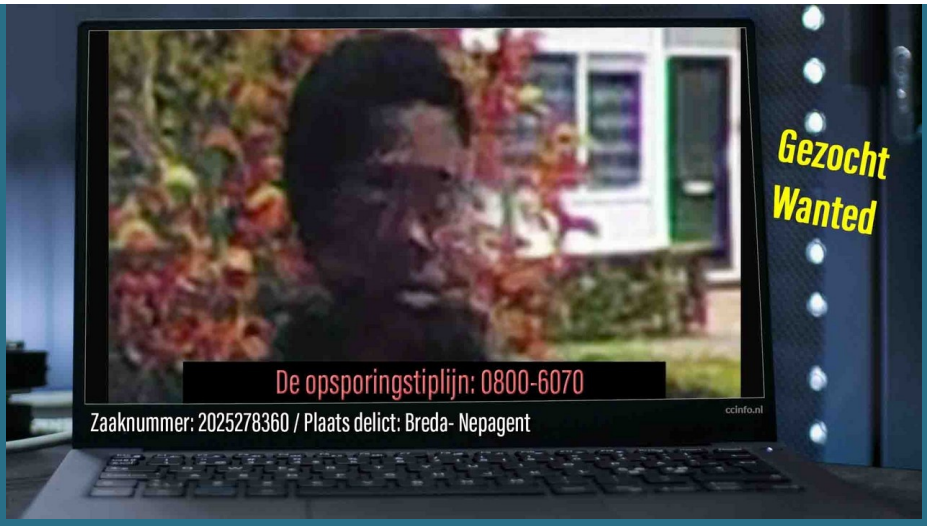
Criminelen innoveren hun aanvalsmethoden door misbruik te maken van legitieme cloudinfrastructuur en de populariteit van kunstmatige intelligentie, waarbij malware wordt verspreid via gemanipuleerde advertenties en chatdiensten. Op het wereldtoneel manifesteren deze dreigingen zich in spionagecampagnes door statelijke actoren uit onder meer Iran en DDoS aanvallen op Belgische gemeenten, wat Europa aanzet tot het nastreven van meer digitale autonomie. Hoewel er stappen worden gezet in de beveiliging en opsporing, zoals de uitbreiding van bug bounty programma's en lokale arrestaties, lopen structurele oplossingen zoals een online aangifteportaal voor ransomware vertraging op.

LEES VERDER

Digitale escalatie raakt vitale infrastructuur en geopolitieke verhoudingen

De digitale veiligheid in België en Nederland staat onder druk door diverse aanvallen, waaronder gijzelsoftware bij een Belgisch tankstationbedrijf en DDoS aanvallen op grote telecom- en energieproviders. Daarnaast werd een Nederlandse cryptomiljonair in het buitenland slachtoffer van dodelijk geweld door een criminele bende. Wereldwijd vormen ernstige kwetsbaarheden in software zoals GeoServer, React en Windows een acuut risico, terwijl hackersgroepen zoals Lazarus en CyberVolk hun methoden professionaliseren via automatisering en het hergebruik van oude infrastructuren. Phishingcampagnes worden steeds geavanceerder en slagen erin om multifactor authenticatie te omzeilen, terwijl infostealers via advertenties inloggegevens buitmaken. Op geopolitiek vlak lopen de spanningen op, waarbij Duitsland Rusland beschuldigt van digitale sabotage en zowel de NAVO als het Verenigd Koninkrijk waarschuwen voor een verslechterende veiligheidssituatie. Tot slot is er een maatschappelijke discussie gaande over de balans tussen privacy en veiligheid, aangewakkerd door de wens van Europol om versleuteling te doorbreken en zorgen over nieuwe wetgeving rondom AI en bankcontrole.

LEES VERDER



Breda - Nepagent

In Breda heeft een oplichter zich voorgedaan als politieagent en een vrouw opgelicht door zich aan te bieden als wijkagent voor een veiligheidsinspectie. Door het vertrouwen in autoriteit te misbruiken, wist de oplichter de vrouw te overtuigen haar binnen te laten, waarna hij geld en sieraden stal. De zaak benadrukt hoe oplichters gebruik maken van emotionele manipulatie en autoriteitsmisbruik. De politie adviseert om altijd eerst te verifiëren of een bezoek van een officiële instantie legitiem is.

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