Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

08-11-2025:

Oekraïne bouwt de eerste 'AI Staat' te midden van oorlog

Tijdens de WINWIN Summit in Kyiv werd een visionair plan gepresenteerd om Oekraïne de eerste "agentische staat" te maken, een overheid aangedreven door kunstmatige intelligentie (AI) die niet alleen reageert op verzoeken van burgers, maar deze proactief anticipeert. Oekraïne streeft ernaar om tegen 2030 tot de top drie landen te behoren in de integratie van AI in de publieke sector. Dit ambitieuze plan is geboren uit de digitale transformatie die is versneld door de oorlog, waarbij Oekraïne al indrukwekkende vooruitgangen heeft geboekt, zoals het digitale platform Diia en digitale ID’s voor vluchtelingen. Partnerschappen met techgiganten zoals Google, NVIDIA, en OpenAI ondersteunen Oekraïne in deze AI-transformatie. Dit plan gaat verder dan software, met focus op technologische soevereiniteit en infrastructuur, waaronder een eigen AI-model in de Oekraïense taal en de ontwikkeling van de halfgeleiderindustrie.

DDoS-aanval (Server Killers) gericht op meerdere Belgische websites

Op 7 november 2025 claimde de hackergroep SERVER KILLERS meerdere DDoS-aanvallen op verschillende websites in België. De doelwitten omvatten onder andere de federale overheidswebsite FPS Economy, de telecombedrijven VOO en edpnet, evenals financiële instellingen zoals Banque CPH en Europabank. Ook de Rijksdienst voor Sociale Zekerheid, D'Ieteren Group, Elia Group en de haven van Zeebrugge werden getroffen. Deze aanvallen veroorzaken verstoringen in de beschikbaarheid van de getroffen diensten. De grootschalige aanval heeft gevolgen voor zowel de publieke als de private sector in België.

NoName voert DDoS-aanvallen uit op websites in België

NoName, een bekende cyberdreigingsgroep, heeft verklaard websites in België en Zweden te hebben aangevallen via gedistribueerde denial-of-service (DDoS) aanvallen. De getroffen sites in België omvatten de Antwerp Low Emission Zone (LEZ), het platform Slim naar Antwerpen, LEZ Brussels, de gemeente Linkebeek en de stad Lo-Reninge. Ook de Zweedse website Alimak werd doelwit. DDoS-aanvallen worden vaak gebruikt om websites tijdelijk offline te halen door een overbelasting van verkeer te veroorzaken, wat de getroffen organisaties belemmert in hun online

activiteiten. Er zijn momenteel geen meldingen van ernstige schade of gegevensverlies, maar de aanvallen kunnen aanzienlijke verstoringen veroorzaken voor zowel overheids- als commerciële diensten. Het is nog niet duidelijk of NoName andere doelwitten in de regio heeft getroffen.

DDoS-aanval op onss.be geclaimd door HEZI RASH

Op 7 november 2025 heeft de groepering HEZI RASH beweerd de website van het Belgische Office national de Sécurité sociale (onss.be) te hebben aangevallen met een DDoS-aanval. Ondanks de claim is de website op het moment van berichtgeving nog steeds actief en operationeel. Deze melding komt op een moment dat de website geen zichtbare verstoringen vertoont, maar de dreiging van DDoS-aanvallen blijft een relevante kwestie voor de beveiliging van overheidswebsites en publieke diensten.

NoName057 voert DDoS-aanval uit op Belgische militaire inlichtingendienst ADIV

Op 6 november 2025 heeft het pro-Russische hackerscollectief NoName057 een DDoS-aanval uitgevoerd op de websites van de Belgische militaire inlichtingendienst ADIV. De aanval werd diezelfde dag opgeëist via een bericht op Telegram. De hackers verwezen naar uitspraken van de Belgische defensieminister over Rusland, wat mogelijk de motivatie voor de aanval was. Het doel van de aanval was om de websites onbereikbaar te maken door servers te overbelasten met verzoeken. De impact was echter beperkt, en er werden geen gegevens gestolen of gevoelige informatie benaderd. De websites waren kortstondig onbereikbaar, maar zijn inmiddels weer volledig operationeel. Defensie bevestigde de aanval, maar meldde dat er geen verdere schade was. Er wordt verwacht dat NoName057 in de toekomst meer aanvallen zal uitvoeren, aangezien ze aangeven een nieuwe campagne tegen België te zijn gestart.

Nederland bereid om controle over Nexperia op te geven als chiplevering herstart

Nederland overweegt om zijn controle over de Chinese chipmaker Nexperia op te heffen, mits de leveringen van essentiële chips uit China weer op gang komen. Dit besluit zou de gespannen verhouding met China kunnen de-escaleren, die de wereldwijde autoproductie beïnvloedt. Het ministerie van Economische Zaken

verklaarde dat het ministerieel besluit dat de Nederlandse overheid invloed gaf op Nexperia mogelijk wordt opgeschort als de chipexport naar Europa herstart. Dit besluit volgde op een machtsconflict tussen Nederland en China over de controle van het bedrijf. De levering van Nexperia's chips, essentieel voor autofabrikanten zoals BMW en Volkswagen, werd belemmerd door een exportverbod vanuit China. De hoop is dat de levering van chips snel hersteld kan worden, wat de druk op de autofabrikanten vermindert.

China's hackers benutten oude kwetsbaarheden voor wereldwijde spionage

China-geassocieerde hackers hebben in april 2025 meerdere CVE-kwetsbaarheden misbruikt om langdurige toegang te verkrijgen tot netwerken van een Amerikaanse non-profitorganisatie. Dit maakte onderdeel uit van bredere aanvallen gericht op organisaties die betrokken zijn bij Amerikaanse overheidsbeleid. De aanvallen werden uitgevoerd met bekende kwetsbaarheden zoals CVE-2021-44228 (Apache Log4j) en CVE-2022-26134 (Atlassian), die gebruikmaakten van massale scantechnieken om toegang te verkrijgen. Na toegang werden er programma's geïnstalleerd om toegang te behouden, waaronder een zelfgemaakte loader die mogelijk een remote access trojan (RAT) activeerde. Deze aanvallen zijn een voorbeeld van China's voortdurende cyberactiviteiten om mondiale doelen te ondersteunen via geavanceerde cyberinfiltraties en tools zoals TOLLBOOTH en Mimikatz. Dergelijke aanvallen benadrukken de geavanceerde en persistente methoden van Chinese hackers, die wereldwijd opereren met diverse malwaretechnieken.

Cavalry Werewolf valt Russische overheidsorganisaties aan voor netwerktoegang via backdoor

In juli 2025 voerde de hacker-groep Cavalry Werewolf een gerichte campagne uit tegen Russische overheidsinstellingen door middel van phishing-aanvallen. Het doel was het verkrijgen van persistente netwerktoegang, het stelen van gevoelige gegevens en het handhaven van langdurige controle over de getroffen systemen. De aanvallen werden geïdentificeerd door beveiligingsanalisten van Dr.Web, nadat een overheidsorganisatie verdachte e-mailverkeer detecteerde. De aanvallers gebruikten verschillende malwarevarianten, waaronder backdoors en trojans voor gegevensdiefstal, die via een multi-stage infectieproces werden verspreid. De

malware werd vaak geïnstalleerd via geëncrypteerde e-mailbijlagen die als officiële documenten vermomd waren. Deze geavanceerde aanvalsmethoden maakten gebruik van open-source tools en legitieme systeemtools om onopgemerkt te blijven en de operationele beveiliging te handhaven. De aanval werd beschouwd als een escalatie in de methoden van de groep, die hun toolkit steeds verder uitbreiden.

QNAP verhelpt zeven zero-day kwetsbaarheden na exploitatie tijdens Pwn2Own

QNAP heeft zeven zero-day kwetsbaarheden verholpen die tijdens de Pwn2Own 2025 competitie in Ierland werden misbruikt om netwerk-opslagapparaten (NAS) van het bedrijf te hacken. De kwetsbaarheden betroffen de besturingssystemen QTS en QuTS Hero, evenals verschillende QNAP-applicaties, zoals Hyper Data Protector en Malware Remover. Het exploiteren van deze kwetsbaarheden werd gedemonstreerd door diverse teams van onderzoekers. QNAP heeft updates uitgebracht voor de getroffen softwareversies en raadt gebruikers aan hun apparaten regelmatig bij te werken en wachtwoorden te veranderen voor extra beveiliging. Gebruikers kunnen de updates installeren via het Controlepaneel of de App Center in QTS en QuTS Hero.

Kritieke SQL-injectie kwetsbaarheid in Django vereist onmiddellijke patch

Op 7 november 2025 werd een kritieke SQL-injectie kwetsbaarheid (CVE-2025-64459) in het populaire webtoepassingsframework Django bekendgemaakt. Deze kwetsbaarheid, die voorkomt in versies voor 5.2.8, 5.1.14 en 4.2.26, stelt aanvallers in staat ongeauthenticeerde SQL-injectie-aanvallen uit te voeren op databases die door Django-applicaties worden gebruikt. Het probleem ontstaat wanneer gebruikersinvoer via dynamische SQL-query’s wordt verwerkt zonder voldoende controle, waardoor aanvallers de mogelijkheid hebben om ongeoorloofde toegang te krijgen, gegevens te wijzigen of zelfs databaseaccounts over te nemen. De kwetsbaarheid heeft een hoge CVSS-score van 9.1 en kan aanzienlijke gevolgen hebben voor de vertrouwelijkheid en integriteit van gegevens. Het wordt sterk aanbevolen om de software te upgraden naar de nieuwste versies om verdere risico’s te vermijden.

Politie waarschuwt voor nepmails over zogenaamde arrestatieprocedure

De politie heeft een waarschuwing uitgebracht voor nepmails die zogenaamd afkomstig zijn van de Eenheid Landelijke Opsporing en Interventies (LO). In de e-mails wordt gesteld dat er een onderzoek is ingesteld naar de ontvanger wegens seksuele strafbare feiten, die digitaal en grensoverschrijdend zouden zijn gepleegd. Tevens wordt beweerd dat er een arrestatiebevel tegen de ontvanger loopt. Ontvangers worden gevraagd persoonlijke informatie te verstrekken. De politie benadrukt dat dit een phishingpoging betreft en waarschuwt mensen om de e-mail onmiddellijk te verwijderen en melding te maken bij de Fraudehelpdesk. Tevens wordt erop gewezen dat de politie nooit op deze manier contact opneemt met burgers en enkel e-mails verstuurt van adressen die eindigen op @politie.nl.

Samsung Galaxy-telefoons via kritiek lek geïnfecteerd met Android-spyware

Aanvallers hebben een ernstig beveiligingslek in Samsung Galaxy-telefoons misbruikt om Android-spyware, genaamd Landfall, te installeren. Dit gebeurde via een kwetsbaarheid in de verwerking van DNG-afbeeldingen, gedocumenteerd als CVE-2025-21042. Het lek werd in 2024 ontdekt en een update werd pas in april 2025 beschikbaar. De spyware werd voornamelijk gebruikt in landen in het Midden-Oosten, zoals Turkije, Marokko, Iran en Irak. De aanvallers verstuurden speciaal aangepaste afbeeldingen via WhatsApp, die bij opening het lek benutten om de spyware te installeren. De spyware kan onder andere de microfoon van de telefoon inschakelen, de locatie van het slachtoffer volgen en gevoelige gegevens zoals foto's en berichten verzamelen. Palo Alto Networks ontdekte de aanval nadat vergelijkbare kwetsbaarheden ook in andere platformen, zoals iOS, werden gebruikt. Er is geen bewijs dat dezelfde aanvaller verantwoordelijk is voor de aanvallen op zowel Android- als iOS-apparaten.

Cisco waarschuwt voor actief misbruik van kwetsbaarheden in firewalls: 591 in Nederland en 86 in België ❗

Cisco heeft gewaarschuwd voor twee kwetsbaarheden in ASA- en FTD-firewalls die actief misbruikt worden in zero-day aanvallen. De kwetsbaarheden, CVE-2025-20333 en CVE-2025-20362, stellen aanvallers in staat om op afstand toegang te krijgen tot beperkte URL-eindpunten zonder authenticatie, en zelfs om op kwetsbare apparaten code uit te voeren. Deze kwetsbaarheden kunnen in combinatie worden gebruikt, waardoor aanvallers volledige controle krijgen over niet-gepatchte systemen. Cisco

heeft al beveiligingsupdates uitgebracht, maar veel apparaten zijn nog niet geüpdatet. CISA heeft een spoedmaatregel genomen, waarbij Amerikaanse federale overheidsinstanties binnen 24 uur hun Cisco firewalls moesten beveiligen tegen deze aanvallen. Shadowserver volgt momenteel meer dan 34.000 internet-verbonden, kwetsbare apparaten. Van deze apparaten bevinden zich 591 in Nederland en 86 in België. Deze aanvallen worden gekoppeld aan de ArcaneDoor-campagne, die eerder al andere zero-day kwetsbaarheden in Cisco firewalls misbruikte.

Malafide NuGet-pakketten bevatten destructieve 'tijdklokken'

Op NuGet, een open-source pakketmanager voor .NET, zijn verschillende kwaadaardige pakketten aangetroffen die sabotage-payloads bevatten, die zijn geprogrammeerd om in 2027 en 2028 te activeren. Deze payloads richten zich voornamelijk op database-implementaties en Siemens S7 industriële controleapparaten. Het kwaadwillige code maakt gebruik van een probabilistische trigger, waardoor de activering afhankelijk is van specifieke parameters op het geïnfecteerde apparaat. De meest gevaarlijke is het pakket Sharp7Extend, dat de communicatie met Siemens PLC's saboteert door het stoppen van Ethernet-communicatie of het corrupt maken van gegevens. De aanval heeft meerdere lagen, met zowel onmiddellijke als vertraagde verstoringen. Het is nog niet duidelijk wie er achter de aanval zit, maar organisaties wordt aangeraden om hun systemen te controleren op de getroffen pakketten.

Valse 0-day-exploit e-mails misleiden crypto-gebruikers

Een nieuwe scam richt zich op cryptocurrency-gebruikers door hen te misleiden met valse 0-day-exploit e-mails. Deze e-mails beweren een winstgevende methode te bieden via een "0-day glitch" en verzoeken gebruikers om een stuk JavaScript-code in hun browser in te voeren. Dit stukje code haalt vervolgens een groter, verborgen programma op dat de browsercontrole overneemt. De code manipuleert de weergegeven informatie, zoals winstpercentages, en zorgt ervoor dat betalingen naar de wallet van de aanvallers worden omgeleid. De scam is goed georganiseerd en heeft zich verspreid via privé cybercrime-forums. Onderzoekers waarschuwen dat gebruikers voorzichtig moeten zijn met het invoeren van onbekende code in hun browser en benadrukken de rol van hebzucht en urgentie in het succes van deze aanvalsmethode.

Fraudeaanval besmet Booking.com-gebruikers via PureRAT malware

Criminelen hebben een grootschalige fraudeoperatie opgezet waarbij hotelreserveringssystemen zoals Booking.com en Expedia zijn aangevallen. Via een phishingaanval ontvangen hotelmedewerkers een e-mail die een link bevat naar een malware-installatie, genaamd PureRAT, die hen toegang geeft tot de reserveringssystemen van hotels. De malware steelt inloggegevens, die vervolgens worden verkocht op het dark web. Zodra de aanvallers toegang hebben tot een echt Booking.com-account, nemen ze contact op met hotelgasten en informeren hen over vermeende betalingsproblemen. Gasten worden naar een valse website geleid om bankgegevens te stelen. Het kwaadwillende systeem heeft al honderden schadelijke domeinen geïdentificeerd en richt zich op een breed scala aan reis- en horecabedrijven. Deze goed georganiseerde fraudemodel blijft veel slachtoffers maken, zowel bij hotels als gasten.

Malicious npm packages deliver Vidar malware through supply chain attack

Tussen 21 en 26 oktober 2025 werd een geavanceerde supply chain-aanval ontdekt waarbij kwaadaardige npm-pakketten werden gebruikt om Vidar infostealer malware te verspreiden naar Windows-systemen. In totaal werden 17 pakketten met 23 releases gepubliceerd, die als legitiem ogende tools, zoals Telegram-bots en icon libraries, werden vermomd. Deze pakketten werden meer dan 2.240 keer gedownload voordat ze uit de registry werden verwijderd. De aanvallers maakten gebruik van twee nieuwe npm-accounts, aartje en saliii229911, en plaatsten code die automatisch schadelijke scripts uitvoerde bij installatie. De malware verzamelde gevoelige informatie, waaronder wachtwoorden en cryptomunten, en exfiltreerde deze naar command-and-control servers. Deze aanval benadrukt de kwetsbaarheden in de npm-ecosysteem en toont aan hoe makkelijk het is voor kwaadwillende actoren om ontwikkelaars te misleiden door gebruik te maken van vertrouwde pakketten.

Nieuwe Android-malware ‘Fantasy Hub’ onderschept SMS-berichten en persoonlijke gegeven

Een nieuwe Android-malware, genaamd Fantasy Hub, is ontdekt. Deze malware, ontwikkeld door Russische dreigingsactoren, wordt verspreid als een Malware-as-a-Service (MaaS) en is gericht op het stelen van persoonlijke gegevens van slachtoffers. Fantasy Hub stelt aanvallers in staat om SMS-berichten, contacten en oproeplogs te onderscheppen, en zelfs twee-factor-authenticatiecodes te stelen. De malware richt zich voornamelijk op financiële instellingen en maakt gebruik van geavanceerde technieken om detectie door beveiligingssoftware te omzeilen. Gebruikers die het slachtoffer worden van deze malware kunnen hun bankgegevens, zoals inloggegevens, verliezen. De verspreiding van de malware gebeurt via Telegram-kanalen, waar criminelen zich abonneren op de dienst en toegang krijgen tot de malware. Fantasy Hub maakt gebruik van versleuteling en andere maatregelen om onopgemerkt te blijven en zijn werking uit te voeren.

LockBit 5.0 introduceert geavanceerde functionaliteiten en twee-fasen uitvoeringsmodel

LockBit 5.0, gelanceerd in september 2025, brengt belangrijke upgrades voor de beruchte ransomware-as-a-service groep. Het nieuwe model bouwt voort op de versie 4.0 codebase, maar introduceert een modulair ontwerp dat gericht is op het verhogen van de evasiecapaciteiten, de destructieve impact en de persistentie binnen netwerken. Een opvallende verbetering is het twee-fasen uitvoeringsmodel, waarbij de infectie wordt opgesplitst in een loader- en payload-fase. De loader is ontworpen voor stealth en anti-analyse, en gebruikt complexe obfuscatie om de uitvoering van de malware te verbergen. Deze benadering maakt het moeilijker voor beveiligingstools om de aanval te detecteren en te stoppen. Het gebruik van API-hashing en procesinjectie zorgt ervoor dat LockBit 5.0 effectief kan voortbestaan, zelfs wanneer beveiligingsmechanismen ingrijpen. Deze nieuwe versie van LockBit bevestigt de reputatie van de groep als een van de meest gevreesde ransomware-bedreigingen in het huidige landschap.

Herodotus Android Banking Malware neemt volledige controle over apparaten en ontwijkt antivirussoftware

De Herodotus Android-banktrojan is een geavanceerde dreiging die Android-gebruikers wereldwijd treft. Het malwareprogramma wordt verspreid via SMS-phishing en vermomt zich als een legitiem hulpmiddel, wat gebruikers misleidt om

een APK-bestand buiten de officiële Play Store te downloaden en te installeren. Zodra het op een apparaat is geïnstalleerd, krijgt de trojan toegang tot belangrijke systeemrechten en kan het banktransacties uitvoeren namens de getroffen gebruiker. Dit vormt een zorgwekkende evolutie van mobiele malware, omdat het nauwelijks detecteerbaar is door traditionele antivirussoftware, ondanks zijn kwaadaardige intenties. Het malwareprogramma gebruikt geavanceerde technieken om automatische detectie te vermijden, zoals het 'humaniseren' van schadelijke acties door vertragingen en realistische typen. Het stelt aanvallers in staat om scherminhoud en toetsaanslagen in real-time te onderscheppen en bankgegevens te stelen.

Hackers kunnen Active Directory-sites aanvallen om privileges te escaleren en domeinen te compromitteren

Onderzoekers van Synacktiv hebben aangetoond dat aanvallers kwetsbaarheden in Active Directory-sites kunnen misbruiken om administratieve rechten te verkrijgen en domeinen te compromitteren. Active Directory-sites worden normaal gebruikt om de netwerkprestaties te optimaliseren door replicatie en authenticatie over verschillende locaties te beheren. De kwetsbaarheid ontstaat doordat deze sites gekoppeld kunnen worden aan Group Policy Objects (GPO’s), die systeeminstellingen regelen binnen een organisatie. Wanneer aanvallers schrijfrechten verkrijgen op deze sites of de bijbehorende GPO’s, kunnen zij schadelijke configuraties injecteren die alle verbonden systemen, inclusief domeincontrollers, compromitteren. Dit geeft aanvallers toegang tot domeinen zonder traditionele beveiligingsmaatregelen te activeren. De onderzoekers benadrukken dat dit aanvalspad vaak over het hoofd wordt gezien door organisaties, wat het een kritieke kwetsbaarheid maakt voor systemen met grote Active Directory-omgevingen.

Verdachte bankhelpdeskfraude aangehouden in Almere

Op 5 november 2025 is een 22-jarige man uit Amsterdam aangehouden op verdenking van bankhelpdeskfraude. De verdachte zou zich telefonisch hebben voorgedaan als een monteur van een internetbedrijf en de 71-jarige bewoonster van Baarn ervan hebben overtuigd om hem toegang te geven tot haar woning om zogenaamd virussen op haar apparaat te verwijderen. Tijdens het bezoek wist hij ongemerkt een groot geldbedrag van het slachtoffer over te maken. Nadat de vrouw

het verlies ontdekte, belde ze direct de politie. De verdachte werd dezelfde dag nog in Almere aangehouden. De politie waarschuwt voor dergelijke oplichtingspraktijken, waarbij oplichters proberen het vertrouwen van hun slachtoffers te winnen door zich voor te doen als betrouwbare hulpverleners.

Virusscanners voor Android getest op detectie van stalkerware

De EFF en AV-Comparatives hebben de effectiviteit van dertien virusscanners voor Android getest op het detecteren van stalkerware. Stalkerware zijn apps die op smartphones geïnstalleerd kunnen worden om slachtoffers op afstand te bespioneren. Het onderzoek toonde aan dat slechts één virusscanner, Malwarebytes, alle stalkerware-apps correct detecteerde. Google Play Protect, de standaardbeveiliging op veel Android-apparaten, miste 53% van de apps, terwijl Trend Micro slechts 59% van de apps detecteerde. Stalkerware kan ongemerkt op de achtergrond draaien en is moeilijk te verwijderen, vaak door blokkering van systeeminstellingen. Het rapport benadrukt dat gebruikers niet uitsluitend moeten vertrouwen op ingebouwde beveiliging en dat virusscanners duidelijke informatie en veilige verwijderingsopties moeten bieden. De opkomst van goedkopere bluetooth-trackers zoals Apple AirTags wordt genoemd als mogelijke vervanger voor traditionele stalkerware-apps.

Verplichte online leeftijdsverificatie in het VK vaak omzeild via VPN-verbindingen

De verplichte online leeftijdsverificatie die in het Verenigd Koninkrijk sinds enkele maanden van kracht is, wordt vaak omzeild door gebruikers via VPN-verbindingen, zo blijkt uit een verslag van de commissie Digitale Zaken van de Tweede Kamer. De verplichting, onderdeel van de Online Safety Act, heeft als doel de toegang tot bepaalde online inhoud te beperken voor minderjarigen. Hoewel steeds meer landen, zoals Spanje, Frankrijk en Denemarken, soortgelijke maatregelen overwegen, blijkt de implementatie in het VK niet volledig effectief. VPN-providers rapporteren een toename van gebruikers die de leeftijdsverificatie ontwijken. In reactie hierop waarschuwde de Britse toezichthouder Ofcom dat websites gebruikers niet mogen aanmoedigen om de controle te omzeilen. Daarnaast wordt er in Denemarken gewerkt aan een digitale identiteits-app die anoniem de leeftijd kan verifiëren.

Softwarebedrijf schikt voor datalek na gestolen login

Het Amerikaanse softwarebedrijf Illuminate Education heeft een schikking getroffen van 5,1 miljoen dollar na een datalek veroorzaakt door de gestolen inloggegevens van een ex-medewerker. Het incident vond plaats in 2021, waarbij de gegevens van miljoenen leerlingen, waaronder persoonlijke en medische informatie, werden gestolen. De aanvaller kreeg toegang tot het systeem via verouderde inloggegevens van de ex-medewerker en wist daarna de toegang te behouden door nieuwe inloggegevens aan te maken. Het bedrijf moet nu diverse beveiligingsmaatregelen doorvoeren, waaronder het verwijderen van inloggegevens van ex-medewerkers, het scheiden van actieve databases van back-ups, en het implementeren van real-time monitoring. Ook moeten scholen hun opgeslagen gegevens controleren en de bewaartermijn en verwijdering ervan nakijken.

EFF bezorgd over Google’s registratieverplichting voor Android-ontwikkelaars

De Electronic Frontier Foundation (EFF) uit zorgen over het plan van Google om app-ontwikkelaars te verplichten zich te registreren met persoonlijke gegevens, waaronder hun naam, adres en een kopie van hun legitimatiebewijs. Deze verplichting is bedoeld om te voorkomen dat kwaadaardige apps op Android-toestellen komen, maar de EFF waarschuwt dat dit kan leiden tot censuur en versterking van Google’s monopolie. De maatregelen zullen eerst in landen zoals Brazilië en Indonesië van kracht zijn, en wereldwijd uitgerold worden in 2027. De EFF stelt dat dergelijke registratievereisten de privacy van ontwikkelaars kunnen schaden en overheden toegang kunnen geven tot de data. Bovendien kan dit de concurrentie onderdrukken, vooral voor alternatieve appstores, zoals F-Droid, die vreest dat dit beleid hun voortbestaan bedreigt.

Waarschuwing voor verdachte link op Dread-site

Op 7 november 2025 werd via een melding op een openbaar platform gewaarschuwd voor een link die op de Dread-site op het darkweb werd gedeeld. De link leidt naar een mogelijk gevaarlijke pagina, waarvan de inhoud op dit moment onduidelijk is. De waarschuwing benadrukt de risico’s van verdachte links op het darkweb, die vaak verbonden zijn met cyberdreigingen zoals ransomware. Gebruikers wordt aangeraden uiterst voorzichtig te zijn met het openen van dergelijke links, gezien de mogelijke connectie met cybercriminaliteit. De melding

geeft aan dat de situatie nog in ontwikkeling is, maar legt de nadruk op de noodzaak van waakzaamheid.

Verkoop van WordPress-toolkit op het darkweb gesignaleerd

Op 7 november 2025 werd gemeld dat er een verkoop van een WordPress-toolkit plaatsvond op het darkweb. Deze toolkit bevat vermoedelijk hulpmiddelen die cybercriminelen kunnen helpen bij het misbruiken van kwetsbaarheden in WordPress-websites. De toolkit lijkt een waardevolle bron te zijn voor kwaadwillenden die zich richten op bekende platformen en open-source software zoals WordPress. Dergelijke tools kunnen worden gebruikt om aanvallen uit te voeren, websites over te nemen of gegevens te stelen. Het is een waarschuwing voor organisaties en website-eigenaren om de beveiliging van hun WordPress-sites te versterken.

Duitse hostingprovider Aurologic GmbH faciliteert kwaadaardige infrastructuur

De Duitse internetprovider Aurologic GmbH heeft zich gepositioneerd als een belangrijke speler binnen de wereldwijde infrastructuur voor cybercriminaliteit. Het bedrijf biedt netwerk- en datacenterdiensten aan risicovolle hostingnetwerken, waaronder verbindingen met hostingproviders die malware-commando-servers voor bekende malwarefamilies zoals Cobalt Strike en Amadey beheren. De infrastructuur van Aurologic is ook een belangrijke schakel voor gesanctioneerde entiteiten, waaronder de Aeza-groep, ondanks internationale sancties. Het bedrijf beschikt over een robuuste Europese interconnectie-infrastructuur en heeft datacenters in Duitsland, Finland en Nederland, wat zorgt voor snelle, redundante datatransmissie door Europa. Door zijn centrale rol biedt Aurologic continuïteit aan netwerken die betrokken zijn bij cybercriminaliteit, desinformatiecampagnes en malwareverspreiding, wat vragen oproept over de scheidslijn tussen technologische neutraliteit en actieve facilitering van cybercriminaliteit.

Singapore voegt lijfstraffen toe voor oplichters

Singapore heeft besloten om strengere maatregelen te nemen tegen online oplichters, die tussen 2020 en september 2025 bijna 3 miljard dollar aan schade veroorzaakten. In een nieuwe wet wordt een minimaal aantal van zes stokslagen

opgelegd aan mensen die zich schuldig maken aan fraude via afstandscommunicatie, zoals bijvoorbeeld valse online advertenties. De overheid heeft aangegeven dat de lijfstraffen ook van toepassing zullen zijn op zogenaamde 'mules', die fraudeurs helpen door bijvoorbeeld inloggegevens of SIM-kaarten aan te bieden. In sommige gevallen kan het aantal slagen oplopen tot 24. Deze maatregelen worden gezien als een manier om de opkomst van digitale oplichting tegen te gaan en de verantwoordelijken stevig te straffen. Het idee is om een sterkere afschrikking te creëren voor degenen die betrokken zijn bij de oplichtingsindustrie.

Meta verdient miljarden met frauduleuze advertenties

Uit interne documenten blijkt dat Meta in 2024 meer dan $16 miljard heeft verdiend met misleidende advertenties op Facebook en Instagram, wat ongeveer 10% van de totale jaarlijkse omzet van het bedrijf vertegenwoordigt. Gebruikers zouden dagelijks zo'n 15 miljard frauduleuze advertenties te zien krijgen, waaronder advertenties voor illegale producten, e-commerce oplichterijen en online casino's. Meta heeft wel maatregelen getroffen, zoals het verwijderen van 134 miljoen misleidende advertenties in 2025, maar de systemen die advertenties markeren als frauduleus werken alleen als er meer dan 95% zekerheid is. Lagere zekerheid leidt tot hogere advertentiekosten voor de adverteerders. De Amerikaanse SEC onderzoekt het bedrijf vanwege advertenties voor financiële oplichterijen. Meta verwacht boetes van $1 miljard, maar is bezorgd dat een scherpe afname van frauduleuze advertenties de bedrijfsresultaten zou kunnen beïnvloeden.