## Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

11-11-2025:

Data-inbraak bij Chinese cybersecurityfirma onthult staatsgesponsorde cyberwapens en doelwitlijst

Begin november 2025 werd bekend dat de Chinese cybersecurityfirma Knownsec slachtoffer werd van een grote datalek, waarbij meer dan 12.000 vertrouwelijke documenten werden blootgesteld. De documenten onthulden gedetailleerde informatie over staatsgesponsorde cyberoperaties, waaronder cyberwapens, interne hackingtools en een lijst van wereldwijde doelwitten. Het lek bevatte ook technische documentatie over de samenwerking van Knownsec met verschillende Chinese overheidsinstanties, evenals gegevens over al 80 buitenlandse doelwitten die al gecompromitteerd zouden zijn. De documenten, waaronder gestolen gegevens van Indiaanse immigratiedossiers, telefoongesprekken van LG U Plus in Zuid-Korea en planinformatie uit Taiwan, werden snel verwijderd van platforms zoals GitHub, maar niet voordat ze zich uitgebreid binnen de cybersecuritygemeenschap verspreidden. Het incident werpt licht op de technische capaciteiten en de geopolitieke omvang van staatsgesponsorde cyberoperaties.

APT-groepen richten zich op bouwsector om RDP-, SSH- en Citrix-inloggegevens te stelen

Advanced persistent threat (APT) groepen, gesteund door staten zoals China, Rusland, Iran en Noord-Korea, richten zich steeds vaker op de bouwsector. De digitale transformatie van de sector, die sterk afhankelijk is van derde partijen, biedt aanvallers kansen om inloggegevens voor systemen zoals Remote Desktop Protocol (RDP), Secure Shell (SSH) en Citrix te stelen. Deze systemen fungeren als toegangspoorten naar gevoelige gegevens, zoals projectinformatie en financiële documenten. Phishingaanvallen en kwetsbaarheden in de toeleveringsketen worden ingezet om toegang te krijgen tot netwerken. Zodra aanvallers binnen zijn, kunnen zij zich lateraal verplaatsen en waardevolle informatie stelen, waaronder contracten en persoonlijke gegevens van medewerkers en klanten. De groeiende ondergrondse marktplaatsen voor gestolen inloggegevens vergemakkelijken de toegang tot netwerken van bouwbedrijven, waardoor cybercriminelen snel hun operaties kunnen opschalen. De situatie benadrukt de noodzaak voor bouwbedrijven om robuuste beveiligingsmaatregelen te implementeren.



Kritieke kwetsbaarheid in populaire expr-eval JavaScript bibliotheek ontdekt

Een ernstige kwetsbaarheid in de veelgebruikte expr-eval JavaScript bibliotheek, die meer dan 800.000 wekelijkse downloads heeft op NPM, maakt het mogelijk om op afstand code uit te voeren via schadelijk ingevoerde gegevens. De kwetsbaarheid, bekend als CVE-2025-12735, werd ontdekt door beveiligingsonderzoeker Jangwoo Choe. De kwetsbaarheid komt voort uit het niet valideren van variabelen in de functie Parser.evaluate(), waardoor een aanvaller kwaadaardige functieobjecten kan doorgeven die tijdens de evaluatie worden uitgevoerd. De beveiligingsscore is 9.8, wat de kwetsbaarheid als kritiek bestempelt. Zowel de originele expr-eval versie als de actieve fork (expr-eval-fork) worden getroffen. Een oplossing is beschikbaar in versie 3.0.0 van expr-eval-fork. Gebruikers van expr-eval wordt geadviseerd over te stappen op deze versie om verdere risico's te vermijden.

Kritieke SQL-injectie kwetsbaarheid in QuMagie stelt op afstand uitvoerbare code mogelijk

Een ernstige kwetsbaarheid is ontdekt in de QuMagie-software versie 2.6.x van QNAP, een multimediaapplicatie voor QNAP NAS-systemen. Deze kwetsbaarheid, gecategoriseerd als SQL-injectie (CVE-2025-52425), kan een aanvaller in staat stellen om op afstand ongeautoriseerde code uit te voeren. De kwetsbaarheid heeft een hoge impact op de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens en systemen. Hoewel er momenteel geen aanwijzingen zijn dat de kwetsbaarheid actief wordt misbruikt, wordt sterk aanbevolen om kwetsbare apparaten bij te werken naar versie 2.7.0 of hoger. Organisaties moeten hun monitoringcapaciteiten versterken om verdachte activiteiten snel te detecteren. Het is cruciaal om de nieuwste updates te installeren en de impact van eerdere compromitteringen te beoordelen.

Nieuwe ransomware Kazu Onion gedetecteerd op Dark Web

Op 10 november 2025 werd via het X-platform door de Dark Web Informer een nieuwe ransomware-software ontdekt, genaamd Kazu Onion. De ransomware is beschikbaar via een Onion-link (6czlbd2jfiy6765fbnbnzuwuqocg57ebvp3tbm35kib425k4qnmiiiqd.onion), waarmee cybercriminelen de aanval kunnen uitvoeren op slachtoffers. Deze malware kan ernstige schade veroorzaken door gegevens te versleutelen en vervolgens losgeld te

eisen voor de decryptie. De ontdekking van Kazu Onion toont aan dat het dreigingslandschap op het Dark Web blijft evolueren, met nieuwe aanvallen die voortdurend opduiken. Het is belangrijk dat organisaties zich bewust zijn van de risico's van ransomware en adequate maatregelen treffen om hun systemen te beschermen tegen dit type dreiging.

Cybercriminelen gebruiken AI-platforms om industriële bedrijven aan te vallen

Cybercriminelen richten zich steeds vaker op productiebedrijven door gebruik te maken van cloudgebaseerde platforms en kunstmatige intelligentie (AI) voor geavanceerde aanvallen. Een recent rapport van Netskope Threat Labs toont aan dat 22 van elke 10.000 gebruikers in de productiebranche maandelijks worden blootgesteld aan kwaadaardige inhoud. Aanvallers maken niet alleen gebruik van traditionele malware, maar ook van vertrouwde cloudservices zoals Microsoft OneDrive, GitHub en Google Drive om schadelijke software te verspreiden. AI-platforms, zoals die van OpenAI en AssemblyAI, worden ook actief aangevallen, waarbij malware wordt verborgen in ogenschijnlijk legitieme bestanden. Dit maakt het voor beveiligingssystemen moeilijk om aanvallen vroegtijdig te detecteren. De toename van dergelijke aanvallen benadrukt de noodzaak voor productiebedrijven om striktere inspectie- en veiligheidsmaatregelen te implementeren, vooral met betrekking tot bestanddownloads uit cloudplatforms.

Hackers misbruiken WordPress-kwetsbaarheden voor SEO-spam

Cybercriminelen richten zich steeds vaker op websites om schadelijke links in te voegen en hun zoekmachineoptimalisatie (SEO) te verbeteren via blackhat SEO-technieken. Deze aanvallen richten zich voornamelijk op online casinospam, die momenteel het meest voorkomende type spam is dat getroffen websites beïnvloedt. De aanvallers maken misbruik van kwetsbaarheden in WordPress-installaties om spaminhoud te plaatsen die online casino's promoot, met name gericht op markten waar gokken zwaar gereguleerd is. Om hun aanwezigheid te verbergen, maken de aanvallers gebruik van meerdere technieken, waaronder het vervangen van originele websitepagina's door pagina's met spam-inhoud. De kwaadaardige code wordt op slimme wijze verborgen in thema- en pluginbestanden van WordPress, wat zorgt voor meerdere lagen van bescherming tegen detectie. Deze geavanceerde malware

maakt gebruik van dynamische content en database-manipulatie om zijn schadelijke code door te voeren, zelfs als onderdelen van de aanval worden ontdekt.

Yanluowang initial access broker pleit schuldig in ransomwarezaak

Aleksey Olegovich Volkov, een Rus die fungeerde als initial access broker (IAB) voor de Yanluowang ransomware-aanvallen, heeft schuld bekend. Deze aanvallen, gericht op acht Amerikaanse bedrijven tussen juli 2021 en november 2022, resulteerden in het encrypten van bedrijfsgegevens en het eisen van losgeldbetalingen variërend van $300.000 tot $15 miljoen. Volkov verkocht toegang tot de netwerken van de slachtoffers aan de ransomwaregroep, die vervolgens losgeld eiste in Bitcoin. Het onderzoek leidde tot het verkrijgen van chatlogs, gestolen gegevens, netwerkreferenties en e-mailaccounts van Yanluowang, waarmee de verdachte werd gelinkt aan de aanvallen. Hij wordt geconfronteerd met een mogelijke gevangenisstraf van 53 jaar en moet een schadevergoeding van meer dan $9 miljoen betalen aan de slachtoffers.

Intel klaagt ex-engineer aan voor diefstal van 18.000 ‘topgeheime’ bestanden

Intel heeft een rechtszaak aangespannen tegen voormalig software-engineer Jinfeng Luo, die ervan wordt beschuldigd 18.000 vertrouwelijke bestanden, waaronder enkele “topgeheime” documenten, te hebben gestolen. Luo, die sinds 2014 voor het bedrijf werkte, kreeg op 7 juli 2024 te horen dat zijn contract zou eindigen, waarna hij enkele dagen voor zijn vertrek de bestanden kopieerde naar een netwerkapparaat. De bestanden bevatten gevoelige bedrijfsinformatie, wat de schade aanzienlijk vergroot. Intel ontdekte de ongebruikelijke gegevensoverdrachten en heeft drie maanden geprobeerd contact met Luo op te nemen, maar hij is onvindbaar. De rechtszaak is aangespannen in een federale rechtbank in Washington, waarbij Intel de teruggave van de gestolen gegevens en schadevergoeding eist. Dit is niet het eerste incident waarbij een ex-werknemer van Intel vertrouwelijke informatie heeft gestolen, aangezien een eerdere zaak resulteerde in een boete en voorwaardelijke gevangenisstraf.

Oekraïne introduceert Diia.AI als eerste nationale AI assistent voor overheidsdiensten

Oekraïne heeft een wereldwijd primeur bereikt door Diia.AI te lanceren als de eerste volledig operationele nationale AI assistent voor overheidsdiensten. Het systeem ondersteunt inmiddels miljoenen inwoners bij het aanvragen van documenten en administratieve handelingen zonder fysieke loketten of complexe formulieren. Tijdens een technologietop in Kyiv werd bevestigd dat Diia.AI meer dan tweehonderd diensten automatiseert en al een groot deel van het interne werk binnen het ministerie van Digitale Transformatie verwerkt. De overheid werkt verder aan een stemfunctionaliteit om de toegankelijkheid te vergroten en ontwikkelt daarnaast een eigen Oekraïense taalmodel om minder afhankelijk te zijn van buitenlandse technologie en beter weerstand te bieden tegen desinformatie. Ondanks de voortdurende oorlog en cyberdreiging vanuit Rusland blijft Oekraïne investeren in digitale innovatie, met als doel een toekomstig staatsmodel waarin overheidsdiensten proactief worden aangeboden.

SK Telecom ziet winst fors dalen door nasleep van grote datalek

De Zuid-Koreaanse telecomaanbieder SK Telecom rapporteert een sterke daling van de operationele winst in het derde kwartaal na de grootschalige cyberaanval die eerder dit jaar aan het licht kwam. Het bedrijf behaalde een operationele winst van 48,4 miljard won, aanzienlijk minder dan de 493 miljard won in dezelfde periode een jaar eerder. De onderneming wijt deze afname aan hoge herstelkosten en compensatiebetalingen. Tijdens de aanval werden gegevens van circa 27 miljoen klanten buitgemaakt, waaronder abonneenummers, authenticatiesleutels, logbestanden en op simkaarten opgeslagen berichten. Onderzoek toont aan dat aanvallers al sinds 2022 onopgemerkt toegang hadden tot interne systemen. Door de financiële impact schort SK Telecom de dividenduitkering op. Het incident onderstreept de langdurige gevolgen van datalekken en de risico’s van ongepatchte of onvoldoende bewaakte systemen binnen vitale telecominfrastructuur.

Britse economie groeit minder door cyberaanval op Jaguar Land Rover

De Bank of England meldt dat de Britse economie in het derde kwartaal minder sterk is gegroeid dan verwacht. Het bruto binnenlands product steeg met 0,2 procent, terwijl de bank rekende op 0,3 procent. De tegenvaller wordt volgens de centrale bank deels veroorzaakt door de grote cyberaanval op Jaguar Land Rover in september 2025. Door de aanval lag de productie van de autofabrikant ongeveer vijf

weken stil, wat leidde tot een geschatte schade van bijna 2,2 miljard euro. De verstoring trof niet alleen het bedrijf zelf, maar had ook gevolgen voor de toeleveringsketen. De Britse overheid verstrekte eind september een noodlening van circa 1,7 miljard euro om verdere economische schade te beperken. Naast de impact van de cyberaanval wijst de Bank of England ook op lagere exportcijfers richting de Verenigde Staten. De verwachting is dat de groei in het vierde kwartaal uitkomt op 0,3 procent

The Washington Post slachtoffer van aanval op Oracle E-Business Suite

De Amerikaanse krant The Washington Post is getroffen door een cyberaanval op het Oracle E-Business Suite-platform. De aanval maakt deel uit van een bredere campagne waarbij naar schatting meer dan honderd organisaties zijn getroffen. Oracle waarschuwde eerder dat criminelen klanten afpersen via een kwetsbaarheid, aangeduid als CVE-2025-61882, in de E-Business Suite. De ransomwaregroep Cl0p heeft de verantwoordelijkheid opgeëist en zegt bedrijfsgegevens te hebben buitgemaakt waarmee slachtoffers worden bedreigd om losgeld te betalen. Het is niet bekend welke gegevens bij The Washington Post zijn gestolen, maar de getroffen software wordt vaak gebruikt voor bedrijfsprocessen die gevoelige financiële en personeelsinformatie bevatten. De aanval illustreert de aanhoudende risico's van ongepatchte bedrijfssoftware en de toenemende impact van grootschalige supply-chain-aanvallen op mediabedrijven en andere sectoren.

ICT-systemen van Duitse gemeente Ludwigshafen offline na cyberaanval

Op 6 november 2025 werd de Duitse gemeente Ludwigshafen getroffen door een cyberaanval, waarbij de ICT-systemen ernstig verstoord raakten. Om verdere schade te voorkomen, werden de systemen van de gemeente offline gehaald. De stad is sindsdien niet bereikbaar via telefoon of e-mail, en haar website toont enkel een verklaring over de aanval. Hoewel de gemeente geen indicaties heeft dat persoonsgegevens zijn gestolen, is er geen informatie over de aard van de aanval of de betrokkenheid van ransomware. Het herstel van de systemen zal minstens de hele komende week duren. Dit incident volgt op eerdere cyberaanvallen in andere Duitse steden, wat wijst op een groeiend patroon van cyberdreigingen tegen lokale overheden. De gemeente adviseert inwoners om voor dringende zaken fysiek langs te gaan bij kantoren, aangezien online diensten tijdelijk niet beschikbaar zijn.

Noyb bekritiseert voorgestelde wijzigingen in de AVG door de Europese Commissie

De Europese Commissie heeft voorstellen gepresenteerd voor wijzigingen in de Algemene Verordening Gegevensbescherming (AVG), die voor veel kritiek zorgen bij privacyorganisatie Noyb. De commissie maakt gebruik van de Omnibus-procedure, die normaal alleen voor technische aanpassingen wordt gebruikt, maar in dit geval wordt toegepast op ingrijpende herzieningen van de privacyregels. Noyb, onder leiding van privacyactivist Max Schrems, stelt dat de wijzigingen vooral ten goede komen aan grote techbedrijven en niet aan kleine bedrijven, zoals oorspronkelijk werd beloofd. De focus van de wijzigingen ligt op het versoepelen van de regels voor AI-training met persoonsgegevens en het verzwakken van de bescherming van gezondheidsgegevens, minderheden en werknemers. Noyb waarschuwt dat de wijzigingen de effectiviteit van de AVG aanzienlijk kunnen ondermijnen, met onbedoelde gevolgen voor de bescherming van persoonsgegevens in verschillende sectoren.

Quad9 waarschuwt voor dreiging door gerechtelijke bevelen rond piraterij

DNS-resolver Quad9 heeft gewaarschuwd voor de groeiende dreiging die gerechtelijke bevelen tegen DNS-providers vormen. Deze bevelen dwingen providers zoals Google, Cloudflare, en Cisco om domeinen te blokkeren die illegale streams van live sport en beschermd materiaal aanbieden. Kleine DNS-providers, zoals Quad9, kunnen echter niet de juridische kosten dragen die deze bevelen met zich meebrengen. Quad9 spreekt van een "existentiële dreiging", aangezien grote bedrijven zoals Google en Cloudflare deze kosten in hun bedrijfsmodellen kunnen verwerken, maar kleinere partijen zoals Quad9 niet over de benodigde financiële middelen beschikken. Dit heeft invloed op de werking van het internet, aangezien DNS-resolvers cruciaal zijn voor de vertaling van webadressen naar digitale paden. Quad9 heeft zich in de rechtszaak tegen deze gerechtelijke bevelen niet laten vertegenwoordigen vanwege de kosten.

Vijf redenen waarom aanvallers LinkedIn gebruiken voor phishing

Phishing-aanvallen vinden steeds vaker plaats via niet-traditionele kanalen, waaronder LinkedIn. Dit platform biedt aanvallers voordelen, zoals het omzeilen van

e-mailbeveiliging en de mogelijkheid om contact te maken met bedrijfsleiders en andere belangrijke doelwitten. LinkedIn is een populaire keuze omdat veel medewerkers het gebruiken voor zakelijke doeleinden, wat de kans vergroot dat zij op kwaadaardige berichten reageren. Aanvallers kunnen eenvoudig bestaande accounts overnemen, waardoor de aanvallen geloofwaardiger lijken. Daarnaast kunnen ze via LinkedIn direct benaderen zonder de beperkingen die e-mailbeveiliging oplegt. Dit maakt de aanvallen goedkoper en gemakkelijker schaalbaar. Verder is LinkedIn ook een krachtige tool voor het identificeren van hooggeplaatste medewerkers, wat de kans op succesvolle spear-phishing aanvallen vergroot. De schade kan enorm zijn, aangezien aanvallers via deze aanval toegang kunnen krijgen tot kritieke bedrijfsdata en cloudplatformen, waardoor ze bredere netwerken kunnen compromitteren.

Explosieve toename cryptofraude: al 29 miljoen euro buitgemaakt in 2025

De schade door cryptofraude is in 2025 explosief gestegen. Tot 1 november werd al 29 miljoen euro buitgemaakt, vergeleken met 25 miljoen euro in 2024. De Fraudehelpdesk ontving meer dan 1200 meldingen van slachtoffers, waarvan 97% betrekking heeft op cryptobeleggingen. De werkelijke schade is waarschijnlijk groter, aangezien veel slachtoffers zich schamen om melding te maken. Criminelen gebruiken social media om slachtoffers te benaderen, waarbij ze zich voordoen als betrouwbare beleggers of experts. Ze misbruiken vaak de namen van bekende Nederlanders en spelen in op de ‘fear of missing out’ (FOMO) om mensen te overtuigen te investeren. Daarnaast wordt de oplichtingstruc ‘pig butchering’ steeds vaker toegepast, waarbij slachtoffers via datingsites worden benaderd en uiteindelijk worden aangespoord om geld te investeren in crypto’s. Slachtoffers wordt geadviseerd aangifte te doen en melding te maken bij de Fraudehelpdesk.