Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

13-10-2025:

Den Hartogh Logistics slachtoffer van ransomwareaanval door Anubis-groep

Den Hartogh Logistics, een van de toonaangevende logistieke dienstverleners wereldwijd, werd getroffen door een ransomwareaanval uitgevoerd door de Anubis-groep. De aanval werd ontdekt op 10 oktober 2025 en heeft geleid tot een datalek binnen het bedrijf. Den Hartogh Logistics is actief in de transport- en logistieke sector en is gevestigd in Nederland. De aanval heeft aanzienlijke impact op hun systemen en heeft de veiligheid van klantgegevens in gevaar gebracht.

Europa’s digitale afhankelijkheid van de VS: wat als de stekker eruit gaat?

Europa is sterk afhankelijk van Amerikaanse techbedrijven zoals Microsoft, Google en Apple voor essentiële digitale diensten. Deze afhankelijkheid werd pijnlijk duidelijk toen Microsoft op last van voormalig president Donald Trump de mailbox van de hoofdaanklager van het Internationaal Strafhof (ICC) uitzetten, wat de kwetsbaarheid van Europa benadrukt. Als de VS besluit deze bedrijven te verbieden diensten te leveren aan Europese overheden, bedrijven en burgers, zou de Europese digitale infrastructuur ernstig worden verstoord. Er zijn weinig Europese alternatieven voor deze diensten, wat de situatie bemoeilijkt. Europese leiders erkennen nu de noodzaak om digitale soevereiniteit na te streven, maar dit kan slechts op lange termijn worden gerealiseerd. Het gebrek aan zelfvoorziening in digitale technologieën heeft Europese landen kwetsbaar gemaakt voor externe invloeden, vooral gezien de strategische rol van technologie in geopolitieke kwesties.

Oorlog in Europa: Drones, cyberaanvallen en nucleaire dreigingen als nieuwe realiteit

De oorlog in Europa is geen toekomstig scenario meer, maar de harde realiteit. Van Oekraïne tot de Baltische Staten worden de strijdvelden gekarakteriseerd door drones, cyberaanvallen en nucleaire dreigingen. Rusland heeft zijn aanvallen uitgebreid met onder andere het schenden van NAVO-luchtruim, radardemping, en het uitvoeren van cyberaanvallen. De strategie van president Vladimir Poetin is om de druk op te voeren door op meerdere fronten tegelijk te escaleren. Het Westen, inclusief de NAVO, lijkt onvoldoende voorbereid op de dreiging van drones, die steeds vaker worden ingezet. Ook het gebruik van olie- en vrachtschepen door

Rusland voor oorlogsinspanningen vergroot de complexiteit van de situatie. Europa wordt geconfronteerd met een hybride oorlog waarbij conventionele strijd wordt gecombineerd met moderne technologieën en nucleaire intimidatie, wat de geopolitieke stabiliteit verder onder druk zet.

Regering grijpt in bij Nijmeegse chipmaker Nexperia, topman aan de kant gezet

De Nederlandse regering heeft ingegrepen bij de chipmaker Nexperia uit Nijmegen wegens ernstige bestuurlijke tekortkomingen. Als gevolg daarvan is de topman, Zhang Xuezheng, voorlopig geschorst. Het ministerie van Economische Zaken greep in op basis van de Wet beschikbaarheid goederen, die de regering toestaat maatregelen te nemen in geval van bedreigingen voor cruciale producten, zoals de chips van Nexperia die worden gebruikt in consumentenelektronica en auto's. De regering stelt dat de bestuurlijke fouten de continuïteit en de technologische capaciteit van Nederland en Europa in gevaar zouden kunnen brengen. Het moederbedrijf Wingtech uit China bekritiseerde het ingrijpen van de overheid, en beschuldigde Nederland van geopolitieke vooringenomenheid. Het beheer van Nexperia’s activa is tijdelijk overgedragen aan een andere partij.

Nieuwe kwetsbaarheid in Oracle E-Business Suite stelt hackers in staat gegevens zonder inlog te benaderen

Oracle heeft een beveiligingswaarschuwing uitgegeven over een nieuwe kwetsbaarheid in zijn E-Business Suite. De kwetsbaarheid, aangeduid als CVE-2025-61884, heeft een CVSS-score van 7,5, wat duidt op een hoge ernst. Het probleem betreft versies van 12.2.3 tot en met 12.2.14 en kan door aanvallers worden misbruikt om ongeauthenticeerde toegang te krijgen tot gevoelige gegevens. De aanval kan plaatsvinden zonder dat er inloggegevens nodig zijn, wat het risico vergroot. Oracle waarschuwt dat de kwetsbaarheid op afstand kan worden geëxploiteerd via HTTP en dringende maatregelen vereist, hoewel er geen meldingen zijn van actieve aanvallen. Dit komt kort na de ontdekking van eerdere aanvallen waarbij dezelfde software werd misbruikt, mogelijk door de Cl0p-ransomwaregroep.

ChaosBot maakt misbruik van CiscoVPN- en Active Directory-wachtwoorden voor netwerkcommando's

ChaosBot, een geavanceerde Rust-gebaseerde backdoor die eind september 2025 opdook, maakt gebruik van gestolen CiscoVPN- en overbevoegde Active Directory-wachtwoorden om toegang te krijgen tot netwerkcomponenten. De aanvallers verspreiden de malware via een techniek genaamd "side-loading" met behulp van het legitieme Microsoft Edge-component identity_helper.exe. Het gebruik van Discord voor commando- en controle (C2)-operaties maakt het moeilijker om de communicatie te traceren. Na de eerste infectie stelt ChaosBot een omgekeerde proxy in om persistent toegang te behouden, en verplaatst zich lateraal binnen het netwerk. De infectie gebeurt via twee hoofdroutes: het misbruik van VPN-gegevens en phishing-e-mails met kwaadaardige snelkoppelingen. ChaosBot gebruikt de Discord-bot van de aanvallers voor communicatie en voert opdrachten uit die via de platformen worden doorgegeven.

Discord ingezet voor datadiefstal via npm, PyPI en RubyGems

Onderzoekers van Socket hebben ontdekt hoe cybercriminelen Discord gebruiken voor commando- en controlemechanismen in de npm-, PyPI- en RubyGems-ecosystemen. Door Discord-webhooks in kwaadaardige pakketten te integreren, kunnen aanvallers gevoelige gegevens zoals configuratiebestanden en gebruikersinformatie uitlekken naar servers die door de aanvallers worden beheerd. Dit vervangt de traditionele, gecontroleerde C2-servers. Voorbeelden van deze technieken zijn onder andere het gebruik van Discord-webhooks in npm-pakketten zoals mysql-dumpdiscord, die vertrouwelijke bestandsgegevens naar een Discord-kanaal sturen. De onderzoekers waarschuwen dat dit nieuwe aanvalsmethoden zijn die de beveiliging van supply chains in gevaar kunnen brengen, omdat Discord-webhooks vaak worden toegestaan door firewallinstellingen en moeilijk te detecteren zijn door traditionele methoden. Het is belangrijk om dependency-pakketten te controleren en risicovolle verbindingen zoals webhooks te blokkeren.

Astaroth banking trojan maakt misbruik van GitHub om operationeel te blijven na uitname

De Astaroth banking trojan maakt gebruik van GitHub om zijn operaties voort te zetten nadat zijn infrastructuur is uitgeschakeld. In plaats van traditionele command-

and-control (C2)-servers, gebruiken de aanvallers GitHub-repositories om malwareconfiguraties te hosten, waardoor de trojan blijft functioneren zelfs na het neerhalen van C2-servers. De aanval richt zich voornamelijk op Brazilië, maar ook andere Latijns-Amerikaanse landen worden getroffen. De trojan wordt verspreid via phishing-e-mails die zich voordoen als documenten van DocuSign, waarna de malware wordt geïnstalleerd en de activiteiten van de slachtoffers monitort. Astaroth verzamelt inloggegevens van bank- en cryptowebsites door middel van keylogging. De malware is ook uitgerust met technieken om analyse te vermijden, zoals het afsluiten bij detectie van emulatoren of analysetools. De trojan maakt gebruik van GitHub om zijn configuratiebestanden te updaten, wat zorgt voor een robuuste back-upinfrastructuur voor het geval de primaire servers ontoegankelijk worden.

SonicWall SSLVPN onder aanval na inbreuk op firewall-back-ups

Na een recente inbreuk op de cloudservice van SonicWall, die gevoelige gegevens van klanten, inclusief gecodeerde configuratie-back-ups, blootstelde, zijn er gerichte aanvallen op de SSLVPN-apparaten van het bedrijf. De aanvallen, die begin oktober 2025 begonnen, maakten gebruik van gestolen geldige inloggegevens in plaats van brute force-methoden. De aanvallers, die waarschijnlijk over insiderkennis beschikten, probeerden toegang te krijgen tot netwerken en systemen. SonicWall heeft bevestigd dat de inbreuk alle klanten met de MySonicWall-back-updienst heeft getroffen, hoewel de schade beperkt was tot enkele procenten van de firewalls. Bedrijven worden aangemoedigd om hun inloggegevens onmiddellijk opnieuw in te stellen en hun beveiliging te verbeteren door multi-factor authenticatie en het toepassen van het principe van minimale rechten. SonicWall heeft ook waarschuwingen gedeeld om organisaties te helpen bij het identificeren van verdachte activiteiten.

Spanje maakt einde aan cybercrime-syndicaat "GXC Team" en arresteert leider

De Spaanse Guardia Civil heeft het cybercrime-syndicaat "GXC Team" ontmanteld en de vermeende leider, de 25-jarige Braziliaan "GoogleXcoder," gearresteerd. Het GXC Team bood een crime-as-a-service platform aan via Telegram en een Russisch sprekend hackerforum, waar ze AI-gestuurde phishingkits, Android-malware en stemfraudetools aanbooden. Het syndicaat richtte zich op banken, transportbedrijven en e-commerce in Spanje, het VK, de VS, Slovenië en Brazilië. De Spaanse

autoriteiten voerden op 20 mei gecoördineerde invallen uit in verschillende steden, waarbij elektronische apparaten en cryptocurrency van slachtoffers werden in beslag genomen. De operaties brachten het volledige netwerk aan het licht, en zes personen werden geïdentificeerd die betrokken waren bij het gebruik van deze diensten. De zaak is nog in onderzoek, en er kunnen verdere arrestaties volgen.

Acht aanhoudingen voor grootschalige hypotheekfraude in Amsterdam en Zaandam

De financiële recherche van de Amsterdamse politie heeft acht personen aangehouden die verdacht worden van witwassen, oplichting, valsheid in geschrifte en hypotheekfraude. De aanhoudingen vonden plaats op vier locaties in Amsterdam en Zaandam. De verdachten, variërend in leeftijd van 27 tot 43 jaar, werkten onder andere in de makelaardij en als hypotheekadviseur. Na de aanhoudingen zijn er vier locaties doorzocht, waar administratie, contant geld en waardevolle goederen zoals horloges en sieraden in beslag werden genomen. Het onderzoek, dat begon in juni, richt zich op het vervalsen van inkomensgegevens om frauduleuze hypotheken aan te vragen. De fraude heeft een aanzienlijke impact op de woningmarkt en kan leiden tot witwassen van crimineel geld. Het onderzoek loopt nog, en verdere aanhoudingen zijn mogelijk.

Vendor RoadRunna waarschijnlijk uitgeschakeld na recente hack

Er zijn aanwijzingen dat de vendor RoadRunna mogelijk is uitgeschakeld na een recente verstoring. Het lijkt erop dat het platform van RoadRunna niet meer actief is, mogelijk als gevolg van een hack of een andere verstoring. RoadRunna was actief op het darkweb en betrokken bij de verkoop van gegevens en mogelijk andere illegale diensten. Deze verstoring heeft invloed op de cybercriminaliteit en kan de operaties van cybercriminelen die afhankelijk zijn van deze vendor verstoren. Dit incident heeft implicaties voor zowel onderzoekers als organisaties die de activiteiten op het darkweb volgen.

Dark Web-verkoop van database met gegevens van 1,09 miljard grensoverschrijdingen

Een dreigingsactor genaamd Fonada biedt op het dark web een enorme database te koop die meer dan 1,09 miljard records bevat van mensen die een grens zijn

gepasseerd. De database, die ongeveer 563 GB groot is en recent werd geüpdatet in juni 2023, bevat gevoelige informatie zoals namen, paspoortnummers en data van vertrek en aankomst bij grensovergangen, zoals luchthavens en andere controlepunten. De veiling is begonnen met een startprijs van $65.000, met verhogingen van $3.500 en een 'blitzprijs' van $95.000. Deze verkoop benadrukt de kwetsbaarheid van grensgegevens en de risico's voor privacy en veiligheid als zulke gevoelige informatie in verkeerde handen valt.

37 miljoen Roblox-gebruikerswachtwoorden te koop op Dark Web

Op het Dark Web worden momenteel 37 miljoen gebruikerswachtwoorden van het populaire online platform Roblox te koop aangeboden. De wachtwoorden worden verhandeld door cybercriminelen, wat gebruikers blootstelt aan het risico van identiteitsdiefstal en ongeautoriseerde toegang tot hun accounts. Deze dreiging onderstreept de groeiende bezorgdheid over de veiligheid van gegevens op het platform, dat wereldwijd miljoenen actieve gebruikers heeft. Gebruikers worden aangespoord om hun wachtwoorden te wijzigen en gebruik te maken van twee-factor-authenticatie om hun accounts beter te beveiligen tegen mogelijke aanvallen. De verkoop van dergelijke gegevens benadrukt de noodzaak voor strengere beveiligingsmaatregelen op online platforms en verhoogde waakzaamheid van gebruikers.

Groep suggereert Nintendo te hebben gehackt

Een hackersgroep, Crimson Collective, heeft gesuggereerd dat zij Nintendo hebben gehackt, maar er is geen bevestiging van het Japanse gamebedrijf. De groep heeft een screenshot online gezet met vermeende gegevens van Nintendo, maar er is geen bewijs dat de hack daadwerkelijk heeft plaatsgevonden. Crimson Collective is ook verantwoordelijk voor de hack op Red Hat, en het is een relatief nieuwe groep. Er is weinig informatie over wat de hackers precies hebben buitgemaakt, en Nintendo heeft tot nu toe niet gereageerd op de beschuldigingen. De groep heeft in het verleden ook Amazon Web Services-omgevingen aangevallen. Ondanks het gebrek aan bewijs blijft het onduidelijk of Nintendo daadwerkelijk het doelwit was van deze aanval. De situatie roept vragen op over de omvang van de mogelijke inbreuk en de gevolgen voor het bedrijf.

Insider-dreigingen: wanneer werknemers overstag gaan naar de donkere kant

nsider-dreigingen vormen een significant risico voor bedrijven, omdat kwaadwillenden toegang hebben tot systemen via legitieme bevoegdheden. Dit maakt hun activiteiten moeilijker te detecteren. Een voorbeeld hiervan is een cybercrimineel die de BBC-correspondent Joe Tidy benaderde, met het aanbod om toegang te geven tot de systemen van de omroep in ruil voor een deel van de losgeldbetaling. Hoewel dergelijke incidenten zeldzaam zijn, kunnen ze ernstige schade veroorzaken, vooral wanneer werknemers, vaak in sleutelrollen zoals systeembeheerders of cloudarchitecten, zich laten omkopen of beïnvloeden door cybercriminelen. Hackers maken gebruik van sociale manipulatie en phishingtechnieken om toegang te krijgen zonder verdachte activiteiten uit te voeren. Experts adviseren dat wanneer iemand benaderd wordt door een cybercrimineel, ze niet in gesprek gaan en altijd interne beveiliging of de autoriteiten waarschuwen.