Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

03-11-2025:

Ansell slachtoffer van Clop ransomwareaanval

Ansell, een wereldwijd toonaangevend bedrijf in beschermingsoplossingen, werd op 31 oktober 2025 getroffen door een ransomwareaanval uitgevoerd door de Clop ransomwaregroep. Het bedrijf is gespecialiseerd in het ontwerpen, ontwikkelen en produceren van beschermende handschoenen, condooms en andere veiligheidskleding. Ansell is actief in verschillende sectoren, waaronder de gezondheidszorg en de industrie, en heeft een lange geschiedenis van meer dan 125 jaar. De aanval werd ontdekt op 31 oktober 2025, en het bedrijf heeft zijn activiteiten in Australië en wereldwijd, inclusief België, gestaakt. De Clop-groep heeft de verantwoordelijkheid voor de aanval opgeëist, en er is een vermoeden van datalekken, waarbij gevoelige gegevens van medewerkers en externe partners mogelijk zijn buitgemaakt.

Ansell biedt een breed assortiment aan persoonlijke beschermingsmiddelen, met de nadruk op handschoenen en beschermkleding voor diverse industrieën zoals gezondheidszorg en de chemische sector. Het bedrijf heeft vestigingen in meer dan 100 landen en biedt producten die voldoen aan strenge veiligheidsnormen en duurzaamheidseisen. Een van de innovaties is de HyFlex™ Precision Comfort Series, ontworpen met AEROFIT™ Technology, die zorgt voor een uitstekende pasvorm en verhoogd draagcomfort. Ansell zet zich in voor duurzaamheid en heeft initiatieven zoals het RightCycle™-programma, dat zich richt op circulaire economie door producten te reinigen en hergebruiken. De organisatie heeft ook het AnsellGUARDIAN veiligheidsbeoordelingsprogramma en biedt producten die voldoen aan milieuverantwoordelijkheid. Met een focus op veiligheid, innovatie en duurzaamheid blijft Ansell een vooraanstaande speler in de wereld van persoonlijke beschermingsmiddelen.

Data inwoners Schiermonnikoog buitgemaakt bij cyberaanval Omrin

Bij een ransomwareaanval op de afvalverwerker Omrin zijn persoonsgegevens van inwoners van Schiermonnikoog buitgemaakt. Gehackte gegevens omvatten namen, adressen, BSN-nummers en RSIN-nummers van zowel eilandbewoners als eigenaren van recreatiewoningen. Daarnaast werden ook adresgegevens van bedrijven gestolen, wat risico’s met zich meebrengt zoals identiteitsfraude en phishing. De aanval vond plaats halverwege oktober 2025 en werd door de

gemeente Schiermonnikoog gemeld bij de Autoriteit Persoonsgegevens. Omrin, dat verantwoordelijk is voor afvalinzameling in het noorden van Nederland, had onterecht BSN-nummers verzameld, waarvoor geen noodzakelijkheid bestond. De gemeente heeft inwoners geadviseerd alert te zijn op verdachte communicatie en bankgegevens te controleren. Verdachte gevallen kunnen gemeld worden bij de Fraudehelpdesk of het Centraal Meldpunt Identiteitsfraude om verdere schade te voorkomen.

Toegang tot Nederlands bedrijf met omzet van $6 miljoen op hackforum

Op een hackforum werd informatie gedeeld over toegang tot een Nederlands bedrijf met een omzet van ongeveer $6 miljoen in de commerciële sector. De toegang wordt beschreven als sterk en betreft een domeinaccount. Dit wijst op mogelijke kwetsbaarheden binnen het systeem van het bedrijf, die kunnen worden misbruikt voor ongeautoriseerde toegang. De details impliceren dat cybercriminelen toegang hebben tot waardevolle gegevens van een commercieel bedrijf, wat het risico op datalekken of andere vormen van digitale criminaliteit verhoogt. Het delen van dergelijke toegangspunten op hackforums is een veelvoorkomende manier waarop aanvallers zich toegang verschaffen tot systemen van bedrijven, wat kan leiden tot schade aan de reputatie en financiële verliezen.

Kwetsbaarheden in windows grafische interface leiden tot risico op remote code execution en geheugentoegang

Recent onderzoek heeft drie kwetsbaarheden geïdentificeerd in de Graphics Device Interface (GDI) van Windows. Deze kwetsbaarheden, CVE-2025-30388, CVE-2025-53766 en CVE-2025-47984, kunnen leiden tot externe code-executie, onterechte toegang tot geheugengegevens en de mogelijkheid voor aanvallers om kritieke gegevens over het netwerk te onthullen. De kwetsbaarheden werden ontdekt door middel van een fuzzing-campagne gericht op Windows GDI en kunnen worden uitgebuit via speciaal aangepaste EMF+ metafiles. De kwetsbaarheden zijn inmiddels door Microsoft gepatcht in de Patch Tuesday-updates van mei, juli en augustus 2025. Desondanks blijft het belangrijk om kwetsbaarheden actief te monitoren en te verhelpen, aangezien gedeeltelijke fixes in het verleden niet altijd effectief waren.

FakeCaptcha payload ingebed in gecompromitteerd nieuwsartikel

Op 31 oktober 2025 werd een FakeCaptcha-payload ontdekt op een gecompromitteerde webpagina van analyticscampus.com. De site, die zich voordeed als een legitiem artikel over een zelfpropagerende Visual Studio Code worm, bevatte in werkelijkheid een misleidende verificatieprompt. Deze prompt instrueerde gebruikers om opdrachten uit te voeren op macOS-systemen, een typische techniek van FakeCaptcha-social-engineeringcampagnes. Het doel was om gebruikers te misleiden en hen te laten uitvoeren van schadelijke payloads of toegang te geven tot hun systemen via de opdrachtregel. De verdachte website wordt aanbevolen om te blokkeren en gebruikers te waarschuwen voor dit type gedrag. Deze aanval benadrukt de voortdurende evolutie van FakeCaptcha-technieken, waarbij zelfs legitiem ogende technologie-artikelen worden misbruikt om malware te verspreiden.

Waarschuwing voor kwaadaardige ChatGPT-apps die gebruikersacties opnemen en gevoelige data stelen

Cybercriminelen maken gebruik van de populariteit van ChatGPT door vervalste mobiele apps te verspreiden die zich voordoen als legitieme ChatGPT-interfaces. Onderzoek heeft onthuld dat deze apps ontworpen zijn om gevoelige gebruikersgegevens te verzamelen en digitale activiteiten te monitoren zonder toestemming. De kwaadaardige apps infiltreren derde partij-appstores en gebruiken overtuigende branding, waardoor ze moeilijk te onderscheiden zijn van echte ChatGPT-toepassingen. Eenmaal geïnstalleerd voeren ze verborgen surveillance uit, terwijl ze de schijn wekken van werkende AI-assistenten. Het risico neemt toe doordat miljoenen gebruikers wereldwijd onofficiële AI-apps downloaden zonder zich bewust te zijn van de ingebedde spyware. Onderzoekers ontdekten dat de malware gebruik maakt van cloudinfrastructuur van Amazon Web Services en Google Cloud om communicatie te maskeren en beveiligingsdetectie te omzeilen. Gevoelige gegevens zoals wachtwoorden, bankcodes en contactgegevens worden gestolen en kunnen worden gebruikt voor verdere aanvallen.

Misbruik van gestolen inloggegevens voedt financieel gemotiveerde aanvallen

In de eerste helft van 2025 hebben financieel gemotiveerde aanvallers hun aanpak veranderd, waarbij ze traditionele malware-aanvallen hebben vervangen door het misbruiken van gestolen inloggegevens en geldige accounttoegang. Deze aanvallers

verkrijgen toegang tot netwerken via gecompromitteerde VPN-inloggegevens, vaak verkregen door phishing, de aankoop van gestolen gegevens of via infostealer-malware. De aanvallers maken gebruik van externe diensten, zoals VPN-infrastructuur en kwetsbaarheden in openbare applicaties, om toegang te verkrijgen en zich lateraal door netwerken te bewegen. Een belangrijk kenmerk van deze aanvallen is het gebruik van legitieme remote managementtools zoals AnyDesk en Atera, wat het detecteren van aanvallen bemoeilijkt. De aanvallers behouden hun toegang door eigen remote toegangstools te installeren en misbruik te maken van verhoogde gebruikersrechten. Deze aanpak stelt de aanvallers in staat om voor langere tijd onopgemerkt te blijven en effectief datadiefstal of andere aanvallen uit te voeren.

Vibe hacking: hoe AI-aangedreven manipulatie de cybercriminaliteit hervormt

Vibe hacking is een opkomende vorm van sociale manipulatie waarbij AI wordt ingezet om de toon, timing en persoonlijkheid van aanvallers te gebruiken om slachtoffers, inclusief andere AI-systemen, te misleiden. Deze techniek maakt gebruik van tekst, stemdeepfakes, korte video's en persona-mimicry om vertrouwen op te bouwen en toegang te verkrijgen tot gevoelige gegevens. Het doel is om mensen of bedrijven te overtuigen om informatie, geld of toegang te delen. Vibe hacking richt zich vooral op de bedrijfswereld, waar aanvallers gebruik maken van AI-modellen zoals Claude Code om vertrouwen op te bouwen en gegevens te stelen. Criminelen gebruiken ook eenvoudige AI-tools om overtuigende stemmen en berichten te genereren. Deze nieuwe vorm van cybercrime is moeilijk te detecteren, omdat de aanvallen zowel menselijke als AI-systemen kunnen misleiden.

Cybercriminelen richten zich op luxe merken met 1.330 valse domeinen

Cybercriminelen hebben in de periode tussen midden augustus en eind september 2025 maar liefst 1.330 valse domeinen geregistreerd om consumenten te misleiden. De domeinen deden zich voor als officiële websites van 23 bekende luxe merken zoals Gucci, Prada, Louis Vuitton, Rolex en Chanel. Deze nepdomeinen waren vaak gelinkt aan 'boutiques' of 'outlets' en probeerden consumenten met vermeende kortingen te lokken. De domeinen werden kort voor de drukke feestdagen geregistreerd, wat suggereert dat ze tijdens de piekverkoopseizoenen geactiveerd zouden kunnen worden. Sommige domeinen zijn nog inactief, maar er wordt

verwacht dat ze zullen worden gebruikt voor verkoop tijdens evenementen zoals Black Friday. De onderzoekers van PreCrime Labs, onderdeel van BforeAI, adviseren merken om proactief domeinen die een risico vormen te registreren en consumenten bewust te maken van veilige koopprakti jken om schade aan hun reputatie en financiën te voorkomen.

FBI watchdog detecteert DNS-wijziging voor lekdomain leakbase.la

Op 2 november 2025 werd een belangrijke DNS-wijziging gedetecteerd door een FBI watchdog. Het betrof het domein leakbase[.]la, dat eerder gekoppeld was aan het IP-adres 185.11.145.245. De wijziging zorgde ervoor dat het domein niet meer bereikbaar was via dit IP-adres, met als gevolg dat er geen nieuwe informatie beschikbaar was. Dit domein werd vaak gebruikt door cybercriminelen voor het aanbieden van gestolen gegevens, met name in verband met datalekken. De verandering kan mogelijk een poging zijn om toegang tot het platform te beperken of om de activiteiten van de cybercriminelen te verstoren.

Gestolen juwelen uit louvre via darkweb te koop aangeboden

Na de grote diefstal in het Louvre in Parijs is een beveiligingsfirma, CGI Group, benaderd om via het darkweb te onderhandelen over de verkoop van gestolen juwelen ter waarde van 88 miljoen euro. De juwelen, die nog niet zijn teruggevonden, werden aangeboden door iemand die beweerde de dieven te vertegenwoordigen. CGI besloot de autoriteiten in Parijs in te schakelen, maar bureaucratische vertragingen verhinderden dat er verder actie werd ondernomen. Het beveiligingsbedrijf had gehoopt de daders te kunnen traceren en de juwelen terug te krijgen. Dit incident doet denken aan eerdere succesvolle samenwerkingen van CGI bij het oplossen van andere grote diefstallen, zoals de miljoenenroof in Dresden in 2019. Inmiddels is Interpol betrokken bij de verspreiding van informatie over de gestolen goederen. Er is echter nog geen informatie over de locatie van de juwelen.

Proton onthult 300 miljoen gestolen inloggegevens, waarvan 49% wachtwoorden

Proton heeft bevestigd dat er 300 miljoen gestolen inloggegevens op het darkweb zijn ontdekt, waarvan 49% wachtwoorden bevat. Deze gegevens zijn afkomstig van zowel kleine bedrijven als individuele gebruikers, waarbij 71% van de records uit

gegevens van kleine en middelgrote bedrijven (SMB's) komt. Proton maakte gebruik van zijn nieuwe Data Breach Observatory-tool om deze informatie direct van de criminele marktplaatsen op het darkweb te verzamelen, in plaats van te vertrouwen op openbaar gemaakte gegevens van getroffen organisaties. De blootstelling van deze gegevens wijst op de kwetsbaarheid van wachtwoordbeveiliging, vooral gezien de vele gevallen van phishing en malware-aanvallen. Experts waarschuwen dat de misbruik van gestolen inloggegevens steeds vaker voorkomt, met aanvallers die gebruik maken van legitieme accounts en tools om in te breken. Gebruikers wordt geadviseerd om wachtwoorden te veranderen, waar mogelijk gebruik te maken van wachtwoorden zonder, en altijd twee-factor-authenticatie in te schakelen.

Eigenwallet biedt veilige, gedecentraliseerde Bitcoin-Monero swaps aan, handig voor cybercriminelen

Eigenwallet, voorheen bekend als UnstoppableSwap, biedt een platform voor gedecentraliseerde, veilige Bitcoin-Monero atomic swaps. Dit platform maakt gebruik van een geavanceerd cryptografisch protocol en open-source desktopsoftware. De service garandeert dat er geen KYC (Know Your Customer) wordt gevraagd, wat de privacy van gebruikers beschermt. De platformen zijn niet-custodial, wat betekent dat gebruikers de controle houden over hun eigen sleutels. Eigenwallet is ook beschikbaar via .onion en I2P-netwerken, wat extra anonimiteit biedt. De site heeft geen registratievereisten en biedt een peer-to-peer netwerk voor transacties. Hoewel de privacy scores hoog zijn, is de verwerkingstijd voor transacties vaak traag. Er is geen beleid voor een bug bounty of privacybeleid beschikbaar. Deze kenmerken maken het platform handig voor cybercriminelen die op zoek zijn naar manieren om transacties anoniem uit te voeren.

We are keeping an eye 👀 on you, cybercriminals!

China hervat export van Nexperia-producten onder voorwaarden

China heeft aangekondigd de export van Nexperia-producten, geproduceerd in Chinese fabrieken, onder bepaalde voorwaarden te hervatten. Deze beslissing volgt op gesprekken tussen de Amerikaanse president Donald Trump en zijn Chinese tegenhanger Xi Jinping, waarbij de exportbeperkingen werden versoepeld. Het exportverbod werd opgelegd door China nadat Nederland het bedrijf onder curatele had gesteld vanwege zorgen over het uitlekken van technologische kennis naar

China. De versoepeling van het exportverbod is bedoeld om de productie van cruciale chips voor de wereldwijde markt te waarborgen, vooral voor de auto-industrie, die werd getroffen door de verstoring van de chipleveringen. De specifieke voorwaarden voor de hervatting zijn nog niet duidelijk, maar China benadrukt dat bedrijven die aan bepaalde criteria voldoen, vrijstellingen kunnen krijgen.

Grote bedrijven gewapend tegen cyberaanvallen, kwetsbaarheid ligt bij toeleveranciers

Nederlandse bedrijven zijn steeds beter voorbereid op cyberaanvallen, maar de kwetsbaarheid ligt bij toeleveranciers, die vaak niet hetzelfde beveiligingsniveau kunnen bieden. Volgens experts zoals Willemijn Aerdts van de Universiteit Leiden, maken statelijke actoren uit landen als Rusland en China gebruik van deze zwakke schakels. Grote bedrijven in vitale sectoren, zoals de defensie- en chipindustrie, spoorwegen en vliegvelden, realiseren zich vaak hun kwetsbaarheid, maar kunnen niet altijd garanderen dat hun externe leveranciers dezelfde veiligheidsmaatregelen treffen. Aanvallers zoeken vaak naar manieren om via deze kleinere bedrijven toegang te krijgen tot grotere systemen, bijvoorbeeld door besmette hardware of malware te leveren. Bewustzijn over de dreigingen is essentieel, evenals het versterken van de beveiliging bij zowel grote bedrijven als hun toeleveranciers.

Zico Kolter leidt OpenAI safety panel met macht om onveilige AI-releases te stoppen

Zico Kolter, professor aan Carnegie Mellon University, leidt een panel bij OpenAI dat de autoriteit heeft om de release van nieuwe AI-systemen te stoppen als ze als onveilig worden beschouwd. Het panel heeft de mogelijkheid om technologische releases uit te stellen totdat de risico’s zijn gemitigeerd, bijvoorbeeld als AI wordt gebruikt voor massavernietigingswapens of schadelijk is voor de geestelijke gezondheid. Kolter benadrukt dat AI-beveiliging niet alleen gaat om existentiële dreigingen, maar ook over de bredere impact van AI op de samenleving. Na OpenAI’s recente verschuiving naar een voor-profit structuur, is het panel cruciaal geworden om te zorgen dat veiligheid voorop blijft staan bij zakelijke overwegingen. Kolter en zijn team worden nauwlettend gevolgd, aangezien ze een belangrijke rol spelen in het waarborgen van de veiligheid van AI-systemen.

Open VSX rotatie van tokens voorkomt supply-chain malware-aanval

De Open VSX-registry heeft toegangstokens geroteerd nadat deze per ongeluk waren gelekt door ontwikkelaars in openbare repositories, wat cybercriminelen in staat stelde schadelijke extensies te publiceren als onderdeel van een supply-chain aanval. De lekken werden twee weken geleden ontdekt door Wiz-onderzoekers, die meer dan 550 geheime sleutels blootlegden die toegang gaven tot projecten met 150.000 downloads. Het lek werd snel geïdentificeerd en de schadelijke extensies werden op 21 oktober uit de Open VSX-registry verwijderd. De aanval werd geïdentificeerd als "GlassWorm", die gebruik maakte van onzichtbare Unicode-tekens om ontwikkelaarsgegevens te stelen. De Open VSX en de Eclipse Foundation hebben aangekondigd extra beveiligingsmaatregelen te implementeren om dergelijke incidenten in de toekomst te voorkomen, waaronder kortere tokenlevenscycli en snellere intrekkingsprocessen voor gelekte tokens. Het incident werd inmiddels volledig ingedamd, zonder blijvende impact.

Saoedi-Arabië wil AI-grootmacht worden door energie in overvloed

Saoedi-Arabië wil zijn olie-inkomsten gebruiken om een wereldleider op het gebied van kunstmatige intelligentie (AI) te worden. Het onlangs opgerichte staatsbedrijf Humain, ondersteund door een investeringsfonds van 1000 miljard dollar en goedkope zonne-energie, ziet kansen om zich te positioneren tussen China en de VS. Humain heeft al samenwerkingen gesloten met grote AI-bedrijven zoals Nvidia en Amazon Web Services. De Saoedische overheid streeft ernaar om in tien jaar tijd 6 gigawatt aan datacenters te realiseren. Dit initiatief maakt deel uit van de bredere visie om de Saoedische economie minder afhankelijk te maken van olie-inkomsten. Humain’s CEO, Tareq Amin, gelooft niet in een AI-bubbel en ziet een enorme waarde in de toekomst van AI, ondanks de huidige onvolledige ontwikkeling van de technologie. De groei van AI is volgens Amin nog maar net begonnen.