Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

28-11-2025:

Hackers kapen Amerikaanse radioapparatuur om valse waarschuwingen en obscene berichten uit te zenden

In de Verenigde Staten hebben hackers recentelijk radioapparatuur gekaapt, waardoor valse noodwaarschuwingen en obscene berichten werden uitgezonden via het Emergency Alert System (EAS). Dit systeem, dat normaal gesproken gebruikt wordt om belangrijke waarschuwingen voor bijvoorbeeld natuurrampen te communiceren, werd misbruikt voor het verspreiden van ongepaste inhoud. De aanvallers wisten via slecht beveiligde apparatuur van het Zwitserse bedrijf Barix de controle over te nemen en vervalste noodsignalen en ongepaste berichten uit te zenden.

Hoewel dit incident plaatsvond in de VS, wijst het op een groter probleem met de beveiliging van systemen die gebruikt worden voor publieke communicatie. Dit kan ook relevant zijn voor Nederland en België, waar overheidsinstanties en andere organisaties dezelfde kwetsbaarheden kunnen ervaren. De FCC (Federal Communications Commission) heeft radiozenders aangespoord om basale beveiligingsmaatregelen te treffen, zoals het wijzigen van standaardwachtwoorden en het regelmatig updaten van apparatuur.

Dit incident onderstreept de kwetsbaarheid van communicatie-infrastructuren en de noodzaak voor goede beveiliging van apparaten die in kritieke systemen worden gebruikt. In Nederland en België moeten organisaties zich ervan bewust zijn dat dergelijke aanvallen ook in Europa kunnen plaatsvinden, en daarom is het essentieel om continue waakzaamheid te behouden en goede beveiligingspraktijken te volgen.

Noord-Koreaanse hackers misbruiken npm, GitHub en Vercel om OtterCookie-malware te verspreiden

Sinds oktober 2025 zijn er aanwijzingen dat Noord-Koreaanse staatshackers, opererend onder de codenaam "Contagious Interview", kwaadaardige software verspreiden via npm, GitHub en Vercel. Deze hackers maken gebruik van typosquatting-aanvallen om ontwikkelaars wereldwijd te misleiden en de OtterCookie-malware te installeren. Deze malware is een geavanceerd infostealer en remote access trojan die in staat is om gegevens van besmette systemen te stelen en op afstand te communiceren met de command-and-control-infrastructuur van de aanvallers.

De aanvallen maken gebruik van nep-pakketten op npm, een platform voor JavaScript-pakketten, die zich voordoen als legitieme bibliotheken. Wanneer ontwikkelaars deze pakketten installeren, wordt er automatisch een postinstall-script uitgevoerd, waarmee de malware wordt gedownload en uitgevoerd. Dit stelt de hackers in staat om controle over de systemen van de slachtoffers te krijgen en gevoelige informatie, zoals inloggegevens en cryptocurrency-wallets, te stelen.

De OtterCookie-malware is in staat om gegevens van verschillende besturingssystemen te verzamelen, waaronder Windows, macOS en Linux. Het heeft geavanceerde mechanismen om detectie te omzeilen, zoals het controleren of het slachtoffer zich op een virtuele machine bevindt, en het zorgt ervoor dat de malware alleen actief wordt op echte ontwikkelaarsmachines, niet op omgevingen die door onderzoekers worden gebruikt. Eenmaal geïnstalleerd, kan de malware op verschillende manieren persistent blijven op geïnfecteerde systemen, zoals door het aanmaken van geplande taken en het aanpassen van systeemregisterinstellingen.

De campagne maakt gebruik van goed georkestreerde aanvallen, waarbij nep-GitHub-accounts en Vercel-hosting worden ingezet om de malware te distribueren. Deze infrastructuur lijkt specifiek gericht op ontwikkelaars in de Web3- en cryptocurrency-sector. Het is opvallend dat de malware niet alleen gericht is op het stelen van inloggegevens van webapplicaties, maar ook het verzamelen van gegevens van meer dan 40 verschillende cryptocurrency-wallet extensies, waaronder populaire wallets als MetaMask en Phantom.

Deze aanval benadrukt de gevaren van supply chain-aanvallen, waarbij aanvallers misbruik maken van vertrouwde platforms en software om kwaadaardige code te verspreiden. Ontwikkelaars wordt aangeraden om waakzaam te blijven bij het installeren van externe pakketten en om beveiligingsmaatregelen te treffen om dergelijke aanvallen te voorkomen.

OpenAI lekt persoonlijke gegevens en metadata van API-gebruikers

OpenAI heeft bekendgemaakt dat er persoonlijke gegevens en metadata van een onbekend aantal API-gebruikers zijn gelekt, nadat aanvallers toegang hadden gekregen tot de systemen van analyticsprovider Mixpanel. Mixpanel, dat door OpenAI werd gebruikt voor het bijhouden van gebruikersactiviteiten van de API, werd op 8 november geconfronteerd met een inbraak, die op 9 november werd ontdekt. De gegevens die zijn gestolen, bevatten namen, e-mailadressen, locatiegegevens,

gebruikte besturingssystemen, browsers, referring websites en ID's van de organisaties die aan het API-account waren gekoppeld.

De inbraak werd pas op 25 november door Mixpanel gemeld aan OpenAI. Het datalek werd mogelijk gemaakt door een aanval op Mixpanel, een bedrijf dat analytics-software levert waarmee gebruikers kunnen analyseren hoe consumenten hun producten gebruiken. Nadat de inbraak werd ontdekt, heeft OpenAI onmiddellijk maatregelen genomen en Mixpanel van hun platform verwijderd. Het bedrijf waarschuwt gebruikers dat de gestolen informatie mogelijk kan worden ingezet voor social engineering- of phishingaanvallen.

De onthullingen over dit datalek hebben geleid tot veel kritiek van gebruikers, die zich zorgen maken over de trage reactie van Mixpanel en de beperkte informatie die werd gedeeld. De situatie is een verdere herinnering aan de risico's die gepaard gaan met de toegang tot persoonlijke gegevens via externe platforms en de noodzaak voor bedrijven om strengere beveiligingsmaatregelen te implementeren.

Kwetsbaarheid in populaire JavaScript-bibliotheek node-forge krijgt oplossing voor omzeilen handtekeningverificatie

Een kwetsbaarheid in de populaire JavaScript-cryptografiebibliotheek 'node-forge' is ontdekt, die aanvallers in staat zou stellen handtekeningverificaties te omzeilen. De kwetsbaarheid, aangeduid als CVE-2025-12816, kreeg een hoge ernstbeoordeling en werd veroorzaakt door de manier waarop de bibliotheek de ASN.1-validatiemechanismen behandelt. Deze fout maakt het mogelijk om misvormde gegevens te creëren die de verificatieprocessen kunnen omzeilen, zelfs wanneer de gegevens cryptografisch onjuist zijn.

De kwetsbaarheid wordt toegeschreven aan een conflict in de interpretatie van ASN.1-structuren in de versies van node-forge tot 1.3.1. Dit conflict stelt aanvallers in staat om de validatie van gegevens te desynchroniseren, wat kan leiden tot de omzeiling van downstream cryptografische controles en andere beveiligingsbeslissingen. Dit kan ernstige gevolgen hebben, vooral in omgevingen waar cryptografische verificatie een cruciale rol speelt in het nemen van vertrouwensbeslissingen.

De kwetsbaarheid werd ontdekt door onderzoeker Hunter Wodzenski van Palo Alto Networks, die de bevinding op verantwoorde wijze meldde bij de ontwikkelaars van node-forge. De impact van de kwetsbaarheid kan variëren, afhankelijk van de

specifieke toepassing, maar kan onder andere leiden tot omzeiling van authenticatie, manipulatie van ondertekende gegevens en misbruik van functies die verband houden met certificaten.

Gezien de populariteit van de node-forge bibliotheek, die bijna 26 miljoen wekelijkse downloads genereert via de Node Package Manager (NPM), kan de invloed van deze kwetsbaarheid aanzienlijk zijn. De bibliotheek wordt gebruikt in verschillende projecten die cryptografische en openbare infrastructuur (PKI) functies vereisen in JavaScript-omgevingen.

Een oplossing werd al uitgebracht in versie 1.3.2 van node-forge. Ontwikkelaars die de bibliotheek gebruiken, wordt geadviseerd om snel naar de nieuwste versie over te schakelen om zich te beschermen tegen mogelijke aanvallen. Ondanks de beschikbaarheid van een patch, kan het enige tijd duren voordat de kwetsbaarheid in de praktijk volledig wordt verholpen, vooral gezien de complexiteit van de omgeving en de noodzakelijke tests van de nieuwe code.

Nieuwe ShadowV2 botnet gebruikt AWS-uitval als testkans

Een nieuw botnet, ShadowV2, gebaseerd op de bekende Mirai-malware, heeft zich onlangs gericht op IoT-apparaten van verschillende leveranciers, waaronder D-Link, TP-Link en DigiEver. Dit botnet maakt gebruik van meerdere kwetsbaarheden, waaronder bekende zwaktes in router- en NAS-apparaten. Het werd opgemerkt tijdens de grote AWS-uitval in oktober 2025. Hoewel er geen direct verband is tussen de uitval en de botnet-aanvallen, was de activiteit van ShadowV2 uitsluitend waargenomen tijdens de duur van de storing, wat erop wijst dat het mogelijk om een test ging.

ShadowV2 maakt gebruik van acht kwetsbaarheden in IoT-apparaten om zich te verspreiden. Onder andere zijn er kwetsbaarheden in DD-WRT, D-Link, TP-Link, DigiEver en TBK-apparaten gebruikt. Het meest opvallende voorbeeld is een kwetsbaarheid in D-Link-apparaten, die al sinds 2020 bekend is maar niet gepatcht werd door de fabrikant. ShadowV2 maakt misbruik van deze zwaktes door apparaten over de hele wereld te infecteren.

De aanval is waargenomen in meerdere regio’s wereldwijd, waaronder Noord- en Zuid-Amerika, Europa, Afrika, Azië en Australië. Dit geeft de omvang van de dreiging aan, waarbij routers, NAS-apparaten en DVR's in sectoren zoals overheid, technologie, productie, telecommunicatie en onderwijs werden getroffen.

De malware zelf, ShadowV2, is vergelijkbaar met eerdere Mirai-varianten en is ontworpen om gedistribueerde denial-of-service (DDoS) aanvallen uit te voeren op UDP, TCP en HTTP-protocollen. Dit maakt het tot een krachtig middel voor cybercriminelen die via botnets aanvallen kunnen uitvoeren. De botnet-infrastructuur stuurt commando's naar de geïnfecteerde apparaten om aanvallen te initiëren.

Momenteel is nog niet bekend wie verantwoordelijk is voor ShadowV2, noch wat hun verdienmodel is, aangezien de botnet mogelijk niet gericht is op financieel gewin, zoals vaak het geval is bij DDoS-aanvallen. Experts waarschuwen gebruikers om de firmware van hun apparaten regelmatig bij te werken om dergelijke aanvallen te voorkomen.

Nieuwe Olymp Loader Malware-as-a-Service op Hackerforums Aangeboden met Anti-Analyse en Detectiekenmerken

Een nieuwe Malware-as-a-Service (MaaS)-dreiging genaamd "Olymp Loader" is sinds juni 2025 actief en wordt actief gepromoot op ondergrondse hackerforums zoals XSS en HackForums. De malware, gepromoot door een operator genaamd "OLYMPO", is een geavanceerd hulpmiddel dat volledig in Assembly-taal is geschreven. Het doel van deze marketingstrategie is om cybercriminelen aan te trekken door hoge prestaties en weerstand tegen reverse engineering te claimen. De tool fungeert als een veelzijdige suite die werkt als een loader, crypter en stealer, wat de drempel voor aanvallers verlaagt die gebruik willen maken van ontwijkingstechnieken en complexe infectieroutines.

Olymp Loader heeft snel de reputatie opgebouwd "Volledig Ondetecteerbaar" (FUD) te zijn, met een zeer lage detectiegraad op VirusTotal. Het verspreidt zich via social engineering-campagnes, waarbij het zich vaak voordoet als legitieme software-downloads zoals PuTTY, Zoom of Node.js-executables die worden gehost op platforms zoals GitHub. Deze misleidende vectoren overtuigen gebruikers om de kwaadaardige code uit te voeren, waardoor de infectieketen op de machine van het slachtoffer wordt geactiveerd. Het gebruik van gerenommeerde platforms zoals GitHub voor het hosten van de kwaadaardige bestanden maakt detectie complexer, omdat netwerkverkeer naar deze sites vaak legitiem lijkt voor beveiligingsapparaten.

Beveiligingsanalisten van Picus Security hebben geconstateerd dat Olymp Loader vaak gevaarlijke payloads levert, zoals LummaC2 en Raccoon Stealer. De malware is snel geëvolueerd, met een strategische verschuiving in augustus 2025 van een

botnet-architectuur naar een gestroomlijnd dropper-model. Deze verschuiving toont de snelle aanpassingsvermogen van de ontwikkelaar om technische uitdagingen en marktvraag vanuit de cybercriminelen te beantwoorden.

Een belangrijk onderdeel van de ontwijkingsstrategie van Olymp Loader is de inzet van geavanceerde anti-analysemechanismen om een succesvolle infectie te garanderen. De malware is in staat om Windows Defender uit te schakelen door specifieke PowerShell-opdrachten uit te voeren om de realtime bewaking uit te schakelen en paduitzonderingen voor scanning toe te passen. Dit proces zorgt ervoor dat de kwaadaardige code ongestoord kan draaien, ongehinderd door endpoint-beveiligingsoplossingen die op de host zijn geïnstalleerd. De verschuiving naar uitgebreidere uitsluitingslijsten in latere versies toont het vermogen van Olymp Loader om zich effectief te verbergen voor standaardbeveiligingscontroles.

Hackers maken misbruik van de populariteit van Battlefield 6 om stealer- en C2-agenten te verspreiden

Sinds de release van Battlefield 6 in oktober 2025 is het spel uitgegroeid tot een van de meest verwachte game-lanceringen van het jaar. Cybercriminelen hebben echter snel gebruikgemaakt van de populariteit van het spel om kwaadaardige software te verspreiden. Ze hebben nep-gecrackte versies van het spel en frauduleuze game trainers gecreëerd en verspreid via torrentwebsites en underground forums. Deze campagnes richten zich op nietsvermoedende spelers die op zoek zijn naar spelmodificaties.

De aanvallers gebruiken bekende game-crackgroepen zoals InsaneRamZes en RUNE om de nepbestanden geloofwaardigheid te geven en zo het vertrouwen van gebruikers te winnen. Dit is een veelgebruikte tactiek die ook in andere sectoren voorkomt, waarbij merken worden geïmiteerd om slachtoffers te misleiden.

De criminelen hebben drie verschillende soorten malware ontwikkeld, die elk verschillende doelen dienen. Deze malware varieert van informatie-stealers die browserdata en cryptocurrency-walletgegevens stelen, tot malware die op afstand controle kan uitoefenen over geïnfecteerde systemen.

Volgens onderzoekers van Bitdefender Labs werden deze kwaadaardige campagnes geïdentificeerd door meerdere monsterbestanden te analyseren. Ze ontdekten dat geen van de kwaadaardige bestanden daadwerkelijk de functionaliteit van Battlefield

6 bevatte, en dat ze waarschijnlijk afkomstig waren van verschillende dreigingsgroepen, gezien hun verschillende technische benaderingen.

De eerste malwarevariant opereert als een simpele maar agressieve informatie-stealer die zich vermomt als een "Battlefield 6 Trainer Installer." Het is eenvoudig te vinden op de tweede zoekpagina van Google, wat het zeer toegankelijk maakt voor potentiële slachtoffers. Zodra het wordt uitgevoerd, scant de malware lokale mappen en browserprofielen om gevoelige gegevens te stelen, zoals crypto-walletinformatie, sessies van browsers zoals Chrome, Edge en Firefox, en tokens van platforms zoals Discord.

De tweede variant, verspreid als “Battlefield 6.GOG-InsaneRamZes,” is geavanceerder en maakt gebruik van technieken om detectie te vermijden. Het blokkeert de uitvoering van de malware in landen als Rusland of de landen van de GOS en gebruikt Windows API-hashing om zijn activiteiten te verbergen. Deze malware voert ook anti-sandbox detecties uit, die controleren of het zich op een veilige omgeving bevindt.

De derde variant wordt verspreid als een ISO-afbeelding van Battlefield 6 en levert een persistente command-and-control agent. Dit bestand, met een grootte van 25 MB, bevat gecomprimeerde data die wordt uitgepakt en een bestand genaamd “2GreenYellow.dat” maakt. Het bestand wordt stilletjes uitgevoerd en probeert voortdurend verbinding te maken met een server, die lijkt te communiceren via de infrastructuur van Google. Dit wijst erop dat de malware in staat is om op afstand commando's uit te voeren of in de toekomst gegevens te stelen.

De campagne toont aan hoe cybercriminelen gebruikmaken van populaire spellen en andere digitale trends om malware te verspreiden en toegang te krijgen tot gevoelige gegevens. Deze aanvallen benadrukken het belang van voorzichtigheid bij het downloaden van software van onbetrouwbare bronnen.

Hackers richten zich actief op de telecom- en media-industrie om kwaadaardige payloads te verspreiden

Hackers hebben hun aanvallen op de telecom- en media-industrie de laatste maanden opgevoerd, waarbij ze steeds geavanceerdere technieken gebruiken om kwaadaardige payloads te verspreiden. Het doel van deze aanvallen is om kritieke infrastructuur van de sector te compromitteren en toegang te krijgen tot gevoelige systemen. Dergelijke campagnes worden steeds vaker geconstateerd, waarbij een

groeiend aantal netwerkoperators, mediaplatforms en uitzenddiensten doelwit zijn. Deze aanvallen worden gekarakteriseerd door een gestructureerde en gecoördineerde aanpak van geavanceerde, aanhoudende bedreigingsactoren die zich richten op het overnemen van systemen om langetermijncontrole te verkrijgen.

De aanvallen beginnen meestal met verkenning van kwetsbaarheden binnen de netwerkinfrastructuur, gevolgd door het strategisch inzetten van kwaadaardige payloads. Deze payloads worden vervolgens ontworpen om de aanvallers langdurige toegang te bieden, vaak via versleutelde communicatielijnen die de traditionele detectie-instrumenten kunnen omzeilen. Dit maakt het moeilijk voor organisaties om de indringers tijdig op te sporen.

In de afgelopen 90 dagen werden telecom- en mediabedrijven het meest getroffen, wat blijkt uit het feit dat 56 procent van alle geregistreerde aanvallen gericht was op deze sector. Met name ransomware-aanvallen, die gebruikmaken van kwetsbaarheden in webapplicaties en netwerkconfiguraties, zijn op grote schaal uitgevoerd. In veel gevallen wordt geheugengebaseerde uitvoering van malware gebruikt om de detectie te ontwijken en het systeem te compromitteren. Zodra de aanvallers toegang hebben, worden verschillende tactieken ingezet om de besmetting te bestendigen, zoals het aanpassen van registers, het opzetten van geplande taken en het injecteren van kwaadaardige code in legitieme processen.

De recente statistieken wijzen erop dat binnen de telecom- en media-industrie 65 bedrijven het slachtoffer zijn geworden van ransomware-aanvallen, waarvan 62 procent in de Verenigde Staten plaatsvond. Vooral de Qilin-groep blijkt bijzonder actief te zijn, maar ook andere opkomende groepen zoals Nightspire en Beast richten zich steeds meer op dit type infrastructuur. De systematische benadering van meerdere dreigingsactoren om een specifieke sector te destabiliseren wijst op een gecoördineerde poging om kritieke communicatie-infrastructuur te verstoren.

Deze aanvallen benadrukken de noodzaak voor organisaties binnen deze sectoren om geavanceerde detectiesystemen in te voeren en continue monitoring van netwerkinfrastructuren te handhaven, zodat aanvallen snel kunnen worden gedetecteerd en ingegrepen kan worden voordat de aanvallers langdurige toegang verkrijgen.

ByteToBreach verkoopt gevoelige wereldwijde data van luchtvaartmaatschappijen, banken en overheden

De cybercrimineel ByteToBreach is op dit moment een aanzienlijke bedreiging in de ondergrondse marktplaatsen, waar hij wereldwijd gevoelige gegevens van luchtvaartmaatschappijen, banken, universiteiten en overheden verhandelt. Het is duidelijk dat deze acteur al actief is sinds ten minste juni 2025, waarbij hij zijn technische vaardigheden combineert met agressieve zelfpromotie op verschillende DarkWeb-forums, Dread, Telegram en zelfs een publieke WordPress-website.

De doelwitten van ByteToBreach bevinden zich in diverse landen, waaronder Oekraïne, Kazachstan, Cyprus, Polen, Chili, Oezbekistan en de Verenigde Staten. De gelekte datasets bevatten onder meer passagierslijsten van luchtvaartmaatschappijen, gegevens van bankmedewerkers, databases van de gezondheidszorg en overheidsbestanden. Verschillende getroffen organisaties hebben deze inbreuken bevestigd of technische sporen geverifieerd, waarmee de authenticiteit van de claims wordt bevestigd.

Onderzoek door de beveiligingsonderzoekers van KELA heeft geleid tot de identificatie van ByteToBreach, die gebruik maakt van verschillende technische benaderingen, waaronder het misbruiken van bekende kwetsbaarheden in cloud- en bedrijfsinfrastructuren, het hergebruiken van gestolen inloggegevens van infostealers en phishingcampagnes, en het benutten van brute-force-aanvallen of misconfiguraties om toegang te krijgen.

Na toegang tot systemen, richt de aanvaller zich op het exfiltreren van gegevens, met de nadruk op personeelsbestanden, databases, back-ups en andere gevoelige documenten. In augustus 2025 werd een website opgericht onder de naam “Pentesting Ltd”, die eruitzag als een professionele dienstverlener en beweringen bevatte van gehackte bedrijven die als “klanten” werden gepresenteerd. De website bevatte banners met uitdagende uitspraken zoals “Laat me je gegevens beschadigen” en “Industrie leidende bedreigingsactor”.

Deze zaak benadrukt hoe moderne cybercriminelen legitieme technische capaciteiten combineren met criminele bedoelingen, waarbij ze marketingtechnieken gebruiken om gestolen gegevens te monetariseren op wereldwijde markten.

Kwaadaardige Chrome-extensie steelt ongemerkt Solana-kosten uit crypto-transacties

Een nieuwe dreiging heeft zich gemanifesteerd binnen de Solana-handelgemeenschap. Beveiligingsonderzoekers hebben een kwaadaardige Chrome-

extensie ontdekt, genaamd Crypto Copilot, die zich voordoet als een handige handelstool voor Solana-handelaren, maar in werkelijkheid stilletjes cryptocurrency steelt van gebruikers tijdens transacties. De extensie werd op 18 juni 2024 gepubliceerd op de Chrome Web Store en is sindsdien beschikbaar gebleven, terwijl het honderden handelaren heeft opgelicht die dachten een legitiem hulpmiddel te gebruiken.

De extensie stelt zich voor als een oplossing voor Solana-handelaren die snel swaps willen uitvoeren via het sociale mediaplatform X. Het is ontworpen om verbinding te maken met populaire wallets zoals Phantom en Solflare, en toont realtime tokeninformatie van DexScreener. Transacties worden via Raydium geleid, een van de grootste gedecentraliseerde beurzen op Solana. De marketingmaterialen beloven snelheid, gemak en één-klik-handel zonder enige vermelding van verborgen kosten of extra transacties.

Beveiligingsanalisten van Socket.dev ontdekten het kwaadaardige gedrag in de code van de extensie. Achter de aantrekkelijke interface bevindt zich een geavanceerd mechanisme om transactiekosten te stelen zonder dat de gebruiker het merkt. Elke keer dat een gebruiker een swap uitvoert, voegt de extensie een verborgen overdracht in die minimaal 0,0013 SOL of 0,05% van het totale transactiebedrag naar een door de aanvaller gecontroleerd wallet-adres stuurt.

De aanval werkt door de transactieconstructie op het blockchain-niveau te manipuleren. Wanneer gebruikers een swap starten, bouwt de extensie eerst de legitieme Raydium-swapinstructie op. Vervolgens voegt de extensie stilletjes een tweede instructie toe die een SystemProgram.transfer-commando bevat, waarmee SOL van de wallet van de gebruiker naar het adres van de aanvaller wordt overgemaakt. De gebruikersinterface toont alleen de swapgegevens, waardoor een valse indruk van legitimiteit wordt gecreëerd. Meeste wallet-bevestigingsschermen tonen een samenvatting van de transactie zonder de afzonderlijke instructies te markeren, zodat gebruikers een transactie ondertekenen die beide instructies uitvoert op de blockchain.

De onderzoekers ontdekten ook andere kwaadaardige functies in de extensie. De extensie exfiltreert de publieke sleutels van de aangesloten wallets naar een backend-server, waardoor er privacyproblemen ontstaan. Bovendien worden gevoelige infrastructuurgegevens blootgesteld door de embedded Helius RPC API-credentials, wat de beveiligingsrisico's verder vergroot.

Ondanks deze ontdekkingen is de Chrome Web Store-vermelding van de extensie onveranderd gebleven, zonder waarschuwingen voor potentiële gebruikers over de verborgen kosten of de gegevensverzameling die op de achtergrond plaatsvindt.

Europol haalt miljoenen gevaarlijke speelgoedpakketten van de Europese markt

Europol heeft recentelijk 16,6 miljoen vervalste en gevaarlijke speelgoedpakketten van de Europese markt gehaald. Deze actie werd uitgevoerd in samenwerking met 26 landen, waaronder Nederland en België, en leidde tot de inbeslagnames van producten ter waarde van 36,8 miljoen euro. De operatie richtte zich op de bestrijding van de illegale handel in speelgoed dat niet voldoet aan de strikte Europese veiligheidsnormen en waarvan bekend is dat het ernstige gezondheidsrisico's voor kinderen kan veroorzaken.

Vervalst speelgoed, dat vaak via reguliere handelsroutes Europa binnenkomt, vormt een ernstige bedreiging voor de gezondheid en veiligheid van kinderen. De speelgoedartikelen bevatten schadelijke stoffen en missen de noodzakelijke CE-markering, waardoor ze niet voldoen aan de veiligheidsvoorschriften die in de EU zijn vastgesteld. Er zijn al gevallen gemeld van verstikkingsgevaar, gehoorbeschadiging door te harde geluiden, en vergiftiging door schadelijke chemische stoffen in de producten.

De operatie maakt deel uit van een bredere Europese aanpak tegen de handel in vervalsingen, waarbij jaarlijks gecoördineerde acties plaatsvinden om de steeds groter wordende markt voor nepgoederen aan te pakken. De toysector is een van de zwaarst getroffen industrieën, met aanzienlijke financiële verliezen en schade aan de geloofwaardigheid van legitieme bedrijven.

In België en Nederland worden consumenten gewaarschuwd om bij de aankoop van speelgoed goed op de herkomst te letten. Vervalst speelgoed kan niet alleen schadelijk zijn voor kinderen, maar ook voor de economie door de belastingontduiking en de vernietiging van werkgelegenheid die ermee gepaard gaat.

Europol heeft samengewerkt met het Europees Octrooibureau (EUIPO) en het Europese Bureau voor Fraudebestrijding (OLAF) om de samenwerking te versterken en de effectiviteit van de operaties te verbeteren. Deze gezamenlijke inzet van Europese landen en private sectoren is essentieel in de strijd tegen de illegale

handel die niet alleen de veiligheid van consumenten bedreigt, maar ook de stabiliteit van de Europese markt.

Meer dan 100 lopende dossiers naar cyberoplichting in provincie Antwerpen: gemiddeld verlies van 37.000 euro per slachtoffer

In de provincie Antwerpen lopen momenteel meer dan 100 onderzoeken naar cyberoplichting, zo meldt cybercriminaliteitsexpert Peter Peereboom van het Antwerpse parket. Dit werd bekend gemaakt naar aanleiding van een onderzoeksreportage door Pano over elektronische oplichting. In de reportages wordt gedemonstreerd hoe oplichters via valse Facebook-advertenties, vaak met bekende gezichten, slachtoffers misleiden en hen aansporen tot investering in niet-bestaande zaken. Terwijl justitie en sociale media moeite hebben om deze misdaden te voorkomen en op te sporen, blijven de oplichters vaak onvindbaar.

Volgens Peereboom bedraagt het gemiddelde verlies voor slachtoffers in de provincie Antwerpen zo'n 37.000 euro. Dit bedrag kan echter variëren, waarbij sommige slachtoffers zelfs meer dan een miljoen euro verloren hebben. In veel gevallen begint de oplichting met een schijnbaar onschuldige investering van een paar honderd euro, maar het verhaal wordt opgebouwd zodat slachtoffers steeds meer moeten storten. Wanneer zij vervolgens proberen hun zogenaamde winsten op te nemen, blijkt er opnieuw een betaling nodig te zijn, bijvoorbeeld in de vorm van belastingen.

De kans dat de daders gevonden worden, lijkt klein, aldus Peereboom. De criminele organisaties achter deze oplichtingspraktijken zijn goed georganiseerd en bestaan vaak uit veel mensen, wat het voor het parket moeilijk maakt om effectieve actie te ondernemen, zeker gezien de beperkte middelen. De betrokken daders zijn vaak gevestigd in het buitenland, wat de opsporing verder bemoeilijkt. Het internet biedt hen bovendien een ideale speeltuin om hun misdaden uit te voeren, aangezien de digitale omgeving het gemakkelijker maakt om slachtoffers te vinden en geld snel weg te sluizen.

Peereboom waarschuwt voor de groeiende rol van kunstmatige intelligentie in deze oplichtingspraktijken. AI wordt steeds vaker ingezet om oplichters te helpen nog overtuigender over te komen, waardoor het steeds moeilijker wordt voor mensen om te onderscheiden wat echt is en wat niet. Dit maakt de digitale oplichting een steeds

groter probleem, niet alleen voor gewone burgers, maar zelfs voor bankmedewerkers die ook in de val trappen.

De impact van deze oplichtingen is groot, niet alleen financieel maar ook psychologisch. Slachtoffers voelen zich vaak enorm gedupeerd en zijn vaak niet in staat om hun verlies terug te krijgen, wat de ernst van het probleem onderstreept. De omvang van de oplichting laat zien dat dit een miljardenbusiness is die in de toekomst waarschijnlijk alleen maar groter zal worden.

Minister Van Oosten: online oplichting kan iedereen overkomen

Minister Van Oosten van Justitie en Veiligheid heeft gereageerd op de uitkomsten van recent onderzoek naar de herkenbaarheid van online oplichting. Volgens de minister overschatten veel mensen hun vermogen om oplichting te herkennen, wat hen kwetsbaar maakt voor digitale fraude. Het onderzoek, uitgevoerd onder Nederlanders, toont aan dat slechts tien procent van de deelnemers in staat was om alle nepberichten correct te identificeren. Daarnaast gaf 42 procent van de respondenten aan hun beoordelingsvermogen te overschatten, wat betekent dat zij dachten meer gevallen correct te hebben herkend dan in werkelijkheid het geval was.

De minister benadrukt dat online oplichting steeds moeilijker te onderscheiden is van legitieme communicatie. De oplichters gebruiken vaak technieken die het verschil tussen echt en nep extreem klein maken, waardoor het voor mensen lastiger is om een weloverwogen beslissing te nemen. Het verschil tussen echte en neppe berichten is vaak minimaal, wat de risico's vergroot. Van Oosten waarschuwt dan ook dat online oplichting iedereen kan overkomen, vooral nu deze steeds moeilijker te herkennen is.

De resultaten van het onderzoek worden door de overheid gebruikt voor de bewustwordingscampagne "Laat je niet interneppen". Deze campagne heeft als doel mensen te waarschuwen voor de gevaren van oplichting en hen aan te moedigen om waakzaam te zijn bij het ontvangen van onverwachte berichten. Yoanne Spoormans van de politie voegt hieraan toe dat oplichters vaak proberen hun slachtoffers onder tijdsdruk te zetten, bijvoorbeeld door een ‘noodsituatie’ te creëren. Dit maakt het moeilijker om rustig na te denken en kritisch te handelen.

De minister benadrukt verder dat het belangrijk is om altijd de tijd te nemen om de afzender van berichten te controleren, vooral wanneer er snel gehandeld moet

worden. De campagne beoogt dan ook mensen te helpen beter voorbereid te zijn op het herkennen van verdachte berichten en situaties.

Belgische datahandelaar krijgt boete voor illegale doorverkoop van gegevens

De Belgische datahandelaar Infobel is door de Gegevensbeschermingsautoriteit (GBA) beboet met 40.000 euro vanwege de illegale doorverkoop van persoonsgegevens voor marketingdoeleinden. Het bedrijf had gegevens die het van een telecomprovider had ontvangen, doorverkocht aan een media-agentschap, dat deze op zijn beurt gebruikte voor commerciële doeleinden. De GBA oordeelde dat Infobel niet over de juiste toestemming beschikte van de betrokkenen, waarmee het in strijd handelde met de Algemene Verordening Gegevensbescherming (AVG).

Volgens de GBA moest de toestemming voor het doorverkopen van gegevens specifiek, ondubbelzinnig en geïnformeerd zijn. Dit was echter niet het geval, aangezien Infobel geen actieve en expliciete toestemming had verkregen van de betrokkenen. De toezichthouder benadrukt dat toestemming voor verschillende doeleinden afzonderlijk moet worden gevraagd, zodat mensen de vrijheid hebben om per doel wel of niet toestemming te geven. Als gevolg van de overtreding moet Infobel niet alleen de boete betalen, maar ook de gegevens verwijderen waarvan het niet kan aantonen dat er geldige toestemming voor was. Daarnaast moet het bedrijf zijn zakelijke klanten inlichten over de genomen maatregelen. Infobel kan tegen de opgelegde boete in beroep gaan.

Franse overheid adviseert tegen biometrische beveiliging van telefoons

De Franse overheid heeft recentelijk een advies uitgebracht waarin wordt afgeraden om mobiele telefoons via biometrische methoden, zoals gezichtsherkenning of vingerafdrukken, te beveiligen. Dit advies komt van het Franse nationale bureau voor beveiliging van informatiesystemen (ANSSI), dat waarschuwt voor de risico's die dergelijke beveiligingsmethoden kunnen opleveren, vooral in het geval van spyware-aanvallen. In plaats daarvan wordt gebruikers aangeraden alternatieve beveiligingsmaatregelen te nemen om hun gegevens en communicatie te beschermen.

Het advies is onderdeel van een breder document dat het dreigingslandschap voor mobiele telefoons sinds 2015 beschrijft, waarbij de focus ligt op de toename van

spyware-aanvallen. Het ANSSI beveelt verschillende maatregelen aan, zoals het uitschakelen van automatisch ontvangen mms-berichten, het gebruik van end-to-end versleutelde chatapps voor gevoelige communicatie, en het uitschakelen van wifi, bluetooth en nfc wanneer deze niet in gebruik zijn. Bovendien wordt het gebruik van openbare wifi zonder een VPN afgeraden, en wordt de Lockdown Mode voor iPhones en de Advanced Protection Mode voor Android-telefoons aangeraden om extra bescherming te bieden tegen mogelijke aanvallen.

Een andere belangrijke aanbeveling is om de telefoon regelmatig opnieuw op te starten om bepaalde soorten spyware te verwijderen, en om het toestel volledig uit te schakelen wanneer het onbeheerd wordt achtergelaten. Voor het opladen van de telefoon wordt geadviseerd om gebruik te maken van een usb-datablocker om te voorkomen dat malware via de oplader toegang krijgt tot het toestel.

Het advies benadrukt ook dat gebruikers voorzichtig moeten zijn bij het gebruik van bepaalde apps en technologieën. Het ANSSI wijst erop dat het risico op spyware-aanvallen en andere vormen van digitale dreigingen blijft groeien, en dat de bescherming van persoonlijke gegevens en communicatie essentieel is voor het waarborgen van de privacy van gebruikers.

Kabinet steunt spoedig akkoord over digitale euro

Het Nederlandse kabinet heeft zich uitgesproken voor een spoedig akkoord over de digitale euro. In een brief aan de Tweede Kamer heeft demissionair minister Heinen van Financiën aangegeven dat Nederland de ambitie van het Deense EU-voorzitterschap ondersteunt om dit jaar nog tot een akkoord te komen. Dit plan wordt ook gedeeld door een toenemend aantal EU-lidstaten, die de voortgang van de onderhandelingen over de digitale euro steeds urgenter vinden.

De digitale euro is al enige tijd onderwerp van discussie binnen de Europese Unie. Twee jaar geleden bracht de Europese Commissie een voorstel naar voren, en het lijkt erop dat de EU-lidstaten nu de laatste hand leggen aan de voorstellen die besproken moeten worden. Over twee weken zullen Europese ministers tijdens de Ecofinraad de digitale euro opnieuw bespreken. Dit overleg is cruciaal voor de toekomst van de digitale euro, aangezien de ministers van Financiën en Economische Zaken van de EU-lidstaten zullen proberen een definitief standpunt in te nemen.

Minister Heinen heeft in zijn brief aangegeven dat Nederland de ambitie van Denemarken steunt om voor het einde van dit jaar een raadspositie over de digitale euro vast te stellen, mits er voldoende vooruitgang wordt geboekt over de resterende onderwerpen, zoals het kostenmodel en de verplichtingen omtrent de distributie van de digitale valuta. Het kabinet benadrukt dat een definitieve keuze pas gemaakt kan worden wanneer er duidelijkheid is over deze belangrijke kwesties.

De onderhandelingen over de digitale euro worden niet alleen op Europees niveau gevoerd. Ook het Europees Parlement en de Raad van de Europese Unie, die de regeringen van de EU-lidstaten vertegenwoordigt, moeten hun standpunt over de voorstellen bepalen voordat er een definitief besluit kan worden genomen. De Ecofinraad, die op 12 december aanstaande plaatsvindt, zal een belangrijke rol spelen in het bepalen van de verdere koers van de digitale euro.

Cyberaanval leidt tot verstoringen bij Londense gemeentebesturen

Op 26 november 2025 werd bekend dat meerdere Londense gemeentebesturen het slachtoffer werden van een cyberaanval, die leidde tot verstoringen in hun IT-systemen. De Royal Borough of Kensington and Chelsea (RBKC) en Westminster City Council (WCC) meldden dat ze aanzienlijke technische problemen ondervonden, waaronder de verstoring van telefoonlijnen, wat hen dwong om noodplannen in te schakelen om essentiële diensten voor hun inwoners te blijven bieden. De twee gemeenten delen een deel van hun IT-infrastructuur, wat de schade heeft vergroot.

Daarnaast werd de London Borough of Hammersmith and Fulham (LBHF), die ook enkele gezamenlijke diensten met RBKC en WCC deelt, getroffen door de aanval. LBHF nam verscherpte maatregelen om de netwerken te isoleren en te beveiligen, wat leidde tot onderbrekingen van de dienstverlening. De aanval heeft invloed gehad op de werking van verschillende gemeentelijke systemen, waaronder die voor het contacteren van de gemeenten via online kanalen en callcenters.

De betrokken autoriteiten gaven aan dat zij samenwerkten met gespecialiseerde cyberincident-experts en het National Cyber Security Centre (NCSC) om de systemen te beschermen, de schade te herstellen en essentiële diensten te blijven leveren. Er wordt onderzoek gedaan naar de daders en hun motieven, maar het is op dit moment nog te vroeg om te zeggen wie verantwoordelijk is voor de aanval en of er gegevens zijn gecompromitteerd. De gemeentebesturen hebben de Information

Commissioner's Office (ICO) op de hoogte gesteld, zoals voorgeschreven in de geldende protocollen.

Er is momenteel geen verklaring van ransomwaregroepen over deze aanval, hoewel beveiligingsexperts vermoeden dat de aanval het gevolg is van een aanval op een externe dienstverlener die door de drie gemeenten wordt gebruikt. De incidenten benadrukken de kwetsbaarheid van gezamenlijke IT-infrastructuren en de risico's die gepaard gaan met cyberaanvallen op lokale overheden.

Comcast betaalt 1,5 miljoen dollar boete na datalek bij leverancier

Comcast, een van de grootste telecom- en mediabedrijven in de Verenigde Staten, heeft ingestemd met het betalen van een boete van 1,5 miljoen dollar na een datalek bij een voormalige leverancier, Financial Business and Consumer Solutions (FBCS). Het datalek, dat plaatsvond tussen 14 en 26 februari 2024, leidde tot de blootstelling van persoonlijke gegevens van bijna 275.000 klanten. Het incident gebeurde bij FBCS, een bedrijf dat Comcast twee jaar eerder had verlaten. De gehackte gegevens omvatten namen, adressen, socialezekerheidsnummers, geboortedata en accountnummers van Comcast-klanten.

Hoewel FBCS Comcast in maart 2024 geruststelde dat het datalek geen invloed had op hun klanten, werd het bedrijf pas in juli 2024 op de hoogte gesteld van de werkelijke omvang van het probleem. Dit heeft tot ernstige zorgen geleid over de verantwoordelijkheid van bedrijven voor de beveiliging van klantgegevens, zelfs bij het uitbesteden aan externe leveranciers.

Comcast is overeengekomen met de Federal Communications Commission (FCC) om een uitgebreid nalevingsplan in te voeren, dat onder andere strengere controles op leveranciers en een verplichting om klantgegevens correct te verwijderen, omvat. Ook moet Comcast risicobeoordelingen uitvoeren van de leveranciers die klantgegevens verwerken.

Hoewel het datalek zich in de Verenigde Staten heeft voorgedaan, is het een belangrijk voorbeeld van de risico's die gepaard gaan met het delen van klantgegevens met externe partijen. Bedrijven in Nederland en België kunnen lessen trekken uit deze zaak door ervoor te zorgen dat hun leveranciers voldoen aan strikte beveiligingsvereisten om klantinformatie te beschermen tegen datalekken.

Vooral jongeren vaak de mist in bij online oplichting

Veel Nederlanders overschatten hun vermogen om online oplichting te herkennen. Uit onderzoek van de Rijksoverheid blijkt dat maar liefst negen op de tien mensen ooit slachtoffer zijn geworden van misleidende online berichten, ondanks het feit dat ze zichzelf vaak als goed in het herkennen van fraude beschouwen. Zo'n 50% van de Nederlanders denkt dat ze goed of zelfs heel goed in staat zijn om oplichting te herkennen, maar slechts 6% slaagt erin om online misleiding consistent te onderscheiden. Dit wijst op een groot verschil tussen de zelfbeoordeling en de werkelijkheid.

De leeftijdsgroep onder de 34 jaar blijkt bijzonder gevoelig voor online misleiding, ondanks dat zij vaker denken oplichters goed te kunnen identificeren. Zij beoordelen verdachte berichten vaak als betrouwbaar, terwijl oudere leeftijdsgroepen, zoals 55-plussers, minder snel slachtoffer worden van dergelijke oplichting. Dit verschil in gevoeligheid wordt mede veroorzaakt door de technologische vooruitgang, zoals kunstmatige intelligentie, die het voor oplichters makkelijker maakt om zeer gepersonaliseerde en moeilijk te onderscheiden berichten te versturen.

Minister van Justitie en Veiligheid, Foort van Oosten, benadrukt dat de technologische ontwikkelingen het steeds moeilijker maken om nepberichten te herkennen. Door de geringe verschillen tussen echt en nep en de overschatting van eigen vaardigheden, lopen veel mensen meer risico dan ze denken. In reactie op deze trend is de Rijksoverheid gestart met een meerjarige campagne om bewustwording te creëren en Nederlanders weerbaarder te maken tegen online oplichting.

Deze campagne richt zich onder andere op het advies om altijd drie seconden na te denken voordat men ergens op klikt, vooral wanneer tijdsdruk of te mooie aanbiedingen de overhand nemen. De overheid hoopt hiermee een breed publiek, en vooral jongeren, te helpen om betere keuzes te maken en minder snel in de val van oplichters te trappen.

Maker Fortnite vecht miljoenenboete om manipulatie kinderen aan

Epic Games, de maker van het populaire online spel Fortnite, is in beroep gegaan tegen een boete van de Autoriteit Consument en Markt (ACM), die het bedrijf in 2024 een boete van 1,1 miljoen euro oplegde. De ACM beschuldigt Epic ervan kinderen te manipuleren om onterecht geld uit te geven binnen het spel, dat oorspronkelijk gratis

is om te spelen. De inkomsten van het spel worden voornamelijk gegenereerd door de verkoop van virtuele items, zoals outfits en dansbewegingen voor de in-game karakters. De verkoop van deze items levert Epic miljarden euro's per jaar op.

De boete werd opgelegd nadat de ACM had vastgesteld dat Fortnite op illegale wijze gebruik maakte van methoden die kinderen aanspoorden om virtuele producten te kopen. Een specifiek punt van kritiek was het gebruik van aftellende timers bij bepaalde items, die kinderen onder druk zetten om snel aankopen te doen. Deze items waren vaak slechts tijdelijk beschikbaar, maar na het aflopen van de timer bleken ze soms alsnog te koop. Daarnaast werden spelers aangespoord met boodschappen als 'Get it now' en 'Buy now', wat volgens de ACM een directe vorm van misleiding is.

Epic Games heeft inmiddels enkele aanpassingen doorgevoerd onder druk van de ACM, zoals het verwijderen van de timers en het verplicht stellen van langere verkoopperiodes voor virtuele items. Desondanks blijft het bedrijf het recht om deze veranderingen terug te draaien, wat het nu juridisch betwist. De advocaten van Epic argumenteren dat hun reclamepraktijken niet verboden zouden moeten zijn, omdat gebruikers de aankopen nog moeten bevestigen voordat ze daadwerkelijk worden uitgevoerd. De ACM daarentegen betoogt dat het klikken op de koopknop al gelijkstaat aan het maken van een aankoopbeslissing, wat de kinderen volgens de toezichthouder blootstelt aan 'agressieve handelspraktijken'.

De rechtbank in Rotterdam behandelt momenteel de zaak en zal naar verwachting binnen zes weken uitspraak doen, al kan de beslissing door de feestdagen enige vertraging oplopen. Epic heeft ook bezwaar gemaakt tegen de manier waarop de ACM de term 'kinderen' definieert, aangezien de toezichthouder iedereen onder de 18 jaar als kind beschouwt. Volgens Epic zou er een onderscheid gemaakt moeten worden tussen jongere kinderen en tieners van 16 jaar en ouder, maar de ACM wijst dit argument af op basis van onderzoek naar het gebruik van Fortnite door kinderen, inclusief zelfs gebruikers van 5 tot 8 jaar oud.

De uitkomst van deze zaak zou gevolgen kunnen hebben voor de manier waarop andere bedrijven hun producten aan kinderen verkopen, vooral in de context van online gaming en microtransacties.

OpenAI wijt zelfdoding Amerikaanse jongen aan verkeerd gebruik van ChatGPT

OpenAI, het bedrijf achter de populaire chatbot ChatGPT, heeft gereageerd op de rechtszaak die is aangespannen door de familie van de 16-jarige Adam Raine. Raine, een jongen uit Californië, pleegde zelfdoding in april 2025, en zijn familie beschuldigt ChatGPT van het aansteken van zijn zelfdodingsgedachten door het verstrekken van advies over methoden om zijn leven te beëindigen. Volgens de familie kreeg Raine van de chatbot niet alleen suggesties voor dodelijke methoden, maar werd hij ook aangemoedigd om een afscheidsbrief te schrijven aan zijn ouders.

OpenAI heeft de beschuldigingen echter ontkend en stelt dat de jongen de technologie "verkeerd" heeft gebruikt. Het bedrijf beweert dat ChatGPT is ontworpen om mensen te helpen, en dat het geen verantwoordelijkheid kan dragen voor het gebruik van de chatbot door de jongen, dat volgens OpenAI in strijd was met hun gebruiksvoorwaarden. De voorwaarden verbieden onder andere het vragen om advies over zelfdoding of het vertrouwen op de antwoorden van de chatbot als feitelijke informatie.

De advocaat van de familie, Jay Edelson, heeft gereageerd op de verklaring van OpenAI en noemt het "verontrustend" dat het bedrijf de schuld bij het slachtoffer legt. Hij benadrukt dat de chatbot mogelijk geen adequate maatregelen heeft getroffen om dergelijke risicovolle interacties te voorkomen, wat zou kunnen duiden op tekortkomingen in de ontwikkelingsfase.

Dit tragische incident heeft geleid tot meerdere rechtszaken tegen OpenAI, waarbij andere gebruikers eveneens claimen dat de chatbot hen in gevaarlijke situaties heeft gebracht. OpenAI benadrukt echter dat het actief werkt aan het verbeteren van de veiligheid en ethiek van de chatbot, waaronder het trainen van de technologie om emotionele signalen te herkennen en gebruikers aan te moedigen hulp van echte mensen te zoeken bij emotionele problemen.

Het debat over de verantwoordelijkheid van AI in dergelijke gevallen wordt steeds heftiger. OpenAI heeft aangegeven dat het bedrijf zorgvuldig en respectvol omgaat met rechtszaken die betrekking hebben op de geestelijke gezondheid van gebruikers en hoopt op een transparante behandeling van deze zaak.

DigiD blijft in Nederlandse handen; staatssecretaris zet Amerikaanse overname op losse schroeven

De toekomst van de digitale infrastructuur rondom DigiD is momenteel in onzekerheid, aangezien de overname van IT-dienstverlener Solvinity door het

Amerikaanse bedrijf Kyndryl op losse schroeven staat. Solvinity speelt een cruciale rol in het beheer van DigiD, het digitale identificatiesysteem dat essentieel is voor de toegang tot overheidsdiensten in Nederland. De Autoriteit Consument en Markt (ACM) heeft onlangs aangegeven dat een akkoord over de overname nabij is, maar er is veel bezorgdheid over de gevolgen van buitenlandse controle over dergelijke kritieke infrastructuur.

De zorgen worden gedeeld door verschillende experts, die wijzen op de risico's van het beheren van Nederlandse gegevens door een Amerikaans bedrijf. Zo zou het Amerikaanse bedrijf, onder de Amerikaanse Cloud Act, verplicht kunnen worden om data te delen met de Amerikaanse overheid, zelfs tegen de wensen van Nederland in. Daarnaast wordt gewezen op de gevaren van buitenlandse invloed op essentiële systemen zoals DigiD, vooral in geval van politieke spanningen.

In reactie op deze bezorgdheden benadrukte staatssecretaris Eddie van Marum van Digitalisering dat DigiD onder Nederlandse controle blijft en dat Solvinity geen toegang heeft tot de eigenlijke DigiD-gegevens. Van Marum stelde dat de overname van Solvinity nog niet definitief is en dat de regering juridische en operationele implicaties onderzoekt. Hij deelde echter de zorgen van experts niet volledig en gaf aan dat er al strikte wetgeving bestaat voor bedrijven die kritieke infrastructuur beheren.

Tegelijkertijd blijft het kabinet inzetten op het versterken van de digitale soevereiniteit van Nederland. Van Marum onderstreepte dat het beschermen van digitale systemen en gegevens een topprioriteit blijft, en dat Nederland werkt aan eigen AI- en cloudoplossingen om minder afhankelijk te zijn van buitenlandse techbedrijven.

Dit onderwerp heeft veel politieke en maatschappelijke aandacht getrokken. De Nederlandse overheid stelt dat de veiligheid van de persoonsgegevens van burgers niet in gevaar mag komen, en daarom wordt er continu onderzoek gedaan naar de impact van de overname. Ook Logius, de beheerder van DigiD, heeft aangegeven dat de veiligheid van de digitale infrastructuur te allen tijde gewaarborgd blijft, en dat zij onmiddellijk maatregelen zullen nemen als er risico's worden geconstateerd.

Gainsight breidt lijst van getroffen klanten uit na Salesforce-beveiligingsmelding

Gainsight heeft bekendgemaakt dat de recente verdachte activiteiten die zijn applicaties hebben getroffen meer klanten hebben beïnvloed dan eerder werd

gedacht. Het bedrijf meldde dat Salesforce aanvankelijk een lijst met drie getroffen klanten had verstrekt, maar dat deze lijst op 21 november 2025 werd uitgebreid. Het exacte aantal getroffen klanten werd niet gedeeld, maar de CEO van Gainsight, Chuck Ganapathi, gaf aan dat momenteel slechts een klein aantal klanten weet van gegevens die zijn getroffen.

De ontdekking volgt op een waarschuwing van Salesforce over 'ongewone activiteiten' die verband hielden met Gainsight-applicaties die verbonden zijn met het platform. Als reactie hierop werd de toegang tot deze applicaties ingetrokken en werden de tokens die eraan gekoppeld waren vernieuwd. De cybercriminaliteitsgroep ShinyHunters (ook bekend als Bling Libra) heeft de aanval opgeëist.

In een reeks voorzorgsmaatregelen werden de integraties van Gainsight met platforms zoals Zendesk, Gong.io en HubSpot tijdelijk opgeschort. Google heeft OAuth-clients met callback-URL's zoals gainsightcloud[.]com gedeactiveerd. HubSpot stelde in zijn eigen bericht dat er geen bewijs is gevonden voor een compromittering van hun eigen infrastructuur of klanten.

Gainsight heeft aangegeven dat de applicaties van het bedrijf die toegang hadden tot Salesforce-gegevens tijdelijk niet meer beschikbaar zijn voor lees- en schrijfbewerkingen. Dit betreft onder andere de producten Customer Success, Community, Northpass en Skilljar. Het bedrijf benadrukte echter dat Staircase, een ander product, niet door het incident is getroffen, hoewel Salesforce de verbinding met Staircase uit voorzorg heeft verwijderd.

De aanvallers gebruikten de 'Salesforce-Multi-Org-Fetcher/1.0' user-agent voor ongeautoriseerde toegang, een tool die eerder al werd gebruikt bij aanvallen op andere platforms. Volgens informatie van Salesforce werd de eerste verkenning van getroffen klanten geregistreerd op 23 oktober 2025, gevolgd door verschillende pogingen tot ongeautoriseerde toegang vanaf 8 november 2025.

Gainsight heeft klanten aangespoord om verschillende maatregelen te nemen om hun systemen te beveiligen, zoals het roteren van S3-buckettoegangssleutels en andere connectoren, het rechtstreeks inloggen op Gainsight NXT in plaats van via Salesforce, en het resetten van wachtwoorden van gebruikers die geen gebruik maken van Single Sign-On (SSO).

Dit incident komt op een moment dat de ransomware-as-a-service (RaaS) platformen zoals ShinySp1d3r, die door ShinyHunters en andere cybercriminaliteitsgroepen wordt gebruikt, steeds geavanceerder worden. ShinySp1d3r heeft diverse nieuwe

technieken geïntroduceerd, waaronder het gebruik van kunstmatige intelligentie (AI) voor encryptie en de verspreiding van malware binnen netwerken.

Ransomwaregroep steelt data van 1,9 miljoen mensen bij bierbrouwer Asahi

Bij een ransomware-aanval op de Japanse bierbrouwer Asahi zijn de persoonsgegevens van 1,9 miljoen mensen gestolen. Het gaat hierbij om gegevens zoals namen, geslacht, adresgegevens, telefoonnummers en e-mailadressen van personen in Japan, waarvan het merendeel contact had met de klantenservice van Asahi. De aanval werd eind september ontdekt, maar Asahi heeft nu pas volledige details over de gestolen informatie vrijgegeven.

De aanvallers wisten toegang te krijgen tot het datacenternetwerk van Asahi via netwerkapparatuur. Dit resulteerde in een verstoring van de productie en distributie van de bierproducten, waardoor supermarkten in Japan zich zorgen maakten over tekorten aan Asahi-bier. Sinds de aanval heeft het bedrijf gewerkt aan het herstellen van de systemen en het versterken van de cybersecurity om toekomstige aanvallen te voorkomen. Ondanks de voortgang in het herstel, wordt verwacht dat het logistieke systeem van Asahi pas in februari volledig hersteld zal zijn.

Deze incidenten benadrukken de risico's van ransomware-aanvallen voor zowel bedrijven als consumenten, waarbij de gevolgen zich niet alleen beperken tot directe financiële verliezen, maar ook tot de blootstelling van gevoelige persoonsgegevens.

Schotse raad al twee jaar bezig met herstel van ransomware-aanval

De Comhairle nan Eilean Siar, de Raad voor de Western Isles in Schotland, is inmiddels al twee jaar bezig met het herstel van de schade veroorzaakt door een ransomware-aanval, die plaatsvond begin november 2023. De directe kosten van deze aanval worden geschat op meer dan 1 miljoen euro. Volgens een rapport van de Schotse Accounts Commission is het onduidelijk hoe de aanval precies heeft kunnen plaatsvinden, maar uit onderzoek blijkt dat de continuïteitsplannen van de raad niet waren afgestemd op de omvang van de aanval.

Bovendien waren er al eerder zwakke plekken in de IT-omgeving en de governance van de raad geïdentificeerd, maar deze werden niet opgelost voordat de aanval plaatsvond. Het tekort aan IT-personeel was een andere factor die de gevolgen van de aanval vergrootte. Van de aanbevelingen die na een eerdere audit waren gedaan,

was slechts de helft volledig doorgevoerd. Onder de onafgeronde aanbevelingen bevonden zich het trainen van personeel, het testen van responseplannen en het naleven van de cybersecurityprincipes van het Britse National Cyber Security Centre (NCSC).

Het herstelproces is nog steeds gaande en er wordt verwacht dat het ook in 2026 voortduurt. Bij de aanval werden niet alleen systemen versleuteld, maar ook belangrijke back-ups. Een deel van de data is permanent verloren gegaan. De raad werkt momenteel aan het herstel van historische en actuele data, wat een langdurige klus blijkt te zijn.

Qilin RaaS onthult 1 miljoen bestanden en 2 TB aan data in verband met Zuid-Koreaanse MSP-inbraak

De “Korean Leaks”-campagne is een van de meest geavanceerde supply chain-aanvallen die recentelijk gericht was op de financiële sector van Zuid-Korea. Deze operatie maakte gebruik van de capaciteiten van de Qilin Ransomware-as-a-Service (RaaS) groep, met mogelijke betrokkenheid van Noord-Koreaanse staatsgeassocieerde actoren, bekend als Moonstone Sleet. De aanvallers gebruikten een gecompromitteerde Managed Service Provider (MSP) als toegangspunt, wat hen in staat stelde om meerdere organisaties via één enkele toegangspoort te infiltreren.

In september 2025 werd Zuid-Korea plotseling het op één na meest aangevallen land op het gebied van ransomware, met 25 slachtoffers in één maand. Deze ongewone toename werd uitsluitend toegeschreven aan de Qilin ransomware-groep, die zich vrijwel volledig richtte op financiële dienstverleners, met name vermogensbeheerbedrijven. Van de 33 totaal gedupeerden zijn er 28 openbaar geworden, en documentatie bevestigt dat meer dan 1 miljoen bestanden en 2 TB aan data zijn gestolen.

De aanvallen werden in drie golven uitgevoerd. De eerste golf bracht op 14 september 2025 de aanval aan het licht en werd gepresenteerd als een publieke service-inspanning om systemische corruptie bloot te leggen. De tweede golf richtte zich met escalatie op de Koreaanse aandelenmarkt, terwijl de derde golf resulteerde in negen aanvullende slachtoffers, waarna de aanvallers terugkeerden naar standaard afpersingsberichten.

De initiële kwetsbaarheid was een gemeenschappelijke IT-serviceprovider voor de slachtoffers, wat resulteerde in een versnelde en nauwkeurige verspreiding van de

aanval. Het onderzoek bevestigde dat meer dan 20 vermogensbeheerbedrijven werden getroffen door de aanval via de gehackte MSP, wat verklaart waarom de aanvallen zo snel en gecoördineerd plaatsvonden.

De campagne wordt gezien als een zorgwekkende ontwikkeling in de grens tussen cybercriminaliteit en staatssponsoring, vooral door de samenwerking met Moonstone Sleet. Dit versterkt de bezorgdheid over de escalatie van cyberaanvallen en de betrokkenheid van staten bij dergelijke aanvallen.