Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

04-12-2025:

Bpost bevestigt 'cyberincident' met gestolen klantengegevens na publicatie door ransomwarebende

Bpost heeft een "cyberincident" bevestigd nadat eerder deze week 30GB aan data van het postbedrijf door een ransomwaregroep werd gepubliceerd. Het bedrijf beschrijft het incident als een "beperkt datalek" waarbij persoonlijke en zakelijke informatie van een "klein aantal klanten" zou zijn gestolen.

De hack vond plaats bij een specifieke afdeling van bpost die losstaat van de post- en pakketbezorging. Deze afdeling maakt gebruik van een uitwisselingsplatform dat beheerd wordt door een externe leverancier. Het bedrijf heeft niet gespecificeerd wat voor type gegevens precies zijn buitgemaakt.

Bpost meldt dat het direct maatregelen heeft genomen om het datalek in te perken en dat de dagelijkse operaties van het bedrijf hierdoor niet worden beïnvloed. Het postbedrijf werkt naar eigen zeggen samen met cyberexperts en heeft de autoriteiten over het incident geïnformeerd. De betrokken klanten zullen "tijdig geïnformeerd" worden over het incident.

De 30GB aan data, verdeeld over 5140 bestanden, verscheen eerder deze week op de website van de ransomwaregroep TridentLocker. Er is geen informatie vrijgegeven over de vraag of bpost om losgeld is gevraagd.

Oekraïense hackers intensiveren aanvallen op Russische luchtvaart- en defensiesector

Aan Oekraïne gelinkte hackers hebben hun cyberaanvallen op de Russische luchtvaartindustrie en de bredere defensiesector geïntensiveerd. Dit gebeurt met behulp van op maat gemaakte malware en gerichte spear-phishing om gevoelige informatie zoals ontwerpen, planningen en interne e-mails te stelen. De campagne richt zich zowel op de belangrijkste aannemers als op kleinere leveranciers binnen de sector. Het primaire doel van de operatie is het in kaart brengen van productieketens en het blootleggen van kwetsbaarheden binnen de Russische oorlogsindustrie. De gestolen data, waaronder informatie van onderzoekslaboratoria, testlocaties en logistieke bedrijven die vliegtuigen, drones en raketsystemen ondersteunen, kan inzicht geven in onderdelentekorten, leveringsvertragingen en softwarefouten. Dit biedt Oekraïense planners een duidelijker beeld van de operationele gereedheid van Rusland.

De kwaadaardige software werd voor het eerst opgemerkt eind 2024 in de vorm van spear-phishing golven. Deze e-mails werden gericht verstuurd naar ingenieurs en projectmanagers die werkzaam zijn in avionica, geleidingssystemen en

satellietverbindingen. De lokmiddelen bestonden uit valse vacatures, uitnodigingen voor conferenties of updates over contracten. De bijlagen in deze e-mails exploiteerden vaak verouderde kantoorsoftware op Windows-hosts. Na het openen van het bestand, plaatste het een kleine loader die onopgemerkt de weg vrijmaakte voor de hoofd-payload. Beveiligingsanalisten van Intrinsec identificeerden de malware nadat ze herhaaldelijk uitgaand verkeer hadden waargenomen vanuit een afgelegen kantoor van een defensie-integrator naar zeldzame commandoservers die werden gehost op robuuste infrastructuur. Het technische onderzoek toonde aan dat de aanvallers elke payload zorgvuldig hadden afgestemd op de rol van het slachtoffer, door het toevoegen van op maat gemaakte modules voor het verzamelen van e-mails, het stelen van documenten en het vastleggen van inloggegevens.
De infectieketen, hoewel eenvoudig, wordt als intelligent beschouwd. De eerste loader, vaak een kleine DLL, wordt alleen in het geheugen uitgevoerd en haalt een tweede-fase script op via een vooraf gedefinieerde URL. Dit script injecteert vervolgens de uiteindelijke payload in een vertrouwd proces, zoals explorer.exe, waardoor het moeilijker te onderscheiden is van normale gebruikersactiviteit. De payload maakt gebruik van een compacte commandolus om flexibel te blijven. Deze logica stelt de operator in staat om te schakelen tussen stille data-diefstal en handmatige controle. Ondanks het duidelijke ontwerp, vermijdt de malware opzichtige persistentietrucs. In plaats daarvan vertrouwt het op geplande taken en gekaapte updatetools om na herstarts terug te keren, terwijl het moeilijk te detecteren blijft. De gebruikte tools zijn fundamenteel eenvoudig, maar worden ingezet met precisie en planning.

Tienduizenden WordPress-sites kwetsbaar door kritiek RCE-lek in plug-in
Tienduizenden WordPress-websites lopen momenteel een ernstig beveiligingsrisico door de aanwezigheid van een kritieke kwetsbaarheid in de plug-in Advanced Custom Fields: Extended. Door dit lek kunnen kwaadwillenden op afstand de volledige controle over een website overnemen via zogeheten remote code execution (RCE). Hoewel er sinds 21 november een beveiligingsupdate beschikbaar is, blijkt uit actuele cijfers dat tienduizenden beheerders deze update nog niet hebben geïnstalleerd.
Het beveiligingslek is geregistreerd onder de code CVE-2025-13486 en is vastgesteld in de plug-in Advanced Custom Fields: Extended. Dit is een specifieke uitbreiding voor de veelgebruikte Advanced Custom Fields (ACF) plug-in. Terwijl de basisversie van ACF op meer dan twee miljoen websites actief is, wordt de kwetsbare 'Extended' variant op ruim honderdduizend websites gebruikt. Het beveiligingsbedrijf Wordfence, dat het lek rapporteerde, heeft de ernst van de kwetsbaarheid vastgesteld op een score van 9.8 op een schaal van 1 tot 10.

De oorzaak van het probleem ligt in een functie binnen de software die op afstand kan worden aangeroepen, maar de gebruikersinvoer niet correct verwerkt. Hierdoor kunnen aanvallers zonder enige vorm van authenticatie willekeurige code uitvoeren op de server. Naast het uitvoeren van code stelt de kwetsbaarheid aanvallers in staat om willekeurige andere WordPress-functies aan te roepen. Een van de mogelijke scenario's is dat een aanvaller zichzelf een nieuw beheerdersaccount toewijst, waardoor de website volledig kan worden overgenomen.
De ontwikkelaars van Advanced Custom Fields: Extended hebben op 21 november versie 0.9.2 uitgebracht om dit beveiligingslek te verhelpen. Uit data van WordPress.org blijkt echter dat de uitrol van deze patch traag verloopt. Meer dan vijftigduizend websites die de plug-in gebruiken, hebben de update nog niet geïnstalleerd. Zolang deze websites op een verouderde versie draaien, blijven zij vatbaar voor aanvallen die gebruikmaken van deze specifieke kwetsbaarheid.

Kritieke kwetsbaarheden in Picklescan lieten kwaadaardige PyTorch modellen onopgemerkt code uitvoeren
Drie kritieke beveiligingsfouten zijn recentelijk openbaar gemaakt in de open-source tool Picklescan, een hulpprogramma dat is ontworpen om Python pickle-bestanden te scannen op verdachte import- of functieoproepen voordat deze worden uitgevoerd. Pickle is een veelgebruikt serialisatieformaat binnen machine learning, onder meer door PyTorch, om modellen op te slaan en in te laden. Dit formaat brengt echter een aanzienlijk beveiligingsrisico met zich mee, aangezien het kan worden misbruikt om automatisch willekeurige Python-code uit te voeren zodra een bestand wordt geladen. Picklescan is juist bedoeld om dit risico te mitigeren.
De door JFrog ontdekte kwetsbaarheden maakten het in essentie mogelijk om de scanner te omzeilen, de gescande modelbestanden als veilig te presenteren en de uitvoering van kwaadaardige code mogelijk te maken. Dit opende de deur voor een mogelijke supply chain-aanval door de distributie van schadelijke machine learning-modellen met ondetecteerbare code.
De drie geïdentificeerde kritieke fouten (CVE-2025-10155, CVE-2025-10156 en CVE-2025-10157) hadden alle een hoge CVSS-score. CVE-2025-10155 betrof een omzeiling van de bestandsextensie, waardoor de scanner kon worden ondermijnd en het model toch werd geladen bij gebruik van een standaard pickle-bestand met een PyTorch-gerelateerde extensie zoals .bin of .pt. CVE-2025-10156 maakte het mogelijk om het scannen van ZIP-archieven uit te schakelen door een Cyclic Redundancy Check (CRC)-fout te introduceren. De derde fout, CVE-2025-10157, betrof een omzeiling van Picklescan's controle op onveilige globale variabelen, wat leidde tot de uitvoering van willekeurige code door een bloklijst van gevaarlijke imports te omzeilen. Succesvolle

exploitatie van deze kwetsbaarheden stelde aanvallers in staat om kwaadaardige pickle payloads te verbergen in bestanden met gangbare PyTorch-extensies of opzettelijk CRC-fouten te introduceren in ZIP-archieven die schadelijke modellen bevatten. Na een verantwoordelijke melding op 29 juni 2025 zijn de drie kwetsbaarheden opgelost in Picklescan versie 0.0.31, die op 9 september werd uitgebracht.
Daarnaast werd door SecDim en DCODX nog een vierde kwetsbaarheid (CVE-2025-46417) met hoge ernst in dezelfde tool gedetailleerd. Deze fout kon worden misbruikt om de bloklijst van Picklescan te omzeilen en kwaadaardige pickle-bestanden toe te staan gevoelige informatie via DNS te exfiltreren wanneer het model werd geladen. In een geschetst aanvalsscenario kon een aanvaller legitieme Python-modules zoals linecache en ssl hergebruiken om gevoelige gegevens uit bestanden zoals /etc/passwd te lezen en deze gegevens via ssl.get_server_certificate() naar een domein onder hun controle te verzenden. De gelekte inhoud verscheen in DNS-logs.
Deze bevindingen illustreren fundamentele problemen, waaronder een te grote afhankelijkheid van één scanningtool en discrepanties in de manier waarop beveiligingstools en PyTorch omgaan met bestanden. Dit maakt de beveiligingsarchitecturen kwetsbaar voor aanvallen. Deskundigen benadrukken dat de toenemende complexiteit van AI-bibliotheken zoals PyTorch, met nieuwe functies, modelformaten en uitvoerpaden, sneller groeit dan beveiligingsscanningtools zich kunnen aanpassen.

Kritieke Elementor-kwetsbaarheid laat aanvallers WordPress-adminrechten verkrijgen

Een ernstige kwetsbaarheid is geïdentificeerd in de King Addons for Elementor WordPress-plug-in, een component die wereldwijd in meer dan tienduizend actieve installaties wordt gebruikt. De kwetsbaarheid, geclassificeerd als een niet-geauthenticeerde privilege-escalatie, stelt aanvallers in staat om volledige administratieve controle over de getroffen WordPress-websites te verkrijgen. Dit wordt bereikt door het registreren van een nieuw account met beheerdersrechten zonder enige noodzakelijke authenticatie.
Het beveiligingslek, aangeduid met CVE-2025-8489, heeft een kritieke CVSS-score van 9.8. De grondoorzaak ligt in een onjuiste rolbeperking binnen de gebruikersregistratiefunctie van de plug-in. Het probleem bevindt zich specifiek in de handle_register_ajax() functie, die faalt in het adequaat valideren van de gebruikersrol tijdens het aanmaken van een account. Een aanvaller kan hierdoor een speciaal opgesteld registratieverzoek versturen via de plug-in's AJAX-handler, waarbij

de gewenste rol als 'administrator' wordt gespecificeerd, wat vervolgens door het systeem wordt geaccepteerd.
Zodra de aanvallers administratieve toegang hebben verkregen, beschikken zij over de mogelijkheid om kwaadaardige bestanden te uploaden, de website-inhoud te manipuleren, spam te injecteren, of achterdeurtjes te installeren om persistente toegang tot de gecompromitteerde omgeving te behouden.
Het beveiligingsprobleem werd oorspronkelijk gemeld op 24 juli 2025. Op 25 september 2025 bracht de leverancier een gepatchte versie, 51.1.35, uit die de onderliggende fout verhelpt. Beveiligingsanalisten van Wordfence identificeerden de kwetsbaarheid en maakten de details op 30 oktober 2025 openbaar via de Wordfence Intelligence-database. De getroffen versies van de plug-in varieerden van 24.12.92 tot en met 51.1.14. De actieve exploitatie door aanvallers begon een dag na de publieke bekendmaking, op 31 oktober 2025. Sindsdien heeft de Wordfence Firewall al meer dan 48.400 exploitpogingen tegen kwetsbare websites geblokkeerd.

Microsoft pakt LNK-kwetsbaarheid in Windows stilletjes aan
Microsoft heeft onlangs een kwetsbaarheid in Windows gepatcht die het mogelijk maakte om kwaadaardige code te verbergen in .LNK-bestanden. Deze kwetsbaarheid, aangeduid als CVE-2025-9491, werd actief misbruikt door aanvallers om systemen aan te vallen. Het probleem deed zich voor bij de verwerking van .LNK-bestanden, die normaal gesproken worden gebruikt om snelkoppelingen naar programma's en bestanden aan te maken.
De kwetsbaarheid zorgde ervoor dat gevaarlijke commando’s, die normaal zichtbaar zouden moeten zijn bij het inspecteren van het bestand, onzichtbaar werden gemaakt. Dit werd mogelijk doordat in het bestand een speciaal bewerkte "whitespace" werd toegevoegd, waardoor kwaadaardige commando’s pas na 260 zichtbare tekens zichtbaar waren. Hierdoor konden aanvallers hun kwaadaardige code verbergen voor de gebruiker.
Het probleem werd oorspronkelijk gemeld door securitybedrijf ZDI in september 2024, maar Microsoft gaf aanvankelijk aan dat het niet voldoende ernstig was om een patch uit te brengen. Pas later, nadat de details openbaar werden gemaakt, besloot Microsoft de kwetsbaarheid onopgemerkt te verhelpen tijdens een reguliere patchronde in november 2025. In de nieuwe update is nu het volledige Target-commando zichtbaar, ongeacht de lengte ervan, wat de exploitatie van de kwetsbaarheid voorkomt.
Het is niet de eerste keer dat dergelijke kwetsbaarheden worden aangetroffen in .LNK-bestanden. Eerder werden soortgelijke technieken, zoals bij de Stuxnet-aanval, gebruikt om systemen te compromitteren. De ontdekking van deze kwetsbaarheid

komt op een moment dat aanvallers steeds vaker gebruik maken van verborgen technieken om hun schade te maximaliseren zonder dat gebruikers het merken.

Onderzoeker waarschuwt voor hacks via updateproces Notepad++

De Britse beveiligingsonderzoeker Kevin Beaumont heeft gewaarschuwd voor gerichte aanvallen op organisaties waarbij de veelgebruikte teksteditor Notepad++ een centrale rol lijkt te spelen. Volgens de onderzoeker zijn er bij ten minste drie organisaties beveiligingsincidenten vastgesteld op systemen waar deze software in gebruik was. Het vermoeden bestaat dat kwaadwillenden via de processen van Notepad++ de eerste toegang tot de netwerken wisten te verkrijgen. Beaumont benadrukt dat het onderzoek nog loopt en dat het volledige plaatje nog niet compleet is, maar hij deelt zijn bevindingen om tijdig bewustzijn te creëren.
De kwetsbaarheid lijkt zich te concentreren rondom het update-mechanisme van de software, dat gebruikmaakt van een component genaamd GUP of WinGUP. Wanneer de applicatie controleert op updates, wordt informatie over de huidige versie naar een server van Notepad++ gestuurd. Als antwoord stuurt deze server een XML-bestand terug met daarin de locatie waar de nieuwe update gedownload kan worden. Hoewel dit proces via een beveiligde HTTPS-verbinding zou moeten verlopen, wijst Beaumont erop dat het mogelijk blijkt om dit verkeer op het niveau van de internetprovider te manipuleren en de beveiliging te omzeilen. Bij oudere versies van de editor verliep dit verkeer zelfs nog via het onbeveiligde HTTP-protocol.
Een ander kritiek punt betreft de verificatie van de gedownloade bestanden. Hoewel de downloads van Notepad++ digitaal ondertekend zijn, maakten eerdere versies gebruik van een zelfondertekend root-certificaat dat publiekelijk beschikbaar was op ontwikkelplatform GitHub. Vanaf versie 8.8.7 is de ontwikkelaar overgestapt op een certificaat van GlobalSign, wat de betrouwbaarheid van de softwareverificatie ten goede komt. De onderzoeker merkt echter op dat er een periode is geweest waarin updates niet adequaat werden gecontroleerd, wat ruimte bood voor mogelijk misbruik. De aanvallen op de getroffen organisaties zouden ongeveer twee maanden geleden hebben plaatsgevonden.
In reactie op potentiële risico's is er vorige maand een update voor Notepad++ uitgebracht. Deze update richt zich specifiek op het beter beveiligen van het installatieproces van de updates zelf. De verbetering moet voorkomen dat een aanvaller de url voor het downloaden van updates kan kapen. Beaumont geeft aan dat hij de ontwikkelaar van de software niet beschuldigt, maar dat de situatie wel directe aandacht van systeembeheerders vereist. Organisaties wordt geadviseerd om alert te zijn op verdachte activiteiten rondom de editor en om te controleren of gebruikers over de nieuwste versie, nummer 8.8.8, beschikken.

Microsoft Waarschuwt voor Grootschalige Phishingaanvallen met Parkeerboetes en Bloedtestuitslagen

Op de avond voor Thanksgiving hebben aanvallers een aanzienlijke hoeveelheid phishing-e-mails verspreid. Dit meldt Microsoft via X. De onderwerpen van de e-mails waren onder andere een vermeende parkeerboete en de uitslag van een bloedtest. Eén variant van de phishingmail beweerde dat de afzender een parkeerboete had ontvangen die in feite voor de ontvanger bestemd was, met als reden de sterke gelijkenis tussen de kentekens van de afzender en de beoogde ontvanger. Een hyperlink in de e-mail zou dienen om de parkeerboete in te zien.
De andere phishingmail informeerde de ontvanger dat de uitslag van een bloedtest beschikbaar was en te raadplegen via de bijgevoegde link. De webpagina waarnaar de phishing-e-mails leidden, instrueerde de bezoeker om een captcha op te lossen. Vervolgens werden gebruikers gevraagd om een kwaadaardig PowerShell-commando uit te voeren, onder het valse voorwendsel dat dit noodzakelijk was voor het voltooien van de captcha. Door dit commando uit te voeren, werd echter malware op de computer van de gebruiker geïnstalleerd. Deze malware gaf de aanvallers toegang tot het systeem en de mogelijkheid om bestanden te versleutelen. Microsoft gaf aan dat deze specifieke phishingcampagne voornamelijk gericht was op gebruikers in de Verenigde Staten.

Omvangrijke Shai-Hulud 2.0 malware-aanval op NPM lekt tot 400.000 ontwikkelaarsgeheimen

De recente Shai-Hulud 2.0-aanval, de tweede van dit type, heeft rond de 400.000 ruwe ontwikkelaarsgeheimen blootgelegd. Dit gebeurde nadat de malware honderden pakketten in het Node Package Manager (NPM)-register had geïnfecteerd en de gestolen gegevens vervolgens publiceerde in 30.000 GitHub-repositories. Hoewel het open-source TruffleHog scanning-instrument slechts ongeveer 10.000 van de blootgestelde geheimen als geldig kon verifiëren, constateerden onderzoekers van cloudbeveiligingsplatform Wiz dat meer dan 60% van de gelekte NPM-tokens op 1 december nog steeds actief was.
De oorspronkelijke Shai-Hulud-dreiging ontstond medio september, waarbij 187 NPM-pakketten werden gecompromitteerd met een zichzelf verspreidende payload. Deze payload identificeerde accounttokens via TruffleHog, injecteerde een kwaadaardig script in de pakketten en publiceerde deze automatisch op het platform. Bij de tweede aanval waren meer dan 800 pakketten (alle geïnfecteerde versies meegerekend) getroffen en bevatte de malware een destructief mechanisme dat de

thuismap van het slachtoffer kon wissen wanneer aan bepaalde voorwaarden werd voldaan.
Uit de analyse van de Wiz-onderzoekers blijkt dat verschillende soorten geheimen via de Shai-Hulud 2.0-aanval in de 30.000 GitHub-repositories terechtkwamen. Ongeveer 70% van de repositories bevatte een contents.json-bestand met GitHub-gebruikersnamen en -tokens, evenals momentopnamen van bestanden. De helft van de repositories bevatte het truffleSecrets.json-bestand met TruffleHog scanresultaten. Daarnaast bevatte 80% van de repositories het environment.json-bestand met OS-informatie, CI/CD-metadata, NPM-pakketmetadata en GitHub-inloggegevens. Vierhonderd repositories hostten het actionsSecrets.json-bestand met workflowgeheimen van GitHub Actions. De malware gebruikte TruffleHog zonder de validatievlag, wat betekent dat de 400.000 blootgestelde geheimen een bekend formaat volgen, maar niet allemaal actueel geldig of bruikbaar zijn. Desondanks stelt Wiz dat de gegevens, na zware ontdubbeling, nog steeds honderden geldige geheimen bevatten, waaronder cloud-, NPM-tokens en VCS-inloggegevens.
Analyse van 24.000 environment.json-bestanden toonde aan dat ruwweg de helft uniek was. 23% van de infecties kwam van ontwikkelaarsmachines, terwijl de rest afkomstig was van CI/CD-runners en soortgelijke infrastructuur. Verder waren de meeste geïnfecteerde machines, 87%, Linux-systemen en betrof 76% van de infecties containers. Wat betreft de distributie van CI/CD-platforms, voerde GitHub Actions de boventoon, gevolgd door Jenkins, GitLab CI en AWS CodeBuild. De meest voorkomende besmettingsbronnen waren de pakketten @postman/tunnel-agent@0.6.7 en @asyncapi/specs@6.8.3, die samen verantwoordelijk waren voor meer dan 60% van alle infecties. De infectie vond in 99% van de gevallen plaats via de preinstall-gebeurtenis, die het bestand node setup_bun.js uitvoerde. Wiz voorziet dat de daders achter Shai-Hulud hun technieken zullen blijven verfijnen, met de voorspelling dat er in de nabije toekomst meer aanvalsgolven zullen ontstaan, mogelijk gebruikmakend van de reeds verzamelde inloggegevens.

Malafide Rust-crate verspreidt systeemspecifieke malware onder Web3-ontwikkelaars

Onderzoekers op het gebied van cyberbeveiliging hebben een kwaadaardig Rust-softwarepakket ontdekt dat is ontworpen om zich te richten op systemen met Windows, macOS en Linux. Het pakket, genaamd "evm-units", deed zich voor als een hulpmiddel voor de Ethereum Virtual Machine (EVM) en bevatte functies om onopgemerkt code uit te voeren op machines van softwareontwikkelaars.
De Rust-crate werd half april 2025 geüpload naar de centrale opslagplaats crates.io door een gebruiker met de naam "ablerust". In de acht maanden dat het pakket

online stond, werd het meer dan 7.000 keer gedownload. Bovendien was "evm-units" opgenomen als afhankelijkheid in een ander pakket van dezelfde auteur, "uniswap-utils", dat op zijn beurt meer dan 7.400 keer werd gedownload. Beide pakketten zijn inmiddels verwijderd uit de pakketrepository.
Volgens beveiligingsonderzoekers downloadt het pakket een payload op basis van het besturingssysteem van het slachtoffer en of het antivirusprogramma Qihoo 360 actief is. De payload wordt weggeschreven naar een tijdelijke systeemmappen en vervolgens stilzwijgend uitgevoerd. Het pakket levert schijnbaar het Ethereum-versienummer als output, waardoor het slachtoffer niet argwanend wordt.
Een opvallend kenmerk van het pakket is de expliciete controle op de aanwezigheid van het proces "qhsafetray.exe", dat geassocieerd wordt met de 360 Total Security-antivirussoftware van de Chinese beveiligingsleverancier Qihoo 360. De kwaadaardige code is specifiek ontworpen om een ogenschijnlijk onschadelijke functie genaamd "get_evm_version()" aan te roepen. Deze functie decodeert een externe URL ("download.videotalks[.]xyz") en benadert deze om een payload van de volgende fase op te halen.
De uitvoering van de payload verschilt per besturingssysteem. Op Linux-systemen downloadt de code een script, slaat dit op als /tmp/init en voert het uit op de achtergrond met behulp van het nohup-commando, wat de aanvaller mogelijk volledige controle kan geven. Op macOS-systemen wordt een bestand genaamd init gedownload en via osascript en nohup op de achtergrond uitgevoerd. Op Windows wordt de payload opgeslagen als een PowerShell-scriptbestand ("init.ps1") in de tijdelijke map. Hier controleert de code op het lopende proces "qhsafetray.exe" alvorens het script uit te voeren. Als dit antivirusproces niet wordt gedetecteerd, maakt het een Visual Basic Script-wrapper aan die een verborgen PowerShell-script zonder zichtbaar venster uitvoert. Als het proces wel wordt gedetecteerd, wordt de uitvoeringsstroom licht gewijzigd door PowerShell direct aan te roepen.
De verwijzingen naar EVM en Uniswap, een gedecentraliseerd cryptocurrency-uitwisselingsprotocol, wijzen erop dat dit incident in de softwareleveringsketen gericht was op ontwikkelaars in de Web3-sector. De packages werden aangeboden als hulpprogramma's gerelateerd aan Ethereum. De verantwoordelijke actor, "ablerust", had een platformonafhankelijke loader voor een tweede fase ingebed in een onschuldig ogende functie. Doordat de kwaadaardige afhankelijkheid in een ander veelgebruikt pakket werd getrokken, kon de code automatisch worden uitgevoerd tijdens de initialisatie.

Analyse van het kwetsbaarheidslandschap en exploitatietrends in Q3 2025

Gedurende het derde kwartaal van 2025 bleef het totale aantal geregistreerde kwetsbaarheden, gemeten in CVE's, stijgen. Het maandelijks gepubliceerde aantal bleef consistent boven de cijfers van voorgaande jaren, wat resulteerde in ruim duizend meer gepubliceerde kwetsbaarheden dan in dezelfde periode vorig jaar. De algehele trend van geregistreerde kwetsbaarheden vertoont een stijging naar het einde van het kwartaal toe, met een verwachte lichte daling tegen het jaareinde ten opzichte van het septembercijfer. De maandelijkse distributie van kritieke kwetsbaarheden, gedefinieerd als CVSS > 8.9, was echter marginaal lager dan de cijfers van 2024.
Wat betreft exploitatiestatistieken op Windows-systemen bleven kwetsbare Microsoft Office-producten de meest voorkomende doelwitten. De meest gedetecteerde exploits richtten zich op de oudere kwetsbaarheden CVE-2018-0802 en CVE-2017-11882, beide kwetsbaarheden voor uitvoering van code op afstand in de Equation Editor-component. Ook CVE-2017-0199, een kwetsbaarheid in Microsoft Office en WordPad, werd veelvuldig misbruikt. Het aantal Windows-gebruikers dat exploits tegenkwam, nam in het derde kwartaal toe ten opzichte van het vorige kwartaal, maar bleef lager dan het cijfer van Q3 2024. Op Linux-apparaten nam het aantal gebruikers dat exploits tegenkwam toe, waarbij het cijfer in Q3 2025 reeds meer dan zes keer het niveau van Q1 2023 bereikte. De meest gedetecteerde kwetsbaarheden in de Linux-kernel omvatten CVE-2022-0847, bekend als Dirty Pipe, en CVE-2021-22555, een heap overflow in de Netfilter kernel-subsysteem, die veelvuldig wordt misbruikt door middel van geheugenmodificatietechnieken.
In de analyse van openbaar gepubliceerde exploits bleven die gericht op het besturingssysteem domineren. Opmerkelijk was de significante stijging van het aandeel browserexploits in het derde kwartaal, dat daarmee gelijk kwam te staan aan het aandeel van exploits in overige software. Er verschenen geen nieuwe publieke exploits voor Microsoft Office-producten, hoewel Proof-of-Concepts voor kwetsbaarheden in Microsoft SharePoint werden vrijgegeven. Deze werden geclassificeerd onder besturingssysteemkwetsbaarheden vanwege hun impact op OS-componenten.
Aanvallen van Advanced Persistent Threat-groepen (APT) in Q3 2025 werden gedomineerd door zero-day kwetsbaarheden. De geviseerde software wijst op de opkomst van een nieuwe standaard toolkit voor het verkrijgen van initiële toegang tot infrastructuur en het uitvoeren van code op zowel randapparatuur als binnen besturingssystemen. Ook oudere kwetsbaarheden, zoals CVE-2017-11882, werden nog ingezet, vaak met data-obfuscatie om detectie te omzeilen.
Wat betreft de Command and Control (C2) frameworks was Metasploit het meest voorkomende framework, met een toegenomen aandeel ten opzichte van Q2,

gevolgd door Sliver en Mythic. Het relatief nieuwe framework Adaptix C2 werd bijna onmiddellijk door aanvallers in praktijkscenario's omarmd. Kwetsbaarheden die werden gebruikt om C2-agenten te lanceren en zich door het netwerk van het slachtoffer te verplaatsen, waren onder meer CVE-2020-1472, bekend als ZeroLogon, en CVE-2021-34527, bekend als PrintNightmare, evenals de directory traversal-kwetsbaarheden CVE-2025-6218 of CVE-2025-8088.
Een van de meest opvallende kwetsbaarheden die publiekelijk werden beschreven, was ToolShell, een reeks kwetsbaarheden in Microsoft SharePoint, waaronder CVE-2025-49704 en CVE-2025-49706, en de patch-omzeilingen CVE-2025-53770 en CVE-2025-53771. Deze combinatie van onveilige deserialisatie en een authenticatiebypass stelde aanvallers in staat met slechts enkele verzoeken volledige controle over de server te verkrijgen. Deze kwetsbaarheden werden in juli gepatcht. Daarnaast was er CVE-2025-8088, een directory traversal kwetsbaarheid in WinRAR. Bij deze kwetsbaarheid worden relatieve paden gebruikt om WinRAR te misleiden de archiefinhoud in systeemdirectory's uit te pakken, waarbij gebruik wordt gemaakt van Alternate Data Streams en omgevingsvariabelen.

Calisto richt zich op Reporters Without Borders met geavanceerde phishingcampagne

De Franse ngo Reporters Without Borders (RSF) was in mei en juni 2025 doelwit van een phishingcampagne uitgevoerd door de Russische hackercollectief Calisto, ook wel bekend als ColdRiver of Star Blizzard. Calisto is een groep die al sinds 2017 actief is en wordt geassocieerd met de Russische inlichtingendienst FSB. De groep richt zich vaak op organisaties die betrokken zijn bij de ondersteuning van Oekraïne, evenals andere strategische doelwitten, zoals militaire en onderzoeksinstellingen in het Westen.
De aanval op RSF omvatte een typische spear-phishing-aanval, waarbij de aanvallers ProtonMail-adressen vervalsten om inloggegevens te stelen. De phishingmail leek afkomstig van een vertrouwde contactpersoon en vroeg de ontvanger om een document in te zien. Het document was echter niet bijgevoegd, wat bedoeld was om de ontvanger te verleiden naar het ontbrekende bestand te vragen. Deze tactiek werd gebruikt om de slachtoffer naar een kwaadaardige website te leiden.
In een andere aanval werd een ZIP-bestand verstuurd met een vervalste PDF-extensie, maar het bestand was niet functioneel als een PDF. Dit werd gedaan om de aanvaller in staat te stellen de ontvanger naar een phishingsite te leiden waar inloggegevens konden worden verzameld. De pagina die werd gepresenteerd, was een vervalste ProtonMail-loginpagina, ontworpen om inloggegevens en, in sommige gevallen, tweefactorauthenticatie-codes te onderscheppen.

Calisto blijft zijn aanvallen uitvoeren met geavanceerde technieken, zoals AiTM (Adversary-in-the-Middle), waarbij de aanvaller tussen de gebruiker en de legitieme website komt te staan om de gegevens van het slachtoffer te onderscheppen. Deze gerichte aanvallen op ngo's en strategische organisaties benadrukken de kwetsbaarheid van dergelijke entiteiten voor cyberdreigingen die verband houden met geopolitieke conflicten.
Voor organisaties in Nederland en België die betrokken zijn bij persvrijheid, internationale samenwerking of steun aan Oekraïne, is het van cruciaal belang zich bewust te zijn van deze geavanceerde phishingcampagnes. Cyberdreigingen van staatssponsors kunnen ernstige gevolgen hebben voor de veiligheid van zowel de digitale als de fysieke wereld van dergelijke organisaties.

'Water Saci'-hackers gebruiken AI om WhatsApp Web-gebruikers aan te vallen en bankgegevens te stelen
Een recente, geavanceerde cybercampagne genaamd 'Water Saci' heeft Braziliaanse gebruikers van WhatsApp Web in het vizier genomen. Deze aanvalsmethode onderschept de communicatie op het platform om banktrojans te verspreiden en financiële gegevens te ontvreemden. Door de accounts van slachtoffers te compromitteren, sturen de aanvallers overtuigende berichten naar de contacten van het slachtoffer, waardoor een snelle, zichzelf verspreidende infectielus ontstaat die traditionele beveiligingsmaatregelen via social engineering effectief omzeilt.
De aanvalsketen vangt doorgaans aan wanneer gebruikers berichten ontvangen met kwaadaardige bijlagen. Dit zijn vaak ZIP-archieven, PDF-lokmiddelen die als Adobe-updates worden vermomd, of directe HTA-bestanden met specifieke naamgevingspatronen. Zodra een slachtoffer deze bestanden opent, wordt een complexe meerfasige aanvalssequentie uitgevoerd, waarbij Visual Basic-scripts en MSI-installatieprogramma's betrokken zijn. Dit proces downloadt op een heimelijke manier een banktrojan, terwijl tegelijkertijd automatiseringsscripts worden geïmplementeerd om de WhatsApp-sessie van het slachtoffer te kapen voor verdere verspreiding.
Beveiligingsanalisten hebben vastgesteld dat deze campagne een belangrijke verschuiving in malware-ontwikkeling markeert, waarbij kunstmatige intelligentie (AI) wordt ingezet om de mogelijkheden te versnellen. De aanvallers lijken Large Language Models (LLM's) te hebben gebruikt om hun propagatiecode te vertalen en optimaliseren, waarbij ze zijn overgestapt van PowerShell naar een robuustere, op Python gebaseerde infrastructuur. Deze strategische verandering verbetert hun vermogen om de malware te verspreiden over verschillende browsers, waaronder

Chrome, Edge en Firefox, waardoor detectie door standaard beveiligingsprotocollen moeilijker wordt.
Een cruciaal technisch onderdeel is het whatsz.py-script, dat eerdere PowerShell-varianten vervangt. Analyse toont dwingende bewijzen van AI-geassisteerd coderen, zoals scriptharders die expliciet "Versao Python Convertido de PowerShell" vermelden, en opmerkingen als "version optimized with errors handling". Dit script maakt gebruik van componentbestanden zoals chromedriver.exe om het infectieproces te automatiseren. Het gebruikt Selenium om de WA-JS-bibliotheek te injecteren, contactlijsten te extraheren en vervolgens kwaadaardige bestanden in bulk naar nietsvermoedende slachtoffers te verzenden. De Python-code vertoont een geavanceerde objectgeoriënteerde structuur met geavanceerde foutafhandeling. De geavanceerde automatisering stelt de malware in staat om autonoom te functioneren, taken te pauzeren en te hervatten om op te gaan in normaal netwerkverkeer, terwijl de voortgang aan een command-and-control-server wordt gerapporteerd, wat uiteindelijk zorgt voor aanhoudende toegang.

Hackers omzeilen MFA-beveiliging met Evilginx via nagebootste Single Sign-On portals

In de hedendaagse digitale beveiligingsomgeving wenden kwaadwillenden zich tot geavanceerde technieken om multi-factor authenticatie (MFA) te omzeilen en onbevoegde toegang te verkrijgen tot cloudaccounts. Een belangrijk hulpmiddel dat hierbij wordt ingezet, is Evilginx, een krachtige ‘adversary-in-the-middle’-tool (AiTM). Dit framework fungeert als een reverse proxy tussen het slachtoffer en de daadwerkelijke inlogpagina’s voor Single Sign-On (SSO). Het doel is om het slachtoffer te verleiden tot het invoeren van hun inloggegevens en het voltooien van de MFA-procedure, waarna de aanvallers sessiecookies kunnen stelen.
Het gebruik van Evilginx stelt aanvallers in staat om phishing-aanvallen uit te voeren waarbij de inlogschermen nauwkeurig het uiterlijk en gedrag van legitieme SSO-pagina’s nabootsen. Voor de gebruiker lijkt de valse site legitiem, compleet met vertrouwde huisstijl en een geldig TLS-certificaat. De aanval begint doorgaans met gerichte phishing-e-mails die slachtoffers naar deze zorgvuldig nagemaakte SSO-portals leiden. Deze phishing-pagina’s kopiëren de lay-out, scripts en flows van veelgebruikte identiteitsplatforms, inclusief zakelijke SSO-gateways. De sites zijn zo ontworpen dat ze precies lijken op het inlogproces van de echte service.
Zodra een gebruiker zijn of haar inloggegevens invoert en de MFA-procedure voltooit, onderschept Evilginx op de achtergrond de sessiecookies en tokens, terwijl het verkeer nog steeds naar de legitieme provider wordt doorgestuurd.
Beveiligingsanalisten van Infoblox identificeerden recente campagnes waarbij Evilginx

werd ingezet om legitieme zakelijke SSO-sites na te bootsen en tokens te stelen voor platformen voor e-mail en samenwerking. Zij merkten op dat de gestolen cookies aanvallers de mogelijkheid bieden om sessies opnieuw af te spelen zonder dat zij nogmaals een wachtwoord of MFA-code nodig hebben. Dit verschuift het risico van traditionele diefstal van inloggegevens naar een volledige sessie-kaping of 'session hijack'.
De gevolgen van een dergelijke aanval zijn aanzienlijk voor zowel organisaties als individuele gebruikers. Met een actief sessietoken kunnen aanvallers e-mails lezen, wachtwoorden voor gekoppelde applicaties resetten, nieuwe MFA-methoden installeren en backdoor-toegang creëren. Dit kan leiden tot 'business email compromise' (BEC), grootschalige gegevensdiefstal en heimelijke toegang op lange termijn die moeilijk te herleiden is naar de oorspronkelijke phishing-klik.
Een belangrijk aspect van Evilginx is de manier waarop het detectie ontwijkt tijdens dit proces. Het framework stuurt alle inhoud van de echte SSO-site door, inclusief scripts, stijlen en dynamische prompts, wat traditionele visuele inspecties bijna nutteloos maakt. Bovendien maakt het gebruik van echte certificaten op lookalike-domeinen, waardoor browserbeveiligingsindicatoren, zoals het groene hangslotje, nog steeds groen en geruststellend verschijnen. Onderhuids proxy't en herschrijft Evilginx HTTP-headers om de sessie in stand te houden, terwijl het tegelijkertijd gevoelige cookies onderschept voor diefstal. Door de cookies op de proxylaag te loggen, kunnen aanvallers sessiegegevens bemachtigen voordat deze worden beschermd door het apparaat van de gebruiker of de beveiligingshulpmiddelen van de onderneming.

Vroege signalen van insider-bedreigingen via authenticatie- en toegangscontrole
Insider-bedreigingen blijven een van de grootste beveiligingsuitdagingen voor organisaties. Deze bedreigingen vertonen zich vaak niet direct via opvallende waarschuwingen, maar manifesteren zich in kleine, ongewone activiteiten die gemakkelijk in normale dagelijkse bedrijfsvoering verborgen gaan. Dit maakt het voor veel bedrijven moeilijk om deze vroege signalen tijdig te detecteren, waardoor schade kan optreden voordat ze zich ervan bewust zijn, zoals datalekken, reputatieschade of verstoringen van systemen.
Het belangrijkste probleem bij het detecteren van insider-bedreigingen is het fundamentele toewijzingsprobleem. Wanneer een medewerker toegang krijgt tot bedrijfsystemen of gegevens verplaatst tussen goedgekeurde locaties, lijken deze acties volledig normaal. Traditionele beveiligingstools richten zich op het blokkeren van evidente bedreigingen, maar missen vaak de subtiele gedragingen die wijzen op kwaadwillende bedoelingen. Dit probleem wordt groter wanneer organisaties falen

om wat er binnen hun netwerk gebeurt te koppelen aan activiteiten van buitenaf, zoals medewerkers die communiceren op dark web-forums of bedrijfsgeheimen verkopen aan concurrenten.
Nisos, een beveiligingsbedrijf, heeft aangetoond dat significante indicatoren van insider-bedreigingen vaak weken of zelfs maanden voor daadwerkelijke datadiefstal of systeemcompromis zichtbaar worden. Deze indicatoren worden duidelijker wanneer organisaties meerdere gegevensbronnen combineren, zoals interne activiteitlogboeken en externe inlichtingen verzameld uit openbare bronnen. Dit geïntegreerde onderzoek stelt bedrijven in staat om patronen te identificeren die anders over het hoofd gezien zouden worden.
De eerste en meest onthullende indicator is ongewone authenticatie- en toegangsactiviteiten. Werknemers die van plan zijn gegevens te stelen, proberen vaak bedrijfssystemen te benaderen vanuit onverwachte locaties, inloggen op verschillende platforms binnen korte tijd of hun gebruikelijke toegangstijden te veranderen. Een werknemer kan bijvoorbeeld plotseling inloggen vanuit drie verschillende landen binnen een paar uur of bestanden openen op ongebruikelijke tijden buiten hun normale werktijden. Hoewel een enkele vreemde login een normale zakenreis kan weerspiegelen, moet herhaald gedrag worden onderzocht, aangezien dit vaak voorafgaat aan grotere dataverzamelingsactiviteiten. Dit zijn de momenten waarop insiders testen of ze door systemen kunnen bewegen zonder automatische waarschuwingen te triggeren.
Het begrijpen van deze afwijkingen vereist context en correlatie met andere activiteiten. Bedrijven die zich alleen richten op afzonderlijke incidenten missen vaak het bredere patroon. Door ongewone toegangspatronen te combineren met informatie over medewerkers die online over hun bedrijf praten of die in datalekdatabases voorkomen, ontstaat een veel duidelijker beeld. Deze geïntegreerde aanpak verandert geïsoleerde gebeurtenissen in betekenisvolle bedreigingsindicatoren die beveiligingsteams in staat stellen om in te grijpen voordat schade optreedt.

BPFDoor en Symbiote rootkits treffen Linux-systemen via eBPF-filters
De BPFDoor- en Symbiote-rootkits zijn twee geavanceerde malwarefamilies die zich richten op Linux-systemen. Deze rootkits maken gebruik van eBPF (extended Berkeley Packet Filter) technologie om zich onopgemerkt te houden voor traditionele detectiesystemen. Deze aanvallen vormen een ernstige dreiging voor de netwerkbeveiliging, aangezien ze de kern van het systeem binnendringen en zich verbergen onder de gebruikelijke beveiligingsmaatregelen.

De rootkits, die voor het eerst verschenen in 2021, maken gebruik van de eBPF-technologie die is ingebouwd in de Linux-kernel. eBPF biedt gebruikers de mogelijkheid om programma's direct in de kernel te laden, waarmee netwerkpakketten en systeemoproepen kunnen worden geïnspecteerd en gemanipuleerd. Hoewel deze technologie oorspronkelijk werd geïntroduceerd voor legitieme doeleinden, zoals netwerkbewaking en beveiliging, wordt eBPF nu misbruikt door kwaadwillende actoren om bijna ondetecteerbare achterdeuren te creëren. Deze achterdeuren kunnen netwerkcommunicatie onderscheppen en toegang tot systemen behouden zonder traditionele beveiligingsmeldingen te triggeren.
In 2025 alleen al werden 151 nieuwe monsters van BPFDoor en drie monsters van Symbiote gedetecteerd. Dit toont aan dat deze dreigingen nog steeds actief worden ontwikkeld en ingezet tegen kritieke infrastructuren. De rootkits gebruiken de eBPF-technologie op een manier die buiten het zicht van gebruikelijke beveiligingstools opereert, wat het detecteren van deze aanvallen bijzonder moeilijk maakt. Dit vormt een aanzienlijke uitdaging voor netwerkbeheerders en beveiligingsteams die moeite hebben om de kwaadwillende communicatie van de rootkits te blokkeren zonder legitiem verkeer te verstoren.
Een opvallende ontwikkeling in de evolutie van deze rootkits is het gebruik van verschillende poorten voor communicatie. De nieuwste versie van Symbiote, die in juli 2025 werd gedetecteerd, ondersteunt nu IPv4- en IPv6-verkeer over verschillende protocollen, waaronder TCP, UDP en SCTP, op niet-standaard poorten. Dit verhoogt de complexiteit voor netwerkbeheerders die proberen kwaadaardig verkeer te blokkeren. BPFDoor, aan de andere kant, maakt gebruik van geavanceerde technieken om DNS-verkeer op poort 53 te filteren, waardoor het onopgemerkt blijft bij reguliere netwerkactiviteiten.
Het detecteren van deze rootkits vereist gespecialiseerde technische expertise en tools zoals reverse engineering-software, waarmee de bytecode van eBPF kan worden geanalyseerd. Dit maakt het voor veel organisaties moeilijk om snel in te grijpen en deze aanvallen te stoppen. De rootkits blijven zich ontwikkelen en steeds beter in staat om traditionele beveiligingssystemen te omzeilen, wat hun aantrekkingskracht vergroot voor statelijke aanvallers die langdurige toegang tot systemen willen behouden.
Deze ontwikkeling markeert een verschuiving in de manier waarop malware wordt ontwikkeld. In plaats van de brede verspreiding van ransomware of botnets, richten deze rootkits zich op diepgaande, verborgen toegang en langdurige controle over systemen. Deze geavanceerde aanvalstechnieken benadrukken de noodzaak voor

versterkte beveiligingsmaatregelen die in staat zijn om met deze nieuwe vormen van bedreigingen om te gaan.

K.G.B RAT verspreid met geavanceerde detectiebypass-tools op hackerfora

Een zorgwekkende ontwikkeling heeft zich voorgedaan binnen het cybercriminaliteit-ecosysteem, waarbij cybercriminelen de K.G.B RAT (Remote Access Trojan) verspreiden via ondergrondse hackerfora. Deze trojan wordt gepromoot als een volledig ondetecteerbare dreiging, die gebruik maakt van geavanceerde technieken om traditionele beveiligingsmaatregelen en antivirussoftware te omzeilen.
De K.G.B RAT is onderdeel van een toolkit die niet alleen de RAT zelf bevat, maar ook een crypter en HVNC (Hidden Virtual Network Computing)-functionaliteit. Deze combinatie maakt het mogelijk om uiterst verfijnde aanvallen uit te voeren tegen kwetsbare systemen. Het gebruik van een crypter stelt de malware in staat zijn binaire handtekening te veranderen met elke compilatie, waardoor hash-gebaseerde detectiemechanismen ineffectief worden. Daarnaast maakt HVNC het mogelijk voor aanvallers om op afstand toegang te krijgen tot geïnfecteerde systemen via een virtuele desktopomgeving, waardoor ze ongezien kunnen inloggen, wachtwoorden kunnen stelen en laterale bewegingen kunnen maken binnen het netwerk.
De verspreiding van deze malware vormt een ernstige bedreiging voor organisaties in verschillende sectoren, omdat de infecties onopgemerkt kunnen blijven door traditionele beveiligingssystemen. Het gebruik van versleutelde communicatiekanalen en de afwezigheid van bekende commando- en controlehandtekeningen maken het nog moeilijker voor beveiligingsteams om aanvallen te detecteren. De combinatie van deze geavanceerde technieken maakt de K.G.B RAT een van de meest uitdagende dreigingen in de huidige cyberbeveiligingslandschap.
De aanwezigheid van dergelijke geavanceerde tools op openbare forums suggereert dat zelfs aanvallers met relatief beperkte technische vaardigheden nu toegang hebben tot krachtige middelen voor het uitvoeren van remote aanvallen. De makers van deze malware benadrukken actief de betrouwbaarheid en stealthmogelijkheden van de K.G.B RAT, wat de potentiële gevaren vergroot, aangezien dit soort tools steeds toegankelijker wordt voor kwaadwillenden.
Deze ontwikkeling onderstreept de noodzaak voor organisaties om hun beveiligingsmaatregelen te herzien en te versterken. Traditionele endpointbeveiliging is niet langer voldoende om dergelijke geavanceerde dreigingen te detecteren. Het is essentieel dat bedrijven zich richten op gedragsanalyse en netwerkverkeerinspectie als primaire verdedigingsmechanismen tegen dergelijke ondetecteerbare malware.

Wees alert op nieuwe 'Executive Award'-campagne die Stealerium-malware verspreidt via ClickFix

Een nieuwe phishingcampagne met het thema "Executive Award" richt zich op organisaties en combineert sociale manipulatie met de levering van geavanceerde malware. Deze aanval verloopt in twee fasen: eerst worden gebruikers misleid om hun inloggegevens in te voeren via een nep HTML-formulier, waarna de Stealerium-informatiediefstalsoftware wordt geïnstalleerd om de systemen te compromitteren. Deze campagne is een voorbeeld van de toenemende trend waarbij aanvallers identiteitsdiefstal combineren met malware-infecties in een enkele, gecoördineerde aanval.

De aanval begint met een goed gemaakte phishingpagina met de naam "Virtual-Gift-Card-Claim.html", die zich voordoet als een legitieme zakelijke awardmelding. Gebruikers die met deze pagina interactie hebben, geloven dat ze hun accountgegevens moeten verifiëren om de prijs te claimen, maar in werkelijkheid worden hun inloggegevens direct verzonden naar een Telegram-command-and-control-server die door de aanvallers wordt beheerd. Deze fase van de aanval fungeert als de eerste stap in de infectieketen.

Security-analisten van SpiderLabs identificeerden de malware na het analyseren van de infrastructuur en aanvalspatronen van de campagne. Ze ontdekten dat wanneer een gebruiker in de phishingpagina trapt, een schadelijk SVG-bestand met de naam "account-verification-form.svg" wordt afgeleverd. Dit bestand activeert een geavanceerd PowerShell-script dat via de ClickFix-exploitketen werkt, een bekende techniek die de Windows-berichtenprotocols misbruikt om verborgen commando's uit te voeren. De PowerShell-code downloadt en installeert vervolgens de Stealerium-malware op de computer van het slachtoffer zonder dat de gebruiker hiervan op de hoogte is of toestemming heeft gegeven.

Stealerium vormt een ernstige bedreiging omdat het stilletjes gevoelige informatie steelt van geïnfecteerde systemen. De malware communiceert met command-and-control-servers op specifieke IP-adressen en maakt gebruik van meerdere download- en uitvoeringspunten om aanvullende componenten en opdrachten te verkrijgen. Dit maakt het mogelijk voor aanvallers om hun aanval in real-time aan te passen op basis van de systeemomstandigheden en de reeds geïmplementeerde beveiligingsmaatregelen.

De kracht van deze aanval ligt in de manier waarop gebruik wordt gemaakt van legitieme Windows-functies tegen de gebruikers. Het schadelijke SVG-bestand opent de embedded PowerShell-opdrachten met minimale zichtbaarheid, waardoor de uitvoering van de malware nauwelijks opvalt voor traditionele beveiligingssystemen. Van daaruit downloadt Stealerium aanvullende componenten, zoals de hoofddll-

bestanden en batchscripts, en garandeert het de persistentie van de infectie, zodat de malware overleeft na systeemherstarten en doorgaat met het stelen van gegevens.
Organisaties moeten letten op ongebruikelijke PowerShell-activiteit, verdachte SVG-bestandsexecuties en netwerkverbindingen naar de bekende command-and-control-infrastructuur. Endpoint-detectiesystemen moeten worden geconfigureerd om pogingen om PowerShell-opdrachten van niet-standaardbronnen uit te voeren, te markeren. Verder moeten netwerken die toegang willen blokkeren tot de kwaadaardige IP-adressen en DNS-verzoeken die aan deze campagne zijn gekoppeld, goed gemonitord worden.
Gebruikers moeten waakzaam blijven voor ongevraagde e-mails die melding maken van een "executive recognition" of awardmeldingen, aangezien deze een effectieve vorm van sociale manipulatie blijven voor aanvallers.

Aisuru botnet achter recordbrekende 29,7 Tbps DDoS-aanval
Het Aisuru-botnet heeft in de afgelopen drie maanden meer dan 1.300 gedistribueerde denial-of-service (DDoS)-aanvallen uitgevoerd, waarbij één van deze aanvallen een nieuw record vestigde met een piek van 29,7 terabit per seconde (Tbps). Het botnet, dat in omvang varieert van 1 tot 4 miljoen geïnfecteerde apparaten wereldwijd, biedt een botnet-as-a-service, waarbij cybercriminelen delen van het netwerk kunnen huren om massale aanvallen uit te voeren. Deze apparaten, vaak routers en IoT-apparaten, worden geïnfecteerd via bekende kwetsbaarheden of brute force-aanvallen op zwakke wachtwoorden.
Cloudflare, een bedrijf gespecialiseerd in internetinfrastructuur, heeft meer dan 2.800 aanvallen van dit botnet gemitigeerd sinds het begin van 2025, waarvan bijna 45% hyper-volumetrisch waren. Dit houdt in dat de aanvallen meer dan 1 Tbps of 1 miljard pakketten per seconde bereikten. Het record van 29,7 Tbps werd bereikt in het derde kwartaal van 2025 en duurde slechts 69 seconden. De aanval maakte gebruik van een techniek genaamd "UDP carpet-bombing", waarbij verkeer naar gemiddeld 15.000 bestemmingspoorten per seconde werd gestuurd.
Hoewel de specifieke doelen van de aanvallen niet altijd openbaar worden gemaakt, blijkt uit de gegevens dat Aisuru zowel internetinfrastructuur als specifieke sectoren zoals gaming, hosting, telecommunicatie en financiële dienstverlening heeft aangevallen. Cloudflare merkt op dat deze aanvallen zo ingrijpend kunnen zijn dat ze zelfs delen van de internetinfrastructuur kunnen verstoren, zelfs wanneer ze niet direct het doelwit zijn. Dit betekent dat ongefilterde aanvallen ernstige gevolgen kunnen hebben voor vitale infrastructuren, waaronder de zorg, nooddiensten en militaire systemen.

De opkomst van hyper-volumetrische DDoS-aanvallen is een zorgwekkende trend die steeds vaker voorkomt. De statistieken van Cloudflare tonen aan dat het aantal van deze aanvallen het afgelopen jaar gestaag is toegenomen, met een stijging van 189% in DDoS-aanvallen die meer dan 100 miljoen pakketten per seconde bereiken, en een verdubbeling van aanvallen die de 1 Tbps overschrijden. Dergelijke aanvallen veroorzaken aanzienlijke verstoringen, zelfs als ze maar enkele seconden duren, wat leidt tot langdurige hersteltijden voor de getroffen systemen.

Toename van automatisch gegenereerde "elf-stats" pakketten op npm

In de afgelopen dagen heeft de Socket Threat Research Team een toename waargenomen van automatisch gegenereerde npm-pakketten met de naam "elf-stats", die elk twee minuten worden gepubliceerd. Het gaat hier om eenvoudige malware-varianten die via nieuwe accounts zijn verspreid. In totaal zijn er ten minste 420 unieke pakketten geïdentificeerd die deel uitmaken van deze campagne. Deze pakketten volgen een consistent naamgevingspatroon, zoals "elf-stats-[naam]", en hebben beschrijvingen die vermelden dat ze automatisch om de twee minuten worden gegenereerd. Sommige beschrijvingen refereren zelfs naar zogenaamde 'capture the flag'-uitdagingen of tests.

Een van de pakketten, "elf-stats-nutmeg-chimney-245", bevat bijvoorbeeld code die een commando uitvoert om gegevens te verzamelen en via een POST-aanroep naar een externe server te sturen. Dit soort gedrag is typerend voor de malware in deze campagnes. Het blijkt dat de auteur van deze pakketten geen andere pakketten heeft gepubliceerd en waarschijnlijk alleen verantwoordelijk is voor de publicatie van deze specifieke malware.

De meeste van deze pakketten zijn inmiddels door npm verwijderd, maar enkele blijven actief en worden nog steeds gehost op het platform. De snelle en repetitieve publicaties van deze pakketten lijken te wijzen op een geautomatiseerde poging om de npm-gemeenschap te verstoren met schadelijke software. Hoewel sommige van de beschrijvingen suggereren dat deze pakketten voor tests of uitdagingen zijn, zijn de geobserveerde codepatronen onveilig en niet geschikt voor gebruik in echte omgevingen.

Npm is momenteel bezig met het verwijderen van de getroffen pakketten en het monitoren van de situatie. Het wordt aangeraden om alle pakketten die dit naamgevingspatroon volgen, als onbetrouwbaar te beschouwen en niet te installeren totdat ze volledig kunnen worden beoordeeld.

Zuid-Koreaanse politie pakt hackers op na inbreuk op 120.000 IP-camera's

De National Office of Investigation in Zuid-Korea heeft bekendgemaakt dat er vier verdachten zijn gearresteerd in verband met een grootschalige hackoperatie waarbij toegang werd verkregen tot tienduizenden beveiligingscamera's. De verdachten wisten in te breken in meer dan 120.000 IP-camera's die geïnstalleerd waren in zowel particuliere woningen als commerciële instellingen door het hele land. De verkregen beelden, waaronder intiem en seksueel expliciet materiaal, werden vervolgens verkocht aan een buitenlandse website voor volwassenen.
Uit het politieonderzoek blijkt dat de verdachten op grote schaal opereerden. Een van de hoofdverdachten, die als werkloze staat geregistreerd, wist toegang te krijgen tot ongeveer 63.000 camera's. Hij produceerde en verkocht honderden illegale video's, waarmee hij naar schatting 35 miljoen Zuid-Koreaanse won verdiende in virtuele valuta. Een tweede verdachte, werkzaam als kantoormedewerker, hackte 70.000 camera's en verdiende hiermee ongeveer 18 miljoen won. Een derde verdachte richtte zich op een kleiner aantal camera's maar produceerde eveneens illegaal materiaal, waaronder beelden van minderjarigen. De vierde verdachte had toegang tot ruim honderd camera's.
De autoriteiten hebben vastgesteld dat de gestolen beelden werden geüpload naar een specifieke buitenlandse website die gespecialiseerd is in voyeuristische content. Opvallend is dat de twee hoofdverdachten vorig jaar verantwoordelijk waren voor maar liefst 62 procent van alle uploads op dit platform. De politie werkt momenteel samen met internationale opsporingsdiensten om de beheerders van deze website te identificeren en het platform uit de lucht te halen.
Naast de hackers richt het politieonderzoek zich ook op de afnemers van het illegale materiaal. Er zijn inmiddels drie personen gearresteerd die de beelden hadden aangeschaft. Zij riskeren gevangenisstraffen tot drie jaar. Park Woo-hyun, directeur van het beleid voor cyberonderzoek bij de nationale politie, benadrukte in een verklaring dat ook het bekijken of bezitten van dergelijk illegaal materiaal als een ernstig strafbaar feit wordt beschouwd en actief zal worden onderzocht.
Om verdere schade te voorkomen, zijn er beschermingsmaatregelen getroffen voor de slachtoffers. De politie heeft 58 locaties geïdentificeerd waar inbreuk is gepleegd en de betrokkenen op de hoogte gesteld. Hen is geadviseerd wachtwoorden te wijzigen en verzoeken in te dienen om beelden offline te halen. De politie wijst erop dat veel van deze inbreuken mogelijk worden gemaakt door zwakke beveiliging, zoals het gebruik van standaardwachtwoorden of verouderde firmware op IP-camera's.

Europese politie breekt Noords gokimperium op, verbonden met drugshandel en witwassen

In een gecoördineerde internationale operatie hebben de Spaanse nationale politie en de Zweedse politie tussen 28 en 29 november 2025 een crimineel netwerk opgerold dat zich bezighield met illegaal gokken, drugs en witwassen. De operatie vond plaats in Spanje en Zweden, met de deelname van zo'n 150 politieagenten. Zes locaties werden doorzocht, waaronder panden in Stockholm en Murcia, waar grote hoeveelheden illegale goederen en bewijs van criminele activiteiten werden aangetroffen.
Vijf belangrijke verdachten werden gearresteerd, waarvan drie in Zweden en twee in Spanje. Bij de invallen werden contant geld, luxe goederen en horloges ter waarde van enkele honderdduizenden euro's in beslag genomen. In Zweden werd een illegale gokclub ontdekt met een jaarlijkse omzet van 20 miljoen euro. Ook werden er drugs gevonden die bestemd waren voor de lokale markten, waarmee het netwerk zijn invloed in de regio wilde vergroten.
Het criminele netwerk, dat bekendstaat om zijn gewelddadige en intimiderende tactieken, heeft niet alleen de goksector in de regio gecontroleerd, maar bood ook diensten aan andere criminele groepen, zoals geldwitwassen. De samenwerking tussen verschillende Europese wetshandhavingsinstanties, gecoördineerd door Europol, maakt duidelijk hoe grensoverschrijdende criminele netwerken opereren, wat van belang is voor de veiligheid in Nederland, België en de bredere Europese regio.
Europol benadrukte de rol van het netwerk als belangrijke facilitator binnen de criminele omgeving, en de operationele successen onderstrepen de noodzaak van internationale samenwerking bij de bestrijding van georganiseerde misdaad.

Twee mannen aangehouden voor grootschalige retourfraude
Op dinsdag 2 december heeft de politie twee mannen uit Baarn aangehouden op verdenking van grootschalige oplichting. De mannen zouden een online verkoopplatform voor tonnen hebben opgelicht door te profiteren van retourfraude. Ze bestelden gedurende een langere periode allerlei producten, voornamelijk multimedia- en elektronica-artikelen, op de website van het platform. Vervolgens deden zij alsof ze de producten hadden geretourneerd, terwijl de goederen nooit bij het bedrijf aankwamen. In plaats daarvan werden de artikelen verkocht op andere websites voor tweedehands goederen, wat hen mogelijk enkele honderdduizenden euro's opleverde.
Het onderzoek werd gestart nadat het online verkoopplatform aangifte deed van de oplichting. De twee verdachten werden op basis van het onderzoek geïdentificeerd. Op 2 december voerde de politie meerdere doorzoekingen uit in Baarn, waarbij verschillende goederen die verband hielden met de oplichting werden aangetroffen.

Ook werden er contant geld, kilo's vuurwerk, verdovende middelen en een vuurwapen gevonden in de woningen en een opslagbox van de verdachten.
De politie legde beslag op de goederen en diverse voertuigen als slachtofferbeslag, een maatregel die bedoeld is om schade aan de slachtoffers van de oplichting te vergoeden. Dit beslag op crimineel vermogen is een belangrijk onderdeel van de strijd tegen criminaliteit, omdat het de verdachten financieel raakt en laat zien dat misdaad niet loont. Er wordt niet uitgesloten dat er meer aanhoudingen in het onderzoek zullen volgen.

Veroordeling voor verzamelen en verspreiden van kinderporno in Dilsen-Stokkem (B)
Een 58-jarige man uit Dilsen-Stokkem is veroordeeld tot vijftien maanden cel, met uitstel onder voorwaarden, voor het verzamelen en verspreiden van kinderporno. De zaak kwam aan het licht toen via het IP-adres van de man beelden van seksueel misbruikte kinderen werden verspreid. Bij een huiszoeking in juni 2025 vond de politie op de computer van de verdachte meer dan 60.000 afbeeldingen. De man verklaarde via het darkweb naar seksueel misbruikmateriaal te hebben gezocht, met een specifieke focus op meisjes van vijftien of zestien jaar oud. Het blijkt dat hij zich met deze activiteit vooral in het weekend bezig hield.
Tijdens de rechtszaak werd benadrukt dat de man psychologische begeleiding nodig heeft, waartoe hij werd verplicht. De rechter legde hem ook de verplichting op een persoonlijkheidsonderzoek te ondergaan en medewerking te verlenen aan controles van zijn elektronische apparaten. Daarnaast werd hij uit zijn rechten ontzet.
Deze zaak onderstreept de belangrijke rol van opsporing in het tegengaan van cybercriminaliteit en de gevaren van het darkweb, waar illegale inhoud gemakkelijk toegankelijk is.

Autoriteit Persoonsgegevens start controles op beveiliging patiëntgegevens in de zorg
De Autoriteit Persoonsgegevens (AP) heeft aangekondigd de komende maanden steekproefsgewijs controles uit te voeren bij ziekenhuizen, huisartsen en andere zorgaanbieders om na te gaan hoe zij patiëntgegevens beveiligen. Deze actie volgt op het feit dat de zorgsector in 2024 de meeste meldingen van datalekken bij de privacytoezichthouder deed. Vorig jaar ontving de AP bijna zevenduizend meldingen van datalekken bij zorgaanbieders.
De toezichthouder benadrukt dat zorgorganisaties de verantwoordelijkheid hebben om medische gegevens extra te beschermen. Dit omvat zowel het beveiligen van de gegevens tegen aanvallen en datalekken, als het waarborgen dat enkel de

behandelend arts en bevoegde medewerkers toegang hebben tot een medisch dossier van een patiënt.
Volgens AP-voorzitter Monique Verdier moeten patiënten en cliënten erop kunnen vertrouwen dat zorgaanbieders zorgvuldig omgaan met hun medische gegevens. De impact van gestolen of onrechtmatig ingezien medische gegevens wordt als groot beschouwd. De AP heeft als doel met deze controles zorgaanbieders ertoe aan te zetten de noodzakelijke beschermingsmaatregelen te treffen, zoals vastgelegd in de Algemene Verordening Gegevensbescherming (AVG).

Schikking Avast resulteert in $15,3 miljoen compensatie voor misleide gebruikers
De Amerikaanse toezichthouder Federal Trade Commission (FTC) heeft bekendgemaakt dat meer dan honderdduizend gebruikers van de antivirussoftware van Avast een totale som van 15,3 miljoen dollar zullen ontvangen. Deze uitkering volgt op een schikking die Avast vorig jaar trof met de FTC. De schikking had betrekking op het op oneerlijke wijze verzamelen en doorverkopen van browsegegevens van gebruikers die de browser-extensie of antivirussoftware van het bedrijf hadden geïnstalleerd.
Volgens de FTC werden de browsegegevens van gebruikers via de programma's verzameld, oneindig lang bewaard en zonder duidelijke kennisgeving of toestemming van de gebruikers doorverkocht. De toezichthouder stelde dat Avast gebruikers heeft misleid door te claimen dat de software de privacy zou beschermen door third-party tracking te blokkeren, terwijl niet werd gemeld dat hun eigen browsegegevens werden verkocht. De FTC oordeelde dat Avast hiermee de Amerikaanse wet heeft overtreden, waarbij de gegevens werden verkocht aan meer dan honderd derde partijen.
Avast verzamelde de gegevens, waaronder informatie over zoekopdrachten en bezochte websites, via de extensies en antivirussoftware. Deze praktijken vonden plaats sinds ten minste 2014. De verzamelde data kon worden gebruikt om gevoelige informatie over de gebruikers af te leiden. De onderneming heeft het her-identificeren van gebruikers op basis van de verkochte gegevens niet verboden, en in sommige contracten met een dergelijk verbod was de formulering zodanig dat derde partijen niet-persoonlijke identificeerbare informatie aan het browsegedrag konden koppelen. Sommige producten van het databedrijf Jumpshot waren zelfs ontworpen om klanten in staat te stellen specifieke gebruikers en hun browsegeschiedenis aan andere reeds in hun bezit zijnde informatie te koppelen.
Al in 2019 kwam naar buiten dat Avast miljoenen verdiende met het verhandelen van het browsegedrag van gebruikers via databedrijf Jumpshot, waarin Avast een meerderheidsbelang had. Na de onthulling over het dataverzamelen verwijderden

Google en Mozilla de browserextensies van Avast uit hun extensie-stores. Avast voerde aanpassingen door, maar door aanhoudende kritiek werd Jumpshot begin 2020 opgeheven.
De totale schikking die Avast moest betalen bedroeg 16,5 miljoen dollar, waarvan 15,3 miljoen dollar wordt verdeeld onder de getroffen gebruikers. Eerder dit jaar ontvingen 3,7 miljoen klanten die Avast tussen augustus 2014 en januari 2020 hadden aangeschaft een e-mail van de FTC om online een aanvraag voor een vergoeding in te dienen. Uiteindelijk hebben meer dan 103.000 Avast-gebruikers een geldige claim ingediend. De gemiddelde schadevergoeding per gebruiker komt neer op ongeveer 150 dollar.

Wijdverbreide storing bij ChatGPT: gebruikers ervaren fouten en verdwenen conversaties
De AI-aangedreven conversatiedienst ChatGPT van OpenAI heeft wereldwijd te kampen gehad met een grootschalige storing, waardoor gebruikers op grote schaal geen toegang konden krijgen tot de functionaliteiten van de chatbot. De problemen manifesteerden zich doordat gebruikers bij het proberen te bereiken van de chats diverse foutmeldingen ontvingen. De meest gemelde symptomen waren onder meer de boodschap "something seems to have gone wrong" en de melding "There was an error generating a response" in reactie op gebruikersvragen. In sommige gevallen bleef de applicatie langdurig laden zonder een resultaat te produceren.
Een bijkomend en significant probleem was dat sommige gebruikers meldden dat hun eerdere conversaties volledig waren verdwenen, terwijl nieuwe berichten ook bleven hangen in een laadproces. De omvang van de verstoring was aanzienlijk; volgens DownDetector ondervonden op het hoogtepunt van de problemen meer dan dertigduizend gebruikers wereldwijd hinder.
OpenAI erkende de problemen en bevestigde dat het bedrijf op de hoogte was van de storingen en werkte aan een oplossing. De onderneming identificeerde verhoogde fouten bij de toegang tot de getroffen diensten. Gedurende de middag, omstreeks 15:14 uur ET, begon de functionaliteit van ChatGPT geleidelijk terug te keren. Hoewel de dienst weer online kwam, bleef de snelheid en responsiviteit in de initiële herstelfase nog traag.

Explosieve Groei in AI-Toepassingen bij Nederlandse Overheidsinstanties
Nederlandse overheidsorganisaties maken in toenemende mate gebruik van AI-toepassingen, zoals chatbots, zo blijkt uit onderzoek van TNO. Het aantal getelde AI-toepassingen bij ministeries, gemeenten, provincies en agentschappen is in een jaar tijd aanzienlijk gestegen, van acht naar 81. Deze systemen betreffen generatieve AI,

waarmee geautomatiseerd teksten en beelden gecreëerd kunnen worden na een verzoek van de gebruiker.
Gemeenten zijn de grootste gebruikers van deze technologie, waarbij chatbots een prominente rol spelen. Een voorbeeld hiervan is de chatbot GEM, die wordt ingezet door een samenwerkingsverband van 25 gemeenten, waaronder de steden Utrecht, Tilburg en Rotterdam, om vragen van inwoners te beantwoorden.
In driekwart van de gevallen wordt de AI-technologie intern gebruikt door medewerkers van overheidsorganisaties. In een kwart van de gevallen is de toepassing gericht op direct gebruik door burgers. Een voorbeeld van deze laatste categorie is Tolkie, een leeshulp die informatie begrijpelijker maakt voor laaggeletterden door middel van functies als het uitleggen van woorden, het voorlezen, vertalen en samenvatten van teksten.
Volgens het onderzoek van TNO bevindt 29 van de 81 toepassingen zich in een experimentele fase, zoals een pilot. Daarnaast zijn er toepassingen die zich nog in de ideefase bevinden of op het punt staan in het werkproces van organisaties te worden geïntegreerd. Tussen juni 2024 en juni 2025 zijn er 73 nieuwe AI-toepassingen bij overheidsorganisaties geïntroduceerd, wat de snelle digitalisering van de overheid onderstreept.
De sterke toename brengt echter ook uitdagingen met zich mee, voornamelijk omdat het merendeel van de toepassingen draait op Amerikaanse modellen. Dit roept vragen op over controle, veiligheid en de digitale onafhankelijkheid van de overheid, aldus TNO. Overheidsorganisaties onderzoeken momenteel mogelijkheden om de afhankelijkheid van Amerikaanse leveranciers te verminderen.

E-commerceplatform Bol.com verwijdert gehele sekspoppen-categorie na rechterlijke toetsing illegale content

Bol.com, een van de grootste e-commerceplatforms in Nederland en België, heeft de gehele productcategorie van sekspoppen tijdelijk offline gehaald. Deze maatregel is een direct gevolg van een recente strafrechtelijke uitspraak waarbij de rechter oordeelde dat poppen die via dergelijke platformen verhandeld werden, een gelijkenis vertoonden met minderjarigen, wat in strijd is met het sinds 1 januari geldende verbod op kindersekspoppen.
De aanleiding is de veroordeling van een 38-jarige man in november tot een celstraf. De rechtbank stelde vast dat de door hem bezeten poppen kenmerken van een kind vertoonden, met name in de verhoudingen van de benen en heupen, en oordeelde dat dit bezit bijdraagt aan de instandhouding van een markt die de seksualisering van kinderen faciliteert. Het is in deze context dat de advocaten van de veroordeelde aangaven dat de poppen mogelijk via het Bol.com-platform waren aangeschaft.

Hoewel Bol.com in zijn eigen partnerbeleid de verkoop van kindersekspoppen – gedefinieerd als driedimensionale objecten die realistisch een minderjarige voorstellen en voor seksuele doeleinden kunnen worden gebruikt – reeds verbiedt, is de uitspraak voor het bedrijf aanleiding geweest tot actie. De webwinkel benadrukt de afkeuring van "alles wat in verband wordt gebracht met kinderporno" en stelt dat de tijdelijke verwijdering van de totale categorie noodzakelijk is voor een grondig onderzoek naar het aanbod van verkooppartners. Dit onderstreept de voortdurende uitdaging van online tussenpersonen bij het effectief monitoren en handhaven van de wetgeving tegen illegale content op hun platforms.

T-Mobile/Odido geconfronteerd met netwerkbeschikbaarheidsproblemen
Telecomprovider Odido (voorheen T-Mobile Nederland) werd op woensdagochtend 3 december 2025 geconfronteerd met een significante verstoring binnen haar netwerk. Het incident, dat rond 10.00 uur begon, resulteerde in ernstige problemen met de beschikbaarheid van mobiele communicatiediensten voor een deel van het klantenbestand. Gebruikers in Nederland rapporteerden hinder bij het opzetten van spraakverbindingen en het realiseren van dataverkeer via internet.
Een woordvoerder van Odido heeft bevestigd dat de onderbreking het directe gevolg was van een intern netwerkprobleem. Er zijn op dit moment geen indicaties dat de storing is veroorzaakt door een externe, kwaadwillige actie, zoals een DDoS-aanval, hoewel de gevolgen voor de kritieke functie van het netwerk vergelijkbaar zijn met een inbreuk op de beschikbaarheidspijler.
Na het identificeren van de technische oorzaak, heeft de provider onmiddellijk maatregelen genomen om de situatie te mitigeren. Klanten werden stapsgewijs opnieuw aangesloten op het netwerk. De provider heeft aangegeven dat de diensten inmiddels volledig zijn hersteld. Dit incident onderstreept de inherente kwetsbaarheid van grootschalige telecominfrastructuur ten aanzien van zowel technische falen als potentiële cyberdreigingen die gericht zijn op het verstoren van de beschikbaarheid van communicatienetwerken.

Nieuwe leiding Defensie Cyber Commando: Jorrit de Gruijter benoemd tot plaatsvervangend commandant
Kolonel Jorrit de Gruijter is benoemd tot plaatsvervangend commandant van het Defensie Cyber Commando (DCC) in Den Haag. De benoeming volgt op zijn vertrek als commandant van het Air Mobility Command en Vliegbasis Eindhoven, een functie die hij vijf jaar bekleedde.
Op dinsdag droeg kolonel De Gruijter het commando over de vliegbasis en het Air Mobility Command officieel over aan zijn opvolger, kolonel Daan Boissevain.

De Gruijter was sinds november 2020 de commandant op Vliegbasis Eindhoven en vervulde hiermee de langstzittende termijn in de geschiedenis van de basis sinds de overname door de Koninklijke Luchtmacht in 1952. Zijn periode kenmerkte zich door een intensieve inzet bij diverse internationale militaire en humanitaire operaties. Ter erkenning van zijn inspanningen voor het Air Mobility Command, de luchtmacht en de veiligheid van Nederland, ontving kolonel De Gruijter het Ereteken van Verdienste in brons. De onderscheiding werd uitgereikt door de commandant Lucht- en Ruimtestrijdkrachten, luitenant-generaal André Steur.

SIM-koppelingsplicht en periodiek uitloggen als nieuwe strategie tegen grensoverschrijdende cyberfraude

Het Indiase Ministerie van Telecommunicatie (DoT) heeft een significante wijziging doorgevoerd in de Telecommunications (Telecom Cyber Security) Rules van 2024. Deze maatregelen verplichten communicatiediensten die via apps worden aangeboden, waaronder bekende platforms zoals WhatsApp, Telegram en Signal, tot strikte technische aanpassingen. Het doel is de cyberveiligheid te versterken en specifiek het misbruik van telecommunicatie-identificatiegegevens voor internationale fraude en oplichting tegen te gaan.

De nieuwe regels vereisen dat deze apps – die gebruikmaken van een Indiaas mobiel nummer voor unieke gebruikersidentificatie – uitsluitend kunnen functioneren wanneer er een actieve, geverifieerde SIM-kaart in het apparaat is geïnstalleerd. Dit staat bekend als SIM-binding en beoogt de anonimiteit en het misbruik van onjuist gekoppelde nummers te elimineren. De verplichte naleving van de richtlijn moet binnen negentig dagen worden gerealiseerd.

Deze maatregel is een directe reactie op een beveiligingslek dat wijdverbreid werd uitgebuit voor grensoverschrijdende cybercriminaliteit. Het DoT stelt dat accounts op berichtendiensten operationeel bleven, zelfs nadat de bijbehorende SIM-kaart was verwijderd, gedeactiveerd of naar het buitenland was verplaatst. Dit faciliteerde de uitvoering van anonieme scams, 'digitale arrestatie'-fraude en oplichting waarbij Indiase nummers werden gebruikt om de overheid te imiteren.

Naast de continue SIM-koppeling introduceert de richtlijn een mechanisme voor periodieke herauthenticatie van web- en desktopsessies. De webversies van de berichtenplatforms moeten elke zes uur automatisch worden uitgelogd. Gebruikers worden daarna verplicht hun apparaat opnieuw te koppelen, bijvoorbeeld via een QR-code. De overheid motiveert deze maatregel door te stellen dat langdurige, ononderbroken sessies het mogelijk maken voor fraudeurs om accounts op afstand te besturen zonder de originele SIM-kaart. Door de verplichte, frequente herverificatie wordt extra frictie in het criminele proces ingebouwd en wordt de mogelijkheid tot

accountovername-aanvallen, misbruik op afstand en de inzet van muilezelrekeningen structureel verminderd.
Deze strenge beperkingen waarborgen dat elk actief account en de bijbehorende websessies zijn gekoppeld aan een door Know Your Customer (KYC) geverifieerde SIM-kaart. Dit verhoogt de traceerbaarheid van de nummers die worden ingezet bij onder meer beleggingsfraude en phishing-scams. Het is opmerkelijk dat deze SIM-bindings- en automatische sessie-uitlogregels reeds van toepassing zijn op bank- en betalingsapps die gebruikmaken van het Unified Payments Interface (UPI) systeem in India, waarmee deze beleidslijn nu wordt uitgebreid naar de communicatiesector.
In samenhang hiermee werkt het DoT aan de oprichting van een Mobile Number Validation (MNV) platform. Dit gedecentraliseerde en privacyvriendelijke mechanisme zal dienstverleners in staat stellen om te verifiëren of een mobiel nummer dat voor een digitale dienst wordt gebruikt, daadwerkelijk overeenkomt met de geregistreerde identiteit van de persoon. Het platform is specifiek ontworpen om de stijging van muilezelrekeningen en identiteitsfraude tegen te gaan, waarmee het vertrouwen in het digitale transactieverkeer verder wordt verankerd.

Onderzoek onthult: Dashcams binnen seconden te kapen voor grootschalige surveillance

Dashcams hebben zich wereldwijd gevestigd als belangrijke hulpmiddelen voor bestuurders, dienend als betrouwbare getuigen bij ongevallen of geschillen langs de weg. Cybersecurity-onderzoekers uit Singapore hebben echter een verontrustende kwetsbaarheid blootgelegd: deze apparaten kunnen binnen enkele seconden worden overgenomen en worden ingezet als krachtige bewakingstools.
De bevindingen, die werden gepresenteerd tijdens de Security Analyst Summit 2025, tonen aan dat aanvallers authenticatiemechanismen kunnen omzeilen om toegang te krijgen tot video-opnames met hoge resolutie, audio-opnamen en precieze GPS-gegevens die op de apparaten zijn opgeslagen. Het onderzoek richtte zich op twee dozijn dashcam-modellen van ongeveer vijftien verschillende merken, waarbij de populaire Thinkware-dashcam als uitgangspunt diende.
De meeste dashcams beschikken, zelfs zonder cellulaire connectiviteit, over ingebouwde Wi-Fi die koppeling met een smartphone mogelijk maakt via mobiele apps. Deze connectiviteit creëert een aanzienlijk aanvalsoppervlak dat kwaadwillende actoren kunnen exploiteren om opgeslagen gegevens op afstand te downloaden. Beveiligingsonderzoekers van Kaspersky identificeerden dat veel modellen gebruikmaken van hardgecodeerde standaardwachtwoorden en een vergelijkbare hardware-architectuur, waardoor ze kwetsbaar zijn voor massale exploits. Eenmaal

verbonden, verkrijgen aanvallers toegang tot een ARM-processor die een lichtgewicht Linux-build draait.
Onderzoekers ontdekten diverse methoden die aanvallers gebruiken om de authenticatie van de fabrikant te omzeilen. Directe bestandstoegang stelt hackers in staat om videodownloads aan te vragen zonder wachtwoordverificatie, aangezien de webserver de inloggegevens alleen controleert bij het hoofdtoegangspunt. MAC-adres-spoofing maakt het mogelijk voor aanvallers om de unieke identificatiecode van de smartphone van de eigenaar te onderscheppen en te repliceren. Daarnaast omvatten de methoden replay-aanvallen, waarbij legitieme Wi-Fi-uitwisselingen worden opgenomen voor latere exploitatie.
Misschien wel het meest alarmerend is de mogelijkheid tot wormachtige verspreiding die de onderzoekers ontwikkelden. Zij schreven code die direct op geïnfecteerde dashcams functioneert, waardoor gecompromitteerde apparaten automatisch dashcams in de nabijheid kunnen aanvallen terwijl voertuigen met vergelijkbare snelheden in het verkeer rijden. Een enkele kwaadaardige payload, ontworpen om meerdere wachtwoorden en aanvalsmethoden uit te proberen, zou potentieel ongeveer een kwart van alle dashcams in een stedelijke omgeving kunnen compromitteren.
De verzamelde gegevens maken volledige bewegingsregistratie, bewaking van gesprekken en identificatie van passagiers mogelijk. Door het extraheren van GPS-metadata, tekstherkenning van verkeersborden en het gebruik van OpenAI-modellen voor audiotranscriptie, kunnen aanvallers gedetailleerde samenvattingen van ritten genereren, waardoor slachtoffers effectief worden gede-anonimiseerd op basis van geanalyseerde gedragspatronen.

Fabrikant slimme toiletcamera heeft toegang tot "end-to-end versleutelde" beelden

De fabrikant van de slimme toiletcamera Dekoda, Kohler Health, heeft toegang tot de beelden die zijn verzameld door het apparaat, ondanks dat deze volgens het bedrijf "end-to-end versleuteld" zijn. De camera maakt foto’s van de ontlasting van de gebruiker en analyseert deze via een gekoppelde app die data uitwisselt met de servers van Kohler.
Kohler Health beweert dat de privacy van gebruikers wordt gewaarborgd door "end-to-end encryptie". Dit suggereert dat de gegevens alleen toegankelijk zouden moeten zijn voor de gebruiker. Echter, het bedrijf heeft bevestigd dat het zelf het "einde" van de encryptie is en daarmee in staat is om de beelden te ontsleutelen. Dit betekent dat Kohler toegang heeft tot de persoonlijke data die door het apparaat wordt verzameld, iets wat niet duidelijk naar voren kwam in eerdere communicatie.

De kritieken richten zich op de verwarrende terminologie van "end-to-end encryptie", die vaak wordt geassocieerd met systemen waarbij alleen de gebruiker toegang heeft tot versleutelde gegevens. In dit geval is dat niet zo, wat leidt tot zorgen over de manier waarop deze term wordt gepresenteerd om vertrouwen te wekken.
Kohler verklaart verder dat de verzamelde gegevens, zoals foto's van de ontlasting, kunnen worden gebruikt voor het trainen van AI-modellen. Dit gebeurt, aldus het bedrijf, uitsluitend met geanonimiseerde data.
Deze situatie roept vragen op over de transparantie van bedrijven die claimen strikte privacymaatregelen te hanteren, maar tegelijkertijd toegang hebben tot de gegevens die ze verzamelen. Het benadrukt de noodzaak voor duidelijke communicatie over privacypraktijken, vooral wanneer het gaat om gevoelige persoonlijke data.

American Express krijgt 1,5 miljoen euro boete voor illegaal plaatsen cookies
De Franse dochteronderneming van American Express, American Express Carte France, is door de Franse privacytoezichthouder CNIL beboet voor het illegaal plaatsen van cookies. Het bedrijf kreeg een boete van 1,5 miljoen euro vanwege het overtreden van cookieregels. American Express plaatste trackingcookies zonder de vereiste toestemming van gebruikers, wat in strijd is met de geldende privacywetgeving.
Volgens de CNIL werden de cookies al geplaatst voordat gebruikers de mogelijkheid kregen om hun voorkeuren aan te geven via een cookievenster. Dit is een duidelijke schending van de Europese privacyregels, die eisen dat gebruikers expliciet toestemming moeten geven voor het plaatsen van trackingcookies. Daarnaast werden er trackingcookies uitgelezen, zelfs nadat gebruikers hun toestemming hadden ingetrokken.
De Franse toezichthouder liet weten dat de boete werd bepaald door de ernst van de overtredingen en de lange tijd dat de regels voor het plaatsen van cookies bekend waren. Als verzachtende omstandigheid werd meegewogen dat het bedrijf inmiddels wijzigingen heeft doorgevoerd om zich aan de wetgeving te houden. Onlangs kreeg ook de Franse uitgever Conde Nast een boete van 750.000 euro voor vergelijkbare overtredingen.
Deze zaak benadrukt het belang van het naleven van de privacywetgeving, met name voor bedrijven die actief zijn in Europa. Het is van essentieel belang dat organisaties transparant zijn over het gebruik van cookies en dat gebruikers de mogelijkheid krijgen om geïnformeerde keuzes te maken over hun gegevens.