Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

09-10-2025:

Politie onderzoekt ransomware-aanval op bedrijven in Volendam

De politie onderzoekt momenteel een ransomware-aanval die verschillende bedrijven in Volendam heeft getroffen. Tot nu toe is er één aangifte binnengekomen, maar er wordt rekening gehouden met meer slachtoffers. Het administratiekantoor in Volendam lijkt direct getroffen te zijn, terwijl een drukkerij slechts beperkte internetproblemen ervoer door aanpassingen van de systeembeheerder. De zaak is overgedragen aan de cybercrime-afdeling van de politie, die de oorzaak van de aanval onderzoekt. Volgens het Nationaal Cyber Security Centrum (NCSC) werden vorig jaar 121 bedrijven in Nederland getroffen door ransomware. De exacte schade en het aantal getroffen bedrijven in Volendam zijn op dit moment nog onbekend.

Noord-Koreaanse hackers stelen meer dan $2 miljard aan cryptocurrency in 2025

Noord-Koreaanse hackers hebben in 2025 naar schatting meer dan $2 miljard aan cryptocurrency gestolen, wat het hoogste jaarlijkse totaal ooit is. Dit brengt het totale bedrag dat door deze hackers is gestolen op meer dan $6 miljard. Volgens de Verenigde Naties en overheidsinstanties worden de gestolen fondsen gebruikt om de ontwikkeling van nucleaire wapens te ondersteunen. De diefstal is bijna drie keer zoveel als in 2024 en overtreft het vorige record van $1,35 miljard in 2022, grotendeels veroorzaakt door aanvallen op de Ronin Network en Harmony Bridge. De grootste aanval in 2025 was de hack van Bybit in februari, waarbij $1,46 miljard werd gestolen. Dit jaar werden 30 cryptoheists aan Noord-Koreaanse hackers toegeschreven. Elliptic, een blockchain-expert, benadrukt dat de werkelijke cijfers waarschijnlijk hoger zijn, aangezien veel incidenten niet gerapporteerd worden.

Nieuwe hacktivistalliantie gevormd door KAL EGY 319 en DigitalStormSec

De hacktivistische groeperingen KAL EGY 319 en DigitalStormSec hebben officieel aangekondigd een nieuwe alliantie te vormen. Deze samenwerking vergroot hun gezamenlijke capaciteit om cyberaanvallen uit te voeren, wat de bredere cyberbeveiliging beïnvloedt. De twee groepen hebben een aantal gemeenschappelijke doelen en zijn bekend om hun betrokkenheid bij cyberaanvallen met politieke en sociale doeleinden. Het is nog niet duidelijk welke specifieke doelen de alliantie in de toekomst zal aanvallen, maar de impact op zowel particuliere als

overheidsdoelen kan significant zijn. De oprichting van deze alliantie benadrukt de groeiende trend van samenwerking tussen hacktivisten en hun toegenomen aanwezigheid op de internationale cyberdreigingskaart.

Nieuwe hacktivistenalliantie gevormd door ClawSec Team en BDAnonymous

De hacktivistische groepen ClawSec Team en BDAnonymous hebben een nieuwe alliantie aangekondigd. Deze samenwerking heeft tot doel hun cyberaanvallen verder te coördineren en uit te breiden. Beide groepen hebben zich in het verleden al onderscheiden door het uitvoeren van digitale aanvallen gericht op zowel overheidsinstellingen als particuliere organisaties. De officiële aankondiging benadrukt hun gezamenlijke inzet voor het uitvoeren van "digitale acties" met een politieke agenda, hoewel de specifieke doelwitten voor toekomstige aanvallen niet volledig worden gedeeld. Deze alliantie kan mogelijk leiden tot een toename van cyberdreigingen, met name voor landen die als doelwit worden gezien door hacktivistische groeperingen. De ontwikkeling is belangrijk voor zowel nationale als internationale beveiligingsdiensten die moeten inspelen op de dynamiek van deze nieuwe coalitie van digitale activisten.

Polen getroffen door ongekende trollenaanval te midden van Russische drone-inbraak

In de nacht van 10 september 2025 werd Polen overspoeld door een enorme hoeveelheid pro-Russische desinformatie op sociale media, gelijktijdig met de insluiting van 19 Russische drones in Pools luchtruim. Veel berichten beschuldigden Oekraïne of de NAVO, terwijl ze de drones aanvielen als een “buitenlandse provocatie” die Polen in een wereldconflict zou moeten trekken. Cybersecurity-experts gaven aan dat ongeveer 200.000 berichten in slechts enkele uren werden geteld, wat resulteerde in een “tsunami van desinformatie”. Berichten beweerden dat de Poolse strijdkrachten en NAVO machteloos waren ondanks hun enorme middelen en beschuldigden de autoriteiten ervan de waarheid voor het publiek te verbergen. De desinformatiecampagne breidde zich ook uit naar sociale netwerken in Frankrijk, Duitsland en Roemenië. De omvang van deze campagne roept bezorgdheid op over de strategie van Rusland om twijfel te zaaien over de betrouwbaarheid van de NAVO en publieke steun voor militaire uitgaven te ondermijnen.

WordPress-sites onder aanval door kwetsbaarheid in Service Finder Bookings plug-in

WordPress-websites worden actief aangevallen door een kritieke kwetsbaarheid in de Service Finder Bookings plug-in, met als resultaat dat aanvallers ongeauthenticeerde admin-toegang kunnen verkrijgen. Deze kwetsbaarheid (CVE-2025-5947) is aanwezig in versie 6.1 van de plug-in, die wordt gebruikt door meer dan zesduizend websites die het Service Finder Theme toepassen. Het beveiligingslek is het gevolg van een onveilige implementatie van de "account switching" functie, waarmee aanvallers toegang kunnen krijgen tot willekeurige accounts. De kwetsbaarheid heeft een ernstige impactscore van 9.8 (op een schaal van 1 tot 10). Een eerdere kwetsbaarheid, CVE-2025-23970, werd al door securitybedrijf Patchstack gemeld, maar is nog niet gepatcht in de oudere versie van de plug-in. Gebruikers van de plug-in worden aangespoord om deze te verwijderen of te updaten.

Meerdere Chrome-kwetsbaarheden stellen gebruikers bloot aan willekeurige code-uitvoeringsaanvallen

Google heeft versie 141.0.7390.65/.66 van Chrome uitgebracht voor Windows, Mac en Linux, waarin meerdere kritieke beveiligingskwetsbaarheden zijn opgelost die aanvallers in staat kunnen stellen om willekeurige code uit te voeren op getroffen systemen. De meest ernstige kwetsbaarheid, CVE-2025-11458, betreft een heap buffer overflow in de Sync-component van Chrome, wat ernstige beveiligingsrisico's met zich meebrengt. Een andere belangrijke kwetsbaarheid, CVE-2025-11460, betreft een Use-After-Free-voorwaarde in de Storage-component, die kan leiden tot volledige systeemcompromittering. Daarnaast werd CVE-2025-11211 ontdekt, een out-of-bounds leesfout in WebCodecs. Google heeft geavanceerde detectiemethoden ingezet om deze kwetsbaarheden te identificeren en gepaste mitigaties getroffen om de impact van succesvolle aanvallen te beperken. Gebruikers worden aangespoord om de update onmiddellijk te installeren om de risico's te verkleinen.

Ernstige kwetsbaarheid in Figma MCP stelt hackers in staat code op afstand uit te voeren – Patch nu installeren

Onderzoekers op het gebied van cybersecurity hebben details onthuld over een ernstige kwetsbaarheid in de figma-developer-mcp Model Context Protocol (MCP) server, die aanvallers de mogelijkheid biedt om willekeurige code uit te voeren. De kwetsbaarheid, aangeduid als CVE-2025-53967, is een commando-injectieprobleem dat voortkomt uit het niet saneren van gebruikersinvoer. Dit stelt een aanvaller in staat om systeemcommando's uit te voeren door middel van shell-metatekens. De kwetsbaarheid werd ontdekt door cybersecuritybedrijf Imperva en kan leiden tot volledige externe code-uitvoering met de privileges van het serverproces. De patch is beschikbaar in versie 0.6.3 van Figma MCP, uitgebracht op 29 september 2025. Het wordt aangeraden om gebruik van onbetrouwbare invoer te vermijden en over te stappen naar een veiliger alternatief voor het uitvoeren van shell-opdrachten.

Kritieke kwetsbaarheid in AWS ClientVPN voor macOS maakt privilege-escalatie mogelijk

Een kritieke kwetsbaarheid in de AWS Client VPN voor macOS is ontdekt, die een lokaal privilege-escalatie risico vormt voor gebruikers zonder beheerdersrechten. De kwetsbaarheid, aangeduid als CVE-2025-11462, maakt het mogelijk voor aanvallers om root-rechten te verkrijgen door misbruik te maken van het logrotatiemechanisme van de client. Het probleem treft de versies van de macOS-client tussen 1.3.2 en 5.2.0. Aanvallers kunnen een symbolische link creëren naar een systeemlocatie zoals /etc/crontab en via een interne API een kwaadaardige cron-taak injecteren. Dit stelt hen in staat om met root-rechten wachtwoorden te wijzigen. De kwetsbaarheid heeft een CVSS-score van 7,8, wat wijst op een hoog risico. AWS heeft versie 5.2.1 uitgebracht om deze kwetsbaarheid te verhelpen, en gebruikers wordt aangeraden om onmiddellijk te upgraden.

Clop maakt misbruik van Oracle zero-day voor datadiefstal

De Clop ransomware-groep heeft sinds begin augustus misbruik gemaakt van een zero-day kwetsbaarheid in Oracle E-Business Suite (EBS) voor datadiefstal. De kwetsbaarheid, aangeduid als CVE-2025-61882, werd ontdekt in de BI Publisher Integration van de EBS Concurrent Processing component en stelt aanvallers in staat op ongepatchte systemen op afstand code uit te voeren zonder enige gebruikersinteractie. Oracle bracht onlangs een patch uit om deze kwetsbaarheid te verhelpen. Onderzoek door CrowdStrike toont aan dat de aanvallen gericht zijn op

het stelen van gevoelige documenten, en de groep heeft ook geëist dat bedrijven losgeld betalen om de gestolen data niet online te lekken. Beveiligingsexperts waarschuwen voor de exploitatie van deze kwetsbaarheid door andere kwaadwillende actoren, gezien het recente openbaar maken van proof-of-concept-exploits en de patchrelease.

Hackers gebruiken WordPress-sites voor het injecteren van schadelijke PHP-code

Cybercriminelen richten zich op WordPress-websites door schadelijke PHP-code stilletjes in themabestanden te injecteren. Deze malvertisingcampagne maakt gebruik van onopvallende JavaScript-code die bezoekers omleidt en pop-ups weergeeft zonder alarm te slaan bij beveiligingstools. De aanvallen maken gebruik van zwakke bestandstoegangsinstellingen en verouderde thema's, waarbij hackers via een gecompromitteerd inlogaccount of kwetsbare plugins toegang verkrijgen. De geïnjecteerde code werkt achter de schermen en voegt geen zichtbare inhoud toe aan de pagina's. De aanval wordt uitgevoerd via de wp_head-hook, die een verbinding maakt met een server en schadelijke JavaScript-payloads laadt. Dit script is ontworpen om de activiteit te camoufleren als legitieme CDN-operaties, wat detectie voorkomt. Beveiligingsbedrijven zoals Sucuri hebben de campagne geïdentificeerd door ongewone JavaScript-aanroepen naar verdachte domeinen te detecteren. Deze vorm van aanval kan voor langere tijd actief blijven totdat de geïnjecteerde code wordt verwijderd.

LockBit, Qilin en DragonForce vormen strategische alliantie in ransomware-ecosysteem

De ransomwaregroepen LockBit, Qilin en DragonForce hebben hun krachten gebundeld in een nieuwe strategische alliantie. Dit partnerschap is bedoeld om hun aanvallen effectiever te maken door het delen van technieken, middelen en infrastructuur, wat de operationele capaciteiten van elke groep versterkt. De samenwerking komt kort na de heropleving van LockBit, die zijn reputatie onder zijn partners wil herstellen na de lawine van opsporingsacties in 2024. De alliantie kan mogelijk leiden tot een toename van ransomware-aanvallen op kritieke infrastructuren, met name in sectoren die voorheen als minder risicovol werden beschouwd. Qilin, die zich recent tot de meest actieve ransomware-groep heeft ontwikkeld, zal waarschijnlijk profiteren van deze nieuwe samenwerking. Het

partnerschap wordt gezien als een reactie op de recente daling van ransomware-aanvallen wereldwijd, waarbij Qilin, Akira en andere groepen een aanzienlijk aantal aanvallen op zich hebben genomen.

Chinese hackers zetten open-source Nezha-tool in voor nieuwe aanvalsgolf

Hackers met vermoedelijke banden met China hebben de legitieme open-source tool Nezha omgevormd tot een wapen voor cyberaanvallen. Deze aanvallen maken gebruik van Gh0st RAT, een bekend type malware, en richten zich op servers via kwetsbaarheden in phpMyAdmin. De aanvallers maakten gebruik van een techniek genaamd "log poisoning" om een webshell op een server te plaatsen. Dit stelde hen in staat de server op afstand te besturen en de Nezha-tool in te zetten om de slachtoffers verder te compromitteren. De aanvallen werden voornamelijk gedetecteerd in Taiwan, Japan, Zuid-Korea en Hong Kong, maar ook andere landen, waaronder de VS en het VK, werden getroffen. Nezha wordt gebruikt om de aanval verder uit te voeren door Gh0st RAT te activeren, wat kan leiden tot ernstige schade zoals gegevensdiefstal en netwerktoegang.

Nieuwe, ondetecteerbare FUD Android RAT gehost op GitHub

Een geavanceerde Android Remote Access Trojan (RAT) is ontdekt op GitHub, die aanzienlijke beveiligingsrisico's met zich meebrengt voor mobiele gebruikers wereldwijd. De malware, die volledig ondetecteerbare (FUD) capaciteiten biedt, is beschikbaar via een GitHub-repository en kan moderne beveiligingsmaatregelen en antivirusprogramma's omzeilen. Dit type malware is ontworpen om te functioneren via een webinterface, wat het voor cybercriminelen gemakkelijker maakt om het te gebruiken zonder technische expertise. Het maakt gebruik van geavanceerde technieken, zoals AES-128-CBC-encryptie en anti-emulator mechanismen, om detectie te vermijden. De RAT kan wachtwoorden stelen, ransomware uitvoeren en maakt gebruik van sociale-engineeringtechnieken om gebruikers tot het verlenen van onterecht toegang te verleiden. Het kan ook in legitieme apps geïnjecteerd worden, waardoor het moeilijk te detecteren is door traditionele beveiligingssystemen.

TamperedChef-malware als PDF-editor steelt browsergegevens en biedt toegang tot achterdeuren

De TamperedChef-malware, die zich voordoet als een legitieme PDF-editor, heeft recentelijk geleid tot een toename van malvertising-campagnes die Europese organisaties en individuen aantrekken om een vermeende AppSuite PDF Editor te downloaden. Het programma gedraagt zich in eerste instantie als een normaal PDF-bewerkingsprogramma, maar na twee maanden verandert het in een steelse gegevensdiefstaltool. Zodra de malware actief is, verzamelt het automatisch opgeslagen gebruikersnamen en wachtwoorden uit browsers en stuurt deze naar de aanvallers. Dit wordt gedaan zonder dat de gebruiker zich bewust is van de infectie, doordat de interface van de PDF-editor blijft functioneren. De malware maakt gebruik van een autorun-registry-instelling om bij elke herstart van het systeem opnieuw te starten, zonder administratieve rechten te vereisen. Dit maakt de malware vooral gevaarlijk voor bedrijfsomgevingen met beperkte gebruikersrechten.

Yurei-ransomware maakt gebruik van SMB-shares en verwijderbare schijven om bestanden te versleutelen

Yurei-ransomware, die begin september 2025 opdook, richt zich op Windows-omgevingen met een geavanceerde Go-gebaseerde payload voor versleuteling op grote schaal. Nadat de malware is uitgevoerd, zoekt het naar alle toegankelijke lokale en netwerkstations, voegt het de extensie .Yurei toe aan bestanden en schrijft het unieke losgeldnota's in elke getroffen directory. De ransomware verspreidt zich voornamelijk via gestolen inloggegevens en spear-phishingcampagnes en maakt gebruik van Windows Management Instrumentation (WMI) en op wachtwoorden gebaseerde externe uitvoering om toegang te krijgen tot netwerken. Na infectie schakelt de malware de Volume Shadow Copy Service (VSS) uit en verwijdert het bestaande back-ups. De ransomware verspreidt zichzelf via USB-apparaten en SMB-shares, waarbij het zichzelf als WindowsUpdate.exe of System32Backup.exe kopieert. Dit maakt het moeilijk om het netwerksegmentatiebeleid te doorbreken en detectie te voorkomen.

XWorm-malware via Microsoft DevTunnel verspreid

Er is een verdachte URL geïdentificeerd die via de Microsoft DevTunnel-service een Windows Portable Debug (PDB)-bestand verspreidt, gelinkt aan de XWorm-malwarefamilie. Deze tactiek maakt gebruik van ontwikkel- en cloudomgevingen voor malwaredistributie, waarmee vertrouwen gebaseerde verdedigingsmechanismen

worden omzeild. Het verdachte bestand heeft een hoge betrouwbaarheidsscore van 100%. Het URL-adres is https://05q0h4x0-5500.euw.devtunnels.ms/1.pdb. De waarschuwing betreft een payload levering, en het wordt aanbevolen om toegang tot het genoemde domein te blokkeren op DNS- en proxylagen. Daarnaast moeten pogingen om .pdb-bestanden van onbekende of verdachte domeinen te downloaden worden gemonitord. XWorm-artikelen, inclusief persistentie-mechanismen en registerwijzigingen, dienen te worden opgespoord. Het gebruik van ontwikkel-tunnels in bedrijfsomgevingen wordt alleen aanbevolen wanneer strikt noodzakelijk.

Man aangehouden voor sextortion in Lopik

Een 21-jarige man uit Lopik is aangehouden op verdenking van oplichting van een man uit Deventer. De verdachte chantereerde het slachtoffer met beelden van zijn bezoeken aan erotische websites. Hij dreigde de informatie openbaar te maken tenzij het slachtoffer bijna 2000 euro betaalde. Het slachtoffer voldeed aan de eis. Bij de aanhouding van de verdachte werden meerdere telefoons en gegevensdragers in beslag genomen. Deze vorm van oplichting staat bekend als sextortion, waarbij slachtoffers worden gedwongen geld te betalen om de verspreiding van seksuele beelden of berichten te voorkomen. De politie is bezig met het onderzoeken van mogelijke andere slachtoffers en zaken die verband houden met deze vorm van cybercriminaliteit. Eerder deze week werd in Oost-Nederland ook een man uit Vlaardingen gearresteerd voor sextortion.

Man aangehouden voor seksueel afpersen van meerdere vrouwen

De politie van Oost-Nederland heeft op 7 oktober een 23-jarige man uit Vlaardingen aangehouden, verdacht van seksueel afpersen van vijf vrouwen, een praktijk die bekendstaat als sextortion. De man contacteerde de vrouwen via chatrooms van online videogames en social media, waarna het contact zich verplaatste naar Whatsapp. Na maandenlang contact te hebben gehad, kreeg hij de vrouwen zover dat ze seksueel getinte beelden naar hem stuurden. Vervolgens dreigde hij het materiaal openbaar te maken tenzij zij betaalden. De man ontving meer dan 10.000 euro van de slachtoffers. Het onderzoek gaat verder, en er is beslag gelegd op verschillende mobiele apparaten van de verdachte. De slachtoffers kwamen uit verschillende steden zoals Arnhem, Amsterdam en Den Haag. De politie benadrukt

dat slachtoffers van sextortion nooit schuld hebben en moedigt hen aan om hulp te zoeken bij instanties zoals Centrum Seksueel Geweld.

Vijf verdachten aangehouden dankzij Sky ECC-gegevens in grootschalige cocaïnehandel

Van 1 tot 2 oktober hebben de Colombiaanse politie en de Spaanse Guardia Civil, met ondersteuning van Europol, vijf hoofdverdachten gearresteerd die gelinkt zijn aan de Clan del Golfo, een Colombiaans drugskartel. De verdachten waren verantwoordelijk voor het organiseren van grootschalige cocaïnetransporten van Zuid-Amerika naar Europa. Het onderzoek, dat gebruik maakte van gegevens van het versleutelde communicatieplatform Sky ECC, leidde tot de arrestaties en het doorzoeken van zeven locaties in Colombia. Daarbij werden 25 panden, 9 bedrijven en 17 voertuigen in beslag genomen, met een geschatte waarde van 12 miljoen euro. De verdachten speelden verschillende rollen in het netwerk, waaronder het onderhouden van contacten met andere criminele groepen in Europa en het witwassen van crimineel verkregen geld via complexe schema’s met cryptovaluta. De operatie benadrukt de effectiviteit van internationale samenwerking in de bestrijding van georganiseerde misdaad.

Salesforce weigert losgeld te betalen voor grootschalige datadiefstal

Salesforce heeft bevestigd dat het geen losgeld zal betalen aan de dreigingsactoren achter een reeks datadiefstallen die het bedrijf dit jaar teisterden. De aanval werd uitgevoerd door de groep "Scattered Lapsus$ Hunters", die gegevens steelde van 39 bedrijven, waaronder grote namen als FedEx, Disney, Google, Cisco en McDonald's. De aanvallers lanceerden een dataleksite op het domein van BreachForums om de gestolen gegevens te lekken, tenzij de bedrijven losgeld betaalden. Salesforce waarschuwde klanten dat het geen onderhandelingen zou aangaan en dat er geloofwaardige dreigingsinformatie was die aangaf dat de gestolen gegevens openbaar zouden worden gemaakt. De aanvallers claimden bijna 1 miljard datastukken te hebben gestolen, die openbaar zouden worden als er geen betaling werd gedaan. De aanvallers gebruikten sociale-engineeringaanvallen om toegang te krijgen tot Salesforce-omgevingen en gegevens te stelen, en begonnen hun campagne in 2024.

Gemeente Rijswijk waarschuwt voor malafide qr-codes op parkeerautomaten

De gemeente Rijswijk heeft gewaarschuwd voor malafide qr-codes die op parkeerautomaten zijn geplakt. Deze nep qr-codes worden gebruikt door criminelen om persoonlijke gegevens of betaalinformatie van gebruikers te stelen. Wanneer een persoon de qr-code scant, kan hij in plaats van te betalen voor parkeren, onbewust zijn gegevens prijsgeven. De gemeente benadrukt dat zij geen qr-codes gebruikt voor betaald parkeren. Dit incident volgt op eerdere waarschuwingen in andere gemeenten zoals Den Haag, Vlissingen en Rotterdam, waar vergelijkbare malafide codes zijn aangetroffen. Eind september werd in Brussel een man opgepakt die honderden van deze stickers had geplaatst. De politie vond bij hem een grote hoeveelheid printers en stickervellen. Burgers worden aangespoord om dergelijke qr-codes niet te scannen en verdachte situaties te melden.

DraftKings meldt opnieuw datalek veroorzaakt door credential stuffing

DraftKings heeft gebruikers gewaarschuwd voor een datalek veroorzaakt door credential stuffing, waarbij aanvallers geautomatiseerd toegang kregen tot accounts met eerder gestolen inloggegevens. De aanval, ontdekt op 2 september, resulteerde in de toegang tot persoonlijke gegevens van gebruikers, waaronder namen, adresgegevens, telefoonnummers, e-mailadressen, creditcardinformatie, en meer. DraftKings heeft getroffen accounts geblokkeerd en gebruikers verplicht hun wachtwoord te wijzigen en multifactorauthenticatie in te schakelen. Het bedrijf heeft aanvullende technische maatregelen genomen om dergelijke aanvallen in de toekomst te voorkomen. Dit is niet de eerste keer dat DraftKings doelwit is van een credential stuffing-aanval; eerder werden er al duizenden accounts gecompromitteerd, wat leidde tot financiële schade. Een advocatenkantoor is momenteel een onderzoek gestart naar het datalek. Het is nog niet duidelijk hoeveel gebruikers getroffen zijn door deze recente aanval.

OpenAI verstoort Russische, Noord-Koreaanse en Chinese hackers die ChatGPT misbruiken voor cyberaanvallen

OpenAI heeft drie groepen cybercriminelen verstoord die misbruik maakten van het ChatGPT-platform voor het ontwikkelen van malware en phishing-aanvallen. Een van de groepen, vermoedelijk afkomstig uit Rusland, gebruikte ChatGPT om een remote access trojan (RAT) te ontwikkelen, evenals tools voor credential theft en post-

exploitatie. Deze groep gebruikte meerdere ChatGPT-accounts om complexe code te genereren en technische componenten te ontwikkelen. De tweede groep, uit Noord-Korea, richtte zich op het ontwikkelen van malware voor macOS en Windows, evenals phishing-e-mails en andere technieken. De derde groep, een Chinese hackerorganisatie, gebruikte ChatGPT voor phishingcampagnes en om tools voor netwerkbeveiliging te ontwikkelen. OpenAI blokkeerde ook accounts die betrokken waren bij oplichtingsoperaties en invloedcampagnes, met name uit Cambodja, Myanmar en Nigeria, die ChatGPT gebruikten om sociale media-inhoud te genereren voor fraude en propaganda.

EU-parlement ontvangt miljoenen e-mails van campagne tegen chatcontrole

Het Europees Parlement heeft miljoenen e-mails ontvangen in het kader van een campagne tegen chatcontrole, georganiseerd via de website Fightchatcontrol.eu. Deze site, opgezet door een Deense programmeur, stelt gebruikers in staat eenvoudig e-mails te sturen naar Europarlementariërs over bezorgdheden rondom chatcontrole. De e-mails worden via de eigen e-mailclient van gebruikers verzonden. De campagne heeft volgens de organisator bijna 2,5 miljoen bezoekers aangetrokken, wat heeft geleid tot een aanzienlijke stijging van het aantal ontvangen berichten. Deze groei heeft in sommige EU-lidstaten de steun voor het voorstel van Denemarken voor chatcontrole onder druk gezet. De Europese digitale burgerrechtenbeweging EDRi merkt op dat de campagne het onderwerp meer op de agenda heeft gezet, ondanks eerdere geringe publieke aandacht. De stemming over het voorstel vindt naar verwachting op 14 oktober plaats.