Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

15-11-2025:

Mogelijk datalek bij Eurofiber met publicatie interne gegevens

Op een darkwebkanaal is een melding verschenen over een mogelijk datalek bij Eurofiber, waarbij zowel de volledige database als onderdelen van het interne IT systeem zouden zijn buitgemaakt. De claim is op dit moment niet bevestigd door Eurofiber of andere officiële bronnen, waardoor de omvang en betrouwbaarheid van het bericht nog onduidelijk zijn. Als de melding klopt, kan dit gevolgen hebben voor de continuïteit van netwerkdiensten en de bescherming van klantinformatie, omdat Eurofiber een belangrijke rol speelt in digitale infrastructuur in Nederland en omringende landen. De situatie illustreert hoe snel ongeverifieerde datalekclaims kunnen circuleren via online platforms, vaak voordat verificatie heeft plaatsgevonden. Verdere informatie is nodig om de werkelijke impact te bepalen en om vast te stellen of er daadwerkelijk gegevens zijn gepubliceerd.

RTV Noord slachtoffer spray-aanval, geen specifieke targeting

De hack op RTV Noord was een ransomware-aanval, vermoedelijk een spray-aanval, waarbij de cybercriminelen willekeurig zoveel mogelijk systemen probeerden te compromitteren. Dit soort aanvallen is vaak geautomatiseerd en maakt gebruik van AI om kwetsbare systemen te vinden. Het doel van de aanvallers is om zoveel mogelijk data te stelen en daarna losgeld te eisen, zonder dat er sprake is van gerichte targeting. RTV Noord meldde dat de aanval geen specifieke focus had op de omroep, maar dat de interne systemen werden versleuteld en er mogelijk gevoelige werknemersdata werd gestolen. Ondanks de dreiging van publicatie van de gegevens, besloot de omroep niet te betalen. Er werd bevestigd dat de aanval niet het gevolg was van een medewerker die op een verdachte link had geklikt. De omroep werkt nu samen met andere organisaties en het NCSC aan herstel en versterking van de beveiliging.

Anthropic ontdekt AI-gestuurde hackcampagne vanuit China

Onderzoekers van het Amerikaanse bedrijf Anthropic hebben een cyberoperatie ontdekt waarbij kunstmatige intelligentie werd ingezet om delen van een hackcampagne te automatiseren. Volgens Anthropic is dit de eerste gedocumenteerde aanval waarbij AI zelfstandig digitale inbraken aanstuurt. De

operatie, die wordt gelinkt aan de Chinese overheid, richtte zich op ongeveer dertig personen werkzaam bij technologiebedrijven, financiële instellingen, chemische ondernemingen en overheidsorganisaties. Hoewel de aanval beperkt bleef in omvang, beschouwen de onderzoekers het als een zorgwekkende ontwikkeling vanwege de snelheid waarmee AI-gestuurde aanvallen zich ontwikkelen. De betrokken AI-systemen werden gebruikt om processen binnen de aanvallen te optimaliseren en taken zonder menselijke tussenkomst uit te voeren. Anthropic, bekend van de chatbot Claude, wist de campagne in september te verstoren en de betrokken partijen te waarschuwen. De bevinding onderstreept hoe kunstmatige intelligentie cyberdreigingen steeds effectiever maakt.

Van Weel benadrukt urgentie AI-strategie voor nationale en internationale veiligheid

Het demissionaire kabinet van Nederland maakt zich zorgen over de rol van kunstmatige intelligentie (AI) voor zowel de nationale als internationale veiligheid. Minister van Buitenlandse Zaken, David van Weel, benadrukte dat AI wereldwijd steeds belangrijker wordt, wat een integrale aanpak vereist binnen het buitenlandbeleid van Nederland en Europa. In zijn toespraak tijdens de AI Summit Brainport 2025 stelde Van Weel dat de overheid via de EU, de NAVO en de VN zal pleiten voor effectieve wet- en regelgeving rondom AI. Hij benadrukte ook dat landen zoals China AI gebruiken voor grootschalige surveillantie, wat in strijd is met de Europese normen van privacy en mensenrechten. Het kabinet wil dat Nederland een actieve rol speelt in de ontwikkeling van AI, maar op een manier die aansluit bij de Europese waarden van privacy en individuele rechten.

AfD stelt in Duitse parlementen de vragen waarop Moskou graag een antwoord wil

De Duitse politieke partij Alternative für Deutschland (AfD) heeft een reeks vragen gesteld in de parlementen van de deelstaten waarin zij zich hard maken voor een positie die lijkt te sympathiseren met de Russische belangen. Tino Chrupalla, leider van de AfD, uitte twijfels over de dreiging die Rusland voor Duitsland zou vormen. Deze vragen richten zich op onderwerpen die Moskou als belangrijk beschouwt, zoals de relatie van Duitsland met de NAVO en het buitenlandse beleid ten aanzien van Rusland. De partij lijkt hiermee te spelen op de retoriek van Moskou, wat de situatie in Duitsland verder polariseert. Deze ontwikkeling komt op een moment dat de spanning tussen Rusland en de Europese landen, waaronder Duitsland, aanhoudt

door de geopolitieke situatie. De AfD lijkt te trachten de publieke opinie te beïnvloeden met pro-Russische sentimenten in het politieke debat.

Iraanse hackers lanceren 'SpearSpecter' spionagecampagne gericht op defensie- en overheidsdoelen

De Iraanse hacker-groep APT42 heeft een nieuwe spionagecampagne gelanceerd met de codenaam 'SpearSpecter', gericht op defensie- en overheidsfunctionarissen. De aanval maakt gebruik van sociale-engineeringtechnieken om doelwitten, waaronder belangrijke figuren binnen de Islamitische Revolutionaire Garde (IRGC), te misleiden. In deze campagne worden doelwitten uitgenodigd voor prestigieuze evenementen of belangrijke vergaderingen, waarbij ook familieleden van de doelwitten onder druk worden gezet om toegang te verkrijgen tot gevoelige informatie. De aanvallers gebruiken de TAMECAT-malware, die meerdere kanalen zoals HTTPS, Discord en Telegram gebruikt voor commando- en controle (C2), waarmee ze langdurige toegang verkrijgen tot geïnfecteerde systemen. De malware verzamelt gegevens, steelt informatie uit webbrowsers en maakt screenshots, terwijl de exfiltratie via HTTPS of FTP plaatsvindt. Deze campagne toont de geavanceerde capaciteiten van APT42 in cyberaanvallen gericht op langdurige spionage.

Internationaal advies tegen Akira-ransomware ondertekend door NCSC en FBI

De Akira-ransomware vormt nog steeds een ernstige dreiging voor organisaties wereldwijd. Daarom hebben CISA, FBI, Europol (EC3) en het Nederlandse NCSC een gezamenlijk advies uitgebracht binnen de #StopRansomware-campagne. Het document benadrukt dat organisaties hun systemen moeten bijwerken, kwetsbaarheden moeten verhelpen en een streng identity-, credential- en accessmanagementbeleid moeten hanteren volgens NIST-richtlijnen. De Akira-groep, actief sinds maart 2023, richt zich vooral op middelgrote bedrijven in sectoren als industrie, onderwijs, zorg, ICT en financiële dienstverlening. Sinds april 2023 worden naast Windows ook Linux-systemen aangevallen, waaronder VMware ESXi-omgevingen. De criminelen exploiteren onder meer de kwetsbaarheid CVE-2024-40766 in SonicWall-firewalls en zouden al meer dan 244 miljoen dollar hebben verdiend. Het advies waarschuwt dat de groep banden onderhoudt met bekende ransomwarecollectieven zoals Conti en Howling Scorpius.

Google vermindert memory safety-kwetsbaarheden met Rust

Google meldt dat het aantal memory safety-kwetsbaarheden in Android met een factor duizend is afgenomen sinds het gebruik van de programmeertaal Rust. In vergelijking met oudere C- en C++-code is de kans op fouten aanzienlijk verminderd, terwijl codeaanpassingen vier keer minder vaak worden teruggedraaid en de tijd voor codebeoordeling met een kwart is gedaald. Google breidt het gebruik van Rust uit binnen de Android-softwarestack, waaronder de Linux-kernel, firmware en eigen apps. Ook werkt het bedrijf met partners zoals ARM en Collabora aan een GPU-driver in Rust voor kernelmodus. Ondanks de verbeterde veiligheid blijft de taal niet volledig vrij van risico's. Een recente kwetsbaarheid, CVE-2025-48530, in de CrabbyAVIF-bibliotheek toont dit aan, maar dankzij de Scudo-hardened allocator kon exploitatie worden voorkomen.

Kritieke RCE-kwetsbaarheid ontdekt in ImunifyAV-scanner

Een kritieke kwetsbaarheid in de ImunifyAV-malwarescanner voor Linux-servers kan door kwaadwillenden worden misbruikt om willekeurige code op afstand uit te voeren. De fout bevindt zich in de AI-Bolit-component, die wordt gebruikt in Imunify360, ImunifyAV+ en de gratis ImunifyAV-versie. Door een gebrek aan validatie in de functie 'call_user_func_array' kunnen aanvallers schadelijke PHP-functies uitvoeren, zoals 'system' en 'exec'. De fout treft miljoenen websites die draaien op gedeelde hostingplatforms, waaronder servers met cPanel en Plesk. Volgens Patchstack is de kwetsbaarheid eind oktober ontdekt, waarna leverancier CloudLinux op 10 november een beveiligingsupdate uitbracht naar versie 32.7.4.0. Ondanks het ontbreken van een CVE-nummer of actief misbruik in het wild, benadrukken onderzoekers dat het lek ernstige risico's vormt voor de hostingomgeving. CloudLinux heeft inmiddels een whitelist-mechanisme toegevoegd om misbruik te voorkomen.

Kritieke kwetsbaarheid in ASUS DSL-routers verholpen

ASUS heeft een beveiligingsupdate uitgebracht voor een kritieke authenticatie-omzeilingskwetsbaarheid in meerdere DSL-serie routers. De fout, geregistreerd als CVE-2025-59367, maakt het mogelijk voor externe aanvallers om zonder inloggegevens toegang te krijgen tot niet-gepatchte apparaten. De kwetsbaarheid vereist geen gebruikersinteractie en kan leiden tot ongeautoriseerde controle over

het systeem. De getroffen modellen zijn onder andere de DSL-AC51, DSL-N16 en DSL-AC750. De fabrikant heeft firmwareversie 1.1.2.3_1010 gepubliceerd om het lek te dichten. Hoewel er nog geen aanwijzingen zijn voor actieve exploitatie, waarschuwt ASUS dat dergelijke routerlekken vaak worden gebruikt om apparaten op te nemen in botnetnetwerken die voor DDoS-aanvallen worden ingezet. Eerdere kwetsbaarheden in ASUS-routers zijn in het verleden actief misbruikt door geavanceerde actoren, wat het belang van tijdige updates benadrukt.

Kritieke kwetsbaarheden in N-able N-Central software kunnen leiden tot RCE

Op 12 november 2025 werden twee kritieke kwetsbaarheden (CVE-2025-11366 en CVE-2025-11367) ontdekt in de N-able N-Central software, die wordt gebruikt voor remote monitoring en management. De kwetsbaarheden stellen aanvallers in staat om op afstand zonder gebruikersinteractie code uit te voeren. De eerste kwetsbaarheid betreft een Path Traversal-zwakte, terwijl de tweede gaat over het deserialiseren van onbetrouwbare gegevens. Beide kwetsbaarheden kunnen leiden tot ongeautoriseerde toegang, systeemcompromittatie en gegevensdiefstal. Het exploiteren van deze kwetsbaarheden heeft een hoge impact op de vertrouwelijkheid, integriteit en beschikbaarheid van systemen. Organisaties wordt aangeraden de software onmiddellijk te patchen en hun monitoringcapaciteiten te versterken om verdachte activiteiten snel te detecteren.

Kritieke kwetsbaarheid in Dell Data Lakehouse vereist onmiddellijke patch

Op 14 november 2025 werd een kritieke kwetsbaarheid gemeld in Dell Data Lakehouse (CVE-2025-46608), die te maken heeft met onterecht toegangsbeheer. De kwetsbaarheid is aanwezig in versies vóór 1.6.0.0 en kan door een aanvaller met hoge privileges worden misbruikt om verdere escalatie van rechten te verkrijgen, wat leidt tot volledige controle over het systeem. Deze kwetsbaarheid heeft aanzienlijke impact op de vertrouwelijkheid, integriteit en beschikbaarheid van de getroffen systemen. Er is momenteel geen bewijs van exploitatie, maar het wordt sterk aanbevolen om systemen zo snel mogelijk te patchen naar versie 1.6.0.0 of hoger. Daarnaast wordt aanbevolen om de monitoring- en detectiemogelijkheden te verbeteren om verdachte activiteiten tijdig te herkennen en erop te reageren.

Kritieke kwetsbaarheden in IBM AIX en VIOS, patch onmiddellijk

Op 14 november 2025 zijn ernstige beveiligingslekken ontdekt in IBM AIX- en VIOS-systemen, specifiek binnen de NIM-server. De kwetsbaarheden, variërend van CVSS 8,2 tot 10, maken het mogelijk voor aanvallers om op afstand willekeurige commando's uit te voeren, vertrouwelijke gegevens te stelen en bestandsstructuren te manipuleren. Deze zwakheden kunnen ernstige gevolgen hebben voor de bedrijfsvoering en de vertrouwelijkheid, integriteit en beschikbaarheid van systemen. De kwetsbaarheden zijn gecategoriseerd als CVE-2025-36251, CVE-2025-36250, CVE-2025-36096 en CVE-2025-36236. Organisaties wordt dringend aangeraden om de nodige beveiligingsupdates zo snel mogelijk door te voeren, na grondige tests. Daarnaast wordt het versterken van monitoring- en detectiemogelijkheden aanbevolen om verdachte activiteiten snel te kunnen identificeren.

Kritieke kwetsbaarheid in PostgreSQL pgAdmin vereist directe patch

Er zijn ernstige kwetsbaarheden ontdekt in PostgreSQL pgAdmin tot en met versie 9.9, waaronder LDAP-injectie, TLS-certificaatverificatieomzeiling en remote code execution. De kwetsbaarheden, gelabeld als CVE-2025-12762, CVE-2025-12764 en CVE-2025-12765, kunnen ernstige risico’s veroorzaken, zoals het uitvoeren van willekeurige code op kwetsbare systemen, het blootstellen van vertrouwelijke gegevens en verstoring van bedrijfsprocessen. Een van de kwetsbaarheden kan leiden tot Denial of Service door LDAP-injectie, terwijl een andere de integriteit van versleutelde communicatie ondermijnt door de omzeiling van TLS-certificaatverificatie. De meest kritieke kwetsbaarheid maakt het mogelijk om remote code execution uit te voeren tijdens het herstellen van dumpbestanden. Het wordt sterk aanbevolen om de systemen bij te werken naar de nieuwste versie en verdachte activiteiten nauwlettend te monitoren.

Kritieke kwetsbaarheden in AI-inferentie-engines bij Meta, Nvidia en Microsoft

Onderzoekers hebben ernstige kwetsbaarheden ontdekt in AI-inferentie-engines van grote bedrijven, waaronder Meta, Nvidia en Microsoft, evenals in open-sourceprojecten zoals PyTorch. De kwetsbaarheden, die leiden tot remote code execution (RCE), hebben een gemeenschappelijke oorzaak: de onveilige toepassing van ZeroMQ en Python's pickle-deserialisatie. Dit probleem, bekend als ShadowMQ, is verspreid door codehergebruik tussen verschillende projecten, waardoor dezelfde

kwetsbaarheden in meerdere platforms zijn geïntroduceerd. De kwetsbaarheden in Meta's Llama framework (CVE-2024-50050) en andere engines zoals Nvidia's TensorRT-LLM en Microsoft's Sarathi-Serve maken het mogelijk voor aanvallers om kwaadaardige code uit te voeren door het verzenden van manipulatiegegevens via onveilige verbindingen. De kwetsbaarheden kunnen leiden tot modeldiefstal, privilege-escalatie en het uitvoeren van schadelijke payloads zoals cryptocurrency-miners. De meeste van deze kwetsbaarheden zijn inmiddels gepatcht, maar sommige blijven onopgelost.

Fortinet FortiWeb-lek actief misbruikt voor admin-toegang

Een ernstig beveiligingslek in Fortinet FortiWeb wordt actief uitgebuit om zonder authenticatie nieuwe beheerdersaccounts aan te maken op kwetsbare apparaten. Onderzoekers van Defused, PwnDefend en watchTowr Labs ontdekten dat het gaat om een path traversal-kwetsbaarheid waarmee aanvallers volledige toegang tot systemen kunnen verkrijgen. Het lek treft FortiWeb-versies tot en met 8.0.1 en is verholpen in versie 8.0.2, die eind oktober werd uitgebracht. Desondanks heeft Fortinet geen publieke melding gedaan van de kwetsbaarheid of het verhelpen daarvan, wat tot kritiek in de beveiligingsgemeenschap leidt. Rapid7 bevestigde dat meerdere versies kwetsbaar zijn en dat aanvallen sinds begin oktober sterk zijn toegenomen. De exploit wordt inmiddels breed gedeeld via een openbaar beschikbare tool waarmee willekeurige admin-accounts kunnen worden aangemaakt, wat het risico op misbruik verder vergroot. (CVE-2025-64446 / CVE-2025-40684)

Kraken-ransomware test systemen voor optimale encryptiesnelheid

Onderzoekers van Cisco Talos hebben vastgesteld dat de nieuwe variant van de Kraken-ransomware, opvolger van de vroegere HelloKitty-campagne, een unieke methode gebruikt om de encryptiesnelheid van geïnfecteerde systemen te optimaliseren. De malware voert een prestatietest uit om te bepalen of volledige of gedeeltelijke versleuteling het meest effectief is zonder het systeem te overbelasten. Kraken richt zich op Windows-, Linux- en VMware ESXi-omgevingen en verwijdert vooraf schaduwkopieën en back-ups om herstel te bemoeilijken. De groep valt voornamelijk grote organisaties aan in de Verenigde Staten, het Verenigd Koninkrijk, Canada, Panama, Koeweit en Denemarken. Daarnaast exploiteert zij SMB-kwetsbaarheden voor toegang en gebruikt Cloudflared-tunnels en SSHFS voor

datadiefstal. Na de aanval wist een automatisch script sporen, logbestanden en zichzelf. De operatie is gelinkt aan de voormalige HelloKitty-groep, wat wijst op hergebruik van infrastructuur en tactieken.

Scammers misbruiken WhatsApp schermdelen om OTP's en geld te stelen

Een snelgroeiende dreiging, bekend als de schermdelen-oplichting, maakt misbruik van een functie op WhatsApp om geld en persoonlijke gegevens te stelen. De scam maakt gebruik van het schermdelen, dat sinds 2023 beschikbaar is, en heeft wereldwijd al grote verliezen veroorzaakt. In een specifiek geval in Hong Kong verloor een slachtoffer ongeveer 700.000 dollar. De scam begint met een onverwachte videogesprek van een onbekend nummer, waarbij de oplichter zich voordoet als een vertrouwd persoon, zoals een bankmedewerker of een medewerker van Meta. Ze wekken paniek door te claimen dat het account van het slachtoffer is gehackt of dat er verdachte betalingen zijn. Vervolgens wordt het slachtoffer gevraagd om het scherm te delen of apps zoals AnyDesk of TeamViewer te installeren. De oplichter heeft hierdoor toegang tot gevoelige informatie zoals wachtwoorden en OTP's. Meta werkt aan maatregelen om gebruikers beter te beschermen tegen deze dreiging.

Hackers misbruiken RMM-tools LogMeIn en PDQ Connect voor malwareverspreiding

Hackers maken gebruik van Remote Monitoring and Management (RMM)-tools zoals LogMeIn en PDQ Connect om malware te verspreiden, terwijl ze zich voordoen als legitieme programma's. Ze misleiden slachtoffers door populaire software, zoals Notepad++ of 7-Zip, aan te bieden via valse websites. In plaats van de echte applicaties, installeren gebruikers een aangepaste versie van LogMeIn Resolve of PDQ Connect, waarmee de aanvallers volledige controle krijgen over de computers van de slachtoffers. Het malwareprogramma, PatoRAT, wordt geïnstalleerd en biedt aanvallers de mogelijkheid om functies zoals muisbediening, schermopname, keylogging en het stelen van wachtwoorden uit te voeren. Dit alles gebeurt zonder dat de slachtoffers het merken. Onderzoekers ontdekten drie verschillende dreigingsactoren die deze aanvallen uitvoeren, wat wijst op een gecoördineerde poging om systemen wereldwijd aan te vallen.

Nep Bitcoin-tool verbergt DarkComet RAT-malware

Cybercriminelen hebben een nieuwe campagne gelanceerd waarbij de bekende DarkComet remote access trojan (RAT) wordt vermomd als een Bitcoin-applicatie. Deze malware richt zich op cryptocurrency-gebruikers die tools downloaden van onbetrouwbare bronnen. De DarkComet RAT biedt aanvallers volledige controle over geïnfecteerde systemen en stelt hen in staat om bijvoorbeeld toetsaanslagen te registreren, bestanden te stelen, webcams te activeren en desktopcontrole uit te voeren. De malware wordt verspreid als een gecomprimeerd RAR-bestand, waarin een uitvoerbaar bestand is verpakt als "94k BTC wallet.exe". Dit maakt het moeilijker voor antivirussoftware om de malware te detecteren. Na uitvoering installeert de malware zichzelf in het systeem en maakt het verbinding met een command-and-control-server. Gebruikers worden gewaarschuwd om geen cryptocurrency-tools van onbetrouwbare bronnen te downloaden en om up-to-date beveiligingssoftware te gebruiken om dergelijke dreigingen te detecteren.

ClickFix-aanval richt zich op Windows- en macOS-gebruikers met Infostealer-malware

Een nieuwe variant van de ClickFix-aanval richt zich op zowel Windows- als macOS-gebruikers, waarbij informatie-stelende malware wordt geïnstalleerd. Deze aanval maakt gebruik van een social engineering techniek waarbij gebruikers worden misleid om schadelijke commando’s in hun besturingssysteem in te voeren. De aanval kan traditionele beveiligingssystemen omzeilen, omdat de malware binnen een browser-sandbox draait en niet door gebruikelijke e-mailbeveiliging wordt gedetecteerd. De aanvallers maken gebruik van nepwebpagina’s, gehost op vertrouwde platformen zoals Google Colab en Drive, om slachtoffers naar een besmette downloadlink te leiden. Windows-gebruikers krijgen de ACR-stealer te verwerken, terwijl macOS-gebruikers worden doorgestuurd naar de Odyssey-infostealer. Deze malware steelt niet alleen inloggegevens en persoonlijke informatie, maar fungeert ook als loader voor andere bedreigingen, zoals de SharkClipper cryptovaluta-hijacker.

Malafide campagne maakt gebruik van JSON-opslagservices voor malware

Onderzoekers hebben een geavanceerde aanvalscampagne ontdekt waarbij dreigingsactoren legitieme JSON-opslagservices misbruiken om malware te

verspreiden. Deze campagne, genaamd Contagious Interview, maakt gebruik van populaire platforms zoals JSON Keeper en npoint.io om kwaadaardige code te verbergen in legitieme ontwikkelaarsprojecten. De aanval richt zich voornamelijk op softwareontwikkelaars, vooral die in cryptocurrency- en Web3-projecten, op Windows, Linux en macOS-systemen. De aanvallers gebruiken social engineering, waarbij valse recruiters ontwikkelaars benaderen met nep-sollicitaties, om hen naar trojaanse code te leiden die wordt gehost op GitHub of GitLab. Na het uitvoeren van de geïnfecteerde projecten, wordt de BeaverTail infostealer gedownload, die gevoelige informatie steelt. Vervolgens wordt het InvisibleFerret Remote Access Tool ingezet, wat verdere data-exfiltratie en systeeminbraken mogelijk maakt. De slimme inzet van legitieme infrastructuur maakt het moeilijk voor traditionele beveiligingstools om de aanval te detecteren.

SmartApeSG-campagne maakt gebruik van ClickFix-techniek voor NetSupport RAT

De SmartApeSG-campagne, ook wel bekend als ZPHP of HANEY MANEY, heeft zijn aanvallen verfijnd door gebruik te maken van de ClickFix-techniek, waarbij gebruikers worden misleid om een valse CAPTCHA-pagina in te vullen. Deze techniek is een vervolg op eerdere aanvallen die gebruik maakten van nep-browserupdates en wordt nu ingezet om het NetSupport RAT (Remote Access Tool) te installeren. De campagne richt zich op gebruikers van websites die gecompromitteerd zijn en verborgen kwaadaardige scripts bevatten. Bij het klikken op een valse verificatiebox wordt de NetSupport RAT geïnstalleerd, wat de aanvallers volledige controle over het geïnfecteerde systeem geeft. De aanval maakt gebruik van meerdere fasen, waardoor het voor traditionele beveiligingsmaatregelen moeilijk is om de aanval te detecteren en te verwijderen. De gebruikte techniek bypasses traditionele beveiligingsmaatregelen en is een voorbeeld van social engineering.

Politie neemt 250 servers in beslag bij bulletproof hoster

Het Team Cybercrime Oost-Nederland heeft 250 fysieke servers in beslag genomen tijdens een grootschalig onderzoek naar een zogenoemde bulletproof hoster. Dit type hostingbedrijf biedt klanten volledige anonimiteit en weigert doorgaans mee te werken aan opsporingsonderzoeken. Volgens de politie werd de infrastructuur uitsluitend gebruikt voor criminele activiteiten, waaronder ransomware-aanvallen, botnets, phishingwebsites en de verspreiding van materiaal van kindermisbruik. Het

bedrijf dook sinds 2022 op in meer dan tachtig nationale en internationale onderzoeken naar cyberdelicten. De actie vond plaats in datacenters in Den Haag en Zoetermeer, waarbij ongeveer duizend virtuele servers offline zijn gehaald. De in beslag genomen apparatuur wordt momenteel geanalyseerd. De politie richt zich vooral op het beëindigen van de criminele activiteiten die via deze infrastructuur mogelijk werden gemaakt.

VS richt strike force op tegen Chinese cryptofraudeurs

De Amerikaanse autoriteiten hebben een nieuwe Strike Force opgezet om grootschalige Chinese cryptofraudenetwerken aan te pakken die jaarlijks bijna tien miljard dollar van Amerikaanse slachtoffers buitmaken. De teams, die bestaan uit het ministerie van Justitie, de FBI, de Secret Service en het openbaar ministerie, richten zich op het opsporen van geldstromen, het in beslag nemen van digitale tegoeden en het ontmantelen van infrastructuur in Zuidoost Azië. De betrokken criminele organisaties opereren vanuit compounds in onder meer Cambodja, Laos en Birma, waar ook slachtoffers van mensenhandel tot fraude worden gedwongen. De Amerikaanse overheid meldde dat al meer dan vierhonderd miljoen dollar aan cryptovaluta is veiliggesteld en dat aanvullende sancties zijn opgelegd aan gewapende groepen en bedrijven die deze fraude faciliteren. In eerdere operaties werd ook al een omvangrijke hoeveelheid cryptovaluta in beslag genomen bij leiders van transnationale netwerken.

Google past omstreden Android-registratieregels opnieuw aan

Google heroverweegt de invoering van verplichte identiteitsverificatie voor alle Androidontwikkelaars, nadat het eerder aangekondigde beleid leidde tot stevige kritiek uit de gemeenschap. Het bedrijf wilde vanaf 2026 alleen nog apps toestaan van volledig geverifieerde ontwikkelaars, met als doel het verspreiden van malware via sideloading tegen te gaan. De verplichting om een identiteitsbewijs en een vergoeding te overleggen leidde tot brede weerstand onder gebruikers, studenten, hobbyisten en externe appwinkels. F-Droid waarschuwde zelfs dat het project door deze eisen onhoudbaar zou worden. Google kondigt nu een afzonderlijk accounttype aan voor ontwikkelaars die apps in beperkte kring willen verspreiden en werkt aan een nieuw proces voor ervaren gebruikers die bewust ongeverifieerde apps installeren. Dit traject biedt waarschuwingen maar laat de uiteindelijke keuze bij de

gebruiker. De gefaseerde wereldwijde uitrol van volledige verificatie blijft gepland voor 2026 en 2027.

Checkout.com weigert losgeld na datalek door ShinyHunters

Het Britse betalingsplatform Checkout.com meldt een datalek waarbij de cybercriminele groep ShinyHunters toegang kreeg tot een oud cloudopslagsysteem dat gegevens uit 2020 en eerdere jaren bevatte. Het gaat om documentatie en onboardingmateriaal van handelaren, waarbij minder dan een kwart van de huidige klanten is getroffen, maar ook voormalige klanten kunnen zijn betrokken. De toegang werd verkregen via een derde partij waarvan het systeem niet volledig was uitgefaseerd. ShinyHunters eist losgeld, maar Checkout.com weigert te betalen en kondigt aan het bedrag te doneren aan onderzoekscentra van Carnegie Mellon University en de University of Oxford. Het bedrijf richt zich op herstelmaatregelen en extra beveiliging van zijn infrastructuur. De aanvallers staan bekend om datadiefstal via onder meer phishing, social engineering en misbruik van kwetsbaarheden, en worden in verband gebracht met recente aanvallen op grote platforms. De naam van de getroffen opslagdienst is niet bekendgemaakt.