Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

20-11-2025:

Oorzaak hack bij Clinical Diagnostics nog niet vastgesteld

De oorzaak van de hack bij Clinical Diagnostics, waarbij gegevens werden buitgemaakt van 850.000 vrouwen die deelnamen aan het bevolkingsonderzoek baarmoederhalskanker en patiënten van privéklinieken en huisartsen, is nog steeds niet bekend. Het datalek werd begin augustus 2025 openbaar, maar bijna vier maanden later is het nog niet duidelijk hoe de aanvallers toegang kregen tot de systemen van het bedrijf.

Staatssecretaris Tielen van Volksgezondheid heeft in reactie op Kamervragen laten weten dat de oorzaak van de hack onderwerp is van nader onderzoek. Er is op dit moment geen concrete informatie over wanneer de uitkomsten van dit onderzoek verwacht kunnen worden. De staatssecretaris benadrukt echter dat op basis van de bevindingen van het onderzoek gekeken zal worden welke lessen er getrokken kunnen worden.

In reactie op de situatie werd ook gevraagd of er aanvullende beveiligingsmaatregelen worden ingevoerd voor zorgaanbieders, aangezien zij wettelijk verantwoordelijk zijn voor hun eigen informatiebeveiliging. Tielen gaf aan dat de minister van Volksgezondheid ondersteuning biedt, maar dat zorgaanbieders zelf moeten bepalen welke maatregelen ze nemen om hun systemen te beschermen. Daarnaast wordt er door Z-CERT, het Computer Emergency Response Team voor de Nederlandse zorg, nu een scan uitgevoerd op kwetsbaarheden bij alle laboratoria die betrokken zijn bij bevolkingsonderzoeken naar kanker en screeningsprogramma's voor zwangerschap en geboorte.

Cloudflare kampt met grote storing door databaseproblemen

Op dinsdag 18 november 2025 werd Cloudflare getroffen door een van de ergste storingen in zes jaar, die bijna zes uur duurde. Deze storing belemmerde de toegang tot veel websites en online platforms wereldwijd. De oorzaak van de storing was een wijziging in de toegangsrechten van de database die leidde tot een cascade van systeemfouten door het wereldwijde netwerk van Cloudflare. Het bedrijf verklaarde dat de storing niet het resultaat was van een cyberaanval, maar dat een wijziging in de databasepermissies ervoor zorgde dat er foutieve gegevens werden gegenereerd. Dit leidde tot het aanmaken van een te groot configuratiebestand voor het botmanagementsysteem van Cloudflare, wat het netwerk verstoorde.

De storing begon om 11:28 UTC en veroorzaakte een fluctuerende netwerkverbinding doordat het bestand de vooraf ingestelde limieten overschreed, wat leidde tot systeemcrashes. Dit resulteerde in foutmeldingen en een blokkering van verkeer via Cloudflare's netwerken. De technische teams van Cloudflare werkten snel om de oorzaak van het probleem te identificeren en het systeem te herstellen. Het verkeer herstelde zich om 14:30 UTC, en de volledige operatie was weer in werking tegen 17:06 UTC. De storing had invloed op verschillende belangrijke diensten van Cloudflare, waaronder de CDN, beveiligingsdiensten, Turnstile, Workers KV en de toegang tot dashboards en e-mailbeveiliging. CEO Matthew Prince bood zijn excuses aan voor de impact van de storing en benadrukte dat dergelijke incidenten onacceptabel zijn voor een bedrijf van Cloudflare's omvang.

Hackersgroep Black Witch richt schade aan op 30 Nederlandse websites

De hackersorganisatie Black Witch heeft recentelijk zo'n 30 Nederlandse websites gehackt, waaronder de websites van het Martini Ziekenhuis in Groningen, het Isala Ziekenhuis in Zwolle, en vervoersbedrijf Arriva. De aanvallers plaatsten Nazi-teksten en symbolen, waaronder de cijfers 14 en 18, op de voorpagina’s van de getroffen sites. Deze cijfers verwijzen naar een nazimanifest uit de Tweede Wereldoorlog en worden vaak geassocieerd met extreemrechtse groeperingen. De hackers verklaarden dat de actie niet bedoeld was om schade aan te richten, maar om meer naamsbekendheid te genereren en nieuwe leden te werven voor hun groep.

De getroffen instellingen, waaronder de ziekenhuizen, reageerden snel door de ongewenste inhoud te verwijderen en de websites weer operationeel te krijgen. Het Martini Ziekenhuis gaf aan dat de website werd beheerd door een externe partij en dat er gezamenlijk werd onderzocht hoe de aanval had kunnen plaatsvinden. De aanvallers zouden voornamelijk actief zijn vanuit Frankrijk en Rusland en beweren geen gegevens te hebben gestolen, maar dit is nog niet bevestigd door de getroffen organisaties.

Het onderzoek naar de herkomst van de aanval is nog in volle gang, en de schade door de verspreiding van de extreemrechtse boodschappen blijft onduidelijk. Er wordt geen verdere informatie gedeeld over mogelijke beveiligingslekken die door de hackers zijn misbruikt. De organisaties werken samen met relevante autoriteiten om de aanval grondig te onderzoeken.

Twee Oekraïners verdacht van sabotage op Poolse spoorlijn in Russische hybride aanval

Twee Oekraïense staatsburgers worden verdacht van betrokkenheid bij sabotageacties op Poolse spoorlijnen die gebruikt worden voor de transport van voorraden naar Oekraïne. Dit werd bekendgemaakt door de Poolse premier Donald Tusk. De incidenten, die tussen zaterdag en maandag plaatsvonden, beschadigden een cruciale spoorlijn, die zowel militaire als humanitaire leveringen naar Oekraïne mogelijk maakt. Tusk benadrukte dat de verdachten al langer samenwerkten met Russische inlichtingendiensten.

De sabotage maakt deel uit van een bredere hybride oorlogvoering van Rusland, die fysieke aanvallen combineert met digitale operaties, en vormt een serieuze bedreiging voor de nationale veiligheid van Polen, dat een belangrijke strategische rol speelt in de steun aan Oekraïne. De explosie die een deel van de Warschau-Lublin spoorlijn vernietigde, wordt gezien als een gerichte aanval op de Poolse infrastructuur. Ondanks dat er geen gewonden vielen, werd er aanzienlijke schade aangericht. Onderzoekers ontdekten later extra schade op dezelfde route.

Dit incident benadrukt de groeiende dreiging van hybride aanvallen, waarbij digitale en fysieke aanvallen door staten worden ingezet om kwetsbaarheden in andere landen te exploiteren. Het vormt een belangrijk voorbeeld van de evoluerende aard van cyberoorlogvoering, waarin traditionele infrastructuur steeds vaker doelwit wordt van zowel digitale als fysieke aanvallen.

Karremans schort ingreep bij Nexperia op om relatie met China te verbeteren

De demissionair minister van Economische Zaken, Vincent Karremans, heeft besloten de ingreep bij de chipmaker Nexperia op te schorten. Deze ingreep had tot doel belangrijke beslissingen bij het bedrijf tegen te houden die de chipproductie in Europa in gevaar zouden kunnen brengen. Het opschorten van de maatregel is bedoeld om de relatie met China te verbeteren. Karremans had in september de maatregel genomen na zorgen over de Chinese directeur van Nexperia, die de chipproductie in Nederland zou kunnen verplaatsen naar China. Dit zou leiden tot verstoringen in de productie van belangrijke componenten voor de Europese auto-industrie.

Het conflict ontstond nadat China de export van chips uit Nexperia’s fabriek in China blokkeerde als reactie op de ingreep van de Nederlandse overheid. Dit leidde tot

politieke spanningen tussen Nederland en China. Inmiddels heeft China aangegeven uitzonderingen te maken op het exportverbod, wat de situatie heeft verbeterd. Karremans vertrouwt erop dat China de exportvergunningen voor de Nexperia-chips zal blijven verlenen, waardoor de noodzaak voor verdere overheidsingrepen voorlopig is vervallen.

Hoewel de ingreep is opgeschort, betekent dit niet dat de maatregel volledig is teruggedraaid. Karremans kan de ingreep in de toekomst opnieuw laten ingaan als de situatie verslechtert. Dit besluit is genomen na overleg met Chinese autoriteiten en de toezegging dat de benodigde chips blijven geleverd worden voor de Europese automobielsector. Het is nog onduidelijk welke gevolgen dit heeft voor de langere termijn, aangezien de belangen tussen Nederland, Europa en China complex blijven.

Rusland gebruikt hybride tactieken om Europa te destabiliseren via cyberaanvallen en desinformatie

Rusland zet hybride tactieken in om de stabiliteit van Polen en andere Europese landen te ondermijnen, waarbij cyberaanvallen, desinformatie en sabotage een sleutelrol spelen. Volgens Tomasz Siemoniak, voormalig Poolse minister van Binnenlandse Zaken en momenteel coördinator van speciale diensten, is de uiteindelijke doelstelling van Rusland destabilisatie en het verstoren van de solidariteit tussen westerse landen. De recente Russische aanvallen omvatten niet alleen fysieke sabotages, zoals de inzet van drones in het Poolse luchtruim, maar ook gerichte cyberoperaties en pogingen tot desinformatieverspreiding.

Een van de meest opvallende incidenten was de aanval met Russische drones in september 2025, waarbij meer dan twintig drones het Poolse luchtruim binnendrongen. Hoewel de drones niet bewapend waren, benadrukt het voorval de kwetsbaarheid van Europese infrastructuur voor cyber- en hybride aanvallen, die steeds complexer en schadelijker worden. Dit soort incidenten zijn indicatief voor de steeds grotere rol die digitale en cyberaanvallen spelen in geopolitieke conflicten, en het belang van robuuste cyberbeveiliging binnen de EU.

Siemoniak wijst erop dat Rusland een breed scala aan digitale middelen inzet, waaronder cyberaanvallen, desinformatiecampagnes en manipulatie van de publieke opinie, om de steun voor Oekraïne te verzwakken en verdeeldheid te zaaien binnen de EU. Het doel is niet alleen fysieke schade aanrichten, maar ook sociaal-politieke instabiliteit creëren door online en offline chaos te veroorzaken. Cybercriminelen en

hackers die mogelijk in dienst staan van de Russische staat worden vaak ingezet om gevoelige informatie te stelen of verspreiding van valse informatie te bevorderen.

Polen reageerde adequaat op deze dreigingen, zowel met militaire middelen als door het activeren van NAVO-leden om gezamenlijke veiligheid te waarborgen. Desondanks heeft de inzet van cyberaanvallen en desinformatie een bredere strategische impact, die de Europese landen herinnert aan de noodzaak van een gezamenlijke, robuuste verdediging tegen digitale dreigingen. Dit voorval onderstreept de urgentie voor verdere versterking van de digitale weerbaarheid van Europa tegen hybride dreigingen, die de stabiliteit van naties wereldwijd kunnen ondermijnen.

Polen reageert op Russische sabotage van spoorlijn met sluiting van consulaat in Gdańsk

Polen heeft aangekondigd het Russische consulaat in Gdańsk te sluiten als reactie op sabotage-aanvallen op de belangrijke spoorlijn tussen Warschau en Lublin, een incident dat door de Poolse autoriteiten als "staatsterrorisme" wordt bestempeld. De aanval richtte zich op kritieke infrastructuur en wordt gekoppeld aan Russische inlichtingenactiviteiten, waarbij de aanvallers volgens de autoriteiten samenwerkten met Oekraïense nationals die naar Belarus zijn gevlucht. De sabotage werd uitgevoerd door explosieven en het saboteren van spoorrails en elektriciteitsvoorzieningen.

Dit incident is onderdeel van een bredere trend waarin fysieke en digitale aanvallen door staten worden ingezet om strategische doelen te bereiken. De actie benadrukt de toenemende dreiging van hybride oorlogsvoering, waarbij zowel traditionele als cyberaanvallen worden gebruikt om nationale veiligheid te ondermijnen. Polen, als belangrijke doorvoerroute voor wapenleveranties aan Oekraïne, heeft te maken met een verhoogd risico op dergelijke operaties. De sluiting van het consulaat markeert een escalatie van de diplomatieke spanningen, waarbij Polen zich niet alleen voorbereidt op diplomatieke reacties, maar ook op de versterking van zijn nationale veiligheidsmaatregelen tegen digitale dreigingen en sabotage.

Opschorting maatregel Nexperia en de gevolgen voor digitale infrastructuur

Minister Karremans heeft de maatregel om in te grijpen bij chipbedrijf Nexperia opgeschort, in een poging om de diplomatieke verhoudingen met China te verbeteren. De maatregel werd eerder ingevoerd nadat de Chinese directeur van Nexperia verdacht werd van het leegtrekken van het bedrijf, wat de productie van essentiële chips in Europa zou kunnen bedreigen. Door deze ingreep moest Nexperia toestemming aanvragen voor belangrijke beslissingen, waaronder de export van chips naar Europa, wat vooral van invloed was op de technologie- en auto-industrie.

De opschorting van deze maatregel heeft de levering van Nexperia-chips, essentieel voor veel digitale toepassingen, opnieuw op gang gebracht. De blokkade door China had geleid tot productieonderbrekingen, vooral in sectoren die sterk afhankelijk zijn van halfgeleiders. Ondanks de opschorting blijft de situatie fragiel, en Nederland houdt de mogelijkheid open om de maatregel opnieuw in te voeren als het risico op verlies van technologie en productie naar China opnieuw dreigt.

Deze kwestie benadrukt de kwetsbaarheid van de Europese digitale infrastructuur en de risico’s die verbonden zijn aan geopolitieke spanningen over strategische technologie. De handel in halfgeleiders en de controle over productiecapaciteiten in verschillende landen kunnen invloed hebben op de cyberveiligheid van bedrijven en overheden wereldwijd. De situatie onderstreept de noodzaak voor meer robuuste strategieën om de digitale infrastructuur te beschermen tegen geopolitieke invloeden en de risico’s van buitenlandse controle over kritieke technologieën.

Fortinet waarschuwt voor opnieuw actief misbruikt lek in FortiWeb-firewall

Fortinet heeft opnieuw gewaarschuwd voor een actief misbruik van een beveiligingslek in de FortiWeb-firewall, een apparaat dat bedoeld is om applicaties te beschermen tegen aanvallen. De kwetsbaarheid, aangeduid als CVE-2025-58034, maakt het mogelijk voor geauthenticeerde aanvallers om via HTTP-requests OS-commando’s op de firewall uit te voeren, wat kan leiden tot compromittering van het apparaat. Deze kwetsbaarheid werd eerder al gepatcht in versies 8.0.2, 7.6.6, 7.4.11, 7.2.12 en 7.0.12, maar de kwetsbaarheid werd niet vermeld in de release notes van de updates.

Onlangs bevestigde Fortinet dat er ook andere kwetsbaarheden actief werden misbruikt, waaronder een eerder gepatchte kwetsbaarheid (CVE-2025-64446), maar wederom zonder melding in de betreffende updates. Het Amerikaanse Cybersecurity

and Infrastructure Security Agency (CISA) heeft federale overheidsinstanties opgedragen de patch voor CVE-2025-58034 binnen een week te implementeren. Het CISA hanteert doorgaans een drie weken termijn voor dergelijke patches, maar heeft vanwege de ernst van de situatie besloten een versnelde aanpak toe te passen.

Deze herhaalde waarschuwingen benadrukken de voortdurende risico's die voortkomen uit het niet adequaat communiceren van kwetsbaarheden in beveiligingsproducten en de noodzaak voor bedrijven en overheidsinstanties om tijdig patches toe te passen.

Kritieke kwetsbaarheid in Emby Server stelt systemen bloot aan op afstand code-uitvoering

Op 19 november 2025 werd een ernstige kwetsbaarheid ontdekt in Emby Server, versie 4.8.1.0 en eerdere versies, die het mogelijk maakt voor aanvallers om op afstand kwaadaardige code uit te voeren. Deze kwetsbaarheid, aangeduid als CVE-2025-64325, heeft een CVSS-score van 8.4, wat wijst op een hoge ernst. De kwetsbaarheid ontstaat doordat aanvallers via gemanipuleerde authenticatieverzoeken toegang kunnen verkrijgen tot het beheerdersdashboard van de server. Hierdoor kunnen zij code uitvoeren met administratieve rechten, wat hen in staat stelt om persistentie op de server te verkrijgen en mogelijk andere systemen binnen hetzelfde netwerk aan te vallen.

De kwetsbaarheid vormt een aanzienlijk risico, vooral wanneer de Emby-server openbaar toegankelijk is. Een succesvolle exploitatie kan leiden tot verlies van vertrouwelijkheid en integriteit van de server, terwijl de beschikbaarheid onaangetast blijft.

Het wordt sterk aanbevolen om Emby Server direct te patchen naar de nieuwste versie om deze kwetsbaarheid te verhelpen. Het is belangrijk te realiseren dat het patchen van de software toekomstige aanvallen voorkomt, maar geen oplossing biedt voor eerder opgetreden compromitteringen.

Kwetsbaarheid in ServiceNow AI-agents: tweede-orde promptinjectie mogelijk

Een nieuwe kwetsbaarheid in de ServiceNow Now Assist AI-platformen is ontdekt, die het mogelijk maakt voor aanvallers om de AI-agenten tegen elkaar te laten werken via tweede-orde promptinjectie. Dit maakt misbruik van de agent-naar-agent

ontdekking die standaard in de configuratie van het platform is ingeschakeld. De kwetsbaarheid stelt kwaadwillenden in staat om onbevoegde acties uit te voeren, zoals het kopiëren van vertrouwelijke bedrijfsgegevens, het wijzigen van records en het escaleren van machtigingen.

De kwetsbaarheid wordt mogelijk doordat ServiceNow Now Assist-agenten automatisch worden gegroepeerd en als 'ontdekbaar' gemarkeerd wanneer ze worden gepubliceerd. Dit maakt het mogelijk voor een schijnbaar onschuldige agent om toegang te krijgen tot gevoelige data of interne systemen door een ander agent in het team in te schakelen voor kwaadaardige doeleinden. Het gevaar hiervan is dat de acties vaak onopgemerkt blijven bij de getroffen organisatie, aangezien ze plaatsvinden op de achtergrond. Dit wordt als normaal gedrag binnen de platformconfiguratie beschouwd, maar biedt ruimte voor misbruik via het manipuleren van de instellingen voor agent-communicatie.

Om dergelijke aanvallen te voorkomen, wordt geadviseerd om een gecontroleerde uitvoeringsmodus voor machtigde agenten in te schakelen, de autonome override-optie uit te schakelen en agenten op basis van teamtaken te segmenteren. Het is belangrijk voor organisaties die gebruik maken van Now Assist om hun configuraties zorgvuldig te controleren om zo het risico op dergelijke promptinjectie-aanvallen te minimaliseren.

Kritieke kwetsbaarheid ontdekt in W3 Total Cache WordPress-plugin

Een ernstige kwetsbaarheid in de W3 Total Cache (W3TC) WordPress-plugin is recent ontdekt, waarmee kwaadwillenden PHP-commando’s op de server kunnen uitvoeren door het plaatsen van een commentaar met een kwaadwillige payload. De kwetsbaarheid, aangeduid als CVE-2025-9501, heeft betrekking op alle versies van de W3TC-plugin vóór versie 2.8.13. Het probleem wordt beschreven als een niet-geauthenticeerde commando-injectie.

De W3TC-plugin is geïnstalleerd op meer dan één miljoen websites en wordt gebruikt om de prestaties van sites te verbeteren door laadtijden te verminderen. De ontwikkelaar bracht op 20 oktober 2025 versie 2.8.13 uit, die de beveiligingsfout verhelpt. Desondanks blijkt uit gegevens van WordPress.org dat honderden duizenden websites mogelijk nog kwetsbaar zijn, aangezien er sinds de uitgave van de patch ongeveer 430.000 downloads hebben plaatsgevonden.

Beveiligingsonderzoekers van WPScan melden dat een aanvaller de kwetsbaarheid kan uitbuiten door de _parse_dynamic_mfunc()-functie, die verantwoordelijk is voor het verwerken van dynamische functieverzoeken in gecachete inhoud, te misbruiken. Hiermee kunnen onbevoegde gebruikers PHP-commando's uitvoeren door een schadelijke payload in een commentaar te plaatsen.

Als de kwetsbaarheid wordt misbruikt, kan de aanvaller volledige controle over de getroffen website verkrijgen, aangezien er geen authenticatie nodig is om commando's op de server uit te voeren. WPScan heeft een proof-of-concept (PoC) voor deze kwetsbaarheid ontwikkeld en zal dit op 24 november 2025 publiceren, zodat beheerders voldoende tijd hebben om de benodigde updates te installeren.

Websitebeheerders die niet op tijd kunnen upgraden, wordt aangeraden om de W3 Total Cache-plugin tijdelijk uit te schakelen of maatregelen te nemen om te voorkomen dat opmerkingen schadelijke payloads bevatten die de exploit kunnen activeren. De aanbevolen actie is om over te stappen naar versie 2.8.13 van de plugin.

Aanvallers verspreiden besmette software-updates via gehackte routers

Een groep aanvallers heeft besmette software-updates verspreid via gehackte routers, waarbij zowel organisaties als individuele gebruikers doelwit waren. Dit meldt antivirusbedrijf ESET na een grondige analyse. De aanvallers maken gebruik van de zogenaamde advanced persistent threat (APT) PlushDaemon, die wereldwijd slachtoffers heeft gemaakt, waaronder in de Verenigde Staten, Taiwan, China, Hong Kong, Nieuw-Zeeland en Cambodja.

De aanval begint met het compromitteren van netwerkapparatuur, zoals routers, die door de aanvallers worden overgenomen. Hoe deze apparaten precies worden gehackt, is nog niet bekend, maar ESET vermoedt dat kwetsbaarheden of zwakke wachtwoorden hierbij een rol spelen. Eenmaal in controle van het apparaat installeren de aanvallers malware, die het verkeer van de doelwitten omleidt naar een eigen DNS-server. Deze server controleert vervolgens of de DNS-verzoeken van de doelwitten betrekking hebben op software-updates.

Wanneer het doelwit via HTTP op zoek gaat naar software-updates, kunnen de aanvallers deze communicatie onderscheppen en een vervalste update aanbieden. Als de gebruiker deze update uitvoert, wordt het systeem geïnfecteerd met malware.

Onder de slachtoffers bevinden zich ook gebruikers van de populaire Chinese keyboard-app Sogou. Het doel van de aanvallers lijkt primair gericht op spionage.

ShadowRay 2.0-aanvallen zetten Ray-clusters om in cryptomining-botnets

Een nieuwe wereldwijde aanvalscampagne, ShadowRay 2.0, heeft als doel Ray-clusters die via een oude kwetsbaarheid op het internet toegankelijk zijn. De aanvallers misbruiken een zwakte in de code van het Ray-framework, ontwikkeld door Anyscale, en zetten deze om in een zelf-propaganderend cryptomining-botnet. Het Ray-framework wordt veel gebruikt om kunstmatige-intelligentie (AI) en Python-applicaties te schalen in gedistribueerde systemen die zijn georganiseerd in clusters, of hoofdknopen.

Onderzoekers van het beveiligingsbedrijf Oligo hebben ontdekt dat de dreigingsactor, aangeduid als IronErn440, gebruik maakt van AI-gegenereerde payloads om de kwetsbare Ray-infrastructuur te compromitteren. De aanvallen richten zich op systemen die zonder authenticatie bereikbaar zijn via de openbare internetverbinding. De aanvallers zetten de Ray-clusters niet alleen in voor cryptomining, maar stelen ook data en inloggegevens en voeren DDoS-aanvallen uit.

De ShadowRay 2.0-campagne maakt gebruik van de kwetsbaarheid CVE-2023-48022, die al in de eerdere ShadowRay-campagne van 2023 werd uitgebuit. Hoewel er nog steeds geen oplossing is voor deze beveiligingsflaw, blijft het aantal kwetsbare Ray-servers op het internet enorm groeien. Oligo constateerde recent twee aanvalsgolven, waarvan de eerste via GitLab plaatsvond en eindigde op 5 november, en de tweede via GitHub die op 17 november begon.

De payloads die in deze aanvallen worden gebruikt, worden gegenereerd met behulp van grote taalmodellen, een techniek die goed zichtbaar is in de code en foutafhandelingspatronen. De aanvallers controleren de beschikbare CPU- en GPU-middelen en maken gebruik van het cryptominingprogramma XMRig om Monero te minen. De malware is zo geconfigureerd dat deze zijn activiteiten verbergt, bijvoorbeeld door valse procesnamen zoals ‘dns-filter’ te gebruiken en zijn invloed te verspreiden via cronjobs en systeeminstellingen.

Naast het cryptominen opent de malware Python reverse shells naar de infrastructuur van de aanvaller voor interactief beheer, waardoor toegang wordt verkregen tot gevoelige gegevens zoals MySQL-wachtwoorden en AI-modellen die

op de server zijn opgeslagen. Ook kan de malware DDoS-aanvallen uitvoeren met behulp van de Sockstress-tool.

Omdat er geen patch beschikbaar is voor de kwetsbaarheid in CVE-2023-48022, wordt gebruikers van Ray aangeraden om hun clusters te beschermen door het implementeren van de best practices van de leverancier. Dit omvat het beperken van ongeautoriseerde toegang door middel van firewallregels, het implementeren van extra autorisatie op het Ray-dashboard en het continu monitoren van AI-clusters om afwijkende activiteiten tijdig te detecteren.

Sneaky 2FA phishingkit voegt BitB-pop-ups toe die browseradresbalk nabootsen

De malware cybercriminelen achter de Phishing-as-a-Service (PhaaS)-kit genaamd Sneaky 2FA hebben een nieuwe functie toegevoegd aan hun toolkit: de Browser-in-the-Browser (BitB)-techniek. Deze ontwikkeling maakt het voor cybercriminelen eenvoudiger om massale phishingaanvallen uit te voeren, zelfs door minder ervaren aanvallers. BitB maakt het mogelijk om valse browservensters te creëren die eruitzien als inlogpagina's van legitieme diensten, wat het voor slachtoffers moeilijk maakt om verdachte URLs te identificeren.

BitB werd voor het eerst gedocumenteerd in 2022 door beveiligingsonderzoeker mr.d0x, die aantoonde hoe HTML- en CSS-code gebruikt kunnen worden om een browservenster na te maken dat lijkt op een pop-up inlogformulier. Dit venster toont een legitieme URL, zoals die van Microsoft, waardoor slachtoffers in de veronderstelling verkeren dat ze hun gegevens invoeren op een authentieke inlogpagina, terwijl ze in werkelijkheid op een phishingpagina terechtkomen.

In een recent waargenomen aanval kwamen gebruikers die een verdachte URL bezochten, bijvoorbeeld "previewdoc[.]us", terecht op een Cloudflare Turnstile-check, bedoeld om bot-aanvallen tegen te gaan. Nadat de gebruiker deze controle had doorstaan, werd een valse inlogpagina geladen die leek op een Microsoft-loginformulier. Wanneer het slachtoffer zijn gegevens invoerde, werden deze direct naar de aanvallers verzonden, die hiermee het Microsoft-account konden overnemen.

De aanvallers maken daarnaast gebruik van geavanceerde technieken, zoals het snel wisselen van phishingdomeinen om detectie te vermijden en het toepassen van beveiligingsmaatregelen zoals CAPTCHA en Cloudflare Turnstile. Ze gebruiken ook voorwaardelijke laadtechnieken om ervoor te zorgen dat alleen de bedoelde

slachtoffers toegang krijgen tot de phishingpagina's, terwijl andere gebruikers naar onschuldige websites worden geleid.

De Sneaky 2FA-kit is ook ontworpen om de analyse van de phishingpagina's te bemoeilijken. Zo worden bijvoorbeeld browserontwikkelaarstools uitgeschakeld en wordt de broncode versleuteld. Dit maakt het voor beveiligingsexperts moeilijker om de pagina's snel te inspecteren en te blokkeren.

Deze aanvallen maken deel uit van een bredere trend waarbij cybercriminelen hun phishinginfrastructuur steeds verder professionaliseren, wat hen in staat stelt om geavanceerdere en moeilijker te detecteren aanvallen uit te voeren. Gebruikers moeten waakzaam blijven bij het openen van verdachte berichten of het installeren van browserextensies en organisaties kunnen overwegen om strikte toegangscontrolemaatregelen te implementeren om accountovernames te voorkomen.

Mobiele dreigingen in Q3 2025: Analyse van malware en ransomware

In het derde kwartaal van 2025 werd een aanzienlijke toename van mobiele dreigingen gerapporteerd. De Kaspersky Security Network (KSN) legde de focus op de preventie van 47 miljoen aanvallen die gebruikmaakten van malware, adware of ongewenste mobiele software. Ondanks een lichte afname in het totale aantal aanvallen ten opzichte van het vorige kwartaal, bleef de dreiging van mobiele malware een belangrijk aandachtspunt.

Trojans bleken de meest voorkomende bedreiging, met 15,78% van de getroffen gebruikers die ermee geconfronteerd werden. De data onthult dat er meer dan 197.000 kwaadaardige installatiepakketten werden gedetecteerd, waarvan er 52.723 werden geassocieerd met mobiele banktrojans en 1564 pakketten met ransomwaretrojans.

Opmerkelijke bevindingen zijn onder andere een nieuwe versie van de BADBOX backdoor, die smartphones infecteerde via een kwaadaardige ingebouwde bibliotheek. Ook werd de Trojan-Downloader.AndroidOS.Agent.no gedetecteerd, die gebruik maakte van gemodificeerde apps om advertenties te manipuleren en de gebruiker onbedoeld in te zetten voor frauduleuze activiteiten.

In termen van regionale dreigingen blijkt dat de meeste aanvallen gericht waren op gebruikers in Turkije, India en Iran, met een opmerkelijke toename van ransomware-

aanvallen in Duitsland. Het aantal gedetecteerde ransomware trojans nam meer dan twee keer toe, waarbij de Trojan-Ransom.AndroidOS.Rkor.ii de lijst aanvoerde.

Banking Trojans bleven een prominente dreiging, met de Mamont en Coper varianten die de grootste delen van de aanvallen vertegenwoordigden. De Mamont-varianten waren verantwoordelijk voor 61,85% van de aanvallen, maar Coper trojan varianten stegen in de ranglijst van getroffen gebruikers.

Deze statistieken benadrukken de toenemende dreiging van mobiele malware en ransomware, vooral gericht op banktransacties en gegevensdiefstal via apps. De bevindingen onderstrepen de noodzaak voor verbeterde bescherming tegen deze soorten dreigingen, met name voor gebruikers in risicogebieden.

Microsoft-update creëert aanvalsvector voor infostealers via Agentic OS

Een recente update voor Windows 11 heeft een nieuw potentieel gevaar gecreëerd voor de gebruikersbeveiliging door de integratie van een AI-agent op de taakbalk. Deze zogenaamde "Ask Copilot" is ontworpen om gebruikers te helpen door toegang te bieden tot verschillende functies en gegevens. De AI-agent heeft echter persistent toegang tot verschillende systeemcontexten, bestanden en gebruikersacties, wat het voor aanvallers gemakkelijker maakt om misbruik te maken van de verzamelde gegevens. Door deze centralisatie van gegevens wordt de taakbalkagent een aantrekkelijk doelwit voor cybercriminelen, die gebruik kunnen maken van de vertrouwensrelatie tussen de gebruiker en de agent om gevoelige informatie te stelen.

Infostealers, die vroeger voornamelijk bestanden onderschepten, hebben hun werkwijze geëvolueerd naar wat nu bekend staat als "Agent Hijackers." In plaats van eenvoudige malware die wachtwoorden of bestanden steelt, kunnen aanvallers nu een Word-, Excel- of PDF-bestand maken met verborgen instructies voor de agent. Wanneer de gebruiker de agent aanroept om te helpen, bijvoorbeeld door te vragen om een document samen te vatten, kan de agent onbewust vertrouwelijke informatie zoals wachtwoorden, API-sleutels of zelfs cryptosleutels exfiltreren.

Deze nieuwe aanvalsmethoden maken gebruik van zogenaamde 'Cross-Prompt Injection' (XPIA), waarbij kwaadwillende inhoud in documenten of UI-elementen de instructies van de agent kan omzeilen. Dit biedt aanvallers een effectievere manier om toegang te krijgen tot systemen zonder dat de gebruiker zich hiervan bewust is. De mogelijkheid om sessie-informatie, bedrijfsgegevens of zelfs cryptowalletsleutels

te stelen, maakt deze aanvallen aanzienlijk krachtiger dan traditionele aanvallen die enkel wachtwoorden stelen.

Het is duidelijk dat deze nieuwe aanvalsvector een risico vormt voor zowel individuele gebruikers als bedrijven, vooral gezien de verhoogde mate van toegang die de agent biedt tot het systeem van de gebruiker. In dit licht is het belangrijk dat zowel consumenten als organisaties zich bewust zijn van deze nieuwe dreiging en de potentieel verwoestende impact ervan.

Kwaadaardige 'gratis' VPN-extensie met 9 miljoen installaties hijackt gebruikersverkeer en steelt browsegegevens

Een misleidende browsercampagne heeft miljoenen gebruikers blootgesteld aan uitgebreide surveillance via ogenschijnlijk onschuldige VPN-extensies. Chrome-extensies, die werden gepromoot als 'gratis onbeperkte VPN'-diensten, verzamelden meer dan 9 miljoen installaties voordat de malware werd ontdekt, waarbij deze voor bijna zes jaar onopgemerkt bleef.

Deze extensies beloofden eenvoudige privacyoplossingen met een klik op de knop, maar boden precies het tegenovergestelde: volledige zichtbaarheid in het browsegedrag en netwerkverkeer van de gebruiker. De extensies fungeerden als op afstand bediende proxy-systemen in plaats van traditionele VPN's. Ze haalden verborgen configuratiebestanden op van door aanvallers gecontroleerde servers, pasten proxy-instellingen in realtime aan en onderschepten elke browsernavigatie.

Door het verkeer via ongeautoriseerde servers om te leiden, kregen de aanvallers toegang tot gevoelige informatie, zoals inloggegevens, financiële gegevens en persoonlijke browsepatronen. De campagne toont aan hoe eenvoudige machtigingen, in combinatie met minimale controle, legitiem ogende tools kunnen transformeren in surveillance-instrumenten.

Beveiligingsanalisten van LayerX Security identificeerden en documenteerden de campagne, waarbij twee hoofdlijnen van de extensies werden ontdekt die actief waren van 2019 tot mei 2025. Na het verwijderen van deze extensies verscheen er echter al snel een vrijwel identieke versie, wat suggereert dat de operators vastbesloten bleven hun aanvalsinfrastructuur te handhaven.

In de versie van 2025 werden geavanceerde technieken gebruikt om detectie te vermijden, zoals vertragingen van twee seconden voordat de proxy werd

geactiveerd, wat bedoeld was om analyses door sandbox-tools te omzeilen. De extensie controleerde op concurrerende proxytools en schakelde deze volledig uit, zodat het volledige verkeer van de gebruiker werd gecontroleerd. Dit maakte het mogelijk voor de aanvallers om de gebruikers naar phishing-pagina's of advertentiefarma's om te leiden zonder dat de gebruiker ingreep.

Deze ontdekking benadrukt kritieke beveiligingslekken in de architectuur van browserextensies, waarbij de uitgebreide machtigingen die aan extensies worden verleend niet voldoende runtime-controle bevatten. Dit stelt aanvallers in staat om op afstand volledige controle over de browsers van slachtoffers over te nemen en gevoelige gegevens te stelen.

Duizenden end-of-life Asus-routers gekaapt via bekende AiCloud-lekken

Duizenden end-of-life Asus-routers zijn gekaapt door cybercriminelen door gebruik te maken van bekende kwetsbaarheden in de AiCloud-service. Deze service stelt gebruikers in staat om vanaf het internet toegang te krijgen tot lokale bestanden op apparaten die met de Asus-routers zijn verbonden. Onderzoekers van het cybersecuritybedrijf Security Scorecard hebben vastgesteld dat aanvallers gebruikmaken van zes verschillende kwetsbaarheden, waarvan vier al twee jaar oud zijn. De meeste van de gecompromitteerde routers zijn end-of-life en ontvangen geen beveiligingsupdates meer van Asus, wat hen extra kwetsbaar maakt voor dergelijke aanvallen.

De aanvallen richten zich met name op routers in landen zoals Taiwan, Rusland, Europa en de Verenigde Staten, waarbij onderzoekers ongeveer vijftigduizend besmette IP-adressen hebben waargenomen. Er wordt vermoed dat de gecompromitteerde routers worden gebruikt als zogenaamde Operational Relay Boxes (ORB), waarmee aanvallers hun verkeer kunnen omleiden. Dit maakt het moeilijker om hun activiteiten te detecteren en biedt hen bijvoorbeeld de mogelijkheid om lokale IP-adressen te verkrijgen of aanvallen te verbergen.

Asus heeft updates uitgebracht voor de kwetsbaarheden die zijn ontdekt in hun AiCloud-service, maar de meeste getroffen routers ontvangen deze updates niet meer omdat ze niet langer ondersteund worden. Het gebruik van end-of-life routers zonder ondersteuning vormt dus een significant risico voor zowel consumenten als bedrijven die dergelijke apparaten in hun netwerken gebruiken.

ShinySp1d3r: Nieuwe Ransomware-as-a-Service van ShinyHunters

Een in ontwikkeling zijnde versie van het ransomware-as-a-service platform, genaamd ShinySp1d3r, is onlangs opgedoken en biedt een voorproefje van de aankomende extortiecampagne. Deze ransomware wordt ontwikkeld door de ShinyHunters-groep, bekend van eerdere aanvallen, en richt zich nu op het aanbieden van hun eigen encryptor voor gebruik door hun affiliates. De groep was voorheen afhankelijk van encryptoren van andere ransomwarebendes zoals ALPHV/BlackCat, Qilin, RansomHub en DragonForce, maar is nu bezig met het opzetten van een eigen operatie.

Het ShinySp1d3r platform heeft een encryptor die meerdere geavanceerde technieken gebruikt. Zo wordt de EtwEventWrite functie gemanipuleerd om te voorkomen dat gegevens in de Windows Event Viewer worden gelogd. De encryptor kan processen afsluiten die bestanden in gebruik hebben, en schrijft willekeurige gegevens in tijdelijke bestanden om verwijderde bestanden moeilijker herstelbaar te maken. Daarnaast maakt het gebruik van een aantal anti-analysemethoden, zoals het overschrijven van geheugenbuffers om forensisch onderzoek te bemoeilijken.

De ransomware maakt gebruik van de ChaCha20-encryptie-algoritme met een privé-sleutel die wordt beschermd door RSA-2048. Geëncrypteerde bestanden krijgen een unieke extensie en elke map op het besmette systeem bevat een losgeldbericht met instructies voor de slachtoffers, inclusief een TOX-adres voor communicatie. Het bericht benadrukt dat slachtoffers binnen drie dagen moeten beginnen met onderhandelingen, voordat de aanval openbaar wordt gemaakt via een datalekwebsite op Tor.

Het platform wordt onder de naam "Scattered LAPSUS$ Hunters" gepromoot, wat de samenwerking tussen de ShinyHunters, Lapsus$ en Scattered Spider groepen benadrukt. In tegenstelling tot veel andere ransomware-groepen, claimt ShinyHunters dat bepaalde sectoren, zoals de gezondheidszorg, niet aangevallen zullen worden, hoewel dergelijke beloften in het verleden vaak werden geschonden.

De groep is ook van plan om een geoptimaliseerde "lightning" versie te ontwikkelen, die gericht is op snelheid en eenvoud, en een versnelde versie voor Linux en ESXi te lanceren. De ShinySp1d3r ransomware is nog steeds in de ontwikkelingsfase, maar de gelekte encryptor laat zien dat deze op de korte termijn een serieuze dreiging kan vormen voor organisaties wereldwijd.

WrtHug-campagne kaapt duizenden end-of-life ASUS-routers wereldwijd

De wereldwijde operatie WrtHug heeft duizenden verouderde ASUS WRT-routers gecompromitteerd door zes bekende kwetsbaarheden te exploiteren. De meeste getroffen apparaten bevinden zich in Taiwan, hoewel er ook infecties zijn vastgesteld in Zuidoost-Azië, Rusland, Centraal-Europa en de Verenigde Staten. De aanvallen hebben voornamelijk betrekking op routers die het einde van hun levenscyclus hebben bereikt of die niet meer worden ondersteund door de fabrikant.

De aanvallen maken gebruik van kwetsbaarheden zoals OS-commando-injecties, die door aanvallers worden benut om op afstand toegang te krijgen tot de routers. De kwetsbaarheden zijn onder andere geassocieerd met de AiCloud-service van ASUS, die in veel gevallen wordt misbruikt om een persistentie backdoor te installeren. In de meeste geïnfecteerde routers is een zelfondertekend TLS-certificaat aanwezig, dat in plaats van het standaard certificaat van ASUS is geïnstalleerd. Dit certificaat heeft een ongebruikelijk lange geldigheid van 100 jaar, wat opvalt bij onderzoekers en dient als indicator voor besmetting.

De kwetsbaarheden omvatten onder andere CVE-2023-41345 tot CVE-2023-41348, CVE-2023-39780, CVE-2024-12912 en CVE-2025-2492, waarbij de laatste als de meest kritieke wordt beschouwd vanwege de mogelijkheid om ongeautoriseerde functies uit te voeren. De aanvallers hebben niet geprobeerd om de firmware van de getroffen routers bij te werken, wat betekent dat de apparaten vatbaar blijven voor verdere aanvallen van andere kwaadwillenden. ASUS heeft inmiddels beveiligingsupdates uitgebracht om deze kwetsbaarheden te verhelpen.

Onder de getroffen routermodellen bevinden zich onder andere de ASUS Wireless Router 4G-AC55U en 4G-AC860U, de RT-AC1200HP en de GT-AC5300. Gebruikers van deze apparaten wordt geadviseerd hun firmware bij te werken of, indien hun apparaat niet meer wordt ondersteund, het te vervangen of op zijn minst externe toegang uit te schakelen. Het is bekend dat sommige van de gecompromitteerde routers mogelijk worden gebruikt voor stealth relay nodes in hackoperaties, wat de impact van deze kwetsbaarheden vergroot.

Zero-Day Windows/Office Remote Code Execution Exploit Te Koop Voor $300.000

Op de dark web-markt is een zero-day exploit voor Windows en Office aangemeld, die op afstand code-executie mogelijk maakt. De exploit wordt aangeboden voor een prijs van $300.000. Deze kwetsbaarheid is bijzonder gevaarlijk, omdat het aanvallers

in staat stelt om systemen op afstand te compromitteren zonder dat de gebruiker enige actie hoeft te ondernemen. De prijs voor deze exploit komt voort uit de kracht en het potentieel van de aanval, die kan worden gebruikt om aanzienlijke schade aan te richten in netwerken en systemen.

De zero-day kwetsbaarheid betreft een ongedocumenteerde zwakte in de Windows- en Office-software die kan worden misbruikt voor het uitvoeren van kwaadaardige code zonder dat er een beveiligingspatch beschikbaar is. Aangezien deze kwetsbaarheid nu wordt aangeboden op het dark web, is het waarschijnlijk dat cybercriminelen deze exploit snel zullen gebruiken voor aanvallen, waaronder ransomwarecampagnes en gegevensdiefstal.

De verkoop van zulke exploits benadrukt het groeiende probleem van cybercriminaliteit op het dark web, waar kwetsbaarheden voor aanzienlijke bedragen verhandeld worden. Het verkrijgen van toegang tot deze informatie wordt steeds eenvoudiger, wat de noodzaak voor strengere beveiligingsmaatregelen vergroot. Gezien de potentie van de exploit om grote schade te veroorzaken, is het belangrijk dat gebruikers en organisaties snel reageren en bescherming zoeken tegen dergelijke kwetsbaarheden zodra een patch beschikbaar komt.

Python-gebaseerde WhatsApp-worm verspreidt Eternidade Stealer op apparaten

Cyberbeveiligingsonderzoekers hebben details bekendgemaakt over een nieuwe aanvalscampagne die gebruikmaakt van een combinatie van social engineering en WhatsApp-hijacking om de Delphi-gebaseerde banktrojan Eternidade Stealer te verspreiden. Deze aanvallen richten zich specifiek op gebruikers in Brazilië. De campagne maakt gebruik van de Internet Message Access Protocol (IMAP)-technologie om dynamisch commando- en controle-adressen (C2) op te halen, zodat de aanvallers hun C2-server kunnen bijwerken. Dit stelt hen in staat de aanval continu aan te passen en te verbeteren.

De aanval wordt uitgevoerd via een WhatsApp-wormcampagne, waarbij een Python-script wordt ingezet. Dit is een verschuiving van eerdere aanvallen die gebruikmaakten van PowerShell-scripts. Het Python-script maakt gebruik van WPPConnect, een open-source project, om geautomatiseerd berichten te versturen via gehackte WhatsApp-accounts. Bij deze aanpak wordt het volledige contactlijst van het slachtoffer verzameld, waarbij groepsberichten, zakelijke contacten en uitzendlijsten worden uitgesloten. De verzamelde informatie, inclusief

telefoonnummer en naam van de contacten, wordt naar een server gestuurd die wordt gecontroleerd door de aanvaller. Vervolgens worden kwaadaardige bijlagen naar alle contacten gestuurd via de verstuurde berichten.

Het tweede deel van de aanval wordt uitgevoerd via een MSI-installatiebestand, dat gebruikmaakt van een AutoIt-script om te controleren of het geïnfecteerde systeem zich in Brazilië bevindt. Als het systeem zich niet in Brazilië bevindt, beëindigt de malware zichzelf. Deze hypergeolokaliseerde aanpak toont aan dat de aanvallers zich specifiek richten op Braziliaanse gebruikers.

Wanneer het slachtoffer een gerelateerd bankportaal of een cryptovaluta-wallet opent, wordt de malware geactiveerd en begint het met het stelen van inloggegevens en andere gevoelige informatie. De malware heeft de capaciteit om het systeem te monitoren, toetsaanslagen vast te leggen, schermafbeeldingen te maken en bestanden te stelen. Alle gegevens worden naar de C2-server gestuurd, waar ze door de aanvallers kunnen worden bekeken en geëxploiteerd.

Deze aanvallen maken gebruik van klassieke technieken die worden toegepast door banktrojanen, waarbij schadelijke componenten slechts worden geactiveerd wanneer de gebruiker zich bevindt in een relevante context, zoals het openen van een bank- of crypto-app. Dit maakt de aanval moeilijker te detecteren voor gebruikers of beveiligingssoftware in testomgevingen.

Het gebruik van Python in deze aanval wijst op een trend waarbij cybercriminelen zich steeds meer richten op het automatiseren van hun aanvallen via populaire communicatiemiddelen zoals WhatsApp. De aanvallers blijven de C2-infrastructuur bijwerken, waarbij zij verschillende methoden gebruiken om verbindingen te omzeilen en geofencing-beperkingen te handhaven, zoals blijkt uit de geanalyseerde communicatiegegevens.

TamperedChef-malware verspreidt zich via valse software-installateurs in wereldwijde campagne

De TamperedChef-malware maakt momenteel deel uit van een wereldwijde malvertisingcampagne die gebruikmaakt van vervalste software-installateurs om gebruikers te misleiden en kwaadwillige JavaScript-backdoors te installeren. Deze malware verspreidt zich via nep-installateurs die worden gepromoot via zoekmachineoptimalisatie (SEO) en malvertisingtechnieken, met als doel gebruikers te verleiden tot het downloaden van software die eigenlijk schadelijke code bevat.

De aanvallers benutten legitiem ogende certificaten die afkomstig zijn van bedrijven in de VS, Panama en Maleisië, om hun valse applicaties te ondertekenen. Dit verhoogt de kans dat de software door gebruikers wordt vertrouwd, waardoor de detectie door beveiligingssystemen wordt omzeild. De malware wordt vaak verspreid door middel van advertenties en zoekresultaten die leiden naar geïnfecteerde websites, waar gebruikers worden verleid om de vervalste software te downloaden.

Na installatie van de software wordt een JavaScript-backdoor geactiveerd, die een verbinding maakt met een externe server. Deze server ontvangt verschillende gegevens van het geïnfecteerde systeem, zoals sessie-ID's en machine-ID's, in een versleuteld formaat. Hoewel het exacte doel van de aanvallen onduidelijk blijft, wordt vermoed dat de aanvallers proberen toegang te verkrijgen voor advertentiefraude of gegevensdiefstal. Sectors zoals de gezondheidszorg, de bouw en de productie worden als bijzonder kwetsbaar beschouwd voor deze aanvallen, aangezien ze vaak technische hulpmiddelen gebruiken waarvoor online handleidingen nodig zijn, een gedragslijn die de aanvallers exploiteren.

De campagne blijkt nog steeds actief, en de aanvallers blijven nieuwe technieken ontwikkelen om hun activiteiten voort te zetten. Er zijn meldingen van infecties in landen zoals de VS, Israël, Spanje, Duitsland, India en Ierland, met een aanzienlijke concentratie van gevallen in de gezondheidszorg en de industrie. De continuïteit van de aanval wordt ondersteund door het gebruik van geautomatiseerde en zakelijke infrastructuren die het mogelijk maken snel nieuwe certificaten te verkrijgen en toe te passen.

Nieuwe .NET-malware verbergt Lokibot-malware in PNG/BMP-bestanden om detectie te omzeilen

Een nieuwe vorm van .NET-gebaseerde malware is opgedoken, die gebruik maakt van een geavanceerde methode om de beruchte Lokibot-trojaan te verbergen binnen afbeeldingsbestanden, zoals PNG- en BMP-bestanden. Deze malware maakt gebruik van steganografie, een techniek waarmee verborgen gegevens in ogenschijnlijk onschuldige bestanden worden ingevoegd. Hierdoor wordt het voor beveiligingssoftware veel moeilijker om de bedreiging te detecteren. Het systeem werkt als een loader die het Lokibot-payload uit de afbeeldingbestanden kan extraheren en uitvoeren.

De malware wordt vaak verspreid via phishing-e-mails of via websites die het initiële laadmechanisme hosten. Aangezien antivirussoftware en e-mailgateways vaak afbeeldingsbestanden als veilig beschouwen, worden deze bestanden vaak niet als een bedreiging gezien, wat ze kwetsbaar maakt voor misbruik door aanvallers. Zodra de malware wordt uitgevoerd, haalt deze de verborgen Lokibot-payloads op van externe servers.

De steganografische techniek maakt gebruik van de kleurkanalen van de afbeelding (RGB) om uitvoerbare code te coderen, terwijl de afbeelding zelf ogenschijnlijk ongewijzigd blijft. Dit maakt het lastig voor traditionele detectiemethoden, die normaal gesproken afhankelijk zijn van het identificeren van verdachte bestandskenmerken of gedragsindicatoren. De malware bevat bovendien een eigen decryptieroutine die de Lokibot-payload extra verbergt en de analyse vertraagt, wat het voor onderzoekers nog uitdagender maakt om de dreiging tijdig te ontdekken.

Zodra Lokibot succesvol is geïnstalleerd, fungeert het als een informatie-diefstalprogramma dat gevoelige gegevens steelt, zoals opgeslagen wachtwoorden, browsergeschiedenis en andere authenticatietokens. Dit maakt de malware bijzonder gevaarlijk voor bedrijfsomgevingen, waar werknemers toegang hebben tot meerdere cloudservices.

Deze geavanceerde aanvalsmethode benadrukt de toenemende complexiteit van cyberdreigingen en de voortdurende evolutie van aanvalstechnieken die gericht zijn op het omzeilen van traditionele beveiligingsmaatregelen. De voortdurende ontwikkeling van dergelijke malware vraagt om voortdurende aanpassingen in de detectie- en preventiemethoden van beveiligingssystemen om effectief te kunnen reageren op nieuwe vormen van cyberaanvallen.

Nova Stealer richt zich op macOS-gebruikers door legitieme apps te vervangen om cryptocurrency-portemonnee gegevens te stelen

Een nieuwe malwarecampagne heeft macOS-gebruikers in het vizier, met een specifiek doel: het stelen van gegevens van cryptocurrency-portemonnees. De malware, Nova Stealer genoemd, maakt gebruik van een slimme techniek waarbij legitieme cryptocurrency-applicaties worden vervangen door vervalste versies die bedoeld zijn om herstelzinnen van portemonnees te stelen.

Nova Stealer richt zich op populaire cryptocurrency-portemonnee-applicaties zoals Ledger Live, Trezor Suite en Exodus. Het aanvallende proces begint wanneer een

onbekende dropper een script, genaamd mdriversinstall.sh, downloadt en uitvoert vanaf een command-and-controlserver. Dit script creëert een verborgen directory op het systeem en installeert verschillende componenten, waaronder een scriptmanager en launcher.

Een van de meest opvallende technieken van Nova Stealer is het vervangen van de legitieme applicaties door vervalste versies. Het malwarecomponent mdriversswaps.sh detecteert de aanwezigheid van toepassingen zoals Ledger Live en Trezor Suite op het systeem en verwijdert deze vervolgens. De vervalste applicaties worden gedownload van specifieke domeinen en geïnstalleerd op het systeem. Deze vervangingen gebruiken malafide Swift- en WebKit-code om phishingspagina's weer te geven die de slachtoffers ertoe aanzetten hun herstelzinnen in te voeren.

Wanneer de slachtoffers hun herstelwoorden invoeren, worden de gegevens onmiddellijk naar de command-and-controlserver gestuurd, waarmee de aanvallers de gegevens in realtime kunnen onderscheppen. De malware verzamelt daarnaast andere gevoelige gegevens zoals de configuratiebestanden van de portemonnee en systeeminformatie, die naar de server worden geüpload.

Nova Stealer maakt gebruik van een modulaire opzet, wat betekent dat het malware in verschillende delen kan downloaden om de aanval verder te optimaliseren en het moeilijker te detecteren te maken. Door gebruik te maken van geavanceerde technieken zoals het draaien van scripts in gescheiden schermsessies, blijft de malware vaak onopgemerkt en blijft actief zelfs nadat de gebruiker zich afmeldt.

Deze aanval benadrukt de voortdurende dreiging voor cryptocurrency-gebruikers, vooral op platforms waar de bescherming van herstelzinnen en privésleutels van cruciaal belang is voor de veiligheid van digitale activa.

Destructieve Akira Ransomware-aanval via een enkele klik op CAPTCHA op een kwaadaardige website

Op 19 november 2025 werd een wereldwijde opslag- en infrastructuurorganisatie getroffen door een verwoestende ransomware-aanval, uitgevoerd door de hacker-groep Howling Scorpius. De aanval begon met een ogenschijnlijk eenvoudige actie: een medewerker van het getroffen bedrijf klikte op een zogenaamde CAPTCHA-beveiliging op een geïnfecteerde autodealerwebsite, wat leidde tot een 42 dagen durende inbreuk op de netwerkbeveiliging.

De aanvallers maakten gebruik van de ClickFix-techniek, een geavanceerde vorm van sociale manipulatie waarbij malware zich voordoet als een legitieme beveiligingscontrole. Door deze interactie met de nep-CAPTCHA werd SectopRAT-malware gedownload, een .NET-gebaseerde Remote Access Trojan (RAT) die de aanvallers toegang gaf tot het netwerk van het bedrijf. Eenmaal binnen konden de aanvallers de systemen op afstand besturen, gebruikersactiviteiten volgen, gevoelige gegevens stelen en opdrachten uitvoeren zonder dat dit werd gedetecteerd.

Gedurende de volgende 42 dagen veroverden de aanvallers meerdere bevoorrechte accounts, waaronder die van domeinbeheerders. Ze gebruikten verschillende protocollen zoals Remote Desktop Protocol (RDP), Secure Shell (SSH) en Server Message Block (SMB) om zich door het netwerk te verplaatsen. Het doel was uiteindelijk om Akira-ransomware te installeren, wat resulteerde in een volledige stillegging van de operatie van de organisatie.

De aanvallers verwijderden ook de back-upopslag en exfiltreerden bijna een terabyte aan gegevens. Nadat de ransomware was verspreid, eisten ze een losgeldbetaling, terwijl de aanval de kwetsbaarheden in de netwerkbeveiliging blootlegde. Ondanks het gebruik van twee endpoint detection en response (EDR)-oplossingen, werd de aanval gemist door de beveiligingssoftware, aangezien er onvoldoende waarschuwingen werden gegenereerd. Dit incident benadrukt de groeiende dreiging van sociaal gemanipuleerde aanvallen en de noodzaak van beter afgestelde monitoringtools voor het detecteren van geavanceerde aanvallen.

De beveiligingsspecialisten van Palo Alto Networks, die de aanval onderzochten, slaagden erin de aanvalspaden te reconstrueren en het losgeldbedrag met ongeveer 68% te verminderen. Dit voorval toont aan hoe zelfs geavanceerde bedrijfssystemen kwetsbaar kunnen zijn voor de meest eenvoudige aanvallen, zoals een enkele klik op een nepbeveiliging.

'The Gentlemen' ransomwaregroep met dual-extortionstrategie versleutelt en exfiltreert gegevens

Een nieuwe ransomwaredreiging genaamd "The Gentlemen" heeft zich sinds juli 2025 gepresenteerd en heeft zich snel als een ernstige bedreiging gepositioneerd. Tussen september en oktober 2025 heeft de groep 48 slachtoffers gepubliceerd op hun dark web-lekwebsite. De ransomware werkt als een Ransomware-as-a-Service (RaaS) platform, wat betekent dat geaffilieerde hackers aanvallen kunnen uitvoeren,

terwijl de kernoperators de controle behouden over de infrastructuur en de onderhandelingen.

"The Gentlemen" maakt gebruik van een dual-extortionstrategie, waarbij naast het versleutelen van bestanden, gestolen gegevens ook worden geëxfiltreerd. Dit creëert extra druk op de slachtoffers, die niet alleen worden geconfronteerd met vergrendelde systemen, maar ook met de dreiging dat gestolen informatie openbaar wordt gemaakt op dark web-lekwebsites, tenzij het losgeld wordt betaald.

De ransomware richt zich op Windows-, Linux- en ESXi-platforms en maakt gebruik van geavanceerde encryptie-algoritmes, zoals XChaCha20 en Curve25519, om bestanden te beveiligen, waardoor het herstellen zonder de decryptiesleutel uiterst moeilijk is. Recente updates van de malware bevatten functionaliteiten zoals automatische herstart en het uitvoeren bij het opstarten van het systeem, wat de persistentie op geïnfecteerde systemen verhoogt.

Wat betreft verspreiding gebruikt de ransomware technieken zoals Windows Management Instrumentation (WMI) en PowerShell-remoting om zich over netwerken te verspreiden. Zodra de malware wordt uitgevoerd, heeft het een wachtwoordargument nodig om de encryptieroutine te starten. Daarnaast ondersteunt de malware verschillende operationele modi, waaronder systeemversleuteling onder SYSTEM-rechten en versleuteling van netwerkshares via gemapte schijven en UNC-paden. De ransomware schakelt Windows Defender uit door PowerShell-opdrachten uit te voeren die de realtime bescherming uitschakelen en mappen en processen aan de uitsluitingslijsten toevoegen.

De groep richt zich ook op kritieke services en processen, zoals database-engines (bijvoorbeeld MSSQL en MySQL), back-upsoftware (zoals Veeam) en virtualisatieservices (zoals VMware). Om detectie te vermijden en forensisch onderzoek te bemoeilijken, verwijdert de malware Windows-eventlogs, RDP-verbindinglogs, ondersteuningsbestanden van Windows Defender en Prefetch-gegevens.

Deze anti-forensische benadering bemoeilijkt aanzienlijk de inspanningen van beveiligingsteams om de aanval te onderzoeken en een tijdslijn op te stellen.

Europol onderzoekt 47 miljoen euro in cryptocurrency om digitale piraterij te bestrijden

Van 10 tot 14 november 2025 organiseerde Europol, in samenwerking met het Europese Bureau voor Intellectuele Eigendom (EUIPO) en de Spaanse Nationale Politie, een "Cyber-Patrol Week" gericht op het bestrijden van digitale piraterij. Gedurende deze week werden 30 onderzoekers ingezet, die geavanceerde Open-Source Intelligence (OSINT) technieken en online onderzoeksinstrumenten gebruikten om intellectuele eigendomsdelicten te identificeren. Dit resulteerde in de opsporing van 69 illegale websites, waarvan 25 dienstverleners voor illegale IPTV-diensten werden doorverwezen naar crypto-exchanges voor verdere verstoring.

De gecombineerde jaarlijkse bezoekersaantallen van de 69 doelwitten worden geschat op ongeveer 11,8 miljoen. Onderzoekers traceerden cryptocurrency ter waarde van zo'n 55 miljoen dollar (meer dan 47 miljoen euro) naar verschillende accounts die aan deze diensten gekoppeld waren. Het gebruik van cryptocurrency door criminelen groeit, omdat ze geloven dat dit hen meer anonimiteit biedt bij het aanbieden van illegale diensten. Europol reageerde hierop door cryptocurrencies in te zetten om deze diensten te kopen, wat hen in staat stelde om de criminelen te identificeren en hun inkomstenstroom te verstoren.

De operatie benadrukt de verschuiving van traditionele betaalmethoden naar cryptocurrency, wat nieuwe uitdagingen creëert voor wetshandhavers. De Cyber-Patrol Week toonde de effectiviteit van grensoverschrijdende samenwerking en technologische innovatie bij het bestrijden van intellectuele eigendomscriminaliteit. Meer dan 15 landen en verschillende private organisaties werkten samen, wat resulteerde in waardevolle inlichtingen en de versterking van de samenwerking in de strijd tegen digitale piraterij.

Openbaar Ministerie eist taakstraf voor ddos-aanval op werkgever

Het Openbaar Ministerie heeft tegen een 25-jarige man een taakstraf van 160 uur geëist vanwege het uitvoeren van ddos-aanvallen op de websites van twee bedrijven, waar hij op het moment van de aanvallen werkzaam was. De verdachte voerde de aanvallen uit eind 2023 en begin 2024, net nadat hij bij een callcenter in Sittard in dienst was getreden. De advocaat van de man stelde dat hij de aanvallen had uitgevoerd om zijn collega’s een dag vrij te geven en beschouwde het als “kattenkwaad”. De verdachte bekende de feiten tijdens zijn verhoor. De schade die de ddos-aanvallen bij beide bedrijven hebben veroorzaakt, wordt geschat op 178.000 euro. De rechter zal over twee weken uitspraak doen over de zaak.

Californische man bekent schuld in grootschalige cryptocurrency-witwasoperatie

Een 45-jarige man uit Irvine, Californië, heeft zich schuldig verklaard aan het witwassen van 25 miljoen dollar van een gestolen cryptocurrency-bedrag van 230 miljoen dollar. De man, Kunal Mehta, was betrokken bij een crimineel netwerk dat tussen oktober 2023 en maart 2025 via social engineering toegang verkreeg tot de cryptocurrency-accounts van slachtoffers en de gestolen fondsen overboekte naar wallets onder hun controle.

Mehta fungeerde als witwasser en gebruikte verschillende technieken, waaronder crypto mixers en virtuele privé netwerken (VPN's), om de identiteit van de betrokkenen te verbergen en de herkomst van de fondsen te camoufleren. Deze aanval is een voorbeeld van de kwetsbaarheden in het cryptocurrency-ecosysteem, waarin slecht beveiligde accounts en onvoldoende monitoring van activiteiten kunnen leiden tot grootschalige diefstallen.

Het onderzoek toont aan hoe cybercriminelen steeds geavanceerdere technieken gebruiken om cryptocurrency te stelen en wit te wassen. Dit benadrukt het belang van robuuste beveiligingsmaatregelen en verhoogde waakzaamheid bij zowel gebruikers als aanbieders van cryptoservices.

VS, VK en Australië leggen sancties op aan Russische bulletproof hostingproviders vanwege ransomwarebanden

Op 19 november 2025 kondigden de Verenigde Staten, het Verenigd Koninkrijk en Australië gezamenlijke sancties aan tegen Russische bulletproof hosting (BPH)-providers die cybercriminelen ondersteunen, waaronder ransomwaregroepen. Deze aanbieders leveren servers aan cybercriminelen om hun kwaadaardige activiteiten te verbergen voor wetshandhavers, zoals phishingaanvallen, malwaredistributie, command-and-control-servers en het hosten van illegale inhoud. Ze worden 'bulletproof' genoemd omdat ze weigeren klachten van slachtoffers of verzoeken van de politie om schadelijke inhoud te verwijderen te honoreren.

De Amerikaanse overheid heeft Media Land, een Russische BPH-provider, op de sanctielijst geplaatst. Media Land heeft diensten geleverd aan verschillende cybercriminelen en ransomwaregroepen zoals LockBit, BlackSuit en Play, evenals aan drie zusterbedrijven: Media Land Technology, Data Center Kirishi en ML Cloud.

Volgens Amerikaanse autoriteiten werd de infrastructuur van Media Land ook gebruikt voor DDoS-aanvallen tegen Amerikaanse bedrijven en kritieke infrastructuur, waaronder telecommunicatienetwerken.

De sancties richten zich ook op drie leidinggevenden van Media Land: Aleksandr Volosovik, Kirill Zatolokin en Yulia Pankova. Volosovik wordt beschuldigd van betrokkenheid bij meerdere beruchte cybercriminele groepen, waaronder Evil Corp, Black Basta en LockBit. Daarnaast werden Aeza Group LLC en Hypercore Ltd. gesanctioneerd, die ook betrokken waren bij het leveren van infrastructuur voor ransomware-operaties.

In reactie op de sancties hebben de Five Eyes cybersecurity-agentschappen gezamenlijke richtlijnen gepubliceerd voor internetserviceproviders (ISP's) en netwerkbeveiligers om cybercriminele activiteiten te mitigeren die gebruikmaken van BPH-infrastructuur. De richtlijnen omvatten het identificeren van kwaadaardige internetbronnen via dreigingsinformatie, het uitvoeren van regelmatige verkeersanalyses en het implementeren van filters op netwerkgrenzen.

De sancties bevriezen de bezittingen van de gesanctioneerde entiteiten en individuen in de VS, het VK en Australië. Dit maakt het moeilijker voor andere entiteiten en personen om zaken te doen met deze BPH-providers, aangezien ze ook blootgesteld kunnen worden aan secundaire sancties.

Internationale samenwerking leidt tot arrestaties in mensenhandeloperatie

Op 18 november 2025 werd een grootschalige operatie uitgevoerd tegen een crimineel netwerk dat verantwoordelijk was voor het verhandelen en uitbuiten van meer dan 30 Roemeense vrouwen in Italië. Het netwerk wordt verdacht van een opbrengst van meer dan 1,7 miljoen euro door de slachtoffers te dwingen tot prostitutie. De gezamenlijke operatie, gecoördineerd door Eurojust, bracht 19 verdachten in hechtenis en leidde tot het doorzoeken van 25 locaties in zowel Italië als Roemenië, waar onder andere luxe voertuigen, wapens en contant geld in beslag werden genomen.

Het netwerk vertoonde kenmerken van een gestructureerde piramideorganisatie, waarbij de leiders de financiële en logistieke operaties coördineerden, terwijl familieleden verantwoordelijk waren voor het rekruteren en controleren van de slachtoffers. De slachtoffers werden verleid met de zogenoemde ‘lover boy’-methode,

waarbij de daders zich voordeden als beschermers, en werden overtuigd dat prostitutie een noodzakelijke bijdrage was aan het financieel welzijn van de groep.

Een belangrijk aspect van de operatie was de ontdekking van witwaspraktijken waarbij de criminele opbrengsten werden geïnvesteerd in onroerend goed, luxe voertuigen en sieraden. De succesvolle actie benadrukt de rol van internationale samenwerking bij het bestrijden van mensenhandel en het beschermen van slachtoffers, met een nadruk op de digitale infrastructuren die door criminele netwerken worden gebruikt voor dergelijke operaties.

Grensoperatie in West-Afrika pakt buitenlandse terroristen en georganiseerde misdaad aan

Een door INTERPOL gecoördineerde operatie in West-Afrika heeft geleid tot de arrestatie van 62 verdachten en de inbeslagnames van wapens, explosieven, drugs en vervalste producten. De operatie, genaamd "Operation Screen West Africa 2025", werd uitgevoerd tussen juli en oktober 2025 en bracht wetshandhavingsinstanties uit 12 West-Afrikaanse landen samen. Het doel was de grensbeveiliging te versterken en criminele netwerken die betrokken zijn bij terrorisme en georganiseerde misdaad te verstoren.

Tijdens de operatie werden 1,7 miljoen controles uitgevoerd met behulp van mobiele technologie en de uitgebreide databases van INTERPOL. Dit leidde tot de arrestatie van negen verdachten die in verband worden gebracht met terrorisme, waaronder personen die gelinkt zijn aan de Al-Qaeda-gerelateerde groep JNIM, verantwoordelijk voor aanvallen in Ivoorkust in 2020. Daarnaast werden er 21 slachtoffers van mensenhandel bevrijd.

De operatie bracht ook ernstige misdaadactiviteiten aan het licht, zoals het smokkelen van vervalste medicijnen, cannabis en gestolen voertuigen. Deze inbeslagnames kunnen wijzen op de financiering van terroristische activiteiten en de ondermijning van nationale economieën via illegale handel en fraude. De controles op schepen, die betrokken waren bij zogenaamde "dark operations" en identiteitsmanipulatie, tonen aan hoe criminele netwerken zich wereldwijd proberen te verbergen.

Deze operatie benadrukt de wereldwijde samenwerking tussen landen in de strijd tegen terrorisme en georganiseerde misdaad. De inbeslagnames en arrestaties zijn belangrijke stappen in het verstoren van criminele netwerken die wereldwijd actief

zijn en mogelijk betrokken zijn bij cybercriminaliteit en andere vormen van digitale misdaad.

UK onthult bulletproof hostingoperator gelinkt aan LockBit en Evil Corp

De Britse National Crime Agency (NCA) heeft onlangs de Russische operator Alexander Volosovik geïdentificeerd, ook bekend onder de online namen "Yalishanda", "Downlow" en "Stas_vl". Volosovik heeft jarenlang een bulletproof hostingbedrijf geëxploiteerd, dat werd gebruikt door verschillende vooraanstaande ransomwaregroepen, waaronder LockBit, Evil Corp en BlackBasta. Deze hostingdiensten boden cybercriminelen de infrastructuur die nodig was om grootschalige cyberaanvallen uit te voeren, waarbij de aanvallers hun sporen wisten te verbergen en hun activiteiten moeilijk traceerbaar maakten.

De operatie, die ook samenwerkte met internationale wetshandhavers, heeft geleid tot sancties tegen Volosovik en drie van zijn medewerkers. Dit besluit werd gecoördineerd met maatregelen van de Amerikaanse Treasury's Office of Foreign Assets Control (OFAC) en het Australische ministerie van Buitenlandse Zaken. De NCA benadrukt dat diensten zoals die van Volosovik essentieel zijn voor het voortbestaan van ransomware- en andere cybercriminaliteitsoperaties, aangezien ze de digitale "schilden" bieden die de criminelen beschermen tegen wetshandhaving.

De bulletproof hostingdiensten die Volosovik beheerste, waren bekend om hun vermogen om inhoud te beschermen tegen verwijdering door autoriteiten. Ze werden vaak ingezet voor illegale activiteiten, variërend van phishing tot de handel in gestolen gegevens. In een bekend geval heeft zijn infrastructuur ervoor gezorgd dat het omstreden 8chan-forum weer online kwam, ondanks dat het eerder was gedeplatformd.

In een afzonderlijke actie in Nederland heeft de politie 250 servers in beslag genomen die werden gebruikt door een onbekende bulletproof hostingprovider. Deze dienst had sinds 2022 gewerkt en was verbonden aan meer dan 80 cybercriminaliteitsonderzoeken. Deze inbeslagname biedt wetshandhavers een zeldzame kans om meer inzicht te krijgen in de achterliggende infrastructuur van grootschalige cyberaanvallen.

De recente sancties tegen Volosovik maken deel uit van een bredere strategie van de NCA en haar internationale partners om de ondersteuning van cybercriminaliteit te verstoren. De samenwerking tussen landen als het Verenigd Koninkrijk, de VS,

Australië, Canada en Nieuw-Zeeland speelt een cruciale rol in het aanpakken van de fundamentele diensten die cybercriminelen mogelijk maken.

Nederland onthoudt zich van stemming over aangepast voorstel chatcontrole

Nederland heeft besloten zich te onthouden van stemming over een aangepast Europees voorstel voor permanente vrijwillige detectie van online content door techbedrijven en verplichte leeftijdsverificatie voor appstores en chatdiensten. Het voorstel is bedoeld om de bestrijding van misbruikmateriaal en grooming te versterken. Het werd voorgesteld door de Europese Commissie, maar de lidstaten zijn verdeeld over de uitvoering van dit plan, waardoor onderhandelingen nog niet van de grond zijn gekomen.

Het oorspronkelijke voorstel, dat chatdiensten verplichtte om de inhoud van berichten te controleren, stuitte op veel kritiek. Het ondermijnen van end-to-end encryptie werd gezien als een bedreiging voor de privacy en burgerrechten van gebruikers. Hierdoor werd het voorstel tijdelijk uitgesteld door Denemarken, de voorzitter van de EU.

In de nieuwe versie van het voorstel is het verplicht stellen van detectie van berichten door chatdiensten verwijderd, maar wordt voorgesteld om de tijdelijke regeling voor vrijwillige detectie permanent te maken. Diensten moeten ook risicobeperkingen implementeren en verplicht materiaal melden dat mogelijk verband houdt met kindermisbruik. Bovendien wordt de leeftijdsverificatie voor bepaalde risicodiensten verplicht gesteld.

Minister Van Oosten van Justitie en Veiligheid benadrukt dat, hoewel Nederland enige vooruitgang heeft gezien in de verwijdering van verplichte detectie, er nog steeds grote zorgen zijn over de balans tussen privacy en de doelstellingen van het voorstel. Deze zorgen zijn de reden waarom Nederland zich op 26 november van stemming zal onthouden.

Valentín López blijft actief ondanks fraudezaak met kankerpatient

Valentín López, die eerder in het nieuws kwam wegens het oplichten van een terminale kankerpatient, lijkt zich niets van zijn misdaden aan te trekken. De man werd bekend doordat hij geld had gestolen van een crowdfundingcampagne die bedoeld was voor de medische behandeling van een terminale patiënt. In plaats van het geld voor de behandeling te gebruiken, bleek hij de donaties te hebben geïnd en

het geld te hebben verduisterd. Nadat zijn bedrog aan het licht kwam, verdwenen zijn sociale media-accounts tijdelijk. Onlangs is hij echter weer actief op sociale media, wat vragen oproept over de juridische gevolgen van zijn gedrag.

De heropleving van zijn aanwezigheid op sociale media heeft veel verontwaardiging veroorzaakt bij degenen die zich door hem bedrogen voelden. Vragen over de strafrechtelijke vervolging van López blijven bestaan, vooral omdat er steeds minder transparantie lijkt te zijn over de afhandeling van dergelijke gevallen van online fraude. López heeft zich tot op heden niet schuldig verklaard, wat de verontwaardiging vergroot.

In verband met zijn zaak is ook een malware-aanval die de $32.000 van de donaties voor de kankerbehandeling heeft gestolen, verder onderzocht. De criminelen maakten gebruik van malware die zich verspreidde via een online game en gegevens van ongeveer 970 slachtoffers verzamelde, waaronder inloggegevens voor browsers en cryptocurrency-portemonnees. De malware werd teruggevoerd naar een schadelijk .bat-bestand.

Beveiligingsgroep vx-underground speelde een cruciale rol in het ontmantelen van deze aanval door de malware te reverse-engineeren, waardoor de volledige infrastructuur van de cybercriminelen werd blootgelegd. De aanvallers bleken hun buit openlijk te vieren. Dit incident heeft ernstige bezorgdheid veroorzaakt over de kwetsbaarheid van online platformen, vooral games die mogelijk als distributiemiddel voor malware kunnen dienen. De aanval heeft niet alleen financieel schade aangericht, maar ook het vertrouwen van de slachtoffers beschadigd.

Meta wint rechtszaak tegen Amerikaanse toezichthouder: Impact op digitale veiligheid

Meta heeft een rechtszaak gewonnen tegen de Amerikaanse Federal Trade Commission (FTC), die beschuldigde dat het bedrijf zijn machtspositie had misbruikt bij de overname van Instagram en WhatsApp. De FTC stelde dat Meta deze platforms had overgenomen om de concurrentie te elimineren, wat mogelijk schadelijk is voor de digitale veiligheid en privacy van gebruikers. Deze zaak heeft gevolgen voor de manier waarop grote techbedrijven opereren op het gebied van gegevensbeveiliging en het beheer van sociale netwerken.

De uitspraak benadrukt de macht van bedrijven als Meta en de vraag hoe hun invloed de online beveiliging van gebruikers kan beïnvloeden. Hoewel de rechter

oordeelde dat Meta zijn overnames niet als een monopolie heeft gebruikt, blijven er zorgen over de controle die dergelijke bedrijven uitoefenen over persoonlijke gegevens en digitale markten. Dit kan belangrijke implicaties hebben voor de toekomstige regelgeving rond digitale veiligheid en privacy.

Privacy First bezorgd over digitale euro: risico's voor privacy en veiligheid

De stichting Privacy First uit grote bezorgdheid over de uitrol van de digitale euro en waarschuwt voor de risico's die dit nieuwe systeem met zich meebrengt voor de privacy van burgers en de veiligheid van financiële gegevens. Privacy First stelt dat er tot nu toe onvoldoende politieke discussie is gevoerd over de gevolgen van de digitale euro, zowel binnen Nederland als op Europees niveau.

De organisatie wijst erop dat de invoering van de digitale euro zou kunnen leiden tot een centraal systeem waarin de Europese Centrale Bank (ECB) volledige controle heeft over de financiële gegevens van burgers, wat de weg zou kunnen openen voor meer cyberaanvallen en misbruik van data. De mogelijkheid van een database waarin alle betalingen geregistreerd worden, vergroot het risico op datalekken en hacking, en zou bovendien het gebruik van 'programmeergeld' kunnen betekenen, waarbij burgers alleen bepaalde vormen van betalingen kunnen doen. Dit brengt niet alleen zorgen over privacy met zich mee, maar ook over de veerkracht en veiligheid van het systeem tegen cyberaanvallen.

Daarnaast wijst Privacy First op de dreiging van de uitfasering van contant geld, wat de anonimiteit van financiële transacties verder zou kunnen beperken en tegelijkertijd kwetsbaar maakt voor digitale criminaliteit. Er bestaat ook de mogelijkheid dat de digitale euro zal worden gekoppeld aan een Europese digitale identiteit, wat de toegang tot het systeem nog verder zou centraliseren en potentieel extra risico's voor identiteitsdiefstal en cybercrime met zich meebrengt.

Privacy First roept op tot een diepgaand debat over de invoering van de digitale euro en benadrukt dat het essentieel is om de veiligheid van persoonlijke gegevens en de bescherming tegen digitale misbruik te waarborgen. Het is van cruciaal belang dat er bredere discussies plaatsvinden, zodat de uitrol van dit systeem niet leidt tot onbedoelde gevolgen voor de privacy en veiligheid van Europese burgers.

Brussel presenteert plan voor aanpassen AVG en digitale identiteit voor bedrijven

De Europese Commissie heeft een nieuw voorstel gepresenteerd om de Algemene Verordening Gegevensbescherming (AVG) en de digitale identiteit van bedrijven aan te passen. Deze wijzigingen zijn bedoeld om bedrijven in de EU beter in staat te stellen te opereren in de digitale economie, maar hebben ook gevolgen voor de bescherming van persoonsgegevens en de meldingsplicht bij datalekken.

Een belangrijk onderdeel van het plan is de wijziging van de AVG, waarbij de definitie van persoonlijke gegevens wordt aangepast. Hierdoor zouden datasets met persoonlijke data makkelijker gedeeld kunnen worden, mits de ontvanger deze niet kan gebruiken om individuen te identificeren. Deze verandering kan gevolgen hebben voor de mate waarin data wordt gedeeld met derde partijen, wat het risico op datalekken kan vergroten als de beveiliging niet op orde is.

De Europese Commissie introduceert tevens een centraal meldpunt voor datalekken en beveiligingsincidenten, beheerd door het Europese cyberagentschap ENISA. Dit meldpunt moet het makkelijker maken voor organisaties om datalekken en incidenten snel te melden, wat van cruciaal belang is voor de preventie en respons op cyberaanvallen.

Naast de aanpassingen aan de AVG, wordt er gewerkt aan de oprichting van een "business wallet" voor bedrijven. Deze digitale identiteit moet bedrijven helpen sneller en efficiënter zaken te doen met publieke instanties, maar ook zorgen voor een centrale toegangspoort tot essentiële bedrijfsinformatie. Hoewel bedrijven niet verplicht worden deze wallet te gebruiken, zal de publieke sector verplicht zijn om de belangrijkste functies van de wallet te accepteren. Dit kan het risico op phishing en andere cyberdreigingen verminderen door de integriteit van bedrijfsidentiteiten te waarborgen.

Met de lancering van deze maatregelen wil de Europese Commissie de digitale economie versterken, maar ook zorgen voor betere bescherming van persoonsgegevens en strengere regels voor databeveiliging binnen de EU. De voorstellen zijn nog in ontwikkeling en worden besproken met de lidstaten en het Europees Parlement. De implementatie van de veranderingen zal de komende jaren plaatsvinden en kan grote invloed hebben op hoe bedrijven omgaan met de bescherming van data en de meldingsplicht bij beveiligingsincidenten.

Autoriteit Persoonsgegevens pleit voor wettelijk kader bij OSINT-onderzoeken door overheid

De Autoriteit Persoonsgegevens (AP) heeft gesteld dat er een juridisch kader moet komen voor het verzamelen van gegevens door de overheid via open-source intelligence (OSINT). Het betreft informatie die wordt verzameld uit openbare bronnen op het internet, zoals sociale media, fora en registers, maar mogelijk ook van het darkweb. De AP benadrukt dat dit onderzoek niet gericht is op het opsporen van strafbare feiten, maar op het verzamelen van gegevens over burgers zonder verdenking.

De overheid wil hierbij gebruik maken van kunstmatige intelligentie, softwaretools en nepaccounts om informatie te vergaren. Dit roept zorgen op over de privacy van burgers, aangezien de overheid op deze manier gedetailleerde profielen van mensen zou kunnen opbouwen zonder wettelijke waarborgen. De AP pleit daarom voor een duidelijk juridisch kader, waarin precies wordt vastgelegd wanneer de overheid deze methoden mag inzetten en onder welke voorwaarden. Zo moet er altijd een gerechtvaardigde aanleiding zijn voor elk onderzoek om de privacyrechten van burgers te beschermen.

Noyb waarschuwt voor risico’s digitale omnibus voor de AVG

De recente voorstellen van de Europese Commissie voor de digitale omnibus roepen zorgen op bij privacyorganisatie Noyb. Volgens Noyb zouden de voorgestelde veranderingen de kernprincipes van de Algemene Verordening Gegevensbescherming (AVG) ondermijnen. Max Schrems, oprichter van Noyb, beschrijft het als de grootste dreiging voor digitale rechten in de EU in de afgelopen jaren.

Een belangrijk aspect van de voorstellen is de herziening van de definitie van persoonlijke gegevens. Dit zou bijvoorbeeld betekenen dat gegevens zoals pseudoniemen of willekeurige identificatienummers, die nu onder de AVG vallen, niet langer als persoonlijk beschouwd zouden worden. Dit zou een aanzienlijke impact hebben op sectoren zoals de datahandel en de advertentie-industrie, die vaak gebruikmaken van dergelijke gegevens.

Noyb benadrukt dat de wijzigingen vooral grote technologiebedrijven ten goede zouden komen, terwijl ze de bescherming van persoonsgegevens in veel gevallen zouden verzwakken. Dit zou de wetgeving niet alleen complexer maken, maar ook juridische mazen introduceren die vooral grote bedrijven in staat stellen om de wet te omzeilen. Noyb roept de Europese Commissie op om een strategisch

langetermijnplan te ontwikkelen voor de digitale toekomst van Europa, waarbij de bescherming van persoonsgegevens centraal blijft staan.

NCSC en FBI adviseren ISP's maatregelen tegen bulletproof hosters

Het Nationaal Cyber Security Centrum (NCSC) heeft samen met de FBI, de NSA en andere internationale cyberagentschappen internetproviders opgeroepen om maatregelen te nemen tegen bulletproof hosters. Deze hosters bieden hun diensten aan cybercriminelen en zorgen ervoor dat hun activiteiten moeilijk te traceren zijn. Dit kan variëren van het hosten van illegale inhoud tot het aanbieden van platformen voor cyberaanvallen.

In een recent adviesdocument, getiteld "Bulletproof Defense: Mitigating Risks From Bulletproof Hosting Providers", worden ISP's aangemoedigd om onder andere "know your customer"-protocollen te implementeren. Deze protocollen vereisen dat klanten een verificatiecode naar de internetprovider sturen, zodat de legitimiteit van de klant kan worden geverifieerd. De documentatie vermeldt ook het filteren van IP-ranges die vaak door deze bulletproof hosters worden gebruikt.

Deze maatregelen zijn bedoeld om de verspreiding van cybercriminaliteit via illegale hostingdiensten tegen te gaan, maar het advies benadrukt ook dat de impact op legitieme infrastructuur zorgvuldig moet worden afgewogen. Eerder werd in Nederland een belangrijke actie tegen bulletproof hosting uitgevoerd door de politie, waarbij 250 fysieke servers in beslag werden genomen in een onderzoek naar een malafide hostingbedrijf.

Europese Commissie wil einde maken aan "stortvloed" van cookie-meldingen

De Europese Commissie heeft een hervormingspakket gepresenteerd dat gericht is op het verminderen van het aantal cookie-meldingen dat internetgebruikers dagelijks tegenkomen. Sinds de invoering van de Algemene Verordening Gegevensbescherming (GDPR) in 2018 is het voor websites verplicht om toestemming te vragen voor het gebruik van cookies, wat vaak leidt tot frustratie bij gebruikers door de vele meldingen.

Met het nieuwe voorstel wil de Commissie de regels vereenvoudigen door de manier waarop toestemming wordt gevraagd om te draaien. Gebruikers zullen hun cookievoorkeuren voortaan in de browser kunnen instellen, waardoor websites deze

automatisch respecteren bij latere bezoeken. Dit zou de gebruikservaring verbeteren en de administratieve belasting voor bedrijven verminderen.

Deze verandering heeft echter belangrijke implicaties voor privacy en cybersecurity. Privacyorganisaties uiten hun bezorgdheid over de mogelijke versoepeling van de definitie van ‘persoonsgegevens’, zoals IP-adressen en gebruikers-ID's. Dit kan de controle van burgers over hun gegevens verminderen en bedrijven, met name AI-ontwikkelaars, meer ruimte geven om persoonlijke gegevens te gebruiken zonder expliciete toestemming.

Daarnaast bevat het hervormingspakket voorstellen die gericht zijn op het vereenvoudigen van de regels rond kunstmatige intelligentie (AI). Dit zou bedrijven in staat stellen sneller en efficiënter gebruik te maken van data voor AI-ontwikkeling, maar roept vragen op over de bescherming van persoonsgegevens en het risico van datamisbruik.

Deze hervormingen komen op een moment waarin er wereldwijd steeds meer nadruk ligt op het waarborgen van digitale veiligheid en de bescherming van persoonlijke gegevens. De veranderingen zouden kunnen leiden tot meer transparantie en controle voor gebruikers, maar brengen ook nieuwe uitdagingen met zich mee voor bedrijven die zich aan de privacywetgeving moeten blijven houden.

Kolonel De Gruijter vertrekt naar Defensie Cyber Commando: focus op digitale verdediging

Kolonel Jorrit de Gruijter, die meer dan vijf jaar lang de leiding had over Vliegbasis Eindhoven, maakt de overstap naar het Defensie Cyber Commando. Deze verandering komt op een moment dat de nadruk op cyberveiligheid binnen de krijgsmacht steeds belangrijker wordt. De Gruijter’s ervaring wordt nu ingezet om de digitale slagkracht van de Nederlandse defensie te versterken. Dit onderstreept de groeiende rol van cyberbeveiliging in militaire operaties, waarmee de defensie inspanningen zich niet alleen op fysieke dreigingen richten, maar ook op digitale aanvallen die steeds vaker voorkomen in moderne conflicten.

Zijn vertrek van Vliegbasis Eindhoven markeert een belangrijke verschuiving in de focus van de krijgsmacht naar cyberstrategieën, en benadrukt het belang van digitale verdediging in een tijd van toenemende cyberdreigingen. Het is een ontwikkeling die niet alleen relevant is voor de militaire sector, maar ook voor bredere cyberbeveiligingsinitiatieven in Nederland en wereldwijd.

Gen-Z gebruikt nog slechtere wachtwoorden dan 80-plussers

Jongeren uit generatie Z blijken op het gebied van wachtwoordbeveiliging slechter te presteren dan 80-plussers, zo blijkt uit onderzoek van Nordpass, een populaire wachtwoordmanager. De onderzoekers analyseerden de meest gebruikte wachtwoorden per generatie en kwamen tot verontrustende conclusies. De wachtwoorden die Gen-Z kiest, zijn vaak nog eenvoudiger en kwetsbaarder dan die van oudere generaties. De meest gebruikte wachtwoorden in deze groep zijn simpel en makkelijk te raden, zoals '12345', '123456' en 'password'. Deze patronen komen overeen met die van oudere generaties, maar opvallend is dat Gen-Z hier nog verder in doorgaat met variaties als '12345678' en '123456789'.

In vergelijking met de 80-plussers, die op plaats drie van de lijst namen als 'Susana' en 'Marta' gebruiken, vertonen de jongvolwassenen nauwelijks enige variatie. De enige uitzondering is het wachtwoord 'skibidi', dat op plaats zeven staat, maar dit biedt nog steeds onvoldoende beveiliging. De onderzoekers wijzen erop dat, hoewel deze slechte wachtwoordkeuzes op individueel niveau ernstige gevolgen kunnen hebben, de grotere dreiging ligt bij bedrijfsomgevingen, waar het gebruik van zwakke wachtwoorden zoals 'admin' vaak voorkomt. Dit wachtwoord staat wereldwijd op de tweede plaats van meest gekozen wachtwoorden, en in Nederland zelfs op de eerste plaats.

De onderzoekers stellen vast dat veel mensen kiezen voor gemak in plaats van veiligheid, wat hen kwetsbaar maakt voor cyberaanvallen. Ze raden gebruikers aan om unieke wachtwoorden te kiezen, bijvoorbeeld door een zin te gebruiken in plaats van een simpel wachtwoord. Ook wordt het gebruik van tweestapsverificatie en een wachtwoordmanager sterk aangeraden.

Cloudflare-uitval biedt inzicht in beveiligingslekken

Op 18 november 2025 werd Cloudflare, een van de grootste cloud-diensten voor webbeveiliging, getroffen door een tijdelijke uitval die veel populaire websites offline bracht. De uitval werd veroorzaakt door een interne fout in de databasebeheersystemen van Cloudflare, wat leidde tot een foutieve configuratie van de beveiligingsbestanden. Dit resulteerde in meerdere uren van onbetrouwbare service, waarbij veel klanten niet in staat waren om snel over te schakelen naar alternatieve diensten, doordat ook hun DNS-diensten bij Cloudflare lagen.

Tijdens de uitval ontdekten sommige klanten dat het mogelijk was om hun domeinen tijdelijk van Cloudflare af te halen om de beschikbaarheid van hun sites te garanderen. Dit bood echter ook een ongeplande kans voor cybercriminelen, die mogelijk de kwetsbaarheid van de websites zonder Cloudflare-beveiliging hebben benut. Beveiligingsexperts wijzen erop dat deze uitval bedrijven een belangrijke gelegenheid bood om inzicht te krijgen in hoe hun beveiliging het zou doen zonder de beschermende lagen van Cloudflare, zoals de Web Application Firewall (WAF) en botbescherming.

Deskundigen, waaronder Aaron Turner van IANS Research, benadrukken dat veel bedrijven in het verleden hebben vertrouwd op Cloudflare om aanvallen zoals SQL-injecties en credential stuffing te blokkeren. De tijdelijke onderbreking bracht aan het licht dat sommige bedrijven mogelijk geen robuuste interne beveiligingsmaatregelen hadden voor dergelijke aanvallen, omdat Cloudflare eerder fungeerde als hun primaire beveiligingslaag. Het tijdelijke verlies van deze bescherming resulteerde in een aanzienlijke toename van het aantal verdachte logins en andere beveiligingsincidenten.

Hoewel Cloudflare zelf stelt dat de uitval niet het resultaat was van een cyberaanval, legt de situatie de nadruk op de kwetsbaarheid die ontstaat wanneer bedrijven te veel vertrouwen op één enkel beveiligingsplatform. Beveiligingsexperts raden aan dat organisaties hun afhankelijkheid van Cloudflare of vergelijkbare platforms heroverwegen en alternatieve, redundante maatregelen implementeren om toekomstige uitvallen te kunnen opvangen. Het incident heeft ook duidelijk gemaakt dat bedrijven goed moeten begrijpen welke beveiligingsmaatregelen Cloudflare biedt en wat er gebeurt wanneer deze maatregelen tijdelijk wegvallen.