Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

04-10-2025:

Europese maatregelen tegen drones na luchtruimschendingen

De recente schendingen van het luchtruim in Europa, vooral in Denemarken, hebben de dringende behoefte benadrukt aan beschermende maatregelen tegen drones. Tijdens een informele EU-top in Kopenhagen werden plannen besproken voor een "drone muur", voorgesteld door de Europese Commissie, als antwoord op de toenemende dreiging van drones. Europese landen staan voor de uitdaging om effectieve verdediging tegen deze dreiging te ontwikkelen, waarbij sommige voorstellen zoals het inzetten van dronevloten en elektromagnetische verstoringsapparatuur ter discussie staan. Er wordt gepleit voor samenwerking met Oekraïne, dat ervaring heeft met dronebestrijding. Er is echter bezorgdheid over de afhankelijkheid van militaire middelen, aangezien cyberaanvallen en hybride oorlogsvoering steeds belangrijker worden. De discussie benadrukt de noodzaak voor Europa om haar verdediging aan te passen aan de veranderende aard van conflicten, met een sterke focus op snelle, schaalbare productiecapaciteiten.

Defensie wil cyberwapens inzetten tegen Rusland: offensieve strategie 2025

De Nederlandse Defensie heeft een nieuwe Cyber Strategie 2025 gepresenteerd, waarin wordt benadrukt dat Nederland zich proactiever moet opstellen tegen digitale dreigingen, vooral vanuit Rusland. De strategie richt zich op het inzetten van cyberwapens en virussen om vijandelijke digitale aanvallen te verstoren en systemen plat te leggen. Minister Brekelmans benadrukt dat de verdediging al moet beginnen vóórdat een aanval plaatsvindt. De wetgeving zou waar nodig aangepast moeten worden om offensieve digitale acties mogelijk te maken. Dit komt na een reeks toegenomen cyberaanvallen op Nederland, waaronder aanvallen op de DigiD-dienst en gemeentelijke websites. Volgens Brekelmans is het essentieel dat Defensie zich digitaal sterker maakt om agressieve cyberactoren te verstoren en te voorkomen dat ze ongerept opereren. Er wordt gezocht naar meer digitaal vaardig personeel om de digitale strijdkracht van het leger te versterken.

Nieuwe "Cavalry Werewolf" aanval treft Russische overheidsinstanties met FoalShell en StallionRAT

Een nieuwe cyberaanval, uitgevoerd door een groep met overeenkomsten met YoroTrooper, heeft Russische overheidsinstanties en industrieën getroffen. De aanval, bekend als "Cavalry Werewolf", maakt gebruik van malwarefamilies zoals FoalShell en StallionRAT. De aanvallers verspreidden gerichte phishing-e-mails die zich voordeden als officiële communicatie van de overheid van Kirgizië. De hoofddoelen waren Russische staatsinstellingen, energiebedrijven en industriële ondernemingen. De malware stelt de aanvallers in staat om willekeurige commando's uit te voeren en gegevens te verzamelen via Telegram-bots. FoalShell en StallionRAT werden verspreid via RAR-archieven die schadelijke software bevatten. De aanval maakt deel uit van een breder patroon van aanvallen die gericht zijn op verschillende sectoren, waaronder commercie, financiën en onderwijs, waarbij vaak gevoelige gegevens worden gestolen van kwetsbare webapplicaties.

DrayTek verhelpt kwetsbaarheid in Vigor-routers die remote code execution mogelijk maakt

DrayTek heeft een beveiligingslek in zijn Vigor-routers opgelost, waarmee aanvallers op afstand code kunnen uitvoeren. De kwetsbaarheid, bekend als CVE-2025-10547, stelt ongeauthenticeerde aanvallers in staat om via speciaal gemanipuleerde HTTP en HTTPS verzoeken toegang te krijgen tot de Web User Interface (WebUI) van de router. Dit kan leiden tot een systeemcrash en in sommige gevallen tot het uitvoeren van code op afstand. DrayTek benadrukt dat routers beschermd kunnen worden tegen WAN-aanvallen door remote toegang tot de WebUI en SSL VPN-services uit te schakelen en juiste Access Control Lists (ACL's) in te stellen. Ondanks deze maatregelen kan de kwetsbaarheid ook door lokale aanvallers worden misbruikt. Gebruikers wordt aangeraden de firmware van hun routers bij te werken naar de laatste versie.

Oracle bevestigt afpersing van klanten en roept op tot installeren van updates

Oracle heeft bevestigd dat klanten van de E-Business Suite (EBS) zijn afgedreigd door criminelen, die beweren gevoelige gegevens te hebben gestolen en losgeld eisen om deze niet openbaar te maken. Dit heeft geleid tot een waarschuwing van Oracle om de beveiligingsupdates van juli 2025 te installeren, aangezien de aanvallers misbruik hebben gemaakt van kwetsbaarheden die in die updates werden verholpen. De aanvallen worden mogelijk toegeschreven aan de Cl0p-

ransomwaregroep, hoewel dit nog niet definitief is bevestigd. Oracle benadrukt dat klanten die de updates niet hebben geïnstalleerd, kwetsbaar blijven voor aanvallen. Het bedrijf heeft klanten aangespoord om direct actie te ondernemen, aangezien aanvallen op niet-gepatchte systemen bekend zijn.

Kritieke kwetsbaarheid in AndSoft's e-TMS vereist onmiddellijke patch

Een ernstige kwetsbaarheid is ontdekt in de webapplicatie van AndSoft's e-TMS, die het mogelijk maakt voor aanvallers om op afstand code uit te voeren. Deze kwetsbaarheid, aangeduid als CVE-2025-59735, heeft een CVSS-score van 9.8, wat duidt op een extreem hoog risico. Aanvallers kunnen via de kwetsbare ASP .NET-webpagina's toegang krijgen tot de systemen en vertrouwelijke gegevens stelen of operaties verstoren. Dit kan ook gebruikt worden om verdere aanvallen uit te voeren. De Belgische Cybersecurity Centrum (CCB) adviseert organisaties om de software te updaten naar versie v25.04, waarin de kwetsbaarheid is verholpen. Organisaties wordt aangeraden om monitoring- en detectiesystemen te versterken om verdachte activiteiten snel te kunnen identificeren. Het installeren van de patch voorkomt toekomstige aanvallen, maar biedt geen bescherming tegen eerdere inbreuken.

Studie onthult dat honderden gratis VPN-apps persoonlijke gegevens lekken

Een studie van bijna 800 gratis VPN-apps voor Android en iOS toont aan dat veel van deze apps de privacy van gebruikers in gevaar brengen in plaats van deze te beschermen. De apps vertonen kwetsbaarheden zoals onveilige configuraties, gevaarlijke toestemmingen en verouderde bibliotheken, waardoor persoonlijke gegevens onbedoeld worden gedeeld. Deze apps worden vaak beschouwd als veilige hulpmiddelen, maar blijken in werkelijkheid een zwakke schakel in zowel persoonlijke als zakelijke beveiliging. Kwaadwillende actoren kunnen gebruikersgegevens onderscheppen, zoals inloggegevens en apparaatspecifieke informatie, en zelfs omgevingsgeluiden opnemen. De apps maken misbruik van te brede machtigingen, zoals het lezen van logs of het verzamelen van locatiegegevens, wat leidt tot gegevenslekken. Dit probleem heeft niet alleen invloed op de individuele privacy, maar kan ook leiden tot datalekken binnen bedrijfsnetwerken.

kwetsbaarheden in TOTOLINK X6000R router stellen aanvallers in staat willekeurige commando's uit te voeren

Er zijn ernstige beveiligingsflaws ontdekt in de TOTOLINK X6000R router, die gebruikers blootstelt aan ernstige risico’s, zoals remote code execution en ongeautoriseerde toegang tot systemen. Deze kwetsbaarheden beïnvloeden de webinterface van de router en verschillende administratieve functies, wat meerdere aanvalsvectoren creëert die door kwaadwillende actoren kunnen worden misbruikt om volledige controle over getroffen apparaten te krijgen. De kwetsbaarheden zijn te wijten aan onvoldoende validatie van gebruikersinvoer en slechte beveiligingspraktijken in de firmware van de router. Door de kwetsbaarheden kunnen aanvallers via speciaal samengestelde HTTP-verzoeken willekeurige systeemcommando's uitvoeren op het Linux-systeem van de router. De meest kritieke kwetsbaarheid stelt aanvallers in staat om authenticatiemechanismen te omzeilen en commando's uit te voeren met root-rechten. Het exploiteren van deze kwetsbaarheden vereist alleen netwerktoegang tot het apparaat, waardoor de risico’s bijzonder hoog zijn voor routers die internet-facing zijn.

Meer dan 472 miljoen nieuwe gestolen gegevens

In oktober 2025 werd de Leaked.Domains database geüpdatet met meer dan 472 miljoen nieuwe records, die afkomstig zijn van verschillende datalekken. De update bevatte 451.257 nieuwe combinaties van e-mail en wachtwoorden, evenals enorme hoeveelheden gestolen gegevens, waaronder meer dan 1,8 miljoen logbestanden van Stealer v2, 4 miljoen creditcardgegevens en 281 miljoen records in de PeopleDB. Daarnaast werden er meer dan 12 miljoen nieuwe subdomeinen en 160 miljoen certificaatgegevens toegevoegd. De totale omvang van de database is nu meer dan 39 miljard records, met gegevens die variëren van gestolen inloggegevens en creditcardinformatie tot WHOIS-informatie en DNS-gegevens. De Leaked.Domains-database blijft een belangrijke bron voor cyberdreigingen en moet nauwlettend worden gevolgd door beveiligingsprofessionals.

Microsoft stopt met weergeven van inline SVG-afbeeldingen in Outlook

Microsoft heeft besloten om inline SVG-afbeeldingen niet langer weer te geven in Outlook voor Web en de nieuwe versie van Outlook voor Windows. De wijziging is een veiligheidsmaatregel om cross-site scripting (XSS) aanvallen te voorkomen.

SVG-afbeeldingen, die geschreven zijn in XML en JavaScript ondersteunen, kunnen misbruikt worden door aanvallers om scripts toe te voegen die naar phishingwebsites leiden. Het afgelopen jaar werden er meerdere phishingaanvallen gedetecteerd waarbij SVG-afbeeldingen werden ingezet. Microsoft heeft aangegeven dat minder dan 0,1% van de afbeeldingen in Outlook SVG-afbeeldingen zijn, zodat de impact op gebruikers minimaal is. Normale bijlagen in SVG-formaat worden echter nog steeds ondersteund en weergegeven.

Criminelen claimen diefstal van 1 miljard records uit Salesforce-databases

Criminelen beweren via een nieuwe website dat ze 1 miljard records hebben gestolen uit de databases van Salesforce-klanten, waaronder bedrijven als KLM, Cisco en McDonald's. De aanvallers zouden meer dan honderd Salesforce-installaties van grote bedrijven hebben getroffen. De genoemde bedrijven hebben tot 10 oktober om losgeld te betalen, anders zullen de aanvallers dreigen de gestolen data openbaar te maken. De aanval zou via telefonische phishing en gestolen tokens bij het softwarebedrijf Salesloft zijn uitgevoerd. Hoewel het nog niet zeker is of de website daadwerkelijk van de aanvallers komt, lijken de details te wijzen op een verband met de recente Salesforce-aanvallen. KLM had eerder een datalek gemeld waarbij klantgegevens via een extern platform werden gestolen, maar werd toen niet specifiek aangegeven dat het om Salesforce ging.

Nieuwe CommetJacking-aanval maakt misbruik van Comet-browser

De 'CommetJacking'-aanval maakt misbruik van URL-parameters om verborgen instructies door te geven aan de Comet AI-browser van Perplexity, waardoor gevoelige gegevens van verbonden services, zoals e-mail en agenda’s, kunnen worden gestolen. De aanval vereist geen gebruikersinteractie of inloggegevens, waardoor een aanvaller simpelweg een kwaadaardige URL kan versturen naar de beoogde gebruiker. Comet is een browser die autonoom het web kan doorzoeken en gebruikers kan helpen met taken zoals e-mailbeheer en het doen van aankopen. Onderzoekers van LayerX ontdekten dat door de prompt in de URL aan te passen, gegevens zoals Google-agenda-invites en Gmail-berichten konden worden geëxporteerd en naar een externe server gestuurd. De beveiligingsmaatregelen van Perplexity blijken onvoldoende om deze datadiefstal te voorkomen, aangezien de gegevens kunnen worden gecodeerd voordat ze het systeem verlaten. Ondanks

waarschuwingen van de onderzoekers, heeft Perplexity de risico's tot nu toe niet erkend.

Dark Web berichten wijzen op nieuwe dreigingen

Op het darkweb verschijnen steeds meer berichten over cyberdreigingen die gericht zijn op zowel overheden als bedrijven. Deze dreigingen variëren van ransomware-aanvallen tot de verkoop van gestolen gegevens. Er zijn meldingen van nieuwe hackinggroepen die zich richten op kwetsbare infrastructuren, vooral in sectoren zoals de gezondheidszorg en de financiële wereld. Ook worden er op het darkweb tools en scripts gedeeld die door cybercriminelen kunnen worden gebruikt om beveiligingssystemen te omzeilen. De focus ligt hierbij op het benutten van kwetsbaarheden in populaire software en het misbruiken van nieuwe technieken voor identiteitsdiefstal. Deskundigen waarschuwen voor de toenemende gevaren en raden aan om systemen regelmatig te updaten en gebruik te maken van robuuste encryptie om gegevens te beschermen. Deze ontwikkeling onderstreept de noodzaak voor bedrijven om proactief te blijven in het beveiligen van hun digitale infrastructuren.

Lapsus$ Hunters teast nieuwe DLS

Er is sprake van een nieuwe ontwikkeling met betrekking tot de hacker groep Scattered Lapsus$ Hunters. Het lijkt erop dat deze groep een nieuw DLS (Data Leak Site) aan het teasen is. Deze aankondiging heeft voor enige opwinding gezorgd, vooral onder cybersecurity-experts en onderzoekers. Hoewel er nog geen gedetailleerde informatie beschikbaar is over het beoogde doelwit of de omvang van de geplande datalekken, blijft de beweging van deze groep nauwlettend gevolgd. Scattered Lapsus$ Hunters staat bekend om hun betrokkenheid bij grootschalige datalekken, waarbij zij vaak gevoelige gegevens op het darkweb publiceren. De verwachting is dat deze nieuwe activiteit de focus zal zijn van een aankomende campagne, die mogelijk grote gevolgen heeft voor de getroffen organisaties. Het blijft afwachten welke specifieke doelen in het vizier staan en of dit een nieuwe fase markeert voor de groep.

Crimson Collective gebruikt gelekte authenticatietokens voor inbreuk op klantensystemen

Hackers van de groep Crimson Collective hebben via gelekte authenticatietokens toegang gekregen tot klantensystemen, waarbij gevoelige informatie zoals inloggegevens, tokens en netwerkdata werd gestolen. Het incident werd bevestigd door Red Hat, die ontdekte dat privé GitHub-repositories met klantgegevens waren gecompromitteerd. De hackers claimen al toegang te hebben gekregen tot diverse systemen van klanten. Dit incident vormt een groot risico voor Belgische organisaties die gebruikmaakten van Red Hat Consulting-diensten en voor bedrijven die gevoelige gegevens met Red Hat deelden. De gevolgen kunnen variëren van ongeautoriseerde toegang tot systemen tot verstoring van IT-activiteiten en gevolgen voor de toeleveringsketen. Organisaties wordt aangeraden om alle gedeelde tokens en inloggegevens in te trekken en contact op te nemen met Red Hat voor verdere begeleiding.

Onderzoekers waarschuwen voor zelfverspreidende WhatsApp-malware SORVEPOTEL

Onderzoekers hebben gewaarschuwd voor de opkomst van een nieuwe malwarecampagne, SORVEPOTEL, die zich snel verspreidt via WhatsApp, voornamelijk gericht op Braziliaanse gebruikers. De malware verspreidt zich via phishingberichten met schadelijke ZIP-bestanden die lijken op onschuldige bijlagen zoals ontvangstbewijzen of bestanden van gezondheidsapps. Zodra het bestand op een desktop wordt geopend, activeert een PowerShell-script de malware die zichzelf in de opstartmap van Windows plaatst, zodat het automatisch wordt uitgevoerd bij elke herstart van het systeem. Het belangrijkste doel van deze malware is snelle verspreiding via WhatsApp-web, waarbij het infecteerde accounts spam stuurt naar alle contacten en groepen. Dit leidt vaak tot tijdelijke blokkeringen van accounts vanwege de overtreding van WhatsApp's gebruiksvoorwaarden. Tot nu toe zijn er 477 infecties gerapporteerd, waarvan 457 in Brazilië, waarbij vooral overheids- en bedrijfssystemen getroffen zijn.

Cybercriminelen misleiden gebruikers met merkimitaties voor malwaredistributie

Cybercriminelen hebben een geavanceerde aanvalscampagne gelanceerd waarbij merkimitaties worden gebruikt om malware via smishing (SMS phishing) te verspreiden. In deze nieuwe golf van aanvallen maken de aanvallers gebruik van URL-manipulatie door vertrouwde merknamen in de URL’s te verwerken, zodat

gebruikers minder kritisch worden en de links sneller aanklikken. Deze techniek maakt gebruik van het psychologisch effect waarbij ontvangers meer aandacht schenken aan de bekende merknaam dan aan het volledige URL-adres. De aanvallers registreren domeinen van tevoren, zodat ze een goede domeinreputatie opbouwen, wat helpt om automatische beveiligingsfilters te omzeilen. De aanvallen leiden naar inlogpagina's die bedoeld zijn voor het verzamelen van inloggegevens of die automatisch malware downloaden voor zowel mobiele als desktopplatformen. De gebruikte domeinen, waaronder de .xin-extensie, bieden extra camouflage. De aanvallen zijn een evolutie van de eerdere social engineering-technieken en zijn gericht op het maximaliseren van infecties bij minimale detectie.

Nieuw 'point-and-click' phishing kit omzeilt gebruikersbewustzijn en beveiligingsfilters

Een nieuw phishing kit maakt het mogelijk voor cybercriminelen om gesofisticeerde phishing-aanvallen te creëren zonder diepgaande technische kennis. Dit ‘point-and-click’ gereedschap biedt een gebruiksvriendelijke webinterface waarmee aanvallers pre-geconfigureerde sjablonen kunnen kiezen, merkkenmerken kunnen aanpassen en specifieke doelen kunnen kiezen. Zodra de phishingpagina is opgezet, worden slachtoffers geconfronteerd met onschuldig lijkende downloadverzoeken die in werkelijkheid schadelijke code activeren. Het kit gebruikt vaak gangbare bestandsformaten zoals Microsoft Office-documenten en HTML-toepassingen. Wanneer gebruikers deze documenten openen, worden ze gevraagd om macro’s in te schakelen of scripts uit te voeren, waarmee de schadelijke code wordt geladen. Dit gereedschap maakt gebruik van geavanceerde technieken, zoals het onzichtbaar uitvoeren van code in het geheugen, wat traditionele handtekeninggebaseerde beveiligingssystemen omzeilt.

SideWinder Hacker Group Hosts Fake Outlook/Zimbra Portals to Steal Login Credentials

De SideWinder hacker groep, een staatssponsor die bekend staat om spionagecampagnes in Zuid-Azië, heeft een nieuwe phishingaanval opgezet. De groep maakt gebruik van valse webmailportalen die Outlook en Zimbra nabootsen. Deze portalen worden gehost op gratis platformen zoals Netlify en Workers.dev, en zijn gericht op overheids- en militaire doelwitten in landen als Pakistan, Nepal, Sri Lanka, Bangladesh en Myanmar. De slachtoffers worden verleid met documenten die

thema's van defensie en maritieme zaken bevatten, waarna hun inloggegevens via valse inlogpagina's worden gestolen. De aanvallers gebruiken snelle domeinverandering om de impact van geblokkeerde sites te verminderen. Deze aanpak maakt het moeilijk om de aanvallen te blokkeren en verhoogt het risico op gegevensdiefstal en malwareverspreiding.

nieuwe GhostSocks Malware-as-a-Service zet gecompromitteerde apparaten om in proxies

GhostSocks, een nieuw Malware-as-a-Service (MaaS) aanbod, stelt cybercriminelen in staat gecompromitteerde apparaten om te zetten in SOCKS5 proxies. Dit gebeurt via een webgebaseerd controlepaneel waarmee gebruikers Windows- en UNIX-systemen kunnen beheren. GhostSocks benut het vertrouwen in residentiële IP-adressen om anti-fraude controles te omzeilen en detectie te vermijden. Het platform elimineert de noodzaak voor externe proxyservers, wat de operationele kosten verlaagt. De malware wordt via een "dropper" geïnstalleerd en verkrijgt vervolgens SOCKS5-credentials via een C2-server. Zodra geïnstalleerd, werkt GhostSocks volledig in het geheugen van het slachtoffer, zonder dat er een persistentie-mechanisme wordt geïmplementeerd. De dienst heeft snel tractie gewonnen, zelfs bij meer geavanceerde cybercriminelen, die het gebruiken in combinatie met andere tools zoals LummaStealer om langdurige toegang tot netwerken te behouden.

Nieuwe XWorm V6 variant injecteert kwaadaardige code in legitiem Windows-programma

De XWorm-malware is terug, met een nieuwe versie (V6.0) die op 4 juni 2025 werd aangekondigd. Na het stoppen van officiële ondersteuning voor versie 5.6 in 2024, werd deze versie gepresenteerd als een verbetering, met een patch voor een kritieke kwetsbaarheid in de uitvoering van externe code. XWorm V6 is een modulaire malware, opgebouwd uit een kernclient en verschillende plugins die diverse kwaadaardige activiteiten uitvoeren, zoals het stelen van inloggegevens en het verspreiden van ransomware. Het infectiemechanisme maakt gebruik van een JavaScript-bestand dat via phishing-e-mails of gecompromitteerde websites wordt verspreid. De malware injecteert code in een legitiem Windows-proces, zoals RegSvcs.exe, en gebruikt een versleuteld communicatiekanaal om met een

command-and-control server te verbinden. Dit maakt de malware moeilijker detecteerbaar en vergroot de persistentie op getroffen systemen.

Hackers proberen exploit van Grafana-kwetsbaarheid voor willekeurige bestandlezingen

Grafana, een populaire open-source platform voor gegevensanalyse, is opnieuw het doelwit van grootschalige, gecoördineerde cyberaanvallen. Beveiligingsonderzoekers van GreyNoise merkten op dat er op 28 september plotseling een piek was in pogingen om de kwetsbaarheid CVE-2021-43798 uit te buiten. Deze path traversal-kwetsbaarheid maakt het mogelijk om willekeurige bestanden te lezen op niet-gepatchte systemen. Gedurende één dag werden 110 unieke kwaadaardige IP-adressen gedetecteerd die probeerden toegang te krijgen tot gevoelige configuratie- en inlogbestanden. De aanvallen waren geografisch gericht op de VS, Slowakije en Taiwan, waarbij de meeste aanvallen afkomstig waren uit Bangladesh. De aanvallers gebruikten vermoedelijk wegwerpbare infrastructuur en gedeelde tools. Dit incident benadrukt de blijvende dreiging van verouderde kwetsbaarheden en het belang van voortdurende waakzaamheid, zelfs na patching. Het is aanbevolen om alle Grafana-implementaties bij te werken en verdachte IP-adressen te blokkeren.

Europol-conferentie waarschuwt: strijd tegen cybercriminaliteit hangt af van toegang tot data

Europol heeft tijdens zijn 4e jaarlijkse Cybercrime Conference gewaarschuwd dat cybercriminelen sneller gebruikmaken van encryptie, anonimiseringsmethoden en nieuwe technologieën dan wetshandhavers kunnen reageren. Dit maakt toegang tot gegevens de belangrijkste uitdaging in de strijd tegen cybercriminaliteit. Tijdens de conferentie benadrukte Catherine De Bolle, directeur van Europol, dat digitale bewijslast cruciaal is om misdaad te bestrijden, bijvoorbeeld bij het identificeren van slachtoffers of het voorkomen van terroristische aanvallen. Europese commissaris Magnus Brunner sprak over de noodzaak om de samenwerking tussen overheden en de industrie te versterken en wetgeving bij te werken. Het evenement richtte zich op vijf kernkwesties: privacy vs. toegang tot data, grensoverschrijdende samenwerking, datagestuurde wetgeving, cyberdiplomatie en preventie. Case studies werden gepresenteerd over succesvolle operaties, zoals het verstoren van pro-Russische

hacktivisten en de arrestatie van de beheerder van een invloedrijk Russisch cybercrimeforum.

MeteoBridge-systeem voor weerstations doelwit van aanvallen

Het MeteoBridge-systeem, gebruikt voor het delen van weerdata via publieke netwerken zoals Weather Underground, wordt actief aangevallen, zo meldt het Amerikaanse CISA (Cybersecurity and Infrastructure Security Agency). De kwetsbaarheid, bekend als CVE-2025-4008, stelt aanvallers in staat om via de webinterface van MeteoBridge op afstand commando's uit te voeren. Deze kwetsbaarheid, die kan leiden tot command injection, werd in mei 2025 verholpen met een update naar versie 6.2, maar de technische details werden kort daarna openbaar. CISA waarschuwt dat aanvallers deze kwetsbaarheid nu actief misbruiken, hoewel er geen specifieke details over het misbruik worden gedeeld. Overheidsinstellingen in de VS die het MeteoBridge-systeem gebruiken, moeten de patch voor 21 oktober hebben geïnstalleerd om verdere risico’s te minimaliseren.

Japanse bierbrouwer Asahi platgelegd door ransomware-aanval

De Japanse bierbrouwer Asahi is getroffen door een ransomware-aanval, waarbij systemen zijn verstoord en gegevens zijn buitgemaakt. De aanval heeft de operaties van de brouwerij ernstig beïnvloed, waardoor bestellingen en leveringen nu handmatig worden verwerkt. Sinds de aanval op 29 september is de productie in verschillende brouwerijen stilgelegd, wat heeft geleid tot een dreigend tekort aan Asahi-bier in supermarkten. Asahi heeft bevestigd dat het om een ransomware-aanval gaat, maar de exacte details over de buitgemaakte gegevens worden nog onderzocht. Het bedrijf heeft moeite met het ontvangen van externe e-mails, en de klantenservice is momenteel niet bereikbaar. Asahi hoopt de klantenservice volgende week weer te herstellen, maar het is onduidelijk wanneer alle systemen volledig zullen worden hersteld. De verstoring heeft voorlopig alleen invloed op Japan, en de financiële impact is nog niet bekend.

Verkoop van 1.000.000 rijen MAIL:PASS aan CoinMarketCap mogelijk

Er wordt gemeld dat er een verkoop van één miljoen rijen met MAIL:PASS-gegevens heeft plaatsgevonden naar CoinMarketCap. Deze gegevens bevatten e-

mailadressen en bijbehorende wachtwoorden, die mogelijk gestolen zijn en op het darkweb worden verhandeld. De vermelde gegevens kunnen ernstige gevolgen hebben voor de privacy en beveiliging van de betrokken gebruikers. CoinMarketCap, een platform dat informatie biedt over cryptocurrency, zou een mogelijke doelwit kunnen zijn voor kwaadwillende actoren die deze gegevens willen misbruiken. Het incident benadrukt de voortdurende dreiging van datalekken en de noodzaak voor bedrijven en gebruikers om sterke beveiligingsmaatregelen te treffen, zoals het gebruik van unieke wachtwoorden en tweefactorauthenticatie. Verdere onderzoeken naar de herkomst van de gegevens en de impact op de slachtoffers zijn noodzakelijk om de omvang van de situatie te begrijpen.

Hackers stalen meer dan $127 miljoen in crypto in september volgens PeckShield

In september 2025 werd er volgens cybersecurityfirma PeckShield meer dan $127 miljoen aan cryptocurrency gestolen door hackers. Deze aanzienlijke diefstal werd uitgevoerd door verschillende cybercriminelen die verschillende kwetsbaarheden in crypto-exchanges en -platforms uitbuitten. Hackers maken steeds vaker gebruik van geavanceerde methoden, waaronder phishing-aanvallen en de exploitatie van smart contract-zwaktes, om toegang te krijgen tot digitale portefeuilles en crypto-assets. De meeste van deze aanvallen betroffen populaire cryptomunten zoals Bitcoin en Ethereum. Dit incident benadrukt de voortdurende dreiging voor cryptocurrency-bezitters en de noodzaak voor strengere beveiligingsmaatregelen binnen de crypto-industrie. Experts raden gebruikers aan om gebruik te maken van beveiligde wallets en tweefactorauthenticatie om hun activa te beschermen tegen dergelijke aanvallen.

vermeende verkoop van HTML Payload Packaging Tool voor verkeer/spam

Er wordt melding gemaakt van de vermeende verkoop van een HTML Payload Packaging Tool, die wordt aangeboden voor het genereren van verkeer en spam. Deze tool zou specifiek gericht zijn op het verhogen van webverkeer door middel van kwaadaardige HTML-payloads. Het gebruik van dergelijke tools kan leiden tot verschillende cyberdreigingen, zoals het verstoren van webdiensten en het verspreiden van spamberichten. De verkoper zou de tool aanbieden via de darkweb-marktplaatsen, hoewel er nog geen bevestiging is van de daadwerkelijke transactie. De handel in dergelijke kwaadaardige tools benadrukt de voortdurende groei van cybercriminaliteit, waarbij criminelen zoeken naar manieren om online systemen te

misbruiken voor eigen gewin. Het is belangrijk voor organisaties en individuen om waakzaam te blijven voor verdachte activiteiten die verband houden met dit soort online dreigingen.

Telegram Bot API misbruikt voor XWorm C2-communicatie

Er is een nieuw IOC gemeld waarbij de officiële Telegram Bot API wordt misbruikt als een command-and-control (C2) kanaal voor de XWorm malware. Deze aanpak maakt gebruik van Telegram-infrastructuur om kwaadaardig verkeer te verbergen tussen legitieme versleutelde communicatie, waardoor detectie wordt vermeden. De incidentie werd gemeld op 2 oktober 2025, met een vertrouwensniveau van 50%. De gebruikte URL is een Telegram Bot API link. XWorm wordt aangemerkt als een botnet C2-malware die in de aanval wordt ingezet. Organisaties wordt geadviseerd verdachte verbindingen met Telegram Bot API eindpunten te blokkeren en te monitoren op processen die Telegram-API URL's aanroepen, omdat dit een indicatie van malware-activiteit kan zijn. De waarschuwing benadrukt de groeiende trend van malware die gebruik maakt van legitieme cloud- en messaging-API’s om C2-verkeer te verbergen.

Scattered Lapsus$ Hunters onion live op het dark web

De Scattered Lapsus$ Hunters onion-site is recent gelanceerd. Dit is een dark web-platform dat wordt geassocieerd met de bekende Lapsus$ hackinggroep. Via deze site kunnen gebruikers mogelijk toegang krijgen tot informatie en middelen die verband houden met cybercriminaliteit. De website is bereikbaar via het gebruikelijke .onion-domein, wat duidt op een focus op anonimiteit en privacy. Het is nog niet duidelijk wat de exacte doelen van de site zijn, maar de naam suggereert een mogelijke verbondenheid met andere activiteiten van de Lapsus$ groep. Gezien de aard van de site kan het een belangrijke bron zijn voor onderzoekers die zich bezighouden met het monitoren van cybercriminaliteit en hacking-groepen. Beveiligingsexperts worden gewaarschuwd voor de mogelijke risico's die verbonden zijn aan interactie met dergelijke platforms.