## Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

25-10-2025:

Albert Heijn-franchisenemer Bun bevestigt ransomware-aanval op systemen

Albert Heijn-franchisenemer Bun heeft bevestigd het slachtoffer te zijn van een ransomware-aanval, waarbij een deel van de systemen werd versleuteld. De aanvallers wisten ook gegevens van huidige en voormalige medewerkers te stelen, waaronder persoonlijke informatie zoals paspoorten, salarisgegevens en bankinformatie. Bun exploiteert 29 supermarkten en heeft ongeveer 3500 medewerkers. De aanvallers, die zich hebben geïdentificeerd als de ransomwaregroep ThreeAM, boden een deel van de gestolen data aan via hun website en dreigden met verdere openbaarmaking als er niet betaald werd. Het incident werd op 10 oktober gemeld aan de getroffen medewerkers. Verdere details over de aanval zijn vooralsnog onbekend.

EU en Moldavië versterken digitale samenwerking voor betere veerkracht

De Europese Commissie verwelkomt de intensivering van de digitale samenwerking tussen Moldavië en de EU, met als doel de cyberbeveiliging te verbeteren, desinformatie te bestrijden en Moldavië op te nemen in de EU-roamingzone. De goedkeuring van het gebruik van het EU Cybersecurity Reserve voor Moldavië is een belangrijke stap in de regionale beveiliging en de digitale samenwerking tussen de EU en Moldavië onder de Cyber Solidarity Act. Dit akkoord markeert de eerste succesvolle cyberovereenkomst onder het Deense voorzitterschap en biedt steun bij het aanpakken van ernstige cyberincidenten. Daarnaast zal Moldavië deelnemen aan het ‘Roam Like at Home’-initiatief, waardoor Moldavische burgers en EU-reizigers zonder extra kosten kunnen bellen, sms'en en mobiele data gebruiken. Verder werd een nieuwe hub van de European Digital Media Observatory opgericht om de veerkracht tegen buitenlandse inmenging en desinformatie te versterken.

Bitter APT hackers exploiteren WinRAR zero-day via gemanipuleerde Word-documenten om gevoelige gegevens te stelen

De Bitter APT-groep, ook bekend als APT-Q-37 of 蔓灵花 in China, heeft een geavanceerde cyberespionagecampagne gelanceerd. Deze richt zich op overheidsinstanties, militaire installaties en kritieke infrastructuur in China en Pakistan. De groep maakt gebruik van gemanipuleerde Microsoft Office-documenten

die een onbekende zero-day kwetsbaarheid in WinRAR uitbuiten. Dit leidt tot de installatie van een op maat gemaakte C#-backdoor op de getroffen systemen. De aanval wordt uitgevoerd via twee methoden: een Excel-bestand met VBA-macro's en een WinRAR-paddoorbreking die de kwetsbaarheid voor versie 7.11 en eerder uitbuit. De backdoor stelt de aanvallers in staat om gevoelige gegevens te exfiltreren en op afstand commando's uit te voeren. Het incident werd in oktober 2024 ontdekt door Qianxin-analisten die abnormale netwerkverkeerpatronen detecteerden.

WordPress-sites aangevallen via kwetsbaarheden in plug-ins GutenKit en Hunk Companion

WordPress-sites worden momenteel aangevallen via ernstige kwetsbaarheden in de plug-ins GutenKit en Hunk Companion. Deze plug-ins hebben een publiek toegankelijk API-endpoint dat ongeauthenticeerde aanvallers in staat stelt willekeurige plug-ins te installeren, wat kan leiden tot remote code execution. Meer dan 40.000 websites maken gebruik van GutenKit, terwijl Hunk Companion actief is op meer dan 8.000 websites. De kwetsbaarheden, aangeduid met CVE-2024-9234 en CVE-2024-9707, hebben een CVSS-score van 9,8. Ondanks dat beveiligingsupdates voor deze kwetsbaarheden al meer dan een jaar beschikbaar zijn, is er sinds oktober 2025 actief misbruik van deze lekken. WordPress-beheerders die de updates nog niet hebben geïnstalleerd, worden aangespoord om dit snel te doen en hun websites te controleren op verdachte plug-ins.

Microsoft komt met noodpatch voor kritiek lek in Windows Server

Microsoft heeft een noodpatch uitgerold om een ernstige kwetsbaarheid in Windows Server te verhelpen, specifiek in de Windows Server Update Service (WSUS). Het beveiligingslek, aangeduid als CVE-2025-59287, heeft een score van 9.8 op de CVSS-schaal en stelt aanvallers in staat om op afstand code uit te voeren met SYSTEM-rechten. Deze kwetsbaarheid werd eerder op 14 oktober geïdentificeerd, maar proof-of-concept exploitcode werd inmiddels openbaar. Het lek kan eenvoudig worden misbruikt door het versturen van een speciaal verzoek naar de server. Microsoft heeft aangegeven dat de kans op misbruik toeneemt, en biedt nu een "out of band security update" aan om de kwetsbaarheid volledig te patchen. De patch is beschikbaar voor verschillende versies van Windows Server, waaronder 2012, 2016, 2019 en 2022.

Ook NCSC waarschuwt voor actief misbruik van kritiek Windows Server-lek

et Nationaal Cyber Security Centrum (NCSC) heeft gewaarschuwd voor het actieve misbruik van een kritieke kwetsbaarheid in Windows Server. De kwetsbaarheid bevindt zich in de Windows Server Update Service (WSUS), die het mogelijk maakt voor een ongeauthenticeerde aanvaller om een server op afstand over te nemen. Het probleem heeft de naam CVE-2025-59287 gekregen en is beoordeeld met een score van 9.8 op 10, wat de ernst van de situatie benadrukt. Microsoft bracht eerder een patch uit, maar heeft nu een aanvullende update uitgebracht om het lek volledig te verhelpen. Er is inmiddels ook proof-of-conceptcode beschikbaar, waardoor het risico op misbruik aanzienlijk toeneemt. Het NCSC raadt aan om WSUS niet direct aan het internet te ontsluiten om het risico te beperken.

Windowscomputers aangevallen met Linux-ransomware door Qilin-groep

Antivirusbedrijf Trend Micro heeft gemeld dat Windowscomputers recentelijk zijn aangevallen met Linux-ransomware door de Qilin-ransomwaregroep. De groep heeft wereldwijd al 700 organisaties in 62 landen getroffen, met de meeste slachtoffers in de Verenigde Staten, Frankrijk, Canada en het Verenigd Koninkrijk. De aanvallers maken gebruik van verschillende technieken zoals spear phishing, gestolen inloggegevens en malafide captcha’s om toegang tot systemen te verkrijgen. Na het verkrijgen van toegang wordt malware geïnstalleerd en worden de rechten op het systeem verhoogd. Vervolgens wordt data gestolen en ransomware uitgerold. De aanvallers gebruiken Linux-ransomware die via de remote managementsoftware Splashtop op Windowssystemen wordt uitgevoerd, waardoor endpoint-detectiesystemen kunnen worden omzeild. Na afloop van de aanval eisen de aanvallers losgeld voor het niet openbaar maken van gestolen data.

Klanten Belgische bank doelwit van social engineering-aanval via Android

Klanten van de Belgische bank KBC die een Androidtelefoon gebruiken, worden momenteel getroffen door een social engineering-aanval. Oplichters doen zich voor als medewerkers van telecomprovider Proximus en bellen slachtoffers met de mededeling dat hun simkaart moet worden vernieuwd. Ze sturen een malafide app via WhatsApp, die slachtoffers moeten installeren. Deze app, een kwaadaardig .apk-

bestand, vereist dat de instelling voor het installeren van apps uit onbekende bronnen wordt ingeschakeld. Na installatie krijgen de oplichters controle over de telefoon en kunnen ze fraude uitvoeren met de mobiele bankdiensten van het slachtoffer, inclusief het doen van overschrijvingen. In sommige gevallen wordt het scherm van de telefoon zwart, waardoor deze onbruikbaar wordt. De Belgische overheid waarschuwt om nooit apps te installeren die via onbekende kanalen worden aangeboden en adviseert slachtoffers om contact op te nemen met hun bank.

Dreigingsactoren met stealer-malware verwerken miljoenen inloggegevens per dag

De stealer-malware-industrie heeft zich ontwikkeld tot een geavanceerd crimineel netwerk dat dagelijks honderden miljoenen inloggegevens verwerkt. Criminalen hebben gespecialiseerde malware-families ontwikkeld en platforms gecreëerd voor de verspreiding van gestolen gegevens. Onlangs ontdekte onderzoeken hebben aangetoond dat een enkel Telegram-account dagelijks tot 50 miljoen inloggegevens kan ontvangen. Deze gegevens worden op diverse marktplaatsen, vooral op Telegram, gekocht, verkocht en gedeeld. De operationele structuur van deze criminele netwerken is hiërarchisch, met hoofdverkopers die privékanalen aanbieden voor betalende klanten. Aggregators verzamelen gegevens uit verschillende bronnen en verspreiden deze verder. De technische infrastructuur maakt gebruik van verschillende formaten voor de gestolen gegevens, wat uitdagingen oplevert voor onderzoekers en aggregators bij het verwerken van de informatie. De handel in gestolen inloggegevens wordt steeds meer gecommercialiseerd, met abonnementen die variëren van wekelijkse tot levenslange toegang.

Hackers misbruiken Microsoft 365 Exchange Direct Send om inhoudsfilters te omzeilen en gevoelige data te verzamelen

Cybercriminelen maken misbruik van de Direct Send-functie van Microsoft 365 Exchange Online, een functie die oorspronkelijk was ontworpen voor legacy-apparaten en applicaties om e-mail te versturen zonder authenticatie. Deze functionaliteit wordt nu gebruikt om phishing- en bedrijfs-e-mailcompromis-aanvallen uit te voeren. Direct Send omzeilt de gebruikelijke beveiligingsmechanismen zoals DomainKeys-Identified Mail (DKIM), Sender Policy Framework (SPF) en Domain-based Message Authentication, Reporting and Conformance (DMARC). Aanvallers sturen valse berichten die afkomstig lijken van interne, vertrouwde bronnen, zoals

leidinggevenden of IT-helpdesks. Deze berichten bevatten vaak sociale-engineeringtactieken, zoals goedkeuringen van taken of betalingsverzoeken, om slachtoffers te manipuleren en hun inloggegevens of andere gevoelige informatie te verkrijgen. Microsoft heeft gereageerd door een optie te introduceren om Direct Send te blokkeren en andere beveiligingsmaatregelen te verbeteren.

SharkStealer gebruikt EtherHiding-techniek voor C2-communicatie via blockchain

SharkStealer, een geavanceerde infostealer-malware geschreven in Golang, maakt gebruik van blockchaintechnologie om beveiligde communicatiekanalen op te zetten met command-and-control (C2)-infrastructuren. Deze malware gebruikt de BNB Smart Chain Testnet als een veerkrachtige "dead-drop" oplosser voor C2-kanalen, waarbij traditionele detectiemethoden worden omzeild. SharkStealer past de EtherHiding-techniek toe, waarbij cruciale componenten van de infectieketen op openbare blockchains worden opgeslagen in plaats van op conventionele webservers. Dit maakt gebruik van de transparantie en beschikbaarheid van blockchainnetwerken en zorgt ervoor dat de communicatie moeilijk te verstoren of te monitoren is. De malware maakt slimme contracten op de blockchain voor het ophalen van versleutelde gegevens en het verkrijgen van C2-gegevens, wat de effectiviteit van de aanval vergroot.

Bedreiging: Hackers vallen Azure Blob Storage aan om organisatierepositories te compromitteren

Cybersecurity-onderzoekers hebben een nieuwe aanvalscampagne ontdekt waarbij cybercriminelen misbruik maken van gecompromitteerde inloggegevens om toegang te krijgen tot Azure Blob Storage-containers. Dit stelt hen in staat om de kritieke code en gevoelige gegevens van organisaties te stelen. De aanvallen richten zich specifiek op slecht geconfigureerde toegangsbeveiligingen, waarbij de aanvallers voortdurend containers scannen op waardevolle data. Microsoft waarschuwde dat de aanvallen vaak beginnen met phishingcampagnes en malware, zoals de SharkStealer, die geavanceerde technieken gebruikt om detectie te ontwijken. SharkStealer maakt gebruik van blockchain-technologie via de BNB Smart Chain als communicatiekanaal, wat het voor traditionele beveiligingsmaatregelen moeilijk maakt om schadelijk verkeer te detecteren. Het uiteindelijke doel van de aanvallers is het stelen van toegangscodes en andere vertrouwelijke gegevens. Organisaties

worden geadviseerd om strengere authenticatiepolicies en gedragsmonitoring te implementeren om dergelijke aanvallen te voorkomen.

New fileless Remcos attacks bypassing EDRs with malicious code into RMClient

De Remcos-malware, een commercieel remote access tool dat zich voordoet als legitieme surveillancesoftware, is in het derde kwartaal van 2025 de leidende infostealer geworden, goed voor 11% van de gedetecteerde gevallen. Dit type malware maakt gebruik van fileless-aanvallen, wat betekent dat het geen bestand op de schijf achterlaat en dus traditionele endpoint detection and response (EDR) systemen ontwijkt. De aanvallen beginnen met e-mails die onschuldige bijlagen bevatten, waarna een PowerShell-script wordt uitgevoerd dat een continu downloadmechanisme instelt om schadelijke payloads van een command-and-control server te verkrijgen. Het script injecteert vervolgens de Remcos-malware in het legitieme bestand RmClient.exe, dat digitaal ondertekend is, waardoor het moeilijker te detecteren is. Deze malware richt zich vooral op het stelen van inloggegevens uit browsers. Organisaties wordt aangeraden om hun detectiemethoden te verbeteren door patronen van procesinjectie te monitoren en ongebruikelijke toegang tot inloggegevens te identificeren.

Phishingcampagne misbruikt nep overlijdensclaims om LastPass-klanten te misleiden

LastPass waarschuwt voor een gerichte phishingcampagne waarbij aanvallers zich voordoen als familieleden die toegang vragen tot wachtwoordkluizen via een zogenaamd nalatenschapsverzoek. De e-mails beweren dat een familielid een overlijdensakte heeft ingediend om toegang te krijgen tot de kluis. Slachtoffers worden aangespoord om op een link te klikken om het verzoek te annuleren. Deze link leidt echter naar een valse inlogpagina op lastpassrecovery[.]com, waar gebruikers hun hoofdwachtwoord kunnen invoeren. De campagne wordt toegeschreven aan de groep CryptoChameleon, bekend van eerdere aanvallen op cryptoplatforms zoals Binance en Coinbase. Nieuw aan deze aanval is dat ook passkeys worden misbruikt via domeinen als mypasskey[.]info en passkeysetup[.]com. De actie toont een toenemende verschuiving van cybercriminelen naar phishingcampagnes die zich richten op wachtwoordloze authenticatie.

Nepagenten vermoedelijk betrokken bij dood 80-jarige vrouw in Nieuw West

De recherche vermoedt dat twee verdachten, aangehouden in verband met de gewelddadige dood van een 80-jarige vrouw uit Nieuw West, zich hebben voorgedaan als politieagenten om toegang tot haar woning te krijgen. Het slachtoffer werd op 13 augustus gevonden na zorgwekkend uitblijven van contact met haar bekenden. De politie startte direct een grootschalig onderzoek, wat leidde tot de aanhouding van drie personen, waarvan de vrouw later werd vrijgelaten. De recherche vermoedt dat de vrouw telefonisch werd benaderd door een man die zich als agent voordeed. Kort daarna zou een andere man als ‘agent’ bij haar zijn aangekomen en zich naar binnen hebben gepraat. Waarschijnlijk heeft de vrouw doorgehad dat er iets niet klopte, waarna de confrontatie met de nepagent escaleerde. Er wordt nu actief gewaarschuwd voor deze vorm van oplichting.

Privacy First waarschuwt voor risico's Europese digitale ID in Brussel

Privacy First heeft de Europese Commissie gewaarschuwd voor de risico’s van overidentificatie met de geplande Europese digitale identiteit (EUDI). De stichting maakt zich zorgen over de afhankelijkheid van Amerikaanse techbedrijven voor de implementatie van deze digitale ID, die volgens de Commissie in de toekomst burgers in de hele EU moet kunnen identificeren. Privacy First pleit ervoor dat de Europese Commissie eist dat het gebruik van de EUDI altijd vrijwillig blijft en alleen plaatsvindt wanneer er een onderbouwde noodzaak is. Daarnaast moet de identiteit toegankelijk zijn op apparaten met Europese besturingssystemen om digitale afhankelijkheid van niet-Europese bedrijven te voorkomen. De stichting vraagt verder om strengere eisen voor private partijen die betrokken zijn bij het beheer van de EUDI, om conflicterende commerciële belangen, zoals die van grote techbedrijven, uit te sluiten.

Datalek bij softwareleverancier luchthavens via gestolen ftp-wachtwoord uit 2022

Een belangrijke softwareleverancier voor Europese luchthavens, Collins Aerospace, werd vorige maand aangevallen door twee ransomwaregroepen. De aanvallers maakten gebruik van een ftp-wachtwoord dat in 2022 via infostealer-malware was gestolen. Dit wachtwoord werd op 10 september 2025 gebruikt door de

ransomwaregroep Everest om toegang te krijgen tot de systemen van Collins Aerospace. De aanvallers claimen 1,5 miljoen passagiersrecords en gegevens van duizenden medewerkers te hebben gestolen. De aanval resulteerde in vluchtannuleringen op luchthavens die gebruikmaken van de software van het bedrijf. Hudson Rock, het securitybedrijf dat de aanval onderzocht, meldde dat de ransomwaregroep Everest geen ransomware gebruikte, maar dat er een andere aanval plaatsvond die wel ransomware betrof. Collins Aerospace heeft geen verdere details gedeeld over de aanval met ransomware.

Europese Commissie waarschuwt Meta over schadelijke inhoud op Facebook en Instagram

De Europese Commissie heeft Meta aangeklaagd voor onvoldoende actie tegen schadelijke berichten op Facebook en Instagram. Meta maakt het voor gebruikers te moeilijk om illegale inhoud te melden, zoals berichten over seksueel misbruik en terrorisme. Dit is in strijd met de Digital Services Act, die bedrijven verplicht om het melden van illegale inhoud eenvoudig te maken en snel te reageren. De Commissie heeft ook kritiek op het gebrek aan transparantie bij Meta en TikTok, waarbij onderzoekers niet genoeg toegang krijgen tot openbare gegevens. Als Meta en TikTok niet voldoen aan de eisen, kunnen ze boetes van maximaal 6% van hun wereldwijde jaaromzet verwachten. De Commissie heeft de bedrijven de kans gegeven om te reageren en de overtredingen te verhelpen.

It-leverancier aansprakelijk voor schade door gehackte Azure-omgeving

Een it-leverancier uit Friesland is door de rechtbank Noord-Nederland aansprakelijk gesteld voor de schade van meer dan 800.000 euro die het gevolg is van een gehackte Azure-omgeving. Het incident vond plaats in 2021, toen een cybercrimineel inbrak op de cloudomgeving van de klant van de it-leverancier. Door het uitschakelen van multifactorauthenticatie (MFA) kon de aanvaller de servers gebruiken voor cryptomining, wat resulteerde in hoge kosten. De rechtbank oordeelde dat de it-leverancier verantwoordelijk is voor de schade, omdat MFA niet was ingeschakeld, ondanks eerdere waarschuwingen van de ict-distributeur. De schade werd uiteindelijk door de it-leverancier geregeld met de distributeur, maar de verzekeraar dekte de schade niet. De rechter wees alle vorderingen van de it-leverancier af en verplichtte het bedrijf om ook de proceskosten van 39.000 euro te betalen.