Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

24-10-2025:

Omrin heeft nog steeds last van ransomware-aanval, datalek ontdekt

De Friese afvalverwerker Omrin ondervindt nog steeds hinder van de ransomware-aanval die het bedrijf op 13 oktober trof. Als gevolg van de aanval werkte de Omrin Afvalapp tijdelijk niet, waardoor afvalkalenders niet beschikbaar waren. De kalender is inmiddels weer op de website geplaatst. De aanval leidde ook tot de tijdelijke sluiting van kringloopwinkels en de onbereikbaarheid van de klantenservice, die recentelijk weer operationeel is. De gemeente Het Hogeland heeft daarnaast een waarschuwing uitgegeven over een datalek bij Omrin, waarbij mogelijk persoonsgegevens onbedoeld toegankelijk zijn geworden voor onbevoegden. Het onderzoek naar de oorzaak van het datalek en de details ervan zijn momenteel nog gaande. De ransomware-aanval heeft geen invloed gehad op de afvalinzameling, die doorgaat op de gebruikelijke dagen.

Criminelen publiceren gegevens Albert Heijn-medewerkers op internet

Criminelen hebben duizenden persoonsgegevens van Albert Heijn-medewerkers gestolen en op internet gepubliceerd. De gegevens werden buitgemaakt bij Bun, de grootste franchisenemer van Albert Heijn, en bevatten onder andere personeelsdossiers, kopieën van paspoorten, salarisgegevens, medische informatie en bankgegevens. Het betreft zowel huidige als voormalige medewerkers. De ransomwaregroep ThreeAM wordt verantwoordelijk gehouden voor de aanval, die op 13 oktober begon. Bun exploiteert meer dan 25 supermarkten van Albert Heijn in Nederland. Ook de persoonlijke gegevens van de eigenaren van Bun, waaronder paspoortkopieën en financiële documenten, zijn gepubliceerd. Bun heeft nog niet gereageerd op het datalek en het is onduidelijk hoe de aanvallers toegang kregen tot de gegevens. Dit incident volgt een eerdere aanval waarbij ook gegevens van Albert Heijn-medewerkers werden gestolen.

Noord-Korea steelt miljarden door cyberaanvallen en valse identiteiten

Noord-Koreaanse hackers hebben miljarden dollars gestolen door in te breken op cryptocurrency-exchanges en valse identiteiten te creëren om op afstand technische banen bij buitenlandse bedrijven te verkrijgen. Deze activiteiten worden uitgevoerd om het nucleaire wapenprogramma van het land te financieren, volgens een

internationaal rapport over Noord-Korea's cybercapaciteiten. De cyberaanvallen hebben zich gericht op buitenlandse bedrijven en organisaties, waarbij malware werd gebruikt om netwerken te verstoren en gevoelige gegevens te stelen. Het rapport geeft aan dat Noord-Korea, ondanks zijn kleine omvang, grote investeringen heeft gedaan in offensieve cybercapaciteiten en nu een bedreiging vormt voor buitenlandse overheden, bedrijven en individuen. Noord-Korea heeft ook cryptocurrency gebruikt om geld wit te wassen en militaire aankopen te doen, waarmee het probeert de internationale sancties te omzeilen die het land opgelegd zijn vanwege zijn nucleaire programma.

Iraanse hackers richten zich op meer dan 100 overheidsorganisaties met Phoenix-backdoor

De Iraanse hackergroep MuddyWater, ook wel bekend als Static Kitten, Mercury en Seedworm, heeft meer dan 100 overheidsinstellingen aangevallen met de Phoenix-backdoor. Deze groep richt zich voornamelijk op overheids- en particuliere organisaties in het Midden-Oosten. De aanvallen begonnen op 19 augustus met een phishingcampagne, waarbij kwaadaardige e-mails werden verzonden met besmette Word-documenten. Het document bevatte een VBA-macro die de 'FakeUpdate'-loader op de systemen installeerde, wat leidde tot de invoering van versie 4 van de Phoenix-backdoor. De malware verzamelt systeeminformatie, maakt verbinding met een command-and-controlserver en stelt aanvallers in staat om bestanden te downloaden, up te daten en gegevens te exfiltreren. MuddyWater gebruikte ook een aangepaste infostealer om gegevens van webbrowsers zoals Chrome, Opera en Edge te stelen. De aanvallen zijn duidelijk gelinkt aan de groep door de gebruikte technieken en doelwitten.

Nieuwe documentaire biedt ongecensureerd inzicht in moderne cyberoorlog

De documentaire "Midnight in the War Room," geproduceerd door Semperis, biedt een diepgaand kijkje in de hedendaagse cyberoorlog tussen nationale staten, criminele groepen en verdedigers. De film, die in 2026 zal verschijnen, belicht de menselijke kant van cyberoorlog, met getuigenissen van experts zoals Grace Cassy, voormalig Brits diplomaat, en voormalig CIA-directeur David Petraeus. De documentaire werpt een licht op de impact van cyberdreigingen op economieën en samenlevingen, en benadrukt de constante dreiging voor vitale infrastructuren zoals

water- en energiesystemen. Ook de versnelling van AI, quantumtechnologie en biotech wordt besproken in relatie tot cyberverdediging. De film biedt een belangrijk perspectief op de technologische innovaties en de groeiende dreigingen vanuit zowel staatsactoren als criminele groepen. De productie heeft tot doel het bewustzijn over de ernst van cyberdreigingen te vergroten.

Transparenttribe richt zich op militaire organisaties met DeskRAT

In oktober 2025 werd de cyberespionagecampagne van de groepering TransparentTribe geanalyseerd, die gericht was op Indiase militaire organisaties. De aanval begon met een phishingcampagne, gevolgd door het verspreiden van DeskRAT, een op Golang gebaseerde Remote Access Trojan (RAT). Het kwaadaardige bestand werd verspreid via een ZIP-archief, dat een DESKTOP-bestand bevatte. Bij uitvoering downloadde het bestand een bas64-gecodeerd payload en installeerde DeskRAT, dat via een WebSocket-verbinding met een command-and-control-server (C2) communiceerde. DeskRAT bevat verschillende functies, waaronder het verzamelen van bestanden, het uitvoeren van opdrachten en het onderhouden van persistentie via meerdere technieken. De aanval was gericht op het BOSS-besturingssysteem, dat veel gebruikt wordt door de Indiase overheid. De geïnfecteerde documenten bevatten valse informatie over militaire operaties en werden gebruikt als lokmiddel om de slachtoffers te misleiden.

Adobe waarschuwt voor misbruik van kwetsbaarheid in webwinkels

Adobe heeft webwinkels die gebruikmaken van Adobe Commerce en Magento Open Source gewaarschuwd voor actief misbruik van een kritieke beveiligingskwetsbaarheid (CVE-2025-54236). Aanvallers kunnen via deze kwetsbaarheid volledige controle krijgen over de webshop. Ondanks een beveiligingsupdate van 9 september, heeft bijna twee derde van de webwinkels de update nog niet geïnstalleerd. De kwetsbaarheid, die wordt omschreven als een "security feature bypass", kan volgens sommige experts ook leiden tot remote code execution. Proof-of-concept exploitcode is inmiddels beschikbaar op internet en er zijn al actieve aanvallen gaande. Het securitybedrijf Sansec verwacht dat binnen 48 uur grootschalig misbruik zal plaatsvinden. Webshops wordt dringend aangeraden de update onmiddellijk te installeren om aanvallen te voorkomen.

Lek in FIA-portaal gaf onderzoekers toegang tot paspoort Max Verstappen

Beveiligingsonderzoekers ontdekten een kwetsbaarheid in een portaal van de FIA waarmee ze toegang kregen tot persoonlijke gegevens van Formule 1-coureurs, waaronder Max Verstappen. Via het portaal konden de onderzoekers zich als administrator aanmelden en persoonlijke informatie zoals paspoortgegevens, e-mailadressen, wachtwoordhashes en telefoonnummers inzien. Het probleem werd in juni 2025 ontdekt en de onderzoekers informeerden de FIA, die het portaal direct offline haalde en binnen drie dagen een oplossing implementeerde. De onderzoekers stopten met hun onderzoek nadat ze toegang hadden gekregen tot Verstappen's paspoort en besloten geen verdere gegevens te gebruiken. De kwetsbaarheid is inmiddels verholpen.

Google test opnieuw maatregel in Chrome om cookiediefstal te voorkomen

Google voert deze maand een tweede test uit met Device Bound Session Credentials (DBSC) in de Chrome-browser, een maatregel die moet helpen bij het voorkomen van cookiediefstal door malware. In eerdere tests werd DBSC geïntroduceerd om sessiecookies, die toegang geven tot gebruikersaccounts, te beschermen. De nieuwe methode koppelt een sessie aan het apparaat van de gebruiker, waardoor gestolen cookies alleen op het apparaat kunnen worden gebruikt waar ze zijn aangemaakt. Dit voorkomt dat aanvallers toegang krijgen tot accounts zonder wachtwoorden of tweefactorauthenticatie. DBSC maakt gebruik van een public/private key pair en gebruikt de Trusted Platform Module (TPM) van de computer voor beveiliging. Google heeft aangekondigd dat de test beschikbaar is voor Windowscomputers met een TPM en doorgaat tot maart 2026. Gebruikers kunnen zich aanmelden om deel te nemen aan de test.

CISA waarschuwt voor kwetsbaarheid in Lanscope Endpoint Manager die wordt misbruikt in aanvallen

De Cybersecurity & Infrastructure Security Agency (CISA) heeft een waarschuwing uitgebracht over een kritieke kwetsbaarheid in de Motex Lanscope Endpoint Manager, een hulpmiddel voor het beheer en de beveiliging van eindpunten. De kwetsbaarheid, aangeduid als CVE-2025-61932, heeft een CVSS-score van 9,3 en is te wijten aan een onjuiste verificatie van de herkomst van inkomende verzoeken. Deze fout kan door aanvallers zonder authenticatie worden misbruikt om willekeurige

code op systemen uit te voeren via speciaal gevormde pakketten. Motex, de ontwikkelaar van het product, bevestigde dat sommige klantomgevingen al getroffen zijn door deze aanvallen, wat duidt op een exploitatie van de kwetsbaarheid als een zero-day. De kwetsbaarheid beïnvloedt Lanscope Endpoint Manager versies 9.4.7.2 en lager. Er zijn updates beschikbaar die de kwetsbaarheid verhelpen, en klanten worden aangespoord om deze zo snel mogelijk te installeren.

Kwetsbaarheden in DNS-software kunnen cache poisoning aanvallen opnieuw mogelijk maken

Twee kwetsbaarheden in DNS-resolversoftware, BIND en Unbound, kunnen aanvallers in staat stellen om DNS-caches te vergiftigen en gebruikers naar kwaadaardige bestemmingen te sturen. De kwetsbaarheden, aangeduid als CVE-2025-40778 en CVE-2025-40780, ontstaan door een logische fout en een zwakte in het genereren van pseudo-willekeurige nummers. Deze kwetsbaarheden hebben een ernstclassificatie van respectievelijk 8.6 voor BIND en 5.6 voor Unbound. De BIND-kwetsbaarheden kunnen het mogelijk maken om resultaten te vervalsen, wat kan leiden tot herhaalde cache poisoning-aanvallen. Hoewel de impact minder ernstig is dan de aanvallen uit 2008, kunnen de kwetsbaarheden wel schade veroorzaken in bepaalde omgevingen. Patches zijn inmiddels beschikbaar en het wordt aangeraden deze snel toe te passen.

PoC voor SysAid PreAuth RCE-keten

Een proof of concept (PoC) is gepubliceerd voor een pre-authentication remote code execution (RCE) kwetsbaarheid in SysAid. Deze kwetsbaarheid is gekoppeld aan de CVE-nummers CVE-2025-2775, CVE-2025-2776, CVE-2025-2777 en CVE-2025-2778. De PoC, ontwikkeld door Watchtower Labs, toont aan hoe aanvallers zonder authenticatie een RCE-aanval kunnen uitvoeren, wat mogelijk leidt tot volledige controle over getroffen systemen. Er zijn gedetailleerde documenten beschikbaar die uitleggen hoe de aanval werkt, samen met een GitHub-pagina voor de PoC-code en een uitgebreide write-up die de technische aspecten van de exploit beschrijft.

Waarschuwing: Meerdere kwetsbaarheden in SAUTER modulo-apparaten, patch onmiddellijk!

Er zijn meerdere ernstige kwetsbaarheden ontdekt in SAUTER modulo-apparaten die kunnen worden misbruikt door aanvallers met netwerktoegang. Deze kwetsbaarheden kunnen leiden tot verhoogde privileges, de mogelijkheid om willekeurige commando's uit te voeren op de apparaten en compromitteren van de integriteit, beschikbaarheid en vertrouwelijkheid van de systemen. De kwetsbaarheden bevinden zich in de embedded webserver en de SAUTER CASE Suite interface. Ze omvatten onder andere de mogelijkheid om bestanden naar willekeurige locaties te uploaden, het versturen van onvolledige SOAP-berichten die de server kunnen laten crashen, en het misbruiken van hard-coded certificaten. Aanbevolen wordt om onmiddellijk de beschikbare updates te installeren, aangezien deze de apparaten tegen toekomstige aanvallen beschermen. Organisaties wordt daarnaast aangeraden de monitoringcapaciteiten te verbeteren en verdachte activiteiten snel te detecteren.

Meerdere BIND 9 DNS-kwetsbaarheden kunnen leiden tot cache poisoning of DoS-aanvallen, patch onmiddellijk!

De Internet Systems Consortium (ISC) heeft drie ernstige kwetsbaarheden (CVE-2025-8677, CVE-2025-40778, CVE-2025-40780) ontdekt in BIND 9. Deze kwetsbaarheden kunnen worden misbruikt door een aanvaller om cache poisoning of denial-of-service (DoS) aanvallen uit te voeren tegen getroffen DNS-resolvers. Hoewel er momenteel geen meldingen zijn van actieve exploitatie, vormt dit een groot risico voor netwerken gezien de kritieke rol van DNS. CVE-2025-8677 kan leiden tot CPU-overbelasting door verkeerd geformatteerde DNSKEY-records, terwijl CVE-2025-40778 het mogelijk maakt om vervalste DNS-records in de cache te injecteren. CVE-2025-40780 is gerelateerd aan een zwakte in de Pseudo Random Number Generator (PRNG), die door een aanvaller kan worden misbruikt voor DNS-cache poisoning.

Europese defensiebedrijven doelwit van aanvallen met malafide vacatures

Europese defensiebedrijven, met name die betrokken bij de ontwikkeling van drone-onderdelen, zijn het doelwit geworden van aanvallen waarbij malafide vacatures worden gebruikt. De aanvallers, vermoedelijk gelieerd aan de Noord-Koreaanse groep Lazarus, sturen zogenaamde topfunctie-vacatures naar medewerkers van de bedrijven. De vacatures bevatten een trojaanse versie van de MuPDF reader, die bij

openen malware op het systeem installeert. Het doel van de aanvallen lijkt te zijn het stelen van informatie over de betrokken defensie- en luchtvaarttechnologieën. ESET, dat de aanval analyseerde, waarschuwt dat de Lazarus-groep vaker betrokken is bij aanvallen op de defensiesector. De groep heeft een geschiedenis van het uitvoeren van cyberaanvallen gericht op strategisch belangrijke bedrijven.

Valse AI-zijkanten misleiden gebruikers van Atlas en Comet browsers

Onderzoekers van SquareX hebben een kwetsbaarheid ontdekt in de Atlas- en Comet-browsers van OpenAI en Perplexity. Deze browsers zijn gevoelig voor AI Sidebar Spoofing-aanvallen, waarbij een kwaadaardige extensie een nep-AI-zijkant creëert die lijkt op de echte interface. Door deze valse zijkant kunnen gebruikers misleid worden en risicovolle acties uitvoeren, zoals het downloaden van schadelijke software of het verstrekken van gevoelige gegevens. De onderzoekers demonstreren drie scenario's waarin gebruikers cryptocurrency-gegevens kunnen verliezen, hun Google-account kunnen laten kapen of een apparaat kunnen laten overnemen. De aanval kan worden uitgevoerd door JavaScript in te voegen via een extensie die weinig machtigingen vereist. Ondanks dat OpenAI en Perplexity zijn benaderd, hebben zij nog niet gereageerd. Gebruikers van deze browsers worden geadviseerd om deze tools alleen voor niet-gevoelige activiteiten te gebruiken, gezien de huidige beveiligingsrisico’s.

Microsoft schakelt previewfunctie uit in Verkenner om aanvallen te blokkeren

Microsoft heeft aangekondigd dat de previewfunctie van de Windows Verkenner automatisch wordt uitgeschakeld voor bestanden die gedownload zijn van internet. Deze wijziging is bedoeld om aanvallen te blokkeren waarbij kwaadwillenden NTLM-hashes kunnen stelen via malafide documenten. De wijziging geldt voor bestanden met het 'Mark of the Web' (MotW), wat aangeeft dat het bestand via internet is gedownload, bijvoorbeeld via een e-mailbijlage. Na het installeren van de beveiligingsupdates van oktober 2025 op Windows 11 en Windows Server, zal het proberen te openen van deze bestanden via de previewfunctie een waarschuwing tonen. Gebruikers kunnen de functie uitschakelen door bestanden handmatig te ontgrendelen, maar het is belangrijk om op te merken dat dit mogelijk niet onmiddellijk effect heeft. Deze verandering voorkomt dat aanvallers kwetsbaarheden kunnen misbruiken zonder dat de gebruiker het bestand daadwerkelijk opent.

"Jingle Thief" hackers misbruiken cloudinfrastructuur om miljoenen aan cadeaubonnen te stelen

Een cybercriminaliteitengroep genaamd Jingle Thief richt zich op cloudomgevingen van organisaties in de detailhandel en consumentenservice om cadeaubonfraude te plegen. De aanvallers gebruiken phishing en smishing om inloggegevens te stelen en verkrijgen toegang tot systemen die cadeaubonnen uitgeven. Zodra toegang is verkregen, gebruiken ze deze toegang om ongeautoriseerde cadeaubonnen uit te geven en deze waarschijnlijk door te verkopen op grijze markten. Het gebruik van cadeaubonnen is lucratief, omdat ze eenvoudig te verzilveren zijn met weinig persoonlijke informatie en moeilijk te traceren zijn. Jingle Thief, die al actief is sinds eind 2021, heeft het vermogen om langdurig toegang te behouden tot de cloudomgevingen van de doelwitten en zich onopgemerkt door deze systemen te bewegen. De groep voert gerichte phishing-aanvallen uit om toegang te krijgen tot Microsoft 365-omgevingen, waarna ze uitgebreide verkenning doen naar systemen die cadeaubonnen uitgeven.

YouTube Ghost Network verspreidt malware via duizenden video's

Check Point Research heeft het YouTube Ghost Network ontdekt, een geavanceerd netwerk van kwaadwillende accounts dat gebruik maakt van YouTube-functies om malware te verspreiden. Dit netwerk is sinds 2021 actief en heeft meer dan 3.000 schadelijke video's geüpload, vooral gericht op de categorieën "Game Hacks/Cheats" en "Software Cracks/Piracy". In 2025 is het aantal video's significant toegenomen. De video's bevatten links naar kwaadaardige software die vaak wordt gepromoot met positieve reacties en likes, wat een valse indruk van betrouwbaarheid wekt. Malware zoals infostealers, waaronder Rhadamanthys, werd veelvuldig verspreid. Het netwerk maakt gebruik van verschillende YouTube-accounts met specifieke rollen, zoals video's uploaden, berichten posten en interactie met kijkers. Deze aanpak maakt detectie moeilijker en vergroot de verspreiding van malware. Google heeft al meer dan 3.000 video's verwijderd, maar de voortdurende groei van dit netwerk benadrukt de noodzaak van voortdurende waakzaamheid.

hackers misbruiken oauth-applicaties voor doorlopende cloudtoegang na wachtwoordreset

Cybercriminelen maken gebruik van kwetsbaarheden in OAuth-applicaties om blijvende toegang te krijgen tot cloudomgevingen, zelfs na een wachtwoordreset. Deze aanvallen richten zich specifiek op Microsoft Entra ID-omgevingen, waarbij aanvallers gebruikersaccounts overnemen, gevoelige gegevens exfiltreren en vervolgaanvallen lanceren. Het gevaar van deze aanvallen ligt in het feit dat aanvallers interne applicaties kunnen registreren die toegang hebben tot essentiële bedrijfsbronnen zoals e-mail, documenten en Teams-berichten. Traditionele beveiligingsmaatregelen zoals wachtwoordherstel en multifactor-authenticatie bieden geen bescherming tegen deze aanvallen, aangezien de kwaadwillende applicaties hun toegang behouden, ongeacht wijzigingen in gebruikersreferenties. Beveiligingsonderzoekers hebben geconstateerd dat deze aanvallen vaak beginnen met phishingaanvallen, waarna de aanvallers interne applicaties creëren die moeilijk te detecteren zijn. Dit vergroot de kans op langdurige en onopgemerkte aanvallen.

83 arrestaties in Afrikaanse operatie tegen terrorismefinanciering

In een grootschalige operatie, gecoördineerd door INTERPOL en AFRIPOL, zijn 83 personen gearresteerd in zes Afrikaanse landen vanwege hun betrokkenheid bij terrorismefinanciering en de illegale activiteiten die deze ondersteunen. De operatie, genaamd Operation Catalyst, richtte zich op het verstoren van financiële netwerken die verband houden met terrorisme. Van de arrestanten waren 21 betrokken bij terrorisme-gerelateerde misdrijven, 28 bij financiële fraude en witwassen, 16 bij cyber-enabled oplichting en 18 bij het illegaal gebruik van virtuele valuta. De operatie leidde tot de ontdekking van ongeveer 260 miljoen dollar in fiat en virtuele valuta, met inbeslagnames van 600.000 dollar en de bevriezing van 60 bankrekeningen. De operatie toont de complexe en vaak grensoverschrijdende aard van terrorismefinanciering, waarbij verschillende vormen van criminaliteit, zoals fraude en online oplichting, met elkaar verweven zijn.

AP wijst organisaties op verplichte AI-geletterdheid bij personeel

De Autoriteit Persoonsgegevens (AP) heeft organisaties gewaarschuwd dat zij verplicht zijn om het personeel AI-geletterd te maken. AI-geletterdheid is niet alleen een wettelijke vereiste, maar ook een belangrijke voorwaarde voor het verantwoord gebruik van AI en algoritmes. Organisaties moeten ervoor zorgen dat hun medewerkers beschikken over de juiste kennis en vaardigheden om AI-systemen

verantwoord te gebruiken. De AP benadrukt dat dit ook geldt voor externe partijen die namens organisaties AI inzetten. Organisaties moeten hun aanpak documenteren en de voortgang bijhouden. De AP heeft een handreiking gepubliceerd waarin stappen worden beschreven voor het verbeteren van AI-geletterdheid, waaronder het identificeren van gebruikte AI-systemen, het stellen van concrete doelen en het implementeren van strategieën zoals trainingen. De AP zal de voortgang op dit gebied de komende maanden monitoren door middel van gerichte uitvragen bij Nederlandse organisaties.

Gaming Copilot in Windows 11 roept zorgen op over privacy en beveiliging

De Gaming Copilot van Microsoft, die momenteel wordt uitgerold binnen Windows 11, is volgens de Britse beveiligingsonderzoeker Kevin Beaumont niet in staat een eenvoudige privacytest te doorstaan. De functie maakt gebruik van Copilot Vision, dat via kunstmatige intelligentie analyseert wat gebruikers tijdens het gamen doen en daar advies op baseert. Beaumont ontdekte dat de software zonder melding wordt geïnstalleerd en automatisch screenshots verzamelt van het scherm, inclusief symbolen en teksten. Deze gegevens worden deels via de cloud verwerkt en gebruikt om Microsofts AI-modellen te trainen en gerichte advertenties te tonen. Zelfs wanneer de Copilot in de Game Bar wordt uitgeschakeld, blijft er dataverkeer actief. De onderzoeker waarschuwt dat deze functie een nieuw aanvalsoppervlak aan Windows 11 toevoegt en pleit voor meer transparantie, gebruikerskeuze en een duidelijke onboardingprocedure voor het gebruik van de tool.

Crypto-swaps op Dark Web via CypherGoat platform

Op 22 oktober 2025 werd een bericht gedeeld waarin CypherGoat werd gepromoot, een platform dat anonieme crypto-swaps aanbiedt via verschillende netwerken, waaronder Clearnet, Onion (via Tor) en I2P. Het platform stelt gebruikers in staat om cryptocurrencies te verhandelen tegen de beste tarieven met nadruk op snelheid, privacy en open-source functionaliteit. Gebruikers kunnen via een Clearnet-website of via de versleutelde netwerken Tor en I2P toegang krijgen tot het platform. Dit soort diensten blijft populair binnen de darkwebgemeenschap vanwege hun focus op privacy en de mogelijkheid om traditionele financiële systemen te omzeilen.

Valse telefoontjes over ‘thuisbatterij’ leiden tot oplichting

Er zijn meldingen van valse telefoontjes waarin oplichters zich voordoen als verkopers van thuisbatterijen. Tijdens het gesprek wordt een offertebespreking aangeboden, maar meteen wordt gevraagd om een borgsom van 250 euro te betalen om te voorkomen dat de adviseur voor een dichte deur staat. Na betaling wordt vaak een vervolgtelefoontje ontvangen, waarin wordt gesteld dat men akkoord heeft gegeven voor een lening. Wie het betaalde bedrag terugvraagt, krijgt een dreigend telefoontje waarin wordt aangegeven dat het geld niet wordt teruggegeven. In sommige gevallen wordt de naam van Flanderijn Gerechtsdeurwaarders misbruikt om te dreigen met beslaglegging. De Fraudehelpdesk waarschuwt dat mensen die zulke telefoontjes ontvangen, direct de verbinding moeten verbreken en nooit betalen. Ook wordt aangeraden contact op te nemen voor advies als er al betaald is.

Rusland dwingt Apple om Russische zoekmachine in te stellen als standaard

Rusland heeft de federale anti-monopoliedienst (FAS) opgedragen om Apple te verplichten een Russische zoekmachine, zoals Yandex of Mail.ru, als standaard in te stellen op alle Apple-apparaten die in Rusland of de Euraziatische Economische Unie (EAEU) worden verkocht. Volgens een brief van FAS-directeur Maxim Shaskolsky, die werd verkregen door het staatsnieuwsagentschap TASS, schendt Apple de consumentenbeschermingsregels. Deze regels verplichten elektronische apparaten om een zoekmachine uit Rusland of een ander EAEU-land vooraf geïnstalleerd te hebben. Apple is volgens de FAS momenteel in strijd met deze regels door een niet-EAEU-zoekmachine als standaard in te stellen, wat volgens Rusland leidt tot ongelijke concurrentie voor lokale zoekmachines. Apple heeft tot 31 oktober om aan de eisen van de toezichthouder te voldoen, anders volgen er boetes. Het Russische ministerie van Digitale Zaken waarschuwde Apple voor "ernstige gevolgen" bij niet-naleving.