Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

16-10-2025:

Nieuwe hacktivistische alliantie aangekondigd door NoName057(16) en AnonGhost Official

NoName057(16) en AnonGhost Official hebben officieel een nieuwe alliantie aangekondigd. Beide hacktivistische groepen, die bekendstaan om hun cyberaanvallen op overheidsinstellingen en kritieke infrastructuren, bundelen hun krachten. De alliantie wordt als een nieuwe stap in de wereld van hacktivisme gepresenteerd, waarbij beide groepen hun activiteiten en middelen delen. Deze samenwerking kan leiden tot een intensivering van cyberaanvallen die gericht zijn op zowel nationale als internationale doelen. De betrokkenheid van deze groepen kan de complexiteit van geopolitieke spanningen en digitale dreigingen verder vergroten, aangezien hacktivisten steeds meer invloed uitoefenen in de digitale strijd. Het is nog niet duidelijk welke specifieke doelen deze alliantie zal gaan aanvallen, maar de bekendmaking is een waarschuwing voor een mogelijke opschaling van cyberactiviteiten.

Strategisch directeur Amsterdamse onderneming had zakelijke banden met Telegram en FSB

Vladimir V. en Aleksei Z., twee Russische ondernemers, werkten met hun bedrijf GlobalNet in Amsterdam, dat onder andere Telegram-servers beheerde. Het bedrijf heeft sinds 2016 telecomdiensten geleverd aan Voentelekom, een provider van het Russische leger, en sinds 2024 aan een onderzoeksinstituut voor kernenergie. In hun functie hebben zij zakelijke contacten onderhouden met de Russische geheime dienst, de FSB. Terwijl ze ontkennen Europese sancties te hebben geschonden, blijkt uit onderzoek dat het bedrijf mogelijk in strijd is met de wetgeving door zaken te doen met gesanctioneerde Russische bedrijven. Telegram heeft ontkend ooit zaken te hebben gedaan met GlobalNet, maar bevestigt dat het bedrijf in het verleden wel telecomdiensten voor Telegram heeft geleverd. Vladimir V. beweert dat hij nooit toegang heeft gehad tot gebruikersdata van Telegram. Dit alles komt naar voren in een BNR-onderzoek, waarbij vragen rijzen over de rol van Nederlandse bedrijven in deze activiteiten.

Mysterious Elephant APT: Geavanceerde aanvallen gericht op overheidsinstellingen

Mysterious Elephant is een geavanceerde bedreigingsgroep die sinds 2023 actief is en zich richt op overheidsinstellingen en diplomatieke sectoren in de Aziatisch-Pacifische regio. De groep maakt gebruik van op maat gemaakte en open-source tools, zoals BabShell en MemLoader, om gevoelige informatie te stelen. De recente campagnes, gestart in 2025, tonen een verschuiving in hun technieken, waarbij ze spear phishing en kwaadaardige documenten gebruiken om toegang te krijgen. Een opvallend aspect van hun aanvallen is het gebruik van WhatsApp-specifieke exfiltratie-tools, waarmee ze documenten, afbeeldingen en andere gevoelige gegevens van besmette systemen stelen. De groep is bijzonder gericht op landen zoals Pakistan, Bangladesh en Sri Lanka, waarbij ze specifieke slachtofferorganisaties aanvallen met op maat gemaakte malware. Gezien de geavanceerde methoden en het constante aanpassingsvermogen, blijft Mysterious Elephant een belangrijke bedreiging voor de nationale veiligheid.

Pro-Russische hacktivistengroep valt overheidsportalen, financiële diensten en e-commerce aan

Op 7 oktober 2025 lanceerde een pro-Russische hacktivistengroep een grootschalige cyberaanval gericht op Israël en geallieerde landen. De campagne omvatte 57 gecoördineerde DDoS-aanvallen in één dag, een recordaantal vergeleken met de maand ervoor. De aanval was het hoogtepunt van een bredere strategie, waarbij verschillende hacktivistengroepen samenwerkten, waaronder Arabian Ghosts, Keymous+, OpIsrael, en NoName057(16). Deze samenwerking tussen verschillende ideologische groeperingen benadrukte de grenzen die vervagen in cyberoorlogvoering. De aanvallen richtten zich op overheidswebsites, financiële instellingen en e-commerceplatforms, maar ook op sectoren zoals onderwijs, gezondheidszorg, productie en retail. De aanvallers gebruikten geavanceerde propaganda- en coördinatietools, waaronder Telegram en sociale media, om aanvallen te orkestreren en de zichtbaarheid te vergroten. Dit weerspiegelt een toenemende verfijning van de tactieken en het gebruik van vrijwilligersnetwerken voor de uitvoering van de cyberaanvallen.

Oekraïense cyberaanval kost Russische provider meer dan 66 miljoen roebel

De Oekraïense inlichtingendienst HUR heeft opnieuw een cyberaanval uitgevoerd op de Russische internetprovider Orion Telecom, waarbij de schade meer dan 66

miljoen roebel (ongeveer $840.000) bedraagt. Het incident vond plaats als onderdeel van een bredere campagne door HUR om de digitale infrastructuur van Rusland te verstoren. De aanval leidde tot een datalek, waarbij persoonlijke gegevens van gebruikers werden blootgesteld. Orion Telecom had eerder een klacht ingediend bij de Russische politie en vroeg om een strafrechtelijk onderzoek. De cyberoperatie werd in juni al ingezet, en sinds die tijd zijn verschillende systemen van de provider verstoord, met als gevolg uitval van internet en televisie in meerdere regio's, waaronder een gesloten stad die gespecialiseerd is in uraniumwinning. HUR heeft ook andere Russische netwerken en platforms aangevallen in eerdere operaties, wat de voortdurende digitale strijd tussen de twee landen weerspiegelt.

Microsoft verhelpt drie actief aangevallen kwetsbaarheden in Windows

Op de patchdinsdag van oktober heeft Microsoft 177 kwetsbaarheden verholpen, waaronder drie die actief werden aangevallen. Twee van deze kwetsbaarheden kunnen door een aanvaller, die al toegang heeft tot een systeem, worden misbruikt om zijn rechten te verhogen. De derde kwetsbaarheid maakt het mogelijk voor een aanvaller met fysieke toegang tot een systeem om Secure Boot in IGEL OS 10 te omzeilen. Van de 177 verholpen kwetsbaarheden zijn er zestien als kritiek aangemerkt, waarbij de drie gevaarlijkste CVE-2025-59246, CVE-2025-59287 en CVE-2025-49708 zijn. De impact van deze kwetsbaarheden varieert van 9.8 tot 9.9 op een schaal van 1 tot 10. Microsoft verwacht dat aanvallers de kwetsbaarheden zullen gaan misbruiken, maar de updates worden automatisch geïnstalleerd op de meeste systemen.

Microsoft patcht 6 zerodays en 172 kwetsbaarheden in oktober update

Op de Patch Tuesday van oktober 2025 heeft Microsoft 172 kwetsbaarheden verholpen, waaronder zes zeroday kwetsbaarheden. Deze zerodays waren actief uitgebuit en betroffen onder andere Windows SMB Server en Microsoft SQL Server. Daarnaast zijn er acht "kritieke" kwetsbaarheden opgelost, waarvan vijf betrekking hadden op remote code execution (RCE) en drie op privilege escalation. De update omvatte ook fixen voor 80 kwetsbaarheden met verhoogde privileges, 11 beveiligingsfeature-bypassproblemen, 28 voor informatielekken, en 10 voor spoofing. Microsoft waarschuwt dat de ondersteuning voor Windows 10 eindigt, waardoor gebruikers van dit besturingssysteem aanvullende beveiligingsupdates moeten

aanvragen. Gebruikers die gebruik maken van Azure en andere Microsoft-diensten worden eveneens aangespoord om de nieuwste patches te implementeren om hun systemen te beschermen tegen aanvallen.

Zes zerodays opgelost in oktober Patch Tuesday

De oktober Patch Tuesday van Microsoft lost zes belangrijke zeroday kwetsbaarheden op in Windows en Microsoft SQL Server. Twee van deze kwetsbaarheden waren publiekelijk bekend. Een van de gepatchte kwetsbaarheden is CVE-2025-24990, een probleem met de Agere Modem driver in Windows, dat werd misbruikt om administratieve rechten te verkrijgen. Microsoft verwijdert de driver in de cumulatieve update van oktober, wat leidt tot het niet functioneren van faxmodemhardware. Een andere kwetsbaarheid betreft CVE-2025-59230, die aanvallers in staat stelde om systeemrechten te verkrijgen via Windows Remote Access Connection Manager. Verder werden er beveiligingsupdates uitgebracht voor een Secure Boot-bypass in IGEL OS, en kwetsbaarheden in AMD-processor en TCG TPM2.0-implementaties. De meeste kwetsbaarheden zijn actief misbruikt of openbaar gedeeld, maar Microsoft werkt aan fixes voor kwetsbaarheden die impact kunnen hebben op geheugenintegriteit en systeembeveiliging.

SAP brengt updates uit voor kritieke kwetsbaarheden in producten

SAP heeft beveiligingsupdates vrijgegeven voor twee ernstige kwetsbaarheden die invloed hebben op verschillende versies van hun software. De kwetsbaarheden, CVE-2025-42937 en CVE-2025-42910, zijn van het type directory traversal en onbeperkte bestandsoverdracht, en kunnen ernstige gevolgen hebben voor de vertrouwelijkheid, integriteit en beschikbaarheid van systemen. De eerste kwetsbaarheid, CVE-2025-42937, stelt een aanvaller in staat om systeembestanden te manipuleren door ongevalideerde padinvoer, terwijl de tweede kwetsbaarheid, CVE-2025-42910, een aanvaller in staat stelt om schadelijke bestanden te uploaden naar SAP SRM-systemen. Beide kwetsbaarheden hebben een hoge CVSS-score en moeten onmiddellijk worden gepatcht om potentiële aanvallen te voorkomen. Organisaties wordt aangeraden snel updates te installeren en verhoogde monitoring in te schakelen voor verdachte activiteiten.

ICTBroadcast-servers getroffen door cookie-exploit voor toegang tot remote shell

Een ernstige beveiligingskwetsbaarheid in ICTBroadcast, een autodialer-software van ICT Innovations, wordt actief uitgebuit. De kwetsbaarheid, met het CVE-nummer CVE-2025-2611 (CVSS-score: 9.3), wordt veroorzaakt door onvoldoende invoervalidatie, wat leidt tot ongevraagde remote code-executie. De software geeft sessiecookiedata onveilig door aan shell-processen, waardoor aanvallers shell-opdrachten kunnen injecteren in een sessiecookie en deze op de kwetsbare server kunnen uitvoeren. De kwetsbaarheid betreft ICTBroadcast-versies 7.4 en lager. Cybersecurity-onderzoekers hebben de exploitatie op 11 oktober 2025 gedetecteerd, waarbij aanvallers in twee fasen hun aanvallen uitvoerden, beginnend met een exploit-check op basis van tijd en gevolgd door pogingen om reverse shells op te zetten. Ongeveer 200 online servers zijn kwetsbaar. Momenteel is er geen informatie beschikbaar over een patch voor deze kwetsbaarheid.

Twee kritieke kwetsbaarheden in Red Lion RTU's kunnen volledige industriële controle in gevaar brengen

Onderzoekers hebben twee ernstige beveiligingsflaws ontdekt in de Red Lion Sixnet RTU-producten, die als kritieke kwetsbaarheden zijn beoordeeld met een CVSS-score van 10,0. De kwetsbaarheden, aangeduid als CVE-2023-40151 en CVE-2023-42770, stellen aanvallers in staat om zonder authenticatie toegang te krijgen en root-privileges uit te voeren. De defecten komen voor in de SixTRAK en VersaTRAK RTU's van Red Lion, die worden gebruikt in industriële systemen zoals energie-, water- en transportsectoren. De eerste kwetsbaarheid betreft een authenticatie-bypass bij communicatie via UDP en TCP, terwijl de tweede kwetsbaarheid remote code-executie mogelijk maakt via ingebouwde Linux-shell-ondersteuning. Indien succesvol uitgebuit, kan een aanvaller volledige controle krijgen over de getroffen systemen, wat ernstige gevolgen kan hebben voor de bedrijfsvoering. Gebruikers wordt geadviseerd om de patches zo snel mogelijk toe te passen en authenticatie in te schakelen.

F5 waarschuwt voor diefstal van broncode en kwetsbaarheden

F5 heeft een waarschuwing uitgegeven na de ontdekking dat aanvallers toegang kregen tot de broncode en informatie over niet bekendgemaakte kwetsbaarheden van hun BIG-IP-platform. De aanvallers, die volgens F5 een "zeer geraffineerde

statelijke actor" zijn, hadden langetermijntoegang tot de systemen van F5 en downloadden bestanden die cruciale productinformatie bevatten. Het gaat onder andere om de BIG-IP broncode en details over onbekende kwetsbaarheden in het systeem. Hoewel er geen bewijs is dat de aanvallers de software supply chain of NGINX-code hebben aangepast, werd een veiligheidsupdate voor de BIG-IP-software uitgerold en werden er maatregelen getroffen, zoals het resetten van inloggegevens en het aanscherpen van access controls. F5 benadrukt dat er geen bewijs is van actief misbruik van de kwetsbaarheden, maar waarschuwt dat aanvallers toegang kunnen krijgen tot gevoelige gegevens zoals API-sleutels en systeemtoegang.

Ivanti Endpoint Manager Mobile kwetsbaarheden: dringende patch vereist

Er zijn meerdere kwetsbaarheden ontdekt in Ivanti Endpoint Manager Mobile (EPMM), die systemen blootstellen aan mogelijke aanvallen. De kwetsbaarheden, zoals OS command injection en path traversal, kunnen door geauthenticeerde aanvallers worden misbruikt om op afstand code uit te voeren of ongewenste toegang te krijgen tot bestanden. De hoog-risico kwetsbaarheden, met CVE-2025-10242, CVE-2025-10243 en CVE-2025-10985, kunnen de vertrouwelijkheid, integriteit en beschikbaarheid van het systeem ernstig bedreigen. De kwetsbaarheid CVE-2025-10986 heeft een lager risico, maar kan aanvallers alsnog in staat stellen om gegevens naar onbedoelde locaties op de schijf te schrijven. Organisaties wordt aangeraden de laatste versie van Ivanti EPMM te installeren en hun monitoringcapaciteiten te verbeteren om ongewenste activiteiten snel te detecteren. Het installeren van de patch is essentieel om verdere exploits te voorkomen.

Waarschuwing voor meerdere kwetsbaarheden in Veeam, direct patchen vereist

Veeam Backup & Replication vertoont verschillende kritieke kwetsbaarheden die kunnen leiden tot remote code execution (RCE) en privilege-escalatie. De kwetsbaarheden, geïdentificeerd als CVE-2025-48983, CVE-2025-48984 en CVE-2025-48982, hebben CVSS-scores van respectievelijk 9.9 en 7.3. Aanvallers kunnen deze kwetsbaarheden misbruiken om toegang te krijgen tot de backup-infrastructuur en ransomware te implementeren, wat ernstige gevolgen kan hebben voor de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens. Het wordt sterk aanbevolen om zo snel mogelijk patches te installeren na grondig testen en de

laatste versies van de software bij te werken. Daarnaast is het van belang om de monitoringcapaciteiten te versterken om verdachte activiteiten snel te detecteren en incidenten effectief te melden.

Malafide crypto-stealing VSCode-extensies duiken weer op op OpenVSX

Een cyberaanvaller, genaamd TigerJack, blijft ontwikkelaars doelwit maken met kwaadaardige extensies die via de Visual Code (VSCode) marketplace en OpenVSX registry worden verspreid. Deze extensies worden gebruikt om cryptocurrency te stelen en achterdeurtjes in systemen te plaatsen. Twee extensies die al 17.000 keer gedownload waren op VSCode zijn na verwijdering daar nog steeds beschikbaar op OpenVSX. TigerJack publiceert dezelfde kwaadaardige code onder nieuwe namen, waardoor de dreiging aanhoudt. Naast het stelen van broncode, bevat een van de extensies een cryptominer die de rekenkracht van het systeem gebruikt zonder restricties. Andere extensies kunnen op afstand kwaadaardige code uitvoeren, waardoor aanvallers toegang krijgen tot systemen, bijvoorbeeld voor het stelen van inloggegevens, het installeren van ransomware, of het injecteren van backdoors. Het advies voor ontwikkelaars is om alleen extensies van betrouwbare bronnen te downloaden.

SEO poisoning richt zich op Ivanti VPN-gebruikers via Bing zoekresultaten

Er is een toename van SEO-poisoning-aanvallen die gericht zijn op gebruikers van Ivanti Pulse Secure VPN. Aanvallers maken gebruik van vervalste downloadsites die lijken op de legitieme Ivanti-website, en deze sites worden hoog gerankt in de zoekresultaten van Bing. Gebruikers die klikken op de vervalste links downloaden een trojanized Ivanti Pulse Secure VPN-client die een credential-stealing DLL bevat. Deze malware steelt VPN-inloggegevens door het bestand "connectionstore.dat" te doorzoeken en stuurt de gestolen gegevens naar een server op Microsoft Azure. De aanvallen hebben verband met eerdere incidenten waarbij gestolen VPN-gegevens werden gebruikt voor laterale bewegingen binnen netwerken en het inzetten van ransomware, zoals Akira ransomware. Organisaties wordt aangeraden om Multi-Factor Authenticatie (MFA) in te schakelen en verdachte apparaten direct van het netwerk te isoleren om schade te beperken.

Hackers gebruiken juridische meldingen om info-stealer malware te verspreiden

Hackers hebben een geavanceerde phishingcampagne opgezet die gericht is op gebruikers in Colombia. Ze maken gebruik van valse gerechtelijke meldingen om een complexe, multi-stage malware-levering te realiseren, wat uiteindelijk resulteert in de infectie met AsyncRAT. De aanvallers sturen zorgvuldig samengestelde e-mails die zich voordoen als officiële communicatie van een Colombiaanse rechtbank. De e-mails bevatten SVG-bestanden die, wanneer geopend, de slachtoffers doorsturen naar een vervalste website van het Openbaar Ministerie. Deze site lijkt een legitieme consultatieportaal, maar is bedoeld om malware te installeren. De malware maakt gebruik van verschillende technieken om de slachtoffers te infecteren, waarbij een obfuscated PowerShell-script en Visual Basic-scripts worden uitgevoerd om de malware te injecteren. Het eindresultaat is de installatie van AsyncRAT, waarmee de aanvallers volledige controle krijgen over de geïnfecteerde systemen. De campagne toont een zorgwekkende evolutie in sociale-engineeringtechnieken, waardoor traditionele beveiligingsmaatregelen kunnen worden omzeild.

Nieuwe cyberaanval maakt gebruik van NPM-ecosysteem om ontwikkelaars te infecteren bij het installeren van pakketten

In oktober 2025 ontdekten onderzoekers een geavanceerde phishingcampagne die gebruikmaakt van het NPM-ecosysteem. Deze aanval maakt gebruik van het vertrouwde unpkg.com CDN om schadelijke scripts rechtstreeks via browsers te verspreiden, gericht op werknemers van meer dan 135 bedrijven, voornamelijk in de industriële, technologische en energiesectoren in Europa. In plaats van traditionele schadelijke pakketinstallaties, worden de aanvallen uitgevoerd door goed ogende HTML-bestanden te verspreiden, die lijken op zakelijke documenten, facturen of projectbestanden. Wanneer slachtoffers deze openen, worden ze automatisch naar phishingwebsites geleid. De aanvallers maakten meer dan 175 tijdelijke NPM-pakketten aan, elk met JavaScript-code die de slachtoffers naar de kwaadaardige sites leidde. Het gebruik van open-source hostinginfrastructuur voor phishing vertegenwoordigt een gevaarlijke evolutie van supply chain-aanvallen, waarbij traditionele beveiligingsmaatregelen worden omzeild.

Risico's van gesynchroniseerde passkeys en hoe aanvallers ze kunnen omzeilen

Gesynchroniseerde passkeys verhogen de gebruiksvriendelijkheid maar brengen aanzienlijke beveiligingsrisico's met zich mee, vooral voor bedrijven. Deze passkeys worden gesynchroniseerd via cloudservices zoals iCloud of Google Cloud, wat de kwetsbaarheid vergroot. Aanvallers kunnen misbruik maken van cloud-accountovernames, manipuleren met browserextensies of zwakke herstelmechanismen gebruiken om toegang te krijgen tot accounts. Bovendien kunnen zogenaamde "adversary-in-the-middle" (AiTM) aanvallen authenticatie terugslaan naar zwakkere methoden zoals SMS of OTP, waardoor sterke beveiligingsmaatregelen worden omzeild. In plaats van gesynchroniseerde passkeys, worden apparaatgebonden passkeys, die hardwarebeveiligingssleutels gebruiken, aanbevolen voor enterprise-toepassingen. Deze bieden een veel sterkere bescherming omdat ze specifiek aan een apparaat zijn gebonden, wat een hogere mate van controle en beveiliging biedt. Bedrijven moeten daarom investeren in apparaatgebonden authenticators en zwakkere methoden uitsluiten om de beveiliging te verbeteren. Daarnaast kan MindYourPass een veilig alternatief zijn voor traditionele wachtwoordbeheeroplossingen. Dit systeem slaat geen wachtwoorden op, maar berekent ze telkens opnieuw, waardoor het risico op inbraak wordt geminimaliseerd.

Meer dan 100 VS Code-extensies stellen ontwikkelaars bloot aan verborgen supply chain-risico’s

Onderzoekers hebben ontdekt dat meer dan 100 Visual Studio Code (VS Code)-extensies toegangstokens hebben gelekt, die door kwaadwillenden kunnen worden misbruikt om schadelijke updates naar extensies te verspreiden. Dit vormt een groot risico voor de software supply chain. De getroffen extensies waren verbonden aan een cumulatieve install base van 150.000 gebruikers. In totaal werden meer dan 550 gelekte geheimen aangetroffen in 500 extensies van verschillende uitgevers. Deze geheimen omvatten onder andere API-sleutels van cloud- en AI-providers, evenals database-inloggegevens. De VS Code-extensies, die .vsix-bestanden gebruiken, kunnen onterecht toegang geven tot systeembronnen of zelfs kwaadaardige code uitvoeren. Microsoft heeft inmiddels de gelekte tokens ingetrokken en toegevoegd secret scanning-functionaliteit in de VS Code Marketplace geïntroduceerd om dergelijke risico’s te beperken. Ontwikkelaars wordt geadviseerd voorzichtig te zijn bij het installeren van extensies en automatische updates uit te schakelen.

Nieuwe banking trojan "maverick" verspreidt zich via whatsapp

Een nieuwe malwarecampagne is ontdekt in Brazilië, waarbij een kwaadaardig LNK-bestand via WhatsApp wordt verspreid. Dit bestand bevat de "Maverick" banking trojan, die sterke overeenkomsten vertoont met de Coyote-malware. De infectieketen is volledig fileless, wat betekent dat er geen bestanden op de schijf worden achtergelaten. Nadat het bestand is geopend, installeert de trojan zich en controleert of de machine zich in Brazilië bevindt. De trojan kan onder andere screenshots maken, toetsaanslagen loggen en websites monitoren, met als doel bankgegevens van slachtoffers te stelen. De trojan is ontworpen om de toegang tot 26 Braziliaanse bankwebsites en cryptocurrency-exchange platforms te monitoren. De communicatie met de command-and-control server wordt beveiligd via SSL, en de trojan maakt gebruik van geavanceerde technieken zoals encryptie en obfuscatie om detectie te vermijden. Kaspersky detecteerde in de eerste 10 dagen van oktober al 62.000 pogingen tot infectie in Brazilië.

GhostBat RAT Android-malware steelt bankgegevens via valse RTO-apps

GhostBat RAT is een nieuwe malwarecampagne die gericht is op Android-gebruikers in India. De malware wordt verspreid via valse apps die zich voordoen als de officiële "mParivahan"-app, gebruikt voor regionale transportdiensten. Gebruikers ontvangen smishing-berichten via SMS en WhatsApp met verkorte URL's die hen naar GitHub-hosted payloads leiden. Zodra de kwaadaardige app geïnstalleerd is, vraagt deze om SMS-gerelateerde machtigingen, waardoor de malware toegang krijgt tot bankgerelateerde gegevens. De app toont een phishing-interface die lijkt op de legitieme mParivahan-app, waarbij slachtoffers worden gevraagd voertuig- en mobiele gegevens in te voeren en een nep-betaling van ₹1 te doen ter "verificatie". Gegevens zoals bankgerelateerde SMS-berichten worden vervolgens verzameld en naar aanvallers gestuurd. De malware maakt gebruik van meerdere anti-analysetechnieken om detectie te voorkomen, wat het een aanzienlijke bedreiging maakt voor gebruikers van mobiele banken in India.

Hackers registreren 13.000+ unieke domeinen en gebruiken Cloudflare voor ClickFix-aanvallen

Hackers hebben in 2025 meer dan 13.000 unieke domeinen geregistreerd voor een nieuwe browsergebaseerde malwarecampagne, genaamd "ClickFix." Deze

campagne maakt gebruik van goedkope of gecompromitteerde hostinginfrastructuur, waaronder Cloudflare, om kwaadaardige payloads te verspreiden via valse webpagina's. Gebruikers worden via een CAPTCHA-uitdaging verleid om een commando uit hun klembord te plakken, wat resulteert in het ongewild uitvoeren van schadelijke scripts of uitvoerbare bestanden. De aanval maakt gebruik van eenvoudige social engineeringtechnieken en vereist weinig technische kennis van de aanvallers. De malware is ontworpen om zowel op Windows- als Mac-systemen te werken, en de spreiding van de domeinen toont een geautomatiseerde aanpak van de aanvallers. Dit incident benadrukt hoe hackers door massale domeinnregistratie en het misbruiken van bestaande infrastructuur grote schaal kunnen bereiken.

Amerikaanse overheid vervolgt oprichter Cambodjaanse conglomeraten in $14 miljard bitcoinfraude

De Amerikaanse overheid heeft meer dan $14 miljard aan bitcoin in beslag genomen en de oprichter van het Cambodjaanse Prince Holding Group aangeklaagd in verband met een massale cryptocurrency-fraude. Chen Zhi wordt beschuldigd van het opzetten van een "pig butchering"-oplichting, waarbij slachtoffers werden misleid om cryptocurrency over te maken met de belofte van grote rendementen. De opbrengsten werden gebruikt om luxe goederen aan te schaffen, waaronder jachten en kunstwerken. Chen wordt ook beschuldigd van het uitbuiten van dwangarbeid, waarbij migranten werden gedwongen om online fraude uit te voeren. De zaak werd aangespannen door het Brooklynse federale parket, en de Amerikaanse en Britse autoriteiten hebben sancties opgelegd aan Chen’s bedrijf. Als hij schuldig wordt bevonden, kan hij tot 40 jaar gevangenisstraf krijgen. De in beslag genomen bitcoin kan worden gebruikt om de slachtoffers te vergoeden.

Cyberbeveiliging op de helling door shutdown in de VS

President Donald Trump voert de huidige overheidsstilstand op een ongekende manier, waarbij zijn budgetdirecteur Russ Vought de macht krijgt om beslissingen te nemen over wie wordt betaald of ontslagen. In de derde week van de shutdown worden federale ambtenaren ontslagen, waaronder die werkzaam in de gezondheidszorg, onderwijs en wetenschappen. Vought heeft het bezuinigingsbeleid doorgevoerd en belangrijke militaire uitgaven doorgelaten, maar andere programma's, zoals die gericht op cyberbeveiliging en speciaal onderwijs, worden

gesloten. Het plan wordt bekritiseerd als illegaal en ligt onder vuur van de oppositie, die dreigt juridische stappen te ondernemen. De shutdown heeft tot vertragingen geleid in de heropening van de overheid, waarbij het conflict tussen Democraten en Republikeinen over de gezondheidszorgsubsidies aanhoudt. Ondertussen blijven prioriteiten zoals massale deportaties en de militaire betalingen ongestoord doorgaan.

Bitvavo-directie had jarenlang toegang tot klantgegevens

De directie en aandeelhouders van Bitvavo hadden jarenlang toegang tot persoonlijke gegevens van klanten, waaronder rekeninginformatie. Dit werd bevestigd door het bedrijf, dat aangeeft dat deze toegang in de beginjaren van de onderneming noodzakelijk was vanwege de betrokkenheid van de leiding bij klantregistraties en het beantwoorden van vragen. De toegang werd in de loop van de tijd echter gecontinueerd tot het voorjaar van 2024. Experts wijzen erop dat de privacywetgeving vereist dat toegang tot klantgegevens beperkt blijft tot degenen die deze informatie echt nodig hebben voor hun werk. Bitvavo stelt dat inmiddels alleen bevoegde afdelingen toegang hebben tot klantdata en dat het bedrijf voldoet aan de privacyregels, met regelmatige controles om ongeoorloofde toegang te voorkomen. Een intern onderzoek is gestart naar de naleving van privacy- en gedragsregels, vooral na het vertrek van topman Mark Nuvelstijn.

Discord-beschuldigd bedrijf ontkent lekken van 70.000 id-bewijzen

en bedrijf dat door Discord werd beschuldigd van het lekken van de identiteitsbewijzen van 70.000 gebruikers, ontkent de aantijgingen. Discord had vorige week gemeld dat aanvallers de id-bewijzen van 70.000 gebruikers hadden bemachtigd, die voor leeftijdsverificatie waren verstrekt. Deze gegevens zouden zijn buitgemaakt bij 5CA, een bedrijf dat de klantenservice voor Discord verzorgt. In reactie op de beschuldigingen heeft 5CA verklaard dat hun systemen niet betrokken waren bij het incident en dat de klantgegevens goed beschermd zijn. 5CA werkt nauw samen met Discord en heeft bevestigd dat het incident buiten hun systemen plaatsvond. Ze gaven aan dat het incident mogelijk te wijten is aan een menselijke fout, maar het onderzoek is nog niet afgerond. 5CA belooft verdere updates te verstrekken zodra meer informatie beschikbaar is.

Satellieten lekken wereldwijd geheime informatie: oproepen, teksten, militaire en bedrijfsdata

Onderzoekers hebben met slechts $800 aan basismateriaal ontdekt dat satellieten een breed scala aan ongecodeerde data doorgeven, waaronder duizenden oproepen en tekstberichten van T-Mobile-gebruikers en zelfs communicatie van het Amerikaanse leger. Deze gegevens worden zonder encryptie verzonden, waardoor het mogelijk is voor onbevoegden met de juiste apparatuur toegang te krijgen tot gevoelige informatie. Satellieten sturen constant radioverbindingen naar de aarde, maar ondanks de verwachting dat deze gegevens versleuteld zouden zijn, blijkt dit niet altijd het geval. De openbaarheid van deze informatie stelt een significant beveiligingsrisico voor, aangezien veel van de communicatie die via deze satellieten verloopt vertrouwelijke bedrijfsinformatie en persoonlijke gegevens bevat.

Volkswagen Group France getroffen door ransomware-aanval van Qilin-groep

Op 15 oktober 2025 werd gemeld dat de Volkswagen Group France, een dochteronderneming van Volkswagen AG, het slachtoffer is geworden van een cyberaanval. De Qilin ransomware-groep heeft de verantwoordelijkheid opgeëist voor de aanval, hoewel er nog geen officiële bevestiging van het bedrijf zelf is ontvangen. De details van de aanval blijven voorlopig onduidelijk, maar de gevolgen voor de organisatie kunnen significant zijn, gezien de aard van de ransomware-aanvallen. Volkswagen Group France heeft nog niet gereageerd op de publicaties over het incident.

Brits bedrijf krijgt 16 miljoen euro boete wegens datalek door ransomware

De Britse dienstverlener Capita heeft een boete van 16 miljoen euro gekregen van de Britse privacytoezichthouder ICO, na een datalek veroorzaakt door een ransomware-aanval in 2023. Bij deze aanval werden de gegevens van 6,6 miljoen personen gestolen, waaronder gevoelige informatie zoals strafbladen en financiële gegevens. De aanval begon toen een medewerker per ongeluk een kwaadaardig JavaScript-bestand downloadde, wat leidde tot de verspreiding van Qakbot-malware en Cobalt Strike. Ondanks een beveiligingswaarschuwing werd het getroffen systeem pas na 58 uur in quarantaine geplaatst, waarna de aanvaller zijn rechten verhoogde en uiteindelijk 1 terabyte aan data buitmaakte. De ICO concludeerde dat Capita onvoldoende beveiligingsmaatregelen had getroffen en niet adequaat reageerde op

de waarschuwing. Aanvankelijk was er een boete van 52 miljoen euro voorgesteld, maar na verzachtende factoren werd het bedrag verlaagd.

Mango meldt datalek waarbij klantgegevens zijn blootgesteld

Het Spaanse modebedrijf Mango heeft een datalek gemeld waarbij persoonlijke klantgegevens zijn blootgesteld. Het lek ontstond doordat een externe marketingleverancier werd gehackt, wat resulteerde in de blootstelling van gegevens zoals voornaam, land, postcode, e-mailadres en telefoonnummer van klanten. Mango benadrukte dat gevoelige informatie zoals achternamen, bankgegevens, creditcardinformatie, identiteitsbewijzen en wachtwoorden niet in het lek zijn betrokken. Het bedrijf stelde tevens vast dat de bedrijfsinfrastructuur en interne systemen niet waren aangetast, en dat de bedrijfsvoering niet werd beïnvloed. Na ontdekking van het incident werden alle relevante beveiligingsprotocollen geactiveerd. Mango heeft de Spaanse Autoriteit voor Gegevensbescherming en andere betrokken autoriteiten ingelicht en biedt klanten ondersteuning via een speciaal telefoonnummer en e-mailadres. Er is nog geen informatie over de aanvallers, aangezien er geen ransomwaregroep is die Mango op hun extortieportalen heeft vermeld.

Elasticsearch-lek onthult 6 miljard records van scraping en datalekken

Een misgeconfigureerde Elasticsearch-server heeft meer dan 6 miljard records blootgesteld aan het publieke internet, zonder enige beveiliging of wachtwoord. De server bevatte gegevens verzameld via datalekken en webscraping, waaronder gevoelige informatie zoals bankgegevens, contactgegevens en persoonlijke identificatiegegevens. Onder de gegevens bevonden zich records van de Oekraïense bank Accordbank, met onder meer volledige namen, telefoonnummers, geboortedata en paspoortnummers. De gegevens werden verzameld uit zowel openbare als niet-aangekondigde datalekken. De server was mogelijk in handen van cybercriminelen, die de gegevens per ongeluk publiek toegankelijk maakten voordat ze de server offline haalden. Dit lek benadrukt de risico's van onbeveiligde gegevensopslag en de noodzaak voor bedrijven om hun servers goed te configureren en te beveiligen. Gebruikers wiens gegevens mogelijk zijn gelekt, wordt aangeraden extra voorzichtig te zijn en hun gegevens te monitoren.