Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

06-10-2025:

Teeuwissen Rioolreiniging slachtoffer van ransomwareaanval door Devman groep

Op 3 oktober 2025 werd Teeuwissen.com het slachtoffer van een ransomwareaanval, geclaimd door de Devman ransomwaregroep. De aanvallers eisten een losgeld van 370.000 dollar in ruil voor het ontsleutelen van 80 GB aan gestolen gegevens. Deze aanval heeft de bedrijfsvoering van Teeuwissen verstoord en benadrukt de kwetsbaarheid van bedrijven in de infrastructuursector voor cyberdreigingen.

Bedrijfsnaam: Teeuwissen Rioolreiniging

Naam van de ransomwaregroep: Devman

Ontdekkingsdatum van de aanval: 3 oktober 2025

Sector van het bedrijf: Rioolreiniging en infrastructuur

Land waarin het bedrijf actief is: Nederland

Teeuwissen Rioolreiniging, opgericht in 1968 en gevestigd in Huizen en Barneveld, is een familiebedrijf dat zich richt op het reinigen, aanleggen, onderhouden en inspecteren van rioleringen en rioolgemalen. Met meer dan 210 medewerkers bedient het bedrijf zowel particuliere als zakelijke klanten, waaronder waterschappen en woningcorporaties, door heel Nederland. Daarnaast is Teeuwissen gespecialiseerd in het ledigen en inspecteren van olie- en vetafscheiders, waarbij vrijgekomen afvalstoffen milieuvriendelijk worden verwerkt in eigen beheer.

Discord lekt identiteitsbewijzen gebruikers verstrekt voor leeftijdsverificatie

Discord heeft gemeld dat er een datalek heeft plaatsgevonden waarbij identiteitsbewijzen van gebruikers zijn buitgemaakt. Dit gebeurde nadat een aanvaller toegang kreeg tot de systemen van een extern bedrijf dat door Discord werd ingeschakeld voor klantenservice. De gestolen gegevens omvatten onder andere gebruikersnamen, e-mailadressen, laatste vier cijfers van creditcards, IP-adressen en berichten aan supportmedewerkers. Daarnaast werden kopieën van identiteitsbewijzen gestolen van gebruikers die bezwaar hadden gemaakt tegen de leeftijdsschatting op het platform. Discord voert in sommige landen experimenten uit waarbij gebruikers hun leeftijd kunnen verifiëren door middel van een gezichtsscan. Gebruikers die het niet eens waren met de geschatte leeftijd moesten hun paspoort

of rijbewijs indienen. Discord heeft aangegeven dat het aantal gestolen identiteitsbewijzen beperkt is en getroffen gebruikers worden geïnformeerd.

klantgegevens van Renault gestolen in cyberaanval

Renault UK heeft bevestigd dat enkele klantgegevens zijn gestolen tijdens een cyberaanval op een van zijn externe databronnen. De Franse autobouwer gaf aan dat er geen toegang was tot financiële informatie zoals bankgegevens of wachtwoorden van klanten. Wel werden gegevens zoals namen, adressen, geboortedata, geslacht, telefoonnummers, voertuigidentificatienummers en kentekeninformatie gestolen. Het aantal getroffen klanten werd niet gespecificeerd, maar het bedrijf waarschuwde dat dit mogelijk een breder publiek betreft, inclusief mensen die bijvoorbeeld wedstrijden hebben deelgenomen of gegevens hebben gedeeld zonder een aankoop te doen. Renault stelde dat het incident volledig is geïsoleerd en onder controle is, en werkt samen met de betrokken derde partij om de situatie op te lossen. Klanten die getroffen zijn door de inbreuk worden geïnformeerd en geadviseerd waakzaam te blijven voor verdachte verzoeken om persoonlijke informatie.

München luchthaven hervat vluchten na drones en Denemarken bereidt zich voor op Russische ‘hybride oorlog’

München luchthaven hervatte zijn vluchten nadat eerdere drone-waarnemingen de operaties stillegden, waardoor zo'n 6.500 passagiers werden getroffen. Delen van de luchthavens in Kopenhagen en Oslo waren ook tijdelijk gesloten door drone-inbreuken, die zowel civiele als militaire luchtruimen beïnvloedden. In reactie op deze incidenten verklaarde de Deense premier dat een ‘hybride oorlog’ met Rusland gaande is, wat als de gevaarlijkste situatie sinds de Tweede Wereldoorlog wordt beschouwd. De Deense overheid heeft de inwoners aangespoord om voor drie dagen in hun eigen energiebehoeften en voedsel te voorzien. De autoriteiten in België onderzoeken ook meerdere drone-waarnemingen boven een militair terrein nabij de Duitse grens. De recente dronestrijd in Europa roept bredere zorgen op over de veiligheid van luchthavens en andere kritieke infrastructuren.

Microsoft adviseert om games met kwetsbare Unity-engine te verwijderen

Microsoft heeft gebruikers geadviseerd om games te verwijderen die zijn gemaakt met een kwetsbare versie van de Unity Gaming Engine Editor. De kwetsbaarheid is aanwezig in Unity-versies vanaf 2017.1, die worden gebruikt voor de ontwikkeling van games en apps voor Android, macOS en Windows. Deze kwetsbaarheid maakt het mogelijk voor aanvallers met lokale toegang om willekeurige code uit te voeren binnen de applicatie. Steam heeft al een update uitgerold om het starten van kwetsbare games te blokkeren. Unity zelf heeft de kwetsbaarheid gepatcht en roept ontwikkelaars op om de beschikbare patching tool te gebruiken. Microsoft heeft eveneens een beveiligingsadvies uitgegeven, waarin gebruikers worden aangespoord om kwetsbare games en applicaties te verwijderen totdat een update beschikbaar is. Microsoft Defender zou moeten detecteren en stoppen met misbruik van deze kwetsbaarheid.

Dreiging van OneDrive Checker die 2FA omzeilt

Op 3 oktober 2025 claimde een bedreigingsactor op het darkweb een tool te verkopen, genaamd de "OneDrive Checker," die beweert in staat te zijn de tweefactorauthenticatie (2FA) van OneDrive te omzeilen. Deze tool zou potentiële aanvallers in staat stellen ongeautoriseerde toegang te krijgen tot OneDrive-accounts, zelfs wanneer 2FA is ingeschakeld, wat een aanzienlijke bedreiging vormt voor de veiligheid van gebruikers. De verkoop van dergelijke tools maakt het voor cybercriminelen gemakkelijker om gevoelige informatie te stelen en kan leiden tot verschillende vormen van digitale fraude. Gebruikers wordt geadviseerd om extra waakzaam te zijn en de beveiligingsmaatregelen van hun accounts te versterken om dergelijke aanvallen te voorkomen.

Formbook C2-infrastructuur gekoppeld aan geparkeerde domeinnaam

Er is een domeinnaam geïdentificeerd die mogelijk de infrastructuur ondersteunt voor de Formbook stealer-malware. Het domein, momenteel geparkeerd op het DNS-systeem van Hostinger, lijkt eerder voor kwaadwillende activiteiten te zijn gebruikt, hoewel het momenteel inactief is. DNS-records en certificaatinformatie suggereren een eerdere betrokkenheid bij schadelijke activiteiten. De waarschijnlijkheid van deze toewijzing wordt geschat op 50%. Het domein in kwestie is www.hawala[.]shop, dat als command-and-control (C2)-infrastructuur fungeert voor de Formbook-malware, welke vaak wordt gebruikt om wachtwoorden en andere gevoelige informatie te

stelen. De aanbevolen verdedigingsmaatregelen omvatten het blokkeren van dit domein en bijbehorende IP-adressen, evenals het monitoren op verdachte verkeerspatronen die verband houden met de Formbook-malware.

Scanning-activiteit op Palo Alto-netwerken stijgt met 500% in één dag

GreyNoise, een bedrijf dat zich richt op dreigingsanalyse, heeft een opvallende toename van scanning-activiteit op de loginportalen van Palo Alto Networks gemeld. Op 3 oktober 2025 werd een stijging van bijna 500% waargenomen in het aantal IP-adressen dat deze portalen scant, wat de grootste toename in de afgelopen drie maanden vertegenwoordigt. In totaal waren er 1.300 unieke IP-adressen betrokken, tegenover de circa 200 voorheen. Van deze IP-adressen werd 93% als verdacht en 7% als kwaadaardig geclassificeerd. De meeste IP-adressen werden geassocieerd met de VS, gevolgd door kleinere clusters in het VK, Nederland, Canada en Rusland. GreyNoise stelde dat deze toename vergelijkbare kenmerken vertoont met recente scanning-activiteiten die gericht waren op Cisco ASA, en dat er een overlap is in de gebruikte tools. Er wordt opgemerkt dat dergelijke activiteiten vaak voorafgaan aan de ontdekking van kwetsbaarheden binnen zes weken.

Hackers maken misbruik van Zimbra-kwetsbaarheid via iCalendar-bestanden

Hackers hebben gebruikgemaakt van een kwetsbaarheid in de Zimbra Collaboration Suite (ZCS), aangeduid als CVE-2025-27915, om aanvallen uit te voeren met behulp van iCalendar (ICS)-bestanden. Deze bestanden werden misbruikt om kwaadaardige JavaScript-code in te voeren die zich in de sessie van het slachtoffer nestelde. De kwetsbaarheid ontstond door onvoldoende controle op HTML-inhoud in ICS-bestanden, wat aanvallers in staat stelde om ongeautoriseerde acties uit te voeren, zoals het stelen van inloggegevens en e-mailinvoer. De aanvallen werden in januari gedetecteerd, voordat Zimbra een patch uitbracht. Het doelwit van deze aanvallen was onder andere een Braziliaanse militaire organisatie, met het gebruik van gespoofte e-mails van de Libische marine. Zimbra heeft het probleem opgelost in januari 2025, maar de aanvallen werden al voor de release van de patch uitgevoerd.

CometJacking: nieuwe aanval maakt van AI-browser een datadief

Onderzoekers hebben een nieuwe aanval, genaamd CometJacking, ontdekt die de Comet AI-browser van Perplexity misbruikt. Via een gemanipuleerde URL kunnen aanvallers gevoelige data zoals e-mails en agenda-informatie van gebruikers stelen. De aanval wordt uitgevoerd door een onschuldige ogende link die de browser ertoe aanzet om verborgen opdrachten uit te voeren, die data extraheren en naar een externe server sturen. Deze techniek maakt gebruik van eenvoudige Base64-codering om de dataprotecties van de browser te omzeilen. Het belangrijkste risico is dat de browser al toegang heeft tot gegevens van gekoppelde diensten zoals Gmail en Google Calendar. Deze aanval laat zien hoe AI-native tools nieuwe beveiligingsrisico's met zich meebrengen, waarbij traditionele beveiligingsmaatregelen vaak niet voldoende zijn. Dit benadrukt de noodzaak van veiligheid vanaf het ontwerp voor AI-browsers, met name voor geheugen- en agenttoegang.

Politie onderzoekt inbeslaggenomen seksuele beelden van kinderen

De politie heeft afgelopen week gegevensdragers in beslag genomen in negen verschillende onderzoeken naar bezit van seksuele beelden van kinderen. Negen mannen, in de leeftijd van 21 tot 62 jaar, worden verdacht van dit misdrijf. De inbeslagnames maken deel uit van operatie 'Veilige Haven', uitgevoerd door het Team Bestrijding Kinderporno en Kindersekstoerisme van de eenheid Rotterdam. De verdachten komen uit Rotterdam, Dordrecht, Barendrecht en Capelle aan den IJssel. Het onderzoek richt zich op het grafisch beeldmateriaal en wordt verder onder leiding van het Openbaar Ministerie voortgezet, waarbij ook onbekende slachtoffers worden gezocht. De beelden worden toegevoegd aan de landelijke database. Het onderzoek benadrukt de strijd tegen het downloaden en bezitten van kinderpornografie, een misdrijf dat het misbruik van kinderen in stand houdt.

Signal waarschuwt Duitsland tegen invoering chatcontrole

Meredith Whittaker, het hoofd van Signal, heeft Duitsland in een open brief opgeroepen om tegen de invoering van chatcontrole te stemmen. De nieuwe wetgeving zou vereisen dat alle berichten, foto's en video's op apparaten van gebruikers worden gescand om te bepalen of de inhoud toegestaan is. Signal waarschuwt dat dit de privacy van gebruikers ernstig zou schenden en kan leiden tot massasurveillance. Whittaker stelt dat dergelijke maatregelen het recht op privacy in

Europa bedreigen en dat misbruik door kwaadwillenden niet uitgesloten is. Signal heeft aangegeven dat het, indien de wet wordt ingevoerd, mogelijk de EU zal verlaten in plaats van haar gebruikers in gevaar te brengen. Duitsland speelt een cruciale rol in de aankomende stemming op 14 oktober, en Signal dringt erop aan dat het land standhoudt voor de bescherming van de privacy van haar burgers.

Salesforce reageert op afpersing van klanten door criminelen

Salesforce heeft gereageerd op een recente afpersingspoging waarbij criminelen dreigen data van klanten openbaar te maken. Een website werd gelanceerd waarop bedrijven werden genoemd die volgens de aanvallers slachtoffer zouden zijn van datadiefstal uit Salesforce-omgevingen. De criminelen eisen betaling vóór 10 oktober om publicatie te voorkomen. Salesforce heeft bevestigd bekend te zijn met de afpersing en werkt samen met externe experts en autoriteiten om het incident te onderzoeken. Het bedrijf heeft aangegeven dat er geen aanwijzingen zijn dat het Salesforce-platform zelf is gecompromitteerd en dat de aanvallen niet gerelateerd zijn aan bekende kwetsbaarheden. Salesforce biedt getroffen klanten ondersteuning en waarschuwt voor phishing- en social engineering-aanvallen die vaak door criminelen worden gebruikt.

Signal voegt cryptografische verdediging toe tegen kwantumaanvallen

Signal heeft de introductie aangekondigd van de Sparse Post-Quantum Ratchet (SPQR), een nieuwe cryptografische component die ontworpen is om bedreigingen van kwantumcomputing te weerstaan. SPQR werkt door encryptiesleutels in gesprekken continu bij te werken en oude sleutels te verwijderen, waardoor de veiligheid van toekomstige berichten gewaarborgd blijft, zelfs bij compromittering van sleutels. Het systeem maakt gebruik van post-quantum Key-Encapsulation Mechanisms (ML-KEM) en efficiënte chunking en erasure coding om grote sleutels te verwerken zonder bandbreedte te belasten. De toevoeging van SPQR vormt samen met het bestaande dubbelratelsysteem een “Triple Ratchet”, waarbij beide systemen gezamenlijk een hybride encryptiesleutel genereren. Signal werkt samen met PQShield, AIST en New York University aan dit ontwerp, dat continu zal worden geverifieerd om de beveiliging te waarborgen. De uitrol van de nieuwe functie zal geleidelijk plaatsvinden, waarbij gebruikers automatisch de nieuwste versie van de app moeten bijwerken.

Geclaimde datalek van RIPE NCC (Réseaux IP Européens Network Coordination Centre)

Op 3 oktober 2025 werd via het Dark Web melding gemaakt van een geclaimd datalek bij RIPE NCC, het Europese netwerkcoördinatiecentrum voor IP-adressen. De aanvallers zouden toegang hebben gekregen tot gevoelige gegevens, hoewel de exacte details over het datalek nog niet volledig bekend zijn. RIPE NCC heeft nog geen officiële verklaring afgelegd, maar de melding werd gepost op een platform dat vaak wordt gebruikt door cybercriminelen om gestolen gegevens te verspreiden. Dit incident roept zorgen op over de beveiliging van Europese netwerkinfrastructuren en de mogelijke impact op de bredere internetgemeenschap. Aangezien het RIPE NCC een sleutelrol speelt in het toewijzen van IP-adressen en andere netwerkinstellingen in Europa, zou een inbreuk op zijn systemen verregaande gevolgen kunnen hebben. De situatie wordt nog verder onderzocht door de bevoegde autoriteiten.

ParkMobile biedt $1 compensatie na datalek 2021

ParkMobile heeft de rechtszaak over een datalek uit 2021, waarbij de gegevens van 22 miljoen gebruikers werden gestolen, afgehandeld. De getroffen gebruikers ontvangen nu compensatie in de vorm van een in-app tegoed van $1, dat handmatig geclaimd moet worden en een vervaldatum heeft. Het datalek, veroorzaakt door hackers, leidde tot de publicatie van 4,5 GB aan gevoelige klantinformatie. De rechtszaak resulteerde in een schikking van $32,8 miljoen, waarbij ParkMobile geen schuld erkent. Gebruikers kunnen de compensatiecode tot oktober 2026 gebruiken, maar de aanbieding is enkel van toepassing voor accounts die betrokken zijn bij de rechtszaak. ParkMobile waarschuwt daarnaast voor phishing-aanvallen die momenteel plaatsvinden en roept klanten op om voorzichtig te zijn met verdachte berichten.

Stijging van werkzoekfraude in de VS met 1000% in 2025

Werkzoekfraude is in de VS sterk toegenomen, met een stijging van 1000% in klachten bij de Federal Trade Commission (FTC) tussen mei en juli 2025. Deze fraude wordt aangedreven door economische onzekerheid en de groeiende werkloosheid, met bijna 700.000 ontslagen in de eerste helft van 2025.

Werkzoekfraude is nu de vierde meest voorkomende fraude in het land. Slachtoffers worden vaak misleid met beloften van hoogbetaalde banen voor eenvoudige taken, wat resulteert in gemiddelde verliezen van 2.100 dollar per slachtoffer. Scammers maken gebruik van geavanceerde technologieën zoals AI en deepfakes om geloofwaardige oplichtingsschema's te creëren. De meest getroffen staten zijn Nevada, Florida en Colorado, waarbij Texanen de grootste financiële verliezen rapporteerden. Experts adviseren werkzoekenden om zich bewust te zijn van verdachte aanbiedingen en nooit geld vooraf te betalen of persoonlijke informatie zonder de juiste verificatie te verstrekken.