Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

30-10-2025:

Spijkermat slachtoffer van ransomware-aanval

Spijkermat, een Nederlands bedrijf dat de originele Zweedse Spijkermatten distribueert, is het slachtoffer geworden van een ransomware-aanval door de Radiant-groep. Het bedrijf wordt beheerd door Tisan Internetdiensten BV, gevestigd in Ouddorp, Zuid-Holland. Spijkermat.com verkoopt de Zweedse acupressurematten, ontwikkeld door Susanna Lindelöw, en geproduceerd door Svenska Spikmattan AB in Zweden. De matten voldoen aan strenge kwaliteits- en milieu-eisen en worden sinds 2007 gedistribueerd door Tisan Internetdiensten BV aan consumenten en professionals in de Benelux.

De aanval, die werd ontdekt op 29 oktober 2025, heeft geleid tot een datalek, waarbij gegevens van het bedrijf mogelijk zijn gepubliceerd door de ransomwaregroep. Dit incident benadrukt de kwetsbaarheid van bedrijven, zelfs in sectoren die niet direct geassocieerd worden met technologie.

Russische hackers richten zich op Oekraïense organisaties met stealth-aanvallen

Russische hackers hebben verschillende Oekraïense organisaties aangevallen met behulp van 'Living-Off-the-Land' (LotL) tactieken, waarbij ze minimale malware gebruiken om hun activiteiten verborgen te houden. De aanvallen werden uitgevoerd tegen een grote zakelijke dienstverlener en een lokale overheidsinstantie in Oekraïne. De hackers maakten gebruik van webshells op publieke servers, die waarschijnlijk via niet-gepatchte kwetsbaarheden werden ingezet. Een van de gebruikte webshells, LocalOlive, werd eerder in verband gebracht met de Sandworm-groep. Gedurende de aanvallen werd onder andere PowerShell gebruikt om bestanden te enumereren en processen te monitoren, terwijl tools zoals OpenSSH en RDP werden ingezet om toegang te verkrijgen tot de systemen. Ondanks de beperkte inzet van malware, is het gebruik van legitieme software door de aanvallers een teken van geavanceerde kennis van Windows-systemen. De aanvallen vertonen overeenkomsten met eerdere Sandworm-campagnes.

Polen investeert in Palantir ondanks zorgen over AI militaire systemen

Polen heeft nieuwe overeenkomsten gesloten met de Amerikaanse technologiebedrijven Palantir en Anduril om de militaire capaciteiten te versterken

met data, AI en cybertechnologie. Dit besluit komt kort nadat bekend werd dat Palantir-systemen, ontwikkeld voor het Amerikaanse leger, ernstige beveiligingsproblemen vertoonden. Desondanks tekende het Poolse ministerie van Defensie intentieverklaringen voor samenwerking op het gebied van slagveldanalyse en logistiek. De Poolse wapenproducent PGZ SA zal daarnaast met Anduril werken aan de productie van Barracuda-500M kruisraketten met een bereik van ruim 900 kilometer. Critici wijzen op politieke motieven achter de deals, aangezien Palantir nauwe banden heeft met invloedrijke Amerikaanse politici. De Amerikaanse strijdkrachten hebben intussen aangegeven dat de gemelde tekortkomingen in de Palantir-systemen zijn verholpen, maar details over de Poolse contracten blijven onbekend.

Kritiek XWiki-lek actief misbruikt voor cryptominer-installatie

Aanvallers maken actief gebruik van een kritieke kwetsbaarheid in de open-source software XWiki voor het installeren van cryptominers, aldus het beveiligingsbedrijf VulnCheck. Het lek, aangeduid als CVE-2025-24893, werd eind 2024 door XWiki gedicht, maar wordt momenteel misbruikt door cybercriminelen. Via het lek kunnen ongeauthenticeerde aanvallers op afstand code uitvoeren op kwetsbare systemen. De kwetsbaarheid heeft een hoge ernst met een score van 9,8 op de schaal van 10. XWiki is een veelgebruikte wiki-software en wordt wereldwijd op meer dan achtduizend systemen ingezet. Dit misbruik wordt omschreven als een “low-end operation”, waarbij cryptovaluta wordt gemined door de rekenkracht van getroffen systemen te benutten. Het exacte volume van het misbruik is onbekend.

CISA waarschuwt voor twee actieve kwetsbaarheden in Dassault

De Cybersecurity & Infrastructure Security Agency (CISA) heeft gewaarschuwd voor twee kwetsbaarheden in de DELMIA Apriso-software van Dassault Systèmes, die actief worden misbruikt door aanvallers. De eerste kwetsbaarheid (CVE-2025-6205) betreft een beveiligingsfout van het type "missing authorization", die kwaadwillende actoren in staat stelt op afstand toegang te krijgen tot de applicatie zonder authenticatie. De tweede kwetsbaarheid (CVE-2025-6204) is een code-injectieprobleem waarmee aanvallers met hoge rechten willekeurige code kunnen uitvoeren op kwetsbare systemen. Deze kwetsbaarheden werden in augustus 2025 gepatcht door Dassault Systèmes, maar CISA voegde ze vandaag toe aan de lijst

van "actief misbruikte kwetsbaarheden". De federale agentschappen van de VS zijn verplicht om de kwetsbaarheden binnen drie weken te verhelpen, maar CISA raadt aan om de patches ook buiten de VS zo snel mogelijk toe te passen.

Nieuwe TEE.Fail-aanval onthult kwetsbaarheid in Intel en AMD DDR5-enclaves

Onderzoekers van Georgia Tech, Purdue University en Synkhronix hebben een nieuwe side-channel-aanval ontwikkeld, genaamd TEE.Fail. Deze aanval maakt het mogelijk om geheime sleutels te extraheren uit de trusted execution environment (TEE) van Intel- en AMD-processoren, inclusief Intel's Software Guard eXtensions (SGX) en Trust Domain Extensions (TDX), en AMD's Secure Encrypted Virtualization met Secure Nested Paging (SEV-SNP). De aanval gebruikt een apparaat dat minder dan $1.000 kost om geheugentransacties in DDR5-servers te inspecteren. Dit maakt het voor de eerste keer mogelijk om cryptografische sleutels, waaronder geheime attestiatie-sleutels, te extraheren uit volledig geüpdatete machines. De aanval kan zelfs de beveiliging van Nvidia's GPU Confidential Computing omzeilen, waardoor kwaadwillenden AI-workloads kunnen uitvoeren zonder TEE-bescherming. Hoewel er geen bewijs is dat de aanval in het wild is gebruikt, wordt aanbevolen om softwarematige tegenmaatregelen te implementeren om de risico's te mitigeren.

Kritieke fout in Docker Compose laat aanvallers willekeurige bestanden overschrijven

Een ernstig beveiligingslek in Docker Compose maakt het mogelijk dat aanvallers willekeurige bestanden op hosts overschrijven zonder containers te starten. De kwetsbaarheid, aangeduid als CVE-2025-62725 met een CVSS-score van 8.9, werd ontdekt in de verwerking van externe OCI-artefacten. Door gebruik te maken van gemanipuleerde YAML-bestanden kunnen kwaadwillenden padtraversals uitvoeren en gevoelige bestanden, zoals SSH-sleutels of systeemconfiguraties, aanpassen. Het probleem treedt zelfs op tijdens schijnbaar veilige opdrachten zoals 'docker compose config'. De fout treft miljoenen ontwikkelomgevingen en CI/CD-pijplijnen die Docker Compose gebruiken. Docker heeft het lek inmiddels verholpen in versie 2.40.2 door extra padvalidatie toe te voegen. Gebruikers worden dringend geadviseerd te updaten en gedeelde configuratiebestanden zorgvuldig te controleren om misbruik te voorkomen.

Google Wear OS berichten-app kwetsbaar voor misbruik van apps

Een kwetsbaarheid in de Google Messages-app op Wear OS-apparaten stelt elke geïnstalleerde app in staat om ongemerkt SMS-, MMS- of RCS-berichten te versturen namens de gebruiker. De kwetsbaarheid, aangeduid als CVE-2025-12080, wordt veroorzaakt door onjuiste afhandeling van ACTION_SENDTO-intenties via URI-schema's zoals sms:, smsto:, mms:, en mmsto:. Deze misconfiguratie omzeilt de bevestiging en toestemming van de gebruiker, waardoor aanvallers berichten naar willekeurige ontvangers kunnen sturen zonder detectie. De kwetsbaarheid heeft invloed op de meeste Wear OS-apparaten, aangezien Google Messages de standaardberichtenapp is op veel smartwatches. Het probleem werd ontdekt en gemeld via het Mobile Vulnerability Reward Program van Google en er werd een patch uitgerold in mei 2025. Gebruikers wordt aangeraden hun apparaten snel bij te werken en aandacht te besteden aan app-installaties.

Kritieke XSS-kwetsbaarheid in LiteSpeed Cache-plugin voor WordPress

Een ernstige cross-site scripting (XSS) kwetsbaarheid is ontdekt in de populaire LiteSpeed Cache-plugin voor WordPress, die wereldwijd miljoenen websites blootstelt aan risico’s. De kwetsbaarheid, aangeduid als CVE-2025-12450, wordt veroorzaakt door onvoldoende inputverificatie en het niet ontsnappen van uitvoer in de URL-verwerking van de plugin. Deze fout maakt het mogelijk voor aanvallers om kwaadaardige scripts in webpagina’s in te voegen, wat kan leiden tot diefstal van gevoelige informatie of ongeautoriseerde acties wanneer gebruikers op een speciaal ontworpen link klikken. De kwetsbaarheid heeft invloed op alle versies tot en met versie 7.5.0.1. Een patch is beschikbaar in versie 7.6, die de beveiliging heeft verbeterd. WordPress-beheerders wordt aangeraden om snel te updaten naar versie 7

Cloudflare pakt DDoS-kwetsbaarheden in QUIC aan

Cloudflare heeft twee kwetsbaarheden geïdentificeerd en verholpen in de QUIC-implementatie van hun open-sourcebibliotheek quiche, die gerelateerd zijn aan de verwerking van pakketbevestigingen (ACKs). Deze kwetsbaarheden konden worden misbruikt voor DDoS-aanvallen door middel van zogenaamde "Optimistic ACK"-technieken, waarbij aanvallers voorspelbare ACK-berichten verzenden om een server te overbelasten. Na melding door een beveiligingsonderzoeker werden de

kwetsbaarheden snel gepatcht, en er zijn geen aanwijzingen dat deze kwetsbaarheden daadwerkelijk zijn misbruikt. Cloudflare heeft de infrastructuur gepatcht en bevestigd dat de DDoS-vector is verholpen. De kwetsbaarheden betroffen quiche-versies voor versie 0.24.4 en eerder. Het beveiligingsprobleem is nu opgelost door het valideren van ACK-bereiken en het verbeteren van de verwerking van ACK-signalen om het netwerk eerlijker te houden.

PhantomRaven-aanval richt zich op ontwikkelaars met schadelijke npm-pakketten

De 'PhantomRaven'-campagne richt zich op softwareontwikkelaars door middel van kwaadaardige npm-pakketten die inlogtokens, CI/CD-geheimen en GitHub-gegevens stelen. Deze aanval, die begon in augustus 2025, heeft al 126 npm-pakketten geïntroduceerd die meer dan 86.000 keer zijn gedownload. De kwaadaardige pakketten lijken op legitieme projecten en maken gebruik van 'slopsquatting', een techniek waarbij niet-bestaande pakketnamen door AI-aanbevelingen worden gesuggereerd. De pakketten bevatten een mechanisme dat bij installatie automatisch externe payloads ophaalt, zonder dat de gebruiker actie hoeft te ondernemen. De malware verzamelt gegevens van de geïnfecteerde systemen, zoals omgevingsvariabelen en e-mailadressen, en steelt belangrijke tokens van platforms als NPM, GitHub, GitLab en Jenkins. Dit kan leiden tot supply chain-aanvallen. Ontwikkelaars worden geadviseerd om alleen legitieme pakketten van betrouwbare leveranciers te gebruiken en zorgvuldig te controleren of pakketten authentiek zijn.

Medewerkers kunnen bedrijfsdata verkopen aan hackers van Play

De Play-ransomwaregroep heeft een opmerkelijke verklaring uitgebracht waarin ze stelt dat het welzijn van medewerkers van cruciaal belang is. De groep suggereert dat medewerkers mogelijk toegang tot bedrijfsnetwerken kunnen verkopen aan hackgroepen in ruil voor wederzijdse voordelen. Dit zou bedrijven kwetsbaar kunnen maken voor cyberaanvallen. De opmerking werd gepost als een aankondiging, waarbij de Play-groep hun motief deelde voor het verkrijgen van bedrijfsdata. Dit werpt een licht op de groeiende dreiging van interne bedreigingen, waarbij medewerkers niet alleen doelwit zijn van cybercriminelen, maar ook zelf toegang verkopen voor persoonlijke winst. Deze vorm van samenwerking tussen interne werknemers en externe hackers kan bedrijven in gevaar brengen, en benadrukt de noodzaak van strikte beveiligingsmaatregelen binnen organisaties.

Nieuwe phishingaanval maakt gebruik van onzichtbare tekens in onderwerpregel met MIME-codering

Onderzoekers hebben een nieuwe phishingtechniek ontdekt die gebruik maakt van onzichtbare Unicode-tekens in de onderwerpregel van e-mails, met behulp van MIME-codering. Deze methode blijft grotendeels onbekend bij e-mailbeveiligingsexperts. De aanvallers maken gebruik van "soft hyphen" tekens die in de onderwerpregel van e-mails worden verborgen. Deze tekens zijn onzichtbaar voor de ontvanger, maar wel aanwezig in de e-mailstructuur, waardoor ze de automatische filtermechanismen van e-mailbeveiligingssystemen kunnen omzeilen. Deze techniek breekt bepaalde woorden in de tekst op, zodat ze voor het beveiligingssysteem niet herkenbaar zijn als phishing-indicatoren. De e-mail bevat links naar een malafide webpagina die bedoeld is om inloggegevens van gebruikers te verzamelen. Organisaties worden geadviseerd om hun e-mailfilters te controleren en meer geavanceerde systemen in te zetten om dergelijke obfuscaties te detecteren.

Toename van geautomatiseerde botnetaanvallen gericht op PHP-servers en IoT-apparaten

Experts melden een aanzienlijke stijging van geautomatiseerde botnetaanvallen, gericht op PHP-servers, IoT-apparaten en cloudgateways. Botnets zoals Mirai, Gafgyt en Mozi maken gebruik van bekende kwetsbaarheden in PHP en misconfiguraties in cloudomgevingen om toegang te verkrijgen tot onveilige systemen. Vooral PHP-servers, die veelvuldig gebruikt worden door platforms zoals WordPress en Craft CMS, zijn een belangrijk doelwit vanwege de kwetsbaarheden in verouderde plugins en misconfiguraties. Er worden ook IoT-apparaten en cloudinfrastructuren misbruikt, waaronder systemen van Amazon Web Services en Google Cloud. Aanvallers gebruiken deze kwetsbaarheden om de botnetnetwerken uit te breiden, wachtwoorden te raden en andere schadelijke activiteiten te ontplooien. Beveiligingsexperts adviseren om systemen up-to-date te houden, ontwikkeltools uit productieomgevingen te verwijderen en toegang tot cloudinfrastructuur te beperken om de risico's te verkleinen.

Logins.zip maakt gebruik van Chromium zero-day: Infostealer belooft 99% inlogdiefstal in minder dan 12 seconden

Logins.zip is een nieuwe infostealer die gebruik maakt van kwetsbaarheden in de Chromium-browser. Deze browsergebaseerde tool is in staat tot het stelen van tot 99% van opgeslagen inloggegevens, cookies en autofills in slechts 12 seconden na infectie. Het kan logins, cookies, autofills en creditcardinformatie verzamelen van verschillende browsers zoals Chrome, Firefox en Edge. Logins.zip maakt gebruik van geavanceerde technieken, zoals polymorfe auto-obfuscatie en runtime-injecties, om detectie door beveiligingssoftware te vermijden. De tool wordt gepromoot op ondergrondse forums en biedt een efficiënte methode voor cybercriminelen om gegevens te stelen zonder administratieve rechten, wat het een aanzienlijke dreiging maakt voor gebruikers wereldwijd.

Nieuwe GhostGrab Android malware steelt stilletjes bankgegevens en onderschept SMS-berichten voor OTP's

Een geavanceerde Android banking trojan, genaamd GhostGrab, richt zich wereldwijd op financiële instellingen door in stilte bankgegevens te stelen en eenmalige wachtwoorden (OTP's) via SMS-berichten te onderscheppen. De malware wordt verspreid via geïnfecteerde app stores en schadelijke advertenties, waarbij gebruik wordt gemaakt van sociale engineering-technieken. GhostGrab vraagt uitgebreide machtigingen aan onder het mom van standaardapplicaties, zoals toegang tot SMS en overlaymachtigingen, om bankinloggegevens en OTP's te stelen zonder dat de gebruiker het merkt. Het virus heeft geavanceerde methoden ontwikkeld om detectie door banken te vermijden, zoals emulatordetectie en debuggercontroles. Zodra gegevens zijn gestolen, worden ze versleuteld en naar externe servers gestuurd. Deze malware heeft geleid tot een toename van gevallen van accountovernames en frauduleuze betalingen, wat financiële instellingen ertoe heeft aangezet extra beveiligingsmaatregelen te nemen.

Geavanceerde phishingaanvallen combineren FileFix en cache smuggling technieken

Cybersecurity-onderzoekers hebben een geavanceerde phishingcampagne ontdekt waarbij twee opkomende aanvalstechnieken worden gecombineerd om traditionele beveiligingsmaatregelen te omzeilen. Deze hybride benadering combineert FileFix

social engineering met cache smuggling om malware payloads te leveren zonder netwerkdetectiesystemen te activeren. De aanval begint met een valse FortiClient Compliance Checker-pagina, die slachtoffers misleidt om schadelijke opdrachten uit te voeren via het plakken van inhoud in de adresbalk van Windows Explorer. Vervolgens wordt de cache smuggling techniek gebruikt om kwaadaardige bestanden als legitieme afbeeldingsbestanden op het slachtoffer's systeem te verbergen, waardoor de malware direct vanuit de browsercache kan worden uitgevoerd zonder netwerkverkeer te genereren. De onderzoekers ontdekten ook een verfijnde Exif smuggling techniek die gebruikmaakt van metadata in JPG-afbeeldingen om schadelijke payloads verborgen te houden, wat de detectie door traditionele methoden verder bemoeilijkt.

Dreigingsactoren adverteren Anivia Stealer-malware op darkweb, omzeilt UAC-beveiliging

Anivia Stealer, een geavanceerde informatie-roofmalware, wordt momenteel aangeboden op ondergrondse forums. De malware, ontwikkeld door de dreigingsactor ZeroTrace, richt zich op Windows-systemen, van verouderde XP-installaties tot de nieuwste Windows 11-omgevingen. Het programma maakt gebruik van geavanceerde technieken om de User Account Control (UAC) te omzeilen, waardoor het zonder waarschuwing van het systeem kan opereren. Het steelt gevoelige gegevens zoals browserwachtwoorden, cryptowallets en authenticatiecookies. Anivia Stealer wordt aangeboden via een abonnementsmodel, variërend van €120 voor één maand tot €680 voor levenslange toegang. Onderzoekers hebben de promotiematerialen van de dreigingsactor op cybercriminaliteitsmarkten geïdentificeerd, waarbij de malware wordt gepromoot met als voordeel de automatische privilegeverhoging en het omzeilen van systeembeveiligingsmechanismen. De malware maakt gebruik van versleutelde communicatiekanalen om detectie te vermijden.

Beast ransomware verspreidt zich via SMB-poorten over netwerken

Beast ransomware is een belangrijke dreiging in cyberspace en werd in februari 2025 gelanceerd. Het is een evolutie van de Monster ransomware en heeft zich snel gepositioneerd als een grote Ransomware-as-a-Service (RaaS)-operatie. De groep heeft in juli 2025 een Tor-gebaseerde dataleksite geïntroduceerd en heeft sinds

augustus 2025 wereldwijd 16 slachtoffers gemeld, waaronder organisaties in de VS, Europa, Azië en Latijns-Amerika. Beast verspreidt zich via een netwerkpropagatie-aanpak waarbij het SMB-poorten van gecompromitteerde systemen scant. Dit stelt het in staat om zich door netwerkinfrastructuren te verplaatsen en toegang te krijgen tot gedeelde netwerkmappen. De aanvallers gebruiken phishing als een belangrijke toegangsmethode, vaak samen met de Vidar Infostealer voor gegevensdiefstal voorafgaand aan het inzetten van ransomware. Deze verspreidingsmethode maakt het moeilijk om de dreiging te stoppen zonder adequate netwerkbeveiliging en monitoring.

Gunra ransomware richt zich op Windows en Linux systemen met twee versleutelingsmethoden

Gunra ransomware, actief sinds april 2025, richt zich wereldwijd op zowel Windows- als Linux-systemen. Deze ransomware-campagne gebruikt twee versleutelingstechnieken: een voor Windows (EXE-bestanden) en een voor Linux (ELF-binaries), wat de aanvalscapaciteit vergroot. Organisaties in verschillende sectoren, waaronder de regio Azië-Pacifisch, hebben melding gemaakt van infecties. Gunra volgt een bekend ransomware-model: het versleutelen van kritieke bestanden, het stelen van gevoelige data en het eisen van losgeld, met dreigingen van openbaarmaking bij niet-betaling. Een opvallende technische zwakte werd gevonden in de Linux-versie van de malware, die gebruik maakt van een cryptografisch onveilige methode voor het genereren van versleuteling sleutels, waardoor brute-force aanvallen mogelijk zijn. Dit staat in contrast met de Windows-versie, die een veiligere cryptografische aanpak hanteert, waardoor decryptie vrijwel onmogelijk is.

Malafide npm-pakketten met auto-run functie deployen multi-stage credential harvester

Tien kwaadaardige npm-pakketten zijn ontdekt die automatisch worden uitgevoerd tijdens de installatie en een geavanceerde operatie voor het stelen van inloggegevens inzetten. Deze aanval maakt gebruik van typosquatting, waarbij populaire JavaScript-bibliotheken worden gemimicd, wat de detectie bemoeilijkt. De pakketten gebruiken de postinstall lifecycle hook van npm om direct na installatie uit te voeren, wat zorgt voor onopgemerkte werking. Het malwarepakket detecteert automatisch het besturingssysteem van de geïnfecteerde computer en voert de

aanval uit via Windows, Linux of macOS. Het bevat verschillende lagen van obfuscatie om analyse te bemoeilijken. Na installatie toont het malwarepakket een valse CAPTCHA om de legitimiteit te verbergen en te zorgen dat het niet wordt gedetecteerd door automatische beveiligingsscans. De malware verzamelt gegevens zoals browserwachtwoorden, SSH-sleutels en OAuth-tokens. De gestolen gegevens worden naar een externe server gestuurd, waardoor de aanvaller toegang krijgt tot gevoelige systemen.

Opkomst van valse investeringsplatformen die forexbeurzen imiteren om inloggegevens te stelen

Er is een grote toename van frauduleuze investeringsplatformen die zich voordoen als cryptocurrency- en forexbeurzen. Deze platformen worden gebruikt door cybercriminelen om slachtoffers wereldwijd te misleiden en geld te stelen. Ze maken gebruik van geavanceerde sociale engineering om het vertrouwen van slachtoffers te winnen en hen te manipuleren om geld over te maken naar de aanvallers. De fraudeoperaties zijn geëvolueerd van geïsoleerde aanvallen naar goed georganiseerde, grensoverschrijdende netwerken met gestructureerde rollen en langdurige campagnes. Slachtoffers worden vaak benaderd via sociale mediakanalen zoals Facebook en TikTok, waar de criminelen zich voordoen als succesvolle investeerders. De technische infrastructuur van deze platforms is geavanceerd, met hergebruikte API's en SSL-certificaten, en de platformen maken gebruik van chatbots om betalingen te verwerken. Recente acties van de autoriteiten, zoals de arrestatie van 20 mensen in Vietnam, benadrukken de enorme schaal van deze fraude-operaties.

Nieuwe Gentlemen's RaaS Aangeboden op Hackersforums, Richt zich op Windows, Linux en ESXi-systemen

Een nieuwe ransomware-as-a-service (RaaS) genaamd Gentlemen's RaaS is ontdekt op ondergrondse hackersforums. Deze platform biedt cybercriminelen de mogelijkheid om ransomware-aanvallen uit te voeren op Windows-, Linux- en ESXi-systemen, met de belofte van hoge winst. De operator, bekend als zeta88, biedt een aantrekkelijk verdienmodel waarbij 90% van de losgelden naar de afnemers gaat, terwijl de operator 10% behoudt. Dit systeem maakt gebruik van geavanceerde cryptografische methoden zoals XChaCha20 en Curve25519 en biedt specifieke

lockers voor verschillende besturingssystemen, zoals Windows, Linux en BSD, evenals een aparte locker voor ESXi-systemen. Het platform beschikt over geautomatiseerde self-propagation via WMI, PowerShell en andere commando's, wat het mogelijk maakt snel door netwerken te bewegen en meerdere systemen te versleutelen. De introductie van Gentlemen's RaaS geeft aan dat ransomware-aanvallen steeds meer toegankelijk worden voor een breder publiek van cybercriminelen wereldwijd.

Dreiging: phishingcampagne verspreidt PureHVNC RAT via juridische documenten

Tussen augustus en oktober 2025 heeft een geavanceerde phishingcampagne slachtoffers gemaakt onder Spaanstalige gebruikers, met name in Colombia, door vervalste e-mails te versturen die lijken op officiële communicatie van het Openbaar Ministerie van Colombia. De e-mails bevatten een sociale engineering-aanval waarbij ontvangers worden verleid met valse meldingen over rechtszaken. Het kwaadaardige bestand wordt via een SVG-bijlage gedistribueerd, die een automatisch gedownloade ZIP-archief bevat. Dit archief bevat een hernoemde javaw.exe-bestand dat gebruikt wordt voor DLL-side-loading en de installatie van PureHVNC-malware, een geavanceerde remote access trojan (RAT). Deze malware is bekend om zijn sterke vermijdingscapaciteiten en wordt vaak op darkweb-forums verhandeld. De campagne markeert de eerste keer dat PureHVNC zich richt op Spaanstalige doelwitten met deze methoden. De infectie maakt gebruik van meerdere stadia om detectie te vermijden en biedt aanvallers volledige controle over de geïnfecteerde systemen.

Wereldwijde experts zetten zich in voor gezamenlijke strijd tegen crypto-ondersteunde criminaliteit

De 9e Wereldconferentie over Criminale Financiën en Crypto-activa heeft de nadruk gelegd op de groeiende professionalisering van de misbruik van crypto. Tijdens de bijeenkomst in Wenen werd het belang van drie prioriteiten benadrukt: de ontwikkeling van gemeenschappelijke standaarden, versterkte samenwerking en investeringen in capaciteit. De misbruik van blockchaintechnologie voor criminele doeleinden, zoals drugshandel, financiering van terrorisme en ontwijking van sancties, is steeds complexer en georganiseerder geworden. De samenwerking tussen de publieke en private sector speelt een cruciale rol in de bestrijding van deze dreigingen. Echter, er blijven aanzienlijke hiaten in wetgeving, uitvoering en

capaciteit. De focus ligt op het verbeteren van internationale samenwerking en het ontwikkelen van specialistische teams die in staat zijn cryptoactiva te traceren en voor slachtoffers te herstellen.

Google Chrome gaat websites volgend jaar standaard via https laden

Google Chrome zal vanaf volgend jaar oktober standaard websites via https laden. Als een website enkel via http bereikbaar is, zal de browser de gebruiker om toestemming vragen en waarschuwen voor de risico's die hiermee gepaard gaan. Deze wijziging, die eerst in april 2026 wordt ingeschakeld voor gebruikers met de Enhanced Safe Browsing-optie, wordt door Google geïntroduceerd om de veiligheid te vergroten. Aanvallers kunnen http-verbindingen onderscheppen, waardoor gebruikers mogelijk malafide content laden. Het techbedrijf waarschuwt dat http-sites vaak redirecten naar https-sites, waardoor gebruikers geen kans krijgen om de waarschuwing in de adresbalk te zien. In eerste instantie zal de wijziging enkel gelden voor publieke http-sites, terwijl private sites geen waarschuwing zullen tonen. Google hoopt hiermee de veiligheid van webgebruikers wereldwijd te verbeteren door het gebruik van onveilige verbindingen te beperken.

Duitse overheid geeft advies bij gehackt account

De Duitse overheid heeft een checklist gepubliceerd om burgers te helpen bij het herstellen van een gehackt account. Het advies komt van de Duitse federale politie en het Bundesamt für Sicherheit in der Informationstechnik (BSI). De checklist legt uit hoe gebruikers een gehackt account kunnen herkennen en wat ze moeten doen. Als er geen toegang meer is tot het account, wordt aanbevolen om hulp van de provider in te schakelen en contacten te waarschuwen. Als toegang nog mogelijk is, moeten gebruikers het wachtwoord wijzigen en actieve sessies beëindigen. Ook wordt geadviseerd om tweefactorauthenticatie in te schakelen en beveiligingsupdates te installeren. De checklist biedt ook preventieve maatregelen, zoals het vermijden van openbare wifi-netwerken en voorzichtig zijn met het delen van informatie. Dit komt nadat acht procent van de Duitse respondenten in een BSI-onderzoek aangaf slachtoffer te zijn geweest van een gehackt account.

Problemen bij NS door grote internetstoring Microsoft

De Nederlandse Spoorwegen (NS) ervaren momenteel storingen in de online-reisplanner, de kaartautomaten en de verhuur van OV-fietsen. Deze problemen worden veroorzaakt door een internationale storing bij Microsoft Azure, de cloudservice waarvan NS gebruikmaakt. Sinds 17.00 uur zijn de reisplanner en ticketverkoop niet beschikbaar, maar de reisinformatie op de stationsborden en de toegangspoortjes functioneren nog wel. Er is nog geen duidelijkheid over de duur van de storing. NS raadt reizigers aan om de website 9292.nl te raadplegen voor reisinformatie. De storing volgt op een eerdere technische fout bij de verhuur van OV-fietsen die maandag al speelde. Microsoft heeft inmiddels de storing bevestigd op zijn statuspagina.

Microsoft ondervindt een aanhoudende DNS-storing die wereldwijd klanten hindert bij het inloggen op bedrijfsnetwerken en toegang tot Microsoft Azure en Microsoft 365-diensten. De storing, die al bijna een uur duurt, heeft geleid tot server- en websiteverbindingproblemen voor duizenden gebruikers. Aangetaste klanten ervaren onder andere inlogproblemen bij Intune en Azure-portalen, evenals problemen met de Exchange-beheerdersinterface. Er wordt ook gemeld dat de Azure Front Door Content Delivery Network (CDN)-service uitvalt. Diverse organisaties, waaronder zorginstellingen, hebben last van authenticatieproblemen die de toegang van medewerkers tot bedrijfsnetwerken belemmeren. Microsoft heeft verklaard dat de storing verband houdt met DNS-problemen en adviseert klanten om alternatieve toegangsmethoden, zoals PowerShell of CLI, te gebruiken om resources te bereiken. Het bedrijf onderzoekt de oorzaak en werkt aan herstel van de dienstverlening.

Ex-CISA-hoofd stelt dat AI het einde van de cybersecurity kan betekenen

Jen Easterly, voormalig directeur van CISA, stelde tijdens een conferentie in San Diego dat kunstmatige intelligentie (AI) mogelijk het einde van de cybersecuritysector zou kunnen betekenen. Ze beweerde dat de meeste cyberinbraken het gevolg zijn van slecht ontworpen software die vol zit met kwetsbaarheden. AI zou in staat kunnen zijn deze fouten sneller te detecteren en zo de behoefte aan traditionele beveiligingsteams te verminderen. Easterly benadrukte dat softwarebedrijven vaak snelheid en kosten boven veiligheid stellen, wat de fundamentele oorzaak is van veel cyberdreigingen. Hoewel AI aanvallers krachtiger maakt, ziet ze ook mogelijkheden om deze technologie te gebruiken voor het verbeteren van softwarekwaliteit en beveiliging. Ze stelde verder dat als AI op de juiste manier wordt ingezet, het de verdedigers in cyberspace een significante voorsprong kan geven.

Verkoop van webservers Remote Shell Tool op het darkweb

Op 28 oktober 2025 werd via het darkweb melding gemaakt van de vermeende verkoop van een Remote Shell Tool voor webservers. Dit soort tools wordt vaak door cybercriminelen gebruikt om ongeautoriseerde toegang te verkrijgen tot servers. De verkoop van dergelijke tools op het darkweb vergroot de risico's voor bedrijven, aangezien aanvallers hiermee toegang kunnen krijgen tot systemen. Dit kan leiden tot misbruik, zoals data-exfiltratie of het installeren van ransomware. Het incident benadrukt de noodzaak voor bedrijven om de beveiliging van hun servers en netwerken te verbeteren en om waakzaam te blijven voor mogelijke kwetsbaarheden.

Quasar RAT C2-domein via Ngrok-tunnel geïdentificeerd

Een command-and-control (C2) domein, gebruikmakend van de Ngrok tunneling-infrastructuur, is gekoppeld aan de activiteiten van de Quasar RAT. Het domein 10.tcp.eu.ngrok.io werd waargenomen als verbonden met een AWS-IP-adres. Hoewel de Ngrok-tunnel momenteel inactief is en een foutpagina weergeeft, wordt deze infrastructuur vaak gebruikt door cybercriminelen voor tijdelijke of wegwerpbare C2-punten. De informatie wordt als 100% betrouwbaar geclassificeerd. Organisaties wordt aangeraden om dit domein en gerelateerde Ngrok-subdomeinen te blokkeren in hun perimeter- en endpointbeveiligingsbeleid. Tevens moeten ze alert zijn op indicaties van Quasar RAT, zoals ongebruikelijke verbindingen of activiteit met Ngrok-tunnels. Het misbruik van Ngrok-diensten door trojans zoals Quasar RAT vergemakkelijkt het opzetten van kortdurende, versleutelde C2-kanalen die traditionele beveiligingsmaatregelen omzeilen.

Claimed Sale of Windscribe Checker v1.0 op het darkweb

Op 29 oktober 2025 werd via het darkweb de verkoop van een tool, de "Windscribe Checker v1.0", aangekondigd. Deze tool stelt gebruikers in staat om inloggegevens van Windscribe VPN-accounts te controleren en toegang te verkrijgen tot beveiligde accounts. De tool werd gepromoot als een commerciële aanbieding op verschillende forums en marktplaatsen op het darkweb. Dit type tool wordt vaak gebruikt door cybercriminelen om onbevoegde toegang te verkrijgen tot VPN-accounts en andere beveiligde systemen. De verkoop van dergelijke tools op het darkweb kan leiden tot

verdere schade, waaronder identiteitsdiefstal en financiële fraude, en vormt een voortdurende bedreiging voor de beveiliging van gebruikers van VPN-diensten. Het gebruik van dergelijke hulpmiddelen versterkt de gevaren voor zowel individuele gebruikers als bedrijven die afhankelijk zijn van veilige internetverbindingen.

Aisuru-botnet schakelt van DDoS-aanvallen naar verhuur van residentiële proxies

Het Aisuru-botnet, verantwoordelijk voor recordbrekende DDoS-aanvallen dit jaar, heeft zijn strategie veranderd door duizenden geïnfecteerde IoT-apparaten te gebruiken voor de verhuur aan proxy-diensten. Deze diensten helpen cybercriminelen hun verkeer te anonimiseren door gebruik te maken van zogenaamde "residentiële proxies", wat het moeilijker maakt om kwaadaardig verkeer te traceren. Aisuru heeft inmiddels meer dan 700.000 apparaten geïnfecteerd, zoals slecht beveiligde routers en beveiligingscamera’s, en heeft in de zomer van 2025 een van de grootste DDoS-aanvallen ooit uitgevoerd. De verhuur van proxies wordt steeds meer gebruikt voor dataverzameling, vooral voor kunstmatige-intelligentieprojecten, die profiteren van het moeilijk te detecteren karakter van dit verkeer. De toename van proxies leidt tot grote dataverzamelinspanningen, waardoor onder andere scraping van content voor AI-modellen gemakkelijker wordt. Autoriteiten in de VS en Europa volgen de activiteiten van Aisuru nauwlettend.