Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

21-10-2025:

Nederlandse inlichtingendiensten delen minder met Amerika sinds Trump, kijken meer naar Europa

De AIVD en MIVD delen sinds het aantreden van Donald Trump minder informatie met hun Amerikaanse tegenhangers, vooral vanwege zorgen over de politisering van inlichtingen en schendingen van mensenrechten in de VS. De diensten bekijken per geval of informatie gedeeld kan worden, en stellen dat ze alert zijn op mogelijke misbruik van inlichtingen. Desondanks blijven de banden met de CIA en NSA goed, maar de nadruk ligt nu meer op samenwerking met Europese landen, waaronder Noord-Europa, Groot-Brittannië, Duitsland, en de Scandinavische landen. De toegenomen Russische cyberdreiging heeft deze Europese samenwerking versterkt, aangezien Rusland jaarlijks meerdere succesvolle hacks uitvoert in Nederland. Akerboom en Reesink benadrukken dat de afname in samenwerking met de VS een gevolg is van politieke veranderingen in Amerika en de veranderende aard van internationale dreigingen.

Russische hackers stelen gevoelige gegevens van Britse defensie

Russische hackers hebben toegang gekregen tot de gegevenssystemen van het Britse Ministerie van Defensie en gestolen documenten die gevoelige informatie bevatten over militaire bases, waaronder RAF Lakenheath, waar de F-35-jets van de Amerikaanse luchtmacht zijn gestationeerd. Ongeveer 272.000 personeelsleden van de strijdkrachten zouden getroffen zijn. De cybercriminelen kregen tijdelijk toegang tot het systeem van een onderhouds- en bouwcontractor, de Dodd Group, via ransomware. Er werd bevestigd dat persoonlijke gegevens, zoals namen, bankgegevens en adressen, van militair personeel en veteranen zijn gepubliceerd. Het ministerie van Defensie is een onderzoek gestart naar het incident en bevestigde dat er gegevens op het Dark Web zijn verschenen. Dit volgt op eerdere datalekken, waaronder een incident in 2022 waarin vertrouwelijke informatie over de Afghanistan Response Route werd blootgesteld.

PoC voor Linux HFSC Eltree Use-After-Free kwetsbaarheid in Debian 12 gepubliceerd

Een proof-of-concept (PoC) voor de Linux HFSC Eltree Use-After-Free kwetsbaarheid, aangeduid als CVE-2025-38001, is gepubliceerd. Deze kwetsbaarheid is aanwezig in Debian 12 en kan ernstige gevolgen hebben voor de veiligheid van systemen die deze versie gebruiken. De kwetsbaarheid is ontdekt door een externe onderzoeker en er wordt een beloning van $82.000 geboden voor het melden van een werkende exploit. Het PoC is beschikbaar op GitHub en bevat technische details die kunnen helpen bij het begrijpen van de exploitatie van de kwetsbaarheid. De ontdekking benadrukt het belang van het snel patchen van systemen die kwetsbaar zijn voor deze beveiligingsfout om potentiële aanvallen te voorkomen.

Apache Camel kwetsbaarheden (CVE-2025-27636 & CVE-2025-29891) kunnen interne methoden uitvoeren

De Apache Camel kwetsbaarheden CVE-2025-27636 en CVE-2025-29891, die versies 4.10.0-4.10.1, 4.8.0-4.8.4 en 3.10.0-3.22.3 van de software beïnvloeden, stellen aanvallers in staat om interne Camel-methoden uit te voeren. Het exploiteren van deze kwetsbaarheden kan leiden tot ernstige gevolgen voor systemen die deze versies draaien. Beheerders wordt geadviseerd om snel de patch te implementeren en de nodige beveiligingsmaatregelen te treffen om schade te voorkomen. De kwetsbaarheden zijn gedocumenteerd en er zijn mitigaties beschikbaar via de officiële Apache Camel beveiligingspagina en GitHub. De versies die getroffen zijn, omvatten zowel oudere als recentere releases, wat betekent dat organisaties met verschillende versies van Apache Camel kwetsbaar kunnen zijn. Het is belangrijk voor bedrijven om de juiste updates en beveiligingsmaatregelen door te voeren om risico's te minimaliseren.

Beveiligingslekken in Windows SMB-client en Kentico Xperience actief misbruikt

Er zijn beveiligingslekken ontdekt in de Windows SMB-client en Kentico Xperience die momenteel actief worden misbruikt bij cyberaanvallen. Het Amerikaanse CISA waarschuwt voor een kwetsbaarheid in de Windows SMB-client, aangeduid als CVE-2025-33073, die aanvallers in staat stelt SYSTEM-rechten te verkrijgen. Microsoft bracht eerder een beveiligingsupdate uit, maar aanvallers maken inmiddels actief misbruik van het lek. De impact van de kwetsbaarheid wordt als ernstig beoordeeld met een score van 8.8 op de CVSS-schaal. Daarnaast waarschuwt CISA ook voor

twee kritieke kwetsbaarheden in Kentico Xperience (CVE-2025-2746 en CVE-2025-2747), waarmee aanvallers zonder wachtwoord als administrator kunnen inloggen. Deze kwetsbaarheden hebben een impactscore van 9.8. Kentico bracht al een update uit, maar CISA heeft geen details gegeven over de misbruikgevallen.

76.000 WatchGuard-firewalls missen update voor kritiek RCE-lek, waarvan 1387 in Belgie en 1186 in Nederland

Ongeveer 76.000 Firebox-firewalls van WatchGuard, waarvan 1.387 in België en 1.186 in Nederland, zijn kwetsbaar voor een kritieke kwetsbaarheid die remote code execution (RCE) mogelijk maakt. Het beveiligingslek, aangeduid als CVE-2025-9242, heeft een zwaarte van 9.3 op de schaal van 10. De kwetsbaarheid treft zowel de mobile user VPN als de branch office VPN die gebruik maken van IKEv2, vooral wanneer deze geconfigureerd zijn met een dynamic gateway peer. Hoewel een patch op 17 september beschikbaar werd gesteld, blijkt uit scans van de Shadowserver Foundation dat veel beheerders deze update nog niet hebben geïnstalleerd. De meeste kwetsbare firewalls bevinden zich in de Verenigde Staten, maar ook in Nederland en België werden respectievelijk 1.186 en 1.387 kwetsbare apparaten geïdentificeerd.

Dolby Digital Plus kwetsbaarheid maakt RCE-aanvallen via audio op Android mogelijk

Een kritieke 0-click kwetsbaarheid in de Dolby Digital Plus software voor audiodecodering is ontdekt, waardoor aanvallers op afstand kwaadaardige code kunnen uitvoeren via ogenschijnlijk onschuldige audiobestanden. Onderzoekers van Google Project Zero, Ivan Fratric en Natalie Silvanovich, identificeerden een out-of-bounds schrijfprobleem in de DDPlus Unified Decoder die gegevens in audiobestanden verwerkt. Dit probleem ontstaat door een integer overflow in lengtemetingen, wat leidt tot onvoldoende bufferallocatie en het omzeilen van grenzen bij het schrijven van gegevens. Android-apparaten lopen bijzonder risico, aangezien het decoderingsproces automatisch audio verwerkt, waardoor aanvallen mogelijk zijn zonder dat de gebruiker actie onderneemt. Aanvallers kunnen gemanipuleerde audiobestanden via RCS-berichten verzenden, wat kan leiden tot een crash of, bij verdere exploitatie, code-executie. Gebruikers wordt geadviseerd om snel hun apparaten en berichten-apps bij te werken.

Xubuntu website verspreidde cryptostelende malware via downloadlink

De officiële website van Xubuntu, een op Ubuntu gebaseerde Linux-distributie, heeft tijdelijk cryptostelende malware verspreid. De downloadknop voor het torrent-bestand verwees naar een zip-bestand genaamd "Xubuntu-Safe-Download.zip", dat een .exe-bestand bevatte. Dit bestand installeerde clipper-malware, die speciaal is ontworpen om cryptovaluta te stelen van besmette systemen. De schadelijke link stond twaalf uur lang op de website, voordat deze werd verwijderd. Het is nog onbekend hoe de link op de website is geplaatst. Xubuntu's team verklaarde dat het incident te maken had met een "slip-up" in de hostingomgeving. Om toekomstige incidenten te voorkomen, wordt de website gemigreerd naar een statische omgeving. Gebruikers van cryptovaluta lopen risico op verlies van fondsen doordat de malware het gekopieerde walletadres vervangt met dat van de aanvaller.

TikTok-video’s verspreiden infostealers via ClickFix-aanvallen

Cybercriminelen maken gebruik van TikTok-video's die zich voordoen als gratis activatiegidsen voor populaire software zoals Windows, Spotify en Netflix om informatie-roof malware te verspreiden. Deze video's bevatten zogenaamde "fixes" die gebruikers misleiden om kwaadaardige PowerShell-commando's of andere scripts uit te voeren. Wanneer het commando wordt uitgevoerd, verbindt PowerShell zich met een externe website om een script te downloaden, wat resulteert in de installatie van de Aura Stealer-malware. Deze malware verzamelt opgeslagen inloggegevens van browsers, crypto-portemonnees en andere applicaties. Een extra payload kan worden gedownload die zelfcode compilet met behulp van .NET’s ingebouwde Visual C# Compiler. Gebruikers die deze stappen uitvoeren, moeten hun wachtwoorden onmiddellijk resetten. ClickFix-aanvallen worden steeds vaker gebruikt om verschillende malwarestammen te verspreiden, zoals ransomware en diefstal van cryptocurrency.

Zelfverspreidende GlassWorm-malware treft OpenVSX en VS Code-registers

Een nieuwe supply-chain aanval richt zich op ontwikkelaars op de OpenVSX- en Microsoft Visual Studio-marktplaatsen met de zelfverspreidende malware genaamd GlassWorm. De malware is naar schatting 35.800 keer geïnstalleerd. GlassWorm

verbergt zijn kwaadaardige code door gebruik te maken van onzichtbare tekens en verspreidt zich via gestolen accountgegevens om meer extensies te infecteren. De aanvallers gebruiken de Solana-blockchain voor command-and-control, wat het moeilijk maakt om de aanval te stoppen, met Google Calendar als back-upmethode. Nadat de malware is geïnstalleerd, probeert deze inloggegevens voor GitHub, npm en OpenVSX te stelen, evenals gegevens van cryptocurrency-wallets uit 49 extensies. Het eindstadium van de malware, genaamd ZOMBI, maakt geïnfecteerde systemen onderdeel van een crimineel netwerk. Ondanks pogingen om de extensies te verwijderen, blijven sommige van de geïnfecteerde versies beschikbaar voor download.

Scattered Lapsus$ Hunters ontmanteld na arrestatie van admins

Het hackercollectief Scattered Lapsus$ Hunters (SLSH) is reportedly ontmanteld nadat verschillende admins, waaronder een lid bekend als "Shiny", werden gearresteerd. Deze arrestaties volgen op beschuldigingen van doxxing, waarbij federale agenten het doelwit waren. De claims over deze ontwikkelingen komen van een bron genaamd Sevy. Het is nog onduidelijk of er verdere gevolgen zijn voor andere leden van de groep. De actie komt na een reeks van operaties van het collectief die gericht waren op het compromitteren van systemen en het lekken van vertrouwelijke informatie. De arrestaties kunnen een significante impact hebben op de activiteiten van SLSH, maar de toekomst van de groep blijft onduidelijk.

Amazon verhelpt wereldwijde storing bij Amazon Web Services

Amazon heeft een grote storing in Amazon Web Services (AWS) opgelost waardoor wereldwijd talloze websites en apps tijdelijk onbereikbaar waren. Diensten als Coinbase, Signal, Zoom, Fortnite en Amazon’s eigen Ring-camera’s werden getroffen, evenals diverse banken en overheidssites. Volgens Amazon werd de storing veroorzaakt door een dns-probleem bij het DynamoDB API endpoint, een onderdeel van de NoSQL databaseservice DynamoDB. Hierdoor raakten meerdere AWS-diensten verstoord. Op platforms als Downdetector en Allestoringen.nl kwamen duizenden meldingen binnen van gebruikers die problemen ondervonden. Inmiddels zijn de meeste diensten hersteld, maar sommige klanten moeten hun dns-cache nog handmatig wissen om verbinding te herstellen. De exacte technische oorzaak van het dns-probleem is nog niet door Amazon toegelicht.

F5 gehackt via beveiligingslek in eigen software

5 werd eind 2023 gehackt door aanvallers via een kwetsbaarheid in hun eigen software, die onopgemerkt bleef voor twee jaar. De aanvallers wisten toegang te verkrijgen tot gevoelige gegevens, waaronder broncode en informatie over niet-geopenbaarde kwetsbaarheden. Het beveiligingslek in de software was toegankelijk via internet, en volgens bronnen volgde het personeel van F5 niet de beveiligingsadviezen die het zelf aan klanten verstrekte. F5 ontdekte de inbraak pas in augustus 2025. De aanvallers, vermoedelijk een statelijke actor, hadden langdurige toegang tot de systemen. Het incident leidde tot een noodbevel van de Amerikaanse overheid, die federale diensten verordonneerde om snel updates voor F5-producten te installeren. F5 waarschuwde sinds eind 2023 al voor kwetsbaarheden in hun BIG-IP-platform, dat door duizenden apparaten wereldwijd wordt gebruikt.

AFM en DNB waarschuwen voor digitale afhankelijkheid van Amerikaanse techbedrijven

De Autoriteit Financiële Markten (AFM) en De Nederlandsche Bank (DNB) hebben in een nieuw rapport gewaarschuwd voor de groeiende afhankelijkheid van banken en financiële instellingen van Amerikaanse techbedrijven. Deze afhankelijkheid kan leiden tot concentratie- en systeemrisico’s, waarbij storingen bij één leverancier de hele sector kunnen raken. Het rapport benadrukt de noodzaak voor banken om hun digitale weerbaarheid te versterken en om te werken aan Europese digitale autonomie. Veel banken gebruiken dezelfde IT-aanbieders, wat de risico's vergroot door storingen en cyberincidenten bij deze bedrijven. Banken stappen steeds vaker over op cloudgebaseerde diensten, wat de afhankelijkheid verder vergroot. AFM en DNB stellen dat het verminderen van deze digitale afhankelijkheid op lange termijn een gezamenlijke Europese aanpak vereist en dat volwaardige Europese alternatieven voor techbedrijven ontwikkeld moeten worden.

ACSC komt met checklist voor gebruik clouddiensten: 'risico kun je niet outsourcen'

Het Australische Cyber Security Centre (ACSC) heeft een checklist gepubliceerd voor individuen en mkb-bedrijven die gebruik willen maken van clouddiensten. De

boodschap is duidelijk: gebruikers kunnen risico's niet outsourcen naar de cloudprovider. Het ACSC benadrukt dat de verantwoordelijkheid voor zaken als dataverlies, dataverandering of verlies van toegang bij de gebruiker ligt, zelfs wanneer een cloudprovider wordt ingeschakeld. De checklist maakt duidelijk waar de verantwoordelijkheden van zowel de gebruiker als de cloudprovider liggen, bijvoorbeeld op het gebied van back-ups, incidentresponse en toegangsbeheer. Verder wordt geadviseerd cloudproviders te kiezen die 'secure by default' diensten aanbieden, waarbij de diensten standaard veilig zijn zonder dat de gebruiker extra actie hoeft te ondernemen. Ook moet de provider duidelijk communiceren over de risico's bij het wijzigen van de standaardinstellingen.

Alleged sale of Monolock Ransomware V1.0 via dark web

Er is melding gemaakt van de vermeende verkoop van Monolock Ransomware V1.0 op het dark web. Deze ransomware zou binnenkort beschikbaar komen voor cybercriminelen en een potentieel groot risico vormen voor slachtoffers wereldwijd. De verkoop is besproken door het account "Dark Web Informer" op X, waar het incident werd gedeeld met de bredere cyberbeveiligingsgemeenschap. Monolock Ransomware is bekend om zijn vermogen om bedrijfsnetwerken te compromitteren, systemen te vergrendelen en gegevens te eisen van slachtoffers. Hoewel de exacte details van de verkoop en verspreiding momenteel onduidelijk zijn, wordt verwacht dat deze ransomware verder zal bijdragen aan de groeiende dreiging van ransomware-aanvallen die wereldwijd plaatsvinden. Experts waarschuwen bedrijven om hun systemen goed te beveiligen tegen dit soort aanvallen, aangezien de ransomware snel kan worden ingezet zodra het beschikbaar komt.

Overheid onderzoekt risico's van Roblox voor jonge kinderen

Een groot aantal Nederlandse kinderen maakt gebruik van gameplatforms zoals Minecraft en Roblox, maar de gewelddadige en seksuele inhoud op deze platforms roept zorgen op. Het kabinet onderzoekt momenteel of Roblox en andere platforms voldoende maatregelen nemen om de veiligheid van kinderen te waarborgen. Staatssecretaris Eddie van Marum (BBB) gaf aan dat online leren en contact maken waardevol is, maar dat er ook risico's zijn zoals pesten en ongewenste contacten. Roblox wordt al bekritiseerd vanwege de weinige bescherming tegen schadelijke invloeden, waarbij kinderen onder andere worden aangespoord tot seksueel misbruik

en het delen van naaktfoto's. Hoewel het platform meldt maatregelen te nemen, zoals filters en meldopties, blijken deze vaak eenvoudig te omzeilen. Ouders kunnen ouderlijk toezicht instellen en kinderen bewust maken van de gevaren van online interactie.

131 Chrome-extensies misbruiken WhatsApp Web voor massale spamcampagne

Onderzoekers hebben een gecoördineerde campagne ontdekt waarbij 131 herschreven kloon-extensies van WhatsApp Web voor Google Chrome werden ingezet om massale spam te versturen naar Braziliaanse gebruikers. Deze extensies, die dezelfde codebase, ontwerp en infrastructuur delen, hebben ongeveer 20.905 actieve gebruikers. Ze automatiseren berichten op WhatsApp Web om de anti-spambeperkingen van het platform te omzeilen, zonder dat gebruikers hun toestemming hoeven te geven. De extensies lijken klantrelatiebeheer (CRM)-tools te zijn, maar dienen in werkelijkheid om bulkberichten te verzenden. De campagne loopt al minstens negen maanden en de extensies worden nog steeds geüpdatet. Hoewel deze extensies geen traditionele malware zijn, worden ze als risicovolle spamware beschouwd die misbruik maakt van platformregels. Het doel van de aanval is om de anti-spambeperkingen van WhatsApp te omzeilen en massale berichten te versturen.

Forumpost vraagt om 100K voor snelle prijsdeal op Dark Web

Op 20 oktober 2025 werd een forumpost op het dark web geplaatst waarin een dreigingsactor een bedrag van 100.000 dollar vroeg voor een zogenaamde "blitz prijs". Deze post is afkomstig van een forum waar verschillende cybercriminelen en dreigingsactoren actief zijn. De exacte context van de gevraagde som is onduidelijk, maar het lijkt te wijzen op een tijdelijke aanbieding of snelle transactie, mogelijk gerelateerd aan gestolen gegevens of andere cybercriminaliteit. Het gebruik van dergelijke posts is typerend voor de manier waarop op het dark web verschillende diensten of informatie snel verhandeld kunnen worden. Dit soort transacties heeft vaak te maken met vertrouwelijke of illegale activiteiten, waarbij de snelle handel in informatie of middelen centraal staat.

Hôpital de Pontarlier (FR) slachtoffer van cyberaanval, systeem platgelegd

In de nacht van zaterdag 18 op zondag 19 oktober werd het Centre hospitalier intercommunal de Haute-Comté in Pontarlier getroffen door een cyberaanval. Het ziekenhuis, inclusief alle faciliteiten zoals de EHBO-afdeling, had zijn volledige informaticasysteem uitgeschakeld na de aanval. Het werd getroffen door een “cryptolocker”-type aanval, waarbij een deel van de gegevens werd versleuteld door de aanvallers. Er werd een losgeld geëist voor de vrijgave van de systemen. Medische zorg wordt nog steeds verleend, maar alle diensten zijn nu op papier uitgevoerd. Het ziekenhuis heeft gevraagd om het gebruik van de telefoonsystemen te beperken. De autoriteiten, waaronder de ANSSI en lokale gezondheidsinstanties, werken samen om de impact van de aanval te analyseren en de infrastructuur te beveiligen. De politie onderzoekt de zaak. Er is een klacht ingediend bij de bevoegde autoriteiten.