Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

14-11-2025:

Macron waarschuwt voor Russische spionage en cyberaanvallen in de ruimte

De Franse president Emmanuel Macron heeft gewaarschuwd dat toekomstige oorlogen in de ruimte zullen beginnen en beschuldigde Rusland van spionageactiviteiten in de ruimte sinds de invasie van Oekraïne in 2022. Volgens Macron observeren Russische satellieten Franse ruimteobjecten, worden GPS-signalen op grote schaal verstoord en vinden er cyberaanvallen plaats op ruimtegerelateerde infrastructuur. Hij noemde ook de Russische dreiging om kernwapens in de ruimte te plaatsen “schokkend” vanwege de wereldwijde risico’s. Frankrijk verhoogt daarom de militaire ruimtebegroting met 4,2 miljard euro tot 2030 en investeert in herbruikbare draagraketten en Europese ruimtewaarnemingssystemen, waaronder het Aurore-radarsysteem. Macron benadrukte dat Frankrijk, samen met Duitsland, zijn waarschuwingscapaciteiten uitbreidt en onafhankelijk wil blijven van grote buitenlandse spelers en commerciële ruimtebedrijven.

Automatisering versnelt de cyberoorlog: Aanvallen sneller dan patches

In 2025 bleek uit meerdere industriële rapporten dat 50-61% van de nieuw ontdekte kwetsbaarheden binnen 48 uur na publicatie wordt gemanipuleerd door aanvallers. Dit heeft geleid tot een nieuwe cyberstrijd waarin de snelheid van exploitatie en patching cruciaal is. Cybercriminelen hebben hun processen volledig geautomatiseerd, waarbij AI en geautomatiseerde scripts worden ingezet om snel exploitcode te ontwikkelen en te verspreiden. Dit creëert een gap tussen de snelheid van aanvallen en de vaak langzamere reacties van beveiligingsteams, die afhankelijk zijn van manuele patchcyclusmethodes. De efficiëntie van aanvallers ligt in hun vermogen om te werken met grote volumes, waarbij ze snelheid en automatisering benutten. Organisaties moeten hun benadering van cyberbeveiliging herzien, waarbij automatisering en snelle actie centraal staan om de strijd tegen deze steeds snellere dreigingen aan te gaan. De toekomst van cybersecurity is afhankelijk van de snelheid waarmee verdedigers reageren op kwetsbaarheden.

CISA waarschuwt voor kwetsbaarheid in WatchGuard firewalls, 601 in Nederland en 1154 in België

De Amerikaanse CISA (Cybersecurity & Infrastructure Security Agency) heeft een waarschuwing uitgegeven voor een ernstige kwetsbaarheid in WatchGuard Firebox firewalls, welke actief wordt misbruikt in cyberaanvallen. De kwetsbaarheid, aangeduid als CVE-2025-9242, stelt aanvallers in staat om op afstand kwaadaardige code uit te voeren op kwetsbare apparaten door een out-of-bounds schrijfzwakte in de Fireware OS 11.x, 12.x en 2025.1 versies. CISA heeft deze kwetsbaarheid toegevoegd aan de lijst van Bekende Exploiteerbare Kwetsbaarheden (KEV) en gaf overheidsinstanties tot 3 december de tijd om hun systemen te patchen. WatchGuard had in september al beveiligingspatches uitgebracht, maar bevestigde pas eind oktober dat de kwetsbaarheid actief werd misbruikt. Wereldwijd zijn er nog duizenden kwetsbare apparaten, waarvan 601 in Nederland en 1154 in België. Organisaties wordt aangeraden om deze kwetsbaarheid zo snel mogelijk te verhelpen.

Microsoft SQL Server kwetsbaarheid verhoogt privileges voor aanvallers

Microsoft heeft updates vrijgegeven om een ernstige kwetsbaarheid in SQL Server te verhelpen, die aanvallers in staat stelt om hogere systeemprivileges te verkrijgen. De kwetsbaarheid, aangeduid als CVE-2025-59499, werd op 11 november 2025 openbaar gemaakt en heeft invloed op meerdere versies van SQL Server, waaronder 2016, 2017, 2019 en 2022. Deze kwetsbaarheid is het gevolg van een onjuiste verwerking van speciale tekens in SQL-opdrachten, waardoor SQL-injectie-aanvallen mogelijk zijn. Het gevaar schuilt in het feit dat aanvallers met beperkte toegang via een netwerk de kwetsbaarheid kunnen misbruiken zonder enige gebruikersinteractie. Dit maakt de kwetsbaarheid bijzonder risicovol voor blootgestelde databaseservers. Wanneer deze wordt geëxploiteerd, kunnen aanvallers willekeurige opdrachten uitvoeren met verhoogde machtigingen, wat hen volledige controle over de SQL Server kan geven. Microsoft heeft patches uitgebracht om de systemen te beschermen tegen mogelijke misbruik.

Palo Alto PAN-OS firewall kwetsbaarheid laat aanvallers firewalls opnieuw opstarten

Palo Alto Networks heeft een kritieke denial-of-service (DoS) kwetsbaarheid onthuld in zijn PAN-OS firewallsoftware, die aanvallers zonder authenticatie in staat stelt om firewalls op afstand opnieuw op te starten door middel van speciaal geconfigureerde pakketten. Deze kwetsbaarheid, gemarkeerd als CVE-2025-4619, heeft betrekking op de dataplane van de PAN-OS software. Aanvallers kunnen de fout misbruiken

zonder gebruikersinteractie of inloggegevens. Bij succesvolle exploitatie kan de firewall onverwachts opnieuw opstarten, wat ernstige verstoringen in het netwerkverkeer kan veroorzaken. Herhaalde aanvallen kunnen de firewall zelfs in de onderhoudsmodus plaatsen, wat de werking van het netwerk aanzienlijk verstoort. De kwetsbaarheid heeft invloed op verschillende versies van PAN-OS, waaronder 10.2, 11.1 en 11.2, maar versie 12.1 is niet getroffen. Palo Alto Networks raadt organisaties aan om hun software bij te werken naar de nieuwste versies om het risico te mitigeren.

Kwetsbaarheid OpenAI Sora 2 onthult systeeminstellingen via audiotranscripties

Een kwetsbaarheid in OpenAI's videomodel Sora 2 stelt aanvallers in staat om verborgen systeeminstellingen te extraheren via audiotranscripties. Deze ontdekking, gedeeld door het AI-beveiligingsbedrijf Mindgard, benadrukt de kwetsbaarheid van multimodale AI-systemen voor het lekken van prompts, die normaal gesproken verborgen zouden moeten blijven. Het onderzoek toont aan hoe creatieve prompts via tekst, beeld, video en audio de beveiligingsmaatregelen kunnen omzeilen die ontworpen zijn om interne instructies vertrouwelijk te houden. In plaats van de traditionele tekst-naar-tekst-benadering bleek audio een effectievere manier om de systeeminstellingen te extraheren, omdat het de ruis van visuele outputs vermijdt. De blootgelegde instructies omvatten regels over videoformaten en het vermijden van auteursrechtelijk beschermde of ongepaste inhoud. Hoewel de onmiddellijke risico’s van deze kwetsbaarheid laag zijn, roept de ontdekking op tot strengere maatregelen tegen misbruik, vooral met het oog op de opkomst van deepfake-technologieën en desinformatie.

Android-fotoframes bevatten malware en kwetsbaarheden

De Uhale Android-gebaseerde digitale fotolijsten vertonen meerdere ernstige beveiligingsproblemen, waaronder de automatische download en uitvoering van malware tijdens het opstarten. Onderzoek door Quokka ontdekte dat de apparaten bij het opstarten verbinding maken met servers in China en schadelijke payloads downloaden. Deze malware is gelinkt aan de Vo1d-botnet en Mzmess-malwarefamilies. Bovendien bevat de app talrijke kwetsbaarheden, zoals de mogelijkheid voor man-in-the-middle-aanvallen en root toegang door onveilige TrustManager-implementaties. Veel van de onderzochte apparaten worden met een

standaardinstelling geleverd die SELinux uitschakelt en ze worden vaak direct geroot, wat ze kwetsbaar maakt. Andere gebreken omvatten gebrekkige versleuteling en onvoldoende bescherming tegen het injecteren van kwaadaardige code. Consumenten wordt aangeraden om alleen apparaten van vertrouwde merken te kopen die geen firmwaremodificaties bevatten.

Meer dan 67.000 nep-npm-pakketten overspoelen registry in wormachtige spam-aanval

Onderzoekers hebben een grootschalige spamcampagne ontdekt die de npm-registry heeft overspoeld met duizenden nep-pakketten sinds begin 2024. De aanval, die meer dan 67.000 nep-pakketten heeft gepubliceerd, is gericht op het verstoren van de npm-ecosysteem door willekeurige pakketten te plaatsen. De pakketten bevatten een JavaScript-bestand dat pas actief wordt wanneer een gebruiker het handmatig uitvoert, waardoor het moeilijker te detecteren is door beveiligingssystemen. Het doel lijkt geen datadiefstal of andere kwaadwillende acties te zijn, maar eerder het creëren van ruis in de registry, wat kan leiden tot onbedoelde installatie van deze nep-pakketten door ontwikkelaars. De campagne maakt gebruik van een wormachtig mechanisme, waarbij de pakketten elkaar als afhankelijkheden vermelden, wat de belasting van de registry vergroot. GitHub heeft de kwaadaardige pakketten inmiddels verwijderd.

Valse Chrome-extensie "Safery" steelt Ethereum-wallet seedfrases via Sui-blockchain

Een kwaadaardige Chrome-extensie genaamd "Safery: Ethereum Wallet" is ontdekt, die zich voordoet als een veilige Ethereum-portemonnee, maar een backdoor bevat waarmee het de seedfrases van gebruikers steelt. De extensie werd op 29 september 2025 geüpload naar de Chrome Web Store en is tot op heden nog beschikbaar. De malware encodeert de seedfrases als valse Sui-walletadressen en verstuurt microtransacties naar deze adressen vanuit een door de aanvaller gecontroleerde wallet. Dit stelt de aanvaller in staat om de seedfrases te reconstrueren en vervolgens de fondsen van de slachtoffers te stelen. Gebruikers worden geadviseerd alleen vertrouwde extensies te gebruiken en verdachte extensies te controleren op verdachte blockchain-activiteiten.

Engels-sprekend cybercrimineel ecosysteem 'The COM' drijft een breed scala aan cyberaanvallen

Het Engels-sprekende cybercriminele ecosysteem, bekend als “The COM,” is geëvolueerd van een nichegemeenschap die zich richtte op de handel in sociale mediaaccounts, naar een georganiseerde operatie die enkele van de werelds meest schadelijke cyberaanvallen uitvoert. Oorspronkelijk gericht op het stelen van socialemediagegevens, verschoven de activiteiten tijdens de cryptovalutahype van 2020-2021 naar het stelen van digitale wallets. Deze verschuiving leidde tot nieuwe aanvalsmethoden en verdienmodellen, die de wereld van cybercriminaliteit ingrijpend veranderden. Het COM fungeert nu als een uitgebreid crimineel supply chain-systeem, waar verschillende actoren gespecialiseerd zijn in taken zoals phishing, gegevensdiefstal en witwaspraktijken. Dit ecosysteem opereert volgens een model dat lijkt op legitieme bedrijfsstructuren, wat de schaal en efficiëntie van de aanvallen vergroot. Een van de meest effectieve methoden is social engineering, waarbij aanvallers zich voordoen als legitieme medewerkers om toegang te verkrijgen tot netwerken van organisaties.

MastaStealer maakt gebruik van Windows LNK-bestanden en omzeilt Defender

MastaStealer, een infostealer, wordt ingezet via spear-phishing-aanvallen waarbij LNK-bestanden in ZIP-archieven worden verzonden. Bij het openen van deze bestanden wordt een multistap-infectie geactiveerd. De LNK-bestanden openen Microsoft Edge met een legitiem ogende AnyDesk-website, terwijl in de achtergrond de MSI-installer van een gecompromitteerd domein wordt gedownload. De malware vermijdt detectie door zijn payload in een verborgen map te plaatsen en de naam van een legitiem Windows-proces na te volgen. Een PowerShell-commando wordt gebruikt om de Windows Defender-beveiliging uit te schakelen, waardoor de malware ongehinderd met command-and-control-servers kan communiceren. Dit maakt het voor traditionele beveiligingssystemen moeilijk om de aanval te detecteren. Deze techniek toont aan hoe aanvallers gebruik maken van legitieme Windows-beheerfuncties om beveiligingsmaatregelen te omzeilen.

Operatie Endgame | Criminele infrastructuur ontmanteld in internationale ransomware-operatie

In het kader van Operatie Endgame zijn belangrijke spelers uitgeschakeld die betrokken waren bij internationale cybercriminaliteit. Dit omvatte het neerhalen van infostealer Rhadamanthys, de Remote Access Trojan VenomRAT en het botnet Elysium. Deze operaties verstoorden het businessmodel van vele cybercriminelen wereldwijd, waarbij honderdduizenden slachtoffers werden getroffen door deze malware. In de afgelopen dagen werden 1025 servers, waarvan 83 in Nederland, uitgeschakeld en 20 domeinnamen in beslag genomen. De operaties zijn het resultaat van samenwerking tussen 10 landen en internationale partners zoals Europol en Eurojust. De infostealers en botnets die werden aangepakt, stalen gevoelige persoonlijke gegevens van slachtoffers. Het onderzoek gaat door, en slachtoffers kunnen hun gegevens controleren via de politiewebsite.

Operatie Endgame | Internationale operatie disruptie Rhadamanthys, VenomRAT en Elysium malware

Wetshandhavingsautoriteiten uit negen landen hebben in de nieuwste fase van Operation Endgame meer dan 1.000 servers in beslag genomen die werden gebruikt door de Rhadamanthys infostealer, VenomRAT en Elysium botnet malware-operaties. De gezamenlijke actie, gecoördineerd door Europol en Eurojust, werd ondersteund door verschillende privé-partners, waaronder Cryptolaemus en Bitdefender. Tussen 10 en 14 november 2025 werden in Duitsland, Griekenland en Nederland 11 locaties doorzocht en 20 domeinen in beslag genomen. De operatie leidde ook tot de arrestatie van een belangrijke verdachte in Griekenland, verbonden aan de VenomRAT trojan. De malware-infrastructuur, die honderdduizenden geïnfecteerde computers bevatte, had toegang tot miljoenen gestolen inloggegevens, waaronder meer dan 100.000 crypto-wallets van slachtoffers. Europol adviseert gebruikers om te controleren of hun systemen geïnfecteerd zijn via checkyourhack.politie.nl.

Operatie Endgame | Politie ontmantelt honderden servers van cybercriminelen tijdens internationale operatie

De Nederlandse politie, samen met autoriteiten uit acht andere landen, heeft 1025 servers van cybercriminelen uitgeschakeld, waarvan 83 servers in Nederland. Deze servers werden gebruikt voor het uitvoeren van cyberaanvallen. De operatie is onderdeel van de internationale samenwerking onder de naam Operatie Endgame, die in 2022 van start ging. Tijdens deze actie werden ook meerdere cybercriminelen opgepakt. De servers werden onder andere gebruikt om malware, zoals Rhadamanthys, te verspreiden, waarmee gegevens van slachtoffers werden

gestolen. De politie vermoedt dat de criminelen toegang hadden tot meer dan 100.000 cryptowallets, die mogelijk miljoenen euro's aan crypto bevatten. Er wordt aanbevolen om de website politie.nl/checkjehack te raadplegen, aangezien duizenden gestolen inloggegevens zijn ontdekt tijdens de operatie.

Verdachte aangehouden voor fraude met toegangskaarten

De politie heeft deze maand een verdachte aangehouden in verband met grootschalige fraude met toegangskaarten. Het onderzoek begon in 2021 en sindsdien zijn honderden slachtoffers gemeld. De verdachte, een 42-jarige man uit Utrecht, gebruikte diverse bankrekeningen en telefoonnummers om betalingen te ontvangen voor tickets voor festivals, concerten en sportevenementen, maar leverde de tickets nooit. Het schadebedrag loopt op tot meer dan 14.000 euro, al wordt een hoger bedrag vermoed. Naast fraude wordt de verdachte ook beschuldigd van bedreigingen en beledigingen van potentiële kopers. Er zijn honderden aangiftes van oplichting, waarvan een groot deel betrekking heeft op ticketfraude. De politie benadrukt het belang van het doen van aangifte en het kopen van tickets via officiële kanalen om dergelijke oplichtingspraktijken te vermijden.

Internationale samenwerking tegen cyber-gefaciliteerde mensensmokkel leidt tot honderden nieuwe sporen

Van 15 tot 17 oktober 2025 vond de gezamenlijke operatie Cyberprotect II plaats, waarbij tien landen deelnamen aan een driedaagse 'hackathon'. Deze operatie werd georganiseerd door INTERPOL en Europol, met als doel het verstoren van criminele netwerken die opereren in de Middellandse Zee. Gedurende de operatie werden honderden incidenten, webadressen, gebruikersnamen en telefoonnummers geïdentificeerd die mogelijk gelinkt zijn aan online mensensmokkel. De operationele teams ontdekten 269 unieke gebruikershandels en URL's, 79 potentiële smokkelaars, en 81 telefoonnummers, geregistreerd in 29 verschillende landen. Daarnaast werden meerdere sociale media-accounts aangetroffen die illegale migratiediensten aanboden, waaronder valse reisdocumenten en identiteiten. De gegevens zullen worden gebruikt om nieuwe onderzoeken te starten en lopende zaken te ondersteunen, met als doel de criminele netwerken te ontmantelen die profiteren van kwetsbare migranten.

Grote vraag naar AI veroorzaakt wereldwijde schaarste aan harde schijven

De groei van kunstmatige intelligentie heeft geleid tot een uitzonderlijk hoge vraag naar opslagcapaciteit, waardoor wereldwijde tekorten aan harde schijven en SSD's ontstaan. Grote technologiebedrijven zoals Google, Amazon en Microsoft investeren massaal in datacenters om hun AI-infrastructuren te ondersteunen, maar de productiecapaciteit van fabrikanten kan dit tempo niet bijhouden. Volgens DigiTimes lopen levertijden voor harde schijven inmiddels op tot twee jaar. Om de tekorten te omzeilen schakelen datacenters over op QLC NAND-gebaseerde SSD's, maar ook daar ontstaan nu knelpunten. De vraag in de zakelijke markt drijft de prijzen in de consumentenmarkt op, waardoor fabrikanten als SanDisk hun SSD-prijzen met circa vijftig procent hebben verhoogd. De verwachting is dat deze trend in 2026 verder doorzet, wat gevolgen kan hebben voor de beschikbaarheid en kosten van datacenter- en consumentenopslag wereldwijd.

Oplichters doen zich voor als de Australische politie om cryptovaluta te stelen

Oplichters proberen cryptovaluta te stelen door zich voor te doen als de Australische federale politie. Ze gebruiken gestolen gegevens om valse rapporten in te dienen bij ReportCyber, een tool waarmee cybercriminaliteit gemeld kan worden. Deze oplichters benaderen slachtoffers via telefoon, met een zogenaamd officieel referentienummer dat uit ReportCyber afkomstig zou zijn. Een slachtoffer werd gebeld door iemand die zich voordeed als de politie en zei dat het slachtoffer betrokken was bij een datalek met cryptovaluta. Vervolgens werd het slachtoffer verzocht om het rapport in te voeren en zijn e-mail te gebruiken om de status te controleren. Later belde een tweede oplichter om het slachtoffer te overtuigen cryptovaluta over te maken naar een 'cold storage'-account. Het slachtoffer kreeg argwaan en beëindigde het gesprek. Het Australian Cyber Security Centre waarschuwt voor dergelijke oplichters en adviseert mensen altijd voorzichtig te zijn met verzoeken om cryptovaluta over te maken.

Google start met verificatie van Android-ontwikkelaars

Google heeft aangekondigd dat vanaf september 2026 alleen nog apps van geverifieerde ontwikkelaars zullen worden toegelaten op Android-apparaten. Ontwikkelaars kunnen nu al beginnen met de verificatie van hun identiteit via de Android Developer Console. Deze verificatie vereist onder andere het verstrekken

van naam, adresgegevens, e-mailadres en telefoonnummers, evenals het uploaden van een kopie van hun legitimatiebewijs. Het doel van deze maatregel is om de verspreiding van malafide apps te voorkomen. De verificatie is niet alleen van toepassing op de Google Play Store, maar ook op alternatieve appwinkels. Google heeft aangegeven dat er een speciaal account voor studenten en hobbyisten komt, waarbij de volledige verificatievereisten mogelijk niet van toepassing zijn, hoewel de details hierover nog niet duidelijk zijn. Het bedrijf benadrukt dat het veilig houden van Android-gebruikers een topprioriteit is.

Voormalig Europarlementariër Breyer waarschuwt voor aangepast voorstel over Chat Control

Voormalig Europarlementariër Patrick Breyer waarschuwt voor een vernieuwde versie van het EU-voorstel Chat Control, dat probeert verplicht chatverkeer te scannen, onder het mom van het tegengaan van kindermisbruikmateriaal. Breyer noemt de wijziging "politieke misleiding", aangezien lidstaten zoals Nederland eerder tegen dergelijke voorstellen waren. Het nieuwe plan verplicht providers om 'alle passende maatregelen' te nemen tegen risico’s, wat in de praktijk kan leiden tot scans van privéberichten door AI en algoritmes. Dit zou het onderscheid tussen onschuldige en criminele communicatie moeilijk maken. Daarnaast bevat het voorstel verplichte identificatie voor minderjarigen en een verbod op chatapps voor jongeren onder de 16 jaar. Breyer pleit voor het schrappen van verplichte scans, het beperken van AI-gesprekken tot alleen CSAM en het behoud van anonimiteit op het internet.

Neptelefoontjes namens Amazon leiden tot oplichting

Er zijn meldingen binnengekomen over neptelefoontjes namens Amazon, waarbij slachtoffers een Engels- of Nederlandstalig bandje horen. In het bericht wordt beweerd dat er een bestelling van een iPhone 15 is geplaatst. Het bandje biedt twee opties: de transactie bevestigen of annuleren. Wie het keuzemenu volgt, wordt doorgeschakeld naar een zogenaamde medewerker die vraagt om een app op de computer te installeren om de bestelling te annuleren. In werkelijkheid installeert de app malware, waardoor de oplichters de controle over de computer kunnen overnemen. Melders geven aan dat na het installeren van de app, online aankopen zijn gedaan en geld is overgeschreven naar onbekende rekeningen. Het advies is om

het telefoontje onmiddellijk te beëindigen, het nummer te blokkeren en melding te maken bij de Fraudehelpdesk.

Opnieuw afpersmails over bezochte pornosites

Er zijn weer meldingen binnengekomen van afpersmails waarin wordt gedreigd met de verspreiding van vermeende erotische filmbeelden. In de e-mail stelt de afzender dat hij de computer van het slachtoffer heeft gehackt en toegang heeft gekregen tot gevoelige gegevens. Hierbij wordt beweerd dat beschamende beelden van de ontvanger zijn gemaakt tijdens een bezoek aan een pornosite. Soms wordt een oud wachtwoord genoemd om de dreiging te onderbouwen, maar dit wijst vaak op een eerder datalek, niet op daadwerkelijke toegang tot de computer. De afperser eist betaling in bitcoins om de verspreiding van de beelden te voorkomen, maar de inhoud van de mail is een bluf. Het is belangrijk om geen geld te betalen en de mail te negeren en te verwijderen.

Ransomware in fragmentatie en herkomst van LockBit en Qilin versterken dreiging en sectorimpact in 2025

In het derde kwartaal van 2025 steeg het aantal actieve ransomwaregroepen tot een record van 85, waarvan de top 10 slechts 56% van de slachtoffers vertegenwoordigde, een afname ten opzichte van het eerste kwartaal. De activiteit bleef stabiel op gemiddeld 535 slachtoffers per maand, wat een stijging is ten opzichte van 420 in het voorgaande jaar. De terugkeer van LockBit 5.0 in september 2025 markeert een mogelijke hercentralisatie van ransomware-affiliategroepen onder een groot merk. Qilin werd de meest actieve groep, met gemiddeld 75 slachtoffers per maand, gevolgd door Akira en INC Ransom. De geografische concentratie van aanvallen verschuift, waarbij Zuid-Korea nu in de top 10 van getroffen landen staat, voornamelijk door een gerichte campagne van Qilin. De productiesector en zakelijke diensten blijven de zwaarst getroffen sectoren, terwijl de gezondheidszorg stabiel blijft op 8% van de slachtoffers.