Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

28-10-2025:

Softwarebedrijf Irias.nl slachtoffer van datalek in broncode

Irias.nl, een Nederlands software- en IT-dienstverleningsbedrijf dat gespecialiseerd is in Geo/GIS-oplossingen, is het slachtoffer geworden van een datalek. Volgens een bericht van een bedreigingsactor op een hackersforum heeft het incident in oktober 2025 plaatsgevonden, waarbij de broncode van het bedrijf werd gestolen. De actor heeft een voorbeeld van de gestolen gegevens gedeeld in de vorm van een directorylijst en beweert dat de volledige set broncode beschikbaar is om te downloaden op het forum. Dit datalek benadrukt de toenemende dreiging van intellectuele eigendomsdiefstal in de technologie- en softwaresector.

Operation ForumTroll: Kaspersky koppelt APT-aanvallen aan Dante spyware van Memento Labs

Kaspersky heeft de ForumTroll APT-campagne gekoppeld aan de commercieel ontwikkelde Dante spyware, geproduceerd door Memento Labs (voorheen Hacking Team). Het onderzoek onthult een geavanceerde phishing-aanval, waarbij slachtoffers via gepersonaliseerde links naar een kwaadaardige website werden geleid. Deze aanvallen, gericht op media, universiteiten en financiële instellingen in Rusland en Wit-Rusland, werden uitgevoerd met behulp van een zero-day-exploit in Google Chrome. De malware werd geanalyseerd en blijkt deel uit te maken van een serie van gerichte aanvallen met als doel spionage. Kaspersky ontdekte ook dat de Dante spyware, die gebruik maakt van geavanceerde anti-analysetechnieken, in andere aanvallen werd ingezet, waarbij het gerelateerd werd aan eerdere malware van Hacking Team. Het onderzoek biedt belangrijke inzichten in de werkwijze van APT-groepen en de evolutie van commerciële spyware.

Bedrijven moeten zich beter voorbereiden op cyberaanvallen vanuit rusland

In Warschau komen NAVO-parlementsleden bijeen om te spreken over de groeiende dreiging van cyber- en hybride aanvallen, vooral vanuit Rusland en China. Experts waarschuwen dat bedrijven in Nederland onvoldoende voorbereid zijn op dergelijke aanvallen. Vooral vitale infrastructuren zoals energievoorziening, telecommunicatie en transport zijn kwetsbaar. Een hybride dreiging, zoals de recente drones die Europese luchthavens plaagden, is een voorbeeld van de destabiliserende tactieken

die worden ingezet. Er wordt een gebrek aan bewustzijn gezien bij bedrijven, die zich vaak meer richten op aandeelhouders dan op voorbereid zijn op een conflict. Het versterken van de digitale weerbaarheid bij toeleveranciers van vitale bedrijven is essentieel om de keten te beschermen. De NAVO-parlementariërs zullen naar verwachting met weinig concrete oplossingen komen, aangezien hybride aanvallen moeilijk te voorkomen zijn, maar wel sneller op te sporen.

Twee hacktivistische groepen bundelen krachten in nieuwe alliantie

De hacktivistische groepen TwoNet en NoName057(16) hebben een officiële alliantie aangekondigd. Dit nieuws heeft geleid tot bezorgdheid in de cybersecuritygemeenschap, aangezien beide groepen bekend staan om hun cyberaanvallen op doelwitten die als politiek of ideologisch gevoelig worden beschouwd. De nieuwe samenwerking kan de dreiging voor zowel overheden als bedrijven wereldwijd vergroten. Experts waarschuwen voor de mogelijke versterking van hun cyberaanvallen, waarbij ze gebruik maken van gezamenlijke middelen en expertise. De alliantie kan ook de tactieken en strategieën van beide groepen verbeteren, wat leidt tot complexere aanvallen die moeilijker te voorspellen en te voorkomen zijn.

Noord-Koreaanse Chollima-groep breidt malware-aanvallen uit met BeaverTail en OtterCookie

De Noord-Koreaanse Chollima-groep, gelinkt aan het Reconnaissance General Bureau, heeft zijn aanvalscapaciteiten versterkt door de integratie van twee nieuwe malwarestammen: BeaverTail en OtterCookie. Deze evolutie richt zich met vernieuwde verfijning op de cryptocurrency- en blockchainsectoren, waarbij gebruik wordt gemaakt van een combinatie van sociale-engineeringtactieken en technische supply chain-exploitatie. De campagne, genaamd Contagious Interview, maakt gebruik van legitieme jobplatforms en wervingskanalen om trojan-geïnfecteerde sollicitatie-applicaties te verspreiden. Het malware-pakket infiltreert systemen via schijnbaar onschuldige supply chain-vectoren, zoals een cryptocurrency-thema schaakplatform. De geavanceerde malware is ontworpen om browserprofielen te scannen en cryptocurrency-wallets te stelen, specifiek gericht op MetaMask, Phantom en Solflare extensies. De malware omvat ook anti-analysemethoden,

waaronder foutafhandelings- en omgevingcontrolemechanismen, en bevat een keyloggermodule die gegevens van toetsaanslagen en schermafbeeldingen opvangt.

Ex-L3Harris executive aangeklaagd voor spionage

Peter Williams, voormalig directeur van L3Harris' cyberdivisie Trenchant, is aangeklaagd voor het stelen van bedrijfsgeheimen met de intentie deze aan een Russische koper te verkopen. Volgens het Amerikaanse ministerie van Justitie heeft Williams tussen april 2022 en juni 2025 zeven bedrijfsgeheimen van twee anonieme bedrijven verkregen, wetende dat deze buiten de VS verkocht zouden worden, specifiek aan een koper in de Russische Federatie. De aanklacht beschrijft hoe Williams zonder toestemming de bedrijfsgeheimen heeft gekopieerd, gedownload, geüpload, en verstuurd. De details van de gestolen geheimen zijn onbekend, maar de bedrijven L3Harris en Trenchant worden niet beschuldigd van enige misdaad. Indien schuldig bevonden, eist de aanklager dat Williams al zijn eigendommen verliest, inclusief luxe goederen en cryptocurrency, met een schadevergoeding van 1,3 miljoen dollar.

Predatory Sparrow Group valt kritieke infrastructuur aan om data te vernietigen en verstoringen te veroorzaken

De Predatory Sparrow-groep, een hacktivistenorganisatie die vermoedelijk banden heeft met Israëlische belangen, heeft zich gepositioneerd als een van de meest destructieve cyberaanvalsgroepen die kritieke infrastructuur in het Midden-Oosten aanvallen. De groep richt zich voornamelijk op Iraanse en Syrische doelen, waaronder spoorwegen, staalfabrieken en financiële instellingen. De campagnes van de groep kenmerken zich door opzettelijke vernietiging van data, verstoring van operaties en het uitzenden van provocerende berichten om psychologische schade te veroorzaken. Sinds 2019 heeft de groep steeds geavanceerdere technieken gebruikt, zoals het gebruik van de "Meteor"-wiper-malware, waarmee ze grote verstoringen veroorzaakten in de Iraanse spoorwegsector. Recent heeft Predatory Sparrow ook financiële infrastructuren aangevallen, waaronder de Bank Sepah en Nobitex, waar ze miljoenen aan cryptocurrency vernietigden. De groep maakt gebruik van geavanceerde malware en aanvalstechnieken, waaronder versleutelde configuratiebestanden en batchscripts om systemen volledig te saboteren.

NCSC verwacht misbruik van kwetsbaarheden in DNS-software BIND 9

Het Nationaal Cyber Security Centrum (NCSC) waarschuwt voor kwetsbaarheden in de populaire DNS-serversoftware BIND 9. Deze kwetsbaarheden, CVE-2025-40778 en CVE-2025-40780, kunnen door aanvallers worden misbruikt om cache-poisoning uit te voeren, waarbij gebruikers naar malafide locaties worden doorgestuurd. De kwetsbaarheden worden als zeer ernstig beoordeeld, met een score van 8.6 op een schaal van 10. BIND 9 maakt gebruik van een zwakke pseudo-random number generator, wat het voor aanvallers mogelijk maakt om de source port en query ID te voorspellen. Het andere lek zorgt ervoor dat BIND 9 vervalste gegevens in de servercache accepteert. Het NCSC roept organisaties op om de beveiligingsupdates zo snel mogelijk te installeren om misbruik te voorkomen. Aanvallers kunnen de kwetsbaarheden binnen korte tijd uitbuiten.

Kritieke kwetsbaarheden in Dell Storage Manager kunnen systemen compromitteren

Dell Technologies heeft drie kritieke kwetsbaarheden in zijn Storage Manager-software bekendgemaakt, die aanvallers de mogelijkheid bieden om authenticatie te omzeilen, gevoelige informatie openbaar te maken en ongeautoriseerde toegang tot systemen te verkrijgen. De kwetsbaarheden treffen versies van Dell Storage Manager tot 20.1.21. De ernstigste kwetsbaarheid (CVE-2025-43995) heeft een CVSS-score van 9.8 en kan leiden tot volledige systeemcompromittatie. Een andere kwetsbaarheid (CVE-2025-43994) maakt informatie openbaar en verstoort de beschikbaarheid van de dienst. De derde kwetsbaarheid (CVE-2025-46425) betreft een onjuiste beperking van XML-verwijzingen, wat het lezen van gevoelige bestanden mogelijk maakt. Dell raadt aan om updates te installeren om deze kwetsbaarheden te verhelpen, met de nadruk op de versie 2020 R1.22 of later. Er zijn nog geen meldingen van actieve exploitatie, maar snelle actie wordt aanbevolen om mogelijke inbreuken te voorkomen.

QNAP waarschuwt voor kritieke ASP.NET-kwetsbaarheid in Windows-back-upsoftware

QNAP heeft klanten gewaarschuwd voor een ernstige kwetsbaarheid in de ASP.NET Core-webserver die ook van invloed is op de NetBak PC Agent, een Windows-hulpprogramma voor het maken van back-ups naar QNAP NAS-apparaten. De kwetsbaarheid, gemarkeerd als CVE-2025-55315, kan door aanvallers met lage

privileges worden misbruikt om inloggegevens van andere gebruikers te stelen of beveiligingsmaatregelen te omzeilen via HTTP-aanvraag-smuggling. Gebruikers van de NetBak PC Agent moeten hun systemen bijwerken door de nieuwste ASP.NET Core-runtimecomponenten te installeren, of de NetBak-app opnieuw te installeren om de beveiligingslekken te verhelpen. QNAP adviseert dringend om de laatste Microsoft ASP.NET Core-updates te installeren om het systeem te beveiligen tegen potentiële aanvallen.

Kritieke kwetsbaarheid in UniFi Access-app blootlegt API-beheer zonder authenticatie

Ubiquiti's UniFi Access-app bevat een ernstige kwetsbaarheid die het API-beheer blootstelt zonder vereiste authenticatie, waardoor aanvallers mogelijk volledige controle over de toegangsbeheersystemen kunnen krijgen. De kwetsbaarheid werd ontdekt door Catchify Security en heeft betrekking op versies van de UniFi Access-app van 3.3.22 tot 3.4.31. Door een configuratiefout in versie 3.3.22 kunnen kwaadwillende actoren toegang krijgen tot het systeem zonder dat daarvoor privileges nodig zijn, wat ernstige gevolgen kan hebben voor de fysieke beveiliging van gebouwen. Ubiquiti heeft de kwetsbaarheid erkend en een patch uitgebracht in versie 4.0.21. Gebruikers wordt aangeraden snel te updaten om verdere risico's te vermijden. De kwetsbaarheid heeft een CVSS v3.1-score van 10.0, wat aangeeft dat de impact groot kan zijn op vertrouwelijkheid, integriteit en beschikbaarheid.

Hackers gebruiken ClickFix-techniek voor NetSupport RAT-loaders

Cybercriminelen hebben hun aanvallen verder verfijnd door de ClickFix-techniek in te zetten voor het verspreiden van NetSupport Manager, een legitiem beheertools dat nu wordt misbruikt voor ongeautoriseerde toegang tot systemen. In 2025 is deze techniek steeds gebruikelijker geworden. Het proces begint met social engineering waarbij slachtoffers op valse ClickFix-pagina's terechtkomen die hen misleiden om schadelijke opdrachten via het Windows Run Prompt uit te voeren. Hierdoor wordt een infectieketen opgestart die uiteindelijk resulteert in de installatie van NetSupport. Deze geavanceerde aanvalsmethode maakt gebruik van PowerShell-gebaseerde loaders en obfuscatie om detectie te omzeilen. De aanvallers werken in groepen samen en optimaliseren hun leveringsinfrastructuur om het succespercentage te

verhogen. Organisaties moeten verdachte ClickFix-pagina's en ongewone NetSupport-installaties snel isoleren en grondig analyseren.

Hackers exploiteren kwetsbaarheid in Microsoft WSUS - 2800 gevallen blootgesteld online

Hackers maken actief gebruik van een ernstige kwetsbaarheid in de Windows Server Update Services (WSUS) van Microsoft. De kwetsbaarheid, aangeduid als CVE-2025-59287, maakt het mogelijk om op niet-gepatchte WSUS-servers op afstand code uit te voeren, wat aanvallers volledige controle kan geven over bedrijfsnetwerken. Beveiligingsonderzoekers hebben ontdekt dat er minstens 2.800 blootgestelde WSUS-instanties online zijn, waarvan de meeste in Noord-Amerika en Europa. Deze kwetsbaarheid werd als kritiek geclassificeerd met een CVSS 3.1-score van 9,8, vanwege de eenvoud waarmee ze zonder authenticatie kan worden geëxploiteerd. Hackers gebruiken deze kwetsbaarheid om kwaadaardige updates te implementeren, gevoelige gegevens te stelen of achterdeuren te installeren. Microsoft heeft patches beschikbaar gesteld, maar slechts 40% van de blootgestelde systemen heeft deze toegepast, waardoor de risico’s blijven toenemen. Het wordt aanbevolen om WSUS-servers goed te beveiligen en regelmatig te controleren op kwetsbaarheden.

DigiD-app ondersteunt nu alle Nederlandse reisdocumenten voor ID-check

De DigiD-app biedt nu ondersteuning voor alle Nederlandse reisdocumenten bij het uitvoeren van een ID-check. Dit maakt het mogelijk voor gebruikers met in het buitenland uitgegeven documenten om deze toe te voegen aan hun DigiD-app en veilig in te loggen bij organisaties die extra controle vereisen. Voorheen werden niet alle documenten correct geregistreerd in de Basisregistratie Personen, wat leidde tot mislukte ID-checks. DigiD maakt nu gebruik van het Basisregister Reisdocumenten, waarin alle Nederlandse reisdocumenten zijn opgenomen, ongeacht de plaats of instantie van uitgifte. Dit zorgt voor een verbeterde en veilige verificatie van de identiteit van gebruikers.

Europol pleit voor Europese trace-back afspraken tegen telefoonspoofing

Europol heeft gepleit voor EU-brede afspraken om telefoonspoofing effectief aan te pakken. In een position paper benadrukt de Europese opsporingsdienst de toename van fraude via telefoonspoofing, waarbij criminelen zich voordoen als legitieme instanties zoals banken. Europol stelt dat er gelijke technische standaarden nodig zijn, aangezien deze momenteel tussen landen verschillen, wat kwetsbaarheden veroorzaakt. Ook wordt er gepleit voor het opzetten van een internationaal traceback mechanisme waarmee opsporingsdiensten telefoongesprekken kunnen traceren via telecomproviders. Europol wil dat deze systemen grensoverschrijdend werken en dat er gestandaardiseerde processen voor informatie-uitwisseling komen. Verder wordt het belang van een geharmoniseerd juridisch kader voor traceback verzoeken onderstreept. Tot slot wijst Europol op de rol van anonieme prepaiddiensten en callback scams die de strijd tegen spoofing bemoeilijken.

Gegevens van passagiers Dublin Airport gestolen bij ransomware-aanval

Bij een ransomware-aanval op de softwareleverancier Collins Aerospace zijn mogelijk de gegevens van miljoenen passagiers gestolen die van Dublin Airport vertrokken tussen 1 en 31 augustus 2025. De aanval werd uitgevoerd door twee verschillende ransomwaregroepen. De aanvallers kregen toegang tot een server met boardingpasgegevens van passagiers die via de luchthaven reisden. De gestolen informatie omvatte boekingsreferentie, naam en Frequent Flyer nummer. De Ierse autoriteiten hebben het incident gemeld bij de privacytoezichthouder DPC, en luchtvaartmaatschappijen, waaronder SAS, waarschuwen inmiddels hun klanten. In totaal vlogen 3,8 miljoen passagiers deze maand via Dublin Airport, waarvan een aanzienlijk aantal mogelijk getroffen is door het datalek.

Nationale cybercrisisoefening test samenwerking, communicatie en respons

Op 23 oktober 2025 organiseerden het Centrum voor Cybersecurity België (CCB) en het Nationaal Crisiscentrum (NCCN) een grootschalige cybercrisisoefening. Het doel was om het nationale cybernoodplan te testen en te verfijnen. De simulatie draaide om een ransomware-aanval in de energiesector, waarbij onder andere een windmolenpark en het mobiele datanetwerk in Brussel getroffen werden. Belangrijke stakeholders zoals het BIPT, de federale parketten en ELIA werkten samen in een table-top oefening, die gericht was op besluitvorming en communicatie zonder IT-systemen te verstoren. De oefening benadrukte de noodzaak van verbeterde

informatiestromen en gestructureerde communicatie. De geleerde lessen worden gebruikt voor een grotere oefening in 2026. Deze regelmatige oefeningen zijn essentieel voor het verhogen van de paraatheid van organisaties en overheden in geval van echte cybercrisissen.

Qilin ransomware maakt gebruik van Mspaint en Notepad om gevoelige bestanden te vinden

Qilin ransomware is een van de snelst groeiende cyberdreigingen van 2025, met meer dan 40 slachtoffers per maand wereldwijd. Deze ransomware, die oorspronkelijk als Agenda bekend stond, heeft zich gepositioneerd als een ernstige dreiging die organisaties in verschillende sectoren en regio's treft. Het maakt gebruik van een dual-extortion-aanpak, waarbij bestanden worden versleuteld en gevoelige gegevens worden gestolen en openbaar gemaakt. De meeste aanvallen richten zich op de productiesector (23%), gevolgd door professionele diensten (18%). Qilin maakt gebruik van gestolen VPN-inloggegevens en de afwezigheid van multi-factor authenticatie om netwerken binnen te dringen. Vervolgens wordt er gebruik gemaakt van ingebouwde Windows-tools zoals mspaint.exe en notepad.exe om waardevolle bestanden te vinden. Dit handmatige proces stelt aanvallers in staat om gevoelige gegevens te extraheren voordat encryptie plaatsvindt. Qilin heeft een geavanceerde aanpak ontwikkeld, waarbij ook cloud-gebaseerde exfiltratie wordt ingezet.

Landen opgeroepen om VN-verdrag tegen cybercrime niet te ondertekenen

Een coalitie van privacyorganisaties en burgerrechtenbewegingen heeft opgeroepen tot het niet ondertekenen van het VN-verdrag tegen cybercriminaliteit. Zij vrezen dat het verdrag grensoverschrijdende mensenrechtenschendingen zou kunnen faciliteren en schadelijk kan zijn voor klokkenluiders en onderzoeksjournalisten. 72 landen ondertekenden het verdrag, dat internationale samenwerking beoogt bij het voorkomen van cybercrime, het verzamelen van digitaal bewijsmateriaal en het strafbaar stellen van cybergerelateerde misdrijven. Critici wijzen op het gebrek aan waarborgen voor mensenrechten, zoals het recht op vrije meningsuiting. Het verdrag zou landen ook verplichten digitale surveillancebevoegdheden in te stellen, die volgens tegenstanders kunnen leiden tot politieke vervolging van dissidenten, activisten en journalisten. De Europese Commissie en EU-lidstaten hebben het verdrag wel ondertekend.

X vraagt gebruikers om security key voor 2FA opnieuw te registreren

Socialmediaplatform X heeft gebruikers die een security key voor tweefactorauthenticatie (2FA) gebruiken, zoals een Yubikey of passkey, gevraagd deze opnieuw te registreren. Dit is noodzakelijk om het domein twitter.com uit te faseren, aangezien de huidige security keys gekoppeld zijn aan twitter.com. Gebruikers moeten hun security key opnieuw registreren om deze te koppelen aan X.com. Als dit niet gebeurt vóór 10 november 2025, kunnen gebruikers niet meer inloggen op hun account. De bestaande security key kan opnieuw gebruikt worden, maar gebruikers moeten deze actie ondernemen om toegang tot hun account te behouden. Alternatief kunnen ze een andere 2FA-methode kiezen of besluiten geen 2FA meer te gebruiken.

Hackers wijzigen geslacht van Brigitte Macron op belastingformulieren

Brigitte Macron, de Franse first lady, werd slachtoffer van een cyberaanval waarbij hackers haar naam op haar belastingformulier wijzigden naar "Jean-Michel", een mannelijke variant van haar naam. De Franse overheid bevestigde dat de hackers toegang hadden gekregen tot haar persoonlijke belastingdossier via een online account. Deze wijziging werd ontdekt door een medewerker van Macron, die de aanval aan het licht bracht. De zaak heeft geleid tot bezorgdheid over de kwetsbaarheid van overheidswebsites en de veiligheid van persoonlijke gegevens. De hackers zijn nog niet gepakt, en de Franse autoriteiten onderzoeken de aanval verder. De incidenten benadrukken de voortdurende dreiging van cyberaanvallen op gevoelige overheidsdata en de kwetsbaarheid van persoonlijke informatie tegen manipulatie.

iOS 26 verwijdert bewijs van Pegasus en Predator spyware-infecties door het overschrijven van het ‘shutdown.log’ bestand bij herstart

Met de introductie van iOS 26 heeft Apple een belangrijke wijziging doorgevoerd die invloed heeft op forensisch onderzoek naar malware-infecties. Pegasus en Predator spyware, die bekend staan om hun gebruik van zero-click kwetsbaarheden voor spionage, hebben in het verleden sporen achtergelaten in het ‘shutdown.log’ bestand, wat onderzoekers hielp bij het traceren van infecties. iOS 26 overschrijft nu

dit logbestand bij elke herstart, waardoor eerder opgeslagen gegevens over infecties permanent worden gewist. Deze wijziging voorkomt dat forensische experts bewijs van compromittering kunnen vinden, zelfs nadat spyware zoals Pegasus geprobeerd heeft zichzelf te verwijderen. Dit vormt een aanzienlijke uitdaging voor digitale forensische analyse en versterkt de effectiviteit van malware bij het maskeren van infecties. De verandering roept vragen op over de bescherming van gebruikers en het bewaren van digitaal bewijs.