Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

18-10-2025:

Noord-Koreaanse hackers gebruiken schadelijke scripts voor keylogging via Chessfi trojaan

Noord-Koreaanse hackers hebben een nieuwe informatie-steler verspreid via een gemanipuleerde Node.js applicatie genaamd Chessfi. Deze malware maakt gebruik van twee bestaande tools, BeaverTail en OtterCookie, die samen een complex JavaScript-payload vormen. Het slachtoffer wordt misleid door valse werkgelegenheidsaanbiedingen en gevraagd de applicatie te installeren onder het mom van een codeerbeoordeling. Eenmaal geïnstalleerd, worden inloggegevens, cryptowallets en gebruikersactiviteiten gestolen. Cisco Talos ontdekte de campagne toen ze ongebruikelijke netwerkactiviteit op een gecompromitteerd systeem onderzochten. De malware creëert een verbinding met een command-and-control server en kan bestanden stelen, shell-opdrachten uitvoeren en keylogging-acties uitvoeren. Daarnaast worden regelmatig screenshots gemaakt en gegevens van het klembord geüpload naar de server. Het infectiemechanisme is complex en ontwijkt detectie door een meerfasige infectieketen en verborgen processen.

North Korean hackers use fake interview attack to deploy OtterCandy malware

Cybercriminelen die geassocieerd worden met de Noord-Koreaanse groep WaterPlum hebben een geavanceerde nieuwe malware, OtterCandy, gelanceerd. Deze malware, die fungeert als een platformonafhankelijke RAT (Remote Access Trojan) en gegevensdief, maakt gebruik van de ClickFake Interview-campagne. Deze sociale-engineeringaanval verbergt zich als een legitiem sollicitatieproces in de blockchain- en cryptocurrencysectoren. Aanvallers creëren geloofwaardige nepwebsites, zoals BlockForgeX, die als sollicitatie- en interviewplatforms dienen, waarbij slachtoffers worden verleid om schadelijke software te downloaden onder het mom van instructies voor camera-instellingen of stuurprogramma-updates. De malware is sinds juli 2025 actief op Windows, macOS en Linux-systemen en biedt geavanceerde functies zoals het stelen van wachtwoorden, systeeminformatie en cryptocurrency-portemonneegegevens. OtterCandy heeft een verbeterd zelfbehoudsmechanisme, waardoor het blijft draaien, zelfs na pogingen tot detectie.

267.000 F5-apparaten benaderbaar vanaf internet, waarvan 3.800 in Nederland en 1.800 in België

Ongeveer 267.000 apparaten van de fabrikant F5 zijn wereldwijd benaderbaar vanaf het internet, met 3.800 van deze apparaten in Nederland en 1.800 in België. Dit werd vastgesteld door The Shadowserver Foundation op basis van een online scan. De ontdekking komt nadat F5 deze week updates heeft uitgebracht voor verschillende kwetsbaarheden, nadat een aanvaller broncode en informatie over niet openbaar gemaakte beveiligingslekken had gestolen. De kwetsbaarheid kan voor verschillende aanvallen worden misbruikt, wat leidde tot een noodbevel van de Amerikaanse overheid. Dit beval federale overheidsdiensten op om binnen een dag de F5-updates te installeren. De apparaten worden vaak gebruikt voor load balancing, application delivery, firewalls en VPN-toepassingen. Organisaties wordt dringend geadviseerd de updates zo snel mogelijk toe te passen om risico's te mitigeren.

Kritieke deserialisatiekwetsbaarheid in Apache ActiveMQ NMS AMQP Client, direct patchen aanbevolen

Er is een ernstige kwetsbaarheid ontdekt in de Apache ActiveMQ NMS AMQP Client (versies tot en met 2.3.0), die het mogelijk maakt om via deserialisatie van onbetrouwbare gegevens op afstand code uit te voeren. Deze kwetsbaarheid, aangeduid als CVE-2025-54539, kan worden misbruikt door een aanvaller die een malafide AMQP-broker controleert of imiteert. Tijdens de communicatie tussen de client en broker wordt ongecontroleerd data gedeserializeerd, wat leidt tot de uitvoering van kwaadaardige code. Dit kan leiden tot een volledige compromittering van de cliëntsysteemintegriteit, -beschikbaarheid en -vertrouwelijkheid. Gebruikers wordt sterk aangeraden om onmiddellijk te upgraden naar versie 2.4.0 om de kwetsbaarheid te verhelpen. Het installeren van de update moet met prioriteit worden uitgevoerd, na grondig testen.

Hackers gebruiken psychologische trucs in phishingcampagnes

Hackers maken gebruik van psychologische technieken, zoals FOMO (fear of missing out), om gebruikers te misleiden. Ze sturen een Teams-uitnodiging met een PDF-bestand en een QR-code. Wanneer gebruikers de uitnodiging openen, denken ze een belangrijke compensatie of bonus te missen. De PDF bevat een link naar een website waar gebruikers hun accountgegevens moeten invoeren, wat hen blootstelt aan accountdiefstal. De aanvallers gebruiken vervolgens het gestolen account om e-mails te sturen naar de contacten van het slachtoffer. Dit type phishing is bijzonder

effectief omdat de e-mail niet fysiek aanwezig is, wat de nieuwsgierigheid van de gebruiker opwekt. Dit zorgt ervoor dat de gebruiker de link alsnog volgt, wat de kans op succesvolle infecties vergroot.

Malicious npm package delivers AdaptixC2 post-exploitation agent

Een nieuw gevaar werd ontdekt binnen de npm-ecosysteem, waarbij een kwaadwillig pakket met de naam "https-proxy-utils" werd gebruikt om de AdaptixC2-agent te verspreiden. Deze agent, een alternatief voor het bekende Cobalt Strike, werd in de lente van 2025 voor het eerst kwaadaardig aangetroffen. Het npm-pakket, dat zich voordeed als een nuttige tool voor proxygebruik, bevatte een post-installatiescript dat het malware-framework op de apparaten van slachtoffers installeerde. Dit pakket was bedoeld voor Windows, macOS en Linux, waarbij het systeemafhankelijke methoden gebruikte om de agent te laden. De aanval maakt het voor aanvallers mogelijk om op afstand toegang te krijgen, opdrachten uit te voeren, processen te beheren en persistentie te bereiken. Dit incident benadrukt de groeiende dreiging van supply chain-aanvallen binnen open-source softwareomgevingen zoals npm.

Exploit van zwakke authenticatie in Zendesk door e-mailbommen

Cybercriminelen maken misbruik van een gebrek aan authenticatie in Zendesk, een platform voor klantenservice, om e-mailinboxen te overspoelen met bedreigende berichten. Deze berichten komen van verschillende Zendesk-klanten zoals CapCom, Discord en Tinder. Zendesk, dat bedrijven helpt bij klantenservice, heeft een systeem waarin e-mails worden verstuurd zonder verificatie van de afzender. Dit maakt het mogelijk om anonieme tickets aan te maken, wat misbruikt kan worden door spammers om ongewenste berichten te sturen. Zendesk erkent het probleem en heeft klanten aangeraden om hun instellingen te verbeteren door geverifieerde e-mailadressen voor tickets te vereisen. Hoewel Zendesk beweert dat er maatregelen zijn tegen massale aanvragen, konden aanvallers duizenden e-mails versturen binnen enkele uren door de zwakke configuratie. Dit incident benadrukt het belang van sterke beveiligingsinstellingen voor klantenserviceplatforms.

hackers gebruiken TikTok-video's om zelfcompilerende malware te verspreiden via PowerShell

Cybercriminelen maken gebruik van TikTok om malwarecampagnes te verspreiden die zogenaamd gratis softwareactiveringen aanbieden, maar in plaats daarvan schadelijke payloads afleveren. Het aanvallende script maakt gebruik van social engineering-tactieken en trapt gebruikers, die op zoek zijn naar gratis software zoals Photoshop, in om PowerShell-opdrachten uit te voeren. De gebruikers worden aangemoedigd een schijnbaar onschuldige opdracht te geven, die op afstand kwaadaardige code laadt. Dit leidt tot de installatie van AuroStealer-malware, die gevoelige informatie steelt. De aanval maakt gebruik van zelfcompilerende technieken waarbij C#-code tijdens de uitvoering wordt gecompileerd, wat traditionele detectiemechanismen omzeilt. Het gebruik van een dynamisch geïnjecteerde shellcode binnen het geheugen zorgt ervoor dat er geen bestanden op de schijf worden geschreven, waardoor de malware moeilijker te detecteren is. Deze campagne is gericht op gebruikers die naar gebroken versies van software zoeken, wat de risico's van het downloaden van programma's uit onbetrouwbare bronnen benadrukt.

Bende achter telefoonfraude met 1200 simboxes en 40.000 simkaarten opgerold

De Letse autoriteiten hebben vijf personen aangehouden die verdacht worden van het faciliteren van grootschalige telefonische fraude, zoals WhatsAppfraude, investeringsfraude en oplichting via online marktplaatsen. Bij de aanhoudingen zijn 1200 simboxes en 40.000 actieve simkaarten in beslag genomen, evenals vijf servers, twee domeinnamen, 431.000 euro op bankrekeningen, 333.000 dollar in cryptovaluta en vier dure auto's. De bende bood telefonische diensten aan andere criminelen, die via de simboxes frauduleuze sms-berichten konden versturen en valse online accounts konden registreren. Europol beschrijft de operatie als een "cybercrime-as-a-service" die criminelen in staat stelde hun identiteit en locatie te verbergen. In Oostenrijk alleen zou deze fraude al voor een schade van 4,5 miljoen euro hebben gezorgd. Het netwerk wordt nog onderzocht, met meer dan 49 miljoen online accounts die mogelijk betrokken zijn.

INTERPOL-operatie levert recordaantal arrestaties op en cruciale informatie over terroristisch vervoer

INTERPOL heeft tijdens Operatie Neptune VII, die plaatsvond van juli tot september 2025, grenscontroles uitgevoerd op meer dan 70 locaties in Europa, het Midden-Oosten en Noord-Afrika. In totaal werden 328 personen geïdentificeerd die onder INTERPOL Aankondigingen stonden, waarvan 57 met verdachte banden met terrorisme. De operatie leidde tot 153 arrestaties, meer dan twee keer zoveel als het vorige jaar. Onder de gearresteerden bevond zich Igor Grechushkin, de eigenaar van het schip dat ammoniumnitraat vervoerde en betrokken was bij de explosie in Beiroet in 2020. Daarnaast werden 130 gestolen reisdocumenten en grote hoeveelheden drugs en gestolen luxeauto's in beslag genomen. De operatie leverde ook waardevolle informatie op over de bewegingen van buitenlandse terroristische strijders, die door middel van Blue Notices konden worden gevolgd.

Kredietbeoordelaar Experian krijgt boete van 2,7 miljoen euro wegens overtreden AVG

De Autoriteit Persoonsgegevens (AP) heeft kredietbeoordelaar Experian Nederland een boete van 2,7 miljoen euro opgelegd voor het overtreden van de Algemene Verordening Gegevensbescherming (AVG). Experian verzamelde gegevens van consumenten zonder voldoende duidelijk te maken waarom deze verzameld werden. Ook werden de gevolgen van het gebruik van deze gegevens niet goed afgewogen en was het gebruik van bepaalde gegevens onterecht. De gegevens kwamen uit zowel openbare als niet-openbare bronnen, zoals het Handelsregister en telecom- en energiebedrijven. De boete volgt op klachten van consumenten die nadelige gevolgen ondervonden van de kredietscores, zoals het weigeren van klanten of het verhogen van borgsommen. Experian heeft inmiddels zijn activiteiten in Nederland stopgezet en zal de verzamelde data verwijderen. Het bedrijf gaat niet in beroep tegen de boete.

Microsoft beëindigt ondersteuning voor Office 2016 en 2019

Microsoft heeft gebruikers deze week herinnerd dat de ondersteuning voor Office 2016 en Office 2019 op 14 oktober 2025 is beëindigd. Office 2016 heeft sinds oktober 2020 geen reguliere ondersteuning meer, terwijl Office 2019 drie jaar later, in oktober 2023, deze ondersteuning verloor. Hoewel deze versies van Office blijven functioneren, zullen ze kwetsbaar zijn voor aanvallen omdat Microsoft geen beveiligingsupdates, bugfixes of technische ondersteuning meer levert. Het gebruik

van verouderde versies kan de beveiliging, naleving en productiviteit van organisaties negatief beïnvloeden. Microsoft raadt aan om zo snel mogelijk te upgraden naar ondersteunde versies zoals Microsoft 365 Apps. Voor klanten zonder een Microsoft 365-abonnement, biedt Office 2024 een standalone versie, en ook Office LTSC 2024 is beschikbaar voor commerciële en overheidsklanten.

Odido krijgt boete van 1,5 miljoen euro voor onvoldoende beveiliging aftapsysteem

Odido heeft een boete van 1,5 miljoen euro gekregen van de Rijksinspectie Digitale Infrastructuur (RDI) wegens onvoldoende beveiliging van zijn aftapsysteem. Dit systeem, dat is ontworpen om gesprekken en berichten af te tappen op last van de officier van justitie of de inlichtingendiensten, voldeed niet aan de wettelijk gestelde eisen. Er was geen adequaat beveiligingsplan en het personeel met toegang tot het systeem werd niet goed gescreend. Hierdoor hadden ook leveranciers toegang tot gevoelige informatie, zoals staatsgeheimen en strafrechtelijke gegevens. Odido heeft inmiddels maatregelen genomen om de beveiliging te verbeteren en de risico's te verkleinen. Het onderzoek naar deze tekortkomingen vond plaats tussen 2021 en 2022.

Minecraft-mods: wanneer gamehacks risicovol worden

Minecraft-mods kunnen de spelervaring verrijken, maar ze vormen ook een beveiligingsrisico. Sommige mods verbergen malware, zoals trojans, infostealers, ransomware en cryptominers. Kwaadwillende actoren gebruiken populaire platforms zoals GitHub, Bukkit en CurseForge om schadelijke mods te verspreiden. In het verleden zijn duizenden Minecraft-spelers geïnfecteerd via nep-mods die zogenaamd de spelervaring verbeterden. Dergelijke malware kan apparaten overnemen, gevoelige gegevens stelen of cryptocurrency mijnen. Om het risico te verkleinen, wordt geadviseerd alleen mods van vertrouwde platforms zoals CurseForge te downloaden, de reputatie van de ontwikkelaar te controleren en verdachte bestandstypen te vermijden. Verder wordt aangeraden om Minecraft in een niet-beheerderaccount te spelen, regelmatig back-ups te maken en beveiligingssoftware te gebruiken. Als je denkt dat je een schadelijke mod hebt geïnstalleerd, moet je deze verwijderen en je systeem scannen met antimalwaretools.

Microsoft rapport: 80% van cyberaanvallen heeft financieel motief

In het rapport van Microsoft over digitale verdediging wordt benadrukt dat 80% van de onderzochte cyberaanvallen vorig jaar gericht was op het stelen van inloggegevens om persoonlijke of andere gevoelige informatie te verkrijgen. In meer dan de helft van de gevallen waren financiële motieven de drijfveer, in plaats van spionage. De meeste aanvallen werden uitgevoerd door cybercriminelen, hoewel nation-state actoren een belangrijke bedreiging blijven vormen. Microsoft meldt dat landen zoals China en Iran zich richten op spionage, terwijl Noord-Koreaanse hackers zich richten op het genereren van inkomsten. De onderzoekers wijzen ook op het gebruik van AI door zowel aanvallers als verdedigers. Aanvallers gebruiken AI om phishing te automatiseren en malware te creëren, terwijl verdedigers AI inzetten om bedreigingen te identificeren en phishingpogingen te detecteren. Microsoft benadrukt het belang van sterke beveiligingsmaatregelen, zoals multifactor-authenticatie, om identiteitsdiefstal te voorkomen.