Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

20-10-2025:

Noord-Koreaanse hackers vormen groeiende dreiging voor Europa

Noord-Koreaanse hackers zijn steeds actiever en vormen een grote dreiging voor Europese bedrijven en instellingen, vooral in strategische sectoren zoals defensie, lucht- en ruimtevaart, en energie. Volgens analisten heeft het land zijn cybercapaciteiten aanzienlijk versterkt, niet alleen voor financieel gewin, maar ook voor spionage. Noord-Korea steelt steeds vaker geheime informatie, gericht op zowel commerciële als overheidsdoelen in Europa. De staatshackers gebruiken verschillende methoden, van ransomware-aanvallen tot het verkrijgen van toegang tot vitale infrastructuur via valse IT-werknemers. Noord-Korea's cyberoperaties zijn vaak financieel gemotiveerd, maar dragen bij aan het regime's bredere doelen, zoals kernwapenontwikkeling. Analisten benadrukken dat Noord-Korea niet langer gezien moet worden als de kleinere speler in het oosten, maar als een serieuze geopolitieke dreiging die het Westen serieus moet nemen. Het land werkt ook nauw samen met Russische cybercriminaliteit om zijn doelen te bereiken.

Nieuwe .NET CAPI Backdoor Doelt op Russische Auto- en E-Commercebedrijven via Phishing ZIP's

Een nieuwe cyberaanval is gericht op de Russische auto- en e-commerce sector met behulp van een onbekende .NET malware, genaamd CAPI Backdoor. De aanvallen verspreiden zich via phishing e-mails die een ZIP-bestand bevatten, dat een vals belastingdocument en een Windows-snelkoppeling bevat. Wanneer de snelkoppeling wordt uitgevoerd, installeert de malware zich via het legitieme programma "rundll32.exe." De backdoor kan gegevens stelen van webbrowsers zoals Google Chrome, Microsoft Edge en Mozilla Firefox, en maakt screenshots. Het kan ook systeeminformatie verzamelen en bestanden exfiltreren naar een externe server. Daarnaast probeert de malware persistentie te behouden door een geplande taak in te stellen en een snelkoppeling in de opstartmap van Windows te maken. Onderzoekers vermoeden dat de aanvallen gericht zijn op de Russische auto-industrie vanwege een specifiek domein dat zich voordoet als een legitieme site.

China beschuldigt VS van cyberaanval op nationaal tijdcentrum

China heeft de Amerikaanse Nationale Veiligheidsdienst (NSA) beschuldigd van het uitvoeren van cyberaanvallen op het nationale tijdcentrum van China. Volgens de beschuldigingen heeft de NSA in 2022 kwetsbaarheden in de berichtenservices van een buitenlandse mobiele telefoonmerk misbruikt om gevoelige gegevens van medewerkers van het tijdcentrum te stelen. Tussen 2023 en 2024 zou de NSA ook geprobeerd hebben om toegang te krijgen tot kritieke tijdsystemen. Het tijdcentrum is verantwoordelijk voor het genereren en distribueren van de officiële tijd van China en levert tijdsynchronisatie aan sectoren zoals communicatie, financiën, energie, transport en defensie. De Chinese regering beweert bewijs te hebben van de aanval, maar heeft dit niet openbaar gedeeld. Deze beschuldiging zou de spanningen tussen de VS en China verder kunnen verergeren, bovenop de bestaande handel, technologie en Taiwankwesties.

Microsoft verhelpt ernstig ASP.NET Core-kwetsbaarheid

Microsoft heeft deze week een kwetsbaarheid gepatcht die als de ernstigste ooit werd aangemerkt voor ASP.NET Core. De kwetsbaarheid, aangeduid als CVE-2025-55315, is aangetroffen in de Kestrel-webserver van ASP.NET Core en maakt het mogelijk voor aanvallers om een HTTP-verzoek te smokkelen, waarmee ze andere gebruikers kunnen beïnvloeden, inloggegevens kunnen stelen of beveiligingsmaatregelen kunnen omzeilen. De aanvallers kunnen ook de server verstoren. Microsoft heeft veiligheidsupdates vrijgegeven voor verschillende versies van ASP.NET Core en Visual Studio, en raadt ontwikkelaars aan om snel te patchen door de juiste updates te installeren en hun applicaties opnieuw in te stellen. De kwetsbaarheid kan ernstige gevolgen hebben, waaronder het inloggen als een andere gebruiker en het uitvoeren van schadelijke verzoeken op de server.

ConnectWise verhelpt kwetsbaarheid in Automate voor AiTM-aanvallen

ConnectWise heeft een beveiligingsupdate uitgebracht voor zijn Automate-product, waarin twee kwetsbaarheden werden verholpen. De ernstigste kwetsbaarheid, CVE-2025-11492, had een ernstscore van 9.6 en stelde aanvallers in staat om gevoelige informatie via onbeveiligde HTTP-verbindingen af te luisteren of te wijzigen, wat gevaarlijke man-in-the-middle (AiTM) aanvallen mogelijk maakte. De tweede kwetsbaarheid, CVE-2025-11493, betrof het ontbreken van integriteitscontrole voor updatepakketten, wat een aanvaller in staat stelde om malafide updates te

verspreiden. Deze kwetsbaarheden betroffen vooral on-premise installaties van Automate, maar cloudgebaseerde versies zijn inmiddels geüpdatet. ConnectWise raadt aan om de nieuwe versie onmiddellijk te installeren om verdere risico's te voorkomen. Er zijn op dit moment geen meldingen van actieve aanvallen, maar het risico op exploitatie is groot.

PoC en exploit voor Redis gevonden

Op 17 oktober 2025 werd een Proof of Concept (PoC) en exploit voor CVE-2025-32023 gedeeld via het PlaidCTF 2025 evenement, specifiek gericht op de "Zerodeo" aanvalsmethode. Deze kwetsbaarheid heeft betrekking op de Redis software en kan leiden tot Remote Code Execution (RCE), waarmee aanvallers mogelijk volledige controle over het systeem kunnen verkrijgen. De details van deze exploit werden gedeeld op GitHub, waar zowel de PoC als een adviserende link naar de officiële beveiligingswaarschuwing voor Redis te vinden zijn. Dit maakt het mogelijk voor cybercriminelen om kwetsbare systemen aan te vallen en gevoelige gegevens te compromitteren. Gebruikers van Redis wordt geadviseerd om hun versies te updaten naar de gepatchte versies om het risico op misbruik van deze kwetsbaarheid te minimaliseren.

PoC-framework voor kwetsbaarheden in Apple AirPlay

Een PoC-framework genaamd AirBorne is ontwikkeld voor twee ernstige kwetsbaarheden in Apple's AirPlay-service, aangeduid als CVE-2025-24252 en CVE-2025-24132. Het framework werd gedeeld op GitHub en richt zich op de misbruikmogelijkheden van deze kwetsbaarheden. AirBorne maakt gebruik van gecombineerde technieken die de blootstelling van AirPlay aan aanvallen vergroten. De kwetsbaarheden kunnen mogelijk leiden tot ongeautoriseerde toegang tot apparaten die AirPlay ondersteunen, wat de integriteit en veiligheid van gebruikers in gevaar brengt. Dit stelt aanvallers in staat gevoelige gegevens te verkrijgen of andere schadelijke activiteiten uit te voeren. Het framework biedt cybercriminelen de mogelijkheid om de kwetsbaarheden te testen en uit te buiten. Beveiligingsonderzoekers en Apple-gebruikers worden aangespoord om op de hoogte te blijven van nieuwe updates en patches die deze kwetsbaarheden verhelpen.

Proof of Concept voor Windows Disk Cleanup Tool EoP gepubliceerd

Een proof of concept (PoC) voor de kwetsbaarheid CVE-2025-21420 in de Windows Disk Cleanup Tool is openbaar gedeeld. Deze kwetsbaarheid betreft een elevation of privilege (EoP), die aanvallers in staat stelt om met verhoogde rechten toegang te krijgen tot systemen. De PoC is beschikbaar op GitHub, waar het mogelijk is om de exploit te testen. Het risico van deze kwetsbaarheid ligt in de mogelijkheid voor aanvallers om kritieke systeeminstellingen te manipuleren, wat kan leiden tot verdere aanvallen. De kwetsbaarheid is relevant voor Windows-gebruikers, en het is aanbevolen om snel updates en patches te installeren om deze dreiging te mitigeren.

Silver Fox breidt Winos 4.0-aanvallen uit

Het cybercriminele groep Silver Fox heeft zijn aanvallen met de Winos 4.0-malware, ook bekend als ValleyRAT, uitgebreid naar Japan en Maleisië. Deze aanvallen maken gebruik van de HoldingHands RAT, ook wel Gh0stBins genoemd. De aanvallen worden uitgevoerd via phishingmails met kwaadaardige PDF-bestanden die valse links bevatten. Winos 4.0 wordt vaak verspreid via phishing en SEO-vergiftiging, waarbij slachtoffers worden verleid naar nepwebsites die populaire software nabootsen. Silver Fox, een Chinese hacker groep, heeft eerder al bekende kwetsbaarheden uitgebuit om deze malware te verspreiden. De aanvallen gebruiken de HoldingHands RAT om op afstand toegang te verkrijgen tot geïnfecteerde systemen, waarbij gevoelige informatie kan worden verzameld en verdere schadelijke payloads kunnen worden gedownload. Dit is onderdeel van een bredere campagne die gericht is op bedrijven in Azië, met name in de financiële en technologie sectoren.

Grote malwarecampagne via valse macOS-tools verspreidt Odyssey Stealer en AMOS

In de afgelopen maanden is er een grote malwarecampagne gericht op macOS-ontwikkelaars, waarbij valse downloadwebsites zich voordoen als vertrouwde platforms zoals Homebrew en LogMeIn. De aanvallers gebruiken social engineering-technieken, zoals het manipuleren van de clipboard en het obfusceren van commando’s, om slachtoffers te misleiden. De gedownloade malware, Odyssey Stealer en AMOS, is in staat om systeeminformatie, browsergegevens en cryptovaluta-inloggegevens te stelen. De campagne maakt gebruik van meer dan 85

phishingdomeinen, die via gedeelde SSL-certificaten en servers met elkaar zijn verbonden. De malware wordt geïnstalleerd door gebruikers naar een kwaadaardige terminalopdracht te sturen die automatisch een secundaire payload downloadt. De campagne maakt gebruik van langlopende infrastructuur en voortdurend gewijzigde technieken om detectie te vermijden. De gebruikte infrastructuur vertoont tekenen van langdurige activiteit, wat wijst op een goed georganiseerde en aanhoudende dreiging.

Top tien van kwetsbaarheden die momenteel worden aangevallen in Nederland

De lijst van meest aangevallen kwetsbaarheden in Nederland toont een variëteit aan kwetsbaarheden die momenteel actief worden benut door aanvallers. De top drie wordt aangevoerd door CVE-2023-38646 in Metabase, gevolgd door CVE-2023-42793 in JetBrains TeamCity, en CVE-2023-22515 in Atlassian Confluence. Deze kwetsbaarheden worden voornamelijk geassocieerd met bekende aanvallen, zoals ransomware en exploitatie van gestolen toegang. Verder in de lijst bevinden zich oudere kwetsbaarheden, waaronder CVE-2019-1653 in Cisco's RV320/RV325, die nog steeds doelwit zijn van aanvallen. Andere kwetsbaarheden, zoals die in Apache Log4j en SolarWinds Serv-U, blijven ook actief ondanks dat ze al enkele jaren bekend zijn. Het is opvallend dat sommige kwetsbaarheden, zoals CVE-2024-28995 in SolarWinds, relatief recent zijn, maar snel op de radar van aanvallers staan.

Top tien van kwetsbaarheden die momenteel worden aangevallen in België

In België worden verschillende kwetsbaarheden in uiteenlopende systemen momenteel actief aangevallen. De top drie kwetsbaarheden wordt geleid door CVE-2023-22515 in Atlassian Confluence, gevolgd door CVE-2023-42793 in JetBrains TeamCity. Beide kwetsbaarheden zijn bekend bij aanvallers en kunnen leiden tot bekende aanvallen. Andere kwetsbaarheden in apparaten zoals de Zyxel P660HN-T1A v1 en v2 (CVE-2017-18368) en Huawei’s Home Gateway HG532 (CVE-2017-17215) blijven risico’s vormen. Ook kwetsbaarheden in softwareproducten zoals ThinkPHP5 (CNVD-2018-24942) en Draytek’s Vigor series (CVE-2020-15415) zorgen voor beveiligingsproblemen. Verder verschijnen er nieuwe kwetsbaarheden, zoals CVE-2025-3248 in Langflow, die in de nabije toekomst steeds meer op de radar van aanvallers komen. Ondanks dat sommige kwetsbaarheden weinig recente

meldingen hebben, blijven ze een potentieel risico voor de digitale veiligheid in België.

Top tien van kwetsbaarheden die momenteel wereldwijd worden aangevallen

Wereldwijd worden diverse kwetsbaarheden in netwerksystemen en IoT-apparaten actief aangevallen. De top drie bestaat uit CVE-2023-42793 in JetBrains TeamCity, CVE-2023-22515 in Atlassian Confluence, en CVE-2017-17215 in Huawei's Home Gateway HG532. Deze kwetsbaarheden worden vaak misbruikt voor aanvallen en vormen grote risico's voor de digitale veiligheid. Andere kwetsbaarheden, zoals CVE-2023-20198 in Cisco IOS XE en CVE-2019-12780 in Belkin Wemo, blijven eveneens frequent doelwit van aanvallers. Vooral apparaten zoals de Dasan GPON Home Router (CVE-2018-10562) en de Realtek SDK (CVE-2014-8361) worden massaal aangevallen, met implicaties voor de gebruikersbeveiliging. De lijst wordt verder aangevuld door kwetsbaarheden in oudere producten van Zyxel en Netgear, die ondanks hun leeftijd nog steeds actief worden misbruikt. Deze kwetsbaarheden vormen een voortdurende bedreiging voor zowel bedrijven als consumenten wereldwijd.

Trending CVE's en kwetsbaarheden op sociale media

Er zijn verschillende kritieke kwetsbaarheden trending op sociale media. CVE-2025-25257 is een SQL-injectie in Fortinet's FortiWeb, die aanvallers toegang geeft tot gevoelige data. CVE-2025-59230, een zero-day in Windows RasMan, maakt privilege-escalatie mogelijk, waardoor aanvallers SYSTEM-rechten kunnen verkrijgen. Andere opmerkelijke kwetsbaarheden zijn onder meer CVE-2025-49144 in Notepad++ en CVE-2024-4701 in Genie, die beide privilege-escalatie mogelijk maken. Er zijn ook kwetsbaarheden in Google Chrome (CVE-2021-38003) en IIS (CVE-2025-59282), die aanvallers in staat stellen om code uit te voeren met verhoogde rechten. Het is belangrijk dat beveiligingsteams de trending kwetsbaarheden in de gaten houden en snel reageren om de risico's te minimaliseren.

Envoy Air bevestigt datadiefstal door Clop-extortionisten

Envoy Air, een dochteronderneming van American Airlines, heeft bevestigd dat gegevens zijn gecompromitteerd in een aanval op hun Oracle E-Business Suite. Deze aanval werd opgeëist door de Clop-extortionisten, die de gestolen data op hun lekwebsite plaatsten. Het bedrijf meldde dat na het incident snel een onderzoek werd gestart en de wetshandhavers werden ingeschakeld. Hoewel geen gevoelige klantgegevens werden aangetast, kunnen beperkte zakelijke informatie en contactgegevens mogelijk zijn gestolen. Deze aanval maakt deel uit van een bredere campagne van de Clop-groep, die sinds augustus gebruik maakte van een zero-day kwetsbaarheid in Oracle-systemen. Eerder werd al bekend dat Clop in andere gevallen ook Harvard University en tientallen andere organisaties heeft getroffen. Oracle had de kwetsbaarheid aanvankelijk gepatcht, maar later werd onthuld dat de groep een zero-day exploit gebruikte. De Clop-groep is sinds 2019 actief en heeft wereldwijd talrijke datadiefstallen uitgevoerd.

Verkoop van platform voor geldautomatenfraude op het darkweb

We ontdekten de vermeende verkoop van een platform voor het frauduleus ophalen van geld bij geldautomaten, genaamd "Cutlet Maker". Het platform zou worden aangeboden op het darkweb, waar het wordt gepromoot als een hulpmiddel voor het uitvoeren van cash-out fraude via geldautomaten. Er is weinig bekend over de werking van dit platform, maar het blijkt een opkomende dreiging te zijn voor de financiële sector. Dergelijke tools kunnen ernstige gevolgen hebben voor de beveiliging van financiële instellingen en hun klanten. De verkoop van dergelijke platforms is een voorbeeld van hoe criminelen nieuwe technologieën gebruiken om traditionele banksystemen te omzeilen en financieel gewin te behalen via cybercriminaliteit. Deze ontwikkeling benadrukt de voortdurende dreiging van cybercriminaliteit op het darkweb.

Glupteba command-and-control domein geïdentificeerd

Een mogelijk command-and-control domein van de Glupteba botnet is geïdentificeerd. Het domein, dat momenteel een 404 foutmelding retourneert, kan onlangs gedeactiveerd of inactief zijn. Echter, eerdere associaties wijzen op het gebruik van dit domein voor C2-operaties van de Glupteba malwarefamilie. De kans dat dit domein wordt gebruikt voor kwaadwillige activiteiten wordt op 50% ingeschat. De verdachte URL is https://server14.safarimexican[.]net/. Het wordt aanbevolen om

toegang tot dit domein te blokkeren op alle netwerkniveaus, inclusief DNS, proxy en firewall, en om te monitoren op tekenen van Glupteba-activiteiten. Dit omvat bijvoorbeeld HTTP-beaconing of het gebruik van proxygerelateerde opdrachten voor persistentie. Aangezien Glupteba vaak tijdelijke of gerecycled domeinen gebruikt, kan het domein opnieuw worden geactiveerd in toekomstige campagnes, mogelijk met dezelfde registrantpatronen of hergebruikte TLS-certificaten.

Echtpaar berooft meer dan 3.000 mensen in vakantie-oplichterij van £28 miljoen

Een oplichterskoppel, Mark Rowe en zijn vrouw Nicola, hebben meer dan 3.000 slachtoffers beroofd in een vakantie-oplichterij die hen £28,1 miljoen kostte. Het echtpaar richtte hun scam in via de organisatie Sell My Timeshare (SMT), waarbij zij voornamelijk oudere timeshare-eigenaren benaderden die hun eigendommen wilden verkopen. De slachtoffers werden misleid met beloften van waardeloze "Monster Credits", die zouden zorgen voor kortingen op vakanties en winkelaankopen. Veel slachtoffers investeerden aanzienlijke bedragen, soms door leningen af te sluiten, om later te ontdekken dat de credits geen waarde hadden, terwijl zij nog steeds de kosten van hun timeshares moesten betalen. De oplichters gaven het gestolen geld uit aan een luxe levensstijl, waaronder kunst, vastgoed en privévluchten. Mark Rowe kreeg zeven en een half jaar gevangenisstraf voor samenzwering tot fraude, terwijl zijn vrouw schuldig pleitte voor witwassen van geld.