Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

31-10-2025:

Bagnoles.nl getroffen door Qilin ransomwaregroep

Bagnoles.nl, opgericht in 2001, is een gespecialiseerde leverancier van nieuwe en gebruikte auto's, inclusief lichte bedrijfsvoertuigen. Het bedrijf heeft meerdere vestigingen in Europa en biedt concurrerende prijzen aan autobedrijven in heel Europa en daarbuiten. In 2022 werd ECAR BV opgericht voor de verkoop van elektrische voertuigen aan zowel particulieren als autobedrijven. Klanten krijgen exclusieve toegang tot actuele voorraadlijsten en prijzen via een persoonlijke account, en het bedrijf biedt volledige logistieke ondersteuning.

Op 30 oktober 2025 werd Bagnoles.nl getroffen door een ransomware-aanval, waarbij de Qilin ransomwaregroep de verantwoordelijkheid voor de aanval heeft opgeëist. Bagnoles.nl maakt gebruik van Microsoft 365 en Proofpoint Essentials, en de aanval heeft vermoedelijk geleid tot de toegang van gevoelige gegevens, hoewel er geen verdere details over de schade zijn verstrekt.

Canada waarschuwt voor aanvallen op gas- en waterbedrijven

De Canadese overheid heeft gewaarschuwd dat vitale infrastructuren in het land het doelwit zijn geworden van hacktivisten. Industriële controlesystemen van een olie- en gasbedrijf, waterbedrijf en een graandroogsilo zijn aangevallen. Bij het waterbedrijf konden de aanvallers de waterdrukwaarden manipuleren, wat leidde tot een verminderde dienst. Bij het olie- en gasbedrijf werd een Automated Tank Gauge-systeem gemanipuleerd, wat voor een vals alarm zorgde. De graandroogsilo werd aangevallen waarbij de aanvallers temperatuur- en luchtvochtigheidniveaus aanpasten, wat gevaarlijke situaties had kunnen veroorzaken. De getroffen bedrijven zijn anoniem, maar het Canadese cybercentrum adviseert vitale organisaties om hun systemen achter een VPN te plaatsen en gebruik te maken van tweefactorauthenticatie (2FA). Ook worden uitgebreide monitoring en penetratietests aangeraden. De aanvallen lijken opportunistisch, met hacktivisten die zich richten op vanaf internet toegankelijke industriële systemen.

WordPress-sites aangevallen via kwetsbaarheid in plug-in Freeio

Een kritieke kwetsbaarheid in de populaire WordPress-plug-in Freeio wordt actief misbruikt door aanvallers. Deze plug-in wordt gebruikt om WordPress-sites om te

zetten in marktplaatsen voor freelancers. De kwetsbaarheid, aangeduid als CVE-2025-11533, bevindt zich in de registratiefunctie van de plug-in, waardoor aanvallers zich ongeauthenticeerd kunnen registreren als administrator en volledige controle over de website kunnen verkrijgen. Het beveiligingslek is beoordeeld met een ernstige score van 9.8 op een schaal van 1 tot 10. Na de ontdekking op 9 oktober 2025, werden de eerste aanvallen snel waargenomen. Beheerders van WordPress-sites die deze plug-in gebruiken, wordt dringend aangeraden de nieuwste versie van de plug-in te installeren en te controleren of er ongeautoriseerde administrator-accounts zijn aangemaakt.

Kwetsbare Windows-servers in Nederland (81) en België (10) vormen risico na ontdekking van WSUS-kwetsbaarheid

Het Amerikaanse Cybersecurity & Infrastructure Security Agency (CISA) heeft organisaties aangespoord om kwetsbare Windows-servers te controleren vanwege een actieve bedreiging die gebruik maakt van een kritieke kwetsbaarheid in de Windows Server Update Service (WSUS), aangeduid als CVE-2025-59287. Deze kwetsbaarheid kan aanvallers in staat stellen om gevoelige systemen binnen organisaties te compromitteren. De kwetsbaarheid is specifiek van toepassing op Windows-servers waar de WSUS-rol is ingeschakeld. CISA raadt aan de noodpatch van Microsoft te installeren die op 23 oktober is uitgebracht. Als organisaties deze patch niet meteen kunnen doorvoeren, wordt aanbevolen om de WSUS-rol uit te schakelen of inkomend verkeer naar de TCP-poorten 8530 en 8531 te blokkeren. Er wordt ook geadviseerd om verdachte activiteiten te monitoren. Volgens The Shadowserver Foundation zijn duizenden kwetsbare servers nog steeds vanaf het internet toegankelijk, waaronder in Nederland 81 en in België 10.

Kwetsbaarheid in WordPress-plugin stelt privédata bloot

De Anti-Malware Security en Brute-Force Firewall plugin voor WordPress, geïnstalleerd op meer dan 100.000 websites, vertoont een kwetsbaarheid die het mogelijk maakt voor abonnees om bestanden op de server te lezen. Dit kan leiden tot het blootstellen van gevoelige informatie. De kwetsbaarheid, aangeduid als CVE-2025-11705, werd ontdekt door Dmitrii Ignatyev en betreft versies van de plugin tot en met 4.23.81. Het probleem ontstaat door ontbrekende controlemechanismen in de functie GOTMLS_ajax_scan(), waardoor een aanvaller bestanden zoals de wp-

config.php kan lezen. Hierdoor kunnen wachtwoordhashes en gebruikersgegevens worden gestolen. De kwetsbaarheid heeft geen kritiek niveau, aangezien authenticatie vereist is, maar websites met lidmaatschaps- of abonnementsfunctionaliteit zijn kwetsbaar. Na melding van het probleem werd op 15 oktober 2025 versie 4.23.83 van de plugin uitgebracht, die de kwetsbaarheid verhelpt. Het wordt sterk aangeraden om de update te installeren.

Kritieke kwetsbaarheden in Apache Tomcat kunnen leiden tot RCE en console manipulatie, patch direct toepassen

Apache Tomcat versies 9, 10 en 11 bevatten kritieke en hoge-severiteitskwetsbaarheden die kunnen leiden tot remote code execution (RCE) en manipulatie van de console. De kwetsbaarheden CVE-2025-55752 en CVE-2025-55754 kunnen ernstig zijn wanneer ze niet gepatcht worden. CVE-2025-55752 betreft een relatieve pad-traversal kwetsbaarheid die een aanvaller in staat stelt om beveiligingsmaatregelen te omzeilen, terwijl CVE-2025-55754 gebruik maakt van speciaal gemaakte URL's om console manipulatie uit te voeren. Daarnaast is er een medium-severiteitskwetsbaarheid, CVE-2025-61795, die kan leiden tot een denial-of-service (DoS). Het is dringend aan te raden de nieuwste versies van Apache Tomcat te installeren om deze kwetsbaarheden te verhelpen. Patchen moet als hoogste prioriteit worden behandeld.

RediShell RCE-kwetsbaarheid stelt 8.500+ Redis-instanties bloot aan code-uitvoeringsaanvallen

De RediShell RCE-kwetsbaarheid, geïdentificeerd als CVE-2025-49844, werd openbaar bekend in oktober 2025. Deze kwetsbaarheid bevindt zich in de Lua-scripttaal van Redis, een veelgebruikte in-memory database. Door een use-after-free-fout kunnen aanvallers de sandbox van Lua ontsnappen en op kwetsbare systemen remote code uitvoeren. De impact is groot, met wereldwijd meer dan 8.500 Redis-instanties die blootstaan aan deze kwetsbaarheid. Vooral systemen zonder authenticatie, die vaak in ontwikkelomgevingen voorkomen, zijn gevoelig voor deze aanval. Geografische analyses tonen aan dat de meeste kwetsbare systemen zich in de Verenigde Staten, Frankrijk en Duitsland bevinden. De aanval maakt het mogelijk om na toegang verder te escaleren, bijvoorbeeld door reverse shells te installeren of

ransomware te verspreiden. Organisaties wordt dringend aangeraden om hun Redis-versies bij te werken of tijdelijke beveiligingsmaatregelen in te stellen.

LinkedIn phishing richt zich op financiële executives met valse bestuursuitnodigingen

Hackers maken gebruik van LinkedIn om financiële executives te targeten met phishing-aanvallen via directe berichten. De berichten doen zich voor als uitnodigingen om lid te worden van een fictief bestuursorgaan van een nieuw opgericht investeringsfonds, genaamd Common Wealth. De ontvangers worden gevraagd op een link te klikken voor meer informatie, waarna ze worden omgeleid via verschillende redirects naar een malafide website die zich voordoet als een "LinkedIn Cloud Share" platform. Hier wordt hen gevraagd in te loggen via een vervalste Microsoft-loginpagina. Het doel is om de inloggegevens van de slachtoffers te stelen. De aanvallers maken gebruik van CAPTCHA-technologieën om bots te blokkeren, waardoor de pagina's moeilijker automatisch te analyseren zijn. Dit is de tweede LinkedIn phishingcampagne gericht op executives die Push Security heeft gedetecteerd in de afgelopen weken.

"Brash" exploit laat Chromium browsers direct crashen via kwaadaardige URL

De "Brash" kwetsbaarheid in de Blink rendering engine van Chromium stelt aanvallers in staat om browsers binnen enkele seconden te laten crashen. Deze kwetsbaarheid ontstaat door een gebrek aan snelheidsbeperkingen op het "document.title" API, wat betekent dat een aanvaller miljoenen wijzigingen in het documentobjectmodel (DOM) per seconde kan sturen. Dit resulteert in een browser die niet meer reageert en het systeem vertraagt door overmatig gebruik van de CPU. De aanval verloopt in drie fasen: de voorbereiding van de gegevens, het injecteren van snelle bursts van updates, en het verzadigen van de UI-thread van de browser. Brash kan ook worden geprogrammeerd om op specifieke momenten te worden uitgevoerd, wat het tot een krachtig hulpmiddel maakt voor aanvallers. De kwetsbaarheid treft alle browsers op Chromium, zoals Google Chrome, Microsoft Edge en Opera, maar Mozilla Firefox en Apple Safari zijn immuun.

PolarEdge botnet infecteert 25.000+ apparaten en 140 C2-servers door misbruik van IoT-kwetsbaarheden

Het PolarEdge botnet heeft meer dan 25.000 IoT-apparaten in 40 landen geïnfecteerd en 140 command-and-control (C2)-servers opgezet om cybercriminaliteit te ondersteunen. Het botnet, dat sinds februari 2025 bekend is, maakt misbruik van kwetsbare IoT- en edge-apparaten en creëert een netwerk van Relay Box-infrastructuur voor geavanceerde dreigingsactoren. De malware werkt via een client-server architectuur, waarbij besmette apparaten de RPX_Client-component installeren, die communicatie met de C2-servers faciliteert. Geografische analyses tonen een concentratie van infecties in Zuidoost-Azië en Noord-Amerika, met Zuid-Korea als het belangrijkste doelwit. Het botnet richt zich vooral op apparaten van merken zoals KT, Shenzhen TVT, Cyberoam en verschillende routermodellen van Asus, DrayTek, Cisco en D-Link. De malware maakt gebruik van een complexe multi-hop proxyarchitectuur om herkomst van aanvallen te verbergen.

12 kwaadaardige extensies in VSCode Marketplace stelen broncode en exfiltreren inloggegevens

Onlangs is een geavanceerde supply chain-aanval ontdekt die gericht was op ontwikkelaars wereldwijd via de officiële VSCode Marketplace. Twaalf kwaadaardige extensies werden geïdentificeerd, waarvan vier nog actief waren op het moment van rapportage. Deze extensies, die zich voordeden als legitieme productiviteitstools, infiltreerden ontwikkelomgevingen en stelden cybercriminelen in staat om projectcode, gevoelige gegevens en zelfs het klembord te stelen. De aanvallers gebruikten verschillende technieken, waaronder HTTP-verzoeken en persistente socketverbindingen, om de gestolen gegevens naar externe servers te sturen. Het incident benadrukt de kwetsbaarheid van de software-supply chain, waarbij dergelijke extensies toegang kregen tot vertrouwelijke informatie zonder gedetecteerd te worden door standaard beveiligingsscans. Dit voorval onderstreept de noodzaak voor strengere controle en monitoring van extensies op ontwikkelaarsmarktplaatsen.

Nieuwe malware richt zich op WooCommerce-websites met schadelijke plugins die creditcardgegevens stelen

Een geavanceerde malwarecampagne richt zich op WooCommerce-websites, waarbij kwaadwillige plugins worden gebruikt om betaalgegevens van klanten te stelen. De malware maakt gebruik van versleuteling, vervalste afbeeldingsbestanden

en verborgen achterdeurtjes, wat de detectie bemoeilijkt. Het systeem is ontworpen om de beveiliging te omzeilen door administratoren toegang te verschaffen via gestolen inloggegevens of onveilige plugins. Na installatie blijft de malware verborgen in de WordPress-plugin directory en verzamelt het creditcardgegevens via een Javascript-skimmer die actief is op de afrekenpagina's van WooCommerce. De gestolen gegevens worden via verschillende mechanismen geëxfiltreerd naar aanvallers. De malware is gekoppeld aan de Magecart Group 12, een bekende dreigingsactor. Deze aanval benadrukt het risico voor online webwinkels en hun klanten, evenals het belang van up-to-date beveiligingsinfrastructuur.

Ex-directeur defensiebedrijf VS bekent verkopen van exploits aan reseller

Een voormalige directeur van een Amerikaans defensiebedrijf heeft bekend dat hij exploits, oorspronkelijk bedoeld voor de Amerikaanse overheid en bondgenoten, heeft verkocht aan een Russische reseller. De 39-jarige verdachte heeft hiermee 1,3 miljoen dollar verdiend, terwijl de waarde van de gestolen informatie 35 miljoen dollar bedraagt. De exploits, waarvan acht "cyber exploit components" werden verkocht, waren bedoeld voor gebruik door de Amerikaanse overheid. De reseller heeft een breed klantenbestand, waaronder de Russische overheid. De ex-directeur heeft twee aanklachten van het stelen van handelsgeheimen bekend en riskeert maximaal 20 jaar gevangenisstraf en een boete van 500.000 dollar. De naam van het defensiebedrijf en de reseller worden niet vrijgegeven, maar het bedrijf zou Trenchant kunnen zijn.

Nepagent aangehouden, hoogbejaarde vrouw krijgt geld terug

Op de avond van 29 oktober 2025 werd een 97-jarige vrouw uit Breda benaderd door een man die zich voordeed als politieagent. Hij vertelde haar dat hij een buurtonderzoek uitvoerde vanwege misdadigers in de buurt. De vrouw, die zijn legitimatie niet goed kon controleren, vertrouwde de situatie aanvankelijk, maar vroeg alsnog naar zijn legitimatie. Ze gaf de man enkele honderden euro's om foto's van te maken, maar kreeg later argwaan en belde de politie. Kort daarna werden in Amsterdam twee verdachten aangehouden, een 16-jarige en een 20-jarige man, beide uit Amsterdam. Het gestolen geld werd teruggevonden en aan de vrouw geretourneerd. De politie onderzoekt de zaak verder en waarschuwt dat mensen

altijd om legitimatie moeten vragen bij onverwachte bezoeken van zogenaamde politieagenten.

Ex-medewerker Virgin Media O2 beboet voor verkoop klantdata aan fraudeurs

Een voormalige medewerker van Virgin Media O2 is beboet voor het verkopen van klantgegevens aan fraudeurs. De informatie werd gebruikt om minstens 65 mensen op te lichten voor een totaalbedrag van 1,75 miljoen euro. De fraudeurs contacteerden de slachtoffers met de belofte te investeren in cryptovaluta, maar verdwenen met het geld. De Britse financiële toezichthouder FCA vervolgde de 30-jarige ex-medewerker wegens schending van de privacywetgeving, waarvoor een boete van 440 euro is opgelegd. Daarnaast moet de verdachte 570 euro aan proceskosten betalen. De twee fraudeurs die de oplichting uitvoerden, kregen al gevangenisstraffen van twaalf jaar. Dit incident benadrukt het groeiende risico van insider threats in de telecomsector.

Neptelefoontjes namens de bank: Waarschuwing voor oplichting

Er zijn weer meldingen van oplichting waarbij criminelen zich voordoen als medewerkers van banken. Ze gebruiken de techniek 'spoofing' om het telefoonnummer van de bank na te apen. De oplichters proberen het vertrouwen van hun slachtoffers te winnen door te zeggen dat hun bankrekening in gevaar is. Vervolgens vragen ze om geld over te maken naar een ‘veilige rekening’ of om inloggegevens en pincodes te verstrekken. Ook kan men gevraagd worden een programma te installeren waarmee de oplichters op afstand toegang krijgen tot apparaten. Deze oplichting is bijzonder gevaarlijk, omdat de criminelen soms persoonlijke gegevens van hun slachtoffers hebben. Dit kan bijvoorbeeld door eerder geïnstalleerde schadelijke software of door datalekken. De Fraudehelpdesk adviseert om nooit inloggegevens of pincodes te verstrekken en altijd het telefoonnummer van de bank zelf op te zoeken.

Alweer storing bij grote clouddienst, wat maakt ze zo kwetsbaar?

Deze maand waren er twee grote storingen bij clouddiensten van Microsoft en Amazon, waarbij populaire platforms zoals de NS-app, Microsoft Teams, Minecraft, Reddit, Snapchat en andere apps tijdelijk offline waren. De storingen werden

veroorzaakt door kleine technische fouten, maar door de enorme schaal van deze clouddiensten hadden ze een grote impact op wereldwijd gebruik. Azure en AWS vormen een essentieel onderdeel van het moderne internet, met ongeveer de helft van het internet die draait op hun servers. De verspreiding van deze clouddiensten over verschillende datacentra wereldwijd beperkt de gevolgen meestal tot een regio. De cloud biedt bedrijven een kostenefficiënte en schaalbare oplossing voor hun digitale infrastructuur, maar heeft ook nadelen, zoals kwetsbaarheid bij grote storingen en zorgen over de opslag van gevoelige data bij grote Amerikaanse bedrijven.

Amerikaanse geheime dienst geeft tips voor beveiligen van Exchange-servers

De Amerikaanse geheime dienst NSA heeft een reeks aanbevelingen gepresenteerd voor het versterken van de beveiliging van Microsoft Exchange-servers. De NSA benadrukt dat Exchange-omgevingen voortdurend doelwit zijn van cyberaanvallen en dat organisaties altijd een verhoogd risico moeten inbouwen. Vooral nu Microsoft de ondersteuning voor Exchange Server 2016 en 2019 heeft stopgezet, zijn deze versies kwetsbaarder voor aanvallen. De belangrijkste aanbeveling is het up-to-date houden van servers en het inschakelen van de Emergency Mitigation Service, die automatisch beveiligingsmaatregelen toepast zonder de tussenkomst van beheerders. Verder wordt aangeraden beveiligingsbaselines toe te passen, Microsoft Defender Antivirus te gebruiken en de beheerderstoegang tot de servers te beperken. De NSA benadrukt dat door deze best practices te volgen, de kans op succesvolle aanvallen aanzienlijk kan worden verminderd.

Russische ransomwaregroepen gebruiken open-source AdaptixC2 voor geavanceerde aanvallen

De open-source command-and-control (C2) framework AdaptixC2 wordt steeds vaker ingezet door diverse dreigingsactoren, waaronder groepen die verbonden zijn met Russische ransomwarebendes. Oorspronkelijk ontworpen voor ethische hackactiviteiten en penetratietests, wordt AdaptixC2 nu misbruikt voor post-exploitatie en aanvallen. Het systeem, dat onder andere versleutelde communicatie en commando-uitvoering mogelijk maakt, werd voor het eerst openbaar gedeeld door een GitHub-gebruiker in 2024. De framework is inmiddels overgenomen door verschillende ransomwaregroepen, waaronder Fog en Akira, en wordt ook gebruikt

door een initial access broker. Het gebruik van AdaptixC2 is toegenomen, vooral via Telegram, wat zorgen oproept over de banden van de ontwikkelaar met de Russische onderwereld. Er wordt onderzocht of de maker zelf betrokken is bij kwaadwillende activiteiten.