Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

21-11-2025:

Door datalek getroffen patiënten Clinical Diagnostics worden ingelicht

Het laboratorium Clinical Diagnostics in Rijswijk heeft recentelijk getroffen patiënten geïnformeerd over een datalek dat eerder dit jaar plaatsvond. Het lek resulteerde in de openbaarmaking van privégegevens van honderdduizenden mensen wiens lichamelijke onderzoeken door het laboratorium waren verwerkt. De getroffen gegevens betreffen geen informatie van deelnemers aan het Bevolkingsonderzoek Nederland. Patiënten, van wie de gegevens via een huisarts waren doorgegeven, ontvangen brieven van het laboratorium waarin zij worden geïnformeerd over de gebeurtenis. Het laboratorium heeft aangegeven geen precieze datum te noemen voor wanneer deze brieven arriveren.

Huisartsen die rechtstreeks betrokken waren bij de aanvraag van onderzoeken krijgen eveneens een brief. Huisartsen die geen brief ontvangen, maar vermoeden dat patiënten getroffen zijn, kunnen contact opnemen met Clinical Diagnostics voor meer informatie. De omvang van het datalek is nog steeds niet volledig duidelijk. Het lek werd in juli 2025 ontdekt en in augustus gemeld. Begin september werden de eerste patiënten geïnformeerd over de gegevens die waren gelekt. In totaal waren meer dan 941.000 mensen betrokken bij het incident, waarvan gegevens zoals namen, geboortedata, adressen, testuitslagen en burgerservicenummers konden zijn buitgemaakt.

Een klein aantal van de gehackte gegevens werd op het darkweb aangetroffen. Het laboratorium heeft nog niet bevestigd of er losgeld is betaald voor het herstel van de gegevens. De situatie is nog in onderzoek, en de getroffen organisaties zijn bezig met het herstellen van de gevolgen van het incident.

China-Nexus APT groep gebruikt DLL-sideloading techniek voor aanvallen op overheden en media

Een geavanceerde cyberespionagecampagne, uitgevoerd door de China-Nexus APT-groep, richt zich sinds begin 2025 op overheids- en mediageorganisaties in Zuidoost-Azië, met een specifieke focus op landen rondom de Zuid-Chinese Zee. De aanval maakt gebruik van de DLL-sideloading techniek en exploiteert een kwetsbaarheid in WinRAR (CVE-2025-8088) om toegang te krijgen tot de doelwitten.

De aanvallen beginnen met een ogenschijnlijk legitiem bestand, genaamd "Proposal_for_Cooperation_3415.05092025.rar", dat een kwetsbaarheid in WinRAR uitbuit wanneer slachtoffers proberen de inhoud te extraheren. Dit stelt de aanvallers in staat een persistentiescript in de opstartmap van de gebruiker te installeren via een paddoorsteken en een Alternatieve Gegevensstroomtechniek. De campagne maakt gebruik van vier verschillende stadia om de infectie te verspreiden, waarbij elke fase is ontworpen om detectie te vermijden.

In het tweede stadium wordt gebruik gemaakt van een gewijzigde versie van de legitieme OBS-browser, die een aangepaste libcef.dll-bestand laadt om kwaadaardige code uit te voeren. De aanvallers communiceren met hun command-and-control servers via Telegram en hebben toegang tot functies zoals shell-executie, het maken van screenshots en het uploaden van bestanden. In de derde fase wordt Adobe's Creative Cloud Helper misbruikt om een kwaadaardig CRClient.dll bestand te laden, dat versleutelde payloads decrypteert met een eenvoudige XOR-techniek.

De uiteindelijke backdoor biedt uitgebreide mogelijkheden voor remote toegang via HTTPS, waarbij het netwerkverkeer wordt versleuteld om detectie door traditionele beveiligingssystemen te bemoeilijken. De backdoor ondersteunt verschillende commando’s, waaronder het uitvoeren van opdrachten, het laden van DLL-bestanden en het manipuleren van bestanden.

Deze cyberaanvallen richten zich op cruciale infrastructuren in de overheids- en mediasectoren, wat hen tot waardevolle doelen maakt vanwege hun invloed op beleid, publieke opinie en internationale strategische afstemming.

Iraanse hackers gebruiken AIS-gegevens voor fysieke raketaanval

Hackgroepen met banden met Iran hebben geavanceerde cyberoperaties uitgevoerd om fysieke aanvallen te faciliteren, waarbij ze informatie verzamelden via het Automatic Identification System (AIS) van schepen. Deze digitale verkenning was onderdeel van een bredere cyberstrategie om real-world missielanceringen te ondersteunen. Dit toont de toenemende vervaging van de grenzen tussen cyberaanvallen en traditionele militaire operaties, wat nieuwe risico's met zich meebrengt voor de beveiliging van maritieme infrastructuren.

De groep Imperial Kitten, gelinkt aan de Iraanse Revolutionaire Garde (IRGC), voerde tussen december 2021 en januari 2024 digitale verkenning uit op maritieme systemen, met als doel toegang te krijgen tot scheepsinformatie en infrastructuur. Via

hacks op de AIS-systemen en CCTV-camera's van schepen konden de hackers real-time gegevens verzamelen die later werden gebruikt voor gerichte raketaanvallen, zoals de mislukte aanval op 27 januari 2024.

Deze incidenten onderstrepen de geavanceerde technieken die door nation-state actor groepen worden ingezet, waarbij cyberoperaties worden gebruikt om fysieke aanvallen te verbeteren. Dit werpt nieuwe vragen op over de effectiviteit van traditionele cybersecuritymaatregelen en de noodzaak van geïntegreerde strategieën voor zowel cyberbeveiliging als fysieke beveiliging van kritieke infrastructuren wereldwijd.

NHS waarschuwt voor misbruik kwetsbaarheid in 7-Zip

De Britse gezondheidszorgorganisatie NHS heeft een waarschuwing uitgegeven over de actieve exploitatie van een kwetsbaarheid in het populaire archiveringsprogramma 7-Zip, bekend als CVE-2025-11001. Deze kwetsbaarheid stelt aanvallers in staat om via speciaal geprepareerde zip-bestanden remote code execution uit te voeren. Het probleem doet zich voor bij de verwerking van symbolische links in zip-bestanden, waarmee een aanvaller schadelijke bestanden kan plaatsen in een andere directory. Dit kan leiden tot het laden van malware of andere schadelijke code wanneer het zip-bestand door een slachtoffer wordt geopend.

De kwetsbaarheid werd in juli 2025 verholpen in versie 25.00 van 7-Zip, maar het bestaan van het lek werd niet expliciet vermeld in de release notes. De impact van de kwetsbaarheid wordt beoordeeld met een score van 7.0 op de schaal van 1 tot 10, aangezien het slachtoffer het bestand zelf moet openen om de aanval mogelijk te maken.

Volgens NHS Digital wordt de kwetsbaarheid actief misbruikt door aanvallers, maar worden er geen specifieke details over de aanvallen gedeeld. Organisaties die gebruikmaken van 7-Zip wordt geadviseerd de software te updaten naar de laatste versie om beveiligingsrisico's te minimaliseren.

D-Link waarschuwt voor nieuwe RCE-kwetsbaarheden in end-of-life DIR-878 routers

D-Link heeft een waarschuwing afgegeven voor drie kwetsbaarheden in de DIR-878 router, die het mogelijk maken om op afstand commando's uit te voeren. Deze router,

die in 2017 werd geïntroduceerd als een high-performance dual-band draadloze router, heeft zijn einde van de levensduur bereikt, maar wordt nog steeds in verschillende markten verkocht. De kwetsbaarheden kunnen op afstand worden misbruikt en zijn van toepassing op alle modellen en hardwareversies van de DIR-878.

De kwetsbaarheden omvatten onder andere de mogelijkheid voor ongeauthenticeerde afstandsbediening via bepaalde netwerkcommando's die in de router zijn opgeslagen, en via IP-adressen die in de iptables-commando's worden geïnjecteerd. D-Link heeft aangekondigd dat het geen beveiligingsupdates meer zal uitbrengen voor dit model, aangezien de ondersteuning voor de DIR-878 in 2021 is beëindigd. Het bedrijf raadt gebruikers aan om de router te vervangen door een model dat nog actief ondersteund wordt.

Hoewel de kwetsbaarheden als medium-severity zijn beoordeeld door de U.S. Cybersecurity and Infrastructure Security Agency (CISA), kunnen ze misbruikt worden door aanvallers, waaronder botnet-operators, die vaak kwetsbaarheden gebruiken om hun netwerk uit te breiden. De recente toevoeging van deze kwetsbaarheden aan exploit-kits verhoogt de risico's, vooral gezien de beschikbaarheid van de exploitcode.

Dit benadrukt de gevaren van het blijven gebruiken van apparaten die hun levensduur hebben bereikt, zonder verdere ondersteuning voor beveiligingsupdates.

SonicWall SonicOS-kwetsbaarheid kan firewalls laten crashen

SonicWall heeft klanten gewaarschuwd voor een ernstige kwetsbaarheid in de SonicOS-SSLVPN, die aanvallers in staat stelt om firewalls te laten crashen. De kwetsbaarheid, aangeduid als CVE-2025-40601, is een buffer overflow op de stack, die een denial-of-service (DoS) aanval mogelijk maakt. Deze kwetsbaarheid treft zowel Gen8- als Gen7-firewalls, zowel hardware- als virtuele versies.

De kwetsbaarheid kan een remote, ongeauthenticeerde aanvaller in staat stellen om de firewall te laten crashen, wat de werking van netwerken kan verstoren. SonicWall heeft aangegeven dat er momenteel geen meldingen zijn van actieve aanvallen of van bewijs dat de kwetsbaarheid al in het wild wordt misbruikt. Desondanks wordt het dringend aanbevolen om de beveiligingsupdates toe te passen die vandaag zijn uitgebracht.

De kwetsbaarheid heeft invloed op een breed scala aan SonicWall-firewallmodellen, waaronder de TZ270, TZ370, NSa-serie en verschillende andere Gen7- en Gen8-modellen. Beheerders die de patch nog niet kunnen implementeren, wordt geadviseerd de SonicOS-SSLVPN-service uit te schakelen of toegang te beperken tot vertrouwde bronnen.

SonicWall heeft ook updates uitgebracht voor andere producten, waaronder de Email Security-apparaten, die kwetsbaarheden bevatten die kunnen leiden tot code-executie en toegang tot gevoelige informatie. Het bedrijf raadt gebruikers van de betrokken producten aan om ook deze updates snel door te voeren.

AI-gedreven fraude neemt exponentieel toe door deepfakes

Fraude aangedreven door kunstmatige intelligentie (AI) groeit in een alarmtempo, waarbij de impact van deepfake-technologie nu een van de grootste dreigingen vormt. Een recent rapport wijst erop dat fraudepogingen met deepfakes een aanzienlijk percentage van de biometrische fraude uitmaken, waarbij deepfake-selfies in 2025 een stijging van 58% vertonen. Dit markeert de geavanceerde mogelijkheden van fraudsters om legitieme gebruikers te imiteren door middel van synthetische media, waardoor traditionele beveiligingsmaatregelen steeds minder effectief blijken.

De zogenaamde ‘deepfake-apps’ kunnen tegenwoordig verbluffend nauwkeurige gezichtsbewegingen genereren, zelfs vanuit een enkele stilstaande afbeelding, wat het voor criminelen mogelijk maakt om overtuigende valse video’s in real-time te produceren zonder ooit daadwerkelijk videomateriaal van het slachtoffer te hebben. Het gebruik van deze technologie is niet beperkt tot persoonlijke fraude; het wordt ook steeds vaker ingezet in de financiële sector, waar fraudeurs profiteren van de toename van online onboarding. Sectors die zich richten op het aanbieden van aanmeldbonussen, zoals de cryptomarkt, ervaren een stijging van 67% in fraudepogingen tijdens de aanmeldingsfase.

Naast deepfakes worden ook digitale vervalsingen van documenten steeds gebruikelijker. In 2025 waren deze vervalsingen goed voor 35% van de gevallen van documentfraude, een stijging ten opzichte van de 30% in voorgaande jaren. Frauduleuze documenten worden steeds vaker gemaakt via ‘fraud-as-a-service’-platforms op het dark web, waar eenvoudig te gebruiken sjablonen en tools beschikbaar zijn. Dit maakt het voor een breed scala aan kwaadwillende actoren

mogelijk om documenten te vervalsen, wat de toegang tot gevoelige informatie vergemakkelijkt.

De geavanceerde technologieën hebben de fraude-industrie geprofessionaliseerd, waarbij niet alleen individuele hackers maar ook goed georganiseerde, wereldwijde criminele netwerken opereren. Deze netwerken delen tactieken, automatiseren processen en specialiseren zich in specifieke fraudestrategieën. Het rapport benadrukt dat hoewel technologie een grote rol speelt, de beste verdediging tegen deze vormen van fraude blijft dat mensen zich bewust zijn van de gevaren en kritisch blijven in hun interacties, vooral wanneer er sprake is van ongevraagde communicatie of urgentie.

Android-malware kan WhatsApp- en Signal-berichten op telefoon lezen

Onderzoekers hebben recent nieuwe malware ontdekt die in staat is om berichten van populaire chatdiensten zoals WhatsApp, Signal en Telegram te lezen op besmette Android-telefoons. De malware, genaamd Sturnus, heeft zijn oorsprong als banking trojan, wat betekent dat het oorspronkelijk werd ontworpen voor bankfraude. Echter, de malware heeft verdergaande capaciteiten, waaronder het monitoren van communicatie op genoemde platformen.

Sturnus maakt gebruik van de Android Accessibility Service om real-time berichten op het scherm van de telefoon te lezen, inclusief inkomende en uitgaande berichten, en zelfs de volledige inhoud van gesprekken. De malware kan ook de identiteit van de gebruiker stelen door nep-inlogschermen te tonen boven bank-apps, waarmee het gevoelige gegevens zoals bankgegevens verzamelt. Daarnaast is Sturnus in staat om op afstand toegang te verkrijgen tot de besmette telefoon en deze te manipuleren. Zo kan het bijvoorbeeld een zwart scherm tonen terwijl malafide activiteiten op de achtergrond plaatsvinden, zoals frauduleuze banktransacties.

De malware heeft extra beveiligingsmaatregelen ingebouwd om te voorkomen dat het verwijderd wordt. Het kan de telefoon op afstand vergrendelen en blokkeren dat gebruikers de administrator-rechten van de malware in de instellingen kunnen intrekken. Hierdoor wordt het voor slachtoffers bijzonder lastig om de malware te verwijderen, zelfs met tools zoals ADB. Sturnus richt zich momenteel vooral op doelen in Centraal en Zuid-Europa, maar gezien de veelzijdigheid van de malware is het mogelijk dat het zich verder zal verspreiden.

Onderzoekers konden informatie van 3,5 miljard WhatsApp-accounts scrapen

Onderzoekers van de Universiteit van Wenen hebben ontdekt dat ze door een kwetsbaarheid in WhatsApp in staat waren om informatie van 3,5 miljard accounts te verzamelen. De kwetsbaarheid werd veroorzaakt door het mechanisme waarmee WhatsApp gebruikers toestaat andere gebruikers te zoeken op basis van telefoonnummers. Met deze techniek konden de onderzoekers een systeem ontwikkelen waarmee ze tot 100 miljoen telefoonnummers per uur konden controleren, waardoor ze toegang kregen tot publieke gegevens van WhatsApp-gebruikers wereldwijd.

De informatie die werd verzameld omvatte onder andere telefoonnummers, openbare sleutels, tijdstempels, en indien openbaar, ook profielfoto's en tekstberichten. Met deze gegevens konden de onderzoekers aanvullende informatie verkrijgen, zoals het besturingssysteem van de gebruiker, de leeftijd van het account, en het aantal gekoppelde apparaten. Dit stelde hen in staat gedetailleerde profielen te bouwen van WhatsApp-gebruikers wereldwijd.

Uit het onderzoek blijkt dat zelfs met beperkte gegevens van gebruikers waardevolle informatie kan worden afgeleid. Zo konden de onderzoekers miljoenen actieve WhatsApp-accounts identificeren in landen waar WhatsApp officieel verboden is, zoals China, Iran en Myanmar. Verder bleek dat 81 procent van de WhatsApp-gebruikers Android gebruikt, tegenover 19 procent op iOS.

Meta, het moederbedrijf van WhatsApp, heeft de kwetsbaarheid inmiddels verholpen en gaf aan dat er geen aanwijzingen zijn dat kwaadwillenden van deze fout misbruik hebben gemaakt. Hoewel er geen toegang werd verkregen tot privéberichten, onderstreept dit incident de risico's van datalekken en de gevaren van het openbaar maken van telefoonnummers. De onderzoekers hebben hun verzamelde gegevens inmiddels verwijderd.

Meer dan duizend websites besmet door malafide code via gehackt marketingbedrijf

In augustus 2025 werd ontdekt dat meer dan duizend websites besmet waren met malafide code die afkomstig was van een gehackt digitaal marketingbedrijf. Het bedrijf, gevestigd in Taiwan, werd meerdere keren gecompromitteerd door een geavanceerde aanvallergroep die door Google wordt aangeduid als APT24. Deze groep wordt vermoedelijk gelinkt aan China en heeft in de afgelopen jaren herhaaldelijk websites overgenomen om kwaadaardige code te injecteren.

De aanvallers gebruikten een digitale marketingstrategie waarbij zij een JavaScript library aan de klantwebsites aanboden. Wanneer bezoekers op deze websites kwamen, werden zij gefingerprint en, indien aan bepaalde voorwaarden voldaan werd, kregen zij een pop-up te zien die hen verleidde om een "update" voor Google Chrome te downloaden. In werkelijkheid leidde deze update tot de infectie van de systemen met malware.

Het marketingbedrijf werd in juni 2025 opnieuw getroffen, waarbij de aanvallers hun aanvallen beperkten tot één domein. In augustus werd echter voor een periode van tien dagen deze beperking opgeheven, waardoor de malafide code zich op meer dan duizend domeinen verspreidde. Naast het compromitteren van websites verstuurde APT24 ook phishingmails die werden gepersonaliseerd om de slachtoffers verder te misleiden en aan te vallen.

Google wijst erop dat de voortdurende aanvallen van APT24 wijzen op de evolutie van de groep, die gebruikmaakt van steeds geavanceerdere technieken zoals supply chain compromissen, meerlaagse social engineering en het misbruik van legitieme clouddiensten. De aanvallen vormen een toenemende bedreiging voor zowel bedrijven als consumenten, waarbij de aanvallers steeds adaptiever en volhardender worden in hun pogingen tot spionage.

Massale toename in kwaadaardige scanning van GlobalProtect VPN-portalen

Op 14 november 2025 werd een opmerkelijke toename van kwaadaardige scanningactiviteit gedetecteerd die gericht was op de loginportalen van Palo Alto Networks GlobalProtect VPN. Volgens GreyNoise, een bedrijf dat gespecialiseerd is in real-time dreigingsinformatie, steeg de activiteit met maar liefst 40 keer binnen 24 uur. Deze intensivering markeert een piek in de scanningactiviteit die in de afgelopen 90 dagen niet meer werd waargenomen. Gedurende de periode van 14 tot 19 november werden maar liefst 2,3 miljoen sessies geregistreerd die het loginpunt /global-protect/login.esp van de VPN-systemen aanvielen.

De aanvallen richten zich voornamelijk op de Verenigde Staten, Mexico en Pakistan. GreyNoise heeft eerder gewaarschuwd dat deze type scans vaak voorafgaan aan de ontdekking van nieuwe kwetsbaarheden. Het gebruik van bepaalde autonome systeemnummers (ASNs) en herhaalde TCP/JA4-tak-afdrukken suggereert dat deze aanvallen verband houden met eerdere gerelateerde campagnes. Vooral de ASN's

AS200373 (3xK Tech GmbH) en AS208885 (Noyobzoda Faridduni Saidilhom) worden in verband gebracht met deze activiteit.

De toename van dergelijke kwaadaardige probes benadrukt de noodzaak om dergelijke aanvallen niet te onderschatten, omdat ze vaak gepaard gaan met de ontdekking van nieuwe kwetsbaarheden. De afgelopen maanden heeft Palo Alto Networks al meerdere beveiligingsproblemen aangepakt, waaronder de exploitatie van CVE-2025-0108, die later werd gekoppeld aan andere kwetsbaarheden zoals CVE-2025-0111 en CVE-2024-9474. Deze nieuwe toename van scanningpogingen roept opnieuw de vraag op naar de kwetsbaarheid van VPN-systemen, die mogelijk het doelwit kunnen worden van toekomstige aanvallen.

Vals telefoontje uit naam van de Fraudehelpdesk

Op 20 november 2025 ontving de Fraudehelpdesk meldingen van een nieuwe phishing-aanval waarbij criminelen zich voordoen als medewerkers van de Fraudehelpdesk. In deze poging werd de belofte gedaan om gedupeerden van beleggingsfraude te helpen hun verloren geld terug te krijgen. De bellers gaven zich voor als vertegenwoordigers van een Brits bedrijf dat gecontracteerd was door de Fraudehelpdesk om telefonisch contact op te nemen. Ze beweerden dat het kapitaal van de melder bevroren was en boden hun hulp aan om het geld terug te krijgen.

De melder, die in het verleden slachtoffer was geworden van beleggingsfraude, was echter sceptisch en vroeg om verdere informatie per e-mail. Kort daarna ontving de melder een e-mail die zogenaamd afkomstig was van de ‘Fraudehelpdesks van Nederland en België’. De e-mail was gepersonaliseerd en meldde dat er een speciale taskforce was opgericht om gedupeerden van fraudeurs, die inmiddels strafrechtelijk vervolgd werden, te ondersteunen.

In de e-mail werd de melder gevraagd verschillende documenten te verstrekken, waaronder een geldig identiteitsbewijs met foto, een recent bewijs van adres, en documenten die de geleden schade konden aantonen, zoals bankafschriften of correspondentie met de fraudeur. De melder werd ook gevraagd om de ontvangst van de e-mail te bevestigen.

De Fraudehelpdesk heeft bevestigd dat zowel het telefoontje als de e-mail vals zijn. Ze waarschuwt dat de organisatie nooit telefonisch contact opneemt met slachtoffers van fraude voor het terughalen van verloren geld, en nooit e-mails verstuurt over het begeleiden van gedupeerden. Personen die een dergelijk telefoontje ontvangen of

een soortgelijke e-mail krijgen, wordt geadviseerd het contact direct te verbreken en geen documenten met persoonlijke gegevens te verstrekken.

Als je twijfelt of een bericht echt is, neem dan contact op met de Fraudehelpdesk voor verder advies. Het is belangrijk om je bewust te zijn van dergelijke phishing-aanvallen en om nooit persoonlijke informatie via ongewenste communicatiekanalen te delen.

Tsundere Botnet breidt zich uit via game-lokkers en Ethereum-gebaseerde C2-infrastructuur

Er is een uitbreiding van het Tsundere botnet geconstateerd, een steeds grotere bedreiging voor Windows-gebruikers. Het botnet, dat sinds midden 2025 actief is, maakt gebruik van geavanceerde infectiemethoden door MSI- en PowerShell-bestanden die game-thema's, zoals Valorant, Rainbow Six Siege X, en Counter-Strike 2, als lokkertjes inzetten. Dit duidt erop dat aanvallers specifiek gericht zijn op gebruikers die op zoek zijn naar gekraakte versies van deze games.

De besmetting begint wanneer een geïnfecteerd bestand via een legitiem Remote Monitoring and Management (RMM)-tool wordt gedownload, dat vervolgens een MSI-bestand van een gecompromitteerde website haalt. Het installatiebestand zet Node.js in gang en voert een loader-script uit dat de hoofdpayload van het botnet decrypteert. Het botnet maakt gebruik van de pm2-bibliotheek om persistente toegang tot het systeem te verkrijgen en zorgt ervoor dat de malware bij elke opstart opnieuw wordt uitgevoerd.

Het Tsundere botnet gebruikt Ethereum-blockchain-technologie om informatie over de C2-server te verkrijgen, wat zorgt voor dynamische serverrotatie. Dit maakt de aanvalsinfrastructuur moeilijker te traceren en te stoppen, aangezien de serveradressen via slimme contracten op de blockchain kunnen worden aangepast. Dit gebruik van blockchain-technologie vergroot de robuustheid en flexibiliteit van de botnet-operaties.

De verspreiding van dit botnet via game-thema's en de integratie van blockchain-technologie maakt het een geavanceerde dreiging, die moeilijk te detecteren en te blokkeren is voor traditionele beveiligingsmaatregelen. Het Tsundere botnet benadrukt de evolutie van malware en de complexiteit van hedendaagse cyberaanvallen, die steeds meer gebruik maken van gedistribueerde netwerken en innovatieve technologieën om onopgemerkt te blijven.

Rhadamanthys-loader gebruikt geavanceerde technieken om detectie te omzeilen

De Rhadamanthys-malware, die sinds 2022 actief is, heeft zich gepositioneerd als een van de gevaarlijkste stealer-malwares wereldwijd. Het wordt gebruikt in gerichte aanvallen om gevoelige gegevens van slachtoffers te stelen, waaronder inloggegevens en financiële informatie. Het onderscheidt zich door zijn vermogen om traditionele beveiligingstools te omzeilen, wat het bijzonder problematisch maakt voor beveiligingsteams.

Wat de malware bijzonder uitdagend maakt, is de complexiteit van de loader, die fungeert als het primaire mechanisme voor het afleveren van de kwaadaardige lading. In tegenstelling tot de stealer zelf, is de loader bedoeld om de infectie voor te bereiden en bevat meerdere lagen van bescherming om analyse en detectie te voorkomen. Deze bescherming omvat op maat gemaakte obfuscatietechnieken die de code moeilijk te begrijpen maken voor zowel geautomatiseerde tools als menselijke analisten.

Een van de belangrijkste anti-sandboxingtechnieken die de Rhadamanthys-loader gebruikt, is gebaseerd op een tijdgebaseerde analyse van het gebruikersgedrag. Het malwareprogramma verzamelt gegevens zoals de positie van de cursor en de actieve vensters gedurende een bepaalde periode. Als de malware detecteert dat de gegevens niet voldoen aan de kenmerken van een realistische gebruikersomgeving, wordt de payload niet uitgevoerd. Dit systeem is ontworpen om traditionele sandboxes, die vaak geen realistisch menselijk gedrag simuleren, te misleiden. Echter, sommige geavanceerde sandboxes hebben zich aangepast en kunnen de payload alsnog activeren.

De lading die door de loader wordt gedragen, is verder beveiligd met een op maat gemaakte coderingsalgoritme genaamd Flutter en een extra versleuteling met de Chinese SM4-codering. Deze lagen van bescherming maken het uiterst moeilijk voor beveiligingssoftware om de ware aard van de payload te ontdekken.

De complexiteit van de Rhadamanthys-malware benadrukt de steeds geavanceerdere methoden die cybercriminelen gebruiken om hun activiteiten te verbergen en beveiligingstools te omzeilen. Het blijft een belangrijke uitdaging voor zowel analisten als organisaties die proberen zich te beschermen tegen deze dreiging.

Nieuwe ransomware-varianten richten zich op Amazon S3-diensten door misconfiguraties en toegangscontrole te misbruiken

Een nieuwe aanvalsgolf richt zich op cloud-opslagdiensten, met name Amazon Simple Storage Service (S3)-emmanden, door misbruik te maken van configuratiefouten en zwakke toegangsbeheersystemen. Dit soort aanvallen verschilt van traditionele ransomware-aanvallen doordat de aanvallers niet via schadelijke software bestanden versleutelen, maar door toegang te verkrijgen via gestolen inloggegevens, gelekte toegangssleutels of gecompromitteerde AWS-accounts met overmatige machtigingen.

Na toegang te hebben gekregen tot de cloudomgeving, identificeren de aanvallers kwetsbare S3-buckets door te zoeken naar zwakheden zoals uitgeschakelde versiebeheeropties en onjuiste schrijfbevoegdheden. Ze versleutelen vervolgens de data met verschillende technieken, verwijderen bestanden of exfiltreren gevoelige informatie, waarna ze losgeld eisen. Wat deze aanvallen bijzonder riskant maakt, is het gebruik van cloudfunctionaliteiten, waardoor ze moeilijk te detecteren zijn door traditionele beveiligingssystemen.

Trend Micro heeft vijf ransomware-varianten geïdentificeerd die specifiek gericht zijn op S3-opslagomgevingen. Een van de meest gevaarlijke methoden is het gebruik van klantbeheerde versleuteling, waarbij de aanvallers de encryptiesleutel beheren, waardoor de versleutelde data permanent onherstelbaar is, tenzij het losgeld wordt betaald of er een beveiligde back-up beschikbaar is.

Organisaties kunnen zich beschermen tegen deze dreiging door beleidsmaatregelen in te stellen die versleuteling via klantbeheerde sleutels blokkeren en door de CloudTrail-logbestanden op verdachte activiteiten te monitoren.

Russische hacker gearresteerd op Phuket, gezocht door FBI voor cyberaanvallen

Op 6 november 2025 werd een Russische hacker gearresteerd op het Thaise eiland Phuket. De verdachte, een 35-jarige man die door de FBI wordt gezocht, wordt beschuldigd van het uitvoeren van cyberaanvallen op overheidsinstellingen in zowel de Verenigde Staten als Europa. De arrestatie volgde op een internationale aanwijzing van de FBI, die het bevel tot zijn aanhouding had uitgevaardigd.

De verdachte, die op 30 oktober 2025 Thailand binnenkwam, werd in zijn hotel in Phuket gearresteerd. Tijdens de arrestatie werd digitale apparatuur zoals laptops,

mobiele telefoons en digitale portemonnees in beslag genomen. De FBI was aanwezig bij de actie en ondersteunde de Thaise autoriteiten.

De verdachte wordt beschuldigd van betrokkenheid bij geavanceerde cyberaanvallen die gericht waren op gevoelige overheidsinformatie. Er is een uitleveringsverzoek ingediend door de Verenigde Staten, maar het is nog onduidelijk wanneer deze procedure zal worden afgerond. De verdachte zou zich verzetten tegen zijn uitlevering, aldus berichten uit Rusland.

Dit incident benadrukt de groeiende dreiging van internationale hackers die gericht zijn op overheids- en infrastructuurnetwerken wereldwijd.

Oprichters cryptomixer Samourai Wallet veroordeeld voor witwassen van bitcoins

Twee Amerikaanse mannen, oprichters van de cryptomixer Samourai Wallet, zijn veroordeeld tot gevangenisstraffen voor hun betrokkenheid bij het witwassen van bitcoins die afkomstig waren van criminele activiteiten. De ene oprichter kreeg vier jaar gevangenisstraf, terwijl de andere een straf van vijf jaar kreeg. Daarnaast moeten ze elk een boete van 250.000 dollar betalen. De veroordeling volgt op een "plea deal" met de Amerikaanse autoriteiten, waarbij de oprichters instemden met het verbeurd verklaren van 237 miljoen dollar, het bedrag dat via hun cryptomixer was gewassen.

Samourai Wallet was een populaire cryptomixer die gebruikers in staat stelde hun cryptovaluta te verhullen door deze samen te voegen met die van andere gebruikers. Cryptomixers zijn bedoeld om de herkomst en bestemming van cryptotransacties te verbergen, wat voor criminelen een methode was om onrechtmatig verkregen bitcoins te ‘witten’. De Samourai Wallet-app werd meer dan 100.000 keer gedownload en bood twee diensten aan: de Whirlpool-mixer en de Ricochet-dienst. De eerste mengde bitcoins van verschillende gebruikers, terwijl de laatste extra transacties toevoegde om de herkomst verder te verhullen. Volgens de autoriteiten werden meer dan 80.000 bitcoins door de mixer verwerkt, waarvan een groot deel afkomstig was van illegale online marktplaatsen, ransomware-aanvallen en phishing.

De oprichters van Samourai Wallet erkenden in onderschepte berichten dat hun platform specifiek werd aangemoedigd voor het witwassen van crimineel geld. Ze ontvingen provisie voor elke transactie die via hun platform werd uitgevoerd, wat hen meer dan 6 miljoen dollar opleverde. Het onderzoek naar de zaak benadrukt het gebruik van cryptomixers door criminelen om illegale activiteiten te verdoezelen,

terwijl voorstanders beweren dat dergelijke diensten legitieme privacydoeleinden dienen.

Europol versterkt bestrijding van sanctie-omzeiling

Europol heeft haar activiteiten tegen het omzeilen van EU-sancties versterkt door de oprichting van een speciaal team binnen haar European Financial and Economic Crime Centre, genaamd ‘Target Group Sanctions’. Dit team richt zich specifiek op het identificeren en verstoren van criminele netwerken die de sancties, opgelegd in reactie op de Russische agressie tegen Oekraïne, proberen te omzeilen. Europol maakt gebruik van geavanceerde analytische en financiële tracingcapaciteiten om illegale handelsroutes op te sporen en gerelateerde criminele activiteiten zoals witwassen, douanefraude en documentenvervalsing te detecteren.

Naast de operationele versterking door de 'Target Group Sanctions', heeft Europol in samenwerking met het Europese Bureau voor Fraudebestrijding (OLAF) het project 'Project Transporter' gelanceerd. Dit project richt zich op de export van voertuigen naar derde landen die mogelijk via omwegen naar Rusland en Wit-Rusland worden doorgestuurd. Het project beoogt de opsporing van vervalste documenten en de inzet van complexe omleidingsroutes, die vaak worden ingezet om EU-sancties te omzeilen.

Door deze gezamenlijke initiatieven wordt een sterkere, meer gecoördineerde aanpak gegenereerd om criminele netwerken die betrokken zijn bij sanctie-omzeiling te stoppen. Europol en OLAF versterken hiermee de samenwerking tussen lidstaten om de integriteit van de EU-maatregelen te waarborgen.

35 arrestaties bij grootschalig kunstsmokkelonderzoek in Bulgarije

Op 19 november 2025 werd in Bulgarije een grootschalige operatie uitgevoerd tegen een crimineel netwerk dat betrokken was bij de smokkel van cultuurgoederen. Deze operatie, gecoördineerd door de Bulgaarse autoriteiten en ondersteund door Europol, leidde tot 35 arrestaties en de doorzoeking van 131 locaties in verschillende Europese landen. Het netwerk wordt verdacht van het illegaal verhandelen van antiquiteiten, waaronder Griekse en Romeinse voorwerpen van onschatbare waarde.

Het onderzoek begon in 2020 na een inval waarbij 7.000 cultuurvoorwerpen, waaronder zeldzame artefacten en antiquiteiten, werden in beslag genomen. De

meeste van deze objecten hadden geen documentatie van herkomst, wat leidde tot verdenkingen van illegale opgravingen en de verkoop van gestolen cultuurgoederen op de wereldwijde kunstmarkt.

Het gebruik van digitale technologieën en grensoverschrijdende samenwerking speelde een cruciale rol in het opsporen van de verdachten. Europol richtte een taskforce op om informatie te delen en de activiteiten van het netwerk in kaart te brengen. De operatie werd uitgevoerd met steun van landen als Albanië, Frankrijk, Duitsland, Griekenland, Italië en het Verenigd Koninkrijk.

Deze zaak benadrukt de gevaren van digitale en internationale netwerken die de kunstmarkt exploiteren om gestolen cultuurgoederen te verhandelen en wit te wassen. Het illustreert ook de uitdagingen van het verifiëren van de herkomst van kunstwerken en de rol van digitale opsporingsmethoden in de bestrijding van georganiseerde misdaad in de kunstsector.

De in beslag genomen artefacten, waaronder gouden munten en antieke kunstwerken, hebben een geschatte waarde van meer dan 100 miljoen euro. Dit onderstreept de economische impact van kunstsmokkel, die vaak gepaard gaat met digitale en financiële misdrijven.

Internationale samenwerking en het gebruik van digitale opsporingstechnieken zijn essentieel voor het succesvol bestrijden van kunstsmokkelnetwerken en het beschermen van het culturele erfgoed van Europa.

Nieuwe EU-wetgeving bedreigt privacy door herziening van de AVG

De Europese Commissie heeft een nieuw voorstel gepresenteerd, de zogenaamde 'digital omnibus', dat de bescherming van persoonsgegevens binnen de EU zou kunnen verzwakken. Dit voorstel, dat gericht is op het bevorderen van innovatie en het vergemakkelijken van bedrijfsactiviteiten voor techbedrijven, bevat wijzigingen die volgens de Europese burgerrechtenbeweging EDRi de privacy van burgers in gevaar kunnen brengen.

Een van de belangrijkste veranderingen betreft de herdefiniëring van persoonlijke gegevens, wat het voor AI-bedrijven makkelijker maakt om modellen te trainen met persoonlijke data zonder expliciete toestemming van gebruikers. Daarnaast wordt de meldtermijn voor datalekken verlengd van 72 naar 96 uur, en kunnen bedrijven

voortaan gegevens op apparaten van gebruikers verzamelen op basis van 'legitiem belang' zonder voorafgaande toestemming.

EDRi heeft scherpe kritiek op dit voorstel, omdat het bedrijven te veel ruimte geeft om persoonlijke gegevens te verzamelen en verwerken, met minimale transparantie en toezicht. Dit kan leiden tot meer kwetsbaarheden in de bescherming van persoonsgegevens en verhoogde risico's op misbruik van data.

Deze veranderingen kunnen aanzienlijke gevolgen hebben voor de cybersecurity en privacy van gebruikers in de EU. De burgerrechtenbeweging roept op om dit voorstel grondig te heroverwegen, aangezien het de kern van de AVG kan ondermijnen.

Toegang AI-chatbot vlam-chat voor rijksambtenaren roept vragen op over beveiliging

Volgend jaar krijgen duizenden rijksambtenaren toegang tot de AI-chatbot vlam-chat, ontwikkeld door SSC-ICT, die hen moet ondersteunen bij schrijftaken, vertalingen en samenvattingen. Acht ministeries, waaronder Binnenlandse Zaken en Volksgezondheid, hebben zich aangesloten bij dit project, dat naar verwachting 26.000 ambtenaren in een eerste fase zal bereiken. Dit aantal zal tegen medio 2026 verder uitbreiden naar honderdduizend gebruikers.

Vlam-chat draait volledig in een datacenter van de overheid en maakt gebruik van Europese taalmodellen, wat de veiligheid van de overheidsdata moet waarborgen. Het project maakt deel uit van het bredere vlam.ai-initiatieven, dat ook een zoekfunctie biedt voor het doorzoeken van overheidsinformatie. Naast de chatfunctie biedt vlam.ai mogelijkheden zoals het genereren van tekst en het detecteren van taalfouten.

Toch roept de introductie van AI-chatbots binnen de overheid vragen op over de cybersecurity. De bescherming van gevoelige overheidsinformatie is cruciaal, en de integratie van AI kan kwetsbaarheden blootstellen die cybercriminelen kunnen exploiteren. Het is belangrijk dat de beveiliging van deze systemen continu wordt gecontroleerd en verbeterd om misbruik te voorkomen. De inzet van AI-tools in de publieke sector kan verder de complexiteit van het cyberdreigingslandschap vergroten, wat vraagt om verhoogde waakzaamheid bij overheidsinstanties.

Brussel heeft gevolgen van het aanpassen van de AVG niet onderzocht

De Europese Commissie heeft volgens de Autoriteit Persoonsgegevens (AP) de gevolgen van het plan om de Algemene Verordening Gegevensbescherming (AVG) aan te passen niet grondig onderzocht. Dit komt naar voren uit een reactie van de AP op de recente voorstellen van Brussel, die beogen de AVG en de AI-verordening te herzien. De AP stelt dat de voorgestelde wijzigingen niet ten koste mogen gaan van de fundamentele mensenrechten. De privacytoezichthouder wijst erop dat de gevolgen van deze ingrijpende wijzigingen voor zowel burgers, bedrijven als toezichthouders onvoldoende zijn geëvalueerd.

Brussel heeft recent een reeks maatregelen gepresenteerd onder de naam "digital omnibus". Deze reeks beoogt onder andere het aanpassen van de definitie van persoonlijke data en het vergemakkelijken voor AI-bedrijven om gegevens van mensen zonder hun expliciete toestemming te gebruiken voor het trainen van AI-modellen. Critici waarschuwen dat dergelijke wijzigingen vergaande gevolgen kunnen hebben voor de privacy van Europese burgers.

De AP benadrukt dat het recht van individuen om zelf te bepalen wat er met hun persoonlijke gegevens gebeurt, essentieel is en niet zomaar mag worden aangepast. Daarom zal de toezichthouder de voorstellen verder bestuderen en de bevindingen delen met het publiek en relevante ministeries. De AP roept op tot zorgvuldigheid en duidelijkheid bij het doorvoeren van dergelijke aanpassingen, aangezien de veranderingen grote impact kunnen hebben op de uitvoerbaarheid van de wetgeving binnen de EU.

Salesforce onderzoekt datadiefstal via Gainsight-inbraak

Salesforce is momenteel een onderzoek gestart naar een datadiefstal die mogelijk klantgegevens van verschillende bedrijven heeft getroffen. De inbraak is gerelateerd aan de Gainsight-applicatie, die een externe verbinding heeft met Salesforce. Het lijkt erop dat de aanvallers ongeautoriseerde toegang hebben verkregen tot Salesforce-gegevens via deze verbinding, maar er wordt geen kwetsbaarheid binnen het Salesforce-platform zelf gevonden.

Na het detecteren van de ongebruikelijke activiteit heeft Salesforce alle actieve toegangstokens voor Gainsight-gebruikers ingetrokken en tijdelijk de app uit de AppExchange verwijderd. Klanten die getroffen zijn door dit incident zijn op de hoogte gesteld en kunnen verdere assistentie krijgen via de klantenservice van Salesforce.

Het incident doet denken aan eerdere datadiefstallen, zoals de inbraak in augustus 2025 waarbij de "ShinyHunters"-groep miljoenen Salesforce-records heeft gestolen. Dit benadrukt opnieuw de risico's van externe applicaties en integraties met platforms zoals Salesforce, waarbij aanvallers toegang kunnen krijgen tot gevoelige bedrijfsgegevens.

TP-Link klaagt Netgear aan voor smaadcampagne over security en Chinese hacks

TP-Link heeft een rechtszaak aangespannen tegen zijn concurrent Netgear, waarbij het beschuldigt van een smaadcampagne met betrekking tot de beveiliging van TP-Link-producten. Volgens de aanklacht heeft Netgear valse beweringen verspreid over de technologie van TP-Link, waarbij werd gesuggereerd dat deze producten waren gehackt door Chinese hackers. TP-Link stelt dat deze ongegronde beschuldigingen geleid hebben tot een aanzienlijk verlies van omzet, dat het bedrijf op meer dan 1 miljard dollar schat.

De aanklacht werd ingediend bij een federale rechtbank in Delaware, waar TP-Link beweert dat Netgear journalisten en influencers heeft voorzien van misleidende informatie. Bovendien zou Netgear hiermee een eerdere schikking over een patentenkwestie hebben geschonden. In het kader van deze schikking zou TP-Link 135 miljoen dollar hebben betaald aan Netgear, na een uitspraak die oordeelde dat TP-Link patenten van Netgear had geschonden. De schikking bevatte echter ook een verbod op negatieve uitlatingen over de concurrent.

TP-Link heeft in de aanklacht aangegeven dat het wil dat de smaadcampagne stopt en dat het een schadevergoeding eist voor de geleden verliezen. Deze zaak komt op een moment dat TP-Link al te maken heeft met groeiende bezorgdheid in de Verenigde Staten over de veiligheid van haar producten. De Amerikaanse overheid overweegt het bedrijf te classificeren als een bedreiging voor de nationale veiligheid, een stap die mogelijk zou leiden tot een verbod op de verkoop van TP-Link-producten in de VS. Daarnaast is er ook een strafrechtelijk onderzoek gaande naar het mogelijke antitrustgedrag van TP-Link, dat zich schuldig zou maken aan concurrentievervalsing door routers onder kostprijs aan te bieden.

Bericht over uitsluitend elektrische wagens in binnenstad van Herentals blijkt vals: stad werd ethisch gehackt

Op 20 november 2025 ontstond er verwarring in de Belgische stad Herentals, toen een bericht circuleerde dat de binnenstad vanaf 1 mei 2026 enkel nog toegankelijk zou zijn voor volledig emissievrije voertuigen. Het bericht, dat de stad zou omvormen tot een zero-emissiezone, bleek echter vals te zijn. De verspreiding van het bericht was onderdeel van een gecontroleerd experiment, uitgevoerd door een team van ethische hackers, in samenwerking met het stadsbestuur en het cyberveiligheidsproject van Streamz.

Het doel van het experiment was om de digitale systemen van de stad te testen op kwetsbaarheden. De hackers hadden toegang gekregen tot de officiële website, de sociale mediakanalen en de digitale infoschermen van de stad, waar zij een nepbericht publiceerden dat verwees naar een nieuw klimaatbeleid. In dit bericht werd gemeld dat alleen elektrische of waterstofvoertuigen nog toegang zouden krijgen tot het stadscentrum. Het bericht bleek fictief en diende enkel als test om de beveiliging van de digitale systemen te verbeteren.

Het stadsbestuur benadrukte het belang van cyberveiligheid in de moderne samenleving en verklaarde dat dergelijke tests essentieel zijn om de bescherming van kritieke systemen te waarborgen. De burgemeester van Herentals, Jan Bertels, gaf aan dat het experiment waardevolle inzichten had opgeleverd over de kwetsbaarheid van de communicatiekanalen van de stad, waardoor er gerichte verbeteringen kunnen worden doorgevoerd.

Online veiligheid van Nederlanders neemt af door eigen gemakzucht, blijkt uit onderzoek van ABN AMRO

Uit onderzoek van ABN AMRO blijkt dat de online veiligheid van Nederlanders afneemt doordat veel consumenten gemakzucht boven veiligheid stellen. Maar liefst 40 procent van de Nederlanders hergebruikt belangrijke wachtwoorden voor onbelangrijke accounts, wat het risico op online oplichting vergroot. Dit probleem komt vooral naar voren in de feestperiode, wanneer er veel online aankopen worden gedaan. Marco Hendriks, fraude-expert bij ABN AMRO, benadrukt dat dit verhoogde gebruik van hetzelfde wachtwoord voor verschillende diensten kan leiden tot ernstige gevolgen, zoals fraude via bankhelpdeskfraude.

Het onderzoek toont ook aan dat 89 procent van de Nederlanders zich bewust is van de risico's die het gebruik van hetzelfde wachtwoord voor meerdere diensten met zich meebrengt. Ondanks dit besef, verandert 32 procent van de mensen zelden hun

wachtwoorden voor kritieke diensten, en 53 procent onderneemt nauwelijks actie bij datalekken. De stijging in het aantal datalekken, dat in 2024 meer dan 35.000 meldingen opleverde, versterkt deze zorgen. Eén datalek kan al voldoende zijn om persoonlijke gegevens in verkeerde handen te laten vallen.

Fraudeurs profiteren van het gemak van consumenten door gebruik te maken van gestolen gegevens voor verder misbruik. Hendriks waarschuwt dat fraudeurs geen haast hebben en weken later via telefoon of andere kanalen geloofwaardige verhalen ophangen, wat bijdraagt aan de verspreiding van fraude. Hij adviseert consumenten om online veiligheid serieus te nemen en goede maatregelen te treffen, zoals het gebruik van sterke, unieke wachtwoorden en tweestapsverificatie voor belangrijke accounts.

De feestdagen, met hun drukte en verhoogde online activiteiten, vormen een verhoogd risico voor consumenten. Het is daarom van belang om niet alleen het gemak, maar vooral de veiligheid voorop te stellen bij het gebruik van online diensten.

Arbeidsmarkt op het darkweb: groeiend aantal banen en nieuwe trends

De arbeidsmarkt op het donkere web heeft zich de afgelopen jaren verder ontwikkeld. In een recent rapport, dat is gebaseerd op meer dan 2.000 werkgerelateerde berichten verzameld van schaduwfora tussen januari 2023 en juni 2025, worden belangrijke trends zichtbaar. Deze onderzoeksresultaten tonen aan dat de vraag naar professionals binnen de schaduweconomie, met name op het gebied van IT, aanzienlijk is toegenomen.

Het grootste deel van de werkzoekenden op het donkere web is niet specifiek gebonden aan een vakgebied en toont een hoge mate van flexibiliteit. Ruim 69% van de werkzoekenden is bereid om uiteenlopende, vaak informele functies op zich te nemen. De meest gevraagde specialisaties zijn ontwikkelaars, penetration testers en geldwassingsexperts. Reverse engineers blijken de hoogste lonen te ontvangen, wat wijst op de grote waarde van hun vaardigheden binnen de cybercriminaliteit.

Het rapport wijst ook op de aanwezigheid van jongeren die vaak op zoek zijn naar snelle en kleine verdiensten, vaak al bekend met frauduleuze praktijken. Dit bevestigt dat het donkere web een toegankelijk platform is voor nieuwe generaties die zich in de schaduweconomie begeven.

Ondanks de informele aard van de arbeidsmarkt op het donkere web, vertoont deze overeenkomsten met de formele arbeidsmarkt. Er wordt steeds meer waarde gehecht aan praktische vaardigheden en er vinden regelmatig achtergrondcontroles plaats, wat de parallelle ontwikkeling van beide markten benadrukt.

In de toekomst wordt verwacht dat de gemiddelde leeftijd van werkzoekenden op het donkere web zal stijgen, deels door de effecten van wereldwijde ontslagen en de voortdurende economische onzekerheid. De arbeidsmarkt op het donkere web blijft dus niet losstaan van de reguliere arbeidsmarkt, maar wordt beïnvloed door dezelfde mondiale economische krachten.

GenAI vergemakkelijkt cybercriminelen bij het opzetten van gesofisticeerde scams

Generative AI (GenAI) heeft de manier waarop cybercriminelen fraude uitvoeren ingrijpend veranderd. Fraudeoperaties zijn nu sneller, overtuigender en makkelijker op te schalen, wat de detectie en preventie van dergelijke aanvallen aanzienlijk bemoeilijkt. Onderzoek toont aan dat frauduleuze campagnes, die voorheen maanden werk en gespecialiseerde technische kennis vereisten, nu binnen enkele uren kunnen worden opgezet door iedereen met basiskennis van computers.

Vroeger waren scams vaak eenvoudig te herkennen door spelfouten, grammaticale fouten en slecht ontworpen websites. GenAI heeft deze barrières weggehaald door fraudeurs in staat te stellen realistische productafbeeldingen, foutloze teksten, levensechte spraakopnames en zelfs video's te genereren. Deze tools maken het mogelijk om op grote schaal gepersonaliseerde scams te creëren die zelfs de meest waakzame gebruikers kunnen misleiden.

Een belangrijk aspect van deze nieuwe fraudemethoden is de automatisering en het gebruik van modulaire platforms. Cybercriminelen kunnen open-source automatiseringstools gebruiken om workflows op te zetten die verschillende taken automatisch uitvoeren, zoals het genereren van vervalste productafbeeldingen en video's. Deze technologie maakt het niet alleen mogelijk om snel frauduleuze content te creëren, maar ook om op grote schaal verschillende varianten van dezelfde scam aan te bieden.

De opkomst van GenAI in cybercriminaliteit heeft grote gevolgen voor de digitale veiligheid. Met name scams die gebruikmaken van social engineering, zoals romance-imposter scams, zijn explosief gestegen, wat een ernstige bedreiging vormt voor de online veiligheid van consumenten. De snelheid en schaal waarop deze

aanvallen plaatsvinden, benadrukken de noodzaak voor versterkte waakzaamheid en het ontwikkelen van geavanceerdere detectiemethoden om dergelijke frauduleuze activiteiten te identificeren.