Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

04-11-2025:

Risico's van ai, deepfakes en opkomst van agi in geopolitieke context

De huidige technologie, bekend als kunstmatige intelligentie (AI), heeft enorme vooruitgangen geboekt, maar de ontwikkeling van kunstmatige algemene intelligentie (AGI) is slechts een paar jaar verwijderd. Terwijl AI specifieke taken uitvoert, zal AGI, wanneer het verschijnt, menselijke cognitieve capaciteiten nabootsen en taken op een breed scala van gebieden uitvoeren. Dit brengt aanzienlijke risico's met zich mee, zoals misbruik, ongelukken en maatschappelijke schade. In 2025 was er al bezorgdheid over de invloed van AI-chatbots op de geestelijke gezondheid, bijvoorbeeld het tragische geval in België waar een man zelfmoord pleegde na interactie met een AI. Daarnaast neemt de verspreiding van deepfakes – valse foto's, audio en video gegenereerd door AI – toe, wat ernstige gevolgen kan hebben, vooral in politiek en oorlog. De opkomst van AGI zou niet alleen de werkgelegenheid verstoren, maar ook de geopolitieke dynamiek veranderen, waarbij landen AI als een wapen kunnen gebruiken.

DDoS-aanval in België: NoName claimt aanvallen op meerdere websites

De hackercollectief NoName heeft aangekondigd verschillende websites in België te hebben aangevallen. De doelwitten omvatten onder andere citydev[.]brussels, het Parlement van Wallonië en VIVAQUA. Deze DDoS-aanvallen hebben voor tijdelijke verstoringen gezorgd. De groep heeft haar verantwoordelijkheid opgeëist via sociale media, maar de impact van de aanvallen is op dit moment nog niet volledig in kaart gebracht. Er wordt onderzocht of er andere doelwitten zijn getroffen en welke verdere schade er is veroorzaakt. De Belgische autoriteiten zijn bezig met het analyseren van de situatie en het versterken van de beveiligingsmaatregelen van de getroffen instellingen.

Locatiegegevens EU-functionarissen te koop: risico op spionage en chantage

Locatiegegevens van miljoenen mobiele telefoons in België, inclusief die van EU-functionarissen, zijn online te koop. Het onderzoek toont aan dat de gegevens, die afkomstig zijn van datahandelaren, een ernstig risico op spionage en chantage met zich meebrengen. De verzamelde gegevens omvatten 2,6 miljoen telefoons en 278 miljoen coördinaten, waarvan een aanzienlijk aantal EU-functionarissen in Brussel en

andere gevoelige EU-locaties betrof. Dankzij de gedetailleerde bewegingspatronen konden zelfs specifieke werkplekken en woonlocaties van EU-functionarissen achterhaald worden. De gegevens zijn bijzonder waardevol voor buitenlandse overheden die deze informatie kunnen gebruiken voor spionage. De handel in dergelijke locatiegegevens, die vaak niet anoniem is, wordt als een ernstig probleem in de wereld van de cybersecurity gezien. Privacy-adviseurs wijzen op de onrechtmatigheid van het verzamelen en verhandelen van dergelijke gegevens zonder geïnformeerde toestemming van de betrokkenen.

China beschuldigt Nederland van verstoring wereldwijde chipproductie

China heeft Nederland beschuldigd van het veroorzaken van verstoringen in de wereldwijde halfgeleiderproductie en de chipaanvoerketen. Dit zou zijn ontstaan doordat de Nederlandse overheid Nexperia, een dochteronderneming van het Chinese Wingtech, onder curatele heeft gesteld. Het Chinese ministerie van Handel heeft Nederland verzocht om zich niet meer in de interne zaken van bedrijven te mengen en een constructieve oplossing te vinden voor de situatie rondom Nexperia. Volgens China heeft de Nederlandse regering geen constructieve houding aangenomen, waardoor de wereldwijde crisis in de toeleveringsketen is verergerd, ondanks de redelijke eisen van China.

Noord-Koreaanse hackers gebruikt AI-filters bij valse sollicitatiegesprekken

De Noord-Koreaanse hackergroep Famous Chollima heeft AI-deepfakes ingezet om zich voor te doen als software-engineers in valse sollicitatiegesprekken bij bedrijven in de cryptocurrency- en Web3-sector. De hackers stalen identiteiten van Mexicaanse ingenieurs en gebruikten AI-gegenereerde gezichtsfilters om hun ware uiterlijk te verbergen tijdens video-interviews. De opzet was om westerse bedrijven te infiltreren voor bedrijfsespionage en financiering. Bij twee identieke pogingen werden de deepfake-technologieën echter duidelijk misbruikt. De gezichten van de nep sollicitanten vertoonden onregelmatigheden, zoals een stilstaande mond tijdens het praten, wat de oplichting ontmaskerde. De kandidaten waren ook nerveus en vertoonden verdacht gedrag, wat verdere twijfel zaaide over hun geloofwaardigheid. Deze pogingen werden verbonden met de Aziatische VPN-dienst Astrill, wat aangeeft dat de hackers probeerden hun Noord-Koreaanse afkomst te verbergen door via

Amerikaanse IP-adressen verbinding te maken. De hackers gaven snel hun LinkedIn-profielen op na de interviews.

Operatie SkyCloak: Tor-campagne richt zich op het leger van Rusland en Wit-Rusland

De nieuwe operatie SkyCloak richt zich op Russische en Wit-Russische militaire doelen door middel van een geavanceerde multi-stage infectieketen. Deze cyberaanval maakt gebruik van Tor-gebaseerde infrastructuur om verborgen toegang tot de systemen te verkrijgen. De campagne richt zich specifiek op de Russische Luchtlandingstroepen en de Wit-Russische Speciale Eenheden, waarbij gebruik wordt gemaakt van legitieme OpenSSH-binaries en obfs4-bruggen om communicatiekanalen te maskeren. De aanvallen beginnen met phishingmails die zich voordoen als officiële militaire documenten en de besmetting wordt geïnitieerd door PowerShell-opdrachten. Het malwaremechanisme gebruikt verschillende lagen van codering en verbergt zich in verborgen mappen op geïnfecteerde systemen. Dit zorgt voor lange-termijn toegang en maakt het moeilijk om de aanval te detecteren. De operatie maakt ook gebruik van Tor's verborgen diensten voor communicatie, waarbij SSH en andere services via niet-standaard poorten beschikbaar worden gesteld.

Hackers gebruiken gemanipuleerde militaire documenten voor SSH-Tor backdoor-aanval

In oktober 2025 ontdekten onderzoekers bij Cyble Research and Intelligence Labs een geavanceerde cyberaanval die gebruikmaakte van gemanipuleerde militaire documenten om een SSH-Tor backdoor te verspreiden. De aanvallen richtten zich specifiek op personeel in de defensiesector, met name binnen het Special Operations Command, gespecialiseerd in onbemande luchtvaartuigen. De kwaadaardige bestanden waren verpakt in een ZIP-bestand, dat werd vermomd als een Belarussisch militair document. Het malwarepakket maakte gebruik van OpenSSH voor Windows en een Tor-hided service met obfs4-verkeer, waardoor de aanvallers anonieme toegang kregen tot verschillende protocollen op de gecompromitteerde systemen. De techniek bevatte ook geavanceerde methoden om detectie te omzeilen, waaronder een meervoudige infectieketen en tegenanalysechecks. De aanval vertoonde overeenkomsten met eerdere campagnes

van de Russische APT-groep UAC-0125, die sinds 2013 actief is in het aanvallen van Oekraïense militaire doelen.

Nog 74 kwetsbare DNS-servers in Nederland en 18 in België missen belangrijke update voor BIND 9-kwetsbaarheden !

Op 3 november 2025 missen nog steeds 74 DNS-servers in Nederland en 18 in België een essentiële beveiligingsupdate voor twee ernstige kwetsbaarheden in BIND 9, de populairste DNS-software. Deze kwetsbaarheden kunnen leiden tot cache poisoning, waarbij aanvallers DNS-servers vervalste informatie laten verstrekken, waardoor gebruikers naar malafide websites worden geleid. Het Nationaal Cyber Security Centrum (NCSC) waarschuwde voor mogelijk misbruik van deze kwetsbaarheden. De kwetsbaarheden (CVE-2025-40778 en CVE-2025-40780) betreffen respectievelijk een zwakte in de Pseudo Random Number Generator en de acceptatie van onbetrouwbare DNS-records. Meer dan 8200 DNS-servers wereldwijd, missen de benodigde updates. Dit verhoogt het risico op aanvallen. Updates werden eind oktober gepubliceerd, maar veel servers zijn nog steeds kwetsbaar.

Microsoft patch voor WSUS-kwetsbaarheid schakelt hotpatching uit voor Windows Server 2025

Een recente noodpatch voor een kwetsbaarheid in de Windows Server Update Services (WSUS) heeft hotpatching op sommige Windows Server 2025-systemen geblokkeerd. De update, KB5070881, werd uitgebracht om de CVE-2025-59287-kwetsbaarheid te verhelpen, die actief werd misbruikt door cybercriminelen. Deze kwetsbaarheid kan leiden tot remote code execution (RCE) aanvallen. De patch werd al snel teruggetrokken voor systemen die hotpatching gebruiken, nadat het probleem werd ontdekt. In plaats van de hotpatch-methode ontvangen getroffen systemen nu reguliere updates, die een herstart vereisen. Microsoft raadt beheerders aan de gecorrigeerde patch KB5070893 te installeren, die geen problemen veroorzaakt met hotpatching. Het probleem heeft impact op machines die zijn ingeschreven voor hotpatching, maar degenen die deze update nog niet hebben geïnstalleerd, kunnen de nieuwe patch zonder problemen toepassen.

AzureHound-tool voor gegevensexport van Azure blootgelegd

Een beveiligingsprobleem met de AzureHound-tool is onlangs ontdekt. Deze tool, die bedoeld is voor het exporteren van gegevens vanuit Azure voor gebruik in BloodHound, werd misbruikt door cybercriminelen om gevoelige gegevens te verkrijgen. De exploitatie van AzureHound biedt aanvallers toegang tot Azure Active Directory-omgevingen en kan leiden tot escalatie van privileges binnen systemen. Palo Alto Networks heeft een gedetailleerde analyse van het misbruik gepresenteerd in hun rapport. Het gebruik van AzureHound door kwaadwillende actoren kan een bedreiging vormen voor organisaties die afhankelijk zijn van Azure voor hun cloudinfrastructuur. Het incident benadrukt de kwetsbaarheid van cloudgebaseerde systemen voor aanvallen en het belang van robuuste beveiligingsmaatregelen in dergelijke omgevingen.

Hackers gebruiken RMM-tools om vrachtvervoerders aan te vallen en ladingen te stelen

Hackers richten zich op vrachtmakelaars en transportbedrijven door kwaadaardige links en e-mails te versturen. Deze berichten bevatten tools voor remote monitoring en management (RMM), zoals NetSupport en ScreenConnect, waarmee de aanvallers volledige controle krijgen over de systemen van de bedrijven. Het doel van de aanvallers is om de vrachtwagens te kapen en fysieke goederen te stelen. De aanvallen zijn met name gericht op Noord-Amerikaanse bedrijven, maar ook in andere landen zoals Brazilië, Mexico, Duitsland en Zuid-Afrika zijn er incidenten gemeld. De aanvallers gebruiken fraude met vrachtvermeldingen en e-mailinbraken om slachtoffers naar schadelijke URL’s te leiden, waarna de RMM-tools worden geïnstalleerd. Deze tools geven de hackers controle over de systemen, waardoor ze de boekingen kunnen aanpassen en ladingen kunnen stelen. De gestolen goederen worden vaak via internet of in het buitenland verkocht.

Sesameop-malware misbruikt OpenAI Assistants API voor aanvallen

Microsoft-onderzoekers hebben een nieuwe backdoor-malware ontdekt, SesameOp, die de OpenAI Assistants API gebruikt als een verborgen command-and-control kanaal. Het werd aangetroffen tijdens het onderzoeken van een cyberaanval in juli 2025. De malware stelt aanvallers in staat om langdurige toegang tot geïnfecteerde omgevingen te behouden, door gebruik te maken van legitieme cloudservices in

plaats van traditionele malafide infrastructuur. SesameOp haalt gecomprimeerde en versleutelde opdrachten op via de API, welke vervolgens op geïnfecteerde systemen worden uitgevoerd. De aanvallers gebruikten deze techniek voor langdurige spionage. Microsoft werkte samen met OpenAI om de misbruikte API-sleutels uit te schakelen en adviseert bedrijven om firewalllogs te controleren, bescherming in te schakelen en endpointdetectie te configureren.

Nep Solidity VSCode-extensie op Open VSX installeert achterdeur bij ontwikkelaars

Een vervalste Solidity-extensie in de Open VSX-registry heeft zich als een populaire ontwikkeltool voorgedaan, maar bevatte de malware SleepyDuck, een remote access trojan. Deze trojan gebruikt een Ethereum-smartcontract om een communicatiekanaal met de aanvaller te creëren, wat zorgt voor langdurige persistentie. De extensie, genaamd 'juan-bianco.solidity-vlang', werd meer dan 53.000 keer gedownload voordat het kwaadwillige karakter werd ontdekt. De malware wordt geactiveerd wanneer een Solidity-bestand wordt geopend, waarna het systeemgegevens verzamelt en het commando-executiesysteem van de aanvaller opzet. Een uniek kenmerk van SleepyDuck is het gebruik van de Ethereum-blockchain om de C2-server te onderhouden, zelfs wanneer de primaire server offline is. Open VSX heeft inmiddels waarschuwingen geplaatst, maar ontwikkelaars moeten voorzichtig zijn met het downloaden van extensies van onbekende auteurs.

ClickFix payload delivery via compromised Shopify template domain

Op 3 november 2025 werd een waarschuwing uitgegeven over een domein dat zich voordeed als een Shopify-verificatiewebsite. Het domein thesmartboater.com bleek onderdeel te zijn van een ClickFix-payload leveringscampagne. Dit domein imiteerde een standaard "beveiligingsverificatie"-pagina, maar bevatte scripts die gebruikers omleidden of secundaire payloads afleverden. Dit soort infrastructuur wordt vaak gebruikt in ClickFix-campagnes, waarbij gecompromitteerde of verlopen Shopify- en WordPress-sjablonen worden geëxploiteerd voor malwarelevering en phishing-omleidingen. De campagne werd met 100% zekerheid bevestigd. Beveiligingsexperts adviseren om toegang tot thesmartboater.com te blokkeren en netwerkbeacons en omleidingen te monitoren die verband houden met deze ClickFix-campagne.

FBI Watchdog detecteert DNS-wijziging bij cybercriminelen

De FBI heeft een wijziging in de DNS-registratie gedetecteerd voor het domein lkxstress[.]su. Het betreft een verandering van de naamservers (NS), waarbij de vorige naamservers zijn vervangen door de nieuwe servers van beget.com, beget.pro en beget.ru. Deze wijziging kan wijzen op een aanpassing van de infrastructuur van een cybercriminele site die mogelijk wordt gebruikt voor ransomware- of andere cyberaanvallen. De verandering werd op 4 november 2025 geregistreerd.

BankBot-YNRK en DeliveryRAT Android Trojans stelen financiële gegevens

Onderzoekers hebben twee Android-trojans ontdekt, BankBot-YNRK en DeliveryRAT, die gericht zijn op het stelen van gevoelige gegevens van besmette apparaten. BankBot-YNRK vermijdt detectie door de omgeving te analyseren en werkt alleen op specifieke apparaten zoals Google Pixel of Samsung. Het kan financiële gegevens stelen en frauduleuze transacties uitvoeren. De malware maakt gebruik van Android's toegankelijkheidsdiensten om verhoogde machtigingen te verkrijgen en misbruik van applicaties zoals cryptocurrency wallets te maken. DeliveryRAT, dat zich voordoet als voedselbezorg- en bankapps, verzamelt ook gegevens en voert acties uit op de achtergrond. Beide trojans worden verspreid via kwaadwillige apps die onterecht toegang vragen tot systeeminstellingen. Deze malwarefamilies zijn actief sinds midden 2024 en hebben wereldwijd slachtoffers gemaakt, waaronder in Rusland, Brazilië, Polen en andere landen.

Generative ai versnelt reverse engineering van xloader malware

XLoader, een complexe malwarefamilie, blijft een uitdaging voor analisten door de versnelde releases en geavanceerde encryptie- en obfuscatiemethoden. Dit artikel beschrijft hoe generatieve AI wordt ingezet om de reverse-engineering van XLoader te versnellen. Het traditionele proces van handmatige analyse en decryptie wordt aanzienlijk versneld door AI, die complexe functies analyseert, algoritmes identificeert en werkende tools genereert in enkele uren. Dit versnelt de toegang tot gedecrypteerde code en indicatoren van compromittering (IoC's). Check Point Research toonde aan hoe ChatGPT cloudgebaseerde statische analyses uitvoert zonder de noodzaak van zware lokale tools. De AI kan zowel statische als dynamische reverse-engineering effectief combineren, wat de efficiëntie en

samenwerking in onderzoek verbetert. Hoewel AI de efficiëntie verhoogt, blijft menselijke expertise noodzakelijk, vooral bij het oplossen van complexere beschermingsmechanismen van de malware.

Nieuwe Business Email Protection Blokkeert Phishing E-mail Achter NPM Inbraak

In september 2025 lanceerden cybercriminelen een gecoördineerde phishingaanval gericht op NPM-ontwikkelaars. De aanval infiltreerde de accounts van onder andere de bekende ontwikkelaar Josh Junon, bekend als “qix”, en richtte zich op vier andere onderhouders, wat de kwetsbaarheid van softwarerepositories blootlegde. Het slachtoffer van de aanval was goed voor 2,8 miljard wekelijkse downloads. De phishingmails, die zich voordeden als officiële communicatie van NPM, drukten ontwikkelaars aan om hun twee-factor-authenticatie bij te werken om accountopschorting te voorkomen. Deze e-mails, verstuurd vanaf een vervalst domein, wisten bij meerdere ontvangers het wantrouwen te omzeilen. Door de toegang tot de NPM-accounts konden de aanvallers schadelijke JavaScript-clipper malware toevoegen aan populaire pakketten, die cryptocurrency-overdrachten onderschepte en omleidde. De aanval werd gedetecteerd door een nieuw Business Email Protection-systeem, wat een belangrijke bescherming biedt tegen dergelijke aanvallen.

Nieuwe phishingcampagne maakt misbruik van Cloudflare en ZenDesk-pagina's om inloggegevens te stelen

Een geavanceerde phishingcampagne maakt misbruik van het vertrouwen dat in legitieme cloudhostingdiensten wordt gesteld. Cybercriminelen gebruiken Cloudflare Pages en ZenDesk-platforms om op grote schaal inloggegevens te stelen van nietsvermoedende gebruikers. De aanvallers hebben meer dan 600 malafide domeinen geregistreerd onder de *.pages[.]dev-domeinnaamstructuur. Ze passen typografische technieken toe om klantenportalen van bekende merken te imiteren. De phishingpagina's bevatten een live chat-interface waarmee menselijke operators persoonlijke gegevens van slachtoffers verzamelen. Na het verkrijgen van deze gegevens worden de slachtoffers gevraagd een legitiem maar kwaadaardig hulpmiddel te installeren, genaamd Rescue, waarmee aanvallers volledige toegang krijgen tot het apparaat van het slachtoffer. De aanvallers richten zich op

accountovername en fraude, wat deze campagne tot een aanzienlijke bedreiging maakt voor zowel bedrijven als individuen.

Nieuwe TruffleNet BEC-campagne misbruikt AWS SES met gestolen inloggegevens

TruffleNet, een nieuwe Business Email Compromise (BEC) campagne, maakt gebruik van gestolen AWS-credentials om de Amazon Simple Email Service (SES) te misbruiken voor grootschalige phishing- en BEC-aanvallen. De aanvallers benaderen meer dan 800 gecompromitteerde hosts verspreid over 57 netwerken. Dit stelt hen in staat om e-mails te verzenden die afkomstig lijken van legitieme bedrijven, zoals valse facturen met verzoeken om betaling. De aanvallers gebruiken gekaapte WordPress-websites om DKIM-sleutels te verkrijgen en AWS SES in te stellen voor e-mailidentiteit. Het netwerk is specifiek ontworpen voor deze aanval, zonder gebruik te maken van reguliere VPN's of Tor. Fortinet Labs ontdekte de infrastructuur en merkte op dat de aanvallers gebruik maakten van geavanceerde beveiligingsmaatregelen en automatisering om de aanval op grote schaal uit te voeren. De fraudeurs richtten zich onder andere op de olie- en gasindustrie, waarbij ze frauduleuze betalingsverzoeken verstuurden.

Rechter veroordeelt gebruiker phishingplatform LabHost tot 300 dagen cel

De rechtbank Midden-Nederland heeft een 37-jarige man veroordeeld voor zijn betrokkenheid bij het phishingplatform LabHost. Het platform werd gebruikt om phishingsites te creëren voor bank- en telecomfraude. De verdachte kreeg een gevangenisstraf van 300 dagen, waarvan 226 dagen voorwaardelijk. Het onderzoek toonde aan dat de verdachte gegevens op zijn laptop had, waaronder persoonsgegevens en bankinformatie van slachtoffers. Hij had tevens toegang tot 18 gigabyte aan zogenaamde leadlijsten, die gebruikt werden voor online oplichting zoals WhatsAppfraude en bankhelpdeskfraude. De rechtbank oordeelde dat de verdachte zich bijna een jaar had voorbereid op online fraude en hiermee daadwerkelijk fraude had gepleegd. Gezien de ernst van de feiten werd een langdurige straf gerechtvaardigd. De verdachte hoeft echter niet terug naar de gevangenis vanwege persoonlijke omstandigheden.

Drie ex-cybersecurity-experts aangeklaagd voor BlackCat ransomware-aanvallen in de VS

Drie voormalige medewerkers van cybersecuritybedrijven DigitalMint en Sygnia zijn aangeklaagd voor het hacken van netwerken van vijf Amerikaanse bedrijven in BlackCat (ALPHV) ransomware-aanvallen tussen mei en november 2023. De aangeklaagden, Kevin Tyler Martin, Ryan Clifford Goldberg en een nog onbekende mede-dader, worden beschuldigd van samenspanning, afpersing en schade aan beschermde computers. Martin werkte als ransomware-onderhandelaar bij DigitalMint, terwijl Goldberg incidentmanager was bij Sygnia. De aanvallers kregen ongeoorloofde toegang tot de netwerken van de slachtoffers, stalen gegevens, plaatsten encryptiemalware en eisten betalingen in cryptocurrency in ruil voor decryptiesleutels. De slachtoffers waren onder andere een medische apparatenfabrikant in Tampa en een farmaceutisch bedrijf in Maryland. Als ze worden veroordeeld, kunnen de verdachten tot 20 jaar gevangenisstraf krijgen voor afpersing.

Twee nepagenten aangehouden in Nieuw-Beijerland na oplichting

Op donderdag 30 oktober is een bewoner in Nieuw-Beijerland slachtoffer geworden van twee nepagenten. De oplichters belden de bewoner en gaven zich uit als politieagenten. Ze vertelden dat er later die avond een agent zou komen om sieraden en geld op te halen. Even later verscheen de nepagent aan de deur en nam de waardevolle spullen mee. Toen de bewoner twijfels kreeg, belde hij de politie. De echte agenten zagen een verdachte auto en hielden de twee verdachten aan. De buit werd teruggevonden. De aangehouden verdachten zijn een 21-jarige man uit Oud-Beijerland en een 25-jarige man uit Vlaardingen. De politie roept buurtbewoners op om verdachte telefoontjes ook te melden.

Oekraïense hacker MrICQ in Amerikaanse detentie

De Oekraïense hacker Yuriy Igorevich Rybtsov, alias MrICQ, is in de Verenigde Staten aangekomen na zijn arrestatie in Italië. Rybtsov was betrokken bij de cybercriminele groep Jabber Zeus, die zich richtte op het stelen van miljoenen dollars van bedrijven in de VS. De groep maakte gebruik van de Zeus-bankingtrojan om inloggegevens van banken te stelen en geld over te maken naar zogenaamde 'money mules'. Rybtsov wordt beschuldigd van het helpen van de groep bij het

witwassen van de gestolen bedragen via elektronische valuta-omwisseldiensten. Hij was een van de hoofdontwikkelaars van de Jabber Zeus-malware en werkte nauw samen met andere prominente cybercriminelen, waaronder de beruchte Maksim Yakubets. Rybtsov werd gevangen genomen nadat hij zijn laatste beroep tegen uitlevering aan de VS had verloren.

Ontdekking van cybercrimineel ‘303’: veel gezichten, één hacker

Een uitgebreide analyse onthult de identiteit van de cybercrimineel bekend als "303", die actief is onder verschillende aliassen en zich verspreidt over diverse hackingforums en Telegramkanalen. Sinds 2023 heeft deze hacker tientallen datalekken en netwerktoegangen geclaimd, met doelwitten in de VS, Japan, Taiwan, Brazilië en Argentinië. De actor gebruikte meerdere identiteiten en platforms, waaronder BreachForums, DarkForums en Exploit, om databases en toegangspunten te verkopen. Door herhaald gebruik van Telegram-accounts en e-mailadressen werd het mogelijk om de activiteiten van deze hacker te traceren. Het onderzoek wijst ook op een mogelijke band met Zuid-Amerika, specifiek Uruguay, gezien het gebruik van Spaanse gemeenschappen. Ondanks zijn frequente rebranding bleef er altijd een patroon van zelfpromotie en overdrijving, waarmee hij zichzelf als expert in de cybersecuritywereld presenteerde.

LinkedIn gebruikt data van Europese gebruikers voor AI-training

LinkedIn heeft aangekondigd te beginnen met het gebruiken van gegevens van Europese gebruikers voor het trainen van generatieve AI-modellen. Deze gegevens omvatten profielinformatie zoals naam, foto, huidige functie, werkervaring, opleiding, locatie en vaardigheden, evenals openbare content zoals posts, artikelen, reacties en polls. Privéberichten worden volgens LinkedIn niet gebruikt voor de training. Gebruikers kunnen zich via de instellingen afmelden voor het gebruik van nieuwe gegevens, maar de opt-out geldt niet voor eerder verstrekte informatie. De Autoriteit Persoonsgegevens heeft zijn bezorgdheid geuit over het verlies van controle over persoonlijke data zodra deze in de AI-systemen van LinkedIn wordt verwerkt. LinkedIn stelt dat het gebruik van deze gegevens noodzakelijk is voor het verbeteren van gebruikerservaringen, zoals het beter matchen van gebruikers met kansen en het helpen bij het creëren van content.

200 Zweedse gemeenten getroffen door datalek bij IT-leverancier Miljödata

De Zweedse privacytoezichthouder IMY is een onderzoek gestart naar een datalek bij de IT-leverancier Miljödata, dat 1,5 miljoen Zweden heeft getroffen. Het lek gebeurde na een ransomware-aanval die plaatsvond in augustus. Miljödata levert HR-systemen en is een belangrijke speler voor ruim tachtig procent van de Zweedse gemeenten en diverse bedrijven. Door de aanval hadden deze gemeenten geen toegang meer tot hun systemen. Naast het versleutelen van data werden ook persoonlijke gegevens gestolen en vervolgens op het darknet gepubliceerd, waaronder gevoelige informatie van veel Zweden. IMY onderzoekt nu of de beveiliging bij Miljödata onvoldoende was en wat er moet worden gedaan om soortgelijke incidenten in de toekomst te voorkomen. De onderzoekers hebben nog niet aangegeven wanneer het onderzoek zal worden afgerond.

Hacker steelt meer dan 120 miljoen dollar van Balancer DeFi-protocol

Balancer heeft bevestigd dat hackers zijn gericht op de v2-pools van het platform, waarbij de verliezen worden geschat op meer dan 128 miljoen dollar. Balancer is een gedecentraliseerd financieel (DeFi) protocol op de Ethereum-blockchain, dat fungeert als een automatische marktmaker en liquiditeitsinfrastructuur. Het platform biedt flexibele pools met op maat gemaakte tokenmixen voor gebruikers om activa te storten en handel te verrichten. De hack was het gevolg van een fout in de precisierondingen van de swap-berekeningen in de V2 Compostable Stable Pools. De aanvaller exploiteerde de kleine discrepanties die ontstonden bij elke swap en genereerde zo een aanzienlijke prijsverstoring. Ondanks eerdere audits van het protocol werden deze kwetsbaarheden niet gedetecteerd. De aanvallers zijn nog niet geïdentificeerd, maar DeFi-platforms blijven kwetsbaar voor aanvallen zoals deze.

Diefstal in het Louvre: beveiligingsfouten: het (voor de hand liggende) wachtwoord was “Louvre”

De recente diefstal van kunstwerken ter waarde van bijna €90 miljoen uit het Louvre is een blamage voor het museum. Het bleek dat de toegang tot de video-surveillance-server mogelijk was met het eenvoudige wachtwoord "LOUVRE", wat de zwakke beveiliging blootlegt. Vijf jaar geleden waarschuwde de Nationale Cyberbeveiligingsdienst al voor deze kwetsbaarheid. De dieven slaagden erin het museum in de Apollo Gallery binnen te dringen via een vrachtlift en vluchtten op een

motorfiets met de kroonjuwelen. Er wordt gespeculeerd dat de dieven geen geavanceerde criminelen zijn, maar eerder eenvoudige inbrekers zonder interne hulp. Vier verdachten zijn inmiddels gearresteerd, waaronder een stel uit La Courneuve, wiens DNA werd gevonden op de vrachtlift. De zoektocht naar de gestolen goederen en eventuele andere betrokkenen gaat door. De rol van de verdachten doet vermoeden dat deze diefstal mogelijk niet het werk is van georganiseerde misdaad.

Verkoop van Israël's Iron Dome-systeem geclaimd door actor met -30 reputatie

Op 2 november 2025 werd op het darkweb geclaimd dat het Israëlische Iron Dome-systeem te koop werd aangeboden door een actor die een negatieve reputatie van -30 heeft. Deze actor, actief op het darkweb, heeft eerder in de media aandacht getrokken door het delen van gevoelige informatie en gegevens die doorgaans geassocieerd worden met cybercriminaliteit. Het is echter niet duidelijk of deze bewering van de actor geloofwaardig is of dat het slechts een poging tot misleiding is. De aanbieding heeft veel reacties uitgelokt, waaronder discussies over de mogelijke implicaties van een dergelijke verkoop, als het al waar zou zijn. De kwestie roept zorgen op over de veiligheid van kritieke systemen en de rol van het darkweb bij de verspreiding van gevoelige militaire technologie.

Ernst & Young stelt 4TB SQL-database bloot op het open internet

Ernst & Young heeft een fout ontdekt die resulteerde in de blootstelling van meer dan 4 terabyte aan gegevens in een SQL-database. De gegevens waren toegankelijk via het open internet en bevatten gevoelige informatie, waaronder persoonlijke gegevens en bedrijfsinformatie. Deze ontdekking benadrukt de risico's van slecht geconfigureerde databases en de noodzaak voor strengere beveiligingsmaatregelen bij het beheren van vertrouwelijke gegevens. Er wordt momenteel onderzocht hoe lang de gegevens blootstonden en welke impact dit heeft gehad op betrokken organisaties. Het incident heeft geleid tot een bredere discussie over de kwetsbaarheden van cloud- en serveromgevingen, evenals de verplichting van bedrijven om goede beveiligingsprotocollen te volgen. Ernst & Young heeft stappen ondernomen om het probleem te verhelpen en de beveiliging te versterken, maar het incident blijft een belangrijk voorbeeld van de risico's van onvoldoende bescherming van bedrijfsdata.

Helft van Vlaamse jongeren slachtoffer van misdrijf: 'cyberflashing' meest voorkomend

Volgens een recent rapport van het Jeugdonderzoeksplatform (JOP) is de helft van de Vlaamse jongeren in het afgelopen jaar slachtoffer geworden van een misdrijf. Het meest voorkomende misdrijf is cyberflashing, waarbij seksueel getinte foto's ongewenst worden verstuurd. Ongeveer 1 op de 4 jongeren heeft hiermee te maken gehad, met variaties tussen steden: in Gent meldde 30% van de jongeren dit fenomeen, terwijl in Brussel 21% werd gerapporteerd. Naast cyberflashing werden jongeren ook vaak lastiggevallen op straat (16%) en slachtoffer van diefstal (16%). Het rapport toont aan dat jongeren uit grotere steden zoals Brussel en Gent vaker slachtoffer zijn van misdrijven dan hun leeftijdsgenoten in de rest van Vlaanderen. Opvallend is dat jongeren die slachtoffer werden, meestal geen hulp zochten, hoewel zij in de meeste gevallen steun bij familie of vrienden vonden.

Interview met AURA: De ontwikkeling van een nieuwe Infostealer

AURA is een relatief nieuwe speler op de markt van infostealers, met een groeiende gemeenschap van gebruikers. Het ontwikkelteam benadrukt de technische superioriteit en stabiliteit van hun product, met ervaren programmeurs die dagelijks nieuwe technologieën toepassen. De naam AURA is gekozen vanwege de associatie met succes, wat weerspiegeld wordt in hun logo. Hoewel AURA soms wordt vergeleken met Lumma, wordt dit ontkend door het team, die stelt dat de enige gelijkenis in de visuele aspecten ligt, door het gebruik van een gemeenschappelijk webtemplate. AURA richt zich op snelle groei, met een klantenbestand dat sneller toeneemt dan sommige concurrenten die al jaren actief zijn. Het product werkt niet in CIS-landen, wat bewust is geïmplementeerd als beveiligingsmaatregel. Het team heeft ambitieuze plannen om de leider in de markt te worden, ondanks de uitdagingen en concurrentie.