Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

12-11-2025:

Everest ransomwaregroep claimt aanval op AGFA

Op 10 november 2025 werd bekend dat de Belgische multinational AGFA het slachtoffer is geworden van een cyberaanval, geclaimd door de Everest ransomwaregroep. AGFA is actief in de ontwikkeling van analoge en digitale beeldsystemen, evenals IT-oplossingen voor onder andere de gezondheidszorg en de grafische industrie. De aanval werd gedetecteerd door Ransomware.live en vond plaats op dezelfde dag. De Everest ransomwaregroep, bekend om hun aanvallen op grote organisaties, heeft de verantwoordelijkheid voor de aanval opgeëist. Er is momenteel geen specifieke informatie over de aard van de gestolen data of de omvang van de schade. AGFA is een van de vele bedrijven die in 2025 getroffen zijn door een reeks ransomware-aanvallen, wat de risico's voor bedrijfsbeveiliging verder benadrukt.

EU beschermt media en verkiezingen tegen Russische hybride aanvallen

De Europese Unie werkt aan een pakket maatregelen om de media en verkiezingen te beschermen tegen buitenlandse inmenging, met name door Rusland. In een conceptdocument beschuldigt de EU Moskou ervan wantrouwen in democratische systemen te zaaien door desinformatie en vervalsing van historische feiten. Het document noemt als voorbeeld de Roemeense presidentsverkiezingen van november 2024, die werden geannuleerd na beschuldigingen van Russische inmenging. De EU wil de financiering van vrije media verhogen en fusies van nieuwsorganisaties beter monitoren om pluralisme te bevorderen. Ook wordt voorgesteld om een Europees centrum op te richten voor het coördineren van de bestrijding van buitenlandse inmenging. De commissie noemt verkiezingen nu als "kritieke infrastructuur" en benadrukt de groeiende dreiging van cyberaanvallen en kunstmatige intelligentie. Mediawaakhond Reporters Without Borders roept de EU op ambitieuze maatregelen te nemen om de zichtbaarheid van betrouwbare media te vergroten.

APT37-hackers misbruiken Google Find Hub voor Android-dataloos-aanvallen

Hackers van de Noord-Koreaanse groep APT37 maken misbruik van de Google Find Hub-tool om de GPS-locatie van hun slachtoffers te volgen en op afstand

fabrieksinstellingen van Android-apparaten te resetten. De aanvallen richten zich voornamelijk op Zuid-Koreanen en beginnen via de populaire berichtendienst KakaoTalk. De aanvallers gebruiken een kwaadaardig bestand dat zich voordoet als een stressverlichtingsprogramma en, zodra uitgevoerd, toegang biedt tot de slachtoffers' apparaten. Na infectie halen de hackers gevoelige gegevens uit Google- en Naver-accounts en gebruiken vervolgens Find Hub om Android-apparaten te wissen. Dit wordt gedaan om slachtoffers te isoleren, aanvalsporen te verwijderen en het herstel te vertragen. De slachtoffers verliezen toegang tot hun apparaten, terwijl de aanvallers hun KakaoTalk-account gebruiken om kwaadaardige bestanden naar de contacten van het slachtoffer te verspreiden. Het wordt aanbevolen om multi-factor-authenticatie in te schakelen om dergelijke aanvallen te voorkomen.

NoName en PalachPro kondigen nieuwe hacktivistenalliantie aan

De hacktivistische groeperingen NoName en PalachPro hebben aangekondigd samen te werken in een nieuwe alliantie. De samenwerking werd officieel bekendgemaakt op 11 november 2025 en markeert een belangrijke stap in de gezamenlijke activiteiten van deze twee groepen. Beide groeperingen zijn bekend om hun betrokkenheid bij cyberaanvallen die gericht zijn op het destabiliseren van overheden en bedrijven, met name door middel van DDoS-aanvallen en andere digitale verstoringen. De alliantie benadrukt de groeiende kracht van hacktivistische netwerken die invloed willen uitoefenen op politieke en maatschappelijke processen wereldwijd. Het is nog onduidelijk wat de concrete doelen van de nieuwe alliantie zijn, maar het wordt verwacht dat de groepen gezamenlijk nieuwe cyberaanvallen zullen uitvoeren.

NoName richt zich op meerdere Belgische websites met DDoS-aanvallen

De cybercriminelen van de groep NoName hebben meerdere websites in België aangevallen met gedistribueerde denial-of-service (DDoS) aanvallen. De getroffen websites behoren tot onder andere de stad Antwerpen, Proximus Group, de gemeente Waimes, de stad Bastogne, en verschillende andere gemeentelijke en bedrijfswebsites zoals C.P. Bourg en Telenet Group. De aanvallen zijn gericht op het verstoren van de toegang tot deze sites, wat mogelijk ernstige operationele verstoringen heeft veroorzaakt. NoName heeft de verantwoordelijkheid voor de aanvallen opgeëist. DDoS-aanvallen zijn een veelgebruikte tactiek van

cybercriminelen om systemen te overbelasten en offline te halen, wat leidt tot schade aan de infrastructuur van getroffen organisaties.

Russische regio Ulyanovsk schakelt mobiel internet uit tot einde van de oorlog

In de Russische regio Ulyanovsk is het mobiele internet permanent uitgeschakeld, een maatregel die van kracht blijft "tot het einde van de oorlog tegen Oekraïne". Lokale autoriteiten gaven aan dat de federale regering de beslissing had genomen en dat regionale functionarissen hier geen invloed op hadden. De internetblokkade geldt voor woonwijken, sociale instellingen en kantoren in de regio. Om de impact te verzachten, is een zogenaamde "witte lijst" geïntroduceerd, waarop goedgekeurde Russische websites, zoals staatsdiensten en social media platforms, toegankelijk blijven. Ondanks deze maatregelen blijft het voor veel inwoners moeilijk om verbonden te blijven, vooral voor diegenen die afhankelijk zijn van mobiel internet. De beslissing maakt deel uit van bredere federale veiligheidsmaatregelen die de communicatie in gebieden nabij strategische objecten moeten beschermen.

Kan het VK het Israëlische model voor cyberverdediging volgen?

Leiders in de Britse cybersecurity roepen de regering op om het startup-gedreven model van Israël te volgen en Britse cybersecurity-bedrijven te steunen in plaats van afhankelijk te blijven van grote Amerikaanse techbedrijven. In een open brief aan de Britse regering wordt gepleit voor meer overheidssteun om een onafhankelijk cyber-ecosysteem op te bouwen dat vergelijkbaar is met dat van Israël. Het voorstel benadrukt het belang van het aankopen van technologie van opkomende Britse startups en het invoeren van belastingvoordelen voor organisaties die Britse cybersecuritytools testen. Daarnaast wordt er gepleit voor de oprichting van een Britse versie van Israël's elite cybereenheid, Unit 8200, die als motor fungeert voor het succes van veel technologiebedrijven. Deze oproep is een reactie op eerdere gesprekken tussen investeerders, oprichters en overheidspersoneel, die zich zorgen maken over de beperkte samenwerking tussen de overheid en startups.

Kritieke kwetsbaarheid in Samsung Galaxy-smartphones toegevoegd aan KEV-database

CISA heeft een kritieke kwetsbaarheid (CVE-2025-21042) in Samsung Galaxy-smartphones toegevoegd aan de Known Exploited Vulnerabilities (KEV)-database. De kwetsbaarheid betreft een library voor afbeeldingsverwerking, die aanvallers in staat stelt willekeurige code uit te voeren op kwetsbare apparaten. Deze kwetsbaarheid kan via geprepareerde DNG-afbeeldingen via WhatsApp worden verspreid en maakt het mogelijk dat de Landfall-spyware op de smartphone wordt geïnstalleerd. Het lek werd in september 2024 aan Samsung gemeld en in april 2025 gedicht. Desondanks wordt het sinds medio 2024 actief misbruikt. De KEV-database helpt organisaties bij het prioriteren van noodzakelijke patches door kwetsbaarheden die actief worden misbruikt te markeren. CISA adviseert gebruikers om updates te installeren om zich tegen deze bedreiging te beschermen.

Hackers misbruiken Triofox-kwetsbaarheid om toegangstools te installeren via antivirusfunctie

Hackers hebben een kwetsbaarheid in Triofox, een platform voor bestandsdeling en externe toegang, misbruikt om op systemen kwaadaardige toegangstools te installeren. De kwetsbaarheid, CVE-2025-12480, stelde aanvallers in staat om authenticatie te omzeilen en toegang te krijgen tot de configuratiepagina's van het platform. Via deze toegang konden zij een nieuwe beheerder aanmaken, die vervolgens werd gebruikt om kwaadaardige bestanden te uploaden en uit te voeren. Deze bestanden werden gedownload via de ingebouwde antivirusfunctie van Triofox, die door de aanvallers werd geconfigureerd om scripts uit te voeren. De gecompromitteerde systemen werden gebruikt voor verdere verkenning en het escaleren van privileges door gebruikerswachtwoorden te wijzigen. Gebruikers van Triofox wordt aangeraden hun systemen te updaten naar de laatste versie en de antivirusinstellingen te controleren om ongeautoriseerde scripts te voorkomen.

SAP verhelpt kritieke kwetsbaarheden in SQL Anywhere Monitor en Solution Manager

SAP heeft zijn november 2025 beveiligingsupdates uitgebracht, waarin meerdere kwetsbaarheden worden aangepakt. Een van de belangrijkste kwetsbaarheden betreft hardcoded inloggegevens in de niet-GUI versie van de SQL Anywhere Monitor, aangeduid als CVE-2025-42890. Deze kwetsbaarheid heeft de hoogste ernstscore van 10,0 en kan aanvallers in staat stellen om willekeurige code uit te

voeren door toegang te krijgen tot beheerdersfunctionaliteiten. Daarnaast is er een kritieke code-injectiekwetsbaarheid in de SAP Solution Manager (CVE-2025-42887), die de integriteit van het systeem in gevaar kan brengen. Beide kwetsbaarheden kunnen leiden tot volledige controle over de getroffen systemen. SAP adviseert gebruikers om de updates zo snel mogelijk toe te passen om deze risico's te mitigeren. De updates verhelpen ook andere kwetsbaarheden met een lagere ernstscore.

Microsoft Patch Tuesday verhelpt 1 zero-day en 63 kwetsbaarheden

Op de Patch Tuesday van november 2025 heeft Microsoft een reeks beveiligingsupdates uitgebracht voor 63 kwetsbaarheden, waaronder een actief misbruikte zero-day in de Windows Kernel. Deze kwetsbaarheid, CVE-2025-62215, maakt het mogelijk voor aanvallers om systeemprivileges te verkrijgen via een race-conditie in de kernel. Naast deze zero-day zijn er vier andere ernstige kwetsbaarheden verholpen, waaronder twee voor remote code execution, één voor privilege escalation, en één voor informatielekken. In totaal betreft het 29 privilege-escalatie kwetsbaarheden, 16 voor remote code execution, en diverse andere, waaronder beveiligingsomzeilingen en denial of service. Gebruikers van Windows 10 wordt geadviseerd om over te stappen naar Windows 11 of het Extended Security Update-programma te volgen, aangezien de ondersteuning voor Windows 10 afloopt. Deze maand is ook de eerste ESU-update voor Windows 10 uitgerold.

Microsoft brengt cumulatieve updates voor Windows 11 uit

Microsoft heeft op 11 november 2025 de cumulatieve updates KB5068861 en KB5068865 uitgebracht voor Windows 11 versies 25H2, 24H2 en 23H2. Deze updates richten zich op de oplossing van beveiligingskwetsbaarheden, bugfixes en de toevoeging van nieuwe functies. De updates zijn verplicht, aangezien ze de Patch Tuesday-beveiligingspatches voor november 2025 bevatten, die kwetsbaarheden verhelpen die eerder dit jaar werden ontdekt. De belangrijkste wijzigingen omvatten een vernieuwde startmenu-interface, verbeterde batterij-indicatoren op het vergrendelingsscherm en nieuwe instellingen voor Microsoft 365 Copilot voor commerciële apparaten. Verder zijn er diverse bugfixes doorgevoerd voor onder andere de taakbalk, bestandsverkenner en instellingen. Microsoft heeft aangegeven dat dit de laatste update is voor versie 23H2, aangezien de ondersteuning voor deze

versie nu eindigt. Er zullen geen optionele updates in december worden uitgebracht, maar de Patch Tuesday-updates gaan zoals gepland door.

Microsoft brengt update KB5068781 uit voor Windows 10 Extended Security Update

Microsoft heeft de KB5068781-update uitgebracht, de eerste Extended Security Update (ESU) voor Windows 10, nadat de ondersteuning voor dit besturingssysteem vorige maand eindigde. Deze update is beschikbaar voor zowel consumenten als zakelijke klanten die zich hebben aangemeld voor de ESU, wat hen tot drie jaar lang toegang biedt tot beveiligingsupdates. De update verhelpt een foutmelding die ten onrechte aangeeft dat Windows 10 LTSC-apparaten de ondersteuning hebben bereikt, terwijl deze in werkelijkheid doorloopt tot januari 2027. De update bevat ook de maandelijkse Patch Tuesday-beveiligingspatches, die 63 kwetsbaarheden aanpakken, inclusief één voor een actief misbruikte escalatie-van-privilegeskwetsbaarheid. Dit is een verplichte update, die automatisch wordt geïnstalleerd en gebruikers vraagt hun apparaat opnieuw op te starten na de installatie.

Synology verhelpt kritieke kwetsbaarheid in BeeStation na Pwn2Own-demonstratie

Synology heeft een kritieke kwetsbaarheid verholpen in zijn BeeStation-producten, die werd gedemonstreerd tijdens de Pwn2Own hackingwedstrijd in Ierland. De kwetsbaarheid (CVE-2025-12686) betreft een probleem waarbij de grootte van de invoer niet wordt gecontroleerd, wat kan leiden tot remote code execution (RCE). Deze kwetsbaarheid beïnvloedt meerdere versies van BeeStation OS, dat wordt gebruikt in Synology’s netwerkopslagapparaten, welke bedoeld zijn voor consumenten als "persoonlijke cloud". De kwetsbaarheid werd door onderzoekers van Synacktiv, Tek en anyfun, met succes uitgebuit tijdens de wedstrijd, waarvoor ze een beloning van $40.000 ontvingen. Synology raadt gebruikers aan om BeeStation OS bij te werken naar versie 1.3.2-65648 of hoger om de kwetsbaarheid te verhelpen.

Zoom Workplace VDI Client voor Windows kwetsbaar voor privilege escalation

Een beveiligingsfout is ontdekt in de Zoom Workplace VDI Client voor Windows, waardoor aanvallers de mogelijkheid krijgen om hun privileges op kwetsbare

systemen te verhogen. De kwetsbaarheid, gemarkeerd als CVE-2025-64740, heeft een hoge ernst met een CVSS-score van 7,5. Deze zwakte wordt veroorzaakt door onjuiste verificatie van cryptografische handtekeningen in de installatie van de Zoom-software. Wanneer misbruikt, kan een aanvaller met lokale toegang hogere beheerdersrechten verkrijgen, wat kan leiden tot ongeautoriseerde commando's, toegang tot gevoelige gegevens of het compromitteren van de systeembetrouwbaarheid. De fout komt voor in versies van de Zoom Workplace VDI Client vóór 6.3.14, 6.4.12 en 6.5.10. Hoewel de kwetsbaarheid enige interactie van de gebruiker vereist, blijft de impact significant, vooral in bedrijfsomgevingen waar Zoom veel gebruikt wordt. Zoom heeft updates uitgebracht om het probleem te verhelpen en beveelt aan dat gebruikers zo snel mogelijk upgraden.

Phishingplatform Quantum Route Redirect misbruikt 1.000 domeinen

Een nieuw phishingplatform, Quantum Route Redirect, wordt wereldwijd ingezet om inloggegevens van Microsoft 365 gebruikers buit te maken. Het systeem maakt gebruik van ongeveer duizend domeinen die vooraf zijn ingericht om snel grootschalige campagnes te starten. Onderzoekers zien dat aanvallen beginnen met overtuigend ogende e-mails die bijvoorbeeld lijken op DocuSign meldingen, betalingsverzoeken of gemiste berichten. Slachtoffers worden doorgestuurd naar een pagina waar hun gegevens worden onderschept, terwijl het platform geautomatiseerde beveiligingstools juist naar onschuldige sites leidt. Deze aanpak maakt gebruik van gecompromitteerde of geparkeerde domeinen, wat de betrouwbaarheid voor slachtoffers vergroot. Het platform biedt aanvallers dashboards om verkeer te volgen en onderscheid te maken tussen echte bezoekers en bots. De meeste activiteiten zijn gericht op gebruikers in de Verenigde Staten, maar het platform is actief in negentig landen. Analisten verwachten een verdere toename door de effectieve omzeiling van URL-scans.

Valse sms-berichten namens banken en Bitvavo

Er zijn meldingen van valse sms-berichten die zogenaamd van banken of Bitvavo afkomstig zijn. In deze berichten wordt aangegeven dat er een inlogpoging is gedaan vanuit het buitenland. Ontvangers worden gevraagd een telefoonnummer te bellen als zij zelf geen inlogpoging hebben gedaan. Bij contact via dit nummer wordt een zogenaamde medewerker geïnformeerd, die de ontvanger vertelt dat hij of zij moet

helpen het saldo te beveiligen. Dit kan door software te downloaden of inlogcodes te verstrekken. In werkelijkheid wordt het saldo gestolen. De afzender lijkt de echte nummer van Bitvavo te gebruiken, maar dit is een geval van spoofing. Het advies is om niet naar het opgegeven nummer te bellen en het bericht te verwijderen.

Kwaadwillig npm-pakket gericht op GitHub-repositories ontdekt

Onderzoekers hebben een kwaadaardig npm-pakket met de naam "@acitons/artifact" ontdekt, dat lijkt op het legitieme pakket "@actions/artifact" en gericht is op repositories van GitHub. Het pakket bevat een post-installatiescript dat tokens uit de buildomgeving van GitHub-repositories probeert te stelen. Deze tokens zouden vervolgens gebruikt kunnen worden om nieuwe schadelijke bestanden te publiceren als GitHub. Het kwaadaardige pakket werd gedownload via zes versies tussen 4.0.12 en 4.0.17 en is sinds de ontdekking verwijderd. Het pakket werd in totaal 47.405 keer gedownload. Een andere npm-pakket, "8jfiesaf83", werd ook geïdentificeerd, maar is inmiddels verwijderd, na 1.016 downloads. Het malware-script is ontworpen om gegevens in een versleuteld bestand te exfiltreren naar een specifieke GitHub-onderdomein. Deze campagne lijkt gericht te zijn op GitHub zelf en mogelijk een testaccount.

AI-gedreven supply chain aanvallen nemen 156% toe

AI-aangedreven aanvallen op software-supply chains zijn de afgelopen tijd exponentieel gestegen, met een toename van 156% in het afgelopen jaar. Traditionele beveiligingsmaatregelen blijken steeds minder effectief tegen de nieuwe, meer geavanceerde dreigingen, waarbij aanvallers gebruik maken van AI-gegenereerde malware die polymorfisch, contextbewust en semantisch gecamoufleerd is. Hierdoor is het steeds moeilijker voor detectietools om deze aanvallen op te sporen. Malafide uploads van softwarepakketten naar open-source repositories hebben geleid tot ernstige incidenten, zoals de 3CX-inbraak die 600.000 bedrijven wereldwijd trof. AI-malware kan nu zelfstandig zijn code aanpassen om traditionele beveiligingsmechanismen te omzeilen, wat resulteert in aanzienlijk langere detectietijden. Experts adviseren bedrijven om AI-bewuste beveiligingsmaatregelen te implementeren, zoals gedragsanalyse en runtime bescherming, en zich voor te bereiden op strengere regelgeving zoals de EU AI-wetgeving, die hoge boetes kan opleggen voor ernstige inbreuken.

Bedreigingsactoren maken gebruik van RMM-tools voor het verspreiden van Medusa- en DragonForce-ransomware

In 2025 werd een nieuwe golf van ransomware-aanvallen gemeld, gericht op Britse organisaties, waarbij gebruik werd gemaakt van kwetsbaarheden in de SimpleHelp Remote Monitoring and Management (RMM)-platforms. Twee bekende ransomware-groepen, Medusa en DragonForce, exploiteerden drie ernstige kwetsbaarheden (CVE-2024-57726, CVE-2024-57727, CVE-2024-57728) om via vertrouwde derde partijen toegang te krijgen tot systemen. In plaats van direct te richten op organisaties, richtten de aanvallers zich op de RMM-infrastructuur van leveranciers, waardoor ze door de toegenomen vertrouwensbanden toegang kregen tot de netwerken van klanten. Beide groepen gebruikten geavanceerde technieken om de beveiliging van de systemen te omzeilen, waaronder het uitschakelen van Microsoft Defender en het verkrijgen van toegang via remote management-tools. De aanvallen resulteerden in ernstige verstoringen, versleuteling van gegevens en de dreiging van gegevensdiefstal op darkweb-leksites.

Bedreigingen gericht op Outlook en Google: aanvallen ompasseren traditionele e-mailbeveiliging

Cybercriminelen richten zich steeds vaker op Outlook en Google, de twee grootste e-mailplatforms ter wereld, waarbij ze traditionele beveiligingslagen omzeilen. Uit het Q3-rapport over e-maildreigingen blijkt dat meer dan 90% van de phishingaanvallen nu op deze platforms is gericht. De onderzoekers van VIPRE hebben 1,8 miljard e-mails geanalyseerd en ontdekten 26 miljoen extra kwaadaardige berichten, een toename van 13% ten opzichte van vorig jaar. Aanvallers maken niet alleen gebruik van geavanceerde malware, maar ook van eenvoudige methoden zoals vervalste loginpagina's en misbruik van vertrouwde links. Dit maakt het voor zowel automatische systemen als menselijke operators steeds moeilijker om legitieme berichten van kwaadaardige te onderscheiden. De aanvallen zijn voornamelijk gericht op het stelen van inloggegevens en het overnemen van e-mailaccounts, wat leidt tot toegang tot netwerken en cloudservices van bedrijven.

Nieuwe VanHelsing ransomware RaaS-aanval op Windows, Linux, BSD, ARM en ESXi systemen

De VanHelsing ransomware is een nieuwe, geavanceerde ransomware-as-a-service (RaaS) operatie die sinds maart 2025 actief is. Deze ransomware biedt criminelen een platform om snel aanvallen te lanceren op verschillende besturingssystemen, waaronder Windows, Linux, BSD, ARM en ESXi, waarmee de potentiële slachtoffers drastisch zijn vergroot. Nieuwe affiliates betalen $5.000 om deel te nemen, waarbij ze 80% van de losgeldbetalingen ontvangen. Dit model vergroot de schaalbaarheid van aanvallen. De ransomware is ontworpen met veel technische flexibiliteit, zoals een uitgebreid systeem voor het aanpassen van aanvallen en de mogelijkheid om laterale bewegingen door netwerken uit te voeren. VanHelsing is nog in ontwikkeling, met regelmatige updates die de effectiviteit vergroten. Het model heeft al geresulteerd in meerdere succesvolle aanvallen, waarbij losgeldbedragen tot $500.000 werden geëist. De operaties lijken bovendien geografische beperkingen te hanteren, met uitzondering van landen binnen de Gemenebest van Onafhankelijke Staten (CIS).

Onderzoek onthult sterke verbanden tussen Maverick- en Coyote-bankingmalware

Onderzoekers van CyberProof hebben sterke connecties ontdekt tussen de Maverick- en Coyote-bankingtrojan, die beide gericht zijn op Braziliaanse gebruikers en financiële instellingen. Beide malwarefamilies maken gebruik van vergelijkbare infectieketens en vertonen bijna identieke gedragingen. De aanvallen beginnen wanneer slachtoffers ZIP-bestanden via WhatsApp ontvangen, die kwaadaardige snelkoppelingbestanden bevatten. Deze bestanden starten PowerShell-commando’s die obfusceren en bedoeld zijn om detectie te vermijden. De malware gebruikt complexe coderingsmethoden zoals Base64 en UTF-16LE om de kwaadaardige commando's te reconstrueren en contact te maken met de infrastructuur van de aanvaller voor verdere infectie. Daarnaast gebruiken beide malwaretypes dezelfde versleuteling om de URL's van banken te decrypten en monitoren ze activiteiten in verschillende browsers. De overeenkomsten tussen deze malwarefamilies wijzen op een gedeelde ontwikkelingsbron.

Phishing via beveiligingsalerts steelt inloggegevens

Er is een nieuwe golf van phishing-aanvallen die zich voordoen als beveiligingsmeldingen. Deze kwaadaardige e-mails lijken afkomstig te zijn van de eigen domeinen van slachtoffers en waarschuwen voor vermeende "geblokkeerde berichten." De aanvallers proberen gebruikers in paniek te brengen en hen te

dwingen op een link te klikken om het probleem op te lossen. Zodra een slachtoffer op de link klikt, wordt het doorverwezen naar een valse inlogpagina die lijkt op legitieme webmailportalen. Deze pagina is zelfs al ingevuld met het e-mailadres van het slachtoffer, wat de echtheid versterkt. De aanvallers gebruiken JavaScript in de e-mailbijlagen om inloggegevens te verzamelen, die vervolgens naar een server van de aanvallers worden gestuurd. Deze campagne maakt gebruik van psychologische manipulatie en technische verfijning om gebruikers te misleiden, wat het belang van goede beveiligingsmaatregelen en waakzaamheid onderstreept.

Politie pakt drie nepagenten op in Hardenberg en Dedemsvaart

Op dinsdag 11 november heeft de politie drie personen aangehouden op verdenking van oplichting door zich voor te doen als agenten. De verdachten werden geïdentificeerd na meerdere meldingen in Hardenberg en Dedemsvaart, waar nepagenten probeerden inwoners op te lichten. De oplichters gebruikten een smoes dat er criminelen in de buurt waren, waarna ze een afspraak wilden maken om waardevolle spullen op te halen. Eén van de verdachten werd op 23 juni al verdacht, maar pas deze week konden de 21-jarige en 17-jarige mannen uit Amsterdam en Almere worden gearresteerd. Daarnaast werd een 22-jarige man uit Amsterdam aangehouden die verdacht wordt van het organiseren van de oplichtingspraktijken. De politie adviseert mensen om altijd 112 te bellen als ze vermoeden dat ze met een nepagent te maken hebben.

Criminelen gearresteerd voor produceren apparaten om auto's te ontgrendelen

Vijf verdachten zijn gearresteerd tijdens een internationale operatie gericht op een netwerk van autodieven. De groep produceerde aangepaste luidsprekers en andere technische apparaten waarmee auto's met gedecodeerde sleutels konden worden ontgrendeld, waardoor de beveiligingssystemen werden omzeild. De operatie werd gecoördineerd door Eurojust en uitgevoerd door Franse en Italiaanse onderzoekers. De hoofdverdachte, die sinds 2022 deze apparaten vervaardigde, verkocht ze wereldwijd via versleutelde berichtenservices voor prijzen tussen de 3.000 en 50.000 euro. De apparaten konden op verschillende bekende automerken, waaronder luxe voertuigen, worden gebruikt. In Frankrijk leidde een stijging van autodiefstallen tot de ontdekking van de apparaten. In totaal werden in Frankrijk zes voertuigen, meer dan

100.000 euro en gestolen apparatuur met een geschatte marktwaarde van 1 miljoen euro in beslag genomen.

"Bitcoin Queen" krijgt 11 jaar cel voor $7,3 miljard Bitcoin-oplichting

Zhimin Qian, een Chinese vrouw bekend als de "Bitcoin Queen", is in Londen veroordeeld tot 11 jaar en 8 maanden gevangenisstraf voor het witwassen van Bitcoin afkomstig van een oplichtingsschema ter waarde van £5,5 miljard ($7,3 miljard). Tussen 2014 en 2017 leidde Qian een fraude-operatie die meer dan 128.000 slachtoffers in China misleidde met beloften van hoge rendementen. Na de ineenstorting van haar plan in 2017, bewaarde ze de opbrengsten in Bitcoin en vluchtte naar het Verenigd Koninkrijk. Daar probeerde ze de cryptocurrency te witwassen via vastgoedtransacties. De Britse autoriteiten confisqueerden 61.000 Bitcoin, wat de grootste inbeslagname van cryptocurrency in het Verenigd Koninkrijk is. Qian werd samen met een andere verdachte in 2024 gearresteerd, waarna ook andere criminelen werden veroordeeld. Dit was mogelijk door intensieve samenwerking met internationale wetshandhavers.

Rhadamanthys infostealer verstoord door verlies servertoegang

De Rhadamanthys infostealer-operatie is verstoord doordat meerdere gebruikers van deze malware-as-a-service melden dat zij geen toegang meer hebben tot hun servers. Rhadamanthys is een infostealer die inloggegevens en authenticatiecookies steelt van browsers en e-mailclients, en wordt verspreid via campagnes die zich voordoen als software cracks of via malafide advertenties. De malware wordt aangeboden op abonnementsbasis, waarbij cybercriminelen maandelijks betalen voor toegang tot het malwarepakket, ondersteuning en een webpaneel voor het verzamelen van gestolen data. Het lijkt erop dat wetshandhavers, vermoedelijk uit Duitsland, toegang hebben gekregen tot de webpanelen van de cybercriminelen, wat leidde tot het verlies van servertoegang. De Tor-websites van de operatie zijn offline gehaald, maar het is nog onduidelijk welke autoriteiten achter deze verstoring zitten. Dit incident wordt mogelijk gerelateerd aan de lopende wetshandhavingsoperatie "Operation Endgame."

Duizenden gokten via Polymarket op verkiezingen: 'Gevaarlijk en illegaal'

Ondernemer Alexander Klöpping onthulde dat hij 8.000 euro won door via het Amerikaanse platform Polymarket te gokken op de uitkomst van de Nederlandse Tweede Kamerverkiezingen. Dit platform, waar gebruikers inzetten op allerlei gebeurtenissen, waaronder politieke verkiezingen, wordt in Nederland als illegaal beschouwd, aangezien het geen vergunning heeft van de Kansspelautoriteit. Klöpping was niet de enige; op Polymarket werd in totaal bijna 33 miljoen dollar ingezet op de verkiezingen. Desondanks omschrijft Polymarket zichzelf als een "voorspellingsplatform" en niet als een gokbedrijf, wat de juridische handhaving bemoeilijkt. Experts, zoals Tony van Rooij van het Trimbos-instituut, maken zich zorgen over de impact van dit platform en de normalisatie van gokken op politiek, wat volgens hen niet zonder risico is, aangezien dergelijke praktijken wettelijk verboden zijn.

Bierleveringen Asahi ernstig verstoord door cyberaanval

Asahi Group Holdings kampt nog steeds met de gevolgen van een ransomware-aanval die een maand geleden zijn interne systemen platlegde. Hierdoor is het bedrijf genoodzaakt bestellingen en leveringen handmatig af te handelen, wat heeft geleid tot een drastische daling van de leveringen, die momenteel slechts 10% van het normale niveau vertegenwoordigen. Dit komt op een ongunstig moment, aangezien december traditioneel de drukste maand voor Asahi is, met een hoge vraag naar bier en geschenkpakketten. Concurrenten zoals Kirin, Suntory en Sapporo profiteren van de verstoring door Asahi’s marktaandeel over te nemen, wat mogelijk langdurige gevolgen heeft voor het herstel van het bedrijf. Bovendien heeft Asahi de publicatie van zijn kwartaalcijfers uitgesteld vanwege de vertragingen in de afwikkeling van transacties en de problemen met het toegankelijk maken van financiële gegevens.

AP waarschuwt meer dan 200 websites over onjuiste cookiebanners

De Autoriteit Persoonsgegevens (AP) heeft meer dan tweehonderd Nederlandse websites gewaarschuwd vanwege misleidende of onjuiste cookiebanners. Ongeveer driekwart van deze websites heeft inmiddels de banner aangepast om te voldoen aan de regels. De overige partijen zullen handhavingsmaatregelen ondergaan. Sinds april 2025 controleert de AP of websites op de juiste manier toestemming vragen voor trackingcookies. Deze cookies mogen alleen worden geplaatst als bezoekers daar vrijwillig en op basis van heldere informatie mee instemmen. Trackingcookies

kunnen namelijk gedrag volgen, profielen opbouwen en voorspellende analyses uitvoeren. Monique Verdier, vicevoorzitter van de AP, benadrukt dat de waarschuwingen gericht zijn op het verbeteren van de cookiebanners, maar dat boetes mogelijk zijn voor degenen die na de waarschuwing geen aanpassingen doorvoeren.