Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

23-10-2025:

PhantomCaptcha ClickFix-aanval richt zich op oorlogshulporganisaties in Oekraïne

Op 8 oktober 2025 werd een gerichte spearphishingaanval uitgevoerd tegen leden van de Oekraïense regionale overheidsadministratie en organisaties die cruciaal zijn voor de oorlogshulp in Oekraïne, waaronder het Internationale Rode Kruis, UNICEF en verschillende NGO's. De aanval, genaamd PhantomCaptcha, gebruikte valse Cloudflare CAPTCHA-verificaties om slachtoffers te misleiden en hen te dwingen een PowerShell-opdracht uit te voeren, wat resulteerde in de installatie van een WebSocket Remote Access Trojan (RAT). Deze malware stelt aanvallers in staat om op afstand commando's uit te voeren en gegevens te exfiltreren. De aanvallen waren beperkt tot één dag, maar de gebruikte infrastructuur was al sinds maart 2025 in voorbereiding. De onderzoekers vermoeden dat de aanvallen mogelijk in verband staan met Russische actoren.

Cavalry Werewolf APT-hackers richten zich op meerdere industrieën met FoalShell en StallionRAT

Tussen mei en augustus 2025 werd een gerichte dreigingscampagne waargenomen waarbij de Cavalry Werewolf APT-groep, ook bekend als YoroTrooper en Silent Lynx, verschillende vitale sectoren in Rusland aanvalt. De groep maakt gebruik van op maat gemaakte malware, zoals FoalShell en StallionRAT, via phishing-aanvallen die officiële correspondentie van de overheid nabootsen. De aanvallen richten zich voornamelijk op de energie-, mijnbouw- en productiesectoren. De malware is ontworpen voor langdurige toegang en uitvoering van commando's op geïnfecteerde systemen. De gebruikte phishing-e-mails, vermomd als communicatie van de Kyrgyzse overheid, bevatten schadelijke RAR-archieven die de malware bevatten. Deze aanvallen zijn bijzonder verfijnd en maken gebruik van verschillende programmeertalen om detectie te omzeilen, wat de dreiging vergroot. Er zijn aanwijzingen dat de groep zich mogelijk richt op andere regio's, waaronder Tajikistan en het Midden-Oosten.

Oracle brengt kritieke beveiligingsupdates uit voor producten

Oracle heeft voor verschillende producten kritieke beveiligingsupdates uitgebracht en roept klanten op om deze onmiddellijk te installeren. De updates richten zich op

producten zoals Oracle E-Business Suite, Oracle GoldenGate, en Oracle Siebel CRM, waarbij kwetsbaarheden zijn verholpen die als ernstig worden beoordeeld (CVSS-score 9.8). De kwetsbaarheden kunnen door ongeauthenticeerde aanvallers op afstand misbruikt worden, met als mogelijk gevolg een volledig gecompromitteerd systeem. Tijdens de oktober-patchronde zijn in totaal 374 beveiligingsupdates uitgebracht, maar niet alle kwetsbaarheden zijn uniek voor een specifiek product. Oracle benadrukt dat er meldingen zijn van aanvallen die gebruik maken van kwetsbaarheden waarvoor al beveiligingsupdates beschikbaar waren. Klanten wordt dan ook dringend aangeraden om de nieuwste patches direct toe te passen.

Hackers exploiteren 34 zero-days op de eerste dag van Pwn2Own Ierland

Tijdens de eerste dag van Pwn2Own Ierland 2025 wisten beveiligingsonderzoekers 34 unieke zero-day kwetsbaarheden te exploiteren, goed voor $522.500 aan prijzengeld. Het hoogtepunt was het hacken van de QNAP Qhora-322 Ethernet-router door het team DDOS, die acht zero-day kwetsbaarheden in een keten gebruikten om toegang te krijgen tot een QNAP TS-453E NAS-apparaat, wat hen $100.000 opleverde. Daarnaast ontvingen verschillende andere teams $40.000 tot $50.000 voor het verkrijgen van root-toegang op apparaten zoals de Synology DiskStation en Canon-printers. Het evenement, georganiseerd door de Zero Day Initiative (ZDI), heeft als doel kwetsbaarheden in apparaten te identificeren voordat kwaadwillende actoren ze kunnen uitbuiten. Na de exploitatie krijgen leveranciers 90 dagen om beveiligingsupdates uit te brengen.

Cursor en Windsurf IDE's kwetsbaar door 94+ n-day Chromium kwetsbaarheden

De nieuwste versies van de geïntegreerde ontwikkelomgevingen (IDE's) Cursor en Windsurf zijn kwetsbaar voor meer dan 94 bekende en gepatchte beveiligingsproblemen in de Chromium-browser en de V8 JavaScript-engine. Ongeveer 1,8 miljoen ontwikkelaars lopen risico door het gebruik van verouderde versies van Chromium en V8, die zijn ingebed in de Electron-runtime die door beide IDE's wordt gebruikt. Deze IDE's zijn gebouwd op oudere versies van de Electron-frameworks, wat hen blootstelt aan beveiligingslekken die al zijn opgelost in nieuwere versies van Chromium. Ondanks een verantwoorde openbaarmaking van het probleem op 12 oktober, blijven de risico's bestaan, aangezien Cursor het rapport als "uit de scope" beschouwt en Windsurf niet heeft gereageerd. Ox Security

demonstreerde hoe de kwetsbaarheden kunnen worden misbruikt, waaronder de mogelijkheid tot een denial-of-service-aanval of zelfs arbitraire code-executie.

Python exploit voor Ivanti Connect Secure ontdekt

Er is een Proof of Concept (PoC) scanner gepubliceerd die kwetsbaarheden in Ivanti Connect Secure detecteert, met de CVE-2025-22457. Deze exploit kan een Remote Code Execution (RCE) aanval uitvoeren, wat het mogelijk maakt voor aanvallers om externe code op het getroffen systeem uit te voeren. De kwetsbaarheid heeft een hoge ernst, met een CVSS-score van 9,0. De PoC is beschikbaar op GitHub en wordt ook besproken op de Redline Cybersecurity-blog. De exploit is opgenomen in de Known Exploited Vulnerabilities (KEV) lijst, wat betekent dat er een verhoogd risico is dat deze kwetsbaarheid actief wordt misbruikt. Het is van groot belang dat bedrijven die Ivanti Connect Secure gebruiken de benodigde patches installeren om de beveiliging van hun systemen te waarborgen.

Kritieke kwetsbaarheid in Squid onthult referenties en beveiligingstokens – onmiddellijk patchen

Er is een kritieke kwetsbaarheid ontdekt in Squid-versies voor 7.2, die informatie over HTTP-authenticatie referenties kan lekken door een fout in de foutafhandelingssystemen. Deze kwetsbaarheid maakt het mogelijk voor aanvallers om gebruikersreferenties en beveiligingstokens te verkrijgen die door vertrouwde clients worden gebruikt voor authenticatie. Dit kan gebeuren zonder dat Squid HTTP-authenticatie vereist, wat het risico vergroot. De kwetsbaarheid heeft een CVSS-score van 10.0, wat het tot een zeer ernstige bedreiging maakt. Het wordt sterk aanbevolen om de nieuwste versie van Squid, versie 7.2, te installeren om de kwetsbaarheid te verhelpen. Als tijdelijke oplossing kunnen beheerders debug-informatie in Squid configureren om te voorkomen dat e-maillinks naar administratormails worden gegenereerd. Verder wordt organisaties geadviseerd om hun monitoring- en detectiemogelijkheden te verbeteren om verdachte activiteiten te identificeren.

Meerdere kritieke kwetsbaarheden in Moxa ICS-apparaten, onmiddellijk patchen!

Moxa heeft een waarschuwing uitgegeven voor meerdere kritieke kwetsbaarheden in hun industriële netwerkapparaten, waaronder de EDR-G9010, EEDR-8010, en andere modellen. Deze kwetsbaarheden stellen aanvallers in staat ongeautoriseerde toegang te verkrijgen tot beheerdersaccounts, opdrachten uit te voeren met verhoogde rechten en apparaten op afstand te beheren. De kwetsbaarheden omvatten verkeerde autorisatie, onterecht uitvoeren van opdrachten met beperkte rechten en het gebruik van hardgecodeerde inloggegevens. Aanvallers kunnen mogelijk de werking van apparaten verstoren, wat leidt tot operationele onderbrekingen of verlies van gegevensintegriteit. Moxa adviseert gebruikers dringend om de apparaten te patchen naar de nieuwste firmware om toekomstige aanvallen te voorkomen. Organisaties wordt ook aangeraden om hun monitoringcapaciteiten te versterken om verdachte activiteiten snel te detecteren.

TARmageddon-kwetsbaarheid in Async-Tar Rust Library kan leiden tot RCE

Onderzoekers hebben een ernstige kwetsbaarheid ontdekt in de populaire async-tar Rust-bibliotheek, die remote code execution (RCE) kan veroorzaken door een bug in het parseren van headers. De kwetsbaarheid, aangeduid als TARmageddon (CVE-2025-62518), heeft een CVSS-score van 8,1 en kan leiden tot het overschrijven van bestanden of het overnemen van build-backends. De kwetsbaarheid werd in augustus 2025 ontdekt en heeft invloed op verschillende veelgebruikte projecten zoals testcontainers en wasmCloud. Aangezien de Tokio-tar bibliotheek niet meer wordt onderhouden, wordt gebruikers aangeraden over te stappen op astral-tokio-tar versie 0.5.6, die de kwetsbaarheid verhelpt. De fout ontstaat door inconsistenties in de verwerking van PAX- en ustar-headers bij het bepalen van bestandsgrenzen, waardoor aanvallers extra archieven kunnen insluipen en bestanden kunnen overschrijven. Deze kwetsbaarheid benadrukt het belang van waakzaamheid, zelfs bij talen zoals Rust die bekendstaan om hun geheugenbeveiliging.

Vidar-malware gebruikt multi-threading voor sneller stelen van wachtwoorden

Een nieuwe versie van Vidar-malware maakt gebruik van multi-threading om sneller wachtwoorden en andere inloggegevens van besmette systemen te stelen. Door meerdere threads tegelijk te gebruiken, kan de malware inloggegevens uit verschillende applicaties tegelijkertijd verzamelen, wat de snelheid van de aanval vergroot. Vidar past zich aan de prestaties van het slachtoffer aan: op snellere

systemen worden meer threads gebruikt, terwijl op langzamere systemen minder threads worden ingezet. Deze malware richt zich op verschillende browsers, zoals Google Chrome, Firefox en Edge, en steelt ook gegevens uit cryptowallets en programma's zoals Discord en Steam. Vidar wordt aangeboden als malware-as-a-service voor $300 per levenslang abonnement. Het wordt verspreid door cybercriminelen, die de gestolen gegevens naar hun servers sturen, waarna de malware de sporen van de aanval verwijdert om het forensisch onderzoek te bemoeilijken.

ToolShell-aanvallen gericht op organisaties over vier continenten

Hackers die vermoedelijk verband houden met China hebben de ToolShell-kwetsbaarheid (CVE-2025-53770) in Microsoft SharePoint misbruikt om aanvallen uit te voeren op overheidsinstanties, universiteiten, telecomproviders en financiële instellingen. De kwetsbaarheid, die on-premise SharePoint-servers aantast, werd op 20 juli als actief uitgebuit gemeld, en Microsoft bracht een spoedupdate uit. De aanvallen maken gebruik van remote code execution zonder authenticatie. Drie Chinese dreigingsgroepen – Budworm, Sheathminer en Storm-2603 – hebben de kwetsbaarheid benut voor toegang tot systemen. De aanvallers gebruikten een reeks tools, waaronder Zingdoor en ShadowPad, om systemen verder te compromitteren. De aanvallen richtten zich op organisaties in het Midden-Oosten, Zuid-Amerika, de VS, Afrika en Europa, waarbij zij diverse malware-instrumenten inzetten voor het verkrijgen van persistente toegang en het verzamelen van informatie.

Nep Nethereum NuGet-pakket gebruikt homoglyph-truc om crypto wallet sleutels te stelen

Onderzoekers hebben een nieuwe supply chain-aanval ontdekt waarbij een vals Nethereum NuGet-pakket werd gebruikt om crypto wallet sleutels te stelen. Het kwaadwillige pakket, genaamd Nethereum.All, maakte gebruik van een homoglyph-truc waarbij de letter "e" werd vervangen door een Cyrillisch symbool om ontwikkelaars te misleiden. Het pakket bevatte een functie die gevoelige gegevens zoals privésleutels en mnemonische zinnen naar de aanvaller stuurde via een Command-and-Control server. Het pakket werd geüpload op 16 oktober 2025 door een gebruiker met de naam "nethereumgroup" en werd vier dagen later verwijderd door NuGet voor schending van hun gebruiksvoorwaarden. Dit incident volgt op

eerdere gevallen waarbij soortgelijke homoglyph-trucs werden gebruikt in andere NuGet-pakketten, wat het belang van zorgvuldige verificatie van softwarepakketten benadrukt.

SnakeStealer: Een groeiende dreiging voor persoonlijke gegevens

SnakeStealer is een malware die in 2025 de top van de infostealer-detecties heeft bereikt, bekend om zijn vermogen om waardevolle persoonlijke gegevens te stelen, zoals inloggegevens, financiële informatie en cryptocurrency-gegevens. Het werd voor het eerst gedetecteerd in 2019 en maakt gebruik van verschillende verspreidingsmethoden, waaronder phishing, malafide e-mailbijlagen, en zelfs piraterijsoftware. Het volgt het "malware-as-a-service" model, waardoor het gemakkelijk toegankelijk is voor aanvallers van verschillende vaardigheidsniveaus. De malware is modulair, wat betekent dat aanvallers functies kunnen in- of uitschakelen, zoals het stelen van wachtwoorden, het vastleggen van toetsaanslagen en het nemen van schermafbeeldingen. Om zich te beschermen tegen deze bedreiging, wordt aangeraden om ongevraagde berichten te vermijden, systeem- en app-updates uit te voeren, en multi-factor authenticatie in te schakelen. Dit benadrukt de snelle adaptatie van de cybercriminelen en de industrialisatie van cybercriminaliteit.

Lumma Infostealer malware steelt browsercookies, cryptocurrency-wallets en VPN/RDP-accounts

Lumma Infostealer is een malware die sinds augustus 2022 actief is en snel populair werd door malware-as-a-service platforms. De malware wordt voornamelijk via phishing-sites verspreid die zich voordoen als software-installateurs. De schadelijke code wordt verpakt in een NSIS-installatiepakket, ontworpen om detectie via handtekeningen te vermijden. Bij uitvoering worden AutoIt-modules in het geheugen samengevoegd, waarna obfuscatie wordt toegepast om de kwaadaardige activiteit te verbergen. Lumma steelt browsercookies, accounttokens en cryptowallet-bestanden, en maakt gebruik van gestolen gegevens voor sessieovername, wat multi-factor authenticatie kan omzeilen. Het doelwit is zowel consumenten als bedrijven, waarbij de gestolen gegevens vaak leiden tot ongeautoriseerde toegang tot digitale middelen en netwerken. Verdere aanvallen, zoals ransomware, kunnen volgen. Beveiligingsmaatregelen zoals endpointdetectie, gedrag gebaseerde analyse en

blokkades voor bekende C2-domeinen worden aanbevolen om deze dreiging te mitigeren.

OM onderzoekt sadistisch onlinenetwerk '764'

Het Openbaar Ministerie (OM) onderzoekt het sadistische onlinenetwerk '764', waarin jonge mensen worden gedwongen tot gewelddadige en seksueel misbruikende handelingen. Dit netwerk, dat beelden van extreem geweld en zelfbeschadiging bevat, wordt beheerd door een man uit Eindhoven die onder de naam Cxrpse opereerde. De man werd gearresteerd op verdenking van terrorisme en zit momenteel vast in een zwaarbeveiligde gevangenis. In de chatgroepen werden jongeren gemanipuleerd via platformen zoals Roblox en Discord om foto’s te sturen, waarna ze werden gechanteerd met steeds extremere verzoeken. Het OM maakt zich zorgen over de omvang van deze netwerken, die volgens de autoriteiten steeds gewelddadiger worden. Verdere arrestaties van betrokkenen hebben inmiddels plaatsgevonden, en tientallen slachtoffers zijn geïdentificeerd. Het OM benadrukt de gevaren van dergelijke netwerken en de impact op de slachtoffers.

183 miljoen gecompromitteerde e-mailadressen toegevoegd aan HIBP

Op 22 oktober 2025 werden 183 miljoen gecompromitteerde e-mailadressen toegevoegd aan de zoekmachine Have I Been Pwned (HIBP). Hiervan waren 16,4 miljoen adressen nieuw voor de database. Deze adressen werden verzameld uit "stealer logs", bestanden die door infostealer-malware worden aangemaakt en die inloggegevens van slachtoffers bevatten. De gegevens werden verzameld door securitybedrijf Synthient en bestaan uit 3,5 terabyte aan informatie. E-mailadressen die zijn opgenomen in deze logbestanden, kunnen nu door de eigenaren worden gecontroleerd op HIBP, waar ze kunnen zien op welke websites hun gegevens zijn gebruikt. Van de 183 miljoen e-mailadressen was 91 procent al eerder bekend via andere datalekken, maar 16,4 miljoen adressen waren nieuw. HIBP biedt gebruikers de mogelijkheid om hun wachtwoorden aan te passen op de betreffende websites.

Synthient stealer logs en credential stuffing data onthuld

Synthient, een threat intelligence platform, heeft 3,5 terabyte aan data vrijgegeven, bestaande uit stealer logs en credential stuffing lijsten. Deze data bevat 23 miljard

rijen, waarvan een groot deel afkomstig is van infostealers die wachtwoorden van geïnfecteerde machines verzamelt. Synthient heeft deze gegevens naar "Have I Been Pwned" (HIBP) gestuurd, wat resulteerde in de ontdekking van 183 miljoen unieke e-mailadressen, waarvan 8% nooit eerder waren gezien. De verzamelde gegevens bevatten ook inloggegevens van verschillende websites, waaronder sociale media, crypto-sites en online casino's. Het gebruik van deze gestolen gegevens kan leiden tot accountovername via credential stuffing, wat risico's met zich meebrengt voor veel gebruikers. Synthient blijft het aantal nieuwe ontdekkingen vergroten, en de gegevens blijven op HIBP beschikbaar voor zoekopdrachten.

WhatsApp toont waarschuwing bij delen van scherm met onbekenden

WhatsApp introduceert een nieuwe waarschuwing voor gebruikers die hun scherm delen tijdens videogesprekken met onbekende contacten. Het doel is om fraude te voorkomen, met name door scammers die proberen gevoelige informatie, zoals bankgegevens, te verkrijgen. Meta, het moederbedrijf van WhatsApp, wijst erop dat ouderen vaak het slachtoffer zijn van dergelijke scams, zoals blijkt uit cijfers van de FBI, waarbij ouderen in 2024 4,9 miljard dollar verloren door oplichting. De waarschuwing verschijnt wanneer gebruikers hun scherm delen met onbekenden en adviseert hen om dit alleen te doen met vertrouwde contacten. Daarnaast test Meta in Messenger een tool die scams in chats detecteert en gebruikers waarschuwt. De detectie vindt plaats op het toestel van de gebruiker, zodat de end-to-end encryptie behouden blijft.

Cyberaanval Jaguar Land Rover kost het Verenigd Koninkrijk 2,2 miljard euro

De cyberaanval op Jaguar Land Rover (JLR) heeft het Verenigd Koninkrijk 2,2 miljard euro gekost en heeft meer dan vijfduizend organisaties getroffen, volgens het Cyber Monitoring Centre (CMC). Het incident, dat begon op 2 september, verstoorde de productie en verkoop van het bedrijf, met een tijdelijk werkstop van personeel. JLR is sindsdien begonnen met het gefaseerd herstarten van systemen en productie, hoewel de verstoring nog weken kan aanhouden. De kosten worden toegeschreven aan productieverlies, herstelkosten, verstoringen in de logistieke keten, lagere autoverkopen en gevolgen voor leveranciers en lokale bedrijven. Het CMC benadrukt dat de schade mogelijk verder zal oplopen, afhankelijk van de impact op de

operationele technologie en onverwachte vertragingen in het herstel. De aanval toont het strategische belang van cyberweerbaarheid in de industriële basis van het VK.

Ziekenhuis Maagdeneilanden bijna 5 maanden offline na ransomware-aanval

Het Juan F. Luis Hospital op de Amerikaanse Maagdeneilanden was bijna vijf maanden offline na een ransomware-aanval in april. De aanval verstoorde belangrijke systemen, waardoor het ziekenhuis geen elektronische facturen meer kon indienen. Dit resulteerde in een verlies van tussen de 750.000 en 800.000 dollar per week, hoewel de CEO benadrukte dat het verlies niet permanent was, maar tijdelijk door de vertraging. Het personeel moest overstappen op handmatige procedures, wat leidde tot een daling van de efficiëntie en de moraal. De aanvallers kwamen binnen via een gemiste kwetsbaarheid op twee servers. Inmiddels is 80 tot 85 procent van het personeel weer toegang tot het elektronisch patiëntendossier, maar financiële diensten en andere systemen zijn nog niet volledig hersteld. Het ziekenhuis heeft ondertussen de ICT-infrastructuur volledig vernieuwd en legt meer nadruk op cybersecurity.

Nieuwe hackinggroep Genesis

Genesis is een recent ontdekte hackinggroep die meerdere Amerikaanse organisaties aanvalt, met doelwitten in de groothandel, juridische sector, financiën, gezondheidszorg en de productie-industrie. De groep beweert ongeveer 2,24 TB aan gevoelige gegevens te hebben buitgemaakt, waaronder bedrijfsdocumenten, financiële gegevens, loonadministratie, persoonlijke en medische informatie, juridische bestanden, e-mails en back-ups van databases. Enkele slachtoffers waren eerder al het doelwit van andere ransomwaregroepen, zoals Play en Kraken, wat wijst op mogelijk gedeelde toegangspunten. Genesis heeft aangegeven puur financieel gemotiveerd te zijn, zonder affiliaties, en dreigt met publicatie van de gestolen data als betalingen uitblijven. Ze claimen data te verwijderen na betaling, maar verhogen de druk door waardevolle "geparseerde" mappen vrij te geven om de impact te maximaliseren.

Verkoop van privé PSN brute-force tool op het darkweb

Er is melding gemaakt van de vermeende verkoop van een brute-force checker voor het PSN (PlayStation Network) op het darkweb. Deze tool wordt mogelijk aangeboden voor de onterecht toegang tot accounts van PSN-gebruikers. De tool is gericht op het kraken van inloggegevens door middel van brute-force aanvallen, waarbij combinaties van wachtwoorden systematisch worden geprobeerd. Dit soort aanvallen kan ernstige gevolgen hebben voor de veiligheid van gebruikersaccounts en persoonlijke gegevens. De verkoop van dergelijke tools benadrukt de voortdurende dreiging van cybercriminelen die zich richten op populaire platformen zoals PSN. Het is een voorbeeld van hoe het darkweb wordt gebruikt voor de verkoop van cyberaanvaltools die wereldwijd schade kunnen veroorzaken.

Ongeautoriseerde toegang tot 2.100 Fortinet-systemen verkocht op het darkweb

Er is melding gemaakt van de verkoop van ongeautoriseerde toegang tot 2.100 Fortinet-systemen op het darkweb. Deze toegang wordt aangeboden op een malafide marktplaats, wat de kwetsbaarheid van de betrokken systemen vergroot. Het verkoopaanbod betreft vermoedelijk systemen die zijn gecompromitteerd door cybercriminelen, en het is nog onduidelijk of de toegang daadwerkelijk is verkregen door een eerdere exploit of door andere middelen. Dit incident benadrukt de aanhoudende dreiging van aanvallen via zwakke plekken in veelgebruikte netwerksystemen. Het is cruciaal voor bedrijven en organisaties om hun netwerken regelmatig te monitoren en beveiligingsupdates tijdig door te voeren om dergelijke incidenten te voorkomen.

Exploit in BetterBank DeFi protocol leidt tot verlies van $5 miljoen

Van 26 tot 27 augustus 2025 werd het BetterBank DeFi-protocol slachtoffer van een aanval waarbij de beloningssystemen werden gemanipuleerd. De aanvaller maakte gebruik van een kwetsbaarheid in het systeem van bonusminting, wat resulteerde in een initiële verlies van ongeveer $5 miljoen. Na onderhandelingen keerde de aanvaller ongeveer $2,7 miljoen terug, wat de financiële schade verlaagde tot een netto verlies van ongeveer $1,4 miljoen. De aanval was mogelijk door een ontwerpflauw in de smart contractfunctie voor het minten van ESTEEM-tokens zonder adequate validatie van de liquidez-pools. Hoewel dit probleem werd gedocumenteerd in een beveiligingsaudit, werd het niet volledig opgelost, wat leidde tot de exploit. Dit incident benadrukt het belang van grondige beveiligingsaudits en

effectieve communicatie tussen ontwikkelteams en beveiligingsexperts. Het herstel van een deel van de gestolen fondsen is opmerkelijk, maar het incident toont de risico's van onvoldoende beveiliging in DeFi-platforms.

Philips Hue Bridge en Samsung Galaxy S25 gehackt tijdens Pwn2Own

Onderzoekers hebben tijdens de Pwn2Own-wedstrijd in Cork, Ierland, de Philips Hue Bridge en Samsung Galaxy S25 succesvol gehackt door onbekende kwetsbaarheden te benutten. De Philips Hue Bridge, een smart hub voor het bedienen van lampen, werd gecompromitteerd door een authenticatie bypass en een out-of-bounds write, waarmee de onderzoekers code konden uitvoeren. Dit resulteerde in een beloning van 20.000 dollar. Een ander team gebruikte vier kwetsbaarheden, wat hen 40.000 dollar opleverde. Daarnaast werden vijf nieuwe kwetsbaarheden in de Hue Bridge gedemonstreerd, wat een beloning van 16.000 dollar opleverde. Wat betreft de Samsung Galaxy S25 slaagden onderzoekers van Summoning Team erin de telefoon te compromitteren via een aanval via de browser, wat hen 50.000 dollar opleverde. Updates voor deze kwetsbaarheden van Philips en Samsung worden nog verwacht.

Rival hackers onthullen vermeende operators van Lumma Stealer

Een rivaliserende hacker-groep heeft de identiteit van de vermeende operators van Lumma Stealer, een krachtige datadiefstal-malware, openbaar gemaakt. Lumma Stealer is sinds 2022 actief als Malware-as-a-Service (MaaS), gericht op het stelen van wachtwoorden, creditcardgegevens en crypto-wallets. De onthullingen, die tussen augustus en oktober 2025 plaatsvonden, bevatten gevoelige gegevens van vijf individuen die betrokken waren bij de ontwikkeling van de malware. De informatie werd gedeeld op de website "Lumma Rats". Dit lek leidde tot een aanzienlijke afname van de activiteiten van Lumma Stealer, wat resulteerde in klanten die op zoek gingen naar alternatieven zoals Vidar en StealC. De onthullingen zouden een interne strijd tussen criminelen weerspiegelen, mede als gevolg van een mislukte poging van de wetshandhaving om Lumma Stealer in mei 2025 te stoppen.