Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

08-10-2025:

Sunweb weigert compensatie voor phishing-slachtoffers na datalek

Sunweb heeft aangekondigd dat klanten die het slachtoffer zijn geworden van phishingmails, verstuurd uit naam van de reisorganisatie, geen compensatie hoeven te verwachten. Hackers kregen via een inbraak toegang tot klantgegevens, waaronder e-mailadressen en telefoonnummers. De phishingmails, die klanten dreigden hun reis te annuleren als ze niet betaalden, waren overtuigender door de gestolen gegevens. Ondanks erkenning van het datalek, waarbij de reisorganisatie zegt de beveiliging te hebben verbeterd, blijft Sunweb bij de beslissing geen schadevergoeding te bieden. Advocaten wijzen erop dat de reisorganisatie volgens de Algemene Verordening Gegevensbescherming (AVG) wel degelijk aansprakelijk kan zijn, vooral als klanten kunnen aantonen dat het datalek leidde tot schade. De Autoriteit Persoonsgegevens onderzoekt het incident verder.

Pilot met noodsteunpunten voor overstromingen en cyberaanvallen in Nederland

Nog dit jaar wordt een pilot gestart voor de inrichting van noodsteunpunten in alle 25 Nederlandse veiligheidsregio's. Deze steunpunten, die in brandweerkazernes als centrale commandoposten zullen fungeren, moeten dienen als informatiesites voor crisissituaties zoals overstromingen, cyberaanvallen en stroomuitval. De bedoeling is om in 2026 de pilot volledig te implementeren. Naast de centrale posten komen er op lokaal niveau ondersteuningspunten, bijvoorbeeld in voetbalkantines en buurthuizen, waar mensen terechtkunnen bij noodgevallen. Het Veiligheidsberaad, bestaande uit de burgemeesters van de veiligheidsregio's, wil uiteindelijk duizend hoofdsteunpunten en 3600 lokale steunpunten oprichten. Het kabinet ondersteunt het initiatief, waarbij de noodsteunpunten ook ingezet moeten worden in geval van grootschalige cybercrises, hybride aanvallen of zelfs een militair conflict. De pilot zal de effectiviteit van deze steunpunten in het vergroten van de weerbaarheid testen.

Nieuwe hacktivistische alliantie gevormd door NoName057(16) en Hider_Nex

De hacktivistische groepen NoName057(16) en Hider_Nex hebben officieel aangekondigd een alliantie te vormen. Deze samenwerking komt te midden van toenemende cyberdreigingen en geopolitieke spanningen, waarbij de twee groepen zich richten op het uitvoeren van cyberaanvallen ter ondersteuning van hun politieke

doelstellingen. De alliantie versterkt de capaciteit van beide groepen, die zich eerder hebben bewezen met verschillende gerichte aanvallen op overheidsinstanties en kritieke infrastructuur. Dit samenwerkingsverband kan een significante impact hebben op de cyberdreigingen die gericht zijn op landen met strategische belangen voor de betrokken actoren.

Android voor tweede keer in 10 jaar tijd zonder maandelijkse beveiligingsupdates

Voor de tweede keer in tien jaar heeft Google besloten om geen maandelijkse beveiligingsupdates voor Android uit te brengen. Sinds augustus 2015 heeft Google elke maand beveiligingsbulletins gepubliceerd om kwetsbaarheden in Android-systemen te verhelpen. Echter, in juli dit jaar werd er voor het eerst een leeg beveiligingsbulletin gepost, en ook in oktober zijn er geen updates verschenen. Qualcomm heeft deze maand eveneens geen updates uitgebracht, hoewel Samsung wel updates heeft gepusht voor zijn apparaten, zonder dat er kritieke kwetsbaarheden werden aangepakt. Google heeft aangegeven een nieuw updatemodel te hanteren, waarbij alleen beveiligingslekken met een hoog risico maandelijks worden gepatched, terwijl andere kwetsbaarheden pas per kwartaal worden verholpen. Deze veranderingen zijn nog niet officieel bevestigd door Google zelf.

Zimbra Collaboration webclient kwetsbaar door actieve XSS-aanvallen, patch vereist

Op 7 oktober 2025 werd een kritieke kwetsbaarheid in de Zimbra Collaboration webclient bekendgemaakt, die actief wordt misbruikt. Het betreft een opgeslagen cross-site scripting (XSS) kwetsbaarheid (CVE-2025-27915) die de versies 9.0, 10.0 en 10.1 van de webclient beïnvloedt. Een aanvaller kan kwaadaardige JavaScript-code injecteren in een ICS-bestand (Icloud kalender), dat vervolgens aan een e-mail wordt toegevoegd. Wanneer een slachtoffer dit bestand opent, wordt de schadelijke code uitgevoerd, waardoor de aanvaller toegang krijgt tot gevoelige gegevens zoals cookies, sessies en accountinformatie. Dit kan leiden tot ongeautoriseerde acties, zoals e-mailomleiding of datalekken. De Belgische Cybersecurity Centrum (CCB) adviseert onmiddellijk de kwetsbare systemen te patchen en waarschuwt om verdachte activiteiten te monitoren.

Microsoft: kritiek GoAnywhere MFT-lek gebruikt bij ransomware-aanvallen

Microsoft heeft aangekondigd dat een ernstige kwetsbaarheid in de Fortra GoAnywhere MFT-oplossing is misbruikt bij ransomware-aanvallen. Het probleem, aangeduid als CVE-2025-10035, werd voor het eerst ontdekt op 11 september 2025, maar er was toen nog geen beveiligingsupdate beschikbaar. Het lek stelt aanvallers in staat om commando's uit te voeren op de server via een "valide gefalsificeerde licentierespons". Microsoft waarschuwt dat de kwetsbaarheid, met een score van 10.0 op de schaal van 10, ernstige gevolgen kan hebben, zoals het verkrijgen van systeem- en gebruikersinformatie, langdurige toegang tot systemen en het uitvoeren van latere aanvallen met malware. De eerste meldingen van misbruik dateren van 10 september, acht dagen voor de uitgave van een patch door Fortra. Organisaties wordt aangeraden om hun systemen te controleren op verdachte activiteiten en aanvullende beveiligingsmaatregelen te treffen.

FBI waarschuwt Oracle EBS-klanten om dringende patch te installeren

De FBI heeft een waarschuwing uitgegeven voor organisaties die gebruikmaken van Oracle E-Business Suite (EBS). Een ernstige kwetsbaarheid in het systeem is al misbruikt door criminelen om gevoelige gegevens te stelen en deze af te persen. Het beveiligingslek betreft EBS-software, die gebruikt wordt voor Enterprise Resource Planning (ERP) en vaak gevoelige informatie bevat. Het National Cyber Security Centrum (NCSC) meldt dat er al exploitcode in omloop is, wat betekent dat het risico op aanvallen groter wordt. Organisaties wordt dringend aangeraden om de recent uitgebrachte noodpatch onmiddellijk te installeren om verdere schade te voorkomen. De FBI benadrukt dat systemen die vanaf het internet toegankelijk zijn, in bijzonder gevaar lopen om volledig gecompromitteerd te worden. Daarnaast wordt geadviseerd om netwerklogs te controleren op verdachte activiteiten.

Verdachte HTX-thema domein geïdentificeerd voor potentieel C2-activiteit

Een domein dat zich voordoet als een loginpagina van de HTX cryptocurrency-exchange, is geïdentificeerd als mogelijk phishing-portaal met het risico op command-and-control (C2)-activiteit. Het domein, htx-user[.]at, wordt vermoed te dienen voor zowel het verzamelen van inloggegevens als voor het coördineren van botnet-communicatie. De dreiging wordt met een vertrouwen van 75% ingeschat. De verdachte infrastructuur heeft een DNS IP-adres van 95[.]129[.]234[.]137. Verdere

analyse toont aan dat de site een vervalste loginpagina heeft, die gebruikers kan misleiden. Het wordt aangeraden het domein en bijbehorende IP-adres te blokkeren via DNS, proxy en endpoint-beveiliging. Er wordt ook geadviseerd om verdachte uitgaande verbindingen naar cryptocurrency-gerelateerde domeinen te monitoren, vooral die welke zich voordoen als legitieme cryptoportalen.

Verkoop van Oracle E-Business exploit op Dark Web geclaimd door dreigingsactor

Een dreigingsactor heeft via sociale media geclaimd een N-day exploit van Oracle E-Businesses (CVE-2025-61882) te verkopen op het Dark Web. Deze kwetsbaarheid heeft invloed op Oracle E-Business Suite en kan mogelijk worden gebruikt om systemen te compromitteren. Het is niet duidelijk of de exploit al in het wild is aangetroffen of dat het enkel wordt aangeboden voor toekomstige aanvallen. De ontdekking benadrukt de voortdurende dreiging van kwetsbaarheden in populaire bedrijfssoftware en de risico's die hiermee gepaard gaan voor organisaties wereldwijd. Gebruikers van Oracle E-Businesses wordt geadviseerd waakzaam te blijven en hun systemen te monitoren op mogelijke aanvallen die gebruik maken van deze kwetsbaarheid.

Cybercriminelen achter WARMCOOKIE-malware voegen nieuwe functies toe aan hun arsenaal

De WARMCOOKIE-backdoor, die in 2024 opdook, wordt verspreid via phishing en malvertising. De malware is ontworpen als een modulaire backdoor, waarmee aanvallers op afstand toegang krijgen tot systemen. Het aanvankelijke doel was eenvoudig, maar de malware is inmiddels geëvolueerd. De afgelopen maanden zijn er nieuwe functies toegevoegd, zoals het vermogen om uitvoerbare bestanden, DLL's en PowerShell-scripts uit te voeren. De malware maakt gebruik van dynamische stringbanken en GUID-stijl mutexen om detectie te vermijden en zorgt voor verbeterde stealthcapaciteiten. In aanvulling op het initiële gebruik in phishingcampagnes, wordt de malware nu ingezet via geavanceerde malvertising- en spamsystemen. Een belangrijk kenmerk van de malware is dat het campagnes bijhoudt door een campagne-ID, die de verspreiding van infecties mogelijk maakt. Deze evolutie benadrukt de persistentie van de dreiging, wat WARMCOOKIE een complexe uitdaging maakt voor incidentrespons en beveiligingsteams.

Onderzoekers onthullen antivirus-bypasstechnieken van Asgard Protector malware

In de afgelopen maanden hebben onderzoekers zich gericht op de Asgard Protector, een geavanceerde crypter die door cybercriminelen wordt gebruikt om schadelijke payloads te verbergen. Sinds eind 2023 wordt de crypter steeds vaker ingezet door cybercriminelen om infostealers en remote access trojans (RAT's) te verbergen binnen ogenschijnlijk onschuldige installers. Deze techniek omzeilt traditionele antivirussoftware en bemoeilijkt het incidentenbeheer aanzienlijk. De malware maakt gebruik van een self-extracting archive om schadelijke componenten uit te pakken en te verbergen. Bovendien wordt de schadelijke code in het geheugen gedecodeerd en gecomprimeerd, zonder dat een uitvoerbaar bestand op de harde schijf wordt achtergelaten, waardoor het moeilijk is om de infectie te detecteren. Het gebruik van complexe technieken, zoals obfuscatie en het omzeilen van sandbox-omgevingen, zorgt ervoor dat de malware onopgemerkt blijft voor veel detectiesystemen.

Ransomware-groepen gebruiken remote access tools voor stealth en persistentie

Ransomware-groepen hebben hun tactieken veranderd door niet langer alleen op malware te vertrouwen, maar populaire remote access tools zoals AnyDesk en Splashtop te misbruiken om in netwerken in te breken en hun aanwezigheid te behouden. Deze tools worden vaak als legitiem beschouwd en worden daarom niet gedetecteerd door traditionele beveiligingssystemen. De aanvallers verkrijgen toegang via phishing en credential stuffing, en gebruiken de tools om laterale bewegingen binnen netwerken te maken. In plaats van op maat gemaakte malware te gebruiken, verbergen de aanvallers hun activiteiten door bestaande administratietools te misbruiken, waardoor ze moeilijk te detecteren zijn. Deze tactieken hebben geleid tot aanzienlijke schade, waaronder versleutelde bestandsdelen en uitgeschakelde back-ups. Organisaties moeten hun vertrouwde tools heroverwegen en meer gerichte monitoring en gedragsanalyse implementeren om dergelijke aanvallen tijdig te detecteren.

ShinyHunters breidt afpersingscampagne uit naar grote bedrijven

De cybercriminele groep ShinyHunters heeft een nieuw afpersingsplatform gelanceerd, waarop ze bedrijven dreigen te schaden door gestolen data van klanten te publiceren, tenzij ze een losgeld betalen. De groep heeft in 2025 al meer dan een miljard klantgegevens van Salesforce gestolen door middel van voice-phishing-

aanvallen. Tot de getroffen bedrijven behoren onder andere Toyota, FedEx, Disney en UPS. ShinyHunters claimt ook verantwoordelijk te zijn voor een recente inbraak bij het softwarebedrijf Red Hat, waarbij duizenden gevoelige klantgegevens werden gestolen. Daarnaast zijn ze betrokken bij de inbreuk op Discord-gegevens. Salesforce heeft bevestigd dat de diefstal van gegevens van derden geen kwetsbaarheid in hun eigen platform betreft, en weigert de eisen van de afpersers in te willigen. De groep heeft aangekondigd data te publiceren als de bedrijven geen losgeld betalen voor 10 oktober 2025.

Derde verdachte aangehouden in bankpasfraude onderzoek hospice in Ermelo

De politie heeft een derde verdachte aangehouden in het onderzoek naar een bankpasfraudezaak die plaatsvond in een hospice in Ermelo. De 23-jarige man uit Zaandam werd op dinsdagochtend in zijn woonplaats gearresteerd. Begin juni van dit jaar werden er voor meer dan 100.000 euro aan luxegoederen gekocht met geld van het hospice, onder andere in Amsterdam, Zaandam en Antwerpen. Het onderzoek kreeg veel media-aandacht, waaronder een bijdrage in het opsporingsprogramma Plaats Delict. Hierin werden beelden van de verdachten getoond, waardoor twee eerdere verdachten uit Zaandam werden geïdentificeerd en aangehouden op 22 september. Dankzij de uitzending werd ook de derde verdachte herkend en opgepakt. De politie bedankt de kijkers van Plaats Delict voor hun hulp en doet verder onderzoek.

Twee arrestaties na cyberaanval op kinderopvangketen

Twee personen zijn gearresteerd in verband met een cyberaanval op de Kido kinderopvangketen in Londen. Een 17-jarige jongen en een 22-jarige man werden opgepakt in Hertfordshire, op verdenking van computercriminaliteit en afpersing. De hackers stalen persoonsgegevens van ongeveer 8.000 kinderen, waaronder foto’s, namen en adressen. De cyberaanval werd op 25 september gemeld bij de politie, die werd geïnformeerd door de Action Fraud cybercrime-melddienst. De aanvallers, die zich Radiant noemden, eisten een losgeld van £600.000 in Bitcoin. Ze dreigden de gestolen gegevens te publiceren op het dark web. Nadat ze aanvankelijk enkele kinderen online hadden geplaatst, verwijderden ze later al het gestolen materiaal en beweerden dat de gegevens van alle 8.000 kinderen waren gewist. De Kido keten

heeft de autoriteiten snel geïnformeerd en werkt samen met cyberexperts om het incident te onderzoeken.

Nederland telt 19,2 miljoen apparaten die via eigen simkaart data uitwisselen

Nederland heeft momenteel 19,2 miljoen apparaten die via M2M-simkaarten (Machine-to-Machine) gegevens uitwisselen. Deze simkaarten worden onder andere gebruikt door auto's, rookmelders, alarmsystemen en slimme energiemeters. Het aantal M2M-simkaarten is in het tweede kwartaal met 400.000 gestegen. De Autoriteit Consument & Markt (ACM) heeft aangegeven dat de vraag naar deze nummers blijft groeien, mede door de toename van Internet of Things (IoT)-toepassingen. De M2M-simkaarten gebruiken het 0970-nummer, in tegenstelling tot de traditionele 06-nummers. Aangezien er maar een beperkte hoeveelheid 06-nummers beschikbaar is voor mobiele toepassingen, wordt het steeds belangrijker om voor M2M-apparaten de 0970-nummers te gebruiken. De ACM verwacht op de korte termijn geen tekort aan nummers, maar de druk zal toenemen als het extraterritoriaal gebruik van 0970-nummers mogelijk wordt.

Nederlands nepnieuws eenvoudig te fabriceren met Sora 2.0

Met de nieuwste versie van de videogenerator Sora 2.0 van OpenAI is het gemakkelijker dan ooit om nepnieuws te creëren. Deze technologie kan snel video's genereren die lijken op nieuwsuitzendingen van bekende media, zoals de NOS en BNR. Hoewel de video's visueel realistisch zijn, is de audiokwaliteit vaak lager, met typische ruis die herkenbaar is als AI-geluid. Toch kan het moeilijk zijn om de nepvideo's te onderscheiden wanneer ze op platforms zoals Instagram of TikTok verschijnen, vooral als ze met een mobiel apparaat worden bekeken. Sora 2.0 heeft nog geen officiële beschikbaarheid in Nederland, maar buitenlandse actoren kunnen via een Amerikaans account toegang krijgen. Dit biedt mogelijkheden voor het verspreiden van nepnieuws, wat zorgen baart over de risico's voor de publieke opinie en informatiebeveiliging. Het toevoegen van een watermerk kan nepvideo's identificeren, maar dit kan eenvoudig worden verwijderd.

Je gamingmuis kan je afluisteren, studie onthult verrassende kwetsbaarheid

Onderzoekers van de Universiteit van Californië, Irvine, hebben aangetoond dat optische muizen met een hoge resolutie in staat zijn om minuscule trillingen op een bureau waar te nemen en deze om te zetten in spraak. Deze muizen, die vaak worden gebruikt voor gaming of grafisch ontwerp, kunnen trillingen vastleggen die ontstaan wanneer iemand spreekt. Deze trillingen worden door de muis sensoren geregistreerd en kunnen, mits het systeem toegang heeft tot deze rauwe data, geanalyseerd worden. Het proces vereist geen geavanceerde malware, omdat het gewoonlijk beschikbare software kan benutten. De onderzoekers gebruikten signaalverwerkingstechnieken om de trillingen te isoleren en om te zetten naar verstaanbare spraak, met een nauwkeurigheid van 42% tot 61%. Deze ontdekking benadrukt de potentiële privacygevaren van alledaagse technologieën in een tijd waarin apparaten steeds vaker sensorfunctionaliteiten bevatten.