Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

07-10-2025:

Sunweb waarschuwt klanten na lekken van persoonsgegevens voor phishing

Sunweb heeft bevestigd dat de persoonlijke gegevens van klanten zijn gelekt, wat heeft geleid tot phishingaanvallen. Gegevens zoals namen, e-mailadressen, telefoonnummers en boekingsinformatie werden gestolen. De aanvallers gebruikten een gecompromitteerde mailserver van een onbekend bedrijf om phishingmails te versturen, waarin klanten werd gevraagd om hun gegevens te bevestigen en betalingen te doen, met dreigementen van annuleringen van vakanties. De reisorganisatie heeft alle getroffen klanten geïnformeerd en maatregelen getroffen om het systeem af te sluiten. Ook is het incident gemeld bij de Autoriteit Persoonsgegevens. Sunweb waarschuwt klanten dat ze nooit om bevestigingen via links in e-mails vragen en alleen e-mails versturen vanuit hun eigen domeinen.

Nieuwe hacktivistische alliantie aangekondigd

De hacktivistische groepen UNIT 2012022023 en V For Vendetta Cyber Team hebben op 6 oktober 2025 officieel een nieuwe samenwerking aangekondigd. Deze alliantie zou de krachten bundelen om hun cyberoperaties te versterken, wat kan leiden tot een toename van gerichte aanvallen en cyberoperaties. Hacktivisme is een steeds grotere bedreiging voor de cybersecuritysector, met dergelijke allianties die het moeilijker maken om aanvallen te voorspellen of te voorkomen. De groepen hebben verschillende ideologische doelen en doelen, wat hun acties in cyberspace verder complex maakt. De impact van deze samenwerking kan variëren, maar het is duidelijk dat de alliantie de wereldwijde cyberdreigingen verder zal beïnvloeden, vooral in gebieden waar politieke of sociale instabiliteit heerst.

Nieuwe hacktivistenalliantie tussen CLOBELSECTEAM en TwoNet

De hacktivistengroepen CLOBELSECTEAM en TwoNet hebben op 6 oktober 2025 een nieuwe alliantie aangekondigd. Deze samenwerking markeert een versterking van hun gezamenlijke cyberoperaties en zal waarschijnlijk leiden tot nieuwe cyberdreigingen. De groepen staan bekend om hun gerichte aanvallen op overheidsinstellingen en bedrijven, waarbij ze zowel digitale verstoringen veroorzaken als gevoelige informatie lekken. De nieuwe alliantie vergroot hun bereik en capaciteit om verschillende soorten cyberaanvallen uit te voeren, wat voor zowel

bedrijven als overheden een grotere dreiging vormt. Hacktivisme blijft een belangrijk onderdeel van de hybride oorlogsvoering, waarbij ideologische motieven de acties van deze groepen aandrijven.

Rapport verbindt onderzoeksbedrijven BIETA en CIII aan China's MSS Cyberoperaties

Een recent rapport heeft het Chinese bedrijf Beijing Institute of Electronics Technology and Application (BIETA) gelinkt aan de Chinese Ministerie van Staatsveiligheid (MSS). Dit blijkt uit bewijs dat ten minste vier medewerkers van BIETA mogelijk banden hebben met MSS-functionarissen en de Universiteit voor Internationale Betrekkingen, die banden heeft met MSS. BIETA en haar dochteronderneming CIII zijn betrokken bij de ontwikkeling van technologieën voor inlichtingen-, tegeninlichtingen- en militaire missies die relevant zijn voor de nationale veiligheid van China. Hun werk omvat onder andere steganografie voor covert communicatie, malware-distributie en het ontwikkelen van forensisch onderzoeksmateriaal. De technologieën van BIETA ondersteunen vermoedelijk de operaties van het MSS en worden gebruikt door staatsveiligheidsdiensten en hun onderaannemers.

Oracle verhelpt zero-day kwetsbaarheid in E-Business Suite na diefstal door Clop

Oracle heeft een kritieke zero-day kwetsbaarheid in zijn E-Business Suite (EBS) verholpen, die werd misbruikt door de Clop-ransomwaregroep. De kwetsbaarheid, aangeduid als CVE-2025-61882, stelt aanvallers in staat om op afstand code uit te voeren zonder authenticatie. Dit maakt de exploit bijzonder gevaarlijk. De aanval werd specifiek gericht op de Oracle Concurrent Processing-productcomponent van EBS, wat een score van 9,8 op de CVSS-beoordelingsschaal oplevert. Clop gebruikte deze kwetsbaarheid om grote hoeveelheden gegevens van slachtoffers te stelen. Dit incident volgt op eerdere aanvallen van Clop, waarbij ook zero-day kwetsbaarheden werden geëxploiteerd in platforms zoals Accellion en MOVEit. Oracle heeft een spoedpatch vrijgegeven, maar gebruikers moeten eerst de oktober 2023 Critical Patch Update installeren voordat ze de nieuwe beveiligingsupdates kunnen toepassen.

Kritieke kwetsbaarheid in Redis servers maakt externe code-uitvoering mogelijk

Een ernstige kwetsbaarheid, geïdentificeerd als CVE-2025-49844, is ontdekt in Redis-servers die de Lua scripting-engine gebruiken. Deze use-after-free-kwetsbaarheid stelt aanvallers in staat om op afstand code uit te voeren, mits ze geauthenticeerd zijn en rechten hebben om Lua-scripts uit te voeren. De kwetsbaarheid ligt in de manier waarop Redis het geheugengebruik binnen Lua afhandelt, waardoor aanvallers geheugen kunnen manipuleren, wat leidt tot een geheugenbeschadiging en de mogelijkheid om willekeurige code uit te voeren. Dit kan ernstige gevolgen hebben voor de integriteit, vertrouwelijkheid en beschikbaarheid van gegevens in Redis-databases. Als tijdelijke oplossing wordt aanbevolen om de uitvoering van Lua-scripts te blokkeren door Redis Access Control Lists (ACLs) aan te passen. Een formele patch is nog niet beschikbaar.

PoC-exploit voor Sudo-kwetsbaarheid maakt root-toegang mogelijk

Een proof-of-concept (PoC) exploit voor CVE-2025-32463, een kwetsbaarheid in de Sudo-tool, is openbaar beschikbaar gesteld. Deze zwakte, die zich voordoet bij lokale privilege-escalatie (LPE), maakt het mogelijk voor een gebruiker met beperkte rechten om root-toegang te verkrijgen onder specifieke configuraties. De kwetsbaarheid bevindt zich in de manier waarop Sudo omgaat met chroot-paden en omgevingen bij het uitvoeren van commando's met verhoogde rechten. Onder bepaalde omstandigheden kan een aanvaller uit de beperkte omgeving ontsnappen en als root werken. De PoC toont een eenvoudige exploitatie-aanpak: verifiëren van de Sudo-versie, uitvoeren van het script en het verkrijgen van root-rechten. Beheerders wordt geadviseerd om Sudo bij te werken naar versie 1.9.17p1 of later om de kwetsbaarheid te verhelpen. Tot die tijd kunnen strengere Sudo-beperkingen en toegangbeveiligingsmaatregelen helpen om misbruik te voorkomen.

Cybercrime treft driekwart Nederlanders, maar slimme apparaten blijven vaak onveilig

Het afgelopen jaar heeft driekwart van de Nederlanders te maken gehad met pogingen tot cybercrime, waarbij slecht beveiligde slimme apparaten een belangrijke rol spelen. Twee derde van de Nederlanders zegt hun apparaten regelmatig te updaten, maar een aanzienlijk deel doet dit niet of slechts sporadisch, wat betekent dat er minimaal 2,5 miljoen apparaten onveilig zijn. De Nederlandse overheid start

daarom de campagne 'Doe je Updates' om het belang van updates te benadrukken. Slimme apparaten, zoals thermostaten en babyfoons, zijn kwetsbaar voor hackers, die ze kunnen gebruiken voor onder andere DDoS-aanvallen en datadiefstal. De minister van Economische Zaken, Karremans, opende de campagne door te laten zien hoe eenvoudig het is om deze apparaten te hacken. Cyberaanvallen worden steeds heviger, en zelfs de zwaarste DDoS-aanvallen van het jaar werden via dergelijke apparaten uitgevoerd.

Nederland heeft 790 Cisco-firewalls met actief aangevallen kwetsbaarheden

In Nederland zijn er 790 Cisco-firewalls met kwetsbaarheden die momenteel actief worden aangevallen. Deze kwetsbaarheden bevinden zich in de Cisco Adaptive Security Appliance (ASA) en Secure Firewall Threat Defense (FTD) software, waarvoor beveiligingsupdates al op 25 september zijn uitgebracht door Cisco. De kwetsbaarheden (CVE-2025-20333 en CVE-2025-20362) stellen aanvallers in staat om volledige controle over de apparaten te verkrijgen, zowel met als zonder inloggegevens. Ondanks dat de updates beschikbaar zijn, blijven wereldwijd nog zo'n 45.000 apparaten kwetsbaar, waarvan er 790 in Nederland en 120 in België worden aangetroffen. Het Nationaal Cyber Security Centrum (NCSC) heeft organisaties dringend aangespoord om de updates onmiddellijk te installeren. Deze kwetsbaarheden bieden aanvallers toegang via internet, wat een direct risico vormt voor de beveiliging van organisaties in zowel Nederland als België.

XWorm malware verschijnt opnieuw met ransomware-module en meer dan 35 plugins

De XWorm-malware is terug met nieuwe versies die verspreid worden via phishingcampagnes. Het oorspronkelijke project, ontwikkeld door XCoder, werd vorig jaar verlaten, maar andere cybercriminelen hebben de malwaresoftware overgenomen. De nieuwe varianten, XWorm 6.0, 6.4 en 6.5, bevatten meer dan 35 plugins, waaronder een ransomware-module. De malware kan worden gebruikt om gegevens te stelen van browsers en apps, op afstand toegang te krijgen tot computers, en bestanden te versleutelen. De ransomware-module is in staat om bestanden te versleutelen, waarbij de originele bestanden worden verwijderd en een losgeld wordt geëist. De malware is op grote schaal verspreid, met 18.459 infecties in verschillende landen, waaronder Rusland, de VS, India, Oekraïne en Turkije.

Cyberbeveiligingsonderzoekers adviseren organisaties om meerdere lagen van bescherming te implementeren om de impact van XWorm te verminderen.

Nieuwe ransomwaregroep: Kyber Onion breidt zich uit

Op 5 oktober 2025 werd de opkomst van een nieuwe ransomwaregroep, Kyber Onion, gemeld. De groep is actief op het dark web en heeft een eigen leaksite, waarmee ze hun aanvallen op doelwitten verspreiden. Kyber Onion heeft een Onion-domein geclaimd als onderdeel van hun activiteiten. Dit domein is toegankelijk via het Tor-netwerk, wat een verhoogde anonimiteit biedt voor de aanvallers. De groep heeft potentieel een bredere impact op organisaties door geavanceerde encryptietechnieken en gestructureerde afpersing. De groep wordt als een nieuwe dreiging beschouwd in de ransomware-landschap, met de mogelijkheid om snel schade aan te richten. De politie en beveiligingsexperts houden de ontwikkelingen rondom Kyber Onion nauwlettend in de gaten.

Fraudehelpdesk waarschuwt voor valse berichten namens gerechtsdeurwaarders en incassobureaus

Oplichters versturen frauduleuze e-mails die beweren afkomstig te zijn van gerechtsdeurwaarders of incassobureaus, aldus de Fraudehelpdesk. In de berichten wordt gedreigd met sancties, zoals beslaglegging, als een vermeende openstaande factuur niet binnen twee dagen wordt betaald. Deze e-mails zijn vaak onpersoonlijk, maar kunnen soms ook een persoonlijke aanhef bevatten. De berichten komen zowel van fictieve als bestaande gerechtsdeurwaarderskantoren, en in sommige gevallen wordt het logo van de Koninklijke Beroepsorganisatie van Gerechtsdeurwaarders (KBvG) onterecht gebruikt. Daarnaast bevatten de mails soms een iDeal-betaallink, maar dit is niet altijd het geval. Ontvangers wordt aangeraden voorzichtig te zijn en bij twijfel contact op te nemen met de betreffende instantie via officiële kanalen.

Chinese cybercriminaliteit gebruikt IIS-servers voor SEO-fraude wereldwijd

Een Chinese cybercriminaliteitsgroep, UAT-8099, is verantwoordelijk voor een wereldwijde SEO-fraude-operatie, waarbij ze misbruik maakt van kwetsbare Microsoft Internet Information Services (IIS)-servers. De groep steelt waardevolle inloggegevens, configuratiebestanden en certificaatgegevens. De aanvallen richten

zich op landen zoals India, Thailand, Vietnam, Canada en Brazilië, met als doel mobiele gebruikers, zowel Android als iPhone, te benadelen. UAT-8099 gebruikt verschillende technieken zoals webshells, open-source hackingtools en aangepaste malware genaamd BadIIS om zoekmachine-rangschikkingen te manipuleren. Eenmaal toegang verkregen tot een IIS-server, installeert de groep malware, verhoogt hun privileges en gebruikt tools zoals Cobalt Strike en RDP om hun toegang te behouden. Deze SEO-fraude wordt bereikt door middel van het plaatsen van backlinks die de zichtbaarheid van websites verhogen, wat hun zoekresultaten beïnvloedt.

Productie Jaguar Land Rover weken verstoord door cyberaanval

De productie bij Jaguar Land Rover (JLR) zal nog weken verstoord blijven door de cyberaanval die eind augustus plaatsvond. Dit heeft een aanzienlijke impact op de autofabrikant, die verwacht pas deze week een deel van de productie te kunnen hervatten. De fabriek in Wolverhampton, die de motoren voor JLR produceert, zal als eerste weer opstarten. De schade is echter groot, aangezien niet alleen de productie, maar ook de verkoop en distributie van onderdelen zijn stilgelegd. Naast fabrieken in het Verenigd Koninkrijk zijn ook locaties in Slowakije, China en India getroffen. De aanval is opgeëist door de cybercriminaliteitsgroep Scattered Lapsus$ Hunters. Om de situatie het hoofd te bieden, heeft de Britse overheid een lening van 1,7 miljard euro verstrekt aan JLR, die deels bestemd is voor getroffen toeleveranciers. De aanval heeft daarnaast ook geleid tot ontslagen bij een metaalverwerker in het VK.

Politie uitgerukt voor TikTok-prank met AI-inbreker

De politie is de afgelopen tijd meerdere keren uitgerukt voor meldingen van inbraken, waarbij het in werkelijkheid om een TikTok-prank ging. In deze prank gebruiken kinderen AI-gegenereerde foto's van een inbreker in huis, om hun ouders te foppen. De ouders, bezorgd over de situatie, belden vervolgens 112. In sommige gevallen werd zelfs een helikopter ingezet om te zoeken naar de vermeende dader. De politie, die deze grappen wel grappig vindt, waarschuwde echter dat de situatie niet uit de hand moet lopen. Er zijn meerdere meldingen van ouders die dachten dat er daadwerkelijk ingebroken was, maar het betrof slechts een foto. De exacte frequentie van de onterecht uitrukken van de politie is onbekend.

Oplichters gebruiken deepfakes van Gisele Bündchen voor frauduleuze Instagram-advertenties

Een groep verdachte oplichters in Brazilië heeft miljoenen dollars verdiend met online fraude door gebruik te maken van deepfakes van supermodel Gisele Bündchen en andere beroemdheden in Instagram-advertenties. De autoriteiten hebben vier verdachten gearresteerd en meer dan 20 miljoen reais (ongeveer 3,9 miljoen dollar) aan verdachte fondsen bevroren. Dit markeert een van de eerste pogingen in Brazilië om het groeiende gebruik van kunstmatige-intelligentie tools voor het manipuleren van beelden en video's van beroemdheden voor online oplichting tegen te gaan. De politie onderzoekt meerdere gevallen van fraude waarbij deepfakes van beroemdheden werden gebruikt om consumenten misleidende aanbiedingen, zoals nepadvertenties voor huidverzorgingsproducten en gratis prijzen, te doen. Het gebruik van deepfakes in deze oplichterijen heeft bijgedragen aan een toename van de bezorgdheid over de effectiviteit van sociale mediaplatforms in het bestrijden van dergelijke misdrijven.

Nederland grootste host voor online kindermisbruikmateriaal in Europa

Nederland is het grootste knooppunt in Europa voor het hosten van online kindermisbruikmateriaal (CSAM), blijkt uit een recent rapport van het Global Child Safety Institute, Childlight. Meer dan 60% van al het CSAM in West-Europa wordt gehost in Nederland, dat ook verantwoordelijk is voor 30% van het wereldwijde totaal. Landen als Litouwen, Slovenië en Luxemburg vertonen eveneens hoge percentages van CSAM. In 2024 waren er meer dan 880 gevallen per 10.000 inwoners in Nederland, een aanzienlijk hoger aantal dan bijvoorbeeld San Marino of Andorra. De Europese Commissie overweegt strenge maatregelen, waaronder het automatisch scannen van berichten om CSAM op te sporen, wat bij velen tot bezorgdheid leidt over de privacy. Er zijn echter zorgen over de effectiviteit en de impact van deze maatregelen op de persoonlijke vrijheid van gebruikers van digitale diensten.