## Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

22-10-2025:

Hackers gebruiken Snappybee-malware en Citrix-kwetsbaarheid om Europese telecomnetwerk te breken

Hackers, vermoedelijk gelieerd aan de Chinese cyberespionagegroep Salt Typhoon, hebben in juli 2025 geprobeerd toegang te krijgen tot een Europees telecombedrijf. Ze exploiteerden een kwetsbaarheid in een Citrix NetScaler Gateway-apparaat om hun aanval te starten. Na het verkrijgen van toegang gebruikten de aanvallers de Citrix Virtual Delivery Agent (VDA) om hun positie verder te verstevigen, met behulp van SoftEther VPN om hun oorsprong te verbergen. Tijdens de aanval werd de Snappybee-malware geïntroduceerd, vermoedelijk een opvolger van ShadowPad-malware die eerder door dezelfde groep werd gebruikt. Deze malware werd via een techniek genaamd DLL-side-loading geïntroduceerd, waarbij legitieme antivirussoftware werd misbruikt om de kwaadaardige code uit te voeren. De aanval werd echter op tijd opgemerkt en verholpen voordat er ernstige schade ontstond.

Google identificeert drie nieuwe Russische malwarefamilies van COLDRIVER-hackers

Google Threat Intelligence heeft drie nieuwe malwarefamilies geïdentificeerd, gelinkt aan de Russische hacker groep COLDRIVER. Deze malware, genaamd NOROBOT, YESROBOT en MAYBEROBOT, werd ontwikkeld vanaf mei 2025 en vertoont een versneld ontwikkeltempo. De aanvallen van COLDRIVER hebben zich ontwikkeld van de eerder gebruikte LOSTKEYS malware naar de nieuwe "ROBOT" families. De nieuwe malware werd verspreid via zogenaamde ClickFix-lures die gebruikers misleiden tot het uitvoeren van schadelijke PowerShell-opdrachten. De aanvallen lijken gericht te zijn op het verzamelen van inloggegevens van belangrijke doelwitten, zoals NGO-medewerkers en beleidsadviseurs. Het gebruik van NOROBOT en MAYBEROBOT is opvallend flexibel en werd snel ingezet na de publieke onthulling van de eerdere malware. Google benadrukt dat de hackers voortdurend de malware aanpassen om detectie te vermijden en gerichte spionageactiviteiten voort te zetten. Dit volgt op de arrestatie van drie jonge mannen in Nederland, verdacht van het verlenen van diensten aan een buitenlandse overheid.

Russische hackers evolueren malware in "I am not a robot" captchas

De door de Russische staat gesteunde hacker groep Star Blizzard heeft zijn aanvallen geïntensiveerd met nieuwe, voortdurend evoluerende malwarefamilies, waaronder NoRobot en MaybeRobot. Deze malware wordt ingezet via complexe leveringsketens, beginnend met social engineering-aanvallen via ClickFix. De groep, ook bekend als ColdRiver, UNC4057 en Callisto, is overgestapt van de eerder gebruikte LostKeys malware, minder dan een week na publieke bekendmaking van de kwetsbaarheid. De aanvallen beginnen vaak met valse CAPTCHA-pagina's die slachtoffers misleiden om schadelijke software uit te voeren. Sinds juni heeft de groep verschillende versies van NoRobot ingezet, die zijn geoptimaliseerd voor stealth en effectiviteit. De operatie wordt toegeschreven aan de Russische inlichtingendienst FSB, en de aanvallen richten zich op spionage, waarbij gevoelige gegevens van doelwitten zoals overheidsinstanties en journalisten worden gestolen.

DDoS-aanval door HEZI RASH gericht op Belgisch parlement

HEZI RASH heeft een DDoS-aanval geclaimd op meerdere websites, waaronder die van het Belgische parlement. De aanval is gericht op het verstoren van de toegankelijkheid van de site, wat de werking van de betrokken instellingen kan belemmeren. Hoewel andere doelwitten, zoals de Turkse Defensie en het Istanbul Expo Center, ook werden aangevallen, is de impact op België het meest opvallend, aangezien het parlement een belangrijk doelwit was. De details over de schade zijn op dit moment nog niet volledig bekend, maar de aanval benadrukt de kwetsbaarheid van overheidswebsites voor dergelijke cyberaanvallen.

Zyxel Authorization Bypass kwetsbaarheid laat aanvallers systeemconfiguraties downloaden

Een kritieke kwetsbaarheid in de Zyxel ATP- en USG-series firewalls stelt aanvallers in staat de autorisatiecontrole te omzeilen en toegang te krijgen tot gevoelige systeemconfiguraties. De kwetsbaarheid, aangeduid als CVE-2025-9133, betreft apparaten met firmwareversies tot V5.40(ABPS.0) en maakt het mogelijk om configuraties te bekijken en te downloaden, zelfs wanneer twee-factor-authenticatie (2FA) is ingeschakeld. Het probleem is het gevolg van onvoldoende commando-filtering in de webinterface, waardoor aanvallers ongeautoriseerde commando's kunnen injecteren. Deze kwetsbaarheid kan ertoe leiden dat wachtwoorden, API-sleutels en netwerkinstellingen worden gestolen, wat laterale beweging binnen

netwerken of persistente toegang via gewijzigde configuraties vergemakkelijkt. Zyxel heeft nog geen patch uitgebracht, maar experts adviseren onmiddellijke mitigaties, zoals het uitschakelen van externe webtoegang en het implementeren van strikte firewallregels voor CGI-eindpunten. Organisaties wordt aangeraden om configuraties te auditen om datalekken te voorkomen.

Kritieke kwetsbaarheid in TP-Link Omada Gateways vereist directe patch

Op 21 oktober 2025 werd een ernstige kwetsbaarheid ontdekt in TP-Link Omada Gateway-apparaten, aangeduid als CVE-2025-6542. Deze kwetsbaarheid maakt het mogelijk voor aanvallers om op afstand commando's uit te voeren op de apparaten, waardoor volledige controle over het systeem kan worden verkregen. Het probleem ontstaat doordat de webbeheerdersinterface van de gateway onvoldoende validatie van gebruikersinvoer uitvoert. Er is geen authenticatie vereist voor het misbruik van deze kwetsbaarheid, waardoor de kans op exploitatie groot is. Daarnaast zijn er gerelateerde kwetsbaarheden, zoals CVE-2025-7850, die na inloggen als beheerder kunnen worden misbruikt. Het wordt sterk aangeraden om snel de benodigde patches te installeren om verdere risico's te voorkomen. Organisaties moeten hun monitoringcapaciteiten verbeteren om verdachte activiteiten tijdig te detecteren.

Ivanti onthult 13 kwetsbaarheden in Endpoint Manager – geen patches beschikbaar

Ivanti heeft 13 kwetsbaarheden onthuld in de Ivanti Endpoint Manager (EPM) software, waarvan twee als kritisch en elf als medium worden geclassificeerd. De kritieke kwetsbaarheden kunnen leiden tot remote code execution en privilege escalatie. Organisaties die verouderde versies van EPM gebruiken, lopen een hoog risico, vooral omdat de systemen als centraal beheersysteem fungeren en een breed netwerk kunnen bereiken. Ivanti adviseert dringend om te upgraden naar EPM 2024 en de aanbevolen mitigaties toe te passen. De kwetsbaarheden omvatten onder andere path-traversal en SQL-injecties die schadelijke toegang tot databases mogelijk maken. Ivanti raadt klanten aan om toegang te beperken tot beheerderssystemen, sterke authenticatie toe te passen en de toegang tot de configuratie zorgvuldig te controleren. Aangezien er geen patches beschikbaar zijn, wordt aanbevolen om de systemen met de hoogste prioriteit te upgraden zodra de patches beschikbaar komen.

Apache Syncope Groovy RCE-kwetsbaarheid laat aanvallers schadelijke code injecteren

Apache Syncope, een open-source identiteitsbeheersysteem, vertoont een kwetsbaarheid die aanvallers in staat stelt om op afstand code uit te voeren via de Groovy-scriptingfunctie. Deze kwetsbaarheid, CVE-2025-57738, treft versies voor 3.0.14 en 4.0.2. Het probleem ontstaat doordat er geen beveiligingsomgeving is voor Groovy-scripts, waardoor aanvallers kwaadaardige code kunnen uploaden die draait met volledige systeemprivileges. De kwetsbaarheid maakt misbruik van het ontbreken van beperkingen bij het laden en uitvoeren van Groovy-scripts. Aanvallers kunnen via eenvoudig geauthenticeerde HTTP-verzoeken systemen compromitteren, toegang krijgen tot bestanden, of zelfs processen starten. De kwetsbaarheid is vooral gevaarlijk voor insiders of gecompromitteerde accounts met administratieve rechten. Apache heeft de kwetsbaarheid verholpen in versies 3.0.14 en 4.0.2 door een sandbox voor Groovy in te voeren, die gevaarlijke bewerkingen blokkeert. Gebruikers wordt geadviseerd direct te upgraden naar de nieuwste versie.

VS meldt actief misbruik van beveiligingslek in Oracle E-Business Suite

Het Amerikaanse CISA heeft bevestigd dat aanvallers actief misbruik maken van een kwetsbaarheid in Oracle E-Business Suite (EBS) om vertrouwelijke informatie te stelen. De kwetsbaarheid, aangeduid als CVE-2025-61884, werd op 11 oktober door Oracle gepatcht, maar de noodzaak van een update werd pas later duidelijk. Het gaat om een server-side request forgery (SSRF) die ongeautoriseerde toegang tot gevoelige gegevens mogelijk maakt. Meer dan honderd organisaties zouden getroffen zijn, en aanvallers dreigen de gestolen data openbaar te maken tenzij er losgeld wordt betaald. Het CISA heeft Amerikaanse overheidsinstanties opgedragen de patch voor 11 november te installeren. Oracle heeft geen verdere details verstrekt over het misbruik, maar het incident benadrukt de ernst van de kwetsbaarheid voor bedrijven die EBS gebruiken.

QNAP-apparaten en Synology BeeStation gehackt tijdens Pwn2Own-wedstrijd

Tijdens de jaarlijkse Pwn2Own-hackwedstrijd hebben onderzoekers succesvol kwetsbaarheden aangetoond in apparaten van QNAP en Synology. De QNAP Qhora-322-router en TS-453E-NAS werden gecompromitteerd, waarbij aanvallers toegang kregen via onbekende kwetsbaarheden. Bij de Synology BeeStation Plus konden

onderzoekers met behulp van een beveiligingslek code met rootrechten uitvoeren op het NAS-systeem. De aanvallen werden beloond met bedragen variërend van 20.000 dollar tot 100.000 dollar, afhankelijk van de complexiteit van de hacks. Pwn2Own biedt onderzoekers beloningen voor het vinden van kwetsbaarheden in populaire software en hardware, en dit jaar werden ook andere apparaten zoals printers van HP en Canon succesvol aangevallen. De ontdekte kwetsbaarheden zijn inmiddels gedeeld met de leveranciers, maar er zijn nog geen beveiligingsupdates beschikbaar voor de getroffen apparaten.

PassiveNeuron: Geavanceerde cyberespionagecampagne richt zich op servers wereldwijd

De PassiveNeuron-cyberespionagecampagne richt zich op servers van overheids-, financiële en industriële organisaties wereldwijd, met name in Azië, Afrika en Latijns-Amerika. Het aanvallende groep maakt gebruik van APT-implantaten zoals Neursite en NeuralExecutor, evenals de Cobalt Strike-tool. De aanvallen worden vaak uitgevoerd via Microsoft SQL-servers, waarbij aanvallers kwetsbaarheden uitbuiten of toegang verkrijgen via brute-forcing van databaseaccounts. Na toegang te hebben verkregen, installeren ze webshells en andere kwaadaardige software om controle over de systemen te krijgen. De campagne maakt gebruik van complexe laadtechnieken, waarbij de aanvallers DLL-bestanden gebruiken die via een reeks stadia uiteindelijk de schadelijke payloads laden. Deze implantaten stellen aanvallers in staat om gegevens te verzamelen, processen te beheren en netwerkverkeer te proxyen. Het gebruik van de Dead Drop Resolver-techniek voor communicatie met de command & control-servers suggereert mogelijk een Chinese oorsprong voor de aanvallen, hoewel de toeschrijving nog onduidelijk is.

Opkomende phishingtechnieken in 2025: PDF-bestanden, kalenderaanvallen en MFA-omzeiling

In 2025 passen cybercriminelen verfijnde technieken toe om phishingaanvallen te maskeren en beveiligingsmaatregelen te omzeilen. PDF-bestanden worden steeds vaker gebruikt als bijlagen, met QR-codes die de links naar kwaadaardige websites verbergen. Daarnaast worden sommige PDF-bestanden versleuteld en met wachtwoorden beveiligd, wat het moeilijker maakt voor automatische scanners om ze te detecteren. Oude methoden, zoals phishing via agenda-afspraken, maken een

comeback. De aanvallers sturen e-mails met lege kalenderuitnodigingen, waarin een verborgen link is opgenomen die na acceptatie via een herinnering kan leiden naar een phishingpagina. Ook wordt er geëxperimenteerd met CAPTCHA-verificatie om bots te omzeilen. Aangezien steeds meer gebruikers hun accounts beschermen met multi-factor authenticatie (MFA), proberen aanvallers methoden te ontwikkelen om MFA te omzeilen, zoals phishing-sites die zowel wachtwoorden als eenmalige wachtwoorden (OTP's) proberen te stelen. Gebruikers moeten waakzaam blijven bij verdachte e-mailbijlagen en altijd de URL controleren voordat ze inloggegevens invoeren.

Nieuwe phishingaanvallen via valse vacatureaanbiedingen om Facebook-inloggegevens te stelen

Een nieuwe phishingcampagne maakt gebruik van valse vacatureaanbiedingen van bekende merken zoals KFC en Red Bull om inloggegevens voor Facebook te stelen. De aanvallers gebruiken deze valse aanbiedingen, voornamelijk voor de functie van Social Media Manager, om slachtoffers te misleiden. De e-mails bevatten een link naar een nep-website die lijkt op Glassdoor, waar slachtoffers zich moeten aanmelden via hun Facebook- of e-mailaccount. Na het invoeren van hun gegevens krijgen de slachtoffers een nep-inlogscherm voor Facebook te zien, waarna hun inloggegevens worden gestolen. De e-mails maken gebruik van merkimpersonatie en lijken afkomstig van vertrouwde diensten zoals Google Workspace en Microsoft 365. De scam maakt gebruik van slimme tekstgeneratoren om meerdere varianten van berichten te versturen, wat de kans op succes vergroot. Gevaarlijke tekens zijn onder andere verdachte URL's en mismatched afzenderadressen.

Autoriteit Persoonsgegevens waarschuwt tegen AI-chatbots voor stemadvies

De Autoriteit Persoonsgegevens (AP) heeft gewaarschuwd tegen het gebruik van AI-chatbots voor stemadvies. In een recent rapport stelt de privacytoezichthouder dat deze chatbots niet geschikt zijn voor het verstrekken van stemadvies vanwege gebrek aan transparantie, vertekende informatie en ongecontroleerde gegevensbronnen. Volgens de AP kunnen kiezers verkeerde adviezen krijgen, waarbij de bron van de informatie onduidelijk blijft. De chatbots vertonen bovendien een sterke bias ten opzichte van politieke partijen, wat kan leiden tot beïnvloeding van verkiezingsuitslagen, vooral bij grootschalig gebruik. De AP roept ontwikkelaars

op maatregelen te nemen om te voorkomen dat hun systemen voor dit doel worden ingezet. Chatbots die stemadvies geven worden volgens de AI-verordening als "hoogrisicosystemen" beschouwd, waarvoor strikte eisen gelden. De waarschuwing volgt op onderzoek naar vier populaire chatbots: ChatGPT, Gemini, Mistral en Grok.

Europese publieke dns-dienst dns0.eu per direct gestopt

De Europese publieke dns-dienst dns0.eu is per direct stopgezet vanwege een gebrek aan tijd en middelen, zo hebben de oprichters aangekondigd. De dienst werd in 2023 gelanceerd door een Franse non-profitorganisatie en was bedoeld om EU-burgers en organisaties te beschermen tegen cyberdreigingen. De dienst bood ook een "kindvriendelijke" versie die advertenties, porno, piraterij, dating-apps en volwassen YouTube-video's blokkeerde. Het was een samenwerking tussen de oprichters van NextDNS, malwarebestrijder Abuse.ch en registrar Gandi.net. Als alternatief wordt nu DNS4EU, een door de EU aangeboden dns-dienst, aanbevolen. Dns0.eu heeft gebruikers in de problemen gebracht door plotseling offline te gaan, maar biedt geen verdere details over de reden van de stopzetting. De DNS-dienst speelde een cruciale rol in het blokkeren van risicovolle domeinen en sites met schadelijke inhoud.

VK roept bedrijven op om cybersecurity prioriteit van directie te maken

De Britse overheid heeft een open brief gestuurd naar de grootste bedrijven in het Verenigd Koninkrijk, waarin ze oproept om cybersecurity een topprioriteit te maken binnen de directie. Dit besluit is genomen na een reeks ernstige cyberincidenten bij onder andere Jaguar Land Rover, Marks & Spencer, en Transport for London. De Britse autoriteiten benadrukken dat cybersecurity essentieel is voor het voortbestaan van bedrijven en de bredere economie. Ze roepen bedrijven op om drie belangrijke maatregelen te nemen: cybersecurity moet een strategisch onderwerp worden binnen de top van het bedrijf, bedrijven dienen zich aan te melden voor het Early Warning System van de overheid, en ze moeten zorgen dat hun leveranciers voldoen aan de "Cyber Essentials"-normen. Deze oproep werd specifiek gericht aan FTSE 350-bedrijven. Het Britse NCSC heeft deze boodschap vandaag opnieuw benadrukt.

Apple waarschuwt exploit-ontwikkelaar voor gerichte spyware-aanval op iPhone

Apple heeft een ontwikkelaar van iOS-exploits gewaarschuwd dat zijn iPhone het doelwit was van een gerichte spyware-aanval. De ontwikkelaar werkte voor Trenchant, een bedrijf dat overheden ondersteunt bij nationale veiligheidsoperaties. Trenchant is betrokken bij het zoeken naar kwetsbaarheden en het ontwikkelen van exploits voor misbruik. Het is onbekend of de aanval succesvol was, maar de ontwikkelaar was eerder dit jaar ontslagen vanwege vermoedens van informatielekken, wat mogelijk verband houdt met de waarschuwing van Apple. Dit incident is de eerste keer dat een exploit-ontwikkelaar openbaar wordt gewaarschuwd door Apple, hoewel het bedrijf in het verleden meerdere keren waarschuwingen heeft gestuurd naar gebruikers die het doelwit waren van "mercenary spyware". Verdere details over andere waarschuwingen zijn niet bekend.

Verkoop van gedecentraliseerde botnet loader malware op het Dark Web

Op 21 oktober 2025 werd er op het Dark Web melding gemaakt van de vermeende verkoop van een gedecentraliseerde botnet loader malware. Deze malware wordt aangeboden door onbekende actoren die deze software gebruiken om botnets te creëren. Het doel van een botnet is vaak het uitvoeren van Distributed Denial of Service (DDoS)-aanvallen, maar de malware kan ook andere schadelijke activiteiten ondersteunen. De vermelding wijst op de steeds meer geavanceerde technieken die cybercriminelen inzetten om deze botnets te verspreiden en te gebruiken. Aangezien de malware via een gedecentraliseerd netwerk werkt, kan het moeilijker zijn voor beveiligingsmaatregelen om het te detecteren en te stoppen. Deze ontwikkeling benadrukt de voortdurende groei van cyberdreigingen die via het Dark Web worden verhandeld, wat voor organisaties en gebruikers wereldwijd risico’s met zich meebrengt.

Cyberaanval legt Gemeentebestuur Untereisesheim stil

Op maandag 20 oktober 2025 werd de gemeentelijke administratie van Untereisesheim getroffen door een zware cyberaanval. De aanval resulteerde in ernstige verstoringen van de publieke dienstverlening, doordat ransomware de serverdata versleutelde. De gehele IT-infrastructuur werd getroffen, behalve het telefoonsysteem. De gemeente werkt intensief aan het minimaliseren van de gevolgen voor de burgers en het herstellen van de systemen. Er wordt nauw samengewerkt met de Cybersicherheitsagentur Baden-Württemberg en het

Landeskriminalamt om het incident te onderzoeken en de situatie te stabiliseren. De aanval heeft de werking van de gemeentelijke diensten ernstig belemmerd, maar er worden inspanningen geleverd om de getroffen systemen zo snel mogelijk weer operationeel te maken.