Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

11-10-2025:

Volendams ict-bedrijf getroffen door ransomware via beveiligingslek in server

Een ict-bedrijf uit Volendam werd deze week getroffen door een ransomware-aanval. De aanvallers maakten gebruik van een kwetsbaarheid in de server van het bedrijf, waardoor ze toegang kregen tot klantgegevens. Deze gegevens werden vervolgens versleuteld. Het ict-bedrijf meldde dat de aanval op 7 oktober plaatsvond en dat de herstelwerkzaamheden nog gaande zijn. De getroffen klanten werden geïnformeerd, maar het aantal slachtoffers is nog niet bekend. Het bedrijf heeft geen losgeld betaald en de herstelwerkzaamheden zijn inmiddels gestart, waarbij sommige servers opnieuw werden geïnstalleerd en back-ups werden gecontroleerd. Het ict-bedrijf heeft aangifte gedaan bij de politie en de Autoriteit Persoonsgegevens op de hoogte gesteld van het incident.

Hongarije beschuldigd van spionage in de EU: oproep tot sancties tegen Orban-regime

Een recente onthulling heeft aangetoond dat de regering van Viktor Orbán in Hongarije betrokken zou zijn bij een spionagenetwerk in Brussel, waarbij geprobeerd werd invloed uit te oefenen op de hoogste niveaus van buitenlandse regeringen. Het netwerk zou opereren onder de leiding van Orbán en gericht zijn op het vergaren van inlichtingen en het beïnvloeden van besluitvormingsprocessen binnen de EU en NAVO. Critici stellen dat de EU dringend een mechanisme moet ontwikkelen om deze spionageactiviteiten aan te pakken, met harde straffen voor degenen die schuldig worden bevonden aan landverraad of andere schadelijke activiteiten tegen de veiligheid van de EU. De zaak heeft al geleid tot een breed debat over de mogelijke uitsluiting van Hongarije uit belangrijke internationale organisaties, waaronder de EU en NAVO.

Polen beschuldigt Rusland van toegenomen cyberaanvallen op kritieke infrastructuur

Polen heeft aangegeven dat de hoeveelheid cyberaanvallen door Rusland op kritieke infrastructuur aanzienlijk is gestegen. Het Ministerie van Digitale Zaken meldde dat de militaire inlichtingendiensten van Rusland hun middelen voor dergelijke aanvallen dit jaar hebben verdrievoudigd. Van de 170.000 cyberincidenten die dit jaar tot nu toe zijn geregistreerd, wordt een groot aantal toegeschreven aan Russische actoren.

Polen ervaart dagelijks tussen de 2.000 en 4.000 incidenten, waarvan 700 tot 1.000 serieuze dreigingen zijn. Naast water- en rioleringssystemen richt de Russische cyberaanval zich ook steeds meer op de energiesector. Deze toename van Russische cyberactiviteiten komt overeen met fysieke aanvallen, zoals de drone-aanval van 10 september. De Poolse regering beschouwt Rusland als een serieuze bedreiging voor haar nationale veiligheid, vooral gezien de steun van Polen aan Oekraïne en de voortdurende spanningen met Moskou.

Noord-Koreaanse IT-werknemers infiltreren wereldwijd bedrijven voor spionage

Noord-Korea heeft duizenden IT-werknemers wereldwijd ingezet om via vervalste identiteiten te infiltreren in bedrijven. Deze werknemers opereren voornamelijk vanuit landen als China, Rusland en Zuid-Oost Azië, en gebruiken VPN's, virtuele servers en "laptop farms" om hun herkomst te verbergen. Ze verkrijgen freelance- of fulltimebanen via platforms zoals LinkedIn, Upwork en GitHub, waarbij ze gestolen of gehuurde identiteiten en AI-gegenereerde profielfoto’s gebruiken. Eenmaal binnen kunnen ze malware verspreiden, data stelen of afpersing uitvoeren, terwijl ze tevens hun salarissen naar het regime doorsluizen. Microsoft heeft deze operaties gelabeld als "Jasper Sleet" en "Moonstone Sleet", met meer dan 10.000 actieve operaties wereldwijd. De dreiging breidt zich uit naar niet-IT-sectoren, zoals architectuur en industrieel ontwerp, waar toegang tot gevoelige infrastructuur kan leiden tot grotere risico's, waaronder spionage en de omzeiling van sancties.

Actieve exploitatie van kwetsbaarheden in Gladinet en TrioFox aangetroffen

Cyberbeveiligingsbedrijf Huntress heeft actieve exploitatie ontdekt van een niet-gepatchte kwetsbaarheid in de producten Gladinet CentreStack en TrioFox. De zero-day kwetsbaarheid, aangeduid als CVE-2025-11371, maakt het mogelijk om systeembestanden onbedoeld te onthullen en op afstand code uit te voeren. Deze kwetsbaarheid heeft betrekking op alle versies van de software tot en met 16.7.10368.56560. De eerste meldingen van exploitatie werden op 27 september 2025 geregistreerd. De aanval maakt gebruik van een eerder ontdekte kwetsbaarheid in de software, CVE-2025-30406, waarmee een aanvaller op afstand code kan uitvoeren. Gebruikers wordt aangeraden om de "temp" handler in de Web.config-bestanden van de applicatie uit te schakelen om misbruik te voorkomen totdat er een patch beschikbaar is.

Kritieke GitHub Copilot-kwetsbaarheid stelde aanvallers in staat broncode uit privé-repositories te exfiltreren

Een kritieke kwetsbaarheid in GitHub Copilot Chat, beoordeeld met 9,6 op de CVSS-schaal, stelde aanvallers in staat om broncode en geheime gegevens uit privé-repositories onopgemerkt te exfiltreren. De exploit maakte gebruik van een nieuwe techniek voor promptinjectie, gecombineerd met een omzeiling van GitHub's Content Security Policy (CSP), waardoor aanvallers aanzienlijke controle kregen over de Copilot-instantie van het slachtoffer. Ze konden kwaadwillende code of links suggereren en gevoelige informatie, zoals AWS-sleutels, uitlekken. De aanvallen werden uitgevoerd door gebruik te maken van de verborgen "invisible comments"-functie van GitHub, waarmee een kwaadaardige prompt werd ingevoegd. GitHub heeft de kwetsbaarheid op 14 augustus 2025 gepatcht door het uitschakelen van alle afbeeldingsweergave binnen de Copilot Chat-functie.

ZDI onthult dozijn ongepatchte RCE-lekken in Ivanti Endpoint Manager

Beveiligingsbedrijf ZDI heeft twaalf kwetsbaarheden ontdekt in Ivanti Endpoint Manager (EPM), een systeem voor het beheren van laptops, smartphones en servers. Deze kwetsbaarheden, die remote code execution (RCE) mogelijk maken, zijn nog niet gepatcht. Ivanti heeft aangekondigd de beveiligingslekken pas in maart 2026 te zullen verhelpen. Het Zero Day Initiative (ZDI) meldde de kwetsbaarheden in juni 2025 aan Ivanti, waarna het bedrijf drie maanden kreeg om een oplossing te bieden. Elf van de twaalf kwetsbaarheden zijn beoordeeld met een impactscore van 7.2, terwijl de ernstigste een score van 8.8 heeft. Misbruik van de kwetsbaarheden vereist dat de aanvaller geauthenticeerd is of interactie van een gebruiker heeft. In afwachting van een patch adviseert ZDI organisaties om het gebruik van Ivanti EPM te beperken.

Apple verhoogt beloning voor zeroclick-aanvallen op iPhones naar 2 miljoen dollar

Apple heeft de beloning voor onderzoekers die kwetsbaarheden in iPhones ontdekken verhoogd, met een speciale focus op zeroclick-aanvallen. Deze aanvallen vereisen geen gebruikersinteractie en stellen aanvallers in staat om iPhones te compromitteren. De beloning is nu opgelopen tot 2 miljoen dollar, met de

mogelijkheid om meer dan 5 miljoen dollar te verdienen bij het omzeilen van de Lockdown Mode en het vinden van kwetsbaarheden in beta-versies van iOS. Ook zijn de beloningen voor draadloze aanvallen en aanvallen via één klik verhoogd naar 1 miljoen dollar. Apple benadrukt dat dergelijke aanvallen meestal afkomstig zijn van spywareleveranciers en statelijke actoren, die miljoenen dollars investeren in de ontwikkeling van dergelijke technieken. Sinds de lancering van het beloningsprogramma in 2020 heeft Apple meer dan 35 miljoen dollar uitgekeerd aan beveiligingsonderzoekers.

Kritieke XSS-kwetsbaarheid in Juniper Networks Junos Space, patch direct installeren

Een ernstige kwetsbaarheid is ontdekt in Juniper Networks Junos Space, versie < 24.1R4. De kwetsbaarheid, aangeduid als CVE-2025-59978, maakt het mogelijk voor kwaadwillenden om schadelijke scripts op webpagina's op te slaan. Wanneer een bevoegde gebruiker de pagina bekijkt, worden de scripts uitgevoerd, wat kan leiden tot ongeautoriseerde acties op het platform. Dit vergroot het risico op het compromitteren van accounts en het uitvoeren van acties met beheerdersrechten. Organisaties worden geadviseerd om de nieuwste versie van de software te installeren en hun monitoringcapaciteiten te verhogen om verdachte activiteiten tijdig te detecteren. Patching biedt bescherming tegen toekomstige aanvallen, maar kan geen eerdere compromittering herstellen.

Fortra onthult volledige tijdlijn exploitatie CVE-2025-10035 in goanywhere mft

Fortra heeft de bevindingen van hun onderzoek naar CVE-2025-10035, een ernstige kwetsbaarheid in GoAnywhere Managed File Transfer (MFT), onthuld. De kwetsbaarheid werd voor het eerst op 11 september 2025 ontdekt na een melding van een klant. Het bedrijf ontdekte verdachte activiteiten gerelateerd aan de kwetsbaarheid en bracht onmiddellijk een hotfix uit voor versies 7.6.x, 7.7.x en 7.8.x van de software. Op 15 september werden volledig gepatchte versies vrijgegeven. Fortra waarschuwde klanten wiens GoAnywhere-beheerdersconsole toegankelijk was via het publieke internet. De kwetsbaarheid, die te maken heeft met deserialisatie in de License Servlet, kan leiden tot command injectie zonder authenticatie. Hoewel de kwetsbaarheid voornamelijk een risico vormt voor systemen

met een openstaande beheerdersconsole, wordt aanbevolen om de toegang tot deze consoles te beperken en monitoring in te schakelen.

Criminelen stelen via gekaapte Workday-accounts salaris universiteitspersoneel

Criminelen hebben via phishingaanvallen Workday-accounts van personeel bij Amerikaanse universiteiten gekaapt en hun salaris gestolen. De aanvallers stuurden phishingmails naar universiteitsmedewerkers, waarbij links naar man-in-the-middle phishingpagina's werden gestuurd. Deze pagina's verzamelden zowel inloggegevens als MFA-codes. Zodra de aanvallers toegang hadden, logden ze in op het Exchange Online-account van de slachtoffers en verwierven ze toegang tot Workday, waar ze bankrekeningnummers wijzigden naar hun eigen rekening. De aanvallers voegden soms ook hun eigen apparaat toe voor blijvende MFA-toegang. Ze creëerden regels in Exchange Online om e-mails van Workday te verwijderen, waardoor slachtoffers niets bemerkten. Microsoft adviseert het gebruik van phishingbestendige MFA-methoden om deze aanvallen te voorkomen, aangezien de gebruikte techniek ook op andere HR- en salarisplatforms van toepassing kan zijn.

Nieuwe cyberaanval gericht op telecomklanten

In de afgelopen maand is een nieuwe cybercampagne gestart die gericht is op klanten van grote telecomproviders, waaronder Telenet, Vodafone, Proximus en Orange. Deze aanval gaat verder dan de gebruikelijke phishingaanvallen. Slachtoffers die malafide websites bezoeken, downloaden per ongeluk een trojan van de AntiDot-malwarefamilie, die volledige controle over hun apparaat kan overnemen. De malware kan bank- en crypto-applicaties bespioneren, oproepen blokkeren en monitoren, berichten lezen en zelfs elke toetsaanslag registreren. JustGuard heeft reeds de actieve malafide domeinen verwijderd en malwaremonsters gedeeld met de bredere beveiligingsgemeenschap. Ze monitoren tevens nieuwe infrastructuur die met dezelfde groep in verband staat. Een gedetailleerd blogbericht met belangrijke indicatoren van compromittering en technische analyse wordt binnenkort verwacht.

Rondodox-botnet richt zich op 56 kwetsbaarheden in wereldwijd aanvalspatroon

Het RondoDox-botnet is sinds juni 2025 actief en richt zich op 56 kwetsbaarheden in meer dan 30 verschillende apparaten, waaronder DVR’s, NVR’s, CCTV-systemen en

webservers. Deze kwetsbaarheden, waarvan sommige eerder werden onthuld tijdens de Pwn2Own-hackcompetities, zijn vooral n-day flaws die door het botnet worden uitgebuit. Het botnet gebruikt een zogenaamde “exploit shotgun”-strategie, waarbij meerdere kwetsbaarheden tegelijk worden aangevallen, zelfs als de activiteit opvallend luidruchtig is. Onder de kwetsbaarheden die het botnet exploiteert, bevinden zich CVE-2023-1389 (TP-Link Archer AX21 router) en CVE-2024-3721 (TBK). De botnetontwikkelaars maken snel gebruik van exploits die tijdens Pwn2Own-evenementen zijn gepresenteerd. Om zich te beschermen tegen RondoDox en andere botnetaanvallen, wordt aangeraden de nieuwste firmware-updates toe te passen en verouderde apparatuur te vervangen.

Valse CAPTCHA-pagina gebruikt voor het leveren van kwaadaardige payloads

Een verdachte URL is geïdentificeerd die een valse CAPTCHA-verificatiepagina via Cloudflare serveert. Deze site lijkt te worden gebruikt als tussenstation voor de levering van kwaadaardige payloads, waarbij gebruikers worden misleid om schadelijke content te downloaden of uit te voeren. De kans op kwaadaardigheid wordt ingeschat op 50%. De URL in kwestie is https://guard-google[.]com/, welke wordt gemeld als een indicator voor payloadlevering. Het wordt aangeraden om toegang tot deze URL te blokkeren via DNS, proxy en endpointbeveiliging. Verder moeten bedrijven waakzaam zijn voor gebruikersactiviteit met valse CAPTCHA-uitdagingen die vaak worden gebruikt in drive-by malwarecampagnes. Gebruikers moeten worden geïnformeerd over de gevaren van dergelijke CAPTCHA-tactieken die meestal verborgen payload-omleidingen verbergen.

Nieuwe ransomwaregroep TENGU Onion geïdentificeerd op het darkweb

Een nieuwe ransomwaregroep, genaamd TENGU Onion, is recentelijk geïdentificeerd op het dark web. De groep is actief op een onion-site, toegankelijk via het Tor-netwerk, met het doel gegevens van slachtoffers te versleutelen en losgeld te eisen. De identificatie van TENGU Onion werd gedeeld door een bekende bron, Dark Web Informer. De website van de groep is te vinden op een specifieke onion-url die momenteel wordt gemonitord door cybersecurity-experts. Deze nieuwe dreiging komt op het moment dat ransomware-aanvallen wereldwijd blijven toenemen. De betrokkenheid van deze groep vormt een potentieel risico voor organisaties en bedrijven die kwetsbaar zijn voor dergelijke aanvallen. Experts adviseren bedrijven

om waakzaam te blijven en noodzakelijke beveiligingsmaatregelen te treffen om aanvallen van dergelijke groepen te voorkomen.

Lapsus$ Shiny Hunters dreigen met datalekken als losgeld niet wordt betaald

De hackinggroep Lapsus$ Shiny Hunters (SLSH) heeft een PGP-bericht ondertekend waarin ze dreigen vertrouwelijke gegevens van bedrijven openbaar te maken als deze niet betalen. De groep heeft aangegeven dat op 10 oktober 2025, om 23:59 uur New York-tijd, alle bedrijven die hun losgeld niet hebben betaald, worden blootgesteld. Het bericht werd gepost door de Dark Web Informer en bevat links naar een verwijderbare tekst die vermoedelijk meer details bevat over de dreiging. De groep gebruikt doorgaans PGP-signaturen om hun communicatie te authenticeren en heeft eerder meerdere datalekken geëist van bedrijven. Het bericht benadrukt de voortdurende dreiging van ransomware-aanvallen door SLSH en andere cybercriminelen, waarbij bedrijven worden gedwongen om hoge bedragen te betalen om te voorkomen dat gevoelige informatie op het dark web wordt gelekt.

Evolutie van UTA0388's spionagemalware: van HealthKick naar GOVERSHELL

De Chinese dreigingsactor UTA0388 is verantwoordelijk voor een reeks gerichte phishingcampagnes in Noord-Amerika, Azië en Europa. Deze campagnes, die gebruikmaken van volledig gefabriceerde identiteiten en organisaties, zijn ontworpen om de malware GOVERSHELL te verspreiden. Oorspronkelijk werden de phishingmails gestuurd met links naar schadelijke archieven die de malware bevatten. De aanvallen evolueerden naar meer verfijnde technieken, waaronder phishing met rapportopbouw om vertrouwen op te bouwen bij de slachtoffers voordat de kwaadaardige link werd verstuurd. GOVERSHELL, een backdoor die via DLL-side loading wordt geïnstalleerd, heeft verschillende versies die functies uitvoeren via PowerShell, zoals systeeminformatie ophalen en externe servers raadplegen. De aanvaller maakte gebruik van OpenAI's ChatGPT om de inhoud van de phishingmails te genereren, wat aantoont hoe geavanceerd de operaties van UTA0388 zijn. Deze campagne is sterk gericht op Aziatische geopolitieke kwesties, met een bijzondere focus op Taiwan.

175 kwaadaardige npm-pakketten ingezet in phishingcampagne met 26.000 downloads

Onderzoekers hebben 175 kwaadaardige npm-pakketten ontdekt die gebruikt werden voor een phishingcampagne, Beamglea, die zich richt op 135 bedrijven wereldwijd, voornamelijk in de industrie, technologie en energie. De pakketten werden 26.000 keer gedownload en bevatten scripts die slachtoffers omleiden naar inlogpagina's voor het verzamelen van referenties. Deze aanvallen maakten gebruik van npm's publieke registry en unpkg.com's CDN om verdachte JavaScript-bestanden te hosten. Wanneer slachtoffers een speciaal gemaakte HTML-bestand openen, wordt hun e-mailadres doorgegeven aan een phishingpagina, die hen een voorkeursformulier toont met hun eigen gegevens al ingevuld. Dit verhoogt de kans op succes voor de aanvallers. Het misbruik van legitieme infrastructuren zoals npm en unpkg.com illustreert de steeds veranderende technieken van cybercriminelen.

Data-leak sites bereiken een recordhoogte met nieuwe Scattered Spider RaaS en LockBit 5.0

Het ransomware-landschap onderging een ingrijpende verandering in het derde kwartaal van 2025, met de opkomst van het ShinySp1d3r RaaS van Scattered Spider. Dit vertegenwoordigt de eerste grote Engelstalige ransomware-operatie die de Russische dominantie uitdaagt. Tegelijkertijd maakte LockBit zijn comeback met versie 5.0, waarbij kritieke infrastructuren als legitieme doelen werden aangemerkt, wat de traditionele grenzen van ransomware-aanvallen verlegde. Het aantal actieve data-leak sites bereikte een record van 81 in het derde kwartaal, waarbij kleinere, opkomende groepen nu het vacuüm vulden dat door de grotere ransomware-operaties was achtergelaten. Deze verschuiving vergrootte de dreiging en breidde ransomware-aanvallen uit naar nieuwe regio's en sectoren. De integratie van social engineering en geavanceerde encryptie door ShinySp1d3r verhoogde de druk op slachtoffers, die zowel operationeel als financieel werden benadeeld.

Nieuwe polymorfe Python-malware muteert bij elke uitvoering

Een recent ontdekte Python-gebaseerde remote access trojan (RAT), genaamd nirorat.py, vertoont ongekende polymorfe eigenschappen door zijn code elke keer dat hij wordt uitgevoerd te muteren. Het malware-sample werd eerst op VirusTotal ontdekt en kreeg een lage detectiescore van slechts 26/100, ondanks dat het een

volledige suite van RAT-functionaliteiten bevat. De malware maakt gebruik van Python's introspectie- en code-modificatietechnieken om signature-gebaseerde detectie te omzeilen. De mutatie wordt gedreven door functies zoals selfmodifyingwrapper, die de code in geheugen decoderen en reconstrueren zonder een bestandspad achter te laten. De malware wordt voornamelijk verspreid via phishing-e-mails met een ogenschijnlijk onschadelijk Python-script en via gecompromitteerde netwerkschijven. Door zichzelf volledig in geheugen uit te pakken, vermijdt de malware schijfartefacten. Traditionele signatuurtools kunnen dit type dreiging niet effectief detecteren, wat gedragsanalyse en realtime monitoring noodzakelijk maakt.

Phishingcampagne maakt gebruik van Zoom-docs om Gmail-inloggegevens te stelen

Een geavanceerde phishingcampagne richt zich op werkzoekenden door gebruik te maken van legitieme Zoom documentdelingsfuncties. De cybercriminelen doen zich voor als HR-afdelingen en sturen uitnodigingen voor Zoom-documenten, waarmee ze Gmail-inloggegevens proberen te verkrijgen. De aanvallen omzeilen traditionele beveiligingsmaatregelen, zoals SPF, DKIM en DMARC, door e-mails te versturen die van een betrouwbare bron lijken te komen. Slachtoffers ontvangen e-mails die uitnodigen om documenten te bekijken, waarna ze via een reeks kwaadaardige websites naar een vervalste inlogpagina voor Gmail worden geleid. Deze valse pagina ziet er identiek uit aan de officiële Google-loginpagina en wordt gebruikt om inloggegevens in real-time te stelen via WebSocket-verbindingen. Deze techniek maakt het mogelijk om gestolen inloggegevens direct te valideren en accounts snel over te nemen.

SnakeKeylogger via weaponized e-mails gebruikt PowerShell om gevoelige data te stelen

SnakeKeylogger is een geavanceerd infostealer dat gebruik maakt van PowerShell en sociale manipulatie om data te exfiltreren. De malware verspreidt zich via phishing-e-mails die zich voordoen als betaalverzoeken van vertrouwde bedrijven. De bijgevoegde bestanden bevatten een onschuldig lijkende BAT-script die bij uitvoering een PowerShell-payload laadt. Deze payload is ontworpen om toetsaanslagen en systeemgegevens te stelen en te verzenden naar een externe server. De malware maakt gebruik van legitieme Windows-functies en aangepaste

scripts om detectie te vermijden. Het malwareprogramma zorgt voor persistentie door geplande taken en registervermeldingen te creëren, zodat het blijft draaien na herstarts van het systeem. De verkregen informatie wordt in batches verzonden naar een command-and-control server. Geadviseerd wordt om endpointbeveiliging bij te werken en verdachte activiteiten te monitoren.

Stealit-malware misbruikt Node.js Single Executable via nepinstallaties van games en VPN-apps

De Stealit-malware maakt gebruik van een nieuwe functie van Node.js, de Single Executable Application (SEA), om kwaadaardige payloads te verspreiden via vervalste installateurs van games en VPN-applicaties. Deze malware wordt gedistribueerd via bestandsdelingswebsites zoals Mediafire en Discord. SEA stelt Node.js-applicaties in staat om als op zichzelf staande uitvoerbare bestanden te draaien, zonder dat Node.js vooraf geïnstalleerd hoeft te zijn. De malware bevat een remote access trojan (RAT) en ondersteunt onder andere bestandsextractie, webcamcontrole en ransomware. De malware is ontworpen om te draaien zonder detectie, door onder andere anti-analysetechnieken toe te passen en de Microsoft Defender Antivirus uit te schakelen voor specifieke mappen. De malware heeft tot doel gebruikers te infecteren via populaire apps en wordt gecommercialiseerd met prijzen die variëren van $29,99 voor een wekelijkse licentie tot $1.999,99 voor een levenslange licentie.

SonicWall VPN-apparaten misbruikt voor Akira-ransomware-aanvallen

Criminele actoren maken gebruik van kwetsbaarheden in SonicWall SSL VPN-apparaten om Akira-ransomware te verspreiden. Sinds juli 2025 zijn er meerdere incidenten gemeld in Noord-Amerika en EMEA, waarbij aanvallers gebruikmaken van de kwetsbaarheid CVE-2024-40766 in SonicOS-versies tot 7.0.1-5035, wat hen in staat stelt om op afstand code uit te voeren zonder authenticatie. Na toegang tot het netwerk voeren de aanvallers verkenning uit, verzamelen ze inloggegevens en bewegen ze lateraal door het netwerk voordat de ransomware wordt geactiveerd. In de getroffen sectoren, waaronder de maakindustrie, onderwijs en gezondheidszorg, werd vaak eerst data geëxfiltreerd voordat de versleuteling begon. De aanvallers gebruiken ook technieken om hun aanwezigheid in het netwerk te behouden, zoals het hergebruiken van gestolen inloggegevens en het misbruiken van

misconfiguraties. Organisaties wordt aangeraden om de patches van augustus 2024 toe te passen en verdachte externe SSH-verkeer te monitoren.

FBI neemt BreachForums over, gebruikt door ShinyHunters voor Salesforce-extorsie

De FBI heeft gisteravond alle domeinen van het BreachForums-hackerforum in beslag genomen, een platform dat werd gebruikt door de ShinyHunters-groep om gestolen bedrijfsdata te lekken na ransomware- en afpersingsaanvallen. Het forum diende als toegangspunt voor gegevensdiefstal van Salesforce-klanten, zoals bedrijven die weigerden losgeld te betalen. Wetshandhavingsinstanties in de VS en Frankrijk werkten samen om de serverinfrastructuur van het forum in handen te krijgen. Na de inbeslagname bevestigde ShinyHunters via Telegram dat alle back-ups van BreachForums sinds 2023 gecompromitteerd waren. Ondanks de inbeslagname blijft het datalek van de Salesforce-gegevens, waarbij onder andere bedrijven zoals FedEx, Disney en Google betrokken zijn, doorlopen. De criminelen gaven aan geen nieuwe versies van BreachForums te lanceren, maar benadrukten dat dergelijke fora als lokker-sites moeten worden beschouwd.

Discord Zendesk-lek veroorzaakt door omgekochte helpdeskmedewerker

Aanvallers hebben de helpdeskmedewerkers van Discord in Zuidoost-Azië omgekocht om toegang te verkrijgen tot interne systemen van het bedrijf. Eén medewerker accepteerde een bribe van $500, gevolgd door enkele duizenden dollars, wat leidde tot de beveiligingsinbreuk. Het incident heeft blootgelegd hoe kwetsbaar interne systemen kunnen zijn wanneer medewerkers financieel gemotiveerd worden om hun toegangsmacht te misbruiken. De aanval heeft mogelijk gevoelige gegevens blootgesteld en is een voorbeeld van de risico's van menselijke fouten binnen organisaties, zelfs in beveiligingsgevoelige omgevingen zoals die van Discord.

Vermeende verkoop van brute-forcer en checker tool abcproxy.com op het darkweb

Op 9 oktober 2025 werd een tool genaamd abcproxy.com Brute & Checker te koop aangeboden op een dark web forum. Deze tool, gepresenteerd door de gebruiker "Credit card," is ontworpen om CAPTCHA-beveiligingen te omzeilen en kan inlog- en e-mailwachtwoordlijsten controleren. De tool ondersteunt zowel SOCKS5- als HTTP-

proxies en wordt gratis aangeboden via een downloadlink op Mega. In de aanbieding wordt een voorbeeld van de output van de tool getoond, samen met een VirusTotal-link voor de binaire versie van de tool. De verdachte actor biedt geen details over de specifieke slachtoffers of bedrijven die getroffen kunnen zijn door het gebruik van deze tool, en de ernst wordt als laag geclassificeerd. Dit incident benadrukt de voortdurende dreiging van brute-force tools en hun rol in cybercriminaliteit.

Telegram-oprichter waarschuwt voor dreigende dystopie door afname privacy en vrijheid

Pavel Durov, oprichter van Telegram, uit zijn ernstige bezorgdheid over de afnemende privacy en vrijheid in de wereld. Hij waarschuwt dat we ons snel bewegen richting een dystopische toekomst, waarin het vrije internet steeds verder wordt ingeperkt. Durov wijst op bedreigingen zoals de invoering van digitale identiteitsbewijzen, verplichte online leeftijdsverificatie en strengere chatcontrole. Hij benadrukt dat het vrije woord onder druk staat, vooral in Westerse landen waar mensen die kritiek op overheden uiten steeds vaker worden vervolgd. Volgens Durov bevinden we ons in de laatste generatie die nog vrijheden had, die nu snel worden afgenomen. De Telegram-oprichter noemt de situatie zorgwekkend en besluit dat er weinig reden is om zijn verjaardag te vieren, gezien de ernst van de huidige ontwikkelingen.