Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

27-10-2025:

SideWinder Hacking Group maakt gebruik van ClickOnce-infectieketen voor StealerBot malware

De SideWinder hackinggroep heeft een geavanceerde aanvalstechniek ontwikkeld die gebruik maakt van ClickOnce-applicaties om StealerBot malware te verspreiden. In september 2025 werden gerichte aanvallen gedetecteerd tegen diplomatieke en overheidsinstellingen in Zuid-Azië, waaronder Sri Lanka, Pakistan, Bangladesh en India. Deze aanvallen vormen een belangrijke verschuiving in de tactieken van de groep, waarbij de traditionele Microsoft Word-exploits vervangen zijn door een complexere infectieketen via PDF's en ClickOnce-applicaties. De aanvallen werden uitgevoerd via zorgvuldig samengestelde spear-phishing e-mails, die slachtoffers ertoe brachten om een ogenschijnlijk legitiem Adobe Reader-updatebestand te downloaden. Door middel van DLL side-loading van legitieme MagTek binaries wisten de aanvallers beveiligingswaarschuwingen van Windows te omzeilen. De malware, eenmaal geactiveerd, voert geavanceerde spionage-operaties uit, waaronder het verzamelen van systeeminformatie en het exfiltreren van gevoelige data.

Europese dronebedrijven doelwit van Noord-Koreaanse hackers

Een Noord-Koreaanse hackersgroep richt zich op Europese bedrijven die werken aan drone-technologie. De aanvallen, die plaatsvonden in Centraal- en Zuidoost-Europa, maken deel uit van een grootschalige cyberspionagecampagne uitgevoerd door de 'Lazarus-groep', een aan Noord-Korea gelieerde cyberaanvallers. Deze groep is al bekend door eerdere aanvallen, zoals het hacken van Sony en het stelen van cryptovaluta. De aanvallen zijn gericht op het verkrijgen van technische informatie over droneontwerpen, welke mogelijk kunnen bijdragen aan de Noord-Koreaanse droneproductie, die zich richt op het ontleden en nabouwen van bestaande technologie. De hackers gebruiken social engineering om medewerkers van bedrijven te verleiden op schadelijke bestanden te klikken. Bedrijven die betrokken zijn bij de productie van drones, waaronder defensiebedrijven, zijn risicovol doelwit van deze spionage.

Achtduizend Windows WSUS-servers direct toegankelijk vanaf internet

Meer dan achtduizend Windows WSUS-servers zijn direct vanaf het internet bereikbaar, wat een aanzienlijke beveiligingsrisico vormt. Dit werd ontdekt door Eye Security, die het actief misbruik van de kwetsbaarheid CVE-2025-59287 rapporteerde. Via deze kwetsbaarheid kunnen aanvallers op afstand code uitvoeren op de getroffen servers. Microsoft bracht op 14 oktober een update uit, maar deze bleek onvoldoende. Een noodpatch werd op 23 oktober uitgebracht, gevolgd door "security hot patches" voor verschillende versies van Windows Server. Het Nationaal Cyber Security Centrum (NCSC) waarschuwt dat WSUS-servers niet direct vanaf het internet toegankelijk mogen zijn. De Amerikaanse CISA heeft inmiddels een waarschuwing uitgegeven en Amerikaanse overheidsinstellingen opgedragen de patch vóór 14 november te installeren. Het aantal servers dat de noodpatch nog niet heeft geïnstalleerd, is onbekend.

Tenable Proof of Concepts en kwetsbaarheid in WSUS-servers

Tenable heeft een centrale repository van proof of concepts (PoC) gedeeld, waarin onderzoek en ontdekkingen van kwetsbaarheden worden verzameld. Dit GitHub-platform biedt beveiligingsexperts toegang tot praktische voorbeelden van kwetsbaarheden die verder onderzocht kunnen worden. Recent is er wereldwijd melding gemaakt van misbruik van een kwetsbaarheid in de Windows Server Update Services (WSUS), aangeduid als CVE-2025-59287. Deze kwetsbaarheid kan leiden tot remote code execution (RCE) wanneer bepaalde poorten (8530 en 8531) worden blootgesteld. Microsoft heeft op 24 oktober 2025 een update uitgebracht om de kwetsbaarheid te verhelpen. Experts adviseren bedrijven deze patch zo snel mogelijk toe te passen of, indien niet mogelijk, de blootgestelde poorten te blokkeren en de WSUS-serverrol uit te schakelen. De exploitatie van deze kwetsbaarheid is momenteel actief waargenomen in de praktijk.

Smishing Triad linked to 194.000 malicious domains in global phishing operation

Een smishing-operatie, gelinkt aan een groep genaamd de Smishing Triad, maakt gebruik van meer dan 194.000 kwaadaardige domeinen om wereldwijd gebruikers te targeten. De aanval richt zich op verschillende diensten en is financieel zeer winstgevend, met opbrengsten van meer dan $1 miljard in de afgelopen drie jaar. De infrastructuur van de aanval is voornamelijk gehost op populaire Amerikaanse clouddiensten, ondanks dat de domeinen zijn geregistreerd via een Hong Kongse

registrar. De campagne heeft zich uitgebreid naar het vervalsen van diensten zoals tolheffingen, pakketleveringen en bankdiensten, en heeft inmiddels de brokeraccounts van gebruikers als doelwit. De dreiging is groot door de snelheid waarmee domeinen worden geregistreerd en vervangen, wat helpt om detectie te ontwijken. De Smishing Triad maakt gebruik van een gefragmenteerd phishing-ecosysteem waarbij meerdere actoren betrokken zijn, waaronder phishing-kit ontwikkelaars en datamakelaars.

Nieuwe Python RAT vermomd als legitieme Minecraft-app steelt gevoelige gegevens van gebruikers

en nieuwe Python-gebaseerde remote access trojan (RAT) heeft zijn weg gevonden naar de gamegemeenschap, vermomd als een legitieme Minecraft-client. Het malwareprogramma, genaamd Nursultan Client, maakt gebruik van de Telegram Bot API voor commando- en controle-infrastructuur, waardoor aanvallers gegevens van geïnfecteerde machines kunnen stelen en deze op afstand kunnen bedienen. Het programma wordt verpakt met PyInstaller, wat het bestand uitzonderlijk groot maakt (68,5 MB), een techniek die kan helpen om beveiligingssoftware te omzeilen. Na installatie verbergt de malware zijn aanwezigheid door het consolevenster te verbergen en toont een valse installatievoortgangsbalk. Het programma richt zich niet alleen op Discord-authenticatietokens, maar kan ook screenshots maken, de webcam inschakelen en gedetailleerde systeeminformatie verzamelen. De malware lijkt via een Malware-as-a-Service-model te worden verspreid, wat suggereert dat meerdere aanvallers toegang kunnen krijgen tot gepersonaliseerde versies.

Warlock ransomware maakt gebruik van SharePoint ToolShell zero-day kwetsbaarheid

In juli 2025 begon de Warlock ransomwaregroep de kritieke zero-day kwetsbaarheid in Microsoft SharePoint, bekend als CVE-2025-53770, te exploiteren. Deze kwetsbaarheid, ontdekt op 19 juli 2025, werd een belangrijke vector voor de verspreiding van Warlock ransomware wereldwijd. Het gebruik van deze zero-day markeerde een escalatie in de dreigingsomgeving, waarbij bekende exploitatiemethoden werden gecombineerd met nieuwe malwaretactieken. Warlock bleek in juni 2025 voor het eerst te verschijnen, maar de aanvallen begonnen pas echt op te vallen na de exploitatie van de SharePoint kwetsbaarheid. De

ransomwaregroep is bekend om zijn Chinese operationele basis, wat een afwijking is van de traditionele Russische ransomwaregroepen. De aanvallen richtten zich op organisaties uit verschillende sectoren wereldwijd, van ingenieursbedrijven in het Midden-Oosten tot financiële instellingen in de VS. Warlock maakt gebruik van DLL-sideloading en een aangepaste command-and-controlstructuur om persistentie en communicatie te waarborgen.

Cybercriminelen misleiden gebruikers met nep-financiële hulpaanbiedingen

Een wereldwijd netwerk van oplichters, bekend als "Vulnerability Vultures", richt zich op kwetsbare groepen, voornamelijk ouderen, door middel van misleidende financiële hulpaanbiedingen. Deze oplichters maken gebruik van vervalste persona's en impersoneren vertrouwde figuren, zoals de FBI en bekende nieuwsorganisaties, om slachtoffers te lokken. In 2024 werden er door mensen boven de 60 jaar de meeste klachten ingediend bij de FBI, goed voor een verlies van 4,8 miljard dollar. De oplichters benaderen slachtoffers via sociale media en leiden hen vervolgens naar frauduleuze websites waar ze persoonlijke en financiële gegevens verzamelen. De fraudeurs gebruiken kunstmatige intelligentie en vervalste media om een geloofwaardige indruk te maken en de slachtoffers te misleiden. De operaties zijn geografisch divers, met aanwijzingen dat de daders zich bevinden in Nigeria, Zuid-Azië en de VS.

Nieuwe malwareaanval maakt gebruik van variabele functies en cookies om kwaadaardige scripts te verbergen

Een nieuwe geavanceerde malwarecampagne richt zich op WordPress-websites en maakt gebruik van PHP-variabele functies en cookie-gebaseerde obfuscatie om traditionele beveiligingsmechanismen te omzeilen. Deze aanval maakt gebruik van een evolutie in obfuscatie-technieken, waarbij kwaadaardige code wordt verspreid over meerdere HTTP-cookies en dynamisch wordt gereconstrueerd tijdens de uitvoering. Dit maakt statische analyse bijzonder uitdagend, omdat de kwaadaardige intentie verborgen blijft totdat alle cookie-componenten zijn samengevoegd en uitgevoerd. De aanval is in september 2025 meer dan 30.000 keer gedetecteerd, wat wijst op de brede inzet en effectiviteit ervan tegen kwetsbare websites. Het malwareprogramma richt zich voornamelijk op PHP-gebaseerde webapplicaties, vooral WordPress-installaties, en injecteert backdoor-scripts die opdrachten via

speciaal opgezette cookies accepteren. De techniek maakt gebruik van een multi-stage uitvoering om detectie te voorkomen en biedt volledige controle over de getroffen systemen.

Caminho malware loader gebruikt LSB steganografie om .NET payloads te verbergen in afbeeldingsbestanden

Een geavanceerde malware-operatie uit Brazilië maakt gebruik van steganografische technieken om kwaadaardige payloads te verbergen in ogenschijnlijk onschuldige afbeeldingsbestanden. De Caminho-loader, die sinds maart 2025 actief is, vormt een groeiende dreiging voor organisaties in Zuid-Amerika, Afrika en Oost-Europa. De campagne begint met zorgvuldig samengestelde spear-phishing e-mails, die gecomprimeerde archieven bevatten met JavaScript of VBScript-bestanden. Deze scripts maken gebruik van sociale-engineering technieken, zoals valse facturen en offertes, om ontvangers te misleiden. Na uitvoering haalt het script een obfuscerende PowerShell-payload op van Pastebin-achtige diensten, die vervolgens steganografische afbeeldingen van archive.org downloadt. De malware maakt gebruik van Least Significant Bit (LSB) steganografie om verborgen .NET-bestanden uit afbeeldingsbestanden te extraheren. Deze aanpak voorkomt traditionele beveiligingsmaatregelen die afhankelijk zijn van domeinnaamreputatie en blocklists. De campagne maakt gebruik van vertrouwde platforms om de detectie te omzeilen en levert verschillende soorten malware, zoals REMCOS RAT, XWorm en Katz Stealer.

Nieuwe phishingmethode misbruikt Microsoft Copilot Studio om OAuth tokens te stelen

Onderzoekers van Datadog Security Labs hebben een nieuwe phishingtechniek ontdekt, genaamd CoPhish, die misbruik maakt van Microsoft Copilot Studio agents om frauduleuze OAuth-toestemmingsverzoeken te versturen via legitieme Microsoft-domeinen. Aanvallers kunnen kwaadaardige chatagents creëren die gebruikers via een valse aanmeldknop naar schadelijke applicaties leiden, waardoor hun sessietokens worden onderschept. De aanval is bijzonder overtuigend omdat de webpagina’s worden gehost op officiële Microsoft-adressen, waardoor gebruikers minder snel argwaan krijgen. Microsoft erkent het probleem en werkt aan beveiligingsmaatregelen in toekomstige updates. Tot die tijd adviseert het bedrijf

organisaties om beheerdersrechten te beperken, het aanmaken van gebruikersapplicaties uit te schakelen en toestemmingsverzoeken nauwlettend te controleren via Entra ID. De aanval richt zich vooral op beheerdersaccounts, waardoor toegang tot bedrijfsdata en cloudomgevingen kan worden verkregen.

Cybercriminelen richten zich wereldwijd op publieke sectoren en essentiële diensten in gerichte aanvallen

In 2025 blijven ransomware-aanvallen tegen de publieke sector toenemen, ondanks verbeterde bewustwording en verdedigingsmaatregelen. Wereldwijd werden 196 publieke instellingen getroffen door ransomware-campagnes, wat resulteerde in ernstige verstoringen van vitale overheidsdiensten en een verlies van vertrouwen. Deze aanvallen, waarbij de methodes steeds geavanceerder worden, hebben geleid tot een operationele uitvaltijd die tussen 2018 en 2024 wereldwijd 1,09 miljard dollar kostte voor overheidsinstanties. De aanvallers maken vaak gebruik van dubbele afpersingstechnieken, waarbij naast versleuteling van bestanden ook gevoelige data wordt gestolen en gedreigd met publieke onthulling. De VS heeft het hoogste aantal slachtoffers, met 69 getroffen instanties in 2025. Het groeiende aantal aanvallen benadrukt de kwetsbaarheid van overheidsdiensten, die vaak niet de middelen of technische capaciteiten hebben om zich voldoende te beschermen tegen deze bedreigingen.

Nieuwe phishingaanval omzeilt beveiliging met UUID's voor Secure Email Gateways

Een nieuwe, geavanceerde phishingaanval maakt gebruik van willekeurig gegenereerde Universal Unique Identifiers (UUID's) om beveiligingssystemen, zoals Secure Email Gateways (SEGs), te omzeilen. De aanval maakt gebruik van een JavaScript-gebaseerd script dat dynamisch UUID's genereert, samen met een willekeurige domeinkeuze en servergestuurde pagina-vervanging, wat leidt tot succesvolle pogingen om inloggegevens te stelen. In plaats van statische redirects te gebruiken, past de techniek browsergebaseerde manipulaties toe via DOM-modificatie, waardoor phishingpagina's worden weergegeven zonder URL-veranderingen. De kwaadwillende code wordt meestal ingebed in HTML-bijlagen of vervalste platforms zoals Microsoft OneDrive en Adobe Acrobat Sign. De aanval is bijzonder effectief door de personalisatie van de phishingpagina’s, die wordt

aangepast op basis van de context van het slachtoffer, wat het vertrouwen vergroot en de kans op succesvolle gegevensdiefstal verhoogt.

Hackers hijacking IIS-servers met blootgestelde ASP .NET-machine sleutels

Hackers hebben een geavanceerde aanval uitgevoerd op Microsoft IIS-servers, waarbij gebruik werd gemaakt van verouderde kwetsbaarheden in de beveiliging van ASP .NET-machine sleutels. Deze sleutels, die al sinds 2003 openbaar beschikbaar zijn, werden gebruikt om kwaadaardige modules in servers te injecteren, waardoor aanvallers op afstand commando's konden uitvoeren en frauduleuze zoekmachineoptimalisatie konden bedrijven. De aanval richtte zich op ongeveer 240 server-IP-adressen en 280 domeinnamen in verschillende sectoren, waaronder overheidsinstanties, kleine bedrijven en e-commerceplatforms. Na het verkrijgen van toegang tot deze servers, installeerden de aanvallers een rootkit om hun aanwezigheid te verbergen en voerden ze verschillende technieken uit om verhoogde machtigingen te verkrijgen. Deze aanvallen blijken naast de financiële fraude ook ernstigere veiligheidsrisico's te veroorzaken, aangezien ze kunnen leiden tot spionage of andere kwaadwillende activiteiten door derden.

Vault Viper exploiteert online gokwebsites met op maat gemaakte browser om schadelijke software te installeren

Criminele netwerken in Zuidoost-Azië maken gebruik van de bloeiende illegale gokmarkt om kwaadaardige software te verspreiden. Een recent ontdekte campagne richt zich op het Universe Browser-programma, een op Chromium gebaseerde browser die wordt gepromoot als privacytool. De browser wordt via gokwebsites gedistribueerd, die door criminele netwerken worden beheerd. Het doel van de browser is om alle gebruikersverbindingen via servers in China te leiden en tegelijkertijd meerdere kwaadaardige programma's op de achtergrond te installeren. De malware heeft kenmerken van remote access trojans, zoals keylogging en verborgen netwerkverbindingen. De criminele actoren, gelinkt aan de Baoying Group, beheren gokplatforms in Cambodja en de Filippijnen en bedienen zowel legitieme als frauduleuze netwerken. De software bevat geavanceerde anti-analysetechnieken, wat het onderzoek bemoeilijkt.

Hackers gebruiken Telegram Messenger voor gevaarlijke Android-malware

Een geavanceerde backdoor genaamd Android.Backdoor.Baohuo.1.origin is ontdekt in gemanipuleerde versies van de Telegram X-messenger, waarmee aanvallers volledige controle over de accounts van slachtoffers krijgen zonder opgemerkt te worden. De malware verspreidt zich via misleidende advertenties in apps en derde partijen, die zich voordoen als legitieme dating- en communicatiesites. Met meer dan 58.000 besmette apparaten, verspreid over ongeveer 3.000 smartphone-modellen en andere Android-apparaten, vormt dit een serieuze bedreiging voor mobiele malware. De malware steelt vertrouwelijke informatie zoals inloggegevens, wachtwoorden en chatgeschiedenissen en verstopt accountindicatoren. Het maakt gebruik van de Redis-database voor command-and-control-operaties, een techniek die nog niet eerder werd gedocumenteerd in Android-malware. De backdoor maakt het mogelijk om gegevens zoals sms-berichten en contacten te verzamelen, wat de situatie verergert voor slachtoffers die gevoelige informatie verliezen.

LockBit 5.0 valt actief Windows, Linux en ESXi omgevingen aan

LockBit, een bekende ransomware-operatie, is teruggekeerd met de release van versie 5.0, codenaam "ChuongDong". Na maanden van inactiviteit, veroorzaakt door law enforcement-acties in 2024, heeft de groep zijn infrastructuur hersteld en zijn aanvallen hervat. De nieuwe variant richt zich op organisaties over meerdere platforms, met een verbeterde technische aanpak. In september 2025 zijn tientallen organisaties in West-Europa, Amerika en Azië getroffen, waarvan de helft door de LockBit 5.0 variant. Het merendeel van de aanvallen richtte zich op Windows-systemen, terwijl de rest Linux- en ESXi-omgevingen betroffen. LockBit 5.0 maakt gebruik van versleuteling die het detecteren bemoeilijkt en versnelt de versleuteling van bestanden. De aanvallen zijn uitgevoerd door het heropgerichte netwerk van LockBit's Ransomware-as-a-Service-model. LockBitSupp, de beheerder van de groep, heeft nieuwe partners geworven, die toegang krijgen tot encryptietools voor een storting van $500 in Bitcoin.

Hackers stelen Discord-accounts met RedTiger-gebaseerde infostealer

Cybercriminelen gebruiken de open-source RedTiger tool om een infostealer te bouwen die Discord-accountgegevens en betaalinformatie verzamelt. Deze malware kan ook inloggegevens in browsers, gegevens van cryptocurrency-wallets en game-

accounts stelen. RedTiger is oorspronkelijk een penetratietesttool die verschillende modules bevat voor het scannen van netwerken en het kraken van wachtwoorden. De infostealer-component heeft de mogelijkheid om systeeminfo, browsercookies, wachtwoorden en crypto-bestanden te stelen, evenals gegevens van platforms zoals Roblox en Discord. De malware kan ook screenshots maken van het bureaublad van het slachtoffer. Na het verzamelen van de gegevens worden deze geüpload naar een cloudopslagservice en ontvangen de aanvallers een downloadlink via een Discord-webhook. De tool kan worden verspreid via Discord-kanalen, malwaresites en sociale netwerken. Gebruikers wordt aangeraden Discord-tokens in te trekken, wachtwoorden te wijzigen en multi-factor authenticatie in te schakelen om zichzelf te beschermen.

Twee tieners aangeklaagd voor £39 miljoen TfL-cyberaanval

Twee tieners zijn aangeklaagd voor hun vermeende betrokkenheid bij een cyberaanval op Transport for London (TfL) in 2024. Thalha Jubair (19) uit Oost-Londen en Owen Flowers (18) uit Walsall staan terecht voor samenspanning om ongeautoriseerde handelingen te verrichten volgens de Computer Misuse Act. De aanval, die op 31 augustus 2024 begon, veroorzaakte drie maanden verstoringen bij TfL, inclusief problemen met live-informatie van de metro, reisgeschiedenis en betalingen via de Oyster-app. De National Crime Agency beschuldigt de hackgroep ‘Scattered Spider’ van de aanval. TfL schat de schade op £39 miljoen, en ongeveer 5.000 klanten werden gewaarschuwd dat hun persoonlijke gegevens, zoals bankrekeningnummers en e-mailadressen, mogelijk zijn bekeken. De tieners werden op 16 september 2024 gearresteerd en hun rechtszaak is gepland voor juni 2026.

Verkoop van 200.000 inloggegevens op darkweb treft gamediensten

Op het darkweb wordt een dataset met naar schatting tweehonderdduizend gestolen inloggegevens te koop aangeboden. De combinatie van gebruikersnamen en wachtwoorden lijkt afkomstig van populaire online platforms zoals Roblox, Steam en Valorant. Volgens meldingen van Dark Web Informer worden dergelijke gegevens vaak gebruikt voor accountovername, identiteitsfraude en de verkoop van virtuele items binnen games. De herkomst van de gegevens is nog niet bevestigd, maar het risico bestaat dat slachtoffers hun accounts verliezen of dat aanvallers toegang krijgen tot gekoppelde betaalgegevens. Dit soort grootschalige credential-

combinaties duidt op voortdurende phishing- en malwarecampagnes gericht op gamers en hun online profielen. Gebruikers van de genoemde diensten wordt geadviseerd hun wachtwoorden te wijzigen en waar mogelijk multifactorauthenticatie te activeren.

PVV-Kamerleden verspreiden heimelijk AI-beelden van Timmermans; tientallen doodsbedreigingen tot gevolg

Twee PVV-Kamerleden plaatsten op een populaire Facebookpagina AI-gegenereerde beelden van Frans Timmermans, waarbij hij werd afgebeeld in een arrestatiesituatie. Deze beelden, die nauwelijks van echte foto's te onderscheiden waren, lokten tientallen doodsbedreigingen uit richting Timmermans. De beelden werden gepost op een Facebookpagina die dagelijks honderdduizenden mensen bereikte. GroenLinks en PvdA hebben aangifte gedaan tegen de Kamerleden wegens laster en bedreigingen. Volgens experts is het verspreiden van dergelijke nepbeelden een strafbaar feit, omdat het doelbewust de reputatie van Timmermans aantast. De pagina werd kort na het onderzoek van de Volkskrant offline gehaald. Experts beschouwen dit incident als een ernstig dieptepunt voor de parlementaire democratie, waarbij het vertrouwen in de politiek verder wordt aangetast.