Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

01-11-2025:

Ransomware-aanval op VZW Avalon (B)

VZW Avalon, een kleinschalige zorgvoorziening in Buggenhout, België, die zorg op maat biedt voor mensen met een beperking, is slachtoffer geworden van een ransomware-aanval door de Incransom ransomwaregroep. De instelling richt zich op persoonlijke begeleiding en een aangepaste omgeving om de bewoners optimaal te ondersteunen. De aanval werd ontdekt op 31 oktober 2025, waarbij 38.554 bestanden werden versleuteld, met een totale bestandsgrootte van meer dan 31 gigabyte. De ransomwaregroep heeft de verantwoordelijkheid voor de aanval opgeëist, en er is aangegeven dat gevoelige gegevens mogelijk zijn blootgesteld.

Chinese hackers gebruiken Windows zero-day om Europese diplomaten te bespioneren

Een Chinese hackinggroep maakt gebruik van een zero-day kwetsbaarheid in Windows om Europese diplomaten te bespioneren. De aanvallen richten zich op diplomaten in landen zoals Hongarije, België en andere Europese landen. De aanvallen beginnen met spearphishing-e-mails die leiden naar schadelijke LNK-bestanden die een Windows-kwetsbaarheid (CVE-2025-9491) uitbuiten. Deze bestanden installeren de PlugX-remote access trojan (RAT) malware, waarmee de aanvallers toegang krijgen tot systemen en gevoelige gegevens kunnen stelen. De aanvallen zijn toegeschreven aan de Chinese APT-groep UNC6384, ook bekend als Mustang Panda, die eerder betrokken was bij spionagecampagnes gericht op diplomatieke doelwitten in Zuidoost-Azië. Het gebruik van de kwetsbaarheid is wereldwijd verspreid, met meerdere staten en cybercriminelen die deze kwetsbaarheid actief uitbuiten. Microsoft heeft tot nu toe geen officiële patch voor de zero-day uitgebracht, ondanks eerdere waarschuwingen.

Nieuwe hacktivistenalliantie aangekondigd tussen OverFlame en M.O.L.O.T.

De hacktivistische groepen OverFlame en M.O.L.O.T., beide afkomstig uit Rusland, hebben hun nieuwe alliantie aangekondigd, waarmee zij hun krachten bundelen voor gezamenlijke cyberaanvallen. De twee groepen hebben een lange geschiedenis van aanvallen op zowel commerciële als overheidsinstellingen, en de samenwerking tussen hen zal waarschijnlijk leiden tot een verhoogd aantal cyberaanvallen. Dit

nieuwe bondgenootschap kan de dreiging voor organisaties wereldwijd vergroten, aangezien beide groepen bekend staan om hun geavanceerde aanvalsmethoden en politieke doelstellingen. De aankondiging van de alliantie werd via sociale kanalen gedeeld, en er wordt verwacht dat de samenwerking strategisch gericht zal zijn op het verstoren van infrastructuren en het destabiliseren van systemen die zij als vijandig beschouwen.

Amerikaanse overheid bevestigt actief misbruik van VMware-lek

Het Amerikaanse Cybersecurity & Infrastructure Security Agency (CISA) heeft bevestigd dat aanvallers actief misbruik maken van een kwetsbaarheid in VMware Aria Operations en VMware Tools. Deze kwetsbaarheid, bekend als CVE-2025-41244, werd ontdekt in mei 2025 door het securitybedrijf Nviso, dat meldde dat de kwetsbaarheid al sinds oktober 2024 werd gebruikt door de aanvallersgroep UNC5174. Deze groep, die vermoedelijk banden heeft met China, kan via de kwetsbaarheid code als root uitvoeren op een virtual machine. VMware bracht eind september een beveiligingsupdate uit, maar pas na de bevestiging van actief misbruik door CISA werd de dreiging breder erkend. Het Amerikaanse ministerie van Binnenlandse Veiligheid heeft federale overheidsinstanties opgedragen de update vóór 20 november 2025 te installeren.

Massale toename van NFC-relay malware steelt Europese creditcards

NFC-relay malware, die contactloze creditcardinformatie steelt, is de afgelopen maanden snel populair geworden in Oost-Europa. Onderzoekers ontdekten meer dan 760 kwaadaardige Android-apps die deze techniek gebruiken. In tegenstelling tot traditionele banktrojans, maakt NFC-malware gebruik van de Host Card Emulation (HCE) van Android om betaalgegevens te stelen. De malware kan EMV-velden vastleggen, reageren op commando's van betaalterminals en zelfs gegevens naar externe servers sturen om betalingen te doen zonder dat de fysieke kaarthouder aanwezig is. Deze aanvallen zijn voor het eerst opgemerkt in Polen in 2023 en zijn sindsdien verder verspreid naar landen zoals de Tsjechische Republiek, Rusland en Slowakije. Gebruikers wordt aangeraden geen APK’s van buiten de Google Play Store te installeren en regelmatig hun apparaten te scannen met Play Protect.

Linux-kwetsbaarheid geëxploiteerd in ransomware-aanvallen

De Cybersecurity and Infrastructure Security Agency (CISA) heeft bevestigd dat een kritieke privilege-escalatiekwetsbaarheid in de Linux-kernel wordt misbruikt in ransomware-aanvallen. De kwetsbaarheid, aangeduid als CVE-2024-1086, werd in januari 2024 openbaar gemaakt en betreft een use-after-free-fout in de netfilter:nf_tables-kernelcomponent. Hoewel de kwetsbaarheid al in januari 2024 werd gepatcht, wordt deze nu actief gebruikt door ransomwaregroepen. Aanvallers met lokale toegang kunnen hierdoor hun privileges verhogen en mogelijk root-toegang verkrijgen, wat leidt tot systeemovername, gegevensdiefstal en netwerkbewegingen. CISA heeft federale agentschappen opgedragen de systemen te beveiligen, met mitigaties zoals het blokkeren van nf_tables of het beperken van de toegang tot gebruikersnamespaces. Deze kwetsbaarheid heeft invloed op verschillende Linux-distributies, waaronder Debian, Ubuntu en Red Hat.

ClearFake JavaScript Payload Delivered via Compromised Domain

Op 30 oktober 2025 werd een nieuw domein, p2t.lo9q.online, gelinkt aan de ClearFake JavaScript-payload leveringscampagne. Dit domein werd gebruikt om een schadelijke JavaScript-payload te verspreiden via een browser-gebaseerd social engineering hulpmiddel, dat gebruikers misleidt door zich voor te doen als een legitieme beveiligingsupdate van populaire browsers zoals Chrome, Edge en Firefox. Het domein heeft momenteel een 404-respons, wat aangeeft dat de kwaadaardige bestanden mogelijk zijn verwijderd of verplaatst. De malware is gericht op het installeren van kwaadaardige executables. Ter verdediging wordt aangeraden alle verkeer naar dit domein te blokkeren en browsergebaseerde bescherming te implementeren om valse update-oproepen te detecteren. Ook wordt aanbevolen recente webverkeer- en endpoint-telemetrie te controleren op verdachte gedownloade bestanden.

China-Linked Tick Group Exploits Lanscope Zero-Day to Hijack Corporate Systems

De Tick groep, een door China gelinkte cyberespionagegroep, maakt misbruik van een recent onthulde kwetsbaarheid in Lanscope Endpoint Manager (CVE-2025-61932) om toegang te krijgen tot bedrijfsnetwerken. Deze kwetsbaarheid, met een CVSS-score van 9.3, maakt het mogelijk voor aanvallers om met systeemrechten willekeurige commando’s uit te voeren op kwetsbare systemen. Het gebruik van deze

zero-day kwetsbaarheid heeft geleid tot de installatie van een backdoor op getroffen machines, waarmee de aanvallers op afstand kwaadwillige commando's kunnen uitvoeren. De malware die in de aanval wordt gebruikt, genaamd Gokcpdoor, zorgt voor een verborgen communicatiekanaal tussen het geïnfecteerde systeem en een externe server. Naast Gokcpdoor werden ook andere technieken ingezet, zoals het zijladen van DLL-bestanden en het gebruik van het Havoc post-exploitatie-framework om laterale bewegingen en data-exfiltratie te vergemakkelijken. Organisaties worden geadviseerd om kwetsbare Lanscope-servers bij te werken en te controleren of ze onterecht aan het internet zijn blootgesteld.

Nieuwe Airstalk-malware voor Windows maakt gebruik van geavanceerde C2-communicatie om inloggegevens te stelen

Een nieuwe malwarefamilie voor Windows, Airstalk, heeft geavanceerde technieken ontwikkeld om gevoelige gegevens van browsers te stelen via een innovatieve, geheime command-and-control (C2)-communicatie. Deze malware, beschikbaar in PowerShell- en .NET-varianten, maakt misbruik van bestaande infrastructuur voor mobiele apparaatbeheer (MDM) door de AirWatch API, nu bekend als Workspace ONE Unified Endpoint Management, te kapen. Het gebruikt een versleuteld 'dead drop'-mechanisme om gegevens uit te wisselen zonder directe verbinding tussen aanvaller en slachtoffer. De malware richt zich op browsergegevens zoals cookies en bladwijzers. Airstalk onderscheidt zich van andere informatie-stelende malware door zijn vermogen om te functioneren binnen vertrouwde systeembeheertools, wat het moeilijker maakt om op te sporen. De .NET-variant maakt gebruik van een multi-threaded C2-architectuur, wat het mogelijk maakt meerdere taken parallel uit te voeren.

Nieuwe Lampion Stealer gebruikt ClickFix-aanval om stilletjes inloggegevens te stelen

Een nieuwe campagne maakt gebruik van de Lampion banking trojan, die sinds 2019 actief is, maar nu gericht is op Portugese financiële instellingen. De dreigingsactoren achter deze aanvallen hebben hun tactieken verfijnd door gebruik te maken van ClickFix-lures, een misleidende techniek waarbij gebruikers worden verleid om technische problemen op te lossen voordat ze schadelijke payloads uitvoeren. De aanval begint met zorgvuldig opgestelde phishingmails die legitieme

bankoverboekingsmeldingen nabootsen. De berichten bevatten ZIP-bestandbijlagen in plaats van directe links, wat een wijziging is in de tactiek van de groep. Het gebruik van geavanceerde sociale-engineeringtechnieken maakt het steeds moeilijker om deze aanvallen op te sporen. De malware wordt via een complexe infectieketen verspreid, die gebruik maakt van obfuscerende scripts en DLL-bestanden om toegang tot systemen te krijgen. De campagne is actief en op grote schaal, met honderden besmette systemen die onder controle van de aanvallers staan.

Phishingcampagne richt zich op financiële en overheidsorganisaties in Azië

Een geavanceerde phishingcampagne richt zich op financiële en overheidsorganisaties in Oost- en Zuidoost-Azië. De campagne maakt gebruik van meertalige ZIP-bestanden als lokmiddel, gecombineerd met regionale malware-sjablonen om gebruikers te misleiden. Er worden drie clusters geïdentificeerd in traditionele Chinese, Engelse en Japanse varianten, die specifiek gericht zijn op geografische en sectorale doelen. Dit toont een verschuiving naar een schaalbare en geautomatiseerde infrastructuur die meerdere regio's tegelijkertijd kan aanvallen. De aanvallers hebben hun methode verfijnd door gebruik te maken van op maat gemaakte domeinen en regionale identificatoren, zoals “tw” voor Taiwan. De infectiemechanismen zijn ontworpen om traditionele e-mail- en webfilters te omzeilen, waarbij JavaScript wordt gebruikt om IP-adressen en gebruikersinformatie te registreren. Het achterliggende netwerk is gehost op Kaopu Cloud HK, met servers in Tokio, Singapore en Hong Kong, wat de attributie en blokkering bemoeilijkt.

Kimsuky en Lazarus hacker groepen onthullen nieuwe tools voor backdoor en remote access

De Noord-Koreaanse hacker groepen Kimsuky en Lazarus hebben geavanceerde malware tools geïntroduceerd waarmee ze persistent toegang kunnen krijgen tot besmette systemen. Kimsuky gebruikt de HttpTroy malware, terwijl Lazarus een verbeterde versie van BLINDINGCAN inzet. De campagnes van deze groepen omvatten geavanceerde social engineering technieken en gebruik van geëncrypteerde communicatienetwerken om detectie te ontwijken. Kimsuky richtte zich op een Zuid-Koreaanse organisatie, waarbij ze een ZIP-bestand gebruikten dat zich voordeed als een VPN-factuur. Lazarus aanvallen waren gericht op twee

Canadese bedrijven, waarbij ze nieuwe methoden toepasten voor het verbergen van de malware en het verkrijgen van langdurige toegang. Beide aanvallen tonen de voortdurende evolutie van staatssponserde cyberoperaties.

Ierland levert verdachte achter aanvallen met Conti-ransomware uit aan VS

Ierland heeft een 43-jarige Oekraïner, verdacht van het uitvoeren van aanvallen met de Conti-ransomware, uitgeleverd aan de Verenigde Staten. De verdachte werd in 2023 door de Ierse politie aangehouden. Volgens de FBI zijn meer dan duizend organisaties wereldwijd getroffen door deze ransomware, waarbij ten minste 150 miljoen dollar aan losgeld werd betaald. De Conti-ransomware wordt vaker ingezet tegen vitale infrastructuren dan andere ransomware. De verdachte wordt aangeklaagd voor computerfraude en wire fraud, waarvoor hij zware gevangenisstraffen kan krijgen. De Amerikaanse overheid had in 2022 nog een beloning van 10 miljoen dollar uitgeloofd voor informatie over de leden van de Conti-groep.

Vier verdachten aangehouden dankzij oplettende meldster

Een 32-jarige vrouw uit Leiden heeft via haar oplettendheid bijgedragen aan de aanhouding van vier verdachten die betrokken waren bij zes babbeltrucs. De vrouw kreeg op 25 juli een telefoontje van iemand die zich voordeed als bankmedewerker en vertrouwde het niet. Terwijl ze met de oplichter sprak, waarschuwde ze de politie. Twee verdachten, een 19-jarige man en een 21-jarige man uit Amsterdam, werden kort daarna aangehouden. Onderzoek toonde aan dat zij betrokken waren bij vijf andere oplichtingen. Ook werd duidelijk dat deze twee mannen werden aangestuurd door twee andere verdachten, een 23-jarige man uit Almere en een 26-jarige man uit Amsterdam. Deze twee werden eind oktober gearresteerd. Tijdens de aanhoudingen werd een dure auto in beslag genomen. De politie waarschuwt voor babbeltrucs en adviseert altijd 112 te bellen bij vermoedelijke oplichters.

Ontwikkelaars Meduza Stealer gearresteerd in Rusland

Drie jonge IT-specialisten zijn gearresteerd in de regio Moskou, beschuldigd van het ontwikkelen en distribueren van de Meduza Stealer, een infostealer malware. De arrestaties volgden na een aanval in mei 2025 op een overheidsinstelling in de regio

Astrakhan, waarbij vertrouwelijke gegevens werden gestolen. De cybercriminelen schonden een ongeschreven regel binnen de Russische cybercriminaliteit door binnenlandse doelen aan te vallen. Meduza Stealer werd in 2023 gelanceerd als een Malware-as-a-Service (MaaS) en verkocht voor 199 dollar per maand of 1.199 dollar voor levenslange toegang. De malware is ontworpen om zich niet uit te voeren op systemen in Rusland of andere landen van de GOS, maar werd aangepast voor de aanval in Astrakhan. De gestolen gegevens omvatten onder andere inloggegevens, cryptocurrency-wallets, wachtwoordmanagers en 2FA-gegevens. De politie heeft apparatuur, mobiele apparaten en bankkaarten in beslag genomen.

Nepagent uit Capelle aan den IJssel aangehouden na langlopend onderzoek

De politie heeft op 29 oktober een 24-jarige man uit Capelle aan den IJssel aangehouden op verdenking van diefstal, oplichting, computervredebreuk en witwassen. De verdachte maakt deel uit van een groep nepagenten die actief was in heel Nederland. Na zijn arrestatie werden doorzoekingen verricht in Rotterdam Zuid en Capelle aan den IJssel, waarbij diverse goederen in beslag werden genomen. Deze aanhouding is de zevende in een serie van vergelijkbare gevallen. De man wordt voorgeleid aan de rechter-commissaris. Nepagenten benaderen slachtoffers vaak telefonisch, met persoonlijke informatie, en zetten hen onder druk om waardevolle spullen te verstrekken. De politie waarschuwt om verdachte situaties altijd direct te melden en voorziet slachtoffers van preventietips om verdere schade te voorkomen.

Australië waarschuwt voor Cisco-routers besmet met Badcandy-malware

De Australische overheid heeft organisaties gewaarschuwd voor Cisco-routers en switches die besmet zijn met de "Badcandy" malware. Deze malware is een webshell die aanvallers in staat stelt om toegang te krijgen tot besmette Cisco-apparaten. De infectie maakt gebruik van een kwetsbaarheid in Cisco IOS XE, genaamd CVE-2023-20198, die aanvallers de mogelijkheid biedt om een account met beheerdersrechten aan te maken. Dit kan hen volledige controle over het systeem geven. Ondanks dat Cisco in oktober 2023 beveiligingsupdates uitbracht, zijn er in Australië nog steeds besmette apparaten, hoewel het aantal gevallen is afgenomen. De Australische overheid benadrukt het belang van het installeren van de beveiligingsupdate en het

controleren van Cisco-apparaten op mogelijke aanvallers. Eerder dit jaar werd een telecombedrijf in Canada via dezelfde kwetsbaarheid aangevallen.

Historische breuk in de Grote Firewall van China: 500GB censuurdata gelekt

In september 2025 werd meer dan 500 GB aan interne gegevens van de Grote Firewall van China gelekt, wat wordt beschouwd als een van de meest ingrijpende beveiligingsincidenten in de digitale surveillancesector. Het lek bevatte meer dan 100.000 documenten, waaronder broncode, werklogs, configuratiebestanden, e-mails, technische handleidingen en operationele documenten van bedrijven die betrokken waren bij de censuurinfrastructuur van China. Het blootgestelde materiaal biedt ongekende inzichten in de werking van China's digitale surveillancesysteem, inclusief IP-toegangslogs van staatsbedrijven zoals China Telecom en China Unicom. Daarnaast onthult het lek kwetsbaarheden binnen het gedistribueerde handhavingsmodel van de Grote Firewall, met instances van lekken van buitenlandse IP-adressen en vertragingen in het doorvoeren van regels. Dit incident biedt voor het eerst gedetailleerde blauwdrukken van China's censuursysteem.

Australische politie achterhaalt seed phrase van verdachte via decoderen nummerreeks op foto

De Australische politie heeft de seed phrase van een verdachte kunnen achterhalen door een foto op zijn telefoon te analyseren, waarop een nummerreeks stond die toegang gaf tot een cryptowallet met vijf miljoen euro aan cryptovaluta. De verdachte weigerde de toegang tot de wallet te verstrekken, waarop de politie forensisch onderzoek instelde. Ze ontdekten dat de foto een reeks getallen bevatte, verdeeld in groepen van zes, die oorspronkelijk waren gewijzigd door de verdachte om de toegang te bemoeilijken. Na het verwijderen van het eerste getal uit elke reeks, kon de volledige recovery seed phrase van 24 woorden worden gedecodeerd. De wallet werd in beslag genomen, en als de verdachte wordt veroordeeld, zal de cryptovaluta naar de Australische overheid gaan.

Belgische politie meldt toename oplichting via AnyDesk

De Belgische politie meldt een aanzienlijke stijging van oplichtingen waarbij het programma AnyDesk wordt misbruikt. De laatste dagen wordt er zelfs tot zes keer

per dag melding gemaakt van dit soort incidenten. In een geval verloor een oudere vrouw 50.000 euro door deze methode. AnyDesk is software waarmee op afstand computers en smartphones kunnen worden beheerd, en wordt vaak door IT-specialisten gebruikt. Helaas maken oplichters nu gebruik van dit legale platform om slachtoffers te bedriegen. Ze vragen slachtoffers om AnyDesk te installeren, waarna ze toegang krijgen tot persoonlijke systemen en bankgegevens. De politie waarschuwt om alleen software te installeren van vertrouwde bronnen en benadrukt dat slachtoffers de software niet moeten verwijderen, maar het systeem aan de politie moeten overdragen voor onderzoek.