Cybercrimeinfo - cyberdreigingsanalyse (Openbare versie)

10-11-2025:

Russische hackers richten steeds meer cyberaanvallen op België

België is een steeds vaker doelwit van cyberaanvallen, voornamelijk uitgevoerd door natiestaten zoals Rusland. Dit blijkt uit het jaarlijkse rapport van Microsoft over cybercriminaliteit. Van alle aanvallen wereldwijd die Rusland werd toegeschreven, was 5 procent gericht op België. Vorige week werden onder andere Proximus, Scarlet en het UZ Gent getroffen door aanvallen. Hackers, waaronder ‘hacktivisten’, voeren veelal DDoS-aanvallen uit, waarbij ze systemen overbelasten zonder toegang te krijgen tot interne gegevens. Deze aanvallen dienen niet alleen om de economie te verstoren, maar ook om politieke boodschappen uit te dragen. Daarnaast blijkt dat AI steeds vaker wordt ingezet door cybercriminelen, bijvoorbeeld om phishingmails te verbeteren en gerichter te maken, wat de dreiging vergroot. Microsoft raadt aan om veiligheidsmaatregelen zoals tweestapsverificatie en het up-to-date houden van software te hanteren om dergelijke aanvallen te voorkomen.

Russische tussenpersonen betrokken bij drone-incidenten

Een complex netwerk van tussenpersonen, variërend van Russische geheime agenten tot kleine criminelen, speelt een cruciale rol in drone-incidenten. Deze tussenpersonen fungeren als schakel tussen opdrachtgevers, waaronder staten en criminelen, en de uiteindelijke uitvoerders van de dreigingen. Het artikel onderzoekt hoe deze schimmige keten van bemiddelaars niet alleen militaire en politieke conflicten beïnvloedt, maar ook de opkomst van illegale drone-activiteiten in Europa, waar dergelijke drones gebruikt worden voor spionage en sabotage. Er wordt opgeroepen tot een internationale samenwerking om deze keten van tussenpersonen te identificeren en te verstoren.

Noord-Korea dreigt met acties als reactie op cybergerelateerde sancties en VS-Zuid-Korea gesprekken

Noord-Korea heeft gedreigd agressievere militaire acties te ondernemen als reactie op de beveiligingsgesprekken tussen de Verenigde Staten en Zuid-Korea. De Noord-Koreaanse minister van Defensie, No Kwang Chol, verklaarde dat het land sterker zal reageren op de "bedreigingen" van de VS, met als doel de veiligheid te waarborgen en de vrede te verdedigen. No reageerde op de komst van een nucleair

aangedreven vliegdekschip van de VS naar de haven van Busan in Zuid-Korea, wat volgens hem de spanningen op het Koreaanse schiereiland verhoogde. Hij bekritiseerde ook het gezamenlijke bezoek van de Amerikaanse en Zuid-Koreaanse defensieministers aan de gedemilitariseerde zone. Deze kritiek volgt op de lancering van een ballistische raket door Noord-Korea, nadat de VS nieuwe sancties hadden opgelegd aan Noord-Koreaanse individuen die betrokken waren bij cybercriminaliteit.

DDoS-aanval door HEZI RASH gericht op Belgische websites

Op 8 november 2025 heeft de hackercollectief HEZI RASH bekendgemaakt dat het meerdere websites in België heeft aangevallen. De getroffen sites omvatten onder andere de Water Service Company, WaaS, AquaFlanders, het Biosafety Advisory Council (BAC) en het Citizen Dialogue platform in Oost-België. De aanvallen betroffen Distributed Denial of Service (DDoS) aanvallen, waarbij de websites tijdelijk onbereikbaar waren door overbelasting van het netwerkverkeer. DDoS-aanvallen zijn een veelgebruikte tactiek bij cyberaanvallen, waarbij servers worden overspoeld met verzoeken om de toegang tot een website te verstoren. Er zijn nog geen meldingen van schade aan gevoelige gegevens of systemen. De aanval komt op een moment waarop cyberdreigingen in België een groeiende zorg zijn.

Van Russische geheim agenten tot kleine criminelen: de schimmige keten van tussenpersonen achter drone-incidenten

In maart 2024 werd een loods in Londen in brand gestoken door Dylan Earl, een kleine crimineel die via Telegram werd gerekruteerd door de Wagnergroep, een paramilitaire organisatie die wordt gecontroleerd door Rusland. Earl ontving een betaling van 10.000 euro voor de brandstichting, een voorbeeld van hoe Rusland gebruik maakt van zogenaamde 'disposable agents'. Deze agents, vaak onwetend over de Russische betrokkenheid, worden voor kleine taken ingezet, zoals het besturen van drones voor sabotageacties. De criminele netwerken die dit mogelijk maken, gebruiken cryptomunten om de anonimiteit van de opdrachtgevers te waarborgen. Europese inlichtingendiensten hebben vastgesteld dat Russische veiligheidsdiensten vaker criminele netwerken inzetten voor deze hybride oorlogsvoering, met als doel angst te zaaien en besluitvormingsprocessen in Europa te beïnvloeden.

Van Russische geheim agenten tot kleine criminelen: de schimmige keten van tussenpersonen achter drone-incidenten. De vele drone-incidenten in ons land (B) zijn het werk van Moskou. Daar lijken analisten, beleidsmakers en inlichtingendiensten het over eens. Maar hoe? Wie voert uit, wie trekt aan de touwtjes? Een verhaal van motorbendes, cryptomunten en een eindeloze reeks tussenpersonen. In de nacht van 20 maart van vorig jaar reed Dylan Earl, een kleine drugdealer met nood aan cash, samen met drie handlangers die hij inderhaast bijeen had geraapt, in een rode Kia Picanto richting Cromwell Industrial Estate, een industriepark in het noordoosten van Londen. Ze parkeerden hun auto, namen een jerrycan benzine en klommen over een muur. De loods die ze viseerden, werd gebruikt door een bedrijf dat materiaal naar Oekraïne stuurt. Meer dan een miljoen euro aan communicatieapparatuur ging in vlammen op. Twee weken geleden werd Dylan Earl veroordeeld tot zeventien jaar cel voor de brandstichting. Hem was 9.000 pond – een goeie 10.000 euro – beloofd voor de job. Hij werd gerekruteerd via de berichtendienst Telegram, door een account dat leidde naar de Wagnergroep, de paramilitaire organisatie die gecontroleerd wordt door de Russische staat. Earl was, zoals Kenneth Lasoen, expert inlichtingendiensten (Universiteit Antwerpen), het benoemt, een disposable agent. Een wegwerpagent.

Als deze week opnieuw drones zoemen boven Zaventem en Kleine-Brogel, als die luchtverkeer lamleggen en defensieministers in hoogste staat van alertheid brengen, om dan te verdwijnen in de nacht, dan is hetzelfde mechanisme aan het werk, meent Lasoen, en met hem veel collega-analisten en westerse inlichtingendiensten. Voor de goede orde: we weten vooralsnog niet wie de bewuste drones bestuurt, en er zijn nog geen harde bewijzen dat die dronebestuurders orders krijgen vanuit Moskou. “Maar dit is helemaal hun modus operandi”, zegt Lasoen. “We stellen vast dat de Russische geheime diensten steeds vaker gebruik maken van disposable agents. Mensen die benaderd worden met het voorstel om een cent bij te verdienen. Die – in dit geval – de opdracht krijgen om een drone in ontvangst te nemen en die op een bepaald moment en op een bepaalde plek de lucht in te sturen. Die aangestuurd worden via een complex web van tussenschakels en die betaald worden met cryptomunten, met de bedoeling dat die opdracht nooit kan getraceerd worden tot Moskou.” De Europese politiedienst Europol wees er afgelopen voorjaar nog op dat Rusland vaker en vaker beroep doet op criminele netwerken om sabotageacties uit te voeren. En het Internationaal Centrum voor Contraterrorisme (ICCT) in Den Haag bracht in september over dat Russische gevaar een lijvig rapport uit met als titel ‘Criminaliteit als instrument van hybride oorlogsvoering in Europa’. Het schrijft daarin dit. “Moskou wendt zich in toenemende mate tot disposable agents of

wegwerpagenten. Burgers die, vaak onwetend over de Russische rol als organisator, online gerekruteerd worden en eenvoudige taken krijgen waarvoor ze kleine bedragen krijgen." Het rapport heeft het over acties die gaan van anti-NAVO-graffiti spuiten tot brand stichten. En dus ook het laten overvliegen van drones bij kritieke infrastructuren in Europa, zegt oud-kolonel en defensie-expert Roger Housen. "In de voorbije drie jaar zijn er meer dan 100 drone-incidenten geweest, in zowat elk Europees land. Zowel de Nederlandse als de Duitse, de Deense en de Britse inlichtingendiensten zeggen voldoende robuuste indicaties te hebben om naar Moskou te kunnen wijzen. Op basis van het continue afspeuren van het internet, ook van het darkweb, van het volgen van de communicatie in wel en niet versleutelde chatgroepen, van afgeluisterde gesprekken en van getuigenissen van menselijke bronnen, ook in Moskou, krijgt men een idee van wie er achter die sabotageacties zit. Het patroon dat zich aftekent: telkens zijn de uitvoerders freelancers." Housen wijst, net als Lasoen, naar het complexe web van tussenschakels. Naar de schier eindeloze keten die zit tussen opdrachtgever en uitvoerder. "En nee, we kunnen die keten niet reconstrueren van bij een dronepiloot in België helemaal tot bij Poetin. Het Kremlin beslist niet: nu gaan we eens boven Marche-en-Famenne of Kleine-Brogel vliegen. Maar de topmensen van het Russische leger, van de veiligheidsdienst FSB en van de militaire inlichtingendienst GRU hebben wel de latitude – de vrijheid van handelen – om dit soort operaties op te zetten." "Iemand binnen die diensten besluit dus om een drone-operatie in België uit te voeren, en geeft die orders aan een ondergeschikte. Uiteindelijk wordt in ons land een betrouwbare tussenpersoon aangesproken. Iemand van wie men weet dat die Russisch-gezind is. Iemand die in het verleden nog opdrachten heeft uitgevoerd. Die speurt in zijn kennissenkring naar iemand die hij vertrouwt. Die spreekt op zijn beurt een persoon of een groep aan waarvan hij weet dat ze in staat zijn om de opdracht uit te voeren. Een crimineel. Een drugs- of motorbende. Die laatste opdrachtgever in de rij krijgt ook nog de boodschap mee: werk met nog twee of drie extra tussenpersonen. Men plaatst zoveel tussenschotten dat de uiteindelijke uitvoerders niet te weten kunnen komen wie de eerste opdrachtgever is." "Voor pakweg de lokale chapter van een motorbende is dat een makkelijke manier om extra geld te verdienen. Reken op enkele tienduizenden euro's. En het risico is klein. Ze moeten nergens fysiek inbreken, ze moeten niemand neerschieten. Alleen ergens, pakweg in het grensgebied tussen België en Nederland, midden in de nacht, op een discrete manier aan een bosrand zijn, om er enkele drones op uit te sturen. Geen huis-tuin-en-keuken-drones, maar wel dingen die je commercieel kan kopen. En je moet echt geen raketgeleerde zijn om er mee te vliegen, zeker niet als je wat handig bent in

gaming.” “Voor de onderaannemers draait dit enkel om centen”, zegt Housen. Maar voor de opdrachtgever spelen natuurlijk andere motieven. “Dit is psychologische oorlogsvoering. Als de Russen er inderdaad achter zitten, is het omdat ze angst willen verspreiden, onrust creëren, besluitvormingsprocessen beïnvloeden. Doordat dit soort incidenten hier plaatsvinden, zullen we hier ook sneller en meer investeren in systemen van detectie en interceptie van drones. Dat zijn in zekere zin ook luchtafweersystemen, die we dan niet meer aan Oekraïne kunnen geven.”

“Als Moskou hier achter zit, is het om onrust te zaaien”, zegt ook Peter Wijninga, oud-kolonel van de Nederlandse luchtmacht en analist bij het Haags Centrum voor Strategische Studies (HCSS). Alleen wil hij een duidelijke slag om de arm houden. “We zijn absoluut niet zeker. Om dit te dirigeren vanuit Moskou, om die hele keten van agenten en sympathisanten en onderaannemers aan te sturen: dat is een behoorlijke operatie. Als die operatie wordt blootgelegd, neemt de antipathie van de West-Europese bevolking tegenover Rusland alleen maar toe. Ik kan me voorstellen dat Rusland zegt: daar wagen we ons niet aan. Misschien zijn er andere lui met beschikking over professionele drones, die graag opschudding veroorzaken door te gaan vliegen boven een militaire basis waarvan iedereen weet dat er Amerikaanse kernwapens zijn opgeslagen. Het kunnen mensen zijn die net aansturen op meer striktere beveiliging rond zulke plekken.” “Ik ben dan vreselijk aan het speculeren, natuurlijk. Wat ik wil zeggen is dit. Het enige wat we met zekerheid weten, is: iemand wil ons angst aanjagen. En dat lukt aardig. Het doet me wat denken aan de zeppelin scare. In de Eerste Wereldoorlog zetten de Duitsers zeppelins in voor bombardementen. Plots zag iedereen zeppelins vliegen. Nu ziet iedereen drones vliegen. Dat wil niet zeggen dat de waarnemingen niet echt zijn. Maar er is wel een soort drone scare. En we mogen inderdaad beseffen dat we kwetsbaar zijn. Dat we onze vlieghavens – civiel en militair – misschien beter moeten beschermen tegen dit soort incidenten. Dat kan een positief gevolg zijn van al deze drone-incidenten.”

NoName richt DDoS-aanval op Belgische en Zweedse websites

De hackergroep NoName heeft aangegeven meerdere websites in België en Zweden te hebben aangevallen met DDoS-aanvallen. De getroffen organisaties in België zijn ENGIE Electrabel, STIB-MIVB, de LEZ van Brussel, het Directoraat-Generaal voor Statistiek, de Alimak Group en de stad Antwerpen. In Zweden waren vergelijkbare aanvallen gericht op verschillende bedrijfswebsites. Deze acties maken deel uit van een bredere campagne van NoName, die al meerdere keren Europese

infrastructuren heeft getroffen. De gevolgen van de aanval kunnen leiden tot verstoringen in de werking van essentiële diensten en een verstoring van de online beschikbaarheid van de getroffen systemen.

Gevaarlijke runC-kwetsbaarheden kunnen hackers toegang geven tot hostsystemen

Drie recent ontdekte kwetsbaarheden in runC, de container-runtime die wordt gebruikt in Docker en Kubernetes, kunnen door aanvallers worden misbruikt om de isolatiebeperkingen van containers te omzeilen en toegang te krijgen tot het hostbesturingssysteem. De beveiligingsproblemen, geclassificeerd als CVE-2025-31133, CVE-2025-52565 en CVE-2025-52881, kunnen worden benut om schrijfrechten te verkrijgen op het onderliggende systeem met rootbevoegdheden. Dit kan leiden tot ernstige beveiligingsrisico's. De kwetsbaarheden hebben betrekking op versies van runC vóór en na versie 1.0.0-rc3, met beschikbare patches in latere versies. Er zijn momenteel geen meldingen van actieve exploits, maar deskundigen raden aan om voorzorgsmaatregelen te nemen, zoals het gebruik van rootless containers of het inschakelen van gebruikersnamenruimten om de impact van aanvallen te beperken.

Terugkeer GlassWorm malware met nieuwe VSCode extensies

De GlassWorm malwarecampagne is teruggekeerd en heeft drie nieuwe VSCode-extensies toegevoegd aan de OpenVSX-marktplaats. Deze extensies zijn al meer dan 10.000 keer gedownload. De malware richt zich op GitHub-, NPM- en OpenVSX-accountgegevens, evenals op cryptocurrency-walletinformatie van 49 verschillende extensies. Door het gebruik van onzichtbare Unicode-tekens die als lege ruimte worden weergegeven, maar als JavaScript functioneren, kan de malware kwaadaardige acties uitvoeren. Vorige maand was de malware ook al actief via 12 extensies op de OpenVSX- en VS Code-marktplaatsen, die in totaal 35.800 keer werden gedownload, hoewel het aantal downloads mogelijk werd opgeblazen door de aanvaller zelf. De drie nieuwe extensies bevatten dezelfde obfuscatie-truc om beveiligingsmaatregelen te omzeilen. Gegevens van getroffen slachtoffers zijn inmiddels in handen van de onderzoekers en worden gedeeld met wetshandhavers.

Verkoop van ongeautoriseerde toegang tot OpenCart e-commerceplatform op het Dark Web

Er is melding gemaakt van de verkoop van ongeautoriseerde shell-toegang tot een onbekende e-commercewebsite die draait op het OpenCart-platform. Dit wijst op een potentieel beveiligingsrisico voor online winkels, aangezien kwaadwillenden toegang kunnen krijgen tot gevoelige gegevens of de werking van het platform kunnen verstoren. De verkoper en de getroffen website zijn onbekend, maar dergelijke incidenten benadrukken de noodzaak voor bedrijven in de e-commercebranche om hun beveiliging voortdurend te evalueren en te versterken. Het is essentieel dat e-commerceplatforms, zoals OpenCart, extra waakzaam zijn en hun beveiligingsmaatregelen verbeteren om dit soort dreigingen te voorkomen.

Microsoft onthult 'Whisper Leak'-aanval die AI-chatonderwerpen onthult in versleuteld verkeer

Microsoft heeft details gedeeld over een nieuwe zij-kanaalaanval genaamd Whisper Leak, die de mogelijkheid biedt om, zelfs bij versleuteld verkeer, de onderwerpen van gesprekken met AI-taalmodellen af te leiden. Het verkeer tussen gebruikers en modellen kan worden geanalyseerd door middel van patroonherkenning in de pakketgrootte en tijdsverschillen tijdens gestreamde antwoorden van de modellen. Dit maakt het mogelijk voor aanvallers om te achterhalen of het gesprek over gevoelige onderwerpen gaat, zoals politieke kwesties of financiële misdrijven, ondanks de versleuteling van het verkeer via HTTPS. Onderzoekers ontdekten dat met behulp van machine learning-modellen de aanval boven de 98% nauwkeurigheid kan bereiken bij het identificeren van specifieke gespreksonderwerpen. Microsoft en andere AI-aanbieders hebben mitigaties uitgerold, maar de ontdekking wijst op de potentieel toenemende dreiging van deze aanval bij langdurige interacties en het verzamelen van extra trainingdata.

Kritieke kwetsbaarheid in Cisco-firewalls nu ook gebruikt voor DDoS-aanvallen

Cisco heeft een kritieke kwetsbaarheid in zijn firewalls gemeld die nu actief wordt misbruikt voor Denial of Service (DDoS)-aanvallen. Deze kwetsbaarheid maakt deel uit van twee beveiligingslekken (CVE-2025-20333 en CVE-2025-20362) in Cisco's Secure Firewall ASA- en FTD-software. De aanvallers kunnen deze lekken combineren om volledige controle over de systemen te verkrijgen. Dit werd eerder

gebruikt voor het compromitteren van firewalls, maar de nieuwe aanvallen richten zich op het veroorzaken van DDoS-omstandigheden door de firewalls te laten herstarten. De kwetsbaarheden werden in september al gedocumenteerd door Cisco, die sindsdien een beveiligingsupdate heeft uitgebracht. De impactscore van de kwetsbaarheden is 9.9 voor het ernstigste lek. Dit stelt aanvallers in staat om systemen uit te schakelen door middel van DDoS-aanvallen. Cisco heeft geen verdere details over de aanvallen vrijgegeven.

Phishing fraude bij verloren iPhone

Het Zwitserse Nationaal Cyber Security Centre (NCSC) heeft een waarschuwing uitgebracht voor iPhone-eigenaren over een nieuwe phishingfraude die zich richt op verloren of gestolen toestellen. Criminelen sturen sms-berichten die zogenaamd afkomstig zijn van Apple, met de bewering dat de verloren iPhone is teruggevonden. De berichten bevatten gedetailleerde informatie over het toestel en een link naar een valse website die de officiële "Find My" pagina nabootst. Wanneer slachtoffers hun Apple ID inloggen, krijgen de aanvallers toegang tot hun account. Het doel van de fraudeurs is om de Activation Lock te verwijderen, zodat de gestolen iPhone opnieuw kan worden verkocht. Het NCSC raadt gebruikers aan om nooit op verdachte links te klikken, een uniek e-mailadres voor verloren apparaten te gebruiken en de SIM-kaart te beveiligen met een pincode. Apple zelf zal nooit via sms of e-mail contact opnemen over gevonden toestellen.

FBI wil achterhalen wie Archive.ph beheert

De FBI heeft een federale dagvaarding uitgevaardigd naar het Canadese domeinregistratiebedrijf Tucows, waarin wordt geëist dat ze gedetailleerde klantinformatie verstrekken om de anonieme beheerder van Archive.ph (en verwante domeinen zoals Archive.is en Archive.today) te achterhalen. De site, die bekend staat om het omzeilen van betaalmuren, wordt onderzocht in een niet nader gespecificeerde strafrechtelijke zaak. Archive.ph slaat miljoenen webpagina’s op, maar de identiteit van de eigenaar blijft onbekend. Er wordt vermoed dat de oprichter een Russische persoon is, mogelijk met banden in Europa. De dagvaarding vraagt om onder andere de naam, adresgegevens, telefoon- en betalingsinformatie, evenals internetlogs van de eigenaar. Dit onderzoek volgt eerdere acties tegen websites die

content zonder betaling toegankelijk maken. Tucows heeft bevestigd de gegevens uiterlijk 29 november te verstrekken, conform de wetgeving.

WordPress-plugin 0-day te koop op hackforum

Op een hackforum is een 0-day kwetsbaarheid aangeboden voor een populaire WordPress-plugin. De kwetsbaarheid kan door aanvallers worden misbruikt om toegang te krijgen tot websites die de plugin gebruiken, waardoor vertrouwelijke gegevens in gevaar komen. Deze kwetsbaarheid kan aanzienlijke risico's voor de veiligheid van WordPress-gebruikers met zich meebrengen, vooral voor bedrijven en organisaties die afhankelijk zijn van de plugin voor hun webfunctionaliteit. Het aanbieden van dergelijke kwetsbaarheden op illegale marktplaatsen toont de groeiende bedreigingen in de cybercriminaliteit, waarbij steeds meer digitale zwaktes actief worden verhandeld. Beveiligingsspecialisten wordt aangeraden om de getroffen systemen snel te patchen zodra er een fix beschikbaar is, om de impact van dergelijke aanvallen te minimaliseren.

OWASP voegt Software Supply Chain Failures toe aan Top 10 lijst van 2025

OWASP heeft in de 2025-editie van de Top 10 een nieuwe categorie geïntroduceerd: Software Supply Chain Failures. Deze toevoeging weerspiegelt de groeiende bezorgdheid over risico's in de afhankelijkheden en bouwsystemen van software. Aanvallen op de softwareleveringsketen gaan verder dan verouderde componenten en omvatten nu ook inbreuken op tools en infrastructuur die gebruikt worden om software te ontwikkelen en te distribueren. De incidentie van deze kwetsbaarheden is relatief laag, maar ze dragen een hoger exploitatie- en impactrisico. OWASP benadrukt de noodzaak van strengere beveiliging van CI/CD-pijplijnen, afhankelijkheden en ontwikkeltools. De focus verschuift naar een cultuur waarin de componenten in de ontwikkelketen als deel van het dreigingsmodel worden beschouwd, in plaats van als vertrouwde achtergrondtools. Het rapport adviseert organisaties om de integriteit van hun ontwikkelprocessen te waarborgen, onder meer door gebruik te maken van goedgekeurde en ondertekende pakketten en het streng monitoren van ontwikkelomgevingen.