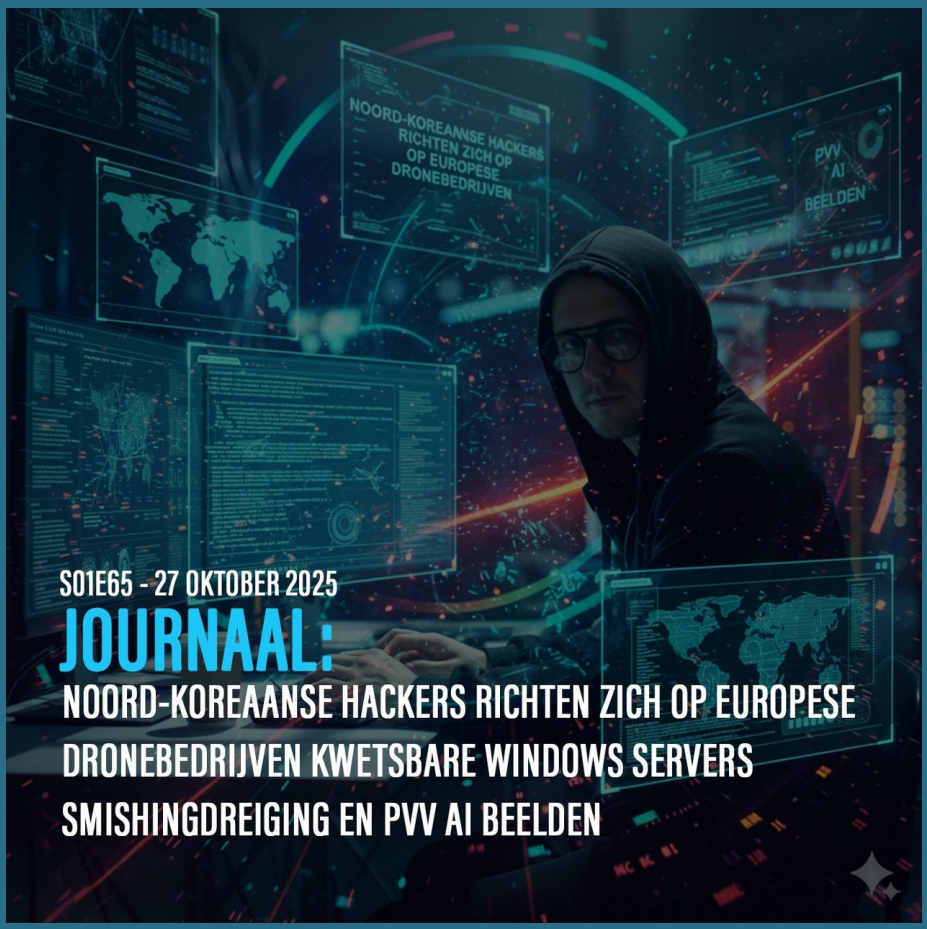
# Cybercrimeinfo

*"Omdat wat waardevol is, beschermd moet worden"*

## Nieuwsbrief 390



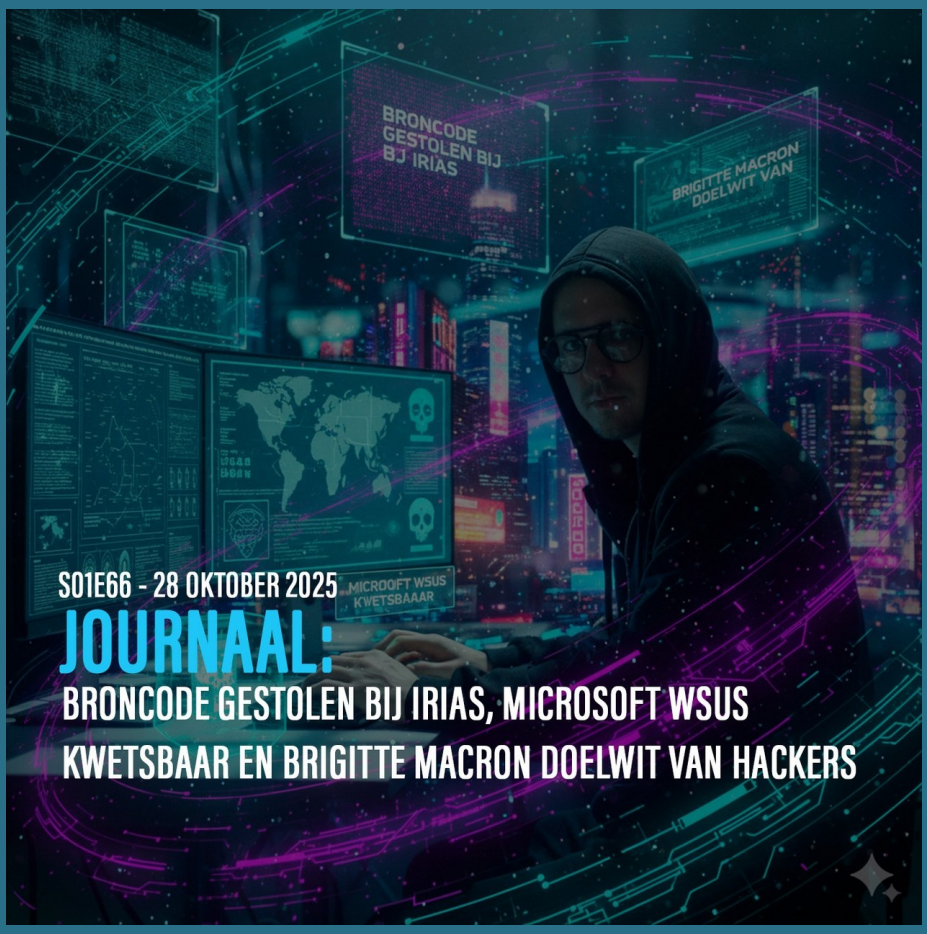

## Noord-Koreaanse hackers richten zich op Europese dronebedrijven kwetsbare Windows servers smishingdreiging en PVV AI beelden

Noord-Koreaanse hackers, waaronder de Lazarus groep, richten zich op Europese bedrijven die werken met drone technologie, met als doel technische gegevens te stelen. Deze aanvallen maken deel uit van een bredere spionagecampagne, waarbij misleidende e-mails worden gebruikt om medewerkers te verleiden schadelijke bestanden te openen. Daarnaast wordt wereldwijd een smishingdreiging via sms-berichten verspreid, waarbij criminelen meer dan 1 miljard dollar hebben verdiend door persoonlijke gegevens van slachtoffers te stelen. Ook zijn kwetsbaarheden in

Windows- en SharePoint-servers ontdekt, die grote risico's vormen voor bedrijven.

LEES VERDER

---

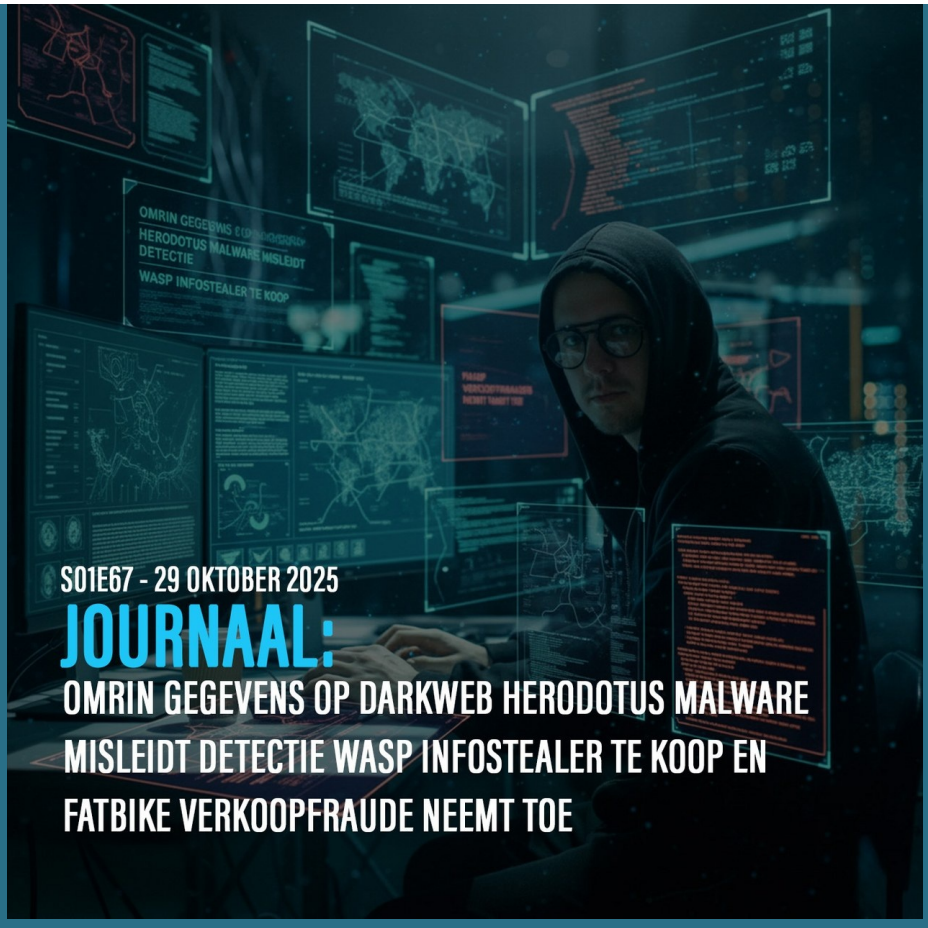



## Broncode gestolen bij Irias, Microsoft WSUS kwetsbaar en Brigitte Macron doelwit van hackers

Irias, een Nederlands softwarebedrijf, werd getroffen door een datalek waarbij de broncode werd gestolen, wat de dreiging van intellectuele eigendomsdiefstal vergroot. Verder werd een kwetsbaarheid in Microsoft WSUS ontdekt, die servers blootstelt aan aanvallen en volledige controle door hackers mogelijk maakt. Brigitte Macron werd het doelwit van een cyberaanval waarbij hackers haar naam op een belastingformulier wijzigden. De dreigingen tegen vitale infrastructuren, zoals energie en communicatie, blijven toenemen door aanvallen van groeperingen als Chollima en ForumTroll, die steeds geavanceerdere technieken gebruiken.

LEES VERDER

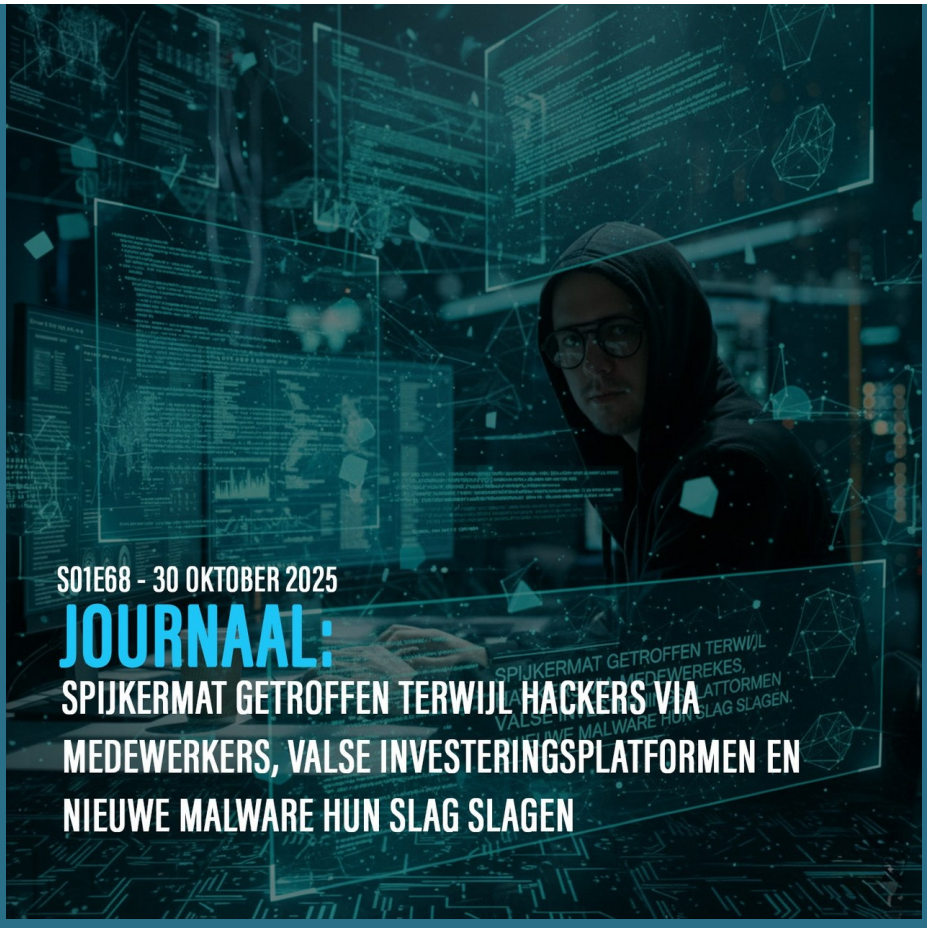
---




## Omrin gegevens op darkweb Herodotus malware misleidt detectie Wasp infostealer te koop en fatbike verkoopfraude neemt toe

De gegevens van Omrin, een Friese afvalverwerker, zijn gestolen en openbaar gemaakt op het darkweb. De aanval, uitgevoerd door de Qilin groep, heeft persoonlijke informatie van medewerkers en bedrijfsgegevens blootgesteld, wat leidde tot verstoringen bij de klantenservice en de Afvalapp. Nieuwe malware, zoals Herodotus, maakt gebruik van vertragingen in tekstinvoer om detectie te omzeilen, en wordt actief verspreid via sms in Italië en Brazilië. Daarnaast neemt fatbike verkoopfraude toe, met een groeiend aantal meldingen van oplichting via malafide webshops.

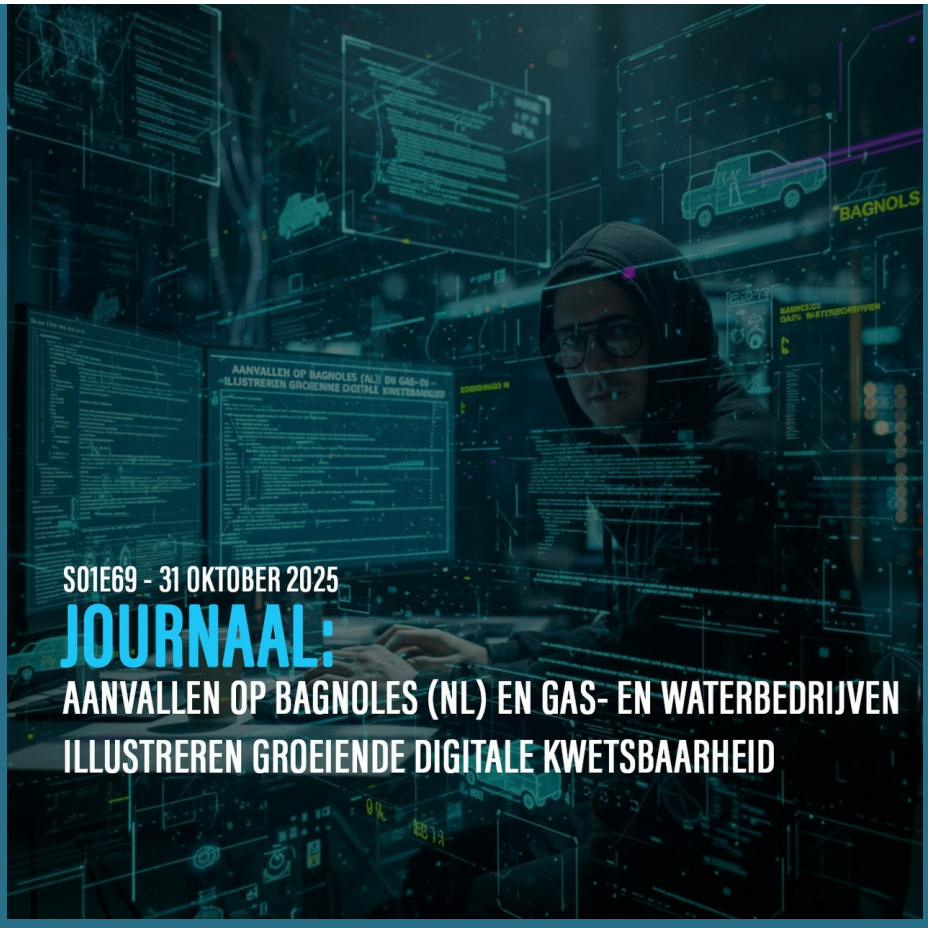
**LEES VERDER**




## Spijkermat getroffen terwijl hackers via medewerkers, valse investeringsplatformen en nieuwe malware hun slag slaan

Spijkermat, een Nederlands bedrijf, werd getroffen door een ransomware-aanval waarbij gegevens werden gestolen. Dit incident benadrukt de kwetsbaarheid van bedrijven, zelfs buiten de technologische sector. Nieuwe dreigingen zoals PhantomRaven malware, die ontwikkelaars aanvalt, en het Aisuru botnet, dat anonieme proxies aanbiedt, verhogen de risico's voor bedrijven en gebruikers wereldwijd. Daarnaast nemen phishingcampagnes en malware die bankgegevens steelt toe. Geopolitieke spanningen blijven een rol spelen, zoals de aanvallen van de Russische Sandworm groep op Oekraïense organisaties. Bedrijven moeten hun systemen voortdurend updaten om zich te beschermen tegen deze gevaren.

LEES VERDER




## Aanvallen op Bagnoles (NL) en gas- en waterbedrijven illustreren groeiende digitale kwetsbaarheid

Bagnoles, een Nederlandse autoleverancier, werd getroffen door een ransomware-aanval van de Qilin-groep, wat leidde tot potentiële gegevensdiefstal of versleuteling van systemen. Dit benadrukt de kwetsbaarheid van bedrijven die afhankelijk zijn van cloudsoftware. Ook werden kwetsbaarheden ontdekt in systemen van Microsoft en WordPress, die hackers toegang kunnen geven tot duizenden servers en websites. Verder worden steeds meer online systemen, zoals WooCommerce-webshops en IoT-apparaten, bedreigd door malware en botnet-aanvallen, wat de noodzaak voor robuuste beveiligingsmaatregelen onderstreept.

**LEES VERDER**


## Belgische zorginstelling geraakt door ransomware, malware steelt betaaldata en diplomaten onder vuur van cyberaanvallen

VZW Avalon, een zorginstelling in België, werd getroffen door een ransomware-aanval die duizenden bestanden versleutelde en de privacy van bewoners mogelijk in gevaar bracht. Tegelijkertijd werd er nieuwe malware ontdekt die contactloze betaalgegevens steelt, wat vooral in Oost-Europa voorkomt. Daarnaast richten cyberaanvallen zich op diplomaten in Europa, waarbij kwetsbaarheden in Windows-systemen worden misbruikt. De toename van cyberdreigingen wordt versterkt door de samenwerking van hacktivistische groepen en de ontdekking van malware die gegevens steelt via internetbrowsers.

**LEES VERDER**

---


## Riel / Breda / Haarlem - Bankhelpdeskfraude

Een man heeft zich in Riel, Breda en Haarlem voorgedaan als medewerker van een beveiligingsbedrijf en gepleegd wat bekend staat als bankhelpdeskfraude. Hij belde een slachtoffer, meldde dat diens bankrekening in gevaar was en vroeg vervolgens

om toegang tot de computer van het slachtoffer. Nadat hij de computer had gecontroleerd, vroeg de fraudeur om contant geld en bleek later dat de rekening was leeggeroofd en er met de bankpas werd gepind. De politie zoekt naar de verdachte en vraagt om tips van getuigen.

## LEES VERDER

---

Luister naar de discussiepodcast over het nieuws van de afgelopen week.

**Luister de podcast nu op Youtube**

**Luister de podcast nu op Spotify**

---

**Meer leren over cybercrime? Ontdek de verschillende vormen en begrippen**

In de Cybercrimeinfo Bibliotheek vind je een uitgebreide verzameling van termen en verschillende vormen van cybercriminaliteit. Van phishing en malware tot ransomware en andere digitale dreigingen, we leggen elke vorm duidelijk uit. Zo krijg je inzicht in wat deze aanvallen inhouden, hoe ze werken en welke risico's ze met zich meebrengen.

Of je nu op zoek bent naar uitleg over specifieke cybercrime termen of meer wilt leren over de verschillende soorten digitale bedreigingen, onze bibliotheek biedt de kennis die je nodig hebt om jezelf beter te beschermen.

Verdiep je in de wereld van cybercrime en vergroot je digitale weerbaarheid.

## BEKIJK DE BIBLIOTHEEK

---

**Beantwoorde vragen en tips voor digitale weerbaarheid**

Op deze pagina vind je antwoorden op veelgestelde vragen, nuttige tips en praktische hulpmiddelen om je digitale veiligheid te verbeteren. Of je nu meer wilt weten over bescherming tegen cyberdreigingen of jezelf beter wilt wapenen tegen online gevaren, wij bieden de informatie die je nodig hebt.

## BEKIJK DE TIPS

---

**Veelgestelde vragen over digitale veiligheid en cybercrime**

Op Cybercrimeinfo vind je antwoorden op de meest gestelde vragen over cybersecurity en cybercrime. Leer hoe je jezelf en je organisatie kunt beschermen tegen digitale dreigingen, van phishing en malware tot ransomware en DDoS-aanvallen. We bieden duidelijke uitleg en praktische tips om je digitale veiligheid te versterken.

## ONTDEK DE ANTWOORDEN

---

**Vergroot je kennis en vaardigheden**

Wil je je kennis over cybersecurity en het darkweb uitbreiden? Bij de Leerplek van Cybercrimeinfo vind je een breed aanbod van cursussen, tutorials en quizzen die je helpen up-to-date te blijven met de nieuwste technieken en dreigingen. Of je nu net begint of al een expert bent, onze interactieve leeromgeving biedt de uitdaging die je nodig hebt om jezelf verder te ontwikkelen.
Test je kennis met uitdagende quizzen en verdien toegang tot de exclusieve Perfecte Score Club. Voor opsporingsambtenaren bieden we binnenkort speciaal op maat gemaakte quizzen aan.

**TEST JE KENNIS**

---


**Contact met Cybercrimeinfo**

Heb je een vraag of probleem? Vul het formulier in en stel je vraag. We reageren zo snel mogelijk, maar houd er rekening mee dat het door de hoge aantallen vragen soms enkele dagen kan duren.

**STEL JE VRAAG**

---

**Steun Cybercrimeinfo en help de strijd tegen cybercriminaliteit**

Elke dag zetten wij ons in om je op de hoogte te houden van de laatste cyberdreigingen en trends. Onze missie is om jou en anderen te beschermen tegen de groeiende risico's in de digitale wereld. Maar we kunnen dit niet alleen. Jouw steun maakt het verschil.
Door te doneren help je ons waardevolle informatie te blijven leveren, nieuwe tools te ontwikkelen en de bewustwording over cybercriminaliteit te vergroten. Elke bijdrage, groot of klein, draagt bij aan de bescherming van digitale veiligheid.
Wil je ons steunen?

Samen maken we de online wereld een stukje veiliger.
Bedankt voor je steun!

**❤ STEUN ONS NU**

---

## Dagelijks cyber journaal van Cybercrimeinfo

Het Dagelijks Cyber Journaal biedt dagelijkse updates over de belangrijkste cyberdreigingen en incidenten in België en Nederland. Dit is bedoeld voor mensen die de ontwikkelingen in cybercrime willen volgen, maar geen tijd hebben om alles bij te houden. Het biedt een efficiënte manier om snel up-to-date te blijven zonder uren te spenderen aan het zoeken naar relevante informatie. De updates zijn beschikbaar in zowel tekst als via een dagelijkse podcast op Spotify en YouTube.

Ontvang dagelijks het cyber journaal tussen 12:00 en 14:00 (behalve zondag).
Schrijf je in en ontvang het automatisch in je mailbox.

E-mailadres *

Voornaam

Achternaam

Inschrijven


## Inschrijven

Ontvang dagelijks het cyber journaal tussen 12:00 en 14:00 (behalve zondag). Schrijf je in en ontvang het automatisch in je mailbox.

**INSCHRIJVEN**

Share Tweet Share Pinterest Bluesky Mastodon