

# Cybercrimeinfo

"Omdat wat waardevol is, beschermd moet worden"



NB388

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



Luister de podcast nu op Youtube



Luister de podcast nu op Spotify

S01E53 - 13 OKTOBER 2025

**JOURNAAL:**  
CYBERAANVAL OP DEN HARTOGH LOGISTICS CHAOSBOT EN  
GEOPOLITIEKE DREIGINGEN BEDREIGEN DIGITALE VEILIGHEID  
IN EUROPA

CYBERAANVAL OP DEN HARTOGH LOGISTICS  
CHAOSBOT EN GEOPOLITIEKE DREIGINGEN  
BEDREIGEN DIGITALE VEILIGHEID IN EUROPA

CYBER JOURNAL

## Cyberaanval op Den Hartogh Logistics ChaosBot en geopolitieke dreigingen bedreigen digitale veiligheid in Europa

Den Hartogh Logistics werd recent getroffen door een cyberaanval, waarbij criminelen toegang kregen tot gevoelige bedrijfsdata. In combinatie met deze aanval werd er op het darkweb een enorme hoeveelheid gestolen persoonlijke gegevens aangeboden, waaronder paspoortnummers. ChaosBot malware werd ontdekt, die via gestolen wachtwoorden toegang krijgt tot netwerken en moeilijk te detecteren is. Ondertussen blijft de Astaroth banking trojan actief, die inloggegevens steelt. Deze incidenten benadrukken de groeiende digitale dreigingen en het belang van verbeterde bescherming tegen cyberaanvallen.

LEES VERDER



## Bun.nl en Omrin slachtoffer van cyberaanvallen en privacy in gevaar door goedkope camera's en spyware

Bun.nl en Omrin werden getroffen door cyberaanvallen waarbij ransomware de systemen vergrendelde, wat leidde tot verstoringen in hun bedrijfsvoering. Bun.nl werkt samen met autoriteiten om de schade te beperken, terwijl Omrin zijn afvalverwerking voortzet ondanks de aanval. Daarnaast worden goedkope camera's uit China en mobiele spyware bedreigingen voor de privacy. Goedkope camera's blijken onvoldoende beveiligd, waardoor hackers toegang krijgen tot privébeelden. Ook spyware op Android-apparaten stelt hackers in staat persoonlijke gegevens te stelen, wat de kwetsbaarheid van consumententechnologie benadrukt.

LEES VERDER



S01E55 - 15 OKTOBER 2025

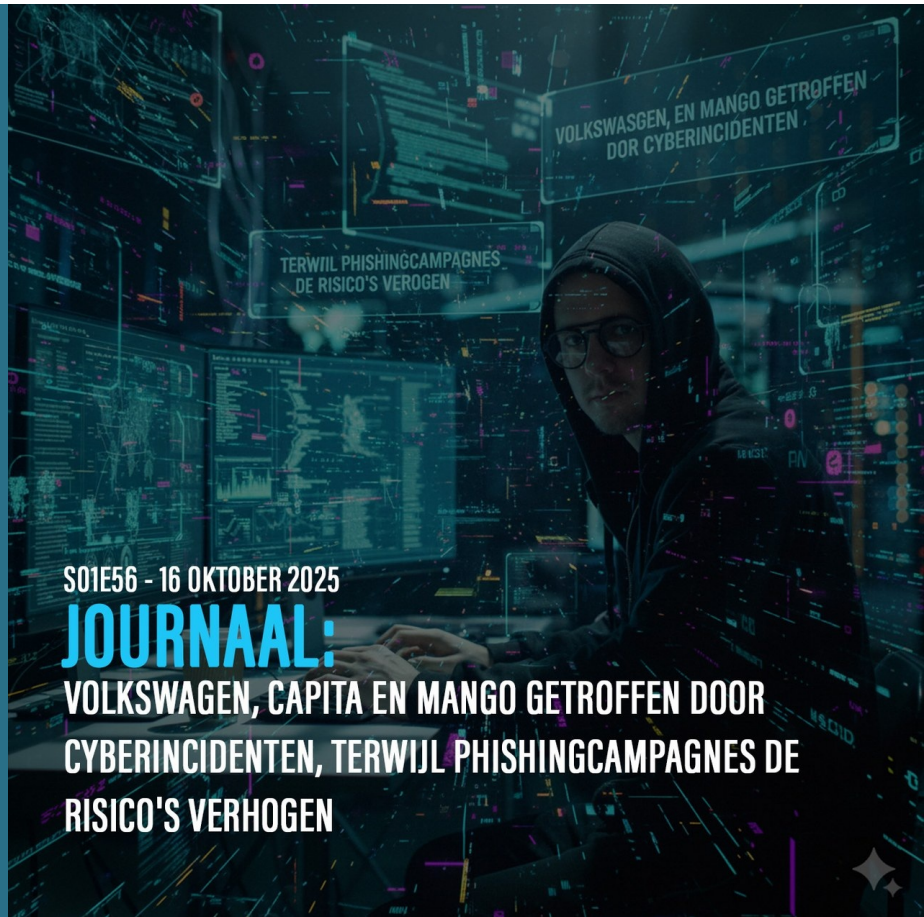
## JOURNAAL:

**RIVM EN OMRIN KAMPEN MET CYBERAANVALLEN TERWIJL  
NIEUWE AI DREIGINGEN EN KWETSBAARHEDEN DE VEILIGHEID  
ONDER DRUK ZETTEN**

### **RIVM en Omrin kampen met cyberaanvallen terwijl nieuwe AI dreigingen en kwetsbaarheden de veiligheid onder druk zetten**

Omrin en het RIVM herstellen van cyberaanvallen die hun systemen verstoorden. Omrin werd getroffen door ransomware, maar heeft het ophalen van afval en klantenservice hervat. Het RIVM had een kwetsbaarheid op de website, waardoor hackers desinformatie plaatsten, maar er werd geen persoonlijke data gelekt. Daarnaast zijn er meerdere kwetsbaarheden ontdekt in populaire software, zoals Android, Autodesk en Elastic Cloud, die de digitale veiligheid onder druk zetten. Ook blijven AI-gedreven aanvallen en supply chain aanvallen toenemen, wat de risico's vergroot voor bedrijven en gebruikers.

**LEES VERDER**



S01E56 - 16 OKTOBER 2025

## **JOURNAAL:** **VOLKSWAGEN, CAPITA EN MANGO GETROFFEN DOOR CYBERINCIDENTEN, TERWIJL PHISHINGCAMPAGNES DE RISICO'S VERHOGEN**

### **Volkswagen, Capita en Mango getroffen door cyberincidenten, terwijl phishingcampagnes de risico's verhogen**

Volkswagen, Capita en Mango zijn recent getroffen door cyberincidenten, waaronder ransomware-aanvallen en datalekken. Volkswagen werd getroffen door een ransomware-aanval die de bedrijfsvoering verstoorde, terwijl Capita een boete kreeg van 16 miljoen euro voor een datalek, veroorzaakt door een ongewenst bestand dat door een werknemer werd geopend. Mango meldde een datalek bij een externe leverancier, waarbij klantgegevens werden blootgesteld. Phishingcampagnes en kwetsbaarheden in software verhogen de risico's, wat bedrijven ertoe aanzet hun beveiliging te versterken en snel te patchen.

**LEES VERDER**



S01E57 - 17 OKTOBER 2025

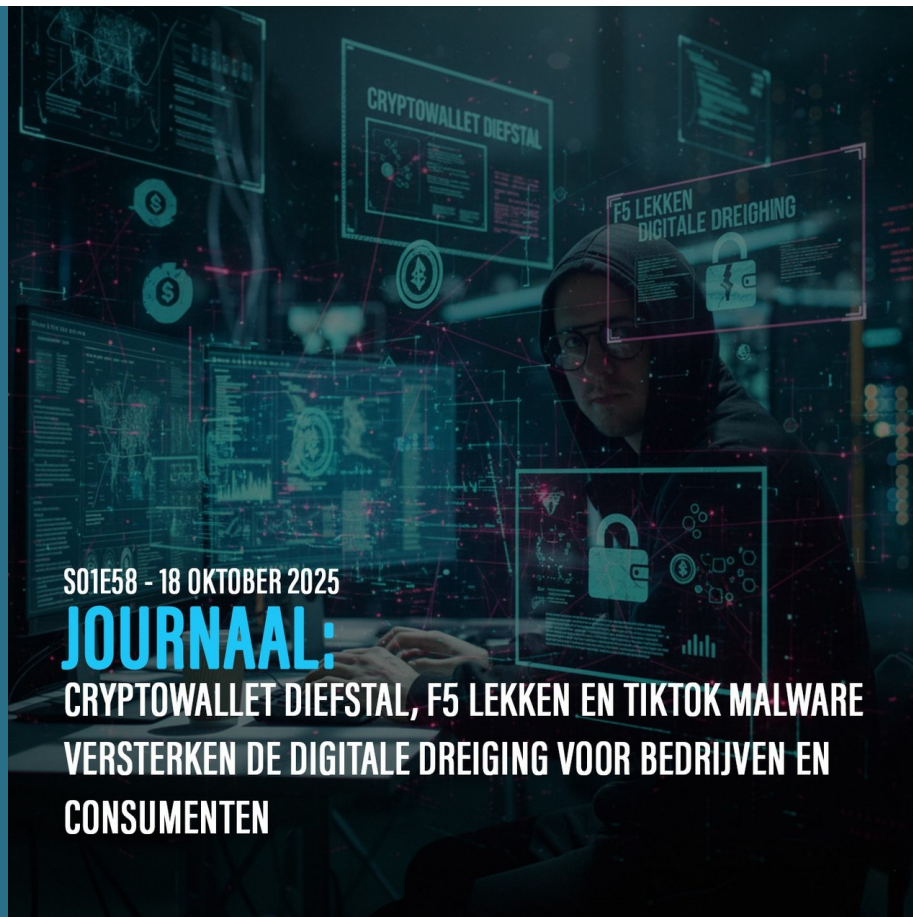
## JOURNAAL:

**PHISHING OP LASTPASS, DATINGFRAUDE IN UTRECHT EN  
BLOCKCHAIN MALWARE VORMEN GROEIENDE DREIDINGEN**

### **Phishing op LastPass, datingfraude in Utrecht en blockchain malware vormen groeiende dreigingen**

Er zijn groeiende digitale dreigingen zoals phishingcampagnes gericht op LastPass en Bitwarden, waarbij aanvallers gebruikers naar nepversies van software lokken om toegang te krijgen tot hun systemen. In Utrecht werden twee vrouwen gearresteerd voor datingfraude, waarbij zij via valse relaties meer dan €550.000 van slachtoffers verduisterden. Daarnaast groeit de dreiging van blockchain malware die zich verstoppt in legitieme transacties, en ransomware-aanvallen waarbij zowel gegevens worden gestolen als versleuteld. Beveiligingsexperts waarschuwen voor deze opkomende risico's.

**LEES VERDER**



S01E58 - 18 OKTOBER 2025

## **JOURNAAL:** CRYPTOWALLET DIEFSTAL, F5 LEKKEN EN TIKTOK MALWARE VERSTERKEN DE DIGITALE DREIGHING VOOR BEDRIJVEN EN CONSUMENTEN

### **Cryptowallet diefstal, F5 lekken en TikTok malware versterken de digitale dreiging voor bedrijven en consumenten**

Cryptowalletdiefstal, F5 kwetsbaarheden en TikTok malware vormen groeiende bedreigingen voor zowel bedrijven als consumenten. Noord-Koreaanse hackers verspreiden schadelijke software via valse werkgelegenheidsaanbiedingen om cryptowallets en inloggegevens te stelen. F5 apparaten vertonen kwetsbaarheden die wereldwijd toegankelijk zijn, wat de beveiliging van bedrijven in gevaar brengt. Phishingaanvallen, TikTok-malware en schadelijke game-mods vergroten de risico's, terwijl psychologische technieken zoals FOMO (fear of missing out) worden ingezet om slachtoffers te misleiden. Bedrijven moeten hun beveiliging versterken om dergelijke aanvallen te voorkomen.

**LEES VERDER**



### **Bankhelpdeskfraude in Rotterdam: 91 jarige vrouw opgelicht**

Een 91 jarige vrouw uit Rotterdam werd slachtoffer van bankhelpdeskfraude. Ze werd gebeld door een nepmedewerker van ING, die haar vertelde dat haar bankrekening mogelijk misbruikt werd. De oplichter vroeg haar bankgegevens, waarmee hij een iPhone en accessoires kocht. Ook probeerde hij meerdere keren geld van haar rekening te pinnen. De verdachte wordt als mogelijk minderjarig beschouwd, waardoor zijn identiteit voorlopig onherkenbaar blijft. De zaak is nog in onderzoek.

## LEES VERDER



### 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 quizzes 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

Deze e-mail is verstuurd aan [{{email}}](#).

Als u geen nieuwsbrief meer wilt ontvangen, kunt u zich [hier afmelden](#).

U kunt ook uw gegevens [inzien](#) en [wijzigen](#).

Voor een goede ontvangst voegt u [info@cybercrimeinfo.nl](mailto:info@cybercrimeinfo.nl) toe aan uw adresboek.