Nederland • België • Wereldwijd

CYBER DREIGINGSRADAR

JAARRAPPORT 2026

Trends en analyses van ransomware- en darkwebdreigingen.

UITGEGEVEN DOOR

Digiweerbaar.nl

Inhoud

01. Voorwoord

Cyberdreigingen ontwikkelen zich voortdurend. Cybercriminelen opereren steeds professioneler, werken internationaal samen en maken gebruik van steeds geavanceerdere aanvalsmethoden.

Ransomware blijft daarbij één van de grootste digitale dreigingen voor organisaties. Waar aanvallen vroeger vooral gericht waren op het versleutelen van systemen, staat tegenwoordig steeds vaker het stelen en openbaar maken van bedrijfsgegevens centraal.

De **Cyber Dreigingsradar** monitort dagelijks actuele cyberdreigingen, waaronder datalekken, kwetsbaarheden, incidenten en andere relevante ontwikkelingen. Op basis van deze informatie ondersteunt Digiweerbaar organisaties bij het verkrijgen van actueel inzicht in het continu veranderende dreigingslandschap.

Dit jaarrapport richt zich specifiek op organisaties die door ransomwaregroepen op hun leksites als slachtoffer zijn gepubliceerd.

De cijfers geven daarmee geen volledig beeld van alle ransomwareaanvallen, maar vormen een waardevolle indicator van zichtbare ransomware- en afpersingsactiviteiten.

Met dit eerste jaarrapport bundelen wij de belangrijkste cijfers, trends en analyses uit de Cyber Dreigingsradar. Wij hopen bestuurders, IT-verantwoordelijken en professionals in de Benelux hiermee te ondersteunen bij het herkennen van ontwikkelingen, het duiden van risico's en het versterken van de digitale weerbaarheid van hun organisatie.

Tegelijkertijd hopen wij met dit rapport bij te dragen aan meer bewustwording van de impact en ontwikkeling van ransomware binnen Nederland en België.

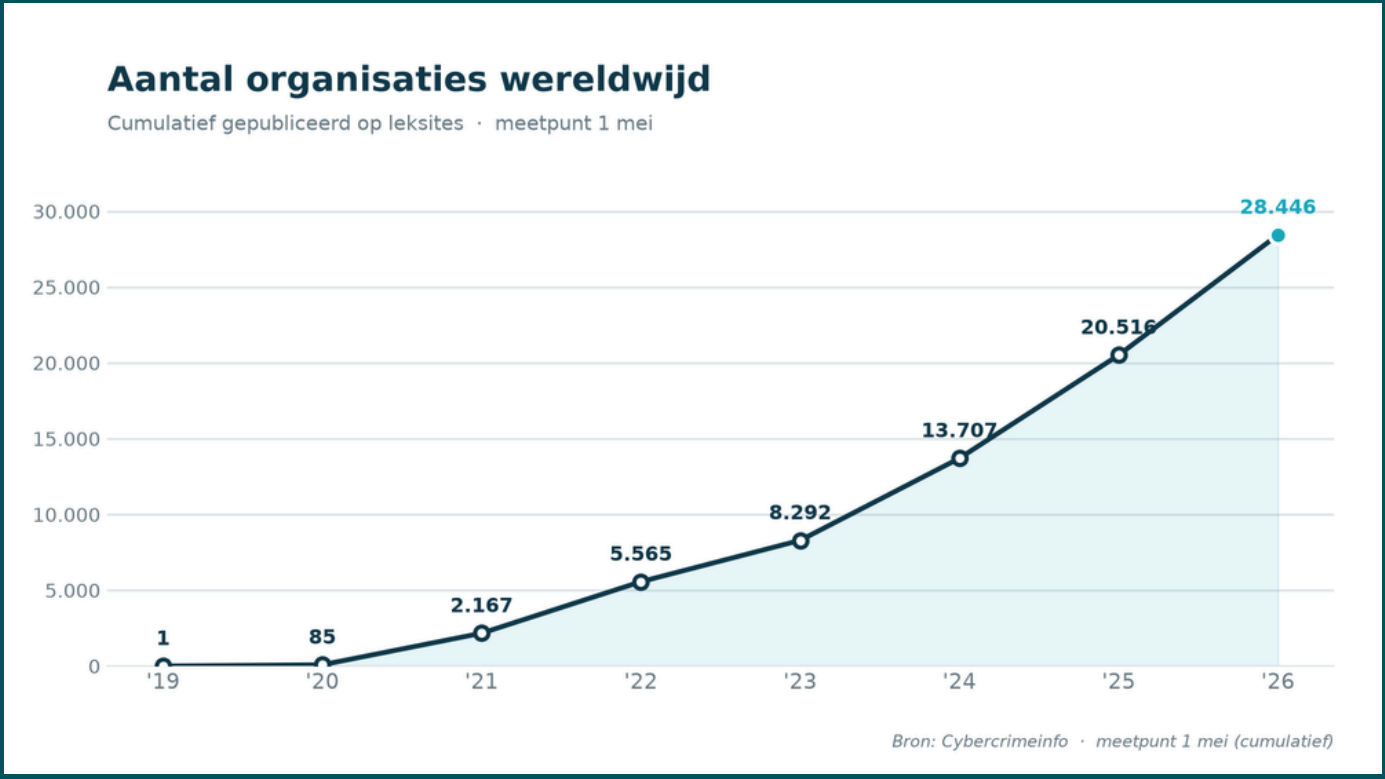
Team Cyber Intelligence
Digiweerbaar.nl

02. KERNCIJFERS

Wereldwijd

28.446
Organisaties wereldwijd gepubliceerd
op ransomware data leak sites

7930
Nieuwe slachtoffers
tussen 1 mei 2025 en 1 mei 2026



Wereldwijd

Per 1 mei 2026 registreerde de Cyber Dreigingsradar wereldwijd 28.446 organisaties waarvan gestolen gegevens door ransomwaregroepen op het darkweb zijn gepubliceerd. Dat zijn 7.930 nieuwe slachtoffers ten opzichte van een jaar eerder, een stijging van 38,6%.

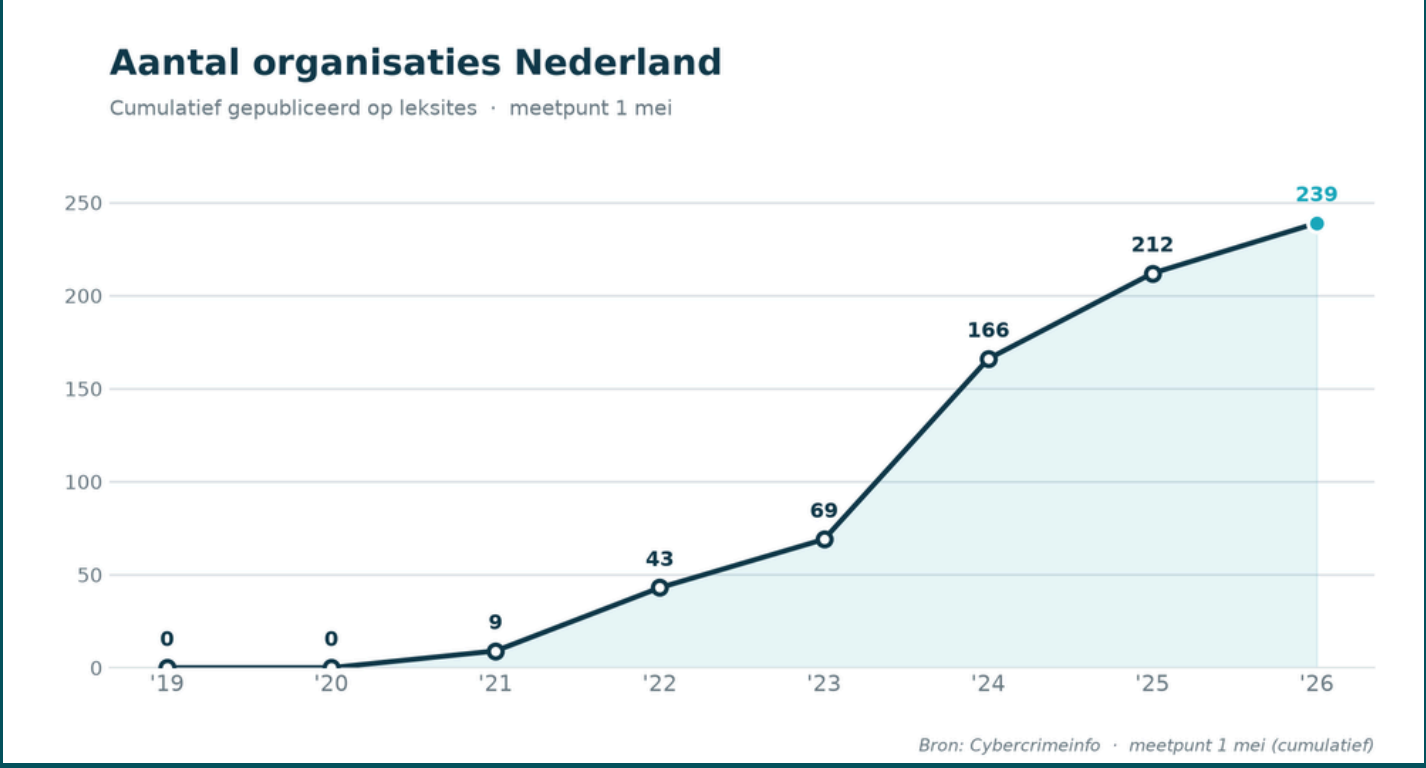
Sinds de eerste registraties in 2020 groeide het aantal bekende slachtoffers van 85 naar 28.446 organisaties.

Hoewel de procentuele groei afvlakt, blijft het absolute aantal nieuwe slachtoffers toenemen. Dit bevestigt dat ransomware wereldwijd een aanhoudende en grootschalige dreiging vormt.

Nederland

239
Nederlandse organisaties gepubliceerd
op ransomware data leak sites

27
Nieuwe slachtoffers
tussen 1 mei 2025 en 1 mei 2026



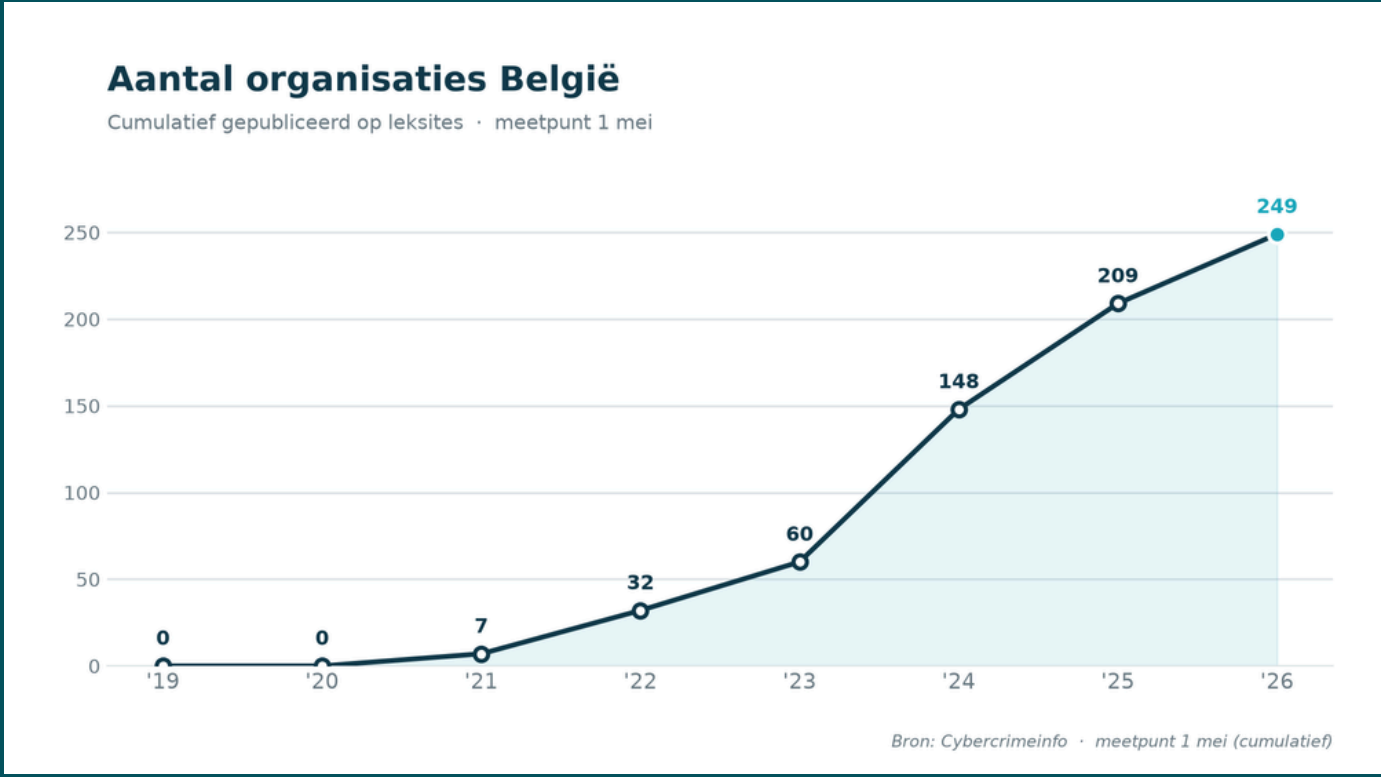
Nederland
Groei zet door, maar tempo neemt af.
Nederland telde op 1 mei 2026 239 geregistreerde organisaties. Ten opzichte van vorig jaar kwamen 27 nieuwe slachtoffers bij (+12,7%).

Na de sterke stijgingen in 2023 en 2024 lijkt de groei in Nederland af te vlakken. Dat betekent echter niet dat de dreiging afneemt. Het aantal geregistreerde slachtoffers bereikt opnieuw een historisch hoogtepunt.

België

249
Belgische organisaties gepubliceerd op ransomware data leak sites.

40
Nieuwe slachtoffers tussen 1 mei 2025 en 1 mei 2026



België

België groeit sneller dan Nederland. België telt op 1 mei 2026 voor het eerst meer geregistreerde organisaties dan Nederland.

Ten opzichte van vorig jaar kwamen 40 nieuwe slachtoffers bij (+19,1%).
Hoewel ook in België de procentuele groei afneemt, is de stijging relatief hoger dan in Nederland.

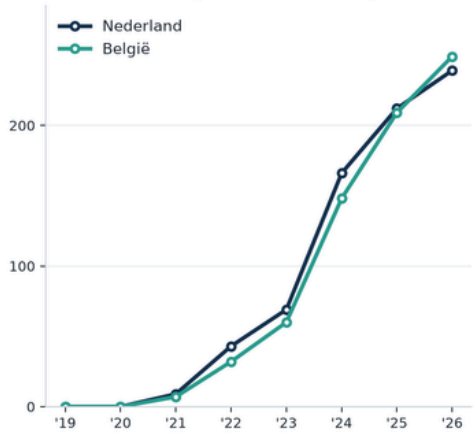
05. TRENDS & ONTWIKKELINGEN

Ransomware in Nederland en België

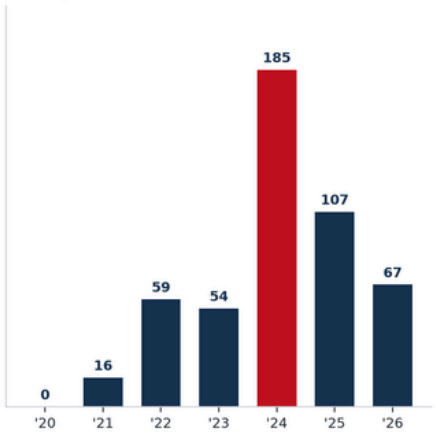
De stand van zaken op 1 mei 2026

488	1,7%	-64%	Qilin
gepubliceerde slachtoffers NL + België	aandeel van het wereldwijde totaal	aanwas t.o.v. de piek in 2024	actiefste groep nu (LockBit voorbij)

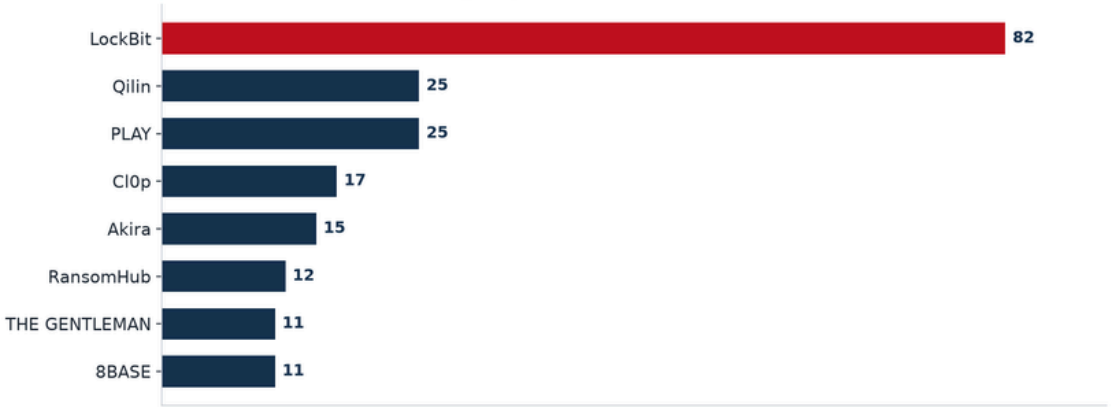
Cumulatieve groei, NL vs België



Jaarlijkse aanwas NL+BE vlakt af



Meest actieve ransomwaregroepen, 2020-2026

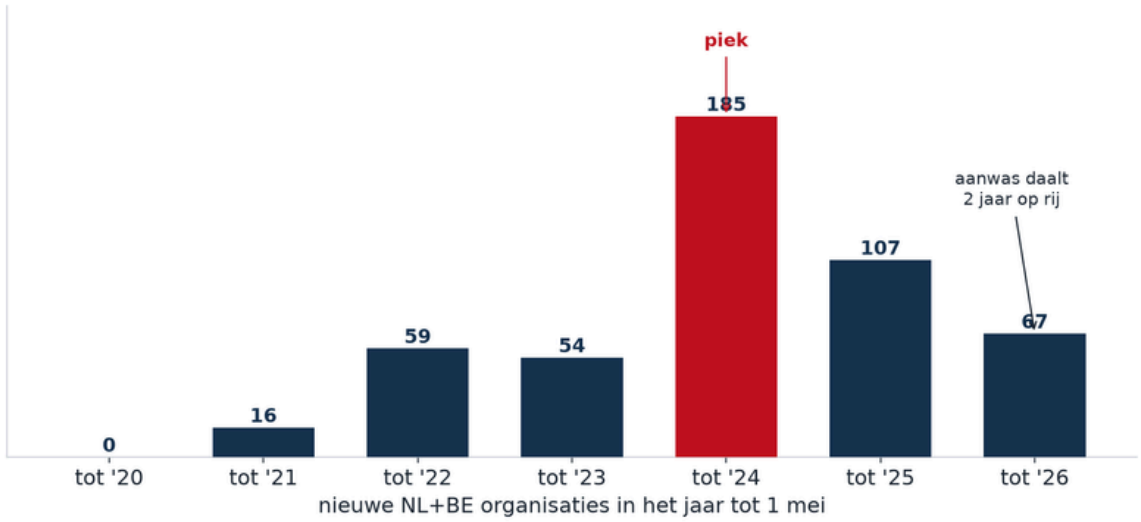


Belangrijkste beweging: LockBit viel weg na Operation Cronos (2024), Qilin nam de leiding over.

Bron: Cybercrimeinfo · 1-mei-master (NL/BE/wereldwijd) + darkwebmonitor · gepubliceerde slachtoffers, een ondergrens

Jaarlijkse aanwas NL + België vlakt af

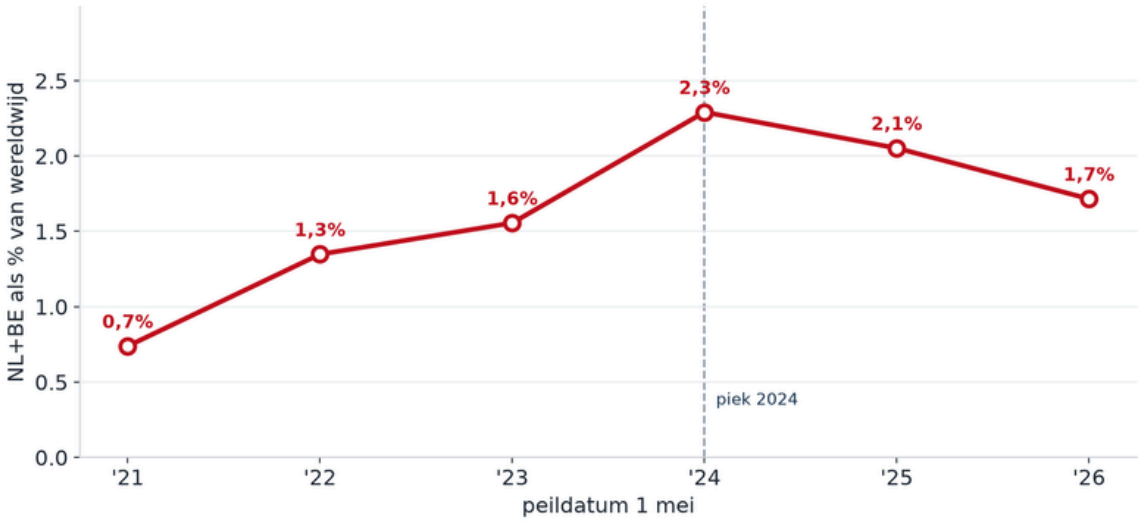
Na de piek in 2024 (185) daalt de aanwas twee jaar op rij · elk jaar is een afgesloten meting



Bron: Cybercrimeinfo, meetpunt 1 mei (cumulatief) · NL/BE/wereldwijd master

NL en België wegen steeds minder zwaar in de wereldcijfers

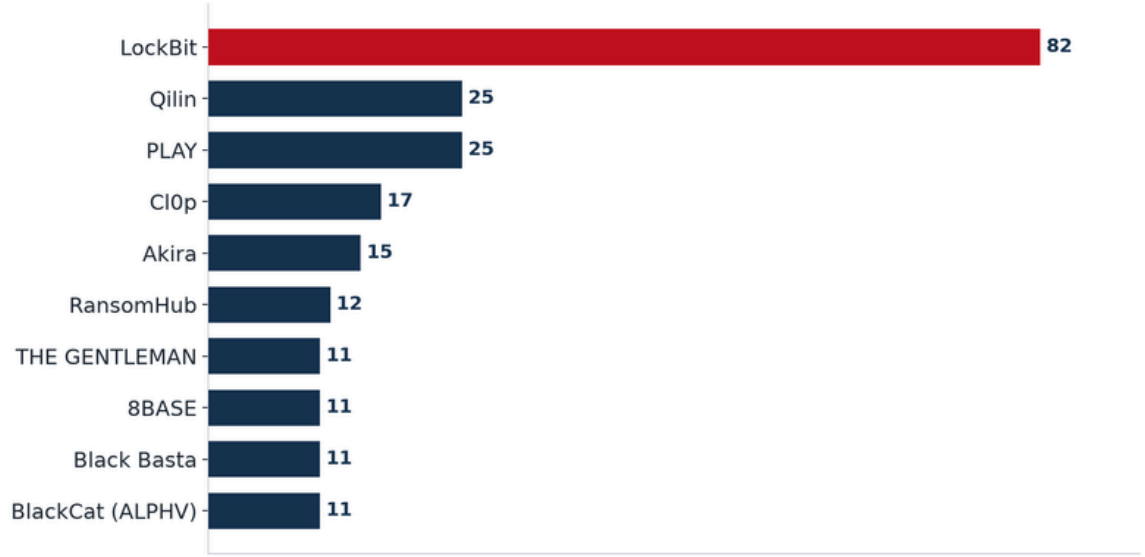
Aandeel piekte in 2024 op 2,3% en zakt terug naar 1,7% · wereldwijd blijft juist versnellen



Bron: Cybercrimeinfo, meetpunt 1 mei (cumulatief) · NL/BE/wereldwijd master

Meest actieve ransomwaregroepen, 2020-2026

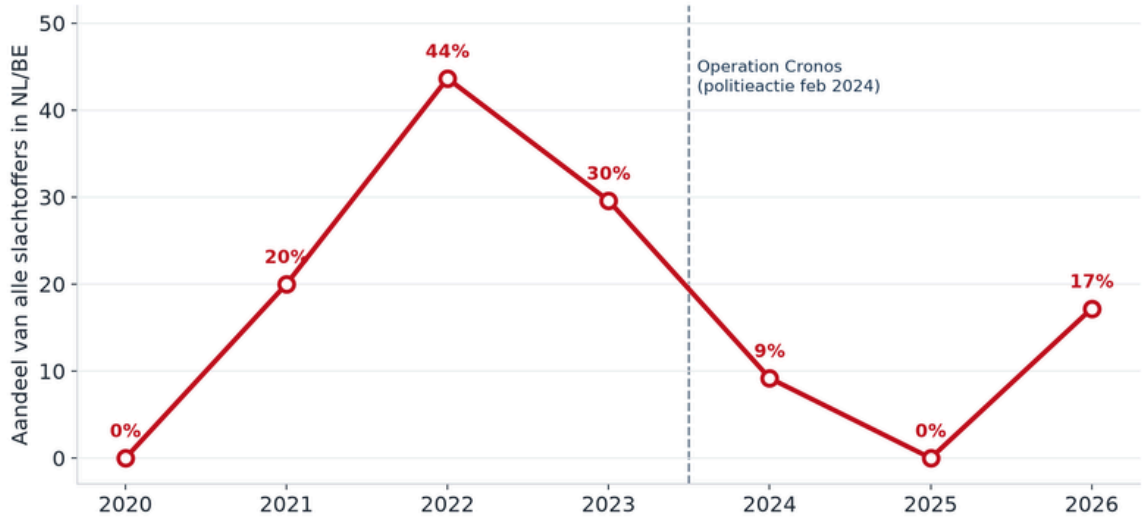
LockBit domineert historisch · top 3 = 29% van alle incidenten



Bron: Cybercrimeinfo darkwebmonitor · indicatief (ondergrens), groep/sector niet in de 1-mei-master

De val en terugkeer van LockBit

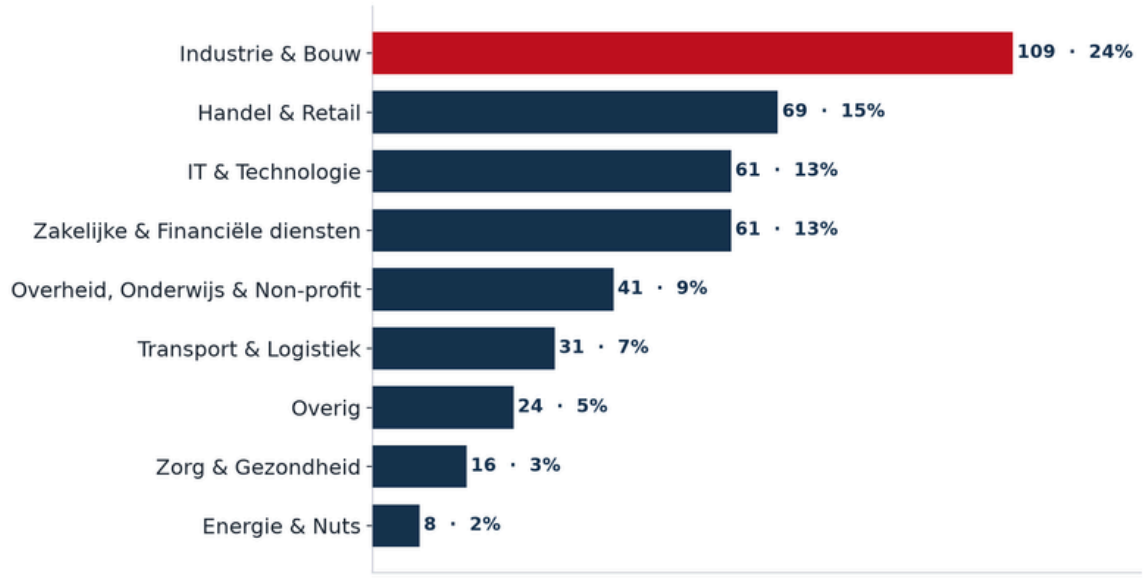
Van 44% marktaandeel (2022) naar 0% (2025) · comeback in 2026



Bron: Cybercrimeinfo darkwebmonitor · indicatief (ondergrens), groep/sector niet in de 1-mei-master

Zwaarst getroffen sectoren

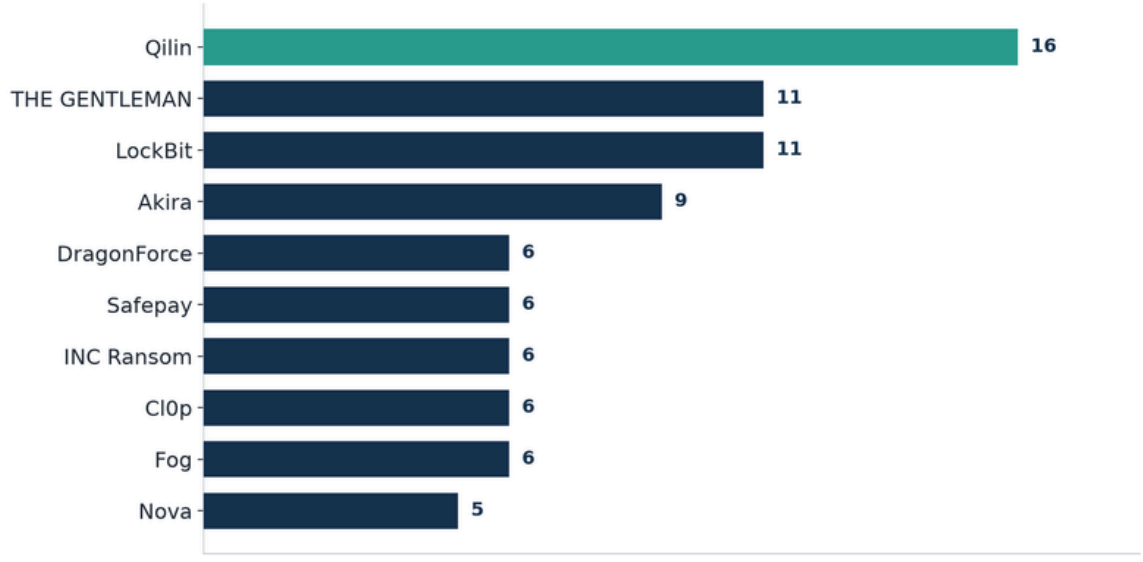
Industrie & bouw is doelwit nr. 1 · zorg blijft opvallend gespaard



Bron: Cybercrimeinfo darkwebmonitor · indicatief (ondergrens), groep/sector niet in de 1-mei-master

Wie vormt nú de dreiging, 2025-2026

Qilin is de nieuwe koploper · sterk versnipperd landschap (102 groepen totaal)



Bron: Cybercrimeinfo darkwebmonitor · indicatief (ondergrens), groep/sector niet in de 1-mei-master

06. Conclusies

1. De groei vlakt af, maar de dreiging blijft groot

De jaarlijkse groei van het aantal nieuwe Nederlandse en Belgische organisaties dat op ransomware-leksites verschijnt, is de afgelopen twee meetjaren afgenomen. Toch blijft het aantal geregistreerde organisaties historisch hoog. Wereldwijd neemt het aantal nieuwe registraties nog altijd toe, wat onderstreept dat de ransomwaredreiging onverminderd groot blijft.

Het meest recente meetpunt is nog voorlopig. Organisaties verschijnen soms pas maanden later op een ransomware-leksite, waardoor de uiteindelijke toename over het afgelopen meetjaar hoger kan uitvallen dan nu zichtbaar is.

2. België passeert Nederland

Op 1 mei 2026 telde België voor het eerst meer geregistreerde organisaties dan Nederland. Daarmee komt België binnen deze meetreeks voor het eerst boven Nederland uit. Op basis van de beschikbare data kan niet worden vastgesteld waardoor deze ontwikkeling wordt veroorzaakt.

3. Het ransomwarelandschap blijft veranderen

De dominante positie van LockBit is de afgelopen jaren afgenomen, terwijl nieuwe groepen zoals Qilin snel terrein hebben gewonnen. Tegelijkertijd laat de terugkeer van LockBit zien dat internationale verstoringen of politieacties niet automatisch leiden tot het verdwijnen van een ransomwaregroep.

4. Industrie en bouw het vaakst getroffen

Binnen de geanalyseerde dataset zijn organisaties uit de industrie- en bouwsector het vaakst slachtoffer van ransomwarepublicaties. Ook handel, IT en zakelijke dienstverlening zijn sterk vertegenwoordigd. Daarnaast laat de aanwezigheid van meer dan 100 verschillende ransomwaregroepen zien dat het dreigingslandschap sterk is versnipperd.

5. Actuele dreigingsinformatie blijft essentieel

De cijfers in dit rapport vormen een ondergrens van het werkelijke aantal ransomwareaanvallen, omdat uitsluitend organisaties zijn meegenomen waarvan gegevens openbaar zijn gepubliceerd op ransomware-leksites. Continue monitoring van het dreigingslandschap blijft daarom essentieel om ontwikkelingen tijdig te signaleren en passende maatregelen te kunnen nemen.

07. Methodologie

Dit jaarrapport is gebaseerd op gegevens uit de Cyber Dreigingsradar van Digiweerbaar.

Voor de analyses zijn meerdere databronnen gecombineerd om een zo volledig en betrouwbaar mogelijk beeld te geven van de actuele ransomwaredreiging.

Gebruikte databronnen:

- Cyber Dreigingsradar (Digiweerbaar) - primaire bron voor de analyses en trendontwikkeling.
- Cybercrimeinfo.nl - historische dataset met ransomwarepublicaties van Nederlandse en Belgische organisaties.
- Openbare ransomware-leksites en andere openbare dreigingsbronnen - gebruikt voor validatie en verrijking van de analyses.

Voor dit rapport zijn twee datasets gebruikt. De cumulatieve dataset (peildata: 1 mei 2025 en 1 mei 2026) vormt de basis voor de analyses van de wereldwijde ontwikkelingen en de vergelijking tussen Nederland en België.

De historische incidentdataset (2020 t/m juli 2026) is gebruikt voor de verdiepende analyses van ransomwaregroepen, sectoren en trends.

Verantwoording & disclaimer

Dit rapport is met de grootst mogelijke zorg samengesteld door Digiweerbaar B.V. op basis van gegevens uit de Cyber Dreigingsradar, Cybercrimeinfo.nl en andere openbare bronnen.

De gepresenteerde cijfers hebben uitsluitend betrekking op organisaties waarvan gegevens openbaar zijn gepubliceerd op ransomware-leksites. De werkelijke omvang van ransomware-incidenten ligt naar verwachting hoger.

Hoewel de informatie zorgvuldig is samengesteld, kunnen aan de inhoud van dit rapport geen rechten worden ontleend. Digiweerbaar B.V. aanvaardt geen aansprakelijkheid voor eventuele onjuistheden of de gevolgen van het gebruik van deze informatie.

Digiweerbaar.nl
Bescherm wat waardevol is

Van inzicht naar actie

De Cyber Dreigingsradar helpt organisaties continu inzicht te houden in actuele cyberdreigingen, ransomware, kwetsbaarheden en ontwikkelingen.

Daarmee ondersteunt de Cyber Dreigingsradar organisaties bij het invullen van hun risicobeheer en dreigingsmonitoring, zoals bedoeld in de NIS2-richtlijn en de Cyberbeveiligingswet.

NIS2

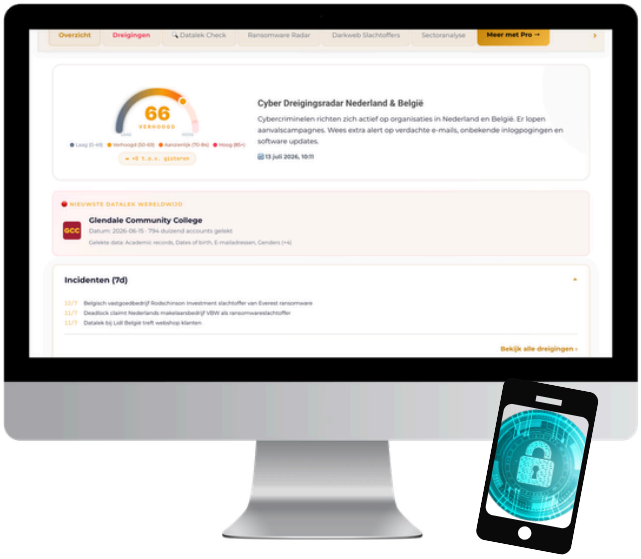
✓ **Dagelijks** bijgewerkte dreigingsinformatie

✓ Ransomware- en darkwebmonitoring

✓ Kritieke kwetsbaarheden (CVE's)

✓ Actuele dreigingen in **Nederland** en **België**

✓ **Gratis** toegankelijk



Gratis aanmelden:

www.digiweerbaar.nl/dreigingsradar/aanmelden

info@digiweerbaar.nl

www.digiweerbaar.nl