TLP:CLEAR

Jaarbeeld Ransomware 2025

Samen brengen wij ransomware in Nederland in beeld

In 2025 hebben het Nationaal Cyber Security Centrum (NCSC), de Politie, het Openbaar Ministerie, Cyberveilig Nederland en cybersecuritybedrijven maandelijks informatie over ransomware-incidenten uitgewisseld in het kader van project Melissa. Deze uitwisseling geeft beter inzicht in hoe vaak en op welke manier organisaties in Nederland worden getroffen door ransomware-incidenten. Want over hoe meer actuele informatie we beschikken, hoe effectiever we ransomware kunnen bestrijden.

In dit jaarbeeld baseren we ons op gecompileerde maandelijkse incident-informatie van de incident-response bedrijven **DEFION Security, DataExpert, Deloitte, Eye Security, Fox-IT, NFIR, Northwave, Tesorion, Kennedy Van der Laan, PwC,** het NCSC en de aangifte cijfers van de Politie over de periode van januari t/m december 2025.

National Cyber Security Centre Ministry of Security and Justice · OM · POLITIE · CYBERVEILIG NEDERLAND

Een jaar aan gedeelde ransomware-incidenten in beeld

Op basis van anoniem delen van informatie: vermoedelijk **92** unieke incidenten.

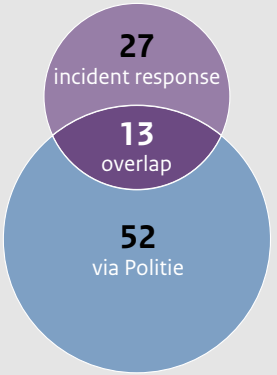
Op basis van maandelijks terugkerende uitvraag en aangiftes van januari t/m december 2025.

Via **10** cybersecurity-dienstverleners, NCSC en de Politie.

Samen meer zicht op ransomware

Door data van incident-response bedrijven te combineren met aangiftedata, maken we ransomware-incidenten inzichtelijk: in 2025 waren er **40** incidenten waarbij deelnemende incident-response bedrijven te hulp schoten en van **65** incidenten is aangifte gedaan bij de Politie. Zowel het aantal incidenten bij incident-response bedrijven als het aantal aangiftes is minder dan in 2024.

Niet elk slachtoffer van ransomware wordt bijgestaan door een van de deelnemende incident-response bedrijven of doet aangifte. Het daadwerkelijke aantal incidenten ligt daarom waarschijnlijk hoger.



Accountovername of kwetsbaarheid vaak gebruikt voor initiële toegang bij ransomware-incidenten

Net als vorig jaar, wordt toegang meestal verkregen door misbruik van kwetsbaarheden en accountovernames. Relatief meer incidenten begonnen met een account-overname in 2025, ten opzichte van 2024.

Een accountovername is vaak het gevolg van gestolen authenticatiegegevens. Infostealers, phishing en Adversary-in-the-Middle (AitM) worden veel ingezet voor het stelen van de gegevens die nodig zijn voor het overnemen van een account. Bij veel van de incidenten waarbij een kwetsbaarheid werd misbruikt, betrof het een kwetsbaarheid in een systeem dat direct vanaf het internet toegankelijk was.[1]
Daarnaast is de inzet van zero-day[2] kwetsbaarheden voor initiële toegang bij een aantal afpersingscampagnes illustratief voor de capabiliteit die enkele cybercriminelen hebben [1, 2]. Voorgaande jaren lieten cybercriminelen ook al zien deze capabiliteit te hebben [3]. Op basis van de beschikbare data is er geen significant verband gevonden tussen de gebruikte methode voor initiële toegang en de daaropvolgende gebruikte ransomware-varianten.

Zorg ervoor dat de basismaatregelen op orde zijn om weerbaarheid te vergroten [4].

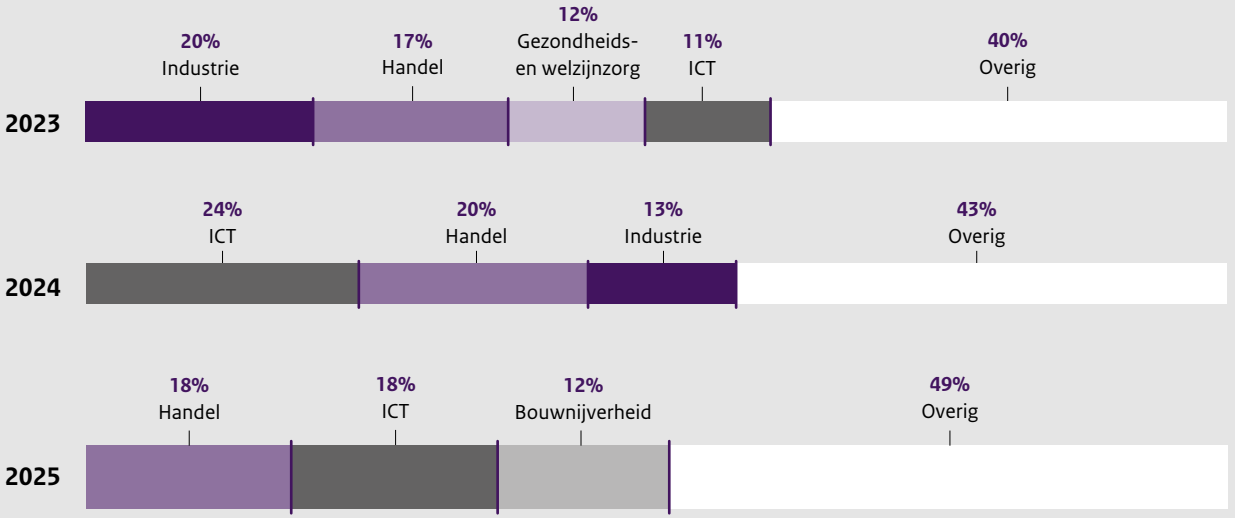
55%
Account take-over

30%
Misbruik van kwetsbaarheden

TLP:CLEAR

De 3 meest getroffen sectoren, vergeleken met voorgaande jaren

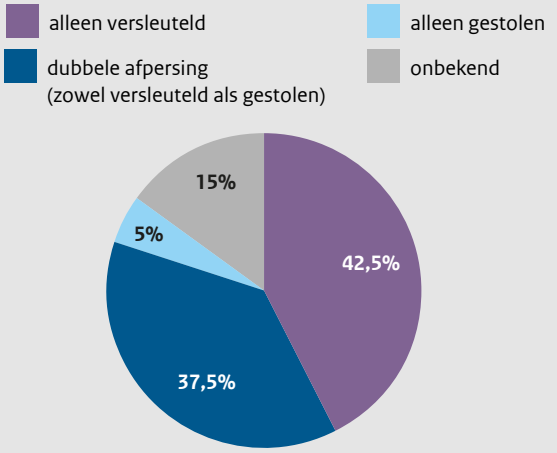
Diverse oorzaken, zoals kwetsbaarheden in technologie die veel wordt gebruikt in een sector, kunnen (tijdelijk) de kans op ransomware-aanvallen in een specifieke sector vergroten.



Dubbele afpersing

In 2025 werd naast versleuteling van data, bij veel van de incidenten ook data gestolen voor (dubbele) afpersing. Met dubbele afpersing zetten criminelen het slachtoffer nog meer onder druk. Vaak wordt gedreigd de gestolen data te publiceren of te verkopen.

Daarnaast worden slachtoffers regelmatig afgeperst door criminelen die data stelen, maar niet versleutelen.



Veranderingen in het ransomware-landschap

De Nederlandse incidenten werden veroorzaakt door diverse ransomware-families. De meest voorkomende ransomware-families in Nederland, waren Akira, Qilin, PLAY, INCransom en verschillende versies van LockBit. Ransomhub, verantwoordelijk voor een groot deel van de incidenten in 2024, is dit jaar aanzienlijk minder dominant: alleen in het eerste kwartaal van 2025 werd activiteit van deze variant waargenomen.

Meer dan de helft van de incidenten werd veroorzaakt door een van de vijf meest voorkomende ransomware-families.

In totaal zijn er **39** unieke ransomware-families waargenomen.

Herstelvermogen

Back-ups en verzekeringen voorkomen niet dat jouw organisatie schade lijdt. Zorg daarom dat de basis-maatregelen op orde zijn en doe altijd aangifte.

43% van de incidenten had een langere hersteltijd dan 3 dagen, **15%** herstelde na een week of later.

41% van de slachtoffers was verzekerd.

72% van de slachtoffers had een bruikbare back-up.

33% van de slachtoffers deed aangifte.

Nieuwe deelnemers welkom

Alleen samen maken we ons beeld van ransomware in Nederland completer en maken we een vuist tegen ransomware. Staat uw bedrijf ransomware slachtoffers bij? Dan bespreken wij graag met u de mogelijkheden en het belang van deelname aan project Melissa. Mail voor meer informatie naar info@cyberveilignederland.nl.

Verantwoording cijfers

Dit jaarbeeld is gebaseerd op gegevens van cybersecurity-dienstverleners en de politie. De incidenten zijn zorgvuldig beoordeeld door security-experts, die een scherpe afbakening van de definitie van ransomware hanteren . Grote en middelgrote organisaties (vanaf ca. 50 fte) zijn in ongeveer 40% van de gevallen zichtbaar in deze bronnen, terwijl dit voor het MKB slechts 10-15% is [5].
Dit suggereert dat het werkelijke aantal ransomware-aanvallen 2-3 keer hoger ligt voor grote en middelgrote bedrijven en tot 10 keer hoger voor kleine bedrijven. De hier genoemde cijfers bieden een schatting van unieke incidenten, aangezien volledige controle op dubbeltellingen door anonimisatie niet mogelijk is.

Eindnoten

1 Veel van de misbruikte kwetsbaarheden in technologie die vanaf het internet toegankelijk is, zitten in edge-apparaten. Meer over edge-apparaten: [7]

2 Een zwakke plek (kwetsbaarheid) in software of hardware, die nog niet bij de ontwikkelaar ervan bekend is [6].

3 “De naam ransomware is een samenvoeging van de woorden ransom (losgeld) en software. De aanvallers gijzelen data van het slachtoffer en gebruiken drukmiddelen om het slachtoffer over te halen te betalen. In sommige gevallen slaan daders de encryptie stap over en gaan direct over tot uploaden.” [8, p. 4]

Bronnen

[1] Google Threat Intelligence Group, “Oracle E-Business Suite Zero-Day Exploited in Widespread Extortion Campaign,” Google Cloud, januari 2026. [Online]. Available: https://cloud.google.com/blog/topics/threat-intelligence/oracle-ebusiness-suite-zero-day-exploitation.

[2] Nationaal Cyber Security Centrum (NCSC), “Ernstige kwetsbaarheid in Oracle E-Business Suite,” Nationaal Cyber Security Centrum (NCSC), 6 oktober 2025. [Online]. Available: https://www.ncsc.nl/waarschuwing/ernstige-kwetsbaarheid-oracle-e-business-suite.

[3] Nationaal Cyber Security Centrum (NCSC), “NCSC waarschuwt voor Cl0p-campagnes die zich richten op filetransfer-systemen,” Nationaal Cyber Security Centrum (NCSC), 6 februari 2025. [Online]. Available: https://www.ncsc.nl/nieuws/ncsc-waarschuwt-voor-cl0p-campagnes-die-zich-richten-op-filetransfer-systemen.

[4] Nationaal Cyber Security Centrum, “Basisprincipes,” Nationaal Cyber Security Centrum, 19 december 2025. [Online]. Available: https://www.ncsc.nl/basisprincipes.

[5] T. Meurs, M. Junger, M. Cruyff and P. G. M. V. D. Heijden, “Estimating the Number of Ransomware Attacks,” 31 augustus 2024. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4942706.

[6] Nationaal Cyber Security Centrum, “Edge devices uitgelegd,” Nationaal Cyber Security Centrum, januari 2026. [Online]. Available: https://www.ncsc.nl/edge-devices/edge-devices-uitgelegd.

[7] Nationaal Cyber Security Centrum, “Wat is een zero-day?,” Nationaal Cyber Security Centrum, januari 2026. [Online]. Available: https://www.ncsc.nl/kwetsbaarhedenbeheer/wat-is-een-zero-day.

[8] Cyberveilig Nederland, “Cyberveilig Nederland publiceert Whitepaper Ransomware met leden, Politie en NCSC,” [Online]. Available: https://cyberveilignederland.nl/upload/userfiles/files/CVNL_Ransomware_def.pdf.