Ransomware-aanvallen op instellingen en bedrijven in Nederland

dr. Tessel Blom, ir. Wazir Sahebali, Kimberly Deppe MSc,
ing. Peter Romijn, Floris Donath, ir. ing. Reg Brennenraedts MBA

In opdracht van:
Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)

Publicatienummer:
2022.173-2319

Datum:
Utrecht, 7-8-2023

Inhoudsopgave

Dank aan begeleidingscommissie voor hun waardevolle reacties in commentaren op dit rapport. De begeleidingscommissie bestond uit prof. em. dr. Marianne Junger (Universiteit Twente), dr. ir. Harald Vranken (Open Universiteit), dr. Rolf van Wegberg (TU Delft), L.W. Kröner (Ministerie van Justitie en Veiligheid) en dr. Simon Zebregs (WODC).

Citeren als: Dialogic, Blom, T., Sahebali, W., et al. (2023). *Ransomware-aanvallen op instellingen en bedrijven in Nederland*. WODC, Den Haag.

Managementsamenvatting

Introductie

In opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (hierna: WODC) heeft Dialogic Innovatie en Interactie (hierna: Dialogic) een onderzoek naar ransomware-aanvallen op instellingen en bedrijven in Nederland uitgevoerd. Het WODC is op zoek naar indicatoren die de omvang en de aard van deze ransomware-aanvallen in kaart kan brengen. Op basis van deze indicatoren moet er een beeld gevormd worden van ransomware-aanvallen in de jaren 2020, 2021 en 2022. Daarnaast moeten de beperkingen van deze indicatoren en databronnen onderzocht worden. Het onderzoek beantwoordt de volgende onderzoeksvragen:

1. Met **welke indicatoren** kan inzicht worden gekregen in de mate waarin ransomware-aanvallen op instellingen en bedrijven in Nederland voorkomen en de aard en gevolgen van deze aanvallen met betrekking tot de eigenschappen van de getroffen instellingen en bedrijven, de response op de aanvallen, de geleden schade en andere gevolgen?
2. Bevatten **bestaande databronnen** gegevens die inzicht bieden in de relevante indicatoren?
3. **Welk beeld** kan aan de hand van de bestaande databronnen worden gevormd voor **de jaren 2020, 2021 en 2022** over de mate waarin ransomware-aanvallen op instellingen en bedrijven in Nederland voorkomen en de aard en gevolgen van deze aanvallen met betrekking tot de eigenschappen van de betrokken instellingen en bedrijven, de response op de aanvallen, de geleden schade en andere gevolgen?
4. **Welke beperkingen** hebben de bestaande databronnen met betrekking tot de beschikbaarheid, volledigheid en kwaliteit van data en in hoeverre gelden er andere beperkingen?
5. Op welke wijze kunnen deze beperkingen worden **verminderd of weggenomen**?

Voor de uitvoering van dit onderzoek is gebruik gemaakt van verschillende dataverzamelingsmethodes: literatuuronderzoek, interviews, analyse van politieaangifte data[1] en web scraping.

Deel 1: Theoretische achtergrond

De indicatoren van ransomware

Databronnen zullen in veel gevallen slechts inzicht kunnen geven in een bepaald aspect van een ransomware-aanval. De indicatoren, die op basis van literatuuronderzoek en interviews relevant zijn gebleken, zijn:

- **Generieke kenmerken van een ransomware-aanval**. Deze indicator beslaat de aanvaller, het doelwit, de wijze waarop toegang is verkregen en de acties die gebruikt worden om druk uit te oefenen op het slachtoffer.

[1] Verkregen binnen het PhD-onderzoek van Tom Meurs naar de aard en omvang van ransomware binnen Nederland.

- **Kenmerken van het slachtoffer**. Bij deze indicator gaat het specifiek over de kenmerken van het slachtoffer, zoals de sector, de grootte of de locatie van de organisatie.
- **Impact van een ransomware-aanval**. Deze indicator brengt de gevolgen van een ransomware-aanval voor de individuele organisatie of de maatschappij in kaart.
- **Frequentie van ransomware-aanvallen**. Bij deze indicator gaat het niet om een specifieke ransomware-aanval, maar hoe vaak bepaalde ransomware-aanvallen op bepaalde slachtoffers met een bepaalde impact plaatsvinden.

De stappen in een ransomware-aanval

De meeste databronnen kunnen slechts inzicht geven in een bepaalde stap van een ransomware-aanval. Daarmee bevatten ze alleen informatie over een bepaalde groep slachtoffers. Bij elke opeenvolgende stap in een ransomware-aanval wordt deze groep slachtoffers kleiner. In dit onderzoek verwijzen wij naar verschillende groepen onder de slachtoffers als *subsets*.

Deel 2: Databronnen

In dit onderzoek zijn onderstaande databronnen geanalyseerd. Elke databron geeft inzicht in een subset van slachtoffers en een beperkte hoeveelheid indicatoren:

1. **Virusscanaanbieders** hebben vaak detectiemechanismes voor ransomware en hebben dus zicht op het aantal pogingen tot een ransomware-aanval.
2. **IT-dienstaanbieders** hebben zicht op verdachte activiteiten van de cybercrimineel wanneer deze binnen is gedrongen.
3. **Incident response bedrijven** worden door het slachtoffer ingeschakeld om de response op de ransomware-aanval te coördineren.
4. **Cybersecurity-verzekeraars** worden door het slachtoffer ingelicht bij een ransomware-aanval en zijn ook betrokken bij de afhandeling.
5. **Politieaangiftes**. Bij een ransomware-aanval kan een slachtoffer hier bij de politie aangifte van doen, maar is hier niet toe verplicht.
6. De **CBS Cybersecuritymonitor** bevraagt een selectie van Nederlandse organisaties of ze het afgelopen jaar te maken hebben gehad met een ransomware-aanval en wat daar de impact van is geweest.
7. De **media** rapporteren over bepaalde ransomware-aanvallen en hebben daarmee ook deels invloed op de impact van aanvallen op de maatschappij. Daarnaast vervullen de media een belangrijke rol als het gaat om de bewustwording van ransomware.
8. Op **websites van ransomware-groepen** wordt gedreigd met het publiceren van gestolen data van slachtoffers en wordt deze data gepubliceerd als er geen losgeld is betaald.
9. De **Autoriteit Persoonsgegevens** heeft zicht op het aantal bij de AP gemelde datalekken. Slachtoffers van een ransomware-aanval moeten, bij een vermoeden van een datalek, een melding maken bij de AP.
10. Het **cryptobetalingsverkeer** bevat losgeldbetalingen naar ransomware-groepen.
11. **No More Ransom** biedt voor bepaalde ransomware-software *decryptors* aan waarmee de versleutelde bestanden ontsleuteld kunnen worden.

Het beeld van ransomware voor de jaren 2020, 2021 en 2022

De bestaande databronnen geven geen eenduidig beeld van ransomware-aanvallen op Nederlandse bedrijven en instellingen voor de jaren 2020, 2021 en 2022. Veel databronnen zijn te generiek, waardoor het bijvoorbeeld niet mogelijk is om er specifiek informatie voor

Nederland uit te halen, of ze beslaan niet de volledige periode 2020, 2021, 2022. Daarnaast spelen er bij een aantal partijen ook commerciële belangen mee of is de informatie die partijen publiekelijk beschikbaar maken zeer beperkt. Desalniettemin schetsen we hieronder per indicator een beeld.

Generieke kenmerken van ransomware-aanvallen

Aanvaller: Het cryptobetalingsverkeer laat in de jaren 2020, 2021 en 2022 zien dat het marktaandeel van de verschillende ransomware-groepen over de tijd sterk schommelt. Het oprollen van een groep leidt vaak tot het ontstaan van nieuwe groepen met een nieuwe software. Deze diversiteit aan ransomware-groepen is ook terug te zien in de rapportages van de virusscanaanbieders, waar vele verschillende ransomware *strains* gedetecteerd worden. Analyses van de websites van ransomware-groepen laten zien dat de LockBit groep in 2021 en 2022 verantwoordelijk is voor de meeste datalekken van Nederlandse organisaties.

Doelwit: Virusscanaanbieders laten zien dat er wereldwijd een toename is van gerichte aanvallen in 2021. Ook tonen deze virusscanaanbieders dat de opkomst van Ransomware-as-a-Service met name te zien is bij consumenten, maar minder bij de grote bedrijven en MKB'ers.

Initiële toegang: Zowel de IT-dienstaanbieders als de incident response bedrijven zeggen dat e-mail de meest gebruikte methode is van initiële toegang (*phishing*), gevolgd door desktop sharing software in de jaren 2020, 2021 en 2022.

Acties om druk uit te oefenen: Er is geen bron die inzicht geeft in de verhouding tussen de verschillende acties die gebruikt kunnen worden (blokkeren, versleutelen, data exfiltratie). Wel hebben we in de interviews opgehaald dat het stelen van data steeds gangbaarder wordt (vaak zelfs zonder de bestanden te versleutelen), terwijl het blokkeren van systemen tegenwoordig minder vaak voorkomt.

Kenmerken van slachtoffer

Locatie: De websites van ransomware-groepen, waar zij slachtoffers publiceren, laten zien dat Nederland in de periode 2021 en 2022 in de lijst van gepubliceerde organisaties op plek 12 staat. Amerikaanse organisaties worden het vaakst gepubliceerd. Ook bij de IT-dienstaanbieders bevinden de meeste slachtoffers van ransomware in de Verenigde Staten.

Sector: De industriële en financiële sectoren worden wereldwijd volgens de incident response bedrijven het vaakst getroffen. Uit de CBS cybersecuritymonitor komen ook de sectoren *industrie* en *financiële dienstverlening* naar voren als meest getroffen. De meeste politieaangiftes van ransomware komen uit de handelssector. Deze bronnen houden andere sectorverdelingen aan, maar wijzen wel met name naar organisaties in de industrie. Ten opzichte van 2020 was er in 2021 een verdubbeling van het aantal aangiftes uit de ICT-sector. Deze toename van aanvallen op de ICT-sector wordt ook beaamd door de Autoriteit Persoonsgegevens, die in 2021 de aanvallen op IT-leveranciers uitlichtten.

Grootte: De CBS Cybersecuritymonitor laat zien dat hoe groter de organisatie is (c.q. hoe meer werkzame personen), hoe groter de kans is dat de organisatie te maken heeft gehad met een ransomware-aanval. Ook de Autoriteit Persoonsgegevens zegt in 2020 voornamelijk meldingen van datalekken te hebben gehad van grotere organisaties die over veel persoonsgegevens beschikken. Leden van het Verbond van Verzekeraars geven daarentegen aan dat zij zien dat met name de kleinere MKB bedrijven door een afhankelijkheid van een enkel systeem en lage bewustwording slachtoffer worden van ransomware.

Impact van ransomware-aanvallen

Losgeld: Incident response bedrijven geven aan dat het aandeel van de aanvallen waarin tot het betalen van losgeld wordt overgegaan over de jaren 2020, 2021, 2022 flink is gedaald. Ook het cryptobetalingsverkeer laat zien dat er ten opzichte van 2020 en 2021 een omslag is geweest in 2022, waarbij alle slachtoffers samen veel minder losgeld betaald hebben. In de periode van juni 2022 tot juni 2023 zijn er daarnaast 32% van de gepubliceerde organisaties van de website van LockBit verwijderd. Organisaties worden vaak van de website verwijderd als ze losgeld betaald hebben. Dat impliceert dat ongeveer een derde van de LockBit slachtoffers die gepubliceerd zijn alsnog betaald hebben. Hier zat slechts één Nederlandse organisatie tussen. Tegenover de daling in de betalingsbereidheid staat wel een stijging in het gemiddeld betaalde losgeldbedrag in die periode. Uit politieaangiftes blijkt dat de gevraagde losgeldbedragen bij Nederlandse slachtoffers in de handel- en ICT-sector gemiddeld boven de miljoen euro uitkomen. Het betaalde losgeldbedrag bedraagt voor kleine bedrijven een groter percentage van de totale omzet dan voor grotere bedrijven (CBS Cybersecuritymonitor).

Kosten: Naast het betalen van losgeld kunnen ransomware-aanvallen ook andere kosten met zich meebrengen, zoals bijvoorbeeld de verstoring van de bedrijfscontinuïteit, het verlies van klanten door reputatieschade, het herstellen van de IT-systemen of het inschakelen van een incident response bedrijf. De politieaangiftes laten zien dat het gevraagde losgeldbedrag in veel gevallen disproportioneel hoog is en dat de geleden financiële schade door een ransomware-aanval uiteindelijk vaak lager ligt.

Frequentie van ransomware-aanvallen

Volgens rapportages van de verzekeraars (op basis van enquêtes) is 26% van de Nederlandse bedrijven in 2022 getroffen door ransomware. In 2021 en 2022 zijn er respectievelijk 107 en 110 aangiftes van ransomware binnengekomen bij de politie. De politie vermoedt dat slechts 2% tot 4% van de slachtoffers aangifte doet. Dat dit percentage laag is komt ook naar voren uit de CBS Cybersecuritymonitor, waar slechts 13% van de bedrijven aangeeft hulp te hebben gezocht bij de politie. Van de organisaties die bevraagd zijn in de cybersecuritymonitor van het CBS zegt slechts 1% een ransomware-aanval te hebben gehad in 2021. Analyses van berichtgeving in de media suggereert dat ransomware met name een 2021 een groot thema was.

Beperkingen

Geen enkele databron in dit onderzoeksrapport is vrij van beperkingen. Een eerste beperking is de beschikbaarheid van (relevante) data. Een aantal databronnen (zoals de virusscanaanbieders, IT-dienstaanbieders, incident response bedrijven en de cybersecurity-verzekeraars) hebben commerciële belangen. Zij publiceren mede daarom geen ruwe data, maar alleen rapportages. Deze rapportages bevatten vaak figuren en conclusies waarvan de oorsprong lastig te achterhalen is, maar die wel een verhaal vertellen dat de noodzaak van deze partijen onderschrijft. Doordat het ook onduidelijk is op basis van welke data of klantsegment de figuren zijn gemaakt, kunnen de resultaten uit de verschillende databronnen ook niet worden gecombineerd. Daarnaast zijn er partijen als het NCSC en de Autoriteit Persoonsgegevens die momenteel niet aan datadeling doen (de AP geeft echter wel aan hiermee bezig te zijn). Een tweede beperking, die voor de meeste databronnen geldt, is dat de databronnen niet specifiek zijn toegespitst op Nederlandse bedrijven en instellingen. De focus van veel databronnen ligt op Noord-Amerika of is wereldwijd. De enige databronnen zich specifiek focussen op Nederland zijn de politieaangiftes, de datalekmeldingen bij de Autoriteit Persoonsgegevens en de uitkomsten van de CBS Cybersecuritymonitor.

Daarnaast is geen enkele databron volledig. Eerder bespraken we al dat databronnen slechts inzicht kunnen geven in een subset van slachtoffers, maar ook daarin zijn ze vaak niet volledig. Zo doen lang niet alle slachtoffers aangifte van een ransomware-aanval of belanden alle slachtoffers van data-exfiltratie op de websites van ransomware-groepen.

Tenslotte is de kwaliteit van de data in sommige gevallen niet toereikend voor het in kaart brengen van ransomware-aanvallen op Nederlandse bedrijven en instellingen. Het steekproefsgewijs bevragen van Nederlandse organisaties over hun ervaringen met ransomware zou een goed beeld moeten kunnen geven van de problematiek. Echter verschilt het percentage tussen de verschillende enquêtes wel heel erg sterk. Uit de enquêtes van de banken en verzekeraars lijkt de frequentie van ransomware overschat te worden, terwijl deze in de CBS Cybersecuritymonitor juist onderschat lijkt te worden. Het probleem bij de banken en verzekeraars ligt waarschijnlijk in de gekozen steekproef (waar disproportioneel veel slachtoffers inzitten), terwijl die bij de CBS Cybersecuritymonitor mogelijk in de vraagstelling ligt. De meeste resultaten uit de rapportages van commerciële partijen voldoen ook niet aan de standaarden van reproduceerbaarheid, waardoor de kwaliteit van de resultaten niet vast te stellen is.

Aanbevelingen

Een centraal punt waar verschillende instanties hun data (geanonimiseerd en/of geaggregeerd) aan kunnen rapporteren zou enkele beperkingen van databronnen (die nu alleen rapportages uitbrengen) weg kunnen nemen. Incident response bedrijven, die zijn benaderd en in Nederland opereren, zeggen dat ze incidenten melden aan het NCSC. Daarnaast beschikt de Autoriteit Persoonsgegevens over meldingen van datalekken en kunnen slachtoffers in het meldproces aangeven dat het over een ransomware-aanval gaat. Zowel het NCSC als de AP delen deze data nu niet (ook niet met elkaar). Ook zou dit centrale punt bij bijvoorbeeld de virusscanbedrijven specifiek data over Nederlandse klanten uit kunnen vragen en de indexeerwebsites van ransomware-groepen kunnen monitoren voor Nederlandse slachtoffers.

Uit een vooronderzoek bleek al dat CBS-wet grondslag biedt voor verplichte data levering door overheidsorganisaties aan het CBS. Het CBS zou, in ieder geval voor overheidsorganisaties, kunnen fungeren als een centraal punt voor data van ransomware-aanvallen. Deze verplichting geldt niet voor commerciële partijen, zoals de verzekeraars, de virusscanaanbieders en de IT-dienstaanbieders. De overheid moet onderzoeken onder welke voorwaarden deze partijen bereid zijn data te delen over aanvallen op Nederlandse organisaties.

Daarnaast zouden slachtoffers meer gestimuleerd moeten worden om aangifte te doen bij de politie. De informatie die uit politieaangiftes komt is zeer rijk, maar helaas doet maar een klein percentage van de slachtoffers aangifte. Mogelijk zouden de verzekeraars hier een rol in kunnen spelen door een aangifte als voorwaarde te stellen voor het uitkeren van het schadebedrag (zoals bijvoorbeeld ook het geval is bij diefstal).

Tenslotte zou de CBS Cybersecuritymonitor uitgebreid en aangepast kunnen worden. De vraagstelling, en dan met name de gegeven voorbeelden, zijn nu erg beperkend. Ze richten zich bijvoorbeeld uitsluitend op *locker* ransomware (terwijl dat weinig meer voorkomt) en vragen niks over versleuteling van documenten of data-exfiltratie. Ook lijken sommige resultaten te impliceren dat niet de juiste persoon binnen een organisatie de vragenlijst heeft ingevuld. Het uitvragen van het kennisniveau van de respondent zou een juiste interpretatie van de resultaten bevorderen. Ook zou een grotere steekproef gewenst zijn, zodat alle subcategorieën (verschillende vormen van ransomware, losgeldbedragen, wel of niet betaald, gemaakte kosten, maar ook bedrijfssector en -grootte) groot genoeg zijn. Slachtoffers van ransomware zijn mogelijk eerder geneigd deel te nemen aan een enquête over ransomware,

dus het zal geen representatief beeld geven van de frequentie van ransomware op Nederlandse instellingen, maar het zou de verhoudingen binnen de groep slachtoffers wel beter in kaart kunnen brengen.

Voor het vormen van een betrouwbaar beeld aan de hand van bestaande databronnen doen wij op basis van bovenstaande vier concrete aanbevelingen:

1. Onderzoek hoe de barrières voor het delen van data over ransomware slachtoffers, zoals de privacy wetgeving, kunnen worden weggenomen (bijvoorbeeld door anonimisering of aggregatie). Stimuleer vervolgens datadeling van overheidsorganisaties als het NCSC, de Autoriteit Persoonsgegevens en de Politie met een centraal punt als het CBS. Artikel 33 van de CBS-wet biedt grondslag voor verplichte datalevering door overheidsorganisaties aan het CBS. Het combineren (en indien mogelijk koppelen) van data over ransomware van (in ieder geval) de overheidsorganisaties is een belangrijke eerste stap naar het vormen van een beeld van de ransomware problematiek.
2. De overheid moet onderzoeken onder welke voorwaarden commerciële partijen zoals de virusscanaanbieders, IT-dienstaanbieders en de verzekeraars bereid zijn data te delen over aanvallen op Nederlandse organisaties. Dit gebeurt idealiter met hetzelfde centrale punt als waarmee de overheidsorganisaties communiceren. Deze commerciële partijen bezitten informatie die overheidsorganisaties niet kunnen vergaren, maar delen deze data niet en rapporteren hier ook niet of nauwelijks over. Daarnaast zijn de rapportages van deze commerciële partijen opgesteld uit eigen belang en vertellen vaak een eenzijdig verhaal dat erop gericht is meer klanten aan te trekken.
3. Onderzoek op welke manier de aangiftebereidheid onder slachtoffers van ransomware verhoogd kan worden. Er zou bijvoorbeeld onderzocht kunnen worden of verzekeraars hier een rol in kunnen spelen door een aangifte als voorwaarde te stellen voor het uitkeren van het schadebedrag (zoals bijvoorbeeld ook het geval is bij diefstal). Politieaangiftes zijn een zeer rijke bron van informatie als het gaat over de kenmerken van het slachtoffer en de impact van de ransomware-aanval, maar momenteel doet slechts een fractie van de slachtoffers aangifte. Daarnaast worden overkoepelende trends uit de aangiftes over de kenmerken van aanvallen gebruikt door het ransomware *taskforce* om de cybercriminelen op te sporen en uit te schakelen.
4. Benut landelijke enquêtes of monitors als de CBS Cybersecuritymonitor beter door de steekproef te vergroten en de vraagstelling met betrekking tot ransomware uit te breiden en te verbeteren. Het landelijk bevragen van organisaties is een goede methode voor het in kaart brengen van de frequentie van ransomware-aanvallen, de kenmerken van de aanvallen en slachtoffers en de impact van ransomware-aanvallen. De huidige resultaten doen echter vermoeden dat het aantal bevraagde organisaties dat in het afgelopen jaar daadwerkelijk slachtoffer was van ransomware erg klein was. Hierdoor kan op basis van deze resultaten geen betrouwbaar beeld gevormd worden van ransomware-aanvallen op Nederlandse bedrijven. Wanneer een organisatie benaderd wordt voor het invullen van de enquête en aangeeft te maken te hebben gehad met een ransomware-aanval, zouden de kenmerken van de aanval, de kenmerken van het slachtoffer en de impact van de ransomware-aanval in detail en voor zover bekend uitgevraagd moeten worden.

1 Introductie

1.1 Inleiding

In opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (hierna: WODC) heeft Dialogic Innovatie en Interactie (hierna: Dialogic) een onderzoek naar ransomware-aanvallen op instellingen en bedrijven in Nederland uitgevoerd. In dit hoofdstuk wordt de aanleiding van het onderzoek besproken (paragraaf 2). Daarna worden de doelstelling en de onderzoeksvragen (paragraaf 3) en de aanpak van het onderzoek op hoofdlijnen (paragraaf 4) behandeld.

1.2 Aanleiding onderzoek

Ransomware wordt gezien als een groeiend probleem. In het Cybersecuritybeeld Nederland 2021 is ransomware benoemd als risico voor de nationale veiligheid. [1] De impact van een ransomware-aanval, waarbij vaak de gehele bedrijfsvoering van een organisatie stilligt, kan zeer groot zijn voor de maatschappij en de economie. Ransomware-aanvallen kunnen ongericht zijn en als doel hebben om vooral zoveel mogelijk computers te blokkeren. Een voorbeeld hiervan is de WannaCry aanval in 2017. [2] Er lijkt echter een ontwikkeling te zijn geweest waarbij de aandacht is verschoven naar gerichte aanvallen op instellingen en bedrijven waarvan wordt verwacht dat zij bereid zijn om een grote som losgeld te betalen. [3] Zo zorgde een aanval op containerterminals in de Rotterdamse haven in 2017 voor een schade van naar verluidt enkele honderden miljoenen euro's. [4] Andere voorbeelden van gerichte ransomware-aanvallen met grote impact zijn die op de Universiteit Maastricht, het ROC Mondriaan en de Gemeente Hof van Twente.

Op dit moment bestaat er geen volledig beeld van de ransomware-aanvallen op instellingen en bedrijven in Nederland en de schade die daaruit voortkomt. Dit gebrek aan inzicht in de omvang en aard van het fenomeen hindert een effectieve aanpak van ransomware. Het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA) geeft in haar *Threat landscape* voor ransomware-aanvallen aan dat er weinig betrouwbare informatie is voor het kwantificeren en analyseren van ransomware-aanvallen. [5] Er zijn veel verschillende organisaties die ieder voor zich informatie hebben over een deel van de ransomware-aanvallen in Nederland en veel incidenten belanden alleen bij private partijen, waardoor de overheid slecht geïnformeerd is. Cybersecuritybedrijven hebben inzicht in de hoeveelheid slachtoffers van ransomware-aanvallen die zij ieder jaar ondersteunen en de hoeveelheid losgeld die daar (eventueel) bij wordt betaald. Leden van het Verbond van Verzekeraars hebben informatie over geclaimde schadebedragen n.a.v. ransomware-aanvallen. Sommige organisaties publiceren op basis van hun eigen data rapportages waarin ze onder andere ingaan op de prevalentie van ransomware-aanvallen. Daarnaast beschikt de politie over de aangiftes die ieder jaar worden gedaan van ransomware en het NCSC en de Autoriteit Persoonsgegevens over de meldingen die bij hen worden gedaan. Ransomware is echter een wereldwijd probleem en het is niet duidelijk in hoeverre het beeld dat wordt geschetst in dergelijke individuele rapportages representatief is voor de situatie in Nederland.

De ambitie is om uiteindelijk in staat te zijn de prevalentie van ransomware-aanvallen en de aard daarvan te kunnen monitoren. Het voorgenomen onderzoek is een eerste stap richting het verwezenlijken van deze ambitie. Hiervoor dient eerst te worden vastgesteld welke indicatoren van belang zijn om de omvang en aard van ransomware-aanvallen op instellingen en bedrijven in Nederland in kaart te brengen. Vervolgens dient te worden vastgesteld welk beeld op basis van bestaande databronnen met betrekking tot deze indicatoren kan worden gevormd voor de jaren 2020, 2021 en 2022 en op welke manier de beperkingen van de

beschikbare data zouden kunnen worden verholpen. Aan de hand van de resultaten van het onderzoek moet kunnen worden vastgesteld welke vervolgstappen nodig zijn om de ransomware-aanvallen op instellingen en bedrijven in de toekomst te kunnen monitoren.

Box 1. CBS vooronderzoek.

Het CBS heeft in opdracht van het NCSC in 2022 een verkenningsonderzoek gedaan naar de beschikbaarheid van data bij Nederlandse partijen over aanvallen met ransomware. In dit onderzoek werd aan de hand van gesprekken met een aantal (overheids)organisaties gekeken of het praktisch en juridisch mogelijk was om datasets te verzamelen en te koppelen waarmee ransomware-aanvallen bij bedrijven in beeld gebracht kunnen worden. Uit dit vooronderzoek kwam naar voren dat artikel 33 van de CBS-wet grondslag biedt voor verplichte datalevering door overheidsorganisaties aan het CBS, maar niet voor verplichte levering door private organisaties. Het CBS verwacht hierdoor dat het mogelijk wel (deels) praktisch haalbaar is om datasets voor het maken van een statistiek over aanvallen met ransomware bij bedrijven te verzamelen en te koppelen, maar dat dergelijk onderzoek wel een langere doorlooptijd zal kennen en een aantal risico's zal hebben.

1.3 Onderzoeksvragen

Het WODC vraagt om inzichten rondom de frequentie en impact van ransomware-aanvallen op Nederlandse bedrijven en instellingen. Ze is op zoek naar indicatoren die de omvang en de aard van deze ransomware-aanvallen in kaart kan brengen. Op basis van deze indicatoren moet er een beeld gevormd worden van ransomware-aanvallen in de jaren 2020, 2021 en 2022. Daarnaast moeten de beperkingen van deze indicatoren en databronnen onderzocht worden. Hiertoe heeft het WODC een vijftal onderzoeksvragen geformuleerd:

1. Met **welke indicatoren** kan inzicht worden gekregen in de mate waarin ransomware-aanvallen op instellingen en bedrijven in Nederland voorkomen en de aard en gevolgen van deze aanvallen met betrekking tot de eigenschappen van de getroffen instellingen en bedrijven, de response op de aanvallen, de geleden schade en andere gevolgen?
2. Bevatten **bestaande databronnen** gegevens die inzicht bieden in de relevante indicatoren?
3. **Welk beeld** kan aan de hand van de bestaande databronnen worden gevormd voor **de jaren 2020, 2021 en 2022** over de mate waarin ransomware-aanvallen op instellingen en bedrijven in Nederland voorkomen en de aard en gevolgen van deze aanvallen met betrekking tot de eigenschappen van de betrokken instellingen en bedrijven, de response op de aanvallen, de geleden schade en andere gevolgen?
4. **Welke beperkingen** hebben de bestaande databronnen met betrekking tot de beschikbaarheid, volledigheid en kwaliteit van data en in hoeverre gelden er andere beperkingen?
5. Op welke wijze kunnen deze beperkingen worden **verminderd of weggenomen**?

1.4 Onderzoeksaanpak

Bij het bepalen van nieuwe indicatoren zijn grofweg twee methodes mogelijk. [6] Er kan een ideale indicator worden bepaald en hierbij de data worden gezocht die hier invulling aan geeft. Of er kan op basis van de data die beschikbaar is een indicator worden bepaald. In onze ervaring is de tweede methode vaak de meest geschikte. Bij de eerste methode blijkt

vaak dat de gewenste data niet beschikbaar is. Maar ook als deze een iets andere vorm heeft, dan zal de indicator moeten worden aangepast. In dit onderzoek verwachten wij dat (hoogwaardige) data over dit onderwerp relatief schaars zal zijn. We hebben daarom een aanpak centraal gesteld waarbij de beschikbare data de indicatoren bepaalt.

Voor de uitvoering van dit onderzoek is gebruik gemaakt van verschillende methoden. Hieronder geven we een overzicht van deze methoden. De toepassing van de onderzoeksmethoden op de verschillende databronnen zal per databron toegelicht worden:

- **Literatuuronderzoek**: Er zijn online veel overzichten te vinden van verschillende partijen die rapporteren over ransomware-aanvallen in zowel Nederland als buitenland. Hierbij valt te denken aan virusscanaanbieders, software aanbieders, incident response bedrijven en (cybersecurity-)verzekeraars. In deze rapportages is gezocht naar observaties die betrekking hebben op de frequentie en impact van ransomware-aanvallen in het algemeen en op Nederlandse bedrijven specifiek. Er is overigens relatief weinig wetenschappelijke, actuele, *peer reviewed* literatuur beschikbaar over de frequentie en impact van ransomware. Dat betekent dat er ook veel bronnen zijn gebruikt die geschreven zijn door marktpartijen die mogelijk een belang hebben bij bepaalde uitkomsten. Daarnaast zal een deel van de *grijze literatuur* gebaseerd zijn op minder grondig onderzoek dan bij wetenschappelijke literatuur typisch het geval is.
- **Interviews**: Er zijn in het kader van dit onderzoek 11 personen geïnterviewd afkomstig uit verschillende groepen respondenten. In Bijlage 1 is een overzicht opgenomen van alle interviewrespondenten. Van elk interview is een verslag gemaakt dat ter validatie is teruggelegd aan de respondent. Deze interviewverslagen zijn niet openbaar en alleen beschikbaar voor het onderzoeksteam.
- **Web scraping**: Om data te verzamelen die gepubliceerd wordt door de ransomware-groepen hebben wij gebruik gemaakt van *web scraping*. Bij web scraping worden websites op geautomatiseerde wijze bezocht en informatie van deze websites binnengehaald. Hierbij hebben wij zowel bestaande overzichten van aanvallen van ransomware-groepen binnengehaald als informatie van individuele *leak sites* op het darkweb.
- **Data-analyse**: Data uit verschillende bronnen (zoals de CBS Cybersecuritymonitor, politieaangiftes, leak sites en nieuwsartikelen) zijn verwerkt en geanalyseerd om trends van de frequentie en de impact van ransomware-aanvallen inzichtelijk te maken.

Deel 1: Theoretische achtergrond

2 Inleiding

Voor het in kaart brengen van de mate waarin ransomware-aanvallen op instellingen en bedrijven in Nederland voorkomen, en de aard en de gevolgen van deze aanvallen, zullen meerdere databronnen nodig zijn. Elke databron zal op zichzelf namelijk een beperkt beeld geven. Deze beperking kan enerzijds komen doordat een databron alleen informatie bevat van een *bepaalde indicator* en niet een volledig beeld van de omvang, aard en gevolgen van ransomware-aanvallen kan geven. Anderzijds zullen de meeste databronnen slechts inzicht geven in een bepaalde fase van een ransomware-aanval en daarmee alleen informatie hebben over een *subset van slachtoffers*. In dit deel beschrijven we deze twee assen (indicatoren en subsets van slachtoffers) waarlangs we in het tweede deel van dit rapport elke databron zullen leggen.

3 De indicatoren van ransomware

Het doel van dit onderzoek is om een beeld te krijgen van ransomware-aanvallen op Nederlandse bedrijven en instellingen. De eerste stap hierin is het vaststellen van de indicatoren die hiervoor van belang zijn. Databronnen zullen in veel gevallen slechts inzicht kunnen geven in een beperkt aantal indicatoren. De indicatoren, die op basis van literatuuronderzoek en interviews relevant zijn gebleken, zijn:

- **Generieke kenmerken van een ransomware-aanval**. Deze indicator beslaat de ransomware-groep, het doelwit, de wijze waarop toegang is verkregen en de acties die gebruikt worden om druk uit te oefenen op het slachtoffer.
- **Kenmerken van het slachtoffer**. Bij deze indicator gaat het specifiek over de kenmerken van het slachtoffer, zoals de sector, de grootte of de plek in de keten van de organisatie.
- **Impact van een ransomware-aanval**. Deze indicator brengt de gevolgen van een ransomware-aanval voor de individuele organisatie of de maatschappij in kaart.
- **Frequentie van ransomware-aanvallen**. Bij deze indicator gaat het niet om een specifieke ransomware-aanval, maar hoe vaak bepaalde ransomware-aanvallen op bepaalde slachtoffers met een bepaalde impact plaatsvinden.

3.1 Generieke kenmerken van een ransomware-aanval

Ransomware-aanvallen kunnen op verschillende manieren geclassificeerd worden. Uit de informatie die beschikbaar is in de bestaande databronnen is gebleken dat de meest informatieve indicatoren voor het in kaart brengen van ransomware-aanvallen 1) de ransomware-groep is die de aanval heeft uitgevoerd, 2) het doelwit van de aanval, 3) de wijze waarop toegang is verkregen en 4) de acties die gebruikt zijn om druk uit te oefenen op het slachtoffer om het losgeldbedrag te betalen.

3.1.1 De ransomware-groep

Ransomware kent vele verschillende groepen en actoren, met vele **verschillende organisatiestructuren**. Bij de opkomst van ransomware werd een aanval van begin tot eind veelal uitgevoerd door één organisatie. Rond 2016 kwam **Ransomware-as-a-service (RaaS)** op. Deze opkomst wordt gezien als een mijlpaal in de organisatorische evolutie van ransomware en zorgde ervoor dat ransomware groepen gingen opereren als ware bedrijven. RaaS is een bedrijfsmodel waarbij de ransomware-software door een organisatie (de *operator*), middels licenties, aangeboden wordt aan andere cybercriminelen (de *affiliates*). [7] Een individu of een groep kan dan de software aanschaffen die geschikt is voor het doelwit dat voor ogen is. [8]

De meeste aanvallen worden uitgevoerd door **een groep van specialisten**. Figuur 1 toont de zogeheten *ransomware kill chain*. Elke stap in deze *chain* kent specialisten die dit ofwel als dienst aanbieden, of samenwerken met andere specialisten om zo zeer effectieve, gecombineerde aanvallen uit te voeren. [1] Ransomware-aanvallen kunnen geclassificeerd worden naar de vlag van de organisatie waaronder de ransomware-aanval is uitgevoerd.

Figuur 1. De ransomware kill chain. Bron: NCTV. [1]

3.1.2 Het doelwit

Ransomware-aanvallen kunnen verschillende typen doelwitten hebben, zowel qua **platform** als qua **slachtoffer**.

Platform

Ransomware kan verschillende typen platforms aanvallen en vervolgens infecteren: PCs/werkplekken, mobiele toestellen, IoT-apparaten/cyber-fysieke systemen, servers en clouddiensten. [9] Gezien de koppeling tussen dergelijke platforms onderling kan een infectie ook overspringen van het ene naar het andere platform. Zo kan een aanval op individuele PCs bijvoorbeeld gebruikt worden om een server of cloudopslag te infecteren.

De meeste ransomware-aanvallen vinden plaats op **PCs en werkplekken** (en dan met name PCs met Windows OS). Ransomware die enkel de toegang tot het systeem blokkeert (*locker* ransomware) op PCs kan vaak relatief makkelijk verholpen worden door de computer te rebooten of door de harde schijf op een ander systeem aan te sluiten. [10, 11] Het is daarentegen een stuk lastiger om versleutelde bestanden te decoderen. Cryptographic ransomware is daarom een groter gevaar voor computers. [9]

De toename van het gebruik van **mobiele toestellen** zoals smartphones maken deze ook een mogelijk doelwit voor ransomware. In 2013 werd de eerste locker ransomware voor Android gebruikers gesignaleerd. Een jaar later werd ook de eerste cryptographic ransomware voor Android smartphones gedetecteerd. [12]

Momenteel is er nog weinig ransomware die **IoT-apparaten** als doelwit heeft. [9] Er wordt echter wel al lange tijd voor deze vorm van ransomware gewaarschuwd. In 2015 werd voor het eerst ransomware gedetecteerd die bestanden op een smartwatch versleutelde en in 2016 werd een Android smart TV door ransomware gelocked. [13, 14] De potentiële dreiging die uitgaat van ransomware op IoT apparaten is echter groot. Met de implementatie van IoT apparaten in onder andere smart homes, smart cities en smart grids ligt het voor de hand dat deze ook vaker doelwit zullen worden van ransomware. Daarbij zal met name de timing en context van de aanval cruciaal zijn. Veel IoT apparaten bevatten geen data en kunnen met een simpele reboot verlost zijn van ransomware, maar wanneer bijvoorbeeld een pacemaker geïnfecteerd is, zullen slachtoffers mogelijk snel overgaan tot betaling. [15]

Slachtoffer

Ransomware kan grofweg twee slachtoffer types maken: consumenten en organisaties. Ransomware-aanvallen op **consumenten** zijn vaak ongericht, waarbij het de aanvaller niet uitmaakt welke organisatie of persoon het slachtoffer wordt. [11] Een enkele ransomware kan duizenden systemen van eindgebruikers infecteren. Echter leidt dit vaak tot lagere losgeld bedragen. Met name de eerste ransomware *strains* hadden eindgebruikers als doelwit. [9]

Met de evolutie van ransomware werden **organisaties** steeds vaker het doelwit van ransomware-aanvallen. In dit soort (vaak) gerichte aanvallen worden slachtoffers van tevoren uitgekozen en wordt veelal gebruik gemaakt van *off the shelf*-tools en bekende zwakheden in systemen. [9] Omdat voor dergelijke zwakheden in de regel al wel patches (updates) beschikbaar zijn, leidt dit ertoe dat met name organisaties die geen of onvoldoende updates toepassen een groter risico lopen om hier slachtoffer van te worden. [16, 11]

Cybercriminelen kunnen meerdere redenen hebben om een specifieke organisatie aan te vallen. Zo kan een organisatie gebruik maken van een bekende zwakheid in de beveiliging waardoor de aanval een hoge kans van slagen heeft. Ook kunnen organisaties uitgekozen worden omdat ze mogelijk een hoge betalingsbereidheid hebben. Dit kan zijn omdat een groot aantal andere bedrijven van ze afhankelijk is, zoals bijvoorbeeld een ICT-leverancier, waardoor de druk om te betalen mogelijk hoger is. Ook kunnen organisaties bijvoorbeeld een cyberverzekering hebben die het betalen van losgeld vergoedt waardoor ze mogelijk makkelijker losgeld betalen. Ransomware groepen acteren wat dat betreft vaak zeer rationeel en maken een simpele kosten-baten analyse: bij welke organisaties is het mogelijke losgeldbedrag hoog en zijn de kosten om binnen te komen laag? De acties die gebruikt worden om druk uit te oefenen op het slachtoffer (*extortion* methodes) hangen ook af van de kenmerken van het slachtoffer en de ketenafhankelijkheid. Deze lichten we in de hier opvolgende paragrafen verder toe.

3.1.3 Initiële toegang

Ransomware-aanvallen kunnen ook geclassificeerd worden naar de wijze waarop toegang tot het systeem verkregen is (*initial access*). Aanvallers kunnen bijvoorbeeld gebruik maken van **phishing e-mails** of van **zwakke of bekende wachtwoorden**. [11] Daarnaast kunnen ze ook **zwakke plekken** in applicaties of systemen exploiteren of zelf **applicaties** uitbrengen die betrouwbaar ogen, maar waarbij de gebruiker onbewust ransomware installeert. [9] De methode van infectie zal ook afhangen van het platform dat doelwit is.

3.1.4 De acties om druk uit te oefenen

Tenslotte kunnen we aanvallen nog classificeren naar de wijze waarop slachtoffers onder druk worden gezet om te betalen. Ransomware kent twee hoofdcategorieën: *cryptors* en *lockers*. *Cryptographic* ransomware versleutelt, verwijdert of overschrijft de bestanden van het slachtoffer. *Locker* ransomware voorkomt dat het slachtoffer toegang heeft tot zijn of haar systemen door het te locken. In tegenstelling tot crytographic ransomware worden bestanden dan niet versleuteld. [9]

Locking ransomware kan het systeem (middels het toegangsscherm of de web browser) **blokkeren**. Om weer toegang tot het systeem te krijgen moet het slachtoffer vervolgens losgeld betalen. Ook kan de Master Boot Record, dat informatie bevat om het systeem op te starten, overschreven of versleuteld worden. [9] Deze laatste manier kan vergaande gevolgen hebben, omdat het ook na het betalen van losgeld moeite kost alles te herstellen. [17] Onder andere de ransomware Petya overschreef de Master Boot Record. [18, 19]

Het **versleutelen van bestanden** kan op verschillende wijzen gebeuren. Bij symmetrische encryptie wordt dezelfde sleutel gebruikt om bestanden te versleutelen en te ontsleutelen. Deze manier van encryptie kan snel een grote hoeveelheid bestanden versleutelen, maar de aanvaller moet de sleutel ook verstoppen voor het slachtoffer: wanneer het slachtoffer de sleutel vindt, kan deze zelf de bestanden ontsleutelen. Voor symmetrische encryptie is verbinding met een *Command and Control* (C&C) server essentieel voor het communiceren van de encryptiesleutel. [20] Het beschermen van de sleutel is geen probleem bij asymmetrische encryptie. Bij asymmetrische encryptie worden een publieke en een privé sleutel gebruikt.

De publieke sleutel kan onderdeel zijn van de ransomware, waardoor begonnen kan worden met het versleutelen voordat er verbinding is met de C&C server. Deze manier van encryptie is echter minder efficiënt in het versleutelen van een grote hoeveelheid bestanden. Bij hybride encryptie worden alle bestanden eerst snel versleuteld middels symmetrische encryptie. Daarna wordt de symmetrische sleutel versleuteld met de publieke sleutel van de aanvaller (asymmetrisch). Omdat deze publieke sleutel meegegeven wordt aan de ransomware is een connectie met de C&C server niet noodzakelijk. [9]

Wanneer aanvallers zowel bestanden versleutelen als (gevoelige) **data stelen** is er sprake van *double extortion*. Aanvallers kunnen dan dreigen met het lekken of verkopen van deze data om het slachtoffer onder druk te zetten te betalen. Slachtoffers lijken sneller bereid te betalen omdat de gestolen data gevoelige (persoons-)gegevens van werknemers en/of klanten kan bevatten. Daarnaast is er angst voor reputatieschade of het verlies van (eigen) intellectuele eigendom aan derden. Ook is soms de schade van datapublicatie zo groot dat slachtoffers van een ransomware-aanval zelfs betalen als ze de versleutelde bestanden kunnen herstellen met een back-up. De inhoud van de gestolen data heeft een grote invloed op de impact van een ransomware-aanval. Het stelen van data wordt steeds gangbaarder, soms zelfs zonder de bestanden te versleutelen, terwijl het blokkeren van systemen tegenwoordig minder vaak voorkomt. [21]

Als de aanvaller data versleutelt, steelt en probeert het herstelproces te belemmeren is er sprake van *triple extortion*. Voor het belemmeren van het herstelproces kunnen er bijvoorbeeld Distributed Denial of Service (DDoS) aanvallen worden ingezet. Dit heeft als doel om het slachtoffer te verstoren bij het terugrollen van eventuele back-ups, zodat de schade wordt vergroot (en de druk om losgeld te betalen hoger wordt). Bij *quadruple extortion* benadert de dader ook nog de klanten van het slachtoffer om hen te informeren dat hun data gestolen is. Hiermee probeert de dader de druk nog verder op te voeren. [11]

3.2 Kenmerken van het slachtoffer

Zoals in de vorige sectie besproken kunnen ransomware-aanvallen *gericht* of *ongericht* zijn. Uit de literatuur en de interviews blijkt dat met name de gerichte aanvallen, waar de ransomware-groepen een organisatie uitkiezen en deze gericht aanvallen, toenemen. Om een beeld te krijgen van de problematiek rondom ransomware-aanvallen in Nederland is het daarom van belang om de kenmerken van deze organisaties in kaart te brengen.

Ten eerste zullen we kijken naar de **sector** waar een organisatie onderdeel van is. Hierbij houden we, waar mogelijk, de sectorindeling (SBI) van het CBS aan. Wanneer sectoren (relatief of absoluut) vaak getroffen worden, zegt dit mogelijk iets over de beveiligingsstandaarden in die sector, over de hoeveelheid aanwezige gevoelige data die uitgebuit kan worden door de cybercriminelen of over de afhankelijkheid van continuïteit in de bedrijfsvoering.

Daarnaast kan er ook gekeken worden naar de **grootte** van de instelling. Dit kan worden uitgedrukt in het aantal werkzame personen bij de instelling, maar ook in bijvoorbeeld de omzet of het aantal klanten. Wanneer er sprake is van *double extortion*, en er daadwerkelijk data gelekt wordt, kan het **aantal** slachtoffers van een datalek snel oplopen. Bij een aanval op IT-leveranciers of bij een marketingbureau kunnen bijvoorbeeld miljoenen e-mailadressen gecompromitteerd zijn.

3.3 Impact van ransomware-aanvallen

De impact die een ransomware-aanval heeft op een organisatie of de maatschappij is van vele factoren afhankelijk. Het hangt bijvoorbeeld af van de aard van de ransomware: zijn

alleen de systeem geblokkeerd of zijn er ook bestanden versleuteld en gestolen? Daarnaast kunnen sommige aanvallen in potentie ontwrichtende gevolgen hebben voor de maatschappij (zoals een aanval op bijvoorbeeld een netbeheerder), terwijl andere met name de individuele organisatie benadelen. Daarnaast kan er ook nog onderscheid gemaakt worden in korte- en lange termijn effecten van een datalek. Persoonsgegevens die rondzwerven zonder weten van het slachtoffer kunnen vele jaren later nog gevolgen hebben, bijvoorbeeld wanneer een kopie van een paspoort gebruikt wordt voor identiteitsfraude.

3.3.1 Impact op individuele organisaties

De impact van een ransomware-aanval op een individuele organisatie is deels afhankelijk van de kenmerken van de organisatie zelf. Wanneer een organisatie afhankelijk is van de beschikbaarheid van IT-systemen en data, bijvoorbeeld voor productie of het betalen van uitkeringen, kan de impact van **de verstoring van de bedrijfscontinuïteit** groot zijn. Andere organisaties hebben hier allicht minder last van en kunnen prima een aantal dagen doorkomen zonder toegang tot IT-systemen en bestanden. Organisaties die daarentegen sterk afhankelijk zijn van data, zoals bijvoorbeeld een marketingbureau, zullen daarentegen een grote impact ervaren van een ransomware-aanval wanneer deze **data gestolen wordt en op straat komt te liggen**. Daarnaast kan het leiden tot **reputatieschade** die het aantrekken van toekomstige klanten bemoeilijkt.

Daarnaast kunnen de **kosten** die gemaakt worden bij de response op een ransomware-aanval een grote impact hebben op de bedrijfsvoering. Hierbij valt bijvoorbeeld te denken aan kosten als:

- De inzet van een incident response bedrijf;
- Het betalen van losgeld;
- Het herstellen van IT-systemen.

Daarnaast bestaat de kans dat de kwaliteit van de beschikbare back-ups of het ontsleutelen niet perfect zijn. In dat geval zal er ook nog een restschade zijn.

3.3.2 Impact op de maatschappij

Een ransomware-aanval op een organisatie kan ook een bredere impact op de maatschappij en de **nationale veiligheid** hebben. Deze impact hangt bijvoorbeeld af van de sector waarin de organisatie zich bevindt of de plek in de keten van de organisatie. Het NCSC focust met name op ransomware-aanvallen bij partijen in de **vitale sectoren**. Bepaalde processen zijn zo essentieel voor de Nederlandse samenleving dat uitval of verstoring tot ernstige maatschappelijke ontwrichting leidt. Deze processen vormen de Nederlandse vitale infrastructuur. Hierbij valt te denken aan elektriciteit, toegang tot internet, drinkwater of betalingsverkeer. [22] Daarnaast opereren veel bedrijven in een **keten**. Een verstoring in de bedrijfscontinuïteit van een bedrijf vroeg in de keten kan gevolgen hebben voor andere bedrijven verderop in de keten. [11]

Het stelen van data heeft daarnaast niet alleen impact op de organisatie, maar ook op de **burgers** wiens gegevens gestolen zijn. Zo kunnen kopieën van een paspoort bijvoorbeeld leiden tot identiteitsfraude. Wanneer de identiteit van een bepaalde burger ook een bepaalde waarde heeft, zoals bijvoorbeeld die van miljonairs of bekende Nederlanders, kan de impact van een ransomware-aanval groter zijn. Daarnaast kan een ransomware-aanval die op het eerste gezicht geen hele bijzondere aanval is door **media-aandacht** toch een grote impact op de maatschappij hebben.

3.4 Frequentie van ransomware-aanvallen

Uit de interviews blijkt dat puur de frequentie van ransomware-aanvallen op zichzelf geen goede indicator is van de problematiek. Niet elke ransomware-aanval is namelijk hetzelfde: een aanval op een lokaal opererende MKB'er wordt bijvoorbeeld gezien als een kleiner probleem dan een aanval op een netbeheerder. De frequentie-indicator wordt betekenisvol als die uitgesplitst kan worden naar kenmerken ransomware-aanval, kenmerken slachtoffer of impact van aanval.

4 De stappen in een ransomware-aanval

Het doel van dit onderzoek is om de databronnen en indicatoren die inzicht geven in de omvang en aard van ransomware-aanvallen in Nederland in kaart te brengen. In het vorige hoofdstuk hebben we de relevante indicatoren besproken. In dit hoofdstuk bespreken we, met het oog op mogelijke databronnen, de verschillende stappen in een ransomware-aanval en de verschillende subsets van slachtoffers die bij elke stap ontstaan.

Eerder haalden we al de veelgebruikte ransomware kill-chain aan. Deze kill-chain bestaat uit de stappen:

1. Verkrijgen van initiële toegang;
2. Consolideren van positie;
3. Wegsluizen van informatie;
4. Inzetten van ransomware;
5. Financiële afhandeling.

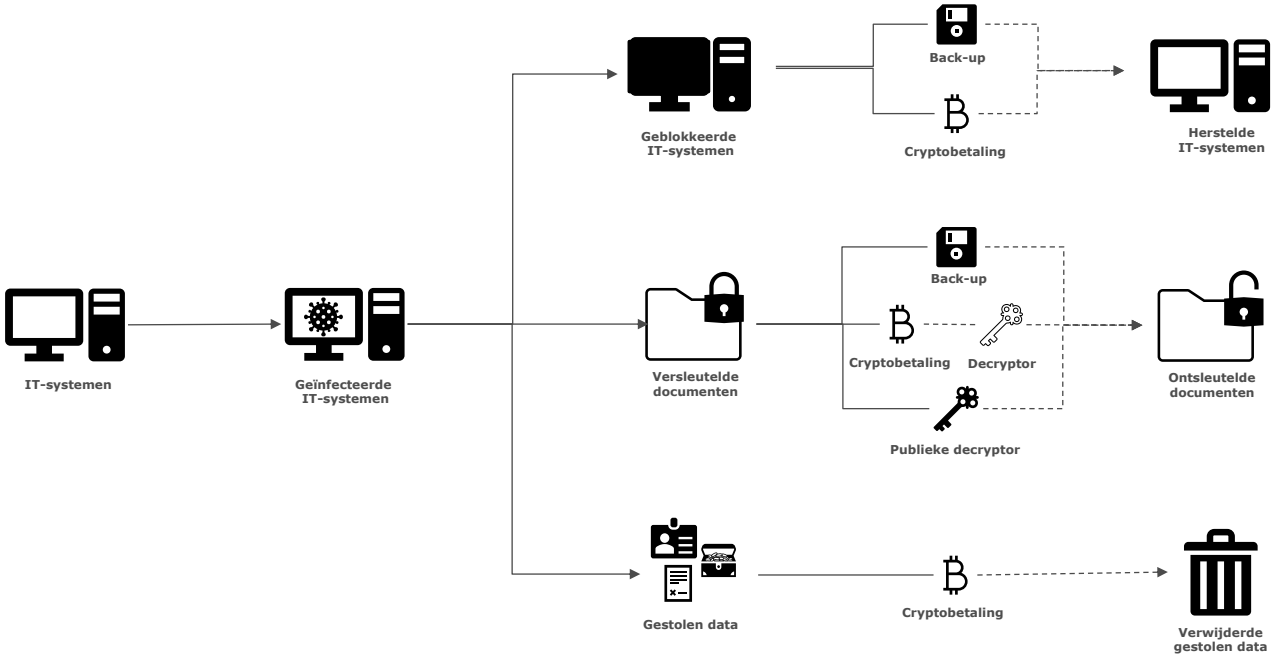
Deze stappen bekijken een ransomware-aanval vanuit het perspectief van de *aanvaller*. Voor de doeleinden van dit onderzoek willen we echter naar een ransomware-aanval kijken vanuit het perspectief van de *slachtoffers*. Op welke punten kunnen we de frequentie en de impact van ransomware-aanvallen meten? Figuur 2 toont hiertoe veelvoorkomende stappen bij een ransomware-aanval, tussen aanval en herstel, vanuit het perspectief van het slachtoffer. Een ransomware-aanval begint bij IT-systemen die door de cybercrimineel aangevallen worden. Wanneer een aanval succesvol is, zijn de IT-systeem geïnfecteerd met ransomware. Een geïnfecteerd systeem kan vervolgens geblokkeerd zijn (door *locker* ransomware), documenten kunnen versleuteld zijn (door *cryptographic* ransomware) en data kan gestolen zijn (data-exfiltratie). Een combinatie van deze drie is ook mogelijk.[2]

Het herstellen van de IT-systemen kan op verschillende manieren gebeuren. Zo kunnen de geblokkeerde IT-systemen hersteld worden middels het terugzetten van een back-up (al dan niet op een nieuw systeem) of door het losgeldbedrag te betalen. Een onvolledige back-up kan ervoor zorgen dat niet het gehele systeem hersteld kan worden en een losgeldbetaling biedt ook geen volledige garantie voor herstel. In Figuur 2 zijn deze lijnen daarom gestippeld weergegeven. Middels een back-up kunnen ook versleutelde documenten (hopelijk) hersteld worden of ontsleuteld worden met behulp van een publiekelijk beschikbare *decryptor*. Tenslotte kan ook hier losgeld betaald worden om de sleutel te ontvangen. Ook hier biedt een losgeldbetaling geen garantie voor het ontvangen van de sleutel en dat de bestanden niet voorgoed beschadigt zijn. Wanneer er data gestolen is, is het betalen van losgeld volgens de cybercriminelen de enige manier om het lekken van deze data te voorkomen en ervoor te zorgen dat de gestolen data (hopelijk) verwijderd wordt.[3]

---

[2] Er zijn ook ransomware-groepen die aan *triple* (waarbij ook middels DDoS aanvallen de netwerken plat worden gelegd) of zelfs *quadruple* extortion (waarbij de klanten van een bedrijf ook actief benaderd worden) doen, echter is dat maar een klein percentage. Deze laten wij daarom in deze figuur buiten beschouwing.

[3] Een andere (en geprefereerde) manier is de systemen waarop de gestolen data staat opsporen en in beslag nemen. Omdat dit in de praktijk vaak moeilijk te realiseren is hebben we die mogelijkheid niet opgenomen in de figuur. Daarnaast is het nog maar de vraag of er geen verdere kopieën van de data elders zijn ondergebracht.



Figuur 2. De stappen in een ransomware-aanval waar (bestaande) databronnen inzicht in kunnen geven. De gestippelde lijnen geven de stappen aan waarvan een het volgen van de stap geen garantie is voor de uitkomst.

De verschillende databronnen zoomen in de meeste gevallen in op een bepaalde stap in de ransomware-aanval. Daarmee kunnen ze alleen inzicht geven in een bepaalde subset van slachtoffers, zoals bijvoorbeeld de slachtoffers waarvan data is gestolen of slachtoffers die losgeld hebben betaald.

Deel 2: Databronnen

5 Inleiding

In dit deel van het rapport bespreken we de verschillende databronnen aan de hand van de subset van slachtoffers die ze beslaan en indicatoren van ransomware: in welke indicator geeft een bron inzicht en wat zegt de bron over die indicatoren? In dit hoofdstuk zullen we de databronnen kort introduceren en aangeven op welk punt de databron inzoomt. Ook zullen we per databron aangeven welke indicatoren ze bevatten. De volgorde van de databronnen is bepaald aan de hand van de chronologie van een ransomware-aanval.

Virusscanaanbieders hebben vaak detectiemechanismes voor ransomware en hebben dus zicht op het aantal *pogingen* tot een ransomware-aanval. Hiermee kunnen ze inzicht geven in de frequentie van ransomware en de kenmerken van de aanvallen (indicatoren). **IT-dienstaanbieders** zullen hier in sommige gevallen ook zicht op hebben, maar zouden in ieder geval zicht moeten hebben op verdachte activiteiten van de cybercrimineel wanneer deze binnen is gedrongen. Ook hebben zij mogelijk meer informatie over de kenmerken van het slachtoffer.

Wanneer een cybercrimineel succesvol een IT-systeem is binnengedrongen dan is dat systeem geïnfecteerd. Op dat moment kan een slachtoffer (een particulier of een organisatie) een **incident response bedrijf** inschakelen of, indien van toepassing, de **cybersecurity-verzekeraar** inlichten. Deze twee databronnen hebben naast informatie over de generieke kenmerken van een aanval en kenmerken van het slachtoffer ook inzicht in de impact van een aanval. Slachtoffers met een geïnfecteerd IT-systeem wordt vervolgens aangeraden om aangifte te doen bij de **Politie**. Deze aangiftes zouden inzicht kunnen geven in alle eerder benoemde indicatoren. Ook vraagt het CBS middels de **CBS Cybersecuritymonitor** bij een selectie van Nederlandse organisaties uit of ze het afgelopen jaar te maken hebben gehad met een ransomware-aanval en wat daar de impact van is geweest. Tenslotte geeft de **media** ook aandacht aan bepaalde (geslaagde) ransomware-aanvallen. Hiermee heeft de media ook invloed op de impact van ransomware op de maatschappij. Daarnaast vervullen de media een belangrijke rol als het gaat om voorlichting over ransomware.

Wanneer er bij een ransomware-aanval data is buitgemaakt, kunnen ransomware-groepen dreigen met het publiceren van deze data op hun eigen **websites op het darkweb**. Om dit te voorkomen verlangt de cybercrimineel dat er losgeld wordt betaald. Een slachtoffer moet bij het vermoeden van een datalek een melding maken bij de **Autoriteit Persoonsgegevens**. De AP heeft daarmee zicht op de frequentie van datalekken en de mogelijke impact daarvan. Losgeldbetalingen (voor elke vorm van ransomware) gebeuren in de meeste gevallen via een cryptobetaling. Analyses van het **Cryptobetalingsverkeer** kunnen dus inzicht geven in de subset van slachtoffers die is overgegaan tot het betalen van losgeld. Tenslotte biedt het platform **No More Ransom** publieke *decryptors* aan waarmee bestanden die versleuteld zijn door bepaalde ransomware *strains* ontsleuteld kunnen worden. Deze laatste databron kan dus mogelijk inzicht geven in de frequentie van bepaalde aanvallen.

In de hierop volgende hoofdstukken zullen we deze databronnen beschrijven, inzicht geven in het beeld dat ze geven over ransomware en de beperkingen van de bron toelichten.

6 Virusscanaanbieders

6.1 Beschrijving databron

Aanbieders van virusscanners hebben zicht op het aantal detecties van malware, zoals ransomware, bij de gebruikers van de virusscansoftware. Daarbij gaat het om de detectie van een stukje kwaadaardige software die via een bepaalde route het systeem van het slachtoffer heeft bereikt om daar een aanval verder te kunnen uitvoeren. Veelal publiceren de aanbieders van antiviruspakketten overzichten van de aantallen malwaredetecties om consumenten bewust te maken van de meerwaarde van hun antivirusproduct. De vraag is dan ook hoe objectief de presentatie van die data is, gezien de commerciële belangen van een virusscanaanbieder.

In dit onderzoek lichten we rapportages van drie verschillende aanbieders toe. Microsoft heeft in 2021 en 2022 specifieke rapportages gewijd aan de mate waarin haar antivirussoftware (Microsoft Defender) pogingen tot ransomware-aanvallen tegen is gekomen op de apparaten van hun klanten (Windows-gebruikers). Verder heeft Symantec enkele whitepapers gepubliceerd op basis van hun antivirusstatistieken en zoomt Kaspersky[4] in hun algehele Threats-rapportage in op aantallen gedetecteerde ransomware-aanvalspogingen. Er zijn ook aanbieders die een live dashboard[5] tonen, maar die data beslaat veelal maximaal een maand en is daarmee minder nuttig voor het detecteren van trends.

De rapportages van virusscanaanbieders kunnen inzicht geven in de generieke kenmerken van een aanval (in de vorm van de gebruikte malware *strain*) en de frequentie van aanvallen in het algemeen. De rapportages geven geen inzicht in de uiteindelijke impact van een aanval, omdat een virusscanner slechts aanvallen dient te detecteren en af te weren en daarmee impact voorkomt. Het detecteren van een aanval leidt normaliter tot een response-actie van de antivirussoftware, waarmee een aanval wordt gestopt (bijvoorbeeld door het in quarantaine plaatsen van geïnfecteerde bestanden) en/of een melding aan de gebruiker of systeembeheerder wordt gemaakt.

Hoewel de aanbieders van virusscanpakketten waarschijnlijk op een grote berg aan data zitten, is er uit de door hun gepubliceerde informatie weinig specifieks te halen. Dit komt onder andere door de selectie van cijfers die wordt gerapporteerd. De regio waarbinnen de aanvallen zijn gemeten is veelal te breed, namelijk wereldwijd, en niet op Nederland toegespitst. Ook verschilt het klantenbestand tussen de verschillende aanbieders enorm, waardoor de cijfers over (potentiële) slachtoffers uit verschillende sectoren en grootteklassen gaat.

De summiere en slecht gedocumenteerde definities en afbakeningen in antivirusrapportages vormen ook een grote beperking. Zo is het in veel gevallen onduidelijk wat er op de Y-as van grafieken staat en op basis van welke data ze gemaakt zijn. Aangezien de rapportages veelal gericht zijn op het demonstreren van de urgentie van beveiliging, gaan ze meer over het algemene beeld dan de details. Een andere beperking vloeit voort uit de meetmethode die hier gehanteerd wordt. Bij antivirussoftware is de detectie niet 100% sluitend. De cijfers kunnen theoretisch gezien afwijken door zowel *false-positives* als *false-negatives*. Dit laatste is met name van belang omdat ransomware-groepen natuurlijk zo min mogelijk gedetecteerd willen worden [23].

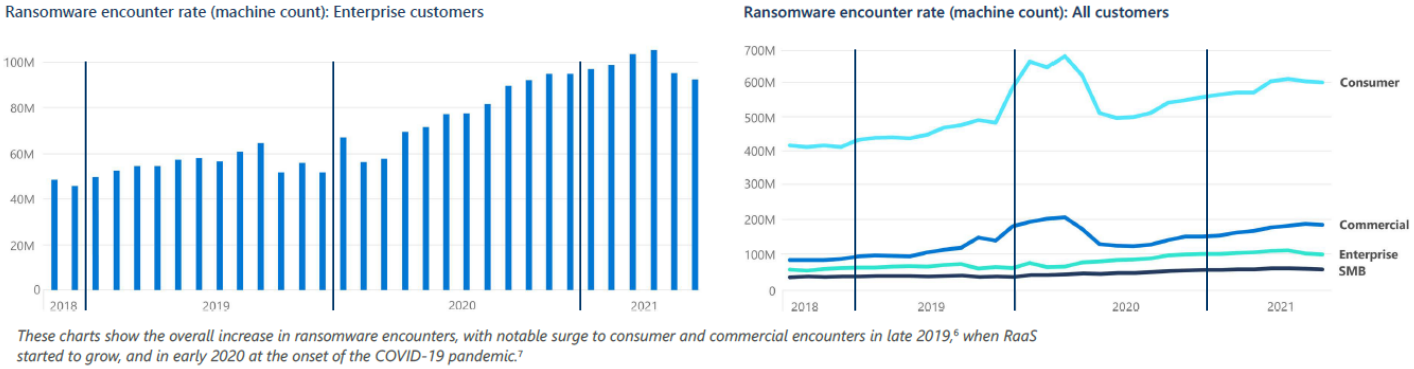
---

[4] Kaspersky is van origine een Russisch bedrijf en het hoofdkantoor zit nog steeds in Moskou. Dit zou mogelijk de content van de rapportages kunnen beïnvloeden.

[5] [AV-TEST] en [Kaspersky]

6.2 Beeld uit databron

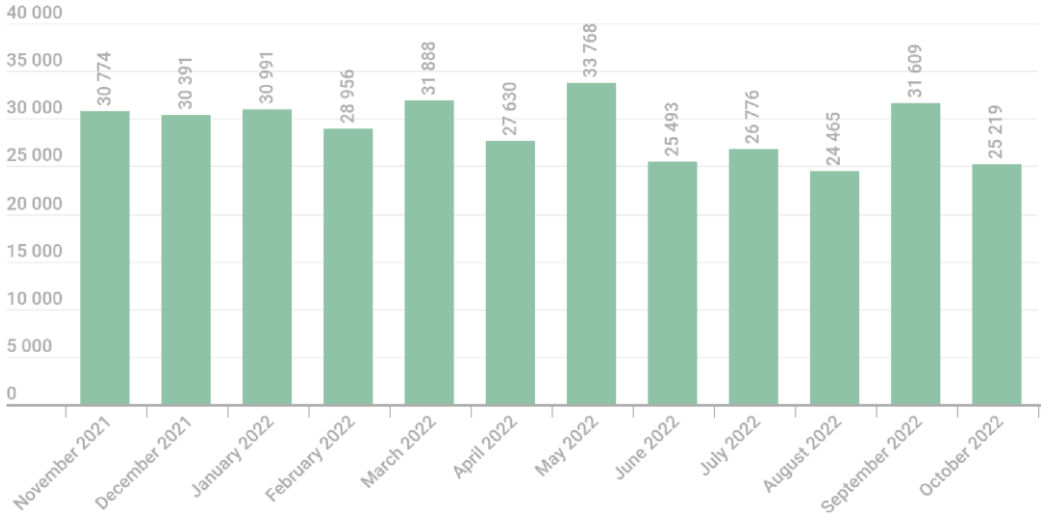
In de rapportages zien we verschillende trends in het aantal wereldwijde ransomware-aanvallen over de afgelopen jaren (Figuur 3, Figuur 4, Figuur 5). Terwijl de cijfers van Microsoft een stijging laten zien in het aantal '*ransomware encounters*' (Figuur 3), zien we bij Symantec een daling in het totaal aantal detecties. Symantec verklaart dit doordat **de algemene aanvallen (bijvoorbeeld via mass-spam campaigns) plaats maken voor gerichtere aanvallen**, die ze wel zien stijgen (Figuur 4, rechts). Bij deze conclusie kunnen echter vraagtekens gezet worden wanneer de x-assen gelijk getrokken worden en we alleen kijken naar 2021. Voor alleen 2021 lijkt er wel degelijk ook een lichte stijging te zijn van het aantal algemene aanvallen (links in Figuur 4).



Figuur 3. Gedecteerde ransomware-aanvallen in Microsoft Defender (links: zakelijke klanten, rechts: alle klanten). Bron: Microsoft, bewerking: Dialogic, locatie: wereldwijd. [32]

Figuur 4. Gedetecteerde ransomware-aanvallen in producten van Symantec (links: alle aanvallen voor 2020 én 2021, rechts: gerichte aanvallen voor 2021). Bron: Symantec, bewerking: Dialogic, locatie: wereldwijd. [23]

De rapportage van Kaspersky toont een stabiele trend in 2021, maar zij tonen het aantal gebruikers dat te maken had met ransomware en niet het aantal aanvallen of detecties (Figuur 5). Veel van de veranderingen in trends zijn te relateren aan actuele ontwikkelingen onder ransomware-groepen, waar in de rapportages ook verdere duiding aan gegeven wordt.



Figuur 5. Aantal Kaspersky gebruikers aangevallen door ransomware Trojans. Bron: Kaspersky, locatie: wereldwijd. [24]

De rapportages splitsen de cijfers veelal uit naar kenmerken van de klant waar een aanval gedetecteerd is, zoals het land en type klant. Deze lijstjes verschillen in uitkomsten en **Nederland komt in de rapportages van bovengenoemde aanbieders niet in de top 10 voor**. De resultaten daarvan zijn natuurlijk ook sterk afhankelijk van het type markt waar de aanbieder zich op richt. Daarnaast rapporteert de ene aanbieder de rangorde aan de hand van absolute aantallen (aantal detecties) en de ander aan de hand van relatieve cijfers (aandeel binnen het totaal aantal apparaten).

Figuur 3 toont de frequentie van detecties naar type klant bij Microsoft Defender. Absoluut gezien zijn de consumenten de grootste groep hierin (dat is namelijk de grootste groep klanten). Kijkend naar de trends, dan is te zien dat consumenten en commerciële klanten gevoelig waren voor de opkomst van Ransomware as a Service (RaaS) en het begin van de pandemie, maar dat dat niet terug te zien was bij de Enterprise- en MKB-klanten (SMB).

Uit de rapporten is ook informatie te verkrijgen over het type aanval. Aan de hand van de verdachte activiteiten die de antivirussoftware detecteert, kan er meer geleerd worden over de aard van de aanval(lers) en de ontwikkelingen daarin. Symantec heeft zo bijvoorbeeld verschillende *attack flows* van verschillende groepen uitgewerkt [25] en trends over de verschillende ransomware-groepen in kaart gebracht [23] (Figuur 6).

Figuur 6. Gedecteerde ransomware-aanvallen per familie. De x-as toont de maanden tussen Januari 2021 en December 2021. Bron: Symantec, locatie: wereldwijd. [23]

6.3 Conclusie

De verschillende virusscanaanbieders presenteren geen eenduidig beeld van ransomware-aanvallen in de periode 2020 tot en met 2022. Daarnaast bevatten de rapportages geen informatie over Nederland specifiek. Ook moeten de commerciële belangen van deze partijen in acht genomen worden: zij hebben er baat bij het probleem op te blazen, zodat consumenten en bedrijven meer antiviruspakketten af gaan nemen.

De rapportages van virusscanaanbieders zijn te algemeen om er daadwerkelijk conclusies aan te kunnen verbinden voor Nederland. Echter zullen zij wel data hebben over afnemers van hun virusscanpakketten in Nederland en het aantal detecties. De Nederlandse overheid zou de mogelijkheid kunnen onderzoeken een verzoek in te dienen bij deze partijen voor het delen van deze data. Dan zou mogelijk een beeld gevormd kunnen worden van het aantal ransomware-aanvalspogingen op Nederlandse systemen (met een virusscanner).

7 IT-dienstaanbieders

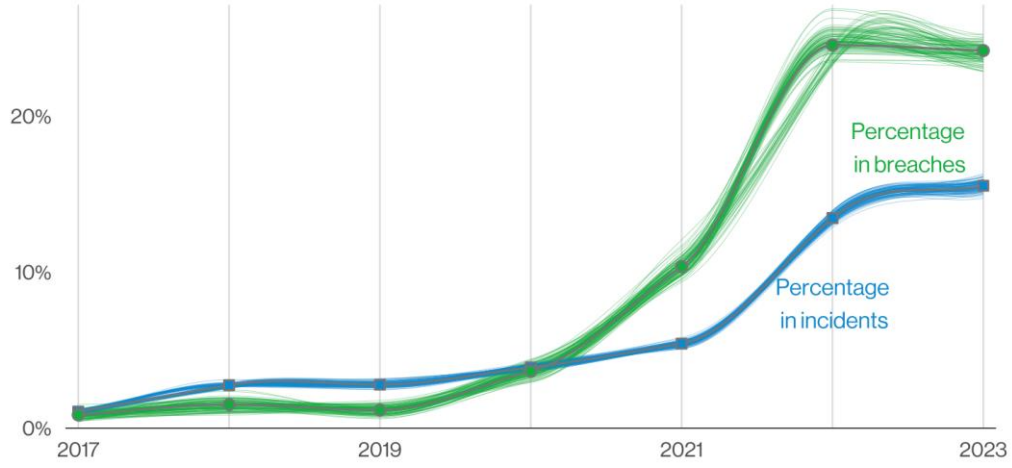
7.1 Beschrijving databron

De aanbieders van IT infrastructuurdiensten zoals netwerkbeheerders, systeembeheerders en telecomaanbieders verzorgen een essentieel deel van de IT-infrastructuur van hun klanten. Zodra een klant tegen een IT-probleem (zoals een ransomware-aanval) aanloopt, kloppen ze vaak als eerst aan bij hun IT-dienstaanbieder (om vanuit daar eventueel doorgestuurd te worden naar een incident response bedrijf). Bij veel grote organisaties zijn deze aanbieders vaak onderdeel van de organisatie, maar bij kleinere organisaties wordt hier in veel gevallen een externe aanbieder voor ingezet. Vooral de groep netwerk- en systeembeheerders is divers. We hebben hier dus niet, zoals bij de virusscanaanbieders, te maken met een klein aantal aanbieders die een overkoepelend beeld kan geven.

Verizon, een grote Amerikaanse telecomaanbieder, brengt een jaarlijkse rapportage over datalekken uit, namelijk de DBIR (Data Breach Investigations Report) [26]. In dat rapport heeft Verizon het afgelopen jaar 16.312 *security incidents* geanalyseerd. De data waarop de rapportage gebaseerd zijn gedeeltelijk online beschikbaar, helaas is het met deze data niet mogelijk om additionele analyses te doen.[6] In de volgende paragraaf zullen we het beeld dat uit de Verizon rapportage naar voren komt bespreken. Verizon heeft echter niet of nauwelijks klanten in Nederland en deze data geven dus met namelijk inzicht in ransomware trends in Noord-Amerika. Daarnaast kijkt ze in haar rapportage naar datalekken in het algemeen.

7.2 Beeld uit databron

Verizon toont dat ransomware één van de grootste categorieën is binnen datalekken (na de categorieën gestolen credit cards en overig). Van alle datalekken in de afgelopen twee jaar is een kwart door ransomware veroorzaakt. Ook is het aandeel van ransomware binnen het totaal aantal incidenten gestegen over de afgelopen jaren: van nog geen 1% in 2017 tot 15,5% in 2023 (Figuur 7). Ook is er een stijging te zien voor de periode van 2020 tot en met 2022 (de focus van dit rapport).



Figuur 7. Ransomware aandeel in lekken en incidenten. Bron: Verizon, locatie: wereldwijd. [26]

[6] [github.com]

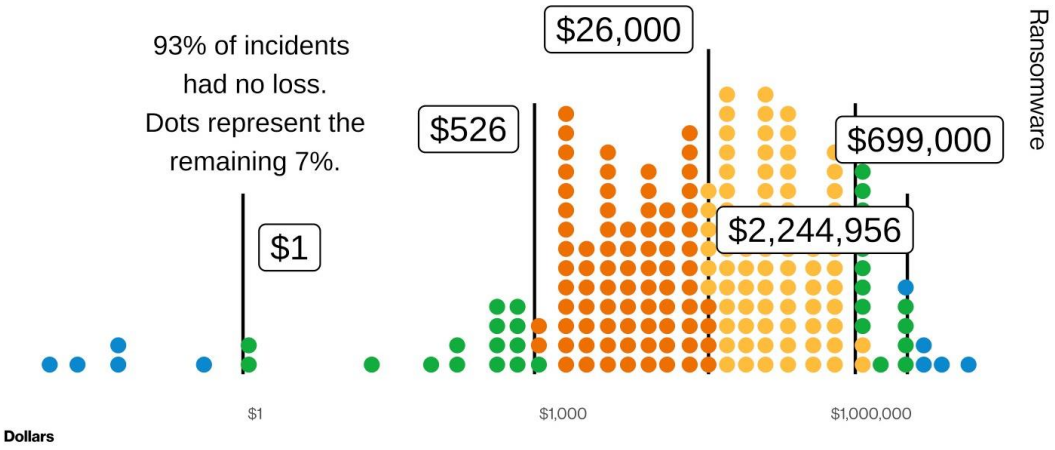
Verizon presenteert ook een samenvatting van het aantal incidenten per sector [27]. Voor een aantal sectoren is hier ook specifiek een uitsplitsing naar ransomware gemaakt. De *professional, scientific and technical services* sector wordt het vaakst getroffen door malware, gevolgd door de *public administration* en *manufacturing* sectoren. Daarnaast **vonden de meeste ransomware-aanvallen plaats in Noord-Amerika** (1.027 aanvallen), gevolgd door Europa, het Midden-Oosten en Afrika (127), Azië en het Pacifische gebied (98) en Latijns-Amerika en het Caribisch gebied (9). Deze verdeling kan deels verklaard worden door het feit dat Verizon met name opereert in Noord-Amerika en daar dus ook de meeste klanten heeft.

Over de aard van de aanvallen geeft Verizon ook enkele inzichten. Als we kijken naar de infectie methode, dan werd er in ruim een derde van de ransomware-incidenten gebruik gemaakt van e-mail en in een kwart van de gevallen van *desktop sharing software* (Figuur 8).

Figure 31. Action vectors for Ransomware (n=690)

Figuur 8. Infectie-methode van ransomware-aanvallen. Bron: Verizon, locatie: wereldwijd. [27]

Daarnaast rapporteert Verizon ook de kosten per ransomware incident (impact). De mediaan van de kosten zou hier liggen op $26.000. Opvallend is dat volgens Verizon er bij 93% van de incidenten geen kosten zijn gemaakt. Hierbij gaat het overigens wel enkel om incidenten die gerapporteerd zijn bij de FBI's Internet Crime Complaint Center (IC3).



Figuur 9. Verdeling van de kosten per ransomware incident (N=2.575). Bron: Verizon, locatie: wereld-wijd. [26]

7.3 Conclusie

De Verizon rapportage geeft wel verscheidene inzichten, echter gaat het hier in veel gevallen niet om Nederlandse incidenten. Waar de cijfers wel naar regio worden uitgesplitst, hanteert de rapportage regio-indelingen die te generiek zijn. Daarnaast geldt voor veel aantallen in de rapportage dat het niet specifiek over ransomware gaat, maar over datalekken in het algemeen.

Veel Nederlandse IT-dienstaanbieders zijn te klein of versnipperd om een beeld te geven van ransomware-aanvallen in Nederland. Voor een compleet beeld zou een centraal orgaan de data over ransomware-aanvallen van iedere IT-dienstaanbieder moeten verzamelen. Met betrekking tot datalekken wordt een dergelijke functie in Nederland indirect al vervuld door de Autoriteit Persoonsgegevens (zie ook Hoofdstuk 10).

8 Incident response bedrijven

8.1 Beschrijving databron

Met de opkomst van ransomware-aanvallen zijn er verschillende partijen opgekomen die zich specifiek richten op de response op een aanval. Aangezien deze partijen worden ingehuurd bij een aanval, is te verwachten dat zij de generieke kenmerken van een aanval en de impact van een aanval gedetailleerd in kaart kunnen brengen.

We hebben verschillende rapportages gevonden waarin wordt gerapporteerd vanuit de incident response:

- VMware heeft een enquête uitgezet in 2022 waarbij 125 cybersecurity- en incident response-professionals wereldwijd zijn bevraagd.
- CrowdStrike rapporteert over aanvallen en volgt zelf 170 cybergroepen.
- Fox-IT rapporteert over waarnemingen van de Managed Detection Response (MDR) en Cyber Incident Response Teams (CIRT) van de NCC Group. Fox-IT zelf is een Nederlands bedrijf binnen de internationale NCC Group.
- Coveware publiceert elk kwartaal een overzicht van de stand van zaken met betrekking tot ransomware-aanvallen. Dit is gebaseerd op de data verzameling vanuit hun eigen incident response afdeling.
- Microsoft vermeldt in hun rapportages ook cijfers vanuit het Microsoft Detection and Response Team (DART).

De incident response bedrijven zullen, gezien hun positie, veel informatie hebben over ransomware-aanvallen. Echter is de publiek beschikbare informatie beperkt tot rapportages. De beschikbare rapportages brengen daarnaast dezelfde beperkingen met zich mee als eerder besproken rapportages, zoals het gebruik van verschillende definities en verschillen in de selecties in het gemeten fenomeen, de regio en de tijdsperiode.

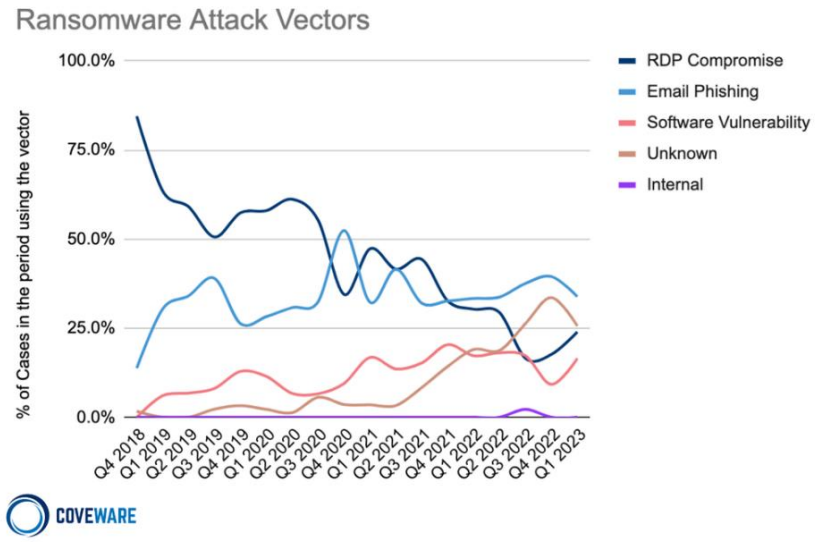
Deze rapportages zijn afkomstig van niet-Nederlandse bedrijven en rapporteren daarom in de meeste gevallen niet specifiek over Nederland. Ook gaan de rapportages niet in op de kosten van het inhuren van een incident response bedrijf. Deze kosten kunnen naar verluidt in sommige gevallen hoog uitvallen. Daarnaast moet ook bij het interpreteren van deze rapportages het commerciële belang van de incident response bedrijven in acht genomen worden.

8.2 Beeld uit databron

Alle rapporten laten zien dat ransomware-aanvallen een grote categorie zijn binnen de cyberaanvallen. CrowdStrike rapporteert bijvoorbeeld **een toename van 82% (van 1474 naar 2686) in het aantal ransomware gerelateerde datalekken tussen 2020 en 2021** [28]. Fox-IT zag ook een stijging in die jaren, maar weer een lichte daling van 2021 naar 2022 (2531 *hack & leak cases*) [29]. Daarnaast geeft Fox-IT aan dat 40% van de cyberaanvallen in de onderzochte periode ransomware-aanvallen betroffen.

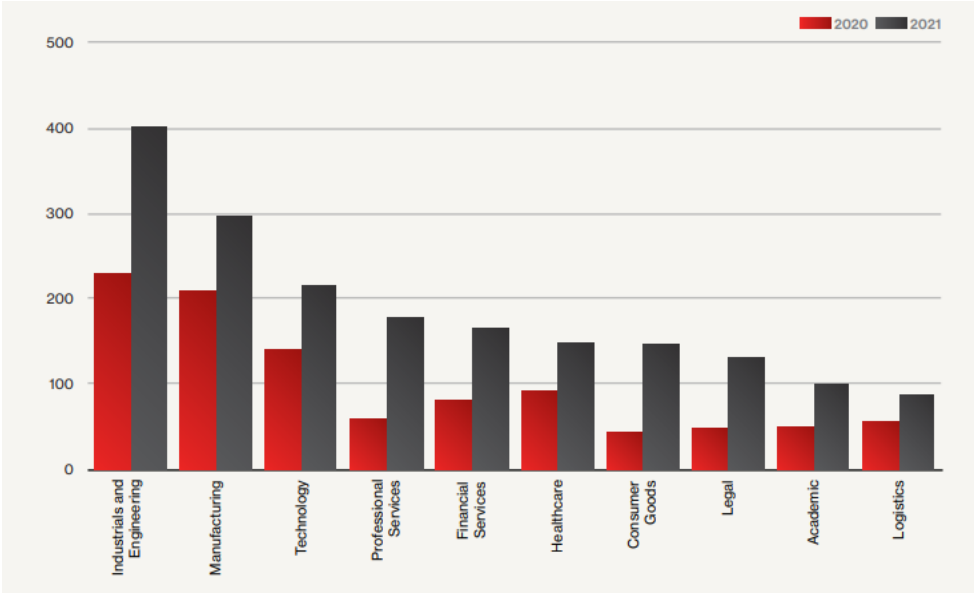
Met betrekking tot de kenmerken van de aanvallen geven de rapportages vanuit de incident response ook inzicht. Uit de enquête van VMware onder cybersecurity en incident response professionals wordt er een verdeling gegeven van de gebruikte afpersingsmethoden bij ransomware. Hierbij bleek er **bij ruim een kwart van de aanvallen sprake te zijn van *double extortion*** [30]. De methoden van afpersing die daarbij zijn ingezet zijn met name blackmail (63%), veiling van de data (60%) en *naming and shaming* (37%) (N.B. tussen deze categorieën bestaat overlap). In de publicaties van Coveware zijn verder per kwartaal

de verschillende gebruikte attack vectors (infectie methodes) in kaart gebracht. [31] Terwijl het remote desktop protocol (RDP) in 2018 veruit de meest gebruikte attack vector was, zien we in het afgelopen jaar (2022) dat phishing de overhand kreeg.

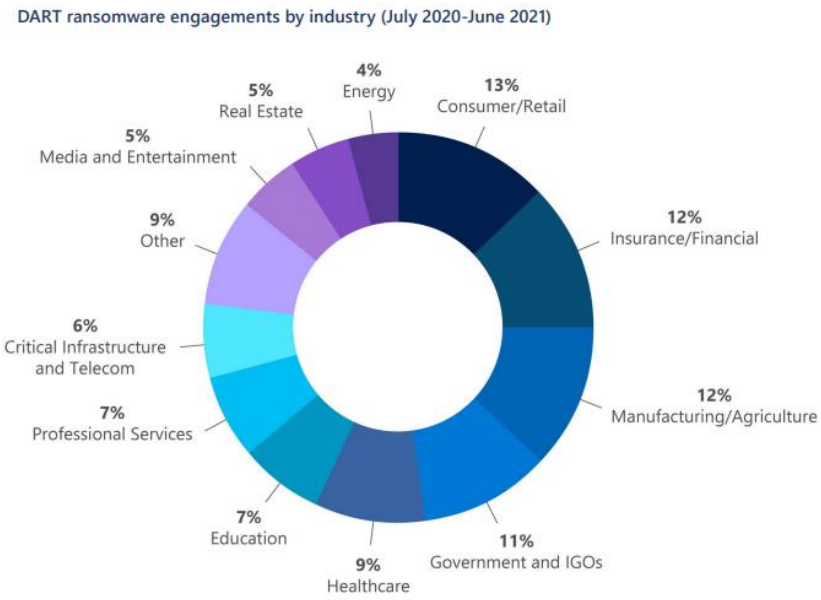


Figuur 10. Trends gebruikte ransomware attack vectors per kwartaal. Bron: Coveware, locatie: wereldwijd. [31]

Zowel Crowdstrike [28], Coveware [31] als Microsoft's DART [32] tonen een overzicht van de meest getroffen sectoren. Hieruit blijken vooral **slachtoffers zich vooral in de industriële en financiële sectoren** te bevinden. De verdeling verschilt echter tussen de rapportages (en zo ook de gehanteerde sectorindeling) (Figuur 11 en Figuur 12). Dit wordt waarschijnlijk mede beïnvloed door het verschil in klantensegment van de partijen.

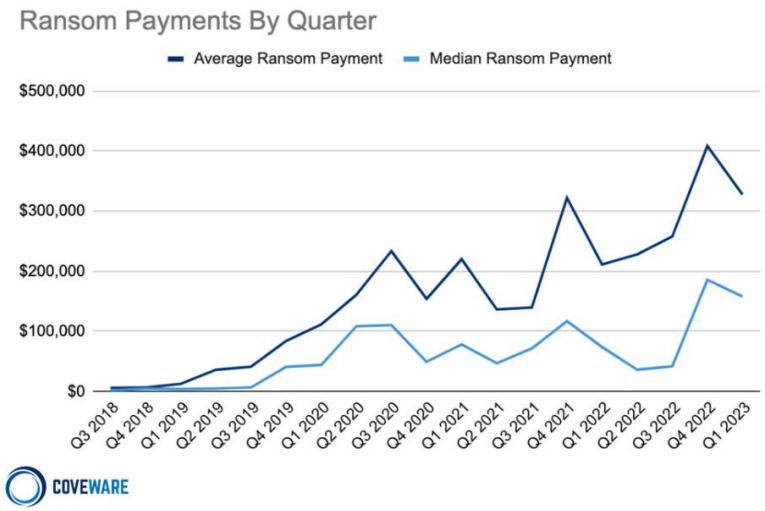


Figuur 11. Datalekken per sector in 2020 en 2021 bekend bij Crowdstrike. Bron: Crowdstrike, locatie: wereldwijd. [28]

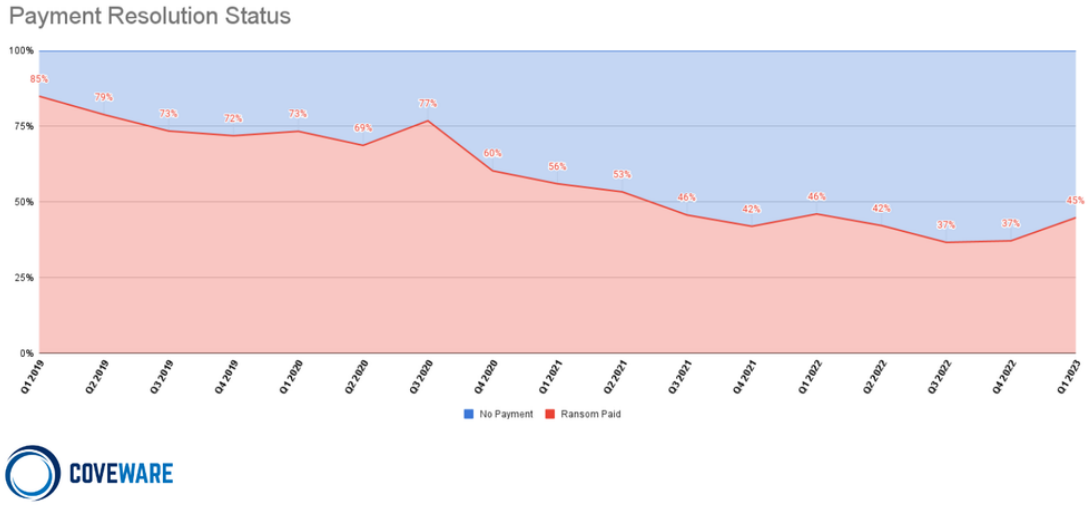


Figuur 12. Ransomware-aanvallen per sector tussen Juli 2020 en Juni 2021. Bron: Microsoft, locatie: wereldwijd. [32]

Coveware rapporteert ook over losgeldbetalingen. Daaruit blijkt dat het bedrag dat gemiddeld betaald wordt door losgeldbetalers **sinds 2018 is toegenomen**. Het gemiddelde betaalde losgeldbedrag door slachtoffers steeg tot Q2 2020, waarna het tot Q3 2021 redelijk stabiel bleef. Vanaf eind 2021 neemt het gemiddelde betaalde losgeldbedrag echter weer toe. De mediaan van het betaalde losgeldbedrag is in die periode minder sterk gestegen. Dit duidt vermoedelijk op een groeiend aantal *outliers* die grote bedragen betaalt (Figuur 13). Daarnaast lijkt het aandeel van de aanvallen waarin tot het betalen van losgeld wordt besloten over de afgelopen jaren flink te zijn gedaald. Terwijl dit in 2019 nog op 85% lag, is dit in 2023 gedaald tot 45% van de aanvallen (Figuur 14). [31]



Figuur 13. Het gemiddelde en de mediaan van losgeldbetalingen per kwartaal. Bron: Coveware, locatie: wereldwijd. [31]



Figuur 14. Het aandeel aan cases waarbinnen er losgeld is betaald. Bron: Coveware, locatie: wereldwijd. [31]

8.3 Conclusie

Een betrouwbaar beeld vormen van ransomware aan de hand van rapportages van commerciële bedrijven is, ook in het geval van de incident response bedrijven, lastig. Dit komt zowel door de commerciële belangen van deze partijen als door parameters die gekozen worden voor het presenteren van de data. Deze zijn vaak niet toegespitst op Nederland en isoleren ransomware in veel gevallen niet specifiek.

Fox-IT is wel een in Nederland gevestigd bedrijf, maar de resultaten in de openbare rapportages zijn gebaseerd op de klanten van de NCC Group (de internationale moederonderneming). Incident response bedrijven geven aan dat zij incidenten rapporteren aan het NCSC en het NCSC daarmee zou moeten beschikken over een beeld van aanvallen op Nederlandse organisaties. Het NCSC heeft data over deze meldingen binnen het kader van dit onderzoek niet gedeeld met de onderzoekers, omdat deze vertrouwelijk zijn en gevoelige informatie bevatten. De opdrachtgever zou in de toekomst mogelijk het NCSC kunnen vragen data op geaggregeerd niveau aan te dragen.

9 Cybersecurity-verzekeraars

9.1 Beschrijving databron

In Nederland is er bij verschillende verzekeraars een cyberverzekering af te sluiten. Daarbij kan in verschillende pakketten verzekerd worden tegen zowel de schade als kosten bij een ransomware-aanval. Een pakket bestaat in veel gevallen uit [33]:

- Advies om cyberrisico's in kaart te brengen en maatregelen te treffen;
- Hulp in de vorm van juridische, forensische, technische en communicatieve bijstand bij een cyberaanval;
- Herstel van schade zoals vervanging van computers, systemen, software en datarecovery;
- Vergoeding van geleden financiële schade, waaronder indien nodig het betalen van losgeld.

In de voorwaarde van de cybersecurityverzekering staat dat bij een vermoeden vanuit de verzekerde dat er iets mis is in de systemen, de verzekeraar al op de hoogte dient te worden gesteld.[7] Verzekeraars kunnen dus al redelijk vroeg in de keten betrokken worden. Op die manier kan de verzekeraar er voor zorgen dat de juiste keuzes worden gemaakt en eventueel andere partijen betrekken bij het proces, zoals incident response bedrijven en advocaten. De informatie in dit hoofdstuk hebben we verzameld uit zowel rapporten (HISCOX *[34, 35]*, Allianz *[36]*, ABN *[37]*) als interviews. De rapportage van HISCOX is gebaseerd op een studie van 5.181 bedrijven uit acht verschillende landen (waaronder ten minste 400 uit Nederland) en verschillende sectoren en bedrijfsgroottes. Hiervan is het echter niet duidelijk in hoeverre dit ook hun eigen klanten betreft. Allianz baseert hun uitkomsten op een survey over 2.712 respondenten (waaronder klanten) uit 94 verschillende landen (waarvan 35 klanten uit Nederland). De rapportage van ABN komt voort uit een onderzoek onder 233 zakelijke klanten. Aangezien ABN ook vele andere diensten aanbiedt, kunnen dit echter ook klanten zijn van andere diensten dan cyberverzekeringen.

In tegenstelling tot de andere bronnen geven de rapporten van de verzekeraars meer cijfers over Nederland specifiek. Toch blijven de methode waarop de data is verzameld en de afbakening verschillen, waardoor de data niet een-op-een te vergelijken of samen te voegen is. Ook geven de verzekeraars zelf aan dat de markt van cybersecurityverzekeringen nog te klein is om een betrouwbaar inzicht in de problematiek rondom ransomware te kunnen geven. Dat verklaart misschien ook waarom de data die ze rapporteren vooral gevoed wordt via enquêtes en niet aan de hand van behandelde cases. Daarnaast kunnen slachtoffercijfers die gebaseerd zijn op enquêtes hoger uitvallen dan ze in werkelijkheid zijn, omdat slachtoffers eerder geneigd zijn mee te doen.

9.2 Beeld uit databron

Van alle bedrijven die door Hiscox in 2022 bevraagd zijn (waarvan het dus niet duidelijk is of die ook allemaal een cybersecurityverzekering hebben) geeft 19% aan getroffen te zijn door een ransomware-aanval. Hiervan heeft twee derde uiteindelijk ook betaald. **Van de bevraagde Nederlandse bedrijven gaf 26% aan te maken te hebben gehad met een ransomware-aanval en zelfs 79% losgeld te hebben betaald.** Nederlandse bedrijven waren daarmee relatief gezien de grootste groep slachtoffers (maar niet met het hoogste

[7] Bron: interview.

percentage betalers). Met name de sterke toename van zowel het percentage Nederlandse bedrijven dat te maken heeft gehad met een ransomware-aanval als het percentage slachtoffers dat losgeld betaald tussen 2021 en 2022 valt op. Voor beiden is de toename onder Nederlandse bedrijven in vergelijking met andere landen met respectievelijk 13% en 31% het hoogst (Figuur 15). Bij de interpretatie van de absolute aantallen moet het commerciële belang van een partij als Hiscox (een verzekeraar) meegenomen worden: voor het werven van klanten hebben zij er baadt bij het probleem zo groot mogelijk te maken. Desalniettemin is de toename van ransomware bij Nederlandse bedrijven opvallend.

Experienced a ransomware attack (%)

	2021	2022	+/-
Belgium	19	15	-4
France	14	19	+5
Germany	19	21	+2
Ireland	16	19	+3
The Netherlands	13	26	+13
Spain	14	22	+8
United Kingdom	13	16	+3
United States	17	17	–

Victims of ransomware that paid (%)

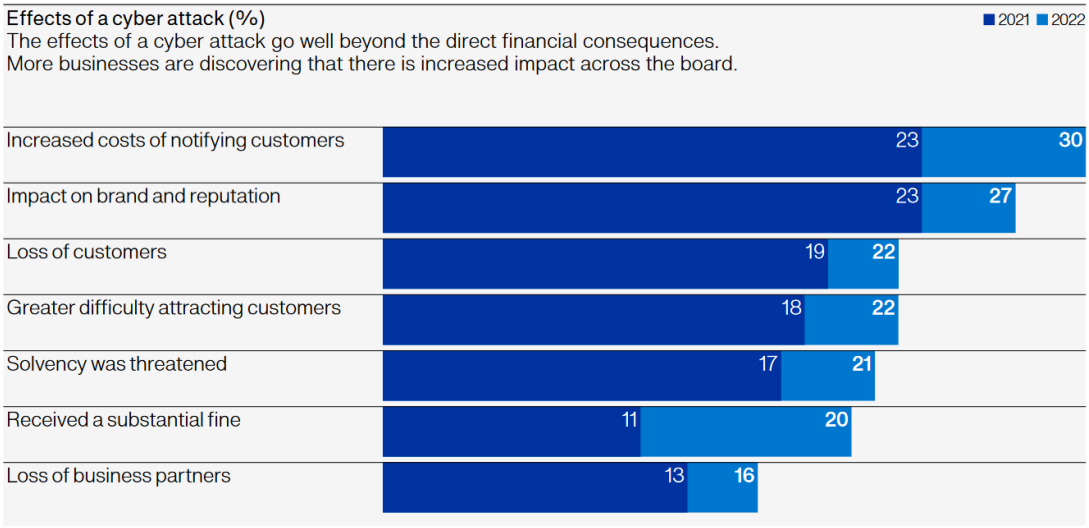
	2021	2022	+/-
Belgium	49	74	+25
France	65	62	-3
Germany	54	48	-6
Ireland	75	80	+5
The Netherlands	48	79	+31
Spain	44	64	+20
United Kingdom	58	63	+5
United States	71	84	+13

Figuur 15. Percentage van bevraagde bedrijven dat te maken heeft gehad met een ransomware-aanval (links) en percentage van slachtoffers dat losgeld betaald heeft (rechts). Bron: Hiscox. [34]

Bij Allianz geeft de helft van de respondenten aan zich het meest zorgen te maken over ransomware-aanvallen als het gaat over cyberrisico's. In 2021 bereikte de schade na ransomware-aanvallen volgens Allianz een recordhoogte van 623 miljoen euro, wat een verdubbeling is van het aantal in 2020 en een stijging van 232% sinds 2019. ABN AMRO geeft ook een stijgende trend aan. **75% van de bevraagde bedrijven zou te maken hebben gehad met cybercriminaliteit (geen specifieke uitsplitsing naar ransomware).**

De verzekeraars geven aan dat ze zien dat **vooral kleinere bedrijven slachtoffer zijn van ransomware**. Kleinere bedrijven hebben vaak minder mindelen en zijn vaker afhankelijk van een enkel systeem. Grotere bedrijven kunnen segmentatie van de systemen toepassen, maar bij MKB bedrijven is dat lastiger. Ook merken de verzekeraars op dat de bewustwording bij kleinere bedrijven minder is omdat deze vaker denken dat ze niet interessant zijn voor cybercriminelen. Daarnaast geven de verzekeraars aan dat ***double extortion***, waarbij zowel de bestanden versleuteld worden als data gestolen wordt, de trend in 2022 was.

Uit het HISCOX onderzoek kwam daarnaast naar voren dat cloud servers, e-mail en corporate servers de meeste gebruikte methoden voor infectie waren. Zoals eerder besproken kan een ransomware-aanval ook op meerdere manieren impact hebben. In Figuur 16 uit het HISCOX rapport is te zien dat de meeste indirecte impact veroorzaakt wordt door het **inlichten en verliezen van klanten en reputatieschade**. Ransomware-aanvallers kunnen door gebruiken te maken van *overprivileged accounts* (accounts met veel rechten) volgens de gesproken verzekeraars de meest impactvolle schade maken. Met name de accounts waar weinig zicht op is kunnen erg makkelijke misbruikt worden door bijvoorbeeld back-ups uit te zetten of het hele systeem te penetreren.



Figuur 16. De impact van een cyberaanval in 2021 en 2022. Bron: Hiscox, locatie: acht Westerse landen. [35]

De cybersecurity-verzekeringen markt is momenteel (in ieder geval volgens de verzekeraars) nog klein. Hierdoor zijn er geen universele premies voor (potentiële) klanten, maar wordt dit per klant bepaald. De gemiddelde betaalde premie is daarmee dus ook niet bekend. Daarnaast kan het ook per klant verschillen welke schade er precies wordt gedekt. Binnen de cyberverzekeringen worden meerdere aspecten vergoed. Zo wordt door sommige verzekeraars onder andere bedrijfsschade, de betaling van losgeld, de IRP-kosten en de AVG-aansprakelijkheid vergoed [38, 39, 40, 41]. Opvallend hieraan is dat het per verzekeraar sterk kan verschillen wat er gedekt wordt en in welke mate. Er bestaat hier dus veel variatie in. Verder vermelden sommige verzekeraars dat boetes enkel vergoed worden indien het wettelijk is toegestaan om de boete te vergoeden. Hetzelfde wordt er bij een bepaalde verzekeraar gezegd over de vergoeding van losgeld. Daarbij wordt zelfs gesteld dat losgeld wordt vergoed als de wet het toestaat, maar dat "vergoeding volgens de wet meestal niet [is] toegestaan" [42]. De verzekeraars geven echter aand dat de meeste verzekeraars losgeld wel vergoeden, maar dat uit analyses van de verzekeraar veelal blijkt dat het gevraagde losgeldbedrag vele malen hoger is dan de totale verwachte financiële schade.

9.3 Conclusie

Het beeld met betrekking tot ransomware dat naar voren komt uit de rapportages van verzekeraars is redelijk zorgwekkend. Uit een rapportage van HISCOX komt bijvoorbeeld naar voren dat 1 op de 4 Nederlandse organisaties in een jaar getroffen is door ransomware en dat bijna 80% van de Nederlandse slachtoffers losgeld betaald. Deze aantallen zijn dermate groot dat er bij de dataverzamelingsmethode vraagtekens gezet moeten worden. Cybersecurity-verzekeraars hebben, net als de commerciële partijen uit de vorige hoofdstukken, namelijk een belang om het probleem zo groot mogelijk te maken. Hoe groter de gevoelde urgentie bij potentiële klanten, hoe groter de kans dat ze een verzekering af gaan sluiten.

De verzekeraars geven aan dat ransomware met name voorkomt bij kleinere bedrijven, mede doordat deze bedrijven vaker afhankelijk zijn van een enkel systeem en de bewustwording van de risico's van ransomware minder is. Daarnaast zien zij *double extortion* (het stelen van data) als de grote trend van 2022.

In plaats van rapportages die de cybersecurity-verzekeraars uitbrengen, zou het interessanter zijn om data te hebben over de schade die vergoed wordt naar aanleiding van een

ransomware-aanval. Deze informatie zou met name waardevol zijn bij het inschatten van de impact van een aanval. Onderzocht zou kunnen worden of aangifte doen bij de politie een voorwaarde voor een cybersecurity claim kan zijn (net als bij bijvoorbeeld diefstal).

10 Politieaangiftes

10.1 Beschrijving databron

Wanneer een bedrijf of een particulier getroffen wordt door een ransomware-aanval (succesvol of niet), wordt aangeraden om hiervan aangifte te doen bij de politie. De informatie uit deze aangiftes kan vervolgens gebruikt worden door een ransomware *task-force* om nieuwe ontwikkelingen te zien in de manier waarop de cybercriminelen te werk gaan of om gemeenschappelijke patronen te ontdekken. De politie onderzoekt meestal niet individuele zaken. Uit de interviews blijkt dat dit simpelweg teveel tijd kost en daarvoor niet voldoende capaciteit beschikbaar is.

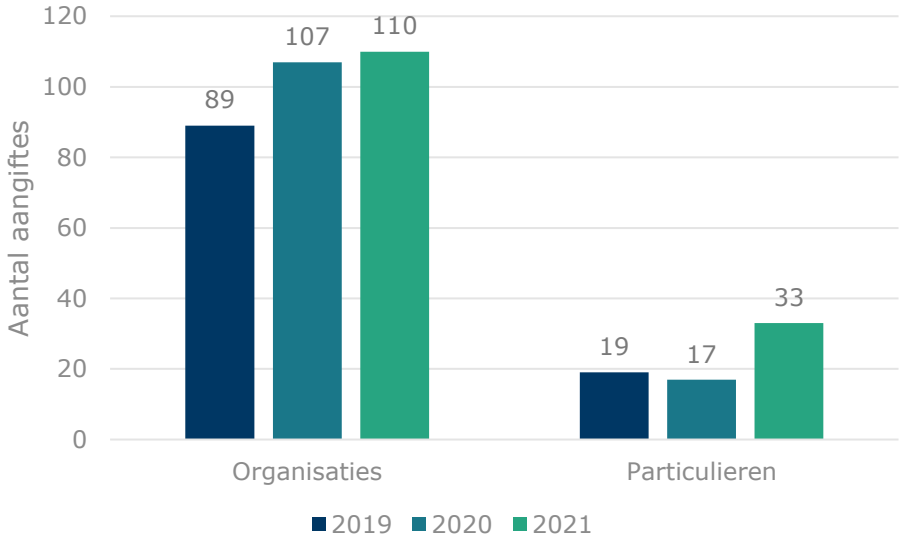
Cijfers over aangiftes bij de politie zijn verkregen binnen het PhD-onderzoek van Tom Meurs naar de aard en omvang van ransomware binnen Nederland en door Tom Meurs gedeeld met de onderzoekers. [43] De data ontvangen van politieaangiftes van ransomware bevat aanvallen tussen 2019 en 2022. Sommige aangiftes uit 2019 beslaan een aanval uit 2018, deze hebben wij buiten beschouwing gelaten. Daarnaast beslaat de data uit 2022 niet het volledige jaar. Hierdoor ligt het totale aantal aangiftes uit 2022 lager dan de voorgaande jaren. In het geschetste beeld lijkt de frequentie van ransomware-aanvallen daardoor af te nemen. Aangezien we daar op basis van deze cijfers nog geen uitspraken over kunnen doen laten we ook deze aangiftes uit 2022 buiten beschouwing.

De grootste beperking van deze databron is dat er over het algemeen heel weinig aangifte wordt gedaan door slachtoffers van een ransomware-aanval. De politie geeft zelf aan dat uit onderzoeken blijkt dat 2% tot 4% van de slachtoffers aangifte doet. Daarbij haalt ze ook een recente actie aan waarbij de Nederlandse politie via een truc met Bitcoinbetalingen 150 decryptiesleutels van de ransomware-groep Deadbolt wist te bemachtigen. [44] Uit onderzoek bleek dat er 1.060 apparaten in Nederland door Deadbolt waren versleuteld, maar de politie had hier in totaal slechts 10 aangiftes van ontvangen.

10.2 Beeld uit databron

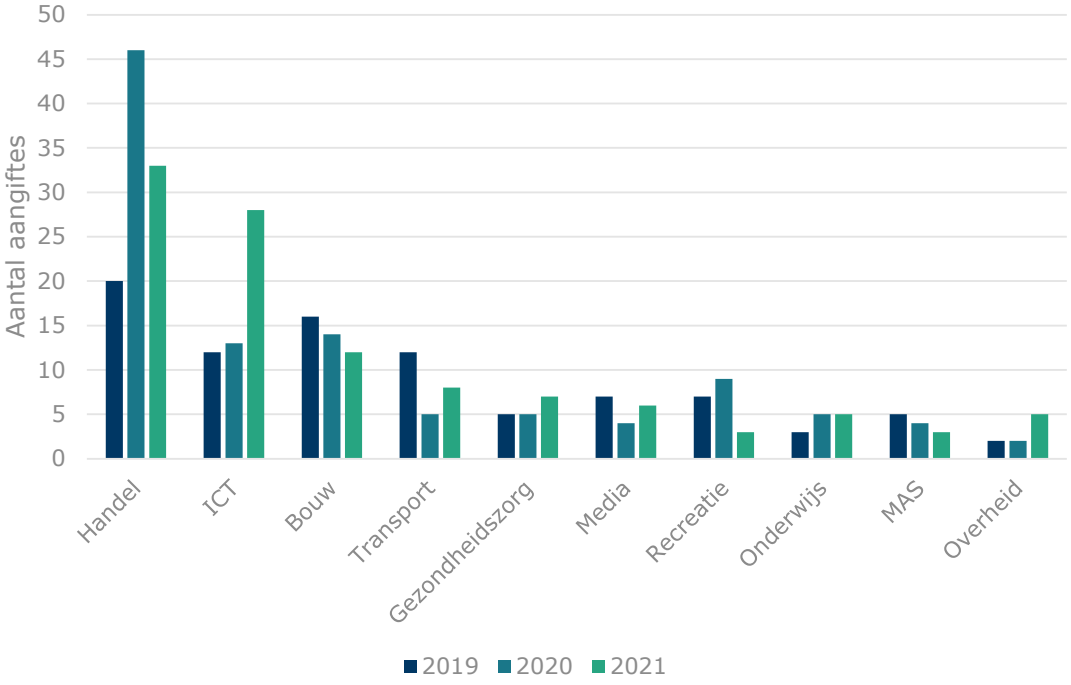
Figuur 17 toont het aantal aangiftes dat bij de Nederlandse politie bekend is als ransomware per jaar, links voor organisaties en rechts voor particulieren. **Ongeveer 100 Nederlandse bedrijven doen ieder jaar aangifte van een ransomware-aanval**, met een lichte stijging van 89 aangiftes in 2019 tot 110 in 2021.[8] Voor Nederlandse particulieren was er in 2021 bijna een verdubbeling van het aantal aangiftes van ransomware-aanvallen; van 17 in 2020 tot 33 in 2021.

[8] Data uit 2022 ontbreekt vooralsnog. Data uit 2019 was wel bekend en is hier, ondanks dat het buiten de periode voor dit onderzoek valt, wel meegenomen.



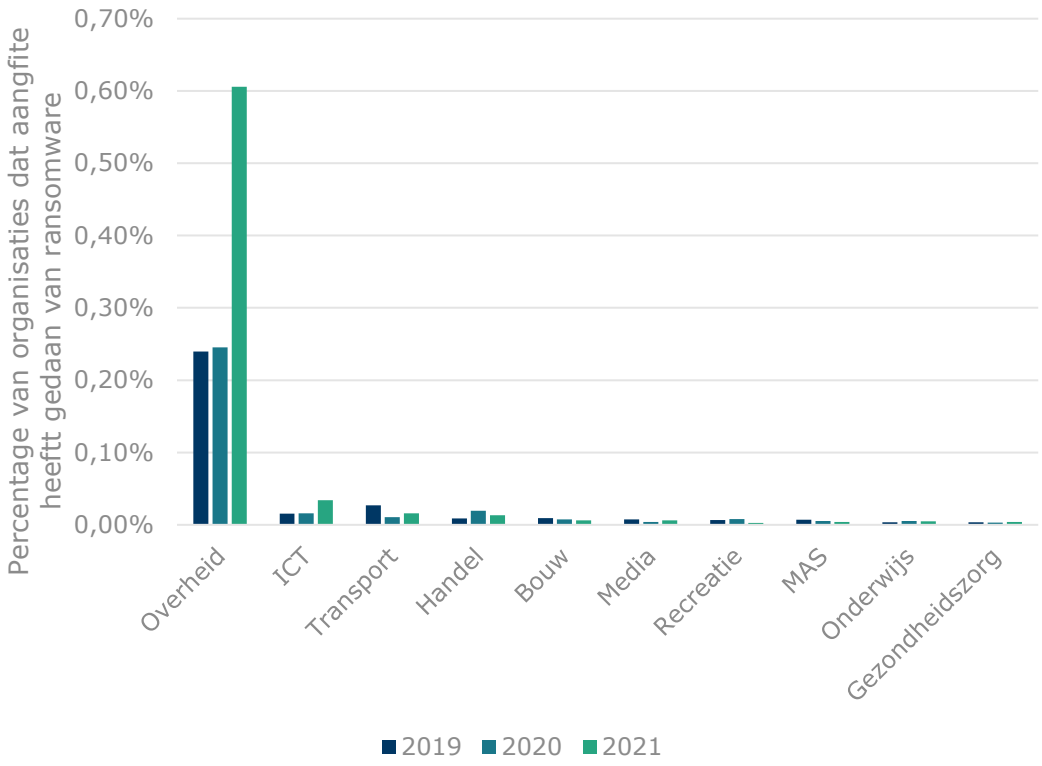
Figuur 17. Aantal aangiftes van ransomware bij de politie per jaar voor organisaties (bedrijven en instellingen) en particulieren. Bron: PhD onderzoek Tom Meurs, bewerking: Dialogic, locatie: Nederland. [43]

De aanvallen kunnen op basis van de aangeleverde data ook uitgesplitst worden naar sectoren. Op basis van informatie uit het handelsregister van de Kamer van Koophandel zijn de organisaties gecategoriseerd naar sectoren. **Het absolute aantal aangiftes van bedrijven in de Handelsector is ieder jaar het hoogst** (Figuur 18). De minste aangiftes zijn in de jaren 2019, 2020 en 2021 uit organisaties binnen de Overheidssector gekomen. Daarnaast is er in 2021 een **verdubbeling van het aantal aangiftes in de ICT-sector** ten opzichte van het voorgaande jaar. [43]



Figuur 18. Aantal aangiftes Nederlandse bedrijven uitgesplitst naar sector. MAS = Milieu en Agrarische sector. Bron: PhD onderzoek Tom Meurs, bewerking: Dialogic, locatie: Nederland. [43]

Voor het duiden van deze cijfers is het echter ook van belang om te kijken naar de omvang van de sector; hoe groter een sector, hoe groter een kans dat er binnen de sector ransomware-aanvallen zullen zijn, wat mogelijk kan leiden tot meer aangiftes. Figuur 19 toont het percentage van bedrijven binnen een sector dat aangifte doet van een ransomware-aanval.[9] Deze figuur zegt weinig, behalve dat het hier heel duidelijk te zien is dat **organisaties binnen de Overheidssector veruit het vaakst aangifte doen van ransomware**: in 2021 deed 0,61% van de organisaties binnen de overheid dit. Dit betekent dat ten minste 1 op de 167 organisaties binnen die sector in dat jaar slachtoffer was van een ransomware-aanval.



Figuur 19. Percentage van bedrijven in een sector dat aangifte doet van een ransomware-aanval. MAS = Milieu en Agrarische sector. Bron: PhD onderzoek Tom Meurs en CBS, analyse en bewerking: Dialogic, locatie: Nederland. [43]

Van ongeveer de helft van de aanvallen in de aangifte dataset is het gevraagde losgeld bedrag bekend. De gemiddelden van de door de aanvallers gevraagde bedragen voor de start van de onderhandelingen staan in euro vermeldt in Tabel 1.[10] Hierin valt te zien dat **de gevraagde losgeldbedragen in de handels- en ICT-sector gemiddeld boven de miljoen euro uitkomen**, terwijl die in de milieu en agrarische sector en de mediasector net iets meer dan 10.000 euro zijn. Ook bij aanvallen op de Overheidssector is het gevraagde losgeldbedrag relatief hoog.

[9] Voor het totale aantal organisaties per sector hebben we een koppeling gemaakt met de sectoren die het CBS hanteert. Hoe deze sectoren gemapt zijn is te vinden in Bijlage 3. Voor de analyse van het aantal aanvallen per sector ten opzichte van de totale grootte van de sector is het aantal bedrijven in het eerste kwartaal van het desbetreffende jaar genomen.

[10] In deze tabel zijn, in tegenstelling tot de figuren in dit hoofdstuk, wel de aangiftes van aanvallen in 2018 en 2022 meegenomen.

Tabel 1. Aantal aanvallen, het gemiddelde financiële verlies in euro, het percentage bedrijven dat losgeld heeft betaald en het gemiddelde van het gevraagde losgeldbedrag in euro (indien bekend) per sector. MAS = Milieu en Agrarische sector. Bron: Meurs et al (2022), locatie: Nederland. [43]

Sector	Aantal aanvallen	Financiële verlies (€)	(%) Losgeld betaald	Gevraagde losgeldbedrag (€)
Bouw	53	256.410	27,5	182.840
Gezondheidszorg	21	77.690	26,3	23.770
Handel	113	737.610	25,5	1.106.800
ICT	60	232.580	30,9	1.343.190
MAS	12	12.500	9,1	13.700
Media	20	344.800	15,8	11.640
Onderwijs	14	49.800	21,4	555.660
Overheid	10	393.330	0	820.350
Recreatie	20	27.000	15	81.020
Transport	29	83.885	30,8	529.540
Totaal	**299**	**1.959.195**	**174,8**	**4.485.670**

Wat opvalt is dat voor de meeste sectoren **het gevraagde losgeldbedrag flink hoger ligt dan het uiteindelijke financiële verlies** dat het slachtoffer gerapporteerd heeft. Alleen bij de bouw-, gezondheidszorg- en mediasector ligt het financiële verlies hoger. Voor bedrijven in de handelssector ligt het gemiddelde financiële verlies door een ransomware-aanval met €737.610 het hoogst. Voor deze bedrijven ligt de volledige bedrijfsvoering er waarschijnlijk uit wanneer de ICT-systemen geblokkeerd zijn.

De politie gebruikt de aangiftedata voor het aanpakken van cybercriminaliteit. Hierbij focust de politie niet op individuele incidenten, maar kijkt het naar onderliggende structuren als de infrastructuur, financiële stromen en communicatie.

10.3 Conclusie

Uit de aangiftes bij de politie komt geen duidelijke trend of beeld naar voren als het gaat om de slachtoffers van ransomware, behalve dat organisaties uit de overheidssector ten opzichte van organisaties uit andere sectoren eerder geneigd zijn om aangifte te doen. Daarnaast laten de aangiftes zien dat het gevraagde losgeldbedrag in veel gevallen vele malen hoger ligt dan de uiteindelijke geleden financiële schade door een ransomware-aanval.

Aangiftes zouden in theorie een zeer waardevolle databron kunnen zijn voor het in kaart brengen van de ransomware problematiek in Nederland omdat 1) de locatie van het slachtoffer bekend is (Nederland) en 2) er rijke informatie wordt uitgevraagd bij een aangifte over de kenmerken van het slachtoffer. Echter doet momenteel slechts een fractie van de slachtoffers aangifte waardoor het als databron niet toereikend is voor het verkrijgen van een totaal beeld. Er zou daarom onderzocht moeten worden hoe de aangiftebereidheid onder slachtoffers van ransomware verhoogd kan worden.

11 CBS Cybersecuritymonitor

11.1 Beschrijving databron

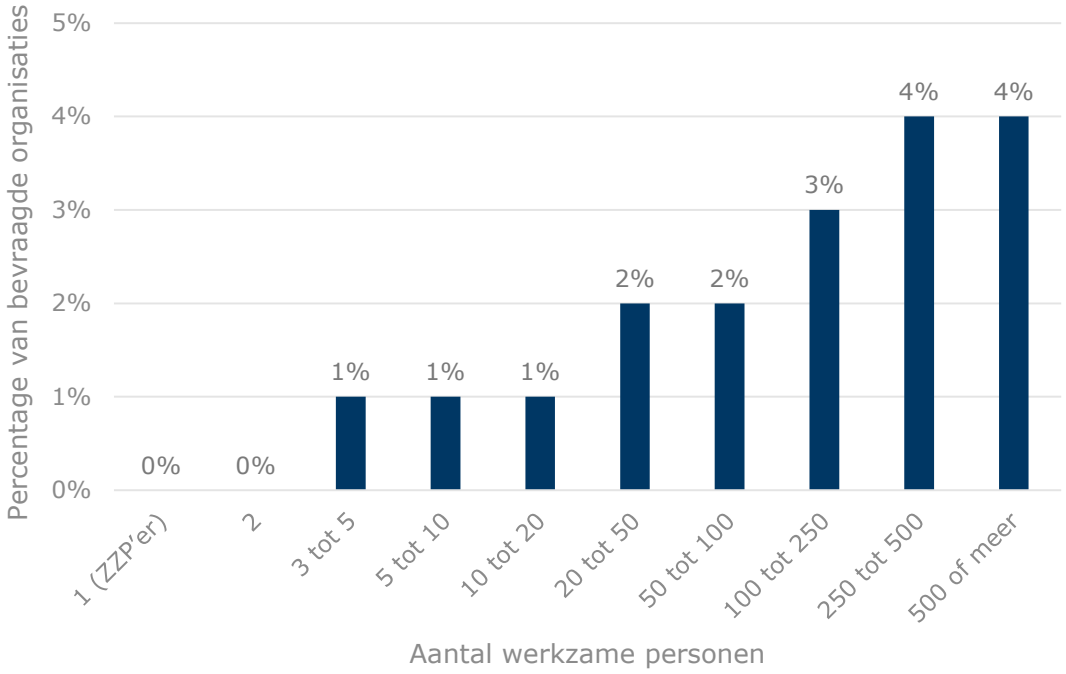
Het CBS zet elk jaar een enquête uit onder bedrijven over het gebruik van informatie- en communicatietechnologie (ICT). Deze enquête bevat sinds 2022 specifiek vragen over ransomware. Het CBS geeft in de rapportage van de vragenlijst aan dat de enquête is uitgezet onder circa 20.000 aselect getrokken Nederlandse bedrijven van 2 of meer werknemers uit verschillende grootteklassen en bedrijfstakken. Voor het classificeren van bedrijfstakken hanteert het CBS de Standaard Bedrijfsindeling (SBI 2008). Daarnaast is in het kader van dit onderzoek naar ICT-gebruik ook specifiek de ICT-sector gedefinieerd. Deze sector is een samentelling van subcategorieën. De overheid en de agrarische sector vallen niet onder de doelgroep voor deze enquête. [45] Een verkorte vragenlijst, die wel de vragen over ransomware bevat, is daarnaast uitgezet onder ongeveer 22.000 ZZP'ers. [46]

Het CBS rapporteert niet over de wijze waarop de steekproef is getrokken (behalve dat die aselect is) en rapporteert ook niet over de (non-)respons van de bevraagde bedrijven en ZZP'ers. Ook is niet bekend hoe de weging van de responses is uitgevoerd en in hoeverre de data representatief is voor de gehele populatie. Hierdoor is bijvoorbeeld de grootte van de subgroepen niet in te schatten. Uit verschillende analyses komen grote verschillen tussen (vergelijkbare) subgroepen naar voren. Door deze onverwachte uitkomsten vermoeden wij dat sommige subgroepen uit een zeer beperkt aantal observaties bevatten. Bij het interpreten van de resultaten uit deze databron moet de beperkte representativiteit van de responses in acht genomen worden.

11.2 Beeld uit databron

De enquête van 2022 bevatte voor de eerste keer ook een specifieke vraag over ransomware in 2021: *"Heeft uw bedrijf in 2021 met een ransomware-aanval te maken gehad? Bij een ransomware-aanval zijn de bestanden of ICT-systemen van uw bedrijf door cybercriminelen geblokkeerd en worden alleen weer vrijgegeven na betaling van losgeld."* Deze definitie van ransomware is smaller dan de definitie die in dit rapport gebruikt wordt, omdat het stelen van data (ook als bestanden niet versleuteld worden) hier niet onder valt.

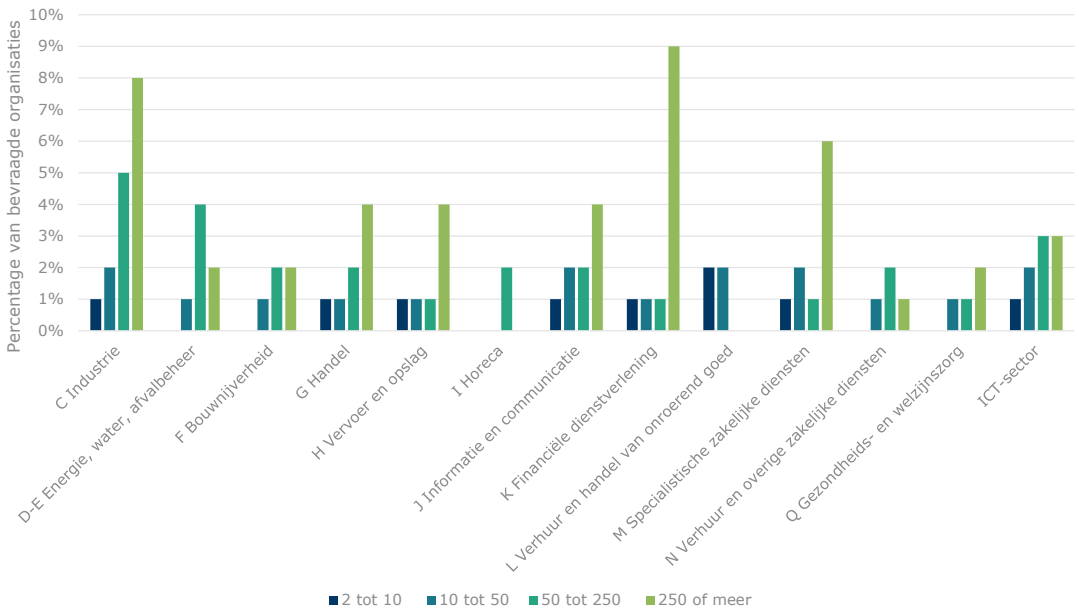
Van alle bedrijven met 2 of meer werkzame personen gaf **slechts 1% aan in 2021 een ransomware-aanval te hebben gehad** en van de ZZP'ers zelfs 0,3%. [47, 48] Het lijkt er op dat **hoe groter de organisatie is (c.q. hoe meer werkzame personen), hoe groter de kans is dat de organisatie te maken heeft gehad met een ransomware-aanval**. Figuur 20 toont dat voor de kleinere organisaties tot 20 werkzame personen 0 tot 1% te maken had met een ransomware-aanval. Dit percentage loopt op tot 4% bij organisaties met 250 of meer werkzame personen.



Figuur 20. Percentage van organisaties dat in 2021 aangeeft in de CBS Cybersecuritymonitor te maken hebben gehad met een ransomware-aanval, uitgesplitst naar aantal werkzame personen. Bron: CBS Statline, bewerking: Dialogic, locatie: Nederland. [47] [48]

In een recente publicatie (augustus 2023) van het CBS over de Cybersecuritymonitor stelt het CBS dat ZZP'ers in absolute aantallen de grootste groep slachtoffers vormen. 0,3% van de ZZP'ers heeft in de enquête aangegeven in 2021 slachtoffer te zijn geweest van ransomware. Dit zijn in totaal 4.000 ZZP'ers. Uit een onderzoek van het Digital Trust Center uit 2023 is naar voren gekomen dat de digitale weerbaarheid van ZZP'ers nog niet op orde is en dat veel basismaatregelen niet voldoende doorgevoerd worden. [49] De groep slachtoffers van bedrijven met twee of meer werknemers bestaat volgens het CBS uit 2.000 bedrijven. [46] De extrapolatie van percentages uit een enquête naar absolute aantallen onder een populatie moet echter voorzichtig geïnterpreteerd worden. Zeker als het gaat om enquêtes over slachtofferschap zijn slachtoffers vaak eerder geneigd deze vragenlijsten in te vullen dan personen of bedrijven die geen slachtoffer zijn geweest. Hierdoor kunnen schattingen over absolute aantallen in sommige gevallen hoger uitvallen dan in werkelijkheid het geval is.

Voor bedrijven met twee of meer werknemers kijken we naar de sector van de organisatie. Figuur 21 toont per bedrijfstak en bedrijfsgrootte het percentage van bedrijven dat aangeeft in 2021 te maken te hebben gehad met een ransomware-aanval. Een aantal opvallende constateringen zijn dat in de Industrie sector (C) het percentage ransomware-aanvallen bij de bedrijven gestaag toeneemt met bedrijfsgrootte: van 1% bij 2 tot 10 werknemers tot 8% bij 250 of meer werknemers. Bij de Financiële dienstverlening (K) en de Specialistische zakelijke diensten (M) hebben de grote bedrijven van 250 of meer werknemers relatief vaak een ransomware-aanval gehad in 2021 (respectievelijk 9 en 6% van de bedrijven), terwijl de kleinere bedrijven in die sector relatief weinig getroffen werden.



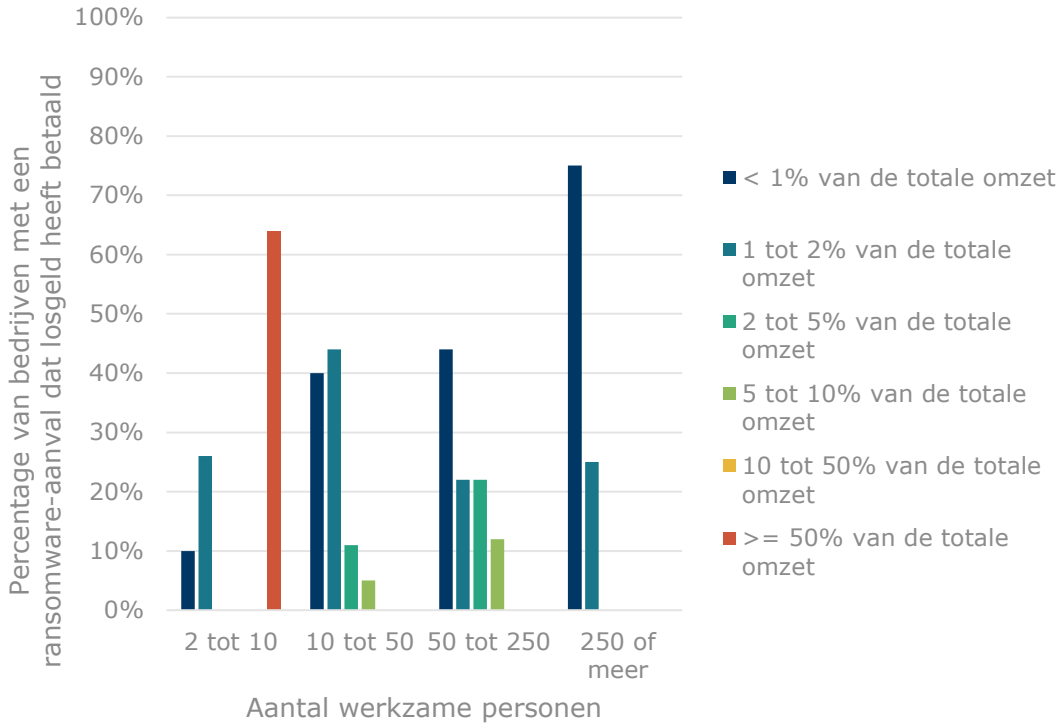
Figuur 21. Percentage van organisaties dat in de CBS Cybersecuritymonitor van 2021 aangeeft te maken hebben gehad met een ransomware-aanval, uitgesplitst naar sector en aantal werknemers. Bron: CBS Statline, analyse en bewerking: Dialogic, locatie: Nederland. [46]

In de enquête wordt aan de bedrijven die aan hebben gegeven met een ransomware-aanval te maken te hebben gehad gevraagd: *"Heeft uw bedrijf de cybercriminelen betaald om de ICT-systemen of bestanden van uw bedrijf weer vrij te geven?"* In feite wordt hier gevraagd of bedrijven losgeld hebben betaald. **Van alle bedrijven met een ransomware-aanval en met 2 of meer werkzame personen gaf 11% aan dat ze losgeld betaald hebben en van de ZZP'ers gaf 0% aan losgeld te hebben betaald.**[11] Hier zit wel variatie in tussen de verschillende bedrijfsgroottes en – sectoren. Over de gehele linie zijn **bedrijven in de Industrie, de Handel en Vervoer en opslag die getroffen worden door ransomware het vaakst overgegaan tot het betalen van losgeld** (zie Tabel 4 in Bijlage 2). Daarnaast betalen ook bedrijven met 50 tot 250 werknemers in de Gezondheids- en welzijnszorg in 31% van de gevallen losgeld. Daartegenover staat bijvoorbeeld dat geen van de grootste bedrijven in de Financiële dienstverlening en de Specialistische zakelijke diensten (waarvan 9 en 6% te maken had gehad met een ransomware-aanval) losgeld betaald heeft. Een verklaring hiervoor zou kunnen zijn dat bedrijven in de Industrie, Handel en Gezondheidszorg het zich niet kunnen permitteren dat de ICT-systemen er te lang uitliggen en daarom besluiten losgeld te betalen.

Daarnaast blijkt dat het losgeldbedrag voor kleinere bedrijven relatief vaak hoger is. Figuur 22 toont het percentage van de omzet in 2021 dat door bedrijven als losgeld is betaald per bedrijfsgrootte. Zo betaalt **64% van de kleinere bedrijven zelfs meer dan 50% van de totale omzet aan losgeld**. Dit kan een grote impact hebben op de bedrijfsvoering. Organisaties waar 250 of meer personen werkzaam zijn, betalen in 75% van de gevallen minder

[11] Uit de enquête van het CBS komt dat 0,3% van de ZZP'ers een ransomware-aanval heeft gehad in 2021. Het aantal ZZP'ers dat de vragenlijst heeft ingevuld is niet bekend bij de onderzoekers van Dialogic, maar het is voorstelbaar dat de groep bevraagde ZZP'ers die een ransomware-aanval heeft gehad slechts uit enkele bestaat. Het feit dat 0% van deze ZZP'ers losgeld betaald heeft, wil dus nog niet zeggen dat ZZP'ers nooit losgeld betalen.

dan 1% van de totale omzet aan losgeld. Voor grote bedrijven met een hoge omzet kan dit echter alsnog een significant bedrag zijn.



Figuur 22. Percentage van de omzet dat door bedrijven, die na een ransomware-aanval over zijn gegaan tot het betalen van losgeld, is betaald. Het betaalde losgeld is uitgedrukt als percentage van de totale omzet van het bedrijf. Bron: CBS Statline, bewerking: Dialogic, locatie: Nederland. [47]

In de rapportage van de Cybersecuritymonitor geeft het CBS aan dat in meer dan de helft van de gevallen de bedrijfsgegevens niet of maar gedeeltelijk werden vrijgegeven na het betalen van losgeld en dat dit met name bij kleine bedrijven voorkwam. [46] Deze constatering, dat het betalen van losgeld dermate vaak niet leidt tot het terugkrijgen van toegang tot de systemen en bestanden, komt in andere databronnen niet naar voren. Uitsplitsingen van de beschikbare data op CBS Statline laten ook zien dat dit alleen bij bedrijven met exact twee werkzame personen het geval is. In die categorie geeft 29% aan losgeld betaald te hebben bij een ransomware-aanval en slechts 1% dat deze betaling zinvol was (zie Tabel 2). In alle andere categorieën geven (nagenoeg) alle bedrijven aan dat het betalen van losgeld zinvol is geweest. [47] Deze specifieke categorie (bedrijven met twee werkzame personen) is ook verantwoordelijk voor de uitkomst dat kleinere bedrijven meer dan 50% van de totale omzet aan losgeld betalen: bedrijven met 2 werkzame personen betalen in 97% van de gevallen meer dan de helft van de totale omzet aan losgeld, terwijl bedrijven met 3 tot 10 werkzame personen maximaal 2% van de totale omzet aan losgeld betaald hebben.

De observaties met betrekking tot zowel de hoogte van het betaalde losgeldbedrag als het zinvol achten van de losgeldbetaling liggen ver uit elkaar tussen categorieën die niet veel zouden moeten schelen (het zijn allen kleine bedrijven). Wij zijn daarom terughoudender in het concluderen dat kleine bedrijven meer dan de helft van de omzet aan losgeld betalen en dat dat het betalen van losgeld in de meeste gevallen niet zinvol is. Om deze conclusie te onderbouwen zouden wat ons betreft de uitkomsten uit de 'outlier' categorie van 2 werkzame personen verklaard moeten worden (zie Tabel 5 in Bijlage 2 voor de resultaten van alle

bedrijfsgroottes). Wij vermoeden dat deze data niet (volledig) representatief is voor de populatie van Nederlandse bedrijven.

Tabel 2. Losgeldbetalingen van kleine bedrijven. Bron: CBS Statline, locatie: Nederland. [47]

	2 werkzame personen	3 tot 5 werkzame personen	5 tot 10 werkzame personen
Ransomware-aanval gehad (% van bedrijven)	0	1	1
Losgeld betaald (% van bedrijven met ransomware-aanval)	29	1	16
Betaling losgeld zinvol (% van bedrijven met ransomware-aanval)	1	1	16
Losgeldbedrag door ransomware-aanval (% van bedrijven die losgeld betaald hebben)			
<1% van de totale omzet	3	0	26
1 tot 2% van de totale omzet	0	100	74
2 tot 5% van de totale omzet	0	0	0
5 tot 10% van de totale omzet	0	0	0
10 tot 50% van de totale omzet	0	0	0
>= 50% van de totale omzet	97	0	0

Naast losgeld werd er ook gevraagd of de ransomware-aanval andere kosten met zich meebracht. Zoals eerder vermeld gaven 38% van de bedrijven aan dat ze andere kosten dan losgeld hebben gehad door de ransomware-aanval. Van alle bedrijven geven de bedrijven met tussen de 50 en 250 werkzame personen het meest aan dat een dat ze door de ransomware-aanval kosten hebben gemaakt: 69 en 64%. In onze optiek valt zelfs dit percentage echter laag uit. Wanneer een ransomware-aanval gedefinieerd wordt als *"Bij een ransomware-aanval zijn de bestanden of ICT-systemen van uw bedrijf door cybercriminelen geblokkeerd en worden alleen weer vrijgegeven na betaling van losgeld."* is het onwaarschijnlijk dat het slachtoffer van een dergelijke aanval geen kosten heeft gemaakt. Het is mogelijk dat 1) de bijzin bij de vraag *"Bijvoorbeeld kosten om geblokkeerde ICT-systemen te vervangen of door kosten door het verlies van bestanden?"* ertoe heeft geleid dat respondenten niet aan ander soortige kosten hebben gedacht (zoals het stilliggen van de bedrijfsvoering door geblokkeerde ICT-systemen) of dat 2) de respondent niet de persoon is binnen de organisatie die hier zicht op heeft.

Daarnaast bevestigt de CBS Cybersecuritymonitor het beeld van de politie dat **het percentage van slachtoffers van een ransomware-aanval dat daadwerkelijk aangifte doet laag is**. In de enquête geeft slechts 13% van de bedrijven met 2 of meer werknemers met een ransomware-aanval aan dat ze hulp hebben gevraagd bij de politie. Het percentage van bedrijven dat na een ransomware-aanval hulp heeft gevraagd bij een cybersecurity bedrijf ligt daarentegen met 39% drie keer hoger.

11.3 Conclusie

Het beeld dat uit de Cybersecuritymonitor van het CBS naar voren komt is dat ZZP'ers in absolute termen de grootste groep slachtoffers vormen, maar dat een groter gedeelte van grote bedrijven in 2021 slachtoffers is geworden van ransomware. Echter is het door de beperkte methodologische verantwoording onverstandig om veel gewicht aan de resultaten uit de enquête te hangen. De responsgraad is niet bekend gemaakt door het CBS en daardoor is het niet in te schatten hoe groot de verschillende subsets van slachtoffers zijn. Als het inderdaad klopt dat maar 1% van de respondenten te maken heeft gehad met een ransomware-aanval dan zullen de uitsplitsingen binnen de groep slachtoffers ook erg klein zijn.

Daarnaast is de CBS Cybersecuritymonitor niet specifiek toegespitst op ransomware. De vragen die op dit thema gesteld worden zijn daarmee redelijk beperkt. Daarnaast betwijfelen we in sommige gevallen of de persoon die de enquête in heeft gevuld de vragen volledig en goed begrepen heeft. Dit komt met name door het hoge percentage dat aangeeft te maken te hebben gehad met een ransomware-aanval maar *geen* kosten te hebben gemaakt.

In theorie zou een landelijke enquête onder Nederlandse instellingen en bedrijven een waardevolle bron kunnen zijn voor inzichten over ransomware-aanvallen op Nederlandse instellingen en bedrijven. Echter zal daarvoor de vraagstelling aangepast moeten worden, zullen meer organisaties deze in moeten vullen en zal de kennis van de respondent voldoende moeten zijn om zowel de vraag te begrijpen als deze te koppelen aan de situatie van de organisatie. Daarnaast is het essentieel voor een correcte interpretatie van de resultaten dat het CBS de methodologie verantwoordt in de rapportage.

12 Media

12.1 Beschrijving databron

Ransomware, ransomware-aanvallen en ransomware-groepen zijn regelmatig het onderwerp van berichten in de media. Daarnaast spelen de media een belangrijke rol in het informeren van de maatschappij en kunnen zij een graadmeter zijn voor de urgentie die gevoeld wordt in de maatschappij rondom het thema ransomware. Door twee mediabronnen te bekijken, één algemene en één technische, over de afgelopen periode hebben wij geprobeerd een beeld te scheppen over de urgentie en aandacht die ransomware heeft gekregen.

Met behulp van webscraping zijn voor de periode 2020 – 2022 de nieuwswebsites nos.nl en tweakers.net onderzocht. Deze zijn gekozen omdat ze 1) makkelijk te scrapen zijn en 2) een ander publiek aanspreken. De NOS is een landelijke nieuwsorganisatie die de gehele Nederlandse maatschappij dient te informeren. Tweakers.net heeft daarentegen een meer technische insteek en geïnteresseerden in cybersecurity zullen eerder daar kijken voor nieuws over ransomware. Voor de websites nos.nl en tweakers.net is een aparte webscraper gebouwd die in de zoekfunctie van de website een aantal zoektermen heeft opgezocht. De artikelen die daarbij naar boven kwamen zijn vervolgens verzameld. Op de websites is gezocht met de volgende zoektermen:

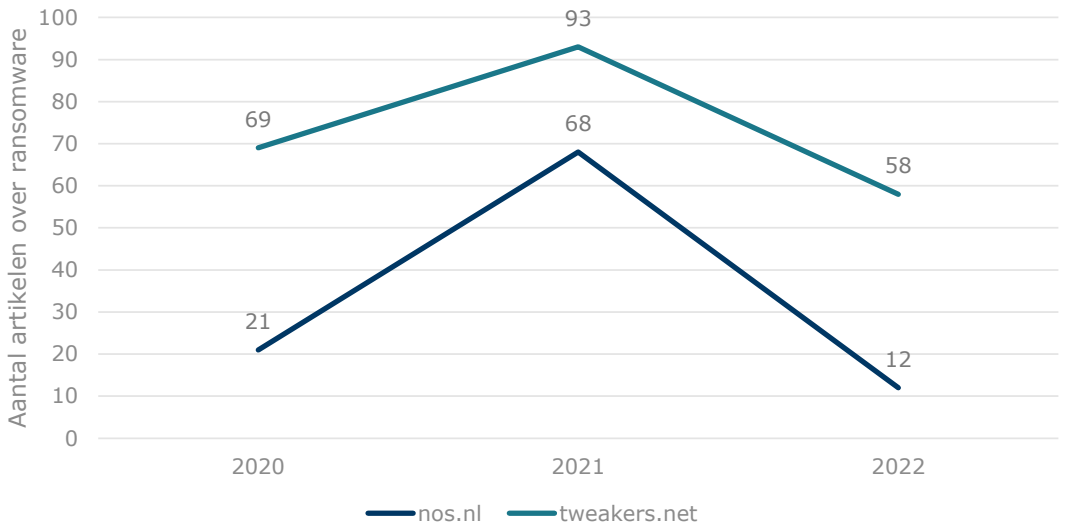
- ransomware
- ransom
- losgeld
- afpersing
- gijzelsoftware
- datalek

Vervolgens hebben we de artikelen geclassificeerd in de volgende categorieën:

- Aanval mogelijk gerelateerd aan ransomware
- Achtergrondverhaal
- Informatie specifieke ransomware groep (voorlichting)
- Oprollen ransomware groep/arresteren dader(s)
- Specifieke aanval
- Specifieke kwetsbaarheid
- Technische aanwijzing
- Irrelevant

12.2 Beeld uit databron

Figuur 23 toont het aantal ransomware artikelen dat ieder jaar gepubliceerd is op nos.nl en tweakers.net (exclusief de artikelen die zijn geclassificeerd als *irrelevant*). **De figuur laat zien dat ransomware in 2021 een groter thema was dan in 2020 en 2022.**



Figuur 23. Het aantal artikelen over ransomware op nos.nl en tweakers.net over ransomware die niet geclassificeerd zijn als 'irrelevant'. Bron: nos.nl en tweakers.net, analyse en bewerking: Dialogic, locatie: wereldwijd.

Deze hogere mate van media aandacht in 2021 wordt met name veroorzaakt doordat er op zowel nos.nl als tweakers.net **meer artikelen gepubliceerd werden over specifieke aanvallen** (respectievelijk 35 en 57 artikelen). Daarnaast publiceerde de NOS in 2021 ook meer achtergrondverhalen over ransomware of ransomware groepen. In 2021 zitten hier onder andere nieuwsartikelen bij van aanvallen op de Hogeschool Arnhem en Nijmegen, RTL, ROC Mondriaan, Universiteit van Amsterdam, de Hogeschool van Amsterdam en de kaasleverancier van de Albert Heijn. Daarnaast werden er meerdere artikelen gewijd aan de ransomware-aanval bij oliepijpleidingbedrijf Colonial uit de Verenigde Staten door de grote gevolgen die deze aanval had. In 2022 nam de berichtgeving over specifieke aanvallen flink af. Dit kan betekenen dat er minder aanvallen waren op grote en/of cruciale bedrijven in de Nederlandse samenleving of dat de aandacht van de media ergens anders was, zoals bijvoorbeeld bij de oorlog in Oekraïne. Er is geen patroon te ontdekken in de momenten van het jaar waarop bepaalde artikelen gepubliceerd worden.

Uit de interviews blijkt echter ook dat **de impact van een aanval deels bepaald wordt door de media**. Recentelijk was er bijvoorbeeld door een ransomware-aanval een storing bij de Media Markt. Experts schatte de impact van deze aanval in eerste instantie niet erg hoog in (de Media Markt vervult immers geen cruciale rol in de maatschappij). Echter bleek de maatschappelijke impact door de media-aandacht en de daaropvolgende vragen in de Tweede Kamer wel groot.

12.3 Conclusie

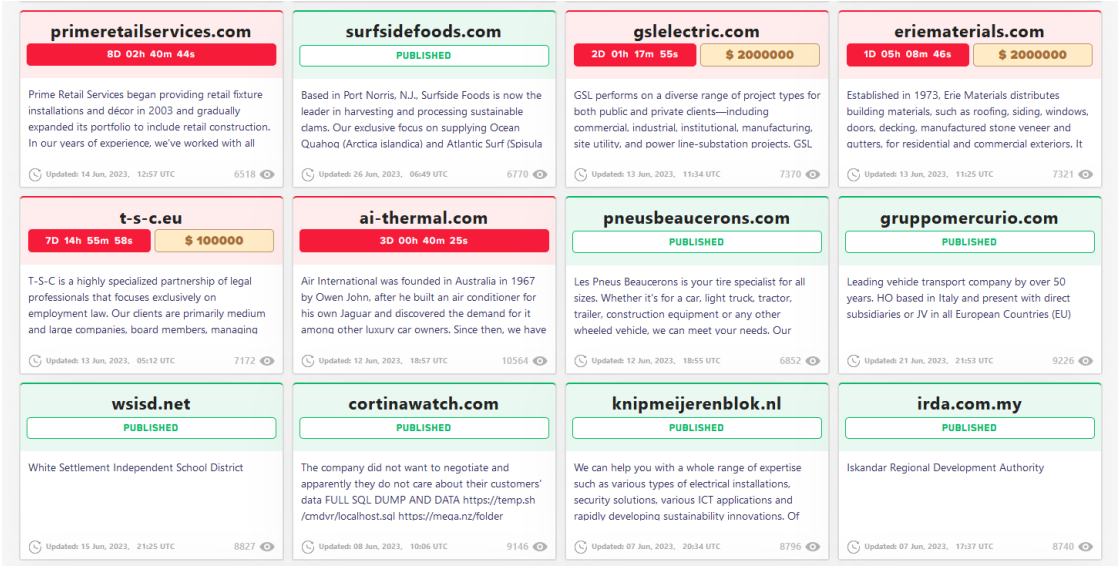
Nieuwsartikelen kunnen een verdieping zijn op andere databronnen, met name als het gaat over de impact van ransomware op de maatschappij. Uit de nieuwswebsites nos.nl en tweakers.net blijkt dat ransomware een groter thema in 2021 was dan in 2020 en 2022. Dit komt met name door een toename van berichtgeving over specifieke ransomware-aanvallen.

Media berichtgeving zal op zichzelf echter geen volledig en betrouwbaar beeld kunnen geven van ransomware-aanvallen op Nederlandse instellingen en bedrijven. Hiervoor is de media te grillig en de nieuwswaardigheid van ransomware-aanvallen te afhankelijk van externe factoren die lastig in kaart te brengen zijn. Zo is de nieuwswaarde van een ransomware-aanval bijvoorbeeld afhankelijk van voorgaande (grote) aanvallen die het nieuws haalden of van zaken die de aandacht van de media trekken (zoals de Oekraïne oorlog) waardoor ransomware op dat moment minder aandacht krijgt.

13 Websites van ransomware-groepen

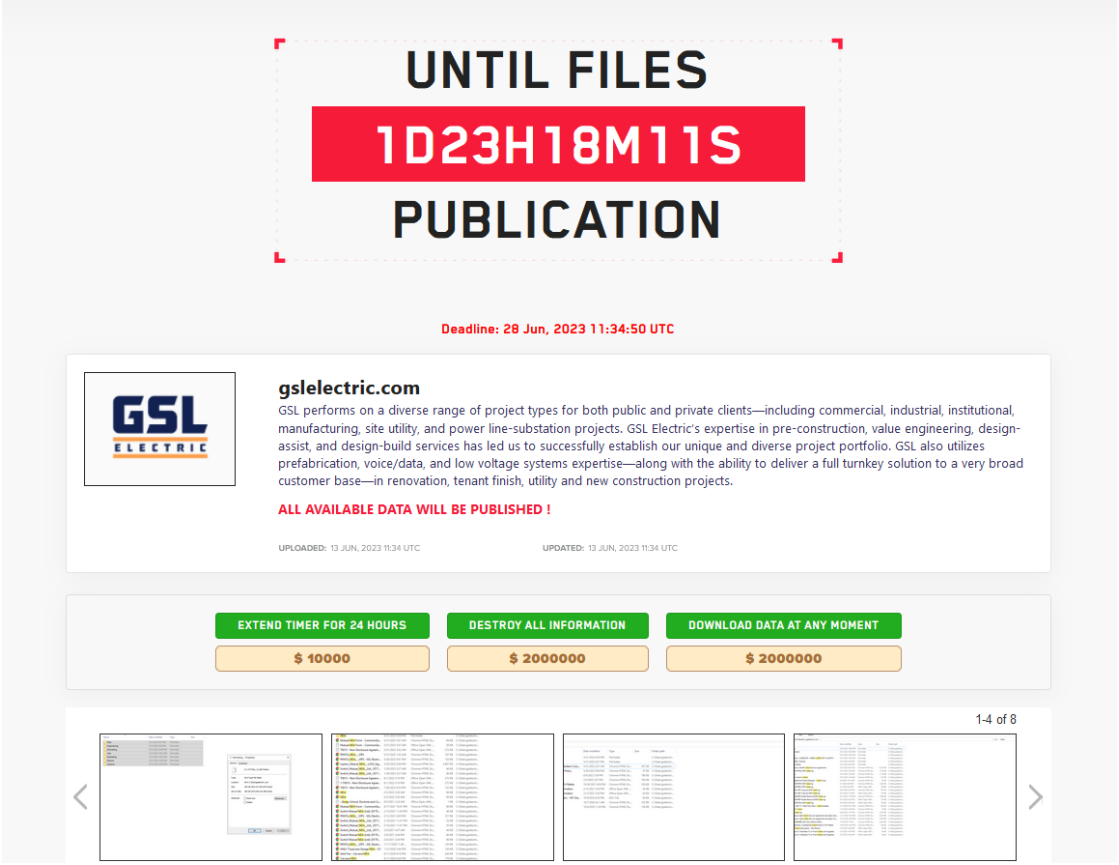
13.1 Beschrijving databron

Ransomware-groepen gebruiken hun websites (ook wel *blogs* genoemd) om druk te zetten op hun slachtoffers. Dit kunnen ze doen door in de onderhandelingen te dreigen met het lekken van de naam van het slachtoffer, wat kan leiden tot reputatieschade bij het slachtoffer (*name&shame*), of door te dreigen met het lekken van data die tijdens de aanval is gestolen. Als een slachtoffer niet op tijd betaalt, dan wordt deze data publiek gemaakt of verkocht (*leak*). Een maatregel zoals het regelmatig maken van back-ups laat de aanvallers in dat geval dus niet zonder inkomen zitten. De meeste ransomware-groepen hebben op het darkweb hun eigen website. Figuur 24 toont de *leak site* van LockBit 3.0. Deze website bevat een combinatie van slachtoffers wiens data al gelekt is (groen) en slachtoffers die nog de tijd hebben om lekken te voorkomen door te betalen. Bij deze slachtoffers (rood) staat vaak een teller afgebeeld die aftelt tot het moment van lekken.



Figuur 24. Voorbeeld van de leak site op het darkweb van LockBit 3.0. Bron: LockBit 3.0 blog.

Ook wordt er in sommige gevallen een publieke betalingsoptie geboden, waardoor ook de personen (bijvoorbeeld klanten van de getroffen organisatie) van wie data gestolen is de kans krijgen om het lekken van de gegevens te stoppen. Figuur 25 toont de *leak* van een aanval op een Amerikaans bouwbedrijf. Alle bestanden van dit bedrijf zullen over iets minder dan twee dagen gepubliceerd worden. De post bevat ook voorbeelden van de data die is gestolen. Als iemand $10.000 in Bitcoin betaalt kan deze deadline met een dag worden verlengd. Iemand (bijvoorbeeld een klant van het bouwbedrijf) kan ook $2.000.000 betalen om alle data te laten verwijderen. Daarnaast kan een kwaadwillend persoon of een concurrent ook $2.000.000 betalen voor het exclusief downloaden van alle data. Op deze manier genereren de cybercriminelen meerdere inkomensstromen. Het is echter niet duidelijk in hoeverre er gebruik wordt gemaakt van deze publieke betalingsopties of dat losgeldbetalingen van slachtoffers de voornaamste bron van inkomen zijn voor de ransomware-groepen.



Figuur 25. Voorbeeld van een leak op LockBit 3.0 met een publieke betalingsoptie. Bron: LockBit 3.0 blog.

Niet elk slachtoffer belandt op de website van een ransomware-groep. Daardoor geeft deze databron geen inzicht in alle slachtoffers van ransomware-aanvallen. Er is over alle partijen heen ook niet één vaste regel te ontdekken die bepaalt of een slachtoffer gepubliceerd wordt. In gepubliceerde communicatie met een slachtoffer zegt een lid van de LockBit groep: *"so that you do not delay the negotiations and there is no action from you, then within 48 hours we will publish your company on our leaks website"*. Dit toont aan dat LockBit het publiceren van de naam van het slachtoffer als drukmiddel gebruikt. Wanneer een slachtoffer dus in een vroeg stadium betaalt, wordt deze mogelijk nooit gepubliceerd op de website.

Ook verdwijnen slachtoffers weer van deze websites als ze wél betalen of verdwijnen de websites in zijn totaliteit van het darkweb (bijvoorbeeld omdat de groep is opgerold). Individuele websites van ransomware-groepen zullen daarom geen historisch overzicht van slachtoffers bevatten. Voor een historisch overzicht hebben wij daarom verschillende 'indexeerwebsites' onderzocht. Deze indexeerwebsites scrapen dagelijks een bepaald aantal websites van ransomware-groepen en bouwen op die manier een overzicht van alle ransomware slachtoffers die gepubliceerd worden. In dit hoofdstuk beschrijven we de data die we via ransomware.live en de weekoverzichten van cybercrimeinfo.nl hebben verzameld middels *web scraping*.

De informatie die door de indexeerwebsites wordt opgehaald en geïndexeerd is niet compleet. Veel individuele veilingwebsites bevatten rijkere informatie, zoals het gevraagde losgeld of de grootte van de gestolen data. Deze rijkere informatie is met name interessant voor het beeld van de impact van een aanval. Omdat LockBit één van de meest actieve

groepen is, hebben we ook de informatie van hun website verzameld en geanalyseerd. Hieronder beschrijven we in het kort de methode voor de data-verzameling per platform voordat we in de volgende sectie de informatie van de bronnen uitwerken.

Ransomware.live

De site ransomware.live indexeert dagelijks de sites van ongeveer 142 ransomware-groepen (leak websites en verschillende partijen in de keten). Daarbij haalt ransomware.live de slachtoffers op die de groepen claimen te hebben gemaakt en aggregeren deze informatie in een overzicht. De code die de website hiervoor gebruikt is openbaar en door iedereen te draaien die zelfstandig een overzicht wilt bijhouden [50]. Wij hebben er voor gekozen om de code van ransomware.live niet opnieuw zelf te draaien, maar het overzicht van ransomware.live te scrapen. Hiermee hebben we leaks vanaf 2020 kunnen verzamelen. Omdat de website zelf een historisch overzicht opbouwt, is het voor ons voldoende om eenmalig het overzicht binnen te halen. De informatie in dit rapport is opgehaald op 3 april 2023. Het overzicht bevat in de meeste gevallen een naam van de getroffen organisatie, een publicatiedatum en de groep verantwoordelijk voor de aanval.

Cybercrimeinfo.nl

Op Cybercrimeinfo.nl (de website is te vinden op ccinfo.nl) wordt onder andere wekelijks een overzicht geplaatst van organisaties die wereldwijd slachtoffer zijn geworden van ransomware. Cybercrimeinfo.nl is een non-profit website die onderhouden wordt door de Nederlandse bedenker. Het wekelijkse overzicht bevat de namen van de slachtoffers die die week getroffen zijn, de website, het land en de sector van de getroffen organisaties. Daarnaast bevat het ook de ransomware-groep verantwoordelijk voor de aanval en de publicatie datum van de aanval op het darkweb. Sinds week 32 in het jaar 2021 staan de Nederlandse en Belgische slachtoffers apart vermeld. Het overzicht wordt wekelijks samengesteld in samenwerking met Dark Tracer, een platform dat criminele activiteiten op het darkweb en deepweb monitort en analyseert. [51] Wij hebben voor dit onderzoek op 28 mei 2023 alle weekoverzichten van cybercrimeinfo.nl gescraped.

LockBit 3.0

De ransomware-groep LockBit is al enkele jaren actief en is momenteel aangekomen bij versie 3.0. In 2022 is de groep overgegaan van LockBit2 naar LockBit3 en zijn alle lekken van de LockBit 2.0 blog verwijderd [52]. Vanaf juni 2022 worden alle slachtoffers geopenbaard op de LockBit 3.0 blog. Deze website[12] hebben wij gescraped om de dataset van slachtoffers te verrijken en om te zien welke slachtoffers verwijderd worden (door een vergelijking te doen met de indexeerwebsites).

LockBit is een ransomware-groep die claimt vanuit Nederland te opereren, compleet apolitiek te zijn en alleen geïnteresseerd is in het verdienen van geld. In Bijlage 4 hebben we de zogeheten *affiliate rules* opgenomen[13]. Deze regels kunnen gezien worden als een HRM document voor personen die geïnteresseerd zijn om zich aan te sluiten bij de groep en bevat de regels waar leden zich aan moeten houden. In de context van dit onderzoek zijn de regels voor het kiezen van een slachtoffer en de regels omtrent het versleutelen van bestanden interessant (zie Box 2). In deze regels vallen een aantal zaken op:

[12] [LockBit mirror website]

[13] LockBit publiceert de *affiliate rules* op hun eigen website.

- De groep hanteert de vuistregel dat bij aanvallen op organisaties uit de kritieke infrastructuur data wel gestolen mag worden, maar dat bestanden niet versleuteld mogen worden.
- Het is verboden om organisaties uit de voormalige Sovjet Unie aan te vallen. LockBit zegt dat dit, ook al opereren ze vanuit Nederland, komt omdat de meeste developers en partners uit deze landen komen.
- De tekst is waarschijnlijk vertaald vanuit het Russisch. De onverwachte term "have rhubarb" (dikgedrukt in Box 2) verschijnt wanneer de Russische tekst door een vertaalmachine gehaald wordt.

Box 2. De slachtoffer regels van de LockBit ransomware-groep. Bron: LockBit 3.0 blog.

Categories of targets to attack:

It is illegal to encrypt files in critical infrastructure, such as nuclear power plants, thermal power plants, hydroelectric power plants, and other similar organizations. Allowed to steal data without encryption. If you can't figure out if an organization is a critical infrastructure, ask your helpdesk.

The oil and gas industry, such as pipelines, gas pipelines, oil production stations, refineries, and other similar organizations are not allowed to be encrypted. It is allowed to steal data without encryption.

It is forbidden to attack the post-Soviet countries such as: Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan, Ukraine and Estonia. This is due to the fact that most of our developers and partners were born and grew up in the Soviet Union, the former largest country in the world, but now we are located in the Netherlands.

It is allowed to attack non-profit organizations. If an organization has computers, it must take care of the security of the corporate network.

It is allowed to attack any educational institutions as long as they are private and have a revenue.

It is allowed to very carefully and selectively attack medical related institutions such as pharmaceutical companies, dental clinics, plastic surgeries, especially those that change sex and force to be very careful in Thailand, as well as any other organizations provided that they are private and ***have rhubarb****. It is forbidden to encrypt institutions where damage to the files could lead to death, such as cardiology centers, neurosurgical departments, maternity hospitals and the like, that is, those institutions where surgical procedures on high-tech equipment using computers may be performed. It is allowed to steal data from any medical facilities without encryption, as it may be a medical secret and must be strictly protected in accordance with the law. If you can't pinpoint whether or not a particular medical organization can be attacked, contact the helpdesk.*

It is very commendable to attack police stations and any other law enforcement agencies that are engaged in finding and arresting hackers, they do not appreciate our useful work as a pentest with postpaid and consider it a violation of the law, we should show them that a competent computer network setup is very important and write a fine for computer illiteracy.

It is allowed to attack government organizations, only with revenue.

13.2 Beeld uit databron

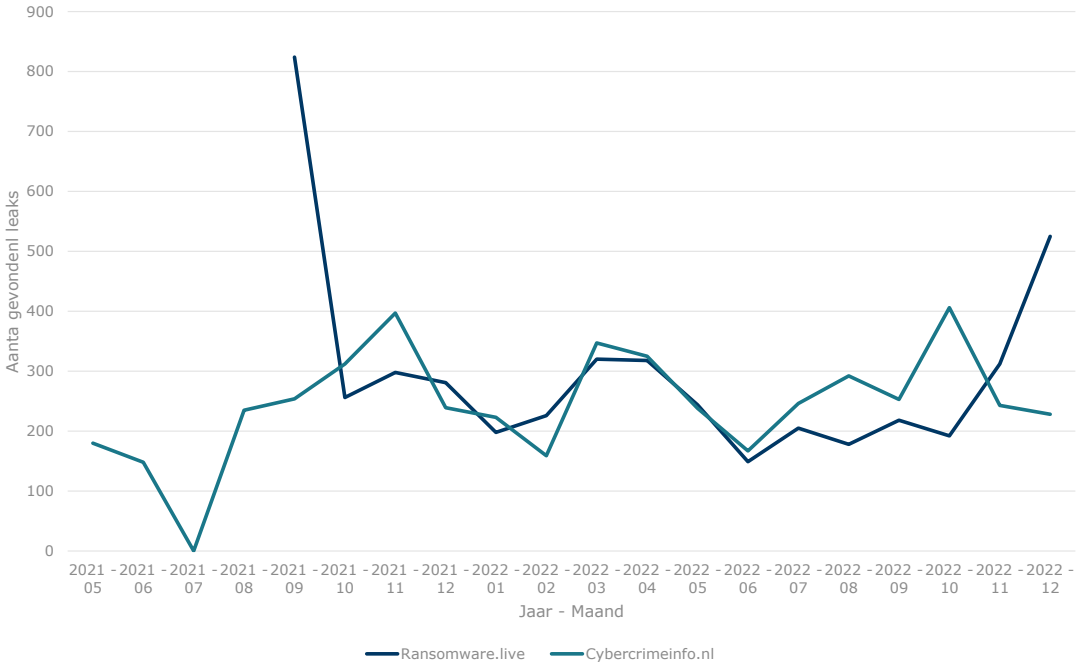
Voor de periode van 2020 tot en met 2022 hebben wij alle leaks die zijn verzameld op ransomware.live en cybercrimeinfo.nl binnengehaald. In totaal hebben wij daarmee 4.797 leaks bij 4.752 unieke organisaties wereldwijd geïdentificeerd op ransomware.live en 5.943 leaks op cybercrimeinfo.nl. Deze gevonden leaks zijn echter niet gelijk verdeeld over de periode tussen 2020 en 2022. Figuur 26 laat zien dat dit met name te maken heeft met het aantal ransomware-groepen dat door de indexeerwebsites is gevolgd. Vanaf september 2021 volgen beide websites consistent meer dan 15 verschillende ransomware-groepen. Omdat het aantal gevolgde groepen in 2020 en begin 2021 erg klein is, laten wij deze periode voor deze databron buiten beschouwing.

Figuur 27 toont het aantal publicaties van alle gemonitorde ransomware-groepen samen, per indexeerwebsite. **Gemiddeld rapporteert ransomware.live 261 publicaties[14] van ransomware-aanvallen wereldwijd per maand en cybercrimeinfo.nl wat minder met 257 publicaties[15].** Over het algemeen lijkt het aantal leaks van ransomware-aanvallen over de maanden die getoond worden in Figuur 27 redelijk stabiel te zijn, waarbij er een lichte golfbeweging te zien is. Omdat de resultaten van ransomware.live en cybercrimeinfo.nl zeer dicht bij elkaar liggen, zullen wij voor de duidelijkheid vanaf hier alleen nog de resultaten van cybercrimeinfo.nl tonen. Cybercrimeinfo.nl bevat meer informatie dan ransomware.live (zoals het land van het slachtoffer) en geniet daarom de voorkeur. Tenzij anders vermeld komen de resultaten overeen met die van ransomware.live.

Figuur 26: Aantal unieke ransomwaregroepen waarvan een leak getoond wordt op ransomware.live en cybercrimeinfo.nl, uitgesplitst per maand voor de periode 2020 - 2022. Bron: ransomware.live en cybercrimeinfo.nl, analyse en bewerking: Dialogic, locatie: wereldwijd.

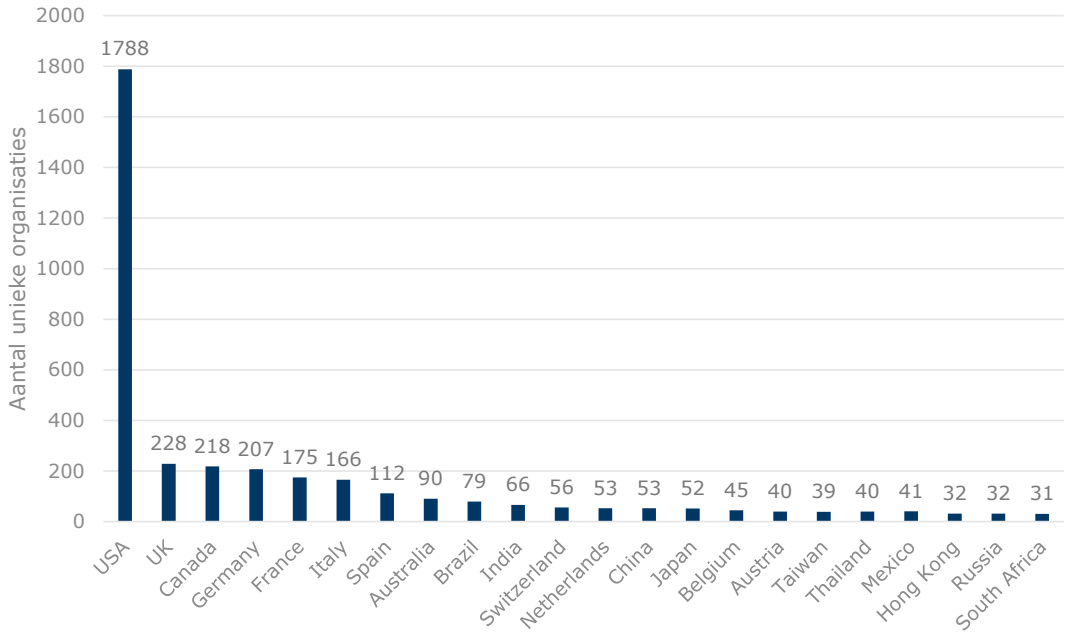
[14] In dit gemiddelde is de uitschieter van september 2021 niet meegenomen.

[15] In dit gemiddelde is de nul score van juli 2021 niet meegenomen.



Figuur 27: Totaal aantal leaks dat voor alle ransomware groepen samen getoond wordt per indexeerwebsite, uitgesplitst naar maand en jaar. Bron: ransomware.live en cybercrimeinfo.nl, analyse en bewerking: Dialogic, locatie: wereldwijd.

Voor de jaren 2021 (vanaf mei) en 2022 laat Figuur 28 zien dat **Amerikaanse organisaties veruit het meest worden gepubliceerd op leak sites na een aanval** (1.778 keer van de in totaal 6.754). De Verenigde Staten worden op gepaste afstand gevolgd door het Verenigd Koninkrijk, Canada, Duitsland en Frankrijk. Nederland staat in deze lijst op plek 12 met 53 aanvallen, voor landen als China en Mexico. Deze relatief hoge plek wordt met name veroorzaakt door aanvallen in 2021. In 2021 stond Nederland namelijk op plek 8, terwijl ze in 2022 gedaald was naar plek 18.



Figuur 28. Aantal leaks van aanvallen op organisaties per land op cybercrimeinfo.nl voor 2021 en 2022. Bron: cybercrimeinfo.nl, analyse en bewerking: Dialogic.

Van de in totaal 6.754 leaks (2021 – 2023) heeft cybercrimeinfo.nl er 53 geïdentificeerd die aanvallen op Nederlandse organisaties betroffen: 26 in 2021 en 29 in 2022. Met 12 aanvallen is de **LockBit groep verantwoordelijk voor 22% van deze leaks**, gevolgd door Conti (9) en Haron en Hive (beiden 5). Omdat LockBit verantwoordelijk is voor de meeste leaks van ransomware-aanvallen op Nederlandse organisaties, hebben we de leak site van LockBit apart *gescraped*.

In juni 2022 is LockBit overgegaan naar de 3.0 versie van hun leak site en is LockBit 2.0 uit de lucht gehaald. Op het moment van scrapen (12 juni 2023[16]) stonden er in totaal 787 organisaties op de leak site, waarvan 10 Nederlandse organisaties[17]. Echter zijn er voor de periode van 27 juni 2022 (de eerste post op LockBit 3.0) en 12 juni 2023 249 unieke organisaties die *nu* niet meer op de LockBit site staan, maar nog wel in de overzichten van Cybercrimeinfo.nl of ransomware.live te vinden zijn (32%). **Organisaties worden vaak van een leak site verwijderd omdat ze losgeld betaald hebben.**

Onder deze organisaties zit één Nederlandse organisatie: de KNVB. LockBit had kopieën van paspoorten en contracten van Oranje-spelers gestolen en vroegen naar verluidt één miljoen euro voor het tegenhouden van het lekken van deze data. [53] Het feit dat de KNVB door LockBit verwijderd is van hun website suggereert dat de KNVB de ransomware-groep losgeld heeft betaald. [54] Van de verwijderde organisaties (die dus hoogstwaarschijnlijk losgeld betaald hebben) komt veruit het grootste aantal uit de VS (79), op afstand gevolgd door Canada (12), Italië (10) en het VK (8).

[16] De focus van dit rapport is de periode 2020 tot en met 2022. Echter is er voor het merendeel van die periode geen data beschikbaar omdat LockBit in juni 2022 is overgegaan naar een nieuwe leak site. Om toch te illustreren wat voor informatie deze databron bevat zullen we daarom de periode juni 2022 tot en met juni 2023 gebruiken.

[17] Op basis van de classificatie van Cybercrimeinfo.nl

13.3 Conclusie

Ransomware-groepen gebruiken hun *leak sites* om druk op hun slachtoffers uit te oefenen zodat ze hopelijk overgaan tot het betalen van losgeld. Het lekken van alleen de naam van het slachtoffer kan al leiden tot reputatieschade en het lekken van gestolen data of persoonsgegevens kan verregaande gevolgen hebben voor het slachtoffer. Door deze websites te monitoren kan dus bijgehouden worden welke groepen op het moment het meest actief zijn en of ze ook slachtoffers in Nederland maken. Daarnaast kan ook bijgehouden worden wat voor data de ransomware-groepen mogelijk gestolen hebben en welk losgeldbedrag ze in sommige gevallen vragen. Een beperking van deze databron is echter dat lang niet alle slachtoffers op deze blogs belanden. Zo zijn er bijvoorbeeld minder Nederlandse organisaties op de indexeerwebsites gevonden dan dat er aangiftes bij de politie zijn geweest.

Het beeld dat uit deze databron naar voren komt is dat het aantal absolute aantal aanvallen op Nederlandse organisaties meevalt (vooral in vergelijking met de Verenigde Staten), maar dat het er wel meer zijn dan het aantal aanvallen op grote landen als China, Japan en Mexico.

14 Autoriteit Persoonsgegevens

14.1 Beschrijving databron

Wanneer er een datalek optreedt is een organisatie (zowel bedrijven als de overheid) verplicht om hier direct een melding van te doen bij de Autoriteit Persoonsgegevens (AP). Bij een datalek gaat het om ongeoorloofde of onbedoelde toegang tot persoonsgegevens, maar ook om het ongewenst vernietigen, verliezen, wijzigen en verstrekken van persoonsgegevens. In de Algemene verordening gegevensbescherming (AVG) heet een datalek een 'inbreuk in verband met persoonsgegevens'. [55]

Wanneer een bedrijf nalaat om melding te doen van een datalek, en daarmee de AVG overtreedt, kan de AP een boete opleggen van maximaal 20 miljoen euro of 4% van de wereldwijde jaaromzet. [56] Deze boete zou kunnen betekenen dat organisaties sneller geneigd zijn om een datalek naar aanleiding van een ransomware-aanval te melden bij de AP, dan bij bijvoorbeeld de politie. Het melden van een datalek gaat via een formulier op de website van de AP. De AP geeft aan dat dit formulier sinds 2022 een aparte categorie voor ransomware bevat, echter is dit in de datalekkenrapportage van 2022 niet terug te vinden. [57] Daarvoor viel ransomware onder de categorie hacking, malware en phishing.

Uit het interview met de AP komt naar voren dat de AP het organisaties wijzen op de plicht en noodzaak om slachtoffers te informeren bij een melding van een ransomware-aanval als haar voornaamste taak beschouwt. Het slachtoffer is hier niet het getroffen bedrijf, maar de natuurlijke personen waar data van is gestolen of gecompromitteerd. De AP bekijkt de impact van een ransomware-aanval vanuit het perspectief van de burger en een aanval op één organisatie kan dus vele duizenden (of in extreme gevallen zelfs miljoenen) slachtoffers hebben.

Het was voor de AP niet mogelijk om binnen het kader van dit onderzoek (geaggregeerde) data te leveren aan de onderzoekers. Hierdoor kunnen we alleen rapporteren over de rapportages die de AP zelf naar buiten brengt. De AP is bezig de data over datalekken te delen met het CBS. In de toekomst kan er door onderzoekers een verzoek gedaan worden bij het CBS om deze data (op geaggregeerd niveau) in te kunnen zien. Echter is het nog onduidelijk wanneer deze data beschikbaar zal zijn.

14.2 Beeld uit databron

Ieder jaar brengt de AP een datalekkenrapportage uit. In 2020 waren er in totaal 23.976 meldingen van een datalek. Het grootste deel van deze meldingen (66%) betreft het versturen of afgeven van persoonsgegevens aan de verkeerde ontvanger via de post of via e-mail. Cyberaanvallen (waaronder ransomware) waren verantwoordelijk voor 5% van deze meldingen: 1.173 meldingen. Dit was een toename van 30% ten opzichte van 2019. Bij 41,5% van de meldingen na aanleiding van een cyberaanval werden meer dan 500 personen getroffen. Dit type datalek kwam het meest voor in de sector Gezondheid en welzijn (13%) gevolgd door Onderwijs (11%), ICT-dienstverlening (9%) en Handel en autobranche (8%). In de rapportage van 2020 merkt AP op dat **vooral grotere organisaties, die persoonsgegevens van veel mensen verwerken, doelwit bleken te zijn van cyberaanvallen**. [58] De kanttekening hier is dat niet elke cyberaanval ook ransomware is.

In 2021 rapporteerde de AP opnieuw een stijging van 88% van meldingen van datalekken door cyberaanvallen. Cyberaanvallen waren in 2021 verantwoordelijk voor 9% van het totale aantal datelekmeldingen (2.210 meldingen; in 2020 was dit nog 5%). Binnen deze toename vielen met name **aanvallen op IT-leveranciers** op. In 2021 heeft de AP 28 datalekken

gezien bij IT-leveranciers die geleid hebben tot 1800 meldingen van getroffen organisaties en naar schatting zijn hier minimaal 7 miljoen slachtoffers bij betrokken. Cybercriminelen richten zich steeds vaker op bedrijven die softwarediensten, digitale werkplekken of opslagruimte leveren aan andere organisaties. Deze IT-leveranciers hebben namelijk vaak veel persoonsgegevens van meerdere organisaties op hun servers staan en daar valt voor criminelen dus veel te halen. Uit een interview met de AP blijkt dat de getroffen IT-leveranciers vaak kleine bedrijven waren die hun beveiliging niet op orde hadden. Aanvallen op deze kleinere leveranciers hebben in één jaar echter wel **7 miljoen slachtoffers** gemaakt.

Het aantal meldingen van cyberaanvallen is in 2022 afgenomen naar 1.826. Ook in 2022 was de Gezondheid en welzijn sector met 23% van de cyberaanvallen de meeste getroffen sector. De AP ontvang deze meldingen met name naar aanleiding van **cyberaanvallen bij ICT-leveranciers in de zorg**. Alleen al door de grootste drie cyberaanvallen bij ICT-leveranciers zijn van ongeveer 900.000 patiënten of cliënten medische persoonsgegevens gelekt. [57]

De AP ziet dat getroffen organisaties als **eerste prioriteit het herstellen van de systemen hebben en pas veel later de mensen wiens gegevens zijn gecompromitteerd of gestolen op de hoogte brengen**. Hierdoor kan de schade oplopen, omdat de slachtoffers zichzelf pas later kunnen beschermen. Ook stelt de AP dat het betalen van losgeld geen garantie is dat de data van burgers niet zal worden gelekt of al gelekt is. Cybercriminelen zitten vaak voor het uitrollen van de ransomware al langer in netwerken en systemen en kunnen in die tijd al gegevens hebben gekopieerd, vernietigd of gewijzigd. Alleen na uitgebreid digitaal forensisch onderzoek kan worden vastgesteld welke persoonsgegevens zijn getroffen en wat er met deze gegevens is gebeurd. Wanneer persoonsgegevens buit gemaakt zijn zal dit, ook al is er losgeld betaald, gemeld moeten worden aan de desbetreffende slachtoffers. Zelfs wanneer er alleen namen en e-mailadressen zijn buitgemaakt bij een ransomware-aanval kan dit grote risico's opleveren voor betrokkenen. Deze gegevens kunnen namelijk misbruikt worden om spam- en phishingaanvallen uit te voeren. [58]

14.3 Conclusie

Het beeld dat naar voren komt uit de datalekken rapportages van de AP is dat met name cyberaanvallen op IT-leveranciers veel slachtoffers maken. In de ogen van de AP zijn de natuurlijke personen waarvan persoonsgegevens (mogelijk) gelekt zijn het slachtoffer van een ransomware-aanval en niet enkel de organisatie wiens IT-systemen getroffen is.

Het is lastig om in te schatten welk deel van de slachtoffers van ransomware daadwerkelijk melding doet bij de AP. De AP heeft namelijk niet of beperkt zicht op ransomware-aanvallen die niet worden gemeld. Desalniettemin is de AP momenteel wel de enige organisatie waar een meld*plicht* voor geldt en waarbij ook specifiek aanvallen op Nederlandse organisaties centraal staan. In potentie zou bij veel ransomware-aanvallen op een organisatie een vermoeden van een datalek moeten zijn en zou de AP dus over veel data kunnen beschikken. Het delen van deze data door de AP met een organisatie als het CBS dat toegankelijk is voor andere overheidsorganisaties of wetenschappelijk onderzoek zou daarmee zeer waardevol kunnen zijn. Er zal wel uitgezocht moeten worden in welke mate het delen van data de meldingsbereidheid van slachtoffers aantast.

15 Cryptobetalingsverkeer

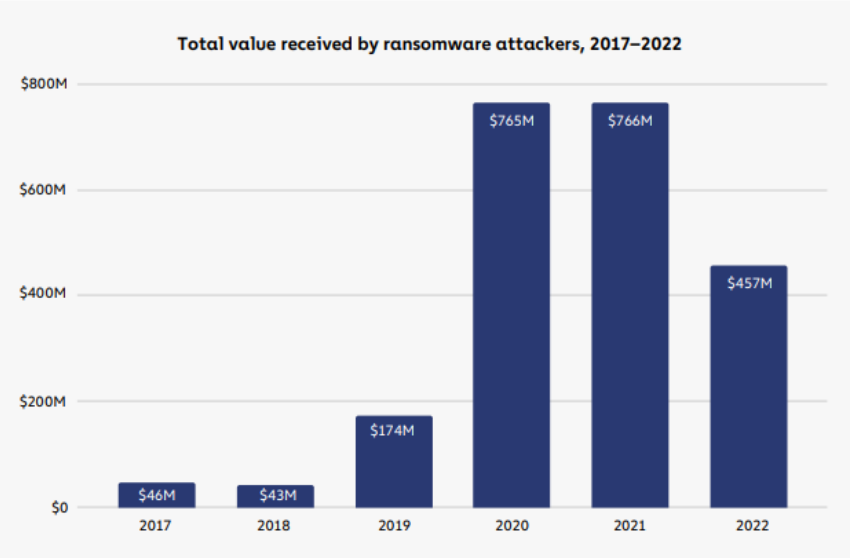
15.1 Beschrijving databron

Ransomware groepen vragen hun slachtoffers in bijna alle gevallen om het losgeld bedrag in *cryptocurrency* (vaak Bitcoin) over te maken naar een wallet van de groep. Deze transacties worden vervolgens, net als alle cryptobetalingen, opgenomen in de blockchain. Wanneer het wallet adres van een ransomware-groep bekend is, kunnen alle transacties naar deze wallet getraceerd worden. Idealiter zouden we specifiek de Bitcoin transacties van Nederlandse exchange bedrijven naar de bekende adressen van ransomware groepen traceren. Echter is het niet mogelijk gebleken om deze Nederlandse adressen te achterhalen en daarmee transacties van Nederlandse organisaties te analyseren.

Het (commerciële) bedrijf Chainalysis analyseert de blockchain en publiceert elk jaar een 'Crypto Crime Report'. Op basis van deze rapportages kunnen we wel een globaal beeld schetsen van ransomware trends wereldwijd. Daarnaast geeft deze bron per definitie alleen inzicht in ransomware-aanvallen waarbij er door een partij (los)geld betaald is.

15.2 Beeld uit databron

Het eerste beeld dat uit de rapportages naar voren komt is dat ransomware er in 2020 en 2021 meer betalingen aan ransomware-groepen plaatsvonden, met een **omslag in 2022 waarbij slachtoffers in ieder geval minder zijn gaan betalen**. Dit is ook duidelijk te zien in Figuur 29, waar het totale bedrag dat ransomware groepen ontvangen hebben in 2022 flink is afgenomen.[18] [59]



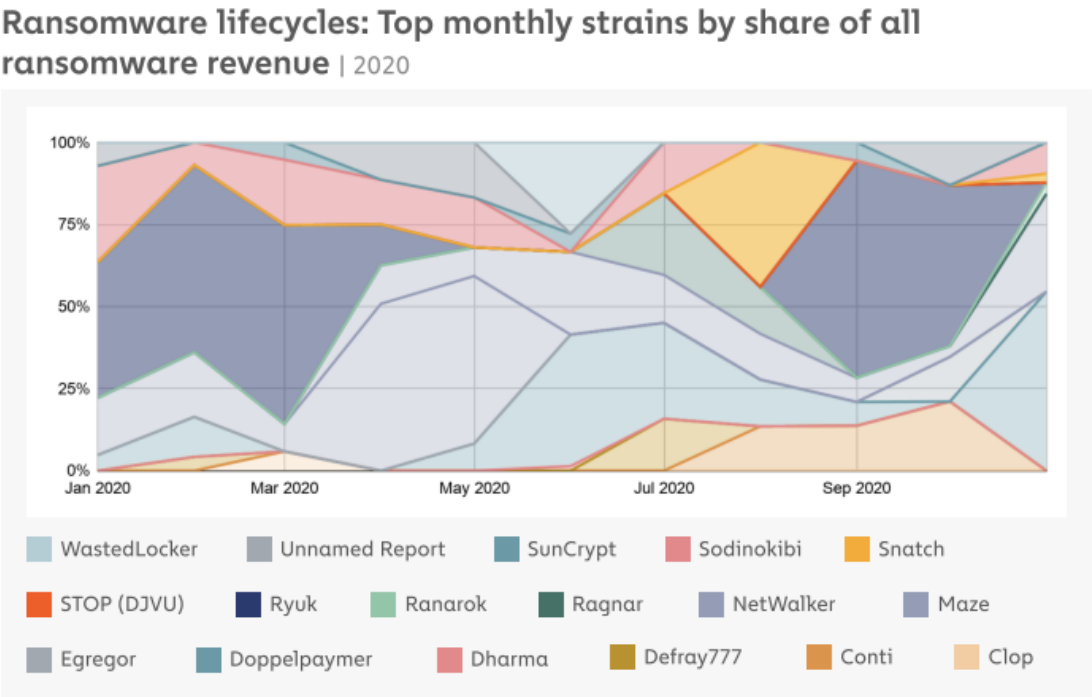
Figuur 29. Totaal losgeldbedrag dat door alle bekende ransomware groepen ieder jaar is opgehaald. Bron: Chainalysis, locatie: wereldwijd. [58]

Chainalysis suggereert dat de afname in losgeldbedragen deels veroorzaakt wordt door veranderingen in cybersecurity verzekeringen. Chainalysis stelt dat deze verzekeringsbedrijven

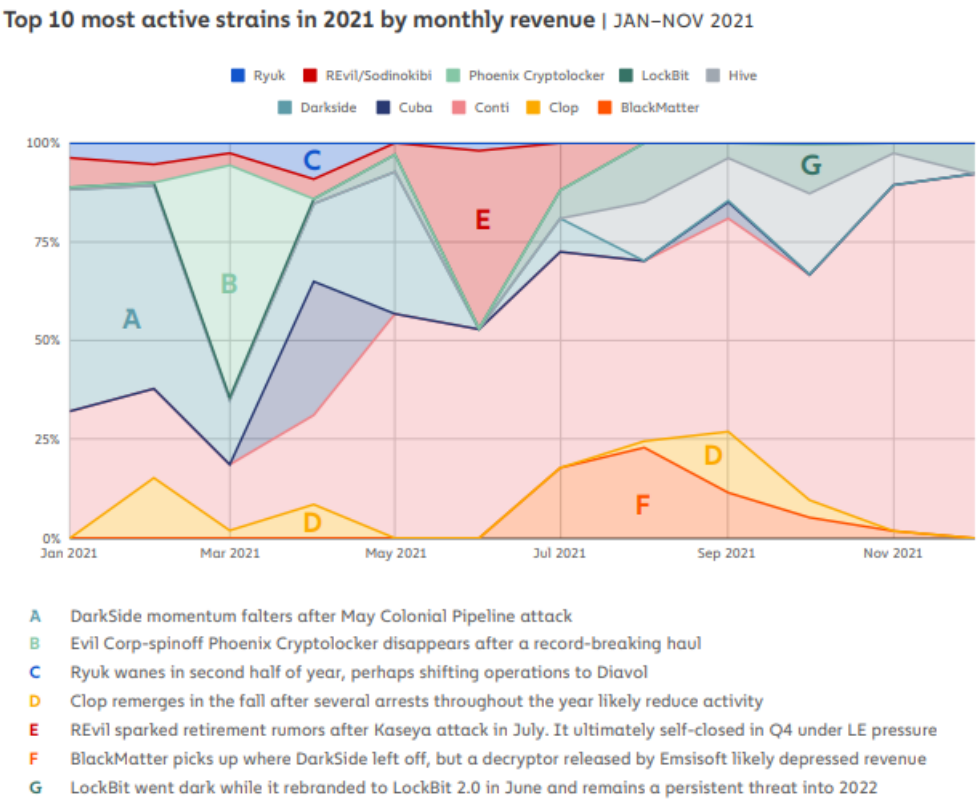
[18] Omdat mogelijk nog niet alle Bitcoin adressen van ransomware-groepen bekend zijn, kan het zijn dat het bedrag van $457M in werkelijkheid hoger is, maar de dalende trend is duidelijk zichtbaar.

in steeds mindere mate toelaten dat hun klanten losgeld betalen. De verzekeraars die in het kader van dit onderzoek betrokken zijn geven daarentegen aan dat de verzekeraar geen onderdeel uitmaakt van het beslisproces over het wel of niet betalen van losgeld. Daarnaast stellen de verzekeraars ook steeds hogere eisen aan bijvoorbeeld de back-up systemen van hun klanten, waardoor het betalen losgeld in sommige gevallen niet meer nodig is.

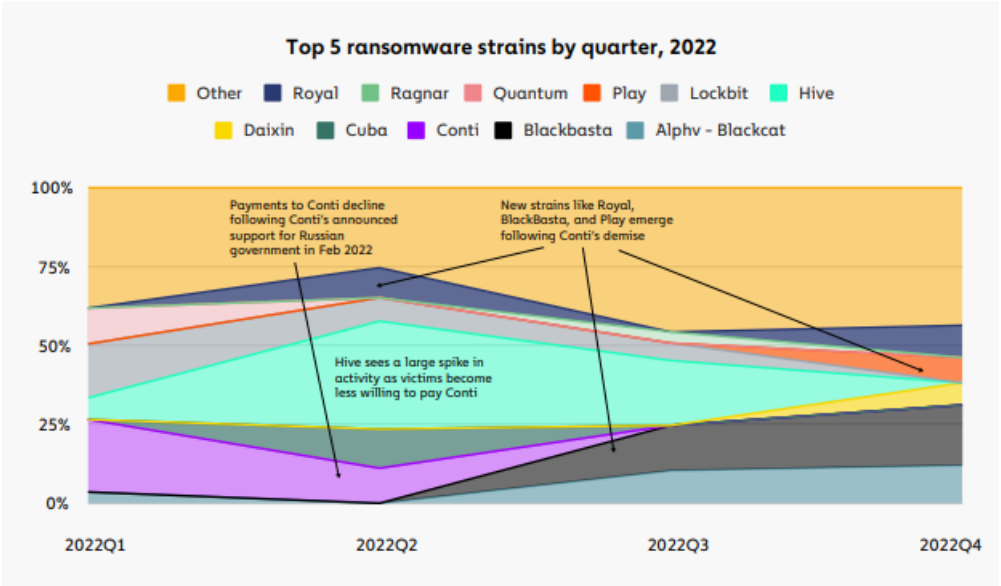
Veel groepen gebruiken Ransomware-as-a-Service (RaaS). Hierdoor zijn er op ieder moment vele verschillende *ransomware strains* in omloop. Chainalysis heeft voor ieder jaar de omzet van de meest winstgevende *strains* gedurende het jaar in kaart gebracht. In deze figuren wordt op ieder tijdpunt het marktaandeel van een bepaalde groep binnen alle betrokken groepen getoond. Hiermee laten de figuren dus niks zien over de totale omzet, maar alleen welke groep op welk moment de meeste omzet draaide. Deze figuren, met name die van 2021 en 2022, laten de relatie tussen de verschillende ransomware groepen en de actualiteit zien. In de figuur van 2022 toont Chainalysis bijvoorbeeld de verminderde inkomsten van de Conti groep nadat die hun medewerking hebben toegezegd aan de Russische overheid. [60]



Figuur 30: Ransomware strains met de meeste omzet per maand in 2020. Bron: Chainalysis, locatie: wereldwijd. [61]

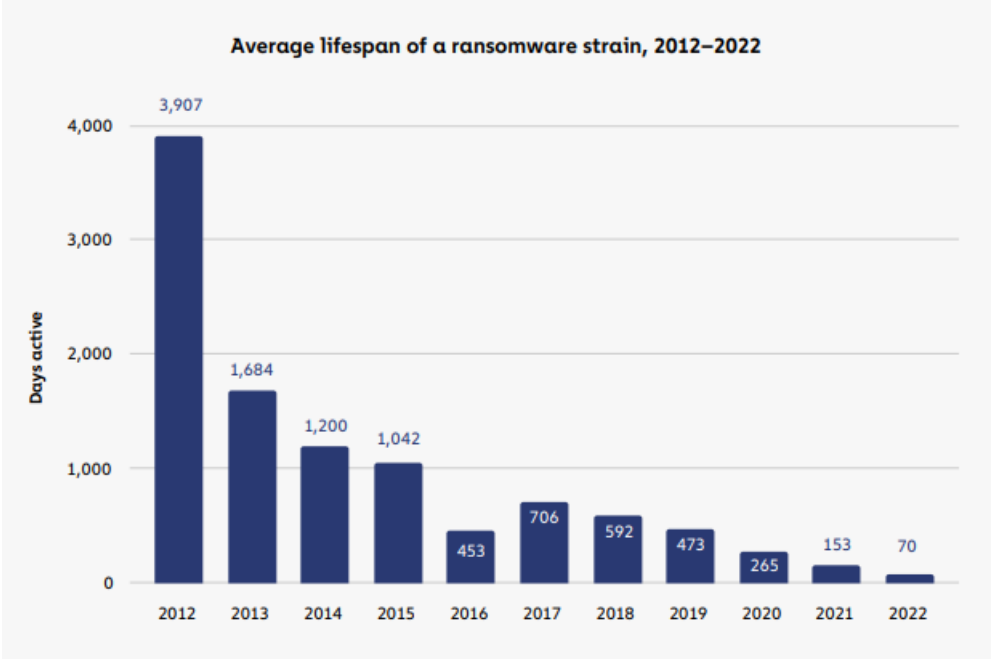


Figuur 31: Ransomware strains met de meeste omzet per maand in 2021. Bron: Chainalysis, locatie: wereldwijd. [60]



Figuur 32: Ransomware strains met de meeste omzet per maand in 2022. Bron: Chainalysis, locatie: wereldwijd. [59]

Wat in deze figuren naar voren komt is dat er maar weinig *strains* zijn die consistent actief zijn. **Het aantal dagen dat een ransomware *strain* actief blijft wordt daarnaast elk jaar korter** (zie Figuur 33). In 2022 is dit gemiddeld nog maar 70 dagen. [59]



Figuur 33: Aantal dagen dat een ransomware strain gemiddeld actief is. Bron: Chainalysis, locatie: wereldwijd. [59]

Binnen het RaaS-model kan eenzelfde ransomware groep meerdere ransomware *strains* (software) gebruiken. Hierdoor is het goed mogelijk dat eenzelfde hoeveelheid cybercriminelen simpelweg werkt met meerdere verschillende *strains*.

15.3 Conclusie

Het feit dat het lastig tot niet te achterhalen zijn of cryptobetalingen naar ransomware-groepen afkomstig zijn van Nederlandse organisaties maakt dat het cryptobetalingsverkeer geen hele waardevolle bron is voor het in kaart brengen van ransomware-aanvallen op Nederlandse organisaties. Wel kan er gekeken worden naar globale trends in betalingen naar ransomware-groepen. Hieruit komt het beeld naar voren dat er in 2022 wereldwijd minder losgeld betaald is dan in de voorgaande jaren.

16 No More Ransom

16.1 Beschrijving databron

No More Ransom is een initiatief van het Team High-Tech Crime van de Nationale Politie, het European Cybercrime Centre van Europol, McAfee en Kaspersky. Deze partijen werken binnen dit project samen met bijna 200 partners uit verschillende sectoren. No More Ransom heeft als doel slachtoffers van ransomware te helpen bij het herstellen van hun versleutelde gegevens, zonder dat zij hier losgeld voor betalen aan de cybercriminelen. Op de website nomoreransom.org kunnen slachtoffers voorbeelden van versleutelde bestanden en alle informatie uit het losgeldbericht (zoals e-mailadressen, website URL's en onion- of bitcoinadressen) uploaden. No More Ransom kan aan de hand hiervan kijken of ze al een sleutel hebben deze ransomware.

De statistieken van No More Ransom verschaffen geen specifieke informatie met betrekking tot ransomware-aanvallen gericht op Nederlandse instellingen en bedrijven, en bieden slechts beperkt inzicht in een kleine subset van slachtoffers, namelijk diegenen waarvoor reeds sleutels beschikbaar zijn.

16.2 Beeld uit databron

Europol rapporteert elk jaar aan het eind van het jaar in een infographic hoeveel sleutels er gedownload zijn, van hoeveel verschillende families deze gedownloade sleutels waren en (in hoeverre bekend) hoeveel losgeld er tot dat moment door deze beschikbare sleutels niet uitbetaald is aan de criminele organisaties. Uit Tabel 3 blijkt dat er tot het einde van 2022 in totaal 10 miljoen sleutels zijn gedownload met het doel om versleutelde bestanden, veroorzaakt door ransomware, te ontsleutelen. Dit waren er 4 miljoen meer dan aan het einde van 2021. In 2021 waren er 'slechts' 1,8 miljoen gedownload. Elk jaar komen er voor ongeveer 10 nieuwe ransomware families sleutels bij. Daarnaast is er voor zover bekend niet openbaar gemaakt hoeveel losgeld er in 2022 uit handen van criminelen is gebleven, maar het ligt in de lijn der verwachting dat dat in 2022 de grens van 1 miljard euro gepasseerd is.

Tabel 3. No More Ransom statistieken. M is miljoen (sleutels of dollars). Bron: No More Ransom, bewerking: Dialogic, locatie: wereldwijd. [62] [63] [64]

Jaar	Gedownloade sleutels	Ransomware families	Losgeld bespaard
2020	4.2M	140	$632M
2021	6M	151	$900M
2022	10M	165	-

Het feit dat er **elk jaar meer sleutels gedownload worden** zou kunnen impliceren dat er meer slachtoffers gemaakt worden met *cryptographic* ransomware. Maar het zou ook kunnen betekenen dat slachtoffers (of de betrokken incident response bedrijven) beter ingelicht zijn over ransomware, eerst de verschillende mogelijkheden (waaronder het zoeken naar een eventueel beschikbare sleutel) onderzoeken en niet direct overgaan tot het betalen van losgeld.

16.3 Conclusie

Elk jaar zijn er meer publieke decryptors beschikbaar en worden deze ook meer gebruikt. Dit kan of betekenen dat er meer slachtoffers van ransomware zijn of dat de slachtoffers die er zijn beter geïnformeerd zijn en bijvoorbeeld niet over gaan tot betalen, maar eerst op zoek gaan naar een andere oplossing. Desalniettemin is het nut van No More Ransom als databron voor het in kaart brengen van ransomware in Nederland zeer beperkt.

Deel 3: Conclusies

17 Antwoord op onderzoeksvragen

1. Met welke indicatoren kan inzicht worden gekregen in de mate waarin ransomware-aanvallen op instellingen en bedrijven in Nederland voorkomen en de aard en gevolgen van deze aanvallen met betrekking tot de eigenschappen van de getroffen instellingen en bedrijven, de response op de aanvallen, de geleden schade en andere gevolgen?

De indicatoren die op basis van literatuuronderzoek en interviews relevant zijn gebleken zijn:

- **Generieke kenmerken van een ransomware-aanval**. Deze indicator beslaat de aanvaller, het doelwit, de wijze waarop toegang is verkregen en de acties die gebruikt worden om druk uit te oefenen op het slachtoffer.
- **Kenmerken van het slachtoffer**. Bij deze indicator gaat het specifiek over de kenmerken van het slachtoffer, zoals de sector, de grootte of de locatie van de organisatie.
- **Impact van een ransomware-aanval**. Deze indicator brengt de gevolgen van een ransomware-aanval voor de individuele organisatie of de maatschappij in kaart.
- **Frequentie van ransomware-aanvallen**. Bij deze indicator gaat het niet om een specifieke ransomware-aanval, maar hoe vaak bepaalde ransomware-aanvallen op bepaalde slachtoffers met een bepaalde impact plaatsvinden.

2. Bevatten bestaande databronnen gegevens die inzicht bieden in de relevante indicatoren?

In dit onderzoek zijn elf bestaande databronnen geïdentificeerd die inzicht kunnen geven in de relevante indicatoren. Bij het interpreteren van de informatie uit deze databronnen moet ook de subset van slachtoffers waar de databron inzicht in geeft meegenomen worden. Er bestaat namelijk geen databron die voor een bepaalde indicator inzicht in kan geven in *alle* slachtoffers van ransomware. Deze databronnen zijn:

1. **Virusscanaanbieders** hebben vaak detectiemechanismes voor ransomware en hebben dus zicht op het aantal pogingen tot een ransomware-aanval.
    a. *Subset van slachtoffers*: Slachtoffers met aangevallen IT-systemen met een bepaalde virusscanner.
    b. *Indicatoren*: Generieke kenmerken van een ransomware-aanval, frequentie van ransomware-aanvallen.
2. **IT-dienstaanbieders** hebben zicht op verdachte activiteiten van de cybercrimineel wanneer deze binnen is gedrongen.
    a. *Subset van slachtoffers*: Slachtoffers met aangevallen IT-systemen waarbij een externe partij de IT-systemen verzorgt.
    b. *Indicatoren*: Generieke kenmerken van een ransomware-aanval, kenmerken van het slachtoffer.
3. **Incident response bedrijven** worden door het slachtoffer ingeschakeld om de response op de ransomware-aanval te coördineren.
    a. *Subset van slachtoffers*: Slachtoffers met geïnfecteerde IT-systemen die de hulp inschakelen van een externe partij.
    b. *Indicatoren*: Generieke kenmerken van een ransomware-aanval, kenmerken van het slachtoffer, impact van de ransomware-aanval.
4. **Cybersecurity-verzekeraars** worden door het slachtoffer ingelicht bij een ransomware-aanval en zijn ook betrokken bij de afhandeling.
    a. *Subset van slachtoffers*: Slachtoffers met geïnfecteerde IT-systemen en cybersecurity-verzekering.

    b. *Indicatoren*: Generieke kenmerken van een ransomware-aanval, kenmerken van het slachtoffer, impact van de ransomware-aanval.
5. **Politieaangiftes**. Bij een ransomware-aanval kan een slachtoffer hier bij de politie aangifte van doen, maar is hier niet toe verplicht.
    a. *Subset van slachtoffers*: Slachtoffers met geïnfecteerde IT-systemen die hiervan aangifte doen.
    b. *Indicatoren*: Generieke kenmerken van een ransomware-aanval, kenmerken van het slachtoffer, impact van de ransomware-aanval.
6. De **CBS Cybersecuritymonitor** bevraagt een selectie van Nederlandse organisaties of ze het afgelopen jaar te maken hebben gehad met een ransomware-aanval en wat daar de impact van is geweest.
    a. *Subset van slachtoffers*: Slachtoffers met geïnfecteerde IT-systemen die door het CBS bevraagd worden.
    b. *Indicatoren*: Kenmerken van het slachtoffer, impact van de ransomware-aanval, frequentie van ransomware-aanvallen.
7. De **media** rapporteren over bepaalde ransomware-aanvallen en heeft daarmee ook deels invloed op de impact van aanvallen op de maatschappij. Daarnaast vervullen de media een belangrijke rol als het gaat om de bewustwording van ransomware.
    a. *Subset van slachtoffers*: Slachtoffers met geïnfecteerde IT-systemen die nieuwswaardig zijn.
    b. *Indicatoren*: Generieke kenmerken van een ransomware-aanval, kenmerken van het slachtoffer, frequentie van ransomware-aanvallen.
8. Op **websites van ransomware-groepen** wordt gedreigd met het publiceren van gestolen data van slachtoffers en wordt deze data gepubliceerd als er geen losgeld is betaald.
    a. *Subset van slachtoffers*: Slachtoffers waar data van is gestolen.
    b. *Indicatoren*: Generieke kenmerken van een ransomware-aanval, impact van de ransomware-aanval.
9. De **Autoriteit Persoonsgegevens** heeft zicht op het aantal bij de AP gemelde datalekken. Slachtoffers van een ransomware-aanval moeten, bij een vermoeden van een datalek, een melding maken bij de AP.
    a. *Subset van slachtoffers*: Slachtoffers met (een vermoeden van) een datalek die dit melden bij de AP.
    b. *Indicatoren*: Generieke kenmerken van een ransomware-aanval, kenmerken van het slachtoffer, impact van de ransomware-aanval.
10. Het **cryptobetalingsverkeer** bevat losgeldbetalingen naar de ransomware-groepen.
    a. *Subset van slachtoffers*: Slachtoffers die losgeld betaald hebben in crypto's.
    b. *Indicatoren*: Impact van de ransomware-aanval.
11. **No More Ransom** biedt voor bepaalde ransomware-software *decryptors* aan waarmee de versleutelde bestanden ontsleuteld kunnen worden.
    a. *Subset van slachtoffers*: Slachtoffers met versleutelde bestanden waarvoor een publieke *decryptor* beschikbaar is.
    b. *Indicatoren*: Generieke kenmerken van een ransomware-aanval.

3. Welk beeld kan aan de hand van de bestaande databronnen worden gevormd voor de jaren 2020, 2021 en 2022 over de mate waarin ransomware-aanvallen op instellingen en bedrijven in Nederland voorkomen en de aard en gevolgen van deze aanvallen met betrekking tot de eigenschappen van de betrokken instellingen en bedrijven, de response op de aanvallen, de geleden schade en andere gevolgen?

De bestaande databronnen geven geen eenduidig beeld van ransomware-aanvallen op Nederlandse bedrijven en instellingen voor de jaren 2020, 2021 en 2022. Veel databronnen

zijn te generiek, waardoor het bijvoorbeeld niet mogelijk is om er specifiek informatie voor Nederland uit te halen, of ze beslaan niet de volledige periode 2020, 2021, 2022. Daarnaast spelen er bij een aantal partijen ook commerciële belangen mee of is de informatie die partijen publiekelijk beschikbaar maken zeer beperkt. Desalniettemin schetsen we hieronder per indicator een beeld.

Generieke kenmerken van ransomware-aanvallen

Aanvaller: Het cryptobetalingsverkeer laat in de jaren 2020, 2021 en 2022 zien dat het marktaandeel van de verschillende ransomware-groepen over de tijd sterk schommelt. Het oprollen van een groep leidt vaak tot het ontstaan van nieuwe groepen met een nieuwe software. Deze diversiteit aan ransomware-groepen is ook terug te zien in de rapportages van de virusscanaanbieders, waar vele verschillende ransomware *strains* gedetecteerd worden. Analyses van de websites van ransomware-groepen laten zien dat de LockBit groep in 2021 en 2022 verantwoordelijk is voor de meeste datalekken van Nederlandse organisaties.

Doelwit: Virusscanaanbieders laten zien dat er wereldwijd een toename is van gerichte aanvallen in 2021. Ook tonen deze virusscanaanbieders dat de opkomst van Ransomware-as-a-Service met name te zien is bij consumenten, maar minder bij de grote bedrijven en MKB'ers.

Initiële toegang: Zowel de IT-dienstaanbieders als de incident response bedrijven zeggen dat e-mail de meest gebruikte methode is van initiële toegang (*phishing*), gevolgd door desktop sharing software in de jaren 2020, 2021 en 2022.

Acties om druk uit te oefenen: Er is geen bron die inzicht geeft in de verhouding tussen de verschillende acties die gebruikt kunnen worden (blokkeren, versleutelen, data exfiltratie). Wel hebben we in de interviews opgehaald dat het stelen van data steeds gangbaarder wordt (vaak zelfs zonder de bestanden te versleutelen), terwijl het blokkeren van systemen tegenwoordig minder vaak voorkomt.

Kenmerken van slachtoffer

Locatie: De websites van ransomware-groepen, waar zij slachtoffers publiceren, laten zien dat Nederland in de periode 2021 en 2022 in de lijst van gepubliceerde organisaties op plek 12 staat. Amerikaanse organisaties worden het vaakst gepubliceerd. Ook bij de IT-dienstaanbieders bevinden de meeste slachtoffers van ransomware in de Verenigde Staten.

Sector: De industriële en financiële sectoren worden wereldwijd volgens de incident response bedrijven het vaakst getroffen. Uit de CBS cybersecuritymonitor komen ook de sectoren *industrie* en *financiële dienstverlening* naar voren als meest getroffen. De meeste politieaangiftes van ransomware komen uit de handelssector. Deze bronnen houden andere sectorverdelingen aan, maar wijzen wel met name naar organisaties in de industrie. Ten opzichte van 2020 was er in 2021 een verdubbeling van het aantal aangiftes uit de ICT-sector. Deze toename van aanvallen op de ICT-sector wordt ook beaamd door de Autoriteit Persoonsgegevens, die in 2021 de aanvallen op IT-leveranciers uitlichtten.

Grootte: De CBS Cybersecuritymonitor laat zien dat hoe groter de organisatie is (c.q. hoe meer werkzame personen), hoe groter de kans is dat de organisatie te maken heeft gehad met een ransomware-aanval. Ook de Autoriteit Persoonsgegevens zegt in 2020 voornamelijk meldingen van datalekken te hebben gehad van grotere organisaties die over veel persoonsgegevens beschikken. Leden van het Verbond van Verzekeraars geven daarentegen aan dat zij zien dat met name de kleinere MKB bedrijven door een afhankelijkheid van een enkel systeem en lage bewustwording slachtoffer worden van ransomware.

Impact van ransomware-aanvallen

Losgeld: Incident response bedrijven geven aan dat het aandeel van de aanvallen waarin tot het betalen van losgeld wordt overgegaan over de jaren 2020, 2021, 2022 flink is gedaald. Ook het cryptobetalingsverkeer laat zien dat er ten opzichte van 2020 en 2021 een omslag is geweest in 2022, waarbij alle slachtoffers samen veel minder losgeld betaald hebben. In de periode van juni 2022 tot juni 2023 zijn er daarnaast 32% van de gepubliceerde organisaties van de website van LockBit verwijderd. Organisaties worden vaak van de website verwijderd als ze losgeld betaald hebben. Dat impliceert dat ongeveer een derde van de LockBit slachtoffers die gepubliceerd zijn alsnog betaald hebben. Hier zat slechts één Nederlandse organisatie tussen. Tegenover de daling in de betalingsbereidheid staat wel een stijging in het gemiddeld betaalde losgeldbedrag in die periode. Uit politieaangiftes blijkt dat de gevraagde losgeldbedragen bij Nederlandse slachtoffers in de handel- en ICT-sector gemiddeld boven de miljoen euro uitkomen. Het betaalde losgeldbedrag bedraagt voor kleine bedrijven een groter percentage van de totale omzet dan voor grotere bedrijven (CBS Cybersecuritymonitor).

Kosten: Naast het betalen van losgeld kunnen ransomware-aanvallen ook andere kosten met zich meebrengen, zoals bijvoorbeeld de verstoring van de bedrijfscontinuïteit, het verlies van klanten door reputatieschade, het herstellen van de IT-systemen of het inschakelen van een incident response bedrijf. De politieaangiftes laten zien dat het gevraagde losgeldbedrag in veel gevallen disproportioneel hoog is en dat de geleden financiële schade door een ransomware-aanval uiteindelijk vaak lager ligt.

Frequentie van ransomware-aanvallen

Volgens rapportages van de verzekeraars (op basis van enquêtes) is 26% van de Nederlandse bedrijven in 2022 getroffen door ransomware. In 2021 en 2022 zijn er respectievelijk 107 en 110 aangiftes van ransomware binnengekomen bij de politie. De politie vermoedt dat slechts 2% tot 4% van de slachtoffers aangifte doet. Dat dit percentage laag is komt ook naar voren uit de CBS Cybersecuritymonitor, waar slechts 13% van de bedrijven aangeeft hulp te hebben gezocht bij de politie. Van de organisaties die bevraagd zijn in de cybersecuritymonitor van het CBS zegt slechts 1% een ransomware-aanval te hebben gehad in 2021. Analyses van berichtgeving in de media suggereert dat ransomware met name een 2021 een groot thema was.

4. Welke beperkingen hebben de bestaande databronnen met betrekking tot de beschikbaarheid, volledigheid en kwaliteit van data en in hoeverre gelden er andere beperkingen?

Geen enkele databron in dit onderzoeksrapport is vrij van beperkingen. Een eerste beperking is de beschikbaarheid van (relevante) data. Een aantal databronnen (zoals de virusscanaanbieders, IT-dienstaanbieders, incident response bedrijven en de cybersecurity-verzekeraars) hebben commerciële belangen. Zij publiceren mede daarom geen ruwe data, maar alleen rapportages. Deze rapportages bevatten vaak figuren en conclusies waarvan de oorsprong lastig te achterhalen is, maar die wel een verhaal vertellen dat de noodzaak van deze partijen onderschrijft. Doordat het ook onduidelijk is op basis van welke data of klantsegment de figuren zijn gemaakt, kunnen de resultaten uit de verschillende databronnen ook niet worden gecombineerd. Daarnaast zijn er partijen als het NCSC en de Autoriteit Persoonsgegevens die momenteel niet aan datadeling doen (de AP geeft echter wel aan hiermee bezig te zijn). Een tweede beperking, die voor de meeste databronnen geldt, is dat de databronnen niet specifiek zijn toegespitst op Nederlandse bedrijven en instellingen. De focus van veel databronnen ligt op Noord-Amerika of is wereldwijd. De enige databronnen zich specifiek

focussen op Nederland zijn de politieaangiftes, de datalekmeldingen bij de Autoriteit Persoonsgegevens en de uitkomsten van de CBS Cybersecuritymonitor.

Daarnaast is geen enkele databron volledig. Eerder bespraken we al dat databronnen slechts inzicht kunnen geven in een subset van slachtoffers, maar ook daarin zijn ze vaak niet volledig. Zo doen lang niet alle slachtoffers aangifte van een ransomware-aanval of belanden alle slachtoffers van data-exfiltratie op de websites van ransomware-groepen.

Tenslotte is de kwaliteit van de data in sommige gevallen niet toereikend voor het in kaart brengen van ransomware-aanvallen op Nederlandse bedrijven en instellingen. Het steekproefsgewijs bevragen van Nederlandse organisaties over hun ervaringen met ransomware zou een goed beeld moeten kunnen geven van de problematiek. Echter verschilt het percentage tussen de verschillende enquêtes wel heel erg sterk. Uit de enquêtes van de banken en verzekeraars lijkt de frequentie van ransomware overschat te worden, terwijl deze in de CBS Cybersecuritymonitor juist onderschat lijkt te worden. Het probleem bij de banken en verzekeraars ligt waarschijnlijk in de gekozen steekproef (waar disproportioneel veel slachtoffers inzitten), terwijl die bij de CBS Cybersecuritymonitor mogelijk in de vraagstelling ligt. De meeste resultaten uit de rapportages van commerciële partijen voldoen ook niet aan de standaarden van reproduceerbaarheid, waardoor de kwaliteit van de resultaten niet vast te stellen is.

5. Op welke wijze kunnen deze beperkingen worden verminderd of weggenomen?

Een centraal punt waar verschillende instanties hun data (geanonimiseerd en/of geaggregeerd) aan kunnen rapporteren zou enkele beperkingen van databronnen (die nu alleen rapportages uitbrengen) weg kunnen nemen. Incident response bedrijven, die zijn benaderd en in Nederland opereren, zeggen dat ze incidenten melden aan het NCSC. Daarnaast beschikt de Autoriteit Persoonsgegevens over meldingen van datalekken en kunnen slachtoffers in het meldproces aangeven dat het over een ransomware-aanval gaat. Zowel het NCSC als de AP delen deze data nu niet (ook niet met elkaar). Ook zou dit centrale punt bij bijvoorbeeld de virusscanbedrijven specifiek data over Nederlandse klanten uit kunnen vragen en de indexeerwebsites van ransomware-groepen kunnen monitoren voor Nederlandse slachtoffers.

Uit een vooronderzoek bleek al dat CBS-wet grondslag biedt voor verplichte data levering door overheidsorganisaties aan het CBS. Het CBS zou, in ieder geval voor overheidsorganisaties, kunnen fungeren als een centraal punt voor data van ransomware-aanvallen. Deze verplichting geldt niet voor commerciële partijen, zoals de verzekeraars, de virusscanaanbieders en de IT-dienstaanbieders. De overheid moet onderzoeken onder welke voorwaarden deze partijen bereid zijn data te delen over aanvallen op Nederlandse organisaties.

Daarnaast zouden slachtoffers meer gestimuleerd moeten worden om aangifte te doen bij de politie. De informatie die uit politieaangiftes komt is zeer rijk, maar helaas doet maar een klein percentage van de slachtoffers aangifte. Mogelijk zouden de verzekeraars hier een rol in kunnen spelen door een aangifte als voorwaarde te stellen voor het uitkeren van het schadebedrag (zoals bijvoorbeeld ook het geval is bij diefstal).

Tenslotte zou de CBS Cybersecuritymonitor uitgebreid en aangepast kunnen worden. De vraagstelling, en dan met name de gegeven voorbeelden, zijn nu erg beperkend. Ze richten zich bijvoorbeeld uitsluitend op *locker* ransomware (terwijl dat weinig meer voorkomt) en vragen niks over versleuteling van documenten of data-exfiltratie. Ook lijken sommige resultaten te impliceren dat niet de juiste persoon binnen een organisatie de vragenlijst heeft ingevuld. Het uitvragen van het kennisniveau van de respondent zou een juiste interpretatie van de resultaten bevorderen. Ook zou een grotere steekproef gewenst zijn, zodat alle subcategorieën (verschillende vormen van ransomware, losgeldbedragen, wel of niet betaald, gemaakte kosten, maar ook bedrijfssector en -grootte) groot genoeg zijn. Slachtoffers van

ransomware zijn mogelijk eerder geneigd deel te nemen aan een enquête over ransomware, dus het zal geen representatief beeld geven van de frequentie van ransomware op Nederlandse instellingen, maar het zou de verhoudingen binnen de groep slachtoffers wel beter in kaart kunnen brengen.

18 Aanbevelingen

Voor het vormen van een betrouwbaar beeld aan de hand van bestaande databronnen doen wij een aantal aanbevelingen:

1. Onderzoek hoe de barrières voor het delen van data over ransomware slachtoffers, zoals de privacy wetgeving, kunnen worden weggenomen (bijvoorbeeld door anonimisering of aggregatie). Stimuleer vervolgens datadeling van overheidsorganisaties als het NCSC, de Autoriteit Persoonsgegevens en de Politie met een centraal punt als het CBS. Artikel 33 van de CBS-wet biedt grondslag voor verplichte datalevering door overheidsorganisaties aan het CBS. Het combineren (en indien mogelijk koppelen) van data over ransomware van (in ieder geval) de overheidsorganisaties is een belangrijke eerste stap naar het vormen van een beeld van de ransomware problematiek.
2. De overheid moet onderzoeken onder welke voorwaarden commerciële partijen zoals de virusscanaanbieders, IT-dienstaanbieders en de verzekeraars bereid zijn data te delen over aanvallen op Nederlandse organisaties. Dit gebeurt idealiter met hetzelfde centrale punt als waarmee de overheidsorganisaties communiceren. Deze commerciële partijen bezitten informatie die overheidsorganisaties niet kunnen vergaren, maar delen deze data niet en rapporteren hier ook niet of nauwelijks over. Daarnaast zijn de rapportages van deze commerciële partijen opgesteld uit eigen belang en vertellen vaak een eenzijdig verhaal dat erop gericht is meer klanten aan te trekken.
3. Onderzoek op welke manier de aangiftebereidheid onder slachtoffers van ransomware verhoogd kan worden. Er zou bijvoorbeeld onderzocht kunnen worden of verzekeraars hier een rol in kunnen spelen door een aangifte als voorwaarde te stellen voor het uitkeren van het schadebedrag (zoals bijvoorbeeld ook het geval is bij diefstal). Politieaangiftes zijn een zeer rijke bron van informatie als het gaat over de kenmerken van het slachtoffer en de impact van de ransomware-aanval, maar momenteel doet slechts een fractie van de slachtoffers aangifte. Daarnaast worden overkoepelende trends uit de aangiftes over de kenmerken van aanvallen gebruikt door het ransomware *taskforce* om de cybercriminelen op te sporen en uit te schakelen.
4. Benut landelijke enquêtes of monitors als de CBS Cybersecuritymonitor beter door de steekproef te vergroten en de vraagstelling met betrekking tot ransomware uit te breiden en te verbeteren. Het landelijk bevragen van organisaties is een goede methode voor het in kaart brengen van de frequentie van ransomware-aanvallen, de kenmerken van de aanvallen en slachtoffers en de impact van ransomware-aanvallen. De huidige resultaten doen echter vermoeden dat het aantal bevraagde organisaties dat in het afgelopen jaar daadwerkelijk slachtoffer was van ransomware erg klein was. Hierdoor kan op basis van deze resultaten geen betrouwbaar beeld gevormd worden van ransomware-aanvallen op Nederlandse bedrijven. Wanneer een organisatie benaderd wordt voor het invullen van de enquête en aangeeft te maken te hebben gehad met een ransomware-aanval, zouden de kenmerken van de aanval, de kenmerken van het slachtoffer en de impact van de ransomware-aanval in detail en voor zover bekend uitgevraagd moeten worden.

Verwijzingen

[1] NCTV (2021). *Cybersecuritybeeld Nederland 2021* [www.nctv.nl] Den Haag: Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).

[2] Kaspersky (2023). *Wat is WannaCry-ransomware?* [www.kaspersky.nl]

[3] Bruijnesteijn, B. (2021). *Opportunistische vs gerichte ransomware-aanvallen* [www.channelweb.nl]

[4] Hartholt, S. (2020). *Rotterdamse Haven krijgt eigen ´cyberkorps´ om hackers te weren* [www.agconnect.nl]

[5] ENISA (2022). *ENISA THREAT LANDSCAPE FOR RANSOMWARE ATTACKS* [www.enisa.europa.eu]

[6] Brennenraedts, R., Holland, C., Batenburg, R., den Hertog, P., te Velde, R., en Jansen, S. (2008). *Go with the dataflow! Analysing the Internet as a data source (IaD): Main report* [www.dialogic.nl] Den Haag: Ministry of Economic Affairs.

[7] SOCRadar (2023). *Evolution of Ransomware: So Far and Hereafter* [socradar.io]

[8] Hitachi Systems Security Inc.. *Why Ransomware-as-a-Service (RaaS) is Exploding as a Cyber Threat* [hitachi-systems-security.com]

[9] Oz, H., Aris, A., Levi, A., en Selcuk Uluagac, A. (2022). *A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions*ACM Computing Surveys (CSUR).

[10]Beaman, C., Barkworth, A., Akande, T.D., Hakak, S., en Khan, M.K. (2021). *Ransomware: Recent advances, analysis, challenges and future research directions.*Computers & security.

[11]Dialogic (2022). *Verkenning risicofactoren ransomware-aanvallen.*Den Haag: WODC.

[12]Lipovský, R., Štefanko, L., en Braniša, G. (2016). *The Rise of Android Ransomware* [www.welivesecurity.com]

[13]Korolov, M. (2015). *Report: IoT is the next frontier for ransomware* [www.csoonline.com]

[14]Trend Micro (2021). *IoT and Ransomware: A Recipe for Disruption* [www.trendmicro.com]

[15]Dickson, B. (2016). *The IoT ransomware threat is more serious than you think* [bdtechtalks.com]

[16]Tajalizadehkhoob, S., Goethem, T.v., Korczyński, M., Noroozian, A., Böhme, R., Moore, T., Joosen, W., en Eeten, M.v. (2017). *Herding Vulnerable Cats: A Statistical Approach to Disentangle Joint Responsibility for Web Security in Shared Hosting* [www.researchgate.net] ACM CCS'17.

[17]Gatlan, S. (2020). *Thanos Ransomware adds Windows MBR locker that fails every time* [www.bleepingcomputer.com]

[18]Trend Micro (2017). *Frequently Asked Questions: The Petya Ransomware Outbreak* [www.trendmicro.com]

[19]Jarno Baselier. *Nieuwe ransomware Petya overschrijft MBR* [jarnobaselier.nl]

[20]Savage, K., Coogan, P., en Lau, H. (2015). *The evolution of ransomware* [its.fsu.edu] Symantec.

[21]Cyberveilig Nederland (2023). *Data-exfiltratie bij een ransomware-aanval* [cyberveilignederland.nl]

[22]Nationaal Coördinator Terrorismebestrijding en Veiligheid. *Vitale infrastructuur* [www.nctv.nl]

[23]Symantec Threat Hunter Team (2022). *The Ransomware Threat Landscape: What to Expect in 2022* [www.symantec.broadcom.com] Symantec by Broadcom Software.

[24]Kaspersky (2022). *Kaspersky Security Belletin 2022* [go.kaspersky.com] Kaspersky.

[25]Symantec Threat Hunter Team (2020). *Targeted Ransomware* [symantec.broadcom.com] Symantec, A Division of Broadcom.

[26]Verizon (2023). *2023 Data Breach Investigations Report* [www.verizon.com]

[27]Verizon (2022). *2022 Data Breach Investigations Report* [www.verizon.com]

[28]CrowdStrike (2022). *2022 GLOBAL THREAT REPORT* [irp.cdn-website.com]

[29]Fox-IT (2022). *Annual Threat Monitor 2022* [www.nccgroup.com]

[30]vmware (2022). *Global Incident Response Threat Report* [www.vmware.com]

[31]Coveware (2023). *Ransomware Quarterly reports* [www.coveware.com]

[32]Micosoft (2021). *Microsoft Digital Defense Report Otober 2021* [query.prod.cms.rt.microsoft.com]

[33]Verbond van Verzekeraars (2023). *Omvang cyberverzekeringsmarkt* [www.verzekeraars.nl]

[34]HISCOX (2022). *Cyber Readiness Report 2022* [www.hiscoxgroup.com]

[35]HISCOX (2021). *Hiscox Cyber Readiness Report 2021* [www.hiscox.com]

[36]Allianz (2023). *Allianz Risk Barometer 2023* [www.agcs.allianz.com]

[37]ABN (2023). *Mkb isoleert zich door beperkt bewustzijn cyberdreiging* [www.abnamro.nl]

[38]CHUBB (2023). *Cyberverzekering CHUBB* [docs.mijnturien.nl]

[39]AIG (2023). *Cyberverzekering AIG: Informatiedocument over het verzekeringsproduct* [verzekeringskaarten.nl]

[40]HISCOX (2022). *Cyber en data risks verzekering* [docs.mijnturien.nl]

[41]Markel (2023). *Cyber 360 MISE 2023: Informatiedocument over het verzekeringsproduct* [verzekeringskaarten.nl]

[42]Centraal Beheer (2023). *Cyberverzekering Voorwaarden* [www.centraalbeheer.nl]

[43]Meurs, T., Junger, M., Tews, E., en Abhishta, A. (2022). *Ransomware: How attacker's effort, victim characteristics and context influence ransom requested, payment and*

financial loss. [www.researchgate.net] Symposium on Electronic Crime Research, eCrime 2022..

[44]Politie (2022). *Nederlandse gedupeerden geholpen in unieke ransomware-actie* [www.politie.nl]

[45]CBS StatLine (2022). *ICT-gebruik bij kleine bedrijven; bedrijfstak en bedrijfsgrootte, 2022* [opendata.cbs.nl]

[46]CBS (2023). *Ruim 2 duizend bedrijven in 2021 de dupe van ransomware* [www.cbs.nl]

[47]CBS StatLine (2022). *ICT-gebruik bij kleine bedrijven; bedrijfsgrootte, 2022* [opendata.cbs.nl]

[48]CBS StatLine (2022). *ICT-gebruik bij zzp'ers; bedrijfstak, 2022* [opendata.cbs.nl]

[49]Digital Trust Center (2023). *Veel kleine bedrijven zijn onvoldoende cyberweerbaar* [www.digitaltrustcenter.nl]

[50]Mousqueton, J. (2023). *Ransomware.live: Ransomware indexer & aggregator* [github.com]

[51]DarkTracer (2023). *The New Frontier of Darkweb Intelligence. Light up the dark* [darktracer.com]

[52]Hotsauce, T. (2022). *Evolution of LockBit to 3.0* [medium.com]

[53]Verlaan, D. (2023). *Cybercriminelen eisen meer dan miljoen euro van KNVB na ransomware-aanval* [www.rtlnieuws.nl]

[54]Hofmans, T. (2023). *Lockbit haalt dreigement over KNVB-data van website* [tweakers.net]

[55]Autoriteit Persoonsgegevens. *Datalekken* [autoriteitpersoonsgegevens.nl]

[56]Autoriteit Persoonsgegevens. *Boetes en andere sancties* [autoriteitpersoonsgegevens.nl]

[57]Autoriteit Persoonsgegevens (2023). *Datalekkenrapportage 2022* [www.autoriteitpersoonsgegevens.nl]

[58]Autoriteit Persoonsgegevens (2020). *Meldplicht datalekken: facts & figures. Overzicht feiten en cijfers 2020.* [autoriteitpersoonsgegevens.nl]

[59]Chainalysis (2023). *The 2023 Crypto Crime Report. Everything you need to know about cryptocurrency-based crime.*Chainalysis.

[60]Chainalysis (2022). *The 2022 Crypto Crime Report. Original data and research into cryptocurrency-based crime.*Chainalysis.

[61]Chainalysis (2021). *The 2021 Crypto Crime Report. Everything you need to know about ransomware, darknet markets, and more.*Chainalysis.

[62]No More Ransom (2020). *NO MORE RANSOM!* [www.europol.europa.eu]

[63]No More Ransom (2021). *Facts & Figures 2021.* [www.rapid7.com]

[64]No More Ransom (2022). *Facts & Figures 2022.* [www.europol.europa.eu]

[65]CBS, (2023). *Bedrijven; bedrijfstak* [opendata.cbs.nl]

[66]Tom Meurs, M.J. E. T. A. A. (2023). *Ransomware: How attacker's effort, victim characteristics and context influence ransom requested, payment and financial loss*Enschede,

[67]CBS, (2023). *SBI codes - Centraal Bureau voor de Statistiek* [sbi.cbs.nl]

[68]BURGESS, M., en NEWMAN, L.H. (2023). *The Unrelenting Menace of the LockBit Ransomware Gang* [www.wired.co.uk]

[69]Alex Scroxton (2022). *Ransomware crews regrouping as LockBit rise continues* [www.computerweekly.com]

[70]News, T.N. (2023). *Number of companies paying ransom to hackers decline, study says* [www.thenationalnews.com]

[71]Liska, A., en Gallo, T. (2016). *Ransomware: Defending Against Digital Extortion*O'Reilly Meida, Inc..

[72]Andronio, N. (2015). *Heldroid: Fast and efficient linguistic-based ransomware detection*University of Illinois at Chicago.

[73]Meland, P.H., Bayoumy, Y.F. F., en Sindre, G. (2020). *The Ransomware-as-a-Service economy within the darknet.*Computers & Security.

[74]Muckin, M., en Fitch, S. (2019). *A Threat-Driven Approach to Cyber Security* [www.lockheedmartin.com] Lockhead Martin White paper.

[75]Trend Micro. *Command and Control [C&C] Server* [www.trendmicro.com]

[76]Mous, A. (2023). *LockBit publiceert cliëntgegevens zorginstelling* [www.vpngids.nl]

[77]NOS (2023). *Cyberaanval bij zorginstelling: gegevens van cliënten gedeeld* [nos.nl]

[78]Goud, N. (2023). *LockBit Ransomware Group feels ashamed for the Cyber Attack* [www.cybersecurity-insiders.com]

[79]LockBit (2022). *Twitter* [twitter.com]

[80]Politie. *Samen tegen cybercrime. Stappenplan voor IT-specialisten.* [www.politie.nl]

[81]Lockheed Martin. *The Cyber Kill Chain* [www.lockheedmartin.com]

[82]Nationaal Coördinator Terrorismebestrijding en Veiligheid (2021). *Cybersecuritybeeld Nederland. CSBN 2021.* [open.overheid.nl] Nationaal Coördinator Terrorismebestrijding en Veiligheid.

Bijlage 1. Overzicht interviewrespondenten

Respondent	Organisatie
Analyst*	NCSC
David Davrados	Autoriteit Persoonsgegevens
Marko van Leeuwen	Verbond van Verzekeraars
Matthijs Jaspers	Nationale Politie
Rik van Dijk	NCSC
Rolf van Wegberg	TU Delft
Statistische onderzoekers**	CBS
Stefan Zwager	Verbond van Verzekeraars
Tom Meurs**	Universiteit Twente
Yasin Chalabi	Verbond van Verzekeraars

* Naam bekend bij onderzoekers

**Schriftelijk contact

Bijlage 2. CBS Cybersecuritmonitor

Tabel 4. Percentage van organisaties met een ransomware-aanval dat losgeld heeft betaald, uitgesplitst naar bedrijfstak aantal werkzame personen. Bron: CBS.

1e digit	Bedrijfstak	2 tot 10	10 tot 50	50 tot 250	250 of meer
C	Industrie	**11%**	**16%**	**1%**	**7%**
D-E	Energie, water, afvalbeheer	0%	0%	0%	0%
F	Bouwnijverheid	0%	0%	**8%**	0%
G	Handel	**31%**	0%	**10%**	**10%**
H	Vervoer en opslag	0%	**5%**	**27%**	0%
I	Horeca	0%	0%	0%	0%
J	Informatie en communicatie	0%	0%	0%	0%
K	Financiële dienstverlening	0%	0%	0%	0%
L	Verhuur en handel van onroerend goed	0%	0%	0%	0%
M	Specialistische zakelijke diensten	**7%**	**11%**	0%	0%
N	Verhuur en overige zakelijke diensten	0%	0%	**9%**	0%
Q	Gezondheids- en welzijnszorg	0%	0%	**31%**	0%
	ICT-sector	**4%**	0%	0%	0%

Tabel 5. Losgeldbetalingen per categorie werkzame personen. Bron: CBS Statline, locatie: Nederland. [47]

Werkzame personen	2	3 - 5	5 - 10	10 – 20	20 – 50	50 – 100	100 – 250	250 – 500	500+
Ransomware-aanval gehad (% van bedrijven)	0	1	1	1	2	2	3	4	4
Losgeld betaald (% van bedrijven met ransomware-aanval)	29	1	16	8	2	0	11	7	2
Betaling losgeld zinvol (% van bedrijven met ransomware-aanval)	1	1	16	8	1	0	9	7	2
Losgeldbedrag door ransomware-aanval (% van bedrijven die losgeld betaald hebben)									
<1% van de totale omzet	3	0	26	50	0	0	44	100	0
1 tot 2% van de totale omzet	0	100	74	44	43	0	22	0	100
2 tot 5% van de totale omzet	0	0	0	0	57	0	22	0	0
5 tot 10% van de totale omzet	0	0	0	6	0	0	12	0	0
10 tot 50% van de totale omzet	0	0	0	0	0	0	0	0	0
>= 50% van de totale omzet	97	0	0	0	0	0	0	0	0

Bijlage 3. Mapping van sectoren

Sector	SBI-sector(en)
Handel	G Handel
ICT	2611 Elektronische componentenindustrie
	2612 Elektronische printplaatindustrie
	2630 Communicatieapparatenindustrie
	2640 Consumentenelektronicaindustrie
	2680 Industrie van informatiedragers
	465 Groothandel in ICT-apparatuur
	582 Uitgeverijen van software
	61 Telecommunicatie
	62 IT-dienstverlening
	631 Gegevensverwerking e.d.; webportals
	951 Reparatie van computers en telecom
Bouw	F Bouwnijverheid
Transport	H Vervoer en opslag
Gezondheidszorg	Q Gezondheids- en welzijnszorg
Recreatie	R Cultuur, sport en recreatie
Media	J Informatie en communicatie
Onderwijs	P Onderwijs
MAS	A Landbouw, bosbouw en visserij
Overheid	O Openbaar bestuur en overheidsdiensten

Bijlage 4. Lockbit Affiliate Rules

The oldest international [Ransomware] LockBit affiliate program welcomes you.
We are located in the Netherlands, completely apolitical and only interested in money.
We always have an unlimited amount of affiliates, enough space for all professionals. It does not matter what country you live in, what types of language you speak, what age you are, what religion you believe in, anyone on the planet can work with us at any time of the year.
First and foremost, we're looking for cohesive and experienced teams of pentestors.
In the second turn we are ready to work with access providers: sale or on a percentage of redemption, but you have to trust us completely. We provide a completely transparent process - you can control the communication with the victim. In case when the company was encrypted and has not paid, you will see the stolen data in the blog.
We also work with those who don't encrypt networks, but just want to sell the stolen data, posting it on the largest blog on the planet.

Brief description of functionality:
- admin panel on the Tor network;
- communication with companies on the Tor network, chat with notifications and file transfer;
- the ability to create private chats for secret communication with companies;
- automatic decryption of test files;
- automatic decrypter output, by pressing the button in the panel;
- possibility of maximum protection of the decrypter, in this case the decrypter is stored on the flash drive;
- StealBit stealer, searchable by file name and extension;
- automatic data uploading to the blog, by you personally without our participation;
- Possibility to specify any Internet port in StealBit for downloading, for example 22 or 3389, to bypass network security policies;
- The ability to upload pictures to the blog;
- Ability to post the history of correspondence with the attacked company to the blog;
- ability to generate builds with different settings, but with one encryption key for one corporate network;
- 2 different encryption lockers for Windows in one panel, written by different programmers, allowing to encrypt the network twice, if time allows, it will be useful for paranoiacs who doubt the reliability and implementation of the cryptographic algorithm and believe in free decryption;
- ability to edit the list to kill processes and services;
- ability to edit the list of exceptions - computer name, names and file extensions that do not need to be encrypted;
- the fastest and most efficient cleanup (without the possibility of recovery) of free space after encryption;
- file name encryption, helps to avoid even partial recovery of a piece of information from the desired file;
- killing and removing Windows Defender;
- impersonation to automatically elevate permissions on local computers;
- SafeMode operation for bypassing anti-viruses and stronger encryption;

- port scanner in local subnets, can detect all shared DFS, SMB, WebDav resources;
- automatic distribution in the domain network at runtime without the need for scripts, GPO or psexec methods;
- safely delete the shadow copies;
- delete artifacts from system journals. It necessary to protect from forensics examination;
- shutting down the computer after finishing work, to make it impossible to remove the dump from RAM;
- printing claims on network printers in infinite numbers;
- work on all versions of Windows, with very flexible settings (exe, dll, ReflectiveDll, ps1);
- running on all versions of ESXi (except 4.0), with very flexible settings;
- work on multiple Linux versions (14 architectures for NAS encryption, RedHat, KVM and others);

All this and much more awaits you, if you join our team. If you do not find one of your favorite features, please inform us, maybe we will add it especially for you.

Rules of the affiliate program:

You must be active to work with our software package.
It is strictly forbidden to give access to the panel to other people. If you work with an affiliate, you may be given a sub-account with correspondence reading rights for your affiliate. You should be aware that your partner may turn out to be a mole or be arrested by the police at any moment.
It is forbidden not to fulfill agreements that you stated in chat before payment. For example, promising to give a file tree, and then not doing so.
It is imperative to download valuable information from every company you attack. If you can't bypass your firewall settings and you don't have the ability to download the information, then perhaps our proprietary StealBit Stealer can help you.
It is not forbidden to work with competitors, but be sure to report it and explain why and what you like from your competitors, we will implement any of your worthy wishes, we care very much about progress and constant development.

Categories of targets to attack:

It is illegal to encrypt files in critical infrastructure, such as nuclear power plants, thermal power plants, hydroelectric power plants, and other similar organizations. Allowed to steal data without encryption. If you can't figure out if an organization is a critical infrastructure, ask your helpdesk.
The oil and gas industry, such as pipelines, gas pipelines, oil production stations, refineries, and other similar organizations are not allowed to be encrypted. It is allowed to steal data without encryption.
It is forbidden to attack the post-Soviet countries such as: Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan, Ukraine and Estonia. This is due to the fact that most of our developers and partners were born and grew up in the Soviet Union, the former largest country in the world, but now we are located in the Netherlands.

It is allowed to attack non-profit organizations. If an organization has computers, it must take care of the security of the corporate network.

It is allowed to attack any educational institutions as long as they are private and have a revenue.
It is allowed to very carefully and selectively attack medical related institutions such as pharmaceutical companies, dental clinics, plastic surgeries, especially those that change sex and force to be very careful in Thailand, as well as any other organizations provided that they are private and have rhubarb. It is forbidden to encrypt institutions where damage to the files could lead to death, such as cardiology centers, neurosurgical departments, maternity hospitals and the like, that is, those institutions where surgical procedures on high-tech equipment using computers may be performed. It is allowed to steal data from any medical facilities without encryption, as it may be a medical secret and must be strictly protected in accordance with the law. If you can't pinpoint whether or not a particular medical organization can be attacked, contact the helpdesk.
It is very commendable to attack police stations and any other law enforcement agencies that are engaged in finding and arresting hackers, they do not appreciate our useful work as a pentest with postpaid and consider it a violation of the law, we should show them that a competent computer network setup is very important and write a fine for computer illiteracy.
It is allowed to attack government organizations, only with revenue.

Percentage rate of affiliate program is 20% of the ransom, if you think that this is too much and because of this you are working with another affiliate program or using your personal software, then you should not deny yourself the pleasure of working with us, just increase the amount of ransom by 20% and be happy.
You receive payments from companies to your personal wallets in any convenient currency and only then transfer the share to our affiliate program. However, for ransom amounts over $500 thousand, you give the attacked company 2 wallets for payment - one is yours, to which the company will transfer 80%, and the second is ours for 20%, thus we will be protected from scam on your part.

You personally communicate with the attacked companies and decide yourself how much money to take for your invaluable pentest work, which should surely be generously paid.

If you have any questions, doubts or complaints, you do not like something, please tell it to TOX support. If you are very shy, you can do it anonymously by creating a new one-time TOX. It is very important for us to know about all our strengths and weaknesses in order to constantly improve our service.

Every candidate to join our affiliate program should understand that we are constantly trying to be hacked and harmed in some way. This is why we pay a lot of attention to the candidates who join our partnership program. When joining, a lot of factors are taken into consideration, such as the reputation on the forums, the team composition, evidence of work with other affiliate programs, your wallet balance, the amount of previous payments and much more. You can also join our team by a guarantee of our partners, who are already active and time-tested.

After many years of experience, we concluded that the most effective way to test a candidate for accession is a deposit. When you join, you deposit 1 bitcoin in our wallet, in fact, this amount is an advance and will be used at your subsequent payments as payment for our

20% share. For example, the company paid you a ransom for decrypting 100 bitcoins, you have to transfer a share of 20 bitcoins to us, but thanks to the deposit you made when you joined, the amount of the share paid will be 19 bitcoins. This procedure is required only once, only when you join the affiliate program. The deposit weeds out insecure newbies, cops, FBI agents, journalists, white haters, web pentesters, competitors, and other small rodent pests. The deposit amount may be reduced or not required at all, depending on what reputation you have and what information you can provide about yourself. For those who are afraid to trust us with their money and think that we are scammers, it is possible to carry out this procedure through a guarantor, any reputable forum, in this case, you make a deposit on the balance of the forum, where we describe the conditions of the deposit, which are very simple, for example, if you can not earn 5 bitcoins in a month, then your deposit goes to us.

Please, be understanding with such a careful attitude to your candidacy, because you personally would not be very pleased if your newly encrypted company was decrypted for free by the FBI thanks to some person who easily gained access to the panel and made a masterful hack of our servers using zero-day vulnerabilities.

Recommended, but not required, application form when joining:

1) Links to your profiles on various hacker forums - the older your account, the better.
2) Describe your experience with other affiliate programs, preferably with some evidence, such as screenshots and transactions that show your payouts.
3) Show your balance in cryptocurrency at the moment.
4) Explain the reasons why you left another affiliate program and want to work with us.
5) Tell about the current accesses you have and are ready to attack immediately after joining us. It is recommended to prove yourself immediately after joining - the sooner you get the first payment, the less doubt will be cast on your identity.
6) It is desirable to have already downloaded information for the blog from the intended target for the attack and provide evidence of the existence of this information, such as screenshots, file tree or access to these files.
7) Ask your friends or acquaintances who already work with us to vouch for you.
8) Request a bitcoin or monero wallet to make a deposit, in case you are confident in your abilities and ready to earn millions of dollars with us.

To summarize, the reasons why it is better to work with us:

LockBit brand - the whole planet knows about us, we are trusted by encrypted companies, we have shown everyone that it is safe to cooperate with us, we are responsible for our words, we have never cheated anyone and always fulfill our agreements. Decrypter work, stolen data is deleted.
Stability: we have been working for 3 years, and no negative news regarding ransomware could scare and stop us, and so far we could not be caught by the FBI. If they couldn't catch us in 3 years, they probably never will, and we will keep working.
Probably the best software and the most extensive list of operating systems and architectures you can attack.
You negotiate and make all the decisions yourself.
Payments to your wallet: there is no way we can cheat you and commit exit scams, as many affiliate programs have done and will continue to

do. In addition, in 3 years we have earned a lot of money, so much so that there is no point in ruining your reputation because of some insignificant amount of a few million dollars.
We store stolen company data for as long as possible on our blog so that companies are afraid to allow leaks and pay for stolen data if there are backups and there is no need to pay for a decrypter.
We have no payout limits - you can encrypt RDP individuals or companies with any income level, any payout is nice for us - both $5,000,000 and $50 million, because we love our work and the process itself, and money is just a nice addition.
The best anti-ddos protection and a lot of mirrors, stability of communication with companies is very important for getting payouts.
Possibility to create private chats for secret communication with Recovery companies: it is very useful to keep secrecy of correspondence and avoid disrupting negotiations.
Decrypter security: the maximum protection for decrypters allows you to be sure that your company will not be decrypted for free due to any vulnerabilities in the web panel.
Bug bounty program: we understand that there is always a possibility of zero-day vulnerability attacks and we fight this threat with all possible means.

This page is translated in Google translator. If you are a native speaker and you see a grammatical error, please let us know so that we can correct it and thus show respect to your language and culture.

Contact:
Dialogic innovatie & interactie
Hooghiemstraplein 33-36
3514 AX Utrecht
Tel. +31 (0)30 215 05 80
www.dialogic.nl