# NAS-ransomware: hoe ransomware-aanvallen tegen NAS-apparaten verschillen van reguliere ransomware-aanvallen

*Tom Meurs, Marianne Junger, Erik Tews & Abhishta Abhishta*

*Een specifiek type ransomware-aanval richt zich op NAS-apparaten. In deze studie onderzoeken we het verschil tussen deze NAS-ransomware en reguliere ransomware. Uit de resultaten blijkt dat er bij NAS-ransomware andere ransomware-varianten bij de aanval worden gebruikt, dat slachtoffers vaker particulieren zijn en dat het gevraagde losgeld en de financiële schade lager zijn dan bij reguliere ransomware-aanvallen. Daarnaast vonden we een temporeel verband tussen NAS-ransomware-campagnes en de bekendmaking van nieuwe kwetsbaarheden. We sluiten het artikel af met een aantal aanbevelingen om het risico op slachtofferschap van NAS-ransomware te verkleinen, waarbij bewustwording centraal staat.*

## 1 Introductie

De afgelopen jaren is de hoeveelheid ransomware-aanvallen toegenomen (Mansfield-Devine, 2022). Veel bedrijven rapporteren enorme schade (Yuryna et al., 2021; Meurs et al., 2022a). Er zijn daarnaast ook ransomware-aanvallen gemeld die veel schade onder particulieren veroorzaken. Deze aanvallen zijn meestal gericht op een specifiek apparaat: de *Networked Attached Storage* (NAS).
De NAS is een apparaat waar meerdere externe harde schrijven op te plaatsen zijn die vervolgens via het open internet toegankelijk zijn. Zo kan je thuis of onderweg gemakkelijk bij je bestanden. Het is een interessant alternatief voor *cloud providers*. Naast het opslaan en de makkelijke toegang wordt NAS ook gebruikt om back-ups te maken. De bekendste merken voor NAS-apparaten zijn QNAP, Netgear, Western Digital, Synology en Asustor (zie figuur 1).

***Figuur 1*** ***Verschillende merken NAS-apparaten: Netgear, Synology, Asustor en Western Digital***


Bron: hardware.info.

Omdat NAS-apparaten toegankelijk zijn via het internet, zijn ze ook kwetsbaar voor verschillende typen malware, zoals ransomware. De afgelopen drie jaar is de hoeveelheid meldingen bij de politie van NAS-ransomware toegenomen van 6 in 2019 tot 33 in de eerste elf maanden van 2022. Hoewel deze cijfers mogelijk een vertekend beeld geven vanwege mogelijk lage aangiftebereidheid, detecteren andere partijen ook een toename in het aantal aanvallen met NAS-ransomware (Hilt & Merces, 2021; Gatlan, 2021a; Sowells, 2022; Witterman, 2021). Aanvallers van NAS-apparaten lijken op basis van rapporten van securitybedrijven vaak een relatief kleine hoeveelheid losgeld van rond de € 500 te vragen. Omdat slachtoffers van deze aanvallen doorgaans geen materiële schade hebben, krijgen dergelijke aanvallen tot op heden geen prioriteit voor opsporingsonderzoek. Met dit artikel willen we meer aandacht vragen voor NAS-ransomware. Hiervoor zijn twee redenen. Allereerst is het vanuit wetenschappelijk oogpunt interessant om verschillende typen aanvallen te vergelijken, want daarmee leren wij iets over hoe aanvallers werken (Junger, Wang & Schlomer, 2020). Daarnaast kunnen deze inzichten worden vertaald in gerichte preventiestrategieën. NAS-ransomware is een *Internet of Things* (IoT)-aanval. IoT is de brede term voor relatief kleine apparaten die verbonden zijn met het internet. Een aantal studies heeft IoT-aanvallen onderzocht. Deze studies richten zich vooral op persistente malware op IoT-apparaten, zoals botnets en cryptojackers (Alrawi et al., 2022; Rodríguez et al., 2022). Persistente malware is malware die als doel heeft om lange tijd ongezien op een computer of IoT-apparaat te blijven. De malware draait op de achtergrond mee en de gebruiker weet daar niets van. Hiermee wordt vaak een botnet tot stand gebracht: een verzameling computers met persistente malware die bediend kan worden door de aanvaller. Een cryptojacker is bijvoorbeeld malware die op de achtergrond het IoT-apparaat gebruikt om cryptovaluta te *minen*.

Alrawi et al. (2022) onderzochten de IoT-malware levenscyclus, zoals die op NAS-apparaten kan worden geïnstalleerd. Zij vonden dat veel IoT-apparaten geen grafische gebruiksomgeving hebben, waardoor het moeilijk is voor gebruikers om een wachtwoord in te stellen. Bovendien bleken veel netwerkapparaten kwetsbaar voor *command injection*, waarbij willekeurige codes op het apparaat uitgevoerd kun-


Tijdschrift voor Veiligheid 2022 (21) 3-4
doi: 10.5553/TvV/.000044

nen worden. Daarnaast stonden er vaak standaardwachtwoorden op, waar criminelen met een *brute-force*-aanval misbruik van kunnen maken. Een *brute-force*-aanval is het gebruik van rekenkracht om zo veel mogelijk wachtwoorden uit te proberen om zo toegang tot een account te krijgen. Omdat NAS verbonden is met het open internet, levert dit veel risico's op.
Voorgaande inzichten over aanvallen met NAS-ransomware zijn gebaseerd op onderzoek van cybersecuritybedrijven. Er is – voor zover bij ons bekend – geen systematisch wetenschappelijk empirisch onderzoek gedaan naar NAS-ransomware. Daarom zal dit onderzoek zich richten op de volgende onderzoeksvraag:

*1. Hoe verschilt NAS-ransomware van reguliere ransomware-aanvallen?*

Om deze vraag te beantwoorden, richten we ons tot de Routine Activiteiten Theorie (Felson & Cohen, 1980). Deze theorie geeft aan dat criminaliteit ontstaat doordat drie elementen in tijd en plaats samenkomen: een gemotiveerde aanvaller, een aantrekkelijk doelwit en de afwezigheid van toezicht. De Routine Activiteiten Theorie (RAT) is ontwikkeld voor offline misdaad. De toepasbaarheid van RAT op cybercriminaliteit is mogelijk anders in een virtuele omgeving (Leukfeldt, 2016; Yar, 2005). Desalniettemin lijken de core-concepten van RAT toepasbaar in de virtuele wereld.

Op basis van het element 'gemotiveerde dader' komen we op de volgende deelvraag:

> *1.1 Wat is het verschil in modus operandi van de aanvaller tussen NAS-ransomware en reguliere ransomware?*

Op basis van het element 'aantrekkelijk doelwit' komen we tot de volgende deelvraag:

> *1.2 Wat is het verschil in slachtofferkenmerken tussen NAS-ransomware en reguliere ransomware?*

Op basis van het element 'tijd' komen we tot de volgende deelvraag:

> *1.3 Hoe verschilt de ontwikkeling over de tijd tussen NAS-ransomware en reguliere ransomware?*

De elementen 'plaats' en 'toezicht' uit de RAT zijn in dit onderzoek buiten beschouwing gelaten. Bij de afronding van dit artikel staan we – zoals de RAT aanmoedigt – met de combinatie van de opgedane inzichten stil bij mogelijkheden om aanvallen met NAS-ransomware te voorkomen. Deze deelvragen worden onderzocht om het fenomeen NAS-ransomware te verkennen en om meer zicht te krijgen op hoe dader- en slachtofferkenmerken samenkomen bij NAS-ransomware ten opzichte van reguliere ransomware. Om deze onderzoeksvragen te beantwoorden analyseren we aangiften van ransomware die zijn gerapporteerd aan de Nederlandse Politie. Door de NAS-aanvallen te vergelijken met reguliere ransomware-aanvallen,

wordt beter duidelijk waarom de aanvallers NAS-apparaten aanvallen en specifieke methoden daarvoor gebruiken. Daarnaast geeft het inzicht welke interventies eventueel succesvol zijn om de impact van NAS-ransomware te verkleinen.
Deze studie is als volgt opgebouwd: in paragraaf 2 richten we ons op eerder onderzoek. In paragraaf 3 richten we ons op de data en methoden, in paragraaf 4 doen we verslag van de resultaten. In paragraaf 5 trekken we een conclusie over in hoeverre de resultaten onze hypothesen ondersteunen. In paragraaf 6 doen we aanbevelingen voor de verschillende partijen die betrokken zijn bij NAS-ransomware: de gebruikers, de verkopers van NAS-apparaten en (lokale) overheidsinstanties. We sluiten het artikel af met een discussie over de sterke en zwakke punten van dit onderzoek en suggesties voor vervolgonderzoek.

## 2 Eerder onderzoek

### *2.1 De modus operandus: crime-script van reguliere en NAS-ransomware*

Om te onderzoeken hoe reguliere en NAS-ransomware van elkaar verschillen, is het belangrijk om eerst de aanvallen zelf te bestuderen, dit wil zeggen: de modus operandus. Dit kan worden gedaan door gebruik te maken van een crime-script (Cornish, 1994; Hutchings & Holt, 2015). Een crime-script is manier om een aanval te analyseren door deze in verschillende opeenvolgende stadia te verdelen, waarin elk stadium een stap is die voltooid moet worden om de aanval uit te voeren (Cornish, 1994).
Voor ransomware-aanvallen zijn verschillende crime-scripts gemaakt (Keshavarzi & Ghaffary, 2020; Meurs et al., 2022b). Keshavarzi en Ghaffary (2020) verdelen de aanval in zes stappen:

1 *infection*: het infecteren van het slachtoffer;
2 *installation*: het installeren van de malware;
3 *communication*: de ransomware communiceert met de aanvaller dat de aanval in gang is;
4 *execution*: de aanvaller versleutelt de bestanden van het slachtoffer;
5 *extortion*: de aanvaller vraagt geld om de bestanden te ontsleutelen;
6 *emancipation*: na betaling ontsleutelt de aanvaller de bestanden, of doet niks en laat het slachtoffer met versleutelde bestanden achter.

Een nadeel van dit type crime-script is dat de nadruk ligt op het versleutelen op een computer, maar niet op het ICT-netwerk (al dan niet gesegmenteerd). Dan wordt *lateral movement* belangrijker (Akamai, 2021). *Lateral movement* is het stap voor stap toegang krijgen tot de computers in het (hele) netwerk om de volledige controle over het netwerk te verkrijgen.
Een tweede uitbreiding op dit model is data-exfiltratie. Aanvallers downloaden soms data van slachtoffers naar hun eigen servers (Meurs et al., 2022b). Deze data bevat vaak gevoelige documenten, zoals paspoorten, salarisstrookjes en andere bedrijfsgevoelige informatie. Als het slachtoffer niet betaalt, dan dreigen aanvallers vaak om de data online te zetten op een zogenaamde leaksite. Sinds 2019 wordt deze tactiek vaak ingezet bij ransomware-aanvallen (Mansfield-Devine, 2022).


doi: 10.5553/TvV/.000044

In vergelijking met reguliere ransomware, lijkt een aanval van NAS-ransomware uit de volgende stappen te bestaan (Arghire, 2022a; Gatlan, 2021a; Censys, 2022):

1 De verkenningsfase. Hierbij wordt het slachtoffer gevonden. Een veelgebruikte manier is via Shodan of Censys. Deze zoekmachines laten NAS-apparaten zien die verbonden zijn met het internet (zie figuur 2). Met Shodan kan gezocht worden op IP-adres of op specifieke apparaten, zoals NAS. Het is vaak de eerste stap om de NAS-ransomware-aanval te plegen.
2 Toegang krijgen tot het apparaat en het uploaden van de malware. Daarmee kan vervolgens automatisch de NAS-schrijf versleuteld worden.
3 Wachten tot het slachtoffer betaalt.
4 Het geld witwassen.

Het grootste verschil met reguliere ransomware is dat NAS-ransomware grotendeels geautomatiseerd plaatsvindt, terwijl bij een reguliere ransomware-aanval de aanvaller veel tijd moet steken in *lateral movement*: toegang krijgen tot het hele netwerk, om daarbij alle computers, inclusief de back-ups indien mogelijk, te kunnen versleutelen. Daarnaast lijkt bij NAS-ransomware geen data-exfiltratie plaats te vinden (Gatlan, 2021a).

Drie bekende NAS-ransomware-varianten zijn Ech0raix, Qlocker en Deadbolt. Met ransomware-variant bedoelen we in deze studie de ransomware-strain. Dat is de extensie van een bestand na versleuteling met ransomware. Ech0raix is actief sinds juni 2019 en is een vorm van Ransomware-as-a-Service (RAAS). Dat houdt in dat de ransomware gekocht kan worden voor een percentage van het losgeld. Oude Ech0raix-aanvallen bestonden met name uit *brute-force*-aanvallen (Gatlan, 2021a), waarbij met trial-and-error wachtwoorden worden achterhaald. De eerste versies van de ransomware van Ech0raix checkten of de NAS in een CIS-land staat, een voormalig Sovjet-land (Sowells, 2022). In dat geval versleutelt het programma niet (Andrioaie, 2021).

***Figuur 2 Schermafbeelding van zoekmachine Shodan***


Bron: www.shodan.io.

Er zijn golven van aanvallen van NAS-ransomware. In februari 2021 werd bij aanvallen vaak gebruikgemaakt van kwetsbaarheden van NAS-apparatuur van het merk QNAP (CVE-2020-2501) (Gatlan, 2021a). Dit hield in dat door buffer-overflow geen inloggegevens nodig zijn om toegang te krijgen tot het apparaat. Een buffer-overflow is het misbruiken van het geheugen van een computer om toegang te

krijgen tot data die daarin opgeslagen staat. De campagne in mei 2021 maakte gebruik van een drietal kwetsbaarheden om toegang te krijgen tot een NAS-apparaat (Witteman, 2021).
Qlocker is actief sinds april 2021 en richt zich op QNAP. Volgens Schouw (2022) hebben ze ongeveer € 350.000 verdiend. De aanvallers vroegen ongeveer 0,02-0,03 bitcoin, dit is ongeveer € 600 tot € 1000 (Schouw, 2022). In december 2021 kwam er een reeks aanvallen met Qlocker-ransomware. Daarbij kwamen de aanvallers in het NAS-apparaat door gebruik te maken van CVE-2021-28799, waarbij ze bij de credentials van het NAS-apparaat konden komen.
Deadbolt is actief sinds december 2021 en is tot op heden het meest geavanceerd. Het richt zich voornamelijk op QNAP NAS-systemen (Kaspersky Lab, 2022). Deze groep claimt over een *zero-day* kwetsbaarheid te beschikken, een kwetsbaarheid die nog nergens bekend is. Een individuele decryptiesleutel voor het ontsleutelen van een NAS-apparaat koste toen 0,03 bitcoin, ongeveer € 1000 (Arghire, 2022a). Deadbolt had in het eerste halfjaar van 2022 ongeveer $187.000 verdiend (Censys, 2022). Ondanks de waarschuwingen van fabrikant QNAP, zijn er volgens de Nederlandse politie ongeveer 15.000 slachtoffers van Deadbolt wereldwijd, waarvan 1100 in Nederland (RTL, 2022).

### *2.2 De aanvaller en zijn slachtoffer*

Om het gedrag van aanvallers en slachtoffers te verklaren, zijn criminologische theorieën van belang (Wortley & Mazerolle, 2008), ook voor onlinecriminaliteit (Holt, Bossler & Seigfried-Spellar, 2015; Holt, Van Wilsem & Leukfeldt, 2018). De belangrijkste theorieën voor dit onderzoek zijn de Routine Activiteiten Theorie (RAT) en het Rationele Keuze Model (RKM). RKM legt de nadruk op het rationele besluitvormingsproces van aanvallers. Aanvallers zijn, aldus Cornish en Clarke (2008), rationele actoren die middelen, doelen, kosten en baten afwegen en rationele keuzes maken die de baten optimaliseren. Ook het plegen van een misdaad is doelgericht gedrag dat is ontworpen om te voorzien in de alledaagse behoeften van aanvallers aan zaken als geld, status, seks en opwinding. Het voldoen aan deze behoeften omvat het maken van soms vrij elementaire beslissingen en keuzes. Deze keuzes zijn geen langetermijnbeslissingen, maar ze worden sterk beperkt door allerlei factoren, zoals de capaciteiten van de overtreders en de beschikbaarheid van relevante informatie (Cornish & Clarke, 2008). Deze rationale afwegingen komen onder andere tot uiting in de modus operandi. Wanneer aanvallers een bepaald doel overwegen, zullen zij hun inspanningen aanpassen aan de mate waarin dit aantrekkelijk of winstgevend is.
De Routine Activiteiten Theorie (RAT) is ontwikkeld door Cohen en Felson (1979) en geeft inzicht in de oorzaken van criminaliteit: om een misdaad te plegen, moet een gemotiveerde aanvaller in de tijd en ruimte samenkomen met een aantrekkelijk doelwit. Bij gebrek aan effectieve controles zal de gemotiveerde overtreder azen op een geschikt doelwit (Cohen & Felson, 1979). Potentiële slachtoffers kunnen een persoon of object zijn dat door aanvallers als kwetsbaar of bijzonder aantrekkelijk wordt beschouwd. RAT benadrukt het belang van blootstelling aan en kwetsbaarheid van doelen en slachtoffers voor potentiële aanvallers en verminderd toezicht om misdaad te verklaren (Akdemir & Lawless, 2020; Holt et al., 2018;

Miró-Llinares, Drew & Townsley, 2020; Reyns, 2017). Vanuit dit perspectief ligt het voor de hand dat potentiële slachtoffers die online sterk aanwezig zijn (bijv. financiële instellingen), over veel geld beschikken en wellicht geen goede beveiliging hebben (bijv. ziekenhuizen) aantrekkelijk zijn voor gemotiveerde daders en daarom een grotere kans hebben op slachtofferschap van bijvoorbeeld ransomware (Junger et al., 2017; Leukfeldt & Yar, 2016; Reyns, 2017). Zoals hierboven al is beschreven, moeten we oppassen met het toepassen van RAT op cybercriminaliteit (Leukfeldt, 2016; Yar, 2005). Volgens Yar (2005) blijven de basiselementen van RAT hetzelfde bij cybercriminaliteit, maar mogelijk hangen deze elementen op een andere manier samen, omdat de omgeving van de misdaad virtueel is en zijn vooral de elementen 'afwezigheid van toezicht', 'plaats' en 'ruimte' fundamenteel anders dan in de offline wereld. Aangezien dit een verkennend onderzoek is en de basiselementen 'potentiële slachtoffers', 'gemotiveerde daders' en 'tijd' van RAT goed toepasbaar zijn op cybercriminaliteit, gebruiken wij deze elementen van RAT in deze studie.

### *2.3 Hypothesen reguliere versus NAS-ransomware*

Gelet op de verschillen in crime-scripts tussen reguliere en NAS-ransomware verwachten we ook verschillen tussen de modus operandi van daders, slachtofferkenmerken en ontwikkelingen over de tijd. De aanval met NAS-ransomware lijkt meer automatisch plaats te vinden, relatief meer particulieren te treffen en duidelijker samen te hangen met de bekendmaking van specifieke kwetsbaarheden van NAS-apparaten. Zoals in de vorige paragraaf beschreven, worden de ransomwarevarianten Ech0raix, QLocker en Deadbolt vaak geassocieerd met NAS-ransomware (Arghire, 2022a; Censys, 2022; Gatlan, 2021a; Witteman, 2021). Terwijl bij reguliere ransomware andere ransomware-varianten genoemd worden, zoals Conti, Lockbit en Revil (Meurs et al., 2022b). Er lijkt dus een verschil in welke ransomware-varianten geassocieerd worden met reguliere en NAS-ransomware.

*Hypothese 1: Er zijn andere ransomware-varianten betrokken bij NAS- dan bij reguliere ransomware-aanvallen*.

Opmerkelijk is dat bij ransomware-aanvallen voor NAS-apparaten minder losgeld gevraagd lijkt te worden dan bij reguliere ransomware-aanvallen. Sowells (2022) meldt dat Ech0raix 0,05 tot 0,06 bitcoins (ongeveer € 500 tot € 600) vraagt voor ontsleuteling. Meurs (2022b) vond dat bij ransomware-aanvallen op bedrijven in Nederland gemiddeld € 720,256 (sd = € 2.632.673) werd gevraagd aan losgeld. Daar zijn verschillende verklaringen voor te bedenken. Allereerst hebben particulieren minder geld te besteden dan bedrijven. Het lijkt mogelijk dat aanvallers enigszins rekening houden met de draagkracht van hun slachtoffers. Daarnaast bestaat het crime-script van een NAS-ransomware-aanval uit minder stappen dan bij een reguliere ransomware-aanval. Vanuit het RKM zouden daders ook minder geld vragen omdat ze er waarschijnlijk minder moeite hoeven te doen voor een succesvolle aanval. Samenvattend leidt dit tot hypothese 2:

*Hypothese 2: Bij een aanval met NAS-ransomware wordt minder losgeld gevraagd dan bij een aanval met reguliere ransomware*.
Rodríguez et al. (2021) onderzochten gebruikers van IoT-apparaten. Ze gebruikten een aselecte steekproef op basis van gebruikers van IoT-apparaten die bekend waren bij een internetprovider. Van de 128 participanten werd 91,2% van de apparaten, waaronder NAS, gebruikt door particulieren. Mogelijk worden NAS-apparaten die aan het open internet verbonden zijn vaker gebruikt door particulieren. Daaruit komen we tot hypothese 3:

*Hypothese 3: Particulieren worden relatief vaker slachtoffer van NAS-ransomware dan van reguliere ransomware-aanvallen*.
In de vorige paragraaf werd beschreven dat de drie grootste NAS-ransomware-varianten Ech0raix, Qlocker en Deadbolt respectievelijk in juni 2019, april 2021 en december 2021 actief werden en dat dit vaak gepaard ging met de publicatie van kwetsbaarheden (Arghire, 2022a; Censys, 2022; Hilt & Merces, 2022; Witteman, 2021). Daar leiden we hypothese 4 uit af:

*Hypothese 4: Er is een verband tussen de timing en aantallen aanvallen met NAS-ransomware en publicatie van nieuwe kwetsbaarheden van NAS-apparatuur*.
Empirische studies naar reguliere ransomware (Connolly, 2020; Meurs et al., 2022b) laten zien dat deze aanvallen niet per se beginnen door het uitbuiten van kwetsbaarheden. Daarentegen lijkt NAS-ransomware vooral samen te hangen met ontdekte en gepubliceerde kwetsbaarheden. Dit suggereert verschillende startpunten voor beide typen aanvallen. Daarom verwachten we dat NAS-ransomware over de tijd niet samenhangt met reguliere ransomware (hypothese 5).

*Hypothese 5: Er is geen temporeel verband tussen de hoeveelheid aangiften van NAS-ransomware en van reguliere ransomware*.

## 3 Data en methoden

### *3.1 De steekproef*

De data voor dit onderzoek is verkregen door in de Nederlandse politiesystemen op het sleutelwoord 'ransomware' te zoeken. Vervolgens zijn handmatig alle zoekresultaten gefilterd op ransomware-aanvallen. De politiegegevens bevatten informatie over ransomware-aanvallen op zowel organisaties (81,4%) als individuen (18,6%) en leveren hiermee een unieke kans om beide typen aanvallen te vergelijken. Twee aspecten zijn belangrijk bij het gebruik van politiedata: aangiftebereidheid en het gebruik van politiegegevens voor wetenschappelijke doeleinden. De aangiftebereidheid van cybercriminaliteit is relatief laag. Studies naar aangiftebereidheid van andere cyberdelicten melden dat slachtoffers in 8 tot 10% van de gevallen aangifte doen (Van de Weijer et al., 2020). Dit is belangrijk om rekening mee te houden bij de interpretatie van de resultaten. Deze resultaten kunnen immers een vertekend beeld geven.
Daarnaast worden in dit onderzoek politiegegevens gebruikt voor wetenschappelijke doeleinden. De wettelijke basis voor het gebruik van politiegegevens voor we-

tenschappelijk onderzoek is artikel 22 van de Wet politiegegevens (Wpg). Daarin staat dat het College van procureurs-generaal toestemming geeft voor het gebruik van politiegegevens voor wetenschappelijk onderzoek mits de data volledig geanonimiseerd gepubliceerd wordt. Hier wordt in dit artikel aan voldaan.
Bij de Nederlandse Politie zijn tussen 1 januari 2019 en 1 juli 2022 453 meldingen en/of aangiften van ransomware-aanvallen gedaan. Hierbij waren er negentien meldingen van niet-succesvolle aanvallen. Deze vallen buiten de scope van deze studie. Er bleven 434 aangiften van succesvolle ransomware-aanvallen over. Daarvan waren er 78 (18%) gericht op NAS-apparaten en 356 reguliere ransomware-aanvallen.

### *3.2 Variabelen*

Bij elke aangifte is een aantal variabelen met de hand gecodeerd. Deze variabelen zijn aan de hand van de deelvragen te groeperen in slachtofferkenmerken, modus operandi van de aanval en informatie over de aangifte, zoals tijdstip van versleuteling en aangifte.

- *1. Slachtofferkenmerken*
  - a. De sector van het slachtoffer: De verschillende sectoren zoals omschreven door de Kamer van Koophandel zijn gebruikt: Bouw, Gezondheidszorg, Handel, ICT, MAS (Milieu en Agrarische Sector), Media, Recreatie en Transport. Daarnaast is er een 'Particulier' als slachtoffer.
  - b. Ondernemingsvorm: Multinational (bedrijf heeft vestigingen in meerdere landen), BV (bedrijven als BV bij de KvK), MKB (bedrijven met minder dan vijf werknemers en meer dan één, rechtsvorm is geen BV), Stichting (bedrijven die ingeschreven zijn als stichting), ZZP (een bedrijf bestaande uit één werknemer, rechtsvorm is geen BV) of particulier. Er zijn in deze dataset geen incidenten met een NV bekend. De bedrijven waarvan de ondernemingsvorm niet in de aangifte stond, werden opgezocht op Zoominfo. Daar staan openbare gegevens van bedrijven.
  - c. Back-up: Heeft het slachtoffer een back-up van de versleutelde betstanden? Deze variabele kent vier categorieën: geen back-up, wel back-up maar kon bestanden niet herstellen, wel back-up maar kon bestanden gedeeltelijk herstellen, en wel back-up en kon bestanden volledig herstellen.
  - d. Betaald: Heeft slachtoffer betaald, en zo ja hoeveel?
  - e. Financiële schade: Welke financiële schade heeft het slachtoffer geleden door de ransomware-aanval? Sommige slachtoffers melden bij de politie de hoeveelheid geleden schade op het moment van aangifte. Bij bedrijven wordt daarbij vaak een bedrag genoemd, bij particulieren vaak immateriële schade. Dit is gecodeerd als: een categorie voor immateriële schade en een voor de hoeveelheid schade in euro, mits gespecificeerd door het slachtoffer.

- *2. Modus operandi*
  - f. Ransomware-variant: Staat er een naam op de *ransom note* of een extensie van de bestanden?

– g. Losgeld: Hoeveel losgeld heeft de aanvaller aan het slachtoffer gevraagd om de bestanden te ontsleutelen?
– h. Persoonlijke *ransom note*: Hoe vaak staat het bitcoinadres op de *ransom note*? Als er geen bitcoinadres op staat, dan moet het slachtoffer contact opnemen met de aanvaller via e-mail of TOR-chat. Bij reguliere ransomware wordt dan afhankelijk van slachtofferkenmerken een losgeldbedrag gevraagd (Meurs, 2022b). Soms zijn slachtoffers bereid te betalen als het losgeldbedrag wordt verlaagd. Aangezien de bedragen van slachtoffers bij NAS-ransomware waarschijnlijk laag zijn, zal dit voor de daders achter NAS-ransomware waarschijnlijk minder opleveren dan bij reguliere ransomware.
– i. Datum aanval: Genoteerd in datum en tijd.

• *3. Metadata*
– j. Aangifte: De status van de melding, is het alleen een melding of ook een aangifte? Heeft de aangifte geleid tot een opsporingsonderzoek?
– k. Wanneer heeft de melding/aangifte plaatsgevonden? Genoteerd in datum en tijd.

### *3.3 Analyse*

Er worden verschillende toetsen gebruikt om het verschil in kenmerken van reguliere en NAS-ransomware met elkaar te vergelijken. Voor de categorische variabelen wordt er getoetst met de chi-kwadraattoets ($\chi 2$). Dit is een gangbare methode om categorische variabelen te toetsen op onafhankelijkheid, zoals aangegeven door Placket (1983).

Numerieke variabelen worden getoetst met de t-toets. Bij de t-toets wordt getoetst of de gemiddelden uit twee steekproeven van elkaar verschillen. Een belangrijke aanname voor de t-toets is dat de steekproeven ongeveer normaal zijn verdeeld. Omdat de variabelen '1e. Financiële schade' en '2g. Losgeld' in euro's gemeten zijn, wordt er een $\log_{10}$-transformatie toegepast. Er wordt getoetst of dit inderdaad de variabelen bij benadering normaal verdeeld maakt met behulp van de Shapiro-Wilk-toets voor normaliteit. Indien deze niet voldoet, dan voeren we de non-parametrische Mann-Whitney U-toets uit om te toetsen of de twee steekproeven van elkaar verschillen. De Mann-Whitney U-toets is een gangbare manier om een non-parametrische t-toets uit te voeren (Zimmerman, 1987).

Ten slotte wordt er getoetst of de gebeurtenissen zoals eerder beschreven, samenhangen in de tijd met NAS-ransomware-aanvallen. Ook wordt er getoetst of er een temporeel verband is tussen de tijd van versleuteling van NAS-ransomware en normale ransomware. Daarvoor wordt de Pearson product-momentcorrelatie gebruikt, een uitbreiding van de standaard Pearson correlatie naar intervaldata, zoals beschreven door Puth, Neuhäuser en Ruxton (2014).


Tijdschrift voor Veiligheid 2022 (21) 3-4
doi: 10.5553/TvV/.000044

## 4 Resultaten

*4.1 Algemene resultaten*

Tabel 1 geeft de verschillende beschrijvende resultaten van deze studie. Sector, ondernemingsvorm, back-up, betaald en financiële schade verschillen tussen NAS-ransomware en reguliere ransomware. Daarnaast verschillen de ransomware-variant, losgeld en persoonlijke ransom note ook van elkaar.

In figuur 3 staan de frequenties van ransomware-aanvallen voor reguliere en NAS-ransomware. In eerste instantie lijkt er geen verband te zijn tussen het tijdstip van versleutelen bij reguliere ransomware en NAS-ransomware. NAS-ransomware lijkt wel samen te hangen met de vier gebeurtenissen uit paragraaf 2, die we hier L1 tot en met L4 noemen:

– L1 is de eerste golf in juni 2019: toen werd de ransomware-variant Ech0raix voor het eerst actief.
– L2 is de tweede golf in februari 2021: QNAP-kwetsbaarheid CVE-2020-2501 werd gepubliceerd. Dit hield in dat door buffer-overflow geen inloggegevens nodig zijn om toegang te krijgen tot het apparaat.
– L3 is de derde golf in april 2021: toen werd de ransomware-variant QLocker voor het eerst actief.
– L4 is de vierde golf in december 2021: toen werd de ransomware-variant Deadbolt voor het eerst actief.

Tijdens het coderen viel op dat veel slachtoffers van NAS-ransomware aangaven dat ze na de aanval op internet hadden gezocht en vonden dat er net een kwetsbaarheid was gepubliceerd voor hun specifieke NAS-type. Het overzicht in tabel 1 lijkt de samenhang met gebeurtenissen L1-L4 te ondersteunen.

Ten slotte verschillen de hoeveelheid meldingen en aangiften niet tussen NAS-ransomware en reguliere ransomware ($\chi 2(3) = 6{,}06$).

*Tabel 1 Overzicht resultaten van deze studie*

| Variabelen | Test, p-waarde | Categorie/ eenheid | NAS-ransomware | Reguliere ransomware |
|---|---|---|---|---|
| **1a. Sector** | $\chi 2(10) = 137{,}28^{***}$ | Bouw | 4 (5%) | 49 (14%) |
| | | Gezondheidszorg | 1 (1%) | 21 (6%) |
| | | Handel | 10 (13%) | 109 (32%) |
| | | ICT | 3 (4%) | 60 (18%) |
| | | MAS | 1 (1%) | 11 (3%) |
| | | Media | 7 (9%) | 13 (4%) |
| | | **Particulier** | **48 (63%)** | **34 (9%)** |
| | | Onderwijs | 0 (0%) | 16 (5%) |
| | | Overheid | 0 (0%) | 11 (3%) |
| | | Recreatie | 1 (1%) | 19 (6%) |
| | | Transport | 1 (1%) | 32 (9%) |

*Tabel 1 (Vervolg)*

| Variabelen | Test, p-waarde | Categorie/ eenheid | NAS-ransom-ware | Reguliere ransomware |
|---|---|---|---|---|
| **1b. Onderne-mingsvorm** | $\chi2(7) = 131,47^{***}$ | BV | 12 (16%) | 158 (42%) |
| | | MKB | 8 (11%) | 75 (20%) |
| | | Particulier | 48 (63%) | 34 (9%) |
| | | Stichting | 2 (2%) | 8 (2%) |
| | | ZZP | 8 (11%) | 22 (6%) |
| | | Multinational | 0 (0%) | 55 (15%) |
| | | Publieke organisatie | 0 (0%) | 23 (7%) |
| **1c. Back-up** | $\chi2(3) = 23,86^{***}$ | Geen back-up | 51 (69%) | 130 (38%) |
| | | Back-up + geen herstel | 7 (9%) | 63 (18%) |
| | | Back-up + gedeeltelijk herstel | 8 (11%) | 63 (18%) |
| | | Back-up + volledig herstel | 8 (11%) | 86 (25%) |
| **1d. Betaald** | $\chi2(1) = 6,5348^{*}$ | Betaald | 6 (9%) | 81 (23%) |
| | | Hoeveelheid betaald (gemid-deld, sd) | € 133 (351) | € 74.332 (€ 248.384) |
| | | Hoeveelheid betaald $\log_{10}$ (gemiddeld, sd) | 0,45 (1,1) | 2,13 (2.27) |
| **1e. Schade** | $t(74) = -7,74^{***}$ | Schade niet gekwantificeerd | 26 (70%) | 51 (28%) |
| | | Hoeveelheid schade (gemid-deld, sd) | € 840 (€ 2105) | € 411.213 (€ 2.678.505) |
| | | Hoeveelheid schade $\log_{10}$ (gemiddeld, sd) | 0,94 (1,5) | 3,25 (2,2) |
| **2f. Ransom-ware-variant** | $\chi2(6) = 183,36^{***}$ | Top 5 | 1. Ech0raix (49%) | 1. Onbekend (28%) |
| | | | 2. Onbekend (26%) | 2. Phobos (13%) |
| | | | 3. Deadbolt (9%) | 3. Revil (13%) |
| | | | 4. Qlocker (5%) | 4. Conti (8%) |
| | | | 5. 0XXX (2%) | 5. Lockbit (6%) |
| **2g. Losgeld** | $W = 823,5^{***}$ | Hoeveelheid losgeld (gemid-deld, sd) | € 1654 (€ 5.667) | € 724.713 (€ 2.640.499) |


Tijdschrift voor Veiligheid 2022 (21) 3-4
doi: 10.5553/TvV/.000044

*Tabel 1 (Vervolg)*

| Variabelen | Test, p-waarde | Categorie/ eenheid | NAS-ransomware | Reguliere ransomware |
|---|---|---|---|---|
| | | Hoeveelheid losgeld $log_{10}$ (gemiddeld, sd) | 2,89 (0,34) | 4,38 (1,19) |
| **2h. Persoonlijke *ransom note*** | $\chi 2(1) = 48{,}89^{***}$ | Hoevaak betalingsgegevens op *ransom note* | 0 (0%) | 214 (57%) |

* p < 0,05; ** p < 0,01; *** p < 0,001

Op basis van deze resultaten kunnen we een uitspraak doen over de uitkomst van de hypothesen (zie tabel 1 voor het overzicht).

*Hypothese 1: Er zijn andere ransomware-varianten betrokken bij NAS- dan bij reguliere ransomware*.
Op basis van '**2f. Ransomware-variant'** in tabel 1 kunnen we stellen dat de ransomware-varianten tussen reguliere en NAS-ransomware van elkaar verschillen. Bijna de helft van de NAS-aanvallen wordt met Ech0raix uitgevoerd, namelijk 49%, bij de reguliere ransomware is er meer spreiding over de varianten, waarbij Phobos en Revil de grootste bijdrage leveren, namelijk 13%.

*Hypothese 2: Bij een aanval met NAS-ransomware wordt een lager losgeldbedrag gevraagd dan bij een aanval met reguliere ransomware*.
Tabel 1, '**2g. Losgeld**', laat zien dat het gevraagde losgeld bij reguliere aanvallen € 724.713 is, terwijl dat bij NAS-ransomware 'slechts' € 1654 is. Bij reguliere aanvallen is het losgeld gemiddeld dus 438 keer hoger.

*Hypothese 3: Er zijn meer particulieren slachtoffer van NAS-ransomware dan bij reguliere ransomware*.
Zoals verwacht laat **'1a. Sector'** (zie tabel 1) zien dat van de NAS-aanvallen 63% bij individuen terechtkomt, terwijl maar 9% van de reguliere aanvallen een particulier treft.

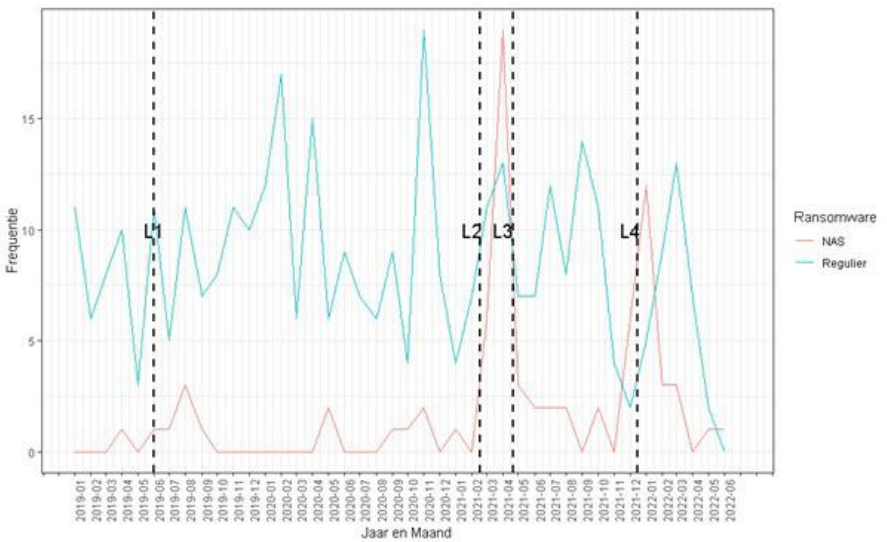
*Hypothese 4: Er is een verband tussen het aantal aanvallen met NAS-ransomware en de publicatie van kwetsbaarheden*.
en
*Hypothese 5: Er is geen temporeel verband tussen de hoeveelheid aangiften van NAS-ransomware en van reguliere ransomware*.
De hypothesen 4 en 5 zijn gebaseerd op dezelfde data en worden daarom gezamenlijk besproken. Om de ontwikkelingen over de tijd te analyseren zijn de Pearson product-momentcorrelaties uitgerekend.

– Tussen gebeurtenissen L1-L4 en NAS-ransomware bleek een correlatie van 0,50 te zitten (t(21) = 2,65, p = 0,01). De 95%-betrouwbaarheidsinterval van die correlatie is 0,11-0,76.
– Tussen gebeurtenissen L1-L4 en reguliere ransomware vonden we geen correlatie: t(41) = -0,04, p = 0,97.

– Tussen reguliere en NAS-ransomware vonden we ook geen correlatie: t(41) = -0,53, p = 0,60.

Kortom, tussen gebeurtenissen L1-L4 en NAS-ransomware is er een temporeel verband, in lijn met hypothese 4. Tussen gebeurtenissen L1-L4 en reguliere ransomware en tussen reguliere en NAS-ransomware niet, in overeenstemming met hypothese 5.

***Figuur 3*** ***Frequentie van ransomware-aanvallen gerapporteerd aan de Nederlandse Politie tussen 1 januari 2019 en 1 juli 2022***




In figuur 3 staat de frequentie van ransomware-aanvallen gerapporteerd aan de Nederlandse Politie tussen 1 januari 2019 en 1 juli 2022. Hierbij gaat het om de datum van versleuteling van bestanden, niet om het moment dat het slachtoffer aangifte doet. De lijnen L1-L4 staan voor specifieke evenementen die invloed lijken te hebben op de hoeveelheid versleutelde NAS-apparaten (zie par. 2).

## 5 Conclusie

Het doel van dit artikel was om de verschillen tussen reguliere en NAS-ransomware te identificeren. Daarbij richten we ons op drie deelvragen: Wat is het verschil in modus operandi, slachtofferkenmerken en trends tussen reguliere en NAS-ransomware?
Onze eerste hypothese is dat de ransomware-varianten verschillen tussen ransomware-aanvallen die zich richten op NAS-apparaten en aanvallen die op een computer of bedrijfsnetwerk zijn gericht. De resultaten ondersteunen dit.
De tweede hypothese is dat NAS-ransomware een ander verdienmodel heeft dan reguliere ransomware. Zoals verwacht, wordt er een flink lager losgeldbedrag ge-


doi: 10.5553/TvV/.000044

vraagd bij NAS-ransomware dan bij reguliere ransomware. Daarnaast lijken slachtoffers van NAS-ransomware minder vaak te betalen.
Daarnaast worden betaalgegevens vaker op de *ransom note* gezet bij NAS-ransomware dan bij reguliere ransomware. Dit betekent dat de *ransom note* niet gepersonaliseerd is, maar voor alle slachtoffers identiek is. Het is dus een meer geautomatiseerde aanval die makkelijk schaalbaar is, maar niet erg gefocust is. Dit lijkt erop te wijzen dat groeperingen achter de NAS-ransomware niet geïnteresseerd zijn om de winst per slachtoffer te maximaliseren, maar eerder op zo veel mogelijk aanvallen te plegen met een iets kleinere winst. Ook eerder onderzoek vond dat makkelijk opschaalbare aanvallen minder tijd en energie kosten, maar ze leveren ook minder op, in lijn maar het Rationale Keuze Model (Junger, Wang & Schlomer, 2020).
De derde hypothese stelt dat particulieren vaker slachtoffer zijn van NAS-ransomware dan van reguliere ransomware. De resultaten in deze studie ondersteunen deze hypothese.
De vierde hypothese wijst op een toename van aangiften van NAS-ransomware rondom de publicatie van kwetsbaarheden. De resultaten in deze studie ondersteunen deze hypothese. Er waren vier momenten in de onderzoeksperiode waarop kwetsbaarheden bekend werden waar verschillende ransomware-varianten misbruik van maakten. Deze gebeurtenissen hingen samen in de tijd met de versleuteling van apparaten met NAS-ransomware.
Samengevat, NAS-ransomware wijkt af van reguliere ransomware (zie tabel 2): er zijn andere ransomware-varianten actief voor de twee typen ransomware, het verdienmodel verschilt, particulieren zijn vaker slachtoffer en aanvallen met NAS-ransomware hangen samen met de publicatie van kwetsbaarheden van NAS-apparaten.

*Tabel 2 Samenvatting verschil NAS-ransomware en reguliere ransomware*

| **NAS-ransomware** | **Reguliere ransomware** |
|---|---|
| Meeste slachtoffers zijn individuele burgers (63%). | Meeste slachtoffers zijn bedrijven (91%). |
| Gemiddeld € 1654 losgeld (sd = € 5667). | Gemiddeld € 724.713 losgeld (sd = € 2.640.499). |
| Slachtoffers hebben vaak los van de losgeldsom geen financiële schade, maar wel een hoop immateriële schade, zoals video's en foto's (70%). | Gemiddeld € 411.213 financiële schade (sd = € 2.678.505). |
| Losgeld en bitcoinadres op *ransom note* (100%). | Losgeld en bitcoinadres in 57% van de incidenten pas bekendgemaakt na contact met aanvallers. |
| Minder stappen om een aanval uit te voeren: verkenning en versleuteling. | Meer stappen om een aanval uit te voeren: verkenning, persistentie, horizontale beweging, data-exfiltratie, versleuteling, onderhandelingen. |
| 4 cycli/campagnes in de afgelopen drie jaar, samenhangend met gevonden kwetsbaarheden van NAS-apparatuur. | Een kleine trend over de jaren, maar geen relatie met onderzochte NAS-kwetsbaarheden. |

## 6 Aanbevelingen

In deze paragraaf doen we aanbevelingen voor drie groepen die met NAS-ransomware te maken hebben: de gebruikers, de verkopers van NAS-apparaten en (lokale) overheidsinstanties.

### *6.1 Gebruikers van NAS-apparaten*

Veelgehoorde adviezen voor cyberveiligheid zijn: een sterk wachtwoord, antivirussoftware en je software up-to-date houden (Gatlan, 2021b). Aan de hand van dit onderzoek kunnen we de volgende conclusies trekken:

- Een sterk wachtwoord is vaak niet voldoende om NAS-ransomware te voorkomen. Hoewel dit wel goed werkt tegen *brute-force*-aanvallen, zien we dat er een trend is van aanvallers om meer op kwetsbaarheden te richten. Deze omzeilen het wachtwoord. Een sterk wachtwoord is dus nog wel aan te raden, maar op zichzelf onvoldoende.
- Het updaten van de software van de NAS is cruciaal om slachtofferschap van ransomware te voorkomen. Vaak blijken gebruikers dat wel te weten, maar het alsnog niet of nauwelijks te doen (Rodríguez et al., 2021). Aangezien NAS-apparaten vaak een functionaliteit hebben om automatisch te updaten, doet de gebruiker er verstandig aan deze aan te zetten.
- Het zou goed zijn om het NAS-apparaat af te schermen van het open internet, zodat het niet vindbaar is via zoekmachines als Shodan en Censys. Een manier om een laag tussen het open internet en het NAS-apparaat te maken is door het NAS-apparaat als VPN-server in te stellen of door het instellen van een eigen *reverse proxyserver*. Een *reverse proxyserver* is een server die je kan instellen die tussen het NAS-apparaat en het open internet staat.

### *6.2 De verkopers van NAS-apparaten*

Partijen die NAS-apparaten verkopen, zouden klanten moeten wijzen op de risico's op malware door het gebruik van NAS. Belangrijk is om te vermelden welke typen malware op een NAS kunnen komen en hoe de kans op malware en ransomware te verkleinen. Tijdens het schrijven van dit artikel lijken de grote verkooppartijen nog geen informatie over mogelijke risico's en kwetsbaarheden van NAS-apparatuur op hun website of in hun winkel te hebben. Eventueel kan de rijksoverheid met de grote verkooppartijen in gesprek om afspraken te maken over het informeren van (potentiële) kopers van NAS-apparaten. Ten slotte kunnen fabrikanten gebruikers helpen door het instellen van automatische updates, waarschuwingen en VPN-oplossingen.

### *6.3 Lokale overheidsinstanties*

Lokale overheidsinstanties kunnen preventiecampagnes starten die zich specifiek richten op het voorkomen van cybercriminaliteit bij particulieren. Bewustzijn van NAS-ransomware zou kunnen zorgen voor minder slachtoffers. Het is belangrijk om bij de preventiecampagnes in te spelen op de risicobeleving van de doelgroep. Dit lijkt namelijk samen te hangen met de effectiviteit van de preventiecampagnes (Ter Huurne, 2008). Bovendien, alleen het notificeren van NAS-gebruikers is niet

voldoende. Rodríguez et al. (2021) onderzochten bij gebruikers van NAS-apparaten welke zelfbeschermende maatregelen gebruikers namen na een notificatie van een kwetsbaarheid. Daaruit bleek dat slechts 24% van de gebruikers alle zelfbeschermende maatregelen nam na meervoudig notificeren. Daaruit valt af te leiden dat bewustzijn niet voldoende is voor zelfbeschermende maatregelen tegen NAS-ransomware. Daarnaast is er maar een relatief kleine groep die gebruikmaakt van NAS-apparaten. Lokale overheidsinstanties kunnen daarom naast NAS-gebruikers ook het gesprek aangaan met bewoners in hun regio over hoe ze in het algemeen veilig data en informatie kunnen opslaan. NAS-ransomware, zoals beschreven in deze studie, kan als casus dienen hoe aanvallers te werk gaan en wat je kan doen om geen slachtoffer te worden. Met deze alternatieve aanpak wordt niet alleen NAS-ransomware bestreden, maar worden ook andere cyberdelicten die gerelateerd zijn aan opslag van data, zoals datadiefstal, bestreden (Bullée & Junger, 2020).

Wat betreft lokale overheidsinstanties zou de (lokale) politie ook een rol kunnen spelen. Gezien de immateriële schade, zou de politie er goed aan doen om een luisterend oor te bieden aan slachtoffers. In de praktijk zien we dat slachtoffers het vaak fijn vinden als ze emotioneel gesteund worden door de politie. Daarnaast kan de politie aan de hand van aangiften kijken of er een aanvalsgolf is die samenhangt met de publicatie van een kwetsbaarheid en daar fabrikanten, gebruikers en andere overheidsinstanties over informeren.

## 7 Discussie

Deze studie beoogt de verschillen tussen reguliere en NAS-ransomware te bestuderen. Daarbij werd gebruikgemaakt van aangiften die slachtoffers hebben gedaan bij de politie. Aangezien zowel particulieren als bedrijven bij de politie aangifte doen van ransomware, bieden politieaangiften de mogelijkheid om reguliere en NAS-ransomware met elkaar te vergelijken.

De politieaangiften kennen echter ook beperkingen. Ten eerste is er de mogelijkheid op selectiebias. Studies naar aangiftebereidheid van andere cyberdelicten melden dat slachtoffers in 8 tot 10% van de gevallen aangifte doen (Van de Weijer et al., 2020). Wel laat veel onderzoek zien dat ernstige feiten ook vaker worden gemeld, ook bij onlinecriminaliteit (Junger, Veldkamp & Koning, 2022). Het is moeilijk te zeggen hoe de aangiftebereidheid de verschillende variabelen in deze studie beïnvloedt. Er is namelijk weinig andere data beschikbaar om hier meer inzicht in te krijgen. Na ons onderzoek hebben we contact gehad met de politie over aangiftebereidheid. Ze merkten op dat er onlangs een politieactie op de ransomware-variant Deadbolt is geweest, waarna slachtoffers die aangifte hadden gedaan een gratis sleutel konden krijgen om hun bestanden te ontsleutelen (RTL, 2022). Nadat de actie in het landelijke nieuws is geweest, waren er vijftien extra aangiften gedaan. Slachtoffers melden dat ze in eerste instantie geen aangifte deden omdat ze verwachtten dat de politie niks kan doen. De actie bewees het tegendeel, waardoor er dus extra aangiften kwamen. Dat de politie niks kan doen is dus een reden waarom de aangiftebereidheid laag is.

Ten tweede, de dataset is door één persoon gecodeerd vanwege de gevoeligheid van de data. Dit kan leiden tot vertekeningen (Artstein & Poesio, 2009). Door twijfelgevallen geanonimiseerd met de onderzoeksgroep te bespreken, hopen we de bias te verkleinen.

Samenvattend, deze studie biedt inzichten hoe NAS- en reguliere ransomware van elkaar verschillen. Dat er ransomware-types zijn waarbij de modus operandi van dader, slachtofferkenmerken en trends verschillen, biedt kansen voor effectievere en efficiëntere interventies tegen elk type ransomware. Desalniettemin zorgen de beperkingen van dit onderzoek ervoor dat meer onderzoek nodig is om de validiteit van de resultaten te verhogen.

Vervolgonderzoek kan zich richten op het gebruik van andere databronnen. Een suggestie is om bijvoorbeeld Shodan en/of Censys te gebruiken om direct systemen die versleuteld zijn te vinden. Daarmee kan beter een inschatting gemaakt worden van de omvang van NAS-ransomware. Het nadeel is dat het onduidelijk is wat de slachtofferkenmerken zijn, aangezien dat via het internet niet zichtbaar is.

Onderzoek dat zich richt op ransomware kan proberen onderscheid te maken tussen reguliere en NAS-ransomware. De verschillende modus operandi, slachtofferkenmerken en trends zijn dusdanig anders tussen reguliere en NAS-ransomware, dat empirisch onderzoek waarschijnlijk de resultaten daarvoor moet corrigeren.

Ten slotte, onderzoek dat zich richt op IoT-malware kan specifieker kijken naar het verschil tussen NAS-ransomware en andere IoT-malware. In deze studie keken we naar het verschil tussen reguliere en NAS-ransomware, maar wellicht zitten er ook verschillen in de modus operandi, slachtofferkenmerken en trends tussen NAS-ransomware en andere IoT-malware. Het onderzoek van deze verschillen kan helpen bij het effectiever bestrijden van de verschillende typen malware.

## Literatuur

Akamai (2021) *What is ransomware?* Geraadpleegd op 11 november 22 november 2022, van www.akamai.com/our-thinking/cybersecurity/what-is-ransomware.

Akdemir, N. & C.J. Lawless (2020) Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. *Internet Research*.

Alrawi, O., C. Lever, K. Valakuzhy, K. Snow, F. Monrose & M. Antonakakis (2021) The Circle Of Life: A Study of The Malware Lifecycle. In: *30th USENIX Security Symposium (USENIX Security 21)* (pp. 3505-3522).

Andrioaie, A. (2021) *An Increased Wave of eCh0raix Ransomware Attacks Hits QNAP NAS Devices*. Geraadpleegd op 26 augustus 2022, van https://heimdalsecurity.com/blog/more-ech0raix-ransomware-attacks-hit-qnap-nas-devices.

Arghire, I. (2022a) *QNAP Warns NAS Users of DeadBolt Ransomware Attacks*. Geraadpleegd op 26 augustus 2022, van www.securityweek.com/qnap-warns-nas-users-deadbolt-ransomware-attacks.

Arghire, I. (2022b) *QNAP Appliances Targeted in New DeadBolt, eCh0raix Ransomware Campaigns*. Geraadpleegd op 26 augustus 2022, van www.securityweek.com/qnap-appliances-targeted-new-deadbolt-ech0raix-ransomware-campaigns.

Artstein, R. & M. Poesio (2009) Bias decreases in proportion to the number of annotators. *In Proceedings of FG-MoL 2005: The 10th conference on Formal Grammar and The 9th Meeting on* (Vol. 139).

Bullée, J.-W. & M. Junger (2020) How effective are social engineering interventions? A meta-analysis. *Information & Computer Security*, *28*(5), 801-830. doi:10.1108/ICS-07-2019-0078

Censys (2022) *Tracking Deadbolt Ransomware Across the Globe*. Geraadpleegd op 11 november 2022, van https://censys.io/tracking-deadbolt-ransomware-across-the-globe.

Cohen, L.E. & M. Felson (1979) Social-change and crime rate trends - routine activity approach. *American Sociological Review*, *44*, 588-608.

Connolly, L.Y., D.S. Wall, M. Lang & B. Oddson (2020) An empirical study of ransomware attacks on organizations: an assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity*, *6*(1), tyaa023.

Cornish, D.B. (1994) The procedural analysis of offending and its relevance for situational prevention. *Crime prevention studies*, *3*(1), 151-196.

Cornish, D.B. & R.V. Clarke (1989) Crime specialisation, crime displacement and rational choice theory. In: *Criminal behavior and the justice system* (pp. 103-117). Berlin, Heidelberg: Springer.

Cornish, D.B. & R.V. Clarke (2008) Rational choice perspective. In: R. Wortley & L. Mazerolle (Eds.), *Environmental criminology and crime analysis*. Abingdon, UK: Willan.

Felson, M. & L.E. Cohen (1980) Human ecology and crime: A routine activity approach. *Human Ecology*, *8*(4), 389-406.

Gatlan, S. (2021a) *New eCh0raix Ransomware Brute-Forces QNAP NAS Devices*. Geraadpleegd op 26 augustus 2022, van www.bleepingcomputer.com/news/security/new-ech0raix-ransomware-brute-forces-qnap-nas-devices.

Gatlan, S. (2021b) *QNAP warns of eCh0raix ransomware attacks, Roon Server zero-day*. Geraadpleegd op 12 november 2022, van www.bleepingcomputer.com/news/security/qnap-warns-of-ech0raix-ransomware-attacks-roon-server-zero-day.

Hilt, S. & F. Merces (2021) *Backing Your Backup. Defending NAS Devices Against Evolving*. Geraadpleegd op 13 december 2022, van www.trendmicro.com/vinfo/us/security/news/internet-of-things/reinforcing-nas-security-against-pivoting-threats.

Holt, T.J., A.M. Bossler & K.C. Seigfried-Spellar (2015) *Cybercrime and digital forensics: An introduction*. Abingdon, Oxon: Routledge.

Holt, T.J., J. van Wilsem & E.R. Leukfeldt (2018) Testing an integrated self-control and routine activities framework to examine malware infection victimization. *Social Science Computer Review*. doi:10.1177/0894439318805067

Hutchings, A. & T.J. Holt (2015) A crime script analysis of the online stolen data market. *British Journal of Criminology*, *55*(3), 596-614.

Huurne, E.F. ter (2008) Information Seeking in a risky world: the theoretical and empirical development of FRIS: A framework of risk information seeking.

Junger, M., B. Veldkamp & L. Koning (2022) *Fraudevictimisatie in Nederland (Fraud Victimization in the Netherlands)*. Geraadpleegd op 13 december 2022, van www.utwente.nl/nl/bms/fraudvic.

Junger, M., V. Wang & M. Schlömer (2020) Fraud against businesses both online and offline: Crime scripts, business characteristics, efforts, and benefits. *Crime science*, *9*(1), 1-15.

Kaspersky Lab (2022) *New ransomware trends in 2022*. Geraadpleegd op 26 augustus 2022, van https://securelist.com/new-ransomware-trends-in-2022/106457.

Keshavarzi, M. & H.R. Ghaffary (2020) I2CE3: A dedicated and separated attack chain for ransomware offenses as the most infamous cyber extortion. *Computer Science Review*, *36*, 100233.

Leukfeldt, E.R. (2016) *Cybercriminal networks: Origin, growth and criminal capabilities*. Den Haag: Eleven International Publishers.

Mansfield-Devine, S. (2022) *Sophos: The State of Ransomware 2022*.

Meurs, T., M. Junger, A. Abhishta & E. Tews (2022a) POSTER: How Attackers Determine the Ransom in Ransomware Attacks. *IEEE S&P Conference*.

Meurs, T., M. Junger, A. Abhishta & E. Tews (2022b) How attacker's effort, victim characteristics and context influence ransom requested, payment and financial loss. *In 2022 APWG Symposium on Electronic Crime Research (eCrime)*. IEEE.

Miró-Llinares, F., J. Drew & M. Townsley (2020) Understanding target suitability in cyberspace: An international comparison of cyber victimization processes. *International Journal of Cyber Criminology*, *14*(1), 139-155.

Nigam, R., H. Zhang & Z. Zhang (2021) *New eCh0raix Ransomware Variant Targets QNAP and Synology Network-Attached Storage Devices*. Geraadpleegd op 26 augustus 2022, van https://unit42.paloaltonetworks.com/ech0raix-ransomware-soho.

Puth, M.T., M. Neuhäuser & G.D. Ruxton (2014) Effective use of Pearson's product–moment correlation coefficient. *Animal behaviour*, *93*, 183-189.

Reyns, B.W. (2017) Routine activity theory and cybercrime: A theoretical appraisal and literature review. In: *Technocrime and criminological theory* (pp. 35-54). Routledge.

Rodríguez, E., M. Fukkink, S. Parkin, M. van Eeten & C. Gañán (2022) Difficult for Thee, But Not for Me: Measuring the Difficulty and User Experience of Remediating Persistent IoT Malware. *arXiv preprint arXiv:2203.01683*.

Rodríguez, E., S. Verstegen, A. Noroozian, D. Inoue, T. Kasama, M. van Eeten & C.H. Gañán (2021) User compliance and remediation success after IoT malware notifications. *Journal of Cybersecurity*, 7(1), tyab015.

RTL Nieuws (2022) *Unieke actie: politie bevrijdt gegijzelde computers dankzij truc met bitcoin*. Geraadpleegd op 11 november 2022, van www.rtlnieuws.nl/nieuws/nederland/artikel/5337913/unieke-actie-politie-probeert-gegijzelde-computers-met-slimme-truc.

Schouw, R. (2022) *Qlocker ransomware maakt wereldwijde comeback op QNAP NAS-apparaten*. Geraadpleegd op 12 november 2022, van https://nl.hardware.info/nieuws/80324/qlocker-ransomware-maakt-wereldwijde-comeback-op-qnap-nas-apparaten.

Sowells, J. (2022) *eCh0raix Ransomware Targeting QNAP Devices*. Geraadpleegd op 26 augustus 2022, van https://hackercombat.com/ech0raix-ransomware-targeting-qnap-devices.

Weijer, S. van de, R. Leukfeldt & S. van der Zee (2020) Reporting cybercrime victimization: determinants, motives, and previous experiences. *Policing: An International Journal*.

Witteman, E. (2021) *QNAP patcht kritieke lekken die ransomware faciliteerden*. Geraadpleegd op 26 augustus 2022, van www.techzine.nl/nieuws/privacy-compliance/457599/qnap-patcht-kritieke-lekken-die-ransomware-faciliteerden.

Wortley, R. & L. Mazerolle (Eds.) (2008) *Environmental criminology and crime analysis*. London, UK: Willan.

Yar, M. (2005) The Novelty of 'Cybercrime'. An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407-427.

Zimmerman, D.W. (1987) Comparative power of Student t test and Mann-Whitney U test for unequal sample sizes and variances. *The Journal of Experimental Education*, *55*(3), 171-174.