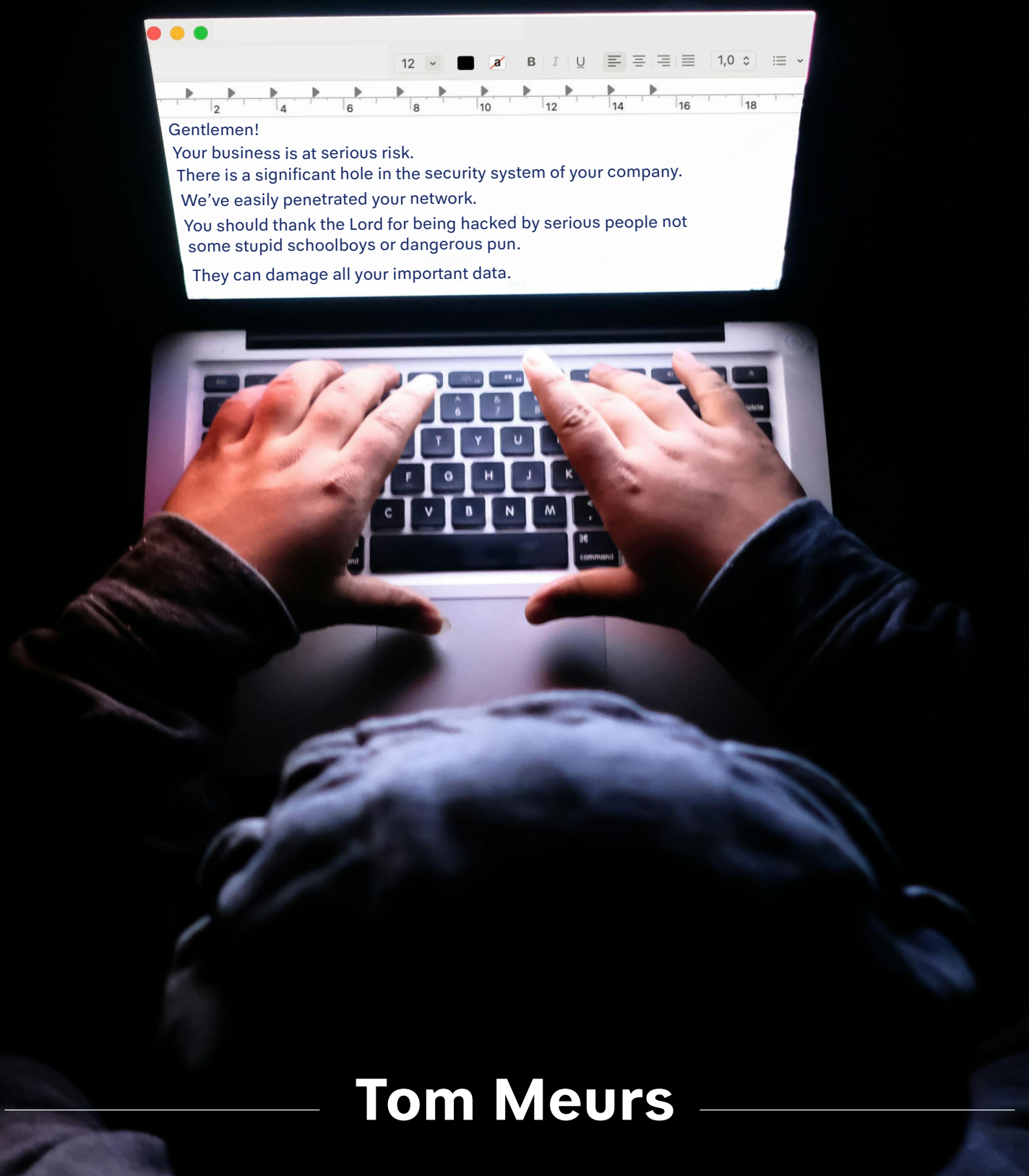
DOUBLE-EXTORTION RANSOMWARE

A Study of Cybercriminal Profit, Effort and Risk



Tom Meurs

Dit magazine is een bewerkte versie van het proefschrift ‘Double-Extortion Ransomware: *A Study of Cybercriminal Profit, Effort, and Risk*’ – **Tom Meurs, 2025**

Vormgeving: Team VAK
Foto’s: Freepik.com

UNIVERSITY OF TWENTE.

AAN HET WOORD

In een ideale wereld zouden criminelen geen ruimte hebben om cyberaanvallen zoals ransomware te plegen. We zouden volledig zijn voorbereid en in staat deze dreigingen adequaat het hoofd te bieden. Maar in werkelijkheid is het criminele landschap complex en blijven cybercriminelen inspelen op kwetsbaarheden in onze systemen.

Elke dag maken criminelen afwegingen om ransomware-aanvallen te plegen, op basis van informatie die ze hebben over de winstgevendheid, de risico's om gepakt te worden, en de inspanning die nodig is om een succesvolle aanval uit te voeren. Deze afwegingen kunnen ertoe leiden dat zij besluiten ransomware-aanvallen te plegen, omdat de combinatie van snel geld en een lage pakkans het aantrekkelijk maakt.

In mijn onderzoek bestudeerde ik het criminele keuzeproces achter ransomware-aanvallen: hoe risico's, winstgevendheid en de benodigde inspanning de criminele besluitvorming beïnvloeden. Ik analyseerde deze factoren om beter te begrijpen hoe we dit soort aanvallen kunnen voorkomen en bestrijden.

In deze samenvatting van het proefschrift deel ik de belangrijkste bevindingen van mijn onderzoek.

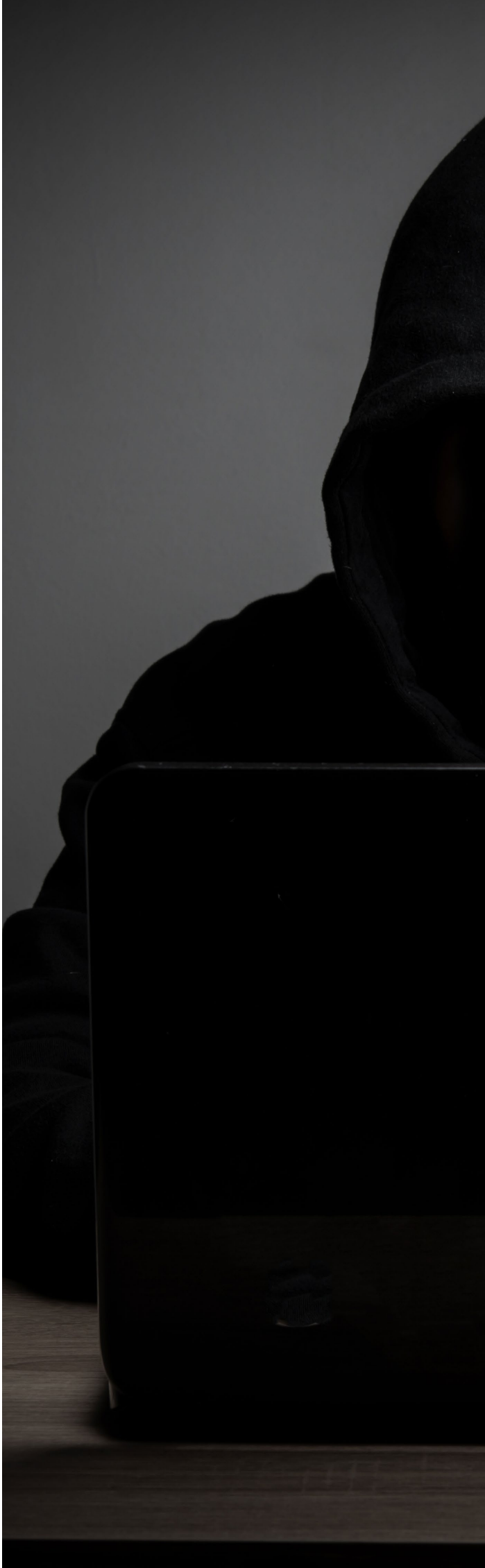
Tom Meurs

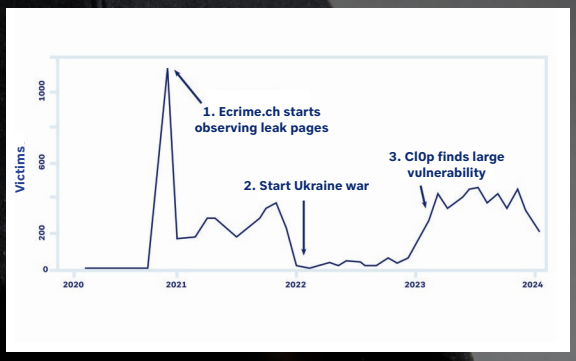
WAAROM DIT ONDERZOEK?

Ransomware is kwaadaardige software waarmee criminelen je bestanden vergrendelen, waardoor je de bestanden niet meer kan gebruiken. Ze vragen dan geld om de bestanden weer vrij te geven. Bij double-extortion ransomware gaat het nog een stap verder: de criminelen dreigen niet alleen je bestanden te vergrendelen, maar zeggen ook dat ze je gegevens openbaar maken als je niet betaalt. Dit maakt het probleem veel groter en stressvoller voor slachtoffers.

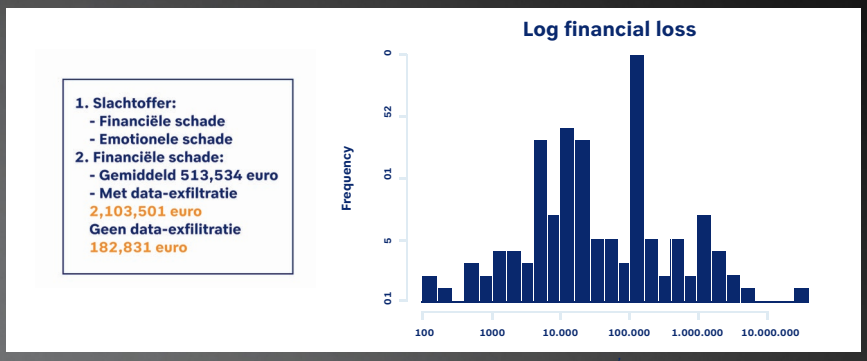
De reden dat ik dit onderzoek heb gedaan, is omdat ransomware de laatste jaren een enorme dreiging is geworden voor bedrijven en organisaties. Dankzij een samenwerking met de politie kreeg ik toegang tot aangiftes van ransomware-aanvallen in Nederland tussen 2019 en 2023. Dat leverde maar liefst 525 gevallen van ransomware-aanvallen op. Daarnaast heb ik gegevens verzameld van bedrijven die incidenten oplossen (incidentresponsepartijen) en informatie van zogenaamde leakpages (websites waar criminelen gestolen gegevens publiceren). Hierdoor kon ik precies onderzoeken hoe winstgevend deze aanvallen zijn voor criminelen, welke risico's ze nemen en hoeveel moeite ze moeten doen om een aanval te laten slagen.

Wat dit onderzoek speciaal maakt, is dat het voor het eerst de winstgevendheid, risico's en inspanning van criminelen combineert om te kijken hoe goed de politie en andere instanties deze aanvallen kunnen bestrijden. Ik heb onderzocht hoe verschillende maatregelen, zoals sancties tegen criminelen, het verstrekken van decryptors (hulpmiddelen om bestanden terug te krijgen zonder te betalen), arrestaties, het bevriezen van cryptomunten en het neerhalen van leakpage-servers, invloed hebben op ransomware-activiteiten. Deze maatregelen blijken effectief te zijn in het verstoren van criminele activiteiten, maar sommige maatregelen werken beter dan andere. Door deze inzichten kunnen we beter begrijpen hoe we criminelen kunnen tegenhouden en kunnen we maatregelen beter afstemmen om ransomware minder aantrekkelijk te maken voor criminelen.



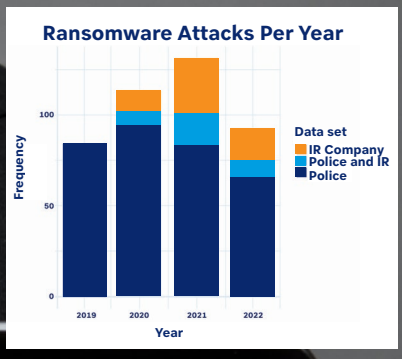


Figuur 1. Aantal ransomware-aanvallen op basis van slachtoffers gepubliceerd op leakpages van ecrime.ch.

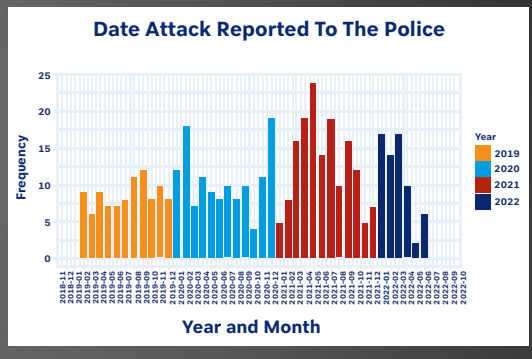


Figuur 2. Hoeveelheid financiële verliezen bij aangifte ransomware.

Figuur 3. Bedrijfsgrootte heeft invloed op kans ransomware (1-50 werknemers = klein, 51=250 werknemers=medium, 251+ werknemers = large).



Figuur 4. Overlap ransomware-aanvallen bij politie en incidentresponsepartij.

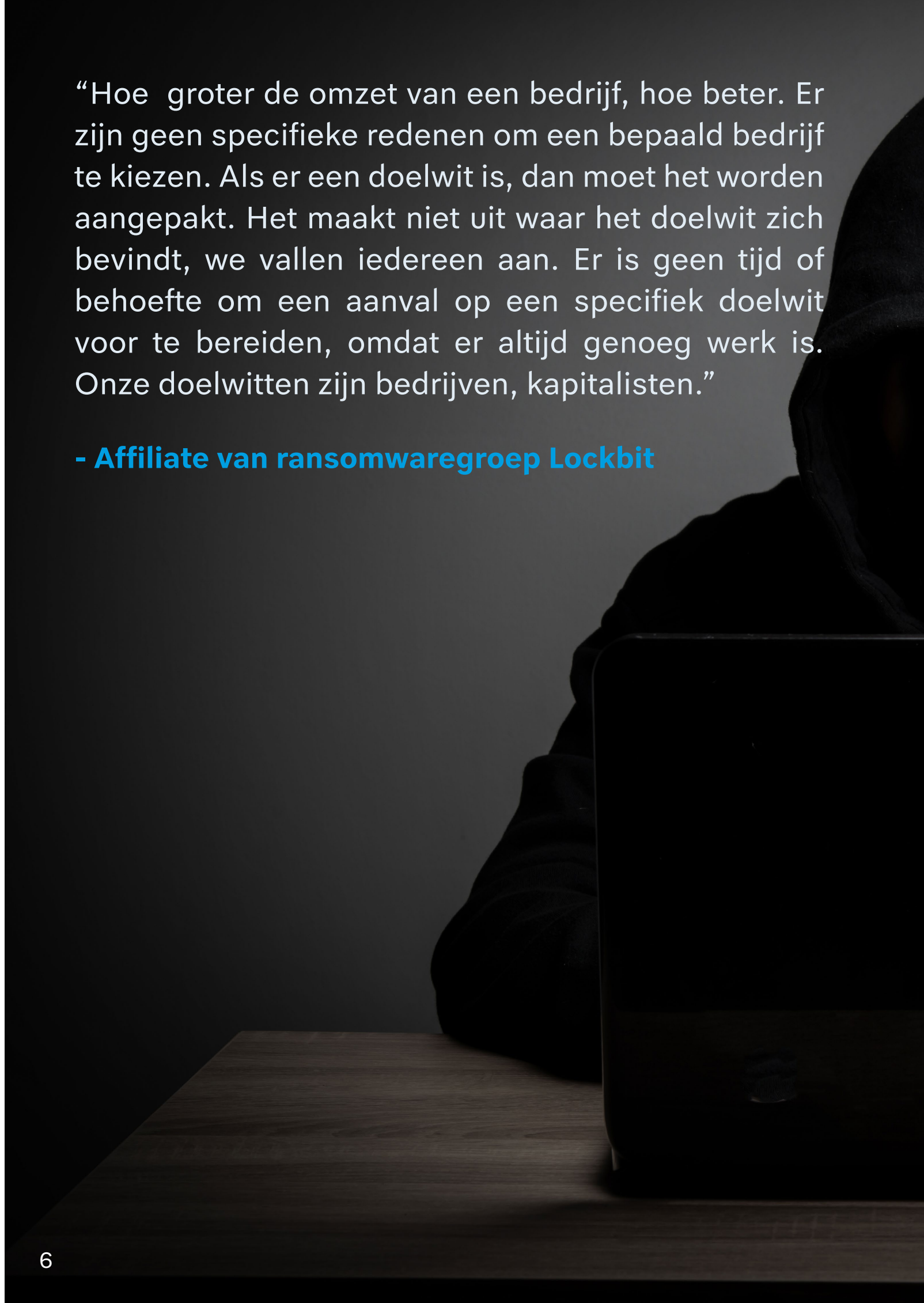


Figuur 5. Aantal aangiftes ransomware politie 2019-2022.

HOE GROOT PROBLEEM IS RANSOMWARE?

Om te kijken hoe groot het ransomwareprobleem is, heb ik gekeken naar hoe vaak ransomware-aanvallen voorkomen en wat de financiële schade daarvan is. Met data van politierapporten, incidentresponsebedrijven en leakpages ontdekte ik dat bij grote bedrijven slechts 41,4% van de ransomware-aanvallen opgemerkt wordt, en bij middelgrote bedrijven is dat 40,2%. Het jaarlijkse risico op een aanval is voor grote bedrijven 1,3% en voor middelgrote bedrijven 0,6%. Helaas kon ik op basis van de huidige data geen betrouwbare uitspraken doen over kleine bedrijven, behalve dat er nog minder aanvallen opgemerkt worden dan bij middelgrote en grote bedrijven.

De financiële schade is aanzienlijk: gemiddeld kost een aanval voor het slachtoffer 513.534 euro. Bij datalekken (data-exfiltratie) stijgt dit naar 2.103.501 euro, terwijl aanvallen zonder datalekken gemiddeld 182.831 euro kosten. Factoren zoals datalekken, gerichte losgeldeisen en Ransomware-as-a-Service (RaaS) vergroten de schade. Bedrijven zonder volledige back-ups rapporteerden vaak grotere verliezen, terwijl bedrijven met goede back-ups de schade beter konden beperken. Kortom, de financiële impact van ransomware-aanvallen is sterk afhankelijk van de voorbereiding van het bedrijf en de manier waarop de criminelen te werk gaan.



“Hoe groter de omzet van een bedrijf, hoe beter. Er zijn geen specifieke redenen om een bepaald bedrijf te kiezen. Als er een doelwit is, dan moet het worden aangepakt. Het maakt niet uit waar het doelwit zich bevindt, we vallen iedereen aan. Er is geen tijd of behoefte om een aanval op een specifiek doelwit voor te bereiden, omdat er altijd genoeg werk is. Onze doelwitten zijn bedrijven, kapitalisten.”

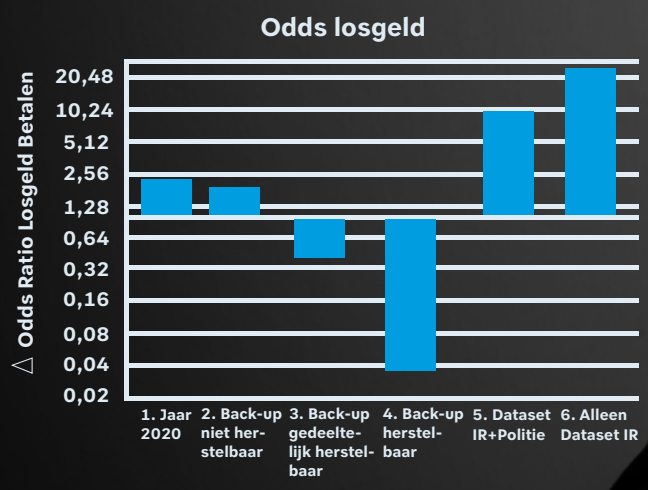
- Affiliate van ransomwaregroep Lockbit

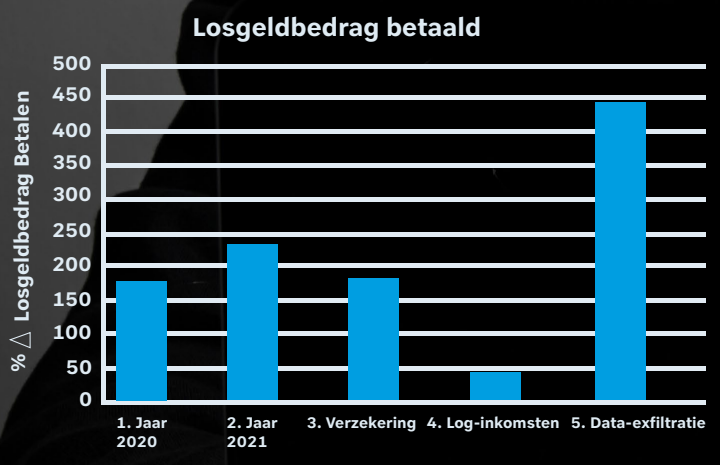
WAT IS HET VERDIENMODEL VAN RANSOMWARE?

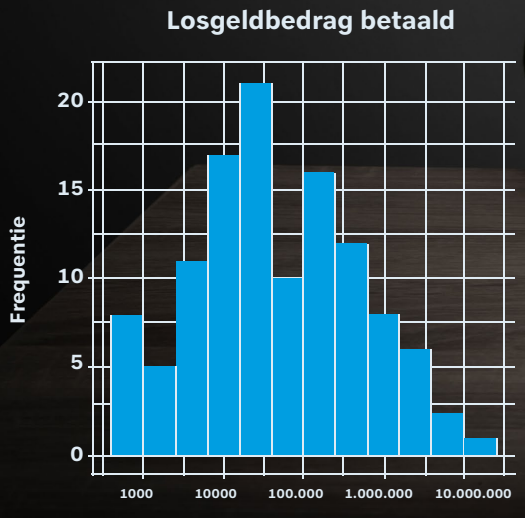
Het verdienmodel van ransomware is simpel: criminelen versleutelen de bestanden van een bedrijf en eisen losgeld om de gegevens terug te geven. Soms stelen ze ook gevoelige data en dreigen ze die openbaar te maken als er niet wordt betaald. Hierdoor voelen slachtoffers nog meer druk om te betalen.

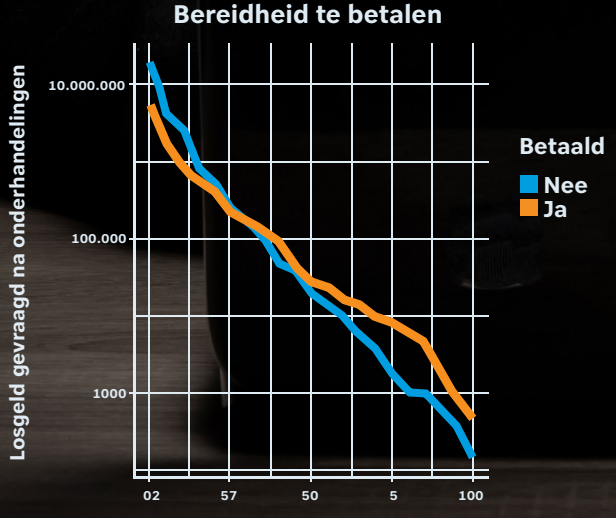
Wat mijn onderzoek speciaal maakt, is dat het laat zien dat verschillende factoren niet alleen bepalen óf bedrijven betalen, maar ook hoeveel ze bereid zijn te betalen. Uit de analyse van 382 ransomware-aanvallen van de politie en een incidentresponsebedrijf blijkt dat het hebben van back-ups de belangrijkste factor is die bepaalt of een bedrijf betaalt. Bedrijven met goede back-ups zijn 27 keer minder geneigd te betalen, omdat ze hun gegevens zelf kunnen herstellen.

Mocht een bedrijf toch besluiten te betalen, dan zijn er andere factoren die de hoogte van het losgeld bepalen. Zo betalen bedrijven met een verzekering of die te maken hebben met gestolen data vaak veel meer. Verzekerde bedrijven betalen gemiddeld 2,7 keer meer losgeld, omdat criminelen weten dat de verzekering de kosten dekt. Wanneer er sprake is van gestolen gegevens (data-exfiltratie), stijgt het losgeld zelfs gemiddeld 4,4 keer. Ook de grootte van een bedrijf speelt een rol: hoe groter de omzet, des te hoger het losgeld dat geëist wordt. Dit toont aan dat criminelen slim inspelen op de situatie van het slachtoffer.









NAS-RANSOMWARE

NAS-ransomware is een vorm van ransomware die zich richt op Network Attached Storage (NAS)-apparaten. Dit zijn apparaten die vaak worden gebruikt door individuen en kleine bedrijven om hun gegevens op te slaan en te delen via een netwerk. NAS-apparaten zijn vaak verbonden met het internet en vormen een gemakkelijk doelwit voor criminelen als ze slecht beveiligd zijn. Bij een aanval op een NAS-apparaat versleutelen de aanvallers de gegevens op het apparaat en eisen losgeld in ruil voor het ontsleutelen van de bestanden. Deze aanvallen zijn doorgaans minder gericht op grote bedrijven en meer op particulieren of kleine bedrijven met minder sterke beveiligingsmaatregelen.

Uit mijn onderzoek naar NAS-ransomware bleek ik dat criminelen een volume-strategie gebruiken, waarbij ze lagere losgeldeisen stellen en meer geautomatiseerde aanvallen uitvoeren op slecht beveiligde NAS-apparaten. Dit betekent dat ze minder inspanning hoeven te leveren, maar wel veel aanvallen kunnen uitvoeren, wat hun winst maximaliseert. In tegenstelling tot reguliere ransomware, die zich richt op bedrijven en hogere losgeldeisen stelt, passen NAS-ransomware-aanvallen in een model van lage risico's en relatief lage inspanning.

NAS systeem

Tabel 2 Samenvatting verschil NAS-ransomware en reguliere ransomware

NAS-ransomware	Reguliere ransomware
Meeste slachtoffers zijn individuele burgers (63%) Gemiddeld € 1654 losgeld (sd = € 5667)	Meeste slachtoffers zijn bedrijven (91%) 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 *randsom 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 versleuting	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

WAT KUNNEN WE DOEN TEGEN RANSOMWARE?

Er wordt vaak gezegd dat ransomware-betalingen verboden zouden moeten worden om criminelen minder te belonen. Maar uit mijn onderzoek blijkt dat veel bedrijven eigenlijk geen keuze hadden tussen betalen of niet betalen. In veel gevallen was hun hele IT-infrastructuur kapot en niet meer herstelbaar, waardoor het betalen van losgeld vaak de enige optie was om een faillissement te voorkomen. Om ransomware effectief te bestrijden, moeten we daarom verder kijken dan alleen het verbieden van betalingen.

Voor mijn studie heb ik verschillende politie-interventies geanalyseerd, zoals het arresteren van daders, het neerhalen van servers (leakpages) waar gestolen gegevens worden gepubliceerd, het bevriezen van crypto-assets, het vrijgeven van decryptie-tools en het opleggen van sancties. Wat opviel, was dat bijna de helft van deze interventies leidde tot het stoppen van ransomware-activiteiten. Dit betekent dat wanneer de risico's voor criminelen toenemen, hun winstgevendheid afneemt en ze eerder geneigd zijn te stoppen. Bovendien was er weinig sprake van "misdaadverplaatsing" (crime displacement), wat laat zien dat deze acties echt effectief waren in het verstoren van hun verdienmodel.

Het verband met winstgevendheid, risico's en inspanning wordt hiermee duidelijk: interventies die de kosten en risico's voor criminelen verhogen, zoals het bevriezen van hun cryptomunten of het neerhalen van hun servers, kunnen hun winst verminderen en hen ontmoedigen om door te gaan. Deze interventies maken het bovendien moeilijker voor ransomware-groepen om verder te opereren, omdat het uitvoeren van aanvallen meer inspanning vereist zonder de zekerheid van een hoge beloning.

Mijn onderzoek laat ook zien dat een combinatie van maatregelen, zoals regelmatige kleine interventies en een gevarieerde aanpak, de beste manier is om ransomware-groepen aan te pakken. Door zowel de winstgevendheid te beperken als de risico's en inspanning voor criminelen te verhogen, kunnen we ransomware minder aantrekkelijk maken en bedrijven beter beschermen.

Intervention	STOP BEFORE	REBRAND BEFORE	CONTINUE	STOP	REBRAND	Total
Arrest	0	4	2	1	0	7
Crypto Freeze	1	0	1	0	0	2
Decryptor	2	0	2	0	2	6
Sanction	1	3	0	1	0	5
Takedown	0	1	1	2	0	4
Takedown, Arrest	0	0	0	2	0	2
Takedown, Decryptor	0	0	1	0	0	1
Takedown, Decryptor, Arrest	0	0	1	1	0	2
Total	4	8	87		2	29

Intervention Type	Freq	Mean Victims	Mean Intervention Time	Mean Uptime Leak Page	Δ Uptime - Intervention Time
Arrest	7	468	399	636	237
Sanction	5	425	727	505	-222
Crypto	2	316	379	671	292
Decryptor	6	243	316	348	32
Takedown	4	171	197	399	202
Multiple interventions	5	540	604	622	18
Interview, Dispute, Shutdown	10	373	442	551	109

OVER MIJ

Ik ben Tom Meurs en heb een achtergrond in psychologie, waarin ik in 2016 afstudeerde met specialisaties in methodologie, psychometrie en klinische psychologie. Daarnaast heb ik een bachelor en master afgerond in Econometrie en Operations Research. Na mijn studie begon ik in 2018 mijn carrière bij TNO, waar ik werkte aan projecten voor de Nederlandse krijgsmacht, politie en de Regionale Inlichtingen- en Expertise Centra (RIEC).

In 2021 begon ik met mijn promotieonderzoek bij de Nederlandse Politie en de Universiteit Twente, gericht op ransomware. Hierbij combineerde ik mijn expertise in statistiek, methodologie en sociale wetenschappen om crimineel gedrag rondom ransomware-aanvallen te analyseren. Mijn promotie werd begeleid door prof. dr. Marianne Junger, met dr. Abhishta en dr. Ir. Erik Tews als dagelijkse begeleiders.

Momenteel richt ik me op de aanpak van cybercriminaliteit door kennis over criminele denkprocessen om te zetten in effectievere en efficiëntere politie-interventies. Hiermee wil ik graag bijdragen aan het verminderen van cybercriminaliteit.