NFIR CYBER SECURITY EXPERTS

WHITEPAPER

ONLINE INBREKERS BEKEKEN

Een crime script analyse van datadiefstal uit organisatienetwerken

VU VRIJE UNIVERSITEIT AMSTERDAM

POLITIEACADEMIE

Hogeschool van Amsterdam

NFIR
Laan van Zuid Hoorn 165
2289 DD Rijswijk

088-323 02 05
info@nfir.nl
www.nfir.nl

IBAN NL 81 RABO 0313 7904 93
KVK 69575347
BTW 8579.24.953.B01

COLOFON

Auteurs:

Renushka Madarie, MSc.[1]

Dr. Marleen Weulen Kranenbarg[2]

Prof. dr. Christianne de Poot[3]

Contact:

info@nfir.nl

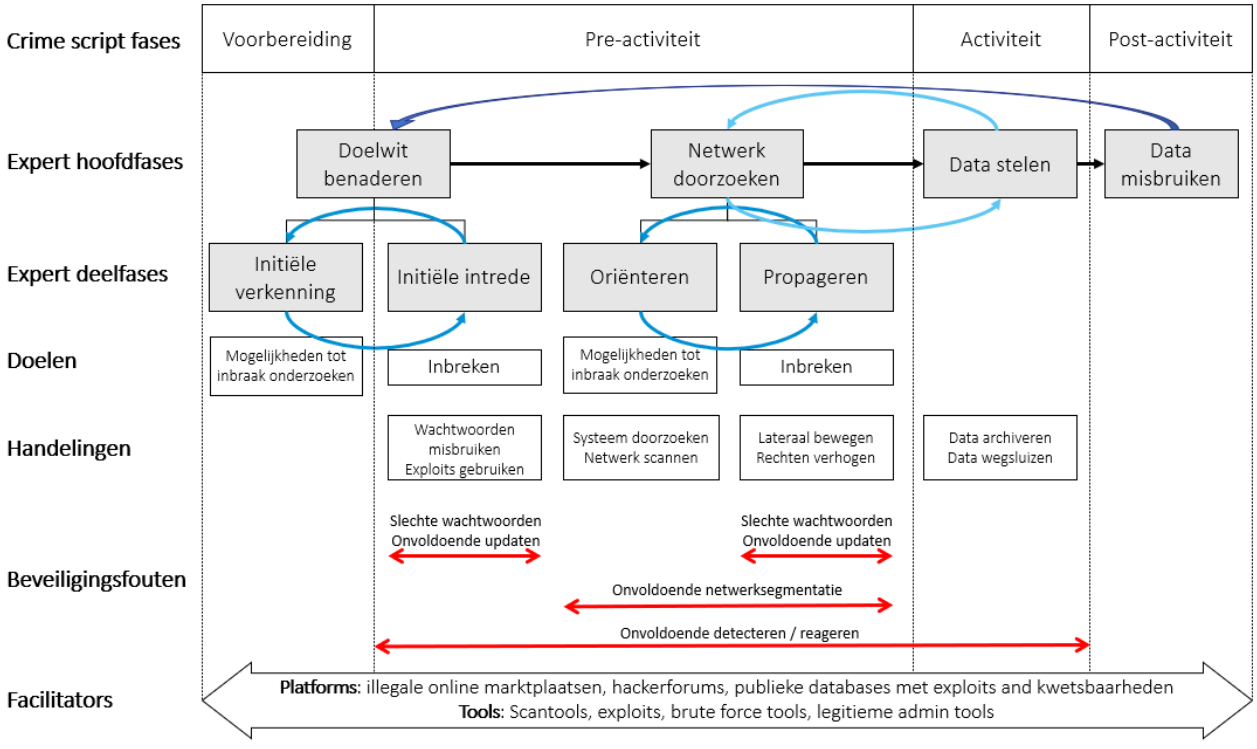
[1] PhD-onderzoeker aan de Hogeschool van Amsterdam, Vrije Universiteit Amsterdam en de Politieacademie.
[2] Universitair docent Criminologie aan de Vrije Universiteit Amsterdam.
[3] Lector Forensisch Onderzoek aan de Hogeschool van Amsterdam en de Politieacademie; hoogleraar Criminalistiek aan de Vrije Universiteit Amsterdam.

Managementsamenvatting

Datadiefstal treft niet alleen individuen, maar ook organisaties. Gegevens van klanten, medewerkers en andere bedrijfsgevoelige informatie worden veelvuldig online gelekt. Data is het nieuwe goud. Ondanks dat de gevolgen voor getroffen organisaties en individuele slachtoffers groot kunnen zijn en datadiefstal steeds vaker voorkomt, is er nog relatief weinig inzicht in het gedrag van datadieven tijdens het inbraakproces in organisatienetwerken. Dit whitepaper beschrijft daarom vanuit een sociaal wetenschappelijk perspectief gedragspatronen van datadieven die specifieke technieken en technologieën overstijgen. Hierbij ligt de focus op datadieven die inbreken via het internet. De hoofdvraag van het onderzoek voor dit whitepaper is:

Hoe handelen online inbrekers die inbreken in systemen en netwerken van organisaties om gegevens te stelen?

Om de hoofdvraag te beantwoorden, is het inbraakproces in delen geanalyseerd. Zo is onderzocht hoe daders doorgaans initieel toegang tot een netwerk verkrijgen, het netwerk doorzoeken en uiteindelijk gegevens stelen. Daarbij is niet alleen gekeken naar wat daders doen, maar ook hoe zij worden gefaciliteerd door zowel beveiligingsfouten als de online beschikbaarheid van hacking tools en kennis. Het onderstaande diagram vat de resultaten van dit onderzoek samen:



Doelwit benaderen

Het diagram laat zien dat daders beginnen met het verkennen van mogelijkheden om online in te breken. Wanneer zij een doelwit voor ogen hebben, kunnen zij op verschillende manieren een initiële toegang verkrijgen. Inbraakmethoden die vaak tot succes leiden zijn het misbruiken van slechte wachtwoorden en technische kwetsbaarheden. Voorbeelden van slechte wachtwoorden zijn veelgebruikte wachtwoorden en wachtwoorden die met de fabrieksinstellingen meekomen. Technische kwetsbaarheden kunnen gevonden worden in, bijvoorbeeld, verouderde software. Zeer kundige daders kunnen ook zero-days misbruiken. Toegang kan echter ook op verschillende soorten online platforms, zoals illegale online marktplaatsen en hackerforums, worden aangeschaft, bijvoorbeeld in de vorm van eerder buitgemaakte inloggegevens.

Netwerk doorzoeken

Eenmaal in een netwerk zullen daders eerst oriënterend gedrag vertonen. Hierbij kunnen zij geautomatiseerd of handmatig het systeem verkennen en bestanden doorzoeken. Vanuit het systeem waarin zij binnen zijn gekomen kunnen zij ook proberen de rest van het netwerk te verkennen. Om systemen en netwerken in kaart te brengen, gebruiken daders niet alleen hun eigen tools, maar ook tools die al geïnstalleerd zijn, zoals scantools voor reguliere beheerwerkzaamheden.

Het propageren omvat het doorhoppen naar andere systemen. Als daders bij het binnentreden nog niet de hoogste gebruikersrechten in een netwerk hebben, zullen zij proberen deze zo snel mogelijk te verhogen. Zo kunnen zij makkelijker naar andere servers bewegen en bestanden met waardevolle informatie inzien die anders afgeschermd zouden zijn. Net als bij de initiële intrede kunnen daders ook bij het propageren buitgemaakte inloggegevens en technische kwetsbaarheden misbruiken om door het netwerk te bewegen. Hierbij hebben zij soms het voordeel dat organisaties het interne netwerk slechter beveiligen dan systemen die direct vanaf het internet toegankelijk zijn.

Data stelen en misbruiken

Daders kunnen gevoelige informatie stelen door deze te kopiëren en weg te sluizen. Grote hoeveelheden data worden hierbij soms gecomprimeerd. Om minder op te vallen, kunnen daders het wegsluizen van data proberen op te laten gaan in de stroom van gebruikelijk netwerkverkeer van de organisatie. Als zij de data eenmaal op hun eigen locatie hebben staan, kunnen zij hier geld aan verdienen door deze, bijvoorbeeld, te verkopen of te gebruiken voor afpersing.

Veelgemaakte fouten

Daders worden bij hun aanval in belangrijke mate gefaciliteerd door veelvoorkomende beveiligingsfouten. De fouten die het vaakst naar voren kwamen in dit onderzoek waren:

1. Het gebruik van slechte wachtwoorden of het niet toepassen van multifactor authenticatie.
2. Het onvoldoende updaten van software.
3. Het onvoldoende toepassen van netwerksegmentatie.
4. Verdachte activiteiten in systemen onvoldoende detecteren of hier onvoldoende op reageren.

Een succesvolle aanval lijkt echter vooral mogelijk door een *opeenstapeling* van beveiligingsfouten

Cyclische processen

Tot slot heeft het inbraakproces een sterk cyclisch karakter. Zo is het inbreken in systemen een kwestie van trial en error, en zullen daders herhaaldelijk oriënterend gedrag vertonen door steeds nieuwe systemen te doorzoeken. Het stelen van data kan dan ook op meerdere momenten tijdens een inbraak plaatsvinden en daders kunnen het netwerk meermaals infiltreren zolang zij toegang hebben. Bovendien kan gestolen data het startpunt vormen voor een volgende inbraak in het netwerk van een andere organisatie.

Inhoudsopgave

1. Introductie

Medewerkers van een Nederlandse gemeente werden enige tijd geleden verrast met een stapel 'ransom notes' in hun printers op kantoor: op geprinte vellen papier sommeerden daders de gemeente losgeld te betalen. De daders waren het netwerk van de gemeente via het internet binnengedrongen en hadden een deel van de systemen versleuteld en een deel verwijderd. Hoewel de gemeente snel aan de bel trok na ontdekking van de aanval, was het kwaad al geschied. De daders hadden een maand eerder toegang verkregen tot het netwerk. Deze toegang werd bemachtigd door de inloggegevens van een account met toegang tot het netwerk te misbruiken. Vermoedelijk waren deze gegevens bemachtigd met een brute force aanval waarbij daders een reeks inlogpogingen doen door verschillende combinaties van wachtwoorden en gebruikersnamen in te voeren. Na binnenkomst in het netwerk verkenden de daders het netwerk, creëerden nieuwe toegangspunten voor zichzelf en installeerden verschillende tools waarmee zij uiteindelijk systemen konden versleutelen en hun sporen konden verwijderen.[4] Het verloop van deze aanval lijkt exemplarisch voor ransomware aanvallen waarbij data is gestolen en gelekt.[5,6]

Zo treft datadiefstal niet alleen personen, maar kunnen ook organisaties als slachtoffer worden beschouwd. Bij digitale aanvallen op organisaties worden niet alleen persoonsgegevens gestolen, maar ook, bijvoorbeeld, accountgegevens van medewerkers en bedrijfsgeheimen. Die gegevens kunnen allerlei andere vormen van criminaliteit in gang zetten. Zo kunnen daders de gestolen gegevens misbruiken voor afpersing en oplichting, en geld verdienen aan de handel in gestolen gegevens.[7] Bovendien kunnen gestolen gegevens dienen als opstapje naar een volgende inbraak in nieuwe accounts en apparaten, bijvoorbeeld door de gegevens te gebruiken in phishing aanvallen.[8]

Ondanks de alomtegenwoordigheid van datadiefstal en de ernst van de gevolgen, is er betrekkelijk weinig wetenschappelijke kennis over het gedrag van datadieven gedurende het inbraakproces in organisatienetwerken. Het inbreken in computer- en netwerksystemen wordt vaak nog op een technische manier onderzocht.[9] Zo wordt onderzocht hoe, bijvoorbeeld, de nieuwste malware werkt of waar nieuwe kwetsbaarheden in systemen zitten en hoe deze het beste verdedigd kunnen worden. In de praktijk zorgt technologische vooruitgang echter voor een kat-en-muisspel tussen aanvallers en verdedigers van onze digitale infrastructuur. Bijvoorbeeld, malware wordt continu doorontwikkeld en als een gat in software wordt gedicht, zullen aanvallers zoeken naar andere gaten in de software. Dit onderzoek richt zich daarom op het vinden van gedragspatronen van datadieven gedurende het inbraakproces die specifieke technieken en technologieën overstijgen.

1.1 Digitale dreigingsmodellen

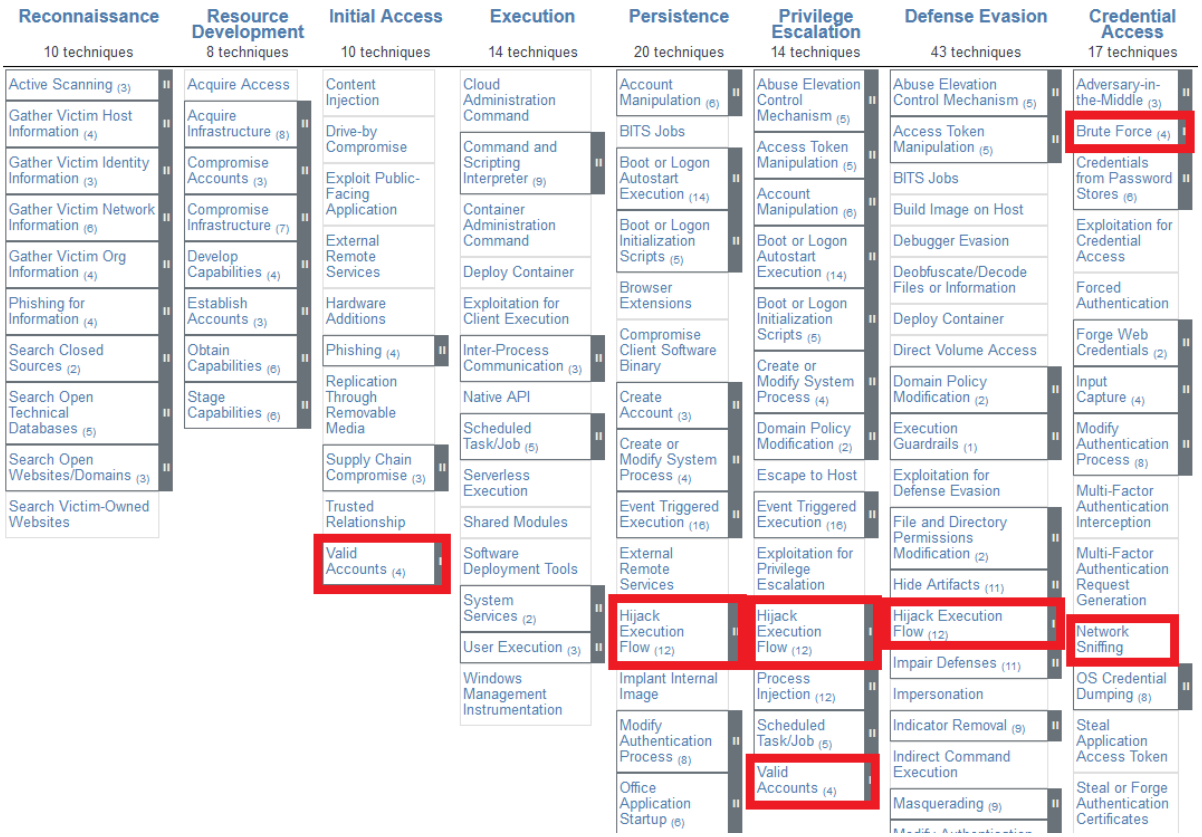
In de praktijk zijn enkele digitale dreigingsmodellen ontwikkeld die beschrijven hoe hackers systemen en netwerken infiltreren en wat zij doen zodra zij binnen zijn. Twee bekende dreigingsmodellen zijn het MITRE ATT&CK raamwerk en de Cyber Kill Chain. Het MITRE ATT&CK raamwerk is in feite een kennisbank op het gebied van digitale inbraaktechnieken en -tactieken.[10] Onderzoekers, systeembeveiligers en andere

---

[4] NFIR (2021). *Onderzoeksrapportage 20107 – Orly*.
[5] Van Trigt, M. (2024). ROC Mondriaan: "Onze daders specialiseren zich in onderwijs- en zorginstellingen". *SURF*.
[6] Dijkstra, M. & Done, Z. (2022). *Red Mudnester: Rapportage*. Hunt & Hackett.
[7] Europol (2023). *Internet Organised Crime Threat Assessment (IOCTA) 2023*, Publications Office of the European Union.
[8] Peng, P., Xu, C., Quinn, L., Hu, H., Viswanath, B. & Wang, G. (2019). *What Happens After You Leak Your Password: Understanding Credential Sharing on Phishing Sites*. ACM Asia Conference on Computer and Communications Security, Auckland, New Zealand.
[9] Mat, S. R. T., Ab Razak, M. F., Kahar, M. N. M., Arif, J. M., Mohamad, S. & Firdaus, A. (2021). Towards a systematic description of the field using bibliometric analysis: Malware evolution. *Scientometrics, 126*(3), 2013–2055.
[10] Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B. (2020). MITRE ATT&CK: Design and Philosophy. *The MITRE Corporation*.

geïnteresseerden kunnen deze kennisbank gebruiken om, bijvoorbeeld, aanvalsscenario's op te stellen, beveiligingsrisico's in kaart te brengen en malafide handelingen in systemen te duiden.[11] Een deel van het ATT&CK raamwerk is afgebeeld in Figuur 1. Figuur 1 laat zien hoe tactieken als 'Reconnaissance' en 'Credential Access' categorieën vormen waaronder verschillende aanvalstechnieken vallen. Bijvoorbeeld, Credential Access, oftewel het bemachtigen van inloggegevens, kan door een 'Brute Force' aanval toe te passen of door netwerkverkeer af te luisteren ('Network Sniffing'). Deze technieken zijn uitgelicht in Figuur 1.

Figuur 1. Een deel van het MITRE ATT&CK raamwerk.



Hoewel dit raamwerk een uitgebreide verzameling technische kennis omvat, is het niet helder op welke data dit model precies is gebaseerd en hoe de categorieën van technieken en tactieken zijn bedacht. Daarnaast lijken de tactieken elkaar van links naar rechts chronologisch op te volgen, maar het is niet duidelijk of en hoe deze met elkaar samenhangen. Bijvoorbeeld, in Figuur 1 beschrijven de eerste kolommen handelingen waarmee daders een eerste toegang verkrijgen, daarna volgen handelingen waarmee zij toegang behouden en vervolgens inloggegevens bemachtigen. Uit de eerder beschreven casus over de Nederlandse gemeente blijkt echter dat de brute force aanval (onder Credential Access) al werd toegepast vóór het verkrijgen van een eerste toegang. Bovendien vallen meerdere technieken (zoals 'Hijack Execution Flow' en 'Valid Accounts') onder verschillende tactieken, wat enige volgordelijkheid verder teniet doet. Ter illustratie zijn ook deze technieken uitgelicht in Figuur 1.

[11] Cybersecurity and Infrastructure Security Agency (2020). Emotet Malware. *Cybersecurity Advisory*.

De Cyber Kill Chain van Lockheed Martin beschrijft daarentegen een proces van zeven opeenvolgende stappen die online inbrekers doorlopen om systemen aan te vallen.[12,13] Deze stappen omvatten, onder andere, verkennend onderzoek naar (potentiële) doelwitten, kwetsbaarheden misbruiken, toegang tot een systeem of netwerk behouden en het einddoel behalen. Volgens de bedenkers van dit model zou een onderbreking van dit proces moeten resulteren in een mislukte aanval. Daarnaast zouden verdedigers een voorsprong kunnen creëren op aanvallers door na te denken over hoe zij de aanvalsketen kunnen onderbreken.

Inmiddels hebben verschillende onderzoekers aanpassingen aan de Cyber Kill Chain voorgesteld, bijvoorbeeld door stappen toe te voegen en anders uit te leggen.[14,15] Opvallend is dat de voorgestelde aanpassingen vaak gaan over handelingen die daders uitvoeren *nadat* zij in een netwerk hebben ingebroken – iets waar het originele model nauwelijks op in gaat. Bovendien suggereren enkele onderzoekers dat een aanval ook meerdere kill chains kan omvatten.[16,17] Dit is omdat, enerzijds, daders herhaaldelijk het netwerk betreden en anderzijds, daders soortgelijke handelingen herhaaldelijk uitvoeren tijdens een inbraak.

1.2 Doelstellingen van dit onderzoek

Het doel van dit onderzoek is het analyseren van gedragspatronen van online inbrekers die specifieke technieken en technologieën overstijgen. Hiervoor is de volgende hoofdvraag opgesteld:

Hoe handelen online inbrekers die inbreken in systemen en netwerken van organisaties om gegevens te stelen?

Om antwoord te kunnen geven op deze vraag is het gehele proces van inbraak tot diefstal onder de loep genomen. Meer specifiek is gekeken naar de volgende drie hoofdfases: het verkrijgen van een eerste toegang, het doorzoeken van het netwerk en het stelen van gegevens. Om handelingen van daders gedurende dit proces te kunnen duiden, zijn deze voorzien van doelen en context. De context omvat zowel de systemen waarin daders inbreken als omgevingsfactoren *buiten* de aangevallen systemen. Zo beschrijft dit onderzoek niet alleen wat daders doen, maar ook hoe zij worden gefaciliteerd bij het verkrijgen van tools, kennis en kansen om in te breken. Door deze gedragspatronen en gelegenheidsstructuren te analyseren, biedt dit onderzoek niet alleen meer inzicht in datadiefstal specifiek, maar verrijkt het ook het begrip van criminele processen in brede zin.

2. Data en methoden

2.1 Dataverzameling

Voor dit onderzoek zijn twaalf cybersecurity experts geïnterviewd bij NFIR. Dit bedrijf biedt cybersecurity diensten aan voornamelijk het midden- en kleinbedrijf (MKB) en organisaties in de publieke sector. Voor de interviews zijn respondenten geworven van verschillende afdelingen binnen het bedrijf om een diverse set

[12] Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.
[13] Lockheed Martin (2024). *Cyber Kill Chain*.
[14] Khan, M. S., Siddiqui, S., & Ferens, K. (2018). A cognitive and concurrent cyber kill chain model. In K. Daimi, G. Francia, L. Ertaul, L.H. Encinas & E. El-Sheikh (Eds.), *Computer and Network Security Essentials*, 585-602.
[15] PRODAFT (2021). *Conti Ransomware Group: In-Depth Analysis*.
[16] Malone, S.T. (2016). *Using An Expanded Cyber Kill Chain Model to Increase Attack Resiliency*. Black Hat USA.
[17] Ussath, M., Jaeger, D., Feng Cheng, & Meinel, C. (2016). *Advanced persistent threats: Behind the scenes*. 2016 Annual Conference on Information Science and Systems, 181–186.

aan kennis en ervaring aan te spreken. Zo kon het handelen van daders vanuit verschillende perspectieven worden belicht. Alle benaderde medewerkers waren bereid tot deelname. In totaal zijn vier forensisch onderzoekers, vier pentesters, twee SOC-analisten en twee personen die zich met threat intel(ligence) bezighouden geïnterviewd. Meerdere respondenten waren op verschillende afdelingen werkzaam. Daarnaast werkten de meeste respondenten ook als incident responder of hebben dat in het verleden gedaan. Omdat de meeste respondenten verschillende cybersecurity functies hebben bekleed, konden zij ook vertellen over andere cybersecurity specialismen dan waar zij zich ten tijde van het interview hoofdzakelijk mee bezig hielden.

De semi-gestructureerde expertinterviews vonden plaats van april tot en met juni 2022 en duurden gemiddeld 75 minuten. De vragen hadden hoofdzakelijk betrekking op hoe daders toegang tot computers en netwerken van organisaties krijgen, wat zij doen als ze eenmaal binnen zijn en hoe zij gegevens bemachtigen. Naarmate er meer herhaling kwam in de antwoorden van de respondenten, werden de vragen specifieker en meer afgestemd op het deelvakgebied van de respondent. Uiteindelijk zijn ook ogenschijnlijke tegenstrijdigheden uit de interviews voorgelegd aan enkele respondenten zodat zij daarop konden reflecteren.

2.2 Data analyse

De interviews zijn woordelijk getranscribeerd en in twee fases geanalyseerd. De eerste fase omvat een thematische analyse van de transcripten.[18] Thematische analyse is een methode om patronen uit data te destilleren en deze vervolgens te analyseren. Dit is een recursief proces waarbij de data meermaals zijn herlezen. Dit begon bij het transcriberen van de data en liep door gedurende het samenvatten en coderen van de transcripten. De codes waren gebaseerd op de eerder beschreven dreigingsmodellen, maar er werd ook een open blik gehouden voor relevante informatie die niet goed bij bestaande codes paste. Zo is een combinatie van thematisch en open coderen toegepast. Uiteindelijk zijn de codes gecategoriseerd en aan elkaar gerelateerd waar mogelijk en zinvol.

Na het coderen is een crime script analyse toegepast. Crime script analyse is een veelgebruikte methode in de criminologie om patronen in dadergedrag in kaart te brengen. Een crime script beschrijft handelingen die daders uitvoeren vóór, tijdens en na het plegen van een misdrijf.[19] De handelingen zijn onderverdeeld in fases die elkaar chronologisch opvolgen. Zo verschaft een crime script inzicht in, onder andere, hoe een bepaalde vorm van criminaliteit gepleegd wordt, welke tools hierbij zoal worden gebruikt en welke omgevingsfactoren invloed hebben op dit proces.[20,21]

Het volgende hoofdstuk beschrijft de fases die datadieven doorlopen tijdens het inbraakproces. Eerst is het proces beschreven aan de hand van de 'expert fases': fases beschreven door de respondenten waarbij de terminologie die zij hanteerden is aangehouden om zo dicht mogelijk bij hun perspectief te blijven. Daarna is het uitgeschreven proces samengevat in een crime script diagram gebaseerd op het vier-fase model van Tompson en Chainey.[22] De fases die zij gebruiken, zijn de Voorbereiding, Pre-activiteit, Activiteit en Post-activiteit. Deze fases beschrijven achtereenvolgens: (1) hoe daders manieren zoeken om het misdrijf te plegen, (2) welke concrete stappen zij zetten om het misdrijf uit te kunnen voeren, (3) de uitvoering van het misdrijf, en (4) handelingen om de plaats delict te verlaten en het misdrijf af te ronden. Het diagram laat

---

[18] Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101.

[19] Cornish, D. (1994). The procedural analysis of offending and its relevance for situational prevention. *Crime Prevention Studies, 3*(1), 151–196.

[20] Borrion, H. (2013). Quality assurance in crime scripting. *Crime Science, 2*(6).

[21] Dehghanniri, H., & Borrion, H. (2019). Crime scripting: A systematic review. *European Journal of Criminology, 18*(4), 1–22.

[22] Tompson, L., & Chainey, S. (2011). Profiling illegal waste activity: Using crime scripts as a data collection and analytical strategy. *European Journal on Criminal Policy and Research, 17*, 179–201.

zien hoe de verschillende expertfases relateren aan de vier theoretische crime script fases, verschillende doelen en omgevingsfactoren.

3. Resultaten

Dit hoofdstuk beschrijft allereerst de drie hoofdfases die daders doorlopen zoals uitgelegd door de respondenten: (1) het verkrijgen van een initiële toegang, (2) het doorzoeken van een netwerk, en (3) het stelen van gegevens. Hierbij hebben de resultaten overigens voornamelijk betrekking op handelingen in netwerken met *Windows* systemen omdat de respondenten deze systemen het vaakst tegenkwamen tijdens hun werkzaamheden. Vervolgens worden beveiligingsfouten beschreven die respondenten regelmatig tegenkwamen bij getroffen organisaties. Dit zijn fouten die gelegenheden creëerden voor daders om in te breken en data te stelen. Het hoofdstuk sluit af met een crime script diagram dat de stappen die daders zetten samenvat en relateert aan doelen en gelegenheidsstructuren.

3.1 Initiële intrede

Hoewel daders fysiek naar een locatie kunnen gaan om daar een apparaat direct met het netwerk te verbinden, zullen zij in de meeste gevallen proberen een aanval over het internet te plegen. Dit onderzoek focust daarom op inbraakpogingen via het internet. Als daders online proberen in te breken, zullen zij logischerwijs eerst op machines stuiten die direct met het internet verbonden zijn in plaats van machines die niet via het internet te benaderen zijn.

Daders kunnen op verschillende manieren online inbreken. Een eerste veelgenoemde manier die daders vaak gebruiken om in te breken is het misbruiken van slechte wachtwoorden. Slechte wachtwoorden kunnen makkelijk te raden wachtwoorden zijn, maar ook wachtwoorden die met fabrieksinstellingen meekomen of gelekte wachtwoorden die niet gewijzigd zijn. Een forensisch onderzoeker legde uit dat zij regelmatig makkelijk te raden wachtwoorden tegenkwamen in hun onderzoeken:

"*Wij hebben bijvoorbeeld een casus gehad waarbij bijvoorbeeld het wachtwoord 'password' was en dan was de 'a' een apenstaartje en de 'o' was een nul. Nou, die staat hoog op zo'n lijst van standaardwachtwoorden. Of welkom2020. Nou, dat was dan een casus in [een ander jaar], maar toch, dat zijn wel de wachtwoorden die je tegenkomt*."

Dat respondenten het gebruik van slechte wachtwoorden "*relatief vaak*" zagen in hun onderzoeken, betekent niet per se dat deze veel voorkomen, maar het is wel een indicatie dat het een belangrijke aanvalsvector is voor daders. Met gestolen of geraden wachtwoorden kunnen daders, bijvoorbeeld, via een VPN of Citrix verbinding inloggen met andermans gebruikersaccount en vanuit diens gebruikersomgeving het netwerk verder doorzoeken.

Naast slechte wachtwoorden gebruiken daders ook bekende kwetsbaarheden in systemen om in te breken. Bijvoorbeeld, wanneer zij zien dat een machine verouderde software draait, dan kunnen zij online nazoeken welke kwetsbaarheden die software waarschijnlijk bevat en of daar exploits voor zijn gepubliceerd. Een exploit is code waarmee een kwetsbaarheid kan worden misbruikt. Niet iedere kwetsbaarheid kan even makkelijk worden geëxploiteerd en een kwetsbaarheid leidt ook niet altijd tot toegang tot een systeem. Een dader zal bij een kwetsbaarheid dus moeten zoeken naar bruikbare en relevante exploits. Net als bij wachtwoorden kan het misbruiken van kwetsbaarheden om in te breken dus ook een kwestie van trial en error zijn.

Zeer kundige daders kunnen ook zero-day aanvallen uitvoeren waarbij zij een kwetsbaarheid uitbuiten waar nog geen patch voor is.[23] In sommige gevallen is deze kwetsbaarheid ook nog niet bekend bij de fabrikant van de software, terwijl in andere gevallen de kwetsbaarheid bekend is gemaakt voordat de fabrikant het probleem heeft kunnen oplossen. In beide gevallen kunnen organisaties zich niet goed kunnen wapenen tegen dit soort aanvallen. Omdat een zero-day aanval de nodige IT-kennis van daders vereist, zagen enkele respondenten alleen grotere organisaties getroffen worden door dit soort aanvallen.

Daders kunnen ook voor een simpelere route kiezen door toegang tot een systeem te kopen. Een threat intel analist legde uit dat sommige daders zich specialiseren in het schrijven van malware, andere daders bieden phishingtools aan, terwijl weer andere daders expert zijn in het hacken van organisaties. Wanneer daders niet goed weten hoe zij de verkregen toegang kunnen uitbuiten, kunnen zij die toegang online te koop aanbieden. Dit kan toegang zijn in de vorm van een technische kwetsbaarheid, zoals een zero-day kwetsbaarheid, maar ook in de vorm van inloggegevens die door phishing zijn bemachtigd.

3.2 Het netwerk doorzoeken

Zodra daders eenmaal toegang hebben gekregen tot het systeem waar zij probeerden in te breken, kunnen zij op verschillende manieren hun aanval voortzetten. Deze paragraaf beschrijft de meest genoemde handelingen die daders verrichten zodra zij binnen in een computersysteem- of netwerk zitten en zoeken naar waardevolle gegevens. De respondenten maakten hierbij onderscheid tussen handelingen gericht op 'oriënteren' en 'propageren'. In de oriëntatiefase verkennen daders systemen en netwerken handmatig of geautomatiseerd. In de propagatiefase proberen daders door te hoppen naar andere systemen, bijvoorbeeld om hun rechten te verhogen en meer waardevolle informatie te vinden.

De forensisch onderzoekers gaven meerdere voorbeelden van ransomwarezaken waarbij daders snel accounts met de hoogste rechten in een netwerk probeerden te bemachtigen. Hoe meer rechten een account heeft, hoe meer soorten acties kunnen worden verricht met dat account. Zo mogen sommige accounts slechts bij bepaalde bestanden of mappen komen, terwijl andere accounts ook programma's mogen installeren en antivirussoftware kunnen uitschakelen. Een van de respondenten gaf als voorbeeld dat een bedrijf haar jaarrekeningen had afgeschermd door slechts bepaalde gebruikers toegang te geven tot die documenten. Daders moesten daarom accounts met hogere rechten bemachtigen om die jaarrekeningen te kunnen bekijken. De meest waardevolle accounts voor daders zijn doorgaans de '*admin*' accounts omdat die de hoogste rechten hebben in een netwerk.[24] Hoewel het soms mogelijk is om met normale gebruikersaccounts al veel gegevens in te kunnen zien en schade aan te richten, is het efficiënter om aanvallen uit te voeren met admin accounts.

Het netwerk doorzoeken lijkt een cyclisch-interactief proces te zijn: stapsgewijs wordt geprobeerd het einddoel te bereiken waarbij steeds een cyclus wordt doorlopen van informatie verzamelen, een aanvalsobject bepalen en het gekozen object aanvallen. Wat daders *kunnen* doen in een systeem hangt af van waar zij in het netwerk zitten, met welke accounts zij kunnen werken en welke kwetsbaarheden er zijn. Wat daders daadwerkelijk doen in een systeem hangt af van het einddoel, oftewel het motief, dat zij hebben.

3.2.1 Oriënteren: Om rechten te verhogen, en meer in het algemeen om waardevolle informatie te vinden, zullen daders eerst oriënterend gedrag vertonen. Door te oriënteren vormen zij een beeld van het systeem waar zij in zitten en van de rest van het netwerk. Oriënteren kan zowel handmatig als geautomatiseerd.

---

[23] Er worden verschillende definities gebruikt voor 'zero-day aanvallen'. Hier wordt de definitie van Bilge & Dumitraş (2012) en Microsoft (2024) gehanteerd.

[24] Hierbij moet worden opgemerkt dat er verschillende typen admin (administrator) accounts zijn. In het geval van Windows systemen zijn er twee soorten admins: lokale administrators en domeinadministrators. Daders lijken doorgaans uit te zijn op domeinadministrator ('domain admin') accounts omdat die de meeste rechten hebben in een Windowsnetwerk.

Handmatige oriëntatie omvat, bijvoorbeeld, door mappen klikken en bestanden bekijken. Dit moet vaak handmatig omdat mappenstructuren en bestandsnamen vaak zijn afgestemd op specifieke organisaties en personen. Structuren en namen variëren dan te veel tussen doelwitten om deze geautomatiseerd te doorzoeken. Een respondent gaf aan dat daders wel zoektermen kunnen gebruiken in de standaard zoeksystemen, zoals Windows Verkenner ('*Explorer*'), om meer geautomatiseerd bepaalde bestanden te vinden. Bijvoorbeeld, daders kunnen zoeken met behulp van zoektermen als 'wachtwoord' of 'vertrouwelijk', of een vertaling hiervan, als zij verwachten deze termen in bestandsnamen terug te vinden. Wanneer daders zoeken naar informatie waarvan de waarde contextafhankelijk is, zullen zij ook meer handmatig werken. Bijvoorbeeld, voor een computer of een scantool is een privéfoto slechts een bepaald type bestand, terwijl de voorstelling van iets of iemand maakt dat de foto een bepaalde lading heeft voor mensen. Omdat tools deze menselijke interpretatie vaak niet of minder goed kunnen vatten, vereist het zoeken naar dit soort ongestructureerde informatie ook vaak enig handwerk.

Uit een eerste oriëntatie van een systeem kan een dader al vrij veel informatie halen. Naast het uitpluizen van mappen kan een eerste beeld worden geschetst van hoe het sociale en het technische netwerk van de organisatie eruitziet. Zo kan uit communicatieplatformen worden afgeleid welke personen er nog meer werken en wie wat met elkaar deelt. Daarnaast kan worden achterhaald met welke andere apparaten de gecompromitteerde machine kan communiceren. Als het rechtenbeheer niet goed is geregeld voor het netwerk, dan kunnen daders zelfs meer doen met het bemachtigde gebruikersaccount dan zou worden verwacht op basis van de werkzaamheden van de legitieme gebruiker. Daders kunnen dan namelijk, bijvoorbeeld, bestanden en mappen inzien die de gebruiker helemaal niet hoeft in te zien.

Met scantools kunnen daders geautomatiseerd de rest van het netwerk in kaart brengen. Zo kunnen zij uitzoeken waar interessante servers zitten, zoals file servers en back-up servers. De forensisch onderzoekers zagen regelmatig dat daders scantools gebruikten. Dit waren zowel tools die al op het systeem stonden[25] als tools die daders hadden geïnstalleerd. Scantools laten daders niet alleen zien welke andere servers in het netwerk zitten, maar helpen ook bij het zoeken naar kwetsbaarheden. Omdat de scantools alleen kunnen scannen op kwetsbaarheden die zij kennen[26], kunnen deze tools niet alle kwetsbaarheden in een systeem of netwerk signaleren. Bijvoorbeeld, scanners zijn minder goed in het herkennen van kwetsbaarheden die ontstaan door hele specifieke software-instellingen op bepaalde apparaten zoals printers en camera's. De pentesters gaven daarom aan dat ook het zoeken naar kwetsbaarheden alsnog enig handwerk kan vereisen.

In aanvulling op het in kaart brengen van systemen in het netwerk, kunnen daders ook nagaan welke accounts in het netwerk actief zijn om hun rechten te verhogen. De meeste respondenten gaven aan dat het aanvallen of uitvragen van centrale autorisatie- en authenticatiesystemen regelmatig voorkomt bij hackaanvallen. Het meest genoemde systeem was de Windows Active Directory (AD). In deze database staat, onder andere, aangegeven wie bij welke bestanden of systemen mag en op welke systemen gebruikers zijn ingelogd. Door de AD aan te vallen kunnen daders direct de hoogste rechten in een netwerk bemachtigen. Zo kan een dader versleutelde wachtwoorden, waaronder die van domain admins, uit de AD halen en die vervolgens proberen te ontsleutelen. Daders kunnen ook informatie uit de AD halen met behulp van tools of technieken die beheerders ook gebruiken om inzicht te krijgen in welke systemen zij moeten hacken om hun rechten te verhogen:

---

[25] Tools die al op het systeem stonden, zijn tools die normaal ook worden gebruikt door netwerkbeheerders voor hun reguliere werkzaamheden. Let op: 'beheerder' refereert hier aan een functietitel en 'admin' aan een type gebruikersaccount (in Windows systemen). Net zoals er verschillende soorten admin accounts zijn, zijn er ook verschillende soorten IT-beheerders. Een goed begrip van deze verschillen vereist echter IT-kennis die buiten het bereik van dit paper valt. (Maar zie hier voor een creatieve uitleg over wat een systeembeheerder is door de Huilende Rappers.)

[26] Onderdeel van scantools zijn zogenaamde 'bibliotheken' die een collectie van kwetsbaarheden kunnen bevatten. Tijdens het scannen put de tool uit deze collectie om na te gaan of een kwetsbaarheid aanwezig is.

"Stel, ik mag inloggen in de bibliotheekcomputer en daar is Pietje ook ingelogd. En Pietje is domain admin, dan is het heel interessant om in te loggen op die bibliotheekcomputer en te kijken of jij bij de gegevens van Pietje kan. Op Windows computers is dat vaak zo. Dus dat is heel waardevolle informatie. Dat gebruiken hackers zeker."

Door in dit scenario op de bibliotheekcomputer in te loggen, kan het geheugen van die computer worden uitgelezen waar mogelijk nog de inloggegevens van het admin account in staan.

3.2.2 Propageren: Om andere systemen te infiltreren, kunnen daders, net als bij de initiële intrede, inloggegevens of (technische) kwetsbaarheden uitbuiten. Deze sectie gaat dieper in op hoe daders deze twee methoden toepassen wanneer zij eenmaal in het netwerk zitten.

Allereerst kunnen daders op meerdere plekken in systemen naar inloggegevens zoeken. Zij kunnen, bijvoorbeeld, wachtwoorden uit het geheugen of systeembestanden extraheren. Op deze plekken zijn wachtwoorden niet of zwak versleuteld als de configuratie niet in orde is. Daders kunnen wachtwoorden ook raden door middel van brute force aanvallen. Hierbij kunnen zij wachtwoordlijsten van veelvoorkomende wachtwoorden gebruiken. Dit resulteert soms in honderden, duizenden of miljoenen opeenvolgende foutieve inlogpogingen. Een forensisch onderzoeker gaf aan dat brute force aanvallen niet alleen werden gezien bij de initiële intrede, maar ook wanneer het daders niet lukte om hun rechten te verhogen, maar toch andere servers wilden infiltreren.

Om andere servers te bereiken, kunnen daders ook misbruik maken van kwetsbaarheden in software. Enkele respondenten gaven hierbij aan dat het interne netwerk soms slechter beveiligd is dan de machines die vanaf het internet te benaderen zijn. Organisaties veronderstellen namelijk soms onterecht dat het interne netwerk minder goed beveiligd hoeft te worden omdat het niet direct benaderbaar is vanaf het internet.

Voor daders is het soms van belang om meerdere kwetsbaarheden uit te kunnen buiten om toegang te blijven houden tot het netwerk. Als organisaties een kwetsbaarheid dichten door systemen te updaten of instellingen aan te passen, dan kunnen daders andere kwetsbaarheden gebruiken als aanvullende toegang tot het netwerk. Daders kunnen ook meerdere gebruikersaccounts hacken of aanmaken die dienen als (extra) achterdeur in het geval dat gebruikers hun wachtwoorden veranderen. Zo zag een forensisch onderzoeker:

"***Soms zijn er nieuwe accounts bijgemaakt zodat de hacker via die extra accounts erin kan. […] Dus je vermomt je als een normale beheerder, zeg maar. […] Dus stel je hebt drie admin accounts: admin1, admin2, admin3. En een hacker maakt admin4. […] Of we zagen [onlangs] een melding dat iemand […] een support account zag met de naam 'support' terwijl IT zeker weet dat ze die naam niet gebruiken. Ja, dan moet een hacker dat wel gedaan hebben.***"

3.3 Gegevens stelen

Het daadwerkelijk extraheren van gegevens is uiteindelijk een kwestie van enkele toetsaanslagen, of zoals een respondent het omschreef: "*Kopiëren. Uploaden*." Forensisch onderzoekers zagen daders de gegevens soms eerst comprimeren en in een archief of map zetten die vervolgens werd weggesluisd. Het wegsluizen zelf kunnen daders snel in grote hoeveelheden of juist langzamer in kleinere stappen doen. Kleinere datapakketjes vallen minder op omdat de extractie dan lijkt op normaal netwerkverkeer – iets wat uiteraard minder uitmaakt in organisaties met veel uitgaand netwerkverkeer. Waar daders de data naartoe sluizen, kan uit firewall logs of sporen op een server worden afgeleid mits organisaties de logs lang genoeg bewaren. Soms zagen de forensisch onderzoekers data verdwijnen naar servers in het buitenland, maar zij zagen ook

dat data werd geüpload naar bekende cloud-opslagdiensten. Welke gegevens daders gestolen hadden of waar zij op uit waren, is niet altijd duidelijk. Bij ransomware aanvallen lijken zij in ieder geval uit te zijn op gegevens waarmee ze de organisatie onder druk kunnen zetten, zoals persoonsgegevens of bedrijfsgeheimen.

3.4 Waar gaat het mis?

Uit de interviews bleek niet alleen hoe daders handelen in organisatiesystemen, maar ook waar organisaties regelmatig steken laten vallen in de beveiliging van hun data. Hoewel onbedoeld, creëren zij zo ook gelegenheden voor daders om in te breken en data te stelen. In deze paragraaf worden vier beveiligingsfouten besproken die respondenten regelmatig tegenkwamen tijdens hun werkzaamheden.

Ten eerste, het gebruik van slechte wachtwoorden. Zoals aangegeven in paragraaf 3.1 kwamen respondenten regelmatig makkelijk te raden of gelekte wachtwoorden tegen in hun onderzoeken. Enkele respondenten merkten ook op dat getroffen organisaties multifactor authenticatie (MFA) vaak niet hadden ingesteld. Als MFA is ingesteld, dan is een extra vorm van authenticatie nodig naast het invoeren van een gebruikersnaam en wachtwoord om in te loggen. Dit kan, bijvoorbeeld, een code zijn die tijdens het inloggen naar de telefoon van de gebruiker wordt gestuurd. Deze code moet de gebruiker vervolgens als extra inlogstap invoeren om toegang tot het systeem te krijgen.

Ten tweede, het onvoldoende updaten van applicaties. Nagenoeg alle respondenten benoemden het niet tijdig updaten van systemen, of het in gebruik houden van verouderde systemen, als andere belangrijke factor die organisaties kwetsbaar maakt voor aanvallen van buitenaf. Door systemen niet of onvoldoende te updaten, blijven bekende kwetsbaarheden in de software aanwezig die daders kunnen misbruiken.

Ten derde, geen of onvoldoende netwerksegmentatie toepassen. Netwerksegmentatie voorkomt inbraken niet, maar kan de schade na een inbraak wel beperken. Met het segmenteren van een netwerk worden digitale branddeuren tussen functionele delen van het netwerk geplaatst. Dit maakt het mogelijk netwerkgebruikers alleen toegang te geven tot die delen van het netwerk waar zij toegang toe horen te hebben voor hun werkzaamheden. Dankzij goede netwerksegmentatie zullen daders meer moeite moeten doen om door een netwerk te kunnen bewegen en grote hoeveelheden data te kunnen stelen. Zowel pentesters als forensisch onderzoekers hoorden echter soms dat beheerders het te veel moeite vonden om het netwerk te segmenteren of dat zij niet door hadden dat het netwerk niet goed was gesegmenteerd. Bijvoorbeeld, machines in een netwerk kunnen weliswaar in groepen zijn opgedeeld, maar als netwerkverkeer tussen de groepen nog steeds mogelijk is, dan is segmentatie onvoldoende toegepast. Zo verzuchtte een respondent: "*Overal staan de deuren wagenwijd open zodra je de voordeur binnen bent*."

Ten vierde, wel detecteren, maar niet reageren. Ook adequate detectie is een maatregel die vooral schade kan beperken na een inbraak. Meerdere respondenten gaven aan dat detectie een belangrijk risico is voor daders. Monitoringsystemen, zoals firewalls en antivirussoftware, geven meldingen wanneer zij ongewenste activiteiten of gevaarlijke bestanden detecteren. IT beheerders of beveiligers zouden hierop moeten reageren door de meldingen te onderzoeken en daar waar nodig actie te ondernemen. Bijvoorbeeld, door misbruikte poorten te dichten, kunnen daders hun toegang tot het netwerk verliezen waardoor zij opnieuw moeite moeten doen om in te breken. Respondenten gaven aan dat organisaties het monitoren echter niet altijd goed op orde hebben of niet altijd de capaciteit hebben om adequaat te reageren op dreigingsmeldingen:

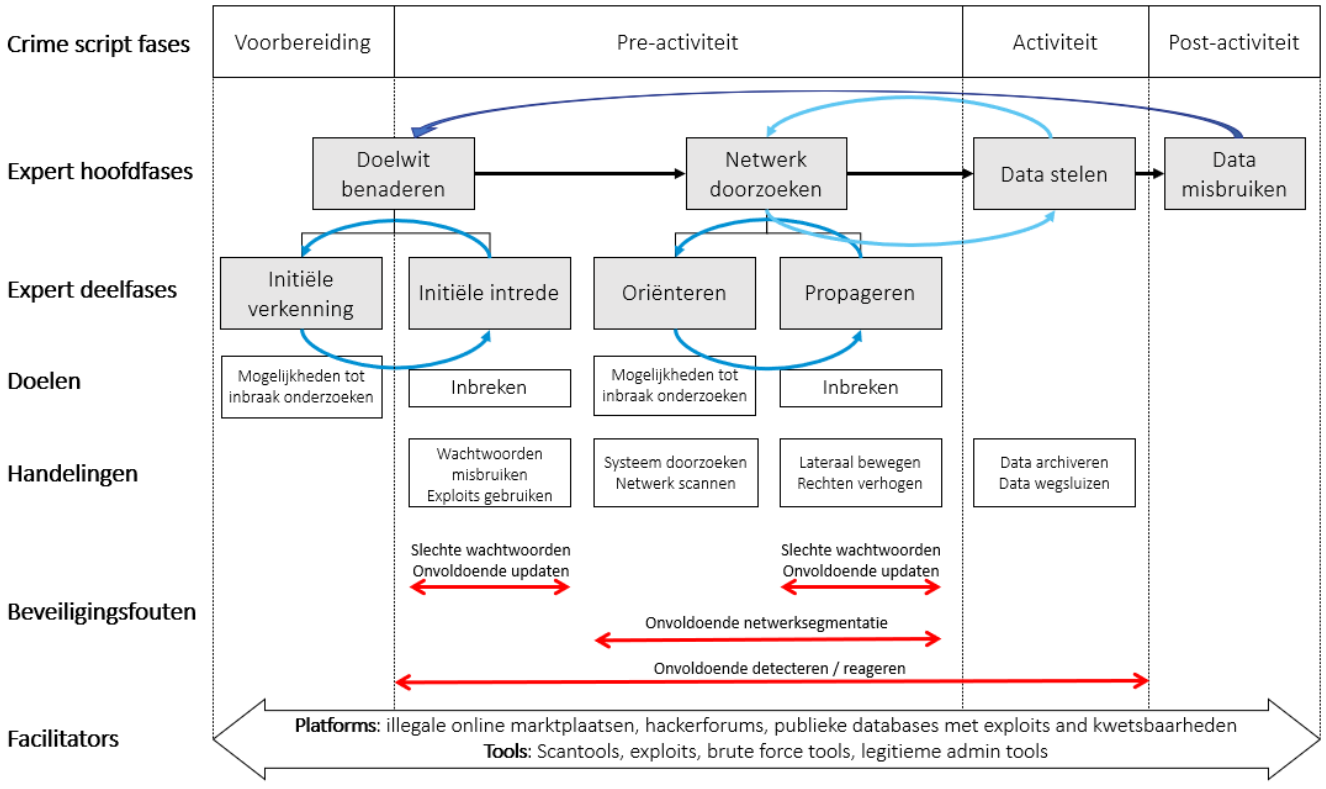
"*Dat zie je vaak bij klanten. Ze hebben van alles aangesloten, ze hebben een malwarescanner, antivirus, weet je wel. Best wel duur. Best wel in geïnvesteerd en dan is ook uitgezocht of dat het beste is. Maar dan worden de meldingen niet opgevolgd want daar heeft niemand tijd voor*."

Overigens lijken gelegenheden voor een succesvolle aanval vooral te worden gecreëerd door een *opeenstapeling* van dit soort menselijke fouten. Zo schetste een forensisch onderzoeker het volgende voorbeeld dat zij vaker zagen bij getroffen organisaties: Medewerker A probeerde samen met een leverancier een probleem op te lossen en zette daarvoor een poort open zodat de leverancier naar binnen kon. Uit haast werd de poort voor iedereen open gezet in plaats van alleen voor de leverancier. Bovendien stond die poort te lang open en controleerde niemand achteraf waarom die poort nog open stond. Medewerker B had bij een andere test een wachtwoord van een admin account gewijzigd naar een heel simpel wachtwoord. Vervolgens vond een brute force aanval plaats op de machine met de open poort en hadden de daders dat simpele wachtwoord geraden waardoor zij zo binnen kwamen met hoge rechten. Doordat hier verschillende personen verschillende fouten maakten waardoor verschillende gaten in de beveiliging ontstonden, hadden daders de gelegenheid om het netwerk te betreden.

3.5 Het crime script: handelingen, doelen en gelegenheidsstructuren

Om meer inzicht te krijgen in de procesmatigheid van het inbreken in netwerken, zijn de beschreven aanvalshandelingen in het vier-fase model van Tompson en Chainey gezet. Het resulterende diagram in Figuur 2 relateert de fases zoals beschreven door de experts aan de crime script fases. Daarbij zijn deze fases gelinkt aan doelen en gelegenheidsstructuren die het handelen van daders faciliteren. Merk op dat Figuur 2 één extra deelfase en twee extra hoofdfases laat zien: namelijk 'Initiële verkenning' respectievelijk 'Doelwit benaderen' en 'Data misbruiken'. Deze fases zijn niet eerder beschreven omdat deze buiten de reikwijdte van het onderzoek vallen. Bovendien vinden deze handelingen buiten het doelwit netwerk plaats waardoor respondenten hier minder over konden vertellen. Omdat deze fases toch af en toe ter sprake kwamen tijdens de interviews, worden deze hier wel kort toegelicht.

Figuur 2. Crime script diagram van datadiefstal uit organisatienetwerken.



Zoals te zien in het diagram, valt ‘Doelwit benaderen’ onder zowel de Voorbereiding- als de Pre-activiteitfase. ‘Initiële verkenning’ omvat verkennende handelingen waarbij daders uitzoeken welke doelwitten aantrekkelijk zijn om aan te vallen en hoe deze aangevallen kunnen worden. Pentesters en threat intel analisten gaven aan dat daders hiervoor gebruik kunnen maken van openbare tools en (semi-)openbare bronnen om informatie te verzamelen over potentiële doelwitten. Dit kan informatie zijn over organisaties en hun medewerkers, maar ook meer technische informatie over doelwitsystemen.

Bijvoorbeeld, online worden veelvuldig lijsten met zwakke wachtwoorden of zogenaamde ‘combolists’ met gelekte combinaties van wachtwoorden en gebruikersnamen gedeeld. Hiermee kunnen daders brute force aanvallen uitvoeren. Daders kunnen ook online zoekmachines gebruiken om technisch kwetsbare apparaten te vinden die verbonden zijn met het internet. Zo kunnen zij met de zoekmachine Shodan zoeken naar apparaten die specifieke kwetsbaarheden bevatten. Aan de hand van de zoekresultaten kunnen zij ongerichte aanvallen uitvoeren waarbij zij het dus niet zozeer op een bepaalde organisatie hebben gemunt, maar in eerste instantie zoeken naar apparaten waar zij makkelijk kunnen inbreken. Daarnaast kunnen zij met scantools inzichtelijk maken welke IP-adressen of subdomeinen organisaties gebruiken. Hieruit kan, onder andere, blijken of een organisatie een VPN-oplossing gebruikt. Via de VPN-oplossing en met gestolen inloggegevens kunnen daders vervolgens een initiële toegang verkrijgen.

De Initiële intrede valt onder de Pre-activiteit fase omdat hier een concreet doelwit wordt aangevallen. Het oriënteren en propageren vallen om diezelfde reden ook in deze fase en dienen als aanloop naar de Activiteit, namelijk het stelen van gegevens. Na het stelen van gegevens hoeven daders het organisatienetwerk niet direct te verlaten, zoals blijkt uit zaken waarin daders al maanden, zo niet jaren, in organisatiesystemen zaten. De Post-activiteitfase is hier daarom niet zozeer een fase waarin daders de plaats delict verlaten of de uitvoering van een misdrijf afronden, maar een fase die vooral beschrijft welke handelingen zoal volgen op het stelen van gegevens. Respondenten gaven hierbij voorbeelden zoals het te koop aanbieden van gestolen gegevens of de gegevens gebruiken om organisaties af te persen. Hoewel dit de laatste fase in het crime script is, kan deze fase dus ook parallel lopen aan de andere fases wanneer daders gedurende langere tijd in een netwerk zitten.

Parallelle processen en herhalende handelingen werden regelmatig beschreven door respondenten. Zo kan het bij de initiële intrede nodig zijn om meerdere kwetsbaarheden na te lopen voordat de inbraakpoging slaagt. Ook om rechten te verhogen moeten daders soms steeds opnieuw inbreken op verschillende machines. Bovendien, hoewel ‘Oriënteren’ in het diagram als handeling onder ‘Netwerk doorzoeken’ valt, kunnen daders herhaaldelijk oriënterend gedrag vertonen gedurende het inbraakproces. Zo legt een respondent uit dat daders bij een ongerichte aanval soms pas later in het proces uitzoeken waar zij hebben ingebroken:

“Je ziet in verschillende fases oriënterend gedrag. In het begin natuurlijk op systeemniveau of op netwerkniveau dat ze aan het ontdekken zijn waar ze zitten. En later in latere fases, dus bijvoorbeeld bij de data-extractie, zie je dat ze ook op zoek zijn naar logo’s en naar jaarrekeningen, ook om te kijken van oké wat kunnen we hier überhaupt [aan losgeld] vragen?”

In dit voorbeeld proberen daders uiteindelijk de hoogte van het losgeld bij een ransomware aanval aan te passen aan de jaaromzet van de organisatie door uit te zoeken wat de jaaromzet is. Zo kunnen zij voorkomen dat zij een organisatie overvragen. Het cyclische karakter van het zoeken naar nuttige informatie is echter terug te zien bij iedere inbraak in een netwerk, ongeacht of de aanval gericht of ongericht is:

"Eigenlijk is het proces van wat een hacker doet vaak eerst informatie verzamelen, dan kijken wat kan ik ermee en de aanval bedenken, aanval uitvoeren. Vervolgens ben je wat verder, opnieuw informatie verzamelen en dat blijf je eigenlijk doen totdat je helemaal binnen bent."

De verschillende *loops* in het proces zijn ook weergegeven in Figuur 2. Deze loops impliceren ook dat het stelen van gegevens niet alleen plaatsvindt nadat daders het netwerk hebben doorzocht. Daders kunnen vanaf het moment dat zij een netwerk hebben geïnfiltreerd zoeken naar gegevens en deze extraheren uit de systemen. Zij kunnen, bijvoorbeeld, vroeg in het proces wachtwoorden stelen om verder in het netwerk te komen en pas later documenten bemachtigen die afgeschermd waren voor accounts met lagere rechten.

In het diagram zijn de fases ook gekoppeld aan doelen die daders logischerwijs bij iedere fase hebben. Ook hieruit volgt het repetitieve karakter van het inbraakproces. Bij zowel het vooronderzoek als de latere oriëntatie zoeken daders naar mogelijkheden om in te breken. Bij zowel de initiële intrede als het propageren breken daders in. Als het inbreken niet direct lukt of als daders op meerdere systemen proberen in te breken, zullen zij opnieuw moeten zoeken naar manieren om in te breken. Ten slotte vormt het volledige crime script één grote cyclus waarbij de gestolen gegevens dienen als input voor volgende inbraken. Zo kunnen daders, bijvoorbeeld, gestolen persoonsgegevens gebruiken voor nieuwe phishing aanvallen.

4. Discussie

Hoewel datadiefstal grote gevolgen kan hebben voor organisaties en bijdraagt aan een reeks andere vormen van cybercriminaliteit, is er relatief weinig bekend over hoe datadieven gegevens uit organisatienetwerken stelen. Dit onderzoek beschrijft dit proces van datadiefstal vanuit criminologisch perspectief. De toegepaste crime script analyse laat patronen zien in het inbraak- en diefstalproces die specifieke technieken en technologieën overstijgen. Dit laatste hoofdstuk beschrijft eerst in hoeverre de resultaten van dit onderzoek overeenkomen met eerder onderzoek naar het gedrag van kwaadwillende hackers die organisatienetwerken aanvallen. Daarbij wordt ook ingegaan op hoe de resultaten nieuw licht werpen op het begrip van criminaliteit in het algemeen. Ter afsluiting volgt een bespreking van enkele beperkingen van dit onderzoek en een korte conclusie.

4.1 Een beter begrip van criminaliteit

Allereerst komen de resultaten van dit onderzoek deels overeen met de digitale dreigingsmodellen. Bijvoorbeeld, net als in het MITRE ATT&CK raamwerk bespraken de respondenten, onder andere, de initiële intrede en het verhogen van rechten. Dat de respondenten deze concepten benoemden, is niet toevallig. Het raamwerk vormt namelijk een 'taal' die specialisten gebruiken om aanvallen te duiden en om hierover te communiceren. Het crime script vormt ook een taal die verschillende partijen kunnen gebruiken om hun kennis op een gestructureerde manier te delen.[27] Daar waar het MITRE ATT&CK raamwerk echter vrij technisch is, kan het crime script beter begrepen worden door personen met minder technische kennis. Dit is belangrijk omdat niet-IT'ers uit diverse disciplines, zoals de sociale wetenschappen en rechtsgeleerdheid, een belangrijke bijdrage kunnen leveren aan de aanpak van cybercriminaliteit, mits zij begrijpen hoe daders hun aanvallen uitvoeren.

[27] Warren, S., Oxburgh, G., Briggs, P., & Wall, D. (2017). How might crime-scripts be used to support the understanding and policing of cloud crime? In T. Tryfonas (Ed.), *Human Aspects of Information Security, Privacy and Trust* (539–556). Springer International Publishing.

Daarnaast sluit dit onderzoek aan bij eerder onderzoek waarin is beschreven hoe illegale online platforms bijdragen aan de verspreiding van hacking tools en diensten, en gestolen data.[28,29] Dit onderzoek laat echter ook zien dat reguliere of legale online platforms inbraken en datadiefstal faciliteren. Daarnaast komen de verschillende expert fases in het crime script ook in grote lijnen terug in onderzoeken naar ransomware aanvallen.[30,31] Opvallend is dat deze onderzoeken digitale aanvallen als een rechtlijnig proces beschrijven terwijl dit onderzoek duidelijk cyclische patronen laten zien. Dit roept vragen op over de manier waarop nu wordt gekeken naar criminele processen.

Het feit dat eerdere onderzoeken deze cyclische patronen vaak niet beschrijven doet vermoeden dat onderzoekers dit gedrag vaak ook niet zien. Dat is niet verrassend. In het geval van fysieke criminaliteit wordt vaak alleen vastgesteld wat daders wél hebben gedaan en niet welke pogingen zijn mislukt. Mislukte pogingen leiden immers niet altijd tot "criminaliteit". Bijvoorbeeld, een mislukte diefstal is geen diefstal en wordt dus vaak niet meegenomen in onderzoek naar diefstal. Daarnaast zijn mislukte pogingen of deels uitgevoerde intenties niet altijd goed waar te nemen. Inbrekers kunnen, bijvoorbeeld, verschillende kamers doorzoeken, maar laten mogelijk niet in alle kamers duidelijke sporen achter. Door een beperkt observatievermogen in de fysieke wereld wordt dadergedrag dus waarschijnlijk vaak onvoldoende gedetailleerd onderzocht. Dit leidt tot hiaten in politieonderzoek wat resulteert in hiaten in wetenschappelijk onderzoek dat is gebaseerd op politiedata, wat vaak het geval is in criminologisch onderzoek.

Een groot voordeel van digitaal forensisch onderzoek is dat hiermee, mits er goed gelogd is, het handelen van daders met grote nauwkeurigheid kan worden gereconstrueerd. Deze reconstructies kunnen zelfs nauwkeuriger zijn dan wanneer daders hun aanval in een interview zouden navertellen. Ook hun geheugen kan hiaten bevatten. Bovendien is met digitaal forensisch onderzoek niet alleen te zien welke handelingen hebben geleid tot een succesvolle aanval, maar ook welke handelingen wél zijn uitgevoerd, maar niet direct leidden tot een succesvolle aanval. Analyse van zowel succesvolle als deels gefaalde aanvallen kan interessante inzichten opleveren. Succesvolle aanvallen verschaffen inzicht in waar het aan beveiliging schortte. Daarentegen kunnen deels gefaalde aanvallen inzicht verschaffen in de effectiviteit van preventiemaatregelen en mogelijk onverwachte hindernissen voor daders aan het licht brengen.

4.2 Beperkingen

Ondanks de waardevolle inzichten die dit onderzoek oplevert, kent het ook enkele beperkingen. Een eerste beperking van dit onderzoek is dat dadergedrag deels is afgeleid uit handelingen van pentesters. Net als kwaadwillende aanvallers proberen pentesters kwetsbaarheden in organisatiesystemen- en netwerken te vinden. Het is alleen de vraag in hoeverre het gedrag van pentesters overeenkomt met het gedrag van daders. Zo hoeven pentesters niet te vrezen voor de politie en zijn zij vaak zelfs gewhitelist door organisaties om te voorkomen dat monitoringsystemen onnodig alarm slaan. Dit maakt dat pentesters mogelijk anders te werk gaan dan kwaadwillenden.

De geïnterviewde pentesters gebruikten echter vaak dezelfde of soortgelijke tools en technieken bij hun werkzaamheden, wat bevestigd werd door de forensisch onderzoekers. Daar waar pentesters duidelijk anders handelden dan kwaadwillenden, gaven zij dit aan en lichtten dat toe. Bijvoorbeeld, pentesters

---

[28] Mirian, A., DeBlasio, J., Savage, S., Voelker, G. M., & Thomas, K. (2019). *Hack for hire: Exploring the emerging market for account hijacking*. The World Wide Web Conference '19, San Francisco, CA, USA.

[29] Madarie, R., Ruiter, S., Steenbeek, W., & Kleemans, E. (2019). Stolen account credentials: An empirical comparison of online dissemination on different platforms. *Journal of Crime and Justice, 42*(5), 551–568.

[30] Matthijsse, S. R., Van 'T Hoff-de Goede, M. S., & Leukfeldt, E. R. (2023). Your files have been encrypted: A crime script analysis of ransomware attacks. *Trends in Organized Crime*.

[31] Wall, D. S. (2021). The Transnational Cybercrime Extortion Landscape and the Pandemic: Changes in ransomware offender tactics, attack scalability and the organisation of offending. *European Law Enforcement Research Bulletin, 22*.

scannen netwerken net als kwaadwillenden, maar laten de scanner vaak sneller draaien omdat zij dus minder hoeven te vrezen voor detectie. Daarnaast zijn de verhalen van pentesters ook gestaafd met de verhalen van andere respondenten, zoals de forensisch onderzoekers. Desalniettemin zou het interessant zijn om de resultaten van dit onderzoek te vergelijken met verhalen van kwaadwillende hackers over hoe zij inbreken in organisatienetwerken en daar data uit stelen.

Een tweede beperking relateert aan de mogelijke generaliseerbaarheid van dit onderzoek. Hoewel meerdere respondenten ervaring hadden met digitale inbraken bij andere organisaties, is de meeste informatie in dit onderzoek gebaseerd op opgedane kennis en ervaring bij NFIR. Ten tijde van de interviews bediende NFIR voornamelijk het MKB en (semi-)publieke organisaties. Het is daarom de vraag in hoeverre de gevonden patronen te generaliseren zijn naar inbraken in veel grotere of buitenlandse organisaties. Dit onderzoek laat echter belangrijke overeenkomsten zien met eerdere onderzoeken naar digitale inbraken en datadiefstal. Bovendien is deze steekproef juist een kracht van dit onderzoek. Veel eerder criminologisch onderzoek naar het gedrag van online inbrekers is gebaseerd op politiedata en jurisprudentie, of juist van kwantitatieve aard.[32,33] Bedrijven stappen echter niet snel naar de politie wanneer zij getroffen zijn door een digitale aanval.[34] Daarnaast verschaft dit kwalitatieve onderzoek diepgaand inzicht in gedragingen en gelegenheidsstructuren die niet altijd goed te vatten zijn in getallen of die eerder over het hoofd werden gezien, zoals de *loops* en de rol van legitieme online platforms. Dit onderzoek vormt daarom een waardevolle aanvulling op eerder onderzoek naar digitaal dadergedrag.

4.3 Conclusie

Onderzoek naar digitale inbraken en datadiefstal is vaak vrij technisch. Met dit onderzoek is vanuit criminologisch perspectief het gedrag van datadieven die inbreken in organisatienetwerken bestudeerd. Met behulp van een crime script analyse zijn patronen in dit gedrag gedestilleerd die specifieke technieken en technologieën overstijgen. Het resulterende crime script beschrijft de verschillende stappen die daders zetten, van de initiële intrede en het doorzoeken van een netwerk tot aan het stelen van data. In tegenstelling tot eerder onderzoek laten de resultaten van dit onderzoek duidelijk zien dat dit proces meerdere *loops* omvat. Daders vertonen herhaaldelijk soortgelijke gedragingen en doen regelmatig een stap terug om uiteindelijk verder te komen met hun aanval. De verschillende gedragingen worden daarbij gefaciliteerd door veelvoorkomende beveiligingsfouten die organisaties maken en diverse illegale én legale online platforms. De nieuwe inzichten die dit onderzoek oplevert, verschaffen niet alleen meer inzicht in cybercriminaliteit, maar ook in criminele processen in het algemeen. Daar waar fysieke criminaliteit vaak deels onzichtbaar blijft, kunnen digitale inbraken veel beter worden gereconstrueerd. Dit biedt interessante mogelijkheden voor toekomstig onderzoek om criminaliteit beter te begrijpen en effectievere interventiestrategieën te ontwikkelen.

---

[32] **Zie bijv.** Fisher, D., Maimon, D., & Berenblum, T. (2021). Examining the crime prevention claims of crime prevention through environmental design on system-trespassing behaviors: A randomized experiment. *Security Journal, 35*(2).

[33] **Of zie bijv.** Holt, T. J., Turner, N. D., Freilich, J. D., & Chermak, S. M. (2022). Examining the Characteristics That Differentiate Jihadi-Associated Cyberattacks Using Routine Activities Theory. *Social Science Computer Review, 40*(6), 1614–1630.

[34] European Commission (2022). *Flash Eurobarometer 496: SMEs and cybercrime*. Publications Office of the European Union.