Crime chain: het verband tussen DDoS-aanvallen en Phishing

M. Junger, Abhishta Abhishta, L.J.M. Nieuwenhuis

Universiteit Twente

Maart 2021

Call Politie en Wetenschap 2018

Voorwoord

De auteurs danken Erik Kemp en Michelle Peters voor hun hulp bij de eerste stappen in de analyses. Ook zijn wij dank verschuldigd aan de leden van de begeleidingscommissie, in het bijzonder Richard Nijeboer, voor zijn adviezen bij het formuleren van de discussie en de beleidsaanbevelingen. Eveneens veel dank aan Tom Meurs en Hans Hendrickx voor hun kritische en secure lezing van het eerdere versies van het manuscript.

Leesijzer

Voor de leesbaarheid zijn een aantal teksten in kaders (boxen) geplaatst. Hierin staat meer informatie over de statistische analyse, en zijn voorbeelden opgenomen van bijzonder DDoS en phishing combinaties.

1. Onderzoeksonderwerp, de belangrijkste onderzoeksvraag en doelstelling

De huidige studie onderzoekt het bestaan van online criminaliteit-sequenties, ofwel '*crime chains'*. Misdaadketens zijn reeksen van verschillende soorten delicten die samen, of in een bepaalde volgorde, voorkomen en met elkaar verband houden om een gecoördineerde reeks acties uit te voeren. Voor de offline wereld spreekt Felson over '... de opeenvolging van gebeurtenissen voor doorlopende criminele samenwerking' (Felson, 2006, p. 16). Felson heeft ze de 'Van Dijk' chain genoemd, naar Jan van Dijk, voormalig hoofd WODC (Felson & Clarke, 1998a; Van Dijk, 1994). Zo kunnen specifieke delicten voorwaarden scheppen voor nieuwe delicten. In de huidige studie onderzoeken wij of er een statistisch verband bestaat tussen Distributed Denial-of-Service (DDoS) -aanvallen en phishing. Tot op heden zijn de meeste online delicten elk afzonderlijk bestudeerd. Er zijn studies naar phishing, DDoS enz. Maar tot op heden zijn deze delicten nooit, voor zover ons bekend, in combinatie onderzocht.

Hieronder beginnen wij met een algemene beschrijving van de voordelen van ICT en het internet voor criminaliteit en wordt beschreven hoe deze voordelen online criminaliteit en samenwerking tussen aanvallers faciliteren. Vervolgens gaan wij dieper in op phishing en DDoS-aanvallen. Tenslotte geven wij aan waarom er verbanden zouden kunnen zijn tussen een aantal cyberdelicten, zoals phishing e-mails en DDoS aanvallen en beschrijven wij de achtergrond van de huidige studie.

1.1 Online criminaliteit en de faciliteiten van het internet

Het internet biedt uitgebreide mogelijkheden om delicten te plegen en te faciliteren. Het is van belang deze kort te bespreken om te begrijpen waarom en hoe coördinatie tussen delicten mogelijk is.

1.1.1 Het open internet

Het is niet moeilijk om in te zien dat criminelen allereerst gebruik maken van het open internet en alle ICT-faciliteiten die beschikbaar zijn voor iedereen. Legale ICT en het open internet bieden allerlei zaken legaal aan die criminaliteit faciliteren. Men kan denken aan legaal beschikbare PGP-telefoons die encryptie gebruiken en daardoor volledig veilige communicatie aanbieden, 'spyware' en legale forums waar men ook illegale goederen kan aanbieden (Bijlenga & Kleemans, 2018; Zabyelina, 2017). Zo slagen criminelen er in om zoekmachines, zoals Bink of Yahoo, te gebruiken om illegale goederen zoals illegale medicijnen, te promoten (Zabyelina, 2017).

1.1.2 TOR, het Dark web en het Darknet

De Tor-technologie is halverwege de jaren negentig ontwikkeld door militaire onderzoekers in de VS. 'Tor' staat voor 'The Onion Router' (McCoy, Bauer, Grunwald, Kohno, & Sicker, 2008; Woollaston, 2020). Het werd door inlichtingenofficieren gebruikt om anoniem bestanden te delen.

Het Darknet is het versleutelde deel van internet dat alleen toegankelijk is met behulp van specifieke software die op zichzelf niet crimineel is. Het gaat bijvoorbeeld om de Tor-browser, maar ook I2P, Zeronet, Freenet, of Openbazaar. Binnen het Darknet bevinden zich de vele criminele websites en services die op deze netwerken worden gehost (IOCTA, 2019, p. 45).

Met het bestaan van TOR en het *dark web* wordt anonieme communicatie mogelijk. Het dark web is een marktplaats en een voedingsbodem voor criminaliteit (Finklea, 2015; Kaur & Randhawa, 2020; Kirkpatrick, 2017). Het gaat om een uitgebreide reeks van ernstige vormen van criminaliteit, zoals de verkoop van criminele producten en diensten, inclusief drugs, kinderpornografie, wapens en explosieven, gecompromitteerde gegevens en kredietkaarten, malware, namaakgoederen, valuta en vervalste documenten (IOCTA, 2019). Zo werden bijvoorbeeld 23 miljoen gestolen creditcards te koop aangeboden op het dark web in de eerste helft van 2019 (IOCTA, 2019).

Daarnaast biedt het dark web allerlei andere faciliteiten aan, die criminaliteit op vele manieren faciliteert. Het fungeert als ontmoetingsplaats voor criminelen en terroristen, en maakt het kopen en verkopen van criminele diensten mogelijk, zoals crime-as-a-service (zie hieronder).

1.1.3 Botnets

Een "botnet" is een collectie van "bots". *Een bot is een computerprogramma dat op een autonome manier taken kan uitvoeren die normaal door mensen uitgevoerd worden. De bot kan bijvoorbeeld een computerspel spelen, een webpagina raadplegen, chatten, of een bericht op een site (bijvoorbeeld een forum of wiki) plaatsen*. Hierdoor ontstaat een enorme slagkracht aan IT capaciteit (Ianelli & Hackworth, 2005). Een botnet ontstaat als aanvallers er in slagen bots te installeren op met het internet verbonden apparaten. Vaak zijn de gebruikers van deze apparaten zich niet bewust dat er bots op hun systeem draaien. Het aantal bots in een botnet is in de orde van grootte van honderdduizenden aangesloten apparaten (Antonakakis et al., 2017).

Botnets kunnen worden gebruikt om een reeks aan illegale activiteiten uit te voeren, zoals Distributed Denial-of-Service (DDoS) -aanvallen, gegevens te stelen, spam te verzenden, andere aanvallers toegang te geven tot computers, om op hun beurt weer

spam en phishing e-mails te verzenden en malware te verspreiden (Goodman, 2017; Wainwright & Kettani, 2019). De eigenaar, of de bot *administrator*, ook wel de bot-herder genoemd, kan het botnet besturen met behulp van Command and Control-software (C&C). Voor een overzicht zie (Hyslip, 2020). Bij botnets komt dus een variëteit aan afzonderlijke delicten samen (Goodman, 2017; Wainwright & Kettani, 2019).

Voor Nederland schatten van Eeten, Asghari, Bauer, and Tabatabaie (2011) voor 2010 dat 5% à 10% van alle machines onderdeel zouden zijn van een botnet, en dat was een ondergrens, aldus de auteurs. Vermoedelijk is dit aantal wat afgenomen, volgens (van Eeten, Lone, Moura, Asghari, & Korczyński, 2016) dankzij betere pr*event*ie. Maar regio's in de wereld met minder goede *security* zijn relatief kwetsbaar voor het infecteren van computers die vervolgens onderdeel worden van een botnet (Antonakakis et al., 2017).

Er bestaan studies naar beruchte botnets en aanvallen. Grote botnets beslaan meerdere landen en zijn een voorbeeld van het internationale karakter van de online criminaliteit. Bij een groot botnet als het Mirai botnet stonden de geïnfecteerde computers vooral in Zuid-Amerika en Azië: '*the bulk of Mirai infections stemmed from devices located in Brazil (15.0%), Columbia (14.0%), and Vietnam (12.5%)* (Antonakakis et al., 2017). Maar de doelen waren Westerse bedrijven, volgens *Krebs on Security* (Antonakakis et al., 2017).

Op dit moment bestaan de grote botnets vooral uit Internet-of-Things (IoT) -apparaten. Een recente studie bestudeerde deze botnets over een periode van 23 maanden. Het beeld dat naar voren komt, is dat van 'wegwerp botnets' (Tanabe et al., 2020). Een IoT-botnet wordt niet zozeer onderhouden, maar steeds helemaal opnieuw samengesteld. Ook de *Command & Control* servers hebben een korte levensduur. In deze formule wordt een botnet onmiddellijk na het samenstellen ervan gebruikt en vervolgens verlaten. Hoewel IoT-botnets minder geavanceerd lijken dan 'gewone' botnets, hebben zij, als voordeel van eenmalig gebruik, dat ze zeer goed bestand zijn tegen blacklisting[1] en *Command & Control* verwijdering (Tanabe et al., 2020).

1.1.4 Cryptomunten

Er bestaan inmiddels een hele serie van cryptomunten, zoals Bitcoin, Ethereum, Litecoin, Altcoins enz. Dankzij deze cryptomunten is online en anoniem betalen makkelijk geworden. Hoewel er wordt geprobeerd om cryptomunten als 'normale' valuta voor te stellen, zijn er belangrijke problemen aan gekoppeld. Ten eerste zijn cryptomunten

[1] Blacklisting is het proces van het op de zwarte lijst zetten van applicaties die gevaarlijk en ongewenst zijn en omvat het creëren van een lijst met alle applicaties of uitvoerbare bestanden die een bedreiging voor het netwerk kunnen vormen, hetzij in de vorm van malware-aanvallen, hetzij simpelweg door de productiviteit te belemmeren.

gevoelig voor prijsschommelingen. Deze prijsvolatiliteit hangt samen met twee essentiële kenmerken van cryptomunten: 1) het gebrek aan regelgeving; en 2) de link met cybercriminaliteit. De link met cybercriminaliteit is tweeledig. Cryptomunten faciliteren criminaliteit dankzij de anonimiteit en het gebrek aan toezicht. Daarnaast zijn diegenen die cryptomunten bezitten of ermee handelen een gewild doelwit voor criminelen, voor fraude en hacking (zie ook hieronder). Voor een uitstekend overzicht, zie Corbet, Lucey, Urquhart, and Yarovaya (2019).

Ook voor phishing (zie Sectie 1.2) en DDoS-As-A-Service (DaaS) helpen de crypto-munten, omdat de ontvangers van het geld anoniem kunnen blijven. De meest populaire betaalmethoden die worden gebruikt door de DaaS-providers waren PayPal en Bitcoin (Jirovský, Pastorek, Mühlhäuser, & Tundis, 2018).

1.1.5 Samenwerking tussen aanvallers Crime-as-a-Service

Aanvallers werkten vroeger en werken nog altijd samen (Kleemans & Soudijn, 2017; Levi & Maguire, 2004). Het internet heeft deze samenwerking in al zijn vormen verder gefaciliteerd, door, onder meer, het gemakkelijker leggen van contacten, anonimiteit en anonieme ontmoetingsplaatsen, zoals hierboven is beschreven (Leukfeldt, Kleemans, & Stol, 2016; Leukfeldt, Kleemans, & Stol, 2017). Daarnaast blijkt dat aanvallers vaker internationaal actief zijn naarmate ze over meer technische kennis beschikken (Leukfeldt et al., 2016; Leukfeldt, Kleemans, et al., 2017). Dit betekent dat er een wereldwijde criminele markt ontstaat en internationale samenwerking tussen criminelen makkelijk wordt, waarmee hun slagkracht enorm kan toenemen (Hyslip, 2020).

Crime-as-a-Service is een optimale vorm van samenwerking om gezamenlijk delicten te kunnen plegen. Aanvankelijk was online criminaliteit iets voor criminelen met veel technische kennis. Soms waren dit de *white hat hackers* ofwel de ethische hackers, individuen gedreven door nieuwsgierigheid en onderzoek. Maar tegenwoordig zijn er tools beschikbaar voor allerlei taken en kan een niet-technisch geschoolde gebruiker diensten en 'tools' online huren of aanschaffen die hem helpen om allerlei delicten te plegen (de Santanna, 2017; Hyslip & Holt, 2019; Jonker et al., 2017; Maestre-Vidal, Sotelo-Monge, Martínez-Monterrubio, Barona-López, & Valdivieso-Caraguay, 2019)}. Hiermee is het vermogen om online criminaliteit te plegen exponentieel gegroeid. Vaak is het voor de technische specialisten winstgevender en minder riskant om een *tool* voor cybercriminaliteit als een dienst te verkopen dan de misdaad zelf te plegen (zie Hyslip (2020) voor een overzicht).

De cybercrime-as-a-Service-activiteiten omvatten nu een ruime verscheidenheid aan cyberdelicten, waaronder het huren van botnets, gedistribueerde denial of service-aanvallen (DDoS), creditcardfraude, malware, spam en phishing-aanvallen. Deze

diensten worden verhuurd of verkocht via hackerforums, directe webverkoop en op het dark web en meestal betaald met cryptomunten (Hyslip, 2020; Putman, Abhishta, & Nieuwenhuis, 2018).

Zoals ook hieronder wordt uitgelegd, is het huren van deze diensten meestal niet duur. Met $20 voor het huren van een botnet voor een maand kom je al een eind (de Santanna, 2017; Hyslip, 2020). Of deze tools of diensten altijd doen wat ze beloven is een tweede (zie hieronder).

Crime-as-a-Service heeft hiermee geleid tot de ontwikkeling van kettingstructuren en verdeelde verantwoordelijkheden (Kruisbergen, Leukfeldt, Kleemans, & Roks, 2018, p. 9) en tot nieuwe criminele economische structuren, ook wel 'ecosystemen' genoemd, waarbij cryptovaluta de betaling vergemakkelijkt (Huang, Siegel, & Madnick, 2017; Kruisbergen et al., 2018; Manky, 2013; Thomas et al., 2015).

Binnen dit ecosysteem spelen s*tressers* en *booters*[2] een belangrijke rol met betrekking tot DDoS-aanvallen. Beiden kunnen worden gebruikt om – op verzoek – aanvallen uit te voeren op de door de aanvaller gekozen doelen. Deze diensten zijn online te huur en zijn – in beginsel – niet illegaal. Het is dus gewoon 'te googelen' (de Santanna & Sperotto, 2014; de Santanna et al., 2015; Noroozian et al., 2016). Veel geld per aanval kosten ze niet, zij zijn verkrijgbaar vanaf $1 (de Santanna et al., 2015; Zand et al., 2017); en de verhuurders kunnen er vaak wel relatief goed mee verdienen (Brunt, Pandey, & McCoy, 2017; Hyslip & Holt, 2019). Opmerkelijk is dat je vaak geen waar voor je geld krijgt, omdat dat de aanval nauwelijks plaatsvindt (de Santanna et al., 2015; Hyslip & Holt, 2019; Zand et al., 2017). de Santanna et al. (2015) probeerden dit uit en vijf van de 14 booters leverde geen aanval op.

1.1.6 Internationale samenwerking

Uit de beschrijving hierboven blijkt dat een groot deel van de online delicten een internationaal karakter heeft, maar dit kan verschillen per type misdrijf. Bij DDoS is dat vaak het geval, zoals hierboven is besproken. Bij phishing die Nederlandse gebruikers bereiken blijkt dat 22% van de phishing e-mails niet in het Nederlands zijn geschreven (Lastdrager, 2018). Onder Nederlandse slachtoffers van CEO-fraude bleek dat bij 63% van de aanvallen een niet-Nederlands Europees banknummer was vermeld en in 35%

[2] Een IP-stresser is een hulpmiddel dat als doel heeft om een netwerk of server te testen op robuustheid. Booters, ook wel *booter services* genoemd, zijn on-demand DDoS-aanvallen (Distributed-Denial-of-Service) die worden aangeboden door criminelen om websites en netwerken plat te leggen. Met andere woorden, booters zijn het onwettige gebruik van IP-stressers (Cloufare, 2020).

van de aanvallen gebruik was gemaakt van bank in Azië (Junger, Wang, & Schlomer, 2020).

Uit het phishing-stappenplan (zie hieronder) blijkt dat op verschillende momenten samenwerking met andere criminelen nodig kan zijn om phishing mogelijk te maken en dat deze samenwerking gemakkelijk op het dark web kan ontstaan. Hiermee ontstaat een online 'ecosystem' van producten en diensten dat allerlei criminele activiteiten mogelijk maakt, ook voor 'non-techies'. Het verhuren dan wel verkopen van programma's of diensten voor online crime heet ook wel 'Crime-as-a-Service' (zie hierboven).

1.1.7 Social engineering

Social engineering is een niet-technische aanval gebaseerd op menselijke interactie, als onderdeel van een groter geheel van aanvallen gericht op een ICT-systeem. Social engineering kan worden uitgevoerd via de telefoon, e-mail, sms-berichten of door middel van persoonlijk contact (voor een overzicht, zie (Bullée & Junger, 2020a, 2020b). Veel online delicten bevatten elementen van fraude en misleiding, ofwel 'social engineering' (Verizon Risk Team, 2019). Aanvallers gebruiken misleiding, bedrog en andere overtuigingstechnieken als aanvalstactiek om slachtoffers gevoelige informatie te laten delen of acties uit te laten voeren waar zij zelf ongemerkt de dupe van worden (Gupta e.a. 2011). Door slimme trucs proberen zij iets van iemand te krijgen: persoonlijke informatie, login-informatie van de bank. Het uiteindelijke doel is meestal geld.

Social engineering wordt beschouwd als één van de belangrijkste online gevaren omdat mensen erg bevattelijk blijken te zijn voor misleiding (Bullée & Junger, 2020a, 2020b; Junger, Montoya-Morales, & Overink, 2017). Social engineering-aanvallen lijken op het eerste legitiem en ongevaarlijke berichten of verzoeken. Hierdoor is de gebruiker zich er vaak in eerste instantie niet van bewust een slachtoffer te zijn (Hadnagy, 2014). Daarom is vaak gesteld dat de mens de zwakste schakel is in informatiebeveiliging (Schneier, 2000).

Een groot probleem, zeker met betrekking tot pr*event*ie en het waarschuwen van gebruikers, is dat er eindeloos veel mogelijkheden zijn voor social engineers (Bullée & Junger, 2020a). De enige beperking is de verbeelding van de aanvallers.

Het succes van social engineering hangt dan ook vooral af van de 'kwaliteit' van de aanval en de wijze waarop hij wordt uitgevoerd. Daarom variëren de 'succespercentages' (succes vanuit het oogpunt van de aanvaller) enorm (zie ook hieronder, de succespercentages van phishing) (Bullée & Junger, 2020a). De succespercentages kunnen uiteen lopen van bijna 0% naar soms meer dan 80% (Sokol e.a. 2017;

Vishwanath 2015; Wright e.a. 2014; Yang e.a. 2017). In persoonlijke verhalen vertellen professionele *penetration* testers vaak dat de kans dat zij ergens binnen komen nagenoeg 100% is.

Social engineering en rampen.

Fraudeurs hebben vaak 'profijt' gehad van rampen (Aguirre & Lane, 2019). Ter illustratie: aanvallers hebben uitgebreid gebruik gemaakt van de Covid-19 crisis om phishing e-mails te ontwerpen. De *Anti-phishing Working Group* (APWG) heeft deze berichten in een aantal categorieën ingedeeld (APWG, 2020c).

1) Zoom phishing e-mails. Tijdens de pandemie verdubbelde het aantal Zoom-gebruikers. Zij werden potentiële slachtoffers van phishing e-mails die van hun account informatie wilde stelen. In andere e-mails probeerde aanvallers gebruikers te verleiden het Zoom programma te downloaden, natuurlijk kregen zij malware in plaats van Zoom.

2) Frauduleuze CEO e-mails[3]*met een verwijzing naar Covid-19*. In CEO-fraude richt een aanvaller zich op werknemers die toegang hebben tot de bedrijfsfinanciën, meestal door hen een e-mail te sturen vanaf een nep of gecompromitteerd e-mailaccount, om, met een smoes, hen te verzoeken geld over te maken. Tijdens de pandemie is de Covid-19 crisis de aanleiding om een 'nieuwe' bankrekeningnummer te versturen waarop geld moet worden gestort, of om geld te laten storten op een rekeningnummer die bestemd is voor 'de slachtoffers van de pandemie'.

3) Phishing e-mails gericht op zorginstellingen. Op 26 maart bleek dat ransomware-aanvallen op zorginstellingen 35 procent hoger waren dan in dezelfde periode van 2016 tot en met 2019. De achtergrond is waarschijnlijk dat zorgverleners verstoringen in de patiëntenzorg willen voorkomen en criminelen zagen hen daarom als doelwitten die waarschijnlijk losgeld zouden betalen. Het bleek dat de meeste aanvallen gericht waren op zorginstellingen met minder dan 500 werknemers. Het lijkt erop dat aanvallers zich richtten op deze kleinere instellingen omdat ze mogelijk kleinere beveiligingsbudgetten hebben en dus minder goed zijn beschermd.

4) *Covid-19 phishing fraude als wereldwijd probleem*. Wereldwijd zijn deze tendensen door de APWG waargenomen en ook andere studies hebben hierover gerapporteerd (Lallie et al., 2020).

De impact van Covid-19 op phishing is in het kader van deze studie interessant omdat het een illustratie vormt van de mate waarin aanvallers responsief zijn ten aanzien van hun omgeving en hierop snel en flexibel kunnen reageren.

[3] CEO e-mails worden ook Business E-mail Compromise' ofwel BEC-aanvallen genoemd.

1.1.8 '*No honour among thieves*' (IOCTA, 2019, p. 22)

Verschillende studies stellen vast dat diegenen die zich op het dark web begeven kwetsbaar zijn voor fraude en diefstal. Zo is het dark web regelmatig niet bereikbaar: er is relatief veel 'downtime' en dat is vaak het gevolg van DDoS aanvallen op het dark web (IOCTA, 2019). In 2019 zijn de drie grootste Darknet-markten het slachtoffer geworden van langdurige DDoS aanvallen, en zijn de moderators van Dream Markt vermoedelijk afgeperst voor $400.000 (≈ EUR 356.000), aldus (IOCTA, 2019). Een ander voorbeeld komt van de wereld van de cryptomunten. Cryptomunten zouden in beginsel veilig moeten zijn. Maar het gebruik van cryptomunten is ook vatbaar voor hacking en diefstal. Zo stalen hackers ongeveer $532,6 miljoen van de in Tokio gevestigde cryptocurrency-exchange Coincheck Inc. (Nolasco Braaten & Vaughn, 2019). Tenslotte, hiervoor werd beschreven dat 5 op de 14 DDoS aanvallen die werden gehuurd geen DDoS-aanval opleverden (de Santanna et al., 2015). Hieronder beschrijven wij meer voorbeelden van phishing en DDoS.

Samenvattend, het internet biedt vele mogelijkheden voor criminelen, zowel op het open net als het darknet. De anonieme omgeving van het darknet heeft vele criminele forums mogelijk gemaakt, waar anoniem samenwerken en handelen kan plaatsvinden. Er zijn verschillende technische systemen ontstaan die criminaliteit steeds gemakkelijker maken, zoals botnets en cryptomunten. Tenslotte, met Crime-as-a-Service wordt het plegen van een ruim scala aan online misdrijven een optie voor criminelen die beschikken over weinig of geen technische kennis.

Hieronder worden de twee delicten besproken waar het in dit onderzoek specifiek om gaat: phishing en DDoS-aanvallen en wordt aangegeven waar de mogelijkheden liggen voor coördinatie en samenwerking tussen aanvallers. Hier zal blijken dat deze delicten bestaan uit een keten van verschillende schakels, waarbij in iedere schakel verschillende daders een rol kunnen spelen of eindverantwoordelijk zijn.

1.2 Phishing

De *Anti-phishing Working Group* (APWG) omschrijft phishing als een misdrijf waarbij zowel social engineering als technische middelen worden gebruikt om de identiteitsgegevens en inloggegevens van financiële accounts van consumenten te stelen. Phishing is één van de belangrijkste modus operandi van online fraude, zoals onder meer online banking fraude (Boerman, Grapendaal, Nieuwenhuis, & Stoffers, 2017, p. 146).

Social engineering-technieken spelen bij phishing een belangrijke rol. Hiermee bedriegen de aanvallers onoplettende slachtoffers door ze te laten geloven dat ze zaken doen met een vertrouwde, legitieme partij, door misleidende e-mailadressen en e-mailberichten te gebruiken. De e-mails moeten gebruikers lokken met een 'goed verhaal': een gevoel van urgentie overbrengen met de noodzaak tot actie, zoals het corrigeren van een fout in een factuur of het beveiligen van een gecompromitteerd account. De bedoeling is om consumenten naar vervalste websites te leiden. Als dat lukt, bezoekt het slachtoffer de phishing-website en vult hij de persoonlijke informatie (persoonlijke identificeerde informatie, PII) in, zoals financiële gegevens, gebruikersnamen en wachtwoorden, waar de aanvaller om vraagt. Deze websites worden phishing-websites genoemd. Via technische middelen kan ook malware op computers worden geïnstalleerd om rechtstreeks inloggegevens te stelen, waarbij vaak gebruik wordt gemaakt van systemen die de gebruikersnamen en wachtwoorden direct van de accounts onderscheppen (APWG, 2020c 17637). Het is een moderne vorm van fraude (Ramzan, 2010). De phishing-website kan ook metadata over de gebruiker vastleggen, zoals het IP-adres van de gebruiker of de taal van het HTTP-verzoek (Oest et al., 2018; Ramzan, 2010).

Phishing kan bestaan uit een enkele e-mail of een veelvoud ervan. Als er een concentratie is in de tijd van identieke of vergelijkbare e-mails, kan worden gesproken over phishing-campagnes (Lastdrager, 2018).

Het uitvoeren van een phishing-aanval gebeurt – voor grote aanvallen – in verschillende stappen (Oest et al., 2018; Oest et al., 2020; Ramzan, 2010):

(1) Allereerst moet een aanvaller een infrastructuur opzetten, zoals een phishing/misleidende website die lijkt op, en het 'gevoel' geeft, van een legitieme website, bijvoorbeeld van een prominent merk.

(2) Daarna stuurt hij berichten naar potentiële slachtoffers, bijvoorbeeld via spam/phishing e-mail, met een link naar de phishing-website.

(3) Hiertoe zijn e-mail adressen nodig. Die kan een 'phisher'[4] proberen online te krijgen via 'spammers'. Spammers kunnen op hun beurt een bot-beheerder (*de bot-herder*) benaderen, die een botnet kan inzetten om phishing e-mails te verzenden naar grote aantallen gebruikers (Ramzan, 2010).

Daarnaast kan een phisher gebruik maken van zogenaamde phishing kits: programma's om gebruikers aan te vallen en die te koop zijn op het Dark web voor redelijke bedragen, van $0.30 tot $1000 (Oest et al., 2018; Oest et al., 2020; Ramzan, 2010).

[4] Wij spreken over aanvallers, of 'phishers', wanneer het in het bijzonder om aanvallers gaat die betrokken zijn bij phishing.

Wel moet deze phisher goed opletten: sommige kits sturen de geoogste PII niet alleen naar de koper van de phishing kit, maar ook naar diegenen die de phishing kit heeft ontworpen (Ramzan, 2010). Indien deze ontwerper van de phishing kit snel is kan hij dus zelf deze PII gebruiken voor het uitvoeren van verdere misdrijven.

(4) Tenslotte downloadt de aanvaller de gestolen informatie van de phishing-pagina (Oest et al., 2020, p. 2).

Soms, zoals ook voorkomt in de data die wij gebruiken, wordt in de e-mail zelf direct gevraagd om PII en andere relevante informatie (bankgegevens) in te vullen en terug te mailen. Dit is technisch gezien eenvoudiger maar wellicht minder overtuigend voor een potentieel slachtoffer.

De phisher kan, na het verzamelen van de PII, gebruik maken van andere criminelen om deze informatie te gebruiken. Voor het daadwerkelijk stelen van geld van een bankrekening moet men bekend zijn met het beveiligingssysteem van de specifieke bank en niet iedereen heeft die kennis (Ramzan, 2010). Daarom verkopen veel phishers de gevangen PII op het dark web en hopen zij op deze manier hun geld te verdienen (Oest et al., 2018; Ramzan, 2010).

Het grootste probleem voor phishers is het 'cash-out'-probleem. Zij kunnen het geld van het rekeningnummer van het slachtoffer stelen maarde vraag is waar ze dat geld naar toe brengen zonder zichzelf te verraden. Zij gebruiken daarvoor de zogn. geldezels (money mules). Een 'geldezel' is een persoon die geld van een derde partij, diegene die geld van een bankrekening heeft gestolen, op zijn eigen bankrekening ontvangt en het naar een andere rekening overmaakt of het contant opneemt en aan iemand anders geeft, om er een commissie voor te krijgen. Hiermee wordt de online keten gebroken en kunnen opsporingsinstanties de oorspronkelijke dief niet meer traceren. Criminelen werven (vaak jonge) geldezels via internet, e-mail, chat, brief, telefoon of op het schoolplein. Deze moeten het gestolen geld naar (vaak buitenlandse) rekeningnummers overmaken. Het werven van deze geldezels is voor criminelen de bottleneck van het hele proces (Florêncio & Herley, 2010).

Aanvallers gebruiken verschillende geavanceerde technieken om detectie door de grote browsers te ontlopen (zie Oest et al., 2020 voor een overzicht):

- Ze kunnen automatische vertaling toepassen wanneer ze internationaal actief zijn;
- Ze gebruiken CAPTCHA, zoals legitieme websites dat doen;
- Ze maken gebruik van c*loaking*-technieken. Dit zijn technieken die het web-verkeer schiften zodat specifieke *security* gerelateerde bezoekers, zoals

cyberanalisten, niet worden toegelaten op de phishing website maar andere informatie te zien krijgen. Alleen de potentiële slachtoffers zijn voor de phisher van belang;

- Slachtoffer-specifieke paden: sommige phishing campagnes genereren automatisch een *sub-pad* dat uniek is voor het IP-adres van elke bezoeker, die wordt vervolgens onmiddellijk omgeleid naar dat pad. Dit pad is niet zichtbaar voor andere IP-adressen.

Door middel van dergelijke technieken kunnen aanvallers, voor gemiddeld 9 uur (Oest et al., 2020), detectiemechanismen ontwijken en moeten zij hun slag slaan.

Aantallen. Het is onmogelijk het precieze aantal phishing e-mails te kennen dat dagelijks wordt verzonden, maar dat het gaat om enorme aantallen is wel helder. In 2019, zo stelt Microsoft, heeft het bedrijf meer dan 13 miljard kwaadwillende en verdachte e-mails geblokkeerd, waarbij meer dan 1 miljard URL's die waren opgezet met het expliciete doel om een phishing-inlogaanval te starten (Microsoft, 2020). En Google vermeldt dat zij dagelijks ongeveer 100 miljoen phishing-e-mails blokkeren (Kurian, April 16, 2020). Deze e-mails bestaan uit grofweg drie categorieën: 1) zeer gerichte, maar geringe aantallen spear-phishing, die gericht is op specifieke individuen, 2) 'boutique phishing' die slechts enkele tientallen mensen moeten bereiken en 3) geautomatiseerde bulk phishing gericht zijn op duizenden of honderdduizenden mensen (Bursztein & Oliveira, 2019). Globaal gesproken, hoe geavanceerder de phishing aanval, hoe geringer de aantallen phishing e-mails, hoe minder geavanceerd, hoe hoger de aantallen phishing e-mails, aldus Bursztein and Oliveira (2019).

De Anti-Phishing Working Group (APWG) publiceert cijfers over phishing. In Figuur 1 worden de aantallen unieke phishing websites getoond die zijn ontdekt sinds 2005 (APWG, 2020a).

Succes van phishing. Zoals hierboven werd aangegeven kan het succes van social engineering sterk variëren. In een grote studie naar een financiële dienstverlener bleek dat 7.42% van de bezoekers van de phishing websites PII achter te laten. Andere studies lieten vergelijkbare succes percentages van 5% tot 8% zien (Oest et al., 2020).

Het is duidelijk dat de directe slachtoffers van phishing geld verliezen. Ook bedrijven zoals banken en creditkaartmaatschappijen kunnen hiervan (mede-) slachtoffer zijn. Zij vergoeden soms de verliezen van klanten. De schade door phishing bij internetbankieren is vorig jaar meer dan verdubbeld, van 3,81 miljoen euro in 2018 tot 7,94 miljoen euro in 2019 (Netherlands Bankers Association (NVB), 2020). Daarnaast lopen zij reputatieschade op (Ramzan, 2010).

Figuur 1. Aantal unieke phishing websites geregistreerd door de APWG, januari 2005-December 2019. Bron APWG (2020b).

1.3 DDoS-aanval

Het kenmerk van een DDoS -aanval is het onbereikbaar maken van een online dienst en hiermee schade te berokkenen aan een slachtoffer (Mirkovic & Reiher, 2004). Bij een DDoS-aanval werken meerdere machines samen om één doel/slachtoffer of meerdere doelen/slachtoffers aan te vallen. Een aanvaller overspoelt een netwerk-server met verkeer. Omdat deze verzoeken constant worden verwerkt, wordt de server overbelast, waardoor diensten van het slachtoffer uitvallen (US-CERT, 2019). Hierdoor hebben legitieme gebruikers geen toegang meer tot informatiesystemen. Het kan gaan om e-mail, websites, of online accounts (Hyslip & Holt, 2019; US-CERT).

Er kan onderscheid worden gemaakt tussen twee typen DDoS-aanvallen: directe aanvallen en reflectieaanvallen (Jonker et al., 2017).

- Bij *directe aanvallen* stuurt de aanvaller grote hoeveelheden berichten naar het systeem van het slachtoffer. Dat kan daarbij gebruik maken van eigen servers maar vaak wordt gebruik gemaakt van bovengenoemde botnets, bots die draaien op apparaten en die onder zijn bevel staan. Om tegenmaatregelen en opsporing door handhavers te verhinderen, maken deze aanvallen vaak gebruik van '*spoofing'.* Het IP-adres van de afzender dat in elk Internet-bericht aanwezig is, wordt vervalst en vervangen door een ander willekeurige afzenderadres, zodat

niet meer kan worden nagegaan waar het bericht vandaan komt. Aanvallers misbruiken kwetsbaarheden in de beveiliging of zwakke plekken in systemen om talloze apparaten te besturen met behulp van commando- en controlesoftware. Bij een Distributed DoS (DDoS)-aanval zijn dus heel veel verschillende apparaten betrokken. Hierdoor neemt de kracht van de aanval enorm toe (US-CERT, 2019). Een aanvaller die een botnet onder controle heeft kan dus vanuit een punt heel veel apparaten tegelijkertijd berichten laten versturen naar één specifiek slachtoffer (Hyslip & Holt, 2019; US-CERT, 2019).

- Bij *reflectieaanvallen* gebruikt de aanvaller servers van derden om de aanval verder te vergroten. De aanvaller verstuurt met opzet (kleine) berichten naar een server waarvan hij weet dat de server deze beantwoordt met een (groot) bericht. Opnieuw gebruikt de aanvaller spoofing. De aanvaller gebruikt het IP-adres van het slachtoffer als afzender. Bij een reflectieaanval verstuurt de aanvaller een klein berichtje naar normale servers die grote berichten gaan versturen naar de vermeende afzender van het slachtoffer. De aanvaller gebruikt gewone servers als een "versterker”. Een aanvaller kan dus eenvoudig contactverzoeken vervalsen in naam van het slachtoffer/doel, waardoor de antwoorden van de reflectoren naar het slachtoffer worden gestuurd en waardoor er overbelasting van het systeem optreedt van het slachtoffer.

DDoS-aanvallen zijn in omvang toegenomen omdat er steeds meer apparaten worden verbonden met het internet. Voorbeelden zijn huishoudelijke apparaten, camera’s en DVD-spelers. Het internet groeit uit tot een het Internet of Things (IoT). Deze IoT-apparaten zijn echter vaak slecht beveiligd, waardoor ze kwetsbaar zijn voor misbruik. Het infecteren van IoT-apparaten (het installeren van bots op dit soort kleine apparaten) wordt meestal niet door gebruikers herkend. Een aanvaller kan zo makkelijk honderdduizenden van deze apparaten inzetten om een grootschalige DDoS aanval uit te voeren zonder dat de eigenaren van het apparaat er iets van vermoeden (Hyslip & Holt, 2019). Voor een bank of een e-commercebedrijf kan dit tot grote problemen leiden, zoals een daling van de verkoop en reputatie-schade (Abhishta, Joosten, Dragomiretskiy, & Nieuwenhuis, 2019). DDoS-aanvallen kunnen verschillende doelen dienen, zoals politiek activisme, maar worden ook vaak gebruikt als middel tot afpersing (Abhishta, Heeswijk, Junger, Nieuwenhuis, & Joosten, 2020; Hyslip & Holt, 2019; Osanaiye, Choo, & Dlodlo, 2016).

Er worden dagelijks grote aantallen aanvallen uitgevoerd (Jonker et al., 2017). Uit een analyse van twee datasets die vrijwel alle DDoS-aanvallen registreren blijkt dat er dagelijks ongeveer 30.000 aanvallen plaats vinden.

De meeste aanvallen zijn gering in omvang en kracht: bij de directe aanvallen is 85% minder dan een uur, en 5% meer dan 3 uur; bij de reflectieaanvallen duurt 60% vijf minuten of minder, 95% duurt een uur of minder. Er zijn nagenoeg geen aanvallen die langer duren dan 3 uur of meer. De meeste aanvallen worden door de organisaties zelf afgehandeld en worden nooit publiek bekend gemaakt. Daar komt bij dat veel organisaties, ook bij grotere aanvallen geen belang hebben bij het bekend maken van DDoS-aanvallen waarvan zij het slachtoffer werden. Meer in het algemeen hebben bedrijven geen belang bij het melden van cyberincidenten (Abhishta, 2019). Meldingen van DDoS-aanvallen kunnen het vertrouwen van de klant negatief beïnvloeden (Fafinski, Dutton, & Margetts, 2010 6454; Lawson, 2009 13536) en kunnen leiden tot een daling van de waarde van een bedrijf op de beurs (Spanos & Angelis, 2016 14070).

Regelmatig, in bijna de helft van de geregistreerde doelen/slachtoffers, worden de doelen vanuit verschillende kanten tegelijkertijd aangevallen, zowel via de directe methode als door reflectie-aanvallen. Meestal gaat het er dan om één specifiek type dienstverlening te verstoren (Jonker et al., 2017, p. 6).

Doelen van de DDoS aanvallen. Een DDoS aanval kan gericht zijn op organisaties, maar ook op particulieren. DDoS aanvallen kunnen verschillende doelen hebben. Ook al lijken DDoS aanvallen op 'online vandalisme', zij hebben vaak zowel economische als niet-economische doelstellingen (Mirkovic & Reiher, 2004). Het doel van een aanvaller beïnvloedt de omvang en de aard van de schade die ze hopen toe te brengen aan het slachtoffer. Abhishta (Abhishta, 2019) stelde de volgende indeling voor (figuur 2).

In deze classificatie kunnen de doelen economisch (d.w.z. wanneer het primaire doel van een aanvaller is om financiële schade toe te brengen) en niet-economisch zijn.

1) Economische doelstellingen. DDoS levert op verschillende manieren geld op voor aanvallers: het kan gaan om losgeld of een beloning.

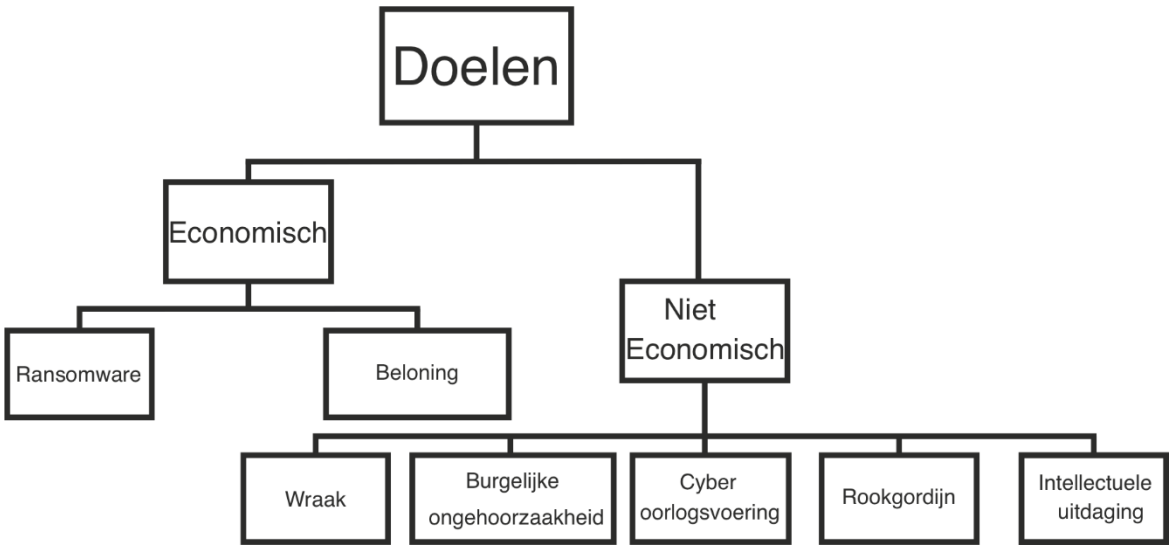
In 2015 lanceerde een cybercriminele groep genaamd 'Armada Collective' een op DDoS gebaseerde losgeldcampagne die bekend staat als DDoS voor bitcoin (DD4BC), waarbij het doel van de groep was om losgeld te innen (Mansfield-Devine, 2015).

Het bestaan van Botnets, stressers en booters illustreert het feit dat DDoS aanvallen voor een beloning worden uitgevoerd ten behoeve van een derde partij.

- Botnets - kunnen worden verhuurd aan andere criminelen. Zo worden botnets ter beschikking gesteld van "attack-for-hire" -diensten, waardoor ook niet-technische gebruikers, zoals scholieren, DDoS-aanvallen kunnen uitvoeren (Abhishta, Junger, Joosten, & Nieuwenhuis, 2019).

- *Stressers* en *booters*[5] kunnen worden gebruikt om – op verzoek – aanvallen uit te voeren op de door de aanvaller gekozen doelen, zoals hierboven werd vermeld.

Figuur 2. Typologie van DDoS aanvallen (bron: Abhishta (2019))



Deze tools zijn beschreven als 'DDoS-as-a-service' en behoren tot het bredere cybercrime ecosysteem (de Santanna et al., 2015).

2) Niet-economische doelen. Aanvallers hebben niet altijd economische doelen. Sauter (2013) bespreekt de rol van DDoS-aanvallen bij het uitbeelden van burgerlijke ongehoorzaamheid en politiek activisme. In dit geval is het primaire doel van aanvallers om de aandacht te trekken van de autoriteiten (bijv. regeringen) en van het publiek. DDoS worden ook ingezet als middel om wraak te nemen, als rookgordijn, als een manier van oorlogsvoering en intellectuele uitdaging (Abhishta, 2019). Volgens een Kaspersky-rapport geloven verschillende bedrijven dat DDoS wordt gebruikt als rook-gordijn, om andere aanvallen te maskeren (Kaspersky Lab, 2016).

Het doel van een DDoS aanval is niet altijd duidelijk. De eerste grootschalige DDoS aanval werd uitgevoerd in 1999, en was gericht tegen de Universiteit van Minnesota, die daardoor drie dagen onbereikbaar werd (Sachdeva, Singh, Kumar, & Singh, 2010). Het

[5] Een IP-stresser is een hulpmiddel dat als doel heeft om een netwerk of server te testen op robuustheid. Booters, ook wel *booter services* genoemd, zijn on-demand DDoS-aanvallen (Distributed-Denial-of-Service) die worden aangeboden door criminelen om websites en netwerken plat te leggen. Met andere woorden, booters zijn het onwettige gebruik van IP-stressers (Cloufare, 2020).

doel van deze aanval is nooit duidelijk geworden, en men veronderstelt dat het ging om de intellectuele uitdaging. (Abhishta, Junger, et al., 2019) maken aannemelijk dat studenten ook hun onderwijsinstelling aanvallen. Hiervoor is een aantal redenen denkbaar: wraak of het voorkomen van het uitvoeren van een test.

Het is lastig om te zeggen welke doelen bij DDoS het meest voorkomen. Aanvallers zijn soms open over hun doel, maar meestal niet. Het doel kun je dan vaak alleen afleiden uit het gekozen slachtoffer. Als een bank wordt aangevallen zou men kunnen concluderen dat er een financieel motief is. Maar hier zekerheid over krijgen is lastig.

Maatschappelijke en financiële gevolgen van DDoS-aanvallen. Net als elke andere cyberaanval kunnen DDoS-aanvallen schade toebrengen aan het slachtoffer. Er zijn verschillende categorieën (Anderson et al., 2013):

1) Verdedigingskosten. Defensiekosten worden gedefinieerd als het financiële equivalent van pr*event*ie-inspanningen. Ze omvatten investeringen in beveiligingsproducten, beveiligingsdiensten enz.

2) Directe verliezen. Directe schade wordt gedefinieerd als de schade dat het slachtoffer ervaart als gevolg van cybercriminaliteit. In het geval van op internet gebaseerde serviceproviders (bijvoorbeeld Hostingproviders, DNS-serviceproviders enz.) kunnen klanten van het slachtoffer besluiten naar een alternatieve provider over te stappen.

3) Indirecte verliezen. Indirecte verliezen zijn, bijvoorbeeld, een verandering in de perceptie van beleggers over de marktwaarde van een bedrijf.

4) Kosten voor de samenleving. De optelsom van de directe verliezen, indirecte verliezen en verdedigingskosten vormen samen de kosten voor de samenleving.

5) Criminele inkomsten. Criminele inkomsten worden gedefinieerd als de bruto-inkomsten uit een misdrijf. Zo zijn er gevallen bekend waarin organisaties gedwongen werden losgeld te betalen om aanvallers ervan te weerhouden deze te DDoSen (Paganini, November 6, 2015).

Dubendorfer, Wagner, and Plattner (2004) stellen een systeemtechnische benadering voor. Ze classificeren de schade als gevolg van DDoS in vier soorten namelijk: downtime-verlies, disaster recovery, aansprakelijkheid en klantverlies.

1.4. De misdaadketens

Onderzoek heeft laten zien dat criminelen opportunistisch zijn en vooral gebruik maken van de gelegenheid tot criminaliteit wanneer die zich aandient (Clarke, 2012; Cohen & Felson, 1979; Felson & Clarke, 1998b; Felson & Eckert, 2016).

Het is daarom niet verwonderlijk dat cybercriminelen gebruik maken van alle mogelijkheden op internet. Vanuit een Rational Choice perspectief (Cornish & Clarke, 2017) ligt het voor de hand dat criminelen ook online met elkaar samenwerken, enige coördinatie toepassen en van de gelegenheid gebruik maken, bijvoorbeeld als een DDoS plaats vindt, om 'slimme' phishing e-mails te redigeren waarin verwezen wordt naar eerdere gebeurtenissen. Zo kunnen ketens van cybercrime ontstaan die criminelen helpen om hun winst te maximaliseren of het risico om gepakt te worden te verkleinen.

Misdaadketens bestaan in de fysieke wereld. Er is nagenoeg geen onderzoek naar online misdaadketens. Onderzoek naar georganiseerde criminaliteit heeft zich meer gericht op andere vormen van criminaliteit, zoals drugshandel, fraude en witwassen en minder op cybercriminaliteit. Daarnaast heeft onderzoek naar online georganiseerde misdaad voornamelijk gekeken naar de daders, hun achtergronden en het netwerkproces (Leukfeldt et al., 2016), maar veel minder naar concrete informatie over modus operandi (Broadhurst, Grabosky, Alazab, Bouhours, & Chon, 2014; Lavorgna, 2015; Lavorgna & Sergi, 2016; Leukfeldt, Lavorgna, & Kleemans, 2017). Een groot WODC-onderzoek naar georganiseerde misdaad heeft er bewust voor gekozen om DDoS-aanvallen niet op te nemen (Kruisbergen et al., 2018, zie toelichting op p. 14), zodat mogelijke relaties tussen DDoS-aanvallen en andere delicten niet konden worden geanalyseerd.

Er is niet veel direct bewijs voor het bestaan van misdaadketens, maar er is wel enig bewijs voor te vinden. Een aantal auteurs wees erop dat aanvallen regelmatig op een gecoördineerde manier plaatsvinden, dit interpreteren wij als een 'misdaadketen' (S. H. Kim, Wang, & Ullrich, 2012; Yegneswaran, Barford, & Ullrich, 2003). Studies van hacking-aanvallen wereldwijd tonen aan dat coördinatie van aanvallen op nationaal niveau zichtbaar is (S. H. Kim et al., 2012). Yegneswaran et al. (2003) onderzochten de coördinatie van aanvallen. Ze beschreven verschillende soorten verkenningen van aanvallers op de poorten van ICT-systemen. Dit zijn 'scans', d.w.z. aanvallen op systemen die uitgebreid onderzoeken welke kwetsbaarheden op een ICT-systeem te vinden zijn. De auteurs vinden inderdaad dat er gecoördineerde scans plaats vinden. Gecoördineerde scans zijn scans vanuit uit verschillende bronnen (5 of meer) gericht op een bepaalde toegang*spoort* binnen een tijdspanne van één uur. Zij worden uitgevoerd door meerdere aanvallers, vanaf verschillende locaties en zijn gericht op een specifieke

poort van een ICT-systeem en vinden allemaal binnen een uur plaats, mogelijkerwijs om een DDoS- aanval te plannen. Yegneswaran et al. (2003) stellen dat deze gecoördineerde scans relatief vaak voorkomen. Zij concluderen dat aanvallers die hun aanvallen coördineren, de meest agressieve aanvallers zijn en verantwoordelijk zijn voor de meeste aanvallen (Yegneswaran et al., 2003, p. 10). In de laatste versies van de Data Breach Investigation Report van Verizon (Verizon Risk Team, 2020) wordt gesproken over incidenten die een middel tot een doel zijn (*a means to an end*). Meestal gaat het dan om het vormen van een botnet.

In de bovengenoemde studies blijkt dat een systematisch begrip van de relaties in de onderwereld van cruciaal belang is voor het ontwikkelen van effectieve, langdurige tegenmaatregelen (Thomas et al., 2015, p. 2). Hierdoor wordt gecoördineerde actie van handhavers een stuk gemakkelijker.

1.5 Vraagstelling van de huidige studie

De huidige studie gaat op zoek naar de statistische relaties tussen DDoS-aanvallen en phishing campagnes die als in misdaadketens met elkaar verbonden zijn.

Uitgangspunt is dat de meeste (hoewel niet alle) online criminaliteit financieel gemotiveerd is. Verizon Risk Team (2018) analyseerde 53.308 beveiligingsincidenten van over de hele wereld. Hiervan was 76% financieel gemotiveerd en 13% spionage,[6] samen goed voor 89 procent van alle incidenten. Anderen toonden ook aan dat het aantal economisch gemotiveerde misdaden enorm is (Bayoumy, 2018; Tcherni-Buzzeo, Davis, Lopes, & Lizotte, 2016). Slachtofferonderzoeken, waarbij alleen naar individuele slachtoffers werd gekeken, toonden ook aan dat de meeste gemelde misdrijven een economisch doel hebben (McGuire & Dowling, 2013).

Op basis van het gepresenteerde literatuuroverzicht willen wij drie hypotheses onderzoeken.

1.5.1 Hypothese 1 (H1): Phishing ten behoeve van de planning van een botnet en DDoS-aanvallen

[6] Spionage is meestal ook financieel motiverend: spionage wordt gedefinieerd als 'inbreuken werden gemotiveerd door het verkrijgen van strategisch voordeel (spionage)' (Verizon Risk Team, 2018, p. 5).

Harris, Konikoff, and Petersen (2013) beschreven DDoS uitgebreid en zij stellen dat phishing-e-mails de malware bevatten die nodig is voor de DDoS-aanvallen: ''*Once malicious code is weaponized (bewapend) or purchased the software can either be delivered via a spam campaign containing the software or through the victim's selection of links within the spam or phishing message to seemingly genuine websites containing the malicious code for download and execution*' (Harris et al., 2013, p. 5).[7] Dit betekent dat dezelfde aanvallers (groep) eerst een phishingcampagne opzetten om malware te verspreiden om zo de botnets te maken en vervolgens de DDoS-aanval uit te voeren. De malware kan worden gedownload wanneer de gebruiker op een link klikt in de phishing e-mail of in een bijlage die het slachtoffer zou moeten downloaden. Soortgelijke bevindingen zijn gemeld door de Nederlandse Politie (Boerman et al., 2017, p. 241; Pappalardo & Messmer, May 16, 2005).

Zoals hierboven vermeld zijn de recente DDoS-aanvallen ook vaak *reflectieaanvallen* (Mansfield-Devine, 2015). Desondanks blijft het mogelijk dat phishingcampagnes voorafgaan aan de DDoS-aanval. Dit brengt ons bij de eerste onderzoeksvraag:

Onderzoeksvraag 1: Vinden er meer phishingaanvallen plaats in de periode die direct vooraf gaat aan een DDoS-aanval? Zo ja, dan onderschrijft dit hypothese 1.

1.5.2 Hypothese 2 (H2): DDoS-aanvallen als afleidingsmanoeuvre of rookgordijn

DDoS-aanvallen kunnen worden gebruikt om het *security*-personeel in de *Security* Operation Centre (SOC) bezig te houden. Terwijl de aanval loopt, kan een phishing-campagne worden gestart om toegang te krijgen tot de IT-systemen (Bulanova-Hristova et al., 2016; Ricks et al., 2018). Onlangs is DDoS geëvolueerd van een doel op zichzelf naar iets dat er alleen maar uit zou moeten zien als een primaire aanvalsmodus maar een ander doel dient, namelijk een rookgordijn voor een andere aanval (Ricks, Thuraisingham, & Tague, 2018). In dit scenario is het doel van de aanvallers om de DDoS te gebruiken als rookgordijn voor de uitvoering van een andere aanval (Ricks et al., 2018; Thomas et al., 2015). Deze nieuwe wijze om een DDoS te lanceren, wordt vaak gebruikt om gegevens, financiën te stelen of andere heimelijke activiteiten uit te voeren.

[7] 'Zodra schadelijke code is gewapend of gekocht, kan de software worden geleverd via een spamcampagne die de software bevat of via de selectie van links door het slachtoffer in het spam- of phishing bericht naar schijnbaar echte websites die de schadelijke code bevatten voor downloaden en uitvoeren' (Harris et al., 2013, p. 5).

Ook door *security*bedrijven zijn verschillende berichten verschenen die aangeven dat DDoS-aanvallen een afleidingsmanoeuvre kunnen zijn. Een Kaspersky-studie stelt:

> *'Meer dan de helft van de ondervraagde bedrijven (56%) gelooft dat DDoS is gebruikt als rookgordijn voor andere vormen van cybercriminaliteit, en van die zakelijke respondenten meldde een grote meerderheid (87%) dat ze ook het slachtoffer waren geweest van een gerichte aanval.'*(Kaspersky Lab, 2016)

Ook is gedocumenteerd dat aanvallers verschillende aanvallen lanceren waarbij één aanval dient als dekmantel voor de 'echte' of hoofdaanval.

Onderzoek op basis van Nederlandse politiegegevens rapporteerde dat '*Om onderzoekers te misleiden, zij* [de aanvallers] *tegelijkertijd een tweede programma, 'ZeuS banking malware', hadden uitgerold, in de hoop dat forensische specialisten zich daarop zouden richten in plaats van op TorRAT.*' (Bulanova -Hristova et al., 2016, p.45). De politie Oost-Nederland is eind 2018 een dergelijk geval tegengekomen (bron: Emma Ratia, Politie Eenheid Oost-Nederland).

De implicatie hiervan is dat DDoS-aanvallen en phishing-campagnes gelijktijdig plaatsvinden, omdat de ene aanval dient om het *security*-personeel bezig te houden terwijl de 'echte' aanval stilletjes kan doorgaan. Onze tweede onderzoeksvraag is daarom:

Onderzoeksvraag 2: Vinden DDoS-aanvallen en phishing-campagnes simultaan plaats? Dan ondersteunt dat de hypothese van DDoS als rookgordijn. In dit geval beschouwen we phishing als het primaire misdrijf en is DDoS secundair, dat wil zeggen ter ondersteuning van de phishing-campagne.

1.5.3 Hypothese 3 (H3): DDoS als context of als verhaallijn

Fraudeurs hebben vaak "geprofiteerd" van rampen (Aguirre & Lane, 2019 17671). Ter illustratie: aanvallers hebben uitgebreid gebruik gemaakt van de Covid-19-crisis om phishing-e-mails te ontwerpen. De Anti-Phishing Working Group (APWG, 2020c) heeft een overzicht gegeven van een aantal aanvallen.

Tijdens de pandemie zijn Zoom-gebruikers potentiële slachtoffers geworden van phishing-e-mails met als doel hun accountgegevens te stelen. Zo probeerden aanvallers gebruikers door middel van phishing gebruikers te verleiden om het Zoom-programma te downloaden, in plaats daarvan downloadde zij malware. Verschillende frauduleuze CEO-e-mails verwezen naar Covid-19. De Covid-19-crisis was voor fraudeurs ook een

aanleiding om een "nieuw" bankrekeningnummer op te sturen waarop geld moet worden gestort, of om een bankrekening te openen ten behoeve van de 'slachtoffers van de pandemie'. In maart '20 was het aantal ransomwareaanvallen op zorginstellingen hoger dan in dezelfde periode van 2016 tot 2019. Deze trends zijn wereldwijd waargenomen door de APWG (APWG, 2020c; Lallie et al., 2020).

Verschillende voorbeelden uit de praktijk geven aan dat DDoS-aanvallen een context of verhaallijn kunnen bieden voor phishing-aanvallen. De Nederlandse Bank (DNB) en Walle (2018) hebben dit beschreven. DNB waarschuwde voor phishing-e-mails en verklaarde: '*… de mogelijkheid bestaat dat het aantal 'phishing mails' zal toenemen vanwege de DDoS-aanvallen van de afgelopen dagen op de websites van banken en andere instellingen'* (DNB, 31 januari 2018).

In het verlengde hiervan is het mogelijk dat DDoS-aanvallen de context of de verhaallijn bieden voor phishing-aanvallen. Het kan om een (groep) aanvallers gaan of verschillende groepen. Beide situaties zouden kunnen voorkomen. De aanvallers grijpen hun kans om te verwijzen naar de DDoS-aanvallen en gebruikers te misleiden. Vermoedelijk zijn zij van mening dat dergelijke e-mails geloofwaardiger zijn en 'echter' lijken. Dit brengt ons bij de derde onderzoeksvraag:

Onderzoeksvraag 3. Is er een stijging in het aantal phishing e-mails na een DDoS-aanval? D.w.z., is er een stijging van het aantal phishing e-mails in het algemeen en is er een stijging in het aantal phishing e-mails die verwijzen naar DDoS-aanvallen of online *security*-problemen? Nogmaals, we gaan ervan uit dat phishing het primaire doel is, en DDOS in dienst hiervan staat, dat wil zeggen ter ondersteuning van de phishing-campagne.

Bewijs hiervoor kan worden gevonden door eveneens de inhoud van de e-mails te onderzoeken die na een DDoS-aanval worden verzonden. Verwacht wordt dat de phishing-e-mails verwijzen naar DDoS of naar problemen van online (on)veiligheid.

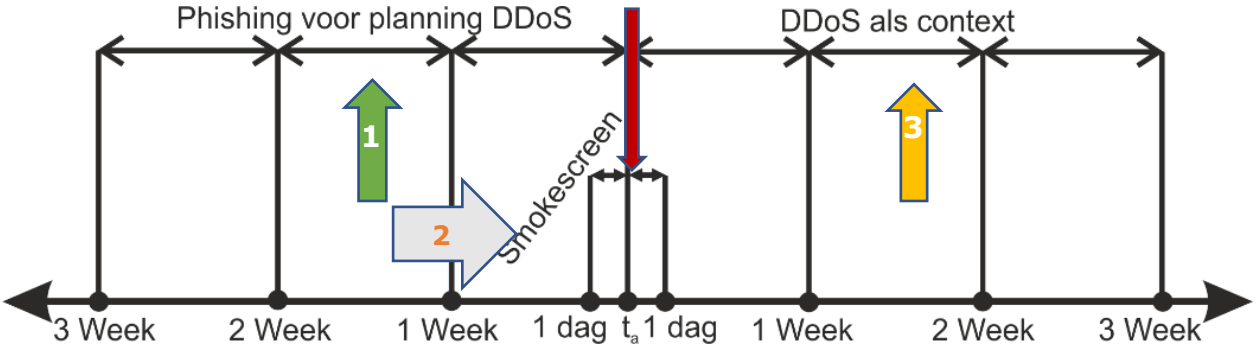
De hypotheses zijn samengevat in Figuur 3. De middelste lijn, aangegeven met de rode pijl is het moment van de DDoS-aanval.

1. De eerste hypothese stelt dat phishing plaatsvindt in de weken die voorafgaan aan de DDoS-aanval, om een botnet te construeren en DDoS te faciliteren (groene pijl);

2. De tweede hypothese houdt in dat DDoS een afleidingsmanoeuvre is voor de phishing-campagne (grijze pijl), beide aanvallen vinden globaal tegelijkertijd plaats;

3: De derde hypothese houdt in dat DDoS de verhaallijn verschaft voor de phishing campagne (gele pijl). De phishing campagne volgt in de weken na de DDoS aanval.

Figuur 3. Schematische voorstelling van de drie hypotheses: (1) H1= groen, (2) H2: grijs en (3) H3: geel. De datum van de DDoS aanval is de rode pijl.



1.5.4 De verhouding tussen de drie hypotheses

Zoals eerder aangegeven (1.4, eerste paragraaf) zijn criminelen opportunistisch, of dat nu offline of online is. Dit betekent dat zij alle opties zullen gebruiken waarvan zij inschatten dat die een gunstige kosten/baten verhouding kunnen opleveren. Voor een discussie over het rational choice perspectief online, zie: (Claude & Siponen, 2014; J. H. Kim, 2015; Mandelcorn, Modarres, & Mosleh, 2013; Redmiles, Mazurek, & Dickerson, 2018; Tambe Ebot & Siponen, 2014; Xu & Hu, 2018).

Het doel van dit rapport is *niet* om aan te tonen dat *alle* aanslagen deel uitmaken van een misdaadketen, maar om te onderzoeken of specifieke aanvallen bestaan die deel uitmaken van deze misdaadketens. Andere aanvallen kunnen nog steeds op zichzelf staande gebeurtenissen zijn. Het is belangrijk om te begrijpen dat het aantal grote cyberaanvallen nog steeds zeldzaam is, dus het is niet reëel om te verwachten dat we in 95% van de gevallen een samenhang tussen aanvallen zullen krijgen. Dit betekent dat voor alle drie hypotheses steun kan bestaan: de hypotheses sluiten elkaar niet uit, ze kunnen alle drie waar zijn. En sommige aanvallen blijven op zichzelf staande incidenten. Aanvallers zijn geen automaten. Soms kunnen ze inspringen op een DDoS aanval en een phishing campagne versturen die veiligheid als thema gebruikt, soms zullen ze andere activiteiten hebben. Wij stellen dus niet dat de relaties tussen phishing en DDoS altijd zullen plaatsvinden.

Ons doel is: het uitzoeken of er een statistisch verband bestaat tussen specifieke DDoS-aanvallen en phishing-aanvallen. Dit betekent dat wij geen uitspraken doen over causaliteit. De coördinatie van misdrijven kan allerlei oorzaken hebben: dezelfde (groep) dader(s), het kan toeval zijn (zie box 4, hieronder) als een phishing aanval misbruik maakt van een toevallige andere gebeurtenis, het kan het gevolg zijn van de coördinatie van toevallig met elkaar in gesprek geraakte dader(s), het kan ook het gevolg zijn van een reactie op een zelfde achterliggende gebeurtenis zoals een datalek. En andere mogelijkheden bestaan wellicht ook nog. Aan fantasie bij daders is vaak geen gebrek.

1.5.5 Relevantie

Voor een beter begrip van cybercrime is het essentieel om te onderzoeken of er verbanden bestaan tussen ogenschijnlijk niet-gerelateerde cyber-aanvallen. Twee belangrijke potentiële effecten van het huidige onderzoek kunnen worden onderscheiden.

1) Versterking van de handhaving. De resultaten van dit onderzoek kunnen de opsporing versterken. Het kan de focus van opsporingsonderzoeken verscherpen, omdat men weet dat daders van specifieke delicten eveneens via het plegen van andere delicten kunnen worden opgespoord.

2) Opsporing. Door de setting en de sequentie van delicten en gerelateerde gebeurtenissen te beschrijven en te begrijpen worden barrièremodellen ontwikkeld ten behoeve van pr*event*ie. Dit gebeurt ook door de Nederlandse politie.

2. Methode

Deze studie maakt gebruik van verschillende datasets. Hieronder worden de gebruikte data en de analysemethode beschreven.

2.1 Data

2.1.1. Phishing data

De gegevens over phishing zijn afkomstig van de Anti-Phishing Working Group (APWG; https://apwg.org/). APWG is een internationale coalitie die de wereldwijde reactie op cybercriminaliteit samenbrengt: de industrie, de overheden, handhavingsorganisaties en NGO's. Daarmee zijn meer dan 2200 instellingen over de hele wereld lid van de APWG. Sinds 2005 analyseren zij en publiceren zij over phishing-berichten en phishing-websites die zij van de deelnemers en gebruikers ontvangen (APWG, 2020a). De APWG wil wetenschappelijk onderzoek faciliteren en stelt daarom data beschikbaar voor de wetenschap.

In totaal zijn 1.908.794 e-mails in de analyse gebruikt. Dit is een samenvoeging van twee sets; 1) 535.470 e-mails die aan de APWG zijn gerapporteerd tussen 01-01-2018 en 31-07-2019; en 2) 1.373.324 e-mails die aan de APWG zijn gerapporteerd tussen 02-09-2019 en 02-07-2020. Er missen dus 2 maanden. In totaal kwamen er meer dan twintig talen voor. Het gaat dus om een set van internationale e-mails. Oorspronkelijk was de wens om Nederlandse e-mails te analyseren, zoals verzameld door de Fraudehelpdesk (Lastdrager, 2018). Maar vanwege bezwaren van de Autoriteit Persoonsgegevens heeft de Fraudehelpdesk besloten dat het beschikbaar stellen van deze data voor analyse niet mogelijk was.

Classificatie e-mails.

Voor hypothese 3, 'DDoS als context of als verhaallijn' moeten wij de inhoud van de e-mails analyseren. Het doel is om onderscheid te maken naar e-mails die verwezen naar DDoS en andere e-mails.

Dit is ingewikkeld omdat de APWG de e-mails als tekst files bewaart. Plaatjes en dergelijke worden ook opgeslagen als tekst bestanden.

In de e-mails komen woorden zoals 'DDoS', of 'Distributed Denial of Service' niet voor. In een random selectie van 100 e-mails waarin de term "DDoS" wel voorkomt is het niet

de inhoud van de e-mail maar gaat het om alfanumerieke tekens die vermoedelijk bij een afbeelding horen. Dit betekent natuurlijk niet dat een verwijzing naar DDoS-aanvallen nooit voorkomen, maar het zal vermoedelijk niet heel frequent zijn,

Omdat verwijzingen naar DDoS niet voorkwamen is, in plaats hiervan, gezocht naar verwijzingen naar *security*, in algemene zin. Hiervoor zijn willekeurig 200 e-mails door één van de onderzoekers gelezen en zijn termen die te maken hadden met verwijzingen naar *security* geteld, het resultaat hiervan is opgenomen in tabel 1.

Tabel 1: Woorden die verwijzen naar '*security*' in 59 phishing e-mails die *security* als onderwerp hebben, frequentie van voorkomen, en vergelijking met 200 aselect gekozen phishing e-mails. De woorden die zijn gebruikt om *security* gerelateerde e-mails te omschrijven zijn vet gedrukt.

Termen die verwijzen naar *security*	**Frequentie van hoog naar laag in 59 '*security* phishing e-mails**	**%**	**Frequentie in alle 200 e-mails**
Security	59	100,0	684
Account	52	88,1	630
Accesses	24	40,7	165
Activity	18	30,5	103
Unauthorised, compromised, unusual, unfamiliar, leak	18	30,5	57
Close down, close & (un)block, expire, suspend	17	28,8	541
Alert, warning	14	23,7	164
Protect	12	20,3	290
Fraud	10	16,9	90
Locked, lock & remove	10	16,9	534
Interrupt	6	10,2	22
Hack	6	10,2	27
Identity_theft	3	5,1	23
Profile profile change	3	5,1	58
Fraud pre*vent*ion	2	3,4	7
Suspend	2	3,4	5
Theft	1	1,7	32

Van de 200 e-mails had 59 iets met veiligheid te maken. De termen 'secure' en '*security*' komen heel vaak voor en betekenen niet altijd dat de gebruiker wordt gewaarschuwd voor veiligheidsproblemen. Het kan bijvoorbeeld gaan om een '*secure message*' die de gebruiker moet downloaden. Het voorkomen van deze twee termen is dus niet

voldoende om een bericht te classificeren als verwijzend naar veiligheidsproblemen. Daarom is besloten om *security* gerelateerde e-mails te omschrijven als: e-mails waarin tenminste één *security* gerelateerd concept in voorkomt, met uitzondering van de termen '*security*', en 'account' (zie Tabel 1).

Enkele voorbeelden van typische e-mails die verwijzen naar veiligheidsissues, zoals fraude met een account, staan in Tabel 2.

Tabel 2: Voorbeeld van drie e-mails die naar *security* verwijzen om PII te verkrijgen.[1]

1)	Due to recent upgrade on our server, we urge all customers to update their account to the new SSL security server as part of our identity theft and fraud pr*event*ion measure. Follow the link below to proceed. "https://XXXXX/XXXX/XXXX/XXXX/XXXX/XXXX">CLICK HERE 2017 Bank of America Corporation. All rights reserved.
2)	For your security, we regulary monitor accounts for possible fraudulent activity. Please read your secure message by opening attachment (pdf). You will be prompted to open (Visit My Account) file or save (download) to your computer.
3)	There's Problem With Your Account! Dear xxx, We've detected unauthorized activity with your account! We need your help to resolve this issue with your account. To resolve your = account, you need to verify your identity. Resolve My Account<http://www-xxxx.xxxx/xxxx> For security reason your account has been locked, until you resolve your ac= count. Sincerely, Apple

[1] Tikfouten en, voor zover mogelijk, de lay-out, zijn overgenomen van het origineel. De oorspronkelijke links zijn vervangen door 'xxx'.

2.1.2 DDoS-data

Informatie over DDoS-aanvallen is niet zomaar beschikbaar omdat organisaties niet altijd melden dat zij slachtoffer zijn geweest. Voor dit onderzoek is daarom gebruik gemaakt van andersoortige publiek beschikbare informatie.

2.1.1.1 Google alerts

Onze data zijn gebaseerd op het systematisch verzamelen van 'Google alerts', ofwel Google meldingen (Abhishta, Joosten, Jonker, Kamerman, & Nieuwenhuis, 2019). De achtergrond hiervan is de volgende. Een groot deel van het internet is benaderbaar via eenvoudige Google-zoekopdrachten. Dit is het gevolg van het feit dat wanneer een nieuwe webpagina wordt gemaakt, deze wordt geïndexeerd en gerangschikt door Google en de metagegevens worden opgeslagen in de database van Google, ten behoeve van een snelle verwerking van zoekopdrachten.

Om mensen te helpen onderwerpen bij te houden, biedt Google ook een service met de naam 'Google Alerts'. Google Alerts[8] is een detectie- en meldingsservice voor nieuwe online inhoud. De meldingen worden via e-mail naar de gebruiker gestuurd wanneer er nieuwe resultaten zijn. Het kan gaan om webpagina's, krantenartikelen, blogs of wetenschappelijk onderzoek dat overeenkomt met de zoektermen van de gebruiker. Er zijn twee type meldingen: `Nieuws' voor nieuwsartikelen die zijn gepubliceerd door geregistreerde nieuwsuitzendingen en 'Web' voor andere vermeldingen van de zoekterm. Voor de constructie van de dataset waren alleen de nieuwe meldingen relevant. De web-meldingen hadden meestal niet betrekking op een DDoS-aanval maar bestonden uit meer algemene informatie over het verschijnsel DDoS en worden daarom niet meegenomen.

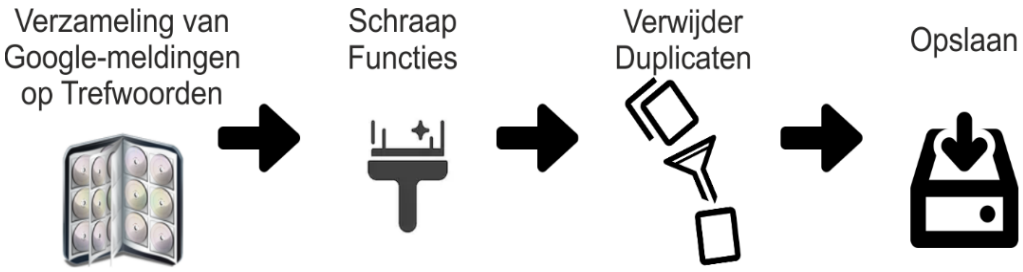
Bij de gegevensverzameling zijn twee zoektermen gebruikt: "DDoS" en "Distributed Denial of Service". Wij zijn met verzamelen van deze meldingen gestart op 20 augustus 2015 en het verzamelen gaat continu door.

De meldingen worden verwerkt met als doel een longitudinale dataset samen te stellen. Om een dataset voor te bereiden ten behoeve van analyses worden de e-mails van Google Alerts op geautomatiseerde wijze verwerkt: - de inhoud van elke e-mail wordt geanalyseerd met een op Python gebaseerde *scraper*. Elke melding heeft een kop, een link en een beschrijvende tekst van de post. Rekening houdend met deze informatie extraheren we de volgende functies uit de inhoud van de melding (zie ook figuur 4):

[8] https://en.wikipedia.org/wiki/Google_Alerts.

- datum,
- titel van elke melding,
- type van elke melding (nieuws of web),
- beschrijvende tekst van elke melding,
- weblink van elke gerapporteerde pagina (url).
- Daarna combineren we de meldingen en verwijderen de duplicaten op basis van de geëxtraheerde links.

Figuur 4. Proces van gegevensverzameling.



Met behulp van deze methode is informatie van 21.086 unieke bronnen vastgelegd die geschreven zijn in bijna 47 verschillende talen. De dataset bestaat uit 'Nieuws'-meldingen van 3.374 verschillende nieuwsbronnen die behoren tot 44 verschillende toplevel-domeinen. Dit laat zien dat het met behulp van Google-meldingen mogelijk is nieuws en andere artikelen over een specifiek onderwerp te verzamelen van een grote verscheidenheid aan websites (zie tabel 3, voor een overzicht).

Tabel 3: Beschrijving van de dataset tot 25 augustus 2020.

Start datum	Aantal nieuws-meldingen	Aantal web-meldingen	Aantal bronnen	Aantal nieuws-bronnen	Aantal talen
20 augustus 2015	34.144	43.767	17.181	7.441	48

Op basis van de datum waarop de waarschuwing is bezorgd en het aantal phishing-meldingen op een dag, is het mogelijk tijdreeksen te maken.

Voor onze analyse beperken we ons tot de DDoS-aanvallen met de grootste impact; aangezien deze gebeurtenissen de meeste media-aandacht kregen, zijn het misschien wel de 'populairste' DDoS-aanvallen van de periode. Deze steekproefstrategie is vergelijkbaar met die in Abhishta et al. (2020). Het doel van deze steekproefprocedure is om de meest gerapporteerde DDoS-aanvallen tussen 2018 en 2020 te extraheren, de periode waarvoor phishing e-mails beschikbaar waren.

Om niet op basis van nepberichten DDoS-aanvallen te registreren is een drempelwaarde bepaald voor het minimumaantal berichten dat nodig is om te stellen dat inderdaad een DDoS-aanval plaatsvond. Deze drempel is, na statistische analyse, bepaald op 32 Google nieuwsberichten (zie box 1). In de praktijk selecteren we aanvallen die op grote schaal in de media zijn gemeld vanwege hun intensiteit of doelwit. Voor meer informatie over de statistische analyse, zie box 1.

Box 1. Statistische analyses

Om te bepalen of er op een dag een DDoS aanval vond, gebruiken we de methodologie die ook werd gebruikt door (Kallus, 2014). We willen dat een minimum aantal nieuwsartikelen bij Google verschijnt. Gekozen is om, van alle dagen in de gekozen periode, de dagen te selecteren met de meeste nieuwsberichten, meer specifiek: de 20% dagen met de meeste berichten. Deze dagen bevatten 32 of meer Google nieuwsberichten die berichten over een DDoS aanval.

De volgende stap is het vertalen van het aantal meldingen naar het werkelijke aantal DDoS-aanvallen. Een enkele aanval kan namelijk gedurende meerdere dagen in het nieuws komen. De teksten van de nieuwsberichten worden onderzocht en bepaald wordt wanneer een DDoS-aanval heeft plaats gevonden. Zie ook (Abhishta, 2019) voor meer informatie.

Een validiteitscheck is uitgevoerd door het analyseren van Nederlandse nieuwswebsites op nieuwsberichten van DDoS aanvallen. Dit is gedaan aan de hand van de volgende vijf sites: https://nos.nl/nieuws/, https://www.nu.nl/, https://www.rtlnieuws.nl/, https://www.*security*.nl/ en https://tweakers.net/. Deze analyse laat zien dat er geen andere Nederlandse DDoS-aanvallen zijn gemeld dan die wij via Google alerts hebben gevonden.

2.2 Analyses

Bij het analyseren van tijdsreeksen maken wij onderscheid tussen twee periodes:

1) De '*event*-periode' vóór (H1), tijdens (H2) of na de DDoS (H3)-aanval is de periode waarin volgens elk van de hypotheses naar verwachting meer phishing e-mails worden verzonden dan gebruikelijk.

1) De 'trendperiode' die voorafgaat aan de DDoS aanval is de 'normale' tijd waarin alles gaat zoals gebruikelijk en een 'normaal' aantal phishing e-mails wordt verzonden.

Omdat we niet zeker kunnen zijn over de aanvalsstrategie van de aanvallers worden analyses per hypotheses voor twee verschillende combinaties van termijnen uitgevoerd:

- een reeks analyses met een 'normale' trendperiode van 30 dagen vóór de DDoS periode en *event*-periode van 5 dagen waarin we verwachten – volgens de hypotheses - dat het gemiddeld aantal e-mails hoger is dan tijdens de trend periode;

- een tweede reeks analyses met een 'normale' trendperiode van 60 dagen voor de DDoS-periode en een *event* periode waarin we verwachten dat het gemiddeld aantal e-mails hoger is van 15 dagen.

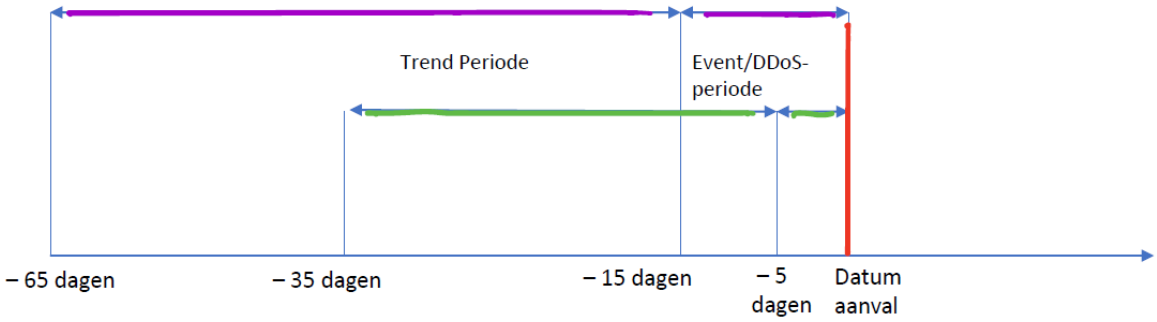
De keuze voor deze twee combinaties van periodes, 30 & 5, en 60 & 15, is arbitrair. Er was geen theorie of eerder onderzoek om dit te bepalen. Het leken ons de periodes waarbinnen mensen activiteiten plannen en uitvoeren. Om het iets minder arbitrair te maken is de combinatie van beide gebruikt. Dit is gedaan omdat niet bekend is hoe aanvallers werken en op deze wijze de hypotheses tweemaal worden getest. Per hypothese wordt het plan verder beschreven.

2.2.1 Hypothese 1: Phishing ten behoeve van de planning van een botnet en DDoS-aanvallen

Voor hypothese 1 ‚'phishing voor de planning van een botnet', wordt het gemiddeld aantal phishing e-mail tijdens de trendperiode van 30 dagen (d.w.z. vijf dagen voor de aanval tot 35 dagen voor de aanval) vergeleken met het gemiddelde aantal gerapporteerde e-mails in de periode van 5 dagen vóór de aanval. De verwachting is dat net voor de DDoS-aanval aanzienlijk meer e-mails zijn dan in de trend periode ervoor.

2) Bij de tweede analyse gebruiken we ook een langere trendperiode van 60 dagen (d.w.z. 15 dagen voor de aanval tot 65 dagen voor de aanval) en een langere *event* periode van 15 dagen vóór de DDoS aanval waarin de verwachting is dat er gemiddeld meer phishing e-mails worden verzonden (figuur 5).

Figuur 5. Phishing als voorbereiding voor botnet en DDoS (H1). Gemiddeld meer phishing tijdens 5 (groen) of 15 (paars) dagen vóór de DDoS aanval (DDoS-periode) dan daarvoor (normale trendperiode), DDoS dag in rood.

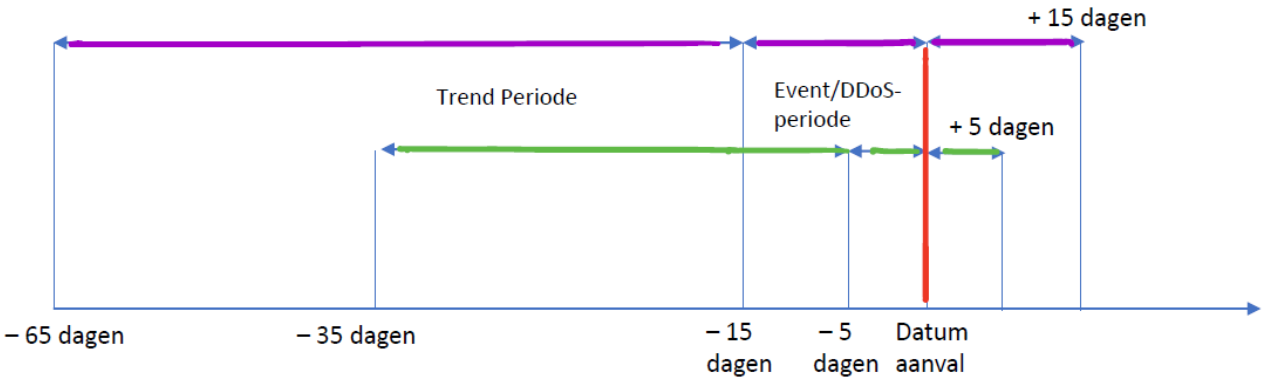


1.4.2 Hypothese 2: DDoS-aanvallen als afleidingsmanoeuvre of rookgordijn

Indien DDoS dient als rookgordijn voor de 'echte' phishingaanval, dan vinden de phishingaanvallen ongeveer tegelijkertijd plaats als de DDoS-aanval. Het gemiddeld aantal phishing e-mails tijdens een trendperiode van 30 dagen wordt vergeleken met het gemiddelde aantal gerapporteerde phishing e-mails tijdens de periode van vijf dagen vooraf en vijf dagen na de DDoS-aanval.

Ook hier, kiezen we, in een tweede analyse voor een ruimere trendperiode van 60 dagen bepaald (dus 15 dagen voor de aanval tot 65 dagen voor de aanval) en een grotere *event*-periode van 15 dagen voor en na de aanval. We tonen de trend- en *event* periode voor hypothese 2 in Figuur 6.

Figuur 6. DDoS als afleidingsmanoeuvre (H2): gemiddeld meer phishing tijdens 5 (groen) of 15 (paars) dagen rondom de DDoS aanval (DDoS periode) dan daarvoor (normale trendperiode), DDoS dag in rood.

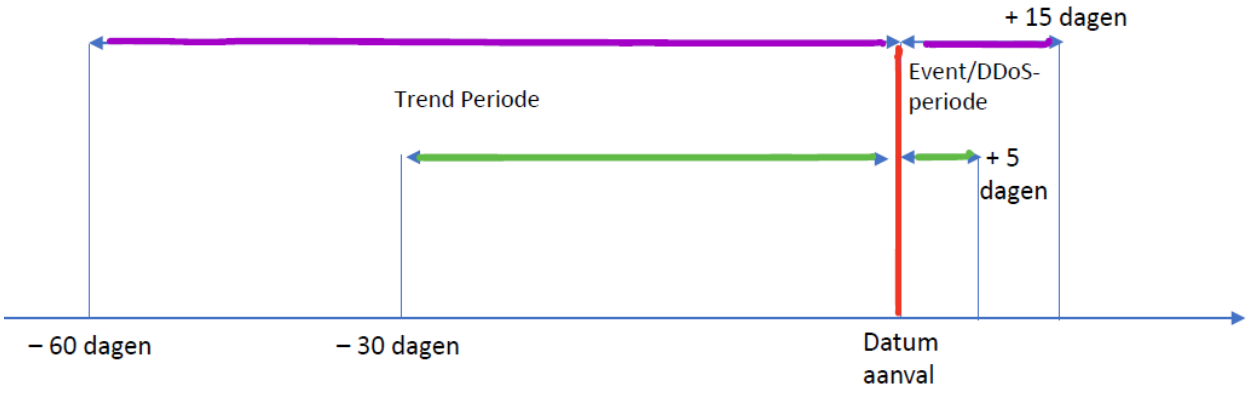


1.4.3 Hypothese 3: DDoS als context of als verhaallijn

Indien DDoS aanvallen als context dienen is de verwachting dat, net na de DDoS aanval meer *security* gerelateerde phishing e-mails plaatsvinden. Opnieuw wordt het gebruikelijke aantal phishing e-mails berekend voor de trendperiode van 30 dagen vóór de aanval tot de dag van de aanval. Deze trend wordt vergeleken met het gemiddelde aantal phishing e-mails tijdens de periode van vijf dagen na de DDoS aanval. De verwachting is, volgends hypothese 3, dat er meer e-mails zijn na de DDoS-aanval.

Opnieuw wordt een tweede ruimere trendperiode van 60 dagen (d.w.z. 60 dagen voor de aanval tot de dag van de aanval) gebruikt en een langere *event* periode van 15 dagen na de aanval. We tonen de trend- en DDoS-periode voor deze hypothese in figuur 7. Tabel 4 presenteert een samenvatting van het analyseplan.

Figuur 7. DDoS als context of als verhaallijn (H3)**:** gemiddeld aantal phishing e-mails 5 (groen) of 15 (paars) dagen na de *event* (DDoS aanval) in vergelijking met ervoor (de normale trendperiode), DDoS dag in rood.



Statistische analyses

Om de statistische significantie van het verschil in aantal gerapporteerde e-mails te testen maken we in alle analyses gebruik van de Mann-Whitney-U test. Omdat we de waarschijnlijkheidsverdeling van deze gegevens niet kennen, kiezen we voor deze niet-parametrische test. Een dispersie-analyse was niet mogelijk vanwege te geringe aantallen rondom veel DDoS-periodes.

Tabel 4. Analyseschema, met de periodes waarvoor het gemiddeld aantal e-mails wordt berekend.

	Trend periode – gebruikelijk aantal e-mails	**Periode met meer e-mails dan in trend periode volgens elk van de hypotheses**	**DDoS-periode**
H1 Phishing als planning	30 dagen ervoor (35 tot 5 dagen voor DDoS)	5 dagen VÓÓR datum DDoS	Dag aanval en $\pm$ 5 dagen (ervoor en erna)
	65 dagen ervoor (65 tot 15 dagen voor DDoS)	15 dagen VÓÓR datum DDoS	Dag aanval en $\pm$ 15 dagen (ervoor en erna)
H2 DDoS als rookgordijn	30 dagen ervoor (35 tot 5 dagen voor DDoS)	5 dagen VÓÓR en 5 dagen NA de datum van de aanval	Dag aanval en $\pm$ 5 dagen (ervoor en erna)
	65 dagen ervoor (65 tot 15 dagen voor DDoS)	15 dagen VÓÓR en 15 dagen NA de datum van de aanval	Dag aanval en $\pm$ 15 dagen (ervoor en erna)
H3 DDoS als context	30 dagen ervoor (35 tot 5 dagen voor DDoS)	5 dagen NA datum DDoS	Dag aanval en $\pm$ 5 dagen (ervoor en erna)
	65 dagen ervoor (65 tot 15 dagen voor DDoS)	15 dagen NA datum DDoS	Dag aanval en $\pm$ 15 dagen (ervoor en erna)

3. Resultaten

3.1 Overzicht van de phishing e-mails en de DDoS-aanvallen

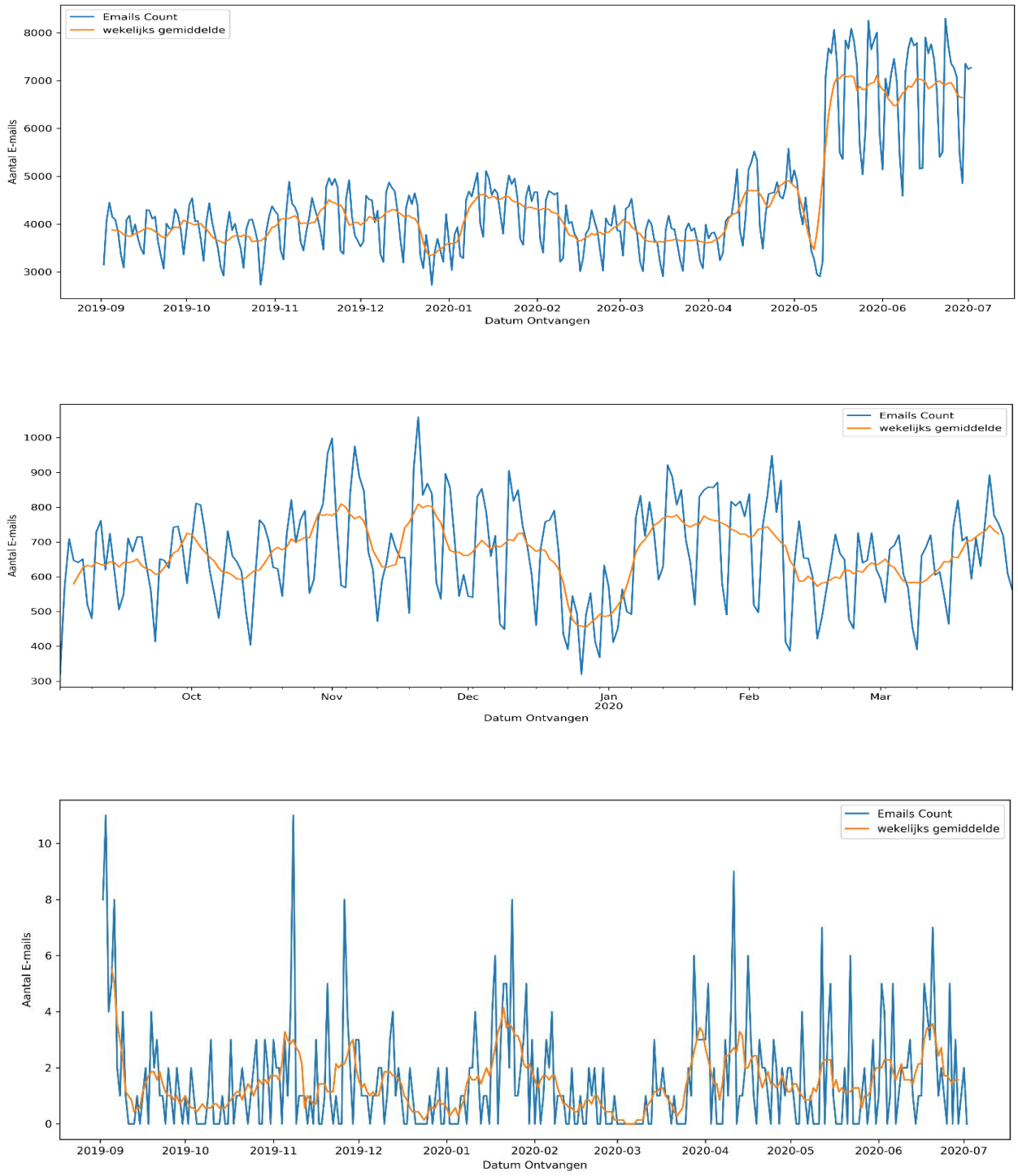
De verdeling van de phishing e-mails over de tijd staat afgebeeld in Figuur 8. Het aantal e-mails van de APWG data schommelt van enkele honderden naar enkele duizenden per dag. De figuren laten zien dat het gebruikelijk is dat het aantal phishing e-mails dagelijks op en neer schommelt en dat het totaal aantal phishing e-mails gestegen is vanaf mei 2020 van ongeveer 4000 dagelijks naar ongeveer 7000. Het aantal e-mails dat gerelateerd is aan security schommelt tussen de 600 en 800 dagelijks. Het aantal e-mails gericht op Nederlandse bedrijven schommelt in de APWG-data tussen de 2 en 4 phishing e-mails. Dit kan verband houden met het feit dat weinig organisaties lid zijn van de APWG en dus hun e-mails daar naar toe sturen. Daarnaast is gebleken, zoals hierboven werd vermeld, dat naar schatting 22% van de e-mails die bij Nederlandse gebruikers aankomen in het Engels of in een ander taal is opgesteld (Lastdrager, 2018).

Het aantal e-mails dat op Nederland is gericht, dit wil zeggen, Nederlandstalige e-mails, is relatief klein. Dat betekent dat het niet voor de hand ligt deze e-mails afzonderlijk te analyseren.

In de random e-mail set die is gecheckt op de verwijzing naar online veiligheid bleek dat 59 van de 200 e-mails (29.5%) die handmatig werden onderzocht expliciet verwezen naar online veiligheid.

Andere veelvoorkomende verhaallijnen hadden betrekking op postpakketten die afgeleverd moesten worden en prijzen of andere geldbedragen die konden worden geïnd.

Figuur 8. Aantal phishing e-mails 2019-09 – juli 2020, huidige studie. Boven: alle e-mails; midden: de phishing e-mails die verwijzen naar *security*; onder: de naar Nederland gestuurde e-mails (let op het verschil in de verticale schaal bij beide plaatjes). Bron APWG, eigen bewerking.



De DDoS-aanvallen

Voor de geselecteerde periode waren in totaal 28 aanvallen bekend. Voor vijf waren er geen phishing e-mails beschikbaar rondom de periode van de DDoS aanvallen, dus deze vijf zijn niet meer meegenomen in de analyse. Daarom verrichten we de analyses voor 23 DDoS-aanvallen (tabel 5). De volledige lijst DDoS aanvallen is opgenomen in de appendix.

De organisaties die zijn aangevallen zijn banken en overheidsorganisaties zoals de Belastingdienst en Digid.

Tabel 5. DDoS aanvallen voor de geselecteerde periode (datum: jjjj-mm-dd).

1	GitHub DDoS	2018-02-28	GitHub	International
2	DDoS to Silence Black Right Movement	2020-06-03	Black rights movement	US
3	DDoS Attacks on OKEx and Bitfinex	2020-02-27	Crypto Currency Exchanges	International
4	Massive DDoS Attack Shuts Down Iran’s Internet	2020-02-21	Iran's Internet Infrastructure	Iran
5	Greece: Government websites hit by cyberattack	2020-01-24	Greek government	Greece
9	DigiD	2018-08-01	DigiD	Netherlands
10	DigiD	2018-07-30	DigiD	Netherlands
11	DigiD	2018-07-31	DigiD	Netherlands
14	ABN Amro	2018-03-09	ABN Amro	Netherlands
15	Belastingdienst	2018-01-29	Belastingdienst	Netherlands
16	Rabobank	2018-01-29	Rabobank	Netherlands
17	DigiD	2018-01-29	DigiD	Netherlands
18	ASN Bank	2018-01-29	ASN Bank	Netherlands
19	SNS	2018-01-29	SNS	Netherlands
20	Regiobank	2018-01-29	Regiobank	Netherlands
21	Rabobank	2018-01-28	Rabobank	Netherlands
22	ING	2018-01-28	ING	Netherlands
23	E-health Letland / Latvia NVD	2018-01-16	E-health Letland / Latvia NVD	Latvia
24	ABN Amro	2018-05-24	ABN Amro	Netherlands
25	Rabobank	2018-05-24	Rabobank	Netherlands
26	DSB	2018-05-13	Deense spoorwegen	Denmark
27	ABN Amro	2018-01-16	ABN Amro	Netherlands
28	ABN Amro	2018-01-28	ABN Amro	Netherlands

Het is opmerkelijk dat er veel DDoS-aanvallen uit Nederland in de internationale dataset zitten. Er kan een aantal redenen hiervoor zijn:

1) In Nederland wordt veel online gebankierd. 91% gebruikte online bankieren terwijl het gemiddelde in de EU bijvoorbeeld, 58% is (Eurostat, 14-10-2020).

2) Wij hebben ons best gedaan zoveel mogelijk Nederlandse aanvallen mee te nemen. Wellicht is zo een vertekening in de data ontstaan door onze aandacht voor Nederland.

3) De DDoS-aanvallen worden geselecteerd op basis van het feit dat ze minstens een paar keer door persbureaus moeten worden vermeld, om het noteren van nepaanvallen te voorkomen. In ons land is er veel nieuws over DDoS. In een groot land als de Verenigde Staten zal het feit dat een bank niet online is vermoedelijk niet zo vaak door persbureaus worden gemeld, in vergelijking met DDoS-aanvallen in Nederland. In India kan een website die niet werkt verschillende redenen hebben, ook dat de internetverbindingen uitvallen. Omdat dit relatief vaak voorkomt is het niet meer nieuwswaardig.

3.2 Hypothese 1. Phishing ten behoeve van de planning van een botnet en DDoS-aanvallen

Hypothese 1 stelt dat phishing kan worden gebruikt om een botnet en/of een DDoS aanval op te zetten. Phishing-e-mails kunnen links bevatten en/of bijlagen die malware bevatten die gebruikt kan worden voor de DDoS-aanvallen. Dit betekent dat aanvallers eerst een phishingcampagne opzetten om malware te verspreiden om zo de botnets te maken en vervolgens de DDoS-aanval uit te voeren. De onderzoeksvraag luid: vinden de DDoS-aanvallen inderdaad relatief kort voor phishing campagnes plaats? Zo ja, dan onderschrijft dit hypothese 1. Om de vraag te beantwoorden vergelijken we:

1. Het gemiddeld aantal phishing e-mails in de trendperiode van 30 dagen voor de DDoS aanval met het gemiddeld aantal phishing e-mails in de *event*-periode van vijf dagen ***vóór*** de aanval.

2. Het gemiddeld aantal phishing e-mails in de trendperiode van 60 dagen voor de DDoS aanval met het gemiddeld aantal phishing e-mails in de *event*-periode van 15 dagen ***vóór*** de aanval.

We verwachten dat net **vóór** de aanval meer phishing plaats vindt dan in de trendperiode.

Tabel 6 laat de resultaten zien. Hierin staat het gemiddeld aantal phishing emails voor de 'normale' trendperiode van 60 dagen vooraf aan de DDoS-aanval en het gemiddeld aantal phishing e-mails net vooraf aan de DDoS-aanval. Van boven naar onder staan de

bedrijven naar de omvang van het verschil in phishing e-mails tussen wat gebruikelijk is (de trendperiode van 60 dagen vóór de DDoS aanval) en wat 15 dagen vóór de DDoS periode aan phishing e-mails wordt verzonden.

Box 2. Aanvallen op de *Black rights movement*.

Een voorbeeld is de DDoS-aanval op de *Black rights movement* en antiracisme organisaties, zoals de *Black Lives Matter beweging*. Die vond plaats op 3 juni 2020. Na de dood van George Floyd en de daaropvolgende protesten in de Verenigde Staten, waren de cyberaanvallen op belangengroepen maar liefst 1120 keer hoger, aldus Brewster (June 3, 2020). Het is onduidelijk wie er achter de aanslagen zit, maar er zijn pogingen ondernomen om de vrijheid van meningsuiting van antiracistische organisaties te neutraliseren, aldus Brewster (June 3, 2020).

Behalve grote DDoS-aanvallen is door de media tevens gemeld dat er uitgebreide phishingaanvallen gecombineerd met malware plaats vonden. Er werden phishing-berichten verzonden met als subject: '"*Vote anonymous about Black Lives Matter*" met als doel een *TrickBot modular banking trojan* te installeren (zie ook Brewster, June 11, 2020; Deeney, June 16, 2020).

In de periode van 60 dagen vooraf waren er dagelijks gemiddeld 4688 phishing emails, en in de periode van 15 dagen net voor de aanval was dat aantal gestegen naar 6935, een stijging van 2.246 phishing emails. Verder is in tabel 6 te zien dat tijdens de 15 dagen vóór de aanvallen op de ABN Amro, de Rabobank, de Deense spoorwegen, de Griekse regering, E-health Letland/Latvia NVD, de ABN Amro, de Belastingdienst, de Rabobank, DigiD, de ASN Bank, de SNS bank, de Regiobank, Iran's Internet Infrastructuur en de Crypto Currency Exchanges een statistisch significante stijging van phishing e-mail plaats vindt.

De statistische analyse laat zien dat, in totaal, bij 13 van de 23 DDoS aanvallen er significant meer phishing e-mails worden verzonden tijdens de periode van 15 dagen voorafgaand aan de DDoS aanval. Bij twee DDoS-aanvallen is het omgekeerde het geval.

Voor de periode 30 versus 5 dagen zijn de verschillen tussen de twee periodes minder helder: in 3 gevallen is er een stijging in de vijf dagen vóór de DDoS aanval (geen tabel getoond). Een voorbeeld van een gecombineerde aanval staat in Box 2, waar een

specifiek doelwit, de *Black rights movement,* tegelijk wordt aangevallen door middel van DDoS en phishing.

Tabel 6. Phishing als planning van een botnet en DDoS: gemiddeld aantal phishing e-mails in de trend periode van 60 dagen voor de DDoS aanval en 15 dagen **vóór** de DDoS aanval; bij 13 van de 23 DDoS-aanvallen zijn er meer phishing e-mails dan in de periode ervoor. (1)

Aangevallen bedrijf (1)	60 dagen voor de aanval	15 dagen voor de aanval	P-Value	Hypothese bevestigd(2)	Verschil in gemiddeld aantal e-mails
Black rights movement ***	4688	6935	0.00	1	2.246
ABN Amro ***	981	1993	0.00	1	1.011
Rabobank ***	981	1993	0.00	1	1.011
Deense spoorwegen ***	680	1586	0.00	1	906
Griekse regering ***	3992	4609	0.00	1	617
E-health Letland / Latvia NVD *	1116	1540	0.06	1	424
ABN Amro *	1116	1540	0.06	1	424
DigiD	1402	1552	0.12		150
DigiD	1372	1521	0.12		150
Belastingdienst **	1496	1636	0.03	1	140
Rabobank **	1496	1636	0.03	1	140
DigiD **	1496	1636	0.03	1	140
ASN Bank **	1496	1636	0.03	1	140
SNS **	1496	1636	0.03	1	140
Regiobank **	1496	1636	0.03	1	140
ABN Amro	1536	1613	0.11		78
Rabobank	1520	1589	0.12		70
ING	1520	1589	0.12		70
ABN Amro	1520	1589	0.12		70
GitHub	1533	1570	0.33		37
DigiD	1436	1457	0.34		21
Iran's Internet Infrastructuur *	4151	3873	0.05		-278.29
Crypto Currency Exchanges **	4162	3755	0.02		-407.09
Aantal vergelijkingen dat de hypothese bevestigt				**13**	

(1) Statische significantie: * p <.10, ** p <.05, *** p <.01.
(2): 1=hypothese bevestigd.

3.2 Hypothese 2. DDoS-aanvallen worden als afleidingsmanoeuvre of rookgordijn gebruikt voor de phishing aanval

Hypothese 2 stelde dat DDoS-aanvallen worden ingezet om het *security*- personeel in de *Security* Operation Centre (SOC) bezig te houden. Terwijl de DDoS-aanval loopt, wordt de phishing- campagne gestart met als doel toegang te krijgen tot de IT-systemen. De onderzoeksvraag luidt: indien de DDoS-aanvallen en phishing-campagnes simultaan plaats vinden, ondersteunt dit de hypothese van DDoS als een rookgordijn voor de 'echte' phishing aanval. Om de vraag te beantwoorden vergelijken we:

1. Het aantal e-mails in de trendperiode van 30 dagen voor de aanval met de DDoS-periode van vijf dagen **vóór & na** de aanval.

2. Het aantal e-mails in de trendperiode van 60 dagen voor de aanval met de DDoS-periode van 15 dagen **vóór & na** de aanval.

We verwachten dat rondom de aanval meer phishing plaats vindt dan tijdens de trendperiode.

Wanneer de trendperiode van 60 dagen wordt vergeleken met de 15 dagen vóór en na een DDoS blijkt, voor 13 DDoS aanvallen dit inderdaad het geval te zijn. Er zijn, rondom deze 13 DDoS aanvallen, significant meer phishing e-mails. Bij de DDoS aanvallen tegen de Black rights movement, de Deense spoorwegen, de ABN Amro bank (twee maal), de Rabobank, E-health Letland / Latvia NVD, en de Griekse regering worden er gemiddeld 15 dagen vóór en 15 dagen na de DDoS aanval dagelijks meer phishing e-mails gemeld bij de APWG (Tabel 7). Opnieuw zijn, van boven naar onder de aanvallen gesorteerd op volgorde van de omvang van het verschil in phishing e-mails tussen beide kolommen.

Voor de vergelijking van de periode van 30 dagen met de periode van vijf dagen vóór & na de aanval zijn de verschillen minder groot. Bij 7 aanvallen is nog altijd meer phishing rondom het moment van aanvallen.

Wanneer de resultaten voor hypothese 1 (tabel 6) worden vergeleken met de resultaten voor hypothese 2 (tabel 7) dan valt op dat van de 13 DDoS aanvallen allemaal dezelfde zijn in beide gevallen. Dat betekent dat bij deze DDoS aanvallen zowel vóór (H1) als vóór en na (H2) de DDoS aanval relatief meer phishing wordt verzonden. Omdat H1 valt onder H2 betekent dit dus dat vooral steun is gevonden voor hypothese 2: DDoS als rookgordijn.

Tabel 7. DDoS als rookgordijn ten behoeve van de planning van phishing: gemiddeld aantal phishing e-mails in de trendperiode van 60 dagen voor de DDoS aanval en 15 dagen **vóór en na** de DDoS aanval; bij 13 van de 23 DDoS-aanvallen zijn er meer phishing e-mails vóór en na de aanval dan in de periode ervoor.

Aangevallen bedrijf (1)	60 dagen voor de aanval	15 dagen voor en na de aanval	P-Value	Hypothese bevestigd (2)	Verschil in gemiddeld aantal e-mails
Black rights movement ***	4688	6914	0.00	1	2226
Deense spoorwegen ***	680	1810	0.00	1	1130
ABN Amro ***	981	1956	0.00	1	975
Rabobank ***	981	1956	0.00	1	975
E-health Letland / Latvia NVD **	1116	1610	0.05	1	494
ABN Amro **	1116	1610	0.05	1	494
Griekse regering ***	3992	4479	0.00	1	486
DigiD	1372	1487	0.12		115
DigiD	1402	1502	0.13		100
DigiD	1436	1501	0.18		65
Belastingdienst **	1496	1550	0.05	1	54
Rabobank **	1496	1550	0.05	1	54
DigiD **	1496	1550	0.05	1	54
ASN Bank **	1496	1550	0.05	1	54
SNS **	1496	1550	0.05	1	54
Regiobank **	1496	1550	0.05	1	54
Rabobank	1520	1523	0.13		3
ING	1520	1523	0.13		3
ABN Amro	1520	1523	0.13		3
Iran's Internet Infrastructuur *	4151	3900	0.03		-251
GitHub	1533	1280	0.30		-253
Crypto Currency Exchanges **	4162	3823	0.01		-339
ABN Amro ***	1536	866	0.00		-670
Aantal vergelijkingen dat de hypothese bevestigt				13	

(1) Statische significantie: * p <.10, ** p <.05, *** p <.01.
(2): 1=hypothese bevestigd.

3.3 Hypothese 3: DDoS wordt als context of als verhaallijn gebruikt in de phishing e-mails

Na de DDoS komen de '*security*-gerelateerde phishing campagnes. De verwachting, volgens hypothese 3, is dat er meer phishing-e-mails verwijzen naar DDoS of naar online (on)veiligheid na een DDoS campagnes.

Onderzoeksvraag 3. Gaan DDoS-aanvallen vooraf aan specifieke phishing-campagnes, d.w.z. phishing-campagnes die verwijzen naar DDoS-aanvallen of online *security*-problemen? Om de vraag te beantwoorden vergelijken we:

1. Het aantal e-mails in de trendperiode van 30 dagen voor de aanval met de DDoS-periode van vijf dagen na de aanval.

2. Het aantal e-mails in de trendperiode van 60 dagen voor de aanval met de DDoS-periode van 15 dagen na de aanval.

We verwachten dat in de periode na de DDoS aanval meer phishing plaats vindt dan in de trendperiode.

Tabel 8 geeft een overzicht van de resultaten. In 9 van de 23 DDoS aanvallen is het gemiddeld aantal e-mails significant verschillend voor de twee perioden. In lijn met onze hypothese zijn er in 6 gevallen meer phishing e-mails na de DDoS aanval. Dit is het geval bij de aanvallen op E-health Letland/Latvia NVD, de ABN Amro bank (twee maal), de Rabobank, de Deense spoorwegen en de *Black rights movement*. In drie gevallen is het aantal e-maile-mails na de DDoS aanval geringer (een andere aanval op de ABN Amro, Github en Crypto Currency Exchanges. Opnieuw zijn, van boven naar onder de aanvallen gesorteerd op volgorde van de omvang van het verschil in phishing e-mails tussen beide kolommen.

Dit beeld verandert wanneer we alleen de periode van 30 dagen ervoor en vijf dagen ***na*** de DDoS-aanval in beschouwing nemen. Bij drie aanvallen stijgt het aantal phishing e-mails significant na de DDoS-aanval: het gaat om de aanvallen tegen de ABN Amro bank, de Rabobank en Deense spoorwegen; hier zien we een relatief sterke stijging van het aantal phishing e-mails na een DDoS aanval (tabel niet getoond).

Security-gerelateerde e-mails

Deze analyses zijn gerepliceerd voor e-mails die een *security* gerelateerd onderwerp hadden. Bij vijf aanvallen, op de Griekse overheid, de ABN Amro (24 mei 2018 en 9 maart 2020), de Rabobank en de Deense spoorwegen, zien we statistisch significant meer *security* gerelateerde e-mails na de DDOS aanvallen. Dit geldt allemaal voor de analyses die met de trendperiode werken van 60 dagen.

Wanneer de analyse wordt herhaald met de trendperiode van 30 dagen wordt geen samenhang gevonden. Integendeel, er lijkt eerder een dalende trend te zijn in security gerelateerde e-mails na de DDoS aanval (data & figuren niet getoond). Dat is het geval bij de grote DDoS-aanval op Irans internetstructuur, Digid en de aanval op de ABN Amro bank van 31 juli 2018.

Twee voorbeelden voor dit type misdaadketens staan in box 3 en 4.

Tabel 8. DDoS als context voor phishing: gemiddeld aantal phishing e-mails in de trend periode van 60 dagen voor de DDoS aanval en 15 dagen na de DDoS aanval; bij 6 van de 23 DDoS-aanvallen zijn er meer phishing e-mails dan in de periode ervoor.

Aangevallen bedrijf (1)	60 dagen voor de aanval	15 dagen na de aanval	P-Value	Hypothese bevestigd (2)	Verschil in gemiddeld aantal e-mails
Black rights movement ***	5324	6893	0.00	1	1569
Deense spoorwegen ***	953	2033	0.00	1	1080
ABN Amro ***	1305	1920	0.00	1	615
Rabobank ***	1305	1920	0.00	1	615
Griekse regering	4123	4348	0.12		224
E-health Letland / Latvia NVD *	1514	1680	0.02	1	166
ABN Amro *	1514	1680	0.02	1	166
DigiD	1384	1545	0.12		161
DigiD	1356	1453	0.23		97
DigiD	1384	1453	0.26		69
Rabobank	1557	1456	0.24		-102
ING	1557	1456	0.24		-102
ABN Amro	1557	1456	0.24		-102
Belastingdienst	1568	1464	0.25		-105
Rabobank	1568	1464	0.25		-105
DigiD	1568	1464	0.25		-105
ASN Bank	1568	1464	0.25		-105
SNS	1568	1464	0.25		-105
Regiobank	1568	1464	0.25		-105
Iran's Internet Infrastructuur	4096	3928	0.15		-169
Crypto Currency Exchanges *	4129	3891	0.06		-239
GitHub*	1542	989	0.09		-553
ABN Amro ***	1561	119	0.00		-1442
Aantal vergelijkingen dat de hypothese bevestigt			som	6	

(1) Statische significantie: * p <.10, ** p <.05, *** p <.01
(2): 1=hypothese bevestigd.

Box 3. *South African Banking*

Over Zuid-Afrika waren voor het huidige onderzoek onvoldoende gegevens over phishing beschikbaar, maar de casus hieronder illustreert de combinatie van aanvallen die kunnen plaatsvinden. Vanuit Zuid-Afrika berichtte Sparrow (29 October, 2020) over een combinatie van aanvallen: ransomware, dat meestal wordt gedistribueerd via phishing en vervolgens DDoS-aanvallen. Sparrow (29 October, 2020) gaf de volgende beschrijving (vrij vertaald en samengevat door de auteur):

Aanval # 1

- Een ransomware aanval haalt services van de stad Johannesburg uit de lucht. Laat in de avond van donderdag 24 oktober 2019 kondigde de stad Johannesburg aan dat hun netwerk was gehackt.
- De aanval was een ransomware-aanval (wat doorgaans betekent dat belangrijke systemen en / of gegevens worden gecodeerd en vergrendeld door malware).
- Belangrijke systemen werden stilgelegd, inclusief onlinediensten, factuurbetalingen en meer. Andere diensten werden getroffen, waaronder het callcenter dat 112 noodoproepen afhandelt.
- De hackers eisten een losgeld van vier Bitcoins, wat overeenkomt met ongeveer $ 37.000 USD. Ook beweerden de hackers achterdeurtjes in de stadssystemen te hebben geïnstalleerd en dreigden zij de gehackte gegevens online te plaatsen.

Aanval 2

Rond dezelfde tijd dat de ransomware-aanval Johannesburg trof, werden DDoS-aanvallen gelanceerd tegen verschillende grote Zuid-Afrikaanse banken, waaronder Standard Bank en ABSA. Net als de Johannesburg-aanval werden deze DDoS-aanvallen zorgvuldig getimed voor maximale schade - de aanvallen sloegen toe op betaaldag, wat resulteerde in een vertraagd salaris in het hele land.

Box 4. *De UvA en HvA hack*

De hackers die de ICT-systemen van de Universiteit van Amsterdam en de Hogeschool van Amsterdam binnendrongen op 17 februari 2021, hebben mogelijk de hand weten te leggen op de versleutelde wachtwoorden van studenten en medewerkers, aldus Het Parool. Volgens de website van de UvA: '*Hackers hebben mogelijk wel toegang tot accountnamen en wachtwoorden. Daarom vragen we iedereen om zijn of haar wachtwoord te wijzigen (Amsterdam, 4 maart, 2021).*

Phishers probeerden in de dagen na de cyberaanval misbruik te maken van de situatie. Studenten en medewerkers kregen nepmails met het verzoek om vanwege de hack hun account te controleren of hun wachtwoord te wijzigen. De truc werd gebruikt om

gebruikersnamen en wachtwoorden in handen te krijgen.

Uva: *We vragen je wel extra alert te zijn op phishing. Er zijn phishing e-mails in omloop die ingaan op de cyberaanval. Een aantal andere aanvallers probeert misbruik te maken van de huidige situatie. Ze sturen e-mails naar medewerkers en studenten, zogenaamd vanuit de HvA of de UvA, met het verzoek om het account te controleren of wachtwoord te wijzigen*.

BRON: (Goedegebuure, 23 februari 2021, 18:25)

4. Discussie

In dit onderzoek is gezocht naar het bestaan van online misdaadketens ofwel '*crime chains'*. Misdaadketens zijn omschreven als reeksen van verschillende type delicten die samen of in een bepaalde volgorde voorkomen en met elkaar verband houden om een gecoördineerde reeks acties uit te voeren. Felson noemde dit '*Van Dijk' chains*, naar Jan van Dijk, voormalig hoofd WODC (Felson & Clarke, 1998a; Van Dijk, 1994) die beschreef hoe specifieke delicten voorwaarden scheppen voor nieuwe delicten.

Het belang van de studie is het volgende: tot op heden zijn online delicten vooral apart bestudeerd. Er is uitgebreid onderzoek gedaan naar phishing en DDoS. Maar, voor zover ons bekend, zijn tot op heden deze delicten nooit in combinatie onderzocht. Onderzoek naar online criminaliteit heeft zich gericht op georganiseerde daders, maar niet op de mogelijke coördinatie van incidenten.

De huidige studie onderzoekt of er een statistisch verband bestaat tussen de tijdstippen van een DDoS-aanval en het gemiddeld aantal phishing e-mails rondom de DDoS periode. Zoals aangegeven betekent dit dat wij er niet van uitgaan dat er sprake is van causaliteit. Achter de coördinatie van misdrijven kan een veelheid aan oorzaken liggen: het kan gaan om dezelfde (groep) dader(s), het kan toeval zijn zoals wanneer een phishing aanval misbruik maakt van het hacken van een universiteit (zie box 4, hierboven), het kan gebeuren dat (groepen) dader(s) toevallig met elkaar in gesprek zijn geraakt en het kan ook het gevolg zijn van dezelfde achterliggende gebeurtenis, zoals een datalek. Tenslotte, sommige aanvallen blijven op zichzelf staande gebeurtenissen.

Het onderzoek analyseert een set van 1.908.794 e-mails die zijn verzameld door de APWG tussen 01-01-2018 en 31-07-2019, 02-09-2019 en 02-07-2020 en 23 DDoS aanvallen in dezelfde periode en waarover is gerapporteerd in de media. Hieronder worden vooral de belangrijkste resultaten besproken.

In de analyses is onderscheid gemaakt tussen de trendperiode en een *event* periode. De '*trend*'-periode verwijst naar het gemiddeld aantal phishing e-mails dat wordt verzonden tijdens een '*normale*' periode. De '*event'*-periode is de tijd waarin, volgens de hypothese, meer e-mails zouden moeten zijn verzonden. Per hypothese wordt het gemiddeld aantal phishing e-mails van de trendperiode vergeleken met het aantal in de *event*periode.

Wij hebben het gemiddeld aantal e-mails vergeleken voor een trendperiode van 30 dagen met een eventperiode van 5 dagen, en een trendperiode van 60 dagen met een eventperiode van15 dagen. De analyse van 60 dagen voor de trendperiode en 15 dagen

voor de eventperiode geeft duidelijker resultaten. Vandaar dat die gebruikt zijn voor de verdere analyse. Voor de drie onderzoeksvragen zijn de volgende resultaten gevonden.

Hypothese 1: Phishing als planning van botnets en/of DDoS-aanvallen. Bij 13 van de 23 DDoS aanvallen zien we meer phishing voorafgaand aan de DDoS aanval. Dit ondersteunt de stelling dat phishing een rol kan spelen ter voorbereiding van een DDoS aanval.

Hypothese 2: DDoS-aanvallen als afleidingsmanoeuvre of rookgordijn en phishing is de 'echte' aanval.

Bij 13 DDoS aanvallen zien we meer phishing voor én na de DDoS aanval, mogelijk ter afleiding van de DDoS aanval. Vooral bij de DDoS aanvallen op de *Black rights movement*, de ABN Amro (twee aanvallen), de Rabobank en de Deense spoorwegen zijn de verschillen relatief groot. Dit ondersteunt de hypothese dat DDoS soms een afleiding kan zijn voor de phishing aanval.

Hypothese 3: DDoS als context of als verhaallijn. De verwachting is dat er een stijging is in het aantal phishing e-mails kort na een DDoS- aanval?

Voor deze onderzoeksvraag kijken we allereerst of het aantal phishing e-mails stijgt na een DDOS aanval en, ten tweede, en of het aantal phishing e-mails dat verwijst naar veiligheidsproblemen of specifiek naar DDoS-aanvallen, stijgt na een aanval. De resultaten laten zien dat, na zes DDOS aanvallen er een stijging is in phishing, tijdens de 15 dagen nadat de aanval heeft plaats gevonden. Wanneer alleen wordt gekeken naar phishing e-mails die verwijzen naar veiligheidsproblemen, dan blijkt dat bij vijf DDoS-aantallen eveneens een stijging is in het gemiddeld aantal phishing e-mails in de 15 dagen na de aanval. Dit ondersteunt de stelling dat phishing e-mails soms DDoS als een context gebruiken in hun verhaal gericht op de gebruiker.

Wanneer de resultaten voor hypothese 1 worden vergeleken met de resultaten voor hypothese 2 dan blijkt dat van de 13 DDoS aanvallen 11 dezelfde zijn in beide gevallen. Dat betekent dat bij die 11 DDoS aanvallen zowel voor als na de DDoS aanval relatief meer phishing wordt verzonden. Ook blijkt dat ná de DDoS aanval ook het aantal phishing e-mails relatief groter is, en ook hier is er overlap met in de DDoS aanvallen. Bij deze aanvallen, namelijk die gericht tegen de Black rights movement, de Deense spoorwegen, de ABN Amro (twee maal), de Rabobank, E-health Letland / Latvia NVD en de Griekse regering zijn het gemiddeld aantal phishing emails zowel voor als na de DDoS-aanvallen relatief hoog.

De conclusie is daarmee dat bij ruim de helft van de door ons bestudeerde 23 DDoS aanvallen DDoS meer phishing e-mails worden verzonden rondom de DDoS aanval.

Het feit dat de dit bij een deel van de aanvallen wordt gevonden is – in onze visie - voldoende ondersteuning voor onze stelling, namelijk dat er soms coördinatie of afstemming plaats vindt of dat een aanvaller gebruik maakt van de omstandigheden, zoals een DDoS aanval om een phishing campagne te lanceren. Samenwerking en/of coördinatie van aanvallen is gemakkelijker geworden dankzij het internet en allerlei vormen van samenwerking, zoals 'crime-as-a-Service' online zijn ontstaan. De huidige studie biedt statistische ondersteuning voor deze vaststelling.

Op basis van de huidige studie kan niet worden vastgesteld of het om bewuste coördinatie gaat van één of meerdere daders, of dat verschillende daders reageren op wat zij online zien gebeuren. Natuurlijk kan beide aan de hand zijn op verschillende momenten. Of er sprake is van groepsaanvallen moet uitgezocht worden. Coördinatie tussen aanvallers lijkt voor de hand te liggen. Verder onderzoek per aanval moet uitwijzen wat de oorzaken van de coördinatie zouden kunnen zijn en welke de modus operandi zijn. Daarnaast is het duidelijk dat sommige aanvallen op zichzelf staande gebeurtenissen zijn.

Er is weinig wetenschappelijke literatuur op dit onderwerp, maar onze gegevens komen wel overeen met een aantal studies over dit onderwerp (Ricks et al., 2018; Yegneswaran et al., 2003). Ook zijn er meerdere casestudies en verslagen van *security* bedrijven die deze resultaten ondersteunen. Zo stelt Rodov, van het *security* bedrijf Imperva, "*However, a DDoS might be aimed at more than just disrupting service. In recent years we've witnessed cases where large service disruptions came in parallel with other attack vecTors, where, whether intentionally or not, DDoS was used as a smokescreen, to pivot the defending team's attention away from a more sophisticated and precise simultaneous offence, such as ATO (Account Takeover) or phishing"* (Rodov, 2020).

Beleidsimplicaties

1) *Versterking van de opsporing*

Opsporingsinstanties richten zich vaak op afzonderlijke misdrijven. De resultaten van dit onderzoek kunnen de opsporing versterken door de setting en de sequentie van delicten en gerelateerde gebeurtenissen beter te beschrijven en te begrijpen. Daardoor kan de focus van opsporing worden verscherpt. Dit kan, bijvoorbeeld, omdat men weet dat daders van specifieke delicten eveneens via het plegen van andere type delicten kunnen worden opgespoord. Ook zouden opsporingsinstanties die zich richten op afzonderlijke (type) delicten vaker onderzoeken kunnen coördineren of gezamenlijk uitvoeren.

Aangezien er een relatie is tussen phishing- en DDoS-aanvallen, kunnen coalitie-initiatieven zoals N*o-more DDoS, DDoS-fingerprinting,* profiteren van de huidige resultaten door inzichten te delen met phishing-gegevensverzamelingsinitiatieven zoals APWG. Dit kan ons helpen de modus operandi van cybercriminelen beter te begrijpen en politietechnieken te ontwerpen die effectiever zijn om cybercriminaliteit op te sporen en wellicht ook kunnen werken als afschrikking.

2) Preventie

Daarnaast zou meer aandacht kunnen zijn voor het feit dat de ene aanval de ander kan inluiden. Als men weet dat een DDoS aanval een rookgordijn kan zijn, kan men als organisatie alerter zijn voor phishing en bijvoorbeeld werknemers hiervoor waarschuwen.

3) Verstoring en barrièremodellen

De Nederlandse politie heeft een uitgekristalliseerd beleid ten aanzien van DDoS. Zij werkt, m.b.t. DDoS aanvallen, met het volgende 'bollen model'.[9] Dankzij een beter begrip van de *misdaadketens* en gerelateerde gebeurtenissen kunnen barrièremodellen worden ontwikkeld ten behoeve van de bestrijding van phishing en DDoS aanvallen. Dit gebeurt ook door de Nederlandse politie en initiatieven zoals de nationale anti-DDoS-coalitie.

[9] Met dank aan Richard Nijeboer voor het toezenden van dit model: 'Cybercrime bestrijden is meer dan alleen opsporen'.

Box 5. 'Bollen model: Cybercrime bestrijden is meer dan alleen opsporen.

- *Preventie*. Pr*event*ie richt zich op het verhogen van de weerbaarheid en bewustwording van potentiële slachtoffergroepen en/of kwetsbare daders.
- *Schadebeperking*. Schadebeperking is de meest pr*event*ieve interventie binnen het verhogen van de weerbaarheid en bewustwording van potentiële slachtoffergroepen en/ of kwetsbare daders.
- *Notificatie*. Notificatie is gericht op het vergroten van de bewustwording van individuen en organisaties omtrent hun slachtofferschap en slachtofferbehandeling in strafrechtelijke onderzoeken.
- *Verstoring*. Verstoring is gericht op het verstoren van het cybercriminele proces, door bijvoorbeeld neerhalen van een C&C-server, botnet, website of forum.
- *Attributie*. Attributie richt zich op de strafrechtelijke aanpak van cybercrime, waarbij in elk onderzoek de mogelijkheid wordt onderzocht om tot verdachten te komen en deze te vervolgen.

4) Delen van gegevens

In het algemeen is het aan te bevelen om data te delen voor wetenschappelijk onderzoek. Dit geldt zeker voor gegevens over cybersecurity en cybercrime (Leukfeldt, 2017). Op dit moment gebeurt dit onvoldoende. Het huidige onderzoek biedt additionele ondersteuning voor het belang van data delen door de nadruk te leggen op samenwerking en coördinatie van delicten. Het is daarmee van belang om cyberdelicten in hun samenhang te bestuderen. Het delen van gegevens is daar een noodzakelijk onderdeel van.

5) *Stimulans om kleine criminaliteit te melden*

Veel DDoS- of phishing-aanvallen leiden mogelijk niet tot verliezen voor bedrijven. Het melden van deze aanvallen zal onderzoekers echter helpen bij het analyseren van deze misdaadketens. Zelfs vandaag de dag zijn de prikkels voor bedrijven om cybercriminaliteit te melden laag, dit kan worden veranderd met beleidsmatige maatregelen. Zoals hieronder wordt betoogd is het verzamelen van meer gegevens voor onderzoek en beleid van belang.

Beperkingen huidige onderzoek

De huidige studie kent een aantal beperkingen. Een belangrijk punt is dat er geen onafhankelijke tests van de hypotheses zijn uitgevoerd aangezien de periodes die

worden onderzocht overlappen. Een probleem is dat dit moeilijk te vóórkomen is gezien de hypotheses.

Een andere beperking is dat deze studie is gebaseerd op e-mails en DDoS-aanvallen die beiden afkomstig zijn uit internationale datasets. Het was mooier geweest om een meer afgebakende geografische eenheid te kunnen bestuderen, zoals alleen Nederland. Helaas was dit, met betrekking tot phishing, niet mogelijk omdat de Autoriteit Persoonsgegevens ons heeft verhinderd gebruik te maken van de phishing dataset van de FraudeHelpDesk. Zoals hierboven is aangegeven is het niet altijd makkelijk om gegevens te vinden over online criminaliteit.

Ons onderzoek laat zien dat er statistische relaties in de tijd bestaan tussen phishing en DDoS. Maar een statistische samenhang betekent niet noodzakelijk causaliteit. Meer gedetailleerd onderzoek is nodig om te kunnen reconstrueren wat door wie en wanneer is gedaan. Het voorbeeld van de Black Rights movement suggereert dat er allerlei processen een rol kunnen spelen waardoor aanvallen op een gegeven moment specifieke doelen aanvallen. Verder onderzoek zou moeten uitwijzen of verschillende daders of dadergroepen hun activiteiten coördineren, ofwel dat aanvallers, zonder onderling contact te hebben, inspelen op wat zij zien gebeuren op het internet, zoals een DDoS-aanval.

De phishingdata van de APWG kennen ook beperkingen en vertekeningen. Deze zijn niet precies in te schatten en zij worden niet toegelicht door de APWG. De APWG-data zijn phishing e-mails van organisaties, bedrijven en overheden die lid zijn van de APWG. Interessant is om op te merken dat, in de APWG-phishing e-mails, Nederlands de zevende meest voorkomende taal is, terwijl Nederlands de 60ste meest gesproken taal ter wereld is (Ghosh, February 15, 2020). Dit suggereert dat een relatief groot aantal phishing e-mails gericht op Nederland in de APWG-data terecht komt; of dat relatief veel Nederlanders actief zijn op de wereldwijde ‘phishing e-mail markt’.

Toekomstig onderzoek

Ons onderzoek is een eerste bijdrage aan een beter begrip van online misdaadketens. Op verschillende fronten is meer onderzoek nodig. Allereerst zou het goed zijn het onderzoek te kunnen repliceren met andere gegevens, zoals gegevens die bijvoorbeeld een langere tijdspanne beslaan of een scherper afgebakende geografische eenheid.

Daarnaast zou het nuttig zijn een meer diepgravend onderzoek uit te voeren van een aantal casus, om de causaliteit te kunnen achterhalen en de achtergronden van de

waargenomen samenhang beter te begrijpen. Het dieper ingaan op aanvallen is daarbij een interessante weg.

Meer data over cybercrime zijn dringend gewenst. Het is spijtig dat de miljoenen phishing e-mails waar de FraudeHelpDesk over beschikt niet gebruikt mogen worden voor wetenschappelijk onderzoek. Zoals aangegeven is er door meerdere partijen op gewezen dat het veld van cybersecurity moeite heeft om aan data te komen om de huidige dreigingen te analyseren en beter te begrijpen. Als Nederlandse beleidsmakers informatie over ons land willen dan zullen ook Nederlandse gegevens moeten worden geanalyseerd.

Literatuurverwijzingen

Abhishta, A. (2019). *The blind man and the elephant: Measuring economic impacts of ddos attacks* (PhD), University of Twente, Enschede, Nl.

Abhishta, A., Heeswijk, W. v., Junger, M., Nieuwenhuis, L. J. M., & Joosten, R. A. M. G. (2020). Why would we get attacked? An analysis of attacker's aims behind ddos attacks. *Journal of wireless mobile networks, ubiquitous computing, and dependable applications, 11*(2). doi:10.22667/JOWUA.2020.06.30.003

Abhishta, A., Joosten, R. A. M. G., Dragomiretskiy, S., & Nieuwenhuis, L. J. M. (2019). *Impact of successful ddos attacks on a major crypto-currency exchange.* Paper presented at the 2019 27th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP).

Abhishta, A., Joosten, R. A. M. G., Jonker, M., Kamerman, W., & Nieuwenhuis, L. J. M. (2019). *Poster: Collecting contextual information about a ddos attack event using google alerts.* Paper presented at the Proceedings of the 40th IEEE Symposium on Security and Privacy (S&P'19), San Fransisco, USA.

Abhishta, A., Junger, M., Joosten, R. A. M. G., & Nieuwenhuis, L. J. M. (2019). *Victim routine influences the number of ddos attacks: Evidence from dutch educational network.* Paper presented at the IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA.

Aguirre, B. E., & Lane, D. (2019). Fraud in disaster: Rethinking the phases. *International Journal of Disaster Risk Reduction, 39*, 101232.

Amsterdam, U. v. (4 maart, 2021). Veelgestelde vragen (faq's). Cybersecurity. Retrieved from https://www.uva.nl/actueel/cybersecurity/faqs.html#Zijn-mijn-persoonlijke-gegevens-veilig

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., . . . Savage, S. (2013). Measuring the cost of cybercrime. In *The economics of information security and privacy* (pp. 265-300): Springer.

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., . . . Kallitsis, M. (2017). *Understanding the mirai botnet.* Paper presented at the 26th {USENIX} security symposium ({USENIX} Security 17).

APWG. (2020a). Report phishing. Retrieved from https://apwg.org/

APWG. (2020b). Trend reports. Retrieved from http://www.antiphishing.org/trendsreports/

APWG. (2020c). Trend reports. 1st quarter 2020 plus covid-19 coverage. Retrieved from http://www.antiphishing.org/trendsreports/

Bayoumy, Y. (2018). *Cybercrime economy-a netnographic study on the dark net ecosystem for ransomware.* Norwegian University of Science and Technology, Department of Computer Science,

Bijlenga, N., & Kleemans, E. R. (2018). Criminals seeking ict-expertise: An exploratory study of dutch cases. *European Journal on Criminal Policy and Research, 24*(3), 253-268. doi:10.1007/s10610-017-9356-z

Boerman, F., Grapendaal, M., Nieuwenhuis, F., & Stoffers, E. (2017). *Nationaal dreigingsbeeld 2017. Georganiseerde criminaliteit*. Driebergen, Nl.: Landelijke Eenheid, Nationale Politie.

Brewster, T. (June 3, 2020). Huge cyberattacks attempt to silence black rights movement with ddos attacks. *Forbes*. Retrieved from https://www.forbes.com/sites/thomasbrewster/2020/06/03/huge-cyber-attacks-attempt-to-silence-black-rights-movement-with-ddos-attacks/?sh=48d15f0742b6

Brewster, T. (June 11, 2020). Watch out: There's a 'big' black lives matter scam about. *Forbes*. Retrieved from https://www.forbes.com/sites/thomasbrewster/2020/06/11/watch-out-theres-a-big-black-lives-matter-scam-about/?sh=2429ac0b62d8

Broadhurst, R., Grabosky, P., Alazab, M., Bouhours, B., & Chon, S. (2014). An analysis of the nature of groups engaged in cyber crime.
Brunt, R., Pandey, P., & McCoy, D. (2017). *Booted: An analysis of a payment intervention on a ddos-for-hire service.* Paper presented at the Workshop on the Economics of Information Security.
Bullée, J.-W., & Junger, M. (2020a). Social engineering. In T. J. Holt & A. M. Bossler (Eds.), *Palgrave international handbook of cybercrime and cyberdeviance* (pp. 1-28). Cham, Switserland: Palgrave Macmillan.
Bullée, J.-W., & Junger, M. (2020b). Social engineering: Digitale fraude en misleiding. *Justitiele Verkenningen, 46*(2).
Bursztein, E., & Oliveira, D. (2019). *Deconstructing the phishing campaigns that target gmail users*. Paper presented at the Black Hat USA 2019, Las vega, Nevada. https://elie.net/talk/deconstructing-the-phishing-campaigns-that-target-gmail-users/
Clarke, R. V. (2012). Opportunity makes the thief. Really? And so what? *Crime Science, 1*(1), 1-9.
Claude, T. E. A., & Siponen, M. (2014). *Toward a rational choice process theory of internet scamming: The offender's perspective*. Paper presented at the International Conference on Information Systems, Auckland, New Zealand.
Cloufare. (2020). What is a ddos attack? Retrieved from https://www.cloudflare.com/learning/ddos/ddos-attack-tools/ddos-booter-ip-stresser/
Cohen, L. E., & Felson, M. (1979). Social-change and crime rate trends - routine activity approach. *American Sociological Review, 44*, 588-608.
Corbet, S., Lucey, B., Urquhart, A., & Yarovaya, L. (2019). Cryptocurrencies as a financial asset: A systematic analysis. *International Review of Financial Analysis, 62*, 182-199. doi:https://doi.org/10.1016/j.irfa.2018.09.003
Cornish, D. B., & Clarke, R. V. (2017). The reasoning criminal: Rational choice perspectives on offending. In *Environmental criminology and crime analysis* (pp. 29-61). Abingdon, Oxon Routledge: Taylor & Francis Group.
de Santanna, J. J. C. (2017). *Ddos-as-a-service: Investigating booter websites.* (PhD), University of Twente, Enschede, Nl. Retrieved from https://research.utwente.nl/en/publications/ddos-as-a-service-investigating-booter-websites
de Santanna, J. J. C., & Sperotto, A. (2014). *Characterizing and mitigating the ddos-as-a-service phenomenon.* Paper presented at the IFIP International Conference on Autonomous Infrastructure, Management and Security.
de Santanna, J. J. C., van Rijswijk-Deij, R., Hofstede, R., Sperotto, A., Wierbosch, M., Granville, L. Z., & Pras, A. (2015). *Booters—an analysis of ddos-as-a-service attacks.* Paper presented at the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM).
Deeney, N. (June 16, 2020). Black lives matter phishing scam distributes malware [Press release]. Retrieved from https://www.metacompliance.com/blog/black-lives-matter-phishing-scam-distributes-malware/
DNB. (31 januari 2018). Persbericht: Dnb waarschuwt voor 'phishing mail' [Press release]. Retrieved from https://www.dnb.nl/nieuws/nieuwsoverzicht-en-archief/Persberichten2018/dnb372138.jsp
Dubendorfer, T., Wagner, A., & Plattner, B. (2004). *An economic damage model for large-scale internet attacks.* Paper presented at the 13th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises.
Eurostat. (14-10-2020). Individuals - internet activities. Retrieved from http://appsso.eurostat.ec.europa.eu.ezproxy2.utwente.nl/nui/show.do?query=BOOKMARK_DS-053730_QID_4CBC0374_UID_-3F171EB0&layout=TIME,C,X,0;GEO,L,Y,0;INDIC_IS,L,Z,0;UNIT,L,Z,1;IND_TYPE,L,Z,2;INDICATORS,C,Z,3;&zSelection=DS-053730INDICATORS,OBS_FLAG;DS-053730UNIT,PC_IND;DS-053730INDIC_IS,I_IUBK;DS-053730IND_TYPE,IND_TOTAL;&rankName1=UNIT_1_2_-

1_2&rankName2=INDICATORS_1_2_-1_2&rankName3=INDIC-IS_1_2_-1_2&rankName4=IND-TYPE_1_2_0_1&rankName5=TIME_1_0_0_0&rankName6=GEO_1_2_0_1&sortC=ASC_-1_FIRST&rStp=&cStp=&rDCh=&cDCh=&rDM=true&cDM=true&footnes=false&empty=false&wai=false&time_mode=ROLLING&time_most_recent=true&lang=EN&cfo=%23%23%23%2C%23%23%23.%23%23%23

Fafinski, S., Dutton, W. H., & Margetts, H. Z. (2010). Mapping and measuring cybercrime. *OII Working Paper No. 18*. doi:Available at SSRN: http://dx.doi.org/10.2139/ssrn.1694107 or http://dx.doi.org/10.2139/ssrn.1694107

Felson, M. (2006). *The ecosystem for organized crime*: European Institute for Crime Prevention and Control, affiliated with the United Nations Helsinki.

Felson, M., & Clarke, R. V. (1998a). *Opportunity makes the thief practical theory for crime prevention* (98). Retrieved from London, UK:

Felson, M., & Clarke, R. V. (1998b). *Opportunity makes the thief. Police research series, paper 98. Policing and reducing crime unit, research, development and statistics directorate*. London: Home Office.

Felson, M., & Eckert, M. (2016). *Crime and everyday life* (5 ed.). Thousands Oaks CA: Pine Forge Press.

Finklea, K. M. (2015). Dark web. In: Congressional Research Service.

Florêncio, D., & Herley, C. (2010). *Phishing and money mules.* Paper presented at the 2010 IEEE International Workshop on Information Forensics and Security, WIFS 2010.

Ghosh, I. (February 15, 2020). Ranked: The 100 most spoken languages around the world. Retrieved from https://www.visualcapitalist.com/100-most-spoken-languages/

Goedegebuure, J. (23 februari 2021, 18:25). Versleutelde wachtwoorden uva en hva mogelijk in handen van hackers. Retrieved from https://www.parool.nl/amsterdam/versleutelde-wachtwoorden-uva-en-hva-mogelijk-in-handen-van-hackers~b42cc20c/

Goodman, N. (2017). A survey of advances in botnet technologies. *arXiv preprint arXiv:1702.01132*.

Hadnagy, C. (2014). *Unmasking the social engineer: The human element of security*: John Wiley & Sons.

Harris, B., Konikoff, E., & Petersen, P. (2013). Breaking the ddos attack chain. *Institute for Software Research*.

Huang, K., Siegel, M., & Madnick, S. (2017). *Cybercrime-as-a-service: Identifying control points to disrupt. Working paper cisl# 2017-17*. Retrieved from Cambridge, MA:

Hyslip, T. S. (2020). Cybercrime-as-a-service operations. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 815-846.

Hyslip, T. S., & Holt, T. J. (2019). Assessing the capacity of drdos-for-hire services in cybercrime markets. *Deviant Behavior, 40*(12), 1609-1625.

Ianelli, N., & Hackworth, A. (2005). Botnets as a vehicle for online crime. *Forensic computer science IJoFCS, 19*.

IOCTA. (2019). *Internet organised crime threat assessment [2019]*. The Hague, Nl.: European Union Agency for Law Enforcement Cooperation 2019.

Jirovský, V., Pastorek, A., Mühlhäuser, M., & Tundis, A. (2018). *Cybercrime and organized crime.* Paper presented at the Proceedings of the 13th International Conference on Availability, Reliability and Security.

Jonker, M., King, A., Krupp, J., Rossow, C., Sperotto, A., & Dainotti, A. (2017). *Millions of targets under attack: A macroscopic characterization of the dos ecosystem.* Paper presented at the Proceedings of the 2017 Internet Measurement Conference.

Junger, M., Montoya-Morales, L., & Overink, F.-J. (2017). Priming and warnings are not effective to prevent social engineering attacks. *Computers in Human Behavior, 66*, 75-87.
Junger, M., Wang, V., & Schlomer, M. (2020). Fraud against businesses both online and offline - crime scripts, business characteristics, efforts, and benefits. *Crime Science, 9*. doi:https://doi-org.ezproxy2.utwente.nl/10.1186/s40163-020-00119-4
Kallus, N. (2014). *Predicting crowd behavior with big public data.* Paper presented at the Proceedings of the 23rd International Conference on World Wide Web.
Kaspersky Lab. (2016). Research reveals hacker tactics: Cybercriminals use ddos as smokescreen for other attacks on business. Retrieved from https://www.kaspersky.com/about/press-releases/2016_research-reveals-hacker-tactics-cybercriminals-use-ddos-as-smokescreen-for-other-attacks-on-business
Kaur, S., & Randhawa, S. (2020). Dark web: A web of crimes. *Wireless Personal Communications*, 1-28.
Kim, J. H. (2015). *Information theft within different organizational types: A rational choice analysis.* Rutgers University-Graduate School-Newark,
Kim, S. H., Wang, Q.-H., & Ullrich, J. B. (2012). A comparative study of cyberattacks. *Communications of the ACM, 55*(3), 66-73.
Kirkpatrick, K. (2017). Financing the dark web. *Communications of the ACM, 60*(3), 21-22.
Kleemans, E., & Soudijn, M. (2017). Organised crime. *Handbook of Crime Prevention and Community Safety*, 394-406.
Kruisbergen, E. W., Leukfeldt, E. R., Kleemans, E. R., & Roks, R. A. (2018). *Georganiseerde criminaliteit en ict. Rapportage in het kader van de vijfde ronde van de monitor georganiseerde criminaliteit*. Den Haag, Nl.: Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC), Ministerie van Justitie en Veiligheid.
Kurian, T. (April 16, 2020). Protecting businesses against cyber threats during covid-19 and beyond. Retrieved from https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond
Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2020). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *arXiv preprint arXiv:2006.11929*.
Lastdrager, E. (2018). *From fishing to phishing.* (PhD PhD), University of Twente, Enschede, Nl. Retrieved from https://research.utwente.nl/en/publications/from-fishing-to-phishing
Lavorgna, A. (2015). Organised crime goes online: Realities and challenges. *Journal of Money Laundering Control, 18*(2), 153-168. doi:doi:10.1108/JMLC-10-2014-0035
Lavorgna, A., & Sergi, A. (2016). Serious, therefore organised? A critique of the emerging" cyber-organised crime" rhetoric in the united kingdom. *International Journal of Cyber Criminology, 10*(2), 170.
Lawson, P. (2009). Identity-related crime victim issues: A discussion paper. *Commission on Crime Prevention and Criminal Justice, 18th session. Accessed May, 13*, 2011.
Leukfeldt, E. R. (Ed.) (2017). *Research agenda the human factor in cybercrime and cybersecurity*. The Hague, Nl.: Eleven International Publishing.
Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2016). Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. *British Journal of Criminology, 57*(3), 704-722.
Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). A typology of cybercriminal networks: From low-tech all-rounders to high-tech specialists. *Crime, Law and Social Change, 67*(1), 21-37.
Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial

cybercrime as organised crime. *European Journal on Criminal Policy and Research, 23*(3), 287-300. doi:10.1007/s10610-016-9332-z
Levi, M., & Maguire, M. (2004). Reducing and preventing organised crime: An evidence-based critique. *Crime, Law and Social Change, 41*(5), 397-469. doi:10.1023/B:CRIS.0000039600.88691.af
Maestre-Vidal, J., Sotelo-Monge, M.-A., Martínez-Monterrubio, S.-M., Barona-López, L.-I., & Valdivieso-Caraguay, Á.-L. (2019). Profits at the dawn of cybercrime-as-a-service.
Mandelcorn, S., Modarres, M., & Mosleh, A. (2013). *An explanatory model of cyber-attacks drawn from rational choice theory.* Paper presented at the American Nuclear Society Meeting on Risk Management for Complex Socio-Technical Systems (RM4CSS), Washington, D.C.
Manky, D. (2013). Cybercrime as a service: A very modern business. *Computer Fraud & Security, 2013*(6), 9-13. doi:https://doi.org/10.1016/S1361-3723(13)70053-8
Mansfield-Devine, S. (2015). The growth and evolution of ddos. *Network Security, 2015*(10), 13-20.
McCoy, D., Bauer, K., Grunwald, D., Kohno, T., & Sicker, D. (2008). *Shining light in dark places: Understanding the tor network.* Paper presented at the International symposium on privacy enhancing technologies symposium.
McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence*. Retrieved from London, UK: https://www.gov.uk/government/publications/crime-against-businesses-headline-findings-from-the-2012-commercial-victimisation-survey--2/crime-against-businesses-headline-findings-from-the-2012-commercial-victimisation-survey
Microsoft. (2020). *Microsoft digital defense report, september 2020*. Retrieved from https://www.microsoft.com/en-us/download/details.aspx?id=101738
Mirkovic, J., & Reiher, P. (2004). A taxonomy of ddos attack and ddos defense mechanisms. *ACM SIGCOMM Computer Communication Review, 34*(2), 39-53.
Netherlands Bankers Association (NVB). (2020). Veiligheid. Retrieved from https://www.bankinbeeld.nl/thema/veiligheid/
Nolasco Braaten, C., & Vaughn, M. S. (2019). Convenience theory of cryptocurrency crime: A content analysis of us federal court decisions. *Deviant Behavior*, 1-21.
Noroozian, A., Korczyński, M., Gañan, C. H., Makita, D., Yoshioka, K., & Van Eeten, M. (2016). *Who gets the boot? Analyzing victimization by ddos-as-a-service.* Paper presented at the International Symposium on Research in Attacks, Intrusions, and Defenses.
Oest, A., Safei, Y., Doupé, A., Ahn, G.-J., Wardman, B., & Warner, G. (2018). *Inside a phisher's mind: Understanding the anti-phishing ecosystem through phishing kit analysis.* Paper presented at the 2018 APWG Symposium on Electronic Crime Research (eCrime).
Oest, A., Zhang, P., Wardman, B., Nunes, E., Burgis, J., Zand, A., . . . Ahn, G.-J. (2020). *Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale.* Paper presented at the 29th {USENIX} Security Symposium ({USENIX} Security 20).
Osanaiye, O., Choo, K.-K. R., & Dlodlo, M. (2016). Distributed denial of service (ddos) resilience in cloud: Review and conceptual cloud ddos mitigation framework. *Journal of Network and Computer Applications, 67*, 147-165. doi:https://doi.org/10.1016/j.jnca.2016.01.001
Paganini, P. (November 6, 2015). Protonmail has paid a $6000 ransom to stop prolonged ddos attacks that knocked its services offline since tuesday. Unfortunately, the attacks are continuing. *Security Affairs*.
Pappalardo, D., & Messmer, E. (May 16, 2005). Extortion via ddos on the rise, criminals are using the attacks to extort money from victimized companies. *ComputerWorld*. https://www.computerworld.com/article/2556543/security0/extortion-via-ddos-on-the-rise.html

Putman, C. G. J., Abhishta, A., & Nieuwenhuis, L. J. M. (2018, 21-23 March 2018). *Business model of a botnet.* Paper presented at the 2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP), Cambridge, United Kingdom.
Ramzan, Z. (2010). Phishing attacks and countermeasures. In *Handbook of information and communication security* (pp. 433-448): Springer.
Redmiles, E. M., Mazurek, M. L., & Dickerson, J. P. (2018). *Dancing pigs or externalities?: Measuring the rationality of security decisions.* Paper presented at the Proceedings of the 2018 ACM Conference on Economics and Computation.
Ricks, B., Thuraisingham, B., & Tague, P. (2018). *Lifting the smokescreen: Detecting underlying anomalies during a ddos attack.* Paper presented at the 2018 IEEE International Conference on Intelligence and Security Informatics (ISI).
Rodov, M. (2020). Lift the ddos smokescreen: Investigate underlying attacks. Retrieved from https://www.imperva.com/blog/lift-the-ddos-smokescreen-investigate-underlying-attacks/
Sachdeva, M., Singh, G., Kumar, K., & Singh, K. (2010). Ddos incidents and their impact: A review. *Int. Arab J. Inf. Technol., 7*(1), 14-20.
Sauter, M. (2013). "Loic will tear us apart" the impact of tool design and media portrayals in the success of activist ddos attacks. *American Behavioral Scientist, 57*(7), 983-1007.
Schneier, B. (2000). *Secrets and lies: Digital security in a networked world*. New York: John Wiley & Sons.
Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. *Computers & Security, 58*, 216-229. doi:http://dx.doi.org/10.1016/j.cose.2015.12.006
Sparrow, J. (29 October, 2020). Cyber attacks hit the city of johannesburg and south african banks. *Hashed Out*. https://www.thesslstore.com/blog/cyber-attacks-hit-the-city-of-johannesburg-and-south-african-banks/
Tambe Ebot, A. C., & Siponen, M. (2014). Toward a rational choice process theory of internet scamming: The offender's perspective.
Tanabe, R., Tamai, T., Fujita, A., Isawa, R., Yoshioka, K., Matsumoto, T., . . . van Eeten, M. (2020). *Disposable botnets: Examining the anatomy of iot botnet infrastructure.* Paper presented at the Proceedings of the 15th International Conference on Availability, Reliability and Security.
Tcherni-Buzzeo, M., Davis, A., Lopes, G., & Lizotte, A. (2016). The dark figure of online property crime: Is cyberspace hiding a crime wave? *Justice Quarterly, 33*(5), 890-911. doi:10.1080/07418825.2014.994658
Thomas, K., Huang, D., Wang, D., Bursztein, E., Grier, C., Holt, T. J., . . . Vigna, G. (2015). Framing dependencies introduced by underground commoditization.
US-CERT. (2019). Understanding denial-of-service attacks. Last revised: November 20, 2019. Retrieved from https://us-cert.cisa.gov/ncas/tips/ST04-015
Van Dijk, J. J. (1994). Understanding crime rates: On the interactions between the rational choices of victims and offenders. *British Journal of Criminology, 34*(2), 105-121.
van Eeten, M., Asghari, H., Bauer, J. M., & Tabatabaie, S. (2011). *Internet service providers and botnet mitigation a fact-finding study on the dutch market. Report prepared for the netherlands ministry of economic affairs, agriculture and innovation*. Retrieved from Delft: http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/01/13/internet-service-providers-and-botnet-mitigation.html
van Eeten, M., Lone, Q., Moura, G., Asghari, H., & Korczyński, M. (2016). Evaluating the impact of abusehub on botnet mitigation. *arXiv preprint arXiv:1612.03101*.
Verizon Risk Team. (2018). *2018 data breach investigations report. 11th edition*. Retrieved from http://www.verizonenterprise.com/DBIR/2013/
Verizon Risk Team. (2019). *2019 data breach investigations report*. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/

Verizon Risk Team. (2020). *2020 data breach investigations report*. Retrieved from https://enterprise.verizon.com/en-nl/resources/reports/dbir/
Wainwright, P., & Kettani, H. (2019). *An analysis of botnet models.* Paper presented at the Proceedings of the 2019 3rd International Conference on Compute and Data Analysis.
Walle, J. v. d. (2018). Phishing after ddos attacks – a good combination? Retrieved from https://phishingtest.com/blog/phishing-after-ddos/
Woollaston, V. (2020). How to access the dark web: What is tor and how do i access dark websites? Retrieved from https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html
Xu, Z., & Hu, Q. (2018). *The role of rational calculus in controlling individual propensity toward information security policy non-compliance behavior.* Paper presented at the Proceedings of the 51st Hawaii International Conference on System Sciences.
Yegneswaran, V., Barford, P., & Ullrich, J. (2003). Internet intrusions: Global characteristics and prevalence. *ACM SIGMETRICS Performance Evaluation Review, 31*(1), 138-147.
Zabyelina, Y. G. (2017). Can criminals create opportunities for crime? Malvertising and illegal online medicine trade. *Global Crime, 18*(1), 31-48.
Zand, A., Modelo-Howard, G., Tongaonkar, A., Lee, S.-J., Kruegel, C., & Vigna, G. (2017). Demystifying ddos as a service. *IEEE Communications Magazine, 55*(7), 14-21.