Ontwikkelingstrajecten van hackers: een longitudinale studie naar defacements op Nederlandse websites

Steve van de Weijer, Rutger Leukfeldt & Thomas Holt

In deze studie onderzoeken we de ontwikkelingstrajecten van hackers, op basis van zelfgerapporteerde web defacements. *Tijdens een web defacement wordt ongewenst de inhoud van een website aangepast. In totaal hebben we 50.330 defacements van websites met een Nederlandse extensie (.nl websites) geanalyseerd, die door 3640 verschillende defacers zijn uitgevoerd tussen januari 2010 en maart 2017. Met behulp van trajectory-modellen kunnen er zes groepen defacers worden onderscheiden in de analyses: twee groepen chronische daders en vier groepen daders die slechts gedurende een korte periode defacements uitvoerden. Deze groepen verschillen ook van elkaar in hun motivaties en modus operandi. De groep hoogfrequente chronische daders bestaat uit minder dan 2% van de daders, maar is verantwoordelijk voor meer dan de helft van alle defacements. Het zou dan ook het meest efficiënt zijn wanneer toekomstige interventies zich met name richten op deze kleine groep chronische daders. Voor vervolgonderzoek zou het interessant zijn om de inhoudelijke boodschap van de web defacements te onderzoeken.*

Introductie

Binnen de criminologie is er de afgelopen decennia veel aandacht geweest voor de ontwikkeling van crimineel gedrag over de levensloop van delinquenten, en diverse studies hebben aangetoond dat er verschillende longitudinale patronen van crimineel gedrag onderscheiden kunnen worden (zie bijv. Jolliffe et al., 2017; Piquero, 2008). In hoeverre dergelijke patronen ook gevonden kunnen worden voor cybercriminaliteit is nog onbekend, voornamelijk door een gebrek aan grootschalige longitudinale data over online delinquentie (Leukfeldt, 2017). Gezien de sterk toegenomen prevalentie van cybercriminaliteit gedurende de afgelopen twee decennia, is het echter van groot belang om ook meer inzicht te krijgen in de ontwikkeling van online crimineel gedrag over tijd.

In deze studie richten we ons op de daders van een specifieke vorm van *hacking* (i.e., het illegaal inbreken in computers of computernetwerken), namelijk *web defacements*. Een defacement wordt ook wel omschreven als het bekladden van een website en kan daarom gezien worden als een digitale vorm van graffiti. Tijdens een defacement wordt ongewenst de inhoud van een website aangepast, zodat er door de defacer geselecteerde afbeeldingen, tekst of geluidsbestanden worden weergegeven (Holt et al., 2017; Jordan & Taylor, 2004). Er kunnen verschillende methoden worden gebruikt om de inhoud van de website aan te passen tijdens een defa-

cement, zoals SQL-injecties, file inclusion, of simpelweg het raden van het wachtwoord van de administrator van de website.[1]
Wij maken gebruik van het archief van web defacements dat wordt bijgehouden op de website 'Zone-H' (www.zone-h.com). Deze website is, in verschillende vormen, al meer dan een decennium actief en geeft defacers de mogelijkheid om publiekelijk te rapporteren over de websites die ze hebben gedefaced. Door de duizenden defacements die er jaarlijks gearchiveerd worden, kan dit archief beschouwd worden als de meest uitgebreide dataset over zelfgerapporteerde defacementactiviteit die beschikbaar is. Dat dit een veelvoorkomende vorm van cybercriminaliteit is, blijkt wel uit de statistieken van Zone-H, die aantonen dat er tussen 2010 en 2016 jaarlijks tussen de 888.000 en 1.608.000 defacements werden gerapporteerd (Romanga & Van den Hout, 2017). Aangezien niet alle defacements aan Zone-H gerapporteerd worden, ligt de daadwerkelijke prevalentie van defacements nog hoger. Gezien deze hoge prevalentie is het van belang om meer kennis te vergaren over defacers en de ontwikkeling van hun betrokkenheid in deze veelvoorkomende vorm van cybercriminaliteit.
In deze studie analyseren wij in totaal 50.330 defacements van Nederlandse websites (i.e., met een .nl extensie), die door 3640 verschillende defacers zijn uitgevoerd tussen januari 2010 en maart 2017. De defacers kunnen hackers betreffen die individueel te werk gaan of groepen hackers die onder dezelfde naam websites defacen. Wij analyseren zowel het aantal uitgevoerde defacements als de actieve periode van deze defacers. Daarmee beantwoorden wij de volgende onderzoeksvragen: In hoeverre kunnen verschillende longitudinale ontwikkelingstrajecten worden onderscheiden onder defacers van Nederlandse websites? En verschillen defacers met verschillende ontwikkelingstrajecten in hun motivaties voor defacements, hun keuze voor aan te vallen websites en de hackingtechnieken die ze gebruiken?

Theorie

Typologische theorieën binnen de criminologie veronderstellen dat de ontwikkeling van delinquent gedrag varieert tussen verschillende typen daders. De meest invloedrijke typologische theorie is waarschijnlijk Moffitts (1993) *dual taxonomy*, waarin een onderscheid gemaakt wordt tussen *adolescence-limited* en *life-course persistent* daders. De laatstgenoemde groep criminelen begint al op jonge leeftijd met delinquent gedrag en pleegt ook gedurende de volwassenheid veel delicten. De groep *adolescence-limited* daders, aan de andere kant, is veel groter en pleegt enkel tijdelijk delicten tijdens de adolescentie. Typologische theorieën zijn de laatste decennia vaak getoetst met behulp van *trajetory analyses* (Nagin, 1999, 2005). Piquero (2008) presenteerde een systematisch overzicht van meer dan tachtig studies die trajectory-analyses gebruikten om ontwikkelingstrajecten van delinquenten

1 Een SQL-injectie is het misbruik maken van een kwetsbaarheid van een computerapplicatie, waarbij de aanvaller de invoer van informatie in een database kan aanpassen. SQL (*Structured Query Language*) is een veelgebruikte standaardtaal om te communiceren met databases. *File inclusion* is het misbruiken van een kwetsbaarheid op een website waardoor de hacker een bestand op de server van de website kan zetten, meestal met behulp van een bestaand script op de webserver.

doi: 10.5553/TvV/.000019

in kaart te brengen. Hij kwam tot de conclusie dat er gemiddeld tussen de drie en vijf groepen onderscheiden kunnen worden met verschillende patronen van criminaliteit over de levensloop. In lijn met Moffitts (1993) taxonomie, werden er ook vaak groepen geïdentificeerd waarvan het delinquente gedrag piekte tijdens de adolescentie of juist gedurende de gehele onderzoeksperiode persistent doorging. Daarnaast wordt er met trajectory-analyses vaak een groep daders gevonden die pas start met crimineel gedrag in de volwassenheid (zie bijv. Van Koppen et al., 2014).[2] Ook in een meer recent systematisch overzicht van Jolliffe en collega's (2017) onder veertien prospectieve longitudinale studies werd bewijs gevonden voor deze drie ontwikkelingspaden van criminaliteit gedurende de levensloop.

De hierboven besproken studies richtten zich zonder uitzondering op 'offline' vormen van criminaliteit. Door een gebrek aan grootschalige longitudinale data over online vormen van criminaliteit (Leukfeldt, 2017), blijft het de vraag of vergelijkbare ontwikkelingstrajecten worden gevonden voor cybercriminelen. Er zijn echter een aantal redenen op basis waarvan verwacht kan worden dat er ook onder web defacers onderscheid te maken is tussen een groep persistente daders is die over een langere periode veel websites aanvallen en een groep die zich slechts gedurende een korte periode bezighoudt met het defacen van websites. Op de eerste plaats zou het zo kunnen zijn dat web defacers meer mogelijkheden hebben om over een langere periode actief te blijven dan traditionele criminelen, gezien de moeilijkheden om cybercriminelen op te sporen en de lage kans om veroordeeld te worden (Brenner, 2008; Holt, 2018; Hutchings & Holt, 2017). Ten tweede willen defacers van websites juist dat hun delict zichtbaar is voor anderen, in tegenstelling tot daders van de meeste traditionele delicten. Deze cybercriminelen kunnen hierdoor geneigd zijn om gedurende een langere periode websites te defacen om zo hun expertise en beheersing van hackingtechnieken aan te tonen (Holt et al., 2017). Anderzijds zullen er echter ook defacers zijn die slechts een paar websites defacen en het slechts beschouwen als opstapje naar meer serieuze hacks (Holt et al., 2017). Ook kunnen ze het aanvallen van websites saai vinden en in het geheel stoppen met hun hackingactiviteiten (Holt, 2010).

Hoewel de longitudinale ontwikkelingstrajecten van hackers nog niet eerder onderzocht zijn, hebben eerdere studies wel getracht verschillende groepen hackers te classificeren op basis van hun vaardigheden en motivaties in plaats van de timing en frequentie van hun delicten (bijv. Rogers, 2006; Van der Wagen et al., 2019). Ook het defacen van websites kan het gevolg zijn van verschillende motivaties, waarbij het in de meeste gevallen niet gaat om financieel gewin van de aanvaller (Woo et al., 2004). Defacers kunnen bijvoorbeeld voor hun eigen vermaak of voldoening hun vaardigheden demonstreren en proberen of ze een specifiek doel echt kunnen aanvallen (Holt, 2007; Jordan & Taylor, 2004; Woo et al., 2004). Het succesvol uitvoeren van een aanval, met name tegen high-profile of publieke doelen, kan er ook toe leiden dat een defacer meer status en respect krijgt binnen de hackersgemeenschap (Holt, 2007; Taylor, 1999; Woo et al., 2004). Daarnaast kan

2 Er bestaat echter discussie of deze late starters pas echt in de volwassenheid beginnen met delinquent gedrag of dat ze dan pas voor het eerst in beeld komen bij justitie (zie bijv. McGee & Farrington, 2010).

een deel van de defacements uitgevoerd zijn vanwege wraak wanneer de hacker in onmin leeft met een bepaalde persoon, bedrijf of instantie (Jordan & Taylor, 2004; Kilger, 2011), terwijl er ook groeiend bewijs is dat sommigen hacks worden uitgevoerd vanuit nationalistische, politieke of ideologische motieven (Andress & Winterfeld, 2013; Holt et al., 2017; Jordan & Taylor, 2004). Holt en collega's (2020) toonden aan dat de verschillende motivaties ook samenhangen met de gebruikte hackingtechnieken en de selectie van het doelwit. In de huidige studie zullen we onderzoeken of web defacers met verschillende longitudinale ontwikkelingstrajecten ook verschillende motivaties hebben om de aanvallen uit te voeren.

Methoden

Data

In deze studie wordt gebruikgemaakt van het archief van web defacements dat wordt bijgehouden op de website Zone-H. Wanneer hackers een website hebben gedefaced, kunnen ze hun acties melden op de Zone-H-website via een onlineformulier. Hierin wordt hun gevraagd om een *hacker handle* (bijv. een online identiteit van het individu of de groep) te gebruiken waaronder de defacement gemeld wordt. Melders wordt ook gevraagd om enkele specifieke kenmerken in te vullen over de web defacements, zoals het betrokken webdomein, de datum en tijd, de gebruikte methode en de motivatie voor de aanval. De informatie wordt doorgestuurd naar de sitebeheerders van Zone-H die de claims valideren en vervolgens de defacement archiveren. De data in het Zone-H-archief biedt hierdoor een compleet overzicht van alle gerapporteerde en geverifieerde defacements en de kenmerken van deze aanvallen. Deze kenmerken worden in deze studie gebruikt als onafhankelijke variabelen en verder beschreven in de subparagraaf Variabelen. Figuur 1 toont het Zone-H-archief zoals dit online te vinden is. De ontwikkelingstrajecten van defacers zijn gebaseerd op het aantal aanvallen dat zij gedurende de onderzoeksperiode hebben uitgevoerd. Hierbij is een onderscheid gemaakt tussen twee typen defacements: *mass defacements* en *single defacements*. Tijdens een mass defacement worden er zo veel mogelijk pagina's, die vanuit dezelfde server worden gehost, tegelijkertijd aangevallen.

Tijdschrift voor Veiligheid 2021 (20) 2
doi: 10.5553/TvV/.000019

Figuur 1 Screenshot van het Zone-H-archief (www.zone-h.org/archive; gemaakt op 2 oktober 2020)

In de data van Zone-H worden alle pagina's die gedurende één mass defacement worden aangevallen echter als een aparte web defacement genoteerd. Om te voorkomen dat het aantal aanvallen wordt overschat door zulke mass defacements hebben we ervoor gekozen om alle websites die tijdens een mass defacement zijn gedefaced door dezelfde hacker, op dezelfde dag, met dezelfde modus operandi en dezelfde motivatie, als één aanval te tellen. Single defacements zijn gericht op een enkele webpagina of url en worden daarom allemaal geteld als aparte aanvallen. Dit resulteerde uiteindelijk in een totaal van 50.330 gerapporteerde aanvallen uitgevoerd door 3640 unieke hackers of hackergroepen,[3] wat neerkomt op een gemiddeld aantal van 13,83 gerapporteerde aanvallen per hacker (variërend tussen de 1 en 4801 gerapporteerde aanvallen). Op basis van de gerapporteerde data van de aanvallen zijn ze opgedeeld over de 29 kwartalen tussen januari 2010 en maart 2017.

3 Gevallen waarbij verschillen in hacker handles duidelijk het gevolg waren van typefouten (bijv. het gebruik van een hoofdletter in plaats van een kleine letter of een ontbrekende spatie tussen twee woorden) zijn gecorrigeerd en geteld als één hacker.

Variabelen

De overige variabelen in de analyses werden gebruikt om verschillen te beschrijven tussen de groepen defacers met verschillende ontwikkelingstrajecten. Allereerst is er een variabele geconstrueerd die de duur van de defacementcarrière aangeeft. Deze duur is gelijk aan het aantal dagen tussen de eerste en laatste aanval van een defacer.

Ten tweede hebben alle defacers de motivaties voor het defacen van een website gerapporteerd. Hierbij konden ze kiezen uit zes opties: 1) voor de lol, 2) voor de uitdaging, 3) om de beste defacer te worden, 4) patriottisme, 5) politieke redenen, 6) wraak tegen een website. Deze zes categorieën zijn door Zone-H bepaald en hierdoor is het mogelijk dat ze enige overlap vertonen (bijv. patriottisme en politieke redenen) en behoren niet alle motivaties die uit andere onderzoeken naar voren kwamen (bijv. nieuwsgierigheid, financieel gewin) tot de antwoordcategorieën.

Een derde variabele geeft aan of een defacer de hoofdpagina of een subpagina van een website heeft gedefaced. Een defacement op de hoofdpagina zal meer aandacht genereren, omdat deze onmiddellijk zichtbaar is voor iedereen en kan duiden op een gerichte aanval, terwijl aanvallen van andere pagina's er mogelijk op wijzen dat een aanvaller simpelweg zo veel mogelijk succesvolle aanvallen wil hebben.

Daarnaast is er een dichotome variabele gebruikt in de analyse die aangeeft of een aanval een mass defacement of een single defacement was.

Een andere dichotome variabele geeft aan of er sprake was van een redefacement (i.e., een aanval op een website die al eerder is gedefaced) of niet.

Verder wordt er een binaire variabele meegenomen in de analyses die het besturingssysteem van de server van de aangevallen website aangeeft. Hierbij kan verwacht worden dat *open source*-programma's, zoals Linux, beter beveiligd zijn dan *closed source*-programma's, doordat problemen publiekelijk worden gerapporteerd en verholpen. Omdat de grote meerderheid van de servers in deze steekproef gebruikmaakt van een variant van een Linux-besturingssysteem, is er een onderscheid gemaakt tussen Linux-besturingssystemen en niet-Linux-besturingssystemen, zoals Macintosh, Microsoft en Unix.

Ook de locatie van de server van de website in de fysieke wereld wordt meegenomen in de analyse. Aangezien de meeste websites met een .nl extensie vanuit Nederland worden gehost, is er een dichotome variabele gecreëerd die aangeeft of de fysieke hosting locatie in Nederland is of niet.

Tot slot rapporteerden de hackers aan Zone-H welke methoden ze gebruikt hebben. Deze zijn gehercodeerd naar zes categorieën: 1) SQL-injecties, 2) bekende kwetsbaarheden, 3) file inclusion, 4) server intrusion, 5) andere methoden, 6) onbekend.

Analyses

Semi-parametric group-based trajectory-modellen zijn gebruikt om defacers met verschillende ontwikkelingstrajecten van elkaar te onderscheiden. In zulke modellen wordt de onbekende onderliggende continue verdeling van – in dit geval – defacements van een onbekend aantal groepen geschat (Nagin, 1999, 2005). In dit geval maken wij gebruik van een *zero-inflated Poisson*-model, aangezien het aantal defacements in een periode (i.e., een kwartaal) een *count*-variabele is en de score op de

doi: 10.5553/TvV/.000019

variabele bovengemiddeld vaak 0 is, doordat veel defacers niet in alle perioden aanvallen uitvoerden. Daarnaast zijn er defacers die erg actief waren gedurende specifieke perioden, wat leidde tot extreem hoge waarden, zoals een hacker(groep) die 2382 aanvallen uitvoerde in één kwartaal. Om voor zulke *outliers* te controleren, werd de uitkomstvariabele in de trajectory-analyse gehercodeerd en zijn de gevallen waarbij een hacker(groep) meer dan tien aanvallen uitvoerde binnen één kwartaal ingesteld als het maximale aantal van tien aanvallen per kwartaal.[4]
Normaliter worden de trajecten bij een trajectory-analyse geschat over de leeftijd van de respondenten. Omdat de Zone-H-data geen informatie over de leeftijd van de defacers bevat, is er in dit geval voor gekozen om het kwartaal waarin de eerste defacement van een hacker(groep) plaatsvond als uitgangspunt te nemen en te kijken hoe het aantal defacements zich in de daaropvolgende kwartalen ontwikkelt. Omdat een aanzienlijk deel van de defacers pas op een later moment binnen de onderzoeksperiode voor het eerst een defacement heeft uitgevoerd, zijn de trajecten niet op basis van alle 29 kwartalen tussen januari 2010 en maart 2017 geschat, maar slechts op de zestien kwartalen (i.e., vier jaar) volgend op de eerste defacement. Indien een hacker bijvoorbeeld de eerste defacement uitvoert in februari 2012, zijn dus de zestien kwartalen van 2012 tot en met 2015 gebruikt om de trajecten te schatten.
Het Bayesian Information Criterion (BIC) werden gebruikt om het optimale aantal groepen te bepalen, waarbij het model met de hoogste BIC-waarde het beste bij de data past. Daarnaast wordt gekeken naar de *average posterior probability of assignement* (AvePP) en *odds of correct classification* (OCC), waarbij waarden hoger dan respectievelijk 0,7 en 5 erop duiden dat defacers met grote nauwkeurigheid aan de groepen zijn toegewezen. Voor meer informatie over de AvePP, OCC en trajectory-modellen in het algemeen zie Bijleveld et al. (2015) of Nagin (2005).

Resultaten

Trajectory-modellen variërend van één tot tien verschillende groepen werden geschat. De BIC-waarden bleven stijgen bij elke additionele groep die aan het model werd toegevoegd, iets wat niet ongewoon is in studies die grote datasets gebruiken (zie bijv. Blokland, Nagin & Nieuwbeerta, 2005; Van Koppen et al., 2014). Nagin (2005) raadt in zulke gevallen aan om meer subjectieve criteria, zoals het doel van de analyse, te gebruiken om het aantal groepen te selecteren. In dit geval kiezen we ervoor om een model met zes groepen te gebruiken, omdat het toevoegen van meer groepen aan het model niet leidt tot substantieel andere trajecten.[5]
Figuur 2 laat de ontwikkeling van de trajecten in het model met zes groepen zien. De eerste groep is veruit de grootste groep (N = 2382; 65,4%) en bestaat uit defacers die in één kwartaal aanvallen hebben uitgevoerd en vervolgens gestopt zijn

4 In totaal kwam het in 560 van de 105.618 gevallen (0,5%) voor dat een hacker(groep) in één kwartaal meer dan tien aanvallen uitvoerde.

5 De *average posterior probability of assignement* (AvePP) en *odds of correct classification* (OCC) in het model met zes groepen zijn alle hoger dan resp. 0,7 en 5 (zie tabel 1). Dit duidt erop dat de defacers met grote nauwkeurigheid aan de groepen zijn toegewezen.

doi: 10.5553/TvV/.000019

met het defacen van websites, of dit niet meer gerapporteerd hebben aan Zone-H. Deze groep hebben we de Sporadische (SP) defacers genoemd. Uit tabel 1 blijkt dat deze SP-defacers gemiddeld slechts 1,61 aanvallen hebben uitgevoerd in een gemiddelde tijdsperiode van 11,83 dagen. Ten tweede komt er een Laag Frequent Dalende (LFD) groep naar voren uit de analyses, die net als de SP-groep slechts enkele aanvallen uitvoerden, maar dit gedurende meerdere kwartalen deden. De 592 defacers (16,3%) in deze groep voerden gemiddeld 5 aanvallen uit binnen een jaar tijd (gemiddeld 344,53 dagen).

Ook de 174 defacers (4,8%) in de derde groep in figuur 2, de Midden Frequent Dalende (MFD) groep, waren slechts een relatief korte periode actief (gemiddeld 400,36 dagen). Met een gemiddeld aantal aanvallen van 15,98 voerden zij echter wel aanzienlijk meer aanvallen uit dan de LFD-defacers. Ten vierde wordt er een Midden Frequent Chronische (MFD) groep onderscheiden in figuur 2. De 143 defacers (3,9%) in deze groep voerden gedurende de gehele onderzoeksperiode een aantal defacements per kwartaal uit en komen zodoende uit op gemiddeld 51,70 defacements gedurende 906,80 dagen.

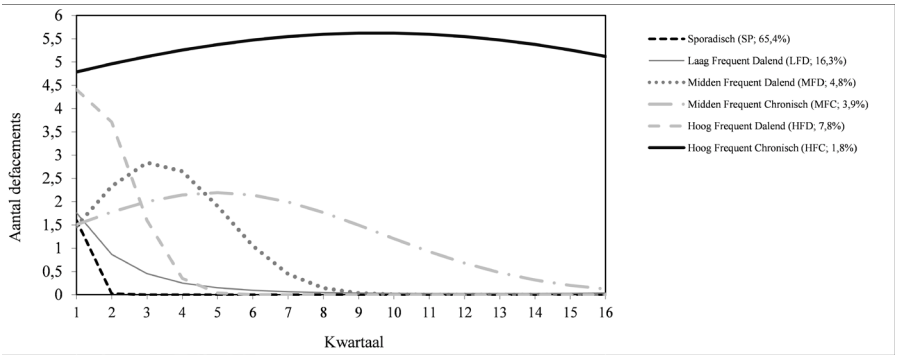
Tot slot toont figuur 2 aan dat er twee groepen zijn waarvan de defacers zeer actief zijn wanneer ze starten met het uitvoeren van defacements. Het aantal defacements van de Hoog Frequent Dalende (HFD) groep neemt daarna echter snel af en na een jaar voert deze groep nog nauwelijks aanvallen uit. De 284 HFD-defacers (7,8%) komen daardoor gemiddeld slechts tot een totaal van 16,27 defacements in een periode van 141,86 dagen. De 65 defacers (1,8%) in de Hoog Frequent Chronische (HFC) groep, daarentegen, bleven gedurende de gehele onderzoeksperiode erg actief en voerden in elk kwartaal een groot aantal defacements uit. Gemiddeld genomen voerden de HFC-defacers 441,88 aanvallen uit in een tijdsbestek van 988,75 dagen. In totaal is deze kleine groep HFC-defacers daardoor verantwoordelijk voor 28.728 van alle 50.330 defacements. In andere woorden, minder dan 2% van de defacers was verantwoordelijk voor 57,1% van alle aanvallen op Nederlandse websites die zijn gerapporteerd aan Zone-H tussen januari 2010 en maart 2017.

Tabel 1 Kenmerken van de zes groepen defacers

Groep	N (%)	Avepp	OCC	Gemiddeld aantal aanvallen	Duur van de defacement-carrière
1. Sporadisch (SP)	2382 (65,4%)	0,95	10,82	1,61	11,83
2. Laag Frequent Dalend (LFD)	592 (16,3%)	0,84	25,63	5,00	344,53
3. Midden Frequent Dalend (MFD)	174 (4,8%)	0,85	99,27	15,98	400,36
4. Midden Frequent Chronisch (MFC)	143 (3,9%)	0,91	219,69	51,70	906,80
5. Hoog Frequent Dalend (HFD)	284 (7,8%)	0,82	57,01	16,27	141,86
6. Hoog Frequent Chronisch (HFC)	65 (1,8%)	0,95	885,76	441,88	988,75
Totaal	3640 (100%)			13,82	147,26

doi: 10.5553/TvV/.000019

Figuur 2 Ontwikkelingstrajecten van de zes groepen defacers

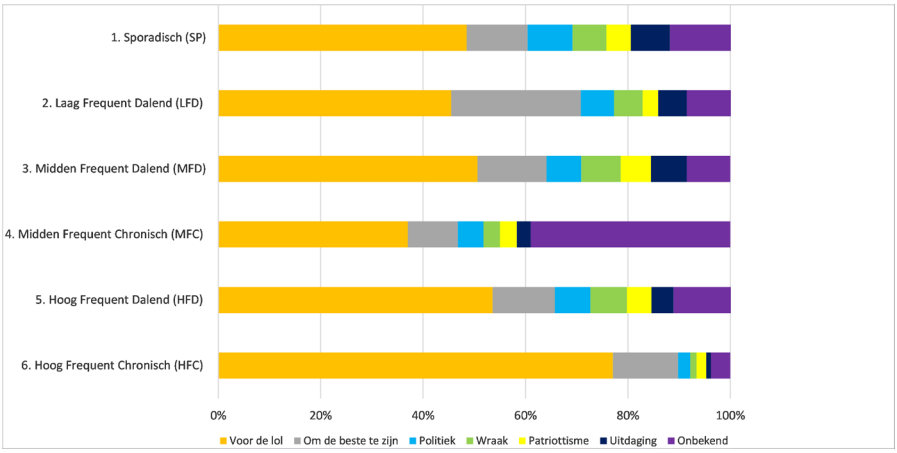


Vervolgens is onderzocht of de zes groepen defacers verschilden in de motivaties die ze hadden voor hun aanvallen. De verdeling van de gerapporteerde motivaties worden getoond in tabel 2 en visueel weergegeven in figuur 3.

Tabel 2 Motivaties van de zes groepen defacers

Groep	Voor de lol	Om de beste te zijn	Politiek	Wraak	Patriottisme	Uitdaging	Onbekend	Totaal
1. Sporadisch (SP)	48,5%	11,9%	8,8%	6,6%	4,8%	7,6%	11,9%	100%
2. Laag Frequent Dalend (LFD)	45,5%	25,3%	6,5%	5,6%	3%	5,6%	8,6%	100%
3. Midden Frequent Dalend (MFD)	50,6%	13,5%	6,8%	7,7%	5,9%	7%	8,5%	100%
4. Midden Frequent Chronisch (MFC)	37,0%	9,8%	5,0%	3,2%	3,3%	2,7%	39%	100%
5. Hoog Frequent Dalend (HFD)	53,6%	12,1%	7,0%	7,1%	4,8%	4,3%	11,2%	100%
6. Hoog Frequent Chronisch (HFC)	77,1%	12,7%	2,4%	1,2%	1,9%	0,9%	3,8%	100%
Totaal	63,6%	12,9%	4,2%	3,1%	2,9%	2,6%	10,8%	100%

Figuur 3 Visuele weergave motivaties van de zes groepen defacers



Gemiddeld genomen zijn de meeste aanvallen uitgevoerd voor de lol (63,6%), om de beste defacer te zijn (12,9%), of zonder een motivatie te rapporteren (10,8%). Er zijn echter ook duidelijke verschillen tussen groepen. De twee chronische dadergroepen defacen, bijvoorbeeld, slechts zelden websites voor de uitdaging (MFC: 2,7%; HFC: 0,9%). In plaats daarvan voeren de HFC-defacers juist vaak aanvallen uit voor de lol (77,1%). De motivatie 'om de beste te zijn' wordt daarnaast relatief vaak gerapporteerd door de LFD-defacers (25,3%), terwijl patriottisme, politiek en wraak relatief vaak door de SP-, MFD- en HFD-defacers worden genoemd als motivaties. De MFC-defacers, tot slot, rapporteren relatief vaak (39%) geen motivatie voor de defacements die zij uitvoeren.

De tabellen 3 en 4 laten de verschillen tussen de zes groepen zien wat betreft de modus operandi die ze gebruikten tijdens hun aanvallen. De resultaten uit tabel 3 laten allereerst zien dat de chronische defacer-groepen relatief weinig hoofdpagina's van websites aanvielen (MFC: 23,2%; HFC: 15,2%), terwijl defacers uit de andere, minder actieve, groepen tussen de 47% en 62,9% van de gevallen de hoofdpagina aanvielen. Ook mass defacements werden vaker gebruikt door de minder actieve defacers: de sporadische daders gebruikten bijvoorbeeld in 40,9% van hun aanvallen een mass defacement, terwijl dit bij slechts 1 op de 10 defacements door de HFC-groep het geval was. Redefacements kwamen relatief weinig voor in deze steekproef, aangezien slechts 15% van de defacements gericht was op een website die al ooit eerder was aangevallen. De HFC-groep (17,5%) gebruikte echter het vaakst een redefacement, terwijl het bij de HFD-defacers het minst vaak voorkwam (9,5%). Tabel 3 toont verder aan dat defacers uit alle groepen het vaakst websites aanvielen die een variant van het Linux-besturingssysteem gebruikten, waarbij er weinig verschillen tussen de groepen worden waargenomen. Tot slot bleek de fysieke locatie vanwaaruit aangevallen websites gehost werden in meer dan driekwart van de gevallen in Nederland te zijn. Defacements van de chronische defacergroepen (MFC: 76,4%; HFC: 83,3%) waren relatief vaak gericht op websites die gehost werden vanuit Nederland.

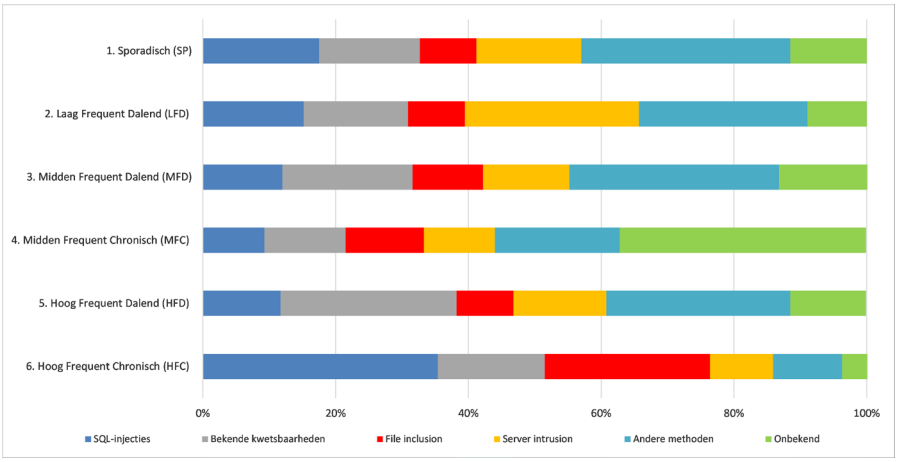
Tabel 3 Doelwitkeuze van de zes groepen defacers

Groep	Hoofdpagina	Mass defacement	Redefacement	Linux	Locatie NL
1. Sporadisch (SP)	62,9%	40,9%	12,9%	83,3%	64,1%
2. Laag Frequent Dalend (LFD)	48,0%	37,0%	11,1%	81,8%	68,1%
3. Midden Frequent Dalend (MFD)	47,3%	39,4%	11,5%	85,9%	70,2%
4. Midden Frequent Chronisch (MFC)	23,2%	23,7%	12,8%	85,6%	76,4%
5. Hoog Frequent Dalend (HFD)	47,0%	35,5%	9,5%	84,7%	74,6%
6. Hoog Frequent Chronisch (HFC)	15,2%	10,3%	17,5%	86%	83,8%
Totaal	26,6%	20,1%	15,0%	85%	787%

Tabel 4 Hackingtechnieken van de zes groepen defacers

Groep	SQL-injecties	Bekende kwetsbaarheden	File inclusion	Server intrusion	Andere methoden	Onbekend	Totaal
1. Sporadisch (SP)	17,5%	15,2%	8,5%	15,8%	31,5%	11,5%	100%
2. Laag Frequent Dalend (LFD)	15,2%	15,7%	8,6%	26,2%	25,4%	8,9%	100%
3. Midden Frequent Dalend (MFD)	12,0%	19,6%	10,6%	13%	31,6%	13,3%	100%
4. Midden Frequent Chronisch (MFC)	9,3%	12,2%	11,8%	10,7%	18,8%	37,1%	100%
5. Hoog Frequent Dalend (HFD)	11,7%	26,5%	8,6%	14%	27,7%	11,4%	100%
6. Hoog Frequent Chronisch (HFC)	35,4%	16,1%	24,9%	9,5%	10,4%	3,8%	100%
Totaal	25,5%	16,6%	18,5%	11,8%	16,9%	10,8%	100%

Figuur 4 Visuele weergave hackingtechnieken van de zes groepen defacers



Ten slotte laten tabel 4 en figuur 4 zien welke methoden de defacers gebruikten voor hun aanvallen. De methoden die in totaal het meest gebruikt werden om websites aan te vallen zijn SQL-injecties (25,5%) en file inclusion (18,5%). Dit is het gevolg van het feit dat HFC-defacers, die verantwoordelijk zijn voor het merendeel van alle aanvallen, deze methoden het vaakst gebruikten wanneer zij websites aanvielen (SQL-injecties: 35,4%; file inclusion: 24,9%). Daarnaast blijkt uit tabel 4 dat de defacers in de HFD-groep relatief vaak misbruik maakten van bekende kwetsbaarheden (26,5%), terwijl de LFD-groep relatief vaak websites binnendrongen middels server intrusion (26,2%). De SP- en MFD-defacers gebruikten relatief vaak (resp. 31,5% en 31,6%) andere methoden, zoals het stelen van wachtwoorden, social engineering, of URL poisoning, om de defacements uit te voeren. De MFC-defacers, tot slot, bleken het vaakst de gebruikte methode niet te rapporteren (37,1%).

Conclusies

In deze studie zijn, door gebruik te maken van de database van de Zone-H-website, groepen hackers geïdentificeerd die verschillen in de frequentie en timing van hun defacements van Nederlandse websites tussen januari 2010 en maart 2017. Zes groepen defacers konden worden onderscheiden: vier groepen die zich maar een beperkte periode bezighielden met het defacen van websites en twee groepen die gedurende de gehele onderzoeksperiode actief waren. Opmerkelijk is de bevinding dat de hoogfrequent chronische groep, die slechts bestaat uit 65 van de 3640 defacers (1,8%), verantwoordelijk is voor meer dan de helft van alle defacements die gedurende de onderzoeksperiode aan Zone-H gerapporteerd zijn (57,1%).
Deze bevindingen hebben ook implicaties voor de praktijk. Om defacements van Nederlandse websites tegen te gaan is het bijvoorbeeld het meest efficiënt als interventies zich op de kleine groep hoogfrequente daders zouden richten. Zij zouden bijvoorbeeld gestimuleerd kunnen worden om hun IT-vaardigheden voor legale

doi: 10.5553/TvV/.000019

doeleinden te gebruiken. In Nederland is men onlangs gestart met Hack_Right, een alternatief of aanvullend straftraject voor jeugdige cybercriminelen, waarbij zij leren hoe ze hun cybertalent op een legale wijze kunnen ontwikkelen (Schiks et al., 2021). Hiervoor is het echter wel noodzakelijk dat de defacers opgespoord en aangehouden kunnen worden. Dat dit slechts zelden gebeurt, blijkt uit het feit dat er jaarlijks maar ongeveer tweehonderd verdachten van computervredebreuk worden aangehouden (CBS, 2018), waarbij dit bovendien niet alleen defacers zijn, maar ook andere typen hackers.

Om de identificatie en opsporing van hoogfrequente defacers te bevorderen is het dan ook van belang om een profiel te hebben van deze defacers. Uit onze resultaten blijkt allereerst dat deze groep defacers in het overgrote merendeel van de gevallen plezier als drijfveer noemt, terwijl motivaties zoals patriottisme, wraak en politieke redenen zelden voorkomen. Ook rapporteren deze defacers zelden dat ze websites aanvallen voor de uitdaging of omdat ze de beste defacer willen zijn. Dit kan mogelijk verklaard worden doordat cybercriminelen die zichzelf willen blijven ontwikkelen niet honderden defacements blijven uitvoeren, maar in de loop van de tijd andere vormen van cybercriminaliteit gaan uitproberen. De resultaten tonen verder aan dat deze frequente defacers hun aanvallen slechts zelden richten op de hoofdpagina van een website en amper gebruikmaken van een mass defacement. Aangezien mass defacements van hoofdpagina's meer aandacht genereren, is de focus op enkelvoudige aanvallen op secundaire pagina's mogelijk een manier van deze frequente defacers om onder de radar te blijven en zodoende langer actief te blijven. Wat betreft de hackingtechnieken gebruiken de chronische defacers het vaakst SQL-injecties en file inclusion. Dit inzicht is van belang voor webbeheerders en *information security officers* van bedrijven. Door hun websites beter te wapenen tegen zulk soort aanvallen kunnen namelijk de meeste defacements van websites voorkomen worden.

De defacers in de overige groepen blijken niet alleen minder defacements uit te voeren gedurende een kortere periode dan de hoogfrequente en chronische defacers, maar hebben ook andere motivaties en andere modi operandi. Defacers in de laagfrequent dalende groep, bijvoorbeeld, rapporteren relatief vaak dat ze de beste defacer willen zijn. Mogelijk voeren deze cybercriminelen dus slechts enkele defacements van websites uit, om vervolgens andere doelen te hacken en hun vaardigheden verder te ontwikkelen. Defacers uit de sporadische groep defacen relatief vaak de homepage van een website en rapporteren daarnaast relatief vaak patriottisme, wraak en politieke redenen als motivaties. Dit kan erop duiden dat het in deze gevallen gaat om hackers die slechts één of twee keer een website defacen om een specifieke boodschap aan zo veel mogelijk mensen te tonen. Ook het feit dat de sporadische daders relatief vaak een mass defacement gebruiken, kan erop duiden dat ze hun boodschap voor zo veel mogelijk mensen zichtbaar willen maken. Tijdens een mass defacement wordt namelijk met één aanval de inhoud van meerdere websites tegelijkertijd aangepast.

Bij het interpreteren van de resultaten van deze studie moet echter wel rekening gehouden worden met enkele beperkingen van de Zone-H-data. Zo weten we alleen wat de online nickname is van degene die de defacement doorgeeft. De identiteit van de melder wordt niet geverifieerd en het is daarom onbekend of alle online

nicknames toe te schrijven zijn aan unieke individuen. Het is dus mogelijk dat één persoon werkt onder verschillende online nicknames of dat één online nickname gebruikt wordt door een hele groep aanvallers. Mogelijk gaat het bij de hoogfrequent chronische defacers vaker om groepen aanvallers, wat kan verklaren dat zij zoveel activiteit vertonen.

Een andere beperking is dat niet alle defacements worden bijgehouden door Zone-H, alleen de defacements die gerapporteerd zijn door de defacers zelf. We hebben dus, ondanks de grote hoeveelheid gerapporteerde defacements, niet de beschikking over alle uitgevoerde defacements op het internet. In hoeverre de gerapporteerde defacements representatief zijn voor alle gepleegde defacements is onbekend. Mogelijk zijn er verschillen in de modus operandi, motivaties en mate van activiteit tussen defacers die zelf hun gepleegde aanvallen online publiceren en defacers die dit niet doen en meer onder de radar blijven. Het is ook mogelijk dat defacers besluiten om hun aanvallen op een gegeven moment niet meer te rapporteren of dit te doen op een andere website of ander forum dan Zone-H. In dat geval leidt dit tot een onderschatting van de frequentie van aanvallen en van de duur dat een defacer actief is. Toch is Zone-H de meestgebruikte website om web defacements te archiveren en biedt het dan ook het meest complete archief dat beschikbaar is.

Ook hebben we in deze studie alleen Nederlandse websites bestudeerd, terwijl de defacers zelf niet uit Nederland afkomstig hoeven te zijn en het goed mogelijk is dat defacers actief zijn op websites uit meerdere landen. Mogelijkerwijs komen de minder actieve defacers vaker uit het buitenland en vallen zij slechts één of twee keer een Nederlandse website aan, maar defacen zij juist vaker websites uit andere landen. Ten slotte is er op basis van de Zone-H-data niets te zeggen over de leeftijd van de defacers. Hierdoor ligt de focus van dit artikel op de ontwikkeling van het uitvoeren van web defacements door de tijd heen, in plaats van gedurende de levensloop van de cybercriminelen. Wij hopen dat deze studie aanleiding biedt om in toekomstig onderzoek longitudinale gegevens te verzamelen gedurende de levensloop van cybercriminelen, zodat onderzocht kan worden in hoeverre empirische bevindingen (bijv. Piquero, 2008) en theorieën over de ontwikkeling van crimineel gedrag gedurende de levensloop (bijv. Moffitt, 1993) generaliseerbaar zijn naar cybercriminaliteit.

Tot slot zou het interessant zijn als er in vervolgonderzoek meer kwalitatief gekeken zou worden naar de content van de defacements en of deze verschilt tussen de verschillende groepen defacers die in deze studie zijn onderscheiden. Hierbij kan men denken aan de vorm van de boodschap (bijv. tekst, afbeeldingen, video's, geluid), maar ook de inhoud van de boodschap (en of deze overeenkomt met de zelfgerapporteerde motivaties). Door het gebruik van longitudinale data kan bovendien onderzocht worden of specifieke thema's (verkiezingen, COVID-19, Black Lives Matters, enz.) ook vaker zichtbaar zijn in de defacements uit de periode waarin deze thema's actueel zijn en of de defacements dus ook als middel gebruikt worden om opinies of *fake news* te verspreiden.

doi: 10.5553/TvV/.000019

Literatuur

Andress, J. & S. Winterfeld (2013) *Cyber warfare: techniques, tactics and tools for security practitioners*. Elsevier.

Bijleveld, C.C.J.H., S.G.A. van de Weijer, V.R. van der Geest & S. Ruiter (2015) *Analysetechnieken voor Niet-Experimentele Gegevens*. Den Haag: Boom Juridische uitgevers.

Blokland, A.A., D. Nagin & P. Nieuwbeerta (2005) Life span offending trajectories of a Dutch conviction cohort. *Criminology, 43*(4), 919-954.

Brenner, S.W. (2008) *Cyberthreats: The Emerging Fault Lines of the Nation State*. New York: Oxford University Press.

Holt, T.J. (2007) Subcultural evolution? Examining the influence of on-and off-line experiences on deviant subcultures. *Deviant Behavior, 28*(2), 171-198.

Holt, T.J. (2010) Examining the role of technology in the formation of deviant subcultures. *Social Science Computer Review, 28*(4), 466-481.

Holt, T.J. (2018) Regulating Cybercrime through Law Enforcement and Industry Mechanisms. *The ANNALS of the American Academy of Political and Social Science, 679*(1), 140-157.

Holt, T.J., J.D. Freilich & S.M. Chermak (2017) Exploring the subculture of ideologically motivated cyber-attackers. *Journal of contemporary criminal justice, 33*(3), 212-233.

Holt, T.J., R. Leukfeldt & S. van de Weijer (2020) An Examination of Motivation and Routine Activity Theory to Account for Cyberattacks Against Dutch Web Sites. *Criminal Justice and Behavior, 47*(4), 487-505.

Hutchings, A. & T.J. Holt (2017) The online stolen data market: disruption and intervention approaches. *Global Crime, 18*(1), 11-30.

Jolliffe, D., D.P. Farrington, A.R. Piquero, J.F. MacLeod & S.G.A. van de Weijer (2017) Prevalence of life-course-persistent, adolescence-limited, and late-onset offenders: A systematic review of prospective longitudinal studies. *Aggression and violent behavior, 33*, 4-14.

Jordan, T. & P. Taylor (2004) *Hacktivism and Cyber Wars*. London: Routledge.

Kilger, M. (2011) Social Dynamics and the Future of Technology-Driven Crime. In: T.J. Holt & B. Schell (eds.), *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications* (pp. 205-227). Hershey, PA: IGI-Global.

Koppen, M.V. van, A. Blokland, V. van der Geest, C. Bijleveld & S. van de Weijer (2014) Late-blooming offending. *Oxford Handbooks Online: Criminology*. Oxford: Oxford University Press.

Leukfeldt, E.R. (2017) *Research agenda the human factor in cybercrime and cybersecurity*. Den Haag: Eleven international publishing.

McGee, T.R. & D.P. Farrington (2010) Are there any true adult-onset offenders? *The British journal of criminology, 50*(3), 530-549.

Moffitt, T.E. (1993) Life-Course-Persistent and Adolescence-Limited Anti-Social Behavior: A Developmental Taxonomy. *Psychological Review, 100*, 674-701.

Nagin, D.S. (1999) Analyzing developmental trajectories: a semiparametric, group-based approach. *Psychological methods, 4*(2), 139.

Nagin, D.S. (2005) *Group-based modeling of development*. Harvard University Press.

Piquero, A.R. (2008) Taking stock of developmental trajectories of criminal activity over the life course. In: A.M. Liberman (ed.), *The long view of crime: A synthesis of longitudinal research* (pp. 23-78). New York, NY: Springer.

Rogers, M. (2006) A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigations, 3*, 97-102.

Romagna, M. & N.J. van den Hout (2017) Hacktivism and Website Defacement: Motivations, Capabilities and Potential Threats. In: 27th Virus Bulletin International Conference, Vol. 1, Madrid, Spain, 2017.

Schiks, J., S. van 't Hoff-de Goede & E.R. Leukfeldt (2021) *Een alternatief voor jeugdige hackers? Plan- en procesevaluatie van Hack_Right*. Den Haag: Politie en Wetenschap.

Taylor, P. (1999) *Hackers: Crime in the Digital Sublime*. London: Routledge.

Wagen, W. van der, E.G. van 't Zand-Kurtovic, S.R. Matthijsse & T.F.C. Fischer (2019) *Cyberdaders: uniek profiel, unieke aanpak? Een onderzoek naar kenmerken van en passende interventies voor daders van cybercriminaliteit in enge zin*. Den Haag: WODC.

Woo, H.J., Y. Kim & J. Dominick (2004) Hackers: Militants or merry pranksters? A content analysis of defaced web pages. *Media Psychology, 6*(1), 63-82.

Tijdschrift voor Veiligheid 2021 (20) 2
doi: 10.5553/TvV/.000019