F-gamers die 'mapsen', 'swipen' en 'bonken': een netnografisch onderzoek naar fraude en oplichting op Telegram Messenger

Robby Roks en Nahom Monshouwer*

De NOS meldt op 3 september 2018 dat er op sociale media als Instagram en Telegram honderden accounts met namen als 'snelgeldverdienen' of 'moneymakers' actief zijn die op grote schaal berichten plaatsen in de trant van 'Wil je snel geld verdienen en ben je 18+? Stuur me dan snel een privéberichtje.'[1] In deze berichten, die vooral gericht lijken op jongeren, wordt gevraagd om tegen betaling bankpassen en pincodes aan te leveren om fraude met pinpassen mogelijk te maken, een fenomeen dat in de wetenschappelijke literatuur ook wel wordt aangeduid als phishing (Lastdrager 2014). Bij banken bestaan er grote zorgen om deze activiteiten, omdat hier de nodige financiële schade mee gepaard gaat. Uit jaarcijfers van de Nederlandse Vereniging van Banken blijkt dat het schadebedrag door phishing in 2019 met bijna € 8 miljoen ruim verdubbeld bleek te zijn ten opzichte van 2018.[2]

Hoewel de geleden schade door consumenten in veel gevallen door de banken wordt vergoed, hebben we hier te maken met vormen van online fraude die een grote financiële schade met zich meebrengen. Deze cybercriminele activiteiten zijn in Nederland eerder onderwerp van studie geweest door Soudijn en Zegers (2012) en Leukfeldt (2014). Beide studies zijn gebaseerd op een wetenschappelijke analyse van

* Dr. R.A. Roks is als universitair docent verbonden aan de sectie Criminologie van de Erasmus Universiteit Rotterdam. R.N. Monshouwer MSc is CCD Analist bij Rabobank. De huidige bijdrage is gebaseerd op het onderzoek dat laatstgenoemde verrichtte in het kader van zijn masterscriptie aan de Erasmus Universiteit Rotterdam.

1 Gortworst e.a. 2018; zie https://nos.nl/artikel/2248735-politie-waarschuwt-voor-ronselaars-op-instagram-en-telegram.html, laatst geraadpleegd op 1 april 2020.

2 Van Teeffelen 2020; zie www.trouw.nl/binnenland/opnieuw-flink-meer-schade-door-phishing-doen-banken-genoeg~b64f36f0/, laatst geraadpleegd op 21 april 2020.

doi: 10.5553/JV/016758502020046002004

afgeronde politieonderzoeken. Soudijn en Zegers beschrijven de modus operandi van phishing op basis van een online cardingforum dat door de politie offline gehaald werd. Op basis van een analyse van de informatie op het forum concluderen Soudijn en Zegers (2012, p. 127) dat fysieke locaties zoals restaurants en clubs waar criminelen elkaar ontmoeten en kennis en informatie uitwisselen – zogeheten *offender convergence settings* (Felson 2006) – langzamerhand lijken over te zijn gegaan naar virtuele ontmoetingsplaatsen. Online, zoals op forums, ontmoeten mensen elkaar, worden goederen, diensten of informatie uitgewisseld en worden nieuwe criminele activiteiten besproken en uitgedacht. Soudijn en Zegers (2012, p. 127) concluderen om die reden dat 'whoever gains admission to the forum thereby opens the doors to an enormous source of contacts'.

Op basis van een analyse van een opsporingsonderzoek naar een cybercrimineel netwerk dat zich bezighield met phishing in Amsterdam laat Leukfeldt (2014) echter zien dat ook de offline wereld een onmisbare rol blijft spelen tijdens cybercriminaliteit. Niet een online forum, maar de straten van Amsterdam waren in de studie van Leukfeldt (2014, p. 235) de offender convergence setting waar de kernleden van het criminele netwerk elkaar hebben ontmoet en waar geldezels werden gerekruteerd om hun bankgegevens ter beschikking te stellen. Het rekruteringsproces vond daarbij zowel plaats in de fysieke straten van Amsterdam alsook op wat Lane (2019) de 'digitale straat' noemt: op socialemediaplatforms (Leukfeldt 2014, p. 231). Een analyse van het gebruik van sociale media door een problematische jeugdgroep uit de Rotterdamse wijk Spangen laat eveneens zien hoe jongeren platforms als Twitter gebruiken om naar specifieke bankpassen te vragen en om te poseren met verschillende betaalpassen (Roks & Van den Broek 2017, p. 40).

Bovenstaande studies illustreren het gebruik van virtuele ontmoetingsplaatsen zoals online fora en socialemediaplatforms in het *crime script* van phishing. Tot op heden zijn er echter geen studies geweest waarin specifiek aandacht wordt besteed aan phishing op Telegram Messenger, ofschoon diverse berichten in de media wijzen op het gebruik van Telegram voor online vormen van fraude en oplichting alsmede voor de handel in allerhande andere criminele goederen en diensten. Telegram lijkt hiervoor geschikt omdat deze gratis berichtendienst gebruikers de mogelijkheid biedt om versleutelde berichten, foto's en videobestanden te delen die, bovendien, een zelfvernieti-

doi: 10.5553/JV/016758502020046002004

gingsfunctie toegewezen kunnen krijgen (Moyle e.a. 2019, p. 102). Op Telegram worden berichten en bestanden versleuteld opgeslagen en daarnaast hebben gebruikers de mogelijkheid middels end-to-endencryptie[3] in de zogenaamde Secret Chats nog anoniemer te kunnen communiceren. Door deze functionaliteiten presenteert Telegram zich als een veilige berichtendienst, die bovendien laagdrempeliger is in termen van toegang en gebruik dan bijvoorbeeld fora op het darkweb.

In deze bijdrage doen wij verslag van een verkennend onderzoek naar online fraude en oplichting op Telegram op basis van een afgeronde masterscriptie (Monshouwer 2019). Ons doel is daarbij om een bijdrage te leveren aan de wetenschappelijke kennis over de modus operandi van online fraude en oplichting, de rol van online offender convergence settings en, ten slotte, het verrichten van wetenschappelijk onderzoek op socialemediaplatforms als Telegram. In deze bijdrage belichten we de volgende onderwerpen. We beginnen met een toelichting op het verrichten van *netnografisch* onderzoek op Telegram. Vervolgens geven we op basis van onze analyse van berichten op Telegram een illustratie en interpretatie van de zogenaamde F-game, een term die verwijst naar verschillende vormen van online fraude en oplichting. We besluiten deze bijdrage met een reflectie op de betekenis van deze bevindingen en het benoemen van enkele theoretische en methodologische implicaties, alsmede enkele suggesties voor vervolgonderzoek.

Netnografisch onderzoek op Telegram

Het berichtenplatform Telegram Messenger werd in 2013 door de Rus Pavel Durov opgericht na een langlopend conflict met de Russische autoriteiten over het afstaan van gebruikersgegevens van VKontakte, een andere succesvolle applicatie die Durov ontwikkelde. Door strenge controles vanuit Rusland en als antwoord op de conflicten met de autoriteiten ontwikkelde Durov met Telegram een socialemedia-

3 Door de end-to-endencryptie in de Secret Chats van Telegram kunnen alleen de zender en ontvanger van het bericht de versleutelde date lezen, waardoor 'no nobody else can decipher them, including us here at Telegram', aldus een antwoord op een van de Frequently Asked Questions op de website van Telegram Messenger (https://telegram.org/faq#secret-chats).

doi: 10.5553/JV/016758502020046002004

platform waarbij *encrypted messaging* en privacy centraal staan.[4] Telegram vertoont bepaalde gelijkenissen met de populaire berichtenservice WhatsApp, niet alleen wat betreft vormgeving, maar ook omdat een account op Telegram gelinkt is aan het telefoonnummer van de gebruiker, waarmee gecommuniceerd kan worden met opgeslagen contacten.

Anders dan WhatsApp biedt Telegram echter de mogelijkheid om lid te worden van verschillende groepen. Een zoekfunctie maakt het mogelijk om verschillende groepen op Telegram te vinden waar de gebruiker lid van kan worden om de gedeelde berichten te lezen en bestanden (afbeeldingen, video's, audio) op te slaan. In de groepen op Telegram hebben gebruikers, net als in de groepchatfunctie op WhatsApp, de mogelijkheid om met alle gebruikers in de groep te communiceren. De Telegramgroepen kunnen tot maximaal 200.000 leden bevatten en beheerders kunnen bots toevoegen om de (in)formele gedragsregels in de desbetreffende groep te handhaven. Gebruikers die zich niet houden aan de (in)formele regels van de groepen lopen het risico om voor een bepaalde tijdsduur verbannen te worden. Als de interactie niet geschikt is voor het grote publiek, hebben gebruikers bovendien de mogelijkheid om op een profiel van een andere gebruiker te klikken en een privébericht te sturen.

De eerste stap tijdens het verzamelen van data in het scriptieonderzoek van de tweede auteur was het selecteren van relevante groepen op Telegram. Het gebruik van de zoektermen 'swipen' en 'bonken' – twee specifieke aanduidingen voor online fraude en oplichting die in het vervolg van deze bijdrage nader toegelicht worden – in combinatie met de plaats 'Utrecht' resulteerde in een aantal groepen. Na uitgebreid rond te hebben gekeken in diverse groepen werd de tweede auteur lid van de groepen 'Swipe en Bonk' (886 leden[5]) en 'UTRECHT + OMGEVING HANDELSGROEP 030' (943 leden). Hiernaast werden ook enkele andere groepen, 'The Hustlers Handelgroep' (3.239 leden), 'Swipers United' (134 leden) en '[Y] SWIPEHANDEL' (796 leden), op regelmatige basis bezocht zonder hier lid van te worden.

Vanaf begin april tot eind juli 2019 verrichtte de tweede auteur netnografisch onderzoek in deze groepen. De term netnografie is schat-

4 Hakim 2014; zie www.nytimes.com/2014/12/03/technology/once-celebrated-in-russia-programmer-pavel-durov-chooses-exile.html, laatst geraadpleegd op 1 april 2020.

5 Het gaat hier om het aantal leden van de groepen tijdens het verrichten van de dataverzameling. Opgemerkt dient echter te worden dat de hoeveelheid leden per groep van dag tot dag, en zelfs van uur tot uur, kan veranderen.

doi: 10.5553/JV/016758502020046002004

plichtig aan Kozinets (2002, p. 62), die het begrip introduceerde om te verwijzen naar 'a new qualitative research methodology that adapts ethnographic research techniques to the study of cultures and communities emerging through electronic networks'. Ondanks dat het *being there*, dat aangemerkt kan worden als een kernbeginsel van dit etnografisch onderzoek, op het internet op een andere manier vormt krijgt, biedt de digitale wereld wel degelijk mogelijkheden om de etnografische traditie online voort te zetten. Urbanik en Roks (2020) beschrijven op basis van hun ervaringen met het incorporeren van onderzoek op sociale media tijdens meer klassiek offline veldwerk dat de traditionele rollen op het participant-observantcontinuüm van Gold (1958) ook online door onderzoekers kunnen worden uitgevoerd. Sociale media bieden immers verschillende functionaliteiten om actief en zichtbaar te participeren, onder andere door te reageren op *posts* en *comments* van andere gebruikers.

De online wereld biedt echter vooral de mogelijkheid om anoniem te observeren, zonder zelf deel te nemen. In de wetenschappelijke literatuur wordt dit ook wel aangeduid als *cyber stealth* (Murthy 2008), *lurken* (Richman 2007; Ferguson 2017) of *creepen* (Trottier 2012). De tweede auteur verkoos deze variant, in het bijzonder omdat de groepen op Telegram de mogelijkheid bieden om de inhoud van de posts en gesprekken te zien, zonder dat de gebruiker zijn aanwezigheid of identiteit kenbaar hoeft te maken. Bovendien biedt Telegram, anders dan bijvoorbeeld socialemediaplatform Snapchat, de mogelijkheid om screenshots van conversaties te maken zonder dat andere gebruikers hier een melding van krijgen. In de onderhavige studie is ervoor gekozen om screenshots te maken van de inhoud van de groepen op Telegram zonder de andere gebruikers hiervan op de hoogte te stellen, in het bijzonder omdat het gaat om delen van het internet die voor iedereen met een internetverbinding en telefoonnummer toegankelijk zijn. Al het verzamelde materiaal dat gebruikt is in de uiteindelijke masterscriptie van Monshouwer (2019) is geanonimiseerd en in sommige gevallen, wanneer een conversatie tussen gebruikers meer gedetailleerd werd beschreven, voorzien van pseudoniemen.

De data zijn verzameld door om de twee dagen de geplaatste berichten in de eerdergenoemde groepen te lezen en screenshots te maken van conversaties en berichten die te maken hadden met phishing. Er is bewust gekozen om niet alle informatie in de groepen in één keer volledig te downloaden, ofschoon deze functie wel beschikbaar is in de

doi: 10.5553/JV/016758502020046002004

Desktop-versie van Telegram. Hier lagen twee redenen aan ten grondslag. De eerste reden had te maken met cybersecurity. Door alles uit een groep te downloaden bestond het risico dat er ook afbeeldingen en bestanden met een zogeheten *encrypted* Remote Access Tool (RAT) – software waarmee je computer of mobiele telefoon voor hackdoeleinden gebruikt kan worden – tussen zouden kunnen zitten, iets waar door diverse gebruikers in de groepen voor werd gewaarschuwd (Monshouwer 2019, p. 22). Ten tweede zou het downloaden van alle informatie resulteren in een enorme hoeveelheid aan data, omdat er meerdere keren per dag dezelfde berichten door gebruikers werden gedeeld. Bovendien werd er ook allerlei content geplaatst die geen betrekking had op fraude, zoals berichten waarin wapens, drugs en designerkleding werden gevraagd of aangeboden. De content over het fenomeen phishing, en fraude meer in het algemeen, in de groepen werd opgeslagen door het maken van screenshots om zo een letterlijke tekstuele weergave van de berichten vast te kunnen leggen. In de periode april tot juli 2019 werden op deze manier meer dan 1.650 screenshots verzameld, die met behulp van Atlas.ti werden geanalyseerd (Monshouwer 2019, p. 25-26).

De F-game op Telegram

In de studie van Monshouwer (2019) lag de primaire focus op het beschrijven van de manieren waarop fraudeurs en oplichters gebruik maken van Telegram. In de geanalyseerde groepen passeerden diverse aan fraude en oplichting gerelateerde activiteiten de revue, waarbij gebruikers specifieke goederen en diensten om deze cybercriminele activiteiten te verrichten aanboden en vroegen. We lichten dit in het vervolg nader toe door meer zicht te geven op de vorm en inhoud van de berichten in de groepen. Vervolgens zoomen we in op de diverse modi operandi die in de bestudeerde groepen werden gedeeld.

'Op zoek naar iemand die dagelijks ECHTE jobs heeft?'

Afgaande op de berichten in de bestudeerde groepen lijkt Telegram dienst te doen als een marktplaats voor een veelvoud aan criminele goederen en diensten. Naast specifieke berichten en conversatie over fraude en oplichting in de vorm van het aanbieden of vragen van cre-

doi: 10.5553/JV/016758502020046002004

ditcardgegevens, bankpassen en methoden om geld afkomstig van phishingaanvallen te gebruiken, passeerden ook afbeeldingen van (vuur)wapens en diverse hard- en softdrugs de revue. De berichten worden gekenmerkt door het veelvuldige gebruik van emoji's en hoofdletters en een doorgaans adverterende stijl, zoals het volgende bericht illustreert:

> 'Yo F-gamers, Op zoek naar iemand die dagelijks ECHTE jobs heeft? Geen praatjesmaker die je kaart dagen lang houd? Dan ben je bij het juiste adres! WAT IS ER NU AAN? CRELAN BELGIE. ING BELGIE. ING NL. Ik meld elke dag welke jobs er zijn en wat je daar voor vangt.' (*The Hustlers Handel*, mei 2019)

De informatie uit het bovenstaande bericht vereist een zekere 'insider knowledge' om te ontcijferen waar door de gebruiker op wordt gedoeld. 'F-game', allereerst, is een term die zowel op straat als online wordt gebruikt als verwijzing naar activiteiten die kunnen worden geclassificeerd als fraude of oplichting. Opmerkelijk hierbij is dat het wordt aangemerkt als een 'game', een term die in de vorm van 'the crack game' op de straten van de Verenigde Staten ook wel wordt gebruikt voor het aanduiden van betrokkenheid bij de handel in specifieke verdovende middelen (Draus & Carlson 2009). In het gebruik van de term 'job' herkennen we bovendien eufemistisch taalgebruik waarbij criminaliteit wordt gezien als werk (Roks 2016, p. 160). Met welke 'jobs' – of 'djoen' of 'djunta', dat zich ook laat vertalen als werk (SMIB 2017, p. 98) – specifiek geld kan worden verdiend, is afhankelijk van wat er 'aan' is, oftewel waar vraag naar is of welke mogelijkheden zich voordoen, zoals in het bovenstaande geval bankpassen uit zowel België (Crelan en ING) als Nederland (ING).
Naast dat er diensten of 'jobs' worden aangeboden, zijn er ook gebruikers die op zoek zijn naar specifieke goederen of diensten. Er wordt daarbij gevraagd naar betaalpassen met bijbehorende pincodes van diverse Europese banken, maar in de geanalyseerde groepen zijn het voornamelijk Nederlandse banken. ABN AMRO wordt daarbij vanwege de groene betaalpassen aangeduid als 'green', ING als 'orra of orange' vanwege de oranje kleur van de pas en 'baro' wordt gebruikt om te verwijzen naar Rabobank. Bovendien gaat de voorkeur uit naar zogenaamde '18+'- of zakelijke kaarten, omdat ze een limiet kennen tot € 10.000 in tegenstelling tot 'kinderkaarten', die 'slechts gevuld

doi: 10.5553/JV/016758502020046002004

kunnen worden tot €5.000'. Naast dat de meeste gebruikers expliciteren wat ze aanbieden of vragen, benoemen ze daarbij ook vaak waar ze niet naar op zoek zijn. Een gebruiker schrijft bijvoorbeeld dat hij of zij niet op zoek is 'naar afhakers, grappenmakers, kleine kinderen en bledders'. Er wordt verwezen naar mensen die hun afspraken niet nakomen, zoals 'afhakers' en 'grappenmakers', naar 'infotrekkers', die enkel vragen stellen, en 'bledders': mensen die enkel praatjes hebben maar de daad niet bij het woord voegen.
Een groot aantal van de bovengenoemde woorden en termen illustreert de veelvuldige aanwezigheid van straattaal in de geanalyseerde groepen op Telegram. Dit valt eveneens te herkennen in het gebruik van specifieke termen voor phishinggerelateerde activiteiten. Naast de eerdergenoemde 'green', 'orra' en 'baro', wordt er meer in het algemeen gevraagd om 'sappies' en 'nip'. In deze termen herkennen we de linguïstische praktijk van 'talking backwards' (Lefkowitz 1989), waarbij woorden omgekeerd worden geschreven, zoals in 'sappies' van 'passen' en 'nip' van 'pinnen'. In Nederland kan deze omgang met taal in het bijzonder worden herleid naar de Amsterdamse Bijlmer, waar het wordt aangeduid als 'Sbimese', een omkering van de verbasterde aanduiding voor het stadsdeel als 'Bims' (SMIB 2017). Meer in het algemeen lijkt deze manier van praten en schrijven te zijn geïnspireerd door het *verlan* uit de banlieues van Frankrijk (Slooter 2019, p. 49).

De modus operandi van 'mapsen', 'swipen' en 'bonken'

We zien het gebruik van straattaal en de omkering van woorden eveneens terugkomen in de beschrijving van een aantal modi operandi die in de bestudeerde Telegramgroepen worden gedeeld, te weten 'mapsen', 'swipen' en 'bonken'. De benaming van de eerste werkwijze wordt nader toegelicht in het volgende bericht:

> 'Nu gaan we ons verdiepen in het Mapsen. Wat is Mapsen? Mapsen is het woord voor spammen. Dat houd in dat je een bericht in één keer verstuurd naar een groot aantal mensen. Bij het mapsen hoort phishen. Bij het phishen krijg je informatie van mensen doormiddel van oplichting.' (*Swipers United*, juli 2019)

doi: 10.5553/JV/016758502020046002004

Allereerst is het opvallend dat er op Telegram een toelichting wordt gegeven op de betekenis van de gehanteerde termen. 'Mapsen', de meervoudsvorm van de omkering van het woord 'spam', houdt in dit geval in dat er berichten worden gestuurd naar zo veel mogelijk telefoonnummers van potentiële slachtoffers. Er wordt hierbij een onderscheid gemaakt tussen zogenaamde gewone 'leads', bestaande uit mensen met een telefoonabonnement bij een specifieke provider, en 'target leads' in de vorm van mensen van wie bekend is dat ze bijvoorbeeld een creditcard hebben. Naar deze 'leads' worden 'nepberichten' gestuurd die afkomstig lijken te zijn van een verzender die wordt vertrouwd, zoals een Nederlandse bank. De berichten bevatten een hyperlink en zodra een slachtoffer daarop klikt, krijgt hij een pagina te zien die identiek lijkt aan de website van zijn eigen bank en wordt hem gevraagd zijn inloggegevens in te voeren. Op het moment van invoeren verkrijgt iemand anders echter ook toegang tot de financiële gegevens van het slachtoffer en wordt het aanwezige geld op de spaar- of bankrekening overgemaakt naar andere rekeningen, om vervolgens zo snel mogelijk contant uit een betaalautomaat te worden gehaald (vgl. Leukfeldt 2014, p. 234).

Opvallend aan de berichten in de geanalyseerde groepen is dat zowel wordt beschreven wat de specifieke activiteit inhoudt, alsook dat gebruikers meer inzicht wordt gegeven in welke handelingen ze stapsgewijs moeten verrichten om dit tot een succesvol einde te brengen. We zien dit terugkomen bij de tweede modus operandi die beschreven werd in de groepen op Telegram: 'swipen'. Met deze term wordt verwezen naar een manier om online producten te bestellen in webshops en te laten leveren, zonder voor de bestelde producten te betalen. In de Telegramgroep 'Swipe en Bonk' wordt uitgebreid beschreven welke stappen achtereenvolgens moeten worden doorlopen om accounts op Zalando, Bol.com of andere e-commercepartijen te 'swipen'.

De eerste drie stappen geven een nadere toelichting op de apparatuur en software die vereist zijn. Opmerkelijk hierbij is dat expliciet wordt benoemd welke software hiervoor gebruikt moet worden, waar deze kan worden gedownload en welke functie dit heeft. Bij 'swipen' wordt bijvoorbeeld benoemd dat gebruik moet worden gemaakt van NordVPN om het IP-adres en de fysieke locatie van de gebruiker te verbergen, en dat er een softwareprogramma moet worden gedown-

doi: 10.5553/JV/016758502020046002004

load om cookies te wissen. Na het doorlopen van deze stappen is het volgens het bericht tijd voor stap 4:

> 'Vervolgens ga je naar de website toe, je logt in en gaat net als elk willekeurig persoon even op de site rond surfen je gaat cookies opbouwen even hier kijken even daar kijken enzovoort enz enzz. Je gaat nooit gelijk inloggen iets opzoeken aanklikken en bestellen. Zodra je een aantal cookies hebt opgebouwd heb je meer slagingspercentage. Oke nu we dit hebben gedaan gaan we naar ons artikel toe… We klikken het aan en zorg altijd dat je net onder de €200 besteld. Op de bestelpagina staan gegevens je MOET NOOOOIT GEGEVENS AANPASSEN VAN EEN ACCOUNT DAN BLOKEERD AFTERPAY. je laat alles precies zoals het is want je gaat bestellen en laten leveren op een afhaalpunt en daarvoor heb je weer een ID kaart nodig. Als het pakketje op het afhlaapunt ligt stuur je iemand erheen of jij zelf met een id kaart en de track en trace code en dan krijg je je pakketje mee!! Veel success' (*Swipe en Bonk*, juli 2019)

Naast deze stapsgewijze toelichting wordt er in de groepen ook expliciet gevraagd om contacten bij PostNL of bezorgers werkzaam bij DHL om deze producten vervolgens tegen vergoeding af te leveren, maar bieden bezorgers zelf ook hun diensten aan in deze groepen om wat extra's te verdienen.

De derde en laatste modus operandi die in de geanalyseerde groepen op Telegram kan worden waargenomen, staat bekend als 'bonken', een term die in deze context gebruikt wordt als synoniem voor het 'gooien' van geld op een pas. 'Bonkers' zijn met andere woorden mensen die toegang hebben tot online bankgegevens van anderen en op zoek zijn naar manieren om de virtuele valuta om te zetten in contant geld. Het cashen van dit geld gebeurt door zogenaamde 'geldezels' (Leukfeldt 2014, p. 239-241). Ook deze modus operandi wordt uitgebreid toegelicht en onderverdeeld in een aantal stappen. Om te 'bonken' is een 'schone' telefoon nodig die niet eerder voor deze activiteit is gebruikt of waarvan de fabrieksgegevens zijn gewist. In tegenstelling tot 'swipen' wordt er bij 'bonken' opgeroepen om geen gebruik te maken van VPN.

Anders dan bij de andere modi operandi is bovendien dat er in het geval van 'bonken' een duidelijke afstemming is vereist tussen verschillende actoren en speelt een wezenlijk deel zich niet online af, maar in de fysieke wereld. Naast mensen die het geld van de rekenin-

doi: 10.5553/JV/016758502020046002004

gen van slachtoffers in juiste verhoudingen overmaken naar andere accounts, moeten de 'nippers' ('pinners') onder flinke tijddruk bij een pinautomaat aanwezig zijn om het overgemaakte geld uit de muur te halen. In het bericht wordt daarbij gespecificeerd dat het geld opgenomen moet worden in delen van € 1.200. Ten slotte wordt aangegeven dat de telefoon waarmee contact is geweest tussen de 'bonker' en de 'nipper' moet worden weggegooid.

Conclusie

In deze bijdrage hebben we een beschrijving gegeven van de modi operandi van online fraude en oplichting op het platform Telegram Messenger. Onze resultaten illustreren dat Telegram, net als cryptomarkten (Martin 2014; Aldridge & Decary-Hétu 2016) of specifieke online fora (Holt & Lampke 2010; Soudijn & Zegers 2012), lijkt te fungeren als een criminele marktplaats. In de bestudeerde groepen op Telegram zijn enerzijds gebruikers actief die goederen en diensten aanbieden en anderzijds gebruikers die op zoek zijn naar specifieke goederen of diensten. Bovendien illustreren de resultaten in deze bijdrage dat er op Telegram uitgebreide en stapsgewijze handleidingen ter beschikking worden gesteld om specifieke criminele activiteiten op een succesvolle manier uit te voeren, en dat gebruikers elkaar informeren over wat er wel en niet lijkt te werken. Het gaat daarbij niet enkel om een toelichting op de modus operandi, maar ook om meer nadrukkelijke informatie over de technologische kanten en benodigdheden om online fraude en oplichting mogelijk te maken. Telegram kan hierdoor worden beschouwd als een *digital offender convergence setting*.

Om toegang te krijgen tot de informatie in de groepen op Telegram hoeft er, anders dan op cryptomarkten, geen verbinding te worden gemaakt met een TOR-netwerk (Martin 2014; Ferguson 2017) en bovendien hoeven gebruikers zich niet te registreren om toegang te krijgen zoals op een online forum gebruikelijk is (Holt & Lampke 2010; Soudijn & Zegers 2012). Wel biedt de encryptie op Telegram gebruikers de mogelijkheid om op basis van een *plastic identity* (Yar 2005) anoniem en veilig te communiceren met anderen. Een wezenlijk verschil met de eerdergenoemde digital offender convergence settings is daarmee de ogenschijnlijke laagdrempeligheid van Telegram, die te

doi: 10.5553/JV/016758502020046002004

vergelijken is met andere, meer conventionele socialemediaplatforms zoals Twitter en Instagram.

De resultaten uit deze verkennende studie roepen de vraag op wie er in deze groepen actief zijn. Het veelvuldige gebruik van straattaal in de berichten en conversatie doet daarbij vermoeden dat het gaat om personen die zijn ingebed in een straatcultuur en hun werkterrein lijken te hebben verplaatst van de fysieke straat naar de digitale straat (Lane 2019). Tot op heden wijzen de beschikbare studies over de digitalisering van straat- en gangculturen vooral op het expressieve gebruik van het internet door (groepen) jongeren op straat, zoals het opbouwen en managen van reputatie, individuele en collectieve identiteitsconstructie en de veranderende dynamiek van geweld (zie voor een overzicht Irwin-Rogers e.a. 2018). De bevindingen uit deze studie illustreren echter dat sociale media ook een gedigitaliseerde kansenstructuur bieden om geld te verdienen, en dat er zelfs sprake lijkt van een diversificatie van traditionele delicten op straat, van de handel in drugs tot betrokkenheid bij cybercriminele activiteiten zoals phishing (Leukfeldt & Roks 2020).

Deze verkennende studie waar de onderhavige bijdrage op is gebaseerd, kent een aantal beperkingen. Allereerst is het onderzoek beperkt tot het volgen van enkele groepen op Telegram gedurende een periode van vier maanden. Een bijkomende beperking is dat we niet weten of ook offline navolging wordt gegeven aan het besprokene in de geanalyseerde Telegramgroepen. Eerdere studies naar de digitale straat wijzen immers op de centrale rol van het wekken van indrukken en discrepanties tussen online en offline identiteiten en gedragingen (Lane 2019; Urbanik & Roks 2020). Wel wekken de negatieve ervaringen in de berichten van sommige gebruikers, die bijvoorbeeld aangeven dat bepaalde aanbieders van goederen of diensten niet te vertrouwen zijn, de indruk dat vraag en aanbod dankzij de Telegramgroepen bij elkaar komen. Bovendien vertonen de gedetailleerde beschrijvingen van de modi operandi in deze bijdrage veel gelijkenissen met de crimescripts van phishing die worden beschreven in eerdere wetenschappelijke studies (Soudijn & Zegers 2012; Leukfeldt 2014).

De relatieve openheid van deze informatie biedt kansen voor zowel opsporingsdiensten als banken en e-commercebedrijven die geconfronteerd worden met de vormen van online fraude en oplichting die in deze bijdrage tot in detail werden beschreven. Bovendien onder-

doi: 10.5553/JV/016758502020046002004

streept dit artikel wat ons betreft de mogelijkheden die Telegram Messenger biedt voor het verrichten van wetenschappelijk onderzoek, temeer omdat er ook groepen zijn die zich specifiek richten op de handel in verdovende middelen, wapens, namaakkleding en andere criminologisch relevante thema's. Onze aanbeveling zou daarbij zijn om vervolgonderzoek niet enkel te beperken tot een observerende rol, maar de ingebouwde beveiligde berichtenservice te gebruiken om te communiceren met zowel aanbieders als vragers van illegale goederen en diensten. Een aanverwant thema dat daarbij bovendien nader uitgediept kan worden, is hoe er op Telegram wordt omgegaan met vertrouwen, omdat er, anders dan op cryptomarkten en online fora, niet gewerkt wordt met rating- en reviewsystemen om gebruikers te laten beoordelen of kopers of verkopers betrouwbaar zijn (Soudijn & Zegers 2012; Holt e.a. 2015).

Literatuur

Aldridge & Decary-Hétu 2016
J. Aldridge & D. Decary-Hétu, 'Cryptomarkets and the future of illicit drug markets', in: EMCDDA (red.), *The Internet and drug markets, EMCDDA insights*, Luxemburg: European Union 2016, p. 23-32.

Draus & Carlson 2009
P.J. Draus & R.G. Carlson, '"The game turns on you": Crack, sex, gender, and power in small-town Ohio', *Journal of Contemporary Ethnography* (38) 2009, afl. 3, p. 384-408.

Felson 2006
M. Felson, *The ecosystem for organized crime* (HEUNI paper No. 26), Helsinki: HEUNI 2006.

Ferguson 2017
R.H. Ferguson, 'Offline "stranger" and online lurker: Methods for an ethnography of illicit transactions on the darknet', *Qualitative Research* (17) 2017, afl. 6, p. 683-698.

Gold 1958
R. Gold, 'Roles in sociological field observation', *Social Forces* (36) 1958, p. 217-223.

Gortworst e.a. 2018
J. Gortworst, A. Pruis & D. Simons, 'Politie waarschuwt voor ronselaars op Instagram en Telegram', *NOS* 3 september 2018, https://nos.nl/artikel/2248735-politie-waarschuwt-voor-ronselaars-op-instagram-en-telegram.html.

doi: 10.5553/JV/016758502020046002004

Hakim 2014
D. Hakim, 'Once celebrated in Russia, the programmer Pavel Durov chooses exile', *New York Times* 2 december 2014, www.nytimes.com/2014/12/03/technology/once-celebrated-in-russia-programmer-pavel-durov-chooses-exile.html.

Holt & Lampke 2010
T.J. Holt & E. Lampke, 'Exploring stolen data markets online: Products and market forces', *Criminal Justice Studies* (23) 2010, afl. 1, p. 33-50.

Holt e.a. 2015
T.J. Holt, O. Smirnova, Y.T. Chua & H. Copes, 'Examining the risk reduction strategies of actors in online criminal markets', *Global Crime* (16) 2015, afl. 2, p. 81-103.

Irwin-Rogers e.a. 2018
K. Irwin-Rogers, J.A. Densley & C. Pinkney, 'Gang violence and social media', in: J.L. Ireland, P. Birch & C.A. Ireland (red.), *The Routledge international handbook of human aggression*, Londen: Routledge 2018, p. 400-410.

Kozinets 2002
R.V. Kozinets, 'The field behind the screen: Using netnography for marketing research in online communities', *Journal of Marketing Research* (39) 2002, afl. 1, p. 61-72.

Lane 2019
J. Lane, *The digital street*, New York: Oxford University Press 2019.

Lastdrager 2014
E.E. Lastdrager, 'Achieving a consensual definition of phishing based on a systematic review of the literature', *Crime Science* (3) 2014, afl. 1, p. 9.

Lefkowitz 1989
N.J. Lefkowitz, 'Verlan: talking backwards in French', *The French Review* (63) 1989, afl. 2, p. 312-322.

Leukfeldt 2014
E.R. Leukfeldt, 'Cybercrime and social ties', *Trends in Organized Crime* (17) 2014, afl. 4, p. 231-249.

Leukfeldt & Roks 2020
E.R. Leukfeldt & R.A. Roks, 'Cybercrimes on the streets of the Netherlands? An exploration of the intersection of cybercrimes and street crimes', *Deviant Behavior* (geaccepteerd, te verschijnen).

Martin 2014
J. Martin, 'Lost on the Silk Road: Online drug distribution and the "cryptomarket"', *Criminology & Criminal Justice* (14) 2014, afl. 3, p. 351-367.

Monshouwer 2019
N. Monshouwer, *'Kom met je spa en we vullen em.' Een netnografisch onderzoek naar het gebruik van Telegram door F-gamers* (masterscriptie Rotterdam), 2019.

doi: 10.5553/JV/016758502020046002004

Moyle e.a. 2019
L. Moyle, A. Childs, R. Coomber & M.J. Barratt, '# Drugsforsale: An exploration of the use of social media and encrypted messaging apps to supply and access drugs', *International Journal of Drug Policy* (63) 2019, p. 101-110.

Murthy 2008
D. Murthy, 'Digital ethnography: An examination of the use of new technologies for social research', *Sociology* (42) 2008, afl. 5, p. 837-855.

Richman 2007
A. Richman, 'The outsider lurking online', in: A.L. Best (red.), *Representing youth*, New York: New York University Press 2007, p. 182-202.

Roks 2016
R.A. Roks, *In de h200d. Een eigentijdse etnografie over de inbedding van criminaliteit en identiteit* (diss. Rotterdam), 2016

Roks & Van den Broek 2017
R.A. Roks & J.B.A. van den Broek, '#HOUHETSTRAAT: Straatcultuur op social media?', *Tijdschrift over Cultuur en Criminaliteit* (7) 2017, afl. 3, p. 31-50.

Slooter 2019
L.A. Slooter, *The making of the banlieue: An ethnography of space, identity and violence* Londen: Palgrave Macmillan 2019.
SMIB, *Smibanese woordenboek*, Amsterdam: Uitgeverij Pluim 2017.

Soudijn & Zegers 2012
M.R. Soudijn & B.C.H.T. Zegers, 'Cybercrime and virtual offender convergence settings', *Trends in Organized Crime* (15) 2012, afl. 2-3, p. 111-129.

Van Teeffelen 2020
K. van Teeffelen, 'Opnieuw flink meer schade door phishing. Doen banken genoeg?', *Trouw* 21 april 2020, www.trouw.nl/binnenland/opnieuw-flink-meer-schade-door-phishing-doen-banken-genoeg~b64f36f0/.

Trottier 2012
D. Trottier, 'Interpersonal surveillance on social media', *Canadian Journal of Communication* (37) 2012, p. 319-332.

Urbanik & Roks 2020
M.M. Urbanik & R.A. Roks, '#GangstaLife: Fusing urban ethnography with netnography in gang studies', *Qualitative Sociology* 2020, p. 1-21.

Yar 2005
M. Yar, 'The novelty of "cybercrime". An assessment in light of routine activity theory', *European Journal of Criminology* (2) 2005, AFL. 4, p. 407-427.

doi: 10.5553/JV/016758502020046002004