Samenvatting

Aanleiding, vraagstelling en scope

Over het witwassen bij cybercrime is, vergeleken met witwassen bij andere delicten, relatief weinig bekend. Bij veel delicten verdienen criminelen geld in contanten. Bij het witwassen van verdiensten uit cybercrime lijken echter in toenemende mate andere digitale betalingsmiddelen te worden gebruikt dan contant geld dat bijvoorbeeld uit drugshandel wordt verkregen. Met de groei van cybercrime in de laatste jaren neemt de urgentie toe om zicht te krijgen op het witwasproces en de betrokken actoren in dit proces. Dit onderzoek richt zich om die reden op het witwasproces, en het in kaart brengen van de betrokken actoren bij banking malware en ransomware. Banking malware is, kort gezegd, kwaadaardige software die bedoeld is om slachtoffers geld afhandig te maken via betalingen met internetbankieren. Ransomware is kwaadaardige software waarmee iemands computersysteem (of bestanden die zich daarop bevinden) wordt 'gegijzeld' en losgeld wordt geëist om het systeem te ontsleutelen. Sinds een paar jaar is een variant van ransomware in opkomst, genaamd cryptoware, waarbij bestanden op een computer versleuteld worden en het losgeld in de virtuele valuta Bitcoin wordt geëist.

De centrale vraagstelling in dit onderzoek is: *op welke wijze en door welke actoren wordt geld verkregen uit banking malware en ransomware (al dan niet digitaal) witgewassen?* Voor de beantwoording van deze vraag zijn zes deelvragen geformuleerd:

1 Wat wordt verstaan onder het witwassen van door banking malware en ransomware verkregen geld en hoe wordt witwassen juridisch gekwalificeerd?
2 Wat zijn digitale betalingsmiddelen, in het bijzonder virtuele valuta zoals Bitcoin, en hoe werken deze digitale betalingsmiddelen?
3 Op welke wijze en door welke actoren wordt geld witgewassen dat:
   a door middel van banking malware wordt verkregen?
   b door middel van ransomware wordt verkregen?
4 Wat zijn de kenmerken van actoren die betrokken zijn bij het witwassen van geld dat wordt verkregen uit banking malware en ransomware?
5 Welke informatie over de modus operandi van actoren, die betrokken zijn het bij het witwassen van geld dat verkregen wordt uit banking malware en ransomware, is beschikbaar op het dark web?
6 Welke rol spelen digitale betalingsmiddelen, in het bijzonder virtuele valuta zoals Bitcoin, bij het witwassen van geld dat wordt verkregen uit banking malware en ransomware?

Methodologie

De onderzoeksvragen zijn beantwoord met behulp van de volgende onderzoeksmethoden: (1) deskresearch, (2) interviews, (3) dossieronderzoek, (4) een 'experiment' met bitcoins en mixing services, en (5) een kwantitatieve analyse van transactiegegevens van de grote Nederlandse banken die zijn gerelateerd aan banking malware en phishing. De deskresearch bestond uit een analyse van de beschikbare literatuur en mediaberichten over cybercrime, witwassen, en digitale betalingsmiddelen. Daarnaast zijn verdiepende interviews afgenomen met behulp met een semigestructureerde vragenlijst bij twintig experts op het gebied van cybercrime, witwassen en het gebruik van digitale betalingsmiddelen. De deskresearch en de interviews leverden kennis op over het gebruik van digitale betalingsmiddelen en het digitaal witwassen van geld dat wordt verkregen uit cybercrime. Tevens zijn vier zaken van het High Tech Crime Team van de Nationale Politie onderzocht die betrekking hebben op cybercrime en witwassen. Door middel van een empirische oefening, waarbij bitcoins werden aangeschaft en door mixing services werden gehaald, is inzicht verkregen in de online dienstverleners op het gebied van witwassen van bitcoins. Ten slotte is een kwantitatieve analyse uitgevoerd van transactiegegevens die zijn gerelateerd aan banking malware en phishing. Deze gegevens hebben inzicht verschaft in de kenmerken van money mules die betrokken zijn in het witwasproces bij banking malware.

Resultaten en conclusies

Het geld dat wordt verkregen uit banking malware en ransomware is doorgaans digitaal van aard. Bij banking malware wordt elektronisch geld buitgemaakt en bij ransomware wordt het losgeld veelal betaald met vouchers of (in toenemende mate en vooral bij cryptoware) met bitcoins. Het witwassen van deze opbrengsten bestaat uit het verbergen of verhullen van de criminele herkomst van het geld. De typologieën die zijn ontwikkeld om opzet bij opzetwitwassen te bewijzen, hebben vooral betrekking op contant geld bij (veelal) drugsdelicten. In de praktijk bestaat daardoor regelmatig onduidelijkheid over de vraag op welke moment bij transacties of bezit van grote sommen virtuele betalingsmiddelen kan worden gesproken van opzet bij witwassen.

Veel typen digitale betalingsmiddelen kunnen worden gebruikt om de verdiensten uit cybercrime wit te wassen. In dit onderzoek wordt een onderscheid gemaakt tussen elektronisch geld en virtueel geld. Elektronisch geld is de digitale weergave van echt geld, terwijl virtueel geld niet door de overheid is gefiatteerd. Virtueel geld kan op zijn beurt centraal of decentraal beheerd zijn en wel of niet inwisselbaar zijn tegen echt geld. Inwisselbaar, centraal

beheerd virtueel geld betreft bijvoorbeeld tegoeden op websites, niet-inwisselbaar centraal beheerd virtueel geld betreft bijvoorbeeld speelgeld in online games en virtuele werelden. Inwisselbaar, decentraal beheerd virtueel geld betreft cryptocurrencies. Veruit de bekendste cryptocurrency is de Bitcoin, met 90% van de totale marktwaarde van virtuele valuta.

In dit onderzoek zijn verschillende modellen beschreven die criminelen gebruiken om geld dat wordt buitgemaakt uit banking malware en ransomware wit te wassen. De onderzoeksresultaten laten zien dat gelden die zijn verkregen uit banking malware en ransomware op zeer veel verschillende manieren kunnen worden witgewassen. Daarbij wordt vaak een combinatie gemaakt van digitale betalingsmiddelen.

Bij banking malware wordt vaak gebruikgemaakt van money mules. Het geld wordt in dat geval vanaf de rekening van het slachtoffer van banking malware overgemaakt naar een rekening van een money mule. Vervolgens neemt de money mule het bedrag zo snel mogelijk op bij een geldautomaat (de zogenoemde 'cash-out'). Deze wijze van witwassen kan deels worden verklaard door de voorkeur van criminelen om contant geld in bezit te hebben. Toch wordt uit het dossieronderzoek en de kwantitatieve analyse ook helder dat direct vanaf de rekening van slachtoffers van banking malware goederen, diensten en/of bitcoins worden aangekocht met behulp van de financiële gegevens van het slachtoffer. Daarbij kan van meerdere online dienstverleners gebruik worden gemaakt.

Bij ransomware wordt het losgeld doorgaans in online vouchers of bitcoins geëist. Bij vouchers wordt de waarde van de vouchers doorgaans bijgeschreven op een online account van een e-wallet-dienst, waarna het geld verder kan worden witgewassen. Het is ook mogelijk de vouchers door te verkopen of direct te besteden bij een online dienstverlener. Doorgaans wordt van een combinatie van witwasmethoden gebruikgemaakt. Indien het geld in bitcoins is geëist, kan de organisatie achter de malware trachten de herkomst van de bitcoins te verhullen door gebruikmaking van een mixing service. Uit de empirische oefening is tevens meer informatie verkregen over mixing services en online witwasdiensten die hun diensten beschikbaar stellen via het 'dark web'. Mixing services maken het mogelijk om bitcoins tegen een commissie om te wisselen tegen andere bitcoins. De bitcoins kunnen vervolgens direct worden besteed of worden omgewisseld bij een fysieke bitcoin-handelaar of Bitcoin exchange. Ten slotte zijn er ook gespecialiseerde illegale online dienstverleners die bereid zijn digitale en virtuele betalingsmiddelen tegen een commissie om te ruilen voor een betaling naar keuze.

Uit deze modellen kunnen de volgende actoren worden geïdentificeerd die op enigerlei wijze betrokken zijn bij het witwasproces van crimineel verkre-

gen geld uit banking malware en ransomware: (1) banken, (2) money mules, (3) geldtransfer kantoren, (4) Payment Service Providers, (5) webwinkels, (6) voucherdiensten, (7) e-wallet-diensten, (8) Bitcoin exchanges, (9) mixing services, en (10) Bitcoin-handelaren. Om in kaart te brengen met welke partijen de politie tijdens opsporingsonderzoeken in aanraking zou kunnen komen zijn in dit rapport de kenmerken van deze actoren beschreven. Met behulp van de transactiegegevens over phishing en banking malware is het mogelijk geweest op de meest gedetailleerde wijze de kenmerken van money mules in Nederland in kaart te brengen. Het beeld dat uit de analyses van de datasets naar voren komt, maakt duidelijk dat money mules voornamelijk jongvolwassenen tussen de 18 en 22 jaar zijn uit armere wijken die zich laten ronselen om tegen betaling hun pinpas af te staan. Hoewel jongeren in de achterstandswijken van de drie grote steden (Amsterdam, Rotterdam en Den Haag) oververtegenwoordigd zijn, komen money mules uit alle gemeenten in Nederland. De jongeren hebben relatief vaak een Oost-Europese nationaliteit.

Uit dit onderzoek komt naar voren dat criminelen er in veel gevallen nog steeds voor kiezen om contant geld te gebruiken. Dit komt omdat contant geld snel en anoniem verplaatst kan worden. Daarmee is en blijft contant geld voor hen aantrekkelijk om ongestoord van de opbrengsten van criminaliteit te genieten, ook bij cybercrime. De omvang van witwassen met contant geld is dan ook vele malen groter dan die van witwassen met digitale betalingsmiddelen, waar in deze studie de nadruk op ligt. Of dat in de toekomst zal veranderen, hangt sterk af van de ontwikkelingen rondom digitale betalingsmiddelen en maatregelen die bedrijven en instellingen nemen om witwassen te bestrijden. Daarbij moeten verschillende expertises van politie en justitie worden ingezet om het witwassen met digitale betalingsmiddelen te bestrijden.

Het verdient aanbeveling te overwegen om Nederlandse Bitcoin exchanges te reguleren. Nederlandse Bitcoin exchanges hebben op vrijwillige basis al een uitgebreid palet aan maatregelen genomen om witwassen tegen te gaan. Maar door regulering zouden zij bijvoorbeeld ook een melding aan de Financial Intelligence Unit (FIU) kunnen doen, hetgeen kan bijdragen aan de opsporing van witwassen met virtuele valuta. Het reguleren van bitcoin exchanges blijft echter een uitdaging, gezien het feit dat online betalingsdiensten wereldwijd hun diensten kunnen aanbieden en daarbij gevestigd kunnen zijn in jurisdicties met minder strenge regelgeving of een gebrek aan toezicht of handhaving. Bovendien zijn er ook andere online betalingsdiensten die het mogelijk maken digitale betalingsmiddelen en virtuele om te zetten en zich in jurisdicties vestigen met meer coulante regelgeving en gebrekkig toezicht. Het blijft noodzakelijk dat betalingsdienstverleners technische maatregelen nemen om verdachte transacties zo goed mogelijk te detecteren

en blokkeren. Daarnaast moeten ook andere partijen, inclusief burgers, technische maatregelen nemen om de kwaadaardige software al aan de voorkant van het proces aan te pakken. Concreet kan daarbij gedacht worden aan het monitoren van netwerkverkeer (ook op phishing e-mails). Burgers en organisaties zouden daarbij in de basis een goede cyberhygiëne moeten aanhouden en regelmatig back-ups moeten maken. Daarnaast is het ook van belang het bewustzijn bij computergebruikers over cybercrime, in het bijzonder ransomware, verder te intensiveren door voorlichting te geven.