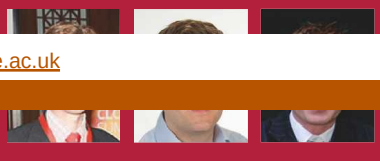


Mr. dr. ir. B.H.M. Custers, mr. J.J. Oerlemans en mr. R.L.D. Pool
bij het WODC. Oerlemans is tevens verbonden aan eLaw.

15. Ransomware, cryptoware en het witwassen van losgeld in Bitcoins

Een van de nieuwste ontwikkelingen op het terrein van cybercrime is ransomware. Dit is kwaadaardige software (malware) die toegang tot iemands computer en/of bestanden daarop blokkeert. Een specifieke vorm van ransomware is zogeheten cryptoware, die de bestanden versleutelt met behulp van cryptografie. Vervolgens eisen de cybercriminelen betaling van losgeld, vaak in de vorm van Bitcoins. Deze bijdrage gaat in op de vraag hoe cybercriminelen ransomware en cryptoware inzetten om geld te verdienen en hoe de verdiende Bitcoins vervolgens worden witgewassen.

1. Inleiding[1]

Elke gebruiker van een computersysteem kent de frustratie wanneer het systeem is vastgelopen. Op dat moment kun je niet meer bij je bestanden. Iets vergelijkbaars, maar dan lastiger op te lossen, gebeurt wanneer iemand het slachtoffer wordt van *ransomware* of *cryptoware*. Ransomware, ook wel 'gijzelsoftware' genoemd, is kwaadaardige software (malware) die de toegang tot een computer en/of bestanden daarop blokkeert. Cryptoware is een recente verschijningsvorm van ransomware, waarbij de bestanden worden versleuteld met behulp van cryptografie.[2] Na besmetting verschijnt bij slachtoffers een scherm waarop staat dat de toegang tot hun computer of een aantal bestanden op hun computer is geblokkeerd. In figuur 1 is een voorbeeld hiervan weergegeven. Het scherm bevat ook een instructie waarin staat beschreven hoe het deblokkeren in zijn werk gaat. Dit is in de vorm van een betaling van losgeld. Het losgeld bedraagt doorgaans enkele honderden euro's per keer.[3] In toenemende mate wordt het losgeld opgeëist in de vorm van Bitcoins.[4] Hoewel de meeste slachtoffers niet weten wat Bitcoins zijn, laat staan er ooit mee betaald hebben, staat in de instructies helder omschreven wat slachtoffers moeten doen om weer bij hun bestanden te komen. Hoewel de politie dringend afraadt losgeld te betalen, is het niet vreemd dat sommige slachtoffers wel degelijk overgaan tot betaling van losgeld, vooral als ze geen back-up hebben van de bestanden. De waarde van de bestanden kan namelijk voor slachtoffers vele malen groter zijn dan het bedrag dat als losgeld wordt opgeëist. Denk bijvoorbeeld aan de versleuteling van familiefoto's en persoonlijke bestanden die van onschatbare waarde kunnen zijn, waardoor slachtoffers toch geneigd zijn het losgeld te betalen. Uit onderzoek blijkt dat circa 10 procent van de Nederlandse

1 Deze bijdrage is gebaseerd op de eerste resultaten van een onderzoek dat de auteurs uitvoeren bij het WODC. Zie www.wodc.nl/onderzoeksdatabase/2540-criminele-dienstverlening-op-internet.aspx. Het volledige onderzoeksrapport zal medio 2016 op de website van het WODC worden gepubliceerd.

2 Er bestaat dus ook ransomware die geen cryptoware is. Een voorbeeld hiervan is WinLock, dat toegang tot computers blokkeerde door het tonen van pornografische afbeeldingen en vervolgens losgeld opeiste. Naar schatting werd hiermee $ 16 miljoen verdiend. Zie R. McMillian, 'Alleged ransomware gang investigated by Moscow police', *PC World* 10 maart 2012 (www.pcworld.com/article/204577/article.html); J. Leyden, 'Russian cops cuff 10 ransomware Trojan suspects', The Register 1 september 2010 (www.theregister.co.uk/2010/09/01/ransomware_trojan_suspects_cuffed/).

3 CSBN, *Cyber Security Beeld Nederland 5*, Den Haag: Nationaal Cyber Security Centrum 2015, p. 12 (www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-5.html). Merk op dat iemand ook meerdere keren slachtoffer kan worden van ransomware.

4 Europol, *An analysis of payment mechanisms used within cybercrime in the EU*, [nog te verschijnen], p. 1 (hierna: Europol 2016).

aangevers zegt betaald te hebben om toegang tot bestanden terug te krijgen.[5] Uiteraard is nooit gegarandeerd dat betaling van het losgeld ook daadwerkelijk toegang verschaft tot de computer en de bestanden daarop, maar kansloos is het ook niet. Ontsleuteling is namelijk onderdeel van het bedrijfsmodel van deze cybercriminelen: als ze nooit zouden ontsleutelen na betaling van het losgeld, zou het aantal slachtoffers dat losgeld betaalt naar verwachting snel afnemen.

Figuur 1. Voorbeeld van een blokkeringsscherm waarbij losgeld wordt opgeëist, nadat de ransomware zich op de computer heeft genesteld. Dit voorbeeld betreft de cryptoware van CTB Locker

Indien geen betaling plaatsvindt of de criminelen hun belofte niet nakomen, kunnen consumenten na infectie onder meer hun opgeslagen documenten en foto's op geïnfecteerde computers en gegevensdragers verliezen. Bedrijven en overheidsinstellingen kunnen tijdelijk niet meer hun werkzaamheden uitvoeren indien de werkcomputers en netwerkschijven worden versleuteld.[6] Cryptoware kan daarnaast ook virtuele harde schijven, externe harde schijven, USB-sticks en back-upschijven infecteren.[7] Bedrijven en overheidsinstellingen die geen back-up hebben gemaakt van bestanden kunnen na infectie met cryptoware flinke schade oplopen.
Volgens Europol is ransomware anno 2015 in termen van schaal en impact een van de belangrijkste bedreigingen op het gebied van cybercrime.[8] Sinds 2014 is een sterke stijging in het aantal slachtoffers van ransomware waar te nemen.

Cybercriminelen kunnen grote bedragen verdienen met ransomware en cryptoware. Met CryptoWall 3 (zie paragraaf 2) werd bijvoorbeeld circa $ 325 miljoen verdiend in een periode van twee maanden.[9] Infecties met cryptoware bij Nederlandse overheidsinstellingen zijn sinds 1 januari 2015 regelmatig in het nieuws gekomen.[10] Voor Nederland wordt een groei voorspeld van ransomware en in het bijzonder cryptoware.[11] Het verspreiden of maken van ransomware is strafbaar op grond van artikel 350a, derde lid, Sr, waarin is bepaald dat het verspreiden of ter beschikking stellen van programma's die bestemd zijn om schade aan te richten in een geautomatiseerd werk strafbaar is met maximaal vier jaar cel. Op het opzettelijk en wederrechtelijk ontoegankelijk maken van computergegevens (bijvoorbeeld via ransomware of cryptoware) staat een maximale gevangenisstraf van twee jaar (art. 350a lid 1 Sr).[12]
Banking malware en ransomware worden doorgaans niet tot de klassieke voorbeelden van high impact crime (woninginbraken, overvallen, straatroof en geweld) gerekend. Gelet op de eigenschappen van deze vormen van cybercrime vallen ze echter in dezelfde categorie: net als ander vormen van high impact crimes, komen banking malware en ransomware veel voor en hebben een grote impact op het slachtoffer.[13]
Deze bijdrage gaat in op de vraag hoe cybercriminelen ransomware en cryptoware inzetten om geld te verdienen en hoe de verdiende Bitcoins vervolgens worden witgewassen. In paragraaf 2 wordt nader ingegaan op de werking van ransomware en cryptoware. Daarbij wordt beschreven hoe computers van slachtoffers worden besmet, hoe ransomware en cryptoware eruitzien en hoe losgeld kan worden betaald. Aangezien het losgeld in toenemende mate in Bitcoins wordt opgeëist, wordt in paragraaf 3 kort de werking van Bitcoins uitgelegd. In paragraaf 4 wordt uiteengezet hoe het witwas-

5 CSBN, *a.w.* (2015), p. 12.
6 S. Hartholt, 'Friese gemeenten getroffen door ransomware', *Binnenlands Bestuur* 9 juni 2015 (www.binnenlandsbestuur.nl/digitaal/nieuws/friese-gemeenten-getroffen-door-ransomware.9478427.lynkx).
7 CSBN, *Cyber Security Beeld Nederland 4*, Den Haag: Nationaal Cyber Security Centrum 2014, p. 84 (www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-4.html).
8 Europol, *The Internet Organised Crime Threat Assessment (IOCTA)*, Den Haag: 2015, p. 7 (www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015) (hierna: Europol 2015a).
9 C. Beek, *Ransomware: an insight to financial gain*, Santa Clara (CA): McAfee 2016 (https://blogs.mcafee.com/mcafee-labs/ransomware-insight-financial-gain/).
10 ANP, 'Steeds meer besmettingen met cryptoware in Nederland', *nu.nl* 16 maart 2015 (www.nu.nl/internet/4011877/steeds-meer-besmettingen-met-cryptoware-in-nederland.html); ANP, 'Overheid vaker doelwit cyberaanval', *nu.nl* 13 augustus 2015 (www.nu.nl/internet/4105537/overheid-vaker-doelwit-cyberaanval.html); CSBN, *a.w.* (2015), p. 17.
11 CSBN, *a.w.* (2015), p. 37.
12 Merk op dat de makers en verspreiders van ransomware en andere kwaadaardige software in veel gevallen verschillende personen zijn, zie M. Sandee, *Game over Zeus. Backgrounds on the badguys and backends*, Whitepaper for the Blackhat US conference 2015 (www.fox-it.com/en/files/2015/08/FoxIT-Whitepaper_Blackhat-web.pdf). Na infectie met malware bij het aanpassen van gegevens op computersystemen kan tevens sprake zijn van computervredebreuk (art. 138ab Sr), zie J.J. Oerlemans & B.J. Koops, 'De Hoge Raad bewijst een slechte dienst in high-tech-crimezaak over botnets', *NJB* 2011, p. 1181-1185.
13 Bijlage bij *Kamerstukken II* 2014/15, 28684, 412 (Veiligheidsagenda 2015–2018).

sen van met cybercrime verdiende Bitcoins in zijn werk gaat. In paragraaf 5 komen de mogelijkheden voor vervolging en inbeslagname van Bitcoins aan bod. In paragraaf 6 wordt afgesloten met enkele conclusies.

2 De werking van ransomware en cryptoware

Computers kunnen op verschillende manieren worden besmet met ransomware en cryptoware. De meest voorkomende manier is via spam, of beter gezegd phishing e-mail,[14] waarbij computergebruikers worden verleid een link naar een website aan te klikken of een besmette bijlage van een e-mailbericht te openen. Wanneer de bijlage wordt geopend, kan dit het installeren van de kwaadaardige software in gang zetten. Wanneer een link wordt aangeklikt naar een website, kan op de achtergrond de kwaadaardige software op de computer worden geïnstalleerd.[15] Soms worden daarbij zogeheten exploit-kits gebruikt, waarmee naar kwetsbaarheden van een computersysteem wordt gezocht. Exploit-kits kunnen ook zelfstandig worden gebruikt, dus zonder phishing e-mail. Uit onderzoek blijkt dat in ruwweg een derde van de gevallen via exploit-kits wordt geïnstalleerd en in ruwweg twee derde van de gevallen via phishing e-mail.[16]

Ransomware is gericht op het vergrendelen van het besturingssysteem van het slachtoffer en/of (in het geval van cryptoware) op het versleutelen van enkele bestanden of de gehele harde schijf. De meest eenvoudige vormen van ransomware betreffen het vergrendelen van het computerscherm, een probleem dat soms alweer is opgelost wanneer een computer opnieuw wordt opgestart. Veel geavanceerder zijn infecties met cryptoware waarbij enkele bestanden of de gehele harde schijf door de kwaadaardige software met sterke encryptie worden versleuteld.[17] Ook gedeelde netwerkmappen op geïnfecteerde computers kunnen worden geïnfecteerd. Op computers die zijn besmet met cryptoware bestaat soms nog wel de mogelijkheid om te surfen naar een website om de betaling uit te voeren.[18]

De in Nederland het meest voorkomende typen van ransomware zijn CTB Locker, CryptoLocker en CryptoWall. Deze vormen van ransomware, alle cryptoware, lijken sterk op elkaar.[19] De eerste drie vormen worden hierna kort besproken. CTB Locker staat voor Curve-Tor-Bitcoin[20] en is cryptoware die wordt verspreid via e-mails. In Nederland gebeurde dit enige tijd met e-mails waarbij de verzender zich voordeed als een financiële instelling met een zogenaamd betalingsformulier als bijlage.[21] Het losgeld bedroeg voorheen één Bitcoin. Sinds 2015 is CTB Locker vernieuwd en bedraagt het losgeld drie Bitcoins (ruim $ 600,=).[22] Opmerkelijk is dat deze nieuwe versie slachtoffers de mogelijkheid biedt om vijf bestanden te selecteren die gratis kunnen worden ontsleuteld. Waarschijnlijk is dit bedoeld om slachtoffers te overtuigen dat betaling van het losgeld inderdaad ontsleuteling van alle bestanden oplevert. Niet uitgesloten is echter dat dit ook gebeurt om na te gaan welke bestanden het meest waardevol zijn vanuit het perspectief van slachtoffers. Nieuwe vormen van ransomware dreigen namelijk ook met het openbaar maken van gevoelige persoonlijke data die op de computers van slachtoffers staat.[23]

> Volgens Europol is ransomware anno 2015 in termen van schaal en impact een van de belangrijkste bedreigingen op het gebied van cybercrime

14 *Spam* verwijst naar ongewenste e-mailberichten. Een deel daarvan is *phishing e-mail*, waarmee wordt geprobeerd mensen naar nepwebsites te lokken of vertrouwelijke gegevens als wachtwoorden en pincodes te ontfutselen.

15 Dit type aanval wordt ook wel een 'drive-by-download' genoemd.

16 Cyber Threat Alliance, *Lucrative ransomware attacks. Analysis of the cryptowall version 3 threat*, 2015, p. 6 (http://cyberthreatalliance.org/cryptowall-report.pdf).

17 Cryptoware maakt meestal gebruik van asymmetrische encryptie. Dit houdt in dat de sleutel die wordt gebruikt voor het versleutelen van bestanden een andere sleutel is dan die wordt gebruikt voor het ontsleutelen van bestanden. Voor elk slachtoffer wordt een unieke sleutel aangemaakt en de sleutel die wordt gebruikt voor het ontsleutelen is slechts beschikbaar op de computer van de dader. C. Beek et al., *McAfee Labs Threat Report*, Santa Clara (CA): McAfee 2015, p. 16 (www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2015.pdf).

18 Bijv. bij CTB Locker wordt daarvoor verbinding gemaakt via het Tor-netwerk naar een betaalpagina om de betaling te verrichten. CSBN, a.w. (2015), p. 36. Tor staat voor 'The Onion Router', gratis software voor anonieme communicatie waarbij IP-adressen van computergebruikers worden gemaskeerd en het netwerkverkeer wordt versleuteld. Zie R. Dingledine, N. Mathewson & P. Syverson, *Tor: the second-generation onion router*, Washington DC: Naval Research Lab 2004.

19 Minder voorkomende typen zijn SynoLocker, Coinvault en TorrentLocker. CSBN, *a.w.* (2015), p. 35.

20 Curve staat voor de cryptografiemethode die gebaseerd is op elliptische curves, Tor staat voor 'The Onion Router', gratis software voor anonieme communicatie, en Bitcoin staat voor de betaalmethode van het losgeld. CTB Locker is ook wel bekend onder de naam 'Critroni'.

21 Y. Klijnsma, 'The state of ransomware in 2015', *Blog Fox-IT* 7 september 2015 (http://blog.fox-it.com/2015/09/07/the-state-of-ransomware-in-2015/). Voor een technische beschrijving van de malware, zie Computer Incident Response Center Luxembourg, *TR-33 Analysis – CTB-Locker/Critroni* (www.circl.lu/pub/tr-33/#ctb-locker-commands-and-states). Beek et al., a.w., p. 18 geven aan dat CTB Locker ook is verspreid via IRC-chat, peer-to-peer netwerken en nieuwsgroepen.

22 Volgens de wisselkoers begin 2016.

23 Een voorbeeld hiervan is Chimera, zie https://blog.botfrei.

CryptoLocker is cryptoware die is gericht op Microsoft Windows en is ergens in het najaar van 2013 voor het eerst gesignaleerd. Verspreiding loopt vooral via besmette e-mailbijlagen. Hoewel de kwaadaardige software betrekkelijk eenvoudig kan worden verwijderd, blijven de bestanden versleuteld op een manier die lastig is te kraken. Het losgeld bedraagt $ 400,=, dat moet worden betaald via prepaid cash vouchers (bijvoorbeeld via MoneyPak of Ukash) of een vergelijkbaar bedrag in Bitcoins.[24] Naar schatting is met CryptoLocker ten minste zo'n $ 28 miljoen afgeperst.[25] Tijdens een internationale operatie van opsporingsdiensten in 2014 werd een database met private sleutels ontdekt die inmiddels online beschikbaar is voor slachtoffers om hun bestanden te ontsleutelen.[26]

Virtueel geld bestaat in de vorm van bijvoorbeeld tegoeden op websites en speelgeld in spelomgevingen Ongeveer 90 procent van de totale marktwaarde van virtuele valuta wordt vertegenwoordigd door Bitcoins

CryptoWall is een van de meest winstgevende voorbeelden van cryptoware op dit moment. Deze familie van ransomware werd ontdekt in juni 2014 en sindsdien zijn verschillende varianten opgedoken. Het losgeld bedraagt $ 500,=, te betalen in Bitcoins. De meest recente versie (versie 3) leverde ongeveer $ 325 miljoen op in een periode van twee maanden, verspreid over honderdduizenden computergebruikers.[27] De meeste slachtoffers waren in Noord-Amerika.

3 Bitcoins en het betalen van losgeld

Als een slachtoffer eenmaal het losgeld in de vorm van Bitcoins heeft betaald, begint voor cybercriminelen het witwasproces. Om te kunnen beschrijven hoe dit in zijn werk gaat, is eerst enige uitleg over Bitcoins nodig. Bitcoins zijn een vorm van virtueel geld, dat wil zeggen een digitale weergave van geld dat niet door een overheid is gefiatteerd (zoals euro's of dollars). Virtueel geld bestaat in de vorm van bijvoorbeeld tegoeden op websites en speelgeld in spelomgevingen. Cryptocurrencies zijn een vorm van virtueel geld dat inwisselbaar is en decentraal wordt beheerd. Bitcoin is zo'n cryptocurrency, net als bijvoorbeeld Litecoin en Dogecoin. Ongeveer 90 procent van de totale marktwaarde van virtuele valuta wordt vertegenwoordigd door Bitcoins.[28] Deze cryptocurrency werd in 2009 opgezet door Satoshi Nakamoto.[29] Dit is het pseudoniem van een onbekend persoon, vermoedelijk zelfs een groep onbekende personen. Bij Bitcoin is er geen centrale autoriteit of bank: het gehele netwerk van Bitcoingebruikers beslist tezamen of een transactie legitiem is of niet.[30] Een nieuwe transactie wordt aan het gehele netwerk van gebruikers gemeld. Vervolgens valideert iedereen de transactie en meldt het resultaat terug aan het gehele netwerk.
Bitcoins worden opgeslagen op een computer[31] in een bestand, de zogeheten Bitcoin wallet of Bitcoinportemonnee.[32] Dit is niet zonder risico's: als het bestand wordt verwijderd of beschadigd, bijvoorbeeld door een computercrash, kan ook de toegang tot het geld in de wallet verdwenen zijn. De inhoud van een Bitcoin wallet kan ook worden gestolen.[33] Dat is mogelijk door een computer te hacken en de Bitcoins naar een ander adres over te maken of door de computer met de Bitcoins wallet daarop te stelen. De Bitcoin wallet kan in de cloud worden opgeslagen, maar ook daaraan zijn risico's

de/2015/10/chimera-ransomware-mit-fokus-auf-firmenrechner/. Merk op dat onduidelijk is of de ransomware echt technisch in staat is gegevens te onthullen. D. Gilbert, 'Chimera ransomware tries to turn malware victims into cybercriminals', *IB Times* 12 april 2015 (www.ibtimes.com/chimera-ransomware-tries-turn-malware-victims-cybercriminals-2211638).

24 Het bedrag in Bitcoins was eerst 2 Bitcoins, maar werd later *neerwaarts* bijgesteld met 0,3 Bitcoins om de fluctuerende waarde van Bitcoins weer te geven. V. Blue, 'CryptoLocker's crimewave. A trail of millions in laundered Bitcoin', *ZDNet* 22 december 2013.

25 Blue, a.w.

26 B. Krebs, 'New site recovers files locked by cryptolocker ransomware', *Krebs on Security* 18 augustus 2014.

27 Cyber Threat Alliance, *a.w.*, p. 5.

28 L. Trautman, 'Virtual currencies. Bitcoin & what now after Liberty Reserve, Silk Road and Mt Gox?', *Richmond Journal of Law and Technology* 2014, nr. 4, p. 46 (http://ssrn.com/abstract=2393537).

29 S. Nakamoto, 'Bitcoin: a peer-to-peer electronic cash system', *Bitcoin.org* oktober 2008 (https://bitcoin.org/bitcoin.pdf).

30 Zie ook A.F. Engelfriet, 'Ontwikkeling en recht: waar gaat het heen met Bitcoin?', *Tijdschrift voor Internetrecht* 2014, p. 149-152.

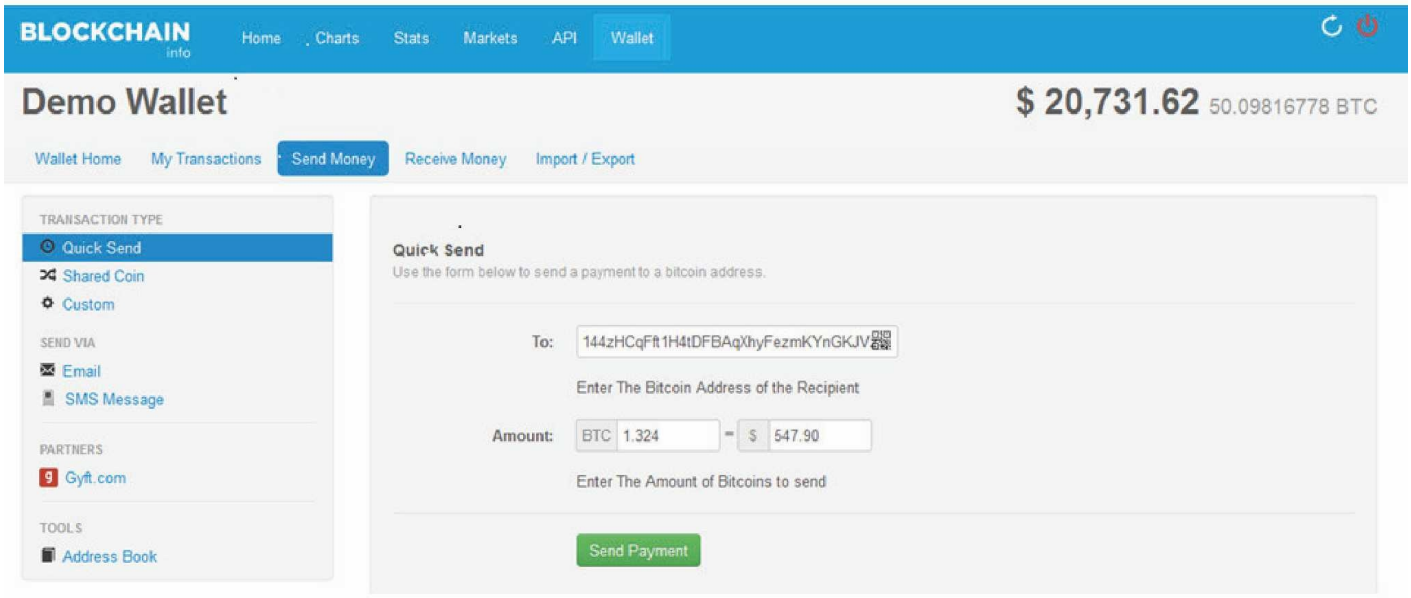
31 Dat kan zijn op de eigen pc, maar ook op een server in de cloud. Ook opslag op een smartphone is mogelijk.

32 Om precies te zijn: eigenlijk worden niet de Bitcoins zelf opgeslagen in de Bitcoin wallet, maar bevat de Bitcoin wallet de sleutels/rechten om gebruik te kunnen maken van een Bitcoinadres. Zonder deze rechten kan een gebruiker het Bitcoinadres niet meer gebruiken om zijn of haar Bitcoins te verplaatsen.

33 Bitcoins zelf zijn gegevens. Deze gegevens zijn echter uniek en op geld waardeerbaar waardoor, gelet op o.a. het Runescape-arrest (HR 31 januari 2012, ECLI:NL:HR:2012:BQ9251, NJ 2012/536, m.nt. Keijzer), het voor de hand ligt dat van diefstal sprake is wanneer iemand zich wederrechtelijk Bitcoins toe-eigent door deze over te maken naar een ander adres.

verbonden. Het is immers maar de vraag of de betreffende clouddienst adequate beveiliging en bescherming biedt.
Bitcoin is zo opgezet dat er uiteindelijk 21 miljoen Bitcoins in omloop zullen zijn. De verwachtingen wanneer de laatste nieuwe Bitcoin wordt geproduceerd lopen enigszins uiteen, van 2033[34] tot 2040.[35] In 2013 waren er ongeveer 12 miljoen Bitcoins in omloop met een waarde van circa € 10 miljard.[36] De koers van de Bitcoin stond in januari 2013 op ongeveer $ 14,= en in februari 2016 op ongeveer $ 380,=.[37]
Bitcoins worden in toenemende mate als geld beschouwd, omdat er steeds meer betalingen mee kunnen plaatsvinden die in de maatschappij ook met 'echt geld' worden verricht. Inmiddels kan ook in Nederland op diverse plaatsen met Bitcoins worden betaald, niet alleen op het internet, maar bijvoorbeeld ook in bepaalde cafés en restaurants, hotels, interieurwinkels en modezaken.[38] Bitcoins zijn volgens de Europese en de Nederlandse wetgeving echter geen officieel geld.[39] De Wet op het financieel toezicht (Wft) kent chartaal (contant), giraal en elektronisch geld.[40] Omdat Bitcoins geen fysieke verschijningsvorm hebben, is het geen chartaal geld. Bitcoins zijn echter ook geen elektronisch geld, omdat geen sprake is van een vordering op een uitgever.[41] Dit is ook door de Minister van Financiën[42] en door de rechter[43] bevestigd. Ook zijn Bitcoins geen financieel product, hetgeen wordt bevestigd door de Europese Centrale Bank.[44] Daarmee kan de conclusie worden getrokken dat Bitcoins en het gebruik van Bitcoins ongereguleerd zijn en niet onderhevig zijn aan enige vorm van financieel toezicht.[45] Bitcoins worden wel beschouwd als vermogen, zodat er wel belasting over dient te worden betaald.[46]
Bitcoins bieden volgens de FBI de gelegenheid tot het genereren, overboeken, witwassen en stelen van illegaal verkregen geld met enige anonimiteit.[47] In principe zijn gebruikers anoniem, maar het is wel zo dat transacties van een (anonieme) gebruiker aan elkaar kunnen worden gekoppeld. Als de identiteit van een gebruiker dus bekend raakt, bijvoorbeeld omdat de gebruiker die zelf prijsgeeft op internet, kan diens gehele transactiehistorie worden achterhaald. Wel is het mogelijk als gebruiker meerdere Bitcoin wallets aan te maken en per wallet meerdere Bitcoinadressen. Slechts per Bitcoin wallet kunnen transacties worden gekoppeld.
Bitcoins kunnen worden aangekocht of verkocht via tussenpersonen, zogeheten Bitcoinwisselkantoren, die Bitcoins aan- en verkopen tegen commissie. De commissie kan bestaan uit een vast bedrag per transactie, een percentage van het transactiebedrag of een combinatie van beide. Daarnaast zijn er ook Bitcoinplatformen waar gebruikers zonder tussenpersonen met elkaar kunnen handelen. Hier worden vraag en aanbod bij elkaar gebracht. Ook bij Bitcoinplatformen wordt vaak een commissie gerekend die kan bestaan uit een vast bedrag per transactie, een percentage van het transactiebedrag of een combinatie van beide. Bij Bitcoinplatformen dient men zich doorgaans te registreren en soms ook identificerende persoonsgegevens te verstrekken. In de praktijk noemen zowel Bitcoinplatformen als Bitcoinwisselkantoren zichzelf een 'Bitcoin Exchange' waardoor het onderscheid tussen Bitcoinplatformen en Bitcoinwisselkantoren soms lastig te maken is. Populaire Bitcoin Exchanges zijn onder meer CleverCoin, Kraken en BitStamp. In Nederland is Bitonic een populaire Bitcoin Exchange. Via Bitcoin Exchanges kunnen transacties plaatsvinden van de ene naar de andere virtuele valuta. Transacties kunnen ook plaatsvinden via overboekingen via een bank, een betaalkaart, contant of onlinebetalingsdiensten zoals PayPal, waarbij het geld op een onlineaccount wordt geparkeerd.
Het uitvoeren van transacties met Bitcoins gaat via de Bitcoin wallet en lijkt vanuit gebruikersperspectief min of meer op het versturen van een e-mailbericht.[48] Om Bitcoins over te kunnen maken naar een andere gebruiker is enkel diens ontvangstadres nodig. Het overboeken komt in de praktijk neer op het invullen van het adres van de ontvanger (de begunstigde), het invullen van het aantal Bitcoins (het transactiebedrag) en het klikken op 'verzenden'. Er is geen verdere verificatie of authenticatie nodig, zoals een pincode.[49] Het versturen is een onomkeerbaar proces. Wanneer te veel is overgemaakt of naar het verkeerde adres is overgemaakt, is dit niet meer ongedaan te maken. In figuur 2 is een voorbeeld weergegeven van een Bitcointransactie.

34 FBI, 'Bitcoin virtual currency. Unique features present distinct challenges for deterring illicit activity', *Wired* 5 september 2012 (www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf).
35 J. Baukema, 'Bitcoin: een (ongereguleerd) betaalmiddel van de toekomst?', *Tijdschrift voor financieel recht* 2013, p. 411-418.
36 Baukema, *a.w.*, p. 413.
37 www.koersbitcoins.net/.
38 Zie bijv. www.watisbitcoin.nl/uitgeven.php voor een lijst met winkels en horecagelegenheden.
39 Engelfriet, *a.w.*
40 Art. 1:1 Wft.
41 Art. 1:1 Wft (elektronisch geld).
42 *Aanhangsel Handelingen II* 2012/13, 2508.
43 Rb. Overijssel 14 mei 2014, ECLI:NL:RBOVE:2014:2667.
44 ECB, *Virtual currency schemes*, Frankfurt am Main 2012 (www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf); *ECB, Virtual currency schemes. A futher analysis*, Frankfurt am Main 2015 (www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf).
45 Zie ook *Aanhangsel Handelingen II* 2012/13, 2162.
46 www.belastingdienst.nl > vermogen > overige bezittingen.
47 FBI, *a.w.*
48 Technisch gezien wordt uiteraard bij e-mail een geheel ander protocol gebruikt. Bitcointransacties zijn bovendien sterker versleuteld.
49 Wel is een private key (cryptografische sleutel) nodig om transacties te kunnen verrichten. Deze zit in de Bitcoin wallet.



Figuur 2. Voorbeeld van een Bitcointransactie via de dienst Blockchain.info

4 Het witwassen van Bitcoins

Nadat een slachtoffer van ransomware Bitcoins heeft overgemaakt naar een daartoe aangewezen Bitcoinadres, begint voor de cybercriminelen het witwasproces. Er zijn verschillende manieren waarop het witwassen van Bitcoins kan plaatsvinden. Doorgaans wordt het witwasproces van Bitcoins gecombineerd met allerlei andere vormen van witwassen zoals we die kennen bij drugshandel en andere vormen van criminaliteit, zoals het verplaatsen van geld naar het buitenland, het investeren in onroerend goed of luxeproducten, afgeschermd consumeren, het fingeren van bedrijfsomzet, gokwinsten en loan-backconstructies.[50] Bij alle vormen van witwassen, ook bij cybercrime, is het gebruik van contant geld nog steeds de meeste voorkomende vorm.[51]

Toch is het interessant om na te gaan op welke wijze Bitcoins worden witgewassen, omdat het virtuele valuta betreft in plaats van een gereguleerde vorm van geld. Europol ziet Bitcoin als dé valuta die gemeenschappelijk onder cybercriminelen wordt gebruikt.[52] In Nederland is nog relatief weinig ervaring opgedaan met opsporingsonderzoeken met betrekking tot cryptoware en het witwassen van cryptocurrencies.

Kennis van de werking van Bitcoins, de betrokken actoren en vervolgingsvraagstukken zijn daarom onontbeerlijk. Hierna beschrijven we drie vormen van witwassen van Bitcoins.

De eerste manier om Bitcoins wit te wassen is met behulp van Bitcoinhandelaren. Dit zijn tussenpersonen die Bitcoins opkopen en daar contant geld voor een hoge commissie tegenover stellen. In deze situatie ontmoeten de cybercrimineel en Bitcoinhandelaar elkaar op een plaats in de fysieke wereld waarna via internet een transactie plaatsvindt. De Bitcoins worden dan rechtstreeks naar de handelaar overgemaakt die contant geld in ruil voor de Bitcoins geeft. Uit verschillende opsporingsonderzoeken is duidelijk geworden dat criminelen hun Bitcoins op deze manier hebben omgewisseld via deze handelaren. Daarbij zijn miljoenen aan Bitcoins gewisseld tegen geld met hoge commissie als vergoeding.[53] De contanten kunnen vervolgens via 'klassieke' methoden verder worden witgewassen of naar het buitenland worden weggesluisd.

De tweede manier om Bitcoins wit te wassen is met behulp van mixing services. Dit zijn online-'dienstverleners' die Bitcoins tegen Bitcoins wisselen, tegen betaling van een commissie.[54] Omdat Bitcointransacties worden bijgehouden in een openbaar register (de zogeheten blockchain), is de

50 Zie voor een overzicht bijv. E.W. Kruisbergen et al., *Georganiseerde criminaliteit in Nederland*, Den Haag: Boom Lemma 2012.

51 Europol, *Why is cash still king?*, Den Haag: 2015 (www.europol.europa.eu/content/why-cash-still-king-strategic-report-use-cash-criminal-groups-facilitator-money-laundering) (hierna: Europol 2015b).

52 Europol (2015a), p. 46: 'Overall, Bitcoin is beginning to feature heavily in many EU law enforcement investigations, accounting for over 40% of all identified criminal-to-criminal payments.'

53 Zie bijv. het persbericht op de website van de Belastingdienst, '10 aanhoudingen in internationaal bitcoins onderzoek', 20 januari 2016 (www.belastingdienst.nl/wps/wcm/connect/nl/fiod/nieuws/10_aanhoudingen_in_internationaal_bitcoins_onderzoek).

54 M. Möser, R. Böhme & D. Breuker, 'An inquiry into money laundering tools in the Bitcoin ecosystem', *eCrime Researchers Summit (eCRS)* 17-18 september 2013, p. 1-14 (http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6805780).

herkomst van Bitcoins, vergelijkbaar met serienummers van bankbiljetten, te traceren. Met behulp van mixing services wordt de herkomst van Bitcoins verder verhuld, omdat Bitcoins worden vervangen door andere Bitcoins. Soms worden Bitcoins van meerdere klanten vermengd, maar soms worden ook nieuwe Bitcoins aangemaakt. Mixing services werken vaak via een Tor-netwerk, waardoor de dienstverlener en de klanten anoniem blijven. Ook lijkt het erop dat mixing services vooral opereren vanuit jurisdicties waarmee weinig of geen justitiële samenwerking plaatsvindt.
Het gebruik van mixing services voor Bitcoins die middels cybercrime zijn verkregen is een verhullingshandeling die past binnen de omschrijving van het delict (opzettelijk) witwassen (art. 420bis Sr). Mixing services hebben geen enkel ander doel dan het verhullen van de herkomst van de Bitcoins en sommige diensten, zoals BitLaundry, maken ook geen geheim van deze doelstelling. Deze doelstelling en het inhouden van commissie zouden als bewijs kunnen dienen voor het vereiste opzet voor het witwassen. Er is nog geen jurisprudentie beschikbaar hierover.
Een derde manier om Bitcoins wit te wassen is het afgeschermd consumeren. Zoals hiervoor al is aangegeven, is het op steeds meer plekken mogelijk om met Bitcoins te betalen. De verdiende Bitcoins kunnen dus door cybercriminelen worden gebruikt om producten en diensten aan te schaffen. Een omzetting naar euro's of dollars is dan niet meer nodig. Het houden van Bitcoins in de portemonnee is geen verhullingshandeling, maar het voorhanden hebben van Bitcoins die afkomstig zijn uit een misdrijf is ook een vorm van witwassen (art. 420bis lid 1 onder b en 420quater lid 1 onder b Sr), mits geen kwalificatieuitsluitingsgronden van toepassing zijn, zie hierna.

5 Vervolging en inbeslagname

Zoals hiervoor aangegeven is het vervaardigen en verspreiden van ransomware strafbaar. Daarnaast is het witwassen van gelden verkregen uit cybercrime strafbaar. In deze paragraaf wordt nader ingegaan op de vraag in hoeverre het gebruik van Bitcoins in het witwasproces past binnen de bestaande strafbaarstellingen.
Onder het witwassen van een 'voorwerp' kan (uiteraard) ook geld worden verstaan. In 2006 heeft de Hoge Raad aangenomen dat met valse Bahreinse dinars kan worden witgewassen, omdat de biljetten met reguliere gelden waren gekocht.[55] Daarom kan ook worden aangenomen dat met virtuele valuta als Bitcoins kan worden witgewassen, omdat die tevens op geld waardeerbaar zijn en met reguliere valuta kunnen worden aangekocht.
In Nederland zijn er al zaken geweest waarin Bitcoins werden gebruikt bij het witwassen. Daarbij ging het om verschillende zaken met betrekking tot banking malware (kwaadaardige software bedoeld om bankgegevens te ontfutselen) waarin Bitcoins werden gebruikt om de opbrengsten wit te wassen. In de zaak MegaServer[56] werden computers en mobiele telefoons besmet met banking malware. Slachtoffers kregen via een e-mailbericht het verzoek om op een (nagemaakte) website persoonsgegevens en het merk van hun mobiele telefoon in te vullen. Daarna werd een sms-bericht gestuurd om de gebruiker onder valse voorwendselen een app te laten installeren op de mobiele telefoon. Hiermee werd het mogelijk om sms-berichten van de bank te onderscheppen en te gebruiken voor overboekingen. Zo konden de criminelen een deel van het klaargezette bedrag overmaken naar een van hun rekeningen. De verdachten hebben het geld vervolgens op verschillende manieren witgewassen. Zo werden verschillende vormen van elektronisch geld aangekocht, waaronder Bitcoins, Ukash, Webmoney en vouchers.[57] In een andere zaak[58] werd via duizenden euro's aan Bitcoins gekocht via rekeningen van money mules.[59] Daarbij werd ook gebruikgemaakt van mixing services. In een weer een andere zaak[60] werden Bitcoins verhandeld via Bitcoin Exchanges.
Voor de opsporingspraktijk is het van belang dat de Hoge Raad in enkele recente arresten zogenaamde kwalificatieuitsluitingsgronden voor het witwassen door middel van plaatsingshandelingen heeft geformuleerd.[61] Deze kwalificatieuitsluitingsgronden brengen met zich mee dat niet voor (opzet) witwassen kan worden veroordeeld, indien wordt vastgesteld dat een verdachte onmiddellijk crimineel verkregen voorwerpen (zoals Bitcoins) uit een zelf begaan misdrijf voorhanden heeft. Daarmee beoogt de Hoge Raad te voorkomen dat een verdachte die een bepaald misdrijf heeft begaan en die daarbij door dat misdrijf verkregen voorwerpen voorhanden heeft zich automatisch ook schuldig maakt aan witwassen.[62]

55 HR 11 april 2006, ECLI:NL:HR:2006:AV2349.

56 Rb. Rotterdam 2 oktober 2015, ECLI:NL:RBROT:2015:7038, ECLI:NL:RBROT:2015:7039, ECLI:NL:RBROT:2015:7041 en ECLI:NL:RBROT:2015:7044.
57 Zie bijv. Europol, a.w. (2016) voor een overzicht en beschrijving van deze betalingsmiddelen die tevens worden gebruikt voor het witwassen van gelden die worden verkregen uit cybercrime.
58 www.om.nl/vaste-onderdelen/zoeken/@32220/hackers-plunderen/.
59 Money mules zijn personen die hun bankrekening (doorgaans tegen een vergoeding) beschikbaar stellen aan criminelen.
60 www.bndestem.nl/regio/breda/cyberbende-rooft-rekeningen-leeg-bredaas-om-leidt-onderzoek-1.5015098.
61 Zie o.a. HR 8 januari 2013, ECLI:HR:2013:BX6910, HR 25 maart 2014, ECLI:NL:HR:2014:702, HR 16 juni 2015, ECLI:NL:HR:2015:1655, HR 13 oktober 2015, ECLI:NL:HR:2015:3028. De kwalificatieuitsluitingsgronden zijn gericht op art. 420bis lid 1 onder b en 420quater lid 1 onder b Sr.
62 M.J. Borgers, 'Rechtsvorming door de Hoge Raad en de reikwijdte van de strafbaarstelling van witwassen', *DD* 2013, p. 361-370.

Voor witwassen is dus, ten opzichte van het gronddelict, nog een extra handeling (de plaatsings- of versluieringshandeling) nodig.
Indien sprake is van een kwalificatieuitsluitingsgrond, moet worden bewezen dat er sprake is van het verbergen of verhullen van de criminele herkomst van het verkregen voorwerp. De politie kan hiermee rekening houden door bij een verhoor al na te vragen om welke reden geld wordt aangetroffen bij een huiszoeking en niet op de bank is gezet. Daarbij moet rekening worden gehouden met het feit dat een verklaring op zichzelf nog niet voldoende is om witwassen te bewijzen, ook moet sprake zijn van een daadwerkelijke gedraging.[63] Het Openbaar Ministerie moet dus motiveren dat verhullingshandelingen of verplaatsingshandelingen hebben plaatsgevonden, terwijl het onder omstandigheden evident kan zijn dat de voorwerpen uit criminele doeleinden zijn verkregen.[64]
In de handhavingspraktijk worden deze motiveringseisen als een belemmering ervaren. De volgende cybercrimezaak is illustratief voor dit probleem.
Op 8 mei 2014 heeft de Rechtbank Rotterdam een verdachte partieel vrijgesproken van witwassen, maar wel een vijfjarige gevangenisstraf opgelegd voor de 'grootschalige en grensoverschrijdende handel in XTC-pillen' via internet.[65] Tijdens de huiszoeking van de verdachte voor drugshandel werd een contant geldbedrag van € 82.900,= aangetroffen, waarvoor de verdachte voor witwassen is veroordeeld. Ontslag van alle rechtsvervolging volgde echter voor een hoeveelheid van ongeveer 325 Bitcoins op de Bitcoinwallet op een USB-stick die in het bezit was van de verdachte. De desbetreffende officier van justitie schatte in dat de verdachte ongeveer € 60.000,= had verdiend aan de handel van XTC op internet tegen betaling in Bitcoins. Echter, omdat de USB-stick te vinden was op de eettafel van de verdachte en verder 'niet gebleken [is] dat verdachte handelingen heeft verricht die erop neerkomen dat hij de aard, herkomst of vindplaats van de Bitcoins heeft verhuld' kon de rechtbank niet komen tot de kwalificatie van witwassen. Borgers en Kooijmans wijzen erop dat:[66]

'(...) het feit dat een verdachte in het bezit is van zowel drugs als geld, niet per definitie de vaststelling rechtvaardigt dat de verdachte zelf het gronddelict heeft begaan waarvan het aangetroffen geld de (directe) opbrengst belichaamt.'[67]

Het kabinet vindt nieuwe wetgeving noodzakelijk teneinde het voorhanden hebben van crimineel verkregen gelden beter te kunnen bestraffen.[68] Daartoe is recentelijk een wetsvoorstel ingediend dat het eenvoudiger moet maken om witwassen te vervolgen.[69] Het voorstel is om een nieuw lid 2 bij artikel 420bis Sr (nieuw) toe te voegen, waarbij duidelijk wordt gesteld dat het verwerven of voorhanden hebben van een voorwerp dat onmiddellijk afkomstig is uit een misdrijf dat de verdachte heeft gepleegd als 'eenvoudig witwassen' wordt verstaan. Daarmee zouden de kwalificatieuitsluitingsgronden die de Hoge Raad heeft geformuleerd teniet worden gedaan.[70]
Tot slot is met betrekking tot zaken waarbij (virtueel) geld wordt witgewassen door middel van Bitcoins kennis over de inbeslagname van Bitcoins onontbeerlijk. Een eerste vraag die daarbij moet worden gesteld is of Bitcoins als goed gekwalificeerd kunnen worden en daarmee vatbaar zijn voor inbeslagname. In de regel worden gegevens binnen het strafrecht niet gekwalificeerd als goed.[71] Echter, in de afgelopen jaren is uit jurisprudentie af te leiden dat gegevens wel degelijk als goed kunnen worden beschouwd voor zover zij uniek zijn en in het economische verkeer waarde hebben.[72] Het Openbaar Ministerie neemt dan ook de positie in dat Bitcoins als goed kunnen worden beschouwd en vatbaar

63 Zie bijv. HR 9 december 2008, ECLI:NL:HR:2008:BF5557 en HR 28 januari 2014, ECLI:NL:HR:2014:188.
64 Zie verder over de kwalificatieuitsluitingsgronden D.J. van Leeuwen, 'Witwassen naar Nederlands recht. Over voorhanden hebben en het bewijs van witwassen', *DD* 2011, p. 297-326; J. Verbaan & J. Nan, 'Probleemoplossingsgericht denken bij het witwassen uit eigen misdrijf afkomstige voorwerpen', *Proces* 2014, p. 272-288; M.J. Borgers & T. Kooijmans, 'Van probleem naar oplossing en weer terug. Het conceptwetsvoorstel aanpassing witwaswetgeving', *DD* 2015, p. 57-74.
65 Rb. Rotterdam 8 mei 2014, ECLI:NL:RBROT:2014:3504.
66 Borgers & Kooijmans, *a.w.*
67 Met verwijzing naar HR 21 januari 2014, ECLI:NL:HR:2014:127, *NJ* 2014/78, m.nt. M.J. Borgers.
68 Zie *Kamerstukken II* 2015/16, 34294, 3, p. 2. Borgers en Kooijmans, *a.w.* wijzen er echter op dat de jurisprudentie van de Hoge Raad voor het delict witwassen nog in ontwikkeling is. In de nabije toekomst raken de witwasbepalingen met de daarbij ontwikkelde kwalificatieuitsluitingsgronden wellicht meer uitgekristalliseerd.
69 Zie het Wetsvoorstel van 1 oktober 2015 tot Wijziging van het Wetboek van Strafrecht met het oog op het verbeteren van de mogelijkheden tot bestrijding van het verwerven en voorhanden hebben van uit misdrijf afkomstige voorwerpen (aanpassing witwaswetgeving).
70 Volgens Borgers en Kooijmans, *a.w.*, zou dit een aantal nieuwe problemen in het leven roepen die nu juist goeddeels door de Hoge Raad waren geëcarteerd.
71 Zie *Kamerstukken II* 1989/90, 21551, 3, p. 3 en HR 3 december 1996, *NJ* 1997/574.
72 Zie HR 31 januari 2012, ECLI:NL:HR:2012:BQ9251 (Runescape), HR 31 december 2012, ECLI:NL:HR:2012:BQ6575 (diefstal van belminuten), Hof Den Haag 3 december 2015, ECLI:NL:GHDHA:2015:3355 (diefstal van eindexamens op de Ibn Ghaldoun school). Zie voor een kritische analyse van deze trend in de rechtspraak B.W. Schermer en J.S. Nan in hun noot bij Rb. Rotterdam 13 februari 2014, ECLI:NL:RBROT:2014:976, *Tijdschrift voor Internetrecht* 2014, p. 83-86. Merk op dat in de memorie van toelichting van de Wet computercriminaliteit III wordt opgemerkt dat gegevens als goed worden aangemerkt indien zij uniek zijn en een individu gegevens uit zijn beschikkingsmacht kan verliezen (*Kamerstukken II* 2015/16, 24372, 3, p. 63).

zijn voor inbeslagname.[73] In ieder geval is helder dat een computer als voorwerp wordt gekwalificeerd dat vatbaar is voor inbeslagname. Op dit moment gelden afhankelijk van de locatie van de computer andere voorwaarden voor de inbeslagname.[74]
Een andere vraag is op welke wijze Bitcoins in beslag kunnen worden genomen. De volgende procedure wordt als standaard verondersteld voor de inbeslagname van Bitcoins.[75]
Als eerste stap moet de computer van de verdachte in beslag worden genomen waarop de Bitcoin wallet is opgeslagen. Als tweede stap kunnen de Bitcoins naar een ander adres worden overgemaakt, bijvoorbeeld naar een Bitcoinadres dat is aangemaakt door opsporingsambtenaren en in het beheer is van het Openbaar Ministerie.[76] Als derde en laatste stap kunnen de 'inbeslaggenomen' Bitcoins via een Bitcoin Exchange worden omgezet in euro's en op een rekening van het Openbaar Ministerie worden gestort. Indien de Bitcoins spoedig worden omgezet in euro's, wordt een snelle potentiële waardevermindering voorkomen. Deze wijze van inbeslagname komt overeen met de wijze waarop Bitcoins in Nederland in beslag worden genomen.[77]

6 Conclusie

Hoewel het maken en verspreiden van ransomware strafbaar is, is deze vorm van cybercrime vooralsnog lastig aan te pakken. Met name cryptoware is bijna niet te ontsleutelen als infectie eenmaal heeft plaatsgevonden. Voor computergebruikers is het beste advies om nooit links en bijlagen te openen van onbekende e-mailberichten, te zorgen voor goede spamfilters, te zorgen voor back-ups van bestanden en nooit te betalen bij ransomware maar in plaats daarvan aangifte te doen. Goede voorlichting kan deze basis-cyberhygiëne verder bevorderen onder computergebruikers.
Het opeisen van losgeld in de vorm van Bitcoins is inmiddels een duidelijke trend. Hoewel bij het witwassen de meeste criminelen, ook cybercriminelen, de voorkeur geven aan contant geld, blijkt het gebruik van Bitcoins voor hen interessant te zijn vanwege het gemak waarmee het geld naar het buitenland kan worden overgemaakt en de (tot zekere hoogte) geboden anonimiteit. Bitcoins worden onder meer witgewassen via Bitcoinhandelaren, mixing services en afgeschermd consumeren. Het witwassen via Bitcoins is strafbaar en Bitcoins kunnen in beslag worden genomen.
Criminelen verdienen grote bedragen met ransomware. Het gebruik van Bitcoins om de winsten van cybercrime wit te wassen biedt voordelen, maar laat ook digitale sporen na. Het is lastig, maar niet altijd onmogelijk om via deze digitale sporen toch daders van ransomware, cryptoware en witwassen van Bitcoins op te sporen.

73 Zie ook het interview met landelijk officier van justitie cybercrime Martijn Egberts door T. van der Geest, 'Misbruik van bitcoins', *Opportuun* 2015, nr. 6, p. 9 (www.om.nl).
74 C. Conings & J.J. Oerlemans, Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend?, *Computerrecht* 2013, p. 24. Merk op dat in het kader van het project Modernisering Wetboek van Strafvordering wordt overwogen de regeling tot inbeslagname ten opzichte van geautomatiseerde werken te wijzigen. Zie p. 79 van de Kamerbrief van minister Van der Steur van 30 september 2015 over de Modernisering van het Wetboek van Strafvordering.
75 UNODC, *Basic manual of the detection and investigation of the laundering of crime proceeds using virtual currencies*, United Nations Office on Drugs and Crime 2014 (www.imolin.org/pdf/imolin/FULL10-UNODCVirtualCurrencies_final.pdf).
76 UNODC, *a.w.*, p. 155.
77 Zie ook Van der Geest, a.w. Overigens koos de FBI in de Silk Road-zaak voor de verkoop van Bitcoins d.m.v. veiling. Zie bijv. 'Manhattan U.S. Attorney announces forfeiture of $ 28 million worth of Bitcoins belonging to Silk Road', 16 januari 2014 (www.justice.gov/usao/nys/pressreleases/January14/SilkRoadForfeiture.php).