HRRS-Nummer: HRRS 2018 Nr. 379
Bearbeiter: Christoph Henckel/Karsten Gaede
Zitiervorschlag: HRRS 2018 Nr. 379, Rn. X

BGH 1 StR 412/16 - Beschluss vom 27. Juli 2017 (LG Kempten)

Datenveränderung (Verändern von Daten: Voraussetzungen, hier: Hinzufügen von Einträgen in einer Registry-Datei); Ausspähen von Daten (erforderliche Dokumentation des Geheimhaltungsinteresses durch besondere Sicherungsvorkehrungen: Firewall); Anordnung des Verfalls (Krypto-Währung als erlangtes Etwas; Verschlechterungsverbot: Anwendbarkeit auf Verfallsanordnung, hier: Wertobergrenze der Verfallsanordnungen bei für verfallen erklärter Krypto-Währung mit hoher Wertvolatilität)

§ 303a Abs. 1 StGB; § 202a Abs. 1 StGB; § 73 Abs. 1 aF StGB; § 73e aF StGB; § 331 StPO

Leitsätze des Bearbeiters

1. Das Hinzufügen von Einträgen in der Registry-Datei eines Computers zum automatischen Starten heimlicher Hintergrundprogramme stellt ein Verändern von Daten im Sinne des § 303a Abs. 1 StGB dar.

2. Ein Verändern von Daten im Sinne des § 303a Abs. 1 StGB liegt vor bei einem Herbeiführen von Funktionsbeeinträchtigungen der Daten, die eine Änderung ihres Informationsgehalts oder des Aussagewerts zur Folge haben. Hierunter fällt jede Form der inhaltlichen Umgestaltung von gespeicherten Daten, wobei es nicht darauf ankommt, ob diese eine objektive Verbesserung darstellt. Entscheidend ist vielmehr, dass ein vom bisherigen abweichender Zustand herbeigeführt wird.

3. Geschützt sind Daten durch den § 202a StGB nur dann, wenn der Verfügungsberechtigte das Interesse an ihrer Geheimhaltung durch besondere Sicherungsvorkehrungen dokumentiert hat (vgl. BGH NStZ 2016, 339). Um von einer Dokumentation an der Geheimhaltung der Daten ausgehen zu können, bedarf es einer zum Tatzeitpunkt bestehenden Zugangssicherung, die darauf angelegt sein muss, den Zugriff Dritter auf die Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren. Darunter fallen insbesondere Schutzprogramme wie Firewalls, die geeignet sind, unberechtigten Zugriff auf die auf einem Computer abgelegten Daten zu verhindern, und die nicht ohne fachspezifische Kenntnisse überwunden werden können und den Täter zu einer Zugangsart zwingen, die der Verfügungsberechtigte erkennbar verhindern wollte (vgl. BGH NStZ 2011, 154).

4. Erlangtes Etwas im Sinne der § 73 Abs. 1 aF StGB ist die Gesamtheit des materiell aus der Tat tatsächlich Erlangten. Hiervon werden - ungeachtet ihrer Rechtsnatur - auch Bitcoins erfasst. Sie stellen angesichts ihres Marktwertes einen realisierbaren Vermögenswert dar, für den der Angeklagte sowohl materiell Berechtigter ist als auch die faktische Verfügungsgewalt hat. Sie sind angesichts der Speicherung in der Blockchain und der Kombination aus öffentlichen und dem Angeklagten bekannten privaten Schlüssel der Wallet hinreichend abgrenzbar und damit tauglicher, wenn auch nicht körperlicher Gegenstand einer Verfallsanordnung. Soweit dagegen geltend gemacht wird, Bitcoins könnten allein deswegen kein Verfallsgegenstand sein, da sie weder Sache noch Recht seien und deswegen der Wortlaut des § 73e aF StGB auf sie nicht anwendbar sei, kann dem nicht gefolgt werden. Die Vorschrift des § 73 Abs. 1 Satz 1 aF StGB enthält gerade keine solche Begrenzung auf Sachen oder Rechte.

5. Das Verschlechterungsverbot gilt auch für die Verfallsvorschriften (vgl. BGH NStZ 2011, 229) und bewirkt, dass die Maßnahme im Falle einer Anordnung nicht über den ursprünglichen Gegenstand hinaus erweitert werden darf (vgl. BGH NStZ 2014, 32). Zwar bleibt die Vermögensabschöpfung auf die Bitcoins beschränkt und erfasst unmittelbar keinen darüber hinausgehenden Gegenstand. Das Entfallen einer Wertgrenze für die Vermögensabschöpfung, die dem Angeklagten im ersten Rechtsgang als Begünstigung gewährt worden war, stellt aber nach der gebotenen faktischen Betrachtungsweise (vgl. hierzu BGH StraFo 2007, 510) eine den Angeklagten - je nach volatiler Entwicklung der Bitcoins - möglicherweise ungleich stärker belastende und damit schwerere Rechtsfolge dar.

Entscheidungstenor

1. Auf die Revision des Angeklagten wird das Urteil des Landgerichts Kempten (Allgäu) vom 13. April 2016

a) im Schuldspruch dahingehend geändert, dass der Angeklagte der Datenveränderung in 327.379 tateinheitlichen Fällen in Tateinheit mit 245.534 tateinheitlichen Fällen des Ausspähens von Daten sowie der

Fälschung beweiserheblicher Daten in 16 Fällen jeweils in Tateinheit mit Computerbetrug, schuldig ist;

b) im Ausspruch über den Verfall weiterer 1.730 Bitcoins dahingehend geändert, dass dieser der Höhe nach auf einen Betrag von 432.500 Euro begrenzt ist;

c) aufgehoben, soweit der Angeklagte in den Fällen 3 und 18 der in den Urteilsgründen enthaltenen Tabelle (IP-Adressen und) verurteilt worden ist.

Insoweit wird der Angeklagte freigesprochen.

2. Die weitergehende Revision des Angeklagten wird mit der Maßgabe als unbegründet verworfen, dass von der Gesamtfreiheitsstrafe ein Monat als vollstreckt gilt.

3. Im Umfang des Teilfreispruchs fallen die Kosten des Verfahrens und die notwendigen Auslagen des Angeklagten der Staatskasse zur Last.

Die von dem Angeklagten zu tragende Gebühr für dieses Revisionsverfahren wird um ein Sechstel ermäßigt. Die Kosten und die dem Angeklagten entstandenen notwendigen Auslagen für dieses Revisionsverfahren trägt die Staatskasse zu einem Sechstel und der Angeklagte zu fünf Sechsteln.

Gründe

Das Landgericht hatte den Angeklagten in einem ersten Urteil wegen Ausspähens von Daten in Tateinheit mit Datenveränderung sowie wegen Computerbetruges in 18 Fällen jeweils tateinheitlich mit Fälschung beweiserheblicher Daten zu einer Gesamtfreiheitsstrafe von drei Jahren verurteilt. Es hatte zudem den Verfall der sichergestellten 86 Bitcoins und den Verfall von Wertersatz (hinsichtlich weitere 1.730 Bitcoins) in Höhe von 432.500 Euro sowie die Einziehung von im Einzelnen näher bezeichneter Computerhardware nebst Zubehör angeordnet. Auf die Sachrüge des Angeklagten hatte der Senat das Urteil mit den Feststellungen aufgehoben. 1

Nunmehr hat das Landgericht den Angeklagten wegen Datenveränderung in 327.379 tateinheitlichen Fällen in Tateinheit mit 245.534 tateinheitlichen Fällen des Ausspähens von Daten und wegen Computerbetruges in 18 Fällen, jeweils in Tateinheit mit Fälschung beweiserheblicher Daten, zu einer Gesamtfreiheitsstrafe von zwei Jahren und zehn Monaten verurteilt. Daneben hat es den Verfall von 86 sichergestellten Bitcoins sowie weiterer 1.730 Bitcoins angeordnet und in der Urteilsformel konkret bezeichnete Computerhardware eingezogen. Hiergegen wendet sich der Angeklagte mit seiner Revision, mit der er die nicht näher ausgeführte Sachrüge erhebt. Sein Rechtsmittel führt zu einer Änderung des Schuldspruchs, einem Freispruch in zwei Fällen sowie einer Beschränkung des Verfalls der Höhe nach; im Übrigen ist es gemäß § 349 Abs. 2 StPO unbegründet. 2

A.

Das Landgericht hat folgende Feststellungen und Wertungen getroffen: 3

I.

Der Angeklagte und der rechtskräftig Verurteilte R. schlossen sich zu einem nicht näher bekannten Zeitpunkt Anfang des Jahres 2012 zusammen, um ein sogenanntes Botnetz aufzubauen. 4

Dabei handelt es sich um einen Zusammenschluss einer Vielzahl von Computern, auf denen Programme - zumeist vom Nutzer unbemerkt - im Hintergrund automatisiert sich wiederholende Rechenaufgaben abarbeiten. Die Programme verbinden sich selbständig mit einem durch den sogenannten Bot-Herder gesteuerten zentralen Command-and-Control-Server, so dass der Bot-Herder infolgedessen die angeschlossenen Rechner fernsteuern und für seine Zwecke nutzen kann. Die Bots werden von den Computernutzern häufig durch das Öffnen eines sogenannten trojanischen Pferdes, einer getarnten Schadsoftware, unbewusst selbst installiert oder es erfolgt eine Infektion des Rechners über eine Sicherheitslücke des Betriebssystems, des Webbrowsers oder eines Programms. Das vom Angeklagten und R. geplante Botnetz sollte einerseits der Erzeugung von Bitcoins, dem sogenannten „Bitcoin-Mining“, und andererseits der Datenspionage dienen. 5

Bitcoin ist ein weltweit verfügbares dezentrales Zahlungssystem und der Name einer virtuellen Geldeinheit. Die Übertragung von Bitcoins geschieht über einen Zusammenschluss von Rechnern über das Internet und wird mithilfe einer speziellen Peer-to-Peer-Anwendung, also ohne Einbeziehung einer als Bank dienenden Zentrale, abgewickelt. Sämtliche Bitcoins werden im öffentlichen Transaktionsregister, der sogenannten Blockchain, gespeichert. Ihre Zuordnung zu einzelnen Teilnehmern erfolgt über persönliche digitale Brieftaschen, sogenannte Wallets, über die das Guthaben verwaltet wird. Hierfür gibt es einen, jedem Teilnehmer des Peer-to-Peer Netzwerks erkennbaren öffentlichen und einen privaten, nur dem Inhaber der Wallet bekannten Schlüssel. Der Marktwert von Bitcoins ergibt 6

sich aufgrund von Angebot und Nachfrage.

Mit jeder Transaktion, die von der Mehrheit der Teilnehmer des Netzwerks als gültig bestätigt werden muss, um als ausgeführt zu gelten, werden bis zum Erreichen der systembedingten Maximalmenge zugleich neue Bitcoins erzeugt. Die für die Bestätigung der Transaktionen erforderlichen Rechenoperationen bestehen in der Lösung kryptographischer Aufgaben, wodurch das öffentliche Transaktionsregister der Kryptowährung, die Blockchain, erweitert wird. Die hierfür zu lösenden Algorithmen werden mit zunehmender Anzahl von Bitcoins immer komplexer und erfordern den Einsatz von zunehmend steigender Rechenzeit und -leistung. Derjenige Teilnehmer, der die Rechenoperation durchgeführt hat, erhält die mit der Erweiterung der Blockchain neu geschürften Bitcoins seiner Wallet gutgeschrieben. Je größer die eingesetzte Rechnerleistung, desto größer ist die Wahrscheinlichkeit, das richtige Ergebnis zu finden. Gewöhnliche Prozessoren sind jedoch nicht rentabel, da die durch sie verursachten Stromkosten den durch die neu generierten Bitcoins erfolgten Wertzuwachs minimieren. Die Stromkosten fallen jedoch bei der Lösung der Rechenaufgaben durch ein Botnetz bei dem Nutzer der mit Schadsoftware infizierten Hardware und nicht bei dem sie über den Command-and-Control-Server steuernden Bot-Herder an, was die Attraktivität der Botnetze für das Schürfen von Bitcoins erklärt. 7

R. kam die Aufgabe zu, die als Musik-, Video- oder Programmdatei zum Herunterladen aus dem Internet getarnte Schadsoftware in Form eines Trojaners nebst Möglichkeit zur Bitcoin-Generierung zu entwickeln. Als Grundlage hierfür diente ihm die als Software frei zugängliche sogenannte Zeus-Komponente, die eine sogenannte Keyloggingfunktion zur Übermittlung von Tastenanschlägen des betroffenen Nutzers und ein Spionageprogramm zur Aufdeckung und Manipulation verschlüsselten Netzwerkverkehrs enthielt. Diese ergänzte er um die TOR-Komponente, ein Netzwerk zur Anonymisierung von Verbindungsdaten, und die der Bitcoin-Generierung dienende Programmkomponente cgminer.exe, welche die Rechnerleistung der Grafikkarte nutzbar machte. Die Schadsoftware wurde sodann mit einer von R. und dem Angeklagten entwickelten Verschleierungsschicht und dem Kernschadprogramm angereichert. Der Angeklagte war für das Hochladen in das Usenet zuständig. Das Usenet ist ein Teil des Internets, der vorwiegend der anonymen Verschaffung illegaler Raubkopien dient und einen besonderen kostenpflichtigen Zugang beim Nutzer voraussetzt. 8

Kurz vor dem 13. März 2012 begann der Angeklagte, mit der Schadsoftware versehene Dateien auf verschiedene Server in das Usenet hochzuladen. 9

Wegen des damit verbundenen hohen Zeitanfalls warb er ab etwa Mitte des Jahres 2012 drei weitere Mittäter, sogenannte Spreader an, die insgesamt mehrere Millionen infizierte Dateien hochluden. 10

Der Trojaner war für die Betriebssysteme ab Windows XP bis Windows 7 bestimmt. Seit der Softwareaktualisierung Servicepack 2 (Herausgabedatum: 25. August 2004) verfügen diese Betriebssysteme standardmäßig (bei Windows XP) über eine aktivierte „Firewall“. Diese lässt sich manuell deaktivieren. Bei einer „Firewall“ handelt es sich um eine Zugriffssicherung für Netzwerke, um Angriffe aus dem Internet auf den Computer des Nutzers zu vereiteln. Hierzu werden insbesondere eingehende Verbindungsanfragen anhand der Konfiguration unter Windows geprüft und sofern keine Erlaubnis in Form einer speziellen, diesen Zugriff erlaubenden Konfiguration vorliegt, abgelehnt. Wäre die vom Nutzer selbst heruntergeladene Schadsoftware nicht als Musik-, Video- oder Programmdatei getarnt gewesen, wäre das Programm, das den Zugriff des Command-and-Control-Servers auf den Computer ermöglichte, mittels der Firewall dieser Kontrolle unterzogen und der Zugriff verweigert worden. 11

In dem Zeitraum vom 13. März 2012 bis zum 4. Oktober 2013 luden insgesamt 327.379 Computernutzer die Schadsoftware auf ihren Rechner herunter. Da sie durch die Tarnung davon ausgingen, es handele sich um die gewünschte Musik-, Video- oder Programmdatei, bejahten sie die Frage, ob das Programm installiert werden solle. Sie installierten sodann unbewusst den Trojaner und setzten in mindestens 245.534 Fällen infolgedessen ebenso unbewusst selbst die Firewall außer Kraft. In der zentralen Registrierungsdatenbank der jeweiligen Betriebssysteme, der sogenannten Registry-Datei, wurde ein Schlüssel und darin ein Wert erzeugt, der als Konfigurationseintrag für die Zeus-Komponente diente. Zudem wurde ein zusätzlicher Eintrag hinzugefügt, wodurch die Schadsoftware, insbesondere die Programmkomponenten Zeus, TOR und cg.miner, beim Hochfahren des Rechners automatisch startete, ohne dass der Computernutzer hiervon Kenntnis erlangte. Diese Veränderung der Registry-Datei führte zu einer grundlegenden Änderung der Datenstruktur und zugleich der Datei ntuser.dat, unter der die Werte des Benutzerprofils hinterlegt sind. Nach Installation des Trojaners nahm der Rechner des betroffenen Nutzers über einen ansonsten verschlossenen Zugang, den Port 42349, Verbindung mit dem Command-and-Control-Server auf. Da es sich um eine ausgehende Verbindungsanfrage handelte, wurde diese durch die Firewall nicht blockiert. Diese ausgehende Verbindung hätte ohne die Funktionen der Schadsoftware die Einrichtung einer speziellen Konfiguration des Systems („Port Forwarding“) erfordert. 12

Anschließend wurden die individuell vergebenen Computernamen, die verwendeten Betriebssysteme sowie weitere Informationen und Tastatur-Eingaben der infizierten Rechner über die Ports 42349 und 9050 an eine vom Angeklagten und R. angelegte Datenbank übertragen und dort gespeichert. Darüber hinaus wurde ab einer Inaktivität 13

des Computernutzers von 120 Sekunden mittels der Programmkomponente cg.miner die Rechenleistung der Grafikkarte für die Lösung komplexer Rechenaufgaben genutzt, für deren Bewältigung Bitcoins gutgeschrieben wurden. Über die Keyloggingfunktion der Zeus-Komponente wurden die letzten 1.000 Tastenanschläge an den Datenbankserver des Angeklagten übermittelt; zudem überschrieb Zeus die Programmcodes der für Ver- und Entschlüsselung zuständigen Netzwerkbibliotheken, so dass die Eingabe von Kontodaten, Geheimnummern und Passwörtern in unverschlüsselter Form an den Angeklagten übertragen wurde.

Die vom Angeklagten und R. betriebene Datenbank zeichnete bis zum Herunterfahren des Hauptservers zum 4. Oktober 2013 Einträge auf, wonach sich 327.379 Nutzer den Trojaner hinuntergeladen hatten. Das Landgericht konnte weder die Anzahl der verwendeten Versionen der Schadsoftware ermitteln, noch wie viele verschiedene Dateien in das Usenet hochgeladen wurden. Infolgedessen ist es zugunsten des Angeklagten davon ausgegangen, dass sämtliche Computernutzer ihre Rechner mit derselben Datei der Schadsoftware aus dem Usenet infiziert haben. 14

II.

Zum Betrieb des Botnetzes wurden insgesamt sieben Server betrieben, wobei es sich um einen Command-and-Control-Server, einen Hauptserver, einen Statistikserver und vier immer wieder wechselnde Server zur Bereitstellung der infizierten Dateien zum Download handelte. 15

Zwischen dem 19. November 2012 und dem 17. März 2013 mieteten entweder der Angeklagte selbst oder die von ihm beauftragten Spreader unter missbräuchlicher Verwendung zuvor durch die beschriebene Vorgehensweise ausgespähter Zugangsdaten in insgesamt 18 Fällen Server für den Betrieb des Botnetzes und die Verbreitung der Schadsoftware an. Die Server wurden aufgrund jeweils neuen Tatentschlusses und nicht aufgrund automatisierter Routinen unter Verwendung der Logindaten der Geschädigten angemietet; deren Freischaltung erfolgte in einem automatisierten Verfahren nach elektronischer Übermittlung des Antrags und der Daten. Hierdurch versprach sich der Angeklagte nicht zurückverfolgt werden zu können und sich die Anschluss- und Nutzungsgebühren zu ersparen. 16

Durch die Anmietung der Server entstand den Anbietern ein Gesamtschaden in Höhe von 7.349,75 Euro, nachdem diese den betroffenen Nutzern die angefallenen Kosten erstattet hatten. In zwei Fällen „entstand den Computernutzern eine Vermögensgefährdung hinsichtlich der Anmietkosten für vier Wochen“. Für diese beiden Fälle konnten weder der betroffene Anschlussinhaber noch der Zeitpunkt des Vertragsabschlusses benannt werden. 17

III.

Während 86 unverschlüsselte Bitcoins beschlagnahmt wurden, konnten weitere 1.730 Bitcoins lediglich vorläufig gesichert werden, weil deren Zugriff passwortgeschützt war, der Angeklagte das Passwort nicht preis gab und eine Entschlüsselung nicht möglich war. 18

B.

I.

Der Schuldspruch wegen Datenveränderung in 327.379 tateinheitlichen Fällen in Tateinheit mit 245.534 tateinheitlichen Fällen des Ausspähens von Daten gemäß §§ 202a, 303a Abs. 1, § 25 Abs. 1 und 2, § 52 StGB weist keinen Rechtsfehler auf. 19

1. Die Überzeugung des Landgerichts von dem insoweit festgestellten Sachverhalt beruht auf einer rechtsfehlerfreien Beweiswürdigung. 20

a) Zwar hat der Angeklagte eine Beteiligung an dem Botnetz bestritten. Das Landgericht hat dies jedoch mit nicht zu beanstandenden Erwägungen als unwahre Schutzbehauptung gewertet und sich hierfür insbesondere auf die Angaben des R. und weiterer Zeugen für die zwischen R. und dem Angeklagten im Tatzeitraum geführte Handykommunikation sowie einen Chat gestützt, in dem der Angeklagte gegenüber einem weiteren Zeugen Details zur Vorgehensweise einschließlich der Benennung des Vornamens des Mittäters R. offen gelegt hat. 21

b) Auch die Feststellungen zur Anzahl der Computersysteme, deren Nutzer sich das vom Angeklagten und R. in das Usenet gestellte trojanische Pferd mitsamt der Schadsoftware heruntergeladen und auf ihrem Computer installiert haben, fußen auf einer tragfähigen Grundlage. Hierzu hat das Landgericht die Einträge in der Datenbank des Hauptservers des Botnetzes ausgewertet und anhand der dort aufgezeichneten 327.379 individuellen IP-Adressen, die neben anderen Merkmalen nach erfolgreicher Installation der Schadsoftware an den Hauptserver des Botnetzes übertragen worden waren, die Anzahl der betroffenen Nutzer bestimmt. Da die IP-Adressen nebst weiteren Angaben nicht ohne die Installation des Trojaners an den vom Angeklagten betriebenen Datenbankserver übertragen worden wären, durfte das Landgericht aus der Aufzeichnung dieser Daten in der Datenbank des Angeklagten auf die erfolgreiche Installation der Schadsoftware schließen. 22

c) Die Wirkungsweise der vom Computernutzer unbewusst installierten Schadsoftware hat das Landgericht auf der Grundlage der nachvollziehbar dargelegten Erläuterungen der Sachverständigen hinreichend genau festgestellt. Insbesondere ergibt sich daraus zum einen, dass das Programm auf die Umgehung der - Zugriffe aus dem Internet verhindernden - Firewall angelegt war, indem es den Computernutzer über den Inhalt der heruntergeladenen und installierten Software getäuscht hat. Zum anderen wird daraus aber auch deutlich, zu welchen Funktionsänderungen die zusätzlichen Einträge in der Registry und damit in der das Benutzerprofil speichernden Datei nt.user.dat führten, dass nämlich Funktionen ausführende Komponenten gestartet, dadurch eine zuvor durch die Konfiguration des Computers nicht erlaubte Verbindung zum Command-and-Control-Server hergestellt und Daten an den Hauptserver des Botnetzes übertragen wurden. 23

d) Soweit das Landgericht davon ausgeht, dass jedenfalls 75 % der betroffenen Nutzer, mithin 245.534 tatsächlich eine aktivierte Firewall auf ihrem Computersystem nutzten, ist auch dies tragfähig begründet. 24

Insoweit waren dem sachverständig beratenen Landgericht konkrete Feststellungen zu den einzelnen betroffenen Computersystemen unmöglich. Denn anhand der übertragenen Daten war weder eine Identifizierung der Nutzer derselben noch deren konkrete Konfiguration zu ermitteln. Zwar waren die IP-Adressen bekannt, anhand des Zeitablaufs konnte aber bei den Internetprovidern keine Zuordnung der betroffenen Accounts mehr erfolgen. 25

Deswegen war das Landgericht befugt, auf das Vorhandensein einer aktiven Firewall indiziell zu schließen (vgl. hierzu BGH, Urteil vom 22. November 2013 - 3 StR 162/13, NStZ 2014, 215, 216; Beschlüsse vom 19. Februar 2014 - 5 StR 510/13, NStZ 2014, 318; vom 4. September 2014 - 1 StR 314/14, NStZ 2015, 98 und vom 24. August 2017 - 1 StR 625/16, ZInsO 2018, 324), zumal da individuelle Leistungsmotive insoweit keine Rolle spielten (vgl. hierzu BGH, Urteil vom 6. September 2017 - 5 StR 268/17, NStZ-RR 2017, 375). 26

Die tatsächlichen Umstände, aus denen es auf das Vorhandensein einer aktiven Firewall bei 75 % der betroffenen Computersysteme geschlossen hat, hat es nachvollziehbar dargelegt. Insoweit hat es sich auf die sachverständigen Darlegungen gestützt, wonach die Wahrscheinlichkeit, dass Internetnutzer keine aktivierte Firewall benutzten, äußerst gering sei. Darauf aufbauend hat das Landgericht zudem berücksichtigt, dass es sich bei den betroffenen Nutzern um solche handelte, die immerhin mit dem Usenet vertraut gewesen seien und einen eigenen kostenpflichtigen Zugang hierzu unterhielten. Um der geringen Wahrscheinlichkeit zu begegnen, dass dennoch infizierte Computersysteme zumindest keine Windows-Firewall aktiviert hatten, hat es von der Anzahl der infizierten Computer einen Abschlag von 25 % vorgenommen und so die Zahl der Computersysteme auf 75 % geschätzt, bei denen die Schadsoftware die Firewall umging. Auch vor dem Hintergrund, dass die Schadsoftware für Betriebssysteme bestimmt war, bei denen die Firewall standardmäßig aktiviert war, lässt diese Vorgehensweise einen Rechtsfehler nicht erkennen. Hierdurch hat das Landgericht pflichtgemäß diejenigen Tatsachen ermittelt, von deren Richtigkeit es überzeugt ist und ist damit der Abbildung der tatsächlichen Verhältnisse möglichst nahegekommen (vgl. zur Schätzung im Steuerstrafverfahren BGH, Beschluss vom 6. April 2016 - 1 StR 523/15, wistra 2016, 363). 27

II.

Auf der Grundlage dieser Feststellungen erweist sich die Verurteilung des Angeklagten wegen Datenveränderung in 327.379 tateinheitlichen Fällen in Tateinheit mit 245.534 tateinheitlichen Fällen des Ausspähens von Daten gemäß §§ 202a, 303a Abs. 1, § 25 Abs. 1 und 2, § 52 StGB als rechtsfehlerfrei. Dabei ist das Landgericht zutreffend von mittelbarer Täterschaft gemäß § 25 Abs. 1 Alt. 2 StGB im Hinblick auf die Installation des Trojaners durch den geschädigten Computerinhaber selbst ausgegangen (vgl. Frank in Hilgendorf, Informationsstrafrecht und Rechtsinformatik, 2004, S. 23 [30] mwN; zur Funktionsweise eines Trojaners siehe MünchKomm-StGB/Graf, 3. Aufl., § 202a Rn. 84). 28

1. Der Angeklagte hat danach Datenveränderung gemäß § 303a Abs. 1 StGB in 327.379 tateinheitlichen Fällen begangen. 29

Gemäß § 303a Abs. 1 StGB macht sich strafbar, wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert. Die Vorschrift schützt das Interesse des Verfügungsberechtigten an der unversehrten Verwendbarkeit der gespeicherten oder übermittelten Daten (Bär in Wabnitz/Janowsky, Handbuch des Wirtschafts- und Steuerstrafrechts, 4. Aufl., 14. Kapitel Rn. 108; Fischer, StGB, 64. Aufl., § 303a Rn. 2; LK-StGB/Wolff, 12. Aufl., § 303a Rn. 4 mwN; vgl. auch BT-Drucks. 10/5058, S. 34). 30

Der Angeklagte und seine Mittäter haben vorliegend durch den Eingriff in die Registry-Dateien und der Datei nt.user.dat der geschädigten Computersysteme Daten im Sinne des § 303a Abs. 1 StGB verändert. 31

a) Diese Dateien sind taugliche Tatobjekte im Sinne der Legaldefinition des § 202a Abs. 2 StGB, nämlich solche, die 32

elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden (Bär aaO Rn. 110; Fischer aaO Rn. 3; MünchKomm-StGB/Wieck-Noodt, 2. Aufl., § 303a Rn. 8; zur nicht unmittelbaren Wahrnehmbarkeit Goeckenjan wistra 2009, 47, 49 mwN). Eine Beschränkung auf Computerdaten, wie in der Richtlinie auf 2013/40/EU vom 12. August 2013, Art. 2 lit.b, lässt sich dem Gesetz nicht entnehmen (Fischer aaO Rn. 3, § 202a Rn. 4 unter Hinweis auf BT-Drucks. 16/3656 S. 10; vgl. demgegenüber aber Heine, NStZ 2016, 441, 443), wobei dies im vorliegenden Fall zu keinen abweichenden Ergebnissen führen würde. Unter den so bestimmten Datenbegriff fallen nach ganz einhelliger Meinung auch Programmdaten, da sie aus einer Vielzahl von Daten zusammengefügt sind und nicht unmittelbar wahrnehmbare Informationen enthalten (vgl. nur MünchKomm-StGB/Graf, 3. Aufl., § 202a Rn. 12 f. mwN; hierzu auch BGH, Beschluss vom 21. Juli 2015 - 1 StR 16/15, NStZ 2016, 339; aA nur v. Gravenreuth, NStZ 1989, 201, 204).

b) Da die Daten sich auf einem für den Angeklagten fremden Speichermedium befanden und ihm kein Nutzungs- oder Zugriffsrecht für bzw. auf diese zustand, braucht der Senat nicht zu entscheiden, welcher einschränkender Kriterien es bedürfte, um eine Verfolgbarkeit allein inhaltlicher Unrichtigkeit von Daten zu verhindern und den Zusammenhang mit § 303 StGB zu wahren (vgl. Bär aaO Rn. 111 f.; Fischer aaO Rn. 4 f.; MünchKomm-StGB/Wieck-Noodt aaO Rn. 9 f.). 33

c) Ein Verändern liegt vor bei einem Herbeiführen von Funktionsbeeinträchtigungen der Daten, die eine Änderung ihres Informationsgehalts oder des Aussagewerts zur Folge haben (BT-Drucks. 10/5058, S. 35; Bär aaO Rn. 118; Bär in Graf/Jäger/Wittig, Wirtschafts- und Steuerstrafrecht, 2. Aufl., § 303a StGB Rn. 20; Heine NStZ 2016, 441, 443; LK-StGB/Wolff, 12. Aufl., § 303a Rn. 27; MünchKomm-StGB/Wieck-Noodt, aaO Rn. 15). Hierunter fällt - entsprechend der Definition in § 3 Abs. 4 Satz 2 Nr. 2 BDSG (in der bis zum 24. Mai 2018 geltenden Fassung) - also jede Form der inhaltlichen Umgestaltung von gespeicherten Daten (LK-StGB/Wolff, 12. Aufl., § 303a Rn. 27; Altenhain in Matt/Renzikowski/Altenhain, § 303a Rn. 10; MünchKomm-StGB/Wieck-Noodt, 2. Aufl., § 303a Rn. 15), wobei es nicht darauf ankommt, ob diese eine objektive Verbesserung darstellt (Fischer aaO Rn. 12; Hilgendorf/Valerius, Computer- und Internetstrafrecht, 2. Aufl., Rn. 589; MünchKomm-StGB/Wieck-Noodt, aaO Rn. 15; aA Altenhain in Matt/Renzikowski/Altenhain, StGB, § 303a Rn. 10). Entscheidend ist vielmehr, dass ein vom bisherigen abweichender Zustand herbeigeführt wird (BT-Drucks. 10/5058 S. 36 zu § 303b, aber unter Bezug auf § 303a; LK-StGB/Wolff aaO Rn. 27). 34

Durch das Hinzufügen der Einträge in der Registry-Datei und die damit verbundene Veränderung des in der Datei nt.user.dat hinterlegten Benutzerprofils, ist eine solche Funktionsbeeinträchtigung der Daten eingetreten. Denn die Schadsoftware startete beim Hochfahren des Rechners automatisch, ohne dass der Computernutzer hiervon Kenntnis bekam. Infolgedessen wurde ein ansonsten verschlossener Zugang zum Internet geöffnet, worüber das Computersystem Verbindung mit dem vom Angeklagten betriebenen Command-and-Control-Server aufnahm und Informationen auf die Datenbank des Angeklagten übertrug. Vor der Hinzufügung dieser Einträge enthielt weder die zentrale Datenbank der betroffenen Computersysteme noch das in der Datei nt.user.dat hinterlegte Benutzerprofil die Information, dass die Programmkomponenten Zeus, TOR und cg.miner beim Hochfahren des Rechners automatisch gestartet werden. Zudem war der für die Verbindung zum Command-and-Control-Server genutzte Port für Verbindungen zum Internet durch die bisherige Konfiguration nicht freigegeben. Nach der Installation der Schadsoftware enthielten sie dagegen einen hiervon abweichenden Inhalt, dass nämlich diese Funktionen - das automatische Starten dieser Komponenten und damit auch die Verbindungsaufnahme zum Internet über einen ansonsten verschlossenen Zugang (vgl. zur Datenveränderung durch Öffnen eines ansonsten verschlossenen Ports Buggisch/Kerling, Kriminalistik 2006, 531, 536; Goeckenjan, wistra 2009, 47, 51; Heine aaO 444; vgl. auch Ernst, NJW 2003, 3233, 3238) - ausgeführt werden. Dadurch ist der Informationsgehalt dieser Dateien umgestaltet und mithin verändert worden. 35

Eine engere, diese Umgestaltung der auf den betroffenen Computersystemen enthaltenen, durch Daten verkörperten Informationen, nicht als Veränderung im Sinne des § 303a Abs. 1 StGB erfassende Auslegung würde dem Schutzzweck der Vorschrift nicht gerecht werden. Denn der Computernutzer betrieb ein Computersystem, welchem er nicht die Informationen gegeben hatte, die die durch die Schadsoftware bewirkten Funktionen, u.a. zum Betrieb eines Botnetzes (vgl. Bär in Graf/Jäger/Wittig aaO: Infektion des Rechners mit Schadsoftware zum Betrieb eines Botnetzes ist Verändern), zugelassen hätte. Sein Interesse an der unversehrten Nutzung des bisherigen Datenbestandes mit den von ihm bestimmten Beschränkungen, insbesondere dem geschlossenen Zugang zum Internet, ist durch die Hinzufügung der Funktionen beeinträchtigt. 36

Auf die Frage, ob ein Verändern von Daten im Sinne des § 303a Abs. 1 StGB auch vorliegt, wenn dem System durch die Installation eines Trojaners lediglich Daten hinzugefügt werden, ohne die vorhandenen (Bestands-)Daten zu verändern (dies verneinend: Hilgendorf/Valerius, Computer- und Internetstrafrecht, 2. Aufl., Rn. 597; Hilgendorf, JuS 1997, 323 [324 f.] und Altenhain aaO Rn. 10; vgl. auch Heine aaO S. 443), kommt es in Anbetracht der getroffenen Feststellungen nicht mehr entscheidungserheblich an. 37

2. Der Angeklagte hat sich tateinheitlich zu der Datenveränderung auch wegen Ausspähens von Daten nach § 202a 38

StGB in 245.534 tateinheitlichen Fällen strafbar gemacht.

Gemäß § 202a Abs. 1 StGB macht sich strafbar, wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft. Die Vorschrift schützt das formelle Geheimhaltungsinteresse des Verfügungsberechtigten (BT-Drucks. 16/3656 S. 9; 10/5058 S. 29; MünchKomm-StGB/Graf aaO Rn. 2 mwN; Schönke/Schröder/Lenckner/ Eisele, StGB, 29. Aufl., § 202a Rn. 1; im Ergebnis auch Bär in Wabnitz/ Janowsky, Handbuch des Wirtschafts- und Steuerstrafrechts, 4. Aufl., 14. Kapitel Rn. 72; Fischer, StGB, 64. Aufl., § 202a Rn. 2; LK-StGB/Hilgendorf, 12. Aufl., § 202a Rn. 6; aA Haft NStZ 1987, 6, 9; Lackner/Kühl/Heger, StGB, 28. Aufl., § 202a Rn. 1). Geschützt sind Daten durch die Vorschrift aber nur dann, wenn der Verfügungsberechtigte das Interesse an ihrer Geheimhaltung durch besondere Sicherungsvorkehrungen dokumentiert hat (BGH, Beschlüsse vom 21. Juli 2015 - 1 StR 16/15, NStZ 2016, 339 und vom 6. Juli 2010 - 4 StR 555/09, NStZ 2011, 154; Valerius in Graf/Jäger/Wittig, Wirtschafts- und Steuerstrafrecht, 2. Aufl., § 202a Rn. 19; BeckOK-StGB/Weidermann, § 202a Rn. 13; kritisch zur Dokumentation des Geheimhaltungsinteresses durch Sicherung, Dietrich NStZ 2011, 247). 39

a) Die Daten waren infolge der jeweils aktivierten Firewall im Sinne des § 202a Abs. 1 StGB gegen unberechtigten Zugang besonders gesichert. 40

Um von einer Dokumentation an der Geheimhaltung der Daten ausgehen zu können, bedarf es einer zum Tatzeitpunkt bestehenden Zugangssicherung, die darauf angelegt sein muss, den Zugriff Dritter auf die Daten auszuschließen oder wenigstens nicht unerheblich zu erschweren. Darunter fallen insbesondere Schutzprogramme, die geeignet sind, unberechtigten Zugriff auf die auf einem Computer abgelegten Daten zu verhindern, und die nicht ohne fachspezifische Kenntnisse überwunden werden können und den Täter zu einer Zugangsart zwingen, die der Verfügungsberechtigte erkennbar verhindern wollte (vgl. dazu BGH, Beschlüsse vom 6. Juli 2010 - 4 StR 555/09, NStZ 2011, 154 Rn. 6 und vom 21. Juli 2015 - 1 StR 16/15, NStZ 2016, 339 Rn. 8 f., jeweils mwN; BT-Drucks. 16/3656 S. 10; MünchKomm-StGB/Graf, 3. Aufl., § 202a Rn. 35 ff. mwN). 41

Auf der Grundlage der rechtsfehlerfrei getroffenen Feststellungen (vgl. oben 1. d) verfügten 245.534 der betroffenen Computersysteme zum Tatzeitpunkt über eine aktivierte Firewall. Diese stellt eine solche besondere Sicherung gegen unberechtigten Zugang dar. Denn sie dient gerade der Verhinderung eines unberechtigten Eindringens in das Netzwerk von außen und des Zugriffs auf (Rechner-)Daten innerhalb des Netzes (vgl. dazu auch Schönke/ Schröder/Lenckner/Eisele, StGB, 29. Aufl., § 202a Rn. 14; Heghmanns in Achenbach/Ransiek/Rönnau, Handbuch Wirtschaftsstrafrecht, 4. Aufl., 6. Teil Rn. 100; vgl. auch allgemein zu softwareintegrierten Sicherungen Bär aaO Rn. 79; Fischer aaO Rn. 9; MünchKomm-StGB/Graf aaO Rn. 45). Einen unkontrollierten Zugriff aus dem Internet auf den eigenen Rechner und mithin einen die jeweilige Firewall überwindenden Zugang wollten die Verfügungsberechtigten durch Verwendung einer solchen Sicherung erkennbar verhindern. 42

b) Der Angeklagte hat sich den Zugang zu den Daten auch durch die Überwindung gerade dieser Zugangssicherung verschafft, indem er die jeweils aktivierte Firewall mithilfe eines Trojaners umgangen hat. Denn erst durch den gezielten Einsatz eines Trojaners, der die Schadsoftware verbarg und den Computernutzer als Tatmittler glauben machte, er lade sich eine harmlose Musik-, Video oder Programmdatei herunter, tatsächlich aber unbewusst die Ausspähprogrammkomponenten installierte, konnten der Angeklagte und seine Mittäter die jeweilige Firewall überwinden und Zugang zu den Daten innerhalb des Netzes erlangen (dazu auch Bär aaO Rn. 83). Ohne diese Täuschungen der Computernutzer mittels des Trojaners wäre der Zugriff auf die Daten durch die Firewall verhindert worden, da durch diese eine eingehende Verbindungsanfrage des vom Angeklagten betriebenen Netzwerks abgelehnt worden wäre. Dieses Ergebnis korrespondiert auch mit einer Auslegung des Willens des Gesetzgebers, demzufolge Hacking-Angriffe mithilfe von Trojanern unter Strafe gestellt werden sollten (vgl. BT-Drucks. 16/3656 S. 9). 43

Durch die beschriebene Vorgehensweise hat der Angeklagte nicht nur das schon tatbestandsmäßige Verschaffen des bloßen Zugangs verwirklicht (vgl. BT-Drucks. 16/3656 S. 9), sondern zusätzlich sich die Daten selbst verschafft, was durch die Einträge in seiner Datenbank belegt wird. 44

c) Weder der Angeklagte noch seine Mittäter waren befugt im Sinne des § 202a StGB, da die ausgespähten Daten nicht zu ihrer Kenntnisnahme bestimmt waren (vgl. hierzu Fischer aaO Rn. 12 mwN; Valerius aaO Rn. 34; Gercke/Brunst, Praxishandbuch Internetstrafrecht, 2009, Rn. 100). 45

d) Ob der Tatbestand des § 202a StGB darüber hinaus auch durch Einsatz der Keyloggingfunktion erfüllt wurde, wie vom Landgericht angenommen, brauchte der Senat hier nicht zu entscheiden. Zweifel daran bestehen, zumal dem Landgericht aufgrund der enormen Datenmenge eine konkrete Zuordnung von gewonnenen, zuvor verschlüsselten Datensätzen nicht möglich war. 46

Die vom Landgericht angenommene zusätzliche Tatbestandsverwirklichung durch die Keyloggingfunktion hat sich bei 47

der Strafzumessung auch nicht ausgewirkt. Soweit dort die „multimodale Verwendungsmöglichkeit“ durch den „Zugriff“ berücksichtigt wird, wird dies von den Feststellungen getragen, ohne dass es auf die weitere Tatbestandsmäßigkeit ankommt.

e) Die Annahme von Tateinheit zwischen der Datenveränderung und dem Ausspähen von Daten durch das Landgericht ist nicht zu beanstanden. 48

III.

Die Feststellungen des Landgerichts tragen die Verurteilung des Angeklagten wegen Computerbetruges in Tateinheit mit Fälschung beweiserheblicher Daten gemäß § 263a Abs. 1 und 2, § 263 Abs. 3 Satz 2 Nr. 1, § 269 Abs. 1 StGB durch Anmietung der Server unter unbefugter Verwendung von Nutzerdaten der Geschädigten allerdings nur in 16 statt - wie vom Landgericht ausgeurteilt - in 18 Fällen. Da insoweit im Hinblick auf den Zeitablauf auszuschließen ist, dass ergänzende, eine Strafbarkeit des Angeklagten tragende Feststellungen getroffen werden können, spricht der Senat den Angeklagten in diesen beiden Fällen aus tatsächlichen Gründen frei. 49

1. Das Landgericht hat sich in neun Fällen mit sachverständiger Hilfe davon überzeugt, dass die Zugangsdaten, nämlich Kundennummern bzw. Passwörter für die Internetprovider oder E-Mail-Adressen der Anschlussnutzer für diese Anmietungen aus der vom Angeklagten im Rahmen des Botnetzes betriebenen Datenbank stammen. Zu dieser Datenbank waren die übertragenen Daten vom infizierten Rechner übermittelt worden. 50

In neun weiteren Fällen konnten die für die Anmietung verwendeten Daten zwar nicht in dem Bestand aus 1,9 Milliarden Daten festgestellt werden. Dennoch hat sich die Strafkammer davon überzeugt, dass der Angeklagte die Server unter Verwendung der durch die Keylogging-Funktion erlangten Daten anmietete. Das hat sie darauf gestützt, dass die angemieteten Server als Infektionsserver genutzt worden seien und der Angeklagte über die Schadsoftware die Möglichkeit gehabt habe, an die verwendeten Zugangsdaten zu gelangen. Nur in sieben dieser Fälle sind der Name des Geschädigten und der Zeitpunkt des Vertragsschlusses bekannt. 51

2. Dieser Schluss auf die Anmietung der Server unter Verwendung der vom Angeklagten mittels der Schadsoftware erlangten Daten ist allerdings nur insoweit tragfähig, als belegt wird, dass eine Anmietung unter Nutzung fremder Zugangsdaten überhaupt erfolgt ist. Soweit nämlich die Namen der Geschädigten bekannt sind, ist in der Zusammenschau ausreichend dargelegt, dass deren Zugangsdaten unbefugt zur Anmietung der Server verwendet worden sind. 52

In zwei Fällen - nämlich in den Fällen 3 und 18 der in den Urteilsgründen enthaltenen Tabelle (IP-Adressen und) - ist dies allerdings nicht der Fall. Insoweit sind weder Feststellungen zu den Geschädigten, noch zu den Tatzeiten und entstandenen Schäden getroffen worden. Festgestellt ist neben der verwendeten IP-Adresse lediglich, dass in diesen Fällen den nicht namhaft gemachten Computerinhabern eine Vermögensgefährdung bezüglich der Anmietkosten für vier Wochen entstanden sei. 53

Die Strafkammer legt hingegen nicht dar, woraus sie in diesen beiden Fällen den Schluss zieht, dass die Anmietung unter Nutzung fremder Zugangsdaten stattgefunden hat. Aus den Feststellungen für diese Fälle folgt zwar, dass der angemietete Server als Infektionsserver genutzt worden ist. Nachdem weder derjenige benannt werden konnte, dessen Daten verwendet worden sein sollen, noch festgestellt worden ist, dass den Providern ein tatsächlicher Schaden entstanden ist, kommt ebenso in Betracht, dass der Angeklagte diese Server unter Verwendung seiner Zugangsdaten angemietet und als Infektionsserver genutzt hat. Diese Möglichkeit wird von der Strafkammer nicht in den Blick genommen und infolgedessen auch nicht ausgeschlossen. 54

3. Eine Anmietung unter diesen Umständen stellt sich allerdings nicht als strafbar dar. 55

a) Danach hat der Angeklagte schon keine Daten im Sinne des § 263a Abs. 1 StGB unbefugt verwendet. Deswegen kommt es nicht mehr darauf an, dass die Höhe des eingetretenen Gefährdungsschadens in diesen beiden Fällen weder konkret festgestellt noch beziffert wird und damit die verfassungsrechtlichen Vorgaben nicht gewahrt sind (vgl. dazu BVerfG, Beschluss vom 23. Juni 2010 - 2 BvR 2559/08 Rn. 135 ff., insbesondere Rn. 150 [zu § 266 StGB], BVerfGE 126, 170 sowie BGH, Urteil vom 15. April 2015 - 1 StR 337/14, NStZ 2015, 514 [515] und Beschluss vom 4. Februar 2014 - 3 StR 347/13, NStZ 2014, 457, jeweils mwN). 56

b) Aber auch eine Fälschung beweiserheblicher Daten kann auf dieser Grundlage nicht angenommen werden. Denn die Speicherung oder Veränderung beweiserheblicher Daten zur Täuschung im Rechtsverkehr ist danach nur strafbar, wenn bei Wahrnehmung der manipulierten Daten eine unechte oder verfälschte Urkunde vorliegen würde. Gleiches gilt für den täuschenden Gebrauch derartiger Daten (vgl. nur BGH, Beschlüsse vom 13. Mai 2003 - 3 StR 128/03; NStZ-RR 2003, 265 und vom 16. April 2015 - 1 StR 490/14, NStZ 2016, 42). Diese Voraussetzungen sind für die 57

zwei fraglichen Fälle hier nicht belegt.

c) Auch eine Strafbarkeit nach anderen Vorschriften kommt für die Anmietung der Server unter diesen Umständen nicht in Betracht. 58

4. Angesichts des Zeitablaufs seit der Anmietung der Server ist auszuschließen, dass weitergehende, den Angeklagten belastende Feststellungen getroffen werden können. Dies ergibt sich schon daraus, dass das Landgericht festgestellt hat, dass über die bekannten IP-Adressen keine Rückschlüsse mehr auf die Nutzer gezogen werden können. Andere Anhaltspunkte zur Erlangung von Informationen über die verwendeten Zugangsdaten bestehen nicht. Der Angeklagte war daher für diese beiden Fälle freizusprechen, § 354 Abs. 1 StPO. 59

IV.

1. Die Strafzumessungserwägungen des Landgerichts sind revisionsrechtlich nicht zu beanstanden. 60

Der Gesamtstrafausspruch konnte trotz der Aufhebung der für diese zwei Fälle verhängten Einzelstrafen von zweimal zehn Monaten infolge des Freispruchs bestehen bleiben. Angesichts der maßvollen Erhöhung der Einsatzstrafe von zwei Jahren und den für die 16 verbliebenen Fälle des Computerbetruges in Tateinheit mit Fälschung beweiserheblicher Daten verhängten Einzelstrafen von jeweils zehn Monaten, konnte der Senat ausschließen, dass die Änderung des Schuldspruchs und der Wegfall von zwei Einzelstrafen in Höhe von jeweils zehn Monaten Einfluss auf die verhängte Gesamtfreiheitsstrafe gehabt hätte. 61

2. Im Hinblick auf die überlange Dauer des Revisionsverfahrens, die der Angeklagte nicht zu vertreten hat, war anzuordnen, dass hinsichtlich der Gesamtfreiheitsstrafe ein Monat als vollstreckt gilt. 62

V.

Die Anordnung des Verfalls der 86 Bitcoins sowie weiterer 1.730 Bitcoins erweist sich - bezüglich letztgenannten dem Grunde nach - als rechtsfehlerfrei. Sie hat allein insoweit keinen Bestand als der Verfall der weiteren 1.730 Bitcoins der Höhe nach nicht auf einen Betrag von 432.500 Euro begrenzt ist. Diesen begrenzenden Ausspruch hat der Senat in entsprechender Anwendung des § 354 Abs. 1 StPO nachgeholt. 63

1. Hinsichtlich der Verfallsanordnung des Landgerichts kommt das vor dem 1. Juli 2017 geltende Recht zur Anwendung. Zwar finden ausweislich der einschlägigen Übergangsvorschrift zum Gesetz zur Reform der strafrechtlichen Vermögensabschöpfung (Art. 316h EGStGB) mit Inkrafttreten des Gesetzes auch für bereits laufende Verfahren grundsätzlich ausschließlich die neuen Regelungen Anwendung (vgl. dazu BT-Drucks. 18/11640, S. 84). Allerdings sind gemäß Art. 316h Satz 2 EGStGB die Vorschriften des Gesetzes zur Reform der strafrechtlichen Vermögensabschöpfung vom 13. April 2017 nicht in Verfahren anzuwenden, in denen bis zum 1. Juli 2017 bereits eine Entscheidung über die Anordnung des Verfalls oder des Verfalls von Wertersatz ergangen ist. Dies ist hier der Fall, sodass die seit dem 1. Juli 2017 geltenden Vorschriften keine Anwendung finden. 64

2. Das Landgericht ist rechtlich zutreffend davon ausgegangen, dass die Bitcoins aus der Tat, nämlich der Datenveränderung gemäß § 303a StGB erlangt wurden und gemäß § 73 Abs. 1 Satz 1 aF StGB dem Verfall unterliegen. 65

a) Die mittels des Botnetzes generierten Bitcoins sind im Sinne des § 73 Abs. 1 Satz 1 aF StGB aus der Tat erlangt. Aus der Tat sind danach alle Vermögenswerte erlangt, die dem Täter unmittelbar aus der Verwirklichung des Tatbestandes selbst in irgendeiner Phase des Tatablaufs zufließen (BGH, Urteile vom 2. Dezember 2005 - 5 StR 119/05, BGHSt 50, 299 [309]; vom 30. Mai 2008 - 1 StR 166/07, BGHSt 52, 227 [246] und vom 28. Oktober 2010 - 4 StR 215/10, BGHSt 56, 39 [45 f.]; Beschlüsse vom 13. Februar 2014 - 1 StR 336/13, wistra 2014, 354 [358] und vom 17. März 2016 - 1 StR 628/15, BGHR StGB § 73 Erlangtes 19). 66

Durch die Datenveränderung wurde auf dem betroffenen Computersystem eine Verbindung zum Command-and-Control-Server über das Internet hergestellt, die vor dem Eingriff durch die Schadsoftware nicht stattgefunden hätte und auch nicht möglich gewesen wäre. Diese Internetverbindung wurde genutzt, um nach 120 Sekunden Inaktivität durch den Computersystemnutzer die Rechnerleistung von dessen Grafikkarte für die Rechenoperationen zu nutzen, die dem Schürfen der Bitcoins dienten. Durch die Nutzung der Rechenleistung erwarb der Angeklagte auch nicht lediglich eine Chance zum Schürfen von Bitcoins, die er erst später realisierte (vgl. hierzu BGH, Urteil vom 21. März 2002 - 5 StR 138/01, BGHSt 47, 260 [269 f.]). Vielmehr flossen ihm die 1.816 Bitcoins ohne jeden weiteren Zwischenschritt, mithin unmittelbar durch die - während der Nutzung der fremden Rechnerkapazitäten - andauernde Verwirklichung des Tatbestandes der Datenveränderung gemäß § 303a Abs. 1 StGB zu. 67

Erlangtes Etwas im Sinne der vorgenannten Vorschrift ist die Gesamtheit des materiell aus der Tat tatsächlich Erlangten (dazu BT-Drucks. 12/989, S. 23; vgl. auch Fischer, StGB, 64. Aufl., § 73 aF Rn. 8). Hiervon werden - ungeachtet ihrer Rechtsnatur (vgl. hierzu Goger, MMR 2016, 431 [432 f.]; Heine, NStZ 2016, 441, 444; Rückert, MMR 2016, 295 [296]; Spindler/Bille, WM 2014, 1357 [1363] jeweils mwN) - auch Bitcoins erfasst. Sie stellen angesichts ihres Marktwertes einen realisierbaren Vermögenswert dar, für den der Angeklagte sowohl materiell Berechtigter ist als auch die faktische Verfügungsgewalt (vgl. hierzu BGH, Beschlüsse vom 12. Mai 2009 - 4 StR 102/09, NStZ-RR 2009, 320 und vom 17. März 2016 - 1 StR 628/15, BGHR StGB § 73 Erlangtes 19) hat. Sie sind angesichts der Speicherung in der Blockchain und der Kombination aus öffentlichen und dem Angeklagten bekannten privaten Schlüssel der Wallet hinreichend abgrenzbar (vgl. hierzu Rückert aaO) und damit tauglicher, wenn auch nicht körperlicher Gegenstand einer Verfallsanordnung (Goger aaO; Heine aaO). Soweit dagegen geltend gemacht wird, Bitcoins könnten allein deswegen kein Verfallsgegenstand sein, da sie weder Sache noch Recht seien und deswegen der Wortlaut des § 73e aF StGB auf sie nicht anwendbar sei (Rückert aaO), kann dem nicht gefolgt werden. Die Vorschrift des § 73 Abs. 1 Satz 1 aF StGB enthält gerade keine solche Begrenzung auf Sachen oder Rechte (Fischer, StGB, 64. Aufl., § 73 aF Rn. 9; Heine aaO; Spindler/Bille aaO; vgl. auch BT-Drucks. 12/989, S. 23). § 73e aF StGB kommt demgegenüber keine einschränkende Wirkung zu. 68

b) Ob der private Schlüssel für die Wallet den Ermittlungsbehörden bekannt ist, hat auf die Möglichkeit der Anordnung des Verfalls keine Auswirkung. Die Kenntnis dieses Schlüssels ist zwar Voraussetzung, um die faktische Verfügungsgewalt über die Bitcoins zu übernehmen. Dies betrifft aber allein die Vollstreckung der Verfallsentscheidung, lässt hingegen die Anordnung des Verfalls unberührt (Heine aaO 445). Soweit der private Schlüssel zum Zeitpunkt der Entscheidung über den Verfall nicht bekannt ist, ist für die Vollstreckung der Anordnung des Verfalls die Mitwirkung des Angeklagten erforderlich. Ob diese erfolgt, kann bei der Entscheidung nicht beurteilt werden, weswegen es für die Anordnungsvoraussetzungen darauf nicht ankommen kann. Es handelt sich vielmehr um eine reine Vollstreckungsfrage. 69

c) Ansprüche von Verletzten stehen der Verfallsanordnung nicht entgegen. Nachdem sich die Ansprüche auf Beseitigung der Datenveränderung nicht auf die Rückerstattung des durch die Tat Erlangten richten (vgl. Fischer, StGB, 64. Aufl., § 73 aF Rn. 17), kommen insoweit nur Ansprüche von Verletzten in Betracht, die auf die Nutzung ihrer Grafikkarte für das Botnetz, also auf den hierdurch verbrauchten Strom bezogen sind. Da den betroffenen Computernutzern aufgrund der Besonderheiten des vorliegenden Falls die Möglichkeit fehlt, einen solchen zivilrechtlichen Anspruch schlüssig behaupten zu können, ihnen mithin kein durchsetzbarer Anspruch erwachsen ist, steht § 73 Abs. 1 Satz 2 aF StGB der Verfallsanordnung nicht entgegen (vgl. hierzu Heine aaO mwN). 70

Regelungsziel dieser Vorschrift ist es, den Angeklagten vor einer doppelten Inanspruchnahme zu schützen und ihm die Mittel zu belassen, die er zur Erfüllung der Ansprüche des Verletzten benötigt (vgl. hierzu nur BGH, Urteil vom 11. Mai 2006 - 3 StR 41/06, NStZ 2006, 680; Beschlüsse vom 10. November 2009 - 4 StR 443/09, NStZ 2010, 693 f. und vom 12. März 2015 - 2 StR 322/14, NStZ-RR 2015, 171). Sie steht also der Anordnung des Verfalls entgegen, wenn zumindest eine abstrakte Gefahr einer doppelten Inanspruchnahme besteht (vgl. hierzu BGH, Beschluss vom 12. März 2015 - 2 StR 322/14, NStZ-RR 2015, 171). Eine solche abstrakte Gefahr besteht zwar auch, wenn die durch die Taten des Angeklagten Geschädigten nicht ermittelt werden konnten und deren Feststellung auch künftig nicht zu erwarten, mithin mit der Geltendmachung und Durchsetzung von Schadensersatzansprüchen gegen den Angeklagten nicht zu rechnen ist (BGH, Beschluss vom 25. Juli 2006 - 4 StR 223/06) oder die Geschädigten bisher tatsächlich untätig geblieben sind (BGH, Urteil vom 11. Mai 2006 - 3 StR 41/06, NStZ 2006, 680; vgl. auch Beschluss vom 9. Dezember 2014 - 3 StR 438/14). Die Gefahr der doppelten Inanspruchnahme entfällt aber, wenn eine erfolgreiche Durchsetzung der Forderung aus Rechtsgründen ausgeschlossen werden kann (vgl. hierzu nur BGH, Urteil vom 11. Mai 2006 - 3 StR 41/06, NStZ 2006, 621 zum Verzicht und zur Verjährung). 71

So liegt es hier. Den Geschädigten ist es nicht möglich, den ihnen entstandenen Schaden zu beziffern. Hierzu müssten sie den gerade durch die Nutzung ihrer Grafikkarte für das Botnetz verbrauchten Strom plausibel machen können. Dies scheitert bereits daran, dass sie wegen der Besonderheit der Tat nicht bestimmen können, wann dies der Fall war. Danach ist es nicht lediglich aus tatsächlichen Gründen nicht (mehr) zu erwarten, dass die Geschädigten keine Ansprüche mehr geltend machen. Vielmehr scheidet es nach der Rechtslage aus, dass es noch zu einer Erfüllung der Ersatzforderung der betroffenen Computernutzer kommen könnte. Da das Risiko einer zumindest theoretischen Doppelbeanspruchung danach nicht besteht, wäre es mit dem Zweck der anzuwendenden Verfallsvorschriften - Abschöpfung des Taterlöses - unvereinbar, in diesem Fall über die Anwendung des § 73 Abs. 1 Satz 2 aF StGB dem Angeklagten die Möglichkeit zu eröffnen, sich die aus der Tat verschafften Vorteile zu sichern (Heine aaO). 72

3. Allerdings ist infolge der Anordnung des Verfalls von Wertersatz in Höhe von 432.500 Euro bezüglich der weiteren 1.730 Bitcoins im ersten Rechtsgang nunmehr gemäß § 358 Abs. 2 Satz 1 StPO die Anordnung des Verfalls der Höhe nach auf diesen Betrag zu beschränken. 73

Durch das aus der Vorschrift resultierende und von Amts wegen zu prüfende (BGH, Urteil vom 14. Oktober 1959 - 2 74

StR 291/59, BGHSt 14, 5 [7]; Beschluss vom 3. April 2013 - 3 StR 60/13, StV 2014, 466; Meyer-Goßner in Meyer-Goßner/Schmitt, StPO, 60. Aufl., § 358 Rn. 13) Verbot der Schlechterstellung darf das angefochtene Urteil in Art und Höhe der Rechtsfolgen der Tat nicht zum Nachteil des Angeklagten geändert werden, wenn lediglich der Angeklagte, zu seinen Gunsten die Staatsanwaltschaft oder sein gesetzlicher Vertreter Revision eingelegt hat. Denn der Angeklagte soll bei seiner Entscheidung darüber, ob er von einem ihm zustehenden Rechtsmittel Gebrauch machen will, nicht durch die Besorgnis beeinträchtigt werden, es könne ihm durch die Einlegung eines Rechtsmittels ein Nachteil entstehen (st. Rspr.; vgl. nur BGH, Urteil vom 10. November 1999 - 3 StR 361/99, BGHSt 45, 308 [310] mwN).

Das Verschlechterungsverbot gilt auch für die Verfallsvorschriften (vgl. nur BGH, Beschlüsse vom 9. November 2010 - 4 StR 447/10, NStZ 2011, 229 und vom 6. Februar 2014 - 1 StR 577/13, wistra 2015, 29) und bewirkt, dass die Maßnahme im Falle einer Anordnung nicht über den ursprünglichen Gegenstand hinaus erweitert werden darf (vgl. BGH, Beschlüsse vom 17. September 2013 - 5 StR 258/13, NStZ 2014, 32 und vom 13. Januar 2010 - 2 StR 519/09, StraFo 2010, 207; Meyer-Goßner in Meyer-Goßner/Schmitt, StPO, 60. Aufl., § 331 Rn. 21; BeckOK StPO/Wiedner, 29. Ed., § 358 Rn. 24). Zwar bleibt die Vermögensabschöpfung auf die Bitcoins beschränkt und erfasst unmittelbar keinen darüber hinausgehenden Gegenstand. Das Entfallen der Wertgrenze für die Vermögensabschöpfung, die dem Angeklagten im ersten Rechtsgang als Begünstigung gewährt worden war, stellt aber nach der gebotenen faktischen Betrachtungsweise (vgl. hierzu BGH, Beschluss vom 28. August 2007 - 4 StR 212/07, StraFo 2007, 510) eine den Angeklagten - je nach volatiler Entwicklung der Bitcoins - möglicherweise ungleich stärker belastende und damit schwerere Rechtsfolge dar (vgl. hierzu BGH, Beschlüsse vom 13. Januar 2010 - 2 StR 519/09, StraFo 2010, 207 und vom 3. April 2013 - 3 StR 60/13, StV 2014, 466). Der Angeklagte durfte darauf vertrauen, dass die neuerliche Vermögensabschöpfung nicht über einen Betrag von 432.500 Euro hinausgeht. 75

VI.

Die Kostenfolge für den freisprechenden Teil ergibt sich aus § 467 Abs. 1 StPO. Die Kostenentscheidung im Übrigen beruht infolge des teilweisen Erfolgs des Rechtsmittels im Hinblick auf die Verfallsentscheidung auf § 473 Abs. 4 StPO. 76