# Modulares Cybercrime

*Dieter Kochheim* [1]

Das Cybercrime ist aus dem Hacking entstanden, wobei nach und nach vom Betrug bekannte Methoden (Social Engineering) und kriminelle Maschen aufgenommen und mit den technischen und handwerklichen Fähigkeiten der frühen Hacker verbunden wurden.[2] Mit der Durchdringung der Informationstechnik in fast alle Wirtschaftsbereiche entstand das Bedürfnis, informationstechnische Prozesse zu automatisieren und fernzusteuern (Fernwartung). Diese Entwicklungen nahm die Cybercrime-Szene auf und entwickelte ihrerseits Malware mit zunächst noch beschränkten Einsatzmöglichkeiten. Auch die kriminellen Instrumente wurden immer feiner und autonomer. Am weitesten entwickelt sind jetzt die Botware, mit der unter der Kontrolle eines Command & Control-Servers – C&C – die Zombies in einem Botnetz gesteuert werden können, die Ransomware, die den Zugang zu dem infiltrierten System verhindert und den Anwender mit einer erpresserischen Forderung konfrontiert, und die Onlinebanking-Malware, die nach dem Einnisten verborgen bleibt und auf das auslösende Ereignis lauert. Sobald der Anwender eine Onlinebanking-Session startet, bezieht diese Malware die angepassten Webseiten der Bank ebenso von einem C&C wie die passenden Kontodaten des Bankdrops. Gleichzeit wählt der C&C einen passenden Finanzagenten, der möglichst ein Bankkonto bei derselben Bank hat wie das Opfer, um schnelle und ungestörte Zahlungen ausführen zu können (*Drop Matching*).

Das gibt den Anlass dazu, die kriminellen Zulieferungen zu strukturieren und die Strafbarkeit der Zulieferer zu skizzieren.

## Fortschreitende Spezialisierung und Kommerzialisierung

Bereits beim Skimming konnten arbeitsteilig tätige Täter festgestellt werden, die sich in Gruppen aufteilen und eine davon zunächst das Ausspähen der Zahlungskartendaten besorgt („Skimmer“ als Täter; *Skimming im engeren Sinne*) und die andere das *Cashing*, also den Beuteerlös durch den Einsatz gefälschter Zahlungskarten mit Garantiefunktion an ausländischen Geldausgabeautomaten. Weitgehend unklar ist dabei geblieben, ob eine dritte Gruppe die Fälschungen produziert oder ob dieser - technisch relativ einfache - Tatschritt von den Cashern ausgeführt wird; wofür nicht zuletzt spricht, dass Daten schneller und unauffälliger in das Ausland gebracht werden können als fertige Fälschungen. Die gelegentlich bemühten Repräsentanten am Ort des Ausspähens, die die ausspähenden Täter anleiten und kontrollieren sollen, sind nie so recht nach-

---

[1] Oberstaatsanwalt Kochheim leitete seit 2001 die IuK-Stelle bei der Generalstaatsanwaltschaft Celle, seit 2007 zunächst die Abteilung zur Bekämpfung der Organisierten Kriminalität und jetzt die Zentralstelle für Wirtschaftsstrafsachen bei der Staatsanwaltschaft Hannover. Im September 2015 erschien sein Buch dem Titel Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik, München (Beck).

[2] So schon: Moritz Jäger, Das Netz der Phisher: Wie Online-Betrüger arbeiten, tecchannel 20.9.2006.

gewiesen worden und dürften eher bei anderen Kriminalitätsformen zum Einsatz gekommen sein (*Enkeltrick*, *Schockanrufe*).

Bei den betrugsnahen Formen des Cybercrime, vor allem im Zusammenhang mit betrügerischen Webshops, dem "eBay"-Betrug (Vorkassebetrug) und vorgetäuschten Zahlungsanweisungen im bargeldlosen Zahlungsverkehr, sind eher Einzelpersonen und sporadisch zusammenarbeitende Tätergruppen in Erscheinung getreten. Die Entwickler von Mal-, Bot- und Ransomware scheinen in informellen Verbünden eingegliedert zu sein (tatgeneigte Schwärme), in denen Know How, spezielle Zulieferungen (*Exploits*, *Root Kits*) und Ergebnisse (Zugangsdaten, Malware, Werkzeuge; Tools) gehandelt und getauscht werden. Der Übergang zwischen einzelnen Experten und spezialisierten Operating Groups dürfte fließend sein (Bolduan 2008[3]). Dagegen wird, wie jüngst vom BKA, jetzt häufiger von kriminelle Dienstleistungsangeboten berichtet.[4]

Ihre frühen Formen zeigten sich in den Hackerfabriken,[5] die zunächst in Bulgarien (1990) und in Russland (1998) entstanden, später in den Schurkenprovidern wie das *Russian Business Network* (2005[6]), das die komplette Hardware und Netztechnik für die anonyme Verbreitung von Inhalten (Bullet Proof-Dienste), Daten und die Kommunikation bereitstellte, sowie von mietbaren Botnetzen (*Simda*; seit etwa 2006). Schon 2001 entstand mit CarderPlanet die erste bekannte Plattform für den Handel mit ausgespähten Daten, Malware und Know How.

Die Angebote von Crimeware-as-a-Service umfassen heute auch den Betrieb von Command & Control-Server, die Zulieferung von Kontakten zu Finanzagenten, die Verbreitung und Pflege von Malware sowie die Beutesicherung durch Wechselstuben (*E-Currencies*) und virtuelle Verrechnungseinheiten (*Vouchers, BitCoins*).

**Modulare Kriminalität**

Das klassische Verständnis von *arbeitsteiliger Kriminalität* ist von der Bande mit dauerhaft gemeinsam handelnden Tätern geprägt, die immer wieder dieselbe Art von Straftaten verüben und womöglich über einen festen Stamm von Hehlern verfügen, die die gestohlene oder ertrogene Beute abnehmen. Für das Cybercrime dürfte hingegen eine projektartige Betrachtung angezeigt sein, die eher beiläufig in 2008 von Bolduan beschrieben wurde und in deren Mittelpunkt ein Koordinator als Projektmanager steht:[7] *Die zentrale Figur jedoch ist ... ein „Independent Business Man" – eine Person, die Kontakte zur Unterwelt pflegt und zwischen Bot-Herdern, Hackern, Malware-Schreibern und Spammern koordiniert. ... mithilfe der Botnetz-Infrastruktur kann der Koordinator Unterneh-*

[3] Gordon Bolduan, Digitaler Untergrund, Technology Review 4/2008, S. 26 ff.; kostenpflichtiger Download.
[4] BKA, Cybercrime. Bundeslagebild 2014, 9.9.2015, S. 6.
[5] François Paget, Cybercrime and Hacktivism, McAfee 15.10.2010 (broken link).
[6] Frank Faber, Unter Verdacht. Eine russische Bande professionalisiert das Cybercrime-Business, c't 11/2008
[7] Gordon Bolduan, Digitaler Untergrund, Technology Review 4/2008, S. 30; kostenpflichtiger Download.

*men mit verteilten Massenangriffen auf ihre Webseiten drohen und so Schutzgeld erpressen, Spam-Wellen mit Werbung für überteuerte Produkte oder Aktien lostreten oder tausendfach persönliche Informationen wie Bankzugangsdaten ergaunern*.

Nach einem von Bolduan zitierten Gewährsmann soll es sich bei den Koordinatoren in aller Regel um frühere KGB-Leute oder Angehörige der russischen Mafia handeln. Der Koordinator betreibt Cybercrime-Management und hat dafür gewisse Gestaltungsfreiräume, je nachdem, welche Aufgaben er an Subunternehmer outsourcen kann und will.[8] Um zum Beispiel eine Phishing-Aktion nach klassischem Modell durchzuführen, braucht er ausgespähte Kontozugangsdaten. Die kann er kaufen, selber erheben oder die Erhebung und den Missbrauch in eine kombinierte Malware-Aktion einbinden. Mit dem Einkauf von Kontodaten, anderen Diensten oder Modulen, die der Koordinator benötigt, kann er national tätige *Operation Groups*, also Subunternehmer oder Vermittler beauftragen. Sobald er über diese Daten verfügt, braucht er noch Hacker für den Kontomissbrauch und Agenten für die Sicherung der kriminell erlangten Gewinne (Finanzagenten, Cashing). Diese "Hacker" müssen mehr vertrauenswürdig als kompetent sein. Der Aufruf eines Homebanking-Portals und der Missbrauch von Kontozugangsdaten einschließlich "normaler" Transaktionsnummern nach dem alten TAN-Verfahren ist eine eher banale Sache gewesen.

Der Koordinator, wie er von Bolduan vorgestellt wurde, entscheidet nach wirtschaftlichen Gesichtspunkten: *Aufwand*, *Ertrag* und *Gewinn*, allenfalls noch angereichert von dem *Entdeckungsrisiko*.[9] Die wirtschaftlichen Messgrößen bestimmen dabei auch die Auswahl der Zulieferer: Kostengünstige, aber überalterte Kontodaten versprechen einen geringeren Erfolg als aktuell abgegriffene, die teurer sind; Medienwechsel zwischen BitCoins und anderen Verrechnungssystemen (Voucher, Wechselstuben, Webmoney) verringern zwar die Beute, aber auch gleichzeitig das Entdeckungsrisiko.

**Formen des arbeitsteiligen Cybercrime**

Das einleitende Schaubild unterscheidet zwischen der Zulieferung nötiger Dienste und technischer Infrastruktur (links, Zulieferung und Rüstphase) sowie den ausführenden Taten (rechts), wobei ausgehend vom Internetradio die geringste kriminelle Zulieferung erfolgt und bei der Crimeware-as-a-Service die kriminelle Grunddienstleistung im Aufbau eines Botnetzes besteht, das die zahlenden Kunden zum Einsatz eigener produktiver Malware nutzen.[10] Die Zeilen von a bis e zeigen, ausgehend von einer noch sozialadäquaten Nutzung der Internettechnik, eine zunehmende kriminelle Spezialisierung der zuliefernden

[8] Siehe auch: Kochheim (Cyberfahnder), Schurken-Provider und organisierte Cybercrime, 13.7.2008.
[9] Siehe auch: Kochheim (Cyberfahnder), modulare Kriminalität. Cybercrime in Projektform, 5.10.2008.
[10] Ich unterscheide funktional zwischen der Basis-Malware, die zur Infiltration und zum Einnisten im angegriffenen System bestimmt ist, und der produktiven Malware, die die bezweckten Schadfunktionen als Onlinebanking-Malware, Keylogger, Ransomware oder andere ausführt. Unter technischen Gesichtspunkten ist diese Unterscheidung zweifelhaft, weil die informationstechnischen Prozesse im Einzelfall miteinander verbunden sein können, fragmentiert ablaufen und sich dann nicht kausal trennen lassen. Die rechtliche Betrachtung wird davon erleichtert und nicht verfälscht.

Dienstleister.

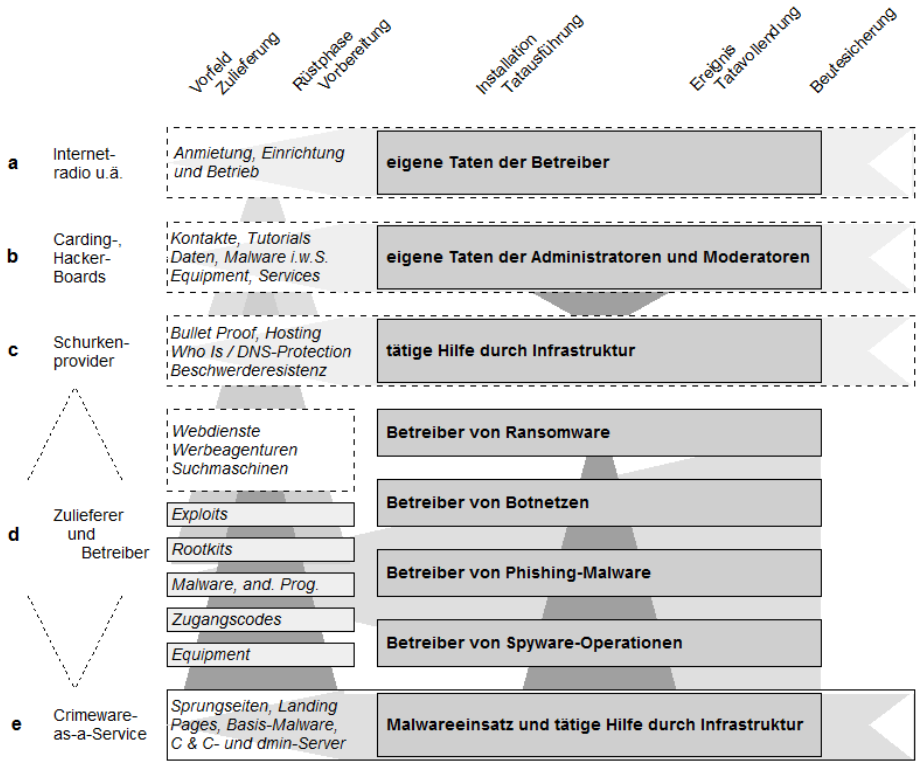


**Abb. 1: Zulieferung von Diensten und Infrastruktur in der Underground Economy**

Internetradio

Mit volksverhetzendem **Internetradio** hat sich der BGH mindestens in zwei Fällen befasst und die Radioveranstalter als kriminelle Vereinigung im Sinne von § 129 angesehen.[11] Sie benötigen einen Host- und Zugangsprovider mit leistungsstarken Anbindungen an das Internet, der das Streaming zulässt und technisch leisten kann. Weil ihm die Tatherrschaft fehlt, kann sich der Provider an den Straftaten der Radioveranstalter nur als Gehilfe beteiligen. Dabei ist zu berücksichtigen, dass der Provider zwar Technik beisteuert, die über übliche Anforderungen hinaus das *Streaming* ermöglicht, aber eben eine Technik, die

[11] BGH Beschl. v. 19.4.2011 - 3 StR 230/10, Rn. 4 ff.; BGH Beschl. v. 14.4.2015 - 3 StR 602/14. Verweise auf das StGB erfolgen ohne den Gesetzeszusatz.

keine andere Spezifikation hat als die, die auch andere Radioveranstalter benötigen. Bei solchen *berufstypischen "neutralen" Handlungen* verlangt der BGH nach einer besonderen *"Solidarisierung" mit dem Täter*,[12] die *nicht mehr als sozialadäquat anzusehen*, also als Beihilfe strafbar ist. *Hält er es lediglich für möglich, dass sein Tun zur Begehung einer Straftat genutzt wird, so ist sein Handeln regelmäßig noch nicht als strafbare Beihilfehandlung zu beurteilen, es sei denn, das von ihm erkannte Risiko strafbaren Verhaltens des von ihm Unterstützten war derart hoch, dass er sich mit seiner Hilfeleistung die Förderung eines erkennbar tatgeneigten Täters angelegen sein ließ*. Für den betroffenen Provider gelten die Grundsätze der üblichen Providerhaftung. Er ist Hostprovider wegen des von dem Radioveranstalter als Dateien zugelieferten Radioprogramms und wegen ihrer Inhalte nicht verantwortlich, solange er *nicht absichtlich mit einem Nutzer seines Dienstes zusammenarbeitet, um rechtswidrige Handlungen zu begehen* (§ 8 Abs. 1 S. 2 TMG). Von strafrechtlicher Bedeutung sind in diesen Fällen nur die Handlungen der Radioveranstalter oder Betreiber anderer Webdienste selber (betrügerische Webshops, schutzrechtswidrige Verbreitung, Mobbing).

Hacking- und Carding-Boards

Ein deutlich größeres *Risiko strafbaren Verhaltens* unterstützen die Betreiber von **Hacking-** und **Carding-Boards** und das besonders dann, wenn sie mit klaren, womöglich auch mehrdeutigen Aussagen für ihr Forum werben. Das beginnt mit der Namensgebung und der öffentlichen Werbung, führt über die Benennung der Threads und die gezielte Moderation in den Gesprächskreisen bis hin zur Gestattung eindeutig krimineller Webshops in geschlossenen Benutzerkreisen, in denen gegen eine Monopolgebühr bestimmte Waren (Skimmingequipment), Programme (Onlinebanking-Trojaner) oder andere Dienste (ausgespähte Daten) angeboten werden dürfen. Die Betreiber unterliegen einer selbständigen strafrechtlichen Haftung, soweit sie eigene Straftaten begehen. Das können eigene Betrugstaten sein, der Handel oder der Erwerb von Betäubungsmitteln oder die Treuhand, durch die die kriminellen Geschäfte der *Vendors*[13] ermöglicht und gesichert werden (Beihilfe, Begünstigung nach Beendigung des Grunddelikts).

Wegen der strukturellen Unterstützung verlangt das Gesetz neben einem strafbaren Grunddelikt (*Akzessorietät*) einen doppelten Gehilfenvorsatz, der sich darin ausdrückt, *dass der Gehilfe die Haupttat in ihren wesentlichen Merkmalen kennt und darüber hinaus in dem Bewusstsein handelt, durch sein Verhalten das Vorhaben des Haupttäters zu fördern*.[14] *Allerdings muss der Gehilfe … die wesentlichen Merkmale der Haupttat, insbesondere deren Unrechts- und Angriffsrichtung, im Sinne bedingten Vorsatzes zumindest für möglich halten und billigen*.[15] *Als Hilfeleistung in diesem Sinne* <ist> *grundsätzlich jede Handlung anzusehen, die die Herbeiführung des Taterfolges durch den Haupttäter objektiv fördert oder erleichtert; dass sie für den Eintritt dieses Erfolges in seinem*

[12] BGH Urt. v. 22.1.2014 - 5 StR 468/12, Rn. 26.
[13] Vendors: Händler.
[14] BGH Beschl. v. 15.11.2012 - 3 StR 355/12, Rn. 4.
[15] BGH Beschl. v. 28.2.2012 - 3 StR 435/11, Rn. 4.

*konkreten Gepräge in irgendeiner Weise kausal wird, ist nicht erforderlich*.[16] Der arglose Gehilfe macht sich nicht strafbar, weil sein förderndes Handeln neben Kenntnis Willen erfordert,[17] und eine indifferente Beihilfe, die sich darin äußert, *"jedwedes" oder "irgendein" Vermögensdelikt fördern* <zu wollen>*, reicht nicht aus*.[18] Dasselbe gilt für den begünstigenden Täter (§ 257). Für die Betreiber von kriminell ausgerichteten Boards (*Administratoren*) und ihren *Moderatoren* auf einer unteren Ebene bedeutet das, dass sie die Taten der Vendors als Gehilfen durch Rat, Tat und Gewährung fördern. Dabei kommt es nur darauf an, dass sie die Straftat als solche ermöglicht haben, und nicht auch darauf, dass die Tat auch ohne ihr Zutun möglich gewesen wäre.

Bullet Proof-Dienste

Auch wegen der **Schurkenprovider** und ihrer Bullet Proof-Dienste[19] kommt es darauf an, wie sie sich werbend und im laufenden Betrieb äußern und darstellen. Ihre Dienste sind zunächst normale Hosting-Dienste, so dass sie wie andere Hostprovider auch vom Telemediengesetz bis zur Grenze zur kriminellen Zusammenarbeit privilegiert werden (§ 8 Abs. 1 S. 2 TMG). Von den anderen Hostprovidern unterscheiden sie sich durch die Verschleierung der Serverstandorte, das *Who Is-Protection*[20] (*DNS-Protection*[21]) und ihre *Beschwerderesistenz*, die allesamt der Anonymisierung ihrer Kunden dienen. Diese Anonymität kann unter politischen und gesellschaftlichen Gesichtspunkten sinnvoll und sympathisch sein, findet jedoch dort ihre Grenzen, wo die Rechte Anderer nachhaltig betroffen sind.[22] Wegen der Strafbarkeit ist zunächst nach den eigenen strafbaren Aktivitäten zu fragen und das waren beim RBN (unsicheren Quellen nach) kinderpornografische Verbreitungen. Bei aktiven Unterstützungshandlungen - vergleichbar der Treuhand in den Carding-Boards - kommt eine unmittelbare Beteiligung als Gehilfe oder als Begünstigung zu den Taten der Kunden in Betracht; im Einzelfall auch wegen Umgangstaten im Vorbereitungsstadium (BtM-Handel, Umgangsdelikte wie nach § 149 Abs. 1). Bei anderen Erfolgsdelikten kommt es auf die Kenntnisse des Schurkenproviders an. Wirbt er aktiv für bestimmte kriminelle Webdienste, die er ausführt, wird er zum Gehilfen, verweigert er die Auskunft über die Identität des Kunden (Beschwerderesistenz), kommen Begünstigung und Strafvereitelung in Betracht (§ 257, § 258).

Beteiligung der Zulieferer

**Dual Use** sind Dienste und Produkte, die einem legalen Zweck dienen, aber auch zu Straftaten missbraucht werden können. Im Hinblick auf den *Hackerparagrafen* hat das BVerfG den - schon im Wortlaut des § 202c unzweideutig angelegten - Schluss gezogen, dass erst die kriminelle Zielrichtung des Angebots

[16] BGH Beschl. v. 23.12.2009 - 1 BJs 26/77-5 - StB 51/09, Rn. 24.
[17] BGH Urt. v. 18.4.1996 - 1 StR 14/96, Rn. 12.
[18] BGH Beschl. v. 28.2.2012 - 3 StR 435/11, Rn. 4.
[19] „Kugelsichere“ Dienste zum Schutz ihrer kriminell handelnden Kunden.
[20] Verschleierung des Inhabers einer Adresse im Domain Name System – DNS.
[21] Verschleierung des Inhabers und des Standortes des Hostspeichers.
[22] Das Russian Business Network – RBN – soll ein einfaches Vergütungssystem gehabt haben. Danach mussten die Kunden umso mehr zahlen je häufiger und drängender die Beschwerden wurden.

und die darin verkörperte Absicht zur Strafbarkeit führen.[23] An *Exploits*,[24] *Root Kits*,[25] Equipment und Malware mag es auch ein akademisches, journalistisches oder aufklärerisches Interesse geben. Der Handel mit ihnen orientiert sich hingegen in erster Linie daran, dass damit Straftaten begangen werden können. Die Zulieferer, die in der Grafik unter d benannt werden, unterliegen deshalb häufig einer selbständigen Strafbarkeit (§ 149 Abs. 1, § 202c, § 263a Abs. 3; § 22b StVG wegen der Wegstreckenzähler und Geschwindigkeitsbegrenzer) und sind spätestens als Gehilfen zu den vollendeten Ausführungstaten ihrer Käufer zu behandeln. Eine Besonderheit stellt § 149 Abs. 1 dar, weil die Strafbarkeit schon bei der einfachen Eignung des Equipments oder der Steuerung (Programm) zur Begehung von Straftaten einsetzt.[26]

Nur wenige Formen des Cybercrime sind als Verbrechen strafbar (§ 12 Abs. 1). Dazu zählen das Skimming beim abschließenden Cashing als Fälschen, Erwerb und Gebrauchen von Zahlungskarten mit Garantiefunktion (§ 152b Abs. 1) und die gleichzeitig gewerbs- und bandenmäßig begangenen Formen des Betruges und des Computerbetruges (§ 263 Abs. 5, § 263a Abs. 2) sowie der Urkundenfälschung, der Fälschung technischer Aufzeichnungen und beweiserheblicher Daten (§ 267 Abs. 4, § 268 Abs. 5, § 269 Abs. 3). Solche Verbrechen kommen im Wesentlichen im Zusammenhang mit moderner Malware in Betracht, die sich beim Onlinebanking (*automatisches Phishing*) wie ein Man-in-the-Middle zwischen den Bankkunden und dem Web-Interface der Bank schaltet und von einem *Command & Control-Server – C&C*, also vollautomatisch gesteuert, den Browser mit gefälschten Webseiten sowie den Daten für Zielkonten (Bankdrop) und Finanzagenten versorgt. Die klassischen Hacking-Delikte wie das Ausspähen und Abfangen von Daten (§ 202a Abs. 1, § 202b) sowie die Datenveränderung und die Computersabotage (§ 303a, § 303b) sind hingegen nur als Vergehen ausgelegt und das gilt auch für die Grundformen der Betrugs- und Urkundsdelikte.

Wenn ein Verbrechen in Rede steht, dann ist nicht nur immer auch der Versuch strafbar (§ 23 Abs. 1), sondern können sich die Täter – nicht aber die Gehilfen – auch schon an einer Verbrechensabrede beteiligen (§ 30), die bereits im sonst straflosen Vorbereitungsstadium angesiedelt ist. Für die Zulieferer und Unterstützer ist dabei von Bedeutung, ob sie Tatherrschaft haben, also ob ohne ihre Tatbeiträge die Tatbegehung ausgeschlossen wäre. Das hat der BGH schon vor etlichen Jahren wegen des Mittäters angenommen, der einen Firmenmantel beschaffte, den seine Komplizen danach zu Betrugstaten nutzten.[27] Sozialadäquate und solche Zulieferungen, die von der finalen Tatvollendung räumlich und zeitlich entfernt sind, zeigen keine täterschaftliche Nähe zur Vollendung und sprechen für eine Beteiligung als Gehilfe. Das gilt etwa für die Lie-

[23] BVerfG Beschl. v. 18.5.2009 - 2 BvR 2233/07, 1151, 1524/08.
[24] Handelbare Schwachstellen einschließlich der Beschreibung ihrer Nutzbarkeit – meistens in Form einer vorgefertigten Programmroutine.
[25] Handelbare Programme zur Tarnung eines Hacking-Angriffs und der dabei installierten Malware.
[26] Siehe auch § 127 OWiG wegen der Sachen, die zur Geld- oder Urkundenfälschung benutzt werden können, und § 275 wegen der Fälschung von amtlichen Ausweisen.
[27] BGH Beschl. v. 29.4.2008 - 4 StR 125/08.

feranten von Skimming-Equipment (Lesevorrichtungen für Kartendaten, Tastaturauflagen für Geldausgabeautomaten) oder zum Fälschen von Zahlungskarten,[28] nicht aber immer für die Ausspäher beim Skimming im engeren Sinne, die auch das Cashing betreiben, dauerhaft mit den ausführenden Tätern zusammenarbeiten[29] oder die ausgespähten Daten an die tatbereiten Fälscher übermitteln.[30]

Die Verbreitung und der Betrieb automatisierter Malware ist im Anschluss an die Rechtsprechung zu den Zeitzünderbomben und Gifttrunken ein *Distanzdelikt*,[31] dessen Versuch erst dann beginnt, sobald *sich die Gefahr für das Opfer verdichtet* und es in den unmittelbaren Wirkungsbereich der Falle gerät.[32] Das ist nicht der Fall bei den Programmierern und Händlern bei der Phishing-Malware, die hingegen nach § 263a Abs. 3 schon im Vorbereitungsstadium belangt werden können, wohl aber bei den (willentlichen) Betreibern von infizierten Webseiten und Landing Pages, von denen Basismalware bereitgehalten und bei der Infektion ohne menschliches Zutun (automatisch) von einem Command & Control-Server unterstützt werden. Er sorgt dafür, dass die öffentlichen, systemischen Daten des angegriffenen Systems verarbeitet (Betriebssystem, Browser, Anwendungsprogramme, Virenscanner, Stand ihrer Updates, Spracheinstellungen des Systems und des Tastaturtreibers, IP-Adresse) und die Erfolg versprechenden Exploits zugeliefert werden. Wird dabei gleichzeitig die produktive Malware installiert (Ransom- oder Botware, Onlinebanking-Malware), dann beteiligt sich der Zulieferer bereits am Versuch der Ausführungstat.

Das gilt nicht für schlichte Keylogger, weil das Ausspähen und das Abfangen von Daten keine Strafbarkeit des Versuchs vorsehen (§ 202a Abs. 1, § 202b). Bereits die Installation der Malware ist jedoch mit Datenveränderungen (§ 303a) und in aller Regel mit einer Computersabotage verbunden (§ 303b Abs. 1 Nr. 2), so dass die Betreiber von maliziösen Webseiten einer selbständigen, täterschaftlichen Strafbarkeit unterliegen, die bei einer erfolgreichen Installation produktiver Malware auch zu einer täterschaftlichen Beteiligung am Versuch des Ausführungsdelikts wird, das mit der produktiven Malware erstrebt wird.

Zwischenergebnisse

Tatferne Zulieferer von kriminellen Diensten, Hardware und Software können sich wegen besonderer Gefährdungsdelikte selbständig (besonders nach § 149 Abs. 1, § 202c, § 263a Abs. 3) oder – wenn sie ausnahmsweise im Rahmen einer Verbrechensabrede tatherrschaftlich tätig werden – sich auch schon im Vorbereitungsstadium strafbar machen. Zu Gehilfen in Bezug auf die Ausführungstaten werden sie, wenn sie ein maßgebliches Verwirklichungsrisiko geschaffen haben. Bei der Zulieferung sozialadäquater Infrastrukturen gilt das einerseits dann, wenn die Zulieferer eigene Straftaten begehen (Schaffung von

---

[28] Jürgen Schmidt, MacGyvers Karten. Kreditkarten-Betrug trotz Chip+PIN, c't 3/2016, S. 76.
[29] BGH Urt. v. 17.2.2011 - 3 StR 419/10, Rn. 12.
[30] BGH Urt. v. 27.1.2011 - 4 StR 338/10, Rn. 2, 8; BGH Beschl. v. 29.1.2014 - 1 StR 654/13; BGH Beschl. v. 11.8.2011 - 2 StR 91/11, Rn. 9; BGH Beschl. v. 14.09.2010 - 5 StR 336/10, Rn. 4.
[31] BGH Urt. v. 26.1.1982 - 4 StR 631/81.
[32] BGH Urt. v. 12.8.1997 - 1 StR 234/97, Rn. 8 bis 10.

Webshops für den BtM-Handel, Absatzhilfe bei der Treuhand in Carding-Boards, Aufforderung zu Straftaten), und andererseits dann, wenn sie gezielt für die Begehung von Straftaten unter Nutzung ihrer Dienste werben (psychische Beihilfe[33]).

Bei zunehmender Automatisierung der maliziösen Einsätze verlagert sich die tatherrschaftliche Beteiligung immer stärker auf den Zulieferer. Weder er selber noch der finale Betreiber von automatisierter Malware müssen dabei in den ausführenden Prozess eingreifen, weil er von einem Command & Control-Server gesteuert wird. Zulieferer (von infizierten Webseiten, *Landing Pages*) und Malware-Betreiben können sich auf die Pflege der Infrastruktur beschränken (Updates, Gewinnung neuer Zombies), ohne als Täter „händisch" in Erscheinung zur treten. Das ist wegen der Ransomware und der Onlinebanking-Malware schon länger bekannt gewesen, gilt aber verstärkt für die Botnetze, die dem *Crimeware-as-a-Service* dienen.

**Crimeware-as-a-Service**

Das Cybercrime hat nicht nur alle neu entstandenen Techniken und wirtschaftlichen Neuerungen besetzt, sondern auch eine zunehmende Tendenz zur geschäftsmäßigen Arbeitsteilung in der Weise, dass maßgebliche Zulieferungen und unterstützende Dienste, die nach besonderem Wissen oder einer stabilen technischen Infrastruktur verlangen, von Experten mietweise oder gegen ein einmaliges Entgelt zugeliefert oder gepflegt werden. Mit der Underground Economy ist ein krimineller Markt entstanden, auf dem nicht nur ausgespähte Daten und Informationen gehandelt werden, sondern zunehmend auch spezialisierte Dienste, Programme und Werkzeuge (BKA 2015):[34] *Bereitstellung von Botnetzen für verschiedenste kriminelle Aktivitäten, DoS-Attacken, Malware-Herstellung und Verteilung, Datendiebstahl, Verkauf/Angebot sensibler Daten, z.B. Zugangs- oder Zahlungsdaten, Vermittlung von Finanz- oder Warenagenten …, Kommunikationsplattformen zum Austausch von kriminellem Know-how, wie beispielsweise Underground Economy Foren, Anonymisierungs- und Hostingdienste zum Verschleiern der eigenen Identität* <und> *sog. Dropzones zum Ablegen illegal erlangter Informationen und/oder Waren*.

Exploit Kits

Danach ist ein Exploit-Kit (Malware-Baukasten) *ein Komplettpaket, das alles enthält, um Systeme zu infizieren und diese auszunutzen, ohne dass man dazu sonderlich viel Programmierkenntnis benötigt - wenn überhaupt welche*.[35] Das *WebAttacker Kit* ist bereits 2006 erschienen und wurde für 15 $ verkauft.[36] Sein Nachfolger (*mPack*) kostete bereits 5.000 bis 10.000 $; dafür wurden auch Support und monatliche Updates geboten.[37] Seit 2009 wurde das *Blackhole Exploit Kit* als erstes im Lizenzmodell vertrieben, bei dem sich die Kosten nach

[33] Grundlegend: BGH Urt. v. 24.10.2001 - 3 StR 237/01, S. 5.
[34] BKA, Cybercrime. Bundeslagebild 2014, 9.9.2015, S. 6.
[35] Steve Santorelli (Cymru Research NFP) nach Olivia von Westernhagen, Einbruch mit Komfort. Exploit-Kits als Basis moderner Cybercrime, c't 18/2015, S. 79.
[36] Symantec Report on Attack Kits and Malicious Websites, Symantec 2011, S. 11.
[37] Symantec Report on Attack Kits and Malicious Websites, Symantec 2011, S. 12.

der Nutzungsdauer richteten.[38] Mindestens 13 Personen waren an seiner Entwicklung und dem Vertrieb beteiligt, die 2013 in Russland festgenommen wurden.[39] Auf 2013 geht eine Studie von Samani und Paget zurück (McAfee),[40] die die grauen und schwarzen Märkte für den Handel mit Schwachstellen (Exploits; Cybercrime-as-a-Service, Research-as-a-Service), die Entwicklung und individuelle Anpassung von Malware (*Crimeware-as-a-Service*), für den Einsatz von Botnetzen für verteilte Angriffe und Spam sowie Bullet Proof-Dienste (Schurkenprovider; *Cybercrime Infrastructure-as-a-Service*) und schließlich für das Passwort-Cracking (Brute Force unter Einsatz des verteilten Rechnens in Botnetzen) und die Beschaffung von Informationen (*Hacking-as-a-Service*) betrachtet.[41] 2015 wurde berichtet, dass im Tor-Netz ein Erpressungs-Trojaner angeboten wird (Tox), der gegen eine Umsatzbeteiligung von 30 Prozent von den Entwicklern selbständig konfiguriert und an die interessierten Täter ausgeliefert wird:[42] *Nach einer kurzen Registrierung fragt der Dienst nur noch, wie viel Lösegeld der von Tox gekaufte Trojaner von seinen zukünftigen Opfern erpressen soll. Optional kann der angehende Online-Ganove noch eine persönliche Botschaft eingeben, die nach der Infektion angezeigt wird. Ist das kurze Formular ausgefüllt, generiert der Dienst den individuellen Schädling und der Download startet …*

Dadurch können Kriminelle *auch ohne eigene technische Kenntnisse und mit vergleichsweise geringem Aufwand Zugang zu hochentwickelten Werkzeugen erhalten, mit denen alle Formen von Cybercrimeangriffen ausgeführt werden können. Mittlerweile wird … häufig sogar Support für die Kunden/Bezieher der Leistungen des Cybercrime-as-a-Service angeboten. Dieser Support beinhaltet beispielsweise: Updates von Schadsoftware, Beratungsdienste, Anti-Erkennungsmechanismen, Hilfestellung bei technischen Problemen. Darüber hinaus werden als weitere Dienstleistungen auch die „Infection on Demand" (Verteilung von Schadsoftware auf Anforderung/Abruf) sowie Test-Portale angeboten, in denen Cyberkriminelle die Schadsoftware bezüglich ihrer Erkennungsraten von aktuellen Cyber-Sicherheitsprodukten testen können. Hierdurch besteht die Möglichkeit, durch Änderungen an der Schadsoftware deren Erfolgsaussichten für eine „Verteileroffensive" zu verbessern*.[43]

Modulare Cybercrime-Infrastrukturen

Während der Koordinator als operativer Projektmanager und „Abnehmer" von kriminellen Zulieferungen tätig wird, handelt es sich bei den Anbietern von „Crimeware-as-a-Service" um spezialisierte Zulieferer, die mit hohem fachlichem

[38] Jürgen Schmidt, Trojaner aus dem Baukasten. Die neuen Tricks der Internet-Gauner, c't 20/2012, S. 102.
[39] Russische Behörde eröffnet Strafverfahren gegen Entwickler des Blackhole-Exploit-Kit, Heise Security 9.12.2013.
[40] Raj Samani, François Paget, Cybercrime Exposed. Cybercrime-as-a-Service, McAfee 28.6.2013.
[41] Charles McFarland, François Paget, Raj Samani, Das heimliche Geschäft mit Daten. Der Markt für gestohlene digitale Informationen, McAfee 20.10.2015.
[42] Ronald Eikenberg, Online-Dienst erstellt maßgeschneiderte Krypto-Trojaner, Heise Security 27.5.2015.
[43] BKA, Cybercrime. Bundeslagebild 2014, 9.9.2015, S. 6.

Wissen schwierige „Halbfertigprodukte“ anbieten oder – um im geschäftsmäßigen Jargon zu bleiben – das Outsourcing infrastruktureller Dienste liefern. Neben den mietbaren Botnetzen und ihren klassischen Diensten wie DDoS, Spam-Versand, anonyme Netzzugänge (Proxy, Socks) und gebündelte Rechenleistung (Brute Force, Mining von BitCoins) sowie den Bullet Proof-Diensten sind jetzt auch Botnetze für das *Affiliate* verfügbar, also dem Einsatz von Malware in bereits kompromittierten Zombies.

In einer BKA-Studie aus 2015 heißt es dazu:[44] *Die Organisationsstruktur, die "Crime as a Service" (CaaS) möglich macht, beschreibt der IT-Sicherheitsdienstleister Fortinet (2013) wie folgt: Wie in jedem legalen Unternehmen setzt die "Chefetage" bzw. die Geschäftsführung ("Executive Suite") das Geschäftsmodell und die Infrastruktur auf. Sie trifft die wesentlichen Unternehmensentscheidungen, beaufsichtigt das operative Geschäft und stellt sicher, dass alles möglichst reibungslos funktioniert. Die Zusammenarbeit mit Partnern sowie strategische Planung bspw. hinsichtlich der Ausweitung des Geschäfts gehört ebenfalls zu ihren Aufgaben. Aufgabe des mittleren Managements ist es, so viele Rechner wie möglich zu infizieren, was diese Kräfte entweder selber erledigen oder mittels Personalvermittler ("recruiter") angeworbener Mitarbeiter, dem Fußvolk ("Infantry"). Dieses steht am Ende der Befehlskette und ist für die Umsetzung der Angriffe verantwortlich. Häufig durch Anzeigen angeworbene Geldkuriere ("money mules") stellen abschließend das Waschen der kriminellen Gewinne sicher. Die Geldbewegungen erfolgen regelmäßig durch anonyme Transferdienste, wie sie bspw. durch Western Union, Liberty Reserve, U Kash oder WebMoney angeboten werden. Speziell zur Anwerbung von Kräften werden Web-Portale eingerichtet. Viele dieser Portale kommen aus Russland ("Partnerkas") und sind nur auf Einladung zugänglich. Es gibt allerdings auch offene Portale. Um das Fußvolk mit den richtigen Werkzeugen auszustatten, kümmert sich das mittlere Management um die Entwicklung der Werkzeuge zur Infektion von Systemen. Diese können bspw. gefälschte Antivirenprogramme, Erpressungsprogramme ("ransomware") oder auch Botnets umfassen*.

Die Terminologie ist noch unklar, unstrukturiert und geprägt von der Vielfalt, die für das IT-Management, die Sicherheitsunternehmen und die Cybercrime-Szene typisch ist. Ungeachtet der im Detail sinnvollen Unterscheidung, die McAfee vorgeschlagen hat,[45] müssen klare Begriffe eingeführt werden, die eine Gruppe von Phänomenen umfassen und beschreiben. Mir erscheint es deshalb angebracht, zwischen den Zulieferungen zum modularen Cybercrime als Oberbegriff und den modularen Infrastrukturdiensten zu unterscheiden, die dem Outsourcing vergleichbar sind.

Danach handelt es sich um **modulare Zulieferungen** bei den Angeboten von Exploit-Händlern, von Root Kits, von abgegriffenen Daten, von einzelnen Diensten aus einem Botnetz (DDoS, Brute Force, BitCoin-Mining, Spam, Socks) und den Infrastrukturen von Bullet Proof-Diensten. Sie erfordern vom

---

[44] Jörg Bässmann, Täter im Bereich Cybercrime, BKA 4.12.2015, S. 46 f.
[45] Siehe oben: Raj Samani, François Paget, Cybercrime Exposed. Cybercrime-as-a-Service, McAfee 28.6.2013.

„Einkäufer“ am Schluss eine kriminelle Tatplanung und –ausführung, mithin kriminelles Know How und Tatbereitschaft. Die **Lieferanten der Crimeware-as-a-Service** sind ein Teil davon, entlasten den zahlenden Täter jedoch von mühseligen Vorbereitungen und der Tatausführung selber. Dabei ist es im Ergebnis gleichgültig, ob sie Zombies zum Affiliate bereit stellen, Finanzagenten für die Beutesicherung oder spezialisierte Malware für das automatische Phishing, Ransomware oder einfach nur geschaffene Backdoors zum Ausspähen von Daten. Sie liefern spezialisierte Dienstleistungen und lassen sich dafür bezahlen.

Im Hinblick auf ihre Tatnähe oder –ferne muss die Beteiligung der Lieferanten am Ausführungsdelikt differenziert betrachtet werden. Die Werbung von Finanzagenten, deren Kontaktdaten an die ausführenden Täter verkauft werden, die Verschaffung von Backdoors oder von besonderem Equipment erfolgt im Schaubild (oben) noch auf der Stufe **d** und wird grundsätzlich noch als Beihilfe bewertet werden müssen. Die Einrichtung und Bereitstellung eines C&C ist bereits so spezialisiert, dass ohne diesem Dienst die spätere Tatausführung ausgeschlossen ist, so dass der Zulieferer und der Ausführungstäter bereits in Mittäterschaft handeln können. Das gilt gleichermaßen für das Affiliate, bei dem der Zulieferer einen Zombie beschafft, die (weitere) Malware vom Ausführungstäter installiert und dieser dann die produktive Malware betreibt. Je weniger der Ausführungstäter selber an der Tatverwirklichung teilnimmt, desto stärker wird die täterschaftliche Rolle des Zulieferers beim Betrieb der produktiven Malware. Danach ist es durchaus möglich, dass der Kunde schließlich nur noch als Hintermann durch den Zulieferer handelt (§ 25 Abs. 1 Alt. 2) oder zum schlichten Anstifter wird (§ 26), wenn er die Tatherrschaft ganz aufgibt.

### Die RIG-Crew leistet Affiliate

In 2015 widmete sich schließlich Olivia von Westerhagen diesem kriminellen Geschäftsmodell unter besonderer Betrachtung der Malwaresteuerung und der RIG-Crew.[46] Das Besondere an dieser Form der Crimeware-as-a-Service ist, dass die gesamte Infrastruktur für die Verbreitung von Malware von dem Anbieter gestellt, betrieben und gepflegt wird und der Mieter nur die Ziele der produktiven Malware bestimmt (produktive Wirkweise, regionale Ausrichtung) und diese zuliefert. Die Miete für die Dienste von RIG soll zwischen 30 $ je Tag und 500 $ pro Monat betragen. Anfang 2015 soll die RIG-Crew etwa 360 Direktkunden und mindestens zwei große Reseller gehabt haben, die über etwa 250 weitere Kunden verfügt haben sollen.[47] Das von Olivia von Westernhagen vorgestellte RIG-Modell zeigt beispielhaft die Funktionsweise der aktuellen Verbreitung von Malware mit einer Infektionsquote von bis zu 70 Prozent;[48] 10 bis 25 Prozent sollen die garantierten Infektionsraten sein.

---

[46] Olivia von Westerhagen, Einbrecher zu vermieten. Ein Blick ins Innenleben des RIG-Exploit Kits, c't 18/2015, S. 84.
[47] Olivia von Westernhagen, Einbruch mit Komfort …, c't 18/2015, S. 82.
[48] Olivia von Westerhagen, Einbrecher zu vermieten …, c't 18/2015, S. 84.

Die RIG-Infrastruktur im Überblick

Die RIG-Crew lässt sich nicht gerne in die Karten schauen und trennt die verschiedenen Instanzen, die für die Verbreitung von Malware benötigt werden.[49] Zunächst muss nämlich der Anwender auf eine *Sprungseite* gelockt werden, von der aus er zu einer *Landing-Page* gebracht wird (präparierte Webseite). Erst hier findet die Einflussnahme des Exploit-Kit-Servers (Command & Control Server), der zunächst das System des Anwenders wegen seiner technischen Daten und Besonderheiten ausspäht (Betriebssystem, Anwenderprogramme, Browsertyp, aktive Applikationen und Stand der Updates). Aufgrund dieser Daten liefert der Exploit-Kit-Server die passenden und Erfolg versprechenden Exploits zu, die zunächst nur die Aufgabe haben, die Sicherheitsvorkehrungen des Anwenders auszuhebeln (Basis-Malware). Die Sprungseiten und die Landing-Pages wechseln ständig und in kurzen Abständen, damit der Standort und die Adresse des Exploit-Kit-Servers unentdeckt bleiben. Er birgt das wertvollste "Kapital" des Betreibers: Bisher unbekannte Schwachstellen (Zero-Day-Exploits) werden auf dem Schwarzmarkt für fünf- bis sechsstellige Beträge angeboten und der Bestand im Exploit-Kit-Server muss ständig gepflegt und aufgerüstet werden.[50] Das strategische Konzept für die Landing-Pages erinnert etwas an die in Botnetzen eingesetzten Fluxserver,[51] wobei es sich jedoch um leistungsstarke gekaperte Zombies handelt, die die Steuerungs- und Verwaltungsaufgaben des Command & Control-Servers tarnen.

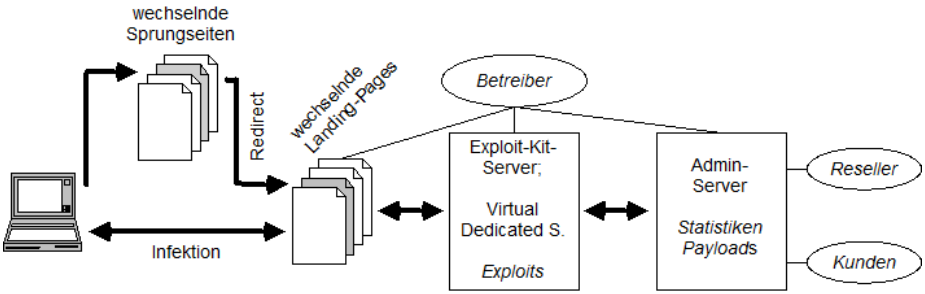


**Abb. 2: RIG-Infrastruktur**

Neben dem Exploit-Kit-Server, der sicher versteckt ist, stellt der Betreiber seinen Kunden den Admin-Server zur Verfügung. Auf ihm werden zunächst die

[49] Die folgende Grafik fasst die beiden Darstellungen aus der c't zusammen: Olivia von Westernhagen, Einbruch mit Komfort …, c't 18/2015, S. 79; dies., Einbrecher zu vermieten …, c't 18/2015, S. 85. Das Exploit-Kit **Angler** soll über eine ganz ähnliche Infrastruktur verfügen: Daniel AJ Sokolov, Exploit-Kit Angler macht Millionen mit Erpressungs-Trojanern, Heise Security 7.10.2015.
[50] Uli Ries, Digitaler Waffenhandel. Das geheime Geschäft mit Zero-Day-Exploits, c't 18/2015, S. 87.
[51] Jürgen Schmidt, Hydra der Moderne. Die neuen Tricks der Spammer und Phisher, c't 18/2007, S. 76.

Payloads bereitgestellt,[52] die den von der Basis-Malware infizierten Zombie nach dem erfolgreichen Einnisten der Basis-Malware anweisen, eine bestimmte produktive Malware zu laden. Erst dann ist die Installation der Malware abgeschlossen. Der Erfolg der Angriffe, die Anzahl der gekaperten Rechner und ihr Betriebszustand werden auf dem Admin-Server in Form von Statistiken angezeigt. Das Geschäftsmodell ist offen für das Affiliate, also die Vermietung gekaperter Rechner zum Nachladen weiterer Malware, und für Reseller (Wiederverkäufer), die ihren Bestand an Zombies an andere Kunden weitervermieten.

Sprungseiten und Weiterleitungen

Die Sprungseiten sind dazu da, den Anwender zunächst zu einem Angebot zu führen, das ihm interessant und lohnend erscheint. Verbreitet sind inzwischen bezahlte Werbeanzeigen auf vielbesuchten Internetseiten (*Malvertising*). Für diesen Einstieg können auch andere Methoden verwendet werden: Eingebettete Links in E-Mails, automatische Routinen in solchen Nachrichten und zum Beispiel Anlagen zu E-Mails, die selbständig den Kontakt zu Landing-Pages aufnehmen. Die üblichen Methoden sind gemietete Werbeeinblendungen in besucherstarken Angeboten (häufig in Form eines iFrames, der eine Weiterleitung bewirkt), in Suchmaschinenausgaben, optimierte Webseiten, die sich gegenseitig referenzieren und dadurch Besucherinteresse vorgaukeln, die Einrichtung von Vertipperseiten, die einen ähnlichen DNS-Namen wie die von bekannten Webangeboten haben, in den Präsentationen sozialer Netze und immer seltener auf gehackten Webseiten. Der Profit, den die produktive Malware schließlich verspricht, macht auch Investitionen sinnvoll, um Werbeplatz zu mieten,[53] eine spezialisierte Werbeagentur oder TrafficHolder für die Kontaktaufnahmen zu beauftragen. Bislang unbekannt sind jedenfalls Formen von Malware, die sich an Netzknoten einnisten und ihrerseits Verbindungsanfragen umleiten.[54] Wichtig ist der ständige Wechsel der Standorte für Sprungseiten und Landing-Pages, um den Standort des Exploit-Kit-Servers zu verschleiern.

Die *TrafficHolder* liefern - häufig garantierte - Besucherzahlen. Zwischen ihnen und stark frequentierten Webseiten gibt es Absprachen (Verträge), so dass die Partner den URL zu ihnen bereitwillig setzen und dafür (nach der Menge der zugeleiteten Anfragen) bezahlt werden. Die Weiterleitung erfolgt unbemerkt im Hintergrund. 10.000 solcher "Entführungen" kosten 30 US-$, wie die c't gemeldet hat.[55] Von dem TrafficHolder bekommt er gleichzeitig eine individuelle Referenznummer zugeteilt, die dem URL angefügt wird und die zur Abrechnung

---

[52] Bei den *Payloads* (auch *Downloader*) handelt es sich meistens nur um Kommandostrings, die den Browser zum Download weiterer Programmteile veranlassen.

[53] Das scheint Anfang 2014 Yahoo zum Verhängnis geworden zu sein, wobei über Werbeeinblendungen Malware verteilt worden sein soll: Yahoo als Virenschleuder: Yahoo.com griff europäische Besucher an, Heise online 6.1.2014.

[54] Solche - zunächst futuristisch anmutenden - Szenarien sind angesichts der Leistungsfähigkeit der Onlinebanking-Malware weder technisch noch gedanklich auszuschließen und praktisch bekannt: Jo Bager, Dušan Živadinovic, Unter Beobachtung, c't 5/2014, S. 77. Malware in der Infrastruktur von Internetknoten oder von Carriern könnte nicht nur Verbindungsabfragen blockieren oder umleiten, sondern auch Inhaltsdaten abgreifen.

[55] Holger Bleich, Geldmaschine Streaming-Abmahnung. Anwaltsschreiben aus Regensburg schüchtern tausende Internet-Nutzer ein, c't 2/2014, S. 18.

zwischen dem TrafficHolder und dem Auftraggeber dient (Betreiber der Webseite, zu der der Besucher "entführt" wird). Als "Lockvögel" kommen vor allem pornografische, und andere beliebte, aber finanziell erfolglose Angebote in Betracht (Kochrezepte, Schularbeitenhilfe, Arbeitssuche und andere). Auch andere Möglichkeiten sind eröffnet: Man hackt Referenzen, zu denen Suchmaschinen nebenbei verweisen (Werbungen), und platziert dort den URL zum TrafficHolder (zum Beispiel durch iFrames), man hostet massenhaft Seiten (Pharming), referenziert sie gegenseitig, damit sie einen hohen Rang in den Suchmaschinen erlangen, und hofft darauf, Interessenten anzulocken, oder man manipuliert DNS-Server (Poisoning), die von sich aus die Abrufe umleiten. Der bekannteste Fall war der DNS-Changer.[56] Dazu ermöglichen sowohl das Internet-Protokoll wie auch die Skriptsprache HTML automatische Weiterschaltungen. Wenn man den Besucher erst einmal abgefangen hat, dann kann man ihn auch beliebig weiterleiten. Er kann dann nur noch darauf hoffen, dass seine Firewall und sein Virenscanner die böswilligen Angriffe abblocken können.

Die technischen Voraussetzungen für eine Weiterleitung von der Sprungseite zu einer Landing-Page sind in der Skriptsprache HTML, in den üblichen Steuerungsroutinen für Webseiten und schließlich in der Servertechnik angelegt. Einfache Beispiele sind die in einer Webseite eingebundenen Umleitungen (*Redirects*) mit einem *CGI-Modul*[57] oder vermittels automatischer *Forwardings*, die als Metadatum im Kopf der präsentierten Seite eingebunden sind.[58] Aufwändiger sind andere Methoden: Mit einem Domain Name Server (oder einer manipulierten Hosts-Tabelle; *Poisoning*) lassen sich nicht nur DNS-Adressen in nummerische Internetadressen auflösen, sondern auch beliebige Adressen hinterlegen, die Betreiber von Autonomen Systemen können auf der Grundlage des Border Gateway Protokolls Adressenanfragen - jedenfalls vorübergehend - zu sich umleiten und Zugangsprovider beherrschen das Routing und können jeden zu einer von ihnen bestimmten Adresse umleiten.

Landing-Pages, Exploit-Kit-Server und Payload

Die Landing-Pages sind das Einfallstor für die Basis-Malware. Sie sind in aller Regel "unsichtbar" in dem Sinne, dass sie keine Grafiken oder Texte vermitteln, sondern im Rahmen des Handshakes die technischen, freiwillig offenbarten Daten des Anwenders erheben: Betriebssystem, Anwenderprogramme, Laufzeitumgebungen, Browsertyp - jeweils mit Versions- und Stand des Updates, Ländereinstellungen, Sprache und IP-Adresse. Mit diesen Daten lässt sich der Anwender lokalisieren und kann der Exploit-Kit-Server die Exploits auswählen und zuliefern, die den größten Erfolg versprechen. Damit befinden wir uns im Stadium der Anlieferung und Installation, das vom Exploit-Kit-Server gesteuert wird. Sobald die Sicherheitsvorrichtungen des Anwenders ausgehebelt wurden, fordert die Landing-Page den *Payload* vom Admin-Server an. Den Payload steuert in aller Regel der Kunde bei, der auch die weitere Betreuung der *produktiven Malware* leisten muss.

---

[56] FBI nimmt DNS Changer-Botnetz hoch, c't 25/2011, S. 41.
[57] SelfHTML, Automatische Umleitungen (Redirects) mit dem CGI-Modul.
[58] SelfHTML, Automatische Weiterleitung zu anderer Adresse (Forwarding).

Die Landing-Pages und die beiden Server werden exklusiv vom Betreiber beherrscht, dem es besonders darauf ankommt, dass der Exploit-Kit-Server, von denen er im Interesse der Ausfallsicherheit (Redundanz) meistens mehrere im Einsatz hat, nicht identifiziert, ausgespäht oder gar manipuliert werden kann. Mit der Zulieferung des Payloads beginnt die Installation der produktiven Malware, wobei die schädliche Routine in aller Regel verschlüsselte Passagen enthält, die von den gängigen Virenscannern nicht erkannt werden können. Mit Hilfe von Root Kits wird die Malware möglichst "tief" im Zombie verankert und getarnt (*Stealth*). Der Installationsvorgang ist damit abgeschlossen und der neue Zombie in der Datenbank des Admin-Servers als Neuzugang vermerkt. Seinem Einsatz steht dann nichts mehr im Wege.

Admin-Server

An der Installation der Malware ist der Admin-Server nur insoweit beteiligt, dass er den vom Kunden oder vom Reseller beauftragten Payload zuliefert. Nach der Installation können die "neuen Zombies" eingesetzt werden. Der Kunde muss sich weder um die Verbreitung, noch um die Installation der gewünschten Malware kümmern. Auch die Aktualisierung der zugelieferten, produktiven Malware und ihre Tarnung kann der Betreiber besorgen.

Anhand der Statistiken auf dem Admin-Server kann der Kunde "seinen" Bestand beobachten und zum Beispiel feststellen, ob die eingesetzte Malware entdeckt und neutralisiert wurde. In diesen Fällen sorgt der Betreiber auch für den Umzug auf andere Zombies.

**Fazit**

Neben der Vielzahl einzeln handelnder Täter, die das Hacking, Carding und Cashing betreiben oder sich innerhalb eines tatgeneigten Schwarms an einzelnen kriminellen Projekten beteiligen, sind seit mehr als 10 Jahren auch Infrastrukturdienste entstanden, die das Cybercrime durch technische Unterstützung, die Zulieferung von Daten, Schwachstellen und Tarnvorrichtungen, von Beutehelfern und schließlich von Komplettpaketen bieten, die die einfache Tatausführung ohne besonderes Fachwissen und ohne großem Aufwand ermöglichen. Es handelt sich um vereinzelte Dienste und um keine Massenerscheinungen, die wir Dank allgemein gehaltener Berichte des BKA und am Einzelfall orientierter Reportagen von Sicherheitsunternehmen sowie aus der Fachpresse nachvollziehen können. Die „Analyse und Auswertung“ der Strukturen in der Underground Economy steht noch am Anfang, ist mangels systematischer Instrumente und vergleichender Untersuchungen fehlerbehaftet und kann deshalb zu erheblichen Fehlschlüssen führen.

In diesem Sinne trägt dieser Beitrag zur Bestandsaufnahme bei und bewegt er sich auf der Ebene, auf der Thesen entstehen, aber noch keine gesicherten Erkenntnisse zu erwarten sind. Er beruht auf journalistischen Berichten, auf einzelnen Berichten von Fachleuten in der Informationstechnik, auf den Analysen des BKA und schließlich aus einigen selbst gemachten Erfahrungen. Daraus entsteht allmählich ein Gesamtbild, das wiederkehrende Eigenschaften erkennen lässt. Spamming, Malware und Botnetze lassen sich ebenso wenig als Tatsache leugnen wie Finanzagenten, digitale Wechselstuben, Bullet Proof-

Dienste oder die Boards, in denen kriminelles Wissen und Dienste gehandelt werden. Manche analytischen Bewertungen brauchen auch Zeit und etliche Erscheinungsformen des Cybercrime werden erst viele Jahre nach ihrem Entstehen erkannt.[59] Bislang besteht jedenfalls kein Anlass, vor dem Cybercrime zu kapitulieren, weil das geltende materielle Strafrecht viele hilfreiche Instrumente bietet, um es zu bekämpfen.

[59] Die Poseidon-Gruppe war bereits 11 Jahre lang tätig, bis über sie Anfang 2016 berichtet wurde: Dennis Schirrmacher, Hacker-Gruppe zwingt Opfern "Support" auf, Heise Security 11.2.2016.