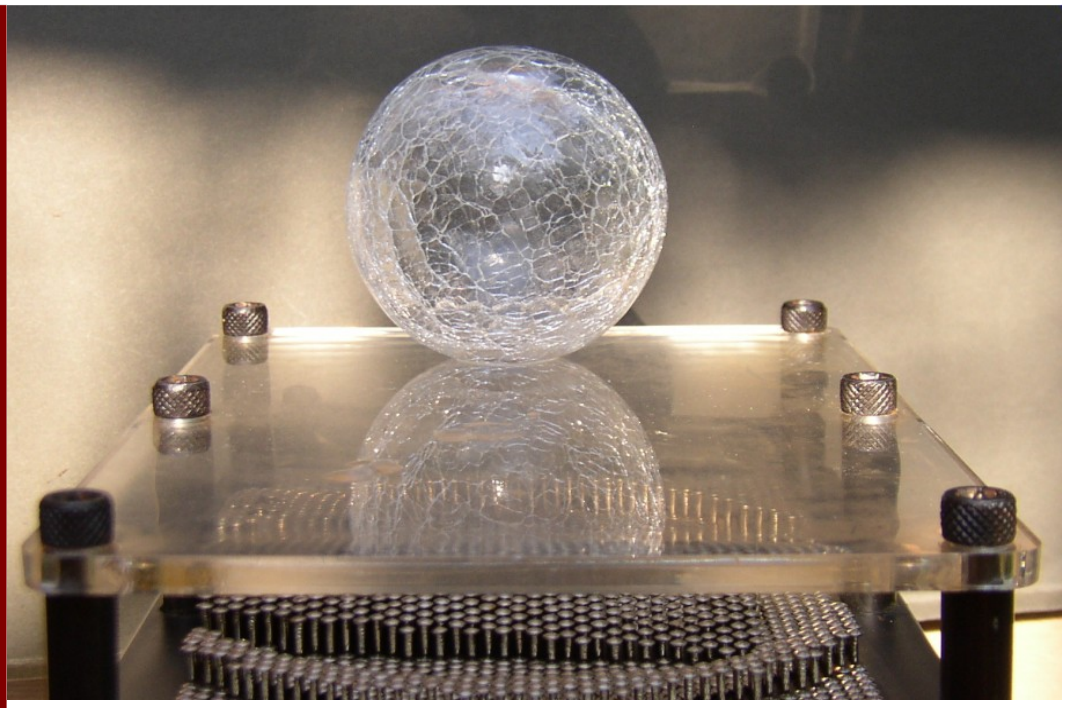


Dieter Kochheim

Über das Verschwinden der Cybercrime

Automatisierte Malware

April 2012

Cyberfahnder 2012

Die Texte im Cyberfahnder werden immer länger und lassen sich immer schwerer am Bildschirm lesen. Zwei jüngere Texte werden hier deshalb im druckfreundlichem PDF-Format präsentiert.

Thema:	**Automatisierte Malware**
Autor:	Dieter Kochheim
Version:	#1.00
Stand:	30.04.2012
Cover, Foto, Grafiken:	© Cyberfahnder, 2012
Impressum:	▸ cyberfahnder.de

Cybercrime - gibt es eigentlich nicht

Essay, 09.04.201

Operation Payback von 2010, zuvor Stuxnet und Night Dragon von 2011. Solche "großen" Meldungen gibt es gegenwärtig nicht [1]. Es scheint ruhig geworden zu sein um die Cybercrime. Gibt es sie nicht mehr? Wo bleiben die vorausgesagten Angriffe im Zusammenhang mit der Industriespionage?

Die Quartalsberichte von McAfee und anderen Sicherheitsunternehmen zeichnen ein anderes Bild. Botnetze und die Verbreitung von Malware schreiten weiter voran und statt Phishing und Homebanking-Trojaner geraten eher erpresserische Infektionen in das Licht der Öffentlichkeit (Bundespolizei, GEMA). Besonders im Trend sind Angriffe gegen die mobile Telefonie und das Abfangen von TAN beim Homebanking. Das Spamming geht zurück, dafür werden die Werbenachrichten gezielter eingesetzt.

Die wichtigsten cyberkriminellen Geschäftsfelder sind immer noch:

- Das Herstellen und Verbreiten von **Malware** zum Ausforschen der infizierten Rechner, ihre Übernahme als Zombies für Botnetze, für erpresserische Angriffe und zur Manipulation des Homebankings.
- Das **Hacking** zur Erlangung von Finanzdaten.
- Der übliche und allgegenwärtige **Betrug** in Tauschbörsen und Webshops.
- Der **Kontoeröffnungs-** und **Warenbetrug**.

Underground Economy

Ein Blick hinter die Kulissen offenbart ein reges Treiben. hacker.yakuza112.org zeigt allein 26 deutschsprachige Boards, die sich fröhlichen Themen wie "carders", "hacking" oder "virus" widmen. Carders dürfte etwa 14.000 Mitglieder und die Russian-Elite etwa 8.000 Mitglieder haben. Solche Boards sind Handelsbörsen für Informationen und kriminelle Dienste. Dank den Happy Ninyas und anderen Zeitgenossen, die solche (gegnerischen) Boards gerne 'mal hacken und als Dump der Öffentlichkeit zur Verfügung stellen, wissen wir mehr über das Innenleben. In aller Regel stehen einige thematisch beschriebene Foren zur Verfügung (Threats), die die wichtigsten Themen wie Carding, Skimming, Malware, Botnetze und Paketstationen abdecken. Sie werden nicht nur thematisiert, sondern in den Foren werden Tipps ausgetauscht und vor allem gehandelt. Versierte Teilnehmer stellen Tutorials über Kontoeröffnungen per Internet, Hacking-Tools oder die Erstellung falscher Ausweise zur Verfügung und beweisen damit ihren Gemeinsinn.

Die Administratoren und Moderatoren verdienen damit Geld. Zunächst verlangen sie Mitgliedsgebühren in erschwinglicher Höhe. Verkaufslizenzen für bestimmte Produkte oder Gifte kosten extra in monatlich zwei- bis dreistelliger Höhe. Am meisten verdienen sie aber an der Treuhand.

Gesicherte Bezahlvorgänge sind nötig, weil hier keiner dem anderen traut. Käufer und Verkäufer zocken gleichermaßen ab, wenn sich ihnen die Gelegenheit dazu bietet. Deshalb müssen alle Geschäfte unter Einschaltung eines vertrauenswürdigen Treuhänders abgewickelt werden, der zunächst den Kaufpreis in Empfang nimmt und das dem Verkäufer mitteilt. Wenn der Käufer den Empfang der Ware bestätigt hat, kehrt der Treuhändern den Kaufpreis nach Abzug seiner gerechten Gebühr an den Verkäufer aus. Der Treuhänder macht auch seine eigenen Geschäfte und vergisst gelegentlich auch die Zahlung an den Verkäufer.

---

1 Kurzkommentar zu diesem Beitrag:
▸ Felix **Knoke**, Netzwelt-Ticker: Was am Dienstag sonst noch in der Netzwelt wichtig war, Spiegel online 10.04.2012

Carding ist nicht etwa nur der Handel mit gestohlenen Zahlungsdienstdaten, um Bankkonten abzuräumen, sondern mit allem, was mit Betrug, Urkundenfälschung und gestohlenen Identitäten zu tun hat. Die Boards vermitteln aber auch die Grundversorgung mit Rauschgift, Medikamenten und Waffen.

Zu den benötigten Werkzeugen gehören sichere Bankkonten. Finanzagenten sind überholt. Besser sind auf falschen Personalien oder von eingeflogenen Ausländern eröffnete Bankkonten, die sich zum Durchlauf mehrerer Tausend Euro eignen. Ein gefälschter Mietvertrag ist schnell gemacht, eine ausländische Identitätskarte auch und eine falsche Gehaltsbescheinigung schon lange.

Auch PostIdent-Bescheinigungen lassen sich einfach fälschen. Um die Bankkorrespondenz zu erhalten, bedarf es nur eines ungebrauchten Briefkastens in einem Mehrfamilienhaus oder eines selbst installierten Briefkastens in einem Abbruchhaus. Der Warenbetrug ist schwieriger. Für ihn muss man seinen falschen Ausweis in einer Postfiliale präsentieren oder eine Packstation nutzen. Unter einem gehackten Zugangskonto oder unter einer falschen Identität, natürlich.

Hosting

Für ein Carding-Board braucht man keinen sicheren Hafen bei einem Schurkenprovider. Alle bekannten Hostprovider bieten für monatlich 20 oder 30 Euro dedizierte Server an, die von dem Kunden administriert werden. Das Board mit den Mitgliederdaten und ihren Beiträgen passt auf eine CD. Auf den Server werden ein Content Management System - CMS - installiert und die Daten geladen.

Boards sind geschlossene Veranstaltungen. Betrogene Kunden, die Rechtsanwälte oder Strafverfolger auf den Hostprovider hetzen, gibt es nicht. Insoweit ist die Carding-Szene fatalistisch. Man handelt unter phantasievollen Namen, betrügt sich gegenseitig und sucht sich ein neues Opfer, wenn man selbst einem anderen auf den Leim gegangen ist. Die schwersten Sanktionen, die man befürchten muss, sind Beschimpfungen (Flames) und der Ausschluss. Ein neuer Name verschafft ein neues Leben und damit wieder einen Zutritt.

Wird es dem Betreiber zu heiß, wechselt er den Hostprovider und macht das Board woanders auf. Hostspeicher ist billig und die Hostprovider sind willig. Sie wollen auch gar nicht wissen, was ihre Kunden treiben. Bleibt das Geld aus oder gibt es Ärger, dann wird der Server platt gemacht und dem nächsten Kunden angeboten. Nach ein paar Postings kommen die Board-Kunden ganz schnell wieder.

Nur um die Domainadresse muss man sich kümmern und einen leistungsfähigen Verwalter finden. carders.cc nutzt dazu das australische Privacyprotect.org, das seinerseits von suspended-domain.com unter directi.com betriebene DNS-Server in Mumbai nutzt. Das ist eine lebhafte Hafenstadt mit 12,5 Mio. Bewohnern im Bundesstaat Maharashtra an der Westküste Indiens und bestens mit dem Internet verbunden.

Ich vermute, dass alle drei Betreiber nur wenige Bestandsdatenfelder vorrätig halten:

Domainname	carders.cc
Zugangscode	●●●●●●●●●
IP-Adresse	●●●.●●●.●●●.●●●
Kontakt	💣@💣.ru
Kunde hat gezahlt	✓
… bis	●●.●●.●●●●

Das ist gelebte Datensparsamkeit nach Herzenslust unserer hiesigen, mehr oder weniger amtlichen Datenschutztrolle.

Einen Schurkenprovider mit sicherem Hosting braucht nur, wer sich an das öffentliche Publikum wendet, um mit Lockangeboten zu betrügen, urheberrechtskritische Multimedia- oder Programmdateien oder seine freie Mei-

nung über den Holocaust oder die Segnungen des Nationalsozialismus zu verbreiten.

Hostspeicher ist billig in Westeuropa und die Internet-Infrastruktur ist hier äußerst leistungsfähig. Der beschwerderesistente Provider aus Russland, Weissrussland oder der Ukraine hat nicht selten hier Hostspeicher für seine deutschen und westeuropäischen Kunden gemietet und zahlt zuverlässig. Das wiederum ist Globalisierung und eine klare Absage an die internationale Rechtshilfe in Strafsachen.

Beutesicherung

Finanzagenten gab's gestern. Heute richtet man Bankkonten unter falschen Personalien ein oder hackt sie. Die Phisher, die der verstorbene Kollege Thelen vor etlichen Jahren verfolgte, mussten noch eine eigene Bank in der Karabik aufmachen, um sich Zahlungskarten auszustellen und die Beute aus dem Geldautomaten an der nächsten Ecke zu holen.

Dank Kreditkarten auf Guthabenbasis aus Gribraltar kann man sich heute diesen Aufwand ersparen. Wechselstuben im alten Ostblock sind zwar teuer, wechseln aber zuverlässig Vouchers in Guthaben auf Kreditkarten um oder überweisen an ein PayPal-Konto. Auch die lästigen Edelmetallkonten (E-Gold u.a.) gibt es nicht mehr, weil sie vom FBI wegen Geldwäsche dicht gemacht wurden.

Lästig sind aber auch die karibischen Online-Kasinos. Sie verlangen tatsächlich, dass man wenigstens ein paar Runden verliert, bis sie das Spielkonto auflösen und den Saldo überweisen. Besser kann man die Beutesicherung bei größeren Beträgen aber nicht tarnen.

Für kleine Beträge gibt es die Vouchers von PaySafeCard oder ukash oder ein Netzwerk nach Hawala-Art. Während Vouchers nachverfolgt werden können, kennt die Hawala keine Buchführung über die Zahler und Zahlungsempfänger. Die Hawalare rechnen untereinander nur nach Volumen ab. Das kennen wir sonst auch vom Clearing beim Roaming und bei dem internationalen, bargeldlosen Zahlungsverkehr.

Cashing-Schäden

Wenn's um die Schäden geht, klagt die Finanzwirtschaft nicht lauthals. Sie bucht sie gegen die Gebühren und bemüht sich um die Begrenzung des Imageschadens.

Angesichts der Reife heutiger Malware kommt die Beute ganz automatisch zum Täter. Er richtet einen Command & Control-Server - C&C - ein und der bedient um sich herum einen Schutzwall von Fluxservern. Diese sind es, die einen Abschnitt eines Botnetzes steuern oder die Homebanking-Malware mit den nötigen Fake-Webseiten und den Informationen über die Zielkonten der Manipulationen versorgen. Der Täter muss nur dafür sorgen, dass die Malware verteilt wird, funktioniert und funktionstüchtig bleibt.

Dagegen sind die erpresserischen Formen der Malware grobschlächtig. Sie fallen mit ihren Vorwürfen ("Sie haben urheberrechtlich geschütztes Material verbreitet" oder Kinderpornographie oder überhaupt etwas anrüchiges getan) und mit ihren freundlichen Anleitungen auf, wo und wie man Vouchers bekommt. Dabei leben sie von einer besonderen Dreistigkeit und bei denen, die sich auf die Erpressung einlassen, darf man durchaus ein schlechtes Gewissen vermuten.

Warum regt sich keiner darüber auf?

Heutige Cybercrime ist ein Massenphänomen. Der einzelne Betroffene zahlt Lehrgelt oder sieht sich ertappt und zahlt Schweigegeld. Die Finanzwirtschaft klagt auch nicht medienwirksam. Ihr geht es nicht an die Substanz und klagen würde bedeuten, man habe seine Geschäftsprozesse nicht im Griff. In den USA sind dafür die Vorstände persönlich haftbar. Dann ist doch lieber eine Klimaanlage im Rechenzentrum ausgefallen anstatt dass ein Hackerangriff erfolgreich war.

gespenstige Ruhe

Die Instrumente der Cybercrime sind ausgefeilt wie nie zuvor und dennoch herrscht eine gespenstige Ruhe. Jedenfalls bleiben die großen Meldungen aus und Anonymous findet nur noch eine nebensächliche Beachtung.

Die Kinderporno- und die Cardingszene wurden von der Strafverfolgung in den letzten beiden Jahren verunsichert. Sie verbessern gerade ihre Abschottung. Der Identitätsdiebstahl äußert sich vor allem in Bankkonten unter Scheinidentitäten ohne Sicherheiten und die Finanzwirtschaft schweigt, solange sie keine richtigen Schmerzen hat. Der geprellte Privatmann ärgert sich und schickt allenfalls seinen Rechtsanwalt zur Akteneinsicht.

Die Underground Economy setzt Massen von Geld um und vieles davon versickert an den Zwischenstationen, bei den Helfern und Helfershelfern.

Sobald das wahre Ausmaß der Underground Economy bekannt würde, könnte jeder Schwarzarbeiter, Hartz IV-Betrüger und Steuersünder (im kleinen Maß) mit Inbrunst behaupten, er werde verfolgt (gehängt) und die wahren Vergeher könnten frei rumlaufen. Recht hätte er, so gesehen! Gegen die schleimigen Täter im Internet gibt es bislang nur wenige Verfahren und die Fanale sind rar.

Es gibt sie. Die raffiniert handelnden Abofallen-Täter in Göttingen haben Bewährungsstrafen bekommen und der wichtigste von ihnen, der die Finanzen verwaltet hat, war nur ein Gehilfe. Sonst wäre das vielleicht doch eine Bande gewesen.

In Wuppertal gab es einen Singvogel und die Strafverfolger konnten eine ganze Skimming-Struktur samt Hinterleute und Geldwäscher ausheben. Sie wurden ganz schwer rangenommen und zu Bewährungsstrafen verurteilt.

Hierzulande verfolgt man BtM-, Grundstoff- und Arzneimittelhändler im Internet, islamistische Aufrührer und Terroristen, aber keine Schurkenprovider. Man könnte sie auch hier finden, wenn man sie suchen würde. Man könnte auch Malware-Manufakturen und Operation-Groups für bestimmte kriminelle Aufgaen finden, wenn man sie suchen würde. Und man könnte auch Skimming-Truppen finden ...

der große Bang

... wird kommen, wenn die Schäden und die allgemeine Verunsicherung überhand nehmen. Ich vertraue der Strafverfolgung, dass sie sich langsam, aber nachhaltig in Bewegung setzen wird. Angst habe ich nur vor den Datenschutztrollen und den Politikern, die ihren Blick vor den Gefahren verschließen und jede Strafverfolgungsmaßnahme mit dem Makel versehen, dass immer nur Unschuldige generalverdächtigt und verfolgt werden.

Das freut die bedenkenlosen Cyberkriminellen, die jede Chance zum Beutemachen nutzen.

Erpressung mit Malware

Automatisierung beim Einsatz von Malware

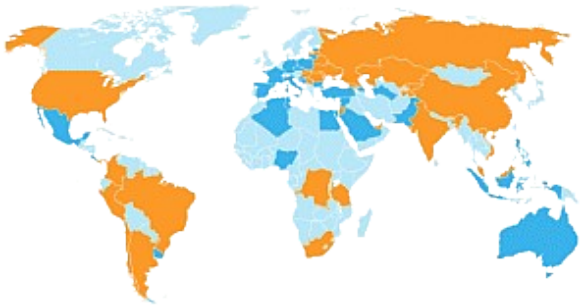
16.04.201

Heise meldete am 13.04.2012: *Die Antiviren-experten von Trend Micro haben einen Lösegeld-Trojaner entdeckt, der den Boot-Vorgang blockiert. Anders als der in Deutschland weit verbreitete BKA-Trojaner nistet er sich dazu im Master Boot Record (MBR) ein. Anschließend führt der Schädling einen Neustart durch und fordert den Nutzer auf, ein Lösegeld in Höhe von 920 Hrywnja (ukrainische Währung, umgerechnet rund 90 Euro) über den Zahlungsdienstleister QIWI an die Erpresser zu zahlen*. [2]

Das Zitat reizt zu einigen Erläuterungen und Spekulationen, zunächst zum Zahlungsverkehr und dann zu den technischen Fragen.

QIWI [3] ist ein russisches Handelsunternehmen, das von Mobiltelefonen über Tickets bis hin zu Versicherungen alles vertickert [4]. Sein Kerngeschäft scheint aber aus Zahlungsverkehrsgeschäften, also Bankgeschäfte im herkömmlichen Sinne, Zahlungskarten und Zahlungsdienste nach dem Vorbild von Western Union, MoneyGram sowie PaySafeCard und anderen zu bestehen. Es ist vor Allem im russisch-asiatischen Bereich sowie vereinzelt in Amerika und Südafrika verbreitet (orange). Filialen in Europa und anderenorts sind in Planung (blau).

Seit 2010 arbeitet das Unternehmen mit ukash zusammen [5] und daher ergibt sich auch eine beachtliche Zahl: QIWI verfügte vor zwei Jahren schon über 100.000 eigene Verkaufsstellen.



Ansonsten ist das Unternehmen in Westeuropa ziemlich unbekannt gewesen. Das ändert sich jetzt durch die Erpressungs-Malware. Jedenfalls die Täter scheinen auf die Integrität des Unternehmens zu vertrauen. Das nennt man dann eine gelungene und typisch russische Markteinführung.

Auf weitere Nachrichten darf man gespannt sein.

ungewöhnliche Angriffstiefe

Bei einer groben Betrachtung eines Computers und seiner Programmabläufe bildet das Basic Input-/Output-System - BIOS - gleichermaßen die Basis für alle Abläufe. Es ist auf jeder Platine fest verlötet, besteht aus einem Chip mit vielen verdrahteten Rechnerfunktionen und prüft und startet alle Hardware-Teile um sich herum. Ohne ihm wird kein Prozessor - also die eigentliche Rechenmaschine, kein Massenspeicher (Festplatte, Diskette, CD, USB-Stick), keine Tastatur, Grafik- oder Soundkarte erkannt und betriebsfähig gemacht. Das BIOS ist für alle Technik verantwortlich und startet schließlich das Betriebssystem.

Das BIOS steht aber nicht für sich allein, sondern hat in seinen heutigen Formen eigene programmierbare und veränderbare Speicher und Dateien, die ihm Informationen zuliefern. Sie fördern seine Anpassungsfähigkeit und machen es anfällig.

Bei einem Angriff mit Malware kommt es darauf an, in möglichst tiefe Ablauffunktionen

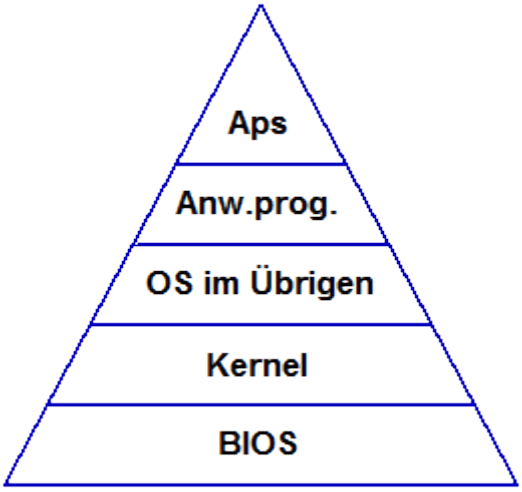
---

2 ▸ Malware blockiert Bootvorgang, Heise online 13.04.2012

3 Übersetzung von Google: ▸ QIWI weltweit.

4 Übersetzung von Google: ▸ Produkte und Dienstleistungen.

5 ▸ Partnerschaft mit QIWI: Ukash erschließt 100.000 Verkaufsstellen in Russland, ukash 01.04.2010



hinein zu kommen, weil sie im Betrieb die höchste Vertrauenswürdigkeit und Akzeptanz haben. Insoweit bildet das BIOS tatsächlich die höchste Instanz (und die Basis).

In den Anfangszeiten wurde noch klar zwischen dem Betriebssystem - Operating System - OS - und der Anwenderoberfläche unterschieden. So lieferte 1994 das Betriebssystem DOS (gemeint ist die Version 6.2) alle Grundfunktionen und dem Anwender einen dunklen Bildschirm, der ihm zur Eingabe von Kommandos aufforderte. Bunte Programme konnte er erst aufrufen, wenn er das richtige Kommando mit der Tastatur eingab.

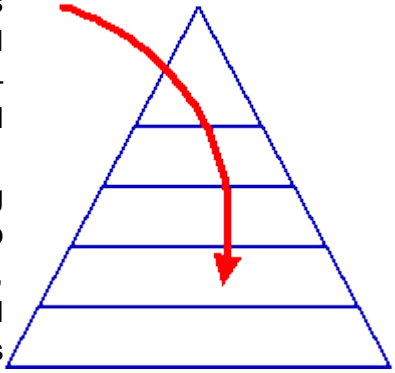
Im heutigen Sprachgebrauch würde man das klassische Betriebssystem den Kernel nennen. Das ist eine Vereinfachung, weil es viele Randunschärfen gibt. Dennoch ist die Aussage richtig: Der Kernel ist der Kern des Betriebssystems und das, was er zulässt, verbietet oder gestaltet, das lässt sich in allen höheren Programmabläufen nicht mehr verändern.

Aus der Sicht von 1994 ist das "OS im Übrigen" das frühe "Windows 3.11". Es brachte den Einstieg in die bunte Windows-Welt und kleine bunte Bildchen - Icons, die Kommandos und andere Steuerzeichen bis heute ersetzen. Eine solche Anwenderoberfläche führt die technischen Grundfunktionen und Standardprozesse zusammen und erleichtert die Bedienung ungemein.

Es ersetzt aber keine Anwenderprogramme und das sind ursprünglich Texteditoren (Word), Tabellenkalkulationsprogramme (Multiplan, Excel), Datenbanken (Access [na ja]) und andere Oberflächen (Grafikbearbeitung, Desktop Publishing [grafische Gestaltung für Flyer, Hefte u.a.], Sounds).

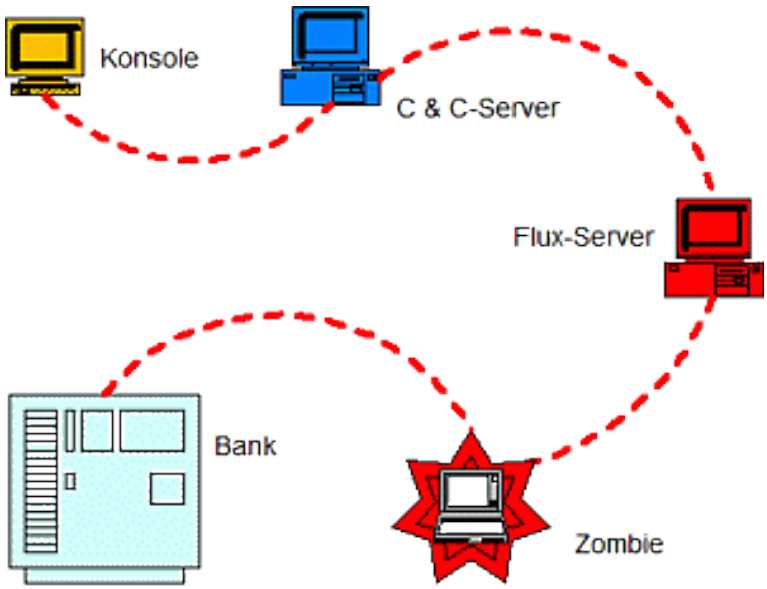
In dem Schaubild oben links werden auch die "Aps" genannt. Sie können nicht trennscharf von den Anwenderprogrammen abgegrenzt werden, weil sie teils als E-Mail- und Web-Browser vollwertige Anwenderprogramme sind. Sie enthalten oder verweisen auf selbständige Ablaufprogramme, die entweder im Hintergrund bleiben (Java, activeX) oder als Anzeigeumgebungen dienen (Acrobat Reader, Shockwave u.a.), die ihrerseits und unkontrolliert bis in das Betriebssystem und den Kernel eingreifen können.

Der neue Lösegeld-Trojaner setzt sich sogar im BIOS selber fest. Er verändert zwar nicht den Chip als solchen, sondern nur die ihm zuliefernden Konfigurationsdateien. Die Konsistenz des Kernels und des BIOS wird von den üblichen Virenscannern und Überwachungsprogrammen nachhaltig überwacht. Deshalb gilt eine Malware, die sich im Kernel einnisten kann, als Besonderheit. Ein Angriff auf das BIOS - jedenfalls auf seine Konfigurationsdateien - kann tatsächlich als etwas noch Besonderes angesehen werden. Der Schritt bis in das BIOS selbst ist Dank seiner "intelligenten" Funktionen (Programmierbarkeit) nicht mehr unmöglich.



Deshalb interessiert mich die Frage, wie weit die Automatisierung der Malware gehen kann, wie sie strafrechtlich zu betrachten ist und welche weiteren Konsequenzen sie aufwirft.

variable Malware



Bislang sind keine Studien veröffentlicht worden, die sich eingehend mit den Formen der Erpressungs-Malware und ihrer Funktionsweise beschäftigen. Die in Europa bekannt gewordenen Varianten des Bundespolizei-Trojaners waren an die nationalen Besonderheiten angepasst. Die deutsche Variante sprach sozusagen Deutsch und nutzte vor Allem die Bundespolizei, um der Schutzgeldforderung Nachdruck zu verschaffen. Dagegen war die spanische Variante in spanischer Sprache gehalten und sie bezog sich auf eine spanische Bundespolizei. Dasselbe gilt für die britische Variante, die natürlich englischsprachig war und sich auf die Metroplitan Police und später auf den Scotland Yard bezog [6].

Für diese Variabilität gibt es drei mögliche Erklärungen:

▷ Es wurden verschiedene Varianten mit nationalen Schwerpunkten verbreitet.

▷ Die Malware ist so komplex und so vollständig, dass sie mindestens drei Varianten mit sich führt. Welche zum Tragen kommt, richtet sich nach den Spracheinstellungen des angegriffen Geräts oder seiner IP-Adresse.

Mit Stuxnet ist eine solche "all-in-one"-Malware bekannt geworden, die sich über (USB-) Speichermedien verbreitete [7]. Sie ist aber nur für eine bestimmte Umgebung konstruiert worden, nämlich für die iranische Urananreicherungsanlage.

▷ Die Malware öffnet nur eine Backdoor, übermittelt an einen Command & Control-Server (Steuerungseinheit) die Umgebungsvariablen und bekommt von dem dann die nötigen Updates und Anweisungen.

Ich vermute, dass die dritte Variante zutrifft. Sie würde in das Bild passen, das von den Botnetzen geprägt ist und von mir auch im Zusammenhang mit Homebanking-Trojanern erwartet wird. Die Malware wird dadurch schlanker, ihr Entdeckungsrisiko wird dadurch geringer und ihr Funktionsumfang muss nicht schon bei ihrer Verbreitung feststehen. Das Modell ermöglicht eine schnelle Aktualisierung, um Virenscanner abzuwehren und Angriffsziele anzupassen.

eingeschränkte Autonomie und Automatisierung

Damit gehe ich von folgender These aus: Die hoch entwickelten Formen der heutigen Malware arbeiten mit einer eingeschränkten Autonomie. Updates und Anweisungen im Einzelfall erhalten sie von einer auswärtigen Steuereinheit (C & C). Diese Strategie hat mehrere Vorteile: Die Malware als solche muss keinen Ballast für Eventualitäten mit sich tragen, sondern kann sich darauf konzentrieren, sich einzunisten und eine Backdoor zu schaffen. Damit ist sie in der Lage, mit einer Steuereinheit Kontakt aufzunehmen und sich mit maßgeschneiderten Funktionen, Rootkits und Aufträgen ausstatten zu lassen.

Das Schaubild oben verdeutlicht das am Beispiel der Homebanking-Trojaner: Sie haben sich mit Hilfe ihrer Steuereinheit in dem Zombie eingenistet und warten auf das "Reiz-

---

6 ▸ **CF**, gezielter Einsatz nach Landesgewohnheiten, 29.12.2011

7 Siehe jetzt auch: ▸ Innenangreifer half bei Stuxnet-Infektion, Heise online 13.04.2012.

kommando", also den Verbindungsaufbau zu einer Bank. Die dabei aufgenommenen Daten übermittelt die Malware an ihre Steuereinheit, die ihr manipulierte Webseiten zuspielt, die dem Anwender schließlich im Browser angezeigt werden. Dazu gehören auch die Daten für manipulierte Verfügungen und die darauf angepassten Bank-Webseiten, die dem Anwender den ordnungsgemäßen Betrieb vorgaukeln.

Aus Botnetzen ist bekannt, dass anstelle eines vom Angreifer kontrollierten C & C-Servers einer von mehreren Flux-Servern agiert [8]. Sie stehen unter der Kontrolle des C & C, haben aber keine direkte Verbindung zur Konsole des Kontrolleurs und in die Kette können noch mehr Flux-Server zwischengeschaltet sein.

Wir haben es insoweit nicht mit einem Man-in-the-Middle-Angriff zu tun. Der MitM ist die Malware selber, nur dass sie ihre Anweisungen von anderen Automaten zugespielt bekommt. An der einzelnen Kontomanipulation oder anderen Aktivität der Malware ist auch kein menschlicher Angreifer beteiligt, sondern das besorgen die Steuereinheiten selbständig und automatisch. Nur im Hintergrund müssen die menschlichen Täter für die Verbreitung der Zombie-Malware und für die Aktualisierung der Steuereinheiten sorgen.

Basis-Malware und produktive Malware

Das dahinter stehende Konzept ist infam, brutal und logisch. Beim klassischen Phishing wurden Kontozugangsdaten ausgespäht, mit denen ein menschlicher Täter eigenhändig Manipulationen ausführen konnte. Das moderne Phishing braucht keinen menschlichen Angreifer, der sich die Zeit um die Ohren schlägt, bis er neue Kontodaten zugeschickt bekommt oder ihm eine Malware meldet: Jetzt ist es soweit! Jetzt macht der Trottel Homebanking! Automaten sind viel schneller und effektiver, wenn professionelle Software eingesetzt wird, die Basis-Malware effektiv verteilt und eingenistet ist und die Fernsteuerung richtig funktioniert.

Dem folgend unterscheide ich zwischen zwei verschiedenen Projektstadien beim Malware-Einsatz. Zunächst muss die Basis-Malware verteilt werden und sich mindestens soweit in den angegriffenen Computern eingerichtet haben, dass sie Kontakt zur Steuerungseinheit aufnehmen kann. Die Steuerungseinheit versorgt die Basis-Malware mit Updates und Anweisungen. Erst dadurch wird die Basis-Malware zur produktiven Malware und kann ihre Nistumgebung optimieren und die von ihr erwarteten Aktionen ausführen. Auch dabei greift sie wieder auf die Zulieferungen der auswärtigen Steuerung zurück.

Das gedankliche Modell dahinter ist funktional ausgerichtet. Die Malware im Einzelfall kann alle Basis- und produktiven Funktionen enthalten - wie Stuxnet, muss aber mindestens die Basis-Funktionen können. Das lässt eine große Spannbreite von Varianten zu und keine ist weniger wahrscheinlich als die andere.

Die Funktionsbreite einer Basis-Malware wird sich immer auch am Einsatzzweck bemessen. Für die Industriespionage, das hat der Night Dragon bewiesen [9], reicht die Perforation des Angriffsziels und die Schaffung einer Backdoor aus. Die Backdoor verschafft dem Angreifer den Zugang und er

8 ▸ Jürgen **Schmidt**, Hydra der Moderne. Die neuen Tricks der Spammer und Phisher, c't 18/2007, S. 76

9 ▸ **CF**, Night Dragon, 13.02.2011

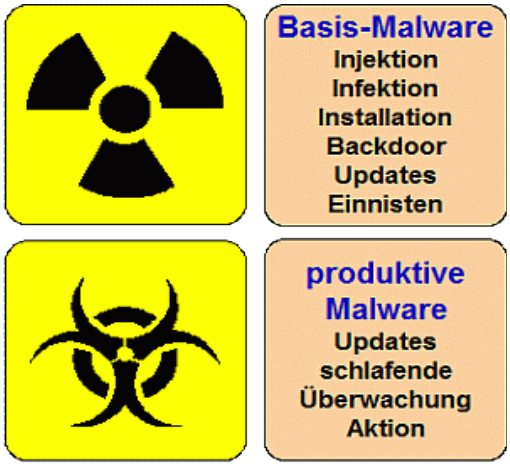
kann mit den Methoden des händischen Hackings alles Weitere machen. Eine reine DDoS-Malware für einen einzigen (Hacktivismus-) Einsatz wird auf eine filigrane Steuerung verzichten können und alle Basis- und produktiven Funktionen Huckepack tragen.

Das erwarte ich bei den erpresserischen Formen hingegen nicht, wenn sie sich auf eine Vielzahl von Varianten einstellen sollen. Auch hier wird es einfache Varianten geben, die eine stark umgrenzte Zielgruppe ins Visier nehmen und deshalb ohne auswärtige Steuerung auskommen. Nachhaltige und langfristige Angriffe kommen ohne sie jedoch nicht aus.

Malware-Installation

In dem Arbeitspapier IuK-Strafrecht [10] habe ich die Schritte bei der Installation von Malware aufgeführt:

Über eine Außenverbindung muss schädlicher Code in den Hauptspeicher des Zielsystems eingebracht (**Injektion**) und dort so verarbeitet werden, dass seine Funktionen ausgeführt werden (**Infektion**). Dazu wird eine Sicherheitslücke missbraucht (**Exploit**), die die Malware dazu nutzt, sich zu **installieren**. Dazu erkundet sie in aller Regel die Umgebungseigenschaften und lädt von einem **Command and Control-Server** im Internet Updates und weitere Programmbestandteile. Anschließend versucht sie sich zu tarnen. Dazu kommen **Rootkits** zum Einsatz, also Programmpakete, die vorhandene Sicherheitseinrichtungen abschalten oder unterlaufen, mit denen die Malware zum jeweiligen Neustart eingebunden (**Einnisten**) und vor Entdeckung getarnt wird. So präpariert kann die Malware ihre schädlichen Funktionen ausführen, kann das System nach wertvollen Informationen durchsuchen (Lizenzschlüssel, Kontodaten, Zugangscodes), Arbeitsprozesse überwachen (Keylogger) und andere Aktionen steuern (Phishing, Botnetze, DDoS,



Spams). Ganz häufig wird dabei auch eine Hintertür eingerichtet (**Backdoor**), die der Angreifer direkt dazu nutzen kann, das angegriffene System als Konsole fur geheime Aktivitäten zu nutzen.

Die Funktionen der Malware, die bis zu ihrer Installation reichen, habe ich oben als die der Basis-Malware bezeichnet [11]. Das damit verbundene Entwicklungsmodell für die automatisierte Malware lässt sich weiter verfeinern (siehe Tabelle auf der nächsten Seite). Dabei ist anzumerken, dass die Verbreitung präparierter Webseiten besonders in Deutschland ein Problem geworden ist [12].

Um eine Malware zum Einsatz zu bringen, bedarf es mehrerer Eingriffsschritte. Zunächst geht es darum, den Malcode zum Opfer zu bringen. Dort muss er sich in die Informationsverarbeitung einschleichen (Injektion und Infiltration) und sich installieren. Erst dann kann er seine maliziösen Funktionen enfalten. Sie können zunächst darin bestehen, dass sich die - produktive - Malware einrichtet, Dank ihrer Steuerungseinheit etabliert (Updates, neue Rootkit-Funktionen) und wartet.

10 ▸ Dieter Kochheim, IuK-Strafrecht, S. 24

11 Der Prozess wird in der ▸ Präsentation Malware-Infektion gezeigt.

12 ▸ Frank **Ziemann**, Viele Malware-Sites liegen in Deutschland, PC-Welt 19.04.2012.
Das führt inzwischen auch zu ungewöhnlichen Maßnahmen: ▸ Google warnt tausende Betreiber gehackter Webseiten, Heise online 18.04.2012.

Phase	Beschreibung	strafrechtliche Würdigung im Zusammenhang mit Homebanking-Trojanern
Vorbereitungsphase	Vorbereitung der Basis- und produktiven Malware. Einrichtung präparierter Webseiten oder von E-Mail-Anhängen. Verbreitung von Spam. Infektion anderer Webseiten .	tateinheitlicher Umgang mit Programmen zur Computersabotage und zum Computerbetrug (▸ §§ 303b Abs. 5 StGB i.V.m. ▸ 202c Abs. 1 Nr. 2 StGB, ▸ 263a Abs. 3 StGB)
Anlieferung	Zulieferung der Basis-Malware bis zu einer Schnittstelle im Zielgerät.	versuchte Computersabotage in Tateinheit mit versuchtem Computerbetrug und mit versuchter Fälschung beweiserheblicher Daten (▸ §§ 303b Abs. 1, Abs. 3, ▸ 263 Abs. 2 i.V.m. ▸ 263a Abs. 2, ▸ 269 Abs. 2 StGB)
Injektion	Überwindung einer Schwachstelle, um die Basis-Malware in einen laufenden Verarbeitungsprozess einzubringen.	vollendete Übermittlung nachteiliger Daten (▸ §§ 303b Abs. 1 Nr. 2 StGB) in Tateinheit mit versuchtem Computerbetrug und mit versuchter Fälschung beweiserheblicher Daten (▸ §§ 263 Abs. 2 i.V.m. ▸ 263a Abs. 2, ▸ 269 Abs. 2 StGB)
Infektion	Aktivierung der Basis-Malware in den Verarbeitungsprozessen des Zielgerätes. Erkundung der Systemumgebung. Kontaktaufnahme zur Steuereinheit und Upload weiterer Komponenten.	wie bei der Injektion
Einnisten	Einrichtung der Programmbestandteile der produktiven Malware.	vollendete Computersabotage (▸ §§ 303b Abs. 1 StGB) in Tateinheit mit versuchtem Computerbetrug und mit versuchter Fälschung beweiserheblicher Daten (▸ §§ 263 Abs. 2 i.V.m. ▸ 263a Abs. 2, ▸ 269 Abs. 2 StGB)
Tarnung	Einsatz von Rootkits, um die Malware vor der Erkennung zu tarnen.	wie beim Einnisten
Einsatz, Kopieren	Unmittelbarer Einsatz: Ausführung der Schadfunktion, zum Beispiel bei erpresserischer Malware oder bei der Übernahme von Zombies in ein Botnetz. Verbreitung der eigenen Basis-Malware. Erforschung der Systemdateien nach verwertbaren Daten (Kontozugangsdaten, Schlüssel für hochwertige Anwenderprogramme). Ruhender Einsatz: Gelegentliche Updates und Ergänzungen des Einnistens. Warten auf ein auslösendes Ereignis (koordinierte DDoS-Attacke, Homebanking). Verzögerter Einsatz nach einem auslösenden Ereignis.	Computersabotage in Tateinheit mit Computerbetrug und mit Fälschung beweiserheblicher Daten (▸ §§ 303b Abs. 1, ▸ 263a Abs. 2, ▸ 269 Abs. 2 StGB)
Deinstallation	Beseitigung der eigenen Programmkomponenten und Spuren nach Abschluss des Einsatzes (Option für reine Spionage-Malware).	

Vorbereitungsphase

Planung, Entwicklung und Einkauf der Malware und anderer Ressourcen:

Der Angriff muss geplant, die Malware (Malcode, Exploits und Rootkits) entwickelt oder gekauft werden. Daneben müssen die Verbreitungswege vorbereitet werden. Dazu gehört der Ankauf von Botnetzen zur Verbreitung von Spam, die Präparierung von fremden oder eigenen Webseiten mit Malcode und ihre Einrichtung (Pharmen). Schließlich müssen auch die Steuerungseinheiten (C & C- / Flux-Server) und Dumps (Ablageorte für ausgespähte Daten) eingerichtet (und gepflegt) werden.

Am Ende startet der Angreifer den Angriff mit einem Kommando und muss sich um nichts weiter kümmern, wenn er automatisierte Malware einsetzt.

Es gibt keine ausdrückliche Strafbarkeit für die Handlungen in der Vorbereitungsphase, so dass es auf die Umstände im Einzelfall ankommt.

Wenn die Täter ein Verbrechen planen, machen sie sich nach ▸ § 30 StGB strafbar. Das wäre der Fall beim Bandencomputerbetrug (▸ § 263 Abs. 5 i.V.m. ▸ § 263a Abs. 2 StGB) oder bei den gleichzeitig banden- und gewerbsmäßigen Formen der Fälschung technischer Aufzeichnungen (▸ § 267 Abs. 4 i.V.m. ▸ § 268 Abs. 5 StGB) oder beweiserheblicher Daten (▸ § 267 Abs. 4 i.V.m. ▸ § 269 Abs. 3 StGB).

Handeln sie als Bande, dann können die vorbereitenden Arbeiten der Mitglieder zu täterschaftlichen Handlungen werden, wenn sie maßgebend waren und schließlich der Erfolg eingetreten ist (neben den genannten Beispielen auch ▸ § 263 Abs. 3 Nr. 1 i.V.m. ▸ § 263a Abs. 2 StGB, ▸ § 267 Abs. 3 Nr. 1 i.V.m. ▸ § 268 Abs. 5 oder ▸ § 269 Abs. 3 StGB, ▸ § 303b Abs. 4 Nr. 2 StGB).

Bilden die Täter sogar eine kriminelle Vereinigung, dann trifft auch die Hinterleute und die Rädelsführer eine strafrechtliche Haftung ungeachtet ihrer unmittelbaren Beteiligung an einzelnen Sraftaten (▸ § 129 Abs. 4 StGB).

Daneben sind einzelne Vorbereitungshandlungen - Umgang mit Skimming-Geräten (▸ § 149 Abs. 1 Nr. 1 StGB), Programmen zum Computerbetrug (▸ § 263a Abs. 3 StGB), zur Computersabotage (▸ § 303b Abs. 5 StGB) oder mit Zugangscodes (▸ § 202c Abs. 1 Nr. 1 StGB) - selbständig srafbar.

Am Ende der Vorbereitungsphase startet der Täter den Prozess der Verbreitung, Infiltration, Einnistung und Aktivierung der Malware. Von da an hat er keinen Einfluss mehr auf den Erfolg - bis sich die Basis-Malware oder die erfolgreich eingenistete produktive Malware meldet. Der Grad der Automatisierung bestimmt, ob dadurch rein automatische Prozesse angestoßen werden oder ein unmittelbares Mitwirken der Täter erforderlich ist.

Distanzdelikte und Fallensteller

Im Zusammenhang mit der automatisierten Malware tritt beim "Start" ein juristisches Problem auf, das einem Bombenanschlag mit einem Zeitzünder gleicht. Der Täter hat zwar alles in seiner Macht stehende getan, um den Erfolg herbeizuführen. Sein weiteres Zutun ist aber nicht mehr erforderlich.

Den strafrechtlichen Versuch definiert ▸ § 22 StGB: *Eine Straftat versucht, wer nach seiner Vorstellung von der Tat zur Verwirklichung des Tatbestandes unmittelbar ansetzt*. Das ist regelmäßig der Fall, wenn der Täter eines von mehreren Tatbestandsmerkmalen erfüllt hat und er seinem Plan folgend ohne weitere Unterbrechung und Zwischenakte die Tat ausführen will. Der BGH hat dazu das schöne Wortbild entwickelt: *Jetzt geht es los!*

Im Versuchsstadium kann der Täter unter den verschiedenen Voraussetzungen des ▸ § 24 StGB straffrei werden, wenn er seinen Plan aufgibt oder den Erfolg verhindert [13].

---

13 Einzelheiten in: ▸ Dieter **Kochheim**, Die goldene Brücke. Gescheiterte Taten, Rücktritt vom Versuch und Straffreiheit, 18.01.2012

Rechtsprechung des BGH zu den Distanzdelikten

Eine Straftat versucht, wer nach seiner Vorstellung von der Tat zur Verwirklichung des Tatbestandes unmittelbar ansetzt (▸ § 22 StGB). Die Grenze von der Vorbereitungshandlung zum Versuch wird nicht erst überschritten, wenn der Täter ein Tatbestandsmerkmal verwirklicht, sondern schon dann, wenn er Handlungen vornimmt, die nach seinem Tatplan der Erfüllung eines Tatbestandsmerkmals vorgelagert sind, in die Tatbestandshandlung unmittelbar einmünden und das geschützte Rechtsgut - nach der Vorstellung des Täters - in eine konkrete Gefahr bringen. Ein Versuch liegt deshalb vor, wenn der Täter Handlungen begeht, die im ungestörten Fortgang unmittelbar zur Tatbestandserfüllung führen sollen oder die im unmittelbaren räumlichen und zeitlichen Zusammenhang mit ihr stehen …

<▸ **BGH**, Urteil vom 26.01.1982 - 4 StR 631/81>

Das gilt nicht zwingend für Distanzdelikte, die ein Zutun des Opfers erfordern, also bei *denen der Täter notwendige Beiträge eines Tatmittlers in seinen Plan einbezieht. Hier liegt zwar ein Ansetzen des Täters zur Tat schon vor, wenn er seine Einwirkung auf den Tatmittler abgeschlossen hat, es ist also nicht erforderlich, dass der Tatmittler seinerseits durch eigene Handlungen zur Tat ansetzt. Ein unmittelbares Ansetzen ist jedenfalls dann gegeben, wenn der Tatmittler in der Vorstellung entlassen wird, er werde die tatbestandsmäßige Handlung nunmehr in engem Zusammenhang mit dem Abschluß der Einwirkung vornehmen (▸ BGHSt 4, 270, 273; ▸ 30, 363, 365 f., ▸ BGHSt 40, 257, 268 f.; ▸ BGHR StGB § 22 Ansetzen 4; ▸ BGHR AO § 370 Abs. 1 Konkurrenzen 12). Demgegenüber fehlt es hieran, wenn die Einwirkung auf den Tatmittler erst nach längerer Zeit wirken soll oder wenn ungewiß bleibt, ob und wann sie einmal Wirkung entfaltet. In diesen Fällen beginnt der Versuch erst dann, wenn der Tatmittler, dessen Verhalten dem Täter über ▸ § 25 Abs. 1 StGB zugerechnet wird, seinerseits unmittelbar zur Tat ansetzt. Entscheidend für die Abgrenzung ist daher, ob nach dem Tatplan die Einzelhandlungen des Täters in ihrer Gesamtheit schon einen derartigen Angriff auf das geschützte Rechtsgut enthalten, dass es bereits gefährdet ist und der Schaden sich unmittelbar anschließen kann.*

<▸ **BGH**, Urteil vom 12.08.1997 - 1 StR 234/97, Rn 8>

Die für Fälle mittelbarer Täterschaft entwickelten Grundsätze gelten auch, wenn - wie hier - dem Opfer eine Falle gestellt wird, in die es erst durch eigenes Zutun geraten soll. Auch diese Fälle sind dadurch gekennzeichnet, dass der Täter sich kraft Beherrschung des Geschehens fremdes Verhalten für seinen Erfolg nutzbar macht. Sie weisen daher eine der mittelbaren Täterschaft verwandte Struktur auf, das Opfer wird dabei zum "Tatmittler gegen sich selbst" (...). Auch hier liegt ein Versuch erst vor, wenn nach dem Tatplan eine konkrete, unmittelbare Gefährdung des geschützten Rechtsguts eintritt.

<ebenda, Rn 9>

Zwar setzt der Täter bereits zur Tat an, wenn er seine Falle aufstellt, doch wirkt dieser Angriff auf das geschützte Rechtsgut erst dann unmittelbar, wenn sich das Opfer in den Wirkungskreis des vorbereiteten Tatmittels begibt. Ob das der Fall ist, richtet sich nach dem Tatplan. Steht für der Täter fest, das Opfer werde erscheinen und sein für den Taterfolg eingeplantes Verhalten bewirken, so liegt eine unmittelbare Gefährdung (nach dem Tatplan) bereits mit Abschluß der Tathandlung vor (etwa wenn der Täter eine Zeitbombe an einem belebten Platz deponiert; vgl. dazu auch RGSt 66, 141: mit Sicherheit in absehbarer Zeit zu erwartendes Betätigen eines Lichtschalters und dadurch bewirktes Ingangsetzen einer "Brandstiftungsanlage"). Hält der Täter - wie hier - ein Erscheinen des Opfers im Wirkungskreis des Tatmittels hingegen für lediglich möglich, aber noch ungewiß oder gar für wenig wahrscheinlich (etwa beim Wegwerfen einer mit Gift gefüllten Schnapsflasche im Wald), so tritt eine unmittelbare Rechtsgutsgefährdung nach dem Tatplan erst dann ein, wenn das Opfer tatsächlich erscheint, dabei Anstalten trifft, die erwartete selbstschädigende Handlung vorzunehmen, und sich deshalb die Gefahr für das Opfer verdichtet.

<ebenda, Rn 10>

Der Abbruch der weiteren Tatausführung reicht zum strafbefreienden Rücktritt, wenn der Täter davon überzeugt, dass er sein Tatziel nicht erreicht hat und es nicht mehr erreichen will (unbeendeter Versuch, ▸ § 24 Abs. 1 S. 1 1. Alt. StGB). Ein beendeter Versuch liegt hingegen vor, wenn der Täter seine Handlungsmöglichkeiten erschöpft hat und er entweder davon überzeugt ist, den Taterfolg erreicht zu haben oder eigenhändig nicht mehr erreichen zu können. Er erlangt dann Straffreiheit, wenn er durch “Zutun” die Tatvollendung (Erfolgseintritt) verhindert (▸ § 24 Abs. 1 S. 1 2. Alt. StGB).

Der Giftmord, bei dem der Tod in unbekannter Zukunft eintritt, und der Bombenanschlag mit Zeitzünder sind sogenannte Distanzdelikte. Für sie gilt, dass der Täter dann den Versuch beendet, wenn er *die den unmittelbaren Angriff bildende Kausalkette in Gang setzt und den weiteren Geschehensablauf aus der Hand gibt* [14].

Der BGH differenziert etwas breiter, wie die Textzusammenstellung auf der vorigen Seite zeigt.

Prozessstart als Beginn des beendeter Versuchs

Danach müssen wir die Grundsätze, die zum Versuch (▸ § 22 StGB) und zur mittelbaren Täterschaft (▸ § 25 Abs. 1 StGB) entwickelt wurden, auch auf den Prozessstart bei der automatisierten Malware anwenden. Schon dabei gibt es verschiedene Lösungen. Um den Überblick nicht völlig zu verlieren, beschränke ich mich auf die Basis-Malware und ihre Aktivitäten bis zum Einnisten. Die ausführenden Funktionen (Einsatz) müssen einer gesonderten Betrachtung unterzogen werden.

Der Prozess des Einnistens ist immer mit einer Datenveränderung (▸ § 303a StGB) und in Anbetracht der heutigen Bedeutung der EDV für Privatleute und Gewerbetreibende auch eine Computersabotage verbunden (▸ § 303b StGB) [15]. Darauf beschränke ich mich hier. Dabei kommt dem Verbreitungsweg eine besondere Bedeutung, weil er die Nähe zum Opfer und den Beginn der Rechtsgutgefährdung bestimmt.

Die Verbreitung der Basis-Malware als Anlage zu einer E-Mail erfordert ein Zutun des Opfers. Es muss (in aller Regel) die Anlage selber starten. Dadurch wird es zum *"Tatmittler gegen sich selbst"* und tritt eine *konkrete, unmittelbare Gefährdung des geschützten Rechtsguts* erst beim Start der Anlage ein. Der Versuch beginnt und endet in diesem Moment.

Dasselbe gilt für Links, die in der E-Mail selber eingebettet sind, wenn sie zu einer präparierten Webseite führen. Mit der Betätigung des Links wird ein geplanter, automatisierter Ablauf in Gang gesetzt, der ebenfalls zur unmittelbaren Gefährdung führt und deshalb gleichzeitig beendet ist. In E-Mails eingebetteter Malcode bedarf keines Zutuns des Opfers. Er ist "scharf", sobald er versandt wird. Somit beginnt der Versuch in diesen Fällen bereits beim Versand der Spam-Nachrichten. Weil ein weiteres Zutun des Tä-

14 ▸ **Wessels**, **Beulke**, Strafrecht Allgemeiner Teil, C.F. Müller 2011 Rn 603 (unter Bezugnahme auf Roxin).

15 ▸ Dieter **Kochheim**, IuK-Strafrecht, S. 44

ters nicht erforderlich ist, ist der Versuch damit auch schon beendet.

Die Einrichtung von Pharmen mit präparierten Webseiten ist vergleichbar den Gifttrunk-Fällen. Eine konkrete und unmittelbare Gefährdung tritt erst ein, wenn das Opfer die präparierte Webseite aufruft. Das ist der Beginn des gleichzeitig beendeten Versuchs.

Wurden dazu fremde Webseiten präpariert, liegt auch darin eine Datenveränderung, die aber als gesonderte Tat nichts mit der Verbreitung der Malware als solche zu tun hat.

Seltener werden Massenspeicher (USB-Sticks, CD / DVD, Speicherkarten, Wechselfestplatten) zur Verbreitung der Malware genutzt. In diesen Fällen tritt die unmittelbare Gefährdung ein, sobald der Datenträger in die Hand des Opfers gerät. Spätestens in diesem Moment verliert der Täter seine Herrschaft über den Angriff und ist der Versuch beendet.

Versuch und strafbare Vorbereitungshandlungen

Die ▸ §§ 303a Abs. 3 und ▸ 303b Abs. 5 StGB verweisen wegen der Strafbarkeit im Vorbereitungsstadium auf den Hackerparagraphen ▸ § 202c StGB. Das führt dazu, dass bereits der Umgang mit der Basis-Malware strafbar ist: *Wer ... Computerprogramme, deren Zweck die Begehung <einer Datenveränderung> ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.* (▸ § 202c Abs. 1 Nr. 2 StGB).

Mit einer etwas schwereren Strafe droht ▸ § 263a Abs. 3 StGB im Hinblick auf Computerprogramme, deren Zweck der Computerbetrug ist. Das betrifft vor Allem die Homebanking-Trojaner.

Danach ergibt sich folgendes Bild für die Strafbarkeit der Täter in der Vorbereitungsphase: Allein schon der Umgang mit der Basis-Malware ist als besonderes Gefährdungsdelikt strafbar (▸ §§ 303a Abs. 3 und ▸ 303b Abs. 5 StGB i.V.m. ▸ § 202c StGB). Nach dem Start der Verbreitung verliert der Täter die Herrschaft über die Basis-Malware. Das bedeutet aber mit Rücksicht auf die Giftfallen-Rechtsprechung des BGH nicht, dass damit auch das Versuchsstadium beginnt. Das kann nur der Fall sein, wenn einer bestimmten Person eine bestimmte Malware zugespielt wird (Spear-Phishing). In den heute üblichen Fällen der Massenverbreitung von Basis-Malware beginnt der Versuch der Computersabotage bei der Zusendung des eingebetteten Schadcodes oder - noch etwas später - sobald das Opfer eine Anlage oder einen Link zu einer präparierten Webseite aktiviert.

Es handelt sich zugleich um ein Massen-Distanzdelikt, was besonders beim Einsatz von Spams mit Malware-Anhängen, Links zu präparierten Webseiten und selbstausführenden Elementen deutlich wird. Das tätige Handeln der Täter endet mit dem Versand. Dadurch werden alle Betroffenen die Opfer ein und derselben Tat. Das begünstigt den Täter, weil er nur wegen einer Straftat innerhalb des dafür vorgesehenen Strafrahmens bestraft werden kann und keine Gesamtstrafe gebildet wird (▸ §§ 53, ▸ 54 StGB). Wenn auch nur bei einem der Opfer die qualifizierenden Merkmale der Computersabotage (▸ 303b Abs. 1 StGB), der schweren Computersabotage (▸ 303b Abs. 2 StGB) oder eines besonders schweren Falls der schweren Computersabotage (▸ 303b Abs. 4 StGB) vorliegen, wird die Tat insgesamt ein Anwendungsfall der qualifiziertesten Form. So kann sich die Strafdrohung schnell von 2 Jahren Freiheitsstrafe (▸ §§ 303a Abs. 1 StGB) über 3 (▸ 303b Abs. 1 StGB) und 5 Jahre (▸ 303b Abs. 2 StGB) auf bis zu 10 Jahre Freiheitsstrafe im Höchstmaß erhöhen (▸ 303b Abs. 4 StGB).

Je nach der Art der produktiven Malware kann sich eine weitere Strafbarkeit aufgrund besonderer Vorschriften ergeben. Sie orientiert sich an der produktiven Malware im Einzelfall.

Anlieferung

Bei der Anlieferung geht es zunächst nur darum, den Malcode zum Zielgerät zu bringen. Die häufigsten Techniken dafür sind verseuchte Anhänge an E-Mails, in E-Mails eingebetteter Code, in Webseiten eingebetteter Code oder Datenträger mit Malcode (zum Beispiel auf verschenkten USB-Sticks). Dieser Schritt ist für das Opfer noch recht harmlos, weil es sich durch sein eigenes Nutzerverhalten (Meidung unsicherer Seiten, kein Starten von dubiosen Dokumenten und Links) und mit Sicherheitsprogrammen (Virenscanner und Firewalls, die nur bestimmte und überwachte Übertragungsprotokolle [Ports] zulassen) vor überraschenden Angriffen schützen kann.

Dennoch ist die Anlieferung die kriminalistisch interessanteste Phase im Zusammenhang mit der automatisierten Malware. Der Angreifer schließt mit ihr seine vorbereitenden Handlungen ab. Die Hintergrundtechnik (Steuerungseinheiten: C & C- und Flux-Server), der Spam-Versand oder die Präparierung von Webseiten und vor Allem die Malware als solche müssen vorbereitet sein und sozusagen "stehen". Alles muss geplant und eingerichtet sein. Von der Anlieferung an läuft die Infiltration automatisch und muss der Angreifer im Wesentlichen dafür sorgen, dass die Steuereinheiten fit bleiben, um die Zombies zu versorgen.

Bei der Anlieferung wird noch nichts am Zielsystem verändert, so dass mit ihr erst der Versuch einer Datenveränderung (▸ § 303a Abs. 2 StGB) oder einer Computersabotage (▸ § 303b Abs. 3 StGB) einsetzt (▸ siehe oben). Im Zusammenhang mit automatisierter Malware ist das manuelle Handeln der Täter aber bereits abgeschlossen, so dass mit der Anlieferung der Versuch beginnt und beendet wird und die Täter nur noch durch tätiges Handeln vom Versuch zurücktreten können (▸ § 24 Abs. 1 S. 1 2. Alt. StGB).

▸ § 303b Abs. 1 Nr. 2 StGB verlagert die strafbare Haftung stark in die Vorbereitungsphase, weil bereits die absichtliche Eingabe oder Übermittlung von maliziösen Code zur Strafbarkeit führt. Die Computersabotage ist jedoch ein besonderer Fall der Sachbeschädigung (▸ § 303 StGB), so dass eine gewisse denkbare oder sogar messbare Beeinträchtigung des angegriffenen Systems verlangt werden muss. Bis auf dem Weg zur Schnittstelle entfaltet der Malcode keine Wirkung, sondern erst, wenn die Schnittstelle ihn durchlässt. Deshalb bin ich der Meinung, dass die Anlieferung als solche noch keine Übermittlung und deshalb noch nicht strafbar ist.

Injektion

Mit der Injektion hat die Basis-Malware die Schnittstelle zum Zielgerät überwunden. Dazu bedarf es einer Umgebung, die den Malcode gewähren lässt, also einer Schwachstelle (Exploit). Damit gelangt die Basis-Malware zunächst einmal in den Hauptspeicher des Zielgerätes und muss die angegriffene Programmumgebung dazu veranlassen, ihre eigenen maliziösen Funktionen zu starten, also als Programm ausgeführt zu werden.

Die wichtigsten Umgebungen hinter einer Schnittstelle sind die Browser (E-Mail, Internet), die proprietären Anwenderprogramme zur Darstellung von Multimedia-Dateien (PDF, Shockwave und andere), die Laufzeitumgebungen für Anwenderprogramme (activeX, Java) und die Betriebssysteme selber, wenn die Anlieferung nicht über die Netzwerkkarte, sondern über andere Schnittstellen erfolgt.

Zu einer gewissen Ehrenrettung für alle Anbieter von Sicherheitslösungen sei angemerkt, dass die wirklich gute Basis-Malware inzwischen gut getarnt ist. Sie wedelt nicht mit dem sinnbildlichem Brecheisen, das von allen beteiligtigten Programmen schnell erkannt werden könnte. Ihre maliziösen Funktionen sind verschlüsselt und können mit heuristischen Methoden (Funktionsabschätzung) nicht unbedingt und zuverlässig er-

kannt werden [16]. Teilweise funktionieren die einzelnen Angriffswerkzeuge nach dem Mamuschka-Prinzip. Das sind die russischen Holzfiguren, die sich öffnen lassen und in ihrem Inneren jeweils eine kleinere Version von sich offenbaren. In dem Zusammenhang hier bedeutet das, dass zunächst ein harmlos wirkender Quellcode von der Malware gebildet wird, der weitere verschlüsselte Elemente enthält. Erst wenn diese auch entschlüsselt werden, entfaltet sich das nächste Angriffswerkzeug.

Sobald die Injektion erfolgreich war, hat auch eine Übermittlung im Sinne von ▸ § 303b Abs. 1 Nr. 2 StGB stattgefunden.

Die Schwelle zur Datenveränderung (▸ § 303a StGB) oder zur Computersabotage im Allgemeinen (▸ § 303b StGB) wird damit aber noch nicht erreicht, was wegen der Vorverlagerung nach ▸ § 303b Abs. 1 Nr. 2 StGB ohne Bedeutung ist. Selbst wenn die Malware in diesem Stadium Programmversionen, Browsereinstellungen und Konfigurationsdateien ausliest, so handelt es sich grundsätzlich um Daten, die von den Anwenderprogrammen "bereitwillig" offenbart werden und noch keinem strafrechtlichen Datenschutz unterliegen (gemeint sind die ▸ §§ 202a, ▸ 202b StGB).

Alle anderen Tatbestände zur Sachbeschädigung an informationstechnischen Systemen können noch nicht erfüllt sein, weil die Malware im Stadium der Injektion noch nichts verändert und manipuliert hat. Der Malcode hat einfach nur die Schnittstelle überwunden, hat den Kontakt zu einer Ablaufumgebung aufgenommen, sich sozusagen angeklemmt, und jetzt muss er in die Verarbeitungsprozesse des Zielsystems hineinkommen.

Infektion, Einnisten und Tarnung

Bei der Infektion entfaltet die Basis-Malware ihre maliziöse Wirkung, weil sie damit direkt in die datenverarbeitenden Prozesse des Zielgerätes eingreift. Während - vor Allem - Virenscanner bei der Injektion nur den verschlüsselten Code der Malware analysieren können, entfaltet sich bei der Infektion der Malcode zum Einnisten und kann an seiner Wirkweise erkannt werden.

Für die Infektion bedarf es deshalb ebenfalls einer Schwachstelle (Exploit), um die Aktivitäten der Basis-Malware zu tarnen. Das kann in der Weise geschehen, dass sie sich in die Abläufe eines als sicher (in dem Sinne: gehört zu mir) angesehenen Programms einbringt oder sich als systemzugehöriges Programm tarnt.

Je nach ihrer Ausrichtung bewirkt die Basis-Malware:

Backdoor Einrichtung einer Außenverbindung, um mit einer Steuerungseinheit Kontakt aufnehmen, Updates und Anpassungen laden zu können.

Virenscanner Abschalten oder Umkonfigurieren vorhandener Virenscanner.

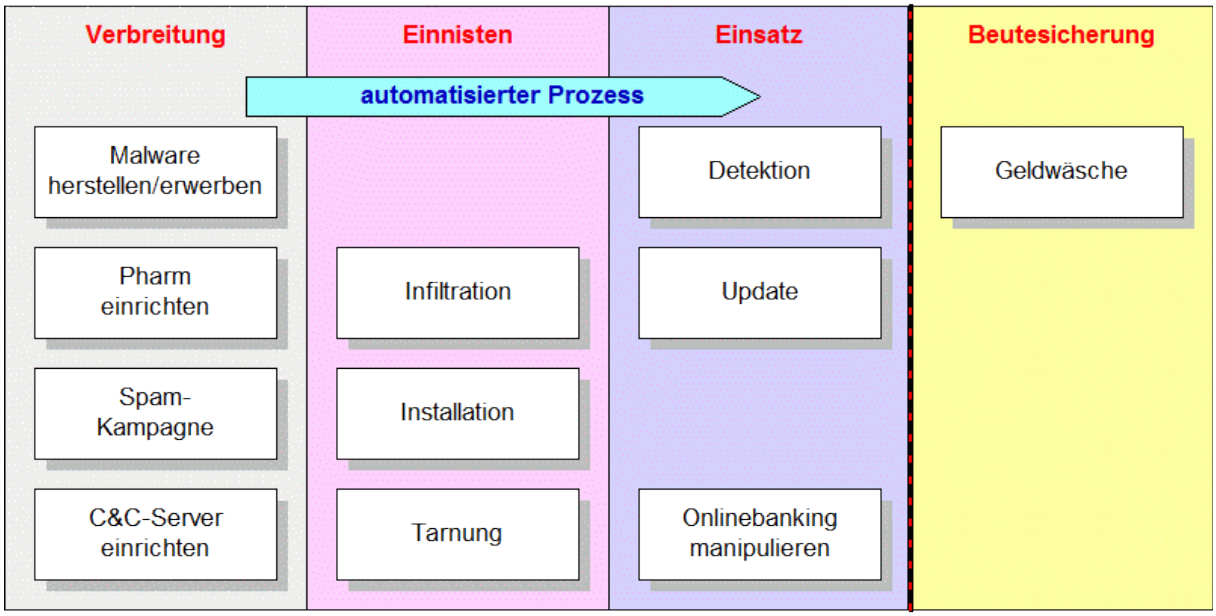
produktive Malware Installation der produktiven Malware, wobei zum Beispiel vorhandene Systemdateien ausgetauscht oder verändert werden. Denkbar ist es auch, dass die Programmkomponenten zu exotischen Massenspeichern (Grafikkarte, Router u.a.) ausgelagert werden, wo sie üblicherweise von Virenscannern nicht erfasst werden.

Autostart Manipulation der Registry oder anderer Autostart-Dateien (Bootsektionen), um den selbsttätigen Start der produktiven Malware zu gewährleisten.

Rootkits Veränderung der Systemrechte, Zeitstempel und Dateigrößen, um die produktive Malware vor

16 In der Artikelserie "Tatort Internet" in der Zeitschrift c't wurden die Mechanismen anschaulich beschrieben: ▸ Dieter **Kochheim**, IuK-Strafrecht, S. 25.

Tatphasen beim Einsatz von Onlinebanking-Trojanern



ihrer Entdeckung zu tarnen.

Alle genannten Maßnahmen verändern das angegriffene System nachhaltig im Sinne der ▸ §§ 303a, ▸ 303b StGB. Spätestens hierbei tritt auch die Vollendung der klassischen Tatbestände der Datenveränderung und Computersabotage ein. Die Art und der Einsatzzweck der produktiven Malware bestimmen ihr weiteres Verhalten.

Erpresserische Malware (Bundespolizei-Trojaner) verändert die Konfigurationsdateien des BIOS, so dass beim nächsten Boot-Vorgang der Systemstart verhindert und die beliebte Zahlungsaufforderung erscheint.

Zombie-Malware (Botware) richtet eine Backdoor ein, nimmt in aller Regel den Kontakt zu einem C & C- oder Fluxserver auf und meldet ihre Betriebsbereitschaft. Moderne Formen der Botware gehen verhältnismäßig schonend mit den Zombies um, um sie lange für das Botnetz verfügbar zu haben. Besonders leistungsfähige Zombies, die zudem ständigen Netzkontakt haben, können auch als Flux-Server oder Fileserver (Ablage von Dateien) für Dumps oder zur Verbreitung von Daten und Codes eingerichtet werden. In aller Regel durchforscht die Botware auch die lokalen Konfigurationsdateien, um Kontodaten, Zugangs- und Schlüsseldaten zu erkunden.

Auf die Datenspionage spezialisierte Malware könnte zunächst ihre Systemumgebung erkunden und Aufzeichnungsroutinen installieren (Keylogger). Sie wird zudem eine Backdoor errichten, um die erkundeten Daten zu übermitteln und um dem Angreifer Zugang zum perforierten System zu geben.

Homebanking-Malware ist besonders darauf ausgerichtet, so lange unerkannt zu bleiben, bis eine Bankverbindung hergestellt wird. Sie wird deshalb nur gelegentliche Anfragen an ihre Steuerungseinheit richten, um Updates abzufordern und zu installieren.

Homebanking-Malware. Überblick

Eine automatisierte Form der Homebanking-Malware soll uns als Beispiel für die tatsächliche und rechtliche Betrachtung der Basis- und der produktiven Malware zeigen.

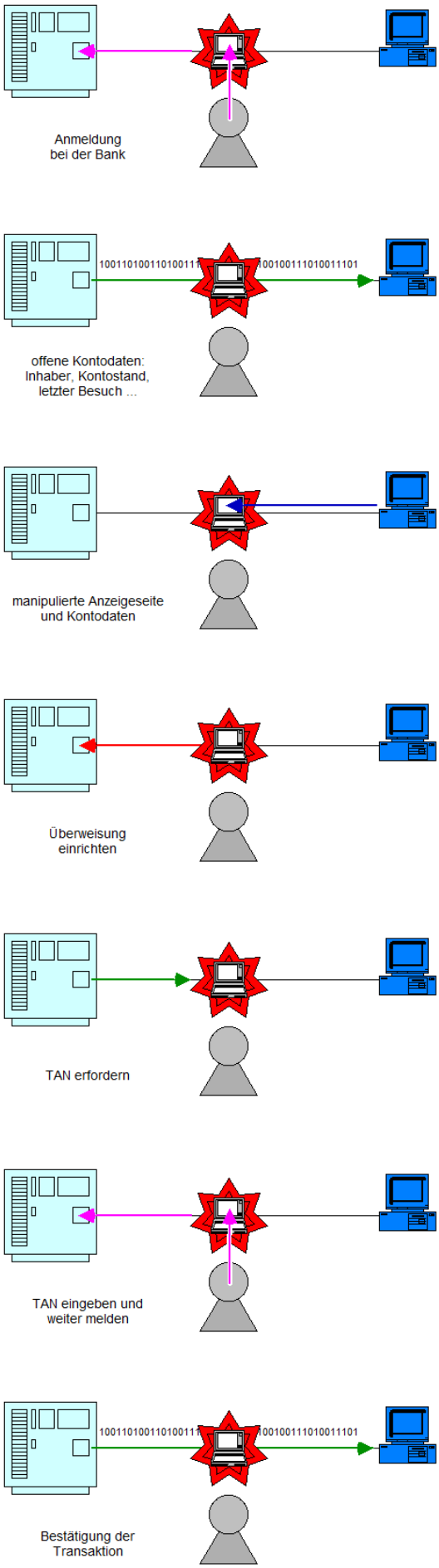
Einen grafischen Überblick gibt das Bild auf der Folgeseite. Eine gesonderte ➔ **Animation** fasst die Tatphasen der Vorbereitung, des Einnistens und des Einsatzes dieser Ausprägung von Malware zusammen. Ihr Ziel, die Manipulation der Verfügungen im Zusammenhang mit Homebanking kann sich als schwere Kriminalität in der Form des gewerbsmäßigen Bandencomputerbetruges erweisen (‣ § 263 Abs. 5 i.V.m. ‣ § 263a Abs. 2 StGB), so dass bereits die Verabredung als solche und alle Handlungen im Vorbereitungsstadium der Strafbarkeit wegen der Verabredung eines Verbrechens unterliegt (‣ § 30 StGB).

Einsatz von Homebanking-Malware

Die Malware ruht, solange der Anwender keine Bank-Webseite aufruft, und tritt dann in Aktion. Die zweite ➔ **Animation** zeigt Beispielhaft den Einsatz einer automatisierten Form von Homebanking-Malware (siehe auch die Grafiken rechts). Sobald der Anwender Kontonummer, Zugangscode und Captcha eingegeben hat, klemmt sie ihn sozusagen vom direkten Zugriff auf die Bankseite ab, übermittelt ihrer Steuerungseinheit die offenen Bankdaten (Kontoinhaber, Kontonummer, Saldo, letzter Besuch usw.) und erhält von der Steuerungseinheit eine nachgemachte Bankseite.

Das kann zum Beispiel die Mitteilung der Bank sein, dass die Einrichtung neuer Sicherheitsvorrichtungen die Eingabe einer bestimmten TAN bedarf.

Unsichtbar und im Hintergrund hat die Malware auch von der Steuerungseinheit die Daten für eine Überweisung erhalten und bei dem Anwender wird jetzt genau die von der Bank angeforderte TAN abgefragt. Nach Abschluss der Transaktion erhält die Malware



neue Bankseiten von der Steuerungseinheit, die sich zunächst für die Aktivierung der neuen Sicherheitsvorrichtungen bedanken und die jüngste Kontobelastung nicht erkennen lassen.

Das böse Spiel kann beliebig häufig wiederholt werden. Kontoübersichten werden von der Malware zunächst an die Steuerungseinheit übermittelt und dort bereinigt. In dieser Version zeigt die Malware dem Anwender die Seite dann an.

Sobald der Anwender eine eigene Überweisung eingibt, werden seine Daten an die Steuerungseinheit gegeben. Von dort hat die Malware bereits die nächsten Überweisungsdaten erhalten und damit die zweite manipulierte Überweisung eingerichtet. Sodann erstellt die Steuerungseinheit eine neue Bankseite, mit der der Anwender zur Eingabe der für seine Transaktion erforderlichen TAN aufgefordert wird. Auch die Bestätigung der erfolgreichen Überweisung mit angepassten Zahlen bekommt der Anwender über die Malware von der Steuerungseinheit übermittelt. Das ihm vorgegaukelte Schauspiel lässt jedenfalls nicht erkennen, dass im Hintergrund ganz andere Kontoverfügungen stattgefunden haben als die vom Anwender gewollten und eingegebenen.

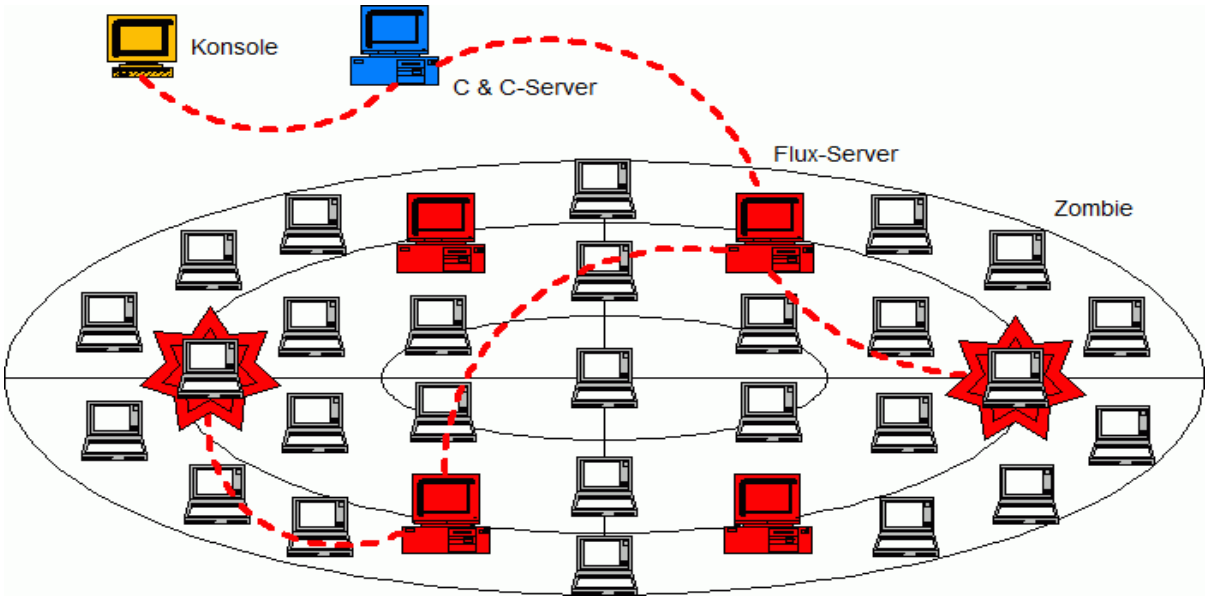
Eine Variante der Malware ändert beim Verlassen der Bankseite die Zugangsdaten zum Internet. Damit wird ein nochmaliger Aufruf der Bankseite verhindert und damit auch kritische Nachfragen bei der Bank.

Der Einsatz von Homebanking-Trojanern in der beschriebenen Form stellt sich bis zum Einnisten in aller Regel als ein besonders schwerer Fall der schweren Computersabotage im Sinne von § 303b Abs. 4 Nr. 2 StGB dar (Gewerbsmäßigkeit insoweit unterstellt). Aufgrund der besonderen Ausrichtung der Homebanking-Malware beginnt der Versuch des Computerbetruges bereits bei der Infektion mit der Basis-Malware, weil bereits dadurch die Gefährdung des Rechtsgutes "Vermögen" im Anschluss an die Giftfallen-Rechtsprechung einsetzt. Die rechtlichen Schlüsse wegen der Strafbarkeit in den Phasen bis zum Einnisten bis schließlich beim Einsatz der Malware ergeben sich bereits aus der Tabelle über die strafrechtliche Würdigung im Zusammenhang mit Homebanking-Trojanern.

Die filigranen Manipulationen an den Bank-Webseiten, die dem Anwender angezeigt werden, machen die Tat schließlich auch zu einer (gewerbsmäßigen) Fälschung beweiserheblicher Daten (§ 267 Abs. 3 Nr. 1 i.V.m. § 269 Abs. 3 StGB).

Die gleichzeitig gewerbs- und bandenmäßigen Formen des Computerbetruges, der Fälschung technischer Aufzeichnungen und beweiserheblicher Daten sind selbständige Verbrechenstatbestände (§§ 263 Abs. 5 i.V.m. 263a Abs. 2, §§ 267 Abs. 4 i.V.m. 268 Abs. 5 StGB oder 269 Abs. 3 StGB). Die Verabredung zu solchen Verbrechen steht selbständig unter Strafe (§ 30 StGB).

Die Verabredung ist wie die Anstiftung oder die Beihilfe eine Form der Beteiligung am Grunddelikt. Im Zusammenhang mit dem Skimming hat der BGH zwar im Sommer 2011 das Konkurrenzverhältnis zwischen Täterschaft am Gefährdungs- und Beteiligung am Grunddelikt offen gelassen. Sobald das Grunddelikt beginnt, endet jedoch das Gefährdungsdelikt. Das bedeutet, dass in der Vorbereitungsphase nicht der Umgang mit Programmen zur Computersabotage und zum Computerbetrug strafbar sind, sondern die Verabredung zum schweren Computerbetrug in Tateinheit mit der Verabredung zum schweren Fälschen beweiserheblicher Daten und in Tateinheit mit dem Umgang mit Programmen zur Computersabotage (§ 30 StGB i.V.m. §§ 263 Abs. 5, 263a Abs. 2, §§ 267 Abs. 4, 268 Abs. 5 StGB und 269 Abs. 3 StGB sowie §§ 303b Abs. 5 StGB i.V.m. 202c Abs. 1 Nr. 2 StGB).



C & C- und Flux-Server

Die wichtigsten Charakteristika beim Einsatz automatisierter Malware sind ausgefeilte Vorbereitungen, die Einrichtung von Steuerungseinheiten und die eingeschränkte Autonomie der Malware selber. Wir sprechen insoweit von hoch entwickelter, professioneller Malware, die von Tätern im internationalen Maßstab eingesetzt wird. Stuxnet stellt insoweit eine Ausnahme dar. Diese Malware konnte auf keine Steuerungseinheiten zurück greifen, musste ihre Basis- und produktiven Teile Huckepack tragen und wurde über USB-Sticks vertrieben.

Meine Annahme, dass die hoch entwickelte Malware automatisiert ist, fußt auf den Informationen, die im Hinblick auf die Botnetze bekannt sind, und auf der Überlegung, dass vor Allem die Basis-Malware "schlank" sein muss, um in die Zielsysteme eindringen zu können. Jede Zusatzfunktion könnte sie auffällig machen und enttarnen. Andeutungen auf entdeckte C & C-Server gibt es häufiger in journalistischen Meldungen, ohne dass ihre genaueren Aufgaben mitgeteilt werden. Gelegentlich ist die Rede davon, dass mehrere C & C-Server für den Betrieb eines Botnetzes im Einsatz seien. Während ich diesen Aufsatz schrieb, erhielt ich eine Bestätigung für meine Annahme, die ich aber nicht näher ausführen kann.

Ein gewissermaßen klassischer Command & Control-Server ist die zentrale Steuerungseinheit für dezentralisierte Serverdienste. Das Filesharing gibt ein frühes Beispiel dafür: Die Steuerungseinheit verwaltete die Informationen darüber, welcher Client die interessanten Informationen verwaltet und vermittelt den Kontakt.

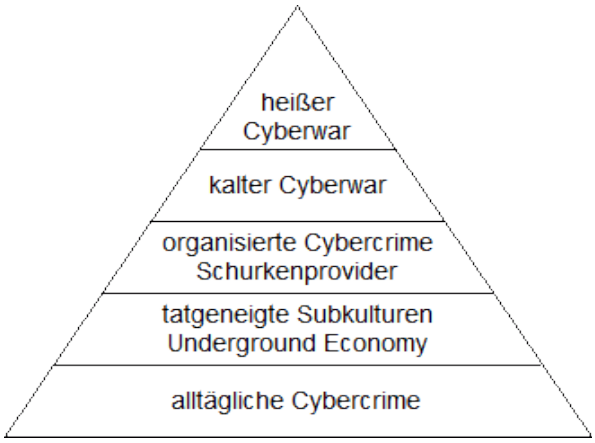
Ein Botnetz lebt davon, dass die eingefangenen Zombies von einer zentralen Steuerungseinheit geleitet werden, Spams versenden, DDoS veranstalten, Dumps zur Verfügung stellen oder als Konsole als Sprungbrett zur konspirativen Kommunikation oder zu kriminellen Handlungen dienen.

Seit fast 5 Jahren wird auch (wenig) über Flux-Server diskutiert. Sie werden eingerichtet, um die Kontakt- und Versorgungsaufgaben des zentralen C & C-Servers zu entlasten und um das Entdeckungsrisiko für die Hinterleute zu verringern. Außerdem erleichtern sie das Netzmanagement, indem sie Teile des Netzes selbständig verwalten und sich gegenseitig mit Updates und Anweisungen versorgen. Fällt einer der Flux-Server aus, übernehmen die anderen seine Aufgaben und wird bei Gelegenheit ein anderer gekapert.

Zunächst wurden Flux-Server als Webserver betrachtet, die nur beschränkte Vermittlungsaufgaben haben. Ihre Steuerungsfunktionen

waren begrenzt und sie waren eher Proxy- und Webserver, die standardisierte Aufgaben und Daten verteilten, ohne dass die Clients einen Kontakt zum "Master of Desaster" aufnehmen mussten. Das klassische Vorbild dafür ist die militärische Meldekette: Die kämpfende Fronteinheit bekommt ihre Einsatzbefehle nicht von der Heeresleitung direkt, sondern von berittenen (bekradeten oder radelnden) Boten.

Es gibt aber keinen zwingenden Grund dafür, dass nur ein C & C eingerichtet wird und tatsächlich wird immer wieder berichtet, dass verschiedenen Malwaren mehrere Internetadressen mitgegeben wurden, an die sie sich wenden sollen. Seit 5 Jahren hat sich die Computertechnik wieder einmal deutlich weiter entwickelt. Die Softwareverteilung und die Backuptechnik ist voran gekommen und ein Flux-Server kann ganz autonom handeln, ohne (nach seiner Installation) je von einem seiner Administratoren persönlich aufgesucht worden zu sein. Andererseits kann genau dieser einsame Flux-Server als Konsole für die nächste Aktualisierung des Botnetzes dienen und die Updates weiter verteilen.



Organisierte Cybercrime

Schon 2010 habe ich die oben abgebildete Pyramide vorgestellt. Die Zuordnung verschiedener Erscheinungsformen der Cybercrime werden hier (Auszug aus einer ➡ **Präsentation**) den verschiedenen Stufen zugeordnet.

Die Tätergruppen, die automatisierte Malware einsetzen, werden im Bereich der organisierten Cybercrime angesiedelt sein. Vielleicht mit Ausnahme von Trittbrettfahrern, die die Technik punktuell einkaufen.

Gehen wir noch einmal an den Ausgangspunkt zurück: Für die Einsatzbereiche Botnetze und Homebanking-Trojaner gibt es klare Hinweise, dass automatisierte Formen von Malware zum Einsatz gekommen sind. Im Zusammenhang mit dem Spionageeinsatz "Night Dragon" soll sie gezielt gegen die Mitarbeiter von Unternehmen und Organisationen eingesetzt worden sein, wobei die Malware selbständig Backdoors als Zugänge für die Angreifer errichtete.

Diese Hinweise habe ich zum Modell für jede Form von hoch entwickelter Malware geformt und auf die erpresserische Malware übertragen, die wegen ihres produktiven Teils relativ anspruchslos ist.

Nicht jede Malware muss diesem Modell genügen und die strafrechtlichen Auswirkungen müssen anhand des Einzelfalls präzisiert werden. Dennoch bin ich der Überzeugung, dass die hier entwickelten Grundsätze einen

guten Rahmen bilden, um die rechtlichen Probleme in den Griff zu bekommen.

Fazit

Mit dem ▸ Arbeitspapier Cybercrime habe ich 2010 nur die Erscheinungsformen der Cybercrime zusammen gefasst und dabei das materielle Cybercrime-Strafrecht respektvoll außen vor gelassen oder allenfalls gestreift. Im Nachhinein hat es sich als richtig erwiesen, dass ich meine materiellen Forschungen zunächst auf eine Erscheinungsform der Cybercrime beschränkt habe, dem ▸ Skimming. So konnte ich das umgrenzte Thema Schritt für Schritt erfassen und mich auch selber fortbilden, zumal die schwierigsten Probleme (wie so häufig) im allgemeinen Teil des Strafrechts liegen: Täterschaft und Teilnahme sowie Vorbereitung und Versuch. Aufsätze zum Skimming gibt es inzwischen viele, aber mir wurde schon mehrfach nachgesagt, dass kein anderer Autor zu tief in die Einzelheiten und Verästelungen eingestiegen ist. Ein besonderes Lob stammt von einem BGH-Richter, der sinngemäß sagte: Wenn ich über das Skimming schreiben wollte, dann könnte ich auch nur von ihnen abschreiben (Mai 2011).

2009 habe ich mich besonders mit den strukturellen Formen der Cybercrime befasst und die seinerzeit entwickelten Grundlagen haben Bestand bewiesen. 2010 habe ich mich endlich auch tieher mit den Boards befasst und auch die dabei gewonnenen Erkenntnisse stimmen noch immer. Ungeplant und überraschend gewann ich auch Erkenntnisse über den Cyberwar, noch bevor er zum öffentlichen Thema wurde (▸ Arbeitspapier Netkommunikation). Meine Unterscheidung zwischen dem Kalten und dem Heißen Cyberwar hat noch immer Geltung.

2011 habe ich zwei heiße Eisen angefasst. Zunächst habe ich den Mut gefasst, über die offenen und verdeckten ▸ Ermittlungen im Internet zu schreiben. Rumzutrollen ist die eine Sache, Farbe zu bekennen die andere. Der Aufsatz hat Bestand bewiesen.

Mit erheblich größeren Respekt bin ich an das umfassende Thema ▸ IuK-Strafrecht heran gegangen. Dazu musste ich zunächst mehrere Rechtsgebiete durchdringen, die auf dem ersten Blick nichts mit dem Cybercrime-Strafrecht zu tun haben scheinen, zum Beispiel dem Recht zur Urkundenfälschung und der kriminellen Vereinigung. Mit den Ergebnissen bin ich auch jetzt noch ganz zufrieden.

Auch der jetzt vorliegende Aufsatz über die automatisierte Malware fußt auf intuitiven Annahmen und verlangte eine tiefere Einarbeitung in fremd erscheinende Rechtsfragen (Distanzdelikte, Giftfallen). Ich habe den Eindruck, dass ich wieder einmal nicht ganz falsch liege.