Cybercrime und politisch motiviertes Hacking

Über ein Whitepaper von François Paget von den McAfee Labs

Dieter Kochheim

Besonders die McAfee Labs [1] und G Data [2] sind in den letzten Jahren mit ihren Studien zu den Strukturen der Cybercrime und der Underground Economy hervorgetreten und haben damit ihre technischen Arbeitsschwerpunkte erheblich erweitert. Auf die nach meinem Eindruck wichtigsten Publikationen haben ich im ▸ Arbeitspapier Cybercrime hingewiesen (S. 121).

Schon im März 2010 erschien bei McAfee die Studie Cybercrime and Hacktivism [3] von François Paget [4], allerdings nur auf Englisch, Chinesisch, Japanisch und „Brasilianisch“ [5]. Paget ist mutig. Er zeichnet Strukturen und nennt Namen und Zusammenhänge [6]. Die besondere Stärke des Textes ist die Ballung von Fakten und Belegen, also die Materialfülle. Paget kommen auch die eigenen Untersuchungen von McAfee zu Gute, auf die er besonders bei seinen grafischen Beispielen und Tabellen zurück greift.

Die analytischen Schlüsse bleiben vorsichtig, beziehen sich mehr auf die Erscheinungsformen als auf die kriminellen, gesellschaftlichen und wirtschaftlichen Mechanismen und könnten mehr Tiefe vertragen. Das vermeidet Paget aus gutem Grund, um sich nicht unnötig angreifbar zu machen.

Pagets Sprache wirkt stellenweise etwas blumig, was mir, der ich sehr ungeübt im Umgang mit englischsprachigen Texten bin, das Verständnis erschwert hat. Zu Gute kommt mir hingegen, dass ich mit der Materie halbwegs vertraut bin.

Der Text ist mir wichtig und seine wesentlichen Aussagen müssen auch im deutschen Sprachraum zur Verfügung stehen. Das ist der Grund dafür, dass ich ihn in eigenen Worten referiere, zusammen fasse und – zumeist in den Fußnoten – kommentiere. Das ist natürlich keine autorisierte Übersetzung, sondern eine persönliche Interpretation und Wiedergabe. Die Grafiken und Tabellen des Originals werden selbstverständlich nicht übernommen und müssen dort betrachtet werden [7].

Was auf den nächsten Seiten folgt, ist Paget, nicht Kochheim, obwohl sich viele unserer Einschätzungen gleichen. Sein Wissen über die Einzelheiten und Fakten habe ich nicht und ich versichere ihm meinen ungeteilten Respekt.

Der Text schwächelt an wenigen Stellen. Das Organisationsmodell der modularen Cybercrime unter Einsatz von Operating Groups und Koordinatoren als Projektmanager ist ihm nicht geläufig, sonst hätte er bestimmte Gruppen und Personen prägnanter seziert. Dasselbe gilt für mein Stufenmodell, in dem die Cybercrime die Basis für die Handelnden im Cyberwar bildet. Das Modell hätte ihm geholfen, die schurkischen Organisationen genauer von der Masse der geneigten Mitläufer zu unterscheiden.

Auch das Schlusswort schwächelt, weil es einige Entwicklungen erst erwartet, die mir längst eingetreten zu sein scheinen. Das gilt etwa für die Geldwäsche-Infrastrukturen der Cybercrime.

---

1 ▸ McAfee Threat Center

2 ▸ GDATA Security Labs

3 ▸ François Paget, Cybercrime and Hacktivism, McAfee Labs 15.03.2010

4 Paget erforscht seit 1990 Malware, ist einer der Gründer der McAfee Labs (1995) und jetzt der Leitende Ingenieur der McAfee Labs in Frankreich.

5 Hacktivism ist ein wenig gebräuchliches Kunstwort, das nichtkommerzielle, aber politisch oder sozial motivierte Hacking-Aktivitäten benennt. Ich habe es deshalb nicht als „Hacktivismus“, sondern als „Hacktivitäten“ übersetzt.

6 Die von Paget angegebenen Quellen habe ich nicht überprüft.

7 Ich verwende Übersetzungshilfen und kann keine sichere Übersetzung verbürgen. Ich versuche, Pagets Erklärungen und Positionen vorzustellen und habe auf die eigentlich gebotene Konjunktiv-Form verzichtet, um die Lesbarkeit zu erleichtern und das Verständnis zu fördern. Meine eigenen Stellungnahmen werden als solche ausgewiesen.

Dabei geht es längst nicht mehr um Bargeldtransfers mit Western Union oder dem kleineren Konkurrenten MoneyGram, sondern um Vouchers und bequeme Kreditkarten auf Guthabenbasis, die keine Identitätsprüfung abverlangen. Bei den besonderen Dienstleistungen für Internetkriminelle fehlen die Webshops, von denen G Data berichtet hat: Hier greift das Outsourcing für die Handelsgeschäfte selber und vor allem für die angeschlossenen Bezahlvorgänge.

Stuxnet war Paget noch nicht bekannt, als sein Text veröffentlicht wurde. Dieser Wurm dürfte die teuerste Malware sein, die bislang bekannt wurde. Sie greift gleich mehrere bislang unbekannte Schwachstellen unter Windows an und ist darauf spezialisiert, die Steuerungen von Industrieanlagen unter einer ganz besonderen Software von Siemens zu penetrieren. Stuxnet ist die erste Malware des Cyberwars, die sich im virtuellen Raum bewegt und dann in der realen Welt wirkt. Das können noch so hinterhältige Phishing-Programme nicht von sich behaupten.

Wir sind, so glaube ich, längst tiefer im Cybersumpf, als er von Paget beschrieben wird. Sein Text vermittelt jedoch das nötige Wissen und die Hintergründe, die wir unseren Betrachtungen und Bewertungen zugrunde legen müssen. Deshalb ist sein Text so wichtig.

1. Cybercrime and Hacktivism

Paget geht es um die Verbindung zwischen dem Internet und der Organisierten Kriminalität. Bereits in der Einleitung (S. 3) weist er darauf hin, dass das Internet die Globalisierung gefördert hat. Es ist zur Heimat der virtuellen Welten und ihrer Volkswirtschaften geworden und hat die Wirtschaftlichkeit von illegalen Aktivitäten gefördert und verstärkt, so dass auch die Straftäter zu internationalen Unternehmern geworden sind.

Aus der Verbindung zwischen dem Internet und der Kriminalität haben sich zwei Formen der "Internetkriminalität" gebildet: direkte, gegen Netzwerke gerichtete Angriffe und die Angriffe, die von diesen Netzwerken ausgeführt werden.

Die Cybercrime wird von Einzelpersonen, vielen Organisierten Internetverbrechern [8] oder Mafia-Gruppen ausgeübt. Neben dem Gewinnstreben sieht Paget weitere Motive für die Beteiligung an der Cybercrime [9]:

⇨ Spieltrieb: Cybercrime ist eine Herausforderung, die Hacker anzieht. Sie genießen die Aufregung und wähnen sich häufig in einer zweifelhaften Anonymität [10].

⇨ Informationen sammeln: Das Internet ist eine ideale Plattform für die Industriespionage.

⇨ Ideologien: Aus den „Nischen der Macht“ (alcoves of power) manipulierte oder in gutem Glauben handelnde "Patrioten" richten zunehmend kriminelle Aktivitäten gegen Institutionen, die sie als einen Feind betrachten.

---

[8] Der Begriff „Organisierte Internetverbrecher“ tauchte 2006 erstmals auf: ▸ Zweite große europäische Studie über das Organisierte Verbrechen und das Internet, McAfee Dezember 2006 (ZIP-Datei).
Fortschreibung: ▸ McAfee Avert Labs-Prognosen zu den Top 10 der Bedrohungen für das Jahr 2008, McAfee 16.11.2007.
Paget benutzt jetzt auch den Begriff Cybermafia (S. 7), den ich nicht für aussagekräftig halte.

[9] Auf den S. 25 und 26 widmet sich Paget der mangelhaften internationalen Strafverfolgung und den sicheren Häfen für Schurkenprovider sowie für Steueroasen. Auf die Wiedergabe seiner allgemein gehaltenen Aussagen wird verzichtet.

[10] Siehe auch S. 22.

⇨ törichtes Verhalten: Einige Leute handeln aus armseligen oder unklaren Gründen.

Dabei scheint in einigen Entwicklungsländern die Wirtschaftsspionage und der Cyberwar zu einem normalen Geschäft geworden zu sein (S. 12). Das gilt laut verbreiteter Vorwürfe für China, Indien und Brasilien, wo Industriespionage und Fälschungen toleriert werden, weil sie die Wirtschaft fördern. Anderenorts genießen Piraten-Netze und Hacker Immunität, wenn sie versprechen, nur ausländische Infrastrukturen anzugreifen [11].

In den USA wird häufig davon berichtet, dass Hacker oder Malware-Schöpfer legale Beschäftigungen finden können. Nachdem zum Beispiel 2009 der Autor des Twitter-Wurm (JS/Twettir) identifiziert worden war, bot ihm exqSoft Solutions einen Job an (S. 22).

Der Kult der Hacker ist jedoch gefährlich. Er gibt der Kriminalität einen positiven Anstrich, obwohl die Handlungen illegal sind. Seine Anhänger werden zu strafbaren Handlungen ermutigt, die mit der lobenswerten Erkundung von Softwarefehlern und Sicherheitslücken nichts zu tun haben (S. 22).

Die russische Gesellschaft ist von schwer gewalttätiger Kriminalität traumatisiert und dürfte die Cybercrime deshalb ignorieren, weil sie keine Blutvergießen auf den Straßen verursacht und sich auch ansonsten auf das öffentliche Leben kaum auswirkt (S. 22). In Russlands Öffentlichkeit werden einige Cybercrime-Syndikate als neue Denkfabriken [12] im digitalen Zeitalter und als Robin Hood-Figuren angesehen, die ihre Familien unterstützen und ihre Beute teilen, indem sie das Kleingeld aus dem übermäßig reichen Westen pressen. Auch in China zeigt eine Umfrage von der Shanghai Academy of Social Sciences aus dem Jahr 2005, dass Hacker und Rock-Stars auf die gleiche Wertschätzung treffen. 43 Prozent der Grundschüler sagten, dass sie Hacker lieben.

Im Osten setzte der Fall der Berliner Mauer im November 1989 dem Kalten Krieges und seinen Spannungen ein Ende (S. 12). Für die enorme Informations-Service-Infrastrukturen mussten neue Ziele gefunden werden, um Ihre Existenz zu rechtfertigen. Eine Option wurde dadurch die Wirtschaftsspionage. Viele Spezialisten verließen ihre Arbeitgeber, schlossen sich großen Industriegruppen an, gründeten eigene Unternehmen oder begannen, mit illegalen Aktivitäten zu liebäugeln.

Viele der neu entstandenen Staaten haben Mühe, die öffentliche Sicherheit, Rechtsstaatlichkeit und eine stabile Wirtschaft aufzubauen (S. 13). Die Schwächen dieser Ländern fördern die Kriminalität.

Neue Spannungen bedrohen die Welt und viele Länder bereiten sich aktiv auf einen Cyberwar vor (S. 12). Staaten wie China oder Russland zögern nicht, die schmutzige Arbeit von Einheiten machen zu lassen, die der Mafia oder "Patrioten"-Gruppen, nahe stehen. Neben ihrem Lohn gewinnen sie Straflosigkeit und Anerkennung. Der Neid der anderen bewirkt, dass sie ihnen nacheifern.

Einen weiteren Schwerpunkt sieht Paget im Terrorismus, der im Netz ebenfalls seine Spuren hinterlässt (S. 18). Dabei scheinen sich terroristische und kriminelle Motive zu vermischen. So wurden im Juni 2007 drei Al-Qaida-Sympathisanten verurteilt, weil sie eine Propaganda-Aktion vorbereiteten. Dazu suchte einer von ihnen, Tariq Al-Daour, seit 2002 Carding-Foren auf (ShadowCrew, CarderPlanet), um mit gestohlenen Kreditkartendaten terroristischen Aktivitäten zu finanzieren.

2. Organisierte Kriminalität und Mafia

Nach dieser Einleitung fasst Paget die international üblichen Definitionen für Organisierte Kriminalität zusammen (S. 3 f.), die der deutschen Übereinkunft entsprechen [13]. „Mafiöse Organisationen“ definiert er anhand des italienischen

[11] Meine Vermutung ist die, dass damit auch „stille Streitkräfte“ für einen künftigen Cyberwar rekrutiert werden.

[12] Im Original: Brainpower. Im Zusammenhang dürfte „Think Tanks“ nahe liegend sein.

[13] Anlage E zu den RiStBV: ▸ Gemeinsame Richtlinien ... über die Zusammenarbeit von Staatsanwaltschaften und Polizei bei der Verfolgung der Organisierten Kriminalität

Strafgesetzbuches (S. 4). Sie

⇨ begehen Verbrechen

⇨ aus Gewinnstreben,

⇨ nehmen Einfluss auf Wirtschaft, Politik und Öffentlichkeit, um sie sich zu unterwerfen,

⇨ und manipulieren dazu auch freie Wahlen,

⇨ um sich oder ihre geneigten Kandidaten durchzusetzen.

Außerhalb Italiens sieht Paget drei Organisationen, die er als mafiös ansieht: Die Russische Mafia, die chinesischen Triaden und die japanischen Yakuzas. Sie gründen auf hierarchischen und patriarchalischen Familien- oder Clan-Strukturen, nehmen für sich Honorität in Anspruch und halten enge Kontakte zu den höchsten Kreisen in Politik und Wirtschaft. Ihre Aktivitäten finden im Legalem wie im Illegalem statt und ihre innere Stabilität festigen sie durch interne Rituale, Ehren-Kodes und Gewalt. Die einfachen Mitglieder haben kein Mitspracherecht, sind zum Gehorsam und zum Stillschweigen verpflichtet. Im Gegenzug dafür bieten die mafiösen Organisationen individuellen Schutz und die Unterstützung der Angehörigen bei Inhaftierung oder Tod.

2.1 Russland und Osteuropa

Die kriminellen Organisationen reichen bis in das zaristische Russland zurück (S. 5). Sie zeichnen sich durch ihre hohe Anpassungsfähigkeit und Stabilität aus. Hinzu kommen ihre direkte Einflussnahme auf Politik, Verwaltung, Staats- und Regierungschefs sowie ihre dauernde Anwerbung jüngster, stärkster und am meisten motivierter Mitglieder.

Ihre kriminellen Geschäfte betrafen zunächst den illegalen Handel mit Kunstwerken, Antiquitäten und Konsumgütern. In den 1970-er Jahren kam der Drogenhandel hinzu. In den späten 1980-er Jahren entstanden die ersten privaten Unternehmen, die vor allem mit dem Import ausländischer Großhandelswaren und Büroausstattungen Gewinne machten. Seit etwa 15 Jahren durchsetzen kriminelle Banden die russische Wirtschaft. Ihre Geschäfte waren zunächst der Handel mit gestohlenen Autos und besonders die Schutzgelderpressung. Durch Prostitution, Drogenhandel und Glücksspiel in Dutzenden Kasinos und Hunderten Spielzimmern sowie durch Geldwäsche sind viele Beteiligte reich geworden.

Die Privatisierungen begannen 1993 bis 1994 und eröffneten außergewöhnliche Aussichten. Es fehlte an klaren rechtlichen Regeln, so dass die kriminellen Organisationen Unternehmen für wenig Geld kaufen oder unter ihren Schutz stellen konnten. Die profitabelsten kriminellen Aktivitäten wurden der Drogenhandel, der Wohnungsmarkt, der Handel mit Metall, Waffen, gefälschtem Wein und Spirituosen. Der schlechte urheberrechtliche Schutz förderte die Produktion und den Verkauf von Software-Raubkopien, DVDs und CDs. In dieser Umgebung durchdrang die Kriminalisierung das gesamte politische Leben.

Die Mafia-Mitglieder im Osten verstecken sich nicht, sondern suchen die Nähe zu den Eliten. Ihr Einfluss zeigt sich besonders dann, wenn sie wegen unzureichender Beweise aus der Haft entlassen werden.

Erstmals in den frühen 1990er fanden zahlreiche hoch qualifizierte und technisch versierte Absolventen in Bulgarien keine Arbeit (S. 7, 12). Einige unzufriedene und desillusionierte Programmierer gründeten „Virus-Fabriken“ und begannen Malware zu schreiben. Mit qualitativ hochwertigen bösartigen Programmen und den dazugehörigen Dienstleistungen lassen sich heute bis zu $ 1.000 US-$ verdienen [14].

In Russland begann der Hacking-Boom 1998 infolge der Finanzkrise (S. 7). Eine Armee von jungen, gut ausgebildeten Programmierern hatte plötzlich keine Arbeit mehr und sie sahen sich einem Umfeld von Korruption [15], wirtschaftlichem Niedergang

[14] Rumänien ist laut Paget bekannt für technische Geräte für das Phishing und das Carding (Skimming); siehe S. 20.

[15] Paget berichtet von einer Umfrage aus 2007 (S. 19), wonach etwa 27 % der Befragten berichteten, von russischen Beamten zur Zahlung von Bestechungs-

und beginnender Internetkriminalität ausgesetzt. Auch hier entstanden „Virus-Fabriken“. Korruption blüht im Schatten anderer Kriminalität (S. 20).

Alexei Galaiko, Ivan Petrichenko und Sergei Popow gründeten 1999 das HangUp-Team, um Malware zu verbreiten (S. 7). Sie wurden 2000 verhaftet, aber schnell wieder freigelassen. Seit 2003 oder 2004 scheint die Gruppe in die Organisierte Cybercrime eingebunden zu sein. Sie entwickelte den Trojaner Berbew, den JavaScript-Wurm Scob und Korgo, einen der ersten Homebanking-Trojaner, die sie zum Verkauf anboten. 2006 arbeiteten sie mit dem Russian Business Network – RBN – zusammen und entwickelten das Gozi Roboter-Netzwerk (Botnet), das SSL-Verschlüsselungen nutzt.

Im März 2001 sagte der russische Hacker Igor Kovalyev in einem Interview mit Wired Magazine (S.12): "Hier ist das Hacking ist eine gute Arbeit, einer der wenigen, ansonsten fehlenden guten Jobs." Der kriminelle Weg bietet einen Ausweg und eine Chance für den sozialen Aufstieg. Qualifizierte Entwickler, zögern nicht mehr, Mafiaorganisationen beizutreten oder für sie gegen Entgelt zu arbeiten.

Im Mai 2001 trafen sich in Odessa 150 Cyber-Kriminelle und gründeten die kriminelle Organisation CarderPlanet (S. 7). Ihr sichtbarer Teil war ein Forum (CarderPlanet.com), in dem hauptsächlich Zahlungskartendaten von Hackern aus den USA und Großbritannien gehandelt wurden. Diese Daten lassen sich kaufen oder können auf Kommission zum Betrug genutzt werden, um mit ihnen Internetgeschäfte abzuwickeln oder Zahlungskarten zu fälschen.

CarderPlanet ist als Organisation nach dem Vorbild der Mafia hierarchisch aufgestellt (Grafik S. 8). Ihre Basis bilden die Mitglieder des Forums. Darüber folgen zwei (untergeordnete) Schichten mit den „Köpfen“ und den „Köpfen der Köpfe“, die das mittlere Management bilden. Das Führungsmanagement besteht aus den Administratoren, die im Wesentlichen auch die „Reviewer“ (Rezensenten, besser: Beobachter) stellen. Sie achten auf die kriminellen Geschäfte der Mitglieder und darauf, dass die Carder-Organisation ihren „gerechten“ Anteil bekommt [16]. An der Spitze der Pyramide steht die Gründungsfamilie und vor allem ihr Gottvater Dmitry Golubov.

Die Cybercrime ist in Russland zum Geschäftsmodell geworden. Zunächst selbständige Unternehmen unter der Leitung von Absolventen technischer und wirtschaftlicher Universitätsausbildungen wurden zu EDV-Abteilungen der russischen Mafia. Vor allem in Moskau sind Management-Teams (Operation Groups) verfügbar, die bei Bedarf von der Mafia (Koordinatoren) angeheuert werden können.

Viele dieser Unternehmen profitieren von der Kronzeugenregelung und dem Schutz durch den russischen Federal Security Service (FSB), der sie gegen Interpol und vor Überstellungen in die USA und nach Europa schützt. Im Gegenzug versprechen sie, keine Angriffe gegen die Regierung und ihre IT-Infrastrukturen zu führen [17]. Diese unausgesprochene Vereinbarung wird seit fast zehn Jahren eingehalten. Wenn die Hacker dennoch verhaftet werden, bieten ihnen die Geheimdienste als eine Alternative zum Gefängnis einen Job in der FSB an.

Die Chaos-Hacker-Crew und die russische antifa-

geld aufgefordert worden zu sein.

Korruption sei in den neuen Staaten Osteuropas weit verbreitet, am meisten aber im Nahen Osten und in Nordafrika.

Siehe auch das Schaubild und die Tabelle auf S. 20 sowie S. 26.

[16] Eine solche Kontrolle ist symptomatisch für die russische Mafia. Der kriminelle Gewinnanteil fließt in den „Obschat“, also in die gemeinsame Kriegskasse, aus der Unterstützungen für „gefallene“ Mitglieder, Kredite für lukrative Projekte und vor allem der Lebensunterhalt für den an der Spitze stehenden „Dieb im Gesetz“ gezahlt werden. Ob CarderPlanet die Mafia-Struktur imitiert oder in die russische Mafia eingebunden ist, bleibt dennoch offen.

[17] Dieses Vorgehen ist typisch für den Kalten Cyberwar, in dem „private“ Fachleute für Malware, Hacking und Botnetze zunächst unter Schutz gestellt werden und ihre kriminellen Geschäfte durchführen dürfen. Im Bedarfsfall werden sie von staatlichen oder mafiösen Agenten nachhaltig daran erinnert, dass sie noch offene Schulden haben.

schistische Front sind wieder verschwunden (S. 17). Dagegen entstanden nationalistische Gruppen wie Nashi und ESM, die eine gewisse Nähe zur gegenwärtigen Regierung zeigen.

Solntsevskaya und Dolgopruadnanskaya sind die zwei größten Mafia-Organisationen in Russland, die sich der Internetkriminalität widmen (S. 8). 25 Prozent der Absolventen der russischen Wissenschafts- und Technologie-Studiengänge bieten sie einen Job. Daneben wurden auch besondere Shkola Hackerov eingerichtet ("Hacker-Schulen"), in denen das Hacking unterrichtet wird. Ihre Teilnehmer können am Ende zwei bis drei Mal mehr als mit ehrlicher Arbeit verdienen.

Vor dem Entstehen von Filesharing-Plattformen (Peer to Peer, P2P) hatten sich verschiedene Mafia-Gruppen auf den Vertrieb „schwarz“ gebrannter Software und Musik-CDs spezialisiert. Immer noch bevorzugen viele Internet-Nutzer einen Kauf zu geringeren Preisen als im regulärem Handel. Sie nutzen zahlungspflichtige – manchmal illegale – Plattformen, deren Preise bei der Hälfte oder einem Drittel der Ladenpreise liegen. Ihr professionelles Aussehen lässt erwarten, dass Sie von leistungsstarken und gut strukturierten Organisationen stammen (S. 21).

Das gilt zum Beispiel für die AllofMP3-Website mit Sitz in Russland, die von Mediaservices betrieben wird. Auf Druck der Musik-Händler musste sie schließen, worauf schnell eine andere Seite mit fast gleichem Namen entstand, die auch alle Kundenkonten der geschlossenen Seite übernahm. Laut London TimesOnline verfügte sie über 5,5 Millionen Kunden und erzielte einen Umsatz von 30 Millionen US-$ (S. 22).

Illegale Kopien beschränken sich nicht auf die kommerzielle Software. Auch böswillige Programme wie MPack, Icepack und FirePack, wurden kopiert und in andere Sprachen übersetzt, bevor sie von Fälschern weiterverkauft wurden (S. 22).

2.2 Asien

Die chinesischen Triaden sind eine der ältesten Mafia-Strukturen in der Welt. Ihr Ursprung kann mindestens bis 1644 zurück verfolgt werden. Sie entstanden aus Geheimbünden und Mönchsorden, die gegen die Invasion von Mandschu-Stämmen Widerstand leisteten (S. 5). Später wandten sie sich in den politischen und kriminellen Untergrund. Unter dem Eindruck einer unerbittlichen Hierarchie sind die Triaden jetzt weltweit am Drogenhandel, bei Schleusungen, an der Piraterie im Zusammenhang mit Audio- und Videokassetten, der Prostitution und Pornographie (auch im Videohandel), am Zinswucher, illegalem Glücksspiel und an Erpressungen beteiligt.

Die Triaden haben vor allem moderne Formen der Erpressung eingeführt: Lösegeldforderungen gegen kommerzielle Webseiten im Zusammenhang mit distributed Denial of Service (DDoS)-Attacken (S. 8). Daneben rüstet seit etwa zehn Jahren auch die chinesische Regierung zum Cyberwar auf, so dass in den USA die Meinung herrscht, China wolle seinen technologischen Rückstand mit den Mitteln des Cyberwars aufholen.

Auch die japanischen Verbrechersyndikate, die Yakuzas, blicken auf eine lange Tradition als Bruderschaften von Straßenhändlern, professionellen Spielern und Ausgestoßene aus der japanischen Gesellschaft zurück, die während der Meiji-Zeit entstanden (1868-1912). In den vier Jahrzehnten nach dem zweiten Weltkrieg erlebten sie neuen Wohlstand aufgrund ihrer Nähe zu den politischen Machthabern. Sie zeigen eine starke, eher symbiotische Einbindung in die Gesellschaft und ihre Einnahmen erzielen sie besonders Handel mit Amphetaminen, Zinswucher, Diskotheken, Glücksspiel, Waffenhandel und Erpressung. Sie waren in die Skandale im Zusammenhang mit den Bankenkrisen in den 1990-er Jahren verwickelt und halten sich seit einem Gesetz von 1992 mehr diskret im Hintergrund. In Bezug auf die Cybercrime sind die Yakuzas besonders bei der digitalen Pornographie und gefälschten CDs, DVDs und Video-Spiele aktiv (S. 9).

2.3 Italien

Der Begriff „Mafia“ ist in Italien seit 1863 überliefert (S. 6). Heute besteht die italienische Mafia aus vier kriminellen Gruppen, die jeweils in einer bestimmten Region angesiedelt sind: die Cosa Nostra in Sizilien, der Camorra in Campania, die N'drangheta in Kalabrien und die Sacra Corona Unita in Apulien. Sie sind in Familien und Clans organisiert und erzielen ihre Einnahmen vor allem aus dem Drogenhandel, der Erpressung, Entführungen gegen Lösegeld, dem Zigarettenschmuggel, Betrug bei öffentlichen Ausschreibungen, durch gefälschte Luxusgüter, Schleusungen, und dem Waffenhandel.

Bereits 2000 sollen drei Viertel des Marktes mit Musik-Raubkopien in der Hand der Organisierten Kriminalität gewesen sein, allen voran der Camorra [18]. Am 20. September 2000 durchsuchte die Mafia-Polizei in Neapel eine Fabrik, die voll mit CD-Rs, mit fast 120 Brennern, 15.000 Jacken, 10.000 CDs und 10.000 Hüllen war (S. 9) [19].

2.4 Nordamerika

Die USA leiden besonders darunter, dass sich kriminelle Gruppen aus allen Teilen der Welt in ihnen niedergelassen haben, darunter russische, japanische, chinesische, italienische, kolumbianische und mexikanische Organisationen.

Zwanzig bis fünfundzwanzig Familien aus der sizilianischen Cosa Nostra sind spätestens seit 1931 unter der Führung von Lucky Luciano in den USA tätig (S. 6). Allein fünf Familien sollen in New York ansässig sein, alle übrigen einzeln in „ihren“ Städten in den USA und zwei Familien in Kanada.

Trotz langer Zurückhaltung leistet die Mafia noch immer einen erheblichen Beitrag zur Organisierten Kriminalität. Sie erzielt ihre Einnahmen besonders aus Erpressungen, Finanzbetrug, Zinswucher, ihrer Kontrolle über die Bauindustrie und andere öffentliche Märkte, dem Glücksspiel, der Prostitution und Pornographie und nicht zuletzt aus den Erträgen aus ihren Investitionen in der legalen Wirtschaft.

Bereits zwischen 1996 und 2002 verdienten mehrere Mitglieder der Gambino-Familie an betrügerischen Internet-Angeboten – vor allem an Pornoseiten – mehr als 750 Millionen US-$. Sie gestanden 2005, von den Besuchern der kostenlosen Seiten als Altersnachweis Kreditkartendaten verlangt und dann missbraucht zu haben (S. 9).

Online-Wetten haben in den englischsprachigen Ländern schnell Eingang in das Internet gefunden und Verbrecher angezogen. Im Mai 2007 beschuldigte die Justiz in New-Jersey die Familien Gambino und Lucchese des illegalen Glückspiels im Zusammenhang mit der Internetseite Topbetters .com. Dort wurden seit 2002 Sport-Wetten und Casino-Spiele aus dem Ausland angeboten. Im Mai 2008 erfolgten deshalb zehn Verhaftungen.

Am 18. Februar 2009 erklärte sich Nicholas "Nicky the Hat" Cimino (im Alter von 49) vor einem Gericht in Pennsylvania des Zinswuchers und des illegales Glücksspiels schuldig. Als Kopf der Organisation erzielte er mit der Unterstützung der Philadelphia-Mafia-Familie einen kriminellen Umsatz von monatlich rund 1 Million US-$. Das Netzwerk für illegale Wetten und Glücksspiel weitete sich bis nach Kalifornien aus und betrieb auch eine nicht genannte Offshore-Website [20].

Ähnliche Nachrichten zeigen, dass der Cosa Nostra nicht mehr nur mit Drogen handelt oder Erpressungen durchführt. Die heutige Mafia setzt neue Technologien ein, um Millionen von Dollar zu stehlen. In Kanada verdiente die Mafia zwischen 2005 und 2006 binnen 18 Monaten 26 Millionen Dollar mit betwsc.com, einer illegalen Seite für Sportwetten. Der Server befand sich in Belize und

[18] Armenien (93 %), Bangladesch und Aserbaidschan (jeweils 92 %) hatten 2008 die weiteste Verbreitung von Software-Raubkopien. In Russland waren es 73 %, in Westeuropa rund 36 % und in Nordamerika etwas mehr als 20 % (Zahlen der BSA, S. 20 f.).

[19] Musik- und Film-Raubkopien sind kein Geschäft mehr für die Mafia, seitdem es die Peer-to-Peer-Netzwerke gibt, die den Geschäftszweig übernommen haben (S. 21).

[20] Der Begriff Offshore wird in diesem Zusammenhang so verwendet, dass Standorte und Firmensitze in Staaten verlegt werden, die geringe Steuern und keine Staatsaufsicht versprechen.

später in der indianischen Reservation of Kahnawake, westlich von Montreal in Québec. Die wichtigste Person hinter der Betrug soll einen persönlichen Gewinn von 17 Millionen C-$ erzielt haben.

2.5 Lateinamerika

In Mittelamerika sind kriminelle Gruppen besonders in Mexiko und Kolumbien aktiv (S. 6). Sie handeln vor allem mit Kokablätter aus Peru und Bolivien als Grundstoffe für das in Kolumbien produzierte Kokain, das sie dann über Mexiko zu den Absatzmärkten in den USA schmuggeln.

Nach dem Verschwinden der Medellin-Kartell-Führer und nachdem ein Führer des Cali-Kartells verstorben ist, hat sich die Situation in Kolumbien geändert. Seither sind kleine und mittlere Kokain-Unternehmen entstanden, die nahtlos in das Wirtschaftsgefüge integriert sind und verdeckt hinter legalen Unternehmen handeln. Ihre Chefs, meistens junge und diskrete Geschäftsleute, vermeiden das Aufsehen durch einen übermäßig auffälligen Lebensstil oder Mordserien. Ihr Geschäft setzt Schweigen voraus. In den Wäldern betreiben die revolutionären Streitkräfte Kolumbiens (FARC) und die National Liberation Army (ELN) Laboratorien. Ihre Guerillas wurden für den Drogenhandel umgeschult.

Trotz mehrerer Verhaftungen florieren die mexikanische Kartelle. Sie scheuen sich nicht, Druck gegen die Regierung auszuüben und die Polizisten und Staatsanwälte zu ermorden, die sie verfolgen. Sie sind besonders aktiv beim Schmuggel, den Schleusungen, dem Handel mit Kokain und der Herstellung von Marihuana und von synthetischen Drogen.

2.6 Nigeria und Elfenbeinküste. Simbabwe

Kriminelle Organisationen aus Nigeria beherrschen einen wesentlichen Teil des weltweiten Handels mit Drogen aus Afrika (S. 7).

Nigerianische Täter sind seit Jahrzehnten in einer besonderen Form des Betruges tätig, dem Vorauszahlungsbetrug, dem der einschlägige Paragraph des nigerianischen Strafgesetzbuches einen international anerkannten Namen gab: 419 fraud. Hierzulande spricht man von der ▸ Nigeria Connection.

In Simbabwe im südlichen Afrika finden wiederholt politische Konflikte statt (S. 11). Zwischen 2005 und 2008 war Robert Mugabes Partei an der Macht und wurden die Oppositionsparteien zum Schweigen verpflichtet. Während dieser vier Jahre waren Gegner des Regimes verantwortlich für viele Website-Defacements und DDoS-Angriffe.

3. internationale Netzwerke

Neben der Mafia sind auch internationale Netzwerke und gemischten Gruppen tätig, die sich teilweise nur wenige Monate, manchmal aber auch jahrelang halten (S. 9).

Der TJX-Fall ist dafür ein Beispiel: Zwischen 2005 und 2007 wurden von 94 Millionen Kunden dieses Unternehmens aus Nordamerika und Großbritannien die Kreditkarten-Nummern gestohlen. Im August 2008 wurden elf Personen verhaftet, darunter drei US-Bürger, ein estnischer, zwei chinesische, ein weißrussischer Täter und drei Ukrainer. Nach Medienberichten waren sie Teil eines internationalen Hacker-Netzwerks, das in das Funknetzwerk (Wi-Fi) und in die Daten der leitenden Angestellten eingedrungen waren. Einige ihrer Hacker sind zu den Daten der Vermittler auf der obersten Ebene vorgedrungen. Nach dem Vorbild von CarderPlanet wurden die gestohlenen Daten in Carding-Foren als vollständige Dumps [21] angeboten. In diesen Foren wurden auch gefälschte Pässe, Reiseschecks und Schul-Diplome gehandelt. Die bekanntesten Boards sind Mazafaka (mehr als 9.000 registrierte Mitglieder), ShadowCrew (mehr als 4.000) und DarkMarket (mehr als 2.000). Noch in 2009 wurden 130 Millionen Datensätze angeboten, die 2007 gestohlen worden waren.

Groß angelegte Betrügereien verlangen nach Leu-

[21] „Dump“ ist der vollständige Datensatz einer Kreditkarte einschließlich Geltungsdauer und Prüfziffer.

ten, die sich auf die Verwendung von gefälschten Kreditkarten spezialisiert haben [22]. Solche Gruppen treffen gezielt zusammen und lösen sich auf, sobald sie bemerkt werden. Im März 2007 verfolgte die Polizei in Florida eine solche Gruppe und verhaftete mehrere ihrer Mitglieder. Sie hatten in Elektronik-Fachgeschäften und bei Juwelieren mithilfe von Geschenk-Gutscheinen Waren im Wert von mehr als 225.000 US-$ eingekauft [23]. Die Gutscheine hatte ein Partner geliefert, der sie zuvor mit gefälschten Kreditkarten erworben hatte. Im Juni 2007 wurde eine andere Gruppe verhaftet, die mehr als 200.000 Kreditkarten von TJX und Polo Ralph Lauren besaß.

4. Politischer Aktivismus und Hacktivitäten

"Aktivismus" bedeutet in Pagets Bericht eine politisch motivierte und direkte Aktion, die im Einzelfall auch gesetzwidrig sein kann. Beispiele dafür sind die Greenpeace-Aktivisten, die auf dem Meer Walfänger blockieren, oder die Jugendlichen, die 2008 versuchten, die olympische Flamme während ihrer Welt-Tournee zu löschen. Gelegentlich werden auch die Aktionen der ETA in Spanien oder der Roten Brigaden in Italien als Aktivismus angesehen, obwohl sie mehrheitlich als Terroristen betrachtet werden (S. 10).

Obwohl der finanzielle Gewinn die wichtigste Motivation für die Internetkriminalität ist, haben einige Gruppen von Computer-Hackern andere Motive. Sie lassen sich von wirtschaftlichen, politischen oder religiösen Interessen leiten, die im Allgemeinen über nationale Grenzen hinausgehen. Ihre Aktionen nennt Paget Hacktivismus, also eine Verbindung aus Hackern und Aktivismus [24].

Wenn eine Hacktivismus-Aktion in der Lage ist, Ängste zu wecken, dann nennen wir das Cyberterrorismus (S. 12), sagt Paget. Offiziell wird Cyberterrorismus definiert als ein "bewusster Akt der Zerstörung, der Kompromittierung [25] oder Änderung von Daten, der Informationsflüsse oder Computersysteme, die für die Regierungen oder Unternehmen für das reibungslose Funktionieren unerlässlich sind [26], der Schaden oder Angst aus politischen, religiösen oder ideologischen Gründen verursacht“. Angriffe, durch die die Elektrizität für mehrere Tage ausfällt oder die Börsendaten zerstören, können zweifellos Ängste auslösen. Solche Angriffe haben wir bislang nicht festgestellt.

Der Begriff „Hacktivism“ wurde 1996 von der Gruppe „Cult of the Dead Cow“ entwickelt (S. 11, 16). Diese legendären Gruppe von Hackern wurde 1984 in Lubbock, Texas gegründet. Ihre Hacktivisten infiltrieren Netzwerke und setzten ihr Können zu Computerangriffen, zur Piraterie, Entführung von Servern und dazu ein, ideologisch geprägte Homepages mit anderen Inhalten zu versehen. Die militanten Hacker wenden sich gegen reaktionäre Meinungsmacher, gegen Scientology, gegen Webseiten der Regierung und gegen große Internet-Unternehmen, denen sie Datenmissbrauch und Geschäftemachereien vorwerfen [27]. Sie blockieren und verunstalten Webseiten, um eine starke Medienaufmerksamkeit zu erregen. Eine bestimmte Nachricht zu verbreiten liefert ihnen häufig nur einen Vorwand für Wettstreite, binnen kürzester Zeit die meisten Webseiten zu verunstalten.

Die Aktivisten vom „Cult“ verurteilten 2006 die Zensur in China (S. 16). Regelmäßig bieten sie neue Werkzeuge zur Erkennung von Schwachstellen [28] an und verteilten im Februar 2008 den GoolagScan, der Webseiten automatisch auf Schwachstellen und Lecks für vertrauliche Informationen prüft.

---

22 Im Zusammenhang mit dem Skimming hat sich dafür der Begriff Cashing eingebürgert.

23 Eine Grafik auf S. 10 zeigt die Einkaufs-Tour der Täter und die von ihnen verursachten Schäden.

24 In einer Tabelle auf S. 18 fasst Paget die wichtigsten Cyberangriffe zwischen 2003 und Anfang 2009 zusammen.

25 Im Original: Degradation (Erniedrigung).

26 In Deutschland würde man von Kritischen Infrastrukturen sprechen.

27 Mit diesem Satz bin ich inhaltlich von Pagets Vorlage abgewichen.

28 Verstärkt werden nicht Betriebssysteme und Anwenderoberflächen angegriffen, sondern Anwenderprogramme; siehe die Listen S. 30, 31.

4.1 Osteuropa

Obwohl das Phänomen der DDoS-Angriffe seit mehr als fünfzehn Jahre bekannt ist, erlangte es erst 2007 durch den Hacktivismus-Angriff gegen Estland eine weltweite Beachtung (S. 11). Trotz gegenteiligter Beteuerungen fiel der Verdacht schnell auf russische Nationalisten, die vom Kreml unterstützt wurden. Im März 2009 übernahmen ein Duma-Abgeordneter und Konstantin Goloskokov, ein 22-jähriger Aktivist, die Verantwortung für die Aktion. Goloskokov verweigert den russischen Behörden kategorisch jede Unterstützung. Allerdings ist seine Zusammenarbeit mit Nashi bekannt, einer antifaschistischen Jugendgruppe. Die manchmal gewalttätige Organisation geht auf eine Initiative von Vladimir Putin aus dem Jahr 2005 zurück und muss als regierungsnah angesehen werden.

Die Angriffe gegen Estland veranlasste die NATO im Mai 2008 dazu, ein Cyberdefense-Zentrum in der estnischen Hauptstadt zu errichten.

In 2008 litten Litauen und Georgien unter Angriffen wegen ihrer Auseinandersetzungen mit Russland. Ein weiterer DDoS-Angriff richtete sich gezielt gegen Radio Free Europe, dessen Programme von den USA gefördert werden.

4.2 China

China beheimatet mehrere Gruppen von jungen Hackern, die in IT-Systeme eingedrungen sind und Webseiten geändert haben. Sie sind bekannt als die Red Hacker Alliance, China-Eagle-Union, Green Army und Honker Union von China. Viele offizielle US-amerikanische Webseiten, aus Taiwan und aus Japan wurden wiederholt aus Südostasien angegriffen. Ihre Zusammenhänge mit der chinesischen Regierung sind schwer nachzuweisen. Die Geschichte von Peng Yinan erregte jedoch unsere Aufmerksamkeit. Im Jahr 2000 gründete er zusammen mit einem anderen Hacker „Javaphile“ und übernahm die Verantwortung für DoS-Angriffe gegen die Webseite des Weißen Hauses im Mai 2001. Peng wurde dafür nie zur Rechenschaft gezogen und scheint heute ein Berater für Shanghais Behörde für öffentliche Sicherheit zu sein.

China ist geprägt von Handlungsaufrufen vieler bekannter und unbekannter Gruppen, die ihre Liebe zu ihrem Land hervorheben und sich gegen anti-chinesische Bestrebungen wenden (S. 16). Das war auch der Fall während der Olympischen Spiele im April 2008, als die chinesische Gruppe Revenge of the Flame beschloss, die Website CNN.com anzugreifen, um die Sache Tibets zu unterstützen. Die Aktion scheiterte an den getroffenen Schutzmaßnahmen [29].

Mit etwa 300 Millionen Internet-Nutzern verfügt China heute über eine wahre Streitmacht von Cyberkriegern (S. 17). Ihre Rekrutierung begann zwischen 1995 und 1997, als die erste Gruppe von Hackern aufgetauchte und auf der Website Voice of the Dragon versuchte, sie zusammenzubringen. Seit 1998 haben sich viele Gruppen der Red-Hacker-Alliance angeschlossen, deren Ziel es ist, alle Gruppen zu vereinen, von denen einige 20.000 bis 80.000 Fans haben. Die ersten strukturierten Angriffe fanden gegen die Websites der indonesische Regierung als Reaktion auf Anti-chinesischen Unruhen statt. Im April 2008 verkündete die Gruppe, dass sie 300.000 Mitglieder habe. Drei große Fraktionen sind bekannt:

⇨ Die Green Army wurde 1997 von einem Hacker gegründet, der als Goodwell bekannt ist (richtiger Name: Gong Wei). Die Gruppe soll mehr als 3.000 Mitglieder haben und "unzählige ausländische Webseiten" gehackt haben. Im Verlauf der Zeit spaltete sich die Green Army in zwei Fraktionen auf. Während die eine dem Meinungsaustausch und dem Hacking treu blieb gründete die andere die Firma NSFOCUS. Dieses Unternehmen veranstaltet eigene Diskussionsforen (isbase.com) und hat mehr als 56.000 Abonnenten.

⇨ Die Honker Union of China tauchte im Jahr 2000 unter der Führung von Lion auf (richtiger Name: Lin-Yong). Ihre Ziele sind der "Schutz der nationalen Souveränität" und die Aufrechterhaltung des Friedens und der Gerechtigkeit. Seit

[29] Paget zitiert an dieser Stelle eine Presseerklärung der Gruppe im Volltext.

2001 ist die Union für ihre regelmäßigen Angriffe gegen amerikanische und westliche Webseiten bekannt. Im Mai 2008 griff sie die regimekritische Webseite Tsering Woeser aus Tibet an.

⇨ Die China Eagle Union wurde 2004 von Wan Tao gegründet. Der Name soll zurückgehen auf den Song "Hotel California" von den Eagles. 2007 erklärte Wan, dass sich die Organisation vor allem der "Förderung der Informationssicherheit" in China widmet. Es scheint, dass die Hacker bei Eagle nur widerwillig mit der chinesischen Regierung zusammen arbeiten.

5. Defacer und andere

Viele Gruppen versuchen, fremde Webseiten zu verändern und damit eine eigene Botschaft zu vermitteln (S. 13). Sie verwenden dazu häufig Bilder oder Symbole, die sich auf den Tod beziehen (z. B. einen Schädel) oder auf das Land (eine Flagge), auf das der „Defacer“ stolz ist. Jeden Monat identifiziert die Website Zone-H mehr als 2.500 solcher Angriffe.

Türkische Nationalisten sind besonders aktiv bei der Verunstaltung von Websites (S. 12). Sie entfalten große Aktivitäten im Web und erheben den Anspruch, aus vielen Gruppen zu bestehen. Während der Fußball-Europameisterschaft Im Juni 2008 änderten sie viele Websites aus den Ländern, gegen die ihre Nationalmannschaft spielte, fügten türkische Flaggen ein und hinterließen manchmal unverständliche Sprüche. Im Mai 2009 drangen die gleichen Gruppen erfolgreich in einige Webserver des US-Verteidigungsministeriums ein.

Die Kosova-Hacker-Gruppe nutzt bevorzugt einen Fehler in Joomla für ihre Angriffe (S. 13).

Seit mehreren Jahren kämpft die Gruppe Whackerz Pakistan gegen indische Interessen (S. 15).

Viele andere Bewegungen verbreiten ihre Ideen im Internet jedoch ohne verwerfliche oder kriminelle Aktionen. In Kolumbien betreibt Oscar Morales eine Facebook-Gruppe, um eine Million Stimmen gegen die FARC zu sammeln. Die Gruppe fordert die Community auf, Gewalt und Extremismus anzuprangern. Mitte Juni 2009 hatten fast 445.000 Menschen die Gruppe besucht.

5.1 Israel und Palästina

Das marokkanischen Team Evil hat sich auf Angriffe gegen israelische und amerikanischen Websites spezialisiert und verbreitet seit 2004 pro-palästinensische Nachrichten (S. 13, 14). Einer seiner Mitglieder sagte einer großen israelischen Nachrichtenagentur: "Wir sind eine Gruppe von marokkanischen Hackern die Site Hacks als Zeichen der Solidarität mit dem Widerstands gegen Israels Krieg durchführt. Wir greifen jeden Tag israelische Websites an; das ist unsere Pflicht. Hacking ist kein Verbrechen. Beendet das Töten der Kinder und wir beenden das Hacking." Im Januar 2009 brach die Gruppe Jurm-Team in die Ynet-Seite ein, die englische Version der israelischen Online-Zeitung Yedioth Aharonoth. Über die Vielzahl pro-palästinensischer Gruppen gibt die Website Arabisch-m.de Auskunft.

Die israelische Gruppe Team Good reagierte seit 2006 auf einige Angriffe vom Team Evil. Es beschädigte den Server des marokkanischen Hostproviders Omihost.com (Multimedia Studios), wo alle Kundendaten verloren gingen.

Das Defacement ist nur ein Teil des Hacktivismus. Ein freiwilliges Botnet wurde von einer Gruppe (The Patriot Team) im Dezember 2008 während des militärischen Konflikts in Gaza eingerichtet, um Angriffe gegen pro-palästinensische Webseiten durchzuführen und damit Israel zu unterstützen.

5.2 Spaßhacker. Informationsfreiheit und -sicherheit

Nur ein Teil der Defacements hat einen ideologischen Ursprung. Andere scheinen aus Spaß oder bei sich bietender Gelegenheit ausgeführt zu werden. Das gilt etwa für die veränderten Presseerklärungen der Schweizer Stadtpolizei in Zürich und die Webseite des europäischen Kernfor-

schungszentrums, die 2008 gehackt und abgeändert wurden (S. 19).

Andere Gruppen sehen sich als Kämpfer für die Informationsfreiheit. 1981 wurde in Deutschland von Hackern, Programmierern und anderen Enthusiasten der Chaos Computer Club gegründet. Der Club erlangte 1984 die Aufmerksamkeit der Medien, weil er erfolgreich 135.000 DM von einer Sparkasse in Hamburg auf sein eigenes Bankkonto verschob. In 1998 demonstrierte die Gruppe, dass ein Mannesmann-Handy mit dem GSM card identification code, der mit dem Comp128-Algorithmus verschlüsselt ist, geklont werden kann. Im Jahr 2004 veröffentlichte der Club mehrere Schwachstellen im OBSOC System der Deutschen Telekom, die nur mit erheblichem personellen und finanziellen Aufwand geschlossen werden konnten. 2006 demonstrierte die Gruppe, wie einfach es ist, die Nedap-Wahl-Computer zu manipulieren, die in Deutschland für die elektronische Stimmabgabe verwendet werden sollten.

Heute setzt sich der Chaos Computer Club verstärkt für die Informationsfreiheit und unüberwachte Kommunikation ein. Er wendet sich aktiv an die Medien und ihm wird einiger politischer Einfluss nachgesagt [30].

Pirate Bay betreibt eine der weltweit größten kostenlosen File-Sharing-Seiten (S. 16). Bis Juni 2009 galt sie als eine obskure Gruppe von Aktivisten und als Einzelerscheinung. Nachdem im April 2009 vier ihrer führenden Leute zum Abschalten des BitTorrent-Servers verurteilt wurden, stieg die Popularität der Partei sprunghaft an. Sie erhielt in Schweden 7,1 Prozent der Stimmen und Sitze im Parlament. Dort spricht sie sich für die Abschaffung der Urheber- und Patentrechte sowie gegen die Überwachung im Internet aus.

[30] Paget sieht die Rolle des CCC sehr skeptisch, wenn er zum Beispiel ausführt, dass die Schließung veröffentlichter Sicherheitslücken der DTAG viel Geld gekostet hat. Dem CCC ist jedoch zuzubilligen, dass er keine kriminellen Aktionen durchgeführt hat, die andere nachhaltig geschädigt haben.

Dafür hat der CCC einige Anerkennungen bekommen. Sowohl im Zusammenhang mit der Onlinedurchsuchung als auch wegen der Vorratsdatenspeicherung hat das BVerfG seine Stellungnahmen eingeholt und über sie ausführlich referiert.

5.3 Online-Spiele. Glücksspiel

Der globale Markt für online-Glücksspiele boomt und die Wachstumsaussichten sind schwindelerregend. 12 Milliarden US-Dollar der Umsätze stammten 2005 aus den USA, die knapp die Hälfte des Marktes bestellen dürfte. Rund 2.000 Unternehmen sind beteiligt und die bekanntesten stammen aus Großbritannien, Österreich und Schweden (S. 22).

Die Finanzanalysten von Christiansen Capital Advisors erwarteten für 2006 einen Umsatz bei den Online-Glücksspielen von 15 Milliarden US-$ und 2010 von 24 Milliarden US-$. Noch optimistischer sagen die Analysten bei Merrill Lynch Brutto-Eimnmahmen von 150 Milliarden US-$ im Jahr 2015 durch Online-Sportwetten voraus.

Die französische Sicherheitsorganisation CERT-LEXSI zählte 2006 aufgrund einer semantischen Analyse von 70 Millionen aktiven Internetseiten 300.000 Seiten mit Bezug zu Online-Glückspielen. Die meisten davon waren nur Verzeichnisse oder boten Bewertungen von anderen Seiten an. Eine detaillierte Studie fand schließlich 14.823 aktive Online-Glücksspiel-Seiten. Nur 1.858 sind lizensiert, fast 90 % werden illegal betrieben (S. 23).

Hinter diesen Seiten verbergen sich viele Glücksspiel-Unternehmer, die schnell reich werden wollen und andere kriminelle Aktivitäten wie Geldwäsche, Phishing und andere Arten von Finanzbetrug betreiben. Die Seiten sind alle anonym registriert. Die finanziellen Transaktionen wickeln sie über anonyme Offshore-Bankkonten oder virtuelle Zahlungssysteme wie PayPal, eGold, NetTeller oder WebMoney ab (S. 23).

Die meisten der großen russischen Schurkenprovider, die wir zum Beispiel als Russian Business Network oder Yambo Financial kennen, begannen ihre kriminellen Aktivitäten mit Kinderpornographie und Online-Casinos.

Neben Online-Spielen ziehen die Online-Wetten, andere Betrüger an. Sie bieten vor allem traditio-

nellen Mafiaorganisationen an, schmutziges Geld zu waschen, finanzielle Verluste zu verdecken und die Aufmerksamkeit der Steuerbehörden zu vermeiden. Die Spieler, die ihnen zum Opfer fallen, bleiben meistens auf den nur versprochenen Gewinnen sitzen.

6. Computer Underground

Seit dem Auftreten der ersten Malware bis vor drei bis vier Jahren haben sich viele Gruppen der Entwicklung von Computer-Viren gewidmet. Sie haben ihre Kreationen aber nicht verkauft, sondern behauptet, ausschließlich Forschung zu betreiben. Sie entwickeln neue Techniken zur Tarnung und Verbreitung von Malware und nutzen dazu Schwächen in Security-Produkten. Dafür werden sie häufig als verantwortungslos angesehen (S. 23).

Gruppen von Hackern ohne klare finanzielle oder politische Motive sind heute weniger geworden als in der Vergangenheit [31]. In Russland mutzen viele Hacker die Zeitschrift Website-xakep.ru. In den Vereinigten Staaten meldet das 1984 gegründete 2600-Magazine seinen Lesern monatlich Treffen in vielen Ländern. Auch in China melden Zeitschriften und ihre Websites Trefforte. Die größten sind HackerXfiles und Hacker Defense Online.

Eine führende Gruppe wurde als 29A bekannt (666 in hexadezimalem Code). Sie entstand 1995 und ihre Mitglieder in West- und Osteuropa sowie in Südamerika wurden zur Quelle bösartigen Codes wie WM/Cap, W32/Donut, W2K/Stream, W64/Rugrat, SymbOS/Cabir. Die Gruppe kündigte im Februar 2008 das Ende ihrer Tätigkeit an.

Das C. Rufus-Security-Team besteht aus fünfzehn Mitgliedern. Ihm wird nachgesagt, den Trojaner für das Ghostnet-Spy-Netzwerk entwickelt zu haben. Ein weiteres Beispiel ist die schwedische Websei-

[31] Bolduan 2008: „Keiner hackt mehr heute zum Spaß, das ist knallhartes Business geworden.“
Als ein Beispiel für etablierte Hacker zitiert Paget beginnend auf S. 23 einen Artikel aus LeMonde über das Metalab in Wien. Siehe insoweit „Metalab“ und „Hackerspace“ in der Wikipedia.

te SweRAT. Eines ihrer Mitglieder verwendet das Pseudonym "shapeless offers Poison Ivy" [32].

7. Bulletproof Hosting

Die Rede vom „kugelsicherem“ Hosting ist unweigerlich mit dem Russian Business Network - RBN - verbunden [33]. Die in diesem Geschäft tätigen Schurkenprovider schotten ihre Kunden von der Strafverfolgung und anderen kritischen Nachfragen ab, indem sie Auskünfte über sie verweigern, getarnte Speichertechniken anbieten, Server maskieren und blockieren sowie Scheinfirmen betreiben. Ihr Geschäftsmodell ist einfach: Je mehr kritische Fragen ankommen, desto teurer wird es für die Kunden [34]. Paget steuert die Auskunft bei, dass die Kunden monatlich im Durchschnitt etwa 600 US-$ bezahlen mussten (S. 26). Als Ende 2007 der Druck gegen das RBN zu groß wurde und es seine Repräsentanz in Petersburg auflöste, fanden seine Kunden schnell andere Anbieter, zum Beispiel die Abdallah Internet Hizmetleri in der Türkei (S. 27).

Seit 2008 gerieten einige andere Hosting-Unternehmen unter Verdacht, von denen einige ohne Vorwarnung vom globalen Netz getrennt wurden: Im Mai 2008 wurde der CEO des Registrars Dynamic Dolphin, Scott Richter, als notorischer Spammer enttarnt. Er stellte seine Tätigkeit ein. Am 21.09.2008 sperrten die großen Carrier Atrivo/Intercage wegen Spam-Aktivitäten von ihren Netzen aus (S. 27). Im September 2008 wurde auch Di-

[32] Paget nennt weitere, aber wenig aussagekräftige Beispiele. Zu den kriminellen Foren bemerkt er später (S. 31), dass sie vorsichtiger geworden seinen und – mit meinen Worten – die Zwiebelschalen-Strategie anwenden. Sie betreiben einen öffentlichen Marktplatz, auf dem sich jeder äußern kann. Zur Sache geht es jedoch erst im abgeschotteten Bereich, zu dem nur vertrauenswürdige Mitglieder Zutritt haben. Ihm folgen meistens noch weitere, mehr vertrauliche Gemächer, die noch weiter von dem Zugriff der Strafverfolgungsbehörden abgeschottet sind.

[33] Siehe: CF, Schurken-Provider und organisierte Cybercrime, 13.07.2008; CF, Russian Bussiness Network, 13.07.2008.

[34] Balduan 2008.

recti verdächtigt, eine große Anzahl illegaler Seiten – vor allem für gefälschte Arzneimittel – zu betreiben. Das Unternehmen kooperierte und nach sechs Monaten waren 75 Prozent der beanstandeten Angebote verschwunden (S. 28).

Wegen seiner verdächtigen Zusammenarbeit mit Atrivo entzog die Internet Corporation for Assigned Names and Numbers – ICANN – im Oktober 2008 dem estnischen Unternehmen EstDomains die Zulassung als Domain Name-Registrar. Wenig später wurde der Unternehmensleiter, Vladimir Tastsin, in Estland wegen Bankbetruges verurteilt (S. 29).

Am 10.11.2008 verschwand der Provider McColo aus dem Internet, nachdem dieses berüchtigte US-Unternehmen vor allem mit Spam-Mails, Verbreitung von Botnetz-Loadern und Malware für DDoS-Angriffe bekannt und von den großen Carriern abgeschaltet wurde. Seither verzeichnen verschiedene Quellen, u.a. SpamCop, einen Rückgang von 35 bis 50 Prozent der weltweiten Spam-Menge (S. 29).

Im August 2009 wurde die Real Host Ltd. [35] wegen kriminellen Aktivitäten verurteilt. Das Unternehmen hatte eine Vielzahl von Internet-Adressen von einem Service-Anbieter in Riga, Lettland, gemietet. Damit wurden Server angesprochen, die das Zeus-Botnet steuerten, Hostspeicher, deren Seiten eine Schwachstelle im Adobe Flash-Player angriffen, und Dropzones, auf denen gestohlene Bankdaten und „Maultiere“ [36] angeboten wurden. Der Provider ist jetzt vom Netz getrennt (S. 29).

Kürzlich hat die US-Verwaltung Pricewert gebeten, die Tätigkeit einzustellen. Das Unternehmen ist auch bekannt als 3FN, APS-Telecom und APS Communications. Dieser Serviceprovider (ISP [37]) hat seinen Sitz in Belize und seine osteuropäischen Besitzer werden beschuldigt, alle möglichen kriminellen Aktivitäten mit den in Kalifornien betriebenen Servern zu ermöglichen.

Rechtliche Schritte gegen Internet-Verbrecher sind selten und langwierig. Mit Ausnahme der Maßnahmen gegen EstDomains und Pricewert scheinen andere Verdächtige nicht sehr besorgt zu sein. Wenn ein ISP getrennt ist, kann er zweifellos seine Geschäfte an anderer Stelle und unter anderem Namen fortsetzen. Die Beispiele zeigen, dass die Kampagnen von Forschern und Journalisten gegen einzelne Schurkenprovider in ihrer Wirksamkeit begrenzt sind.

Auch anderen Hostprovidern wird die Komplizenschaft oder mangelnde Aufsicht über gehostete Inhalte angelastet (S. 30) [38]:

- Xin Net
- eNom
- Network Solutions
- Register.com
- Planet Online
- Regtime—1st Russian registrar to make the list
- OnlineNIC
- Spot Domain/Domainsite
- Wild West Domain
- HiChina Web Solutions

8. kriminelle Methoden

8.1 Sicherheitslücken und Underground Economy

Jedes Jahr werden mehrere tausend Sicherheitslücken entdeckt. Viele werden veröffentlicht und mit Beispielen bewiesen. Sie zeigen viele Schwachstellen, über die zum Beispiel PCs von infizierten Webseiten aus angegriffen werden können.

Cyber-Kriminelle machen seit Jahren Gewinn damit, dass sie diese Schwachstellen selber nutzen

---

35 Ich habe bei einer kurzen Recherche nicht herausfinden können, wo das Unternehmen tätig gewesen sein soll.

36 „Mules“: Finanz- und andere Agenten für die Beutesicherung.

37 Internet Service Provider, ein leider nichts sagender Begriff, der sowohl für Zugangs- als auch für Hostprovider verwendet wird.

38 antispam.de spricht von beschwerdeignoranten Providern und Hostern.

oder ihr Wissen zusammen mit Anwendungen zu ihrem Missbrauch verkaufen [39]. Im Jahr 2008 bemerkten wir eine Zunahme der Angriffe auf Internet-Nutzer, wobei viele dieser Angriffe auf Sicherheitslücken in Applikationen von Drittanbietern zugeschnitten waren (z. B. QuickTime, Acrobat Reader, Real Media und Flash), die beim Surfen im Internet benutzt werden. Verstärkt werden dazu böswillig veränderte oder nachgemachte Webseiten genutzt, die sich dem Anschein einer „sicheren" Seite geben. Besonders in den ersten beiden Quartalen in 2008 erfolgten Wellen von SQL--Injection-Angriffen, bei denen Hacker binnen weniger Stunden bösartigen Code im Hintergrund von Tausenden von Webseiten einbrachten, um die Computer der Besucher zu infizieren (S. 30) [40].

In den vergangenen vier Jahren hat sich wenig geändert. Spezialisierte Webseiten und Foren fördern weiterhin Crimeware-Angebote und -Dienste. Die einfachsten davon bieten nicht mehr als harmlose Informationen zur ersten Kontaktaufnahme. Die Bemühungen der Strafverfolgungsbehörden haben die Internetkriminelle vorsichtiger werden lassen, weil das FBI mehrere Plattformen geschlossen hat, zum Beispiel von ShadowCrew und DarkMarket (S. 31). Für die kriminellen absprachen werden deshalb in aller Regel zunächst sichere Boards und schließlich verschlüsselte Kommunikationskanäle verwendet. Besonders beliebt in Ost und West ist ICQ [41]. Eine Ausnahme bildet China, wo die Internetkriminellen Web-basierte Bulletin Board Systeme bevorzugen, insbesondere die Baidu Post Bar (post.baidu.com) oder das QQ instant-messaging (S. 32).

[39] Die Rede ist von Exploit-Händlern, die sich auf den Verkauf von Schwachstellen und Software-Modulen zu ihrem Missbrauch spezialisiert haben.

[40] Auf den Seiten 30 und 31 folgen Tabellen, in denen die populären Browser, Applikationen und Kommunikationsanwendungen aufgeführt werden, die den meisten Angriffen ausgesetzt waren.

[41] ICQ ist ein Instant-Messaging-Programm, das seit 1998 vom amerikanischen Onlinedienst AOL angeboten wird.

8.2 Geldwäsche und Geldtransfer

Um kriminelle Gewinne zu sichern bedarf es der Geldwäsche, die meistens in drei Schritten erfolgt:

⇨ erste Sicherung illegaler Gelder auf Bankkonten durch Überweisung oder Bargeldtransfer [42].

⇨ Anlage des Geldes, um seine kriminelle Herkunft zu verschleiern.

⇨ abschließend erfolgt die Einbindung, also eine unverdächtige Transaktion, die die kriminelle Herkunft verdeckt.

Der Internationale Währungsfonds schätzt den weltweiten Anteil der Geldwäsche auf zwei bis fünf Prozent des globalen Bruttoinlandsprodukts, das auf 500 Milliarden bis 1,5 Billionen US-§ geschätzt wird. Davon sollen jährlich in 67 Ländern mehr als 30 Milliarden US-$ über das Internet gewaschen werden.

8.3 Carding

Jeden Tag werden Tausende Informationen über gestohlene, unterschlagene und manchmal auch gefälschte Kreditkarten von Cyberkriminellen verkauft. Meistens werden drei Pakete angeboten:

⇨ ***CC Dump*** [43]. Das sind die auf dem Magnetstreifen gespeicherten Daten einer Kreditkarte [44]. In großen Mengen gekauft, kostet ein einfacher Dump nur etwa 10 Cent (US).

⇨ ***CC full Info***. Hierbei erhält man alle Einzelheiten über eine Zahlungskarte und ihren Inhaber, wobei sich die Art der Daten je nach Anbieter un-

[42] Die Rede ist von „Drops", also unauffälligen, sicheren Konten. Gelegentlich werden sie auch als „Mule Accounts" bezeichnet. „Mule" ist sinnbildlich der Geldesel, der als Finanzagent Gelder weiter leitet.

[43] „CC" dürfte von Carbon Copie abgeleistet sein. Das ist das Mehrstück eines Schreibens, das mit Durchschlagpapier hergestellt wird. „Dump" bezeichnet eigentlich den vollständigen Datensatz auf einer Karte (siehe CC full info) und nicht nur die Informationen auf dem Magnetstreifen.

[44] Ich rede meistens von Zahlungskarten. Sie umfassen sowohl die Kredit- als auch die Debitkarten (z.B. Maestro). Für Dritte unterscheiden sie sich kaum noch, weil sie dieselbe Autorisierung durchlaufen, wenn sie mit PIN eingesetzt werden.

terscheiden kann. Je nach Qualität und Herkunftsland schwanken die Kosten zwischen 2 und 30 US-$ (siehe Beispiel auf S. 33).

⇨ ***COBs*** (Credit Card with Change of Billing). Dieses Angebot ist noch leistungsfähiger, weil es die vollständige Kontrolle über das Konto des Karteninhabers zulässt. Es ermöglicht dem Käufer das Ändern der Adresse des Opfers, um zum Beispiel Lieferungen und auf dem Postweg verschickte Kontoauszüge abzufangen oder Ansprechpartner umzuleiten. Die Preise reichen von etwa 80 bis 300 US-$ je nach Kontostand und Überziehungskredit [45].

Die nötige Ausrüstung zum Ausspähen und Erstellen von Karten ist ebenfalls auf dem Schwarzmarkt erhältlich:

⇨ ***Magnetstreifenleser*** (Skimmer). Wenn es an einem Geldautomaten angebracht ist, sammelt dieses elektronische Gerät die Informationen, die auf dem Magnetstreifen gespeichert sind. Solche Geräte kosten zwischen 1.500 und 14.000 US-$.

⇨ ***Tastaturaufsätze*** oder ***Miniatur-Kameras*** zum Ausspähen der Tastureingaben

⇨ Systeme zur ***Fernübertragung*** oder ***Speicherung*** der ausgespähten Daten [46]

⇨ ***WhiteCards*** oder vorgedruckte Karten (kurz „***Plastics***“) mit dem Label und den anderen Aufdrucken der Bank, deren Dumps die Kriminellen gesammelt haben

⇨ ***Schreibsysteme*** für Karten [47]

Das Ausspähen von Daten verspricht ein gutes Geschäft für die Lieferanten [48]. Die Verwender der Daten gehen ein zusätzliches Risiko ein, können aber auch große Gewinne machen. Dabei gibt es zwei übliche Methoden für die Verwendung von Karten: Online-Einkäufe [49], die keine Rechnungs- oder Lieferungadresse benötigen, oder Einsatz der Karten in Ländern [50], die noch nur den Magnetstreifen auslesen. Den Schaden durch gestohlene oder gefälschte elektronische Identitäten beziffert die IDC [51] auf jährlich rund 7 Milliarden $.

Spezielle Carder-Foren stellen den Kontakt zwischen den Cardern (Skimmer im weiteren Sinne) und den Käufern her. In aller Regel kauft ein Täter erst eine Probeeinheit, testet sie und macht dann einen größeren Kauf, wenn er zufrieden ist (zwischen 10 und 100 Einheiten). Seit etwa fünfzehn Jahren haben sich verschiedene Gruppen auf den Kreditkartenbetrug spezialisiert und dazu verschiedene Plattformen eingerichtet, die häufig sehr schnell von den Polizeien in vielen Ländern beobachtet und zerschlagen wurden [52].

Einige der führenden Carder-Seiten sind:.

⇨ ***Boafactory.com***: Diese Webseite wurde von Roman Vega geschaffen (alias "Romeo Stepanenko" und "Boa"). Der Name basiert auf einem von seinen Pseudonymen. Neben den unvermeidli-

[45] Eine Tabelle auf S. 34 führt die von McAfee ermittelten Einzel- und Paketpreise auf. Spitzenpreise erzielen Datensätze aus Kanada und Deutschland.

[46] Auf S. 35 stellt Paget eine Datenübertragung per Bluetooth und GSM vor (SMS). Diesen Aufwand betreiben die Täter in aller Regel nicht und beschränken sich darauf, die Daten auf übliche Speichermedien zu verwahren.

[47] Die Spuren 1 und 2 der Magnetstreifen sind besonders stark magnetisiert. Um auf echte Karten fremde Daten zu schreiben, müssen besonders leistungsfähige Geräte eingesetzt werden.

[48] Ich spreche insoweit vom Skimming im engeren Sinne.

[49] Das Spektrum ist inzwischen breiter:
Geschäfte im Einzelhandel mit falschen oder verfälschten Karten. Der Händler verliert die Ware und kann meistens seine Forderung nicht einziehen.
Online-Handel. Einsatz einer Kreditkarte einschließlich ihrer Prüfziffer (rechts neben dem Unterschriftsfeld). Die Lieferung erfolgt an Paket-Agenten oder Paketstationen.
Wenn der Täter über das Warenhandelskonto des Opfers verfügt, dann er die Lieferadresse beliebig manipulieren.

[50] Hiermit meint Paget das Cashing an Geldautomaten, wobei nicht der EMV-Chip, sondern tatsächlich nur der Magnetstreifen ausgelesen wird. Das funktioniert auch bei vielen POS-Terminals im Einzelhandel.

[51] International Data Corporation. International tätiges Marktforschungs- und Beratungsunternehmen.

[52] Ein Schaubild auf S. 36 zeigt die Namen verschiedener bedeutender Carder-Boards und die Zeitspannen, in denen sie aktiv waren. Es fehlt Carders .cc, also das Board, das heute die größte Bedeutung haben dürfte.

chen "Dumps" und gefälschten Kreditkarten bietet die Webseite auch gefälschte Pässe und Reiseschecks an. Vega, ein 39-jähriger Ukrainer, wurde im Juni 2004 auf Cypern verhaftet, ist bekannt als einer der Administratoren des CarderPlanet. Im Juni 2009 wurde er in die USA ausgeliefert und dem Bundesgericht überstellt. Er wird unter anderem beschuldigt, mehr als 2,5 Millionen US-$ ergaunert zu haben.

⇨ ***CCpowerForums:*** Diese Seite bietet seinen Mitgliedern viele Foren, einschließlich Spezialforen für das Hacking, Exploits (Schwachstellen), Proxies (anonyme Internetzugänge, Trojaner/Keylogger/Bots (Malware), Kreditkarten und eine Hall of Shame (Pranger). Im November 2006 führte die Operation Cardkeeper zur Verhaftung von zwanzig Personen in den USA und in Polen. Fünfzehn Haftbefehle wurden auch für Rumänen und weitere Amerikanern ausgestellt.

⇨ ***DarkMarket.ws:*** dieses Forum scheint bis Oktober 2008 aktiv gewesen zu sein. Obwohl der Zugang zum Forum nur auf Einladung von Bürgen möglich ist, gibt es mehr als 2.000 registrierte Benutzer. Es besteht eine Zusamenarbeit mit CCpowerForums, der internationale Vereinigung für die Förderung krimineller Aktivitäten (The Theft Services) und Mazafaka (S. 36).

⇨ Im August 2006 hackte Iceman, der Administrator von ***CardersMarket***, die Website. Er kopierte das Mitgliederverzeichnis und die Forumsinhalte, um sie in sein eigenes einzufügen. Er entdeckte, dass unter seinen Websiteadministratoren FBI-Agenten waren und versuchte, seine Mitglieder zu warnen. Das Gerücht wurde nicht ernst genommen. Das Forum wurde im Oktober 2008 geschlossen. Dabei hat das FBI in Zusammenarbeit mit den nationalen Polizeidienststellen mehr als fünfzig Verdächtige in den USA, Großbritannien, Türkei und Deutschland festgenommen.

Einer der verdeckten Ermittler wurde als J. Keith Mularski von der National Cyber Forensics Training Alliance aus Pittsburgh, Pennsylvania identifiziert. Sein Pseudonym "Master Splynter" erschien auch auf der schwarzen Liste von SpamHaus, wo es mit dem Namen Pavel Kaminski in Verbindung gebracht wurde. Diese Verzeichnisse waren wenige Stunden nach der Ankündigung verschwunden, DarkMarket werde geschlossen. Einer der Administratoren, Cagatay Evyapan, lebt in der Türkei und ist bekannt unter dem Pseudonym Chao. Er bietet qualitativ hochwertige Skimmer und Tastaturaufsätze an. Im Frühjahr 2007 wurde er angeblich von seinen Komplizen entführt und gefoltert, weil er allzu gesprächig sei.

⇨ Die internationale Vereinigung für die Förderung krimineller Aktivitäten [53], bekannt als ***The Theft Services***, ist nach den Äußerungen des Administrators „Zo0mer“ wahrscheinlich ein Nachfolger der ShadowCrew. Nach einem Artikel, der zuerst in der International Herald Tribune erschien, könnte es sich bei ihm um den Studenten Sergei Kozerev aus Sankt Petersburg handeln.

⇨ Die ***ShadowCrew*** war von August 2002 bis Oktober 2004 aktiv. Dieses Forum bot seine Mitglieder einen Ort, um Informationen zu finden und vor allem zum Kaufen und Verkaufen aller möglichen persönlichen und Bankdaten (Sozialversicherungsnummern, Dumps, geprüfte Kartendaten usw.) sowie gefälschten Dokumenten. Die Webseite wurde von abtrünnigen Mitgliedern der CounterfeitLibrary.com gegründet und war in den USA gehostet.

Im Dezember 2003 hatten die Foren etwa 4.000 Mitglieder, die Privilegien durch ihre aktive Beteiligung an Diskussionen und ihren Beiträgen zu Handlungsanleitungen (Tutorials) erwarben. An höchster Stelle standen die Administratoren, die über neue Mitglieder entschieden und über Zugangsrechte, Verantwortungen und Strafen bei Fehlverhalten bestimmten. Sie waren auch verantwortlich für die Verwaltung und Wartung der Server.

Verschiedenen Moderatoren bewachten ein oder mehrere Diskussionsforen. Sie wurden nach ihrem Wissen und ihren geografischen Standorten ausgewählt. Die illegalen Produkte der Hersteller und

[53] International Association for the Advancement of Criminal Activity

ihre Dienstleistungen wurden getestet und bewertet. Die Prüfer beurteilten die Qualität jedes Angebots und gaben Empfehlungen ab, die die Hersteller online einsehen und die Mitglieder erwerben konnten.

Die Diskussionen wurden in Englisch und Russisch geführt und gleichermaßen von Mitgliedern aus den USA und Osteuropa unterstützt. Davon profitierten die Kriminellen. Die aus den USA spezialisierten sich besonders auf das Hacking und die aus Russland und Rumänien auf das Fälschen von Zahlungskarten.

An der Spitze der Organisation standen mehrere Amerikaner und Moskauer als Websiteadministratoren. Über ihre Identität wird bis heute bei pcianswers.com gestritten.

Die ShadowCrew wurde lange von dem FBI infiltriert, bis endlich einige der Mitglieder der Gruppe den Gerüchten glaubten, die im Umlauf waren. Im Oktober 2004 wurde die Situation brisant und das Forum heruntergefahren. Darauf wurden 28 Personen in mehreren US-Bundesstaaten und im Ausland verhaftet, in Kanada, Großbritannien, Weißrussland, Polen, Schweden, den Niederlanden und der Ukraine. Die Verhaftungen enthalten nicht nur ShadowCrew-Mitglieder, sondern auch von CarderPlanet und DarkMarket. In den Vereinigten Staaten wurden 19 Menschen im Oktober 2004 angeklagt. Mehrere bekannten sich im November 2005 schuldig und wurden im Juni 2006 verurteilt. Auf den Seiten 38 und 39 stellt Paget einige Personen vor, die mit der Shadow Crew in Verbindung gebracht werden.

⇨ Die ***Stealthdivision*** wurde in Malaysia betrieben und hatte nur eine kurze Lebensdauer. Dem Forum wird nachgesagt, dass es von Beau Anthony Franken ("Scarface") gegründet wurde, um CarderPlanet zu ersetzen. Im August 2004 hatte es rund 1.340 Mitglieder, aber nur noch 500 im September und 700 im Oktober. Franken war einer der 28 Personen, die im Oktober 2004 verhaftet wurden.

⇨ ***Carder.su*** ist heute noch aktiv. Es wird vermutet, dass das Forum ein Teil des RU-Centers ist, das seit Februar 2009 einen anonymen Whois-Service anbietet. Dadurch wird die Identität der Domain-Betreiben verschleiert. Die Website ist bei 2x4.ru in Moskau gehostet. Diese von Pavel Ivanov geleitete Firma hostet viele verdächtige Webseiten [54].

⇨ ***CarderPlanet*** (International Callao Alliance): wurde im Mai 2001 von mehr als hundert Kriminellen in Russland und widmet sich besonders dem Thema Carding und dem Online-Handel mit Bankdaten. Dem russischen Forum wurde späten ein englischsprachiges hinzugefügt, um mehr Kunden zu gewinnen. CarderPlanet's Mitglieder waren bestrebt, ihren Einfluss zu erweitern und neue Märkte übernehmen. Im Juni 2004 hatte es 6.900 registrierte Benutzer. Unter den Folgen der Operation Firewall gegen den Konkurrenten ShadowCrew und der Verhaftung mehrerer hochrangiger Manager entschieden sich seine ihre Führer zur Vorsicht und schlossen die Webseite im August 2004 [55].

⇨ ***Mazafaka.ru*** entstand im Jahr 2001 als Treffpunkt für Russisch-sprechende Hacker. Im Juni 2004 trennte sich ein Zweig der Website widmete sich mit mehreren Websites der Finanzkriminalität. Die beliebteste davon war mazafaka.info, die im Februar 2007 9.200 registrierte Benutzer hatte und über einen englischsprachigen Teil verfügte. Empfohlene Mitglieder konnten sich zu einem durchschnittlichen Preis von 50 US-$ registrieren [56]. Nachdem im Sommer 2007 mehrere Leitungspersonen verhaftet wurde tauchte Mitte 2009 ist ein neues Carding-Forum mit diesem Namen auf.

---

[54] Es dürfte sich um einen Schurkenprovider handeln, der im Geschäft mit Bullet Proof-Diensten und WhoIs-Protection wirkt.

[55] Auf S. 40 führt Paget mehrere leitende Personen von CardersPlanet, ihre Tätigkeitsfelder und ihre Strafen auf.

[56] Paget spricht ohne weitere Ausführungen von „dual sponsorship“. Damit dürfte gemeint sein, dass nur solche Mitglieder aufgenommen werden, für die andere bürgen.

Auf S. 41 beschreibt Paget mehrere Personen, die mit Mazafaka in Verbindung stehen.

⇨ ***Cardercrew:*** Diese Carding-Seite wurde angeblich von einer jungen Frau geführt, die als Decepgal bekannt ist. Sie war auch eine Administratorin bei muzzfuzz.com und eine Zeit lang bei der ShadowCrew. Decepgal war am Handel mit gefälschten Kreditkarten in Osteuropa beteiligt und bezahlte mit einem Teil des Geldes ihre Komplizen [57]. Obwohl lange Zeit der Name Diane Dansereau-Avery gehandelt wurde, könnte sich dahinter auch ein junger chinesischer Mann verstecken, der jetzt das Hacking lehrt.

⇨ ***CardersMarket*** wurde im Juni 2005 von Max Ray Butler ("Iceman," "Max Vision," "Aphex," und "Digits") gegründet und diente als Plattform für den Austausch finanzieller und persönlicher Daten. Es wurde im Iran gehostet und hatte im August 2006 fast 1.600 Mitglieder. Als Administrator und Verkäufer war Iceman schon seit 1998 der Polizei bekannt. Seinerzeit wurde wegen des Hackings beim U.S. Department of Defense verhaftet und war er nach einer kurzen Haftstrafe als Informant für das FBI tätig. Butler war auch Sicherheits-Fachmann und fand Schwachstellen in der arachNIDS-Datenbank, bekannt als "Max Vision." Als Fachmann für die drahtlose Kommunikation wollte er seine Mitbewerber auszuschalten und griff im August 2006 die Foren DarkMarket, TalkCash, ScandinavianCarding und TheVouched an, deren Daten er unzugänglich machte. Er stahl seinen Konkurrenten 4.500 Konten und fügte sie in seine eigene Mitgliedsdatenbank ein. Er entdeckte, dass DarkMarket vom FBI und warnte die Carder-Gemeinde. Als Rivale wurde Butler jedoch nicht ernst genommen. Er wurde im September 2007 – wenige Monate nach seinem Mitarbeiter Christopher J. Aragon – erneut verhaftet.

⇨ ***TheGrifters***: Dieses private Forum wurde von David Thomas errichtet, während er ein Informant des FBI war. Es wurde von Dezember 2003 bis September 2004 betrieben. Ein gutes Jahr später wurde es wiedereröffnet und diente als "anti-carding"-Webseite, wo Besucher viele Informationen zum Thema finden konnten.

Steven Lance Roberts ("John Dillinger") wurde mit Thomas bekannt und beteiligte sich an dessen Abenteuer. Er ist ein ehemaliger Bankräuber, der sich auf den Online-Betrug und und die Bank-Piraterie verlegt hat. Nach dem Besuch mehrerer spezieller Foren (z. B. Counterfeit Library, ShadowCrew und CarderPlanet) erhielt er häufig die Daten rumänischer oder russischer Komplizen, die es ihm erlaubten, Kreditkarten zu fälschen und an Geldautomaten einzusetzen. Das Geld wurde dann nach Russland per e-Gold oder Western Union übermittelt und Roberts durfte einen Anteil von 20 bis 30 Prozent der Beute für sich behalten. Seine Kontakte nach Russland schließen auch "King Arthur" ein, einer der ersten, der das Phishing beherrschte. Im Rahmen der Operation Cardkeeper wurde Roberts im Juni 2006 im Alter von 45 Jahren in San Diego, Kalifornien verhaftet.

⇨ Die ***CounterfeitLibrary*** ist eines der ältesten Foren, in dem gefälschter Dokumente und gestohlene persönliche Daten zum Verkauf angeboten werden. Im Juni 2002 zog es die Aufmerksamkeit der Leitung der Illinois University auf sich, weil im Forum gefälschte Abschluss-Diplome anboten wurden. Gleichzeitig wechselten mehrere Mitglieder zum ShadowCrew um dort mit Finanzdaten zu handeln.

9. Menschliche Schwächen. Phishing

Trotz ihrer Risiken verbreiten eCommerce und das Online-Banking. Ihr Wachstum wird häufig als die wichtigste Ursache für die Internetkriminalität angesehen. Hinzu kommt die Leichtfertigkeit, mit der viele Internet-Nutzer Informationen und Zugangsdaten verbreiten, die sie besser geheim halten sollten. Es sind meist die Anwender selbst, die mangels Bewusstsein oder durch Täuschung Einbrüche in die Systeme ermöglichen [58]. Das nutzen die Internetkriminellen aus.

Ein Angriff aus dem Mai 2008 veranschaulicht das Phänomen. Mit einer bösartigen Instant Message

[57] Das dürfte bedeuten, dass Decepgal das Cashing für osteuropäische Auftraggeber betrieb.

[58] Gemeint sind die Techniken, die unter dem Stichwort Social Engineering diskutiert werden.

wurde Nutzern von MSN [59] damit gedroht, dass ihre Konten gelöscht wurden. Um zu erfahren, wer dafür verantwortlich war, gab es einen Link zu einer präparierten Webseite in Hongkong. Wer dem Link folgte, aktivierte damit einen böswilligen Code, der die Nachricht an alle alle Kontakte verbreitete. Ein Journalist von der französischen Newswebseite Zataz entdeckte auf einer Piratenseite eine aufschlussreiche Statistik: Binnen sechs Tage fielen 1.146.904 Internet-Nutzer in diese Falle und im Mai 2008 gab es mehr als 24.000 Besuche pro Stunde.

Der Mangel an Schulung fördert den Fortschritt der virtuelle Kriminalität. Hinzu kommt, dass die Strafverfolgungsbehörden manchmal von den technischen Einzelheiten der Bedrohungen überfordert sind und Staatsanwälten und Richtern die nötige Ausbildung fehlt (S. 42).

Rock Phish ist seit 2004 eine der aktivsten Phishing-Organisationen. Obwohl sie lange mit dem inzwischen aufgelösten RBN [60] verknüpft wurde, werden seine wichtigsten Führer von Experten in Rumänien erwartet. Im Jahr 2006 wurde geschätzt, dass Rock Phish rund 150 Millionen US-Dollar durch Manipulationen mit Bankkonten erbeutete. Schon im Oktober 2006 wurden der Organisation etwa die Hälfte aller Phishing-Angriffe zugeschrieben.

Seit 2008 hat Rock Phish seine Technik durch die Kombination von Phishing und Crimeware verfeinert. Die Bankdaten unvorsichtiger Opfer werden nicht nur auf kriminellen Seiten gesammelt. Sie sind zudem den E-Mails von verschiedenen Trojanern ausgesetzt wie dem berüchtigten Zeus (alias ZBOT, WSNPOEM), der in Verbindung mit dem Neosploit infection kit und dem Asprox-Botnet steht.

[59] Microsoft Network

[60] Russian Business Network

10. Erlös des Einsatzes

10.1 Spam

Eine im Jahr 2008 von der University of California, Berkeley durchgeführten Studie zeigt, dass sich Spam wirtschaftlich lohnt, auch wenn die Antwortrate mit 0,000001 Prozent (1 : 100 Millionen) unglaublich niedrig ist. Die Forschern haben den Eindruck, dass Antwortquote erheblich höher ist. Diese Erkenntnis beruht auf drei Spam-Kampagnen, deren fast 470 Millionen unerwünschte E-Mails sie nachverfolgt haben.

Die meisten Kampagne betreffen pharmazeutischen Produkte. Auf sie entfallen 347,6 Millionen Spam-Nachrichten, hauptsächlich von dem Storm Botnet. Mehr als 10.000 Menschen erlagen der Versuchung, die Webseite des Anbieters zu besuchen. Das ist eine Erfolgsquote von 0,00003 Prozent (3 : 100.000). Nur in einem von 12,5 Millionen Fällen (0,000008 Prozent) wurde das Produkt gekauft. Das ist auf dem ersten Blick eine lächerlich geringe Anzahl. Wenn man jedoch bedenkt, dass täglich 120 Milliarden Spam-Mails gesendet werden, bedeutet eine Erfolgsquote von 1 : 12,5 Millionen, dass täglich fast 1.000 Menschen oder mehr als 360.000 Menschen im Jahr auf Spam hereinfallen. Diese Kampagne war noch nicht einmal eine besonders erfolgreiche. Eine als Aprilscherz getarnte Nachricht hatte den doppelten Erfolg [61].

Obwohl die Studie bestätigt, dass jedes Jahr mehrere Millionen Dollar erzielt werden, widerlegt sie die Vorstellung, dass einige Leute mehrere Millionen Dollar am Tag verdienen könnten. Die Universität berichtetet von einem Jahresumsatz von 3,5 Millionen US-$ nach einer pharmazeutischen Spam-Kampagne. Das ist eine Hochrechnung auf der Grundlage einer Untersuchungsdauer von 26 Tagen und der Feststellung, dass durchschnittlich 140 US-$ ausgegeben werden.

Um ihre Kosten zu verringern, könnten Spammer auch die Betreiber von Botnetzen sein. Der Markt für das Spamming ist begrenzt, so dass die An-

[61] Die Erfolgsquoten werden anschaulich in der Grafik auf Seite 43 dargestellt.

zahl der Beteiligten klein sein könnte. Sie müssten gut organisiert sein und danach streben, Mitbewerber zu verdrängen. Ihre Ausgaben könnten sie auf zwei oder drei gute Programmierer begrenzen.

Nach Schätzungen der Webseite Spamhaus sind etwa 100 kleine Organisationen mit bis zu fünf Mitglieder, also insgesamt 300 bis 400 Spammer, für 80 Prozent aller unerbetenen Nachrichten in Europa und Nordamerika verantwortlich. Die Namen der diese kleinen Banden und andere Informationen können in der Datenbank bei Spamhaus gefunden werden.

Eine riesige Anzahl der beworbenen Angebote betreffen den Verkauf gefährlicher pharmazeutischer Produkte. Die Unternehmen hinter diesen Angebote betreiben ein zwispältiges Spiel. Der öffentliche Teil besteht besteht häufig nur aus Webseiten, mit denen sie versuchen, unschuldige oder unmoralische Partner mit vielversprechenden, erheblichen Einkommen zu gewinnen.

Nachdem die Partner gewonnen wurden, werden sie zu anderen Webseiten gelenkt, die von den gleichen Gruppen betrieben werden. Dort wird der kriminelle Aspekt der Geschäfte sichtbar: Diese Einrichtungen bieten den Partnern Proxyserver [62] oder Botnetze an, um die Gewinne der Spam-Unternehmen zu steigern. Die bekanntesten sind:

⇨ ***GlavMed/Spamit*** hat seinen Ursprung in Russland und wird dem RBN zugeordnet. Diese Organisation scheint das Storm Botnetz verwendet zu haben. Es besteht der Verdacht, dass GlavMed das öffentliche Schaufenster für die Gruppe Spamit ist. Zusammen mit anderen hat GlavMed "Meine kanadische Apotheke" entwickelt und brüstet sich mit den Namen seiner Unterstützer.

⇨ ***SanCash/GenBucks***. Diese öffentlich-private Partnerschaft erlitt einen großen Rückschlag im Oktober 2008. Nach einer Spam-Kampagne vom Ende des Jahres 2007, bei dem ein Botnetz mit 35.000 Maschinen verwendet wurde, das täglich 10 Milliarden Spam-Nachrichten versenden konnte, erwirkte die US Federal Trade Commission bei den Gerichten in Neuseeland eine Geldstrafe von 200.000 NZD (124.000 US-$).

⇨ ***Bulkcarrier***. Diese Firma wurde Ende 2006 gegründet und sie betrieb erfolgreich die Seite specialham.com. Ihr Ziel ist es, die Profis im Spam-Geschäft und Anfänger im Bulk-Mailing-Bereich [63], für den Kauf und Verkauf von verschiedene Dienstleistungen und für die Diskussion über unterschiedliche Spams zusammen zu bringen. Das Unternehmen ist heute noch aktiv, hat sich aber im April 2009 verlagert, um seine Spuren zu verwischen. Es sind mehrere Listen mit den Namen der Führungspersonen und Partner im Umlauf.

⇨ ***Yambo Financials***. Der Leiter dieser bekannten Gruppe ist ein Ukrainer, dessen wichtigstes Pseudonym Alex Polyalov ist. Er könnte hinter den Angeboten in "Meine kanadische Apotheke" stecken und der Kopf mehreren Gruppen einschließlich SanCash und Bulker sein. Das Unternehmen entfaltet angeblich auch betrügerische Aktivitäten in vielen anderen Bereichen, von der Pädophilie bis zu Software-Raubkopien. Obwohl die Gruppe in den USA im Jahr 2005 einen rechtlichen Rückschlag erlitt, ist sie immer noch in Spamhaus' Top 10-Liste.

Es gibt Dutzende anderer Webseiten, von denen die meisten zweisprachig sind (Englisch und Russisch) und die die Überlegenheit der osteuropäischen Länder in diesem Bereich widerspiegeln.

10.2 Crimeware

2007 wurde Malware oft mit Ready-to-Use-Tools erstellt, also mit Baukästen mit einfacher Handhabung. In der Zwischenzeit wurden die Anwendungen und die Malware-Entwicklung Anwendungen anspruchsvoller. Sie erfordern einiges Know-how und fordern ein umfassendes Netzwerkwissen von ihren Anwendern. Heute beobachten wir sowohl preiswerte Fertig- als auch teure Highend-Produkte [64].

[62] Siehe auch S. 54: 5Socks.net; SOCKS v4/v5.

[63] Massen-Versand-Geschäft

[64] Die Tabelle auf S. 46 zeigt mehrere Entwickler-Tools und ihre Preise.

In China scheint ein halbes Dutzend Gruppen zu hinter der Crimeware-Industrie zu stecken. Die Informationen von dort sind manchmal widersprüchlich und es kann schwierig sein, die Namen der Gruppen zu übersetzen. Eine der Gruppen, TheDarkVisitor nennt sie "Crab Group", wird eine der spektakulärsten Infektionen nachgesagt, von denen mehr als 30 Millionen Maschinen betroffen gewesen seien. Scott Henderson führt in einem Anti-Virus-Bericht von Kingsoft aus, dass "in den Hacker-Kreisen das meiste Geld mit der massenhaften viralen Verbreitung verdient wird. Während ein Virus-Autor ein Gehalt von einer Million Yuan in einem Jahr verdienen kann (etwa 150.000 US-$), war es möglich für eine virale Verbreitung zehn Millionen Yuan (1,5 Millionen US-$) jährlich zu verdienen."

Andere Gruppen scheinen jetzt ihre Aktionen auf das chinesische Territorium zu begrenzen. Ihre Namen lauten in grober Übersetzung:

⇨ Mayday Pornography Group

⇨ Wang Xiaofeng Group

⇨ Li Bao-yu Group

⇨ Crab Group

⇨ Jackie Chan Group

⇨ CCTV-Just Group

In Osteuropa ist seit 2003 das ProdexTeam das Online-Schaufenster für das Pseudonym Corpse. Er ist bekannt für die Entwicklung und Verkauf von Trojanern, einschließlich Haxdoor und Nuclear Grabber. Haxdoor war weltweit die erste Malware, die Rootkits einsetzte [65] und in der Lage war, Bankdaten abzufangen [66]. Die schwedischen Bank Nordea verlor 2006 1,1 Millionen US-$ wegen eines der Haxdoor-Varianten. Obwohl Corpse im Oktober 2006 behauptete, dass er seine Aktivitäten beendet habe, soll er immer noch an der Internetkriminalität und Carding beteiligt sein.

Um Marktanteile im Geschäftsfeld Crimeware zu gewinnen, haben sich „Kriminelle Büros" (criminal offices) vervielfacht. Einige sind wegen ihres Gruppennamen, andere durch ein Pseudonym bekannt geworden. Die führenden Produkte sind:

⇨ Gray Pigeons ⇨ Binghe Trojan (China, von 2003 bis 2007)

⇨ HangUp Team ⇨ Berbew, Korgo, and Gozi (Russland)

⇨ IDT Group ⇨ IcePack (Russland 2007)

⇨ DreamCoders Team ⇨ MPack (Russland, von 2006 bis 2007)

⇨ Diel ⇨ FirePack (2007, 2008)

⇨ Shine ⇨ Adrenalin (2008)

⇨ WebAttacker ⇨ inet-lux (Russland, von 2006 bis 2008)

⇨ NeoSploit Team (von 2007 bis 2008)

⇨ Grabarz ⇨ PolySploit (2008)

⇨ Magicz ⇨ Vermarkter von Zeus und seinen Ergänzungen (von 2007 bis heute), Illuminati, vippro123 und andere

⇨ HuGos ⇨ ZeuEsta 6.0 (2009)

⇨ H1t3m (he is the ROOt y0u webmaster) ⇨ ZeuEsta 7.0 (2009)

10.3 Pay Per Install

Das Internet bietet Webmastern eine Vielzahl von Angeboten, damit Geld zu verdienen, dass sie versteckten Code oder irreführende Fenster in ihre Webseiten einfügen, mit denen böswillige oder unerwünschte Software installiert oder die Besucher auf präpariere Webseiten umgeleitet werden. Hinter allen diesen Webseiten stecken mehr oder weniger gut strukturierte Gruppen mit verdächtigen oder geradezu bösartigen Angeboten. Jeder Zweifel an der Bösartigkeit der Angebote entfällt, wenn die Partner pornografische Angebote führen oder Methoden anpreisen, um Besucher umzuleiten.

---

[65] Rootkit: Mechanismen zum Tarnen der Malware besonders vor Anti-Viren-Programme.

[66] Phishing-Malware

10.3.1 Iframe

Iframe ist ein HTML-Tag, mit dem auf einer Webseite weitere Fenster eingeblendet werden können. Man kann sie so einstellen, dass sie unsichtbar sind und dennoch ein Angriffswerkzeug (Mpack type) mit darauf böswillige Software laden oder zu präparierten Webseiten umleiten. Dort wird häufig ein Botnet-Client injiziert, den der Vertriebspartner verkaufen kann.

10.3.2 Adware

Bis Anfang 2009 war Zango der bekannteste Vertreiber von lästigen Programmen zur Präsentation unerwünschter Werbung. Die Programme werden meistens ohne Zustimmung auf den Opfer-Maschinen installiert, wo sie die gespeicherten Daten um gezielte Werbeangebote zu übermitteln. Nachdem die Firma zahlreiche Klagen verloren hatte, feuerte im Juni 2008 68 ihrer Mitarbeiter und schloss ihre Türen im April 2009 für immer. Das Geschäftsfeld haben andere Firmen übernommen.

10.3.3 Gefälschte Anti-Virus-Software und Codecs

Von der gefälschten Antivirus-Software wird der infizierte Anwender nachhaltig davor gewarnt, dass sich auf seinem Computer eine Malware befände. Abhilfe schafft ein kostenpflichtiges Programm, das zumindest bewirkt, dass der digitale Schreihals abgestellt wird. Besonders gut aufgestellt auf diesem Markt ist das russische Unternehmen BakaSoftware, seit 2003 auch bekannt als Pandora Software. 2008 suchte die Unternehmens-Webseite Menschen, die ein Anti-Virus-Vertriebsnetzwerk beitreten sollten. In russischer Sprache versprach sie den Partnern einen nach Verkaufszahlen gestaffelten Anteil von 58 bis 90 Prozent beim Verkauf der angebotenen Antivirus-Software. In vielen Foren in russischer Sprache wird dieses Vertriebsmodell „Kraba“ genannt. In einem Fall soll einem Vertriebspartner durch den Verkauf von rund 3.000 Kopien 146.000 US-$ ausgezahlt worden sein.

Solche Zahlen sind äußerst fragwürdig [67] und die Top-Verkäufer sind zweifellos eng mit der Webseiten-Managern verbunden, die sicherlich mit 90 Prozent am Gewinn beteiligt sind. Um einen echten Gewinn zu machen, muss die nervende Software mit Botnetzen oder präparierte Webseiten massenhaft verbreitet werden. Damit ein ehrgeiziger Verkäufer einen Jahresgewinn von 5 Millionen US-$ verdienen kann, muss er das Produkt auf täglich auf 10.000 bis 20.000 Maschinen installieren.

"Nenastniy" hat im Oktober 2007 eine Spam-Kampagne für den amerikanischen Präsidentschaftskandidaten Ron Paul durchgeführt, wobei das Srizbi Botnet und der Reactor Mailor verwendet wurden. Reactor ist ein 2004 erschienenes Spammer-Tool, das damals von der ukrainischen Firma Elphisoft verkauft wurde.

BakaSoftware ist nicht einzigartig. Andere Unternehmen auf der ganzen Welt betreiben die gleiche Art von Betrug. Auf Antrag der Federal Trade Commission ordneten amerikanische Gerichte im Oktober 2008 deshalb die Einstellung von zwei amerikanischen Unternehmen an, Innovative Marketing Inc. und ByteHosting Internet Services LLC.

10.4 Dienstleistungsangebote

Neben den nötigen Produkten können die Internetkriminellen auch optimierte Dienstleistungen einkaufen, auf die sich andere Gauner spezialisiert haben, auf das Bulletproof Hosting, die Vermietung von Botnetzen, virtuelle Bankgeschäfte und bestellte DDoS-Attacken oder andere. Eine Preisliste gibt es auf S. 52.

Neben verteilten Angriffen (DDoS) gibt es inzwischen verwandte Angebote bei den Telefondiensten: Für ein paar Dutzend Dollar können die Opfer mit Anrufen oder SMS-Nachrichten überflutet werden.

---

[67] Eine Tabelle auf S. 51 führt die TOP-Vertriebspartner von BakaSoftware auf, die von „NeoN“ erhackt wurden.

76service ist eine Entwicklergruppe im Umfeld des RBN gewesen, die 2007 das Gozi Botnet vermietet hat. Die Gruppe ist verschwunden und ein Rivale, loads.cc, ist an ihrer Stelle seit mehreren Jahren tätig. Er bietet den Kunden Gruppen von jeweils 1.000 Maschinen im Land seiner Wahl an.

Jedes Unternehmen im Online-Business hat die Hauptsorge, den DoS-Angriffen seiner Konkurrenten zu widerstehen. Einige davon bieten einen verfeinerten Service: Sie installieren ganz gezielt Malware auf den Computern der ausgesuchten Opfer [68].

11. Schlusswort

Seit fünf Jahren haben wir immer wieder die zunehmende Professionalität der Cyberattacken, die schnell wachsenden Menge an Malware und größer werdenden kriminellen Gewinne angekündigt. Lange Listen mit ausgespähten Bankdaten, wie sie von im Juni 2003 bei W32/Bugbear@MM gefunden wurden, überraschen heute niemanden mehr.

Wir erwarten, dass die Internetkriminalität mehr und mehr mit der herkömmlichen Kriminalität verwachsen wird. Gleichzeitig werden sich das normale Geschäftsleben und die Zahl der finanziellen Transaktionen im Internet weiter erhöhen.

Neben unserem physischen Bankenumfeld entstehen virtuelle Umfelder und elektronische Brieftaschen enthalten virtuelles Geld, das in neuen Finanzzentren die Besitzer wechselt. Schon heute gibt es Prostitution, Drogenhandel und Glücksspiel im Internet. Um ihre Marktanteile zu erhalten werden sich die traditionellen kriminellen Gruppen anpassen müssen. Wir vermuten, dass neue Banden- und Verteilungskriege ausbrechen werden. Letztlich werden alle kriminellen Gruppen ihre Computer-Kommandos haben und das Internet wird eine wachsende Einnahmequelle für sie sein.

Genauso wie die Internetkriminalität und die herkömmliche Kriminalität zusammenwachsen werden, werden sich auch die Cyber-Kriminalität und die Wirtschaftskriminalität verbinden. Das ist die zwingende Logik der Geldwäsche: Der kriminelle Gewinn aus der Internetkriminalität muss in die legale Wirtschaft integriert werden, damit er verwertet werden kann.

Finanzagenten und die lokale Geldwäsche reichen nicht mehr aus, um "schwarzes Geld zu säubern". Die Cyberkriminellen werden deshalb ihre eigenen Geldwäsche-Strukturen entwickeln und dazu tief in die Wirtschaftskriminalität eindringen. Die globale Reichweite des Internets, die verzögerungsfreie Geschwindigkeit von Transaktionen, die Schwierigkeiten bei der Identifizierung der Clients und die Komplexität der territorialen Rechtsordnungen wird den Verbrechern die Arbeit erleichtern.

Diese Entwicklungen gehen einher mit einer Ausbreitung der Gewalt gegen diejenigen, die sich an der Internetkriminalität beteiligen. Ein Beispiel: Cagatay Evyapan ist Fachmann für den Einbruch in Bankkonten und wurde im September 2008 verhaftet. Einige Monate vorher veröffentlichte er das Bild eines seiner früheren Komplizen (Mert Ortac, alias Kier, zwei Monate später verhaftet), den er gefoltert hatte, nachdem er entdeckte, dass „Kier“ mit der Polizei zusammen arbeitet [69].

Die Offshore-Zentren, das Umfeld der Online-Banking-Dienstleistungen und die virtuellen Casinos werden wachsen, die Grenzen zwischen noch legalen und illegalen Geschäften verschwimmen. Trotz der Bemühungen der internationalen Strafverfolgungsbehörden werden die Internetkriminellen die Schwachstellen und Lücken in den internationalen Vorschriften immer raffinierter ausnutzen.

Schließlich werden sich Internetkriminalität, Schurkenstaaten und unabhängige transnationale Einheiten verbinden. Längst haben sich die Gerüchte

[68] Die klassische Verbreitung von Malware erfolgt nach dem Gießkannen-Prinzip. Sie setzt auf Masse und ihren Tätern kommt es nicht auf Begleitschäden an. Die modernen Malware-Strategien sind eher mit chirurgischen Eingriffen vergleichbar und dienen entweder der Industriespionage oder der punktgenauen Sabotage.

[69] Beleg auf S. 55.
Aber: Die Mafia arbeitet diskreter als der profilsüchtige Schläger.

über nationalistische Cyberattacken und von autoritären Regimen bestätigt. Der Cyberwar ist keine Science-Fiction mehr. Viel wahrscheinlich ist es, dass sich instabile Regime, Anti-westliche Staaten, und Terroristen oder radikale Öko-Terroristen der digitalen Kriminalität Kriegsführung zuwenden werden.

Wir sind uns sicher, dass es nicht lange dauern kann, bis wir unwiderlegbare Beweise ihrer Teilnahme finden. Demokratischen Staaten könnten deshalb versucht sein, unter dem Deckmantel des Schutzes unserer Demokratien dieselben Methoden anzuwenden. Das könnte sich zu einem unkontrollierbaren Buschfeuer ausweiten und sich als katastrophal erweisen.

<Damit endet der Text von Paget>

<Hannover, 20.10.2010>