Seminarausarbeitung „An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants“

Ralf Stange
(majere@cs.tu-berlin.de)

Betreuer
Gregor Maier

Seminar „Internet Sicherheit“ ,
Technische Universität Berlin

SoSem 2008 (Version vom 6. Juni 2008)

Zusammenfassung

Die Kommerzialisierung von illegalen Aktivitäten im Internet nimmt stetig zu. Mit Kreditkartendaten, Botnetzwerken oder kompromittierten Rechnern kann und wird Geld verdient.

In ihrer Arbeit „An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants“ [1] untersuchen die Autoren Franklin, Perrig, Paxson und Savage diesen Untergrundmarkt durch Beobachtung und Auswertung von öffentlich zugänglichen An- und Verkaufsgeboten auf frei zugänglichen Chat-Servern.

1 Einleitung

Computersicherheit ist ein Thema, welches häufig aus einer sehr technischen Richtung betrachtet wird. Welche Angriffsmöglichkeiten gibt es, welche Maßnahmen kann ich ergreifen um mich davor zu schützen. Ein potenzieller Angreifer wird bei dieser Betrachtung auf seine technischen Fähigkeiten reduziert. Doch entsprechend dem Zitat „Sicher ist ein System genau dann, wenn die Kosten des Angriffs den erzielbaren Nutzen niemals unterschreiten." [2] ist die Motivation eines Angreifers in der heutigen Zeit von entscheidender Bedeutung. Während noch vor 10 Jahren die Anerkennung in der Szene die Hauptwährung und Motivation für Angreifer war, hat sich mittlerweile ein gewinnorientierter Untergrundmarkt mit Schwachstellen, personenbezogenen Daten und kriminellen Dienstleistungen entwickelt.

Doch wie funktioniert der Handel mit diesen illegalen Daten? Wer bietet sie an, wer kauft sie und welche Preise werden dabei erzielt? Durch die Beantwortung dieser und ähnlicher Fragen könnte man neue Erkenntnise zu realen Bedrohungsszenarien gewinnen. Wenn wir z.B. den Preis eines kompromittierten Rechners kennen und dazu auch die Verfügbarkeit solcher Rechner, dann könnten wir den Preis abschätzen, den es kostet einen bestimmten Webserver mit Denial of Service Attacken lahmzulegen. Zu der bisher vorherrschenden technischen Sicherheitsbetrachtung käme noch die ökonomische hinzu.

Solche illegalen Angebote werden in großer Zahl in öffentlich zugänglichen Chaträumen gehandelt. Die Autoren haben 7 Monate lang solche Chaträume besucht und über 13 Millionen Zeilen an Textnachrichten gesammelt. Aus der Auswertung der Logfiles ergibt sich ein interessanter Einblick in die gehandelten Waren, die Teilnehmer dieser Untergrundmärkte und auch der umgesetzten Geldmengen.

1.1 Was wurde gesammelt – IRC

Bei den beobachteten öffentlich zugänglichen Chaträumen handelte es sich um „public channels" von Internet Relay Chat Servern.

Internet Relay Chat (*IRC*) ist ein Standardprotokoll zum Austausch von realtime Nachrichten über das Internet [3]. Clients verbinden sich mit dem IRC Server, welcher mit anderen IRC Servern zu einem IRC Netzwerk verbunden sein kann.

Nickname, Client-IP Die Identifikation eines IRC-Teilnehmers erfolgt anhand der IP-Adresse des Clients, die von jedem anderen Teilnehmer abfragbar ist und einem frei wählbaren *Nicknamen* durch den User. Der Nickname kann registriert und durch ein Passwort gesichert werden, so dass er nicht mehr von anderen Teilnehmern verwendet werden kann.

Channels Ein IRC Server stellt meist viele unterschiedliche Chaträume (*Channels*) zur Verfügung. In diesen Channels kann jeder Teilnehmer Nachrichten schreiben (*posten*) und die geschriebenen Nachrichten aller anderen Teilnehmer des Channels lesen. Clients bieten die Möglichkeit diese Kommunikation in *Logfiles* zu speichern.

Private Channels Wird eine private Kommunikation gewünscht, so können zwei Teilnehmer einen privaten Channel öffnen. Die dort stattfindende Kommunikation ist privat und kann von den anderen Teilnehmern nicht gelesen werden.

Channel-Administratoren sind Teilnehmer mit erweiterten Rechten. Sie können unter anderem User mit einem für andere User sichtbaren Label versehen.

Channel-Dienste Das sind von den Betreibern installierte Scripte, die die Teilnehmer durch bestimmte Kommandos aufrufen können, z.B. um den letzten Login eines Nicknamen abzufragen.

Während die bisher beschriebenen Begriffe für IRC allgemein gelten, sind in den beobachteten Channels einige Besonderheiten zu erwähnen:

Verifizierte Teilnehmer Technisch nur ein Label der von den Channel-Administratoren vergeben wird und für alle sichtbar ist. Dieses Label wir hier als verifizierter Teilnehmer interpretiert. Normale Teilnehmer in einem Chatraum sind erstmal anonym. Dieser Status als verifizierter Teilnehmer scheint eine wichtige Methode zu sein um das notwendige Vertrauen zwischen den Marktteilnehmern zu schaffen. Häufig werden Geschäfte nur zwischen so markierten vertrauenswürdigen Teilnehmern akzeptiert. Um den Status als verifizierter Teilnehmer zu erlangen ist es gebräuchlich mehrere Beispieldaten der angebotenen illegalen Daten zu senden. Channel-Administratoren sichten diese Daten und vergeben den Status.

Clientidentifizierung Die IP-Adresse einer Quelle kann auch für die Bewertung der Zuverlässigkeit eines Teilnehmers herangezogen werden (z.B. Ausschluss von IPs bekannter Anonymisierungsdienste, etc.). Die Registrierung des Nicknames ist ebenfalls häufig eine zwingende Grundlage für das Vertrauen zwischen den Channel-Teilnehmern.

Illegale Channel-Dienste Die meisten IRC Server bieten automatisierte Dienste zur Verifikation von Kreditkartendaten, Kreditlimits u.ä. an.

1.2 Überblick über die gesammelten Daten

In dem Zeitraum vom Januar bis August 2006 wurden insgesamt 2,4 GB IRC-Logfiles gesammelt. Die Daten stammen dabei von ausgewählten Channels in verschiedenen IRC-Netzwerken. Dabei wurden über 13 Millionen Nachrichten von über 100.000 unterschiedlichen Nicknames gesammelt. Die Autoren geben leider weder die IRC-Server selber an, noch wie sie an die Adressen der Server gelangt sind.

Die so gesammelten Daten sind eine recht unübersichtliche Mischung aus Verkaufs-Postings für illegale Waren oder Dienstleistungen, Gesuche nach selbigen Waren und Dienstleistungen, teilweise mehrfach wiederholt um die Marktaufmerksamkeit zu erhöhen. Teilweise posten auch Scripte Werbung vielfach über den Tag verteilt in die Channels.

Diese Kauf- und Verkaufsgebote können unter den Begriff (Werbe-)*Anzeigen* zusammgefasst werden. Typische beworbene illegale Waren und Dienste sind:

Gehackte Server Hier werden Adressen und Zugansdaten zu kompromittierten Servern gehandelt.

Bankaccounts Hier geht es um Zugangsdaten zu Bankaccounts, Paypal, etc. Meist verbunden mit Kontoständen und Kreditlimits.

Persönliche Daten Hierunter fallen Adressen, Sozialversicherungsnummern, Bankdaten von Personen.

Spam-Listen Angeboten werden umfangreiche Emaillisten als Empfänger zum Spamversand

Adressen von Open-Relays Diese Server können zum Versand von Spam verwendet werden. Meist handelt es sich um falsch konfigurierte Emailserver oder fehlerhafte Webseiten mit Formularen zum Emailversand (Support, etc.)

Spamversand Es wird der Spamversand als Dienstleistung angeboten

Phishingdienste Angebot Webserver zu infizieren oder Mails zu versenden, so dass der Käufer der Dienstleistung an Accountdaten von den betroffenen Nutzern gelangt.

Geldtransfers von gehackten Konten

Neben diesen, bis auf die Illegalität der Waren, recht normalen Verhalten für einen stark frequentierten Marktchannel werden auch regelmäßig direkt illegale Daten in den Channel gepostet (z.B. Kreditkartendaten). Sie dienen um einerseits die Aufmerksamkeit auf Angebote weiterer ähnlicher Daten zu lenken, also quasi Gratisproben und zum anderen als Beweis, dass der Absender der Daten tatsächlich über die angebotenen Daten verfügt.

Diese direkt in den Channel geposteten illegalen Daten werden im Folgenden unter dem Begriff *Sensitive Daten* zusammegefasst. Häufige direkt gepostete Daten sind:

Kreditkartendaten Teilweise vollständig mit Namen und zusätzlichen Informationen. Teilweise nur die Kartennummer.

Social Security Number Die SSN wird zum Identitätsdiebstahl verwendet.

Personendaten Von einzelnen Namen über vollständige Adressen mit Geburtsdatum, Telefonnummer, Bankverbindung und Kreditrahmen.

Accountdaten Von Bankaccounts bis zu gehackten Servern.

Die Bezahlungen erfolgen meist über Kanäle, die von den amerikanischen Behörden nicht oder nur schwer verfolgbar sind (online z.B. der amerikanische Micropaymentanbieter E-Gold mit Sitz in der Karibik oder offline per Western Union Geldtransfer).

1.3 Überblick Auswertungsverfahren

Für statistische Auswertungen ist es notwendig die gesammelten Daten nach Art der Nachricht (Verkaufsgebot, Kaufgebot, sensitive Daten) und dem Inhalt (Kreditkartennummer, gehackter Account, etc.) zu klassifizieren. Umgangsprachliche Anzeigen und unterschiedlich formatiertes Datenmaterial erschweren solch eine Klassifizierung. Die folgende Tabelle zeigt einige Textbeispiele aus den Chat-Logfiles mit einer manuellen Einteilung:

Advertisement / Data	Classification Label(s)
i have boa wells and barclays bank logins...	Bank Login Sale Ad
have hacked hosts, mail lists, php mailer send to all inbox	Hacked Host, Mailing List, Mailer Sale Ads
i need 1 mastercard i give 1 linux hacked root	Credit Card Want Ad, Hacked Host Sale Ad
i have verified paypal accounts with good balance and i can cashout paypals	PayPal Sal Ad, Cashier Service Ad
Card Number: 4123 4567 8901 2345 Exp: 10/09 CVV: 123	Credit Card Data
CHECKING 123-456-XXXX $51,337.31 SAVINGS 987-654-XXXX $75,299.65	Bank account numbers with balance

Für die Auswertung der Logfiles wurden drei verschiedene Methoden verwendet:

Manuelle Auswertung Dazu wurden zufällig aus dem gesamten Datenbestand ca. 3700 Nachrichten ausgewählt und manuell von den Autoren klassifiziert. Die oben angegebene Tabelle stammt aus diesem Teildatenbestand.

Syntaktische Auswertung Bei der syntaktischen Auswertung wurden hauptsächlich mit Regular Expressions nach Daten bestimmten Typs und Formatierung

gesucht. Soweit möglich wurden für gefundene Daten zusätzliche Methoden zur Prüfung verwendet um sicherzustellen, dass die gefundenen Daten korrekt zugeordnet wurden. Bei Kreditkarten erfolgte dies z.B. über die Luhn-Prüfsumme [4]. Bei Sozialversicherungsnummern wurde anhand externer Datenbanken geprüft ob die gefundene Nummer innerhalb eines gültigen Bereiches liegt. Bei IP-Adressen erfolgte eine Prüfung gegen DNS Blacklists.

Semantische Auswertung Die semantische Auswertung erfolgte durch Verfahren aus dem Bereich des maschinellen Lernens (für Interessierte: support vector machines). Als Trainingsmaterial für die Algorithmen wurden 70% der manuell ausgewerteten Datensätze verwendet. Die verbliebenen 30% wurden als Kontrolldaten für den Algorithmus verwendet.

Insgesamt wurden die Chatdaten in 60 Kategorien eingeteilt. Was nicht bewertet werden konnte ist der private Teil der Kommunikation. Es ist davon auszugehen, dass ein Großteil der eigentlichen Transaktionen in privaten Channels erfolgt und die öffentlichen Channels nur der Werbung und ersten Kontaktaufnahme dienen.

2 Marktanalyse

In diesem Kapitel werden die Ergebnisse bei der Analyse des Untergrundmarktes näher betrachtet. Ich fasse dabei die Ergebnisse der Autoren sehr stark zusammen. Wer an den Quellmaterialien oder Trendgrafiken über den Beobachtungszeitraum zu den einzelnen hier angegebenen Ergebnissen interessiert ist, verweise ich auf das Kapitel 3 in der Originalarbeit.

Als erstes betrachten wir die Verteilung der geposteten sensitiven Daten:

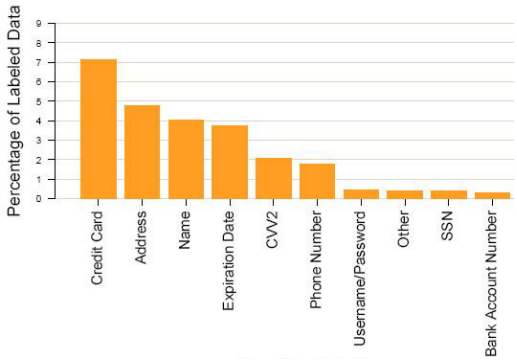

Abbildung 1: Verteilung der sensitiven Daten

Für Abbildung 1 wurden die 3700 manuell klassifizierten Nachrichten als Datengrundlage verwendet. Es wurden dabei weder Wiederholungen von Daten entfernt, noch die Korrektheit der Daten geprüft. Die Abbildung soll nur einen Überblick über die Verteilung der sensitiven Daten zeigen.

2.1 Kreditkartendaten

Mit ihrer festen Struktur der Kartennummer eignen sich Kreditkartendaten sehr gut zur automatischen Erkennung. Zusätzlich können noch offensichtlich falsche Kartendaten durch die Luhn-Prüfsumme identifiziert werden. Eine Garantie, dass die Kreditkarte zum Zeitpunkt des Postings auch tatsächlich verwendbar war liefern uns die Logdaten jedoch nicht.

In dem gesamten Datensatz befanden sich:

- 974.951 Nachrichten mit Kreditkartendaten
- das entspricht ca. 7,4% der gesamten Logfiles
- insgesamt enthielten die Logfiles 100.490 unterschiedliche Kreditkarten

Die häufigsten vertretenen Kreditkartenorganisationen waren:

Card Type	Valid Luhn Digit	Invalid Luhn Digit
Visa	53.321	6.540
Mastercard	26.581	6.486
American Express	5.405	265
Discover Card	1.836	56
Total	87.143	13.347

Um einen Eindruck der Echtheit dieser Daten zu erhalten wurden 181 Kreditkartendaten bei einem Dienstleister überprüft, der die Nummern von gestohlenen oder illegal im Internet verfügbaren Kreditkarten in einer Datenbank sammelt (StolenIDSearch von TrustedID). 51% der 181 Kreditkarten wurden in der Datenbank geführt und können damit als echt angesehen werden.

Um zu verstehen woher die Kreditkarten stammen, wurden die Daten manuell gesichtet. Dabei fielen über 1300 Kartendaten auf die mit dem Label AOL versehen waren. Evtl. Phishing-Opfer die mit der Nutzung ihres AOL-Accounts auch ihre Kreditkartendaten unwissentlich an die Kriminellen weitergeben haben.

Daneben scheinen viele Daten direkt aus Datenbanken Exports zu stammen, erkennbar an den typischen Feldbegrenzern.

Weitere Zahlen zu den gesammelten Kreditkartendaten:

- es werden ca. 400 gültige neue Kreditkartendatensätze pro Tag gepostet
- trotz der leichten Erkennbarkeit werden ca. 90 ungültige pro Tag gepostet
- 40% der Kreditkarten werden maximal eine halbe Stunde lang angeboten
- 17% der Kreditkarten werden nur von einer Quelle gepostet, 50% von maximal 4 unterschiedlichen Quellen

In Abbildung 2 ist die Herkunft der Kreditkarten angegeben. Dabei handelt es sich um das herausgebende Land. Die Information wo die Karten eingesetzt wurden und wo sie kompromittiert liegt nicht vor. Für einen rein englischsprachigen Markt eine überraschend internationale Verteilung der Herkunftsländer.

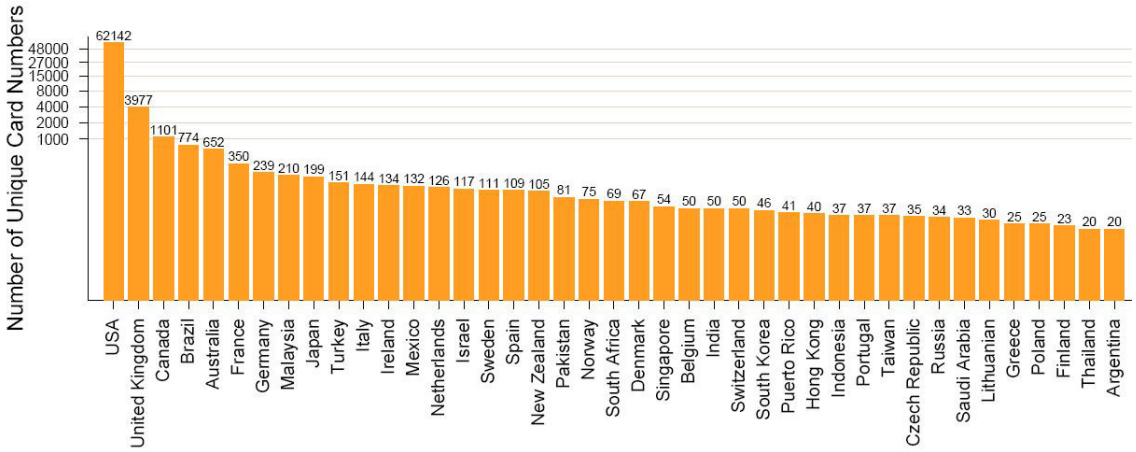

Abbildung 2: Herkunftsländer der Visa und Mastercard Kreditkarten

In dem „Crime Report“ [5] aus dem Jahr 2006 wird ein durchschnittlicher finanzieller Schaden von $427,50 pro illegal verwendeter Karte angegeben. Hochgerechnet auf die in den öffentlichen Channel geposteten Kreditkartendaten ergibt sich ein möglicher Schaden von 37 Millionen Dollar.

2.2 Finanzdaten

Neben Kreditkartendaten finden sich auch Kontoverbindungen und Kontostände in den Logfiles. Diese Finanzdaten scheinen meist direkt per Cut and Paste von den Webseiten der gehackten Accounts zu stammen. Vermutlich auch ein Versuch die Echtheit der Daten durch ihre Herkunft zu belegen.

Da keine Möglichkeit bestand die Korrektheit der Bankdaten und Kontostände zu überprüfen beschränkten sich die Autoren darauf die Geldbeträge dieser Daten aufzuaddieren. Die Gesamtsumme der geposteten Kontostände betrug über 55 Millionen Dollar.

2.3 Social Security Number

Die Social Security Number (SSN) wird im amerikanischen Raum nicht nur von der Sozialversicherung im Gesundheitswesen verwendet, sondern auch von Behörden und privaten Unternehmen als Identitätsnachweis. Sie ist damit ein wertvolles Ziel für Identitätsdiebe.

Die SSNs besitzen ein festes Format und wurden mit Regular Expressions in den Logfiles identifiziert. Zusätzlich kann überprüft werden, ob eine SSN in den von Behörden gültigen ausgegebenen Bereich liegt. Ob jedoch eine spezielle SSN tatsächlich schon ausgegeben wurde konnte nicht geprüft werden. Eine Stichprobe mit 3% der gefunden SSNs gegen eine Datenbank mit gestohlenen SSNs (StolenIDDatabase) gab nur einen einzigen Treffer.

Die Auswertung der Logfiles ergab:

- 19.521 Nachrichten mit SSNs

- das entspricht 0,15% der gesamten Logfiles
- insgesamt enthielten die Logfiles ca. 3.900 unterschiedliche SSNs

2.4 Marktteilnehmer

Nachdem in den vorhergehenden Kapiteln die von den Teilnehmern geposteten Daten betrachtet wurden, wenden wir uns jetzt den Teilnehmern selber zu.

Zur Auswertung wurden die Nicknames und die Client-IP-Adressen der Teilnehmer herangezogen:

Aktivität der Teilnehmer

- ca. 13.000 neue Nachrichten pro Tag
- ca. 45.000 Nachrichten durch Werbescripte

Anzahl der Teilnehmer

- 113.000 unterschiedliche Nicknames
- ca. 1500 Nicknames sind pro Tag aktiv
- ca. 550 neue Nicknames pro Tag

Zeitraum der Aktivität der Teilnehmer

- 25% der Nicknames posten nur eine einzelne Nachricht
- über 50% der Nicknames posten nur innerhalb der ersten Stunde
- 5% der Nicknames sind über den gesamten Untersuchungszeitraum aktiv

Client IP Besonderheiten

- 12% der Clients werden von IPs genutzt, die von unterschiedlichen Diensten als kompromittiert oder offene Proxies geführt werden.

Vertrauensstatus der Teilnehmer:

- Um einen Status als verifizierter Teilnehmer zu erhalten waren im Schnitt weniger als 18 Datensätze mit sensitiven Daten notwendig.
- nur 5% der Teilnehmer mit „verifizierten“ Status sendeten mehr Daten.

2.5 Channel-Dienste

Bei den Channel-Diensten handelt es sich um interaktive Scripte die von den Channel-Administratoren installiert und betrieben werden. Üblicherweise handelt es sich dabei um normale Dienste für die Teilnehmer. So kann ein Teilnehmer mit dem Kommando `!seen <nick>` abfragen wann sich ein anderer Teilnehmer das letzte mal angemeldet hat. In dem beobachteten Untergrundmarkt sind jedoch auch Dienste wie z.B. die Prüfung von Kreditkartenlimits (`!cclimit <CC>`) oder die Herkunft von Kreditkarten anhand ihrer Nummer (`!bank <CC>`) üblich.

Neben dem Ergebnis das die illegalen Dienste intensiv genutzt werden (z.B. `!cclimit` über 129.000 mal), zeigte sich das auch die Kriminellen betrogen werden. Eine Reihe von Channel-Services lieferten keine korrekten Daten. Die notwendigen Abfragen von externen Datenbanken waren überhaupt nicht in dem

Scriptcode implementiert. Scheinbar werden die Channel-Services von den Administratoren genutzt um selber über dieses *phishing* an sensitive Daten zu gelangen.

3 Gehandelte Waren und Dienstleistungen

Die in dem Kapitel 2 untersuchten sensitiven Daten werden von den Teilnehmern nur gepostet um ihre eigentlichen Geschäfte zu bewerben. In diesem Kapitel betrachten wir die beworbenen und gesuchten Waren und Dienstleistungen.

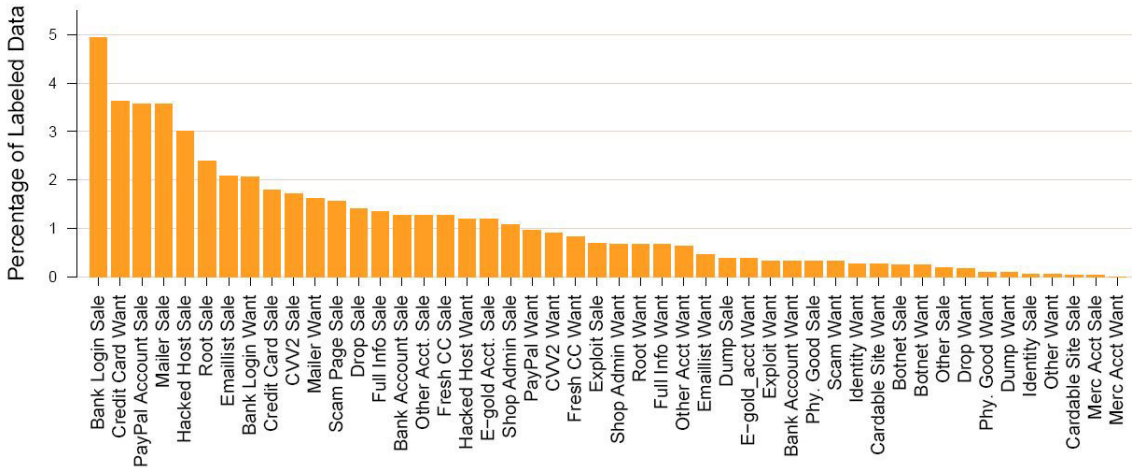

Abbildung 3: Verteilung der beworbenen und gesuchten Waren

In Abbildung 3 findet sich die Verteilung unterschiedlicher Kauf- und Verkaufsgebote über alle klassifizierten Daten. Verkauf- zu Kaufgeboten stehen dabei im Verhältnis 2:1. Was wurde hauptsächlich gehandelt:

Kompromittierte Hosts Darunter fallen Accountdaten von kompromittierten Servern. Täglich werden über 100 neue Server gepostet. Der Preis für einen Account liegt zwischen $3 und $25 (gemittelt pro Tag).

Spam Bulk-Email-Listen für den Spamversand, aber auch Adressen von offenen Mail-Relays oder schlecht implementierten Webformularen die zum anonymen Versand von Spam genutzt werden können.

Accountdaten Das umfasst vollständige Zugangsdaten für beliebige Onlinedienste. Insbesondere Zugangsdaten für Paypal und Onlinebanking werden gehandelt.

Dienstleistungen Es werden nicht nur reale Daten gehandelt, es werden regelmäßig auch Dienstleistungen zu illegalen Aktivitäten angeboten.

Neben simplen Bankdiensten zum Geldtransfer werden auch in normalen Märkten eher unübliche Dienstleistungen angeboten. Z.B. den Betrieb von Botnetzen, die Durchführung von Denial of Service Attacken, aber auch einen „Confirmer“ Dienst. Bei Verwendung von Kreditkarten im E-Commerce werden telefonisch häufig Fragen an den Kreditkartenbesitzer gestellt. Der

Confirmer übernimmt die Rolle des Kreditkartenbesitzers und beantwortet die Fragen des Dienstleisters. Diese Dienstleistung wird in den Channels angeboten und nachgefragt.

4 Gegenmaßnahmen?

Die Beobachtung und Analyse des Marktes ermöglicht erstmals einen tiefen Einblick in die Marktmechanismen eines Untergrundmarktes. Währendessen finden unter den Augen der Beobachter tausende von illegalen Geschäften statt. In diesem Kapitel werden kurz zwei Ideen beschrieben wie man diese Märkte stören könnte.

Sybil Attack Ein Angreifer kann ein Wahlsystem manipulieren, indem er eine große Zahl von wahlberechtigten Identitäten (Sybils) erzeugt und mit ihnen das Wahlergebnis verändern kann.

In Bezug auf den Untergrundmarkt müssten verifizierte Teilnehmer in großer Zahl den Markt eindringen um dann mit falschen Angeboten die echten Händler zu schädigen, sei es durch Senkung des Preises oder durch Vertrauensverlust in den Markt.

Slander Attack Ein anderer Ansatz ist es die vorhandenen verifizierten Teilnehmer durch Falschanschuldigungen deren Vertrauensstatus zu beschädigen. Das Vertrauensverhältnis wird beeinträchtigt und auch hier ist eine Reduktion der Marktaktivitäten zu erwarten.

5 Zusammenfassung

Die Beobachtung mehrerer Untergrundmärkte hat neben einer Reihe interessanter Daten vor allem eines gezeigt: Es gibt einen aktiven und sehr lebendigen Markt mit illegalen Gütern aller Art der sich nicht in geschlossenen Benutzergruppen verstecken muss und der offensichtlich ausreichend gut funktioniert. Käufer gelangen ohne große Eigengefährdung an illegale Daten zur kriminellen Nutzung, die Lieferanten können ihre Ware frei anbieten. Eine Verfolgung der Täter erweist sich auf Grund der hohen Anonymität und den Problemen bei der Nachverfolgung von IP-Adressen über Ländergrenzen als sehr schwierig.

Wichtige Sicherheitsthemen wie der Verkauf von Exploits, Virenbau, Phishing wurden zwar nicht weiter behandelt, werden aber durchaus auch gehandelt.

Mit Vorsicht sind die absoluten Zahlen zu sehen. Insbesondere die Schätzungen zu dem Geldvolumen sind nur Annahmen auf Basis der mitgelesenen Kommunikation. Und gerade auf Grund der Anonymität ist von einer hohen Rate an Betrugsversuchen unter den Marktteilnehmern zu rechnen.

Ein ständiges Überwachen dieser Untergrundmärkte könnte frühzeitig neue Trends aufdecken, Marktverbreitung von neuen Schwachstellen zeigen oder eine aktuelle Quelle sein um die Eintrittswahrscheinlichkeit von bestimmten Sicherheitsrisiken besser abschätzen zu können.

Literatur

[1] Jason Franklin, Adrian Perrig, Vern Paxson, Stefan Savage: *An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants*. Carnegie Mellon University, 2007.

[2] Lutz Donnerhacke, de.comp.security.firewall FAQ. `http://www.iks-jena.de/mitarb/lutz/usenet/Firewall.html`, 12.2007

[3] Jarkko Oikarinen and Darren Reed. *Internet relay chat protocol*. RFC 1459, 1993

[4] *Luhn-Algorithmus*, `http://de.wikipedia.org/wiki/Luhn-Algorithmus`, Version vom 2.6.2008

[5] Internet Crime Complaint Center. Internet crime report. `http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf`, Jan. - Dec. 2006