G Data

Whitepaper 04/2010

Underground Economy - Update 04/2010

Marc-Aurél Ester & Ralf Benzmüller
G Data SecurityLabs

Geschützt. **Geschützter. G Data.**

Inhalt

Auf einen Blick

Polizeischlag gegen die Untergrund-Community

- Die Polizei führte in Deutschland und Österreich Hausdurchsuchungen durch. Dabei wurden rund 50 Wohnungen durchsucht und 4 Personen vorläufig festgenommen.
- Die Razzien zerschlugen das im Untergrund etablierte Forum der „1337 Crew“ (Aussprache: li:t kru:), die laut Polizeiberichten unter anderem für ein Botnetz von über 100.000 infizierten PCs zuständig sind.
- Auch viele andere Boards und Shops sind seit den Razzien nicht mehr online. Die Abschaltungen sind einerseits Vorsichtsmaßnahmen zum Schutz vor Polizeiaktionen und andererseits Notwendigkeit, da einige weitere Untergrundmitglieder verhaftet wurden. Viele Onlinekriminelle haben sich seitdem aus der Szene zurückgezogen – zeitweise oder auch endgültig.
- Der Ausfall des „1337 Crew“ Boards hatte nicht die weitreichende Veränderung zur Folge, die erwartet wurde. Der Schwarzmarkt ist weiterhin aktiv und hat in seinen Strukturen nur wenig Veränderung erfahren. Einige Boards versuchen die Nachfolge der „1337 Crew“ Plattform anzutreten.

Bezahldienstleister Paysafecard attackiert

- Ein beliebtes Zahlungsmittel auf dem Online-Schwarzmarkt ist die Paysafecard. Eine im Februar 2010 eingeführte Änderung des Benutzungssystems hatte jedoch zur Folge, dass große Mengen des sich im Umlauf befindlichen Geldes „eingefroren“ waren. Die Cyber-Kriminellen riefen zu DDoS-Attacken gegen den Paysafecard Dienstleister auf. Die Änderung des Systems wurde am folgenden Tag revidiert.

Veränderungen auf Handelsplattformen und in Foren

- Auf etablierten Untergrundmärkten ändern sich die Verkaufsstrukturen: Mussten früher lediglich Exklusiv-Verkäufer für ihren Shop zahlen, werden aktuell alle Shop-Betreiber zur Kasse gebeten. So sollen unter anderem Betrüger ferngehalten werden.
- Die Betreiber der kriminellen Plattformen haben dazu gelernt und legen mehr Wert auf Anonymität, Sicherheit und Reputation. Dazu werden unter anderem Aufnahmegebühren für die Mitgliedschaft in den Foren eingeführt. Zusätzlich werden interne Mitgliederbewertungen in Ranglisten immer wichtiger.

Veränderungen auf Handelsplattformen und in Foren

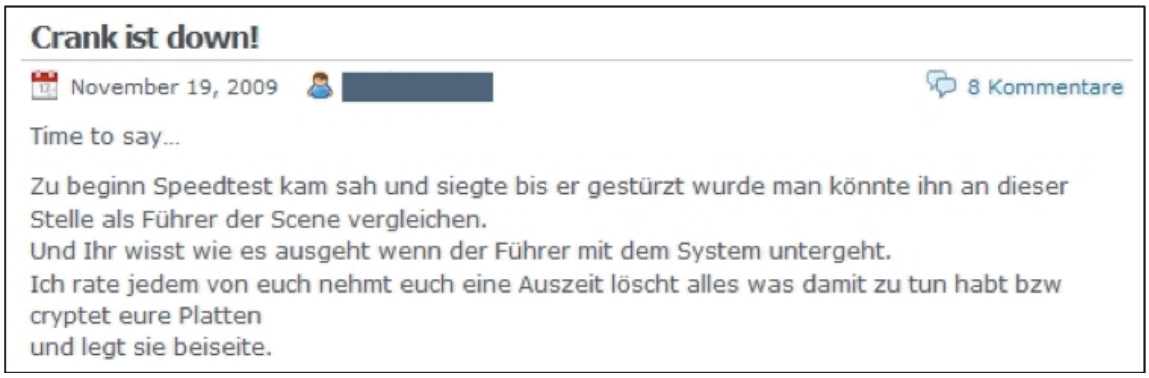
- Insgesamt ist das Preisgefüge seit der letzten Untersuchung stabil geblieben und Schwankungen ergeben sich durch die Wahl des Händlers, Rabatte, Verhandlungsgeschick bzw. Angebot und Nachfrage.

Einleitung

Seit dem ersten G Data Whitepaper über die Underground Economy im September 2009 hat sich einiges geändert. In der nun vorliegenden Untersuchung widmen wir uns den aktuellen Geschehnissen in der Schattenwirtschaft. Insbesondere der Schlag der Polizei im November 2009 gegen die ☞„1337 Crew“ hatte für die deutsche und österreichische Szene nachhaltige Konsequenzen.

Razzien in der Szene

Nach Hausdurchsuchungen im November 2009 hat sich im Umfeld der Onlinekriminalität einiges getan. Über 200 Polizisten aus Deutschland und Österreich führten Razzien (*Raids*) in rund 50 Wohnungen durch und nahmen vier Personen vorläufig fest. Ein besonderer Schlag gelang der Polizei gegen das wohl größte deutsche Untergrundforum: Die Plattform der ☞„1337 Crew“[1].
Im Umfeld der Computerkriminellen wird spekuliert, dass der Anführer des Forums (*Boards*), Pseudonym „Speedtest“, schwach geworden sei und der Polizei eine Menge an belastendem Material ausgehändigt habe. Onlinekriminelle warfen ihm Verrat vor. Bisher ist jedoch noch nicht öffentlich bekannt, welche Informationen er den Behörden gegeben oder vorenthalten hat. Fakt ist jedoch, dass besagter Kopf der Cyberbande bereits am Tag der Festnahme wieder auf freiem Fuß war.



Screenshot 1: Post auf einem Untergrund-Blog zu den Durchsuchungen im November

Polizeiberichten zu Folge soll die „1337 Crew“ unter anderem ein ☞ Botnetz mit über 100.000 infizierten PCs (☞ Zombie-PC) betrieben haben, wobei Informationen aus dem Untergrund darauf schließen lassen, dass es noch viel mehr PCs sein könnten.

Nicht nur das *Board* der „1337 Crew“ war von den Razzien betroffen. Auch viele andere *Boards*, Blogs oder auch Shops stellten ihre Aktivitäten ein und waren offline - teils aus Vorsicht, jedoch auch, weil Mitglieder verhaftet wurden. So gab es auch als „Vorsichtsmaßnahme“ eine ☞ DDoS-Attacke gegen ein *Board*, da befürchtet wurde, dass die Polizei Zugriff auf dieses hat.

[1] Die Erklärungen für Fachbegriffe, die mit ☞ gekennzeichnet sind, stehen im Glossar im Anhang.

Screenshot 2: Auch ein in der Szene sehr bekannter Shop-Anbieter hat seine Pforten wohl endgültig geschlossen, auch wenn dort seit Ende November zu lesen ist, dass man bald wieder online sein werde.

Auswirkungen auf Waren und Dienstleistungen

Entgegen der Erwartung hat der Ausfall einer der bekanntesten Communities kaum einen Einfluss auf den Markt gehabt. Angebot und Preise haben sich nach den Polizeiaktionen nicht großartig verändert und variieren, wie üblich, von Händler zu Händler. Dies ist unter anderem darauf zurückzuführen, dass große Teile des Untergrunds im Ausland beheimatet sind und die 50 Wohnungen/User, die Besuch von den Behörden bekamen, bestenfalls als Tropfen auf dem heißen Stein zu sehen sind.

Name	Preis / €
Packstationen (gephished)	
Postnummer + Off-Pin + On-PW	30
Postnummer + Off-Pin + On-PW + Mail	50
Postnummer + Off-Pin + On-PW + SMS Aus	40
PayPal Accounts	
PayPal + Bank mit E-Mail	4
PayPal + CC + Mail Guthaben: 1.290,71	20
PayPal + CC mit E-Mail	8
PayPal + eBay mit E-Mail	10
Mobilfunk	
25 Vodafone D2 Sim-Karten (auch an PS)	25
6 Vodafone D2 Sim-Karten (Versand an PS)	10
8 Vodafone D2 Sim-Karten (kein Versand an PS)	10
Pharma	
Viagra - 1 Blister - 4 Stück	20

Name	Preis / €
Steam-Accounts	
Aliens vs Predator Uncut	10
Call of Duty: Modern Warfare 2 UNCUT	15
Counter-Strike 1.6	7
Counter-Strike: Source	10
Left4Dead 1	10
Left4Dead 2 Uncut	15
Metro 2033 Uncut	12
Orange Box	10
Supreme Commander 2	12
Gametime & Points	
1000 Wii Points	5
50 EUR PlayStation Network Card	18
800 XBOX Points	5
NCSoft 60 Tage Game Time	10
World of WarCraft 60 Tage Game Time	10
Xbox Live 12 Monate Gold	15
Xbox Live Points Card 4200	18

Tabelle 1: Aktuelle Preisbeispiele aus Untergrund-Shops

Nach wie vor ist in den Untergrundnetzwerken alles erhältlich, was das kriminelle Herz begehrt - von Kreditkarten über gefälschte Dokumente in jeder nur erdenklichen Ausführung, bis hin zum kompletten ☞ Skimming-Equipment für mehrere tausend Euro, um Datendiebstahl an Geldautomaten zu betreiben.

Abb. 1: MSR500M, Portables Kartenlesegerät, ca. 220 - 270 US-Dollar

Abb. 2: Komplettes Skimming-Equipment, z.B. GSM Skimmer, 2.000 - 6.000 US-Dollar

Desweiteren ist zu beobachten, dass immer mehr „professionelles" Equipment in den Untergrundforen gehandelt wird. Gemeint sind Dinge wie Kreditkartenrohlinge, die man im Wunschdesign bestellen kann. Die Preise reichen hier von rund 50 bis 150 Euro pro Kartensatz, Mindestbestellmenge ist dabei meist 10 Stück oder mehr. Auf diese Rohlinge werden dann gestohlene Kreditkartendaten kopiert und zum Bezahlen im Einzelhandelsgeschäft genutzt. Dieses *Instore-Carding* hat den Vorteil, dass man die Ware direkt in Empfang nehmen kann und man so nicht auf Mittelsmänner beim Versand oder Postboxen angewiesen ist. Jedoch muss man persönlich in einen Laden gehen, was eine gehörige Portion mehr Schneid verlangt, als rein virtueller Kreditkartenbetrug.

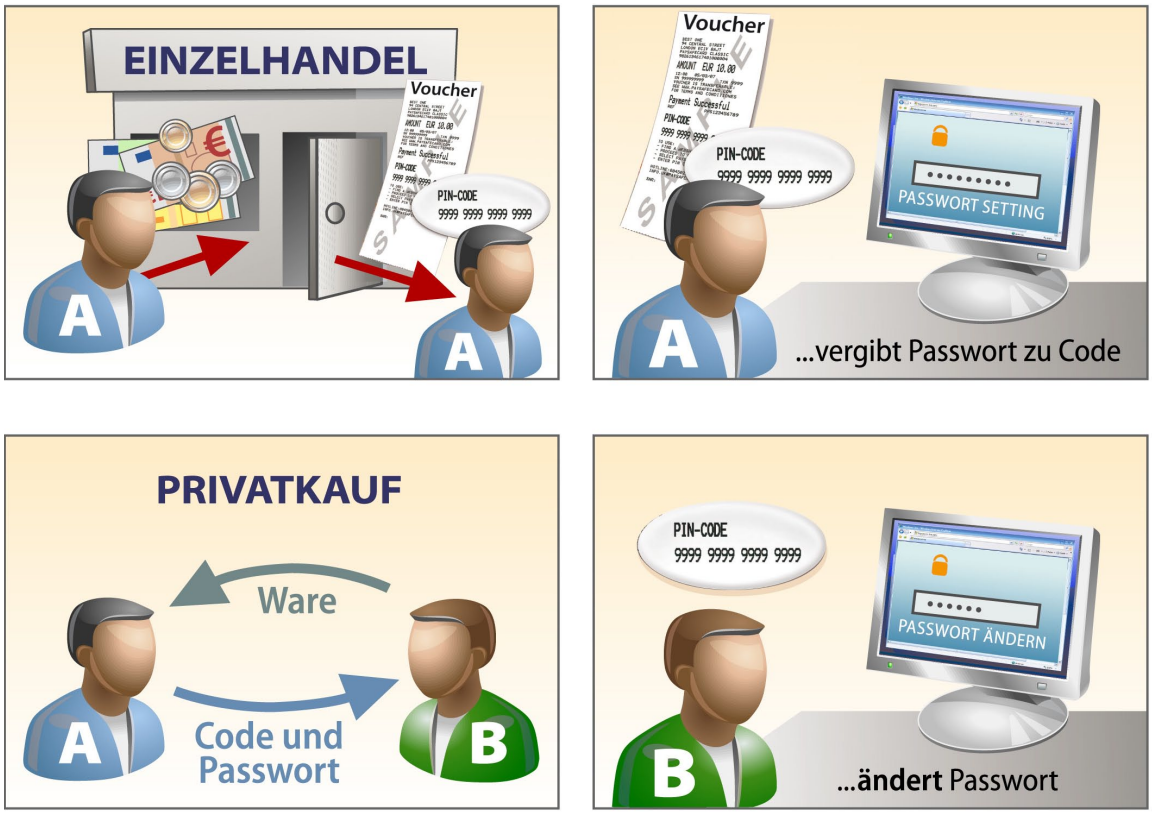
Carding Equipment	Von	Bis	
Kreditkartenrohlinge	45 US-Dollar	150 US-Dollar	Je nach Umfang, z.B. mit Hologramm oder ohne etc. Abnahme meist mind. 10 Stück
Kartendrucker	450 Euro	3500 Euro	Drucker zum Bedrucken von Kartenrohlingen
Kartenleser	250 Euro	900 Euro	Mobile Kartenleser zum Auslesen von Kredit- oder auch Bankkarten
Skimming Set	1.500 US-Dollar	10.000 US-Dollar	Abhängig von Ausführung etc., Funk-Skimmer oder auch Video-Skimmer

Tabelle 2: Aktuelle Preisspanne verschiedener Carding-Produkte aus Untergrund-Shops

Das Beispiel „Paysafecard“

Ein Aufschrei ging durch die Szene, als der elektronische Bezahldienst ☞ Paysafecard (im Folgenden kurz PSC) vor kurzem eine Änderung im Benutzungssystem einführte: Die Änderung betraf die Benutzung von Passwörtern mit einer Paysafecard.

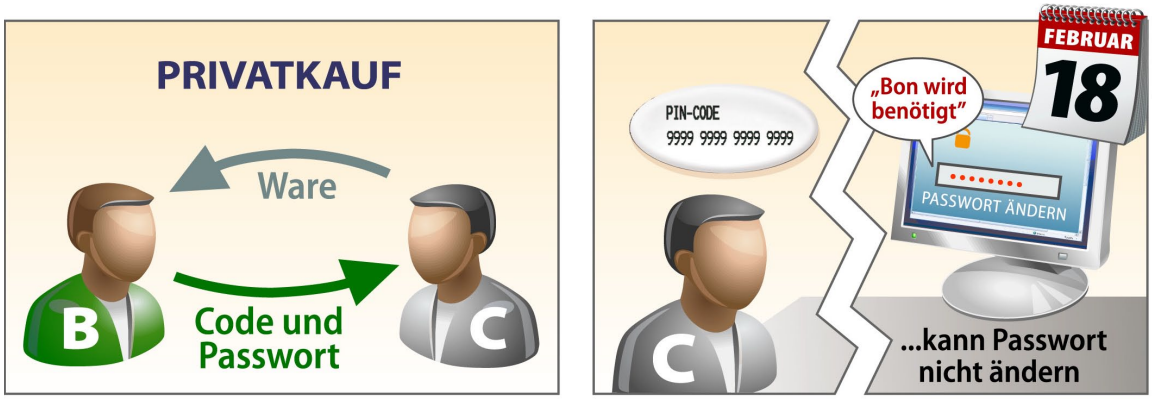
Im Regelfall setzten Besitzer einer Paysafecard ein Passwort, um bei der Bezahlung mit der Karte oder der Weitergabe des Guthabens an andere eine zusätzliche Sicherung zum 16-stelligen PIN-Code zu haben. Die folgenden Grafiken verdeutlichen die Funktionsweise:



Fallbeispiel:

Person A kauft Ware von Person B. Da die Bezahlung anonym erfolgen soll, kauft Person A zunächst Guthaben in Form von Paysafecards und gibt als Bezahlung den PIN-Code und das Passwort einer oder mehrerer PSCs an Person B weiter. Person B ändert dann auf der Homepage des Bezahldienstleisters das Passwort zu der Karte/den Karten und ist im Besitz des Geldes. So ist es möglich, das einmal gekaufte Guthaben beliebig oft an andere Personen weiterzuleiten.

Am 18.02.2010 entschied sich der Bezahl-Dienstleister jedoch dazu, das einfache Hinzufügen von Passwörtern zu neuen PIN-Codes und das Ändern von Passwörtern von alten PIN-Codes zu deaktivieren. Das Einrichten eines neuen Passwortes oder Ändern eines alten Passwortes wollte der Support nur nach Einsendung einer Kopie des Kassenbons durchführen.



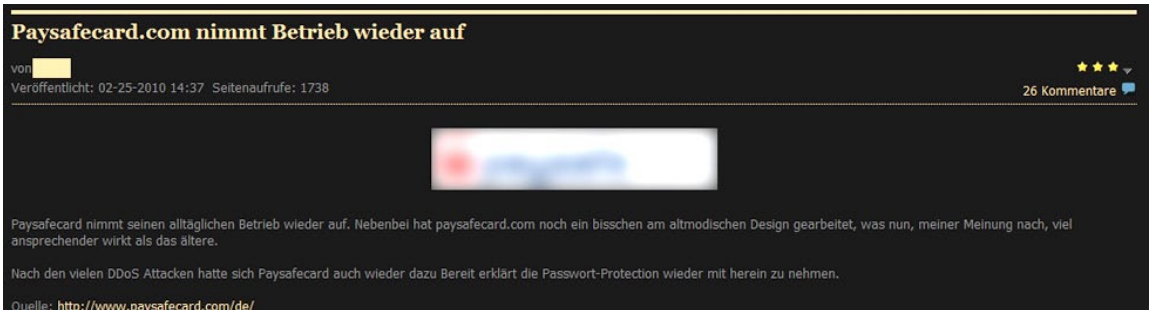
Fallbeispiel:
Sollte das Geld inzwischen bei Person C angelangt sein, weil Person B die Paysafecard-Daten ebenfalls zum Bezahlen benutzt hat, ist es für Person C extrem schwierig bis unmöglich, an einen Scan des Kassenbons von Person A zu gelangen. Somit ist das auf der Paysafecard gespeicherte Geld quasi eingefroren.

Natürlich waren alle Kunden des Paysafecard-Dienstes von dieser Neuregelung betroffen, doch gerade auf dem virtuellen Schwarzmarkt wurde diese Währung für die Untergrund-Gemeinde nun quasi über Nacht wertlos. Als Konsequenz darauf wurde auf Blogs und *Boards* zu DDoS-Attacken gegen die Website des Betreibers, www.paysafecard.com, aufgerufen.

Screenshot 3: Ein Aufruf zur DDoS-Attacke gegen den Bezahldienst Paysafecard

Es kam zu längeren Ausfallzeiten (*Downtime*) der PSC-Homepage, wobei jedoch nicht bekannt ist, ob es schlussendlich durch die Angriffe begründet war, oder durch Wartungsarbeiten, wie offiziell verlautbart.

Nur einen Tag nach den DDoS-Aufrufen, am 19.02.2010, revidierte der Bezahldienstleister seine neue Passwortpolitik. Zum 22.2.2010 sollte eine Einrichtung und Änderung eines Passworts auch wieder ohne die Einsendung des Kassenbons möglich werden. Ein Hackerangriff bleibt offiziell unerwähnt, jedoch rühmt sich der Untergrund damit, dass sie der Grund für die Umstellung waren.

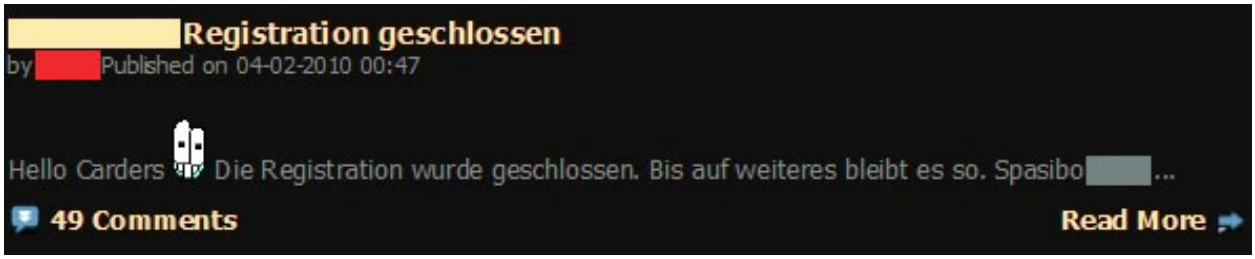


Screenshot 4: Forenmitglieder kommentieren Paysafecard

Prognose zur Entwicklung der Underground Economy

Wie erwartet, sind binnen kurzer Zeit ein gutes Dutzend neue *Boards* aufgetaucht, die sich alle selbst als Nachfolger der „1337 Crew" sehen. Einige von diesen neuen *Boards* sind jedoch auch schon wieder offline, meist verursacht durch Hacking-Angriffe.

Einige der Untergrund-Communities gingen zeitweise interessante Wege, um sich zu schützen. So gab es in einer von ihnen zum Beispiel eine Aufnahmegebühr. Hier musste man in virtueller Währung, zum Beispiel mit einer Paysafecard, 10 Euro an das Board überweisen, um überhaupt aufgenommen zu werden und aktiv im Forum mitwirken zu können. Diese Anmeldung gegen Bezahlung wurde jedoch nach Streitigkeiten in der Führung wieder abgeschafft. Zurzeit ist gar keine Anmeldung für dieses Untergrundforum möglich – eine Begründung dafür ist nicht bekannt.

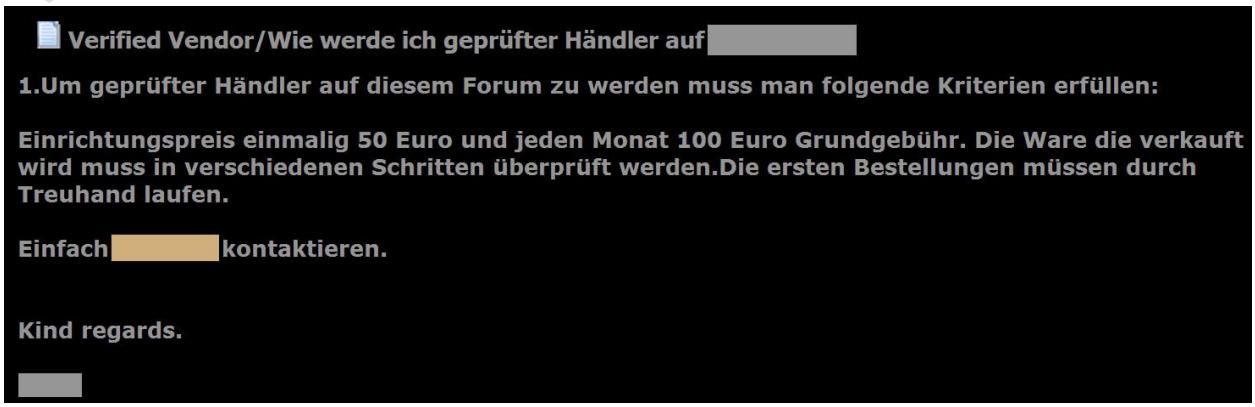


Screenshot 5: Aktuell ist seit Anfang April keine Registrierung mehr möglich.

Auch die Regeln für das Verkaufen von Waren haben sich geändert: Es gab auf diesem besagten *Board* mit Aufnahmegebühr auch Händler-Monopolstellungen, *Patente* genannt.

Gegen eine Summe von mehreren hundert Euro, erhielt der Interessent/Verkäufer das alleinige Recht, *Patent*, beispielsweise Kreditkarten auf dem *Board* anzubieten. Man konnte sich jedoch auch für weniger Geld eine Shop-Lizenz kaufen, wenn man dort seine Waren anbieten wollte – natürlich dann nur in anderen Geschäftsbereichen, als dem Monopolbereich.

Mittlerweile gibt es nur noch normale Händlerlizenzen. Die so genannten Verkaufspatente wurden abgeschafft. Nun muss jeder Verkäufer einen Betrag zahlen, um die Verkaufsberechtigung zu erhalten. Das Prinzip spült Geld in die *Board*-Kasse und soll vor internen Scammern, Betrügern, schützen.



Screenshot 6: Board-Regeln zum Einrichten eines Shops

Natürlich gibt es auch neue Shops. Einige Alte sind ebenfalls noch im Geschäft. Oft gehören diese etablierten und auch neuen Shops direkt zu einem der *Boards* oder dem engerem Dunstkreis.

Es ist ebenfalls zu beobachten, dass immer mehr Wert auf die Reputation gelegt wird. So werden auf den *Boards* Ranglisten, *Rankings*, eingerichtet, anhand derer man sehen kann, welchen Status der jeweilige User auf dem *Board* inne hat. Diese Bewertung der User untereinander ist nicht neu, jedoch gewinnt sie in letzter Zeit immer mehr an Bedeutung.

Insgesamt ist festzustellen, dass die Szene sich noch mehr um ihre Sicherheit und Anonymität bemüht, als es zuvor schon der Fall war. Am Fall des „1337 Crew" Forums haben viele Mitglieder im Untergrund erkannt, dass sie nicht so sicher sind, wie es wohl viele von ihnen gedacht hatten. Viele Onlinekriminelle haben sich auch aus dem Untergrund-Tagesgeschäft zurück gezogen, vielleicht nur temporär, um nicht „mit laufendem Rechner" von der Polizei erwischt zu werden.

Fazit

Die Untersuchungen zeigen, dass die Vorsichtsmaßnahmen innerhalb des Untergrunds zunehmen – dabei zeigen sich sowohl präventive Abschaltungen von Shops und *Boards*, als auch neu aufgestellte Regeln innerhalb der Untergrund-Communities.

Viele Kriminelle sind (noch) auf Tauchstation oder in andere Foren umgezogen. Die Angst vor erneuten Razzien und Untersuchungen der Polizei scheint nicht unerheblich zu sein.

Auch nichtpolizeiliche Ereignisse im Alltag der Szene haben hartnäckige Gegenmaßnahmen zur Folge, wie am Beispiel des Bezahldienstleisters Paysafecard zu sehen war. Die Konkurrenz unter den einzelnen Händlern war in diesem Fall ausgeblendet, für die gemeinsame Sache.

Dadurch dass die Untergrund-Community die Schutzmechanismen erhöht und sich zudem auf weniger, scheinbar besser gesicherte Plattformen konzentriert, wird es schwieriger werden, nachzuvollziehen, was im Untergrund passiert.

Anhang: Glossar

1337 Crew: (Aussprache: li:t kru:) Der Begriff „1337 Crew“ ist ein Eigenname. Er entwickelte sich aus der in IT-Kreisen bekannten Leetspeak, einer Kunstsprache. Dabei werden Buchstaben durch ähnlich aussende Ziffern ersetzt. Das Wort Leetspeak würde in dieser Kunstsprache als „13375P34K“ geschrieben. Leet, oder eben 1337, steht dabei als eine Art Abkürzung für das englische „Elite“.

Botnetz: Ein Botnetz ist ein Verbund aus so genannten Zombie-PCs. Zur Verwaltung des Botnetzes werden Command-and-Control-Server (C&C Server) genutzt. Botnetze werden unter anderem dafür benutzt, gezielte Überlastangriffe auf Webserver zu starten (DoS- und DDoS-Attacken) und um Spam zu versenden.

Bot: Bots sind kleine Programme, die meist unbemerkt im Hintergrund auf den Rechnern der Opfer laufen und dort je nach Funktionsumfang diverse Dinge erledigen – von DDoS-Attacken über E-Mail-Spam bis zum Mitlesen von Tastatureingaben und vielem mehr. Der Funktionsumfang ist primär eine Frage, wie viel Geld man für einen Bot anlegen möchte. Bots mit einem sehr großen Umfang sind naturgemäß teurer als eher einfache Bots, die nur wenig können.

DoS (Denial of Service): Bei einer Denial-of-Service-Attacke werden Rechner (meist Webserver) mit gezielten und/oder sehr vielen Anfragen bombardiert. Dadurch können sie ihre Dienste nicht mehr ausführen und brechen unter der Last zusammen.

DDoS (Distributed Denial of Service): Eine Distributed-Denial-of-Service-Attacke basiert auf demselben Prinzip wie eine DoS-Attacke, jedoch mit dem Unterschied, dass der Angriff von vielen Rechnern aus - also verteilt - durchgeführt wird.

Paysafecard: Das System der „Paysafecard“ ist eine Online-Bezahllösung, als Ersatz für Kreditkarten, Bankkonto oder Bargeld. Man kann diese Karten mit festgelegten Guthaben zwischen 10 und 100 Euro in einer Vielzahl unterschiedlicher Verkaufsstellen erwerben, z.B. Tankstellen, Drogeriemärkten, Lotto-Annahmestellen oder Kartenautomaten für Mobilfunkguthaben und kann das eingekaufte Guthaben im Internet zur anonymen Bezahlung nutzen. Diese gegebene Anonymität macht den Service für normale Einkäufer ebenso interessant, wie für Untergrundhändler.

Skimming: Beim Skimming wird technisches Gerät, wie zum Beispiel Kartenleser und eine Kamera, an einem Geldautomaten angebracht. Der Kartenleser liest die Daten vom Magnetstreifen der Karte des Opfers, während die Kamera die PIN-Eingabe filmt. Die so gewonnenen Daten werden anschließend auf einen gefälschten Kartenrohling überspielt und im Ausland für Zahlungen verwendet. Die Kosten für das Equipment sind recht hoch. In einschlägigen Foren spricht man von einigen tausend Euro, um die nötige Hardware zu erwerben. Mit ein wenig Geschick und Bastelei können die Kosten auf ein paar hundert Euro reduziert werden.

Spam: Mitte der 90er Jahre bezeichnet Spam die übermäßige Verbreitung der gleichen Nachricht in Usenet-Foren. Der Begriff selbst geht auf einen Sketch von Monty Python zurück. Mittlerweile

verwendet man Spam in mehreren Bedeutungen. Als Oberbegriff steht Spam für massenhaft unaufgefordert zugesandten E-Mails. In einem engeren Sinn beschränkt sich der Begriff Spam auf Werbemails; das heißt: Würmer, Hoaxes, Phishing-Mails und AutoResponder werden nicht dazugezählt.

Zombie-PC: Als Zombie bezeichnet man einen PC, der sich über eine Backdoor von einem Außenstehenden fernsteuern lässt. Analog zum filmischen Vorbild gehorcht der Zombie-PC nur noch dem verborgenen Meister und führt dessen oftmals verbrecherische Befehle aus. Viele Zombies werden zu so genannten Botnetzen zusammengefasst.