ALICIA NOORS
MARK B.

NICHTS IST SICHER

TRICKS UND TECHNIKEN VON CYBERKRIMINELLEN VERSTEHEN UND SICH SCHÜTZEN

VORWORT

Das Internet ist längst kein sicherer Ort mehr. Wo zig Millionen Euros täglich dem Besitzer wechseln sind auch Betrüger, Diebe und andere Kriminelle nicht weit...

Wir treffen bei unserer Arbeit immer wieder auf Fälle von Online-Kriminalität. Hierbei steigt die Zahl der Delikte und die Höhe der Schäden seit Jahren kontinuierlich an.

Wir erläutern in diesem Buch, wieviel bzw. wie wenig technisches Know-How es braucht, um an Ihr Geld zu kommen. Dabei machen wir nicht mal vor offiziellen Dokumenten oder Ausweisen halt, mit denen man Ihre Identität leicht stehlen könnte.

Sie werden erstaunt sein, mit welch einfachen Mitteln die meisten dieser kriminellen Maschen klappen und wie die kriminelle Unterwelt im Internet organisiert ist!

INHALTSVERZEICHNIS

WARUM WIR DIESES BUCH GESCHRIEBEN HABEN

Ziel des Buches ist es, zu zeigen, wie einfach und mit welch simplen technischen Mitteln Dinge, die die meisten Menschen für sicher halten, überlistet, kopiert, gefälscht oder anderweitig missbraucht werden können. Nachdem Sie dieses Buch gelesen haben, werden Sie keinem Webshop, Portal, Zahlungsmittel, Ausweis, offiziellem Dokument oder einer Firma mehr uneingeschränkt vertrauen...

Dieses Buch ist ausdrücklich nicht als Anleitung zum Begehen von Straftaten gedacht. Da nach wie vor sehr viele Personen Opfer werden, wollen wir allgemeinverständlich erklären wie einfach es ist mit entsprechender krimineller Energie an das Geld von ahnungslosen Opfern heranzukommen oder deren Identität zu missbrauchen.

Technikinteressierte sollten natürlich auch nicht zu kurz kommen und daher werden wir auch einige Dinge im Detail beschreiben und an den meisten Stellen sogar POC-Code (Proof of Concept) veröffentlichen und grob beschreiben wie dieser Code funktioniert. Dabei achten wir darauf, dass selbst Leser ohne Programmiererfahrung den Ausführungen folgen können, um noch besser zu verstehen, wie wenig hinter so mancher Technik eigentlich steckt.

Außerdem wollen wir mit der oftmals angetroffenen Behauptung aufräumen, dass Angriffe auf Computersysteme sehr schwer auszuführen sind und es sehr viel Wissens bedarf diese durchzuführen. Das stimmt zwar bedingt, allerdings nur für die Entwicklung neuer Angriffe. Die

meisten durchgeführten Angriffe basieren auf bekannten Mustern und setzen deutlich weniger Wissen voraus.

Wir gehen sogar soweit, zu sagen, dass ein Teenager mit Grundlagenwissen zum Thema Programmierung aus dem EDV-Unterricht solche Programme erstellen könnte, wenn er die Methodik dahinter kennt.

Wir sind davon überzeugt, dass sich nur derjenige Schützen kann der weiß wie die Maschen der Betrüger funktionieren und der weiß worauf es Angreifer abgesehen haben. Nur mit diesem Wissen ist man in der Lage verräterische Zeichen und mögliche Bedrohungen zu erkennen.

Programmiersprache Python

Zur Illustration der Angriffe haben wir Python als Programmiersprache gewählt, da diese Sprache sehr einfach ist. Selbst ohne Programmiererfahrung lassen sich Python-Programme mit grundlegenden Englisch-Kenntnissen gut lesen und verstehen.

Einrichtung von Python3

Wenn Sie die Programme bzw. Scripte in diesem Buch selbst ausprobieren wollen dann können Sie Python 3.x unter `https://www.python.org/downloads/`herunterladen. Zum Schreiben der Scripte können Sie die Python-IDLE verwenden und mit dem Menüeintrag `File -> New File` eine neue Programmdatei anlegen.

Interessierte finden eine kleine Einführung in Python 3 auf der Webseite `https://hackenlernen.com/blog.php?t=python_3_crashkurs`. Alternativ dazu verweise ich auf mein Buch "Programmieren lernen mit Python 3" (ISBN: 978-3746091297).

Sollten Sie weitere Module benötigen, werden Sie bei der Ausführung des Scriptes mit einem derartigen Fehler darauf aufmerksam gemacht: `ModuleNotFoundError: No module named 'requests'`

Fehlende Module können über die Eingabeaufforderung unter Windows oder das Terminal in Linux / Mac OSX wie folgt nachinstallieren:

Windows:

`py.exe -3 -m pip install [MODULNAME]`

zB: `py.exe -3 -m pip install requests`

Linux / Mac OSX:

`pip3 install [MODULNAME]`

zB: `pip3 install requests`

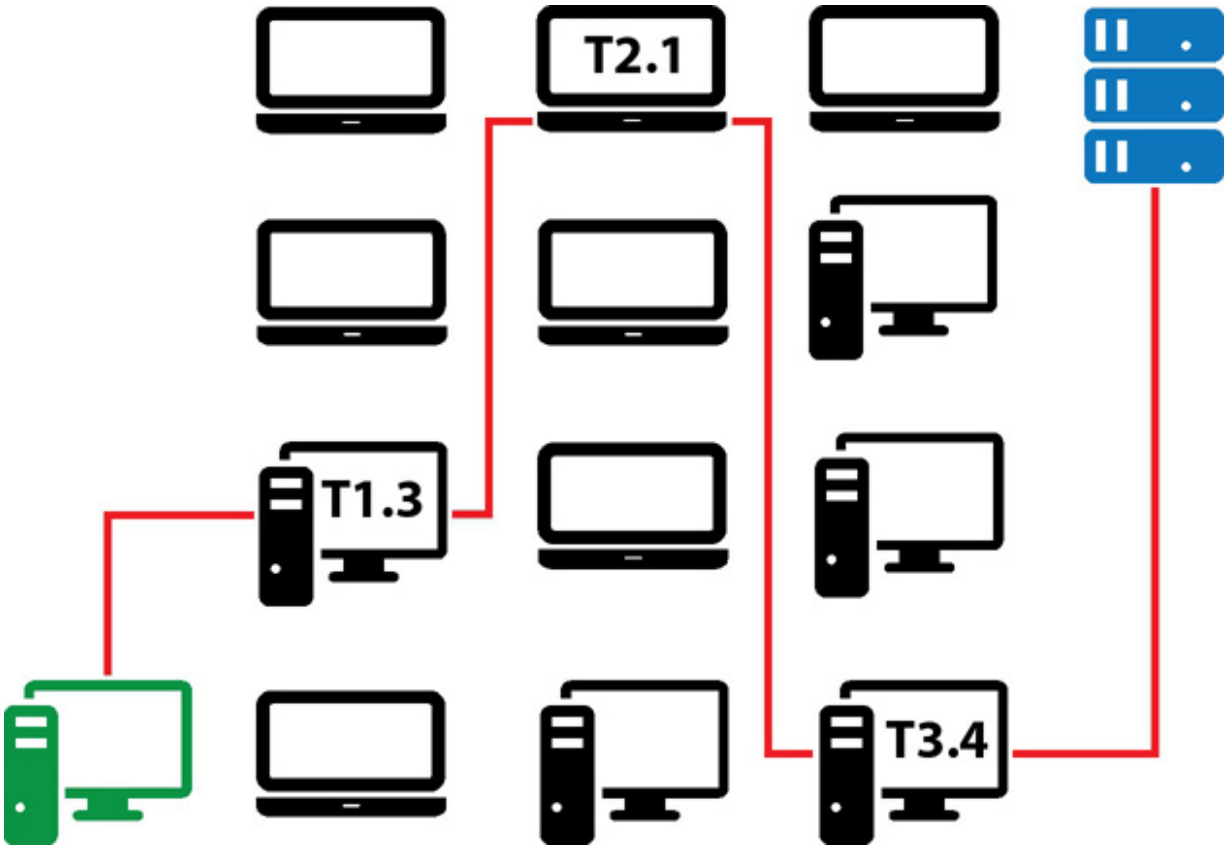
DAS DARKNET

Um diesen Begriff rankt sich derzeit sehr viel Halbwissen im Internet, daher wollen wir uns zuerst einmal ansehen was genau das Darknet ist und wie wir darauf zugreifen können.

Der Hintergrund vor dem diese Entwicklung stattfand war eine sehr erstrebenswerte Idee - Ziel war niemals die Schaffung eines rechtsfreien Raumes in dem Kriminelle ihren Geschäften nachgehen können, sondern die Möglichkeit sich Anonym und ohne jegliche Zensur auszutauschen. Daher nennen Leute in manchen Ländern dieses Netzwerk nicht Darknet, sondern das "freie Internet".

In Ländern wie China, wo die staatliche Zensur viele Inhalte unterdrückt, ist das sogenannte TOR-Netzwerk eine Möglichkeit auf sonst unzugängliche Inhalte zuzugreifen oder kritisch seine Meinung zu äußern.

Grundlage für das Darknet ist dieses TOR-Netzwerk - also sehen wir uns zunächst an wie diese Netzwerk funktioniert:



Hierbei ist der grüne Rechner unser PC, die schwarzen Rechner und Laptops sind andere Rechner im TOR-Netzwerk und in Blau ist der Server dargestellt, den wir erreichen wollen.

Unsere Anfrage an den Server wird also über die Rechner `T1.3`, `T2.1` und `T3.4` an den Server geleitet (hier in Rot eingezeichnet). Aus Sicht des Servers kommuniziert dieser mit dem Rechner T3.4 (dies ist in unserem Beispiel der sogenannte Exit-Node). Natürlich kann der User selbst entscheiden, ob sein Rechner auch als Exit-Node dienen soll oder nicht.

Der Server kann also nicht nachvollziehen wer genau auf die Dienste zugreift. Der Exit-Node sieht ebenfalls nur, dass er mit Rechner `T2.1` kommuniziert und weiß nicht woher die Daten eigentlich stammen. Selbst der Rechner `T1.3` kann

nicht sicher sein, dass der Rechner vor ihm der eigentliche Empfänger ist oder ob dieser die Daten nur für einen anderen Rechner weiterleitet.

Das ganze klingt doch sehr komplex - dank eines Tools namens TOR-Browser ist es allerdings ein Kinderspiel. Dabei handelt es sich um einen modifizierten Firefox, der inklusive TOR-Client komplett fertig vorkonfiguriert heruntergeladen werden kann. Den Download finden Sie hier:

`https://www.torproject.org/download/download.html`

Damit können Sie nicht nur auf das Darknet, sondern auch über das TOR-Netzwerk auf herkömmliche Internetseiten zugreifen. Die drei Umleitungen kosten natürlich Zeit, und natürlich wiessen Sie nicht wie schnell die Internetverbindungen der zwischengeschalteten Rechner sind - also erwarten Sie keine rasend schnelle Verbindung!

Das Darknet besteht aus einfachen Seiten, die auf einigen der Rechner im TOR-Netzwerk zur Verfügung gestellt werden. Diese Seiten sind über kryptische `.onion` Adressen erreichbar. So führt Sie `http://zqktlwi4fecvo6ri.onion` beispielsweise zum "Hidden Wiki" - einer Linktliste, die Sie tiefer in das Darknet führt.

Häufig angetroffenes Halbwissen:

Allein durch das Aufrufen von Darknet-Seiten kann mein Rechner infiziert werden!

Jein; es kommt darauf an, ob die verwendete Browser-Version durch einen bestimmten Angriff verwundbar ist oder nicht. Es gibt durchaus Techniken, die einen Rechner allein durch das Aufrufen einer Webseite infizieren können. Den gleichen Angriffscode kann jemand allerdings auch auf einer beliebigen Internetseite platzieren. So ein Angriff ist also sowohl im Darkweb als auch im Internet möglich, vor allem dann, wenn man veraltete Browser-Versionen verwendet.

Einen solchen Angriff im Darkweb mit der deutlich geringeren Nutzeranzahl aufzusetzen, macht allerdings aus unserer Sicht weniger Sinn, da man eine viel geringere Anzahl an potentiellen Opfern erhält.

Abgesehen davon ist ein deutlich höherer Prozentsatz der Darkweb-Nutzer technisch versiert, und damit werden Ihre Systeme meist sicher konfiguriert und auf dem aktuellen Stand sein, also eher nicht verwundbar gegenüber solcher Angriffe.

Schon der Zugriff auf das Darknet und die Seiten ist illegal!

Jein - auch hier kommt es darauf an auf was man zugreift. Wer im Darknet beispielsweise kinderpornografische Seiten betrachtet macht sich natürlich Strafbar. Wer hingegen auf den diversen Foren, Marktplätzen, etc. unterwegs ist, hat

durch das Betrachten der Angebote noch keine strafbare Handlung begangen, auch wenn die Angebote illegal sind.

Man macht sich erst strafbar, wenn man Kreditkartennummern für seine nächste Shoppingtour oder Drogen für das Party-Wochenende bestellt oder versucht diese zu bestellen!

Im Darknet ist alles nur Abzocke!

Die Zahl der Abzocker im Darknet ist größer als auf her kömmlichen Marktplätzen. Dies wird auch klar bei der Anonymität und der Art der Angebote... Ein geprellter "Kunde" kann schließlich schlecht zur Polizei gehen und anzeigen, dass die bestellen 5 Extasy-Tabletten nicht geliefert wurden oder die Zugangsdaten zu einem fremden PayPal-Account nicht funktionieren!

Dennoch hat sich ein erstaunlich gut funktionierendes System etabliert. Oftmals bieten die Betreiber der Marktplätze einen Treuhand-Service an. Dabei sendet der Käufer das Geld an den Betreiber und dieser bestätigt den Geldeingang gegenüber dem Versender. Wenn nun der Käufer die Ware erhält und die ordentliche und vollständige Lieferung bestätigt, wird das Geld abzüglich einer kleinen Provision an den Verkäufer ausgezahlt.

Bei Streitigkeiten wird dann im Grunde vom Betreiber entschieden wem er glaubt und wer somit recht bekommt. Meist hängt das auch von den Bewertungen ab die Käufer oder Verkäufer auf den Marktplätzen oder in den Foren haben.

Darknet und Deepweb sind das gleiche!

Falsch! Was genau das Darknet ist haben wir bereits besprochen... Das Deepweb hingegen ist jener Teil des

Internet der nicht öffentlich zugänglich ist. Das können versteckte Seiten oder einfach nur Bereiche von Seiten sein, die nur registrierten Usern zur Verfügung stehen. Darunter fallen also beispielsweise Ihr Online-Banking, die Filme und Serien bei Netflix, die nur zahlende Kunden aufrufen können oder auch ein versteckter Ordner auf einem geknackten Server, in dem ein Hacker seine Tools und Scripts abgelegt hat.

Das Tor-Netzwerk und Bitcoins bieten absolute Anonymität!

Falsch! Absolut anonym ist garnichts... Einerseits gibt es durchaus Möglichkeiten einen User eine Falle zu stellen. Ein technisch sehr primitiver Weg wäre, es beim Entpacken des Archives mit dem geklauten Kreditkartennummern auch gleich ein Programm mit zu starten, dass im Hintergrund die eigentliche IP-Adresse an einen Server meldet.

Außerdem sollen Gerüchten zur Folge amerikanische strafverfolgungsbehörden einen Exploit besitzen der das ermitteln der eigentlichen IP von TOR-Nutzern ermöglichen soll. Dafür gibt es zwar starke Indizien aber keine Bestätigung.

Bitcoin-Transaktionen werden in einer sogenannten Blockchain gespeichert. In dieser Blockchain sind alle Transaktionen von Anfang an bis zum aktuellen Zeitpunkt gespeichert, und jeder, der einen vollwertigen Bitcoin-Client am Rechner hat, besitzt auch eine Kopie dieser Blockchain, die bei Ihm lokal gespeichert wird.

Die Transaktionen in der Blockchain sind sichtbar, inklusive alle Einzahler und Empfänger. Diese Protokollierung und unbefristete, dezentrale und damit kaum manipulierbare Aufbewahrung dieser Daten ist der Zweck der Blockchain.

Dennoch ist damit nur nachvollziehbar, dass von der Wallet `1JmfaVr3x5fRKRmuhUBpWNQFy51Sfo4T6u` an die Wallet `3JPTWFkQMCCY4ToSDSWHPzhcb5roduW21U` eine Überweisung von 1,2765 Bitcoin am 17.12.2018 durchgeführt wurde.

Nun kann man allerdings das Internet nach diesen BTC-Adressen durchsuchen und somit auf herkömmlichen Servern eventuell Datenspuren entdecken.

Weiters können Behörden natürlich auch der "Spur des Geldes" folgen und die Transkationen bis zu einem BTC-Exchange oder einer Bargeld-Auszahlung an speziellen Bankomaten verfolgen. Im Falle des Wechslers kann dieser dazu aufgefordert werden zu verraten, an welches Konto oder welchen Online-Bezahldienst mit welchem Usernamen das Geld geflossen ist. Im Falle der Bankomatbehebung muss die Bankomatkarte an irgendjemanden geliefert worden sein.

Spätestens wenn das Geld die Bitcoin-Welt verlässt ist die Anonymität irgendwann nicht mehr gegeben!

Im "Darknet" treiben sich nur Verbrecher herum!

Hierbei wird in der Regel das Wort "Darknet" als Synonym für das TOR-Netzwerk verwendet, was ebenfalls nicht ganz korrekt ist. Wie eingangs bereits erwähnt, ist es in manchen Ländern ein guter Weg staatliche Zensur zu umgehen oder kritische Meinungen zu finden oder zu äußern.

Abgesehen davon sind für Sicherheitstests oftmals sehr gute Exploits (Angriffsprogramme die bestimmte Schwachstellen ausnutzen) zu finden und daher sind auch viele Sicherheitsexperten immer wieder einmal auf Hacker-Foren im Darknet unterwegs.

Außerdem lässt sich damit die ein oder andere IP-Sperre umgehen oder man kann einfach nur den Datensammelwahn mancher Webseiten einen Riegel vorschieben.

Es sind also auch viele Personen im TOR-Netzwerk unterwegs die das Darknet garnicht nutzen genauso wie andere Personen das Darknet für völlig legale Dinge verwenden.

WARENBETRUG

Eine der gängigsten kriminellen Machenschaften im Internet ist der Warenbetrug. Hierbei gibt es eine unglaubliche Vielfalt an möglichen Vorgehensweisen.

In diesem Kapitel wollen wir uns gemeinsam ansehen, wie die am häufigsten auftretenden Straftaten begangen werden.

Sehen Sie dies bitte keinesfalls als vollständige oder endgültige List an! Täglich lassen sich Betrüger neue Abwandlungen oder Kombinationen von bekannten Maschen einfallen.

Nicht existente Artikel

Dieser Betrug ist relativ simpel, aber genauso effektiv. Hierbei spielen Kriminelle mit der Gier der Menschen und bieten meist teure Markenartikel besonders günstig an.

Sehen wir uns nun gemeinsam im Detail an, wie hierbei vorgegangen wird, welche Schutzmechanismen greifen und wie diese Umgangen werden können. Als Beispiel haben wir hierzu eBay verwendet. Die hier gezeigten Vorgehensweisen lassen sich allerdings auch in identer oder leicht abgewandelter Form auf alle große Online-Handelplätze anwenden.

Zuerst benötigen wir einen eBay-Account. Dafür benötigen wir eine Email-Adresse, eine Telefonnummer auf der wir eine SMS empfangen können und eine Kreditkarte oder einen PayPal-Account.

Die Email-Adresse kann bei einem Anbieter kostenloser Email-Accounts wie GMX, GMAIL oder einem der hunterden Mitbewerber erstellt werden. Viele dieser Anbieter verlangen nicht einmal eine Telefonnummer oder ähnliches bei der Registrierung.

Die Telefonnummer stellt ebenfalls kaum eine Hürde dar. Einerseits gibt es diverse Anbieter von SMS-Diensten die gegen eine kleine Gebühr den Versand und Empfang von SMS-Nachrichten anbieten, und andererseits sind in vielen Ländern Europas Prepaid-Simkarten völlig anonym in Supermärkten, Tankstellen oder Trafiken erhältlich. Es gibt sogar Dienstleister, die den Versand von diesen Simkarten ins Ausland anbieten.

Zum Bezahlen der Auktionsgebühren benötigt man entweder eine Kreditkarte oder einen PayPal-Account. Da wir zum Erstellen eines PayPal-Kontos ebenfalls eine Kreditkarte benötigen, wollen wir uns zuerst ansehen, wie wir an eine anonyme virtuelle Kreditkarte kommen.

Einige Bezahldienste wie AdvCash, Neteller oder Skrill bieten die möglichkeit eine virtuelle Kreditkarte zu erstellen. Je nach Anbieter fallen dafür geringe Jahrengebühren zwischen 5 und 15 Euro an. Daher muss der Account vorab mit 10 bis 30 Euro geladen werden. Abgesehen von den Jahresgebühren der Kreditkarte benötigen wir noch einen Euro für die Testabbuchung von PayPal und natürlich ein paar Euro für die ersten eBay-Geschäfte, um ein paar initiale Bewertungen zu erhalten.

Um das Konto des Bezahldienstes "aufzuladen", kommen neben Bitcoins auch einige sogenannte Exchange-Anbieter in Frage. Im Grunde ist ein Online-Exchange nichts weiter als eine virtuelle Wechselstube, um von PayPal zu Neteller, Bitcoin zu Skill, Neteller zu AdvCash, etc. Guthaben zu verschieben. Natürlich fallen auch hier wieder geringe Wechselgebühren an.

Da der Weg des Geldes oftmals nachverfolgbar ist, wird das Aufladen der virtuellen Kreditkarte bzw. des Bezahldienstes ein essentieller Punkt, wenn es darum geht anonym zu bleiben. Genau aus diesem Grund werden wir hier nicht unseren Lösungsansatz veröffentlichen - wir sagen allerdings soviel - ein guter Startpunkt sind anonyme Bezahlkarten wie Paysafecard oder Bezahldienstleister mit lokalen Filialen, die eine Kassa anbieten oder bei denen man Geld mit einem Erlagschein auf ein Verrechnungskonto bei einer Bank einzahlen kann.

An diesem Punkt ist das eBay-Konto einsatzbereit und im besten Falle völlig anonym. Also widmen wir uns PayPal bevor wir den eBay-Account weiter aufauen.

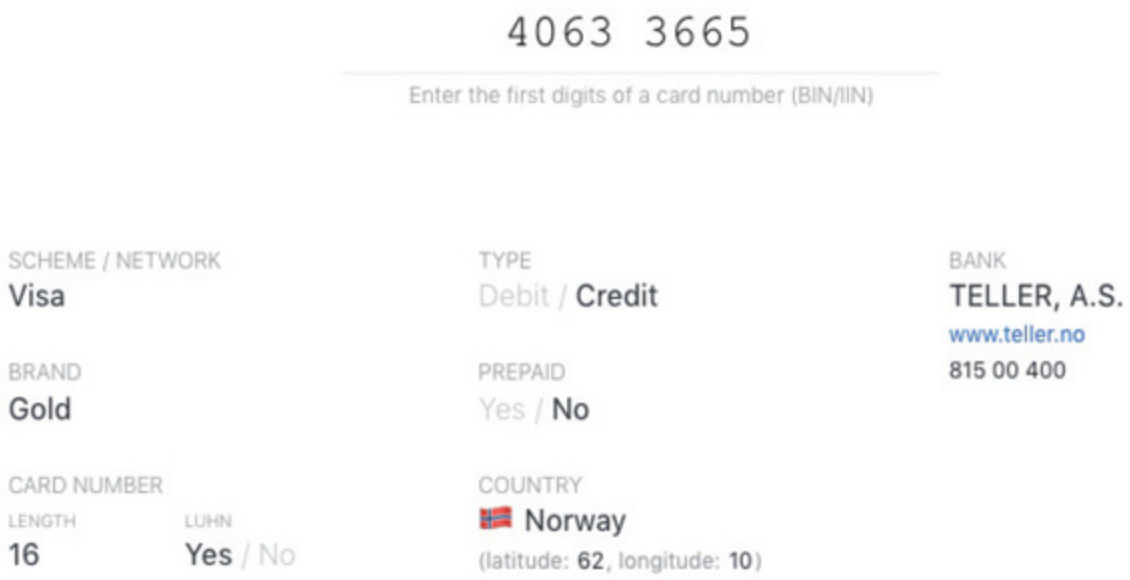
Im Grunde können wir die gleiche virtuelle Kreditkarte für PayPal verwenden, nur mit einer Außnahme - das Land der Karte bzw. der Ausstellenden Bank muss mit Land des PayPal-Kontos übereinstimmen! Daher sehen wir uns an, wie wir das Land und die ausstellende Bank aus der Kreditkartennummer auslesen können.

Auch wenn es einige Leser eventuell gefreut hätte, haben wir uns dagegen entschieden unsere Kreditkartennummern hier abzudrucken und stattdessen eine Dummy-Karte auf der Seite

`https://ccardgenerator.com/generat-visa-card-numbers.php`

mit der Kartennummer `4063 3665 1356 7751` generiert. Ein derartiger Generator kann für einige Zwecke nützlich sein - zB zum Erstellen von Demo-Accounts.

Die ersten Stellen der Kartennummern beinhalten den sogenannten Bank-Idenfier, kurz BIN. Dieser kann beispielsweise mit der Seite `https://binlist.net/` ausgewertet werden. Dank der API dieser Seite lässt sich auch die Verarbeitung verschiedenster Kartennummern automatisieren.



Nun da wir bei diesem Beispiel Norwegen als Ursprungsland der Karte ermittelt haben, müssten wir uns von Norwegen aus mit einer norwegischen Telefonnummer bei PayPal anmelden.

Zum Vortäuschen einer norwegischen IP-Adresse kann man am besten einen VPN-Anbieter wie HideMyAss!, Hide.me, etc. oder diverse Proxy-Server verwenden. Die Telefonnummer lässt sich, wie bereits zuvor, bei eBay einfach bei einem Online-Anbieter freischalten oder als Simkarte besorgen. Diese Dinge müssen stimmig zu einander passen keine zusätzlichen Prüfmechanismen anzustoßen oder mit dem Account gleich auf der Watchlist zu landen...

Nachdem das PayPal-Konto eingerichtet ist und die Kreditkarte hinzugefügt wurde, muss man nur noch bei dem verwendeten Bezahldienst in den Abbuchungen nachsehen welche Verifikations-Nummer im Abbuchungstext steht und diese bei PayPal angeben, und schon ist das Konto einsatzbereit.

Professionelle Betrüger verschleiern Ihre Identität dadurch, dass sie öffentliche WLAN-Hotspots, VPNs, das TOR-Netzwerk oder gehackte Rechner von unbeteiligten bzw. eine Kombination daraus nutzen.

Wenn Sie nun einwenden wollen, dass man an manchen öffentlichen Orten und Kaffees gefilmt wird, gebe ich Ihnen natürlich recht, aber kaum jemand wird so dumm sein, solche Dinge in dem Caffee oder einem Ort zu machen in der er persönlich bekannt oder öfter anzutreffen ist. Außerdem sitzen je nach Tageszeit genügend andere Personen mit dem Tablet, Handy oder Laptop am gleichen Ort.

Was sollen Strafverfolgungsbehörden nun machen, mit verschwommenen Ausdrucken von Standbildern der Überwachungsvideos von Haus zu Haus gehen? Abgesehen davon reichen viele WLAN-Netzwerke auch noch ein gutes Stück aus dem Lokal heraus - also ist es gut möglich, dass sich der eigentliche Täter außerhalb des Aufnahmebereichs der Kamera aufgehalten hat.

Technisch versiertere Leser würden wahrscheinlich noch anmerken, dass jede Netzwerkkarte eine MAC- bzw. Hardware-Adresse hat und diese eindeutig den Hersteller der Netzwerkkarte identifiziert und damit sind auch Rückschlüsse auf den Gerätehersteller bzw. Modell möglich. Auch da stimme ich Ihnen zu, und sofern diese protokolliert wurde und das Protokoll im Router des benutzen WLAN noch vorhanden ist, würde es natürlich die Auswahl eingrenzen, wenn zB nur 2 der 9 Personen im Video ein Apple Macbook benutzen. Aber auch da muss ich Sie enttäuschen - für jedes Betriebssystem gibt es Tools um die MAC-Adresse zu ändern und daher kann man sich oftmals auch nicht darauf verlassen. Vielmehr könnte ein Profi sogar eine falsche

Fährte legen, indem er explizit eine Hardwareadresse verwendet, die auf einen unschuldigen Dritten deutet.

Nachdem nun PayPal und eBay eingerichtet sind, kann man allerdings nicht gleich ein Gaming-Notebook für 1.990 Euro zu verkaufen. Dies lässt alle Alarmglocken schrillen und der Verkauf wird abgebrochen bzw. der Verkäufer aufgefordert, Identitätsnachweise und Besitznachweise wie Ausweiskopien und Rechnungen beizubringen.

Jetzt braucht der Betrüger etwas Geduld, und hier kommen auch die paar Extra-Euros auf der virtuellen Kreditkarte ins Spiel. Zuerst sollte das Konto eine gewisse Mindestzeit bestehen, um nicht genauer beobachtet zu werden.

In diesen paar Wochen kann der Betrüger ein paar Käufe tätigen - hierzu bieten sich einige Anbieter aus Fernost an. Oftmals findet man dort Artikel für ein bis zwei Euro, die manchmals sogar noch Versandkostenfrei oder mit Versandkosten im Cent-Bereich verkauft werden.

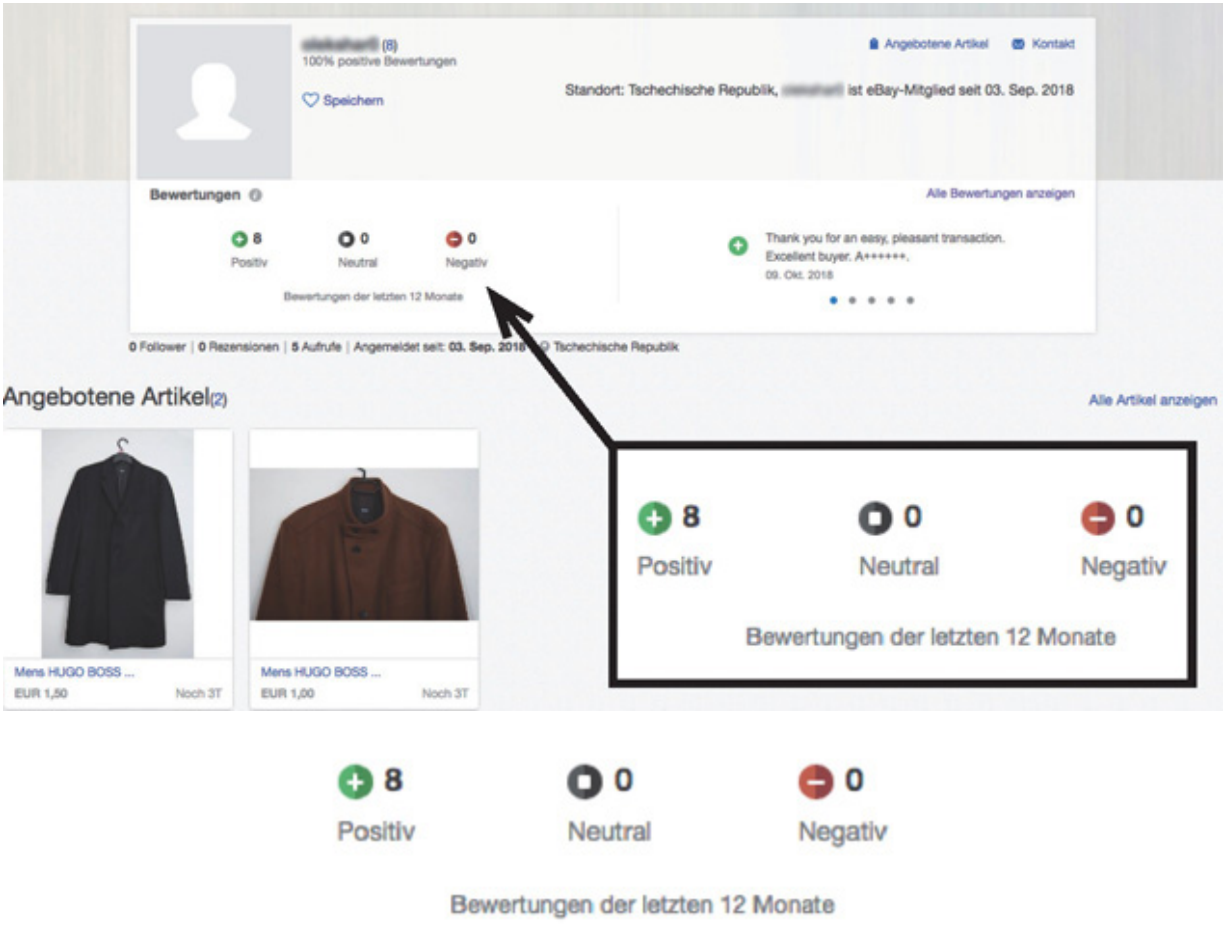
Darüber hinaus geben die diversen Management-Systeme der großen eBay-Verkäufer die Bewertung automatisch nach Zahlungseingang oder beim Versand der Ware ab. So kann man sich für wenige Euro erstmal einige Bewertungen "kaufen". Ob die Lieferung des 99 Cent Gummiarmreifens oder des 1,29 Euro Stringtangas an eine nicht existente Adresse erfolgt ist hierbei egal - einerseits revidiert der Verkäufer die Bewertung nicht, wenn der Artikel zurückkommt und andererseits dauert der Versand alleine meist schon 3-6 Wochen, und von der Lagerzeit am Postamt zur Abholung und einem eventuellen Rückversand sprechen wir erstmal garnicht.

Danach gibt es noch eine weitere Hürde zu überwinden - PayPal friert höhere Transaktionen bei neuen Konten für 21

Tage ein. Daher sollten auch die ersten Verkäufe entweder korrekt ablaufen oder es können nur ein paar Kleinbeträge abgezockt werden. Abgesehen davon haben neue eBayer ein geringeres Monatslimit.

Aber auch das lässt sich mit ein wenig Geld umgehen - zB indem man gleich mehrere Accounts erstellt. Einer kann dann virtuelle Güter wie Lizenzschlüssel, Gutscheincodes, etc. kaufen und der zweite verkauft diese Dinge wieder.

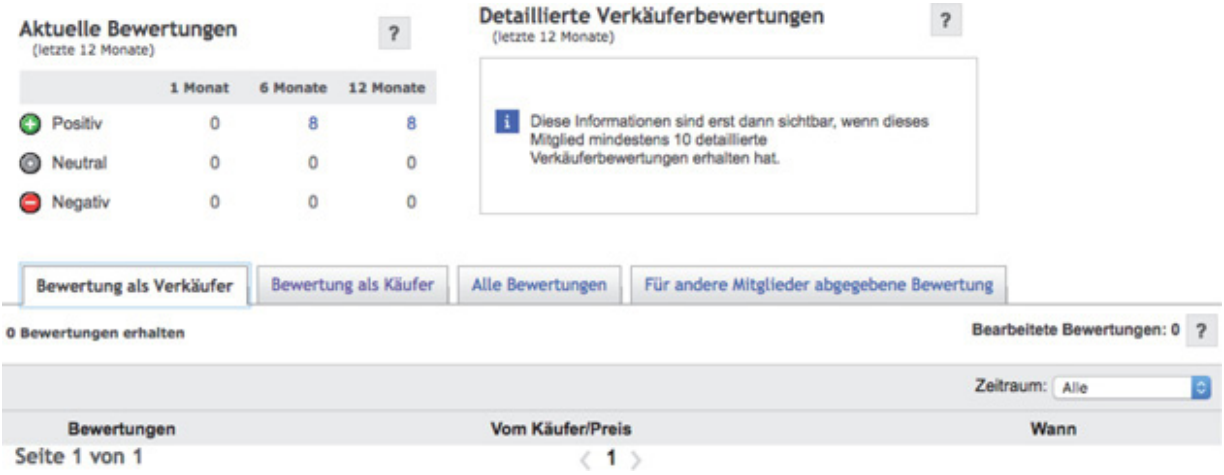
Sehen wir uns also die Alarmzeichen an einem konkreten Beispiel an:



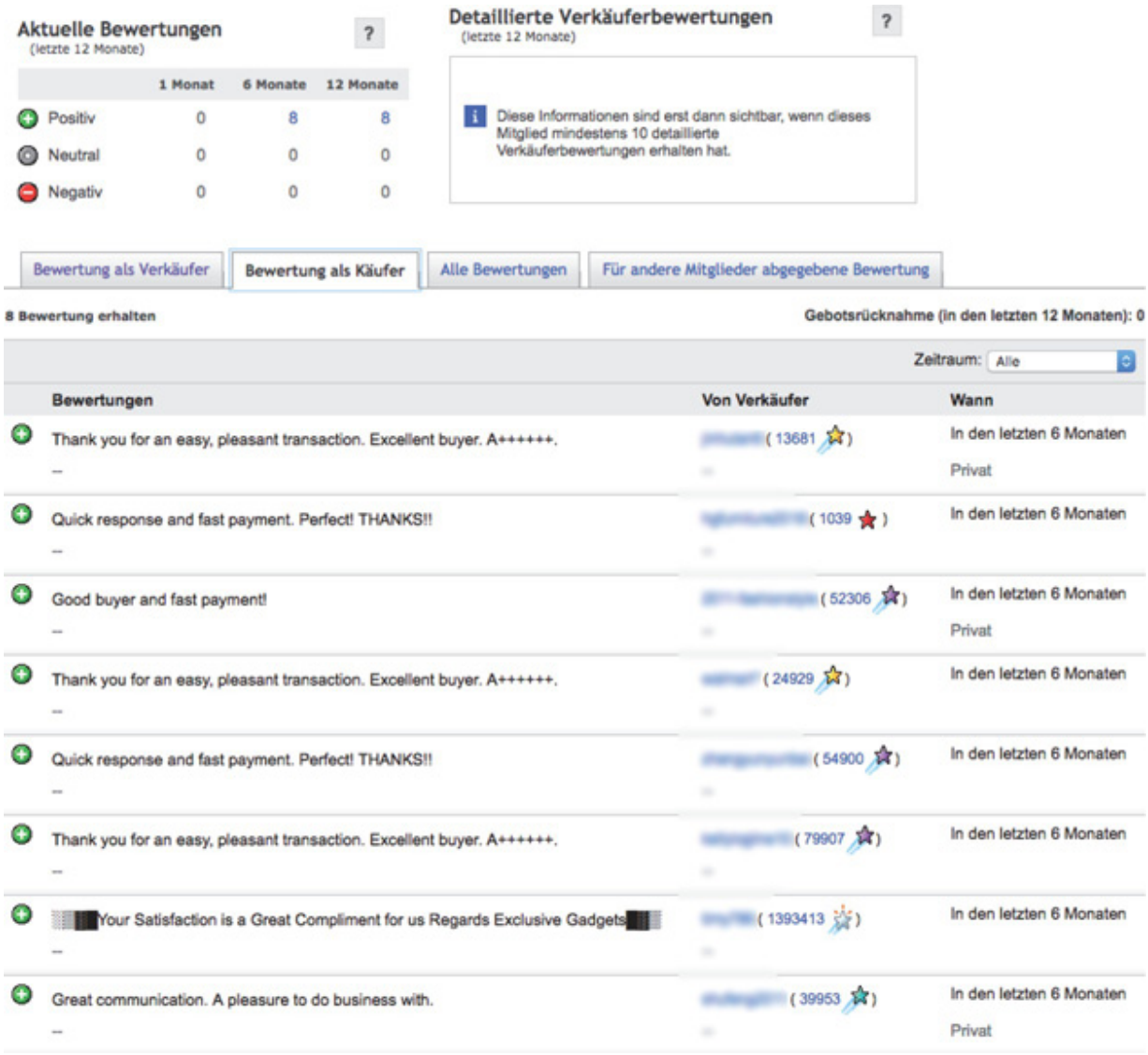
8
Positiv
0
Neutral
0
Negativ
Bewertungen der letzten 12 Monate

Ein Verkäufer mit relativ wenig Bewertungen (hier zB 8) bietet teure Markenartikel (hier zB Hugo Boss Mäntel) an.

Dann schauen wir uns doch gleich noch an wofür dieser Verkäufer die Bewertungen bekommen hat...



Hier sind als Verkäufer keinerlei Bewertungen vorhanden. Das alleine heißt natürlich noch nichts - jeder fängt einmal an. Daher checken wir was er so gekauft hat.



Aktuelle Bewertungen (letzte 12 Monate)

	1 Monat	6 Monate	12 Monate
Positiv	0	8	8
Neutral	0	0	0
Negativ	0	0	0

Detaillierte Verkäuferbewertungen (letzte 12 Monate)

Diese Informationen sind erst dann sichtbar, wenn dieses Mitglied mindestens 10 detaillierte Verkäuferbewertungen erhalten hat.

Bewertung als Verkäufer | **Bewertung als Käufer** | Alle Bewertungen | Für andere Mitglieder abgegebene Bewertung

8 Bewertung erhalten — **Gebotsrücknahme (in den letzten 12 Monaten): 0**

Zeitraum: Alle

Bewertungen	Von Verkäufer	Wann
Thank you for an easy, pleasant transaction. Excellent buyer. A++++++.	[redacted] (13681)	In den letzten 6 Monaten
--	--	Privat
Quick response and fast payment. Perfect! THANKS!!	[redacted] (1039)	In den letzten 6 Monaten
--	--	
Good buyer and fast payment!	[redacted] (52306)	In den letzten 6 Monaten
--	--	Privat
Thank you for an easy, pleasant transaction. Excellent buyer. A++++++.	[redacted] (24929)	In den letzten 6 Monaten
--	--	
Quick response and fast payment. Perfect! THANKS!!	[redacted] (54900)	In den letzten 6 Monaten
--	--	
Thank you for an easy, pleasant transaction. Excellent buyer. A++++++.	[redacted] (79907)	In den letzten 6 Monaten
--	--	
[redacted]Your Satisfaction is a Great Compliment for us Regards Exclusive Gadgets[redacted]	[redacted] (1393413)	In den letzten 6 Monaten
--	--	
Great communication. A pleasure to do business with.	[redacted] (39953)	In den letzten 6 Monaten
--	--	Privat

Bei den Käufer-Bewertungen sehen wir natürlich nicht genau was gekauft wurde, aber zumindest wo. Daher rufen wir einige der Handelspartner diese Kontos auf und sehen nach was diese Shops so anbieten.