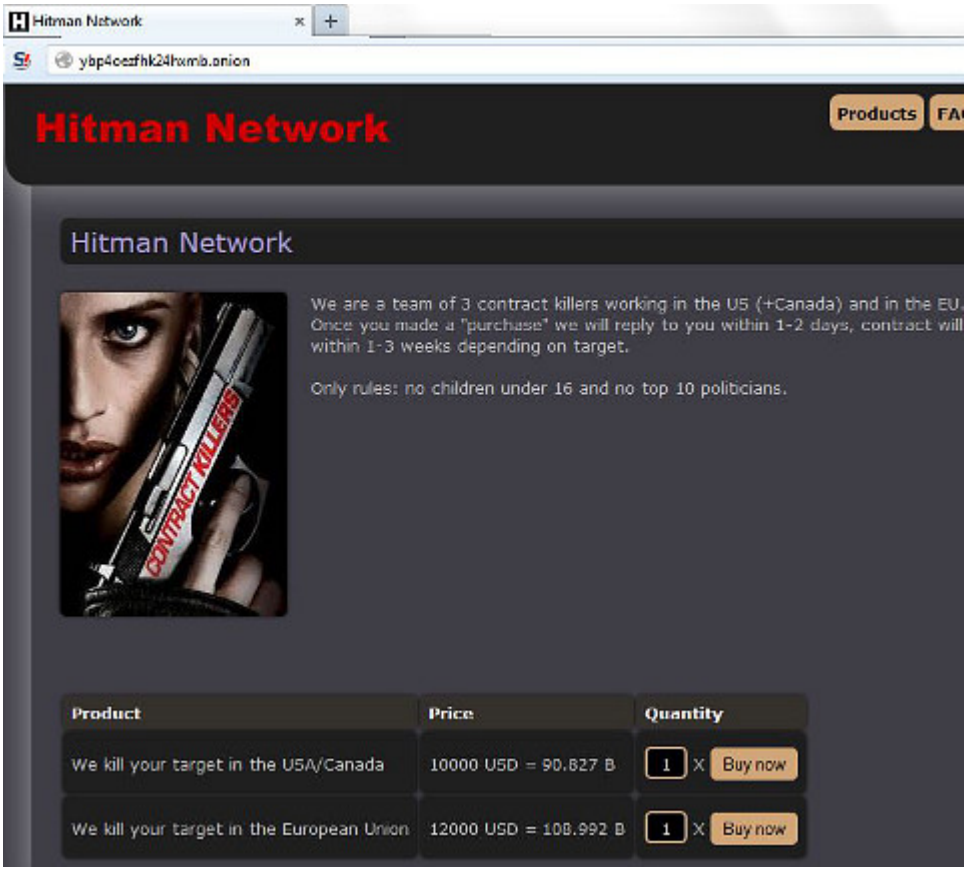
Deepsearch im Darknet [Update]



In den letzten Tagen habe ich mich aus Recherchegründen mehrfach im Darknet herumgetrieben. Ausserdem konnte ich mir nicht erklären, warum Deepsearch, eine Suchmaschine für diesen – verborgenen – Teil des Internet, auf einigen Rechnern und ausgerechnet während meines Seminars zum Thema einfach nicht aufrufbar war.

Wie naiv muss man eigentlich sein, um eine „Contract Killer“-Seite ernst zu nehmen, womöglich mit Vorkasse? 10.000 Dollar pro Kopf – „Quantity: 1“ – „in den Einkaufskorb legen“? LOLWUT?

Das Hiddenwiki (im Darknet erreichbar nur via Tor-Browser) erklärt die Technik und worum es geht: „We all know of the dark underground world of drug dealing, arm dealing and other criminal activities offline. What most of us don’t know is

that the same world exists online.“

Der Kollege Andreas Winterer hatte auf Hyperland schon vor zwei Jahren einen sehr informativen Artikel verfasst – „Das unbekannte Schatten-Internet“ – und auf ein Statement der Hacker-Gruppe *Anonymous* (jeder kann sich diesen Namen zulegen, auch die NSA) hingewiesen, die versucht hatte, in der „#OpDarknet“ mehrere Serverm auf denen besonders ekelhaften Dinge angeboten wurden, lahmzulegen. Das ist wohl nicht wirklich gelungen.
The ‚darknet‘ sites of TOR, I2P, and Freenode peaked our interest. We were aware that, TOR and I2P where originally designed to protect individuals from the oppressive governments of China, Iran and protect Free Speech. (…) What we discovered was quite the opposite. An growing and large of community of pedophiles was abusing such systems for personal profit.“

Anonymous behauptet, die Identität einiger krimineller Nutzer aufgedeckt zu haben; ohne konkrete Beweise bleibt das für mich bloße Denunziation. In der Official Release – 10/15/2011 wird sogar auf Nutzer hingewiesen, deren einschlägige Youtube-Channel auch noch nach zwei Jahren vorhanden sind. Entweder ist also an den Vorwürfen nichts dran, oder es handelt sich um Lockspitzel-Angebote der US-amerikanischen Strafverfolger (denen ist so etwas erlaubt). Ich glaube nicht, dass ein Channel nach dem Hinweis „pädaphile Angebote bei Youtube“ auch nur zehn Minuten online wäre – Youtube hätte das sofort abgeschaltet. Bei Sven Slootweg ist noch ein Statement zu sehen, das sich offenbar auf die „#OpDarknet“ bezieht.

Interessant ist, wie *anonymous* versucht hat, Teile des Darknets anzugreifen:
The WWW started to ask about our tools called ‚The Legion‘, ‚THOR‘ aka ‚Chris Hansen‘. The best way to describe them is to refer at the US patents #5,621,671 and #6,947,978. Many asked if were simply „script kiddies“. No we specifically developed the tools ‚The Legion‘, ‚THOR‘, ‚Chris Hansen‘ in protest of

Lolita City, Freedom Hosting, and the Hidden Wiki.

Aus der Patentbeschreibung für 5,621,671:
Method for geolocating logical network addresses on electronically switched dynamic communications networks, such as the Internet, using the time latency of communications to and from the logical network address to determine its location. Minimum round-trip communications latency is measured between numerous stations on the network and known network addressed equipment to form a network latency topology map. Minimum round-trip communications latency is also measured between the stations and the logical network address to be geolocated. The resulting set of minimum round-trip communications latencies is then correlated with the network latency topology map to determine the location of the network address to be geolocated.

Fazit: Natürlich nutzen Kriminelle auch die gängige Technik, im Internet anonym zu bleiben. Bankräuber nutzen auch die Technik der Fahrzeugkonstruktion, um Fluchtwagen zu benutzen. Das ist der Preis, den man für die Freiheit bezahlen muss. *Anonymous* hingegen schreibt:
One thing is clear, #OpDarknet did reveal that the benevolent community used to uphold Free Speech against the oppressive governments of Iran and China. It is now corrupted by the underground of trading and sale of Child Pornography aka „kiddie porn“.

Das halte ich für waschechtes Agent-provocateur-Sprech. Erstens ist diese Tatsache schon so lange bekannt, wie es Tor und das Darknet gibt, also keine Überraschung, und zweitens ist das ein mehr als durchsichtiger Versuch, die Anonymisierungs-Netze insgesamt zu diskreditieren, was für Leute, die sich „Hacker“ nennen und anonym bleiben wollen, eher eine *contradicio in adiecto* ist.

How to remain anonymous – Always watch your back

Bitte versucht nicht ohne das dementsprechende Wissen, wie man einen Browser „abdichtet“ und wie man vermeidet, Datenspuren zu hinterlassen, in den dunklen Ecken des Internet herumzusurfen. Das ist gefährlich:
„Bei Sicherheitsbehörden aber bedeutet Inkompetenz gefährliche Unberechenbarkeit, wegen der auch das Argument ‚Wer nichts zu verbergen hat…‘ nicht zieht. Das Risiko, in einer Antiterrordatei zu landen, ohne dass man die geringste Ahnung hat, warum, ist sehr real geworden – mit allen Konsequenzen von Einreiseverboten bis hin zum nächtlichen Besuch eines Sonderkommandos.“ (Herbert Braun, Computerzeitschrift c’t, Leitartikel 7/2013)

Update: Vgl. torrorists: „Tor network mostly contains legal content“.