Darknet marketplaces – Study of mechanisms used by Darknet sites and realization of such a site

Fachgebiet: Information Technology Security
Betreuer: Prof. Dr. Emmanuel Benoist
Experte: Daniel Voisard (BAKOM)

Darknet marketplaces sind E-Commerce-Plattformen, auf die man als Teil eines anonymen Netzwerks («Darknet») nur mit speziellen Tools Zugriff erhält. Durch ihre anonyme Natur wird dort mehrheitlich mit illegalen Gütern gehandelt. Dadurch sind sie ständiger Gefahr durch Gesetzeshüter und Konkurrenten ausgesetzt, was dazu führt, dass hohe Sicherheitsvorkehrungen getroffen werden. In dieser Arbeit werden diese Technologien untersucht und selber eine solche Plattform entwickelt.

Die Arbeit ist in zwei Teile gegliedert:

Analyse: Mechanismen der Darknet marketplaces

Zugang zu diesen Marktplätzen im Darknet erhält man über das **Tor-Netzwerk**.

Die Funktionsweise der zugrundeliegende Technologie und deren Schwachstellen stehen im Fokus dieses Teils. Ebenfalls wurden **Tor Hidden Services** – eine Möglichkeit, mit dem sowohl Anbieter eines Servers wie auch die Nutzer anonym bleiben können – und ihre Schwachstellen ausgiebig studiert.

Die anonymen Marktplätze unterscheiden sich in vielen Punkten von herkömmlichen E-Commerce-Plattformen: Als Zahlungsmittel kommt das dezentrale Zahlungssystem **Bitcoin** zum Einsatz, das eingehend untersucht wurde. Auch wurde in Erfahrung gebracht, wie die Marktplätze Geld verdienen, wie die Märkte aus Sicht Käufer und Verkäufer funktionieren, wie die Reputationsbildung abläuft und welche Zahlungsabwicklungsmöglichkeiten (Vorauszahlung, Escrow, Verträge) und zusätzlichen Mechanismen (Foren, PGP, …) zum Einsatz kommen.

Abgeschlossen wird die Analyse durch eine **Sicherheitsanalyse** zweier grosser Marktplätze: Der Platzhirsch Agora wies kaum Mängel an der Sicherheit auf, ein weiterer Markt, Cloud9, machte einen wesentlich unsichereren Eindruck – und wurde prompt im November 2014 vom FBI offline genommen.

Realisierung: Entwicklung eines Darknetmarketplace

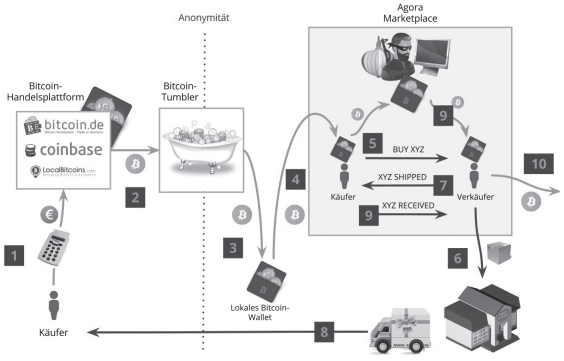
Im zweiten Teil der Arbeit wurde eine PHP-**Webapplikation** geschaffen, die als solcher Marktplatz im Darknet zum Einsatz komme könnte:

Die Applikation bietet die grundsätzlichen Features einer E-Commerce-Plattform (Registristrierung, Verwaltung und Bestellung von Produkten) implementiert aber die **wesentlich höheren Sicherheitsstandards**, die auch stärkere Angreifer abwehren würde.

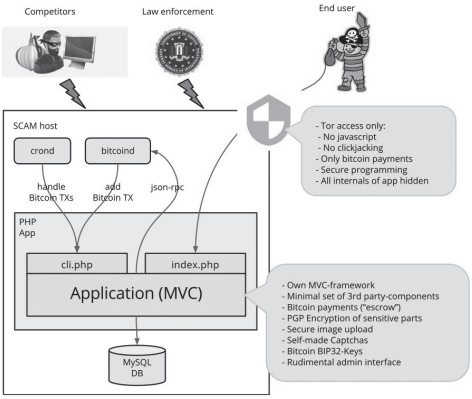
Desweiteren integriert die Applikation Darknet-spezifische Features wie Zahlung per **Bitcoin** und **PGP-Verschlüsselung**. Dabei liegt der Fokus immer auf höchste Sicherheit: So wurden beispielsweise die neuesten Entwicklungen der Bitcoin-Gemeinde zur Implementierung von Verträgen («Multisig») oder hierarchisch-deterministische Bitcoin-Keys für hohe Anoymität integriert.

Die Applikation wurde eingehend auf Sicherheitslücken getestet und mit einer ausführlichen Dokumentation auf Github unter einer **Open-Source**-Lizenz veröffentlicht.
https://github.com/MatthiasWinzeler/scam

Matthias Winzeler



Der Ablauf eines Kaufs auf einem Darknet marketplace von A–Z



Die Architektur der realisierten Applikation (MVC-Applikation mit Bitcoin-Daemon-Integration)