Darknet und Javascript, reloaded

Das Torprojekt hat zur Verhaftung des Darknet-Providers „Freedom Hosting“ ausführlich Stellung bezogen.

The person, or persons, who run Freedom Hosting are in no way affiliated or connected to The Tor Project, Inc., the organization coordinating the development of the Tor software and research. In the past, adversarial organizations have skipped trying to break Tor hidden services and instead attacked the software running at the server behind the dot onion address. Exploits for PHP, Apache, MySQL, and other software are far more common than exploits for Tor. The current news indicates that someone has exploited the software behind Freedom Hosting. From what is known so far, the breach was used to configure the server in a way that it injects some sort of javascript exploit in the web pages delivered to users. This exploit is used to load a malware payload to infect user’s computers. The malware payload could be trying to exploit potential bugs in Firefox 17 ESR, on which our Tor Browser is based. We’re investigating these bugs and will fix them if we can.

Hier sind die Details.

Auch Heise berichtet „Tor-Nutzer über Firefox-Lücke verfolgt“. „Ältere, zum Tor-Browser-Bundle gehörende Firefox-Browser enthalten eine Javascript-Sicherheitslücke, über die sich Code einschleusen und ausführen lässt. “

Deswegen schreibt meine Lieblings-Torfrau Runa ganz richtig : „Firefox vulnerability was Windows-specific and targeted older versions of the Tor Browser Bundle“.

Wer über Tor surft und Javascript aktiviert hat, kann auch gleich das Schloss vor die Tür nageln. Diese

„Sicherheitslücke“ betrifft nur Leute, die sich um Sicherheit wenig kümmern.