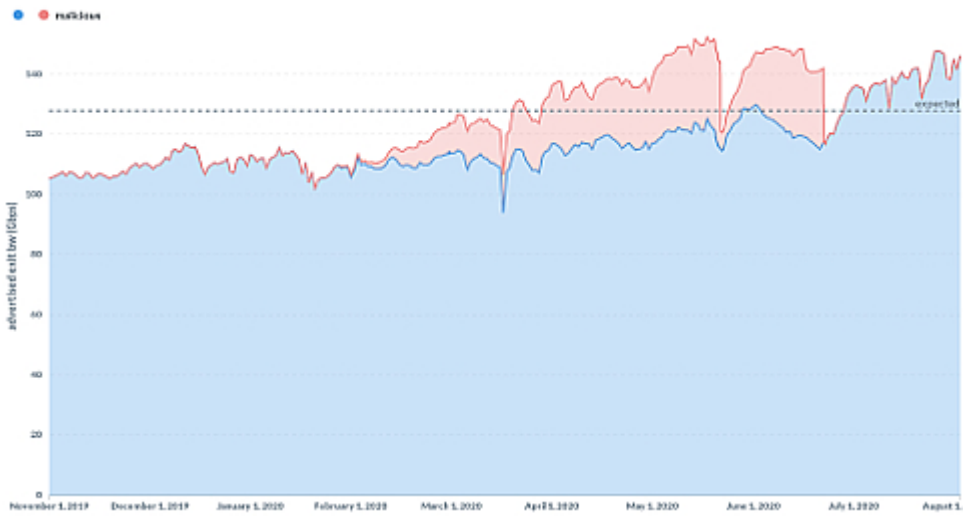
Malicious Tor Relays



Medium.com: „How Malicious Tor Relays are Exploiting Users in 2020 (Part I)
– 23% of the Tor network's exit capacity has been attacking Tor users".

„So far 2020 is probably the worst year in terms of malicious Tor exit relay activity since I started monitoring it about 5 years ago. As far as I know this is the first time we uncovered a malicious actor running more than 23% of the entire Tor network's exit capacity. That means roughly about one out of 4 connections leaving the Tor network were going through exit relays controlled by a single attacker."

Conclusio: **The full extend of their operations is unknown, but one motivation appears to be plain and simple: profit. (…) Malicious relays are just used to gain access to user traffic. To make detection harder, the malicious entity did not attack all websites equally. It appears that they are primarily after cryptocurrency related websites – namely multiple bitcoin mixer services.**

Hintergrundartikel desselben Autors (08.12.2019): The Growing Problem of Malicious Relays on the Tor Network.