Experimental Detection of Hackers' Networks

Amit Rechavi

Cybercrime and hacking have become ubiquitous. Many studies have explored hacking communities, and a few have investigated hacking networks on the country and cross-country levels. We collected data on successful brute-force attacks (BFAs) and system-trespassing incidents (Sessions) on honeypots (HPs). Based on one million interactions, we built a network of hackers and hacked data. The network depicts hacking activities and the different roles of countries in the hacking scene. We found a suspected unique data that were transferred between BFA and Session hackers. Based on these transactions we built the concealed network and examined its topology. Mapping IP addresses and countries, we found that only a few countries lead the hacking activities and function as network's core. Our contribution lies in studying and mapping the dynamics of hacking activity on the country level and in providing insights into the dynamic of the concealed trading in usernames and passwords. Due to the severe consequences of hacking activities, our findings carry both criminological-practical and technological-theoretical implications.