Timeline

- 01.08.2016 - Mirai taucht erstmals auf
- 18.09.2016 - OHV Angriffe beginnen
- 21.09.2016 - Krebs on Security Angriff (ca. 650 GBps)

Ablauf

1. rapid scanning phase
   - scannt semi-random IP Adressen auf Telnet Ports 23 und 2323
   - wenn Opfer gefunden, dann Brutforce Login mit Dictionary aus Credentials
   - wenn erfolgreich, dann senden von IP-Adresse und Credentials an report server
2. report server
   - siehe oben
3. loader program
   - loggt in Gerät ein
   - bestimmt Architektur
4. download & execute malware
   - lädt und führt architekturspezifische Malware aus
   - verschleiert Prozessnamen mit pseudorandom alphanumeric string
   - zusätzlich:
     - killt andere Prozesse auf Port 22 und 23
     - killt auch andere Mirai Varianten
   - Anmerkung: Malware ist nicht persistent. Überlebt Neustart des Geräts nicht.