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.
   - Infizierte Geräte scannen weiter nach neuen Opfern und warten auf Befehle vom Command & Control (C2)-Server, z. B. zur Durchführung von DDoS-Angriffen

- Geografische Verteilung: Zum Beispiel am 21. September 2016: Brasilien (15 %), Kolumbien (14 %), Vietnam (12,5 %) waren die Spitzenländer

Größte Angriffe

Krebs on Security

- Am 20. September 2016 wurde die Webseite von Krebs on Security massiv angegriffen.
- Der Angriff erreichte Spitzenwerte von etwa 620 Gbps (Gbit/s).
- Laut den Forschern von F5 Labs und anderen waren mehrere hunderttausend IoT-Geräte beteiligt, vermutlich mit Standard-Zugangsdaten und offenen Telnet-/SSH-Ports.

OHV (französischer Hosting- und Cloudprovider)

- Kurz nach dem Krebs-Angriff (Ende September 2016) wurde der französische Hosting- und Cloud-Provider OVH Opfer eines massiven DDoS-Angriffs mit Beteiligung des Mirai-Botnetzes.
- In Berichten wird von über 1 Tbps (oder deutlich näher an 1.5 Tbps) Schadtraffic gesprochen, ausgeführt von über 145.607 IoT-Geräten laut OVH CTO.
- Ursprüngliches Ziel war offenbar ein Minecraft-Gaming-Server, der bei OVH gehostet war – die Attacke traf dann aber das Hosting-Netz von OVH sehr breit.

Dyn

- Am 21. Oktober 2016 wurde der US-DNS Provider Dyn (die Infrastruktur vieler großer Websites bereitstellt) durch massiven DDoS in mehreren Wellen angegriffen.
- Laut Dyn wurden „zig Millionen“ IP-Adressen beobachtet, die beteiligt waren.
- Der Angriffsverkehr war an manchen Stellen gemeldet mit Spitzenwerten im Bereich von hunderten Gbps bis über 1 Tbps (je nach Schätzung).
- Der Angriff führte dazu, dass populäre Websites wie Twitter, GitHub, Netflix, Reddit, Airbnb und viele andere beeinträchtigt wurden.