Vergleich der Angriffsvektoren von Malware im IoT- und im PC-Bereich

Hintergrund

Unsichere IoT-Geräten haben in letzter Zeit oft [1,2,3,4] für Schlagzeilen gesorgt. Als Teil eines Botnets sind solche öffentlich erreichbaren Geräte eine Gefahr für das gesamte Internet. Für PCs ausgelegte Malware befällt IoT-Geräte üblicherweise nicht, stattdessen werden dort spezielle Malware-Varianten wie Mirai [5,6] gefunden. Da sich die verwendete Malware unterscheidet, ist anzunehmen dass die genutzten Angriffsvektoren ebenfalls unterschiedlich sind.

Fragestellungen

Im Rahmen der Arbeit sollen die folgenden Fragestellungen bearbeitet werden:

1. Welche charakteristischen Schwachstellen lassen sich bei der Untersuchung bekannt gewordener Malware für IoT-Geräte feststellen?
2. Welche besonderen Merkmale von IoT-Geräten führen dazu, dass die auftretenden Schwachstellen sich von denen anderer Geräte unterscheiden?
3. Wie lassen sich Schutzmechanismen für PCs (beispielsweise Firewalls, Virenscanner, Verhaltensmaßstäbe) auf IoT-Geräte übertragen?
4. Lassen sich aus den besonderen Schwachstellen für IoT-Geräte spezielle Schutzkonzepte ableiten?

Literatur

1. https://t3n.de/news/studie-gefahr-iot-angriffe-1205978/
2. https://www.br.de/nachrichten/netzwelt/wie-kriminelle-iot-schwachstellen-zu-geld-machen,ReZsRWd
3. https://t3n.de/news/studie-gefahr-iot-angriffe-1205978/
4. https://www.datensicherheit.de/aktuelles/iot-botnetze-sind-weiterhin-grosse-gefahr-fuer-unternehmen-30217
5. https://github.com/jgamblin/Mirai-Source-Code
6. Kolias, Constantinos, et al. "DDoS in the IoT: Mirai and other botnets." *Computer* 50.7 (2017): 80-84.
7. Costin, Andrei, and Jonas Zaddach. "Iot malware: Comprehensive survey, analysis framework and case studies." BlackHat USA (2018).