Internet of Malicious Things: Correlating Active and Passive Measurements for Inferring and Characterizing Internet-Scale Unsolicited IoT Devices

Submitted by grigby1 on Tue, 12/01/2020 - 3:35pm

Title	Internet of Malicious Things: Correlating Active and Passive Measurements for Inferring and Characterizing Internet-Scale Unsolicited IoT Devices
Publication Type	Journal Article
Year of Publication	2018
Authors	Shaikh, F., Bou-Harb, E., Neshenko, N., Wright, A. P., Ghani, N.
Journal	IEEE Communications Magazine
Volume	56
Pagination	170?177
Date Published	Sept. 2018
ISSN	1558-1896
Keywords	Collaboration, composability, computer network security, computer security, critical infrastructure, critical infrastructures, electric industrial facilities, Home appliances, Human Behavior, human factors, Internet, Internet background radiation traffic, Internet frontier, internet of malicious things, Internet of Things, Internet-scale Computing Security, Internet-scale insecurities, internet-scale unsolicited IoT devices inference, Internet-wide scanning, IoT cyber security situational awareness, IoT malicious raw data, IoT paradigm, Metrics, Policy Based Governance, pubcrawl, resilience, Resiliency, Scalability, smart home appliances, Smart homes, unsolicited Internet-scale IoT devices, unsolicited IoT devices

Abstract

Advancements in computing, communication, and sensing technologies are making it possible to embed, control, and gather vital information from tiny devices that are being deployed and utilized in practically every aspect of our modernized society. From smart home appliances to municipal water and electric industrial facilities to our everyday work environments, the next Internet frontier, dubbed IoT, is promising to revolutionize our lives and tackle some of our nations' most pressing challenges. While the seamless interconnection of IoT devices with the physical realm is envisioned to bring a plethora of critical improvements in many aspects and diverse domains, it will undoubtedly pave the way for attackers that will target and exploit such devices, threatening the integrity of their data and the reliability of critical infrastructure. Further, such compromised devices will undeniably be leveraged as the next generation of botnets, given their increased processing capabilities and abundant bandwidth. While several demonstrations exist in the literature describing the exploitation procedures of a number of IoT devices, the up-to-date inference, characterization, and analysis of unsolicited IoT devices that are currently deployed "in the wild" is still in its infancy. In this article, we address this imperative task by leveraging active and passive measurements to report on unsolicited Internet-scale IoT devices. This work describes a first step toward exploring the utilization of passive measurements in combination with the results of active measurements to shed light on the Internet-scale insecurities of the IoT paradigm. By correlating results of Internet-wide scanning with Internet background radiation traffic, we disclose close to 14,000 compromised IoT devices in diverse sectors, including critical infrastructure and smart home appliances. To this end, we also analyze their generated traffic to create effective mitigation signatures that could be deployed in local IoT realms. To support largescale empirical data analytics in the context of IoT, we make available the inferred and extracted IoT malicious raw data through an authenticated front-end service. The outcomes of this work confirm the existence of such compromised devices on an Internet scale, while the generated inferences and insights are postulated to be employed for inferring other similarly compromised IoT devices, in addition to contributing to IoT cyber security situational awareness.

URL https://ieeexplore.ieee.org/document/8466375

DOI 10.1109/MCOM.2018.1700685

Citation Key shaikh_internet_2018

🏷

collaboration composability computer network security computer security critical infrastructure critical infrastructures electric industrial facilities Home appliances Human behavior Human Factors internet Internet background radiation traffic Internet frontier internet of malicious things Internet of Things Internet-scale Computing Security Internet-scale insecurities internet-scale unsolicited IoT devices inference Internet-wide scanning IoT cyber security situational awareness IoT malicious raw data IoT paradigm Metrics Policy Based Governance pubcrawl resilience Resiliency Scalability smart home appliances Smart homes unsolicited Internet-scale IoT devices unsolicited IoT devices