World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:14, No:12, 2020

USBware: A Trusted and Multidisciplinary Framework for Enhanced Detection of USB-Based Attacks

Authors : Nir Nissim, Ran Yahalom, Tomer Lancewiki, Yuval Elovici, Boaz Lerner

Abstract : Background: Attackers increasingly take advantage of innocent users who tend to use USB devices casually, assuming these devices benign when in fact they may carry an embedded malicious behavior or hidden malware. USB devices have many properties and capabilities that have become the subject of malicious operations. Many of the recent attacks targeting individuals, and especially organizations, utilize popular and widely used USB devices, such as mice, keyboards, flash drives, printers, and smartphones. However, current detection tools, techniques, and solutions generally fail to detect both the known and unknown attacks launched via USB devices. Significance: We propose USBWARE, a project that focuses on the vulnerabilities of USB devices and centers on the development of a comprehensive detection framework that relies upon a crucial attack repository. USBWARE will allow researchers and companies to better understand the vulnerabilities and attacks associated with USB devices as well as providing a comprehensive platform for developing detection solutions. Methodology: The framework of USBWARE is aimed at accurate detection of both known and unknown USB-based attacks by a process that efficiently enhances the framework's detection capabilities over time. The framework will integrate two main security approaches in order to enhance the detection of USB-based attacks associated with a variety of USB devices. The first approach is aimed at the detection of known attacks and their variants, whereas the second approach focuses on the detection of unknown attacks. USBWARE will consist of six independent but complimentary detection modules, each detecting attacks based on a different approach or discipline. These modules include novel ideas and algorithms inspired from or already developed within our team's domains of expertise, including cyber security, electrical and signal processing, machine learning, and computational biology. The establishment and maintenance of the USBWARE's dynamic and up-to-date attack repository will strengthen the capabilities of the USBWARE detection framework. The attack repository's infrastructure will enable researchers to record, document, create, and simulate existing and new USB-based attacks. This data will be used to maintain the detection framework's updatability by incorporating knowledge regarding new attacks. Based on our experience in the cyber security domain, we aim to design the USBWARE framework so that it will have several characteristics that are crucial for this type of cyber-security detection solution. Specifically, the USBWARE framework should be: Novel, Multidisciplinary, Trusted, Lightweight, Extendable, Modular and Updatable and Adaptable. Major Findings: Based on our initial survey, we have already found more than 23 types of USB-based attacks, divided into six major categories. Our preliminary evaluation and proof of concepts showed that our detection modules can be used for efficient detection of several basic known USB attacks. Further research, development, and enhancements are required so that USBWARE will be capable to cover all of the major known USB attacks and to detect unknown attacks. Conclusion: USBWARE is a crucial detection framework that must be further enhanced and developed.

Keywords : USB, device, cyber security, attack, detection
Conference Title : ICSRD 2020 : International Conference on Scientific Research and Development
Conference Location : Chicago, United States
Conference Dates : December 12-13, 2020