World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:16, No:02, 2022

O.MG- It’s a Cyber-Enabled Fraud

Authors : Damola O. Lawal, David W. Gresty, Diane E. Gan, Louise Hewitt

Abstract : This paper investigates the feasibility of using a programmable USB such as the O.MG Cable to perform a file tampering attack. Here, the O.MG Cable, an apparently harmless mobile device charger, is used in an unauthorized way to alter the content of a file (accounts record-January_Contributions.xlsx). The aim is to determine if a forensics analyst can reliably determine who has altered the target file; the O.MG Cable or the user of the machine. This work highlights some of the traces of the O.MG Cable left behind on the target computer itself, such as the Product ID (PID) and Vendor ID (ID). Also discussed is the O.MG Cable’s behavior during the experiments. We determine if a forensics analyst could identify if any evidence has been left behind by the programmable device on the target file once it has been removed from the computer to establish if the analyst would be able to link the traces left by the O.MG Cable to the file tampering. It was discovered that the forensic analyst might mistake the actions of the O.MG Cable for the computer users. Experiments carried out in this work could further the discussion as to whether an innocent user could be punished for the unauthorized changes made by a programmable device.

Keywords : O.MG cable, programmable USB, file tampering attack, digital evidence credibility, miscarriage of justice, cyber fraud
Conference Title : ICDF 2022 : International Conference on Digital Forensics
Conference Location : London, United Kingdom
Conference Dates : February 15-16, 2022