Systematic literature review and metadata analysis of ransomware attacks and detection mechanisms

Abdullahi Mohammed Maigida, Shafi'i Muhammad Abdulhamid, Morufu Olalere, John K. Alhassan, Haruna Chiroma & Emmanuel Gbenga Dada

Abstract

Ransomware is advanced and upgraded malicious software which comes in the forms of Crypto or Locker, with the intention to attack and take control of basic infrastructures and computer systems. The vast majority of these threats are aimed at directly or indirectly making money from the victims by asking for a ransom in exchange for decryption keys. This systematic literature analysed the anatomy of ransomware, including its trends and mode of attacks to find the possible solutions by querying various academic literature. In contrast to previous reviews, sources of ransomware dataset are revealed in this review paper to ease the challenges of researchers in getting access to ransomware datasets. In addition, a taxonomy of ransomware current trends is presented in the paper. We discussed the articles in detail, the evolution and trend in ransomware researches. Most of the techniques deployed could not completely prevent ransomware attacks because of its obfuscation techniques, but rather recommend proper and regular backup of important files. This review can serve as a benchmark for researchers in proposing a novel ransomware detection methodology and starting point for novice researchers.

https://link.springer.com/article/10.1007/s40860-019-00080-3