ABSTRACT

In the current digital era, data has become a highly valuable asset. Various techniques are used to steal personal data, which can be potentially misused by irresponsible parties. The subject of this research is AQUVAPRN.exe, which is a type of malware known as a Remote Access Trojan (RAT). When this malware is running, the creator of the malware can extract personal data from the infected user's operating system. The AQUVAPRN.exe malware works by running in the background when the application is executed, infecting 36 registry files, creating 65 files, reading 52 files on the infected operating system, and establishing continuous internet connections with a specific IP address, all without the knowledge of the user of the infected computer. The obtained results regarding the AQUVAPRN.exe malware include the IP address 109.51.76.80, which is associated with the city of Lisbon in Portugal, and the MD5 hash value 55c2c12970cda52f58bfad7b8c7d37d5. It is also known that the AQUVAPRN.exe malware uses anti-reverse engineering techniques, specifically obfuscation, to hinder or prevent the malware from being dissected or reverse-engineered to understand the code it is composed of. The Process ID (PID) of the AQUVAPRN.exe process on the infected operating system is 8332, with a virtual address of 0x8e0f57042080.

Keywords: *IP Address, Malware, Obfuscation, Personal Data, RAT*