Unpacking and Decrypting FlawedAmmyy

By Created by:Mike Downey

Archived: 2026-11-20 02:18:53 UTC

Malware authors commonly utilize packers (Roccia, 2017) as a method of concealing functionality and characteristics of their malicious code, making an analyst's job more difficult. Second stage executables may also be encrypted, requiring the analyst to gather an understanding of how this code is manipulated. The ability to unpack and decrypt malicious software is a critical step in understanding intent and the scope of malware capabilities. The goal of this paper is to provide real-world application of the unpacking and decoding techniques required to analyze a remote access Trojan (RAT) known as FlawedAmmyy. While basic static and dynamic analysis will not be covered, this paper will focus on the step-by-step procedures to unpack and decrypt a FlawedAmmyy sample within a debugger.

Source: https://www.sans.org/reading-room/whitepapers/reverseengineeringmalware/unpacking-decrypting-flawedammyy-38930