Unpacking and Decrypting FlawedAmmyy

Michelle Petersen

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...

By Mike Downey

April 22, 2019