How we detected LockerGoga

Guillaume Bonfante[1;2], Corentin Jannier[2], Jean-Yves Marion[1], Fabrice Sabatier[3]

[1]LORIA - Université de Lorraine
[2]cyber-detect
[3]CNRS

Abstract

Our objective is to illustrate the uses of the software Gorille that we develop at cyber-detect. The recent attacks of LockerGoga against Altran in France and Norsk Hydro in Norway illustrate the necessity to have advanced anti-malware defences. Gorille's basis are morphological analysis. As such, the main features of Gorille are the following. It is robust with respect to heavy code obfuscations. It applies on dynamic data that can be forged within a virtual environment. Its detection engine is based on behavior recognition. This contribution is an extended version of our Blog's post.