



Analizando un troyano gusano minero para detectarlo y evitarlo

¹Juan Miguel Alonso Torres

¹**Segurmatica, Cuba**

Con el auge de la minería de cripto monedas los grupos cibercriminales han desarrollado técnicas para infestar los dispositivos de los usuarios y apoderarse del poder de cómputo de los mismos y de esta formar minar cripto monedas secuestrando recursos de otros. En el presente trabajo se ha realizado un análisis del gusano minero AutoHotKey que tiene un nivel de prevalencia muy alto en las redes cubanas. Como resultado se resaltan las técnicas para el análisis del programa maligno y la obtención de indicadores de compromiso para evitar su propagación.

