Extracting actionable data from modern financially motivated malware on windows personal computers

James Wyke

Abstract:

In this report we describe the wide range of techniques used by financial malware to facilitate online banking fraud. It describes how financial malware has evolved over the last decade to become more efficient and effective at facilitating fraud.

We describe actionable data that can be extracted from financial malware and used to remediate existing and protect against future compromises. We assess how that data can be extracted and provide a working solution for the Vawtrak malware family that can be used and extended by Incident Responders, forensic and malware analysts.