Recurring malware checker using MISP: Internship at Commvault

Ethan Fuks
Science & Engineering
Manalapan High School
Englishtown, NJ
426efuks@frhsd.com

Abstract

During my internship at Commvault, I have created a tool that recurrently checks for malware in a user's data by using the Malware Information Sharing Platform (MISP) to obtain newly discovered malware hashes and comparing these against the user. A hash is a unique way of representing a piece of data by encoding it where small changes in the input create big unpredictable changes in the output. This creates a unique signature for each file that can be used to share found malware and compare against it. MISP is an open source software that organizes and collects different feeds of data from various sources including MalwareBazaar and abuse.ch, among many others. Commvault currently uses Google Threat Intelligence and my project evaluated MISP as a free, open source alternative. I created a dummy system to test with 100 files of randomized text and a list of hashes of these was created. Some were selected as malware and were checked against the list. I set up a local instance of MISP in Virtual Box that is perpetually running and able to be queried for found malware. PyMISP, a Python library to query MISP, is used to connect these parts together and recurringly check for malware. I created a write-up for my process of setting up and using MISP for Commvault to use in the future.

Index Terms

Commvault, malware, Malware Information Sharing Platform, MISP, PyMISP, hash function, MalwareBazaar, abuse.ch, open source, internship