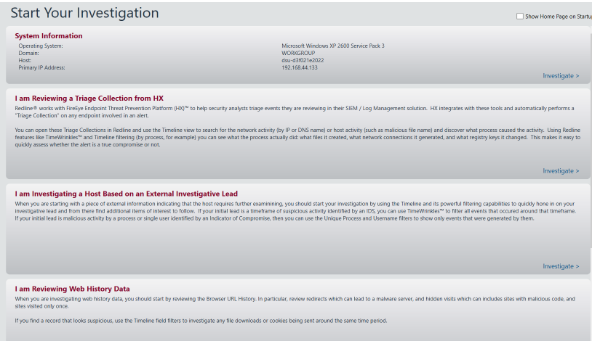
Executive Summary

For Final Project CSC 388

By Vinnan, Sascha Walker

In our current world of cyber crimes digital forensics plays a critical part. To find a great and a free tool is something which is amazing. Hence, we are working on Fireeye’s Redline a tool which lets us analyze a potentially compromised Windows operating system to find malicious activity.

Installation:



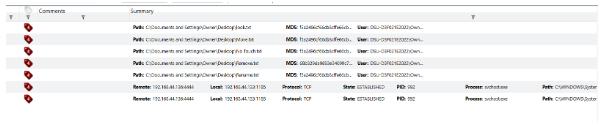
It is highly recommended to install redline in a clean environment free of any malware. If you suspect that your system is compromised, then run the redline from a clean environment.

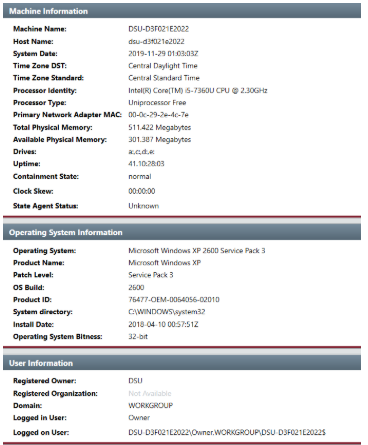
* Download Redline from <http://www.fireeye.com/services/freeware.html>
* Start the installation wizard by opening Redline.msi.
* Click Next in the Welcome to the Redline Setup Wizard window.
* Read the End User License Agreement carefully. To continue installing Redline, select I Agree and then click Next in the License Agreement window.
* Click Next in the Confirm Installation window. Redline should take only a few seconds to install.
* Click Close to complete the installation process.

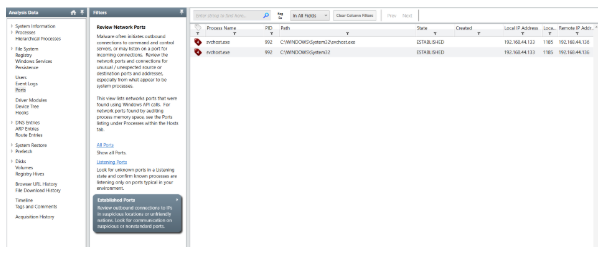
How to start investigation:

To start you will be collecting the data using either the standard collector or the comprehensive collector. Here we need to create a folder to audit data found on the victim computer. This creates a .bat file which needs to be taken to the victim’s machine using a USB or shared network folder.

The comprehensive collector is recommended for one who does not know what they are looking for. I would recommend running the comprehensive collector both before and after an attack. While using this program the comprehensive collector tends to be slow, depending on how much information is stored on the device. The collector is more of a tool to funnel your view to look for with other tools.







Advantages and Disadvantages of Redline:

Pros:

* Very good for looking at network traffic.
* Lists processes currently running and the PIDs, PATH, what user is running them, and the parent process.
* Lists the drivers for the computer.
* Can list the entire giving you the name and if it has been modified. Cannot see deleted files on the system.
* Searching is good, when you press enter when searching it will highlight the files.
* Tagging system is intuitive, and you can comment on the tags if need be
* Clean interface with information categories that help you funnel your search

Cons:

* When running the tool, does not tell you progress on the collection, and then escapes the command window when the tool is done, making it seem like it crashed to people who don’t know how it works.
* Does not show files deleted in attacks.
* Cannot see file contents when looking at the filesystem
* Long wait times for the comprehensive search, which scales on how much information is on your system.
* Did not track the attacker moving around in the filesystem.

Major Information Found:

The major information found is the edited files in the File enumeration section. The networking section gave us the ports that the attacker was listening on. Looking at tasks we can get see persistence from the attacker planted on the system.

Applications of Redline:

The applications of redline include analyzing and viewing imported audit data. Streamline memory analysis and audit and collect all running processes from registry, event logs, memory, network information and web history. Users of FireEye’s Endpoint Threat Prevention Platform (HX) can open triage collections directly in Redline for in-depth analysis.