Mandiant redline user guide

Redline, Mandiant's main free tool, provides users with host discovery capabilities to find signs of malicious activity through storage and file analysis and the development of a threat assessment profile. Redline enables users to thoroughly monitor and collect all running processes and drivers from memory, file system metadata, registry data, event logs, network information, services, tasks, and web history. Analyze and view imported monitoring data, including limiting and filtering results in a specific time frame using Redline's timeline functionality using the TimeWrinkle™ and TimeCrunch™ functions. Optimize storage analysis with a proven malware analysis workflow based on relative priority. Identify processes that are more likely to be examined using the Redline Malware Risk Index (MRI) score. Perform an analysis of the Compromise Indicator (IOC). The Redline Portable Agent comes with a number of IOCs and is automatically configured to collect the data required to perform the IOC analysis and an IOC match result check. In addition, Redline can be used in conjunction with Mandiant for Intelligent Response® (MIR®) and Mandiant for Security Operations™: Investigators can open audits in Mandiant for Intelligent Response (MIR) directly in Redline to quickly identify a malicious process and create an IOC based on analysis. MIR can use this IOC to quickly sweep a network to identify all other systems running the same or similar malware. Mandiant for Security Operations users can open Triage collections directly in Redline to perform an in-depth analysis that allows the user to set a timeline and the scope of an incident. Mandiant Redline 1.11 includes several changes to improve the user experience and adds support for Windows 8 and 2012. A redesigned search box remains open and allows users to search and filter for a specific column. You can also filter lists by multiple tags at the same time and choose whether to include only items that have a comment or not. Finally, the Redline Collector now provides beta support for collecting Windows 2012 and Windows 8 data. Supported operating systems: Windows XP, Windows Vista, Windows 7, Windows 8 (32-bit and 64-bit) User's Guide :: Mandiant Redline 1.11 (PDF) Redline Blog :: Mandiant Redline Blog Windows :: Mandiant Redline v1.11 Official Website :: [Editor's Note: My wife has been complaining for some time that her laptop is running slowly. I'm not whether the system is really slow due to its specifications or the number of images it has :) . But then I thought -- this is a good opportunity to try Redline by Mandiant to wear my Sherlock Holmes hat and maybe I find something interesting. Below are the steps taken to do a live memory capture with Redline and its comprehensive agent collectors for deep malware hunting! Luis] After the identification phase of the incident handling process, which included, have detected malicious acts or deviations from normal operation. The containment phase comes. This is the third stage of responding to computer incidents. Through this step, one of the things we do is an initial analysis of the compromised system by taking a low-profile approach. Is also where we collect the relevant data from the system – in forensic terms this step is where you can preserve digital evidence. Normally, we would make a forensic picture of the affected system for further analysis. One thing that should be part of our forensic image is the disk imaging and a memory dump (volatile data). One of the tools that can help incident handlers view the storage/volatile data for further forensic analysis is The Volatility Framework and associated plug-ins. Another powerful one is Memoryze by Mandiant. Memoryze version 3.0 was released last July and supports a variety of operating systems. Since the release of Memoryze, Audit Viewer has been the tool of choice to interpret and visualize its output. These two tools have evolved and are mixed in Mandiant Redline. Last December, Redline 1.11 was released with support for Windows 8 and 2012. Redline is a free utility that speeds up the process of triaging hosts suspected of being compromised or infected while supporting incoming live storage analysis. In addition, this tool can also help you find malware by using it when Indicators of Compromise (IOC), which is a very powerful method and can be used to find threats at the host or network level. To run Redline and perform live system memory capture, the method suggested in the User's Guide is used. It is very straightforward and consists of the following 6 steps: We went through the user manual and after Mandiant you should install Redline in a pristine system. Mandiant recommends this approach due to the inability to ensure that your system is safe and malware-free. In this way, you would ensure that the results and the IOC database are not compromised. In addition, there is no risk of overwriting or destroying evidence from disks or memory. Mandiant even recommends running the redline on a system that is completely disconnected from the network. That said, I'm lighting up my VMware workstation and installing a new Windows 7 32-bit system. We have not completely disconnected the system from the network. We have positioned it in the Bridge VMnet to have access to our home network and access the Internet to download things. We have downloaded and executed. The first thing it will say is that Redline requires Microsoft .NET 4. If not installed, it will be installed on the Microsoft . NET installation web page. Installation is quick and easy. Just follow the User's Guide. When the installation is complete, you will be presented a nice web interface as shown below. After Redline has been guided by the user guide and getting to know the user guidance, it has ways it calls collectors to collect data from the suspicious system. that the Collector, Comprehensive Collector and IOC Search Collector and the 3 supported methods. We decided to run the Comprehensive Collector to collect most of the data from the system for comprehensive depth analysis. Each of the methods is well explained in the User's Guide. In addition, we have also selected to capture a memory image that is not selected by default. The remaining options in terms of storage, hard drive, system and network remained unaffected. We selected a folder and saved the collector settings. Then we copied the Collector folder into a USB stick. Then we went with the USB stick to my wife's computer and started the RunRedlineAudit.bat script. This script will traverse the collector settings we define and collect all the data and store the results in a folder with the name of the computer host name. It took about 3 hours to capture all the data – the system had 4 GB of ram and a slow hard drive – we then moved the USB stick back into the redline system and used the Analyze Data from the main menu. Then selected by Collector to load the data into Redline. We have selected the folder location of the data and at this stage you can also compare the data with IOC artifacts of your choice. At this stage, we will skip the IOCs. Then click Next and you select the name to save the analysis session. It then starts loading all the data and creating the analysis session. After loading the data we will be presented with a nice Start your Investigation page. This is the home page of your analysis and contains several steps suggested by the tool to support your investigation: I check a triage collection of MSO. I'm investigating a host based on an external Investigative Lead. I'm checking a full live response or a memory image. I check web history data. I would like to search my data with a number of compromise indicators. We will go through the investigation steps in another post. But, it's impressive to see how easy it is to capture an enormous amount of information in an automated way. The tool captures the entire file system structure, network status, system memory, registry content, processes information, event logs, Web browser history, service information, and so on. The interface is also well designed and provides an interesting workflow (collect, import, examine) that presents suggested scan steps that you should take to examine the data and look for signs of evil. As you could see, this part is the boring part (collecting and importing). The interesting part is to become familiar with these live system recordings collected by a variety of good and evil systems. Which then allows you to get a sense of what to look for and start your investigations and search for threats. This requires practice. Practice these kinds of skills, share your experiences, get feedback, repeat the practice and improve until you are satisfied with your performance. Performance. Performance.