

Redline

Users Guide

Please visit our forums: https://forums.mandiant.com/

MANDIANT Redline Users Guide

MANDIANT Corporation

Disclaimer

Copyright © 2012 MANDIANT, INC.

This documentation and any accompanying software are released “as is.” MANDIANT makes no warranty of any kind, expressed or implied, concerning these materials, including without limitation, any warranties of merchantability or fitness for a particular purpose. In no event will MANDIANT be liable for any damages, including any lost profits, lost savings, or other incidental or consequential damages arising out of the use, or inability of use, of documentation or any accompanying software, even if informed in advance of the possibility of such damages.

MANDIANT® and MANDIANT Intelligent Response® are registered trademarks of MANDIANT, INC. Redline™ is a trademark of MANDIANT, INC.

Windows®, Internet Explorer®, and Windows Vista® are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Table of Contents

1. Introducing MANDIANT Redline 1
    1.1. Redline Features 1
    1.2. Working with Redline 1
2. The Redline User Interface 4
    2.1. The Getting Started Screen 4
    2.2. The Redline Menu 5
    2.3. Collecting Data 7
    2.4. Analyzing Data 11
    2.5. The Investigation Window 11
    2.6. Malware Risk Index Report 14
    2.7. Redline Options 16
3. Workflow 22
    3.1. Collecting Data 22
    3.2. Importing Data 25
    3.3. Investigating 27
    3.4. Indicators of Compromise 31
    3.5. Acquisitions 33
A. Installation 36
    A.1. System Requirements 36
    A.2. Installing Redline 36
    A.3. Removing Redline 40
    A.4. Upgrading Redline 40
    A.5. MANDIANT Support 40
B. Incident Response and Investigation Best Practices 42
    B.1. Overall Process 42
    B.2. Data Collection 43
    B.3. Data Handling 43
    B.4. Data Analysis 44
    B.5. Reporting 44
    B.6. Final Words 45
Index 47



Chapter 1
Introducing MANDIANT Redline

MANDIANT transforms how organizations detect, respond to, and contain security breaches. Through our commercial and free products, we equip front-line incident investigators with superlative tools and technologies that support them in providing a quick and effective response when organizations need it the most.

Redline is MANDIANT's free tool for investigating hosts for signs of malicious activity through memory and file analysis, and subsequently developing a threat assessment profile.

1.1. Redline Features

Rapid Triage

When confronted with a potentially compromised host, responders must first assess whether the system has active malware. Without installing software or disrupting the current state of the host, Redline thoroughly audits all currently-running processes and drivers on the system for a quick analysis; for a detailed analysis, it also collects the entire file structure, network state, and system memory.

Reveals Hidden Malware

The Redline Collector can capture and analyze a complete memory image, working below the level at which kernel rootkits and other malware-hiding techniques operate. Many hiding techniques become extremely obvious when examined at the physical memory level, making memory analysis a powerful tool for finding malware. It also reveals "memory only" malware that is not present on disk.

Guided Analysis

MANDIANT Redline streamlines memory analysis by providing a proven workflow for analyzing malware based on relative priority. This takes the guesswork out of task and time allocation, allowing investigators to provide a focused response to the threats that matter most.

Redline calculates a "Malware Risk Index" that highlights processes more likely to be worth investigating, and encourages users to follow investigative steps that suggest how to start. As users review more audits from clean and compromised systems, they build up the experience to recognize malicious activity more quickly.

1.2. Working with Redline

As you investigate a system, here's how Redline will help you focus your attention on the most productive data:

Investigative Steps

Redline can collect a daunting amount of raw information. Its investigative steps help provide a starting place by highlighting specific data and providing views that are most commonly productive in identifying malicious processes. Unless you are pursuing a specific "lead", we recommend working through the steps in order, examining the information for entries that don't match your expectations.

The key to becoming an effective investigator is to review Redline data from a variety of "clean" and "compromised" systems. As you gain experience, you will learn to quickly identify suspicious patterns.

Malware Risk Index Scoring

Redline analyzes each process and memory section using a variety of rules and techniques to calculate a "Malware Risk Index" for each process. This score is a helpful guide to identifying those processes that are more likely to be worth investigating. Processes at the highest risk of being compromised by malware are highlighted with a red badge. Those with some risk factors have a grey badge, and low-risk processes have no badge.

The MRI is not an absolute indication of malware. During an investigation you can refine the MRI scoring by adjusting specific hits (identifying false positives and false negatives) for each process, adding your own hits, and generally tuning the results.

Indicators of Compromise (IOCs)

MANDIANT has developed an open, extendable standard for defining and sharing threat information in a machine-readable format. Going well beyond static signature analysis, IOCs combine over 500 types of forensic evidence with grouping and logical operators to provide advanced threat detection capability.

Redline provides the option of performing IOC analysis in addition to MRI scoring. Supplied a set of IOCs, the Redline Collector will be automatically configured to gather the data required to perform a subsequent IOC analysis; after the analysis is run, IOC hit results are available for further investigation.

For more information about the IOC standard, visit *http://openioc.org/*.

MD5 Whitelisting

By default, Redline collects all processes, a large number of which are standard and known-good. MANDIANT has extracted MD5 hashes of various operating system components, based on standard, unaltered installations and service-pack upgrades — nearly a million hashes for Microsoft Windows components alone and increasing. Redline ships with a collection of common hashes, and you can add more hashes as you discover common components in your own network.

Whitelisting allows you to filter out a large amount of data that is not likely to be interesting: data that corresponds to unaltered, known-good software components. Whitelisting can be toggled on and off, giving you control of the risk one takes by not investigating every process and memory section.

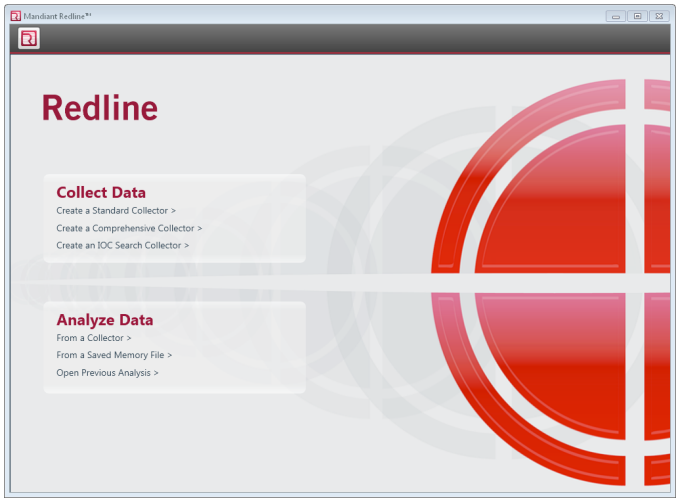
Expanded and updated whitelists are available on MANDIANT forums. These are updated independently of Redline and contain all officially-published Microsoft executables. Please head to *https://forums.mandiant.com/forum/redline* for more information.



Chapter 2
The Redline User Interface

- **Getting Started** or the **The Redline Menu** screen, where you choose the type of analysis you wish to perform.
- A **Start Your Analysis Session** screen which varies depending on the choices you've made; on this screen, you may choose to use Indicators of Compromise, choose an audit file, and configure which audits are performed.
- **The Investigation Window**, which leads you through the analysis steps.
- And **Information Panes**, where you see the results of an analysis, identify suspicious activities, and dig deeper into the suspect system to determine its risk profile.

2.1. The Getting Started Screen



MANDIANT Redline presents a simple **Getting Started** screen when it is run. Each option on this screen, from top to bottom, is described below; the same options are also available through the Redline menu. Detailed descriptions of the major functional components follows this overview.

Under Collect Data

Create a Standard Collector
: Configures a collector that will gather the data needed for a complete Malware Risk Index Analysis. Use this option when you do not intend to look for IOCs.

Create a Comprehensive Collector
: Configures a collector that collects a full suite of data, satisfying the requirements for all audit types. Use this option when digging deeper with an IOC analysis, or when you have only a single opportunity to collect data.

Create an IOC Search Collector
Configures a collector with only those options required by the IOCs you have selected, and nothing else. The data is filtered to return only those items that match an IOC. Use this option when performing single-shot IOC analysis for triage purposes.

Under Analyze Data

From a Collector
Using a Collector, a full memory audit can be quickly collected from multiple target systems and then imported for analysis using this command.

From a Saved Memory File
A number of third-party utilities, can capture a direct image of the physical memory of a system. Although these images lack important information normally derived from an examination of the OS, Registry, and various system files, Redline can perform a limited analysis and report any anomalies.

Open Previous Analysis
An analysis session may be saved, then re-started. Sessions that have been saved to media can be accessed by choosing **Open a Previous Analysis** and locating the session using a standard file selection window.

If you have saved sessions, the most-recently used sessions will be displayed below **Recent Analysis Sessions**. Selecting a session name will immediately restore the session.

2.2. The Redline Menu



At the top of the window, marked by the "**R**" logo, the Redline menu displays the following functions:

Create a Standard Collector
Configures a collector that will gather the data needed for a complete Malware Risk Index Analysis. Use this option when you do not intend to look for IOCs.

Create a Comprehensive Collector
Configures a collector that collects a full suite of data, satisfying the requirements for all audit types. Use this option when digging deeper with an IOC analysis, or when you have only a single opportunity to collect data.

Create an IOC Search Collector
Configures a collector with only those options required by the IOCs you have selected, and nothing else. The data is filtered to return only those items that match an IOC. Use this option when performing single-shot IOC analysis for triage purposes.

Analyze Collected Data
Having collected data using the Standard, Comprehensive, or IOC Search Collectors, start your analysis tasks using this choice.

Analyze a Saved Memory File

The comprehensive Collector generates the best Redline investigative results, but Redline can also use memory images captured with other tools, though with reduced functionality. Select this option if you wish to import a memory file obtained from a suspect system. See *Configuring Collection Options* for details regarding acquisition options.

Analyze this Computer

This option is offered only for training and demonstration purposes. Selecting this option will perform a robust acquisition and analysis of the local system, with options for saving the results. This is an great way to gain experience using Redline but **is not** recommended for investigations.

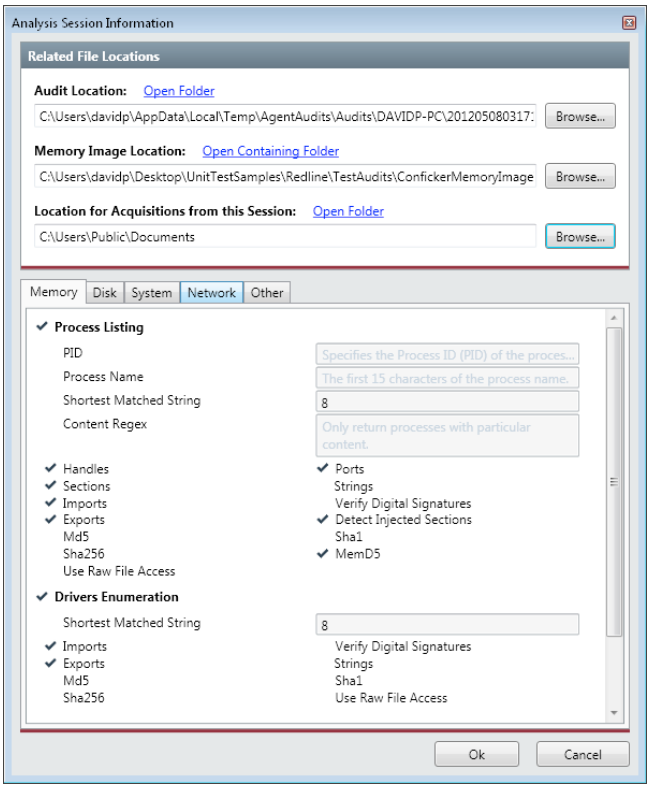
For real-world use on multiple systems, follow the workflow for *Using a Collector*. **It is important that Redline analysis be carried out on a clean and protected workstation:** this is easily accomplished using the Collector to bring captured data from potentially compromised systems to a secure Redline workstation. **Do not risk compromising your collected evidence!**

Open a Saved Analysis

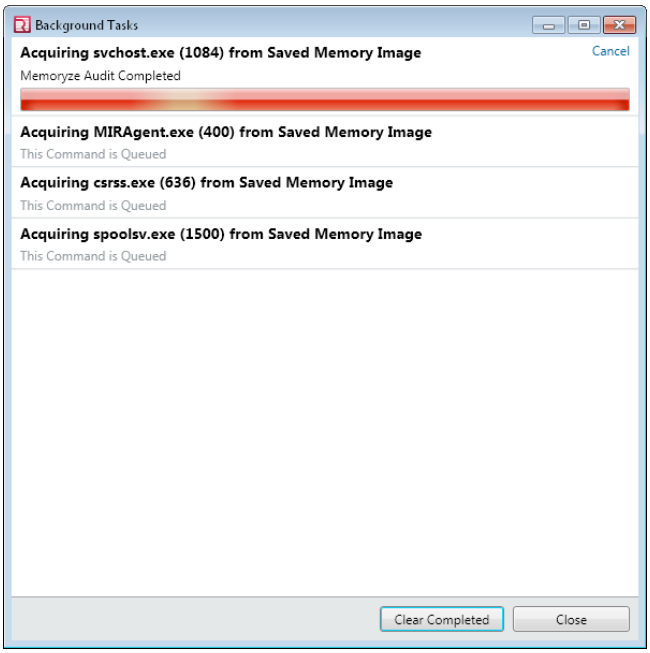
Redline sessions can be saved to storage media for later analysis. Choose this optionn if you wish to continue a saved investigation. Redline analysis files use a `.mans` filename extension.

Session Information

Displays information about the current Analysis session: file storage locations and audit configuration. This item is disabled if an analysis has not yet run.



Background Tasks
Lists completed and in-process tasks.



Help
Opens your browser to the MANDIANT Forums, where you can participate in the Redline user community to seek help, assist others, and learn effective incident response and analysis procedures.

About
Displays version information, links to support webpages, and the End User License Agreement.

Recent Analysis Sessions
Provides quick selection of recently-saved Redline analysis data files.

Redline Options
Configures Redline global options, including adjustment of the rules Redline uses to calculate a Malware Risk Index score. See *Redline Options* for details.

Exit Redline
Quits MANDIANT Redline. Changes are saved automatically while performing an investigation. To continue with an analysis after quitting, you can open the saved audit file directly or select it from the **Recent Analysis Sessions** menu.

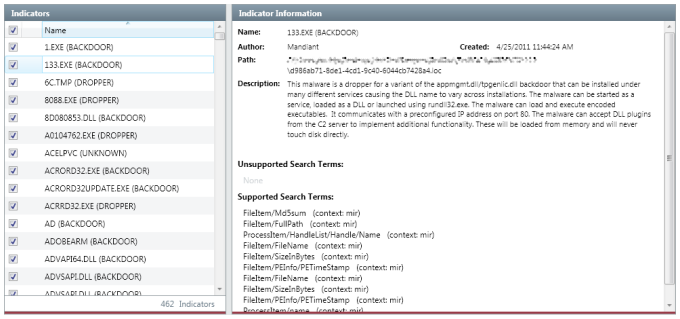
2.3. Collecting Data

After selecting a Standard, Comprehensive, or IOC Collector, you will be presented with the **Start Your Analysis Session** wizard. The contents vary slightly depending on the type of collection being performed.

If you chose a Standard or Comprehensive Collector, you have the option to select the types of data collected; if you select an IOC Collector, you will first select IOCs, then the types of data collected. In either case, you may also choose to perform a live memory acquisition.

2.3.1. Configuring IOC Collection

After selecting an **Indicators of Compromise** folder location, a list of **Indicators** will be displayed on the left. By default, all compatible IOCs in this list are enabled. Each IOC can be enabled and disabled selectively using its checkbox.



To enable or disable the entire list, select the checkbox at the top of the column. Selecting a column header will sort or reverse-sort the list.

Selecting an IOC name displays information about the IOC to the right. In particular, any issues or warnings are listed and a summary of search terms is provided:

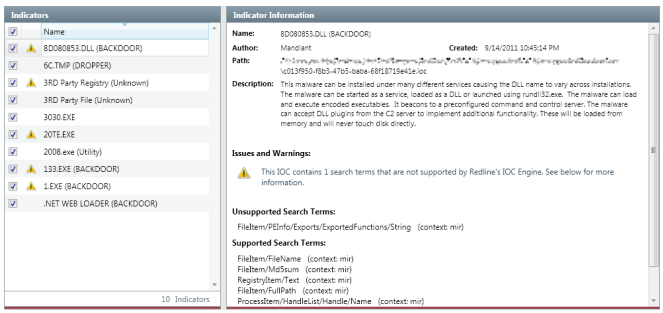
Not Collected Search Terms
: Lists the terms that Redline was unable to hit because the original audit collection did not have the proper modules or params enabled.

Unsupported Search Terms
: Lists terms which are not understood by the IOC engine and do not relate to the audit data schemas. These search terms will not produce any hits in Redline.

Supported Search Terms
: Lists those terms that are recognized by the IOC engine and will be used in Redline data collection and analysis.

If an IOC is not compatible with Redline, it will be highlighted in the **Indicators** list. Selecting the IOC Name will display information about the issue in the **Issues** tab on the right:

- A **Warning** indicates that the IOC will be included in the IOC report, but it may falsely indicate there were no hits (a false negative).
- An **Error** indicates that the IOC can not be included in the IOC report.



IOC hit detection and report generation can be a lengthy process. To improve productivity, Redline executes this functionality as a background task, allowing you to perform investigation tasks while awaiting the report.



After configuring IOC Collector options, you will be presented with the *Section 2.3.2, "Configuring Collection Options"*.

2.3.2. Configuring Collection Options

Review Script Configuration



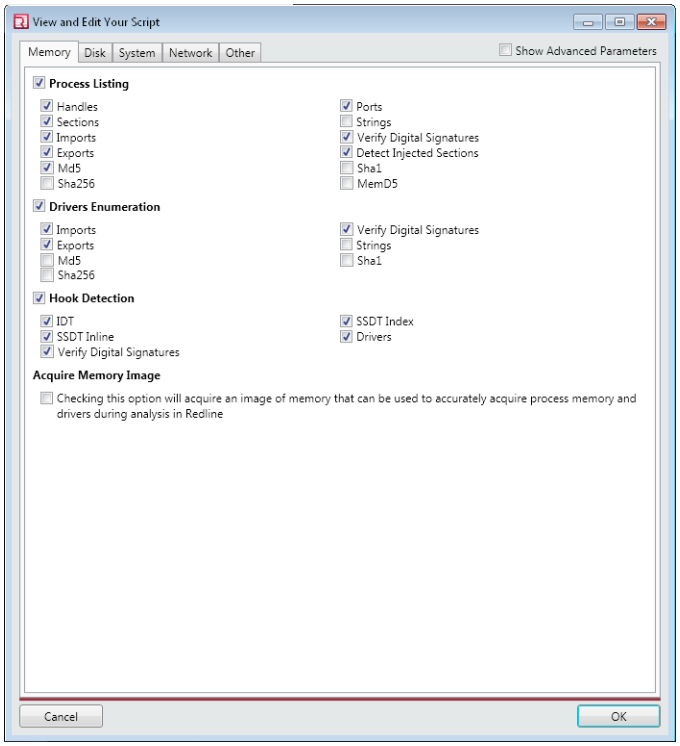
Redline automatically configures Collector options as follows:

Standard Collector
: Configures a collector that will gather the data needed for a complete Malware Risk Index Analysis. Use this option when you do not intend to look for IOCs.

Comprehensive Collector
: Configures a collector that collects a full suite of data, satisfying the requirements for all audit types. Use this option when digging deeper with an IOC analysis, or when you have only a single opportunity to collect data.

IOC Collector
: Configures a collector with only those options required by the IOCs you have selected, and nothing else. The data is filtered to return only those items that match an IOC. Use this option when performing single-shot IOC analysis for triage purposes.

Selecting **Edit your script** allows you to modify the types of data that will be collected. Collection options are categorized as **Memory**, **Disk**, **System**, **Network**, and **Other**. These are arranged as tabs near the top of the window.



Using **Show Advanced Parameters**, at the top right, allows you to adjust values used for minimum string lengths, maximum file sizes, configure pre-filters, and other options useful when performing a specifically-targeted collection.

Note that when using IOCs, Redline will show **Script may not gather all the data required by your IOCs** when the collector configuration is incompatible with the IOCs you previously selected. Use **Click here to fix** to re-enable those options required by your IOCs.

Disabling certain options may reduce the accuracy of MRI calculation

In addition to capturing various data, Collectors can acquire a live memory image of the suspect system. This enables you to "dig deeper" when you find a suspicious process, driver, device, or hook. Select **Acquire Memory Image** to capture a memory image.

Specify Collector Location

Finally, in **Save Your Collector To** provide a save location for the Collector or select **Browse** to select an empty directory using a standard file selector. (A new folder can be created in the file selector using a right-click menu.)

2.3.3. After Configuration

Clicking **OK** starts the Collector build process. A progress bar is displayed during this time.

When complete, **Portable Agent Instructions** will be displayed. If you selected a portable media device for **Save Your Collector To** when configuring collection options, you can begin

auditing suspect machines; otherwise, copy the Collector package to a USB stick or other appropriate media.



While you can run the Collector on the Redline workstation (and this can be valuable while learning to use the software), MANDIANT **strongly** advises that all collection be performed using portable media, and that your Redline workstation remain air-gapped and secure from compromise.

2.4. Analyzing Data

After collecting data using the Redline Collector or a live memory acquisition tool, you can begin your analysis of the suspect system.

Recent Analysis Sessions provides a quick-select for previous sessions. The **Investigation Window** will be opened.

If you select **Open a Previous Analysis**, a standard file selection window will allow you to choose a saved analysis not listed in recent sessions. The **Investigation Window** will be shown.

The other options, **From a Collector** or **From a Saved Memory File**, will present a **Start Your Analysis Session** wizard. The contents vary slightly depending on the type of collection being performed.

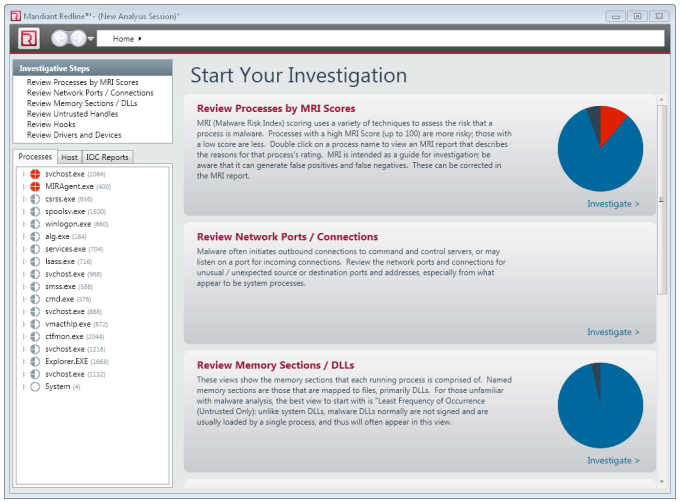
Redline will need to know which **Audit Location** or **Location of Saved Memory Image** folder contains data from the suspect system. You may type a path or **Browse** to use a standard file selector. If you are following MANDIANT best practices, the data is probably on a removable media device.

In either case, you may also choose an **Indicators of Compromise Location** folder. The IOCs will be checked for compatibility with Redline and with the collected data. Incompatible IOCs will be disabled. See *Section 2.3.1, "Configuring IOC Collection"* for details.

Next, provide a location for **Save Your Analysis to** and select **Ok**. Redline will immediately begin an MRI analysis of the data and, upon completion, will present the **Investigation Window**.

2.5. The Investigation Window

After acquiring and analyzing data, MANDIANT Redline assists you in performing a hands-on investigation of the results. The **Analysis Session** screen provides an overview of the investigation process, lists of processes and host system information, and a series of review steps with links to the specialized tools required for each step. Selecting an investigative step changes the **Analysis Session** screen to an informational pane specific to the step or selected item.



The Investigation window commandsmprises, top to bottom, left to right:

Navigation

Redline Menu

See *The Redline Menu*.

Back/Forward

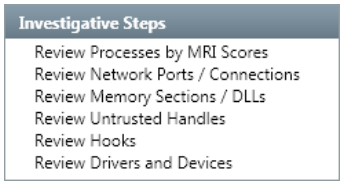
Navigates between investigation pages, similar to a web browser. Clicking the small down arrow to the right will display a list of recently-visited pages.

The address bar to the right provides a “breadcrumbs” trail that can also be used to navigate pages or navigate quickly to views that are not in your immediate history.

Display/Hide Help and Options

Displayed to the right of the address bar when reviewing an investigative step, clicking the arrow will display information about the view and may provide options for displaying more or fewer details.

Investigative Steps



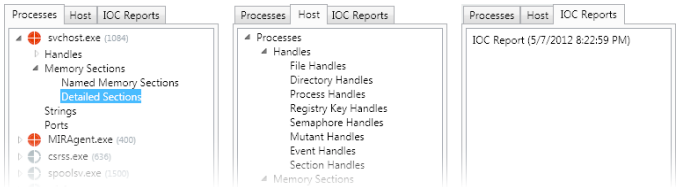
Lists shortcuts to the various investigation review pages. These are duplicated in the main window in the **Start Your Investigation** list of steps.

For each step, lists of findings will be displayed in the **Information Pane** to the right. Double-clicking an entry may display a detailed view of that entry; right-clicking an entry will display options to **Copy** the entry as comma-separated, string and numeric values or **Copy with headers** the same, with the first line providing comma-separated string column headings.

Right-clicking a process, hook, or driver entry provides commands to **Acquire** the associated binaries. For processes, you can also **Search the Web** (Google) for the process name.

Having identified an item of interest, you may drill down to details using the **Quick Select** panel.

Quick Select



The **Quick Select** area provides several views into audit data and analysis.

Processes
Lists running processes, captured when the data was acquired. Each process entry may be expanded to show process detail categories. Clicking a detail item displays full results to the right.

The badge to the left of the process name indicates the Malware Risk Index for that process; the list is sorted according to recommended investigation priority:

A full red badge: The process has hit on at least one specific MRI rule and should be prioritized for investigation first.

A semi-grey badge: The process has a number of negative risk factors and is more worthy of investigative effort than those that do not.

An empty badge: No MRI rule hits or negative risk factors were found.

Host
Lists information about the host system from which the data was acquired. Each entry may be expanded to show host detail categories. Clicking a detail item displays full results to the right.

Some views support acquisitions. Right-click a driver or process to select an acquisition option. A list of acquired data can be viewed by selecting **Acquisition History** in the quicklist. Choose a file path to view the acquisition in the standard file explorer. **Edit** provides a shortcut to **R** → **Session Information**.

IOC Reports
Lists IOC hits reports that have been generated against this analysis session. Selecting a report displays it to the right.

Information Pane

The area to the right changes depending on selections made on the left. When the Investigation window is first opened this area displays **Start Your Investigation** or **System**

Information (if an investigative session is underway), and a list of investigative steps with a description of each step.

As you make selections, the content changes. When an **Investigative Step** is selected the Information pane will list items appropriate to that step: processes, ports, DLLs, drivers, etc.

When available, clicking **Display/Hide** at the top right will display information about the view and may provide options for viewing more or fewer items.

In some views, you may choose **Include Whitelisted Items** and **Hide Whitelisted Items** toggle the listing of items with a checkmark in the **MD5** column. Entries lacking a checkmark are not in the whitelist. A button to the right of this control provides a shortcut to the **Redline Options** → **Whitelist Management** page, where you can change the default view setting.

In lists, double-clicking a process-related entry will open a Malware Risk Index report providing information about the entry and, in particular, descriptions of any discoveries by Redline.

Double-clicking an entry may display a detailed view of that entry; right-clicking an entry (or selection of entries) will display options to **Copy** the data as comma-separated, string and numeric values or **Copy with headers** the same, with the first line providing comma-separated string column headings.

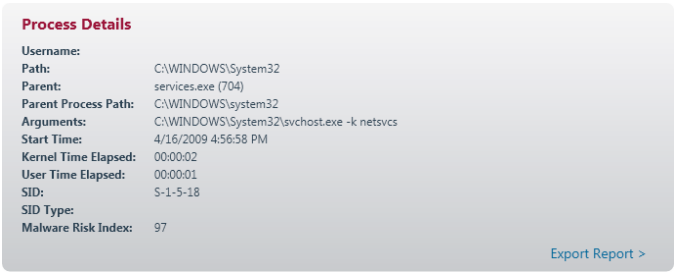
Right-clicking a process, hook, or driver entry provides commands to **Acquire** the associated binaries. For processes, you can also **Search the Web** (Google) for the process name.

2.6. Malware Risk Index Report

The Malware Risk Index Report is displayed when viewing a process in detail, by double-clicking its entry in a table or selecting it through the **Quick Select** on the left. It provides the following sections of information and control:

Process Details

Provides detailed information about the specific process. Use **Export Report** to save a Microsoft Word version of the analysis.

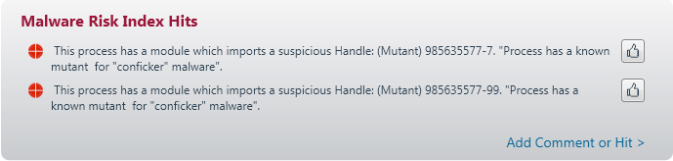


Malware Risk Index Hits

Describes the reasons Redline identified the process as a risk, if it did so.

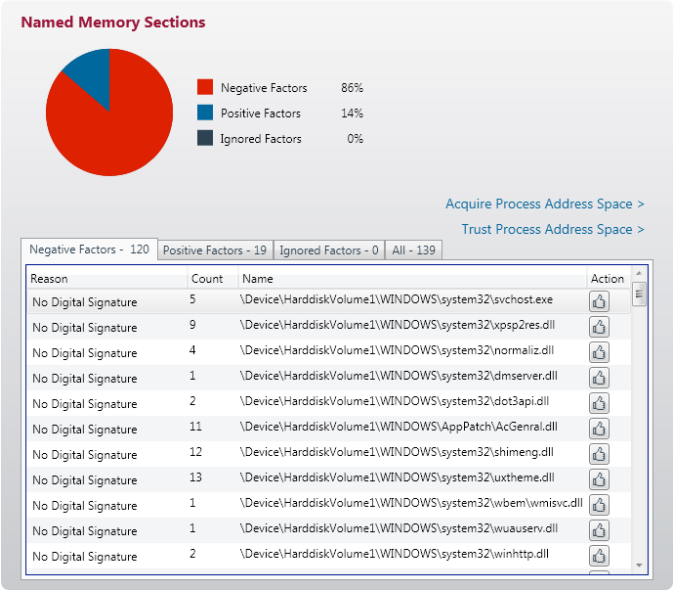
If Redline has generated a false-positive hit or false-negative hit, use **Thumbs Up** or **Thumbs Down** (respectively) to correct Redline's analysis. This will help improve the accuracy of MRI scoring for other processes

Use **Add Comment or Hit** to append additional descriptions to this section. Hits will be shown with a red badge and the text "User Flagged"; comments are shown with a grey badge and the text "Comment". These comments and additional hit factors will be included in exported reports.



Named Memory Sections

Displays a pie graph of risk factors, followed by lists of those factors presented in various tables.



You may use **Thumbs Up** to correct false-positive hits; or **Thumbs Down** to undo a correction and revert to Redline's MRI scoring for that item.

Use **Trust Process Address Space** to mark all **Negative Factors** items as false-positive hits. The **Negative Factors** list will be emptied: its items will be found in **Positive Factors** with "User Trusted" as the reason and an **Cancel** button which will return the selected item back to **Negative Factors**. The original scoring can be restored by clicking **Remove User Trust**.

You can perform a deeper analysis of a suspect process using **Acquire Process Address Space** to fetch a copy of the live memory capture for the item you are investigating. Note that

Redline does not provide tools for inspecting address spaces: you will need to use a third-party tool.

Search

When the Information pane is displaying **Strings**, a **Search** bar is available at the top of the pane. Typing a search term and pressing **Enter** will limit the list to strings that contain your search term.

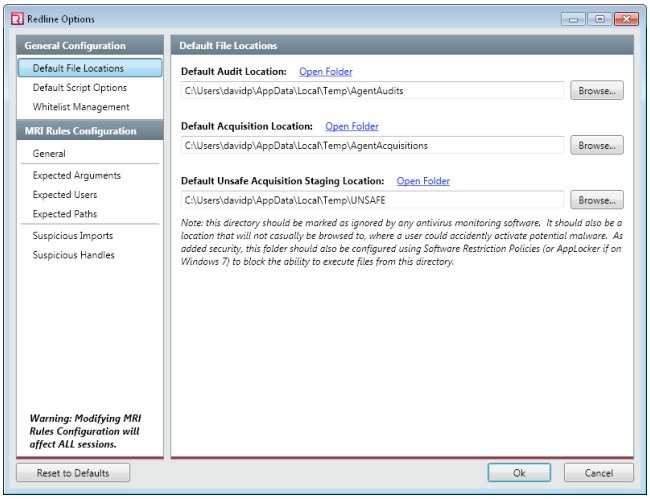
2.7. Redline Options

Selecting **Redline Menu** → **Redline Options** allows you to choose default file locations and to change the rules Redline uses in calculating MRI scores.

There are two sections in the **Redline Options** window: **General Configuration** and **MRI Rules Configuration**. To their right is the option settings area.

2.7.1. General Configuration

Default File Locations
Selects folders for audits, acquisitions, and acquisition staging.



Default Audit Location
The directory where audit data, collected from the local machine or from an image, is stored. Redline names its folders using the host name of the target system and the date and time the audit was collected.

Default Acquisition Location
The directory where processes and drivers acquired from memory images are stored. These files are stored in a password protected ZIP archive as a precaution against accidental activation of malware. This location may be changed on a per-session basis. (The password is “Safe”.)

Default Unsafe Acquisition Staging Location

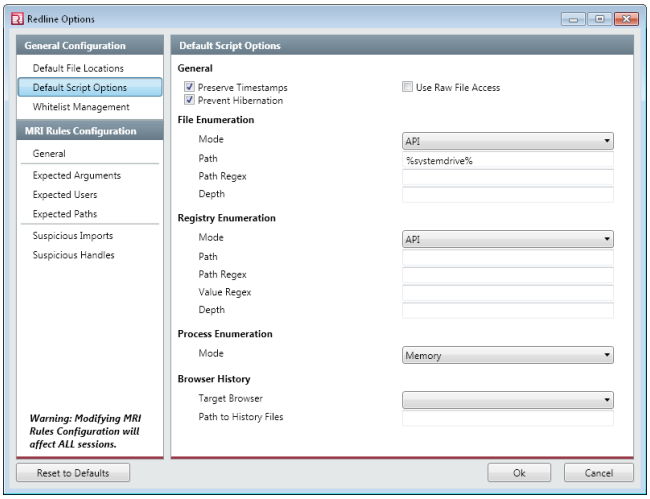
The directory where acquired processes and drivers are temporarily stored during the acquisition process, prior to being archived in a ZIP file in the "Default Acquisition Location" (configurable for each session, defaulting to **Default Acquisition Location**).

It is best to select a directory that is well-secured against accidental end-user discovery and program execution.

Any anti-virus software on the workstation should be configured to ignore this directory, to prevent it from deleting or quarantining any malware.

Default Script Options

Audit modules used in collecting data have several configurable options.



General

Preserve Timestamps

When enabled, file timestamps are not updated when a file is read.

Prevent Hibernation

When enabled, the system being audited will not be allowed to hibernate. This allows the audit to complete in a timely fashion.

Use Raw File Access

When enabled, the operating system is bypassed when reading data.

File Enumeration

Configures the access mode, search path root, path regex, and search tree depth for file enumeration.

Registry Enumeration

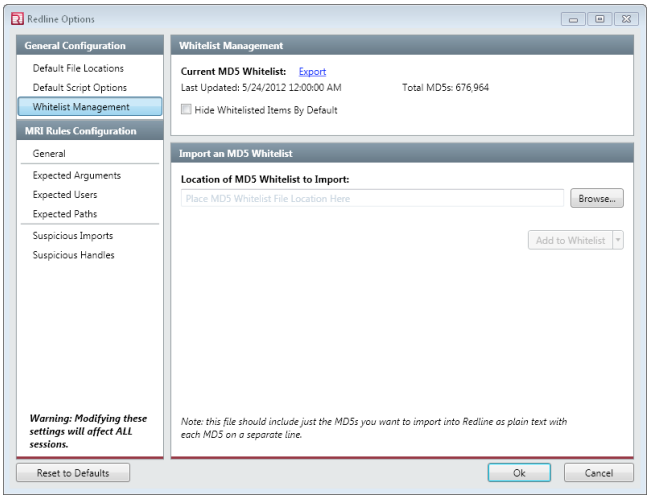
Configures the access mode, search path root, path and value regexes, and search tree depth for registry enumeration.

Process Enumeration

Configures the access mode for process enumeration.

Browser History
Configures which browser caches and histories are enumerated.

Whitelist Management
MD5 Whitelists may be used to hide processes and memory sections that are known-good. [1] Note that changes made to Whitelist settings will be applied to all sessions.



Current MD5 Whitelist
Displays the datestamp and the number of known MD5 hashes. Select **Export** to save the current whitelist as a CSV file.

Hide Whitelisted Items
Selects the default process and memory section views, initially showing or hiding whitelisted items.

Import an MD5 Whitelist

Location of MD5 Whitelist to Import
Select **Browse** to choose a file using the standard file selector. The file format is a simple linefeed-separated list of MD5 hashes.

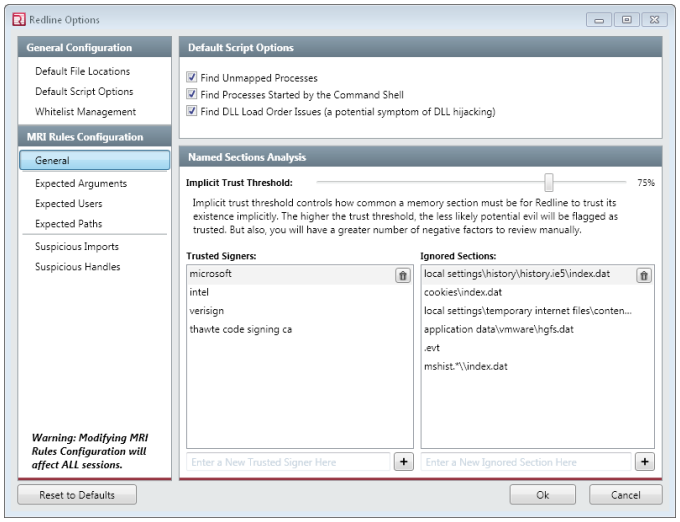
Add to Whitelist and Replace Whitelist
Whitelist files may be appended to or replace entirely the current MD5 Whitelist. The filter will be re-computed after each change. See *MANDIANT Support* for updates.

2.7.2. MRI Rules Configuration



Changes made to MRI Rules will be applied to all new sessions and restarts. Factory defaults can be restored by clicking **Reset to Defaults** at the bottom left of the options window. Note that Reset will affect all user-defined options.

[1] Redline "Malware Risk Index" scoring is probabilistic: there is a one-in-a-trillion risk of whitelisting a hash that is not in the table. We selected this type of filtering because it is incredibly fast and lightweight, important factors when running triage on huge data sets.



2.7.2.1. General

General MRI Configuration

Find Unmapped Processes

When enabled, processes that do not have a mapped memory section for the executable cause an MRI hit.

Find Processes Started by the Command Shell

When enabled, processes that were started by cmd.exe cause an MRI hit.

Find DLL Load Order Issues

When enabled, evidence of DLL hijacking causes an MRI hit. Process memory sections are analyzed and compared against the Process's path; discrepancies cause an MRI hit.

Named Section Analysis

Implicit Trust Threshold

Determines how common a named memory section must be for Redline to trust its existence implicitly. Named memory sections below the threshold cause an MRI hit.

At 100%, a named memory section would have to appear in all processes. Through experience, we have found a 75% threshold strikes a nice balance.

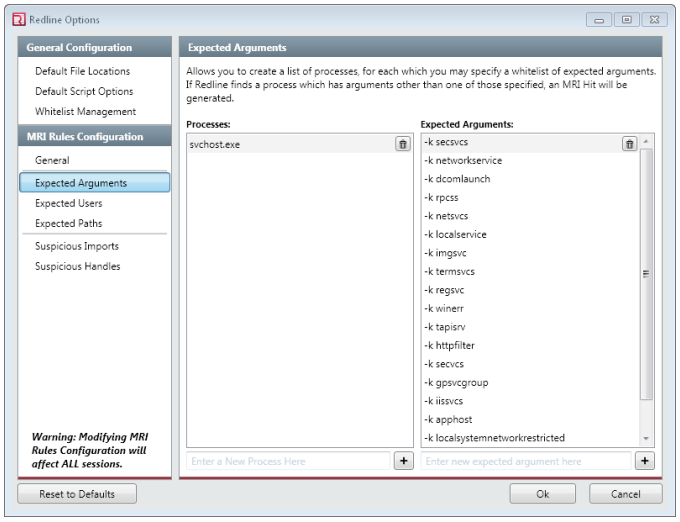
Trusted Signers

Lists certificate signers that are trusted when analyzing a signed and verified memory section. Trusted signatures are a factor in calculating the final MRI score.

Ignored Sections

Lists memory sections that can be safely ignored when calculating an MRI score. These mainly comprise non-binary memory section.

2.7.2.2. Expected Arguments, Expected Users, Expected Paths

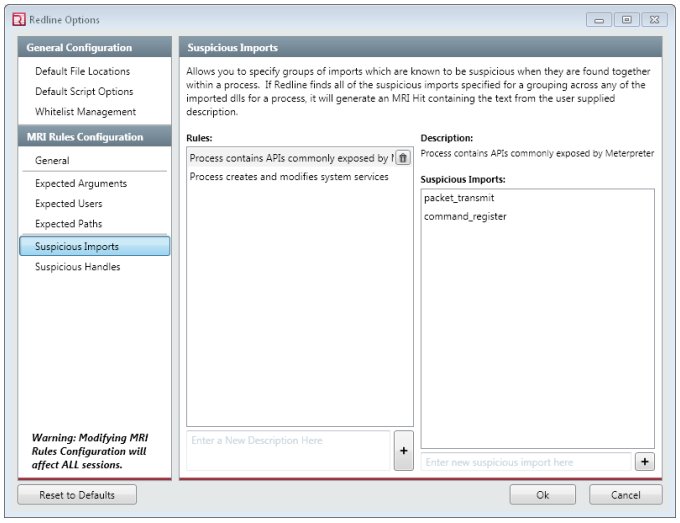


The "expected" set of configuration options whitelists the arguments, users, and paths associated with various system processes. If a process is started with an argument that is not listed, by a user not authorized, or on a path that is not expected, an MRI hit is generated.

Selecting a process name in **Processes** will display a list of its expected arguments, users, or paths as appropriate. New processes can be added by typing the process name in the **Enter a New Process Here** box at the bottom of the left column and clicking + **Add**; existing processes can be removed by selecting them and clicking 🗑 **Remove**.

You may add a new expected argument, user, or path to a selected process by typing it in the **Enter new expected argument or path here** box at the bottom of the right column and clicking + **Add**. Likewise, an item can be removed by selecting it in the right column and clicking 🗑 **Remove**.

2.7.2.3. Suspicious Imports

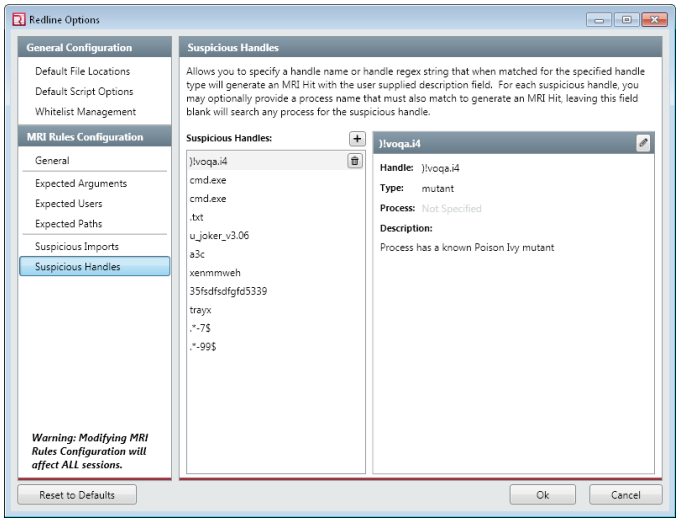


For any process, certain combinations of imported DLLs are indicative of compromise. If a process contains the group of suspicious imports, Redline will generate an MRI hit for that process.

Items listed in **Rules** are text descriptions of the group of suspicious imports. This text is used for the MRI hit description. You may add a new group rule by typing its description in the **Enter a New Description** box at the bottom of the left column and then clicking **Add**. Likewise, an item can be removed by selecting it in the left column and clicking **Remove**.

When a **Rule** is selected the group of DLL imports that should be considered suspicious when they are imported by a process are listed on the right. You can add DLLs by typing their name in the **Enter new suspicious import here** box at the bottom of the right column and clicking **Add**, or remove them by selecting the item and clicking **Remove**.

2.7.2.4. Suspicious Handles



A number of compromises may be identified by the presence of a unique handle name. **Suspicious Handles** allows you to adjust the list of suspicious handles, optionally associating a specific process name with the handle.

Items listed in **Suspicious Handles** are search term strings. New handles are added by clicking **Add**. On the right, you will provide a search term or regular expression (regex) for **Handle**; select the handle **Type**, the name of the **Process** associated with the handle (optional; leave blank to search all processes), and a text that will be used in the MRI **Description**. Handles are removed by selecting them and clicking **Remove**.

To modify an existing handle, select it in **Suspicious Handles**. Its details will be displayed to the right. Click **Edit** to make modifications to the entry, and click **Save** or **Cancel** when finished.



Chapter 3
Workflow

Fundamentally, Redline is a tool for acquiring and examining forensic data from hosts that are suspected of being compromised.

The typical Redline workflow is a three-stage process:

1. Collecting

The first step is collect data for analysis from the potentially compromised system. Redline supports several methods for accomplishing this: we recommend the Redline Collector, installed on a removable storage device. The Collector can then be taken to a host and used to capture and store the required data.

2. Importing

Once data has been collected from a host, it is brought back to a Redline workstation and imported for subsequent analysis. After it is imported, the resulting analysis session is saved as a `.mans` database file. This preserves your MRI hit or risk factor modifications, and reduces the time required to re-open the analysis.

3. Investigating

When the import and analysis is complete, you can begin the investigative process to determine whether a host is compromised and which processes are involved.

3.1. Collecting Data

Data acquisition can be performed using a variety of tools. In order of preference:

- Using the Redline Collector from a removable storage device.
- Using the MANDIANT Incident Response appliance.
- Using the MANDIANT Memoryze or a third-party memory imaging tool.
- Using Redline on the local computer (for training purposes only).

Of these options, the Collector is often the best choice when triaging a small number of systems: simply go to them, run the Collector from its removable storage device, and then return to a Redline workstation to perform an analysis and investigation.

The MIR appliance allows you to perform an audit and acquisition over the network and excels at auditing a large number of systems. When using MIR each system has an installed agent. Communicating with the agents over the network, a MIR installation can sweep tens of thousands of systems, collecting audits and acquisitions for subsequent analysis.

Many third-party tools capture memory as a `dd`-format image file. These can be analyzed by Redline, with some limitations, as described below.

Finally, audits and acquisitions can be performed by Redline on the system on which it is installed. This requires installing Redline and also requires that you perform this work on

a potentially compromised system. This is non-optimal: you can not be certain that your analysis results are not compromised, create the risk of overwriting potential evidence on disk or in memory, and may also tip off the attacker that they are being investigated.

3.1.1. Using a Collector

In order to minimally touch a compromised machine, Redline supports the creation of a standalone, portable Collector tool. This allows you to collect audits without installing Redline on the target system.

Creating a Collector

1. Mount a removable storage device on your (clean) Redline workstation.
2. Select **R** → **Create a Standard Collector** if performing triage; **R** → **Create a Comprehensive Collector** if you intend to do a deep dive.
3. Configure the Collector options. See *Configuring Collection Options* for details.
4. Finally, specify a **Save Your Collector To** folder location, clicking **Browse** to use the standard file selection window to choose the root of the removable media device.

   The Collector and its configuration files will be written to the removable storage device. When this process is complete, you may eject the device.

Collecting Data with a Redline Collector

Once your Collector device has been created it can be mounted on any supported Windows 32– or 64–bit system [1] of interest to perform a collection audit. Simply navigate to the device and run `RunRedlineAudit.bat`.

Redline will load its configuration, auto-detect the host operating system, and collect audit data onto the removable storage device. A typical analysis (without strings) will be under 50MB. Collection of strings greatly increases the size and a live memory acquisition will, of course, require free device space equivalent to the memory of the target system. Issues docs created during an audit can also become sizeable.

Audits and acquisitions for a target system are saved to a directory using a `hostname_date_time` file-naming pattern. You may collect from multiple systems, to the capacity of the removable storage device.

When you have collected audits for the target systems, continue with *Importing from a Collector or Memoryze Output Directory*.

3.1.2. Using a MIR Appliance

MANDIANT Intelligent Response (MIR) is an enterprise-grade solution for threat detection and response. Using MIR, tens of thousands of hosts can be monitored and swept automatically. MIR can collect the same memory analysis data needed by Redline remotely without having to physically visit the machine or locate administrative credentials.

[1] 32–bit Windows 7, Windows, 2003 SP2, Windows 2000 SP4, Microsoft Vista, and Windows XP SP2; 64–bit Windows 7, Windows 2008 R2, and Microsoft Windows 2003 SP2

Creating a MIR Audit Job

To collect information from Agents on a MIR-enabled network:

1. At the MIR Console, choose **File** → **New** → **Host Audit Job**.
2. Populate the **Targets** area with the Hosts that are to be audited. These can be dragged from the **Hosts** library or **Labels** library.

   It is best to test the Host Audit Job on a few hosts to check that the returned results are acceptable. When you are satisfied you can edit the job configuration (if you selected Hosts manually) or Label to add your remaining Hosts.
3. Using **Select an Audit Module to Add...** selector, choose audit modules for the job. Each module you choose will be listed below the selector; if the module has configurable parameters, those settings will be shown, with required parameters outlined with a red box.

   For use with Redline, you need to enable the following modules and settings:

   - System Information
   - Drivers by Signature (DriverList)
     - enumerate imports
     - enumerate exports
     - MD5
     - SHA1
     - SHA256
     - Verify Digital Signatures
   - Drivers by Memory (ModuleList)
   - Hook Detection
     - idt
     - ssdt_index
     - ssdt_inline
     - drivers
     - Verify Digital Signatures
   - Process Listing (Memory)
     - handles
     - sections
     - ports
     - enumerate imports
     - enumerate exports
     - MD5
     - SHA1
     - SHA256
     - Verify Digital Signatures
     - detect injected dlls
4. Click **Save**. You will be prompted to name the Job.

You can now acquire Host data using **Run Immediately** or by scheduling the job.

MIR audits are saved to a database. To open them with Redline, continue with *Opening a MIR Resource in Redline*.

For more information on MIR, consult the **MIR User Guide**.

3.1.3. Using Memory Imaging Tools to Create a Memory File

MANDIANT Memoryze and third-party memory acquisition tools that save their data as a dd-compatible image may be used with Redline. Instructions for capturing a memory image will vary with the tool selected for use.

Note that memory image files do not contain information for digital signatures, file hashes, system audit, and other meta-information captured through the Redline Collector or MANDIANT Intelligent Response. As a result, Redline can perform only a limited analysis of the target system. It is strongly recommended that you use Redline Collector or MANDIANT Intelligent Response to perform audits.

Acquiring a Memory Image

1. Using a third-party memory acquisition tool, configure or use options that correspond to...
   - creating a raw memory dump or snapshot, or
   - dumping physical memory to disk, or
   - saving a “dd”-format image file.
2. Copy or save the memory image to a removable storage device, network share, or other resource that is accessible by the Redline workstation.

Continue with *Importing a Saved Memory File*.

3.1.4. Using Redline on the Local System

Redline can collect data from the local Redline workstation. This feature should only be used for training purposes.

3.2. Importing Data

After audit and acquisition data has been captured, it must be imported into Redline for analysis and investigation.

If you included IOC analysis when configuring the collection parameters, a notification window will be displayed at the bottom of the screen, alerting you that processing and report generation is taking place in the background. This can be a lengthy process, but you are able to continue with your investigation while Redline works on your IOCs.

3.2.1. Importing from a Collector or Memoryze Output Directory

After using a Redline Collector or Memoryze to collect audits from one or more target systems:

1. Mount the Collector or Memoryze removable storage storage device on the Redline workstation,

OR

Make the network share containing the Memoryze output available to the Redline workstation.

2. In Redline select **From a Collector**. Using the standard file selection window, navigate to the removable storage device or network share and select an audit package.

   Audit folders are named using a `hostname\date_time` pattern.

3. Redline will import the data and immediately begin analyzing it and calculating MRI scores.

Continue with *Investigating*.

3.2.2. Opening a MIR Resource in Redline

If you have used MIR to perform an audit, you can investigate the audit results using Redline:

1. In the MIR Console select the **Hosts** library. Open the Host you wish to investigate using Redline. On the right, select the acquired Audit that was generated by the Job you created in *Using a MIR Appliance*.

   OR

   Select the **Jobs** library. Open the Job you created in *Using a MIR Appliance*. On the right, view the **Results** tab and select a Result Set. On the **Audits** tab below the list of Result Sets, select the Audit corresponding to the Host you wish to investigate.

2. Having selected a Redline-compatible Audit, choose **Tools** → **Open With [audit name]** → **Redline**, or right-click and choose **Open With** → **Redline**.

   The Console will query MIR for the Audit files, writing them to a temporary directory on the local machine, and then open Redline. Redline will immediately import the MIR Audit and begin an analysis.

Continue with *Investigating*.

3.2.3. Importing a Saved Memory File

Redline can perform a limited analysis of a "dd"-format memory image file, and will assist you in examining in-memory artifacts.

The time required for doing a memory file import and analysis ranges from minutes to many hours. The two most significant factors are:

- The size of the captured memory image relative to the available memory on the Redline workstation.
- The OS captured in the image.

When importing a memory image, the machine you are using must have sufficient available free memory to load the entire memory image.

To import third-party memory images

1. Copy the image to the Redline workstation. (Do not perform the analysis over a network share; it will take a very long time to complete.)
2. In Redline, select **Analyze a Saved Memory File**.
3. Configure Memoryze, as described in *Configuring Collection Options*.
4. Click **Browse** and, using the standard file selection window, navigate to and select the saved memory image.
5. Redline will import the data and immediately begin an analysis.

   Note that memory image options are limited due to incomplete data capture (file system information is unavailable). See *Configuring Collection Options* for details.

Continue with *Investigating*.

3.3. Investigating

Capturing and importing data are the easiest tasks in any investigation. The real work comes after Redline has performed an analysis and reports the results: manual triage and investigation of suspicious components.

In the following sections, we describe the Malware Risk Index (MRI), the sequence of investigatory steps promoted by Redline, and how to adjust Redline findings to reflect your own analysis of the target system. We also describe the use of IOCs and Acquisitions.

3.3.1. The Malware Risk Index

In its MRI analysis, Redline considers a number of factors that commonly indicate a system is compromised. For example, in the default configuration it is assumed that **svchost** is never legitimately started from the command line; if it was, it registers as a significant MRI hit and the process will be “Redlined”.

Some factors are judged on probability: it is **unlikely** that a named memory section imported into many processes is malware, whereas it is more likely that a named memory section imported into only one process is malware. Thus, the more imports of a named section, the lower the effect on the MRI score of its associated process.

When calculating an MRI score, the default Redline settings tend to create false-positive hits: better to flag an innocent process than to allow a malicious one to slip past. Thus a red badge or high MRI score is a **suggestion** for further investigation.

While performing your analysis you will probably see patterns in Redline’s false-positive hits. These patterns can be used to customize the MRI rules, to reduce the number of false-positives and increase your productivity. Likewise, any false-negative discoveries can be incorporated into the rules, so that future calculations correctly identify the compromise.

The ability to modify the rules comes into significant play when faced with triaging a large number of systems. By performing analysis of a few systems and refining the MRI rules to eliminate false-positive hits, subsequent system analysis will require less work. See *Redline Options* for details.

3.3.2. Typical Investigation Steps

Near the top left of the **Investigation Window**, Redline displays a sequence of six steps. Following this sequence will allow you to perform an efficient analysis of the suspect system. The steps are:

- Review Processes by MRI Scores
- Review Network Ports/Connections
- Review Memory Sections/DLLs
- Review Untrusted Handles
- Review Hooks
- Review Drivers and Devices

A more detailed description of these steps follows:

Review Processes by MRI Scores

The Malware Risk Index of a process helps you prioritize your malware investigation. The higher the MRI score, the more likely Redline has identified a potential compromise. Those processes that are "Redlined" should be manually inspected to determine the reasons Redline scored it as a threat and how to best mitigate that threat.

By default only processes that appear to be a significant risk are listed in the Information pane. Click **Display/Hide** to display options for showing **Redlined Processes** and **All Processes**.

Review Network Ports/Connections

Malware often communicates through network ports, either listening for commands or making outbound connections to exfiltrate data. You should check these lists for unusual or unexpected port connections.

By default, all ports are listed. Click **Display/Hide** to display options for showing **All Ports**, **Listening Ports**, only, or **Established Ports** with outbound connections.

Review Memory Sections/DLLs

Memory section analysis is useful because malware memory sections are atypical. Malware DLLs are more likely to be unsigned and used in only one process. In contrast, legitimate DLLs provide functionality that is typically used by many processes and system DLLs are usually signed. When looking for malware, examining those memory sections which are unsigned and used by few processes is often very productive.

When using MD5 whitelisting, **Include Whitelisted Items** and **Hide Whitelisted Items** toggle the listing of items with a checkmark in the **MD5** column. Entries lacking a checkmark are not in the whitelist.

By default, only unsigned/untrusted memory sections and DLLs with low reference counts are listed. Click **Display/Hide** to display options for showing fewer or greater

items: **Least Frequency of Occurrence (Untrusted Only)**, **Least Frequency of Occurrence**, **Named Sections Only**, **Injected Memory Sections**, and **All Memory Sections**.

Review Untrusted Handles

Handles are used by the operating system to refer to internal objects like files, registry keys, pipes, and other resources. Malware investigation should first focus on handles held by processes that are not trusted, or that are used by very few processes. As with reviewing memory sections and DLLs, experience is required to fully leverage the handles review.

By default only those handles that are **not** in use by at least four trusted processes are displayed. Click **Display/Hide** to display options for showing **Untrusted Handles Only** or **All Handles**.

Review Hooks

Hooks are subroutines injected into the usual system function mechanisms, allowing a third party to monitor and modify data as it moves from source to destination. Redline recognizes several forms of potentially malicious hooking.

By default, only untrusted hooks are displayed. Please be aware that determining the trustworthiness of a hook is difficult to automate: **do not rely on the default view solely**. It is important to manually inspect the other hook categories for signs of malware behaviour.

Click **Display/Hide** to display options for showing **Untrusted Hooks**, **IDT Hooks** (Interrupt Descriptor Table), **SSDT Hooks** (System Service Descriptor Table), **IRP Hooks** (Interrupt Request Packet), and **All Hooks**.

Review Drivers and Devices

Malware authors sometimes use device driver layering to intercept the data they seek, placing a keylogger, file logger, or other data-stealing routine on top of the system device driver. However, many device driver layers are legitimate routines providing common filtering tasks.

When using MD5 whitelisting, **Include Whitelisted Items** and **Hide Whitelisted Items** toggle the listing of items with a checkmark in the **MD5** column. Entries lacking a checkmark are not in the whitelist.

In this last investigative step of Redline analysis, you will need to perform a manual check for signs of malware. It is highly recommended you check the following drivers at a minimum:

`\FileSystem\Ntfs` : The “System Restore” driver is often layered on *\Ntfs*; other drivers may indicate the presence of malware.

`\Driver\Kbdclass` : Keylogging malware will often layer on *\Kbdclass*.

3.3.3. Adjusting and Customizing MRI Rules

The default Redline rules will return a number of false positive factors, because it is worse to miss a compromise than to flag an innocuous process. As you work through an investigation, you can quickly correct these errors. You can even tune the rule set for better performance on systems with known-safe false positive factors (certain drivers, system extensions, etc.)

While viewing a **Malware Risk Index Report** the factors that influenced Redline's calculations are listed with summary descriptions. To the left of each identified factor is a **Thumbs Up** or **Thumbs Down** button which will "flip" the factor and cause an immediate recalculation of all processes' MRI scores.

An MRI score can also be modified by adding a manually-entered hit (comments do not affect the score, hits do). When your hit is saved, MRI scores are recalculated. When adding a hit against an item that is used by multiple processes, the MRI score for those processes may also be affected by the change.

To effect a change in scoring for all investigations, you can modify the rule set directly using the **Redline Options** rules editor. When you save the changes, Redline re-imports and re-scores its findings for the current investigation, and subsequent analyses — including those previously saved — will be calculated using your new settings.

Re-building the rule set for an investigation can take some time, so we recommend "bundling" the changes for a single rules-editing session. Best practice is to investigate a few representative systems while keeping note of patterns of false positive scoring, make your rule changes in bulk, and then re-investigate those systems and any remaining systems.

3.3.4. To Correct False Hits and Factors

When viewing *Malware Risk Index Hits* on the Information Pane

1. Click **Thumbs Up** to the right of the mistaken hit. This changes the hit from a "suspicious sign" to "false positive", removing its influence in calculating an MRI. The thumbs up icon becomes a **Thumbs Down**.
2. Identifying a "false positive" hit results in re-analysis of the audit data. MRI scores are recalculated to reflect the change in status for the corrected hit.
3. The hit description is not removed from the list. If you change your mind, the hit can be restored by clicking **Thumbs Down**, changing it back to the original **Thumbs Up**. MRI scores will be immediately recalculated.

When viewing the *Negative Factors* list

1. Click **Thumbs Up** to the right of the mis-identified factor. This changes its status to "User Trusted" and moves it to the **Positive Factors** list.

   MRI scores are immediately re-calculated for all processes to reflect this change in trust.
2. The item can be returned to its original "untrusted" status by clicking its **Cancel**. The item will be returned to the **Negative Factors** list and MRI scores will be immediately recalculated.

When viewing the *Positive Factors* list

1. Click **Thumbs Down** to the right of the mis-identified factor. This changes its status to "User Untrusted" and moves it to the **Negative Factors** list. All MRI scores are immediately re-calculated

2. The item can be returned to its original "trusted" status by clicking its **Cancel**. The item will be returned to the **Positive Factors** list and MRI scores will be immediately recalculated for all processes.

When viewing the *Ignored Factors* list

- Ignored factors can not be adjusted.

  You can configure ignored factors in **R** → **Redline Options** → **General** → **Named Section Analysis** → **Ignored Sections**.

When viewing the *All Factors* list

- As described for **Negative Factors** and **Positive Factors**, above, click **Thumbs Up** or **Thumbs Down** to trust or distrust a mis-identified factor; or click **Cancel** to restore an item's original trust status.

3.4. Indicators of Compromise

Indicators of Compromise (IOCs) are forensic artifacts of an intrusion that can be identified on a host or network. They comprise a logically grouped set of descriptive terms (each called an "Indicator Term") about a specific threat.

The indicator terms that MANDIANT currently provides for IOCs detail over 500 different types of evidence that can be gathered in an enterprise. Combined with a flexible, nested logical structure, IOCs have far more functionality than standard static signature based technologies.

A simple IOC might simply look for the signature of specific compromise artifacts. These can be the traditional forensic objects such as MD5 checksums, compile times, file size, name, path locations, registry keys, and so on. More complex IOCs include advanced forensic techniques, such as memory forensics, looking for data that are much harder for attackers to change, or artifacts that attackers are more likely to recycle, such as running process components (including process handle names), the imports and exports used by an executable, and more.

These can be combined in different logically-grouped combinations and, as you learn more about the intrusion, further refined to more effectively eliminate false positives and reduce false negatives.
Potentially, the most powerful IOCs describe an attacker's methodology. Indicators attempting to detect methodology do not focus on a specific pieces of forensic evidence directly tied to malware or compromise. Instead, they focus on the common methods that attackers use. Methodology indicators don't necessarily show a specific instance of a compromise, but they will show the result of tactics repeated by a group of adversaries. As such, they are the hardest to write, but when done well they capture evidence of behaviors that are performed only by intruders as opposed to legitimate users

Ultimately, the best IOCs have these properties:

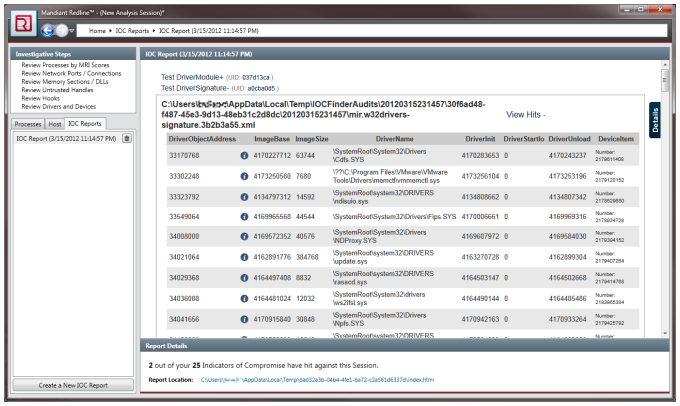
- The IOC identifies only attacker activity.

- The IOC is inexpensive to evaluate — it is typically simple and evaluates information that is less expensive to collect or calculate.

- The IOC is expensive for the attacker to evade. In other words, to evade the IOC the attacker has to drastically change tactics, tools, or approach.

Finally, IOCs are meant to be shared. They are plain text files, which makes them easy to modify and send to others. In the interest of maximizing the value of IOCs in the computer forensics community, MANDIANT provides free tools, schemas, example IOCs, and a stock of standard IOCs identifying the most common compromises or intrusions. More can be learned at *http://www.openioc.org*.

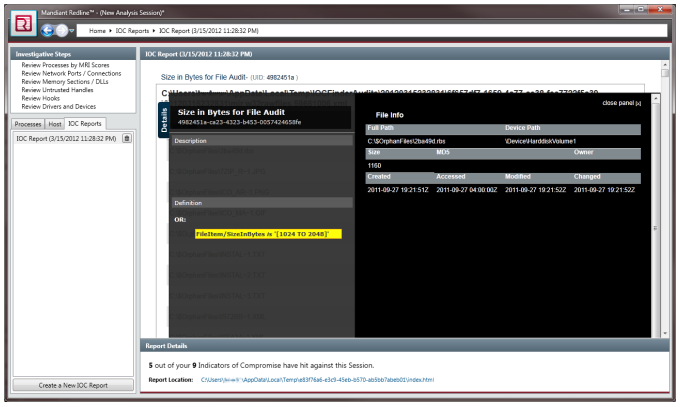
3.4.1. Viewing IOC Reports



IOC Reports are accessed through the **IOC Reports** tab in the left navigation pane. Click **IOC Report** to view the list of IOCs that were discovered on the target system.

For any IOC, selecting the name of the IOC displays a list of audit files that contained hits against the IOC. Clicking the **UID** after the name reveals details of the IOC.

In the list of audit files hit by an IOC, clicking **View Hits +** lists the items that were identified as hits. Selecting the **i**nformation button displays full details of the hit — and, in particular, highlights the IOC terms that were matched by the hit.



At the bottom of the Investigation window, **Report Details** provides a description of how many IOC hits were found, and paths to the report and the IOCs.

3.4.2. Creating New IOC Reports

You may run additional IOCs against the current audit session by selecting the **IOC Reports** tab and choosing **Create a New IOC Report**. The familiar **Start Your Analysis Session** wizard will take you through the process. We recommend using the Comprehensive collector, enabling you to run all IOCs and perform deep analysis of the compromised host.

3.5. Acquisitions

In the course of assessing a potential compromise you may need to perform forensic analysis of drivers and processes. Provided you have a memory image, you can use Redline to extract driver and process images for an in-depth analysis in another tool.

When configuring a Collector (*Section 2.3.2, "Configuring Collection Options"*) you have the option to **Acquire Memory Image**. MANDIANT Memoryze and other memory acquisition tools can also acquire an live memory image, for use with the **From a Saved Memory File** data analysis; consult the documentation for these tools for specific instructions.

To safeguard against accidental compromise of the Redline workstation and accidental triggering of anti-virus software, acquisitions are first staged to the session staging location before being archived in a password-protected ZIP file in the session acquisition location. The default locations are configurable in *Redline Options* and may be configured separately for each session in the **R** → **Session Information** window.

The staging area is a temporary holding area for the acquired files. It should be a directory that is **excluded** from malware detection suites, to avoid accidental deactivation. When the acquisition has been archived, the raw files are deleted to prevent accidental activation.

To view acquired files, select the **Host** tab in the quick select pane on the left, then choose **Acquisition History**. Acquisitions will be listed to the right. At the bottom, the path to the **Acquisition Folder** may be clicked to open the folder; a pencil icon provides a shortcut to **Session Information**, allowing you to change the path.



If the memory image does not match the analyzed audit data, the acquisition may fail or cause unexpected results.

This can happen if, in the time between auditing the system and acquiring its memory image, changes happened to the process or driver you are now attempting to collect. You can work around this problem by creating a new analysis session from the memory image for the express purpose of retrieving process or driver images, while continuing to use the audit data for Redline analysis.

3.5.1. Acquiring a Process

While viewing **Named Memory Sections** in the Information Pane:

- Select **Acquire Process Address Space**. Alternatively, right-click a process name and select **Acquire Process Address Space**

A notification window will be displayed at the bottom of the screen, alerting you that an acquisition is taking place in the background. You may continue working while the acquisition is being performed.

Processes that can not be found in the memory image are treated as a warning condition. These warnings will be written to `issues.*.xml` files in the **Default Unsafe Acquisition Staging Location**.

3.5.2. Acquiring a Driver

While viewing drivers in the Information Pane:

- Right-click the driver name and select **Acquire Driver**.

A notification window will be displayed at the bottom of the screen, alerting you that an acquisition is taking place in the background. You may continue working while the acquisition is being performed.

Note that this functionality requires enabling **Acquire Memory Image** when configuring a Collector (*Section 2.3.2, "Configuring Collection Options"*).

Drivers that can not be found in the memory image are treated as a warning condition. These warnings will be written to `issues.*.xml` files in the **Default Unsafe Acquisition Staging Location**.

3.5.3. Finding Previous Acquisitions

After acquiring processes or drivers:

1. Select the **Host** tab in the quick select pane on the left.
2. Select **Acquisition History**.
3. Acquired files are displayed to the right. Select the file path for the process or driver you wish to inspect. Windows File Explorer will be opened to the directory containing the (zipped, password-protected) acquisition file for that process.
4. Accompanying the acquisition is a plain-text "Readme" file containing the password for the zipfile. At the time of writing, the password is "Safe" (note the capital S).

The acquisition file contains DLLs, memory sections, logs, and results files.

3.5.4. Managing Multiple Sessions

Redline allows you to save an analysis session at any time, to be resumed at a later date. When you re-open the session, MRI scores are re-calculated only if the settings in Redline Options have been changed; thus, opening a saved analysis is generally faster than starting a new analysis.

When re-visiting a saved analysis session, it can be helpful to review **R** → **Session Information** or **Host** tab → **Acquisition History**. These commands provide information about the session configuration and file paths.

Analysis sessions are saved automatically as changes are made. The save file is a database comprising all session information, imported audit data, and analysis calculations.

Opening an Analysis Session

To load a previously-saved analysis session:

1. Select **R** → **Open a Saved Analysis**.
2. Using the standard Windows file selector, select the appropriate `.mans` file. Click **Open**.

   If the Redline Options settings in the saved analysis session match those currently configured in Redline, the analysis will not need to recalculate MRI scores and will open quickly.

   If there have been changes to Redline Options, new MRI scores will be calculated. This will take a little longer, but is significantly faster than importing and analyzing the original memory image.

Opening a Recent Session

Recent analysis sessions are listed in the **R** menu. Select one to open it.



Changes to MRI and Whitelist options will cause re-calculation of scores and returned data when a session is re-opened.



Appendix A
Installation

Redline is installed, uninstalled, and upgraded using the standard Windows wizard. *MANDIANT Support* for Redline is also available.

A.1. System Requirements

Redline requires Microsoft .NET 4, which is available for Windows 7, Windows 7 SP1, Windows Server 2003 SP2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2008 R2 SP1, Windows Vista SP1, Windows XP SP3.

If .NET 4 is not installed, the Redline installer will point a browser at Microsoft's .NET installation page.

Redline Collectors support 32–bit versions of Windows 7, Windows, 2003 SP2, Windows 2000 SP4, Microsoft Vista, and Windows XP SP2; and 64–bit versions of Windows 7, Windows 2008 R2, and Microsoft Windows 2003 SP2.

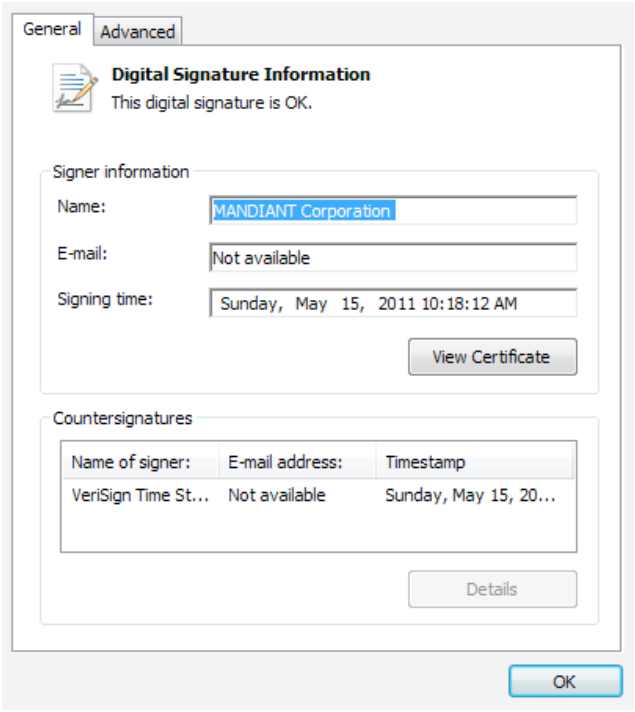
A.2. Installing Redline

A clean environment is required for installation. Typically, this is a workstation known to be secure and free from malware, in an area of the network that precludes it from any exposure to the suspect environment. Often, this workstation is completely disconnected from the network.

If you suspect the Redline workstation is infected, find a clean environment and run Redline from there. **NEVER** attempt to heal a system using a local Redline installation and analysis. Local collection and analysis must be used only for training.

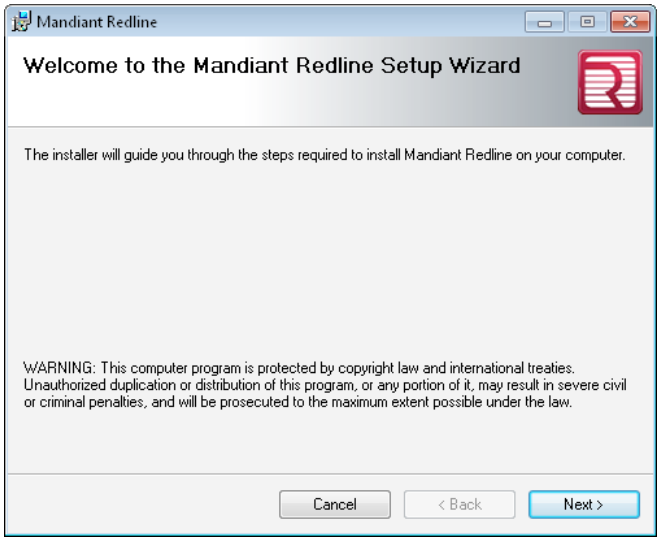
On a clean workstation, free of compromise and disconnected from any source of compromise:

1. Download MANDIANT Redline from *http://www.mandiant.com/resources/download/redline*.
2. Verify the installer image to ensure that you are installing a legitimate edition of Redline:
   a. Right-click the installer, `Redline.msi`, and select **Properties**.
   b. Then select the the **Digital Signatures** tab.
   c. There should be one signature in the list: `MANDIANT Corp`. Select it and click **Details**.
   d. Confirm that Windows reports `This digital signature is OK.` and that VeriSign provided the countersignature. Neither party will have an email address.



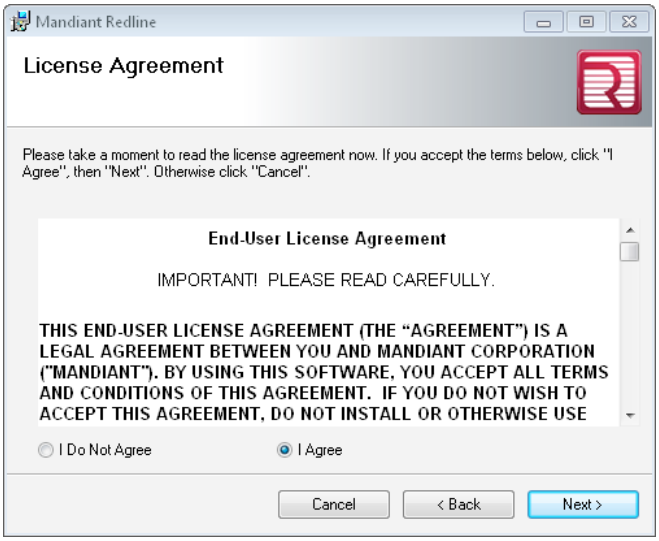
3. Start the installation wizard by locating and double-clicking `Redline.msi`. You may be presented with the standard **Do you want to run this file?** confirmation dialog: click **Run** to confirm that you wish to install Redline.

4. In the **Welcome to the MANDIANT Redline Setup Wizard** window, click **Next**.



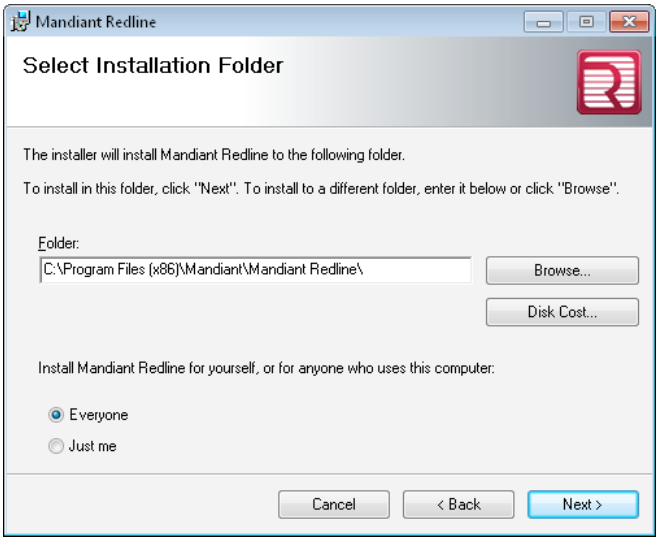
5. In the **License Agreement** window, read the End-User License Agreement carefully.

   If you agree and wish to continue installing Redline, select **I Agree** and then click **Next**.



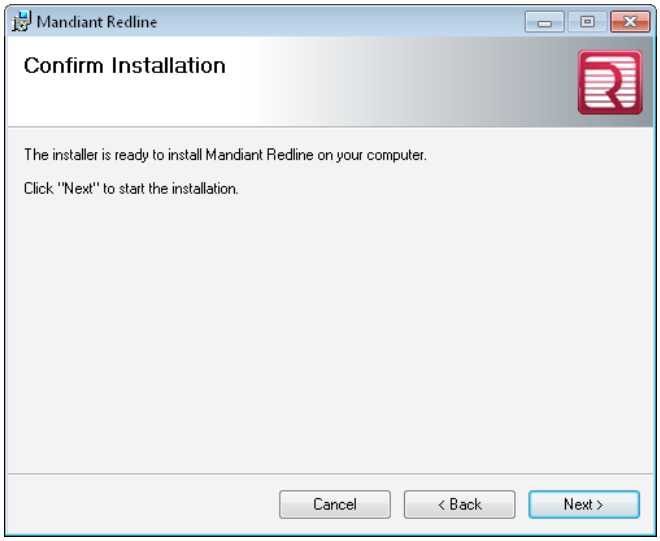
6. In the **Select Installation Folder** window, you may choose a different installation folder and who may use the application; by default, Redline is installed to `C:\Program Files \Mandiant\Mandiant Redline\` for **Everyone** to use.

   Users of MIR Console should note that it expects Redline to be installed at the default location. If you choose a different path, you will need to help MIR Console find Redline.

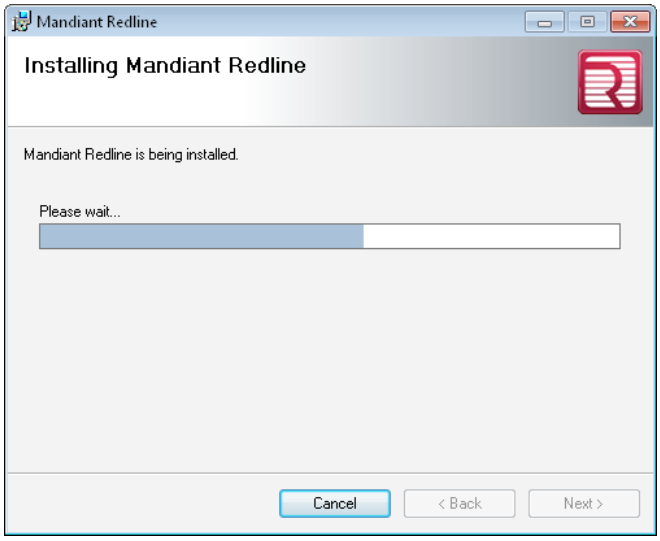


7. In the **Confirm Installation** window, click **Next** to start the installation.

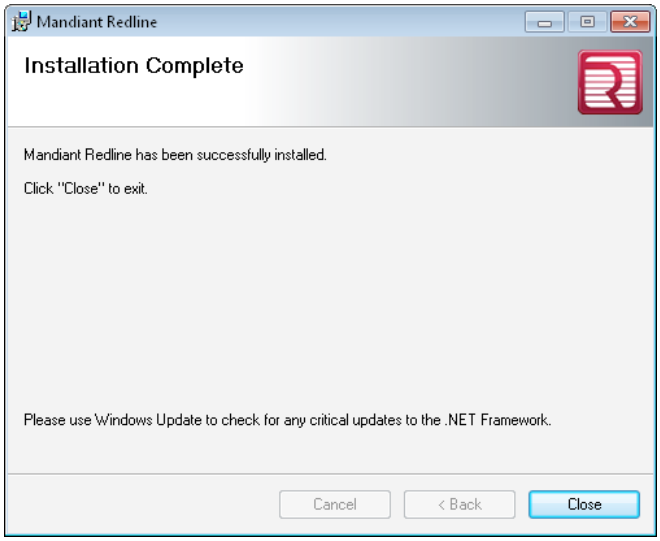
   Windows **User Account Control** may ask you to click **Continue** to allow the installer to proceed.



8. An **Installing MANDIANT Redline** window displays a progress bar while installing the software. Installation should take only a few seconds.



9. When the **Installation Complete** window is displayed, click **Close** to complete the installation process.



MANDIANT Redline is now installed on your system. You can start Redline by opening **Start** → **All Programs** → **MANDIANT** → **Redline** → **MANDIANT Redline**.

A.3. Removing Redline

Redline is easily removed using the standard Windows **Uninstall or change a program** control panel:

1. Open the Windows control panel by selecting **Start** → **Control Panel > Programs** → **Programs and Features** → **Uninstall or change a program** (Vista, Windows 7) or **Start** →**Control Panel** → **Add or Remove Programs** (others).
2. Select **MANDIANT Redline**, then click **Uninstall**. You will be asked to confirm your choice. Click **Yes** and Redline will be removed from the system.

A.4. Upgrading Redline

Redline can be upgraded in-place: simply follow the instructions in *Installing Redline*. Your settings, file history, and preferences will be retained.

A.5. MANDIANT Support

Many MANDIANT users find our community forums to be a valuable resource. Please join us at *https://forums.mandiant.com*.

To help yourself get the best possible support, please consider providing the following information in your forum requests:

- Your Redline version number (from **Help** → **About**).
- If using **From an Intelligent Response Export**, the Agent version number noted in the Host resource in MIR Console.

- A detailed description of the problem, including any screenshots, error messages, or issues documents; and a list of steps and conditions that produce the problem.

For information, updates, and support for the IOC standard, visit *http://openioc.org/*.

For information, updates, and support for using Whitelists, visit *https://forums.mandiant.com/forum/redline*.



Appendix B Incident Response and Investigation Best Practices

Performing an effective live response requires a streamlined live response protocol that spans all the involved departments of an organization. At a minimum the protocol should consider the following guiding principles:

- Automate the collection of a standard data set.
- Minimize reaction time.
- Minimize interaction with the suspect computer.
- Minimize changes to the suspect computer.

MANDIANT consultants have extensive experience performing live response. With this experience comes an understanding of what is normally more important to consider when creating a live response protocol. These can be divided into five topic areas, which we use to help us meet the goals of live response:

- Overall process.
- Data Collection.
- Data Handling.
- Data Analysis.
- Reporting.

B.1. Overall Process

The process used to perform investigative steps should be considered carefully and scrutinized for flaws. The results of a live response could contribute to administrative actions, legal proceedings, or may affect the business or people's lives. Creating a sound process will help ensure findings are accurate, complete, and defensible.

Some amount of co-ordination has to occur for a live response process to be streamlined and effective. For example, if the initial information about the suspect computer is just an IP address, the responders will likely need to determine the hostname and a physical location. The responders must have proper access to the Host to be able to run a live response, and they must have a place to store the data that is collected.

Outline each step of the process, then explore, document, and test them. Some areas that should be considered:

- Define the goal and deliverables of the live response process.
- Define organizational roles and responsibilities.
- Design the process to be repeatable, with an eye to automation.
- Design the process to be clear and easy to follow.
- Consider all operating systems, not just Microsoft Windows.
- Test the tools used in the process.
- Document the process.

- Train all parties involved.

B.2. Data Collection

Changes to a suspect computer are unavoidable when responding to an incident. Understanding and minimizing those changes is important. MANDIANT consultants perform data collection in a manner that minimizes interaction with and modification of the suspect computer. This includes considerations such as:

- Treating the suspect computer as "hot" — do not interact with it unless you have a plan.
- Considering everything you connect to the suspect computer as lost to the attacker.

  For example, MANDIANT consultants do not keep IOCs, documents, reports, or anything else on the thumb drive from which the live response will be run, nor do they connect general network shares to the suspect computer.
- Automate the collection process, perhaps eliminating the requirement to log on to the suspect computer.
- Do not copy or save data to the suspect computer unless there is no other option. Use removable media, a network share (which must be considered compromised), or other remote media options.
- Do not perform any analysis on the suspect computer. Do not "poke around" or "check one thing" on a suspect computer.
- Focus on system data (file listings, logs, etceteras), not user data.

Data collection is a balancing act between collecting too much and too little. MANDIANT consultants tend to lean on the side of collecting excess data in cases where we know little about the situation. There are a number of reasons for this, not the least of which is that our first collection may be our last. Experience has demonstrated to us that in more cases than not, having more data leads to a better outcome. Thus, we tend to collect both volatile (eg. a list of network connections) and critical non-volatile data (eg. event logs).

Finally, consider also the time it takes to collect data and the details of the situation. In cases where time is the most critical component you will want to modify the data collection routine to speed things up; when time is not an issue, you might want to collect more data.

B.3. Data Handling

When MANDIANT consultants collect data, they always consider that data to be evidence. We perform a standard "bag and tag" process that includes creating an evidence tag and initiating a chain of custody. The evidence tag describes the data we collected and the chain of custody documents where it has been.

We recommend maintaining positive control over evidence at all times. Keep the data on encrypted file systems and under lock and key when not in a consultant's direct possession. Perform analysis on working copies, not the original, to prevent accidental alteration or loss. At MANDIANT we lock original copies in a safe or other approved container.

B.4. Data Analysis

The purpose of a live response is to collect and review data that will help an incident responder make a determination, and perhaps evaluate the extent, of a computer security compromise. However, a live response is not a comprehensive forensic analysis: a live response may reveal no evidence of a compromise when, in fact, one exists.

In the context of MANDIANT Redline, MRI scoring assists consultants in identifying compromised systems and prioritizing their response. Dependent on the number of systems being examined, consultants may take a two-pass approach: a quick scan of all systems, followed by a deep scan (including strings and IOCs) of the prioritized systems.

MANDIANT consultants are careful with the creation of IOCs, frequently testing and tweaking them with the goal of making them generic enough to hit on slight variations of the compromise, but at the same time specific enough to reduce false positives. In the context of a single computer the tolerance for false positives is higher, so in those cases we tend to make IOCs that are more generic to increase our odds of finding evil.

B.5. Reporting

MANDIANT consultants create a report of every live response analysis they perform, regardless of findings. We generally create the report as we are performing the analysis, while the details are fresh in our minds. We use a standard template that presents the analysis results in several sections:

Background
How and why the Host was suspect (the initial lead information).

Major Findings
Presented in a list, each with a concise finding sentence followed by one or two sentences of supporting information. We always list the source and earliest evidence of the date the Host was compromised.

Evidence Examined
A list of evidence that was examined.

Timeline of Events
Presented as a table that includes the date, time, and event.

Details
For each analysis performed, details of the analysis and its associated findings.

From a style perspective, we document our findings using active voice, in past tense, and in a factual manner. We always present times in UTC and fully write-out dates in month, day, and four-digit year (eg. January 1, 2011). We also clearly identify our interpretation of facts and the presentation of our opinion.

B.6. Final Words

MANDIANT consultants have performed thousands of live responses over more than ten years, and we wrote this document to convey some of the lessons we have learned. We hope that this information helps you perform your own successful live responses.

Find evil and solve crime!

Licenses

Redline links to the following libraries:

SQLite ADO.NET Provider Version 1.0.77 Public Domain. No license.

Exception Reporter Version 2.1.1 LGPL *http://exceptionreporter.codeplex.com/license*

Log4Net Version 1.2.11 Apache License 2.0 *http://logging.apache.org/log4net/license.html*

Ookii Dialogs Version 1.0.0 *http://www.ookii.org/software/dialogs/*

WPF Shell Integration Library Version v2 MICROSOFT PUBLIC LICENSE (Ms-PL) *http://archive.msdn.microsoft.com/WPFShell/Project/License.aspx*

Index

Symbols

'R' Menu
- About, 7
- Analyze Collected Data, 5
- Analyze this Computer, 6
- Background Tasks, 7
- Exit Redline, 7
- Help, 7
- New by Analyzing a Saved Memory File, 6
- Open a Saved Analysis, 6
- Recent Analysis Sessions, 7
- Redline Options, 7
- Session Information, 6

A

Acquisition
- of Drivers, 34
- of Processes, 33
- Viewing with Windows File Explorer, 34

B

Best Practices, 42

C

Collection
- Creating a Collector, 23
- Local Collection for Training, 25
- Memory Images, 25
- Memoryze, 25
- Third-Party Tools, 25
- Using MIR Appliance, 23
- Using the Collector, 23

Collector
- Collecting Data, 23
- Comprehensive, 9
- Creating, 23
- Importing Data, 25
- IOCs, 9
- Show Advanced Parameters, 10
- Standard, 9

Customer Support, 40

G

Getting Started
- By Analyzing a Saved Memory File, 5
- From a Collector, 5
- Open a Previous Analysis, 5

I

Importing Data
- Memory Images, 26
- Using a Collector, 25
- Using MIR, 26

Indicators of Compromise
- see IOCs, 31

Installing Redline, 36

Investigative Steps, 12, 28

IOCs
- Creating New Reports, 33
- Design of, 31
- Not Collected Search Terms, 8
- Supported Search Terms, 8
- Unsupported Search Terms, 8
- Updating, 41
- Viewing Reports, 32
- Warnings and Errors, 8

M

Malware Risk Index, 27
- Configuration
  - Expected Arguments, Users, and Paths, 20
  - General, 19
  - Suspicious Handles, 21
  - Suspicious Imports, 20
- Correcting False Hits, 30
- Customization, 29
- Report
  - Hit Details, 14
  - Named Memory Sections, 15
  - Process Details, 14
  - Search Function, 16

Memory Image
- Importing Data, 26

MIR
- Collection, 23
- Creating Audit Job, 24
- Importing Data, 26

N

Navigation, 12

O

Options
- Default File Locations, 16
- Default Script Options, 17
- Expected Arguments, Users, and Paths, 20
- MRI General Configuration, 19
- Suspicious Handles, 21

Suspicious Imports, 20
Whitelist Management, 18

Q

Quick Select
Host, 13
IOC Reports, 13
Processes, 13

R

Redline
Installing, 36
Removing, 40
Upgrading, 40

S

Sessions
Saving and Resuming Sessions, 34
System Requirements, 36

U

UI
Analyzing Data, 11
Collecting Data, 7
Getting Started, 4
Information Pane, 13
Investigation Window, 11
Investigative Steps, 12
Malware Risk Index Report, 14
Navigation, 12
Options Window, 16
Overview, 4
Quick Select, 13
'R'edline Menu, 5
Uninstalling Redline, 40
Upgrading, 40

W

Whitelists
Updating, 41