
MANDIANT Best Practices

MANDIANT IOC Finder

Copyright © 2011 Mandiant, Inc.

MANDIANT IOC Finder is a free tool that facilitates incident response and investigation of computer security compromises. IOCs are *Indicators of Compromise* — if the data from the Host contains data that matches an IOC, the evidence is in support of the machine having been compromised.

Investigators use MANDIANT IOC Finder to collect a standard set of data from a Host and to generate reports that list, most importantly, matches between collected data and IOCs. This report generates leads for further investigation and a final determination of the Host's status.

MANDIANT Professional Services Consultants use MANDIANT IOC Finder in cases where the number of Hosts is low or when the use of scalable technology is not feasible. When our consultants use MANDIANT IOC Finder they follow a well-defined set of best practices. This document shares these best practices with the hope that you'll consider using them as well.

1. Incident Response and Investigation Best Practices

MANDIANT consultants frequently respond to suspect computers with the intent to collect volatile data for triage and making a determination of compromise. We call this process *live response*.

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.

1.1. 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.

1.2. 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.

1.3. 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.

1.4. 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 IOC Finder the primary analysis method is to search the collected data for indications of compromise. Most other tools use a similar approach: given information or patterns of data, search for them. As with any search it is only as effective as the tool and search parameters.

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.

1.5. 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.

2. 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!