

MAC-ROBBER INSTALLATION & USE

Taken From the MAC-ROBBER Documentation (Brian Carrier)

Introduction

mac-robber is a Forensics & Incident Response tool used to collect the Modified, Access, and Change (MAC) times from allocated files. It recursively reads MAC times of files and directories and prints them in 'time machine' format to STDOUT. This format is the same that the mactime tool from The Sleuth Kit and The Coroners Toolkit (TCT) read.

mac-robber is based on the grave-robber tool from The Coroners Toolkit (TCT) when using the '-m' flag, except it does not require Perl!

This program has several benefits over using grave-robber:

1. It does not require Perl and therefore a floppy or CD can be easily made with mac-robber compiled for several platforms. By default, the program is compiled to be statically linked.
2. It uses very basic C code so it should compile under any platform. If you encounter a platform that The Sleuth Kit does not support, then compile this on a trusted system, run it from a floppy on the compromised system and send the output to a server using netcat. Then, use mactime on the data from a system that The Sleuth Kit does support. This also works well on file systems that are not supported by specialized forensic tools.
3. C is faster than Perl for these type of operations!

Note that this tool will not show deleted files, unallocated files, or files that have been hidden by rootkits. To view information about those file types, the specialized tools from The Sleuth Kit must be used.

Installation

Type: ***make***

If you do not have gcc (the default compiler), use: ***make CC=cc***

If you are using the Sun cc Compiler, use: ***make sun***

If it gives errors regarding optimization or the static flag, you can use: ***make simple***

Usage

mac-robber takes a list of directories to analyze as arguments:

For example, to analyze the 'mnt' and 'mnt2' directories and send the output to a file:

```
# mac-robber mnt mnt2 > data/body.mac
```

If you want to analyze the system from the root directory and send the data to a server running netcat, use:

MAC-ROBBER INSTALLATION & USE

Taken From the MAC-ROBBER Documentation (Brian Carrier)

```
# mac-robber / | nc 10.0.0.1 8000
```

The server would be running something like:

```
# nc -l -p 8000 > body.mac
```

To analyze the data, the mactime tool from The Sleuth Kit is required. Use the -b flag to import the body file:

```
# mactime -b body.mac 01/01/2001 > timeline.01-01-2001
```

This file uses the readdir function and therefore will update the Access time on directories. Therefore, if you are going to make an image of the disks, do that first. Also, malicious kernel modules could produce incorrect data when run on a compromised host. Make sure that you do not write the output of this program to a drive on the compromised system, it may overwrite unallocated data.