



Chapter 0x8: Dynamic Analysis

 Note:

This book is a work in progress.

You are encouraged to directly comment on these pages ...suggesting edits, corrections, and/or additional content!

To comment, simply highlight any content, then click the  icon which appears (to the right on the document's border).

In the previous chapters, we discussed methods of static analysis ...methods that involve leveraging (static) analysis tools to gain insight into, and understanding of, malicious files and binaries. By definition, such analysis involves examining said items statically, without actually running or executing them.

Oftentimes however, it may be more efficient to simply execute a malicious file in order to (passively) observe its behavior and actions. This is especially true when malware authors have implemented mechanisms designed specifically to complicate or even thwart static analysis ...such as encrypting embedded strings and/or configuration information. `OSX.Windtail` [1] provides an illustrative example; the addresses of its command and control servers (generally something a malware analyst would seek to uncover) are base64-encoded and AES encrypted:

```
01 r14 = [NSString stringWithFormat:@"%@", [self
02 yoop:@"F5Ur0CCFMO/fWHjecxEqGLy/xq5gE98ZviUSLrtFPmGyV7vZdBX2PYYAIfmUcgXHjNZe3ibndAJ
03 Ah1fA69AHwjVjD0L+Oy/rbhmw9RF/OLs="]];
04
05 rbx = [[NSMutableURLRequest alloc] init];
06 [rbx setURL:[NSURL URLWithString:r14]];
07
08 [[[NSString alloc] initWithData:[NSURLConnection sendSynchronousRequest:rbx
09 returningResponse:0x0 error:0x0] encoding:0x4] isEqualToString:@"1"]
```

*encrypted command and control server address
(OSX.WindTail)*

Now, it is possible to manually decode and decrypt the `"F5Ur0CCFMO/fWHjecxE...9RF/OLs="` string (as the encryption key is hard-coded within the malware). However, it is far easier to simply execute the malware and, via a dynamic analysis tool (such as a network monitor), passively ascertain the addresses of the server(s) when the malware attempts to establish a connection.

In this chapter, we will dive into methods of dynamic analysis as a means to passively observe and thus understand Mac malware specimens.

We'll initially focus on:

- Process monitoring
- File monitoring
- Network monitoring

Following discussions of these monitoring tools and techniques, we'll look at more advanced dynamic analysis techniques, such as debugging malicious binaries.

Dynamic Analysis

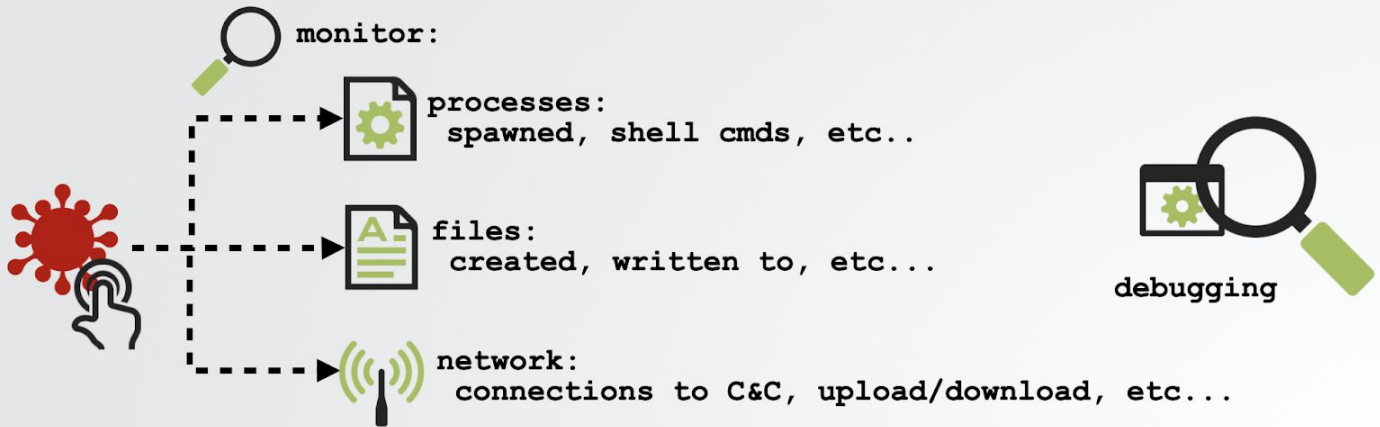
definition

perform analysis in a virtual machine
...or dedicated analysis machine!



Dynamic Analysis:

examination of a sample while running (executing) it.
...relies on monitoring tools, usually culminating with a debugger.



dynamic analysis

Note:

In this section of the book, we discuss methods of dynamic analysis which involve executing the malware (to observe its actions). As such, **always** perform such analysis in a compartmented virtual machine or better yet, on a dedicated malware analysis machine.

...in other words, don't perform dynamic analysis on your main (base) system!

For a detailed "how to" on setting up a virtual machine for (macOS) malware analysis, see:

["How to Reverse Malware on macOS Without Getting Infected"](#) [2]

References

1. "Middle East Cyber-Espionage: Analyzing WindShift's implant: OSX.WindTail"
https://objective-see.com/blog/blog_0x3B.html
2. "How to Reverse Malware on macOS Without Getting Infected"
<https://www.sentinelone.com/blog/how-to-reverse-macos-malware-part-one/>