



(The Art of Mac Malware) Volume 1: Analysis

Part 0x1: (Mac) Malware Basics

 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).

Content made possible by our [Friends of Objective-See](#):



[Airo](#)



[SmugMug](#)



[Guardian Firewall](#)



[SecureMac](#)



[iVerify](#)



[Halo Privacy](#)

To begin, let's discuss various foundational topics of (Mac) malware, as it is important to have such foundations before diving into more advanced topics.

In this introductory section, we'll cover Mac malwares':

■ **Infection Vectors:**

The means by which malware gains access (i.e. infects) a system.

Though social engineering methods are currently the norm, other more creative and stealthy methods of infection systems are gaining popularity.

■ **Methods of Persistence:**

The means by which malware ensures it will be automatically (re)executed by the operating system, on system startup or user login.

Though a handful of methods are regularly (ab)used, there are a myriad of surreptitious means by which malware can gain persistence.

■ **Capabilities:**

The payload of the malware (i.e. its goals).

Malware created by cyber-criminals is generally interested in financial gains, whereas cyber-espionage (state-sponsored) malware seeks to spy on users.