medium.com

The road to Reverse Engineering Malware – secjuice™ – Medium

Pablo Ramos

9-11 minutes

Malware Reverse Engineering Resources are scattered through the Internet and it can became a challenging task for someone just starting in it. Tutorials, courses and books are easy to find after a few Google searches but how to structure that it's a different thing.

If you're willing to invest some time and start dissecting malware for fun, profit, learning or work you might need some resources to guide through it. Here you'll find some of those resources including books, tutorials, workshops , online courses and places where you can pic up some samples to practice the knowledge you'll be learning.

Malware Analysis and Reverse Engineering involves a lot of different topics from Operative Systems, Programming, Cryptography, Networking and many more. Most of the

concepts you'll face while learning how to take these binaries apart will also become valuable in other security topics including offensive and defensive.

Malware Analysis Books

There are bunch of books on Malware Analysis and over the last couple of years, the number of available options have increased a lot. A quick search on Amazon might show some of the available options that you can start with, and you 'll have also a lot of options for learning Assembly, Network Detection and many other tools used for this.

If you're looking for some specific recommendations here is my list:

- Practical Malware Analysis: It a step by step guide with a hands-on approach to learn about the most common techniques applied by analyst to dissect malware. It comes with plenty of exercises and light reading that will lead you to a lot of content. You'll learn the tools and how to apply them to your work. It will cover mostly Windows malware, it's a really good place to start if you have no experience or want to refresh some of the knowledge.
- Malware Analyst's Cookbook: This books comes with a lot of recipes for you to apply when dealing with malware or other sort of files that you need to go through. It not only covers the techniques for analysis, forensics and covering your actions while investigating malware but it will also guide you to

classification and detection with **Yara** or developing your own signatures for ClamAV.

- Windows Malware Analysis Essentials: With a hands-on approach and a lot of details about analysis techniques this book will give you a deep understanding of malware analysis and it'w caveats. It's the latest of the three books and it has a really updated lists of techniques and tools.

  In my opinion these three books will give a good base for starting on Malware Analysis and they're part of a must in any Analyst's Library. There are plenty more involving other platforms as this list is mostly oriented to Windows Malware and x86.

  With mobile devices and IoT being at the center of the scene, ARM, Android and other technologies will also be topics you'll need to cover. But that's for a different post.

Online Resources: Courses, Videos, Workshops and Blogs

Internet if full or resources where to learn about different topics, and with an enormous amount regarding ***Information Security*** and specifically ***Malware Analysis***. As I don't tend to write another Malware Analysis training (I did that when I was at ESET), I'll share a list of really valuable content and some of the resources that I believe have actionable and specific content for you to go through.

In my opinion for a resource to be really helpful it should include lectures, reading, source code or samples and practice, lot's of practice. One of the most important thing you'll need to achieve for Reversing Malware it's actually reversing a lot of samples and also your own code while you're ramping up.

Open Security Training

From the many resources available I always point peers and people to one of the most useful sites I've found about a lot of security topics: Open Security Training. The content on this site covers a wide and detailed list of resources for any Security Enthusiast from x86, Cryptography, Network Detection, ARM, Malware Analysis, Exploiting to Cellular Networks and even more.

Courses are at least one day long, and slides, samples and videos are available for you to go through at you own pace. Some of the courses that I recommend for anyone Interested in Malware Analysis include:

Beginner classes

- Intro to x86—http://opensecuritytraining.info/IntroX86.html
- Intro to x86–6—http://opensecuritytraining.info/IntroX86-64.html
- Life of Binaries—http://opensecuritytraining.info

/LifeOfBinaries.html

- Malware Dynamic Analysis—http://opensecuritytraining.info/MalwareDynamicAnalysis.html

Intermediate Classes

- Introduction to Software Exploits—http://opensecuritytraining.info/Exploits1.html
- Intermediate Intel x86: Architecture, Assembly, Applications, & Alliteration—http://opensecuritytraining.info/IntermediateX86.html

Advanced Classes

- Introduction to Reverse Engineering Software: http://opensecuritytraining.info/IntroductionToReverseEngineering.html
- Reverse Engineering Malware—http://opensecuritytraining.info/ReverseEngineeringMalware.html
- Rootkits: What they are, and how to find them—http://opensecuritytraining.info/Rootkits.html
- The Adventures of a Keystroke: An in-depth look into keyloggers on Windows—http://opensecuritytraining.info/Keylogging.html

Workshops and

While looking at some more content in the Web you'll cross with different Workshops that contains a really hands on approach and will guide you to specific topics. Some of these topics are covered in books, and some are not. This is not a fully extended list but will give you some examples about where to start:

- **Malware Unicorn Workshops RE101 and RE102:**. From 0 to Reverse Engineering Crypto Algorithms used by common malware samples. The first workshop presents a good workflow that it's helpful during any malware analysis task. The RE102 it's a good hands on tutorial and step by step guide to dissect a malware and walk through some of the most common "Anti-" techniques used by malware writers
- https://github.com/RPISEC/Malware: Materials developed by RPISEC. It includes Lectures, Labs and Projects. As a Textbook it references 'Practical Malware Analysis', it also contains a list of further places where to continue to pick up more samples or challenges.

Tools and resources for practice

You won't have to reinvent the wheel for every single technique you learn and with time you'll be able to come up with your own set of favourite tools for any given task. The number of tools out there for you to try it's expanding every

day. A few resources might help you to keep on track with up to date information and where to find challenges to apply all the knowledge you've collected. Here you'll find a few I normally use.

Tools and repo's

- REMnux—https://remnux.org/: REMnux is a Linux distro that comes pre packaged with a bunch of really useful tools for all the types of Malware Analysis you might dive into. I would say it's a must for any Analyst dealing with malware, it will help you to known a wider range of tools in a controlled environment. It's part of my personal lab.
- Awesome Malware Analysis: Following the awesome trend in Github this provides a curated lists of resources, samples, tools, blogs and a bunch of topics. From Threat Intelligence, Detection and Classification and Honeypots up to tools for helping Analyst towards Web traffic anonymizers.

Finding Malware Samples and CTF like challanges

There will be a time where you'll need to find more samples or challenges to keep learning about specific topics or learn to deep dive into some real world malware. Finding curated lists of malware samples for you to analyse it's not that hard. Here's is a list for places where you can look for live malware to analyse or where to find other RE challenges:

- The Zoo (https://github.com/ytisf/theZoo): This Github repo contains a curated list of LIVE malware samples, some of them including source codes. It's intended for analyst fo have a place where to pull out examples for study and learning about RE Malware.
- Flare-On Challenge: Folks from FireEye are annually putting together a CTF like competition where you'll have to go over different levels. These include JavaScript, Windows, Linux and Android binaries for you to pull out the flags.
- Join ESET: Antivirus companies might tend to have CrackMes for you to play around and apply to different positions. Even while being part of the company I use to play around with our CrackMes (I still do) to play around with new techniques and keeping up with trends.

Conclusion?

There is no end of path to Malware Analysis or Reverse Engineering as new technologies and techniques are coming out every day. It is possible and useful to come up with a common ground of knowledge that will help you to walk through this maze.

Continuous practice and learning are ways to keep up to date and be aware of any new piece of malware that might end up in front of you. In Reverse Engineering Practice is key, and having a good list of resources and tools for practice it's the best way to start.

Happy hunting!