Reverse Engineering Resources for 2019

Some RE resources for beginners

malware analysis infosec thoughts

As the New Year has arrived, I wanted to take this time, not to outline my resolutions or goals, but to write the post I wish I had when I got into reverse engineering/ malware analysis. Beware, there are numerous more resources than what is listed here, these are just resources I like and recommend.

Books

Practical Malware Analysis by Andrew Honig and Michael Sikorski

This was my first book on the subject and is a great primer to understanding malware characteristics.

Practical Reverse Engineering: X86, X64, Arm, Windows Kernel, Reversing Tools, and Obfuscation by Bruce Dang

More of a reference book and I have learned alot from this book, but it can be difficult to read.

Reversing: Secrets of Reverse Engineering by Eldad Eilam

This book was enjoyable to read and really covers the basics well.

Reverse Engineering for Beginners by Dennis Yurichev

It’s free and packed full of knowledge.

Tutorials

Malware Unicorn's RE101 course is amazing and introduces you to the tools of the trade quickly. Her entire website is a wealth of information and look up her talks on youtube as well!

Malware Unicorn's RE102 is just as good as the first and really ramps up into some interesting malware tactics.

OpenSecurityTraining.info is like the Khan Academy of Computer Science/ Security.

Lenas Reversing for Newbies is a great introduction to RE.

Flare-On by Fireeye is a CTF they host every year and has write-ups to every solution along with the binary. Plus they provide the flare-vm as well. Amazing training!

Azeria Arm Labs are ARM based RE exercises. ARM is a totally new beast to me and I haven't went through all of these, but it is great from what I have seen.

Virtual Machines

Flare-vm requires a Windows VM to install on top of but this suite will give you every tool you could need to work with Windows-based malware.

Windows Trial VMs are here. Pick your VM software and snapshot it after import, but before powering on. Then Snapshot it again once all the tools are on. Go to the original when your trial is over and can not be renewed.

OA Labs VM is similar to Flare but has less tools and is built for their youtube tutorials. They recommended a Win7 32 bit I believe.

Remnux is an Ubuntu-based toolkit for reverse-engineering. Almost all the tools are command-line based and can handle most jobs. Additionally, the documentation is great and provides starting points for what tools to use and when. And it's free!

Samples

CAPE Sandbox is a open sandbox that allows you to download what is submitted.

The Zoo is a github repo of some popular malware and good stuff to get your feet wet with. Most of the PEs here have write-ups, so you can check your work.

Malpedia houses samples, report links, and yara rules for a ton of malware. My favorite, but you do need to be vetted before joining this site.

0xffff0800 Library is a TOR hosted site (you can just add .to to the end of the URL) with a ton of great samples, mostly from APTs. True hero for hosting this!

Youtube Channels

OA-Labs has great tutorials and knowledge packed videos. Speaking about packers, if you are dealing with one, these guys probably have a video on how to get around it.

Malware Analysis For Hedgehogs is a another great resource, especially the PE videos.

Live Overflow does a great job explaining concepts and showing how to apply those concepts to reversing.

Happy Reversing!

Josh Stepp

Related

ICS Primer

My attempt to give an executive view of the ICS environment

ICS infosec thoughts

Malicious Document Crash Course Part 2: Macros, APTs and OLE!

Dumping and Understanding Macros from an APT OLE2 Document

tutorial infosec malware analysis

Malicious Document Crash Course Part 1: Microsoft Office Documents and Macros

A triaging method for dealing with Microsoft Documents with macros

tutorial infosec malware analysis