The Cyber Intelligence Analyst's Cookbook

Volume 1: A primer for Open Source Intelligence Collection and Applied Research

Open Source Researchers
THE OPEN SOURCE RESEARCH SOCIETY

This book is dedicated to my loving wife, children, and household spirits. My pursuit of knowledge has put them through a lot over the years and continues to do so. I'd also like to dedicate this book to the leaders I've worked closely with over the past few years. Without their support I would not have come this far. I'd also like to thank all the analysts that I've met over the years. Their passion and support for this industry is truly inspiring. Lastly, I'd like to attribute part of this dedication to all the professors, who over the years, have taken the time out of their day to deal with my inquisitiveness.

Table of Contents

Preface

This book. Well, it started out as a manual, or rather a brain dump of my process. I've spent the last year or so examining how I collect Open Source Intelligence (OSINT) and tag it. Pretty simple right? Not so much. What I found over that year was that I continually added new tags to the artifacts, or I was creating new tags because they didn't exist within the database I use for storing this information. I use the Malware Information Sharing Platform (MISP) exclusively for my work. MISP is open, expandable, and can be queried by other apps using several different methods. Most of all, it's free.

Anyways, I started with this brain dump of my process for recording OSINT. The work initially started out just for me. I haven't documented any of my methods, thoughts, what have you in quite some time. I was due for this knowledge transfer. However, as I began writing, I found that a manual wasn't going to cut it. The next thing I know, I'm writing a book, and thirty days-ish later, the first draft was completed. Truthfully, it's an awful book, and I apologize to anyone who attempts to read it. Yet, as I look back over the body of knowledge, I see that I've at least created a good foundation for future volumes. Opportunities for expansion and clarification. Who knows, maybe someone will find what's in this book useful.

The book itself is explicitly written for cyber intelligence analysts. Still, anyone who performs intelligence as a discipline can deconstruct what's here and apply it to any intelligence domain. I'm also assuming the reader, at a minimum, has access to the Internet and can look up the tools used within the book. I've tried my best to add references to the right level of detail and completeness. I do believe in citing sources. Well, I've been beaten into always citing sources through my academic career as a student. So, what exactly is in this book? Part 1 of this book goes over the way I collect and store OSINT into MISP. Part 2 goes over some higher-order analysis that can be applied to the data.

I've placed the book under the GNU Free Documentation License. I've learned a lot from the open community and feel that this particular contribution belongs to the community. Those who take part in the open community, per se, made me. I've had to put a lot of work into myself to get to this point of knowledge in my own life, but I would not have gotten to this point if others hadn't laid the foundation before me. I'm sure folks will argue with the premises and processes I've laid out in this book, and that's totally cool with me. Hell, the one thing I know from my current Ph.D. program at university is to be prepared for the beating. This book is in no way a stone tablet or bible that must be adhered to as gospel truth.

Open Source Researchers