REVERSING DATA STRUCTURES AND ALGORITHMS IN MALWARE

JASON REAVES

Reversing Data Structures and Algorithms in Malware

Jason Reaves

This book is for sale at http://leanpub.com/reversingdatastructuresandalgorithmsinmalware

This version was published on 2020-05-13

Contents

Introduction

There are many obstacles you encounter when doing malware analysis, from unpacking your first sample, mapping out your first routine or breaking into that malwares data encoding routine. One obstacle in particular I've seen give people problems more than others is being able to follow malware as it parses data, data that is sometimes seemingly random hex but instead used for configuration purposes that can depict how malware acts. One experience that seems to help people when reverse engineering these structures and the algorithms that process them is a past in low level development such as assembly or C programming, however this isn't a luxury that everyone can come to malware analysis with such a background. As such I give you this book which is my humble attempt to walk the reader through my process of making sense of it all. From my experience there is a focus when it comes to reversing a packer/crypter that will involve algorithmic reverse engineering, as a construct when it comes to pulling out config data from a bot it will involve a data structure reverse engineering focus and finally C2 will commonly involve doing both.

Most malware comes with some sort of onboard configuration which could be as simple as a command and control server address. Not thinking of the data as strings but more in terms of pure binary data you can start to understand the data in whatever form the developer has chosen to store is ultimately just used by the bot to fulfill the tasks it needs to. Normally the easiest way to find this data is to first understand what it is you are dealing with, ex: if it's ransomware and we want to find some of the data the bot will have on board then a list of file extensions or language flags is a good place to start the bot will have to use certain methods to get this information from the infected host and we can use these bottlenecks to find the locations in the bot where the data has already been decoded and is now being parsed. Once you find the data it's usually a matter of backtracking, I usually use IDA and a debugger to accomplish this task and it can take quite a bit of time and experience to get good at it.

Other common methods I've used is setting breakpoints on suspicious functions such as those performing loops and bitwise instructions or breaking on suspicious data sections in the sample that could be storing information. When people write a bot they usually end up writing a template or stub with a builder in the same manner you would write a crypter or packer and so the configuration data in the bot must either static or be placed in a way that allows the bot to find it such as with a special marker or header this way the builder can update the stub properly and the bot can then make use of the data when it is executed.

Luckily this same system of identifying structures and routines is the same basic principles we will use for reversing protocols by studying the data and determining how the code deobfuscates, packs and organizes this data. Because in the same manner that I mentioned that regardless of how obfuscated a bots configuration data is it must eventually know where to find it this same principal holds true for C2 communications, if a bot wishes to communicate something back to its C2 then it must eventually be useable by the C2 to hold any meaning going forward.

Identifying Structure

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/reversingdatastructuresandalgorithmsinmalware.

Making sense of Data

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/reversingdatastructuresandalgorithmsinmalware.

Locky Config

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/reversingdatastructuresandalgorithmsinmalware.

No Nothing Example

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/reversingdatastructuresandalgorithmsinmalware.

Approaches to reversing algorithms

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/reversingdatastructuresandalgorithmsinmalware.

Simple data searching – Locky config

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/reversingdatastructuresandalgorithmsinmalware.

Decode the data - Locky config cont

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/reversingdatastructuresandalgorithmsinmalware.

Data that shrinks or expands - Locky config cont

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/reversingdatastructuresandalgorithmsinmalware.

Customized Encryption – Shifu Custom RC4

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/reversingdatastructuresandalgorithmsinmalware.

Reversing Malware C2 Command Structure

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/reversingdatastructuresandalgorithmsinmalware.

Appendix A

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/reversingdatastructuresandalgorithmsinmalware.

Kovter Config Parser

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/reversingdatastructuresandalgorithmsinmalware.

Zeus Binstruct Parser

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/reversingdatastructuresandalgorithmsinmalware.

Visual encrypt

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/reversingdatastructuresandalgorithmsinmalware.

Zloader C2 Data Pull Script

This content is not available in the sample book. The book can be purchased on Leanpub at http://leanpub.com/reversingdatastructuresandalgorithmsinmalware.