Malware Analysis Report: "FritzFrog"

CAP6137 Malware Reverse Engineering: P0x04

Naman Arora
naman.arora@ufl.edu

April 27, 2021

Contents

1 Executive Summary

2 Static Analysis

2.1 Basic Identification

Attribute	Value
Bits	64
Endianess	Little
Operating System	
Class	
Subsystem	
Size	Bytes
Compiler Timestamp	
Compiler	
SHA256 Hash	

2.2 Malware Sample Family Identification

2.3 Binary Headers

2.4 A case against Packing

2.5 Interesting Imports

2.6 Interesting Code Constructs

3 Dynamic Analysis

3.1 Interesting Features

3.2 File System Interaction

3.3 Network Interaction

4 Indicators of Compromise

4.1 Host Based

4.2 *YARA* Rule

5 Appendix A: Screenshots