DynaSpy malicious library detection tool

Name

Institutional affiliation

Date of submission

**Introduction**

The DynaSpy Library Monitor is a simple tool that allows users to monitor the loading of shared libraries and detect if the loaded library has a malware or not in a system. It is designed to work on Unix-based operating system- MacOs. The tool is implemented as a C# console application that uses the .NET Core runtime. It uses the libdl dynamic library to load shared libraries, determine if they have been loaded or not and detect if they have malwares or not.

**Problem Statement**

Shared libraries play a crucial role in the whole software ecosystem on Unix-like platforms. These libraries are essential to applications because they facilitate shared functionality and cut down on redundant code. However, if shared libraries aren't properly maintained and managed, they can pose security issues. Accidentally utilizing a shared library can cause issues. This may occur, for instance, if a previously compatible application is upgraded to use a different, incompatible version of a shared library. In this instance, the application might not update to the new version and keep using the older one, which could leave it vulnerable to attacks.

Another problem is the loading of malicious shared libraries. Attackers may be able to trick an application into loading a malicious library by using various techniques, such as modifying the library search path or exploiting vulnerabilities in the application. To overcome these challenges in cyber security, it becomes indispensable to observe and track the loading of shared libraries on any given system. More importantly, we must place our trust in solely those libraries which are considered reliable.

**Solution**

The DynaSpy Library Monitor utility is an easy way to keep tabs on which shared libraries are being loaded into a computer. Users can enter the name of a shared library, and the program will check to see if it has been loaded. The program will also detect if the loaded file has malware or not. The program is written in C# and is a console app that runs on the.NET Core framework. To load shared libraries and check if they are loaded, it employs the libdl dynamic library. The program is meant to be straightforward and easy to operate. If a user wants to keep tabs on a particular shared library, all they have to do is enter the library's name into the tool, and it will do the rest. The instrument will alert the user when the library has been successfully loaded.

**Implementation**

The DynaSpy Library Monitor tool is implemented using the following components:

1. C# programming language

2. .NET Core runtime

3. libdl dynamic library

4. ClamAV.Net

The tool is implemented as a console application that accepts command-line arguments. It uses the NativeMethods class to load the libdl library and the dlopen function to load shared libraries. When the tool is launched, it accepts a command-line argument specifying the name of the shared library to monitor. It then creates an instance of the DynaSpy Library Monitor class and calls the CheckIfLoaded method to determine if the library has already been loaded. If the library has not been loaded, the tool enters a loop that periodically checks if the library has been loaded. If the library is loaded, the tool notifies the user and exits.

The DynaspyLibraryMonitor class is responsible for monitoring the loading of shared libraries. It uses the NativeMethods class to load the libdl library and the dlopen function to load shared libraries. The class exposes a Loaded event that is raised when the library is loaded.

**Testing**

To test the Shared Library Monitor application, we created several shared libraries using C++ and tested the application's ability to load them. The program requires the ‘ClamAV.Net’ NuGet package, which provides the ClamScan class used for malware detection. We then tested the application by entering "libtest.so" into the shared library name textbox and clicking the "Load" button. The application successfully loaded the shared library, and the status label on the form was updated to indicate that the shared library had been loaded and if the loaded file is malicious or not. We repeated this process with several other shared libraries, and in each case, the application was able to load the shared library successfully and detect malicious libraries.

**Conclusion**

The DynaSpy Library Monitor tool provides a simple solution for monitoring the loading of libraries will malicious defects in a system . It is designed to be easy to use and requires no special privileges or system configuration. By monitoring libraries, users can ensure that only trusted libraries are being loaded and that potential security risks are minimized.

The tool can be extended and customized to meet specific needs. For example, it could be integrated into an automated testing system to ensure that only compatible versions of shared libraries are being loaded. It could also be used to monitor the loading of libraries in a containerized environment, where it is important to ensure users get real time notifications of malicious loaded libraries.