

denandz / KeeFarce

Public

Notifications

Fork 134

Star 1k

<> Code

Issues 4

Pull requests

Actions

Projects

Wiki

Security

Insights

master

Go to file

<> Code

prebuilt

src


LICENSE

README.md

README

BSD-3-Clause license

KeeFarce



About

Extracts passwords from a KeePass 2.x database, directly from memory.

Readme

BSD-3-Clause license

Activity

1k stars

78 watching

134 forks

Report repository

Releases

No releases published

Packages

No packages published

Languages

C++ 59.5%

C# 35.0%

C 4.2%

Objective-C 1.3%

KeeFarce allows for the extraction of KeePass 2.x password database information from memory. The cleartext information, including usernames, passwords, notes and url's are dumped into a CSV file in %AppData%

General Design

KeeFarce uses DLL injection to execute code within the context of a running KeePass process. C# code execution is achieved by first injecting an architecture-appropriate bootstrap DLL. This spawns an instance of the dot net runtime within the appropriate app domain, subsequently executing KeeFarceDLL.dll (the main C# payload).

The KeeFarceDLL uses [CLRMD](#) to find the necessary object in the KeePass processes heap, locates the pointers to some required sub-objects (using offsets), and uses reflection to call an export method.

Prebuilt Packages

An appropriate build of KeeFarce needs to be used depending on the KeePass target's architecture (32 bit or 64 bit). Archives and their shasums can be found under the 'prebuilt' directory.

Executing

In order to execute on the target host, the following files need to be in the same folder:

- BootstrapDLL.dll
- KeeFarce.exe
- KeeFarceDLL.dll
- Microsoft.Diagnostic.Runtime.dll

Copy these files across to the target and execute KeeFarce.exe

Building

Open up the KeeFarce.sln with Visual Studio (note: dev was done on Visual Studio 2015) and hit 'build'. The results will be spat out into dist/\$architecture. You'll have to copy the KeeFarceDLL.dll files and Microsoft.Diagnostic.Runtime.dll files into the folder before executing, as these are architecture independent.

Compatibility

KeeFarce has been tested on:

- KeePass 2.28, 2.29 and 2.30 - running on Windows 8.1 - both 32 and 64 bit.

This should also work on older Windows machines (win 7 with a recent service pack). If you're targeting something other than the above, then testing in a lab environment before hand is recommended.

Acknowledgements

- [Sharp Needle](#) by Chad Zawistowski was used for the DLL injection tesh.
- Code by Alois Kraus was used to get the pointer to object C# voodoo working.

License

