Dropbox Client Research: Get Code, Emulate MiM Attack – to Protect Sensitive Data

¡Binary files of Dropbox Client discovered to be compiled and obfuscated Python files – not a big problem for Apriorit Research Department. Use legal Reverse Engineering when you need the 3rd-party application compatibility!

The Client Task

The Client and Apriorit teams were working on a DLP system. At the next stage, the solution had to protect sensitive data from being transferred to the public cloud, in particular, Dropbox.

Cloud storage is a great solution to have your data backed up, handy and shared at any moment. It becomes essential part of work and one of the aspects of business continuity – but at the same time, it is one more channel for the corporate data to "slip away", like email or chats. So a DLP solution must not prevent employees from using such popular cloud tool as Dropbox, while being able to protect data within it.

Such "flexible" 3rd-party solution compatibility can be a hard task, as we do not want to block application functioning, but to influence it in particular manner. All the processes, formats, and protocols are closed by publisher. What a DLP solution vendor can do in this situation? Fortunately, this is one of the cases when reverse engineering can be applied absolutely legally.

"Flexible" Dropbox compatibility in this project consisted in obtaining data for DLP analysis before it was actually transferred to the cloud, and then allow or block this transfer.

Dropbox cares about data transfer security and uses its own format and SSL certificates. So, the desired functionality supposed cutting in the data exchange process, in fact, man-in-the-middle (MiM) attack for Dropbox traffic.

Research Task

Apriorit Research and Reverse Engineering Group task was to research Dropbox data exchange, in particular, describe how the process was organized; restore the data exchange protocol; learn how to get necessary certificates.

Team separated this task in 2 stages:

- ✓ **(Pure research)** Research of Dropbox interaction with file system, and Dropbox application network traffic;
- ✓ **(Reverse Engineering)** Understand Dropbox client internals and data flow paths.

Working On

Dropbox application is developed in Python, and it is a combined PE file with ZIP archive (python stand-alone executable, py2exe). After extracting sources, Apriorit researchers could see the decompilation protection methods Dropbox developers had applied. Authors used changed PYC file formats and also changed byte codes (basic type code values).

In previous projects, Apriorit already resolved and automated the original Python code restoration from original PYC format, so the task was to research changes introduced by Dropbox developers.

Apriorit specialists reversed the modified Python engine Python27.dll and got new values of basic type codes. Using these new codes, researchers managed to restore the original data format and then investigate the Dropbox internals.

Results

Dropbox data exchange procedure was restored step-by-step. Provided prototype was able to successfully intercept, analyze and manage all necessary Dropbox file/folder and network operations. Task took 2 man-weeks to be completed.

Also researchers admitted frequent updates of the Dropbox application that could complicate the developed solution support. Apriorit specialists made up a plan of deeper file system interaction investigation to provide analysis of transferred files on the other level, if required for the next releases.

What's next?

Get the **free estimation** of time and effort for your research task! Unlike many R&D service providers, we understand the specifics of research projects and completely rely on the professional skills of our specialists. So it won't be just one phrase with the total sum and dead line.

Apriorit free research estimation pack includes:

- Basic task dropdown with the research approaches indicated;
- Each task-approach time & effort estimation supported by our broad research project experience;
- Prototype development estimation.

After we've received your request for proposal, usually it takes 2-7 business days to prepare the estimation for your task.

¡ So let's start solution search right now with a zero-risk estimation stage !

All we need to start is a brief research task description sent to the info@apriorit.com with "RFP" mentioned in the subject.