Kernel-level File System Filtering

¡Get IP and other SMB session parameters in kernel mode file system filter driver!

Project Task

The Apriorit Team was in charge with an advanced cyber security project. One of the system modules was a file system filter driver working in the kernel mode – to provide the most secure functioning and widest OS management capabilities.

The task was to improve file activity monitoring feature providing additional information about the user, who accessed a file in a network share; and also organize rule-based network share access. It would suppose filtering file system by IP address, and other SMB session parameters.

How to obtain such data in kernel mode and organize filtering? While there are techniques to implement this for user mode, kernel mode approaches were not documented or researched. The Client's team was not sure if kernel solution could exist at all, and was evaluating the option to return to the user mode driver.

It would cut some important advanced functionality, and so Apriorit Research and Reverse Engineering Department was called up. Preliminary researchers' answer was that some internal APIs would be required, and so it was about system file reverse engineering.

Research Work and Results

The object for reversing was srv.sys file; target OS – x86 Windows family.

Research task was successfully completed in 2 man-weeks using standard reverse engineering techniques. In Research Report, Apriorit specialist described internal Windows APIs to get necessary session parameters and manage file system access at kernel level.

The team implemented required filter driver functionality - providing the client's security application with the advanced file system management features.

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.