Introduction

The tLab system is a corporate local service for remote and secure analysis of suspicious objects. This system is designed to protect against new types of cyber threats against which typical antivirus software is ineffective: targeted attacks, zero-day malware, and user-targeted attacks.

tLab conducts autonomous analysis of program behavior and identification of malicious functionalities on the server (corporate cloud). The system allows for the automation of the behavior analysis procedure for any programs and detects signs of malicious functions within them.

Suspicious objects are launched in virtual containers, where continuous analysis of the behavior of all running programs is conducted.

A unique deep analysis technology of program functionality is used for reliable detection of malicious objects, including zero-day threats.

This technology has an innovative aspect, which involves a mechanism for recognizing specified malicious functionalities. It tracks the behavior history and correlates events of various processes in real time.

Edit this page