Researchers from Sophos reported a new cybercriminal tool that is able to disable the protection of even leading antivirus solutions, including Kaspersky, Sophos and Bitdefender.

The novelty is already actively used by multiple group groups to disconnect EDR (Endpoint Detection and Response) before launching the code.

The tool has become the evolution of the previously known Edrkillshifter, created by the Ransomhub group, but now it is more effective and universal. For disguise, the methods of obstacles, anti -analysis, and sometimes even signed drivers (stolen or compromised) are used.

In one case, the malicious code was introduced into the legitimate utility of the Clipboard Compare from Beyond Compare.

Most often, the modification is carried out after receiving access to the victim system, or through fake installers issued for the official ones.

SOPHOS recommends to include protection against unauthorized changes (Tamper Protection), control the administration rights and update the systems in a timely manner, because Microsoft began to withdraw signatures from outdated drivers.