Zebrocy (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-02 10:48:21 UTC

According to brandefense, Zebrocy is malware that falls into the Trojan category, which the threat actor group APT28/Sofacy has used since 2015. Zebrocy malware consists of 3 main components; Backdoor, Downloader, and Dropper. The Downloader and Dropper take responsibility for discovery processes and downloading the main malware on the systems. At the same time, Backdoor undertakes the duties such as persistence in the system, espionage, and data extraction.

This malware, which is not considered new, has variants in many languages from the past to the present. These include programming languages such as Delphi, C#, Visual C++, VB.net, and Golang. Furthermore, we know advanced threat actors and groups revise their malicious software among their toolkits at certain time intervals using different languages and technologies.

▶ [TLP:WHITE] win_zebrocy_auto (20251219 | Detects win.zebrocy.)
