Download the Zebrocy Malware Technical Analysis Report

brandefense.io/zebrocy-malware-technical-analysis-report/

April 10, 2022

Zebrocy is malware that falls into the Trojan category, which the threat actor group called 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 different languages from the past to the present. These include programming languages such as Delphi, C#, Visual C++, VB.net, and Golang. Furthermore, we know that advanced threat actors and groups revise their malicious software among their toolkits at certain time intervals using different languages and technologies.

It includes many social engineering techniques that direct its victims to open the attached files with a thematic fake mail trending at the point of distribution of malware.

The sectors targeted by the malware are as follows;

- Ministries of Energy and Industry
- Science and Engineering Centers
- Ministry of Foreign Affairs
- National Security and Intelligence Agencies
- Press Services
- Embassies and Consulates