[Research Summary]: Zebrocy Malware - Brandefense

Published: 2022-09-28 · Archived: 2026-04-05 19:03:14 UTC

> This blog post comes from the “Zebrocy Technical Analysis Report” by the Brandefense CTI Analyst Team. For more details about the analysis, download the report.

Execution Summary

In this report prepared by the Brandefense cyber intelligence team, we analyzed malware toolkits belonging to an advanced cyber threat group, Sofacy (other security providers have called it APT28, Fancy Bear, STRONTIUM, Pawn Storm, and Sednit). In the report, malicious software sets belonging to the Sofacy group were shared in more than one version.

You should not consider these anti–malware precautions unique to only Zebrocy and any other malware toolkit. The behavior of groups with a high threat profile, such as Sofacy, must be understood. The techniques we have described explain what they need to do if one becomes the target of a future offensive campaign.

We consider that the report’s attack methods and malware investigations should create cyber security awareness. In addition, TTP findings used by threat actors will contribute by feeding cybersecurity teams.

General Description & Motivation

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.

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

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

The threat group's focus is espionage activities aimed at critical and strategic points of states and organizations. These targets are located in countries in the Middle East, Europe, and North America.

Once the Zebrocy malware had infiltrated the target system, it first has initiated the discovery phase. Then, it starts some actions within the system within the framework of specific rules with metadata of the compromised system and a screenshot.

After the discovery phase, it transmits the files listed below to the command and control server to extract data.

Related file extensions:

- .doc, .docx
- .xls, .xlsx
- .ppt, .pptx
- .exe
- .zip, .rar

We could make a general definition: The Zebrocy malware serves as a target–oriented attack campaign and contains the functions necessary for espionage activities. Furthermore, it is thought that malware is in a structure that is updated periodically and is structured to increase its capabilities with the addition of new modules to the malware.

> This blog post comes from the "Zebrocy Malware Technical Analysis Report" by the Brandefense CTI Analyst Team. For more details about the analysis, download the report.

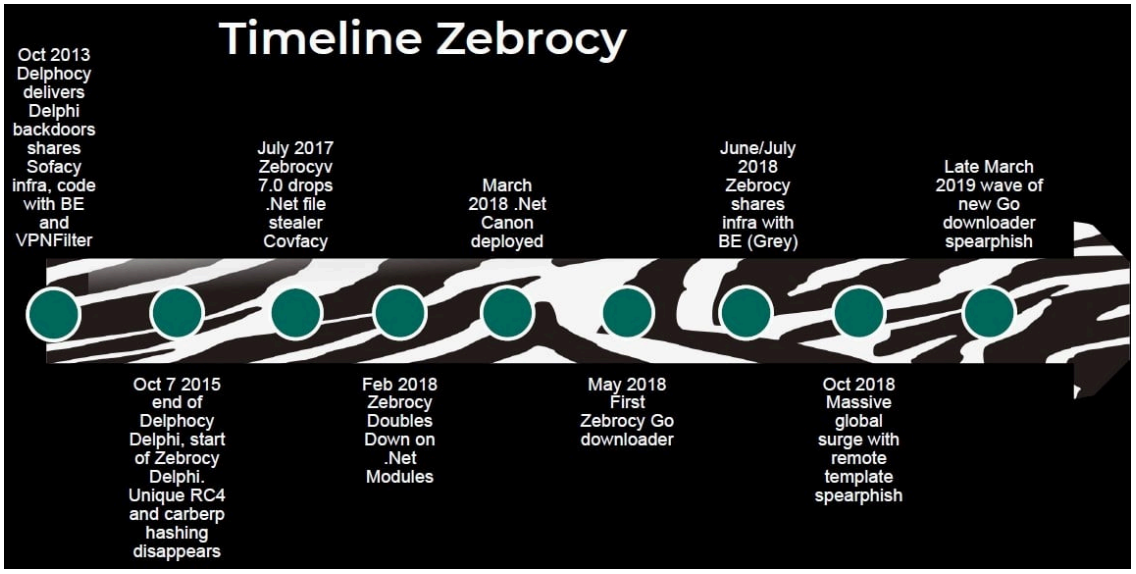

Figure 1: Zebrocy Variant Chart Published by Kaspersky Researchers

---

Source: https://brandefense.io/zebrocy-malware-technical-analysis-report/