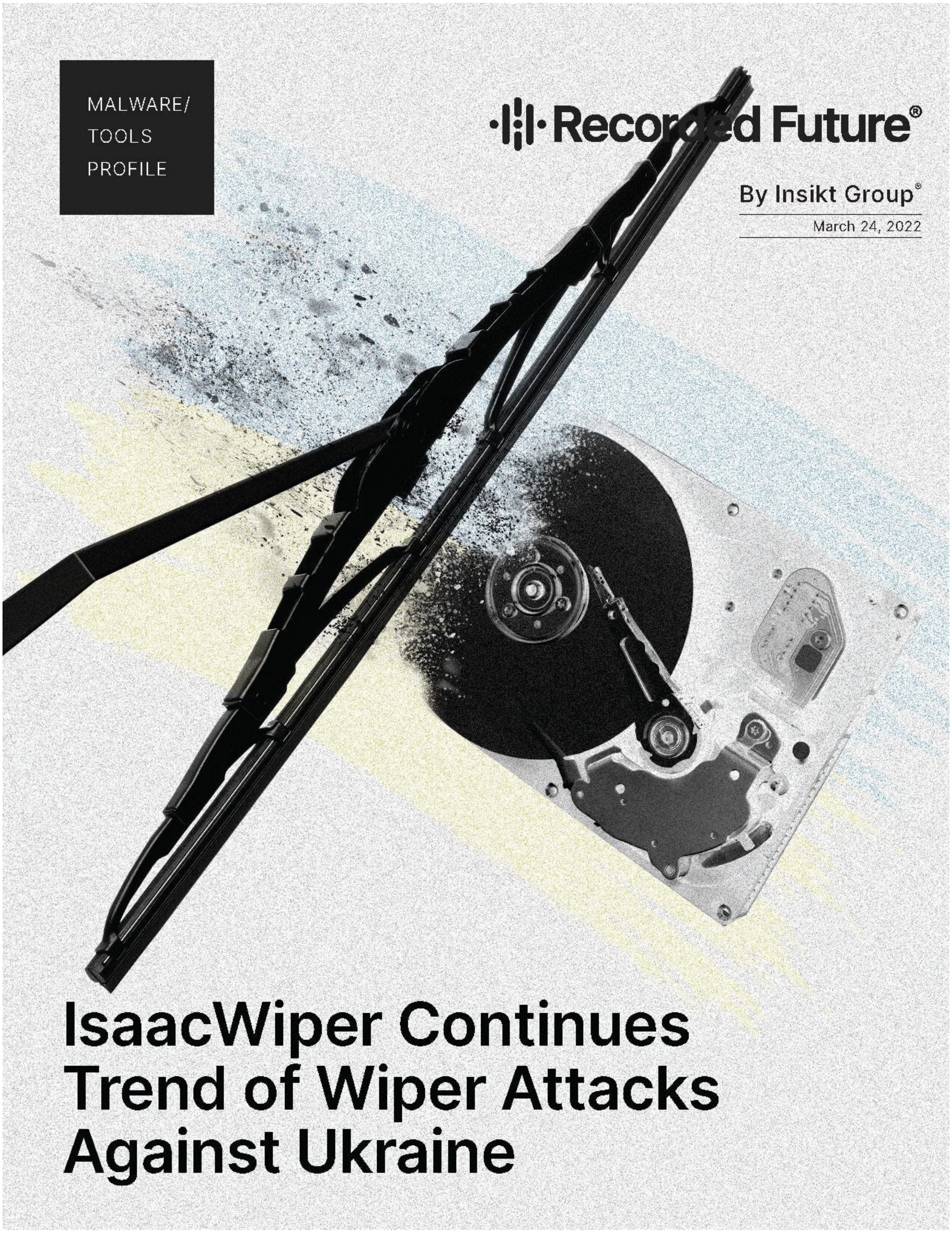
IsaacWiper Continues Trend of Wiper Attacks Against Ukraine

recordedfuture.com/isaacwiper-continues-trend-wiper-attacks-against-ukraine/



MALWARE/
TOOLS
PROFILE

Recorded Future®

By Insikt Group®

March 24, 2022

IsaacWiper Continues Trend of Wiper Attacks Against Ukraine

Insikt Group

***Editor's Note**: The following post is an excerpt of a full report. To read the entire analysis, click here to download the report as a PDF.*

This report is a technical overview of the IsaacWiper malware reported by ESET on March 1, 2022. The malware was primarily delivered to Ukrainian organizations coincident with the Russian invasion of Ukraine. It is intended for those looking for a high-level overview of the malware's tactics, techniques, and procedures (TTPs) and mitigations.

Executive Summary

Following recent wiper attacks against Ukrainian organizations involving the WhisperGate and HermeticWiper malware, a new destructive wiper, IsaacWiper, was observed on February 24, 2022. Although no direct attribution for IsaacWiper or the other wiper malware found targeting Ukraine has been made by researchers, the timing of these destructive attacks in conjunction with tensions and kinetic conflict in Ukraine suggests they are Russian in origin.

Key Judgments

- IsaacWiper is a destructive malware that overwrites all physical disks and logical volumes on a victim's machine.
- There is no code overlap between IsaacWiper, HermeticWiper, or WhisperGate. IsaacWiper achieves a similar outcome by different means.

Background

In a report released on March 1, 2022, ESET researchers identified a new destructive malware that had been affecting a Ukrainian government network since February 24, 2022. This malware, dubbed IsaacWiper, is distinct from the HermeticWiper malware previously reported. ESET stated that they observed IsaacWiper deployed at a Ukrainian organization that was not previously affected by HermeticWiper, although they are still assessing any links between IsaacWiper and HermeticWiper. Furthermore, they are unable to attribute this malware to any known threat actors due to a lack of significant code similarities with known malware. One day after IsaacWiper was initially deployed, the threat actors deployed a second version that included debug log output, indicating that the malware was not working as intended.

***Editor's Note**: This post is an excerpt of a full report. To read the entire analysis, click here to download the report as a PDF.*