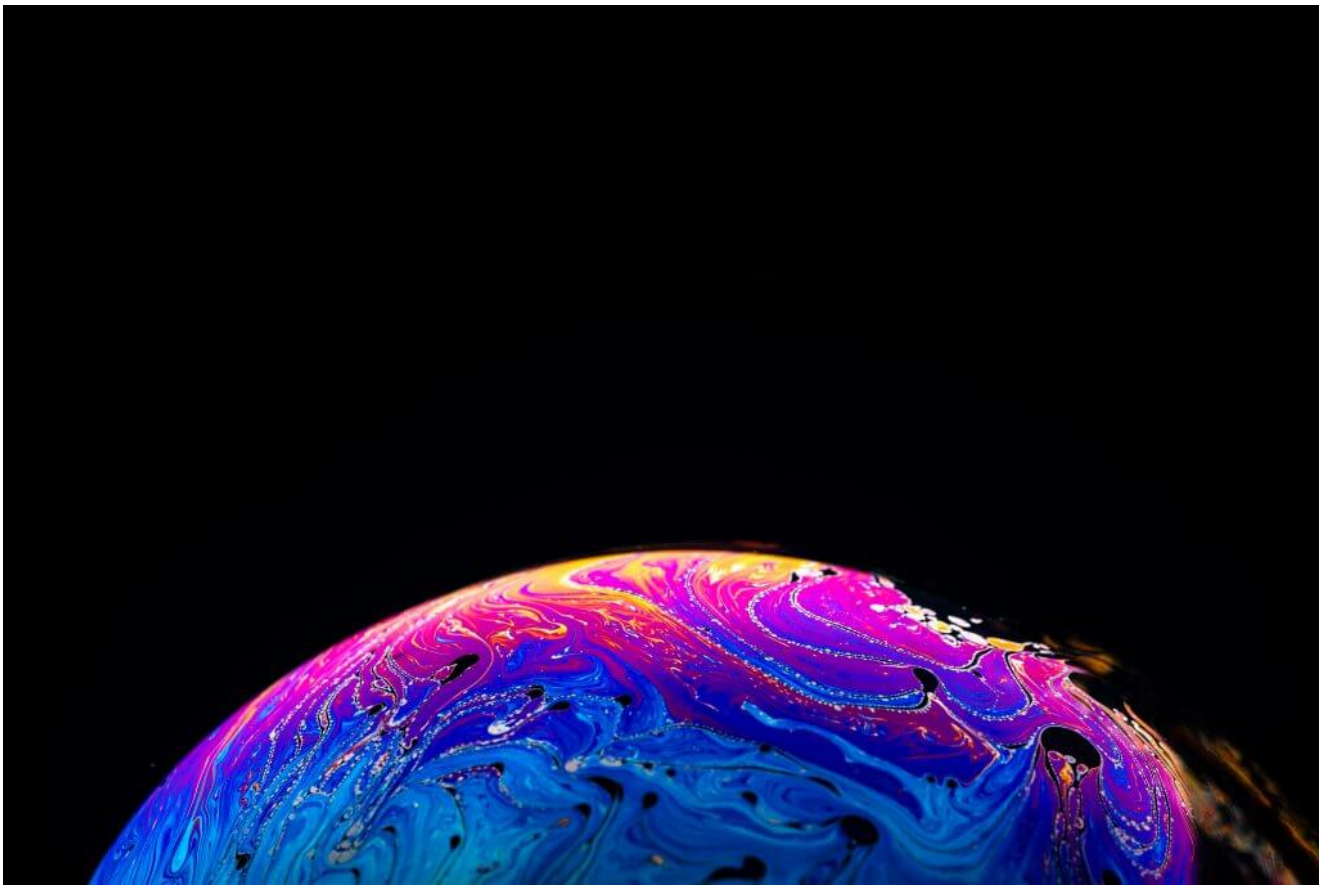
Download the HermeticWiper Technical Analysis Report

brandefense.io/hermeticwiper-technical-analysis-report/

March 10, 2022



As the tension that started between Russia and Ukraine on February 24 turned into a physical conflict, at the same time, cyber-attacks and malware threats came to the fore. Researchers had found that Russian threat actors developed malware that corrupts MBR (Master Boot Record) and disk volumes for Ukrainian organizations.

First, security researchers from ESET and Symantec detected this type of malware. We then analyzed the sample, making sense of it with various IoC findings. As a result, security providers have named this example HermeticWiper.

The malware was detected on thousands of different devices in Ukraine and tagged as KillDisk.NCV. It is named HermeticWiper because of the digital certificate the malware holds. The certificate, issued with Hermetica Digital Ltd, is valid from 2021.

Researchers state they can obtain the certificate by using it on behalf of a front company or confiscating a closed company. However, security researchers have noticed that malware signed with this certificate is no longer seen.


BRANDEFENSE
CYBER THREAT INTELLIGENCE
HermeticWiper
Technical Analysis Report