HC3: Alert

February 25, 2022 TLP: White Report: 202202251000

Hermetic Wiper Malware

Executive Summary

CISA is tracking another destructive wiper malware that was used yesterday being deployed against systems in Ukraine, Latvia, and Lithuania just hours before physical attacks on Ukraine by Russia. This is a different malware than the "Cyclops Blink" malware which was jointly reported yesterday by CISA, NSA, FBI, and UK NCSC. The new malware is being dubbed "Hermetic Wiper" or "Hermetica Wiper." So far, there has been no evidence of this malware being deployed on systems within the United States.

Report

HermeticWiper | New Destructive Malware Used In Cyber Attacks on Ukraine - SentinelOne

Impact to HPH Sector

Because this is a very destructive malware, HC3 recommends all members of the HPH to read the above referenced report and employ the indicators of compromise as best you can.

U.S. organizations should report incidents immediately to the FBI at a local FBI Field Office, CISA at us-cert.cisa.gov/report, or the U.S. Secret Service at a U.S. Secret Service Field Office.

References

ESET
https://twitter.com/ESETresearch/status/1496581903205511181

Ukraine: Disk-wiping Attacks Precede Russian Invasion
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/ukraine-wiper-malware-russia

Second Wiper Attack Strikes Systems in Ukraine and Two Neighboring Countries
https://zetter.substack.com/p/second-wiper-attack-strikes-systems

Contact Information

If you have any additional questions, please contact us at HC3@hhs.gov.

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback