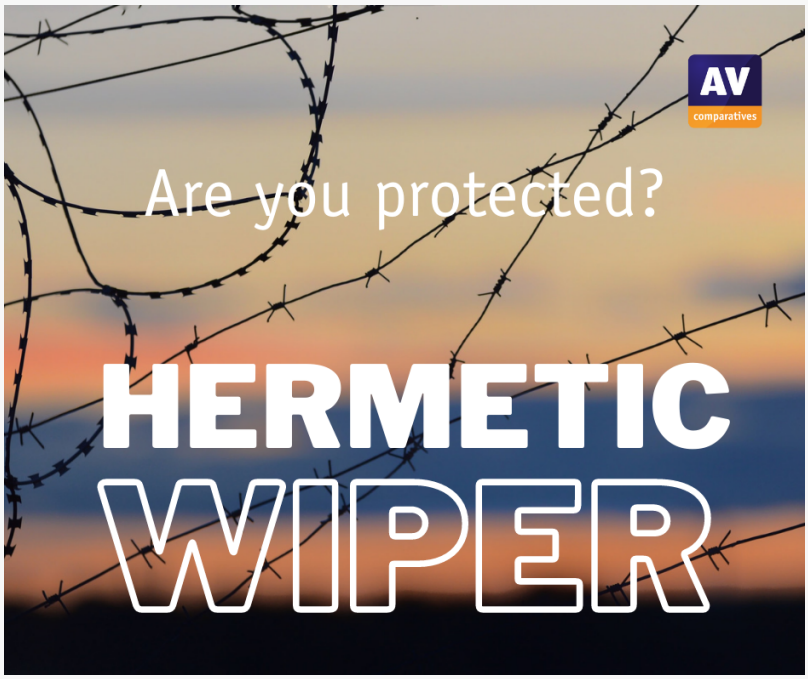
AV-Comparatives tests Anti-Virus Software protection against the Hermetic Wiper malware

Austrian IT-security testing lab AV-Comparatives has tested protection against the recently-emerged Hermetic Wiper malware.



AV-Comparatives tested against Hermetic Wiper

INNSBRUCK, TYROL, AUSTRIA, February 25, 2022 /EINPresswire.com/ -- The data-wiping malware has been used in international targeted attacks. Its aim is not to steal money or data, but simply to make victims' computers unusable. To do this, it abuses the services of a legitimate company that makes disk partitioning software. This type of utility can create, modify and delete the data storage areas (partitions) of a computer's system disk. Hermetic Wiper makes (unauthorised) use of this useful utility program to corrupt the system disk's boot information, meaning that the computer cannot start up. The malware then overwrites the partitions on the disk, making the data on them unreadable, even if the disk is transferred to an uninfected computer.

> It is good to see that all tested AV-Vendors blocked effectively against emerging threats like Hermetic Wiper."
>
> *Peter Stelzhammer, co-founder, AV-Comparatives*

In an attempt to avoid detection, Hermetic Wiper also makes use of a digital code-signing certificate (an indicator of genuine, non-malicious software), which was apparently stolen.

AV-Comparatives has run a malware protection test of programs made by vendors in both its Consumer and Enterprise Main Test Series for protection against variants of Hermetic Wiper. These are:

Enterprise Endpoint Security Vendors
Acronis, Avast, Bitdefender, Cisco, CrowdStrike, Cybereason, Elastic, ESET, Fortinet, G Data, K7, Kaspersky, Malwarebytes, Microsoft, Sophos, Trellix, VIPRE, VMware and WatchGuard.

Consumer Anti-Virus Vendors
Avast, AVG, Avira, Bitdefender, ESET, G Data, K7, Kaspersky, Malwarebytes, McAfee, Microsoft, NortonLifeLock, Panda, Total Defense, TotalAV, Trend Micro and VIPRE.

Logo AV-Comparatives

The Hermetic Wiper malware threats have been tested using the Real-World Protection Test framework, developed by AV-Comparatives.
Date and Time of testing: 25 February 2022, 1530 CET.

All of the tested products were able to protect the system effectively against multiple variants of the Hermetic Wiper malware.

General Advise:

In any conflicts, not only the current ones, an increase of cyberthreats is possible for authorities, institutions and organizations. In addition, an increased threat situation can be expected for all companies and organizations that are located in geographical exposed regions or have a recognizable relationship with them (e.g. trading partners, etc.). Furthermore, disinformation campaigns might be used. It must be taken into account that cyber operations are can be carried out in the phase of preparation of possible escalation stages, such as armed conflicts.

The implementation of the internationally available recommendations is strongly recommended.

Using strong Cybersecurity software and a list of proven measures to strengthen cyber resilience has been published by AV-Comparatives, ENISA and CERT-EU.

https://www.av-comparatives.org/enterprise
https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience

Peter Stelzhammer
AV-Comparatives
+43 720 115542
email us here
Visit us on social media:
Facebook
Twitter

LinkedIn