

## Themida and VMProtect-Protected Malware Can Be Analyzed to Expose Its Crucial Information

DUBAI, DUBAI, UNITED ARAB EMIRATE , June 18, 2024 /EINPresswire.com/ --<u>ANY.RUN</u>, a leading provider of cybersecurity solutions, published research on the use of popular code protectors, Themida and VMProtect, in malware and their effectiveness in concealing malicious functionality.

Malware authors often employ protectors like Themida and VMProtect in an attempt to prevent analysts from reverse engineering malicious code.

These protectors allow malware developers to use sophisticated techniques to hide malicious functionality, including through code



virtualization, obfuscation, anti-debugging, compression, and encryption.

## 

The research team at ANY.RUN analyzed six samples from different malware families that use Themida and VMProtect. The analysts found that none of the samples used code virtualization, making the analysis process much simpler.

Only one sample had anti-debugging enabled, and the malware code itself was largely unprotected, except for the initial stages of compression and decryption. This enabled the team to extract crucial information from malware samples' code, including command-and-control (C2) addresses, important strings, etc.

The research findings highlight a clear trend: most malware families overlook crucial features like virtualization, making reverse engineering significantly easier. In essence, these families use protectors as basic packers, providing minimal obstruction to analysis.

Learn more details about the research on ANY.RUN's blog.

## 00000 000.000

ANY.RUN's suite of cybersecurity products includes an interactive sandbox and a Threat Intelligence portal. Serving 400,000 professionals around the world, the sandbox offers a streamlined approach to analyzing malware families that target both Windows and Linux systems. Meanwhile, ANY.RUN's Threat Intelligence services, which include Lookup, Feeds, and YARA Search, enable users to quickly gather information about threats and respond to incidents with greater speed and precision.

Veronika Trifonova ANYRUN FZCO +1 657-366-5050 email us here Visit us on social media: X YouTube

This press release can be viewed online at: https://www.einpresswire.com/article/720923880

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire<sup>™</sup>, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information. © 1995-2024 Newsmatics Inc. All Right Reserved.