ANY.RUN Details How Threat Actors Use Obfuscators to Mask Malware

DUBAI, UNITED ARAB EMIRATES, February 14, 2024 /EINPresswire.com/ -- ANY.RUN, a cloud-based sandboxing service, published its first article in the series on the use of malware obfuscators, software tools that scramble code to make it difficult to understand and reverse engineer.

□□□ □□□□□□□□□□ □□ □□□□□□□□□□□□ □□□□□:

Modern malware often employs obfuscation techniques to hinder analysis and detection. This creates a significant challenge for security researchers who need to understand the code's functionality and potential harm. This article series aims to equip individuals with the knowledge to tackle obfuscated code with confidence.

□□□□□□□□□ □ □□□□□□□ □□□□□□□□□□□□

The series starts by taking readers through the creation of a simple obfuscator written in .NET. This hands-on approach provides a clear understanding of the basic techniques used, including:

• □□□□□ □□□□□□□□□□: Hiding strings within separate functions with complex names.
• □□□□□□□□□□ □□□□□□□□□□: Splitting strings into individual characters for further obfuscation.
• □□□□□□□□ □□□□□□□□□□□□: Replacing characters with their numerical values to mask their meaning.
• □□□□□ □□□□: Utilizing complex mathematical expressions to represent characters.
• □□□□□□□□ □□□□□ □□□□□□ (□□□) □□□□□□□□□□□□□: Shuffling code blocks while maintaining functionality.

□□□□□□□□□□ □□□ □□□□□□□□□□□

The article then demonstrates how seemingly complex obfuscation can be bypassed using various methods, such as:
• □□□□□□□□□□ □□□ □□□□□□□□□□□: Pausing code execution at key points to inspect variables and memory.
• □□□□□□ □□□□□: Analyzing memory snapshots to reveal hidden strings and data.
• □□□□□□□□□□□□□ □□□□□: Utilizing specialized software like De4dot to reverse engineer obfuscated code.

□□□□ □□□□□

The first article marks the introduction to a series. In upcoming installments, the authors will explore advanced obfuscation techniques used in real-world malware and strategies for extracting meaningful insights from obfuscated code.

Learn more in ANY.RUN's blog post.

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