EINPRESSWIRE

GuLoader: Deobfuscating and Automating Malware Analysis

DUBAI, DUBAI, UAE, May 18, 2023 /EINPresswire.com/ -- ANY.RUN, a cybersecurity company developing an interactive sandbox analytical platform for malware researchers, presents the GuLoader Malware Analysis.

Here are some highlights from the GuLoader malware and deobfuscating its code using the Ghidra scripting engine:

□□□□ □□ □□□□□□□□

GuLoader is a widely used malware loader known for its complex obfuscation techniques that make it difficult to analyze and detect.

□□□□□□□□□ □□□ □□□: □□□
□□□□□□□□□□□□□□ □□□□ □□ □□□□□□□ □□□□□□ □□□□□□□□□?

Deobfuscating code is an essential step in the process of malware analysis. When malware authors create their programs, they often use various obfuscation techniques to make it more difficult to understand and analyze their code. By deobfuscating the code, analysts can gain a better understanding of the malware's functionality, identify its capabilities, and develop effective mitigation strategies.

□□□□□□□□□□□□□□ □□□ □□□□□□□□□□□: □□□□□□□□□□ □□□ □□□□□□□□□□□

ANY.RUN identified various obfuscation techniques often found in GuLoader, including:
- Opaque predicates
- Obfuscated arithmetic expressions
- And junk instructions.

Now, ANY.RUN has focused on developing techniques and strategies to overcome these obfuscation methods and make the code easier to analyze.

Here are some of them:
- “Nopping” all XMM instructions
- Leaving Unconditional JMP Instructions Untouched
- “Nopping” Junk Instructions
- Defeating fake comparison instructions
- Defeating fake PUSHAD instructions
- Defeating fake PUSH instructions
- Calculating Arithmetic Expressions

□□□□□□□□□□ □□□□□□□ □□□□□□□□ □□□□ □ □□□□□□ □□□□□□

ANY.RUN has developed a script that initiates from the chosen instruction, tracks calls and conditional jumps, simplifies, deobfuscates, and disassembles the resulting code. The script avoids jumping over calls with a specific operand value because not all calls result in returns.

It’s important to note that while this approach was specifically tailored for deobfuscating GuLoader, the same general techniques could be applied to other malware samples as well. However, bear in mind that each malware sample might have unique obfuscation techniques, necessitating the development of specific optimization strategies.

ANY.RUN has explored one potential approach to deobfuscating GuLoader, which entails identifying common obfuscation patterns and neutralizing them using various techniques.

Read more with the code & scripts examples in the article at ANY.RUN.

Vlada Belousova
ANYRUN FZCO
2027889264
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/634475198