# ANY.RUN Analyzes Malware With ChatGPT

*ANY.RUN, a cybersecurity company for malware researchers, tested ChatGPT and now is ready to share the expert results.*

DUBAI, UNITED ARAB EMIRATES, February 16, 2023 /EINPresswire.com/ -- ANY.RUN, a cybersecurity company developing an interactive sandbox analytical platform for malware researchers, tested ChatGPT and now is ready to share the expert results.

OpenAI released ChatGPT in November 2022 and by February 2023 the chatbot already has over 600 million monthly visits, according to SimilarWeb. It's scary to think how many people are being armed with the tools to develop advanced malware.

If ChatGPT can build malware, can it help to analyze it? ANY.RUN made a special experiment to investigate if AI can help to perform malware analysis.

How did ANY.RUN test ChatGPT?

ANY.RUN fed the chatbot malicious scripts of varying complexity and asked it to explain the purpose behind the code. The researchers used simple prompts such as "explain what this code does" or "analyze this code". Furthermore, it was made several round ups with malicious scripts of varying complexity.

ChatGPT can recognize and explain simple malware

Based on the testing, it can recognize and explain malicious code, but it only works for simple scripts. The AI understands the purpose of the code, highlights its malicious intent and logically lays out what it does step-by-step.

ChatGPT struggles in real-life situations

The performance the AI was able to show so far is impressive, there is no doubt about it. But in a real-life situation it usually won't be dealing with such simple code, like in the previous examples.

So for the next couple of tests, ANY.RUN ramped up the complexity and provided it with code that is closer to that of what one can expect to be asked to analyze on the job. Unfortunately, ChatGPT just couldn't keep up.


ANY.RUN summary

As long as the researchers provided ChatGPT with simple samples, it is able to explain them in a relatively useful way. But as soon as it was getting closer to real-world scenarios, the AI just breaks down. At least, the researchers weren't able to get anything of value out of it.

It seems that either there is an imbalance and the tool is of more use for red-teamers and hackers, or the articles that warn of its use for creating advanced malware are overhyping what it can do a bit.

In any case, bearing in mind how quickly this technology has developed, it's worth keeping an eye on how it's progressing. Chances are that in a couple of updates it will be a lot more useful.


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

Galina Zueva
ANYRUN FZCO
g.zueva@any.run
Visit us on social media:
Twitter
LinkedIn