ROBO6K

7/29/2023

The future of attacks

With the advent of the large language learning models and AI based systems like ChatGPT, the dark side is ever on the coat tails. With any great strive in the technological world, there will be those using the advances for ill-gotten gains, whether that is for financial reasons, disrupting businesses or to just create chaos. By taking a deeper look into both sides of the coin, we will be better suited to help safeguard each employee and the business as a whole.

Software like ChatGPT does have some built-in safeguards. However, with the correct wording, these can be bypassed into creating entire malware scripts or even used to create ever more convincing phishing campaigns. While it is apparent that the use of these programs seems to be becoming ever more prevalent, developing a straightforward policy for its use is of vital importance. If it has been decided to allow the use of generative AI, finding a reputable vendor with good data security and an iron clad privacy policy will be the first step to using the technology while keeping risk avoidance in the forefront of the strategies.

As AI technology continues to grow, the dark side continues to become ever more prevalent. Creators have now taken the underlying source code and begun creating programs like WormGPT which can be used for BEC, malware creation or even large scale phishing campaigns. Threat actors are also using the software to create threats that continue to morph which allows it to avoid EDR detection. By using simple bypass methods, researchers where also able to create zero-day exfiltration code completely using the AI programs.

2600 SOUTH 1ST STREET
T (512)379-2272 U WWW.ROBO.NET

All of this can lead to the need for ever vigilant employees. There are many things that can be done but they all start with user awareness training. As many in the security world know, you are only as secure as the weakest link. This is why it is becoming imperative to have a very defined process and policy. Things like knowing how vendors are paid or verifying if they are coming from a legit source are paramount in ensuring that employees do not fall victim to fraud. The unfortunate truth is that if an employee voluntarily makes a payment, it is unlikely that it can be recovered.

In summary, the ongoing need to make sure that you are up to speed in the threat landscape is ever present. No matter what your role in any organization that you are apart of, you too have a huge part in the overall security posture. Just keep in mind, am I expecting a bill from this company? Is this the normal way payments are made to this vendor? Have I confirmed verbally that the boss wants to purchase this gift card for an incentive? Become the ever-skeptic and remember to stay safe, up-to date and trust no one that you cannot confirm.

Thank you,

Caleb Leggett

Your ROBO Technician