Lodestone

APRIL 2023

STATE OF CYBER

monthly newsletter

THE RISE OF AI POSES NEW SECURITY THREATS

AI content generation has dominated social media cycles recently. Ranging from a myriad of positive, helpful, and creative solutions of all sorts of tasks, to much more malicious purposes. Lodestone has noticed a consistent pattern of security researchers and malicious actors tout the many uses of AI engines such as ChatGPT to create malware, enhance phishing, and doctor victim communications.

ChatGPT is the most widely used deep learning algorithm, renowned for its ability to generate human-like responses to text-based conversations and queries. By leveraging massive amounts of online data and custom datasets, ChatGPT can produce natural, accurate responses.

In particular, a growing concern from Lodestone is utilizing ChatGPT to mimic individuals and organizations. Training it in language/writing style for target individuals or organizations allowing them to generate fake messages/emails that appear real, for targeted phishing/misinformation. Additionally, they can also exploit features within ChatGPT to generate malicious code, streamlining attacks and launching sophisticated ones quickly, all with no real technical knowledge required.

ChatGPT and other AI engines can be used to drastically reduce timelines and enhance attacks. Organizations should prepare for the baseline of phishing attacks to continue to be more and more sophisticated. Phishing tests and training should reflect this with more difficult scenarios being implemented. Further Lodestone continues to recommend strong layered defenses such as Endpoint Detection and Response software and monitoring to pick up on malicious code brought into the environment sooner.

Consider reaching out to Lodestone to see how we can help improve your security posture.

AI BEING USED TO CREATE DIGITAL CON ARTISTS ON YOUTUBE, WARNS ANALYST

Threat actors have tried to deceive people into downloading malware for years by offering free or illegally obtained versions of popular programs such as Photoshop. Now, they are taking this one step further by employing AI to create realistic video personas that make their ads more believable.

AI FOR AN AI: WHY CHATGPT IS A DOUBLE-EDGED SWORD FOR CYBERSECURITY

This article discusses the pros and cons of ChatGPT for cybersecurity.

TOP 4 WAYS THREAT ACTORS WEAPONIZE AI IMAGE GENERATORS

This article discusses 4 ways threat actors are currently leveraging AI image generators to carry out cyber-attacks.

THE AI RISK LANDSCAPE: HOW CHATGPT IS SHAPING THE WAY THREAT ACTORS WORK

Threat actors are actively attempting to circumvent the safeguards ChatGPT has in place and pushing its boundaries to create malicious code and exploit payloads.

Contact Us: 320 East Main St, Lewisville, TX 75057. Tel: 1-203-307-4984. www.lodestone.com