CHATGPT AS A TOOL FOR CRIME: 5 CYBER THREATS ENABLED BY THE LANGUAGE MODEL.

In late November 2022, OpenAI released ChatGPT, a public generative AI that has raised concerns about its potential to amplify the severity and complexity of cyber threats. As soon as it was announced, security experts predicted that attackers would start using this AI chatbot to craft malware or even augment phishing attacks. It has not taken long for their suspicions to be confirmed, as cybercriminals have already started to use this tool based on the GPT-3 AI language model to recreate malware strains and perpetrate different types of attacks.

With ChatGPT, cybercriminals can leverage generative AI to craft malicious activity, including phishing, identity theft, other social engineering attacks, the creation of malicious bots, and even malware. Attackers only need to create an OpenAI account, which is free of charge, and then make a query. For instance, they can use the ChatGPT system's Large Language Model (LLM) to move away from universal formats and automate the creation of unique phishing or spoofing emails, written with perfect grammar and natural speech patterns tailored to each target. This makes it harder for recipients to detect and avoid clicking on malicious links that may contain malware.

Moreover, cybercriminals can use ChatGPT to impersonate a trusted institution, exploiting the AI's ability to replicate the corporate tone and discourse of a bank or organization. They can then use these messages on social media, SMS, or via emails to obtain people's private and financial information. Additionally, malicious actors can write social media posts posing as celebrities by exploiting this capability. They can also launch social engineering attacks, where they create fake profiles on social media, tricking people into clicking on malicious links or sharing personal information.

Furthermore, ChatGPT can be used to create chatbots, spread spam, launch phishing attacks, or even develop malware. The model enables threat actors with limited technical or no coding skills to generate code in various programming languages, writing malware simply by knowing which functionality it should have. Sophisticated cybercriminals can also use this technology to make their threats more effective or to close existing loopholes.

These advanced threats require advanced solutions. WatchGuard EPDR combines endpoint protection (EPP) and detection and response (EDR) capabilities in a single solution. Thanks to its new and

emerging AI models of machine learning and deep learning, WatchGuard EPDR protects against advanced threats, advanced persistent threats (APTs), zero-day malware, ransomware, phishing, rootkits, memory vulnerabilities, and malware-free attacks. It also provides complete endpoint and server visibility, monitoring, and detecting malicious activity that can evade most traditional antivirus solutions.

WatchGuard EPDR continuously monitors all applications and detects malicious behavior, even if it originates from legitimate applications. It is capable of orchestrating an automated response and providing the necessary forensic information to thoroughly investigate each attack attempt through advanced indicators of attack (IoA).

The innovation of a tool like ChatGPT can be positive for the world and change current paradigms, but it can also do serious harm if it falls into the wrong hands. Having the right cybersecurity solution in place can prevent the negative side of promising tools like this one from reaching your organization through the misuse bad actors can make of them.

In conclusion, ChatGPT poses a cybersecurity risk that must be addressed by organizations. IBSCY, as a WatchGuard certified partner in Cyprus, offers a range of IT security solutions to organizations of all sizes and their employees.

Source