ChatGPT: A Huge Threat to the Cybersecurity Industry?

Original: https://www.btcc.com/en-US/academy/research-analysis/chatgpt-a-huge-threat-to-the-cybersecurity-industry

Since its debut in November, ChatGPT has become the internet's new favorite plaything. The artificial intelligence-powered natural language processing tool quickly amassed over 1 million users, who have used the web-based chatbot for everything from generating wedding speeches and hip-hop lyrics to writing academic papers and programming computer code.

Not only have ChatGPT's human-like abilities taken the internet by storm, but it has also set a number of industries on edge: a New York school banned ChatGPT over fears that it could be used to cheat, copywriters are already being replaced, and reports claim Google is so alarmed by ChatGPT's capabilities that it issued a "code red" to ensure the survival of the company's search business.

It appears the cybersecurity industry, a community that has long been skeptical about the potential implications of modern AI, is also taking notice amid concerns that ChatGPT could be abused by hackers with limited resources and zero technical knowledge.

Just weeks after ChatGPT debuted, Israeli cybersecurity company Check Point demonstrated how the web-based chatbot, when used in tandem with OpenAI's code-writing system Codex, could create a phishing email capable of carrying a malicious payload. Check Point threat intelligence group manager Sergey Shykevich suggested that he believes use cases like this illustrate that ChatGPT has the "potential to significantly alter the cyber threat landscape," adding that it represents "another step forward in the dangerous evolution of increasingly sophisticated and effective cyber capabilities."

Users can generate a legitimate-looking phishing email using the chatbot. When first asked to craft a phishing email, ChatGPT may deny the request. "I am not programmed to create or promote malicious or harmful content," a prompt spat back. But rewriting the request slightly can easily bypass the software's built-in guardrails.

Many of the security experts believe that ChatGPT's ability to write legitimate-sounding phishing emails — the top attack vector for ransomware — will see the chatbot widely embraced by cybercriminals, particularly those who are not native English speakers.

Chester Wisniewski, a principal research scientist at Sophos, said it's easy to see ChatGPT being abused for "all sorts of social engineering attacks" where the perpetrators want to appear to write in a more convincing American English.

"At a basic level, I have been able to write some great phishing lures with it, and I expect it could be utilized to have more realistic interactive conversations for business email compromise and even attacks over Facebook Messenger, WhatsApp, or other chat apps," Wisniewski said.

"Actually getting malware and using it is a small part of the shit work that goes into being a bottom feeder cyber criminal."

The idea that a chatbot could write convincing text and realistic interactions isn't so far-fetched. "For example, you can instruct ChatGPT to pretend to be a GP surgery, and it will generate life-like text in seconds," said Hanah Darley, who heads threat research at Darktrace. "It's not hard to imagine how threat actors might use this as a force multiplier."

Check Point also recently sounded the alarm over the chatbot's apparent ability to help cybercriminals write malicious code. The researchers say they witnessed at least three instances where hackers with no technical skills boasted how they had leveraged ChatGPT's AI smarts for malicious purposes. One hacker on a dark web forum showcased code written by ChatGPT that allegedly stole files of interest, compressed them, and sent them across the web. Another user posted a Python script, which they claimed was the first script they had ever created. Check Point noted that while the code seemed benign, it could "easily be modified to encrypt someone's machine completely without any user interaction." The same forum user previously sold access to hacked company servers and stolen data, Check Point said.

How difficult could it be?

Dr. Suleyman Ozarslan, a security researcher and the co-founder of Picus Security, recently demonstrated how ChatGPT was used to write a World Cup–themed phishing lure and write macOS-targeting ransomware code. Ozarslan asked the chatbot to write code for Swift, the programming language used for developing apps for Apple devices, which could find Microsoft Office documents on a MacBook and send them over an encrypted connection to a web server, before encrypting the Office documents on the MacBook.

“I have no doubts that ChatGPT and other tools like this will democratize cybercrime,” said Ozarslan. “It’s bad enough that ransomware code is already available for people to buy ‘off-the-shelf’ on the dark web; now virtually anyone can create it themselves.”

Unsurprisingly, news of ChatGPT’s ability to write malicious code furrowed brows across the industry. It’s also seen some experts move to debunk concerns that an AI chatbot could turn wannabe hackers into full-fledged cybercriminals. In a post on Mastodon, independent security researcher The Grugq mocked Check Point’s claims that ChatGPT will “super charge cyber criminals who suck at coding.”

“They have to register domains and maintain infrastructure. They need to update websites with new content and test that software which barely works continues to barely work on a slightly different platform. They need to monitor their infrastructure for health, and check what is happening in the news to make sure their campaign isn’t in an article about ‘top 5 most embarrassing phishing phails,’” said The Grugq. “Actually getting malware and using it is a small part of the shit work that goes into being a bottom feeder cyber criminal.”

Some believe that ChatGPT’s ability to write malicious code comes with an upshot.

“Defenders can use ChatGPT to generate code to simulate adversaries or even automate tasks to make work easier. It has already been used for a variety of impressive tasks, including personalized education, drafting newspaper articles, and writing computer code,” said Laura Kankaala, F-Secure’s threat intelligence lead. “However, it should be noted that it can be dangerous to fully trust the output of text and code generated by ChatGPT — the code it generates could have security issues or vulnerabilities. The text generated could also have outright factual errors,” added Kankaala, laying doubt to the reliability of code generated by ChatGPT.

ESET’s Jake Moore said as the technology evolves, “if ChatGPT learns enough from its input, it may soon be able to analyze potential attacks on the fly and create positive suggestions to enhance security.”

It’s not just the security experts who are conflicted on what role ChatGPT will play in the future of cybersecurity. We were also curious to see what ChatGPT itself had to say when we posed the question to the chatbot.

“It’s difficult to predict exactly how ChatGPT or any other technology will be used in the future, as it depends on how it is implemented and the intentions of those who use it,” replied the chatbot. “Ultimately, the impact of ChatGPT on cybersecurity will depend on how it is used. It is important to be aware of the potential risks and to take appropriate steps to mitigate them.”

Read More:

Bonk Airdrop: Where to buy Bonk crypto

When Will Pi Coin Launch: Pi Network Phase 4 Release Date

Is Pi Network Legit Or Scam: Pi Coin Real Or Fake?

Pi Coin Price Prediction: Will Pi Coin Be Worth Anything?

Luna Classic Price Prediction: Will Luna Classic Reach $1?

ADA Cardano Price Prediction 2025, 2030

HBAR Price Prediction 2025, 2030

How to Stake LUNC: Everything You Need to Know

Terra LUNA 2.0 vs. Luna Classic (LUNC): What Are the Differences?

Wild Cash App by Hooked Protocol: Answer Quiz to Earn $HOOK

Hooked Protocol Price Prediction

Gasoline Price Prediction: What Will It Be In Five Years?

Ethereum Price Prediction 2025-2030

XLM Price Prediction 2030: Is XLM a Good Investment?

Best Crypto Casino USA Online in 2023

Metamask Airdrop – To Get $MASK Token for Free?

Leverage in Crypto Trading: Something You Need to Know

Best Crypto Leverage Trading Platform for 2023

What Is Futures Trading in Crypto? A Guide for Beginners

BTCC Crypto Futures Trading Guide