Threat Intelligence Report

2024 Trend: Black Hat Generative AI Tools

One month into 2024, it is clear that artificial intelligence (AI) technology will continue to expand and evolve quickly, becoming an increasingly important variable in 2024. Generative AI, or AI capable of creating images, text, and synthetic data, can be used to augment cybersecurity protections, and can also be used by threat actors to enable cyber attacks. Despite the countless benefits of AI, failing to account for the risks it imposes can leave individuals and organizations vulnerable. Though threat actors have been hesitant to widely adopt mainstream generative AI tools like ChatGPT for malicious uses, due in part to ethical parameters within the technology aimed at preventing illegal activity, threat actors have been successful in using popular tools to improve social engineering messages and phishing campaigns. More concerning, however, is the use of black market AI tools specifically designed to create deepfakes, spread misinformation, access dark web sources, and easily write malicious code. Knowing the risks that these generative AI tools pose allows organizations to adequately prepare to face new threats.

POTENTIAL THREATS

The advent of generative AI technologies has brought about new avenues for threat actors, notably with the development of tools such as WormGPT, FraudGPT, DarkBERT, DarkBART, and DarkGPT. These AI chatbots have been listed for sale across various dark web marketplaces, offering a black hat "alternative" to ChatGPT and other AI chatbots designed to operate under strict ethical limitations. Like ChatGPT, these tools are large language models (LLMs), but are thought to be trained on malware data, dark web data, and other malicious sources that are excluded from commercial LLMs like ChatGPT.

THREAT ASSESSMENT

While research on the use of generative AI in recent cyber attacks remains relatively sparse, the growing availability of these tools has turned the threats posed by generative AI from a theoretical concern to a practical reality. As AI technology improves and becomes more widespread, the commoditization of malicious tools will allow threat actors to more easily leverage AI's capabilities. Specifically engineered for illicit purposes, these tools are tailored to assist in a range of malicious activities including:

- Automating phishing and social engineering attacks: Generative AI tools can craft highly convincing phishing emails or messages that mimic legitimate communication, resulting in higher-quality social engineering attacks.
- Facilitating fraud and scams: Generative AI tools can automate the creation of scam websites, forge documents, or impersonate individuals, making frauds more convincing and difficult to detect.
- Creating malware: Generative AI tools can aid in creating and refining malware. AI tools can also provide exploit tutorials and coding lessons, lowering the barrier to entry in the cyber threat landscape.
- Dark web accessibility: Tools such as DarkBART, which is based on a LLM specific to dark web language structures, are pretrained on dark web data. Another tool, DarkBERT, uses the entire dark web as its LLM integrating knowledge from dark web marketplaces and hacker forums into its output.

RECOMMENDED ACTION

Staying up-to-date on the latest developments in generative AI will allow organizations to proactively address emerging threats from malicious actors using the technology. In addition, organizations should:

- Hold regular training sessions for employees to help them identify signs of phishing emails and report them appropriately. Because generative AI makes phishing emails more realistic than ever, training sessions should highlight sophisticated social engineering techniques.
- Engage a third-party resource for penetration testing activities simulating the most up-to-date threats to ensure defenses are able to handle attacks leveraging emerging technologies.
- Regularly conduct cybersecurity vulnerability assessments, and create a roadmap for efficiently and effectively patching all vulnerabilities detected.
- Continuously monitor systems for anomalous activity to identify threat actors early.

SOURCES

Sources include open-source information from public and private industry reporting.

- Is Artificial Intelligence the Solution to Cyber Security Threats?
- Mitigating AI Cybersecurity Risks from the Top Down
- The Crucial Role of Red Teaming as AI Assumes Centre Stage
- 'DarkBERT' GPT-Based Malware Trains Up on the Entire Dark Web

Why FTI Cybersecurity

Multidisciplinary Expertise

Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

Core team from intelligence agencies, law enforcement, prosecuting offices, and global private sector institutions

Globally Positioned

Ability to respond anywhere in the world

Ability to staff the largest and most complex engagements and investigations

Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

Integrated & Comprehensive

Comprehensive services include crisis communications, e-discovery, forensic investigations, and more

Seamless integration of FTI Consulting's expertise across service offerings

FTI Cybersecurity Global Offices

Americas

Atlanta
Boston
Chicago
Dallas
Houston
Irvine
Los Angeles
Mexico City
Miami
New York
Philadelphia
Roseland
San Francisco
Sao Paulo
Seattle
Toronto
Washington, DC
Wayne

EMEA

Berlin
Brussels
Cape Town
Dubai
Dublin
Dusseldorf
Frankfurt
Johannesburg
London
Madrid
Mumbai
Munich
Paris
Zurich

APAC

Brisbane
Hong Kong
Melbourne
Perth
Shanghai
Singapore
Sydney
Tokyo

CONTACT FTI CYBERSECURITY

Email: #fticybersecurity@fticonsulting.com

Phone: +1-844-CYBR-FTI (+1-844-292-7384)