AI Evolution in Cybercrime: Threats and Deceptive Tactics

Cybercriminals are leveraging artificial intelligence (AI) to craft sophisticated email threats, such as phishing and business email compromise (BEC) attacks, signifying a notable shift in the role of AI in email security as traditional methods have become less effective. Concurrently, these adversaries have turned to fraudulent AI bots as a means to distribute malicious software, masquerading as legitimate AI applications. ESET security researchers uncovered such a deceptive campaign after spotting an advertisement on Facebook that lured users into downloading what purported to be Google's genuine AI tool, "Bard." The ad's irregularities, including an unfamiliar Dublin-based service link and suspicious comments, raised alarms. The campaign's objective was to deceive users into downloading a password-protected file that contained malware disguised as an official Google service, triggering antivirus warnings. These strategies highlight the persistent threat posed by AI applications being exploited by cybercriminals and their evolving tactics.

The CRITICAL**START**® Cyber Research Unit will continue to monitor the situation and work closely with the SOC and Security Engineering team to implement any relevant detections. For future updates the CTI team will post updates via Cyber Operations Risk & Response™ Bulletins and on the CRITICAL**START**® Intelligence Hub.

References:

1. https://www.helpnetsecurity.com/2023/08/23/ai-enabled-email-threats/
2. https://www.infosecurity-magazine.com/news/deceptive-ai-bots-spread-malware/?&web_view=true