Cybersecurity News

Credential Stealing Malware has exploded as result of the latest AI technology

A Serious Threat that is Growing

EndpointLock™
Desktop and Mobile Security

SECURITY NEWS: How to Protect Against New AI Generated Malware

Credential Stealing Malware has exploded as result of the latest AI technology

A Serious Threat that is Growing

ChatGPT is an artificial intelligence chatbot developed by OpenAI, which launched in November 2022 and set the record for the fastest growing user database. According to the latest available data, ChatGPT rose to 100 million users and 1 billion visitors per month within just 2 months of their launch. ChatGPT has been used in a variety of applications including chat bots, virtual assistants, automated customer service systems, and has been recognized as one of the most advanced AI language models currently available.

In January of this year, cybersecurity researchers reported on how ChatGPT could be used to develop polymorphic malware, a type of malicious software that changes its code and appearance to evade detection. And last month, HYAS Institute researcher and cybersecurity expert, Jeff Sims, took it a step further and developed a new type of ChatGPT - powered malware, a polymorphic keylogger. Given the threat posed by this sort of malware, the researchers named it BlackMamba, in reference to the deadly snake.

As per the HYAS Institute's report, the malware can gather sensitive data such as usernames, debit/credit card numbers, passwords, and other confidential data entered by a user into their device. Keyloggers have become increasingly prevalent and dangerous in today's digital age. This malware is polular among hackers as it can be used to steal the credentials needed to launch a data breach.

Once it captures the data, Blackmamba employs MS Teams to transfer it to the attacker's Teams channel, where it is "analyzed, sold on the dark web or used for other nefarious purposes," according to the report. Jeff Simms made the malware shareable and portable by employing a free, open-source utility, to show how easy this malware would be to sell and distribute to other cybercriminals. Additionally, the malware can be shared within the targeted environment through social engineering or email.

The threats posed by open source AI has accelerated the ease and speed at which malware can be created and deployed. By generating new, unique code at runtime, malware like BlackMamba is virtually undetectable by today's predictive security solutions and antivirus.

Take Action to Stop the Threat of Polymorphic Keyloggers

By utilizing **EndpointLock™ Keystroke Encryption** software, all keystrokes are encrypted making them unreadable to keyloggers even if the malware is polymorphic and evades detection.

Keystroke Encryption should not be confused with VPNs, SSL, TLS Encryption, File or Database Encryption. Even with all of these protocols in place, everything the user types is vulnerable and can be easily captured by a keylogger.

EndpointLock™ provides strong cryptography at the time of keystroke entry, where most data breaches begin. This protects the initial transmission of usernames and passwords and other sensitive data entered into any PC or mobile device.

Take Action to Protect your data and your customer's data

With EndpointLock™ Keystroke Encryption

- Programs available for employees and customers/members.
- Let's schedule some time to discuss how we can help you

References:

1. Hackread
2. SecurityBoulevard