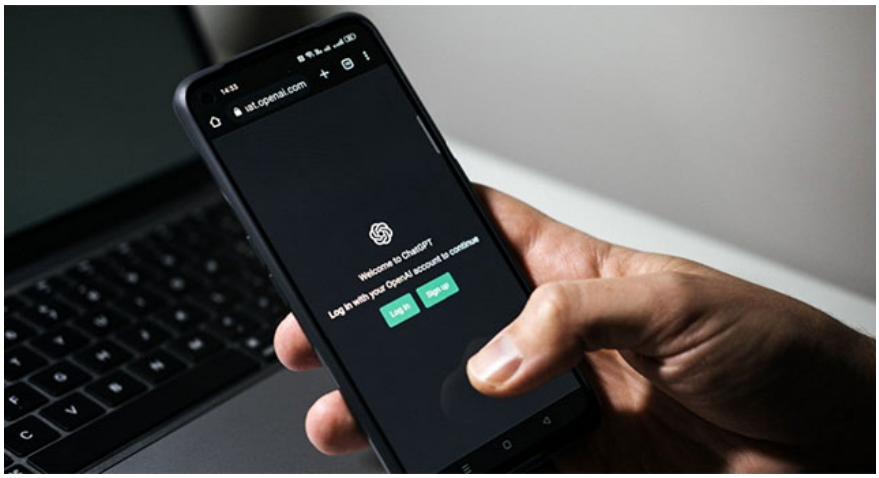
Meta warns of new malware threats, including ChatGPT spoofing malware

Meta has just announced the company's latest efforts to identify and prevent malware campaigns targeting business users.

Meta has just announced the company's latest efforts to identify and prevent malware campaigns targeting business users. Meta's security teams use a variety of security methods to combat malware, including code analysis, continuous improvement of identification systems, product updates, education and support. community.

Meta has also shared threat information with other companies and has taken a series of legal actions against threat actors. These combined efforts have limited the spread of any single strain of malware, while also forcing hacker organizations to invest more resources to continuously adjust attack tactics and techniques.

Meta encourages everyone to exercise caution when downloading software or files from the internet. Before discussing NodeStealer, a recently discovered malware family, Meta shared the latest trends they have observed in the overall picture of malware world activity. . The company's research found that many malware campaigns used custom-built tools to target business users on specific internet services.



Hacker groups have effectively adapted to the disruption and are spreading across multiple internet services to ensure a complex, multi-pronged malware campaign that can withstand the defenses of any service. which case? Meta illustrated this point with the example of a malware family called Ducktail, which has evolved over the past few years. Ducktail targets many social media platforms across the internet, including LinkedIn, various browsers, and even file hosting services. Ducktail has adapted to the ongoing detection and mitigation efforts of enterprise-class security systems by granting admin access to ad-related action requests by attackers send.

Similarly, malware operators used popular trends and issues to attract people's attention, and trick them into clicking on malicious links or downloading malicious code. Meta has investigated and taken action against

several malware families that take advantage of people's interest in ChatGPT to trick them into installing malware that pretends to provide AI functionality. The company also discovered about 10 malware families that use ChatGPT and similar themes to compromise user accounts on the internet.

Malware operators have used cloaking to circumvent automated ad screening systems and leverage popular platforms such as social networks, file sharing services, and even official store to spread their malware. Meta said it successfully blocked more than 1,000 malicious URLs under the ChatGPT theme and shared them with industry colleagues.

Microsoft's remarkable efforts have contributed to forcing malware operators to quickly develop other tactics to maintain operations, making their operations unable to take place easily and effectively. as usual.