# Hackers exploit AI craze on Facebook to spread malicious malware ads



A significant security threat has emerged as millions of Facebook users fall victim to sophisticated scams promoting fake AI tools. Cybercriminals have been identified as part of a group known as UNC6032, which has successfully weaponised the growing interest in artificial intelligence to distribute malware through misleading advertisements. According to a recent report by Google’s Mandiant Threat Defence team, the campaign targets users seeking AI video editing capabilities with fraudulent ads that claim to offer advanced tools. Unfortunately, these "tools" are merely conduits for malware, including Python-based infostealers and various backdoors that compromise personal data.

The scale of the operation is alarming, with researchers estimating that over 2.3 million users may have been exposed to these malicious ads. This number highlights not only the reach of the campaign but also the ease with which it can manipulate social media platforms to masquerade as credible services. Popular AI generator tools, such as those found in Canva Dream Lab, Luma AI, and Kling AI, have been impersonated to lend an air of legitimacy. This practice has become a common tactic among cybercriminals, making it essential for users to remain vigilant.

The criminal tactics have evolved beyond mere impersonation to actively hijacking Facebook accounts and modifying them to promote these fraudulent services. In some instances, attackers have created fake pages for renowned AI platforms like MidJourney, OpenAI's SORA, and ChatGPT. These pages have attracted millions of followers, utilising crafted content and visuals to entice users to download harmful software. Malware variants like Rilide, Vidar, and IceRAT have emerged from such campaigns, stealing sensitive information such as credentials, cryptocurrency wallet data, and even targeting business accounts.

Researchers warn that these schemes are not isolated incidents; they reflect a broader trend of cybercriminals exploiting the popularity of AI to lure unsuspecting individuals and businesses. With increasing numbers of creators and entrepreneurs interested in AI tools, the potential for exploitation is vast. Scammers go beyond creating malicious websites; they leverage platforms such as Facebook to disseminate their ads, driving users towards applications that can severely compromise their systems.

As these attacks proliferate, organisations like Mandiant emphasise the importance of vigilance. Users are advised to thoroughly vet any advertisements for AI services and to verify the legitimacy of the websites they visit. Simple precautions, such as conducting manual searches for AI tools and avoiding downloads from dubious sources, can help shield users from falling prey to these scams. The growing reliance on AI in everyday tasks makes this issue even more pertinent, necessitating increased awareness and critical engagement with online content.

The intersection of AI technologies and cybersecurity continues to pose both opportunities and risks. As this threat landscape evolves, it becomes paramount for users—both individuals and organisations—to be proactive in safeguarding their digital environments from malicious exploitation masked as innovative solutions.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.techradar.com/pro/security/millions-of-users-could-fall-for-fake-facebook-ad-for-a-text-to-ai-video-tool-that-is-just-malware> - Please view link - unable to able to access data
2. <https://www.bleepingcomputer.com/news/security/fake-facebook-midjourney-ai-page-promoted-malware-to-12-million-people/> - Cybercriminals have hijacked Facebook profiles to create fake AI services, such as MidJourney, OpenAI's SORA, ChatGPT-5, and DALL-E, to distribute malware. These fraudulent pages amassed over 1.2 million followers, promoting non-existent desktop versions of AI tools and luring users into downloading malicious executables. The malware, including Rilide, Vidar, IceRAT, and Nova, steals sensitive information like credentials and cryptocurrency wallet data, which is then sold on dark web markets or used for further scams. Users are advised to exercise caution and verify the legitimacy of AI tools before downloading.
3. <https://hackread.com/fake-ai-tools-noodlophile-stealer-facebook-ads/> - Scammers are leveraging fake AI tools and Facebook ads to spread the Noodlophile Stealer malware. Cybersecurity researchers at Morphisec identified a campaign where cybercriminals create convincing fake AI websites, advertised through Facebook groups, offering free AI video and image generation. Users are prompted to upload images, but instead, they download a malicious ZIP archive containing the Noodlophile Stealer. This malware steals browser credentials, cryptocurrency wallets, and can deploy remote access tools like XWorm. The campaign exploits the growing interest in AI, targeting creators and small businesses exploring AI tools.
4. <https://www.bleepingcomputer.com/news/security/fake-ai-editor-ads-on-facebook-push-password-stealing-malware/> - A Facebook malvertising campaign targets users searching for AI image editing tools, tricking them into installing fake apps that mimic legitimate software. Attackers exploit the popularity of AI-driven image-generation tools by creating malicious websites resembling legitimate services, leading users to download and install software that deploys the Lumma Stealer malware. This malware infiltrates systems, collecting sensitive information like credentials, cryptocurrency wallet files, browser data, and password manager databases, which is later sold to cybercriminals or used to compromise online accounts and steal funds.
5. <https://www.bitdefender.com/blog/labs/ai-meets-next-gen-info-stealers-in-social-media-malvertising-campaigns/> - Cybercriminals are actively spreading malware through Meta’s sponsored ad system by impersonating popular AI-based image and video generators. They hijack existing Facebook accounts, change descriptions and visuals to mimic well-known AI tools, and boost legitimacy with news and AI-generated content. Malicious ads prompt users to download software from links like Dropbox and Google Drive, leading to the deployment of information stealers such as Rilide Stealer, Vidar Stealer, IceRAT, and Nova Stealer. These malware variants monitor browsing history, capture login credentials, and facilitate cryptocurrency fund withdrawals by bypassing two-factor authentication.
6. <https://blog.deurainfosec.com/hackers-hijack-facebook-pages-to-mimic-ai-brands-inject-malware/> - Cybercriminals are hijacking Facebook pages to impersonate AI brands and inject malware. They take over existing accounts, modify them to appear as AI-based image and video generators, and populate them with AI-generated content and advertisements. Malicious posts promote fake AI tools, leading users to download software that deploys information stealers like Rilide Stealer V4. This malware targets Chromium-based browsers, monitoring browsing history, capturing login credentials, and facilitating cryptocurrency fund withdrawals by bypassing two-factor authentication through script injections. Users are advised to exercise caution and verify the legitimacy of AI tools before downloading.
7. <https://www.darkreading.com/cyberattacks-data-breaches/attackers-dangle-ai-based-facebook-ad-lures-to-hijack-business-accounts> - Attackers are using AI-based Facebook ad lures to hijack business accounts. Users who click on these ads are redirected to websites listing the advantages of large language models, containing links to download the 'AI package.' The attackers distribute the package as an encrypted archive, evading antivirus detection. Once decrypted, the package installs a Chrome extension designed to steal Facebook cookies, access tokens, and browser data, including managed pages, business account information, and advertisement account details. This campaign exploits the growing interest in AI to socially engineer malicious scams targeting business accounts.