

Warning campaign to spread malicious code through 'green tick' pages on Facebook

Malware advertising activities are distributed by hackers through compromised Facebook pages.

Back in May, Meta quietly released a security report on the latest malware-based threats targeting users on Facebook. With the emergence of AI and ChatGPT, long-standing malware strains, including Ducktail and NodeStealer, have gradually re-emerged and played a central role in the campaign against Facebook's ad system for distribution. unauthorized malware.

The implementation pattern is not complicated. Hackers will target verified (green ticked) Facebook pages, and rename them to be trusted brands like Facebook, Meta, Google AI, Bard, etc. These rebranded pages with The verified green tick is then used to run ads with links to malware.

The Meta side claims to have disrupted the operation of several strains of malware with the ability to quickly adapt in some attack campaigns. According to a Group-IB report, more than 3,200 pages and profiles on Facebook have been compromised to impersonate tech brands, including recently hot keywords like AI, ChatGPT and Bard. After two months of reduced presence, malware groups continue to wreak havoc on Facebook again with a new attack campaign.



AI Marketing

Sponsored · 🌐



!! Hot news

Researchers tested AiGoogle to create a marketing campaign with absolutely no human intervention. And the result was amazing, a perfect marketing campaign.

AiGoogle's latest update July 13 adds more features, languages, and countries.

PC version => <https://sites.google.com/view/ai-marketing-info>

AI increases marketing campaign performance 10x and will become the future of advertising, because AI knows how to identify and segment audiences, create ads, test ads, improve ad performance, and optimize spend—all automatically over time, real time, on a large scale. Use AI and become a technology pioneer today!



TipsMake



AI Marketing

Sponsored · 🌐



In the future AiGoogle will replace people in many professions.

Super Update 10/7, Aigoogole is smarter, learns faster, unlimited creative thinking, great support for content creators, businesses and advertisers.

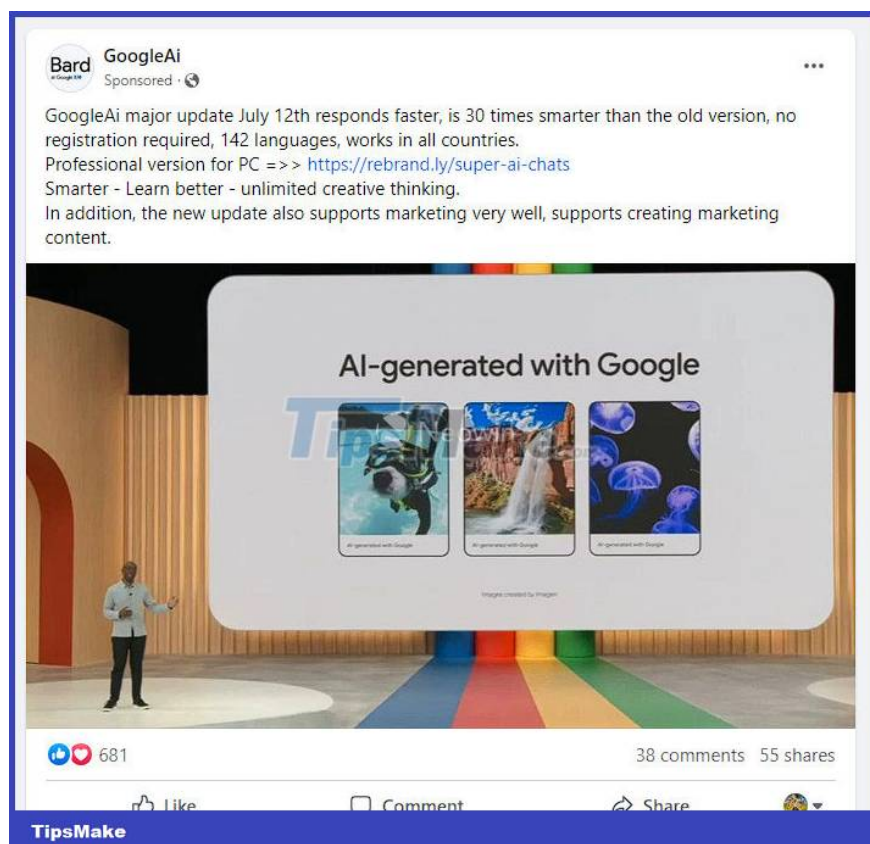
Version for PC => <https://sites.google.com/view/ai-marketing-info>

Support all languages in all countries.

Thousands of businesses have used Aigoogole to increase revenue and optimize efficiency, how about you?



TipsMake



This time, malware advertising activities were distributed by hackers through compromised Facebook pages. International security researchers recently discovered a group of these malicious ads that mimic Google. The ad contains a link to the download page hosted on the Google Sites platform. It includes a direct download link stored on DropBox to a RAR file, which is actually malware with a size of 4.26MB.

In fact, Chrome can detect malware during download and stop it before it can hit the device. However, the problem is that Windows Defender does not detect this software as malicious even when its installer is running on the system.

The screenshot below shows one of the malware websites hosted on site.google.com.

Helping Businesses with Generative AI

With more than 2.8 billion monthly users, Facebook is a powerful and potential advertising platform to reach potential customers. However, managing and optimizing a Facebook ad campaign can be a complicated task for advertisers. That's why GoogleAI Marketing was born to help businesses improve advertising efficiency and achieve better results.

[Download AiGoogle](#)
Setting code : 888

What is GoogleAI?

Google Bard, developed by Google AI, is a sophisticated chatbot powered by a large language model (LLM).

TipsMake

Search downloads

Today

BardAi Install.rar ✕
<https://dl.dropboxusercontent.com/s/2y8ku871z0umu30/BardAi%20Install.rar>
[Show in folder](#)

BardAi Install Properties

General Security Details Previous Versions

BardAi Install

Type of file: RAR File (.rar)

Opens with: **7-Zip File Manager** Change...

Location: D:\Downloads

Size: 4.26 MB (4,471,468 bytes)

Size on disk: 4.26 MB (4,472,832 bytes)

Created: Sunday, 30 July 2023, 6:04:00 pm

Modified: Sunday, 30 July 2023, 6:04:10 pm

Accessed: Today, 30 July 2023, 29 minutes ago

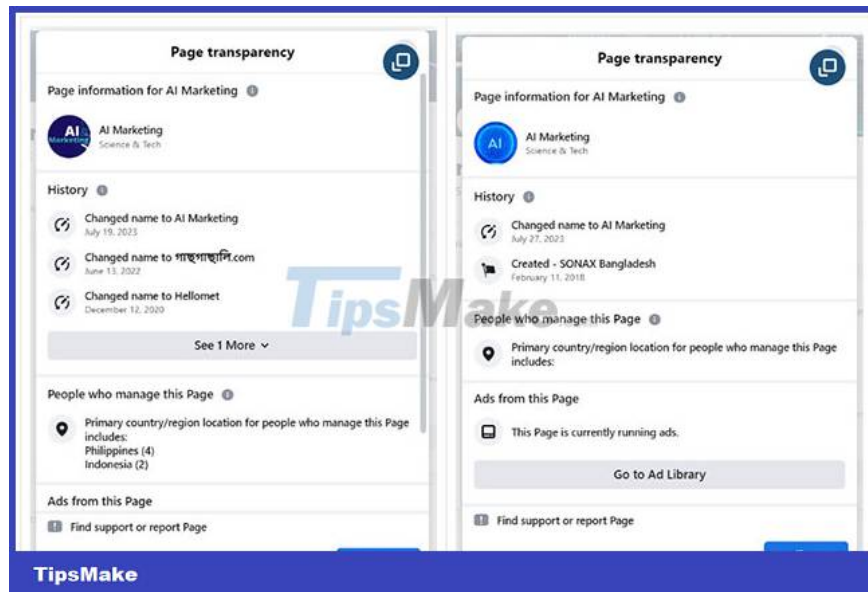
Attributes: Read-only Hidden Advanced...

Security: This file came from another computer and might be blocked to help protect this computer. Unblock

OK Cancel Apply

TipsMake

To limit users' exposure to malware and raise awareness, Facebook has added a "Page transparency" section to all pages to show history of name changes, country origin, and other details of the site. The two recently hacked sites "?????????" on July 19 and "SONAX Bangladesh" on July 27 were both renamed to AI Marketing.



At the moment, these pages are still active, the link to the malware is still available and is being hosted on DropBox. You should be wary of instant downloads with seemingly verified pages on Facebook. If you're unsure of the site's identity, you can navigate to the site's About section for details on the site's history and any past name changes.

You finished reading the article "**Warning campaign to spread malicious code through 'green tick' pages on Facebook**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.