One added line of code and thousands of companies hacked. This is the m

Data: 2025-09-27 06:52:28

Autor: Inteligência Against Invaders

Redazione RHC**:27 September 2025 08:50**

Developers learned to trust the tools that help their AI assistants handle routine tasks, from sending emails to using databases. But this trust proved vulnerable: **the postmark-mcp package, downloaded over 1,500 times a week since version 1.0.16, silently forwarded copies of all emails to an external server owned by its author** . Internal company correspondence, invoices, passwords, and confidential documents were at risk.

The incident demonstrated for the first time that **MCP servers can be used as a full-fledged conduit for supply chain attacks** . Researchers at Koi Security identified the issue when their system detected a sudden change in packet behavior.

An investigation revealed that **the developer had added a single line of code that automatically inserted a hidden BCC address and sent all messages to giftshop.club** . Fifteen releases had previously worked flawlessly, and the tool had become part of the workflows of hundreds of organizations.

The particular danger of the situation is underscored by the seemingly trustworthy nature of the author: *a public GitHub profile, real data, and projects with active histories* . For months, users had no reason to doubt its security. **But the update turned a familiar tool into a leak mechanism** . A classic hijacking played a key role: *npm added a clone of the Postmark repository, adding only a single line about forwarding.*

The extent of the damage is difficult to estimate, but estimates suggest that **hundreds of organizations were unknowingly sending thousands of emails a day to an external server.** No exploits or sophisticated techniques were used: *the administrators themselves granted full access to the AI assistants and allowed the new server to operate without restrictions.*

MCP tools have “god-mode” permissions: they can send emails, connect to databases, execute commands, and send API requests . However, they are not subject to security checks or vendor verification and are not included in the asset inventory. These modules remain invisible to corporate security.

This incident highlighted a fundamental flaw in the MCP architecture. Unlike regular packets, these are specifically designed for autonomous use by AI assistants. Machines are unable to recognize malicious code: to them, sending an email with an additional address appears to be a successful command execution. Therefore, a simple backdoor remains undetected and active until discovered.

Koi specialists recommend removing postmark-mcp version 1.0.16 and later, changing any credentials sent via email, and carefully checking logs for forwarding to giftshop.club. Furthermore, the company recommends **reconsidering the use of MCP servers in general:** *without independent verification, these tools become a primary attack vector for businesses.*

Indicators of compromise include the postmark-mcp package version 1.0.16 or later, the phan@giftshop[.]club address, and the giftshop[.]club domain. Verification is possible by analyzing email headers for hidden BCCs, verifying MCP configurations, and verifying npm installations.

Redazione
The editorial team of Red Hot Cyber consists of a group of individuals and anonymous sources who actively collaborate to provide early information and news on cybersecurity and computing in general.

Lista degli articoli