npm Package Uses QR Code Steganography to Steal Credentials - Against

Data: 2025-09-25 09:52:17

Autor: Inteligência Against Invaders

A malicious npm package named Fezbox has been found using an unusual technique to conceal

harmful code.

The package employs a QR code as part of its obfuscation strategy, ultimately aiming to steal usernames and passwords from web cookies.

The discovery was made by the Socket Threat Research Team.

A New Obfuscation Method

While attackers often rely on methods like string reversal, encoding or encryption to hide malware, Fezbox goes further by embedding a payload inside a QR code. Once activated, the code attempts to extract user credentials from browser cookies and transmit them to a remote server.

Socket flagged the package through its AI-based malware scanner, which identified suspicious behaviors hidden beneath seemingly harmless utility functions. The package, which had at least 327 downloads, has since been removed following Socket's petition to the npm security team for its takedown and the suspension of the associated account.

Read more on supply chain attacks: GhostAction Supply Chain Attack Compromises 3000+ Secrets

How the Payload Works

Fezbox presents itself as a JavaScript/TypeScript helper library with features like QR code generation.

The documentation does not disclose, however, that the library will fetch a QR code from a remote URL and execute whatever code is inside. After a 120-second delay, the malicious script loads and parses the QR code, then runs the hidden payload.

Once decoded, the payload attempts to:

- Retrieve a stored username and password from browser cookies
-

Reverse the string “drowssap” to disguise its intent

- Send the stolen credentials via HTTPS POST to a server hosted on Railway

According to Socket, the use of multiple obfuscation layers, including string reversal, QR code steganography and payload encryption, demonstrates the actor’s focus on stealth.

Lessons for Defenders

Although many modern applications no longer store plain passwords in cookies, the attack highlights the growing creativity in malware design.

“Using a QR code as a steganographic obfuscation technique is quite clever,” the Socket team noted, “[It] shows yet again that threat actors will continue to use any and all tools at their disposal.”

The company also emphasized the importance of automated dependency scanning to catch malicious packages before they are introduced into software projects.