Fezbox Malware: The NPM Package That Steals Cookies with QR Codes - A

Data: 2025-09-26 13:56:24

Autor: Inteligência Against Invaders

Redazione RHC**:26 September 2025 15:55**

Researchers discovered a malicious package called **fezbox** in **npm** that steals victims' cookies. To ensure the malicious activity remains undetected, *QR codes are used to download the malware from the attackers' server.*

According to Socket researchers, attackers have found *a new use for QR codes: hiding malicious code within them.* Analysts have reported that the packet contains hidden instructions to download a JPG image with a QR code, which is then processed to launch an obfuscated payload as part of the second stage of the attack.

At the time of the malware's discovery, the package had been downloaded at least **327 times before npm administrators removed it.** Bleeping Computer notes that the main malicious payload is located in the package's dist/fezbox.cjs file (using version 1.3.0 as an example). The code in the file has been minified and made easier to read after formatting.

The malware also checks whether the application is running in a development environment to evade detection *. "Attackers don't want to risk detection in a virtual or non-production environment, so they add restrictions on when and how their exploit operates,"* the researchers explain. *"If no issues are detected, after 120 seconds, it parses and executes the QR code at the address in the inverted string."*

The result, once logged in, is a URL. According to experts, **storing URLs in reverse order is a masquerade technique used to circumvent static analysis tools** that look for URLs (those starting with http(s)://) in the code.

Unlike the QR codes we typically encounter in real life, this one is unusually dense and contains much more data. As journalists noted, **it's impossible to read with a standard phone camera.** The attackers specifically crafted the QR code to transmit obfuscated code that can be parsed from the packet. The obfuscated payload reads the cookie via document.cookie .

The discovery of this malware **demonstrates a new approach to QR code abuse.** An infected computer can use them to communicate with its command and control server, while to a proxy server or network security tool, this will appear as normal image traffic.

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