Backdoors in Python and NPM Packages Target Windows and Linux

By Deeba Ahmed

Published: 2025-06-02 · Archived: 2026-04-05 18:19:32 UTC

New research from Checkmarx Zero has unveiled a unique malicious software campaign that targets Python and NPM users on both Windows and Linux systems.

Security researcher Ariel Harush at Checkmarx Zero has identified this troubling new trend in cyberattacks. According to their research, shared with Hackread.com, attackers are using typosquatting and name-confusion techniques to trick users into downloading harmful software.

Discover more

Antivirus & Malware

Computer Hardware

computers

What makes this campaign especially unusual is its *cross-ecosystem* approach. The malicious packages, uploaded to PyPI (Python Package Index), mimic the names of legitimate software from two different programming ecosystems: colorama (a popular Python tool for adding color to text in terminals) and colorizr (a similar JavaScript package found on NPM, the Node Package Manager). This means an attacker is using a name from one platform to target users of another, a rarely seen tactic.

The packages uncovered by Checkmarx Zero carried highly risky payloads, designed to give attackers lasting remote access and remote control over both desktops and servers. This allows them to “harvest and exfiltrate sensitive data,” meaning they can steal important information.

On Windows systems, the malware even attempts to bypass antivirus software to avoid being detected. Checkmarx also linked some of the Windows payloads to a GitHub account: `githubcom/s7bhme`.

For Linux users, the malicious packages were found to contain advanced backdoors that could establish encrypted connections, steal information, and maintain a hidden, long-term presence on affected systems.

The campaign, likely designed to attack specific targets, is currently untraceable due to the lack of clear attribution data, leaving it unclear whether it is linked to a well-known adversary.

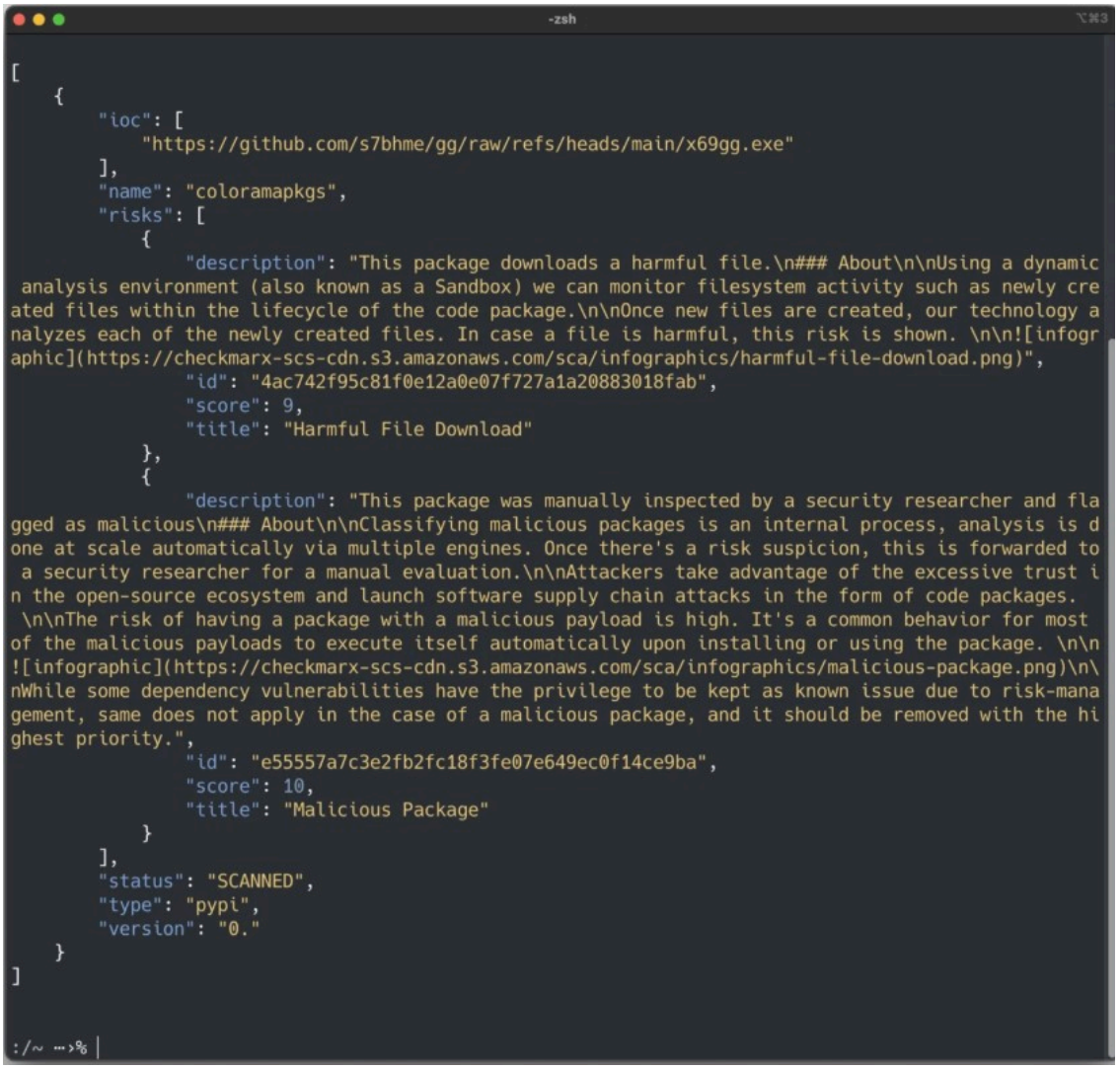
Thankfully, these specific malicious packages have been removed from public software repositories, which has limited their immediate potential for causing damage. Although the immediate threat has been contained, Checkmarx advises organizations to be ready for similar attacks.

Discover more

Software

Technology News

Scripting Languages



Query results for ‘coloramapkgs’ retrieved via the Checkmarx Threat Intelligence API

“By combining typo-squatting and related name confusion attacks, cross-ecosystem baiting, and multi-platform payloads, this attack serves as a reminder of how opportunistic and sophisticated open-source supply chain threats have become,” Checkmarx researchers noted in their blog post.

Researchers suggest checking all active and ready-to-use application code for any signs of these malicious package names. It is also crucial to inspect private software storage areas, like Artifactory, to remove any harmful packages and prevent their future installation.

Furthermore, companies should ensure that these types of dangerous packages aren’t installed on developer computers or in testing environments. These steps are vital for defending against such sophisticated open-source supply chain attacks.

Source: https://hackread.com/backdoors-python-npm-packages-windows-linux/