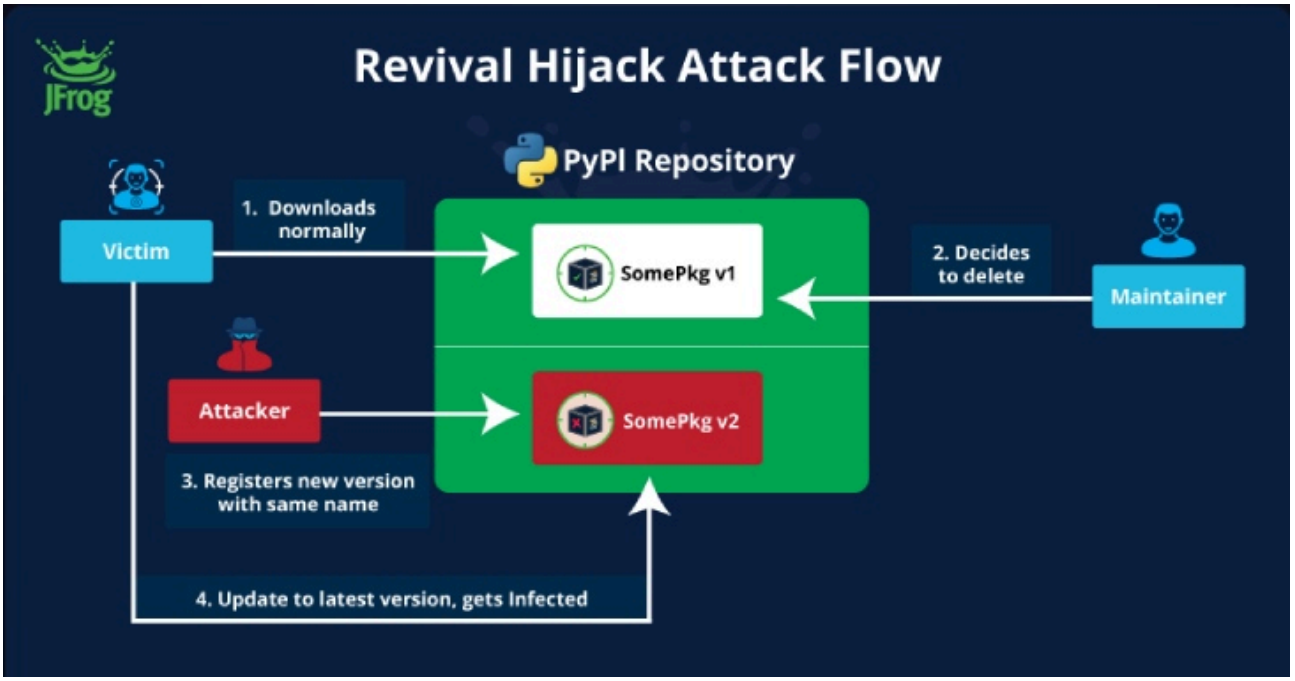
Researchers Find Over 22,000 Removed PyPI Packages at Risk of Revival Hijack

By The Hacker News

Published: 2024-09-04 · Archived: 2026-04-05 14:09:24 UTC



A new supply chain attack technique targeting the Python Package Index (PyPI) registry has been exploited in the wild in an attempt to infiltrate downstream organizations.

It has been codenamed Revival Hijack by software supply chain security firm JFrog, which said the attack method could be used to hijack 22,000 existing PyPI packages and result in "hundreds of thousands" of malicious package downloads. These susceptible packages have more than 100,000 downloads or have been active for over six months.

"This attack technique involves hijacking PyPI software packages by manipulating the option to re-register them once they're removed from PyPI's index by the original owner," JFrog security researchers Andrey Polkovnychenko and Brian Moussalli said in a report shared with The Hacker News.

At its core, the attack hinges on the fact that Python packages published in the PyPI repository may get removed, making available the names of those deleted projects for registration to any other user.

Statistics shared by JFrog show that about 309 packages are removed each month on average. These could happen for any number of reasons: Lack of maintenance (i.e., abandonware), package getting re-published under a different name, or introducing the same functionality into official libraries or built-in APIs.

This also poses a lucrative attack surface that's more effective than typosquatting and which an attacker, using their own accounts, could exploit to publish malicious packages under the same name and a higher version to infect developer environments.

"The technique does not rely on the victim making a mistake when installing the package," the researchers said, pointing out how Revival Hijack can yield better results from the point of view of an adversary. "Updating a 'once safe' package to its latest version is viewed as a safe operation by many users."

While PyPI does have safeguards in place against author impersonation and typosquatting attempts, JFrog's analysis found that running the "pip list --outdated" command lists the counterfeit package as a new version of the original package, wherein the former corresponds to a different package from an entirely different author.

Even more concerning, running the "pip install –upgrade" command replaces the actual package with the phony one without not so much of a warning that the package's author has changed, potentially exposing unwitting developers to a huge software supply chain risk.

JFrog said it took the step of creating a new PyPI user account called "security_holding" that it used to safely hijack the susceptible packages and replace them with empty placeholders so as to prevent malicious actors from capitalizing on the removed packages.

Additionally, each of these packages has been assigned the version number as 0.0.0.1 – the opposite of a dependency confusion attack scenario – to avoid getting pulled by developers when running a pip upgrade command.

What's more disturbing is that Revival Hijack has already been exploited in the wild, with an unknown threat actor called Jinnis introducing a benign version of a package named "pingdomv3" on March 30, 2024, the same day the original owner (cheneyyan) removed the package from PyPI.

On April 12, 2024, the new developer is said to have released an update containing a Base64-encoded payload that checks for the presence of the "JENKINS_URL" environment variable, and if present, executes an unknown next-stage module retrieved from a remote server.

"This suggests that the attackers either delayed the delivery of the attack or designed it to be more targeted, possibly limiting it to a specific IP range," JFrog said.

The new attack is a sign that threat actors are eyeing supply chain attacks on a broader scale by targeting deleted PyPI packages in order to expand the reach of the campaigns. Organizations and developers are recommended to

inspect their DevOps pipelines to ensure that they are not installing packages that have been already removed from the repository.

"Using a vulnerable behavior in the handling of removed packages allowed attackers to hijack existing packages, making it possible to install it to the target systems without any changes to the user's workflow," said Moussalli, JFrog Security Research Team Lead.

"The PyPI package attack surface is continually growing. Despite proactive intervention here, users should always stay vigilant and take the necessary precautions to protect themselves and the PyPI community from this hijack technique."

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.
