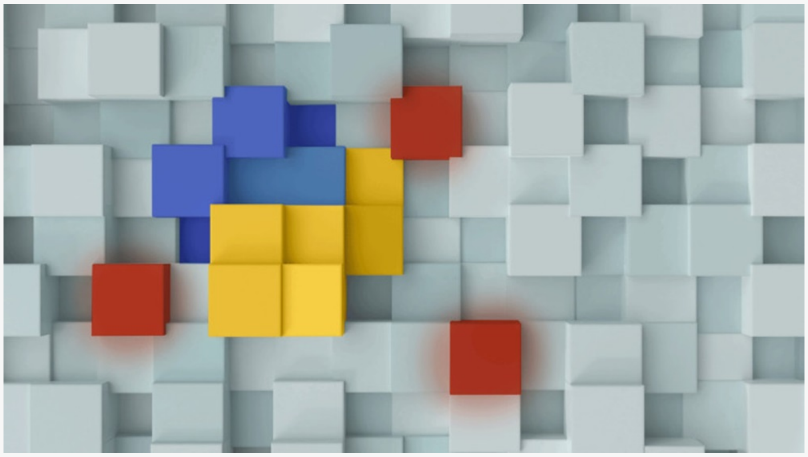
EINPRESSWIRE

ESET Research: Official Python repository served cyberespionage backdoor, gathered 10,000+ downloads



DUBAI , DUBAI, UNITED ARAB EMIRATES, December 27, 2023 /EINPresswire.com/ -- ESET Research has discovered a cluster of malicious Python projects being distributed via PyPI, the official Python (programming language) package repository. The threat targets both Windows and Linux systems and usually delivers a custom backdoor with cyberespionage capabilities. It allows remote command execution and file exfiltration, and sometimes includes the ability to take screenshots. In some cases, the final payload is a variant of the infamous W4SP Stealer, which steals personal data and credentials, or a simple clipboard monitor to steal cryptocurrency, or both. ESET discovered 116 files (source distributions and wheels) across 53 projects that contain malware. Over the past year, victims downloaded these files more than 10,000 times. From May 2023 onward, the download rate was around 80 per day.

PyPI is popular among Python programmers for sharing and downloading code. Since anyone can contribute to the repository, malware – sometimes posing as legitimate, popular code libraries – can appear. “Some malicious package names do look similar to other, legitimate packages, but we believe the main way they are installed by potential victims isn’t via typosquatting, but social engineering, where they are walked through running pip to install an ‘interesting’ package for whatever reason,” says ESET researcher Marc-Étienne Léveillé, who discovered and analyzed the malicious packages.

Most of the packages had already been taken down by PyPI at the time of the publication of this research. ESET has communicated with PyPI to take action concerning those remaining; presently, all of the known malicious packages are offline.

ESET has observed the operators behind this campaign using three techniques to bundle malicious code into the Python packages. The first technique is to place a “test” module with lightly obfuscated code inside the package. The second technique is to embed PowerShell code in the setup.py file, which is typically run automatically by package managers such as pip to help install Python projects. In the third technique, the operators make no effort to include legitimate code in the package, so that only the malicious code is present, in a lightly obfuscated form.

Typically, the final payload is a custom backdoor capable of remote command execution, file exfiltration, and sometimes the ability to take screenshots. On Windows, the backdoor is implemented in Python. On Linux, the backdoor is implemented in the Go programming language. In some cases, a variant of the infamous W4SP Stealer is used instead of the backdoor, or a simple clipboard monitor is used to steal cryptocurrency, or both. The clipboard monitor targets Bitcoin, Ethereum, Monero, and Litecoin cryptocurrencies.

“Python developers should vet the code they download before installing it on their systems. We expect that such abuse of PyPI will continue and advise caution in installing code from any public software repository,” concludes Léveillé.

For more information about the malicious Python projects in PyPI, check out the blog post “A pernicious potpourri of Python packages in PyPI.” Make sure to follow ESET Research on Twitter (today known as X) for the latest news from ESET Research.

About ESET
For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET’s high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET’s R&D centers worldwide, working in support of our shared future. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and X (Twitter).

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here