All VSCode users need to be wary of malicious extensions!

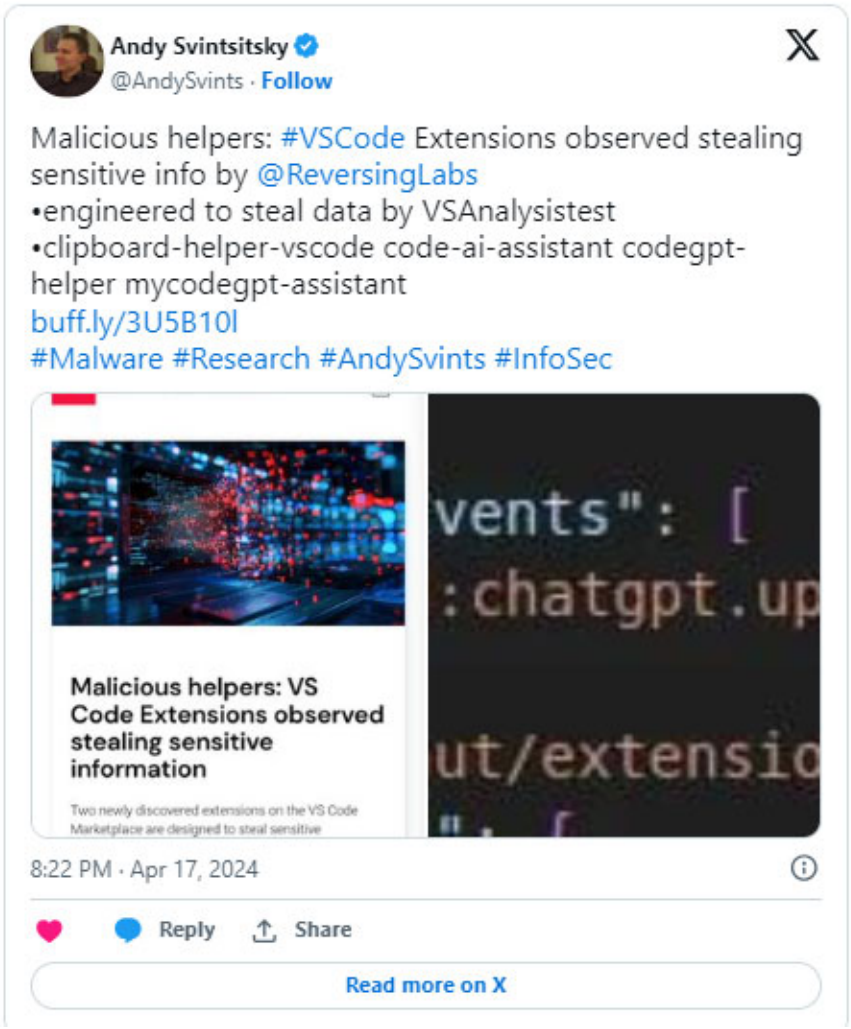
Extending the functionality of your favorite programs with extensions is great, if the extensions work properly and the extension store isn't full of potential dangers.

That's exactly what happened with Microsoft's Visual Studio Code extension store, where tons of malicious extensions are waiting for you to click and install if you're not paying attention.

What is malicious VSC extension?

Malicious VSC extensions often impersonate other, more popular extensions or promise to add new functionality to motivate people to install them. Once installed and activated, they can do anything from tampering with VSC settings to stealing data from computers.

VSC extensions themselves are not the problem. The ability to add extensions to further enhance VSC's utility is what makes it one of the most popular code editors today. However, since installed extensions often have unrestricted access to the VSC installation and to some extent to the PC, this also makes them the perfect vehicle for attackers to inject a malware onto your PC. In a world where scammers can even use your face to commit fraud, it's best to be cautious.



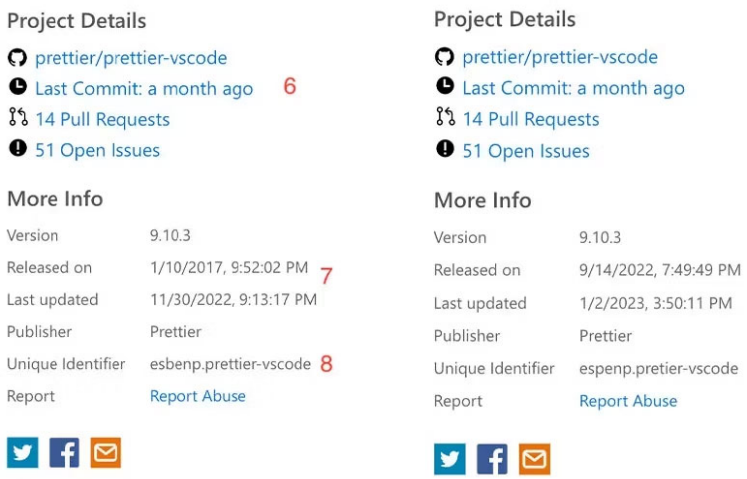
These malicious extensions can be anything from simple data theft tools that can steal Personally Identifiable Information (PII) from a computer to making the machine part of a botnet used to carry out DDoS attacks or spread malware. Additionally, as supply chain attacks become more common, they also open the door to much more serious malware testing, especially considering the multiple VSC installations on devices. related to the work that programmers use while working for their respective organizations.

Security researchers Amit Assaraf, Itay Kruk and Idan Dardikman's deep dive into malicious extensions on the VSC market revealed some interesting statistics:

1. 1,283 extensions with a total of 229 million installations include known malicious dependencies.
2. 87 extensions attempted to read the /etc/passwd file on the host system. This file stores system passwords and other sensitive information.
3. 8,161 extensions communicate using hardcode.
4. 1,452 extensions run unknown binary files or executable DLLs on the server.
5. 267 have hardcoded secrets embedded into them.
6. The code and dependencies of 145 extensions have been confirmed to be highly reliable by VirusTotal.
7. 2,304 extensions are using another publisher's GitHub repository as their official repository.
8. 783 extensions were found to use third-party AI models.

While these numbers don't necessarily indicate malicious activity for every included extension, they raise enough suspicion to make anyone think twice before installing them.

A previous report by security researchers Ilay Goldman and Yakir Kadkoda for AquaSec found similar patterns, with malicious extensions hiding as copies of regular extensions. For example, in the image below, the details on the left belong to the real extension, while the details on the right are from the malicious extension trying to imitate the original extension.



This image also perfectly illustrates why malware in the VSC marketplace is a problem. Almost anyone can upload to the extension and point its information wherever they want, whether it's misleading or malicious.

How do malicious extensions appear on VSC Marketplace?

There are several ways that malicious extensions can appear on the VSC marketplace. However, the two most popular methods are as follows.

Typosquatting

Typosquatting is a technique in which an attacker uses typos of a commonly used program or in this case an extension to distribute a fake program. For example, if you are searching for an extension named "Programmer", a bad actor could create a malicious extension named "Programmerr" or "Programer" and trick you into downloading it.

They often contain data stealers or other malware and can seriously harm your PC. That's actually a mistake that all of us can make sometimes and that costs us dearly.

Fake extensions

As the name suggests, these extensions promise functionality to spoof or impersonate other, more popular extensions to get you to install them. Once installed, they are either obviously inactive or provide some functionality while mainly focusing on PC control or data theft.

This is a fairly common way of distributing malware, and scammers often use the names of large corporations with verified accounts to make their malware appear legitimate. Even the Google Bard app is distributed as

malware using a similar approach.

You finished reading the article "**All VSCode users need to be wary of malicious extensions!**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.