New Campaign Delivers Vidar, Lumma, Atomic, and Octo Malware via GitHub and FileZilla

DUBAI , DUBAI, UNITED ARAB EMIRATES, May 29, 2024 /EINPresswire.com/ -- ANY.RUN reports that a new malware campaign has been discovered, exploiting legitimate services such as GitHub and FileZilla to deliver a variety of malware targeting Windows, macOS, and Android users.

The campaign uses multiple stealers, and researchers believe that the different malware families are being centrally controlled from a shared C2.

The campaign impersonates popular software such as 1Password, Bartender 5, and Pixelmator Pro on GitHub and FileZilla. The campaign distributes Vidar, Lumma, Atomic and Octo. Possibly, more malware families are involved.

The attack chain includes malvertising and SEO poisoning to drive victims to fake repositories that are disguised as legitimate software but actually contain malware-infected applications. This tactic of exploiting trusted services to distribute malware has gained popularity recently: a packed version of Redline distributed via GitHub was spotted in April 2024, and in March hackers used GitHub to distribute the STRRAT and VCURMS remote access trojans.

According to the ANY.RUN Malware Trends Tracker, which aggregates data from 400,000 researchers, Vidar's detections have spiked at the time of writing, making it the most common malware in the tracker.

ANY.RUN is an interactive analysis sandbox that helps analysts analyze how malware behaves

after it has infected a system. For example, by running a Lumma sample in the sandbox, analysts can learn that when executed, it injects itself into the BitLockerToGo system process to evade process-based defenses and potentially elevate privileges. Information like this can help to properly configure security systems to protect against these threats.

Learn more about the story in ANY.RUN's blog.

Veronika Trifonova
ANYRUN FZCO
+1 657-366-5050
email us here
Visit us on social media:
X
YouTube
