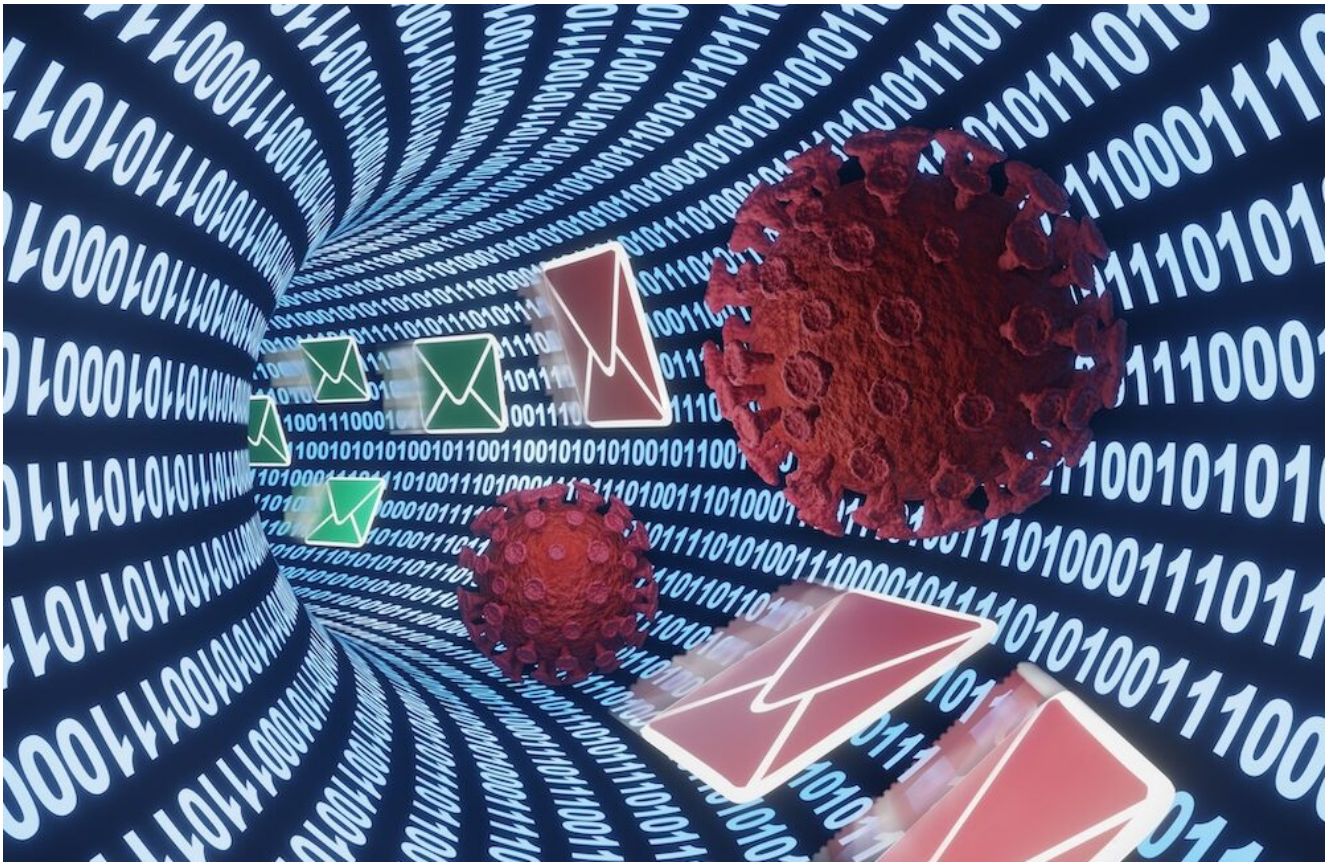
Destructive malware available in NPM repo went unnoticed for 2 years



Some of the payloads were limited to detonate only on specific dates in 2023, but in some cases a phase that was scheduled to begin in July of that year was given no termination date. Pandya said that means the threat remains persistent, although in an email he also wrote: “Since all activation dates have passed (June 2023–August 2024), any developer following normal package usage today would immediately trigger destructive payloads including system shutdowns, file deletion, and JavaScript prototype corruption.”

Interestingly, the NPM user who submitted the malicious packages, using the registration email address 1634389031@qq[.]com, also uploaded working packages with no malicious functions found in them. The approach of submitting

both harmful and useful packages helped create a “facade of legitimacy” that increased the chances the malicious packages would go unnoticed, Pandya said. Questions emailed to that address received no response.

The malicious packages targeted users of some of the largest ecosystems for JavaScript developers, including React, Vue, and Vite. The specific packages were:

Anyone who installed any of these packages should carefully inspect their systems to make sure they’re no longer running. These packages perfectly mimic legitimate development tools, so it may be easy for them to have remained undetected.

https://arstechnica.com/information-technology/2025/05/destructive-malware-available-in-npm-repo-went-unnoticed-for-2-years/