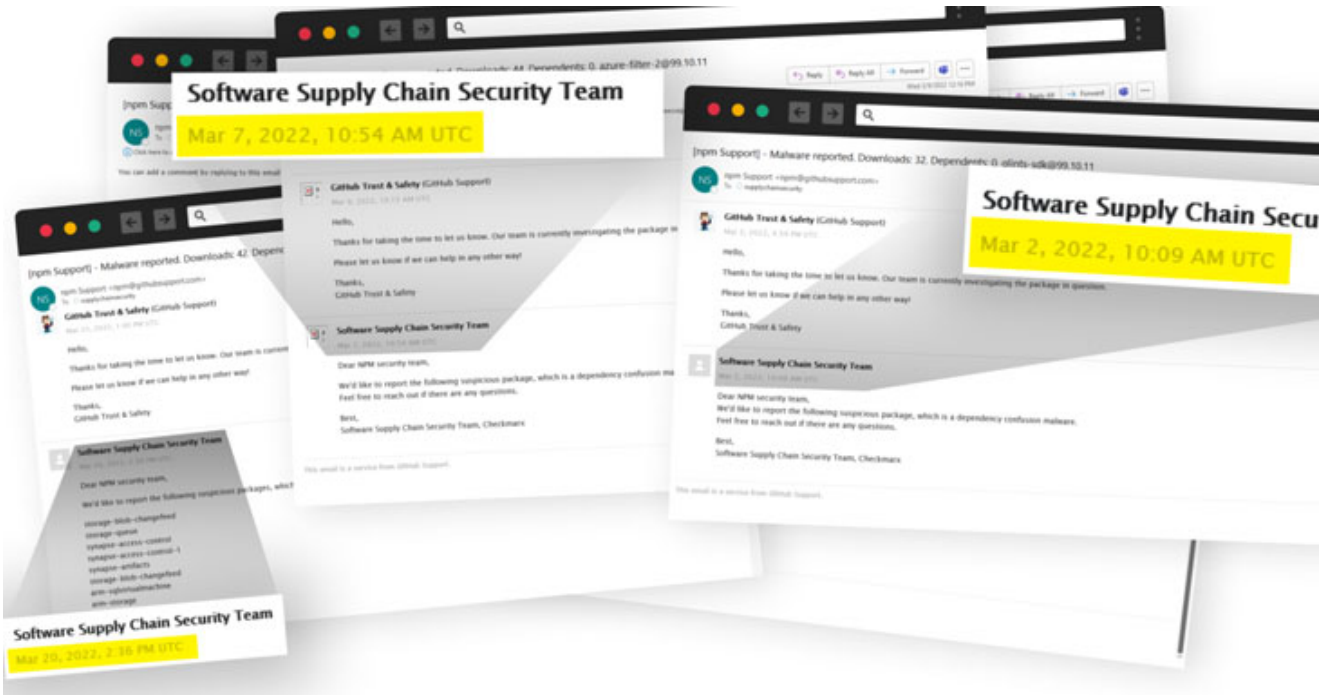
A Large-Scale Supply Chain Attack Distributed Over 800 Malicious NPM Packages

thehackernews.com/2022/03/a-threat-actor-dubbed-red-lili-has-been.html

March 29, 2022



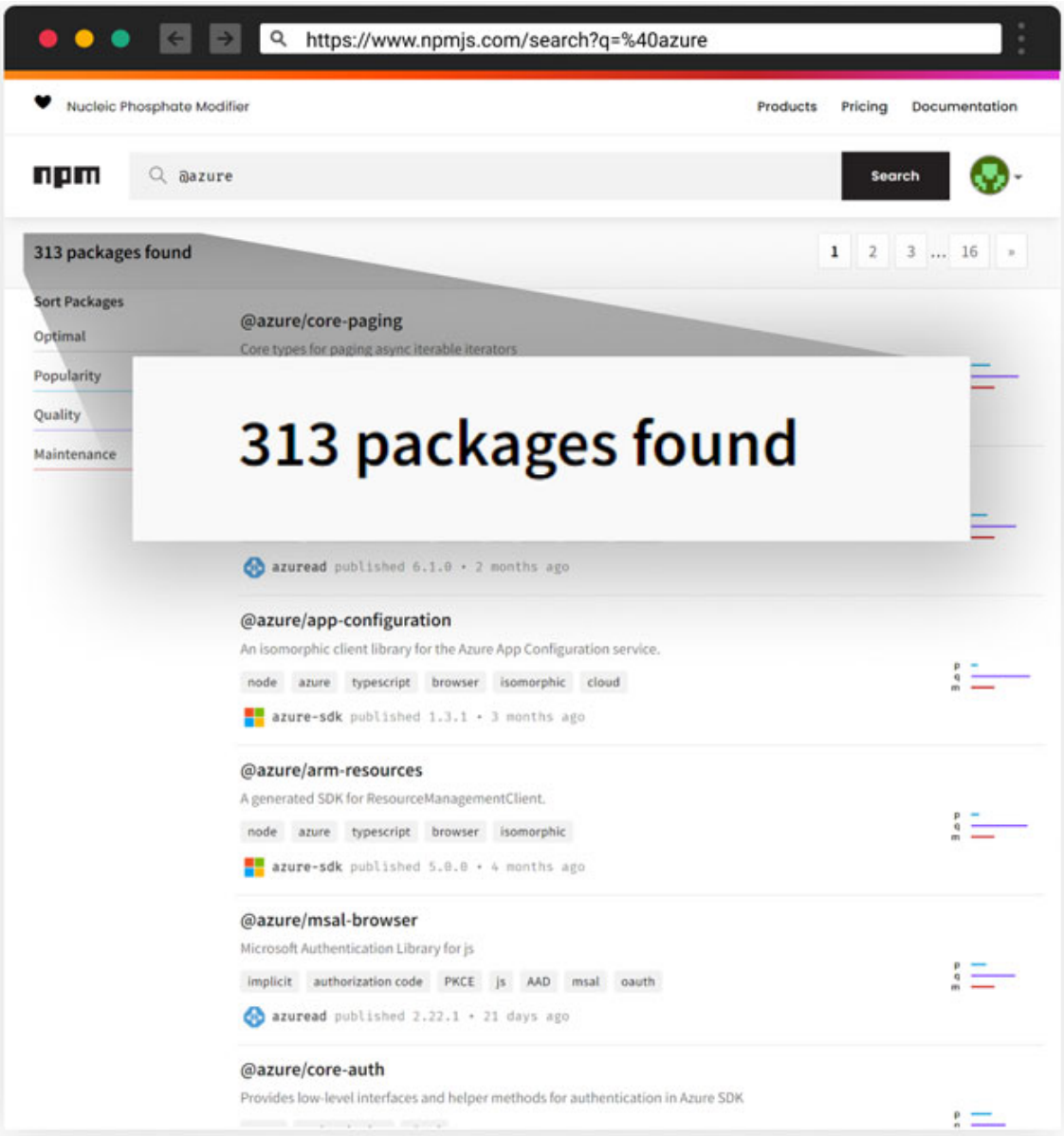
A threat actor dubbed "**RED-LILI**" has been linked to an ongoing large-scale supply chain attack campaign targeting the NPM package repository by publishing nearly 800 malicious modules.

"Customarily, attackers use an anonymous disposable NPM account from which they launch their attacks," Israeli security company Checkmarx said. "As it seems this time, the attacker has fully-automated the process of NPM account creation and has opened dedicated accounts, one per package, making his new malicious packages batch harder to spot."

The findings build on recent reports from JFrog and Sonatype, both of which detailed hundreds of NPM packages that leverage techniques like dependency confusion and typosquatting to target Azure, Uber, and Airbnb developers.

According to a detailed analysis of RED-LILI's modus operandi, earliest evidence of anomalous activity is said to have occurred on February 23, 2022, with the cluster of malicious packages published in "bursts" over a span of a week.

Specifically, the automation process for uploading the rogue libraries to NPM, which Checkmarx described as a "factory," involves using a combination of custom Python code and web testing tools like Selenium to simulate user actions required for replicating the user creation process in the registry.



To get past the one-time password (OTP) verification barrier put in place by NPM, the attacker leverages an open-source tool called Interactsh to extract the OTP sent by NPM servers to the email address provided during sign-up, effectively allowing the account creation request to succeed.

Armed with this brand new NPM user account, the threat actor then proceeds to create and publish a malicious package, only one per account, in an automated fashion, but not before generating an access token so as to publish the package without requiring an email OTP challenge.

"As supply chain attackers improve their skills and make life harder for their defenders, this attack marks another milestone in their progress," the researchers said. "By distributing the packages across multiple usernames, the attacker makes it harder for defenders to correlate [and] take them all down with 'one stroke.' By that, of course, making the chances of infection higher."

SHARE □ □ □ □ □
SHARE □