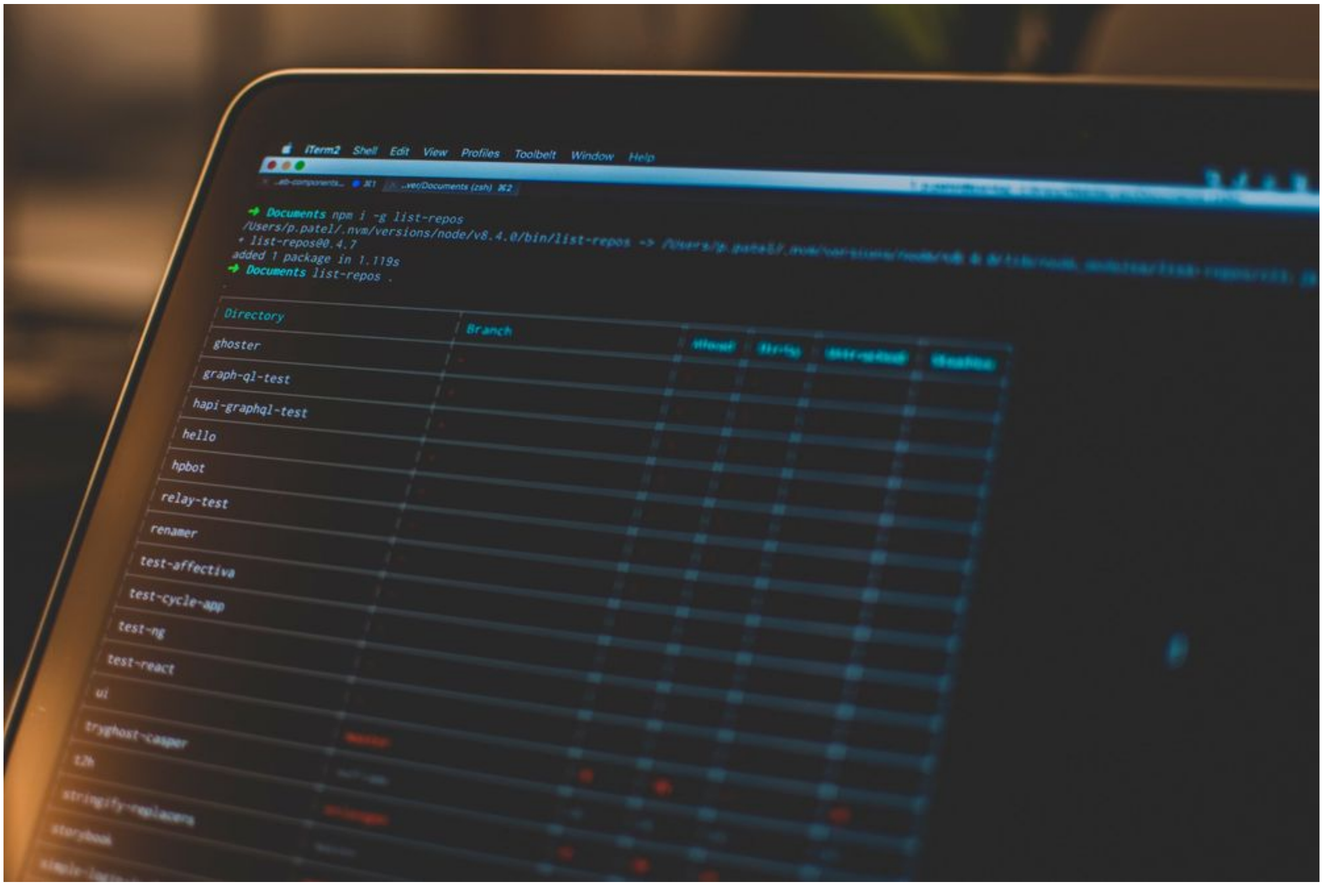
Popular NPM Repositories Compromised in Man-in-the-Middle Attack

bitdefender.com/blog/hotforsecurity/popular-npm-repositories-compromised-in-man-in-the-middle-attack/

Industry News
2 min read

Silviu STAHIE
November 08, 2021



```
➜ Documents npm i -g list-repos
/Users/p.patel/.nvm/versions/node/v8.4.0/bin/list-repos ->
+ list-repos@0.4.7
added 1 package in 1.119s
➜ Documents list-repos .

Directory                      Branch
ghoster
graph-ql-test
hapi-graphql-test
hello
hpbot
relay-test
renamer
test-affectiva
test-cycle-app
test-ng
test-react
ui
tryghost-casper
t2h
stringify-replacers
storybook
```

Unknown hackers compromised two NPM repositories that have been used by millions of people in the past, trying to establish the foundation of a man-in-the-middle attack and deploying a banking trojan.

We’re used to hearing about hackers compromising networks and apps, or simply deploying malware through various other methods, but man-in-the-middle attacks might not seem all that common. Unfortunately, just because they don’t often make the news doesn’t mean they’re rare. Compromising libraries or apps before they reach consumers leaves few traces and can take a long time before it’s discovered.

In this case, NPM issued an advisory warning people that a couple of libraries, ‘coa’ and ‘rc’ have been compromised and infected with malware.

“The npm package coa had versions published with malicious code. Users of affected versions (2.0.3 and above) should downgrade to 2.0.2 as soon as possible and check their systems for suspicious activity,” stated NPM on GitHub. A similar advisory is available for the ‘rc’ package.

“Any computer that has this package installed or running should be considered fully compromised. All secrets and keys stored on that computer should be rotated immediately from a different computer. The package should be removed, but as full control of the computer may have been given to an outside entity, there is no guarantee that removing the package will remove all malicious software resulting from installing it,” NPM added.

The malware attackers deployed seem to be a DanaBot variant, allowing criminals to capture and download information from victims' devices.

Unlike typosquatting attacks, in which criminals create infected libraries with names very similar to the official ones, the attackers managed to compromise the official repositories and replace the files. That's why the NPM team issued a statement on Twitter explaining what likely happened.

"This morning we detected multiple versions of the "coa" package published with malicious code due to a compromised account of a maintainer," said the team. "We quickly removed the compromised versions […] and the compromised account has been temporarily disabled."

They also advised other maintainers to enable multi-factor authentication as soon as possible, indicating the likely path taken by attackers to compromise the repositories.

TAGS

industry news

AUTHOR

Silviu STAHIE

Silviu is a seasoned writer who followed the technology world for almost two decades, covering topics ranging from software to hardware and everything in between.

View all posts