WIKIPEDIA
The Free Encyclopedia

WIKIPEDIA

npm left-pad incident

On March 22, 2016, software engineer Azer Koçulu took down the `left-pad` package that he had published to npm (a JavaScript package manager). Koçulu deleted the package after a dispute with Kik Messenger, in which the company forcibly took control of the package name `kik`. As a result, thousands of software projects that used `left-pad` as a dependency, including the Babel transcompiler and the React web framework, were unable to be built or installed. This caused widespread disruption, as technology corporations small and large, including Facebook, PayPal, Netflix and Spotify, used `left-pad` in their software products.

Several hours after the package was removed from npm, the company behind the platform, npm, Inc, manually restored the package. Later, npm disabled the ability to remove a package if more than 24 hours have elapsed since its publishing date and at least one other project depends on it. The incident drew widespread media attention and reactions from people in the software industry. The removal of `left-pad` has prompted discussion regarding the intentional self-sabotage of software to promote social justice and brought attention to the elevated possibility of supply chain attacks in modular programming.

Background

`left-pad` was a free and open-source JavaScript package published by Azer Koçulu, an independent software engineer based in Oakland, California.[1] The package repetitively prepends characters to a string using a loop.[1] `left-pad` has been characterized as being extremely simple, consisting of only 11 lines of code (when empty lines are discounted) in the final version authored by Koçulu.[2][3]

Koçulu published `left-pad` on npm, the default package manager for Node.js, a JavaScript runtime environment.[4][2] Despite its relative obscurity, `left-pad` was heavily used; the package was used as a dependency by thousands of other software projects and reached over 15 million downloads prior to its removal.[5][6] Some of the projects that required `left-pad` to function were critical to the JavaScript ecosystem at the time. This included Babel, a transcompiler that enables backwards-compatible JavaScript code, Webpack, a module bundling system, and both React and React Native, which are

```
 1   module.exports = leftpad;
 2
 3   function leftpad (str, len, ch) {
 4     str = String(str);
 5
 6     var i = -1;
 7
 8     ch || (ch = ' ');
 9     len = len - str.length;
10
11
12     while (++i < len) {
13       str = ch + str;
14     }
15
16     return str;
17   }
```

Contents of `left-pad` at the time of its npm removal

frameworks widely used for the

development of [websites](#) and [mobile apps](#), respectively.[7][8][1]

In addition to `left-pad`, Koçulu also owned `kik` on npm, which was a tool that allowed developers to set up templates for their projects.[1] On March 11, 2016, Kik Interactive, a Canadian company owning the [instant messaging](#) platform [Kik Messenger](#), contacted Koçulu, requesting that he relinquish control of the `kik` package due to the company's ownership of the "Kik" [trademark](#). [9] Part of the correspondence included the following message from Kik:

> We don't mean to be a dick about [the `kik` package], but it's a registered Trademark in most countries around the world and if you actually release an open source project called kik, our trademark lawyers are going to be banging on your door and taking down your accounts and stuff like that—and we'd have no choice but to do all that because you have to enforce trademarks or you lose them. Can we not come to some sort of a compromise to get you to change the name without involving lawyers? Is there something we could do for you in compensation to get you to change the name?[3]

Koçulu responded shortly after, refusing to change the name of his project, saying:

> hahah, you're actually being a dick. so, fuck you. don't e-mail me back.[3]

Koçulu also requested US$30,000 as compensation "for the hassle of giving up with my pet project for [*sic*] bunch of corporate dicks".[1] On March 18, 2016, Isaac Z. Schlueter, the chief executive officer of npm, Inc., wrote to both Kik Interactive and Koçulu, stating that the ownership of the `kik` package would be manually transferred to Kik Interactive.[1]

Removal

After Koçulu expressed his disappointment with npm, Inc.'s decision and stated that he no longer wished to be part of the platform, Schlueter provided him with a command to delete all 273 modules that he had registered.[9] Koçulu executed the command on March 22, 2016, removing every package he had previously released.[1] `left-pad` was one of the packages that was "unpublished", rendering it no longer publicly accessible on npm.[5] The `left-pad` software project and contents remained available on [GitHub](#).[9]

Users attempting to [build](#) or install any JavaScript project that used `left-pad` as a dependency (including dependents such as Babel or Webpack) received a [404 error](#) that caused the process to fail.[1] Notable software technology corporations used the package, including [Meta Platforms](#), [PayPal](#), [Netflix](#) and [Spotify](#).[8] Kik Interactive's developers themselves faced build problems as a result of the package's removal.[1]

Aftermath

Immediate effects

An hour after he deleted the packages, Koçulu published a post on Medium ("I've Just Liberated My Modules"), explaining that he had unpublished his software projects from npm to protest corporate interests in free and open-source software.[1]

Soon after the deletion, other software developers began to post a flood of complaints, reactions, and workarounds on the project's Git issue tracking system.[7][1]

Maintainers of open-source projects, including Babel, released hotfixes to remove the dependencies that Koçulu had unpublished.[7] Several of Koçulu's other package names were quickly taken over by newly published packages.[3] For example, another developer recreated the `left-pad` package—but released it as version 1.0.0. Since Koçulu published his as version 0.0.3, users continued to encounter problems.[3]

Around two hours after the original `left-pad` package was removed, npm manually "un-un-published" the original 0.0.3 version by restoring a backup.[1] Laurie Voss, chief technology officer of npm, wrote that the company "picked the needs of the many" despite internal disagreements about whether the action was "the right call".[10]

Reactions

npm changed its policy on the removal of published packages to prevent deletion if more than 24 hours have elapsed since its release date and at least one other project requires it as a dependency.[11] On behalf of npm, community manager Ashley Williams apologized for the disruption caused by the incident, stating that the platform "[failed] to protect the community".[11] Kik Interactive also apologized for the incident, with the company's head of messaging Mike Roberts publishing the email chain with Koçulu on Medium and characterizing his interaction as a "polite request".[8] Roberts wrote that they had initially reached out to Koçulu because they wished to publish an open-source package on npm with the name Koçulu was using.[5] Koçulu stated that he was sorry for disrupting other's work, but he believed he did it "for the benefit of the community in [*sic*] long term".[2]

The incident drew varied reactions from users on Twitter, GitHub, Reddit and Hacker News, with many claiming that it briefly "broke the Internet".[2][8][9][1] Many commented on the "move fast and break things" culture of JavaScript development, the unpredictable nature of open-source software, and a perceived over-reliance on modular programming.[2][8][3] Users also expressed disappointment regarding npm's decision to forcefully transfer Koçulu's package to Kik Interactive over a legal threat.[1]

Impact

The incident showed how the disruption of an npm package could lead to a supply chain attack. In addition to the widely publicized `left-pad` incident, a number of individuals had immediately hijacked Koçulu's other packages with unknown code after they were removed.[7] npm released a new policy to prevent malicious takeovers in similar disputes,[3] but the `left-pad` incident is still

cited as an example of over-reliance on external contributors leading to an increased <u>attack surface</u> for software products.[12] Koçulu's intentional self-sabotage of `left-pad` to highlight a social issue has also been described as a precursor to incidences of <u>protestware</u> being published on platforms like npm.[6]

See also

- <u>Hacktivism</u> – Computer-based activities as a means of protest
- <u>peacenotwar</u> – Malware
- <u>Software repository</u> – Storage location for software packages

References

1. Collins, Keith (March 27, 2016). "How one programmer broke the internet by deleting a tiny piece of code" (https://qz.com/646467/how-one-programmer-broke-the-internet-by-deleting-a-tiny-piece-of-code). *Quartz*. Archived (https://web.archive.org/web/20240511142121/https://qz.com/646467/how-one-programmer-broke-the-internet-by-deleting-a-tiny-piece-of-code) from the original on May 11, 2024. Retrieved May 11, 2024.

2. Weinberger, Matt (March 23, 2016). "One programmer almost broke the internet by deleting 11 lines of code" (https://www.businessinsider.com/npm-left-pad-controversy-explained-2016-3). *Business Insider*. Archived (https://web.archive.org/web/20240511182241/https://www.businessinsider.com/npm-left-pad-controversy-explained-2016-3) from the original on 11 May 2024. Retrieved 11 May 2024.

3. Feldman, Brian (March 24, 2016). "One Man Deleted 11 Lines of Code From the Internet and Broke Hundreds of Apps" (https://nymag.com/intelligencer/2016/03/how-11-lines-of-code-broke-tons-sites.html). *Intelligencer*. Archived (https://web.archive.org/web/20240511152254/https://nymag.com/intelligencer/2016/03/how-11-lines-of-code-broke-tons-sites.html) from the original on May 11, 2024. Retrieved May 11, 2024.

4. Claburn, Thomas (April 22, 2019). "NPM is Not Particularly Magnanimous? Staff fired after trying to unionize – complaints" (https://www.theregister.com/2019/04/22/npm_fired_staff_union_complaints/). *The Register*. Archived (https://web.archive.org/web/20240511150602/https://www.theregister.com/2019/04/22/npm_fired_staff_union_complaints/) from the original on May 11, 2024. Retrieved May 11, 2024.

5. Williams, Chris (March 23, 2016). "How one developer just broke Node, Babel and thousands of projects in 11 lines of JavaScript" (https://www.theregister.com/2016/03/23/npm_left_pad_chaos/). *The Register*. Archived (https://web.archive.org/web/20231016134656/https://www.theregister.com/2016/03/23/npm_left_pad_chaos/) from the original on October 16, 2023. Retrieved May 11, 2024.

6. Sharma, Ax (July 27, 2022). "Protestware on the rise: Why developers are sabotaging their own code" (https://techcrunch.com/2022/07/27/protestware-code-sabotage/). *TechCrunch*. Archived (https://web.archive.org/web/20240229175547/https://techcrunch.com/2022/07/27/protestware-code-sabotage/) from the original on February 29, 2024. Retrieved May 11, 2024.

7. Mazaika, Ken (March 24, 2016). "How 17 Lines of Code Took Down Silicon Valley's Hottest Startups" (https://www.huffpost.com/entry/how-17-lines-of-code-took_b_9532846). *HuffPost*. Archived (https://web.archive.org/web/20240511161012/https://www.huffpost.com/entry/how-17-lines-of-code-took_b_9532846) from the original on May 11, 2024. Retrieved May 11, 2024.

8. Miller, Paul (March 24, 2016). "How an irate developer briefly broke JavaScript" (https://www.th everge.com/2016/3/24/11300840/how-an-irate-developer-briefly-broke-javascript). *The Verge*. Archived (https://web.archive.org/web/20240511151328/https://www.theverge.com/2016/3/24/1 1300840/how-an-irate-developer-briefly-broke-javascript) from the original on May 11, 2024. Retrieved May 11, 2024.

9. Gallagher, Sean (March 25, 2016). "Rage-quit: Coder unpublished 17 lines of JavaScript and "broke the Internet" " (https://arstechnica.com/information-technology/2016/03/rage-quit-coder-unpublished-17-lines-of-javascript-and-broke-the-internet/). *Ars Technica*. Archived (https://we b.archive.org/web/20240511153334/https://arstechnica.com/information-technology/2016/03/ra ge-quit-coder-unpublished-17-lines-of-javascript-and-broke-the-internet/) from the original on May 11, 2024. Retrieved May 11, 2024.

10. Tung, Liam (March 23, 2016). "Disgruntled developer breaks thousands of JavaScript, Node.js apps" (https://www.zdnet.com/article/disgruntled-developer-breaks-thousands-of-javascript-nod e-js-apps/). *ZDNET*. Archived (https://web.archive.org/web/20240511162239/https://www.zdne t.com/article/disgruntled-developer-breaks-thousands-of-javascript-node-js-apps/) from the original on May 11, 2024. Retrieved May 11, 2024.

11. Williams, Chris (March 29, 2016). " 'No regrets' says chap who felled JavaScript's Jenga tower – as devs ask: Have we forgotten how to code?" (https://www.theregister.com/2016/03/29/npm gate_followup/). *The Register*. Archived (https://web.archive.org/web/20240511162239/https:// www.theregister.com/2016/03/29/npmgate_followup/) from the original on May 11, 2024. Retrieved May 11, 2024.

12. Claburn, Thomas (February 3, 2022). "Malware-infected npm packages more common than you may fear" (https://www.theregister.com/2022/02/03/npm_malware_report/). *The Register*. Archived (https://web.archive.org/web/20240511164936/https://www.theregister.com/2022/02/0 3/npm_malware_report/) from the original on May 11, 2024. Retrieved May 11, 2024.

Retrieved from "https://en.wikipedia.org/w/index.php?title=Npm_left-pad_incident&oldid=1265068726"