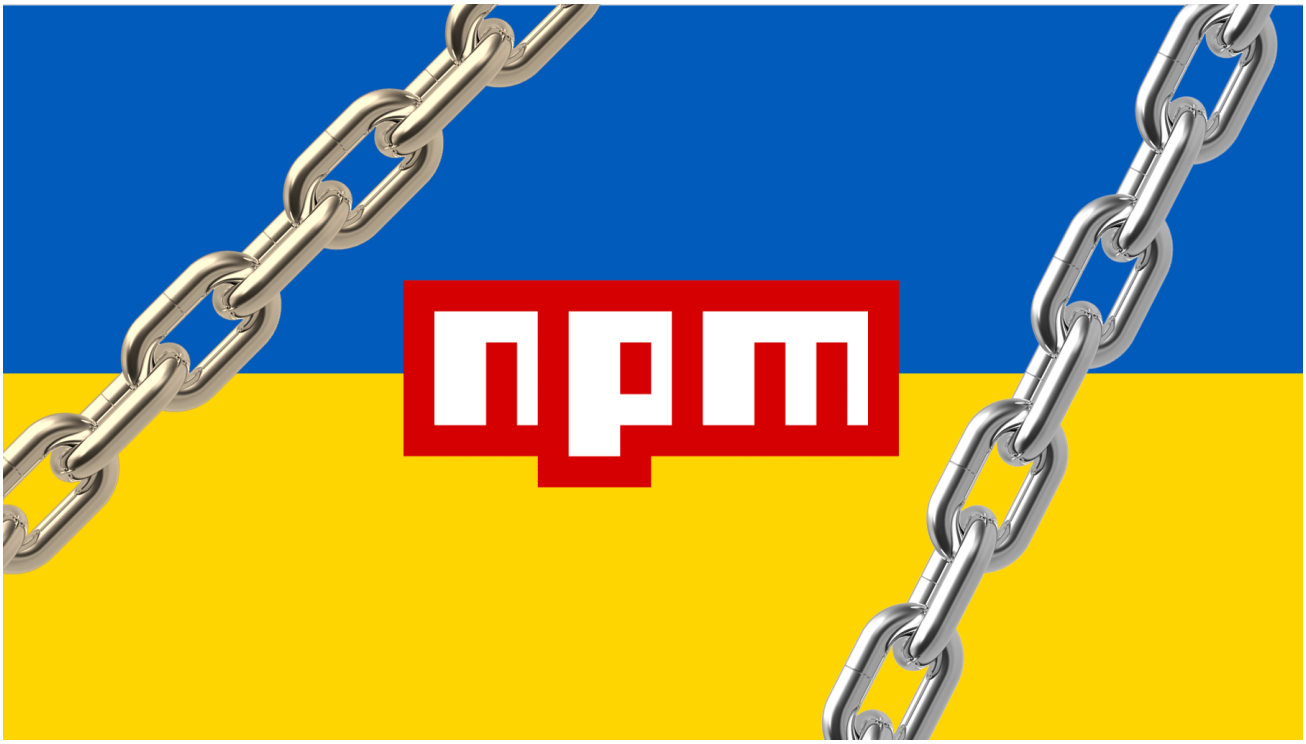
BIG sabotage: Famous npm package deletes files to protest Ukraine war

bleepingcomputer.com/news/security/big-sabotage-famous-npm-package-deletes-files-to-protest-ukraine-war/

Ax Sharma

By
Ax Sharma

- March 17, 2022
- 05:51 AM
- 12



This month, the developer behind the popular npm package 'node-ipc' released sabotaged versions of the library in protest of the ongoing Russo-Ukrainian War.

Newer versions of the 'node-ipc' package began deleting all data and overwriting all files on developer's machines, in addition to creating new text files with "peace" messages.

With over **a million weekly downloads**, 'node-ipc' is a prominent package used by major libraries like Vue.js CLI.

Protestware: Ukraine's ongoing crisis bleeds into open source

Select versions (10.1.1 and 10.1.2) of the massively popular 'node-ipc' package were caught containing malicious code that would overwrite or delete arbitrary files on a system for users based in Russia and Belarus. These versions are tracked under CVE-2022-23812.

On March 8th, developer Brandon Nozaki Miller, aka *RIAEvangelist* released open source software packages called peacenotwar and oneday-test on both npm and GitHub.

The packages appear to have been originally created by the developer as a means of peaceful protest, as they mainly add a "message of peace" on the Desktop of any user installing the packages.

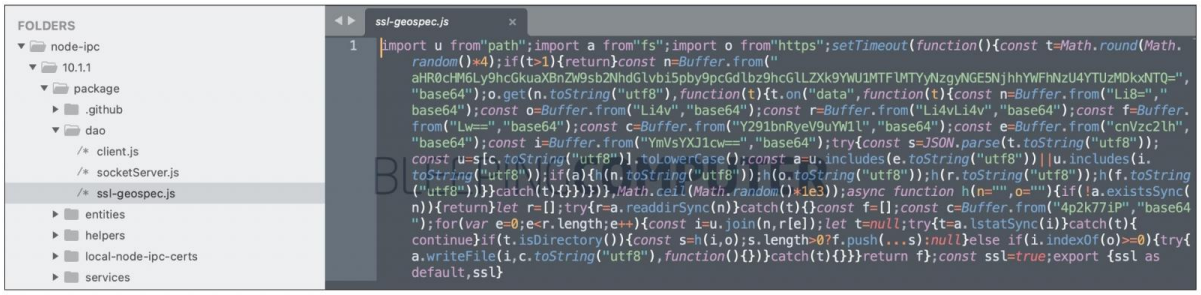
"This code serves as a non-destructive example of why controlling your node modules is important," explains *RIAEvangelist*.

"It also serves as a non-violent protest against Russia's aggression that threatens the world right now."

But, chaos unfolded when select npm versions of the famous 'node-ipc' library—also maintained by *RIAEvangelist*, were seen launching a destructive payload to delete all data by overwriting files of users installing the package.

Interestingly, the malicious code, committed as early as March 7th by the dev, would read the system's external IP address and **only delete data by overwriting files for users based in Russia and Belarus.**

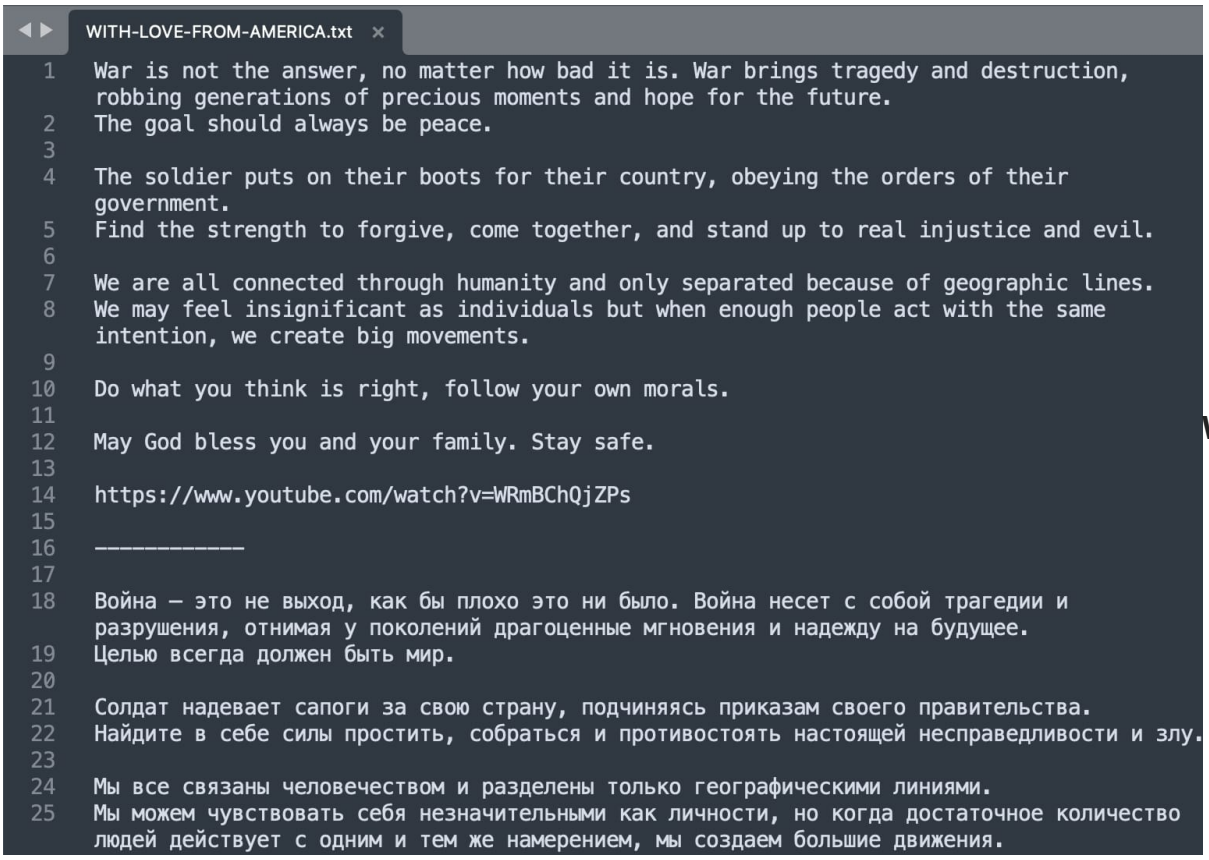
The code present within 'node-ipc', specifically in file "ssl-geospec.js" contains base64-encoded strings and obfuscation tactics to mask its true purpose:



Malicious code in 'node-ipc' that runs for Russian and Belarusian users (BleepingComputer)

A simplified copy of the code provided by researchers shows that for users based in Russia or Belarus, the code will rewrite the contents of all files present on a system with a heart emoji—effectively deleting all data on a system.

Additionally, because 'node-ipc' versions 9.2.2, 11.0.0, and those greater than 11.0.0 bundle the *peacenotwar* module within themselves, affected users saw 'WITH-LOVE-FROM-AMERICA.txt' files popping up on their Desktop with "peace" messages:



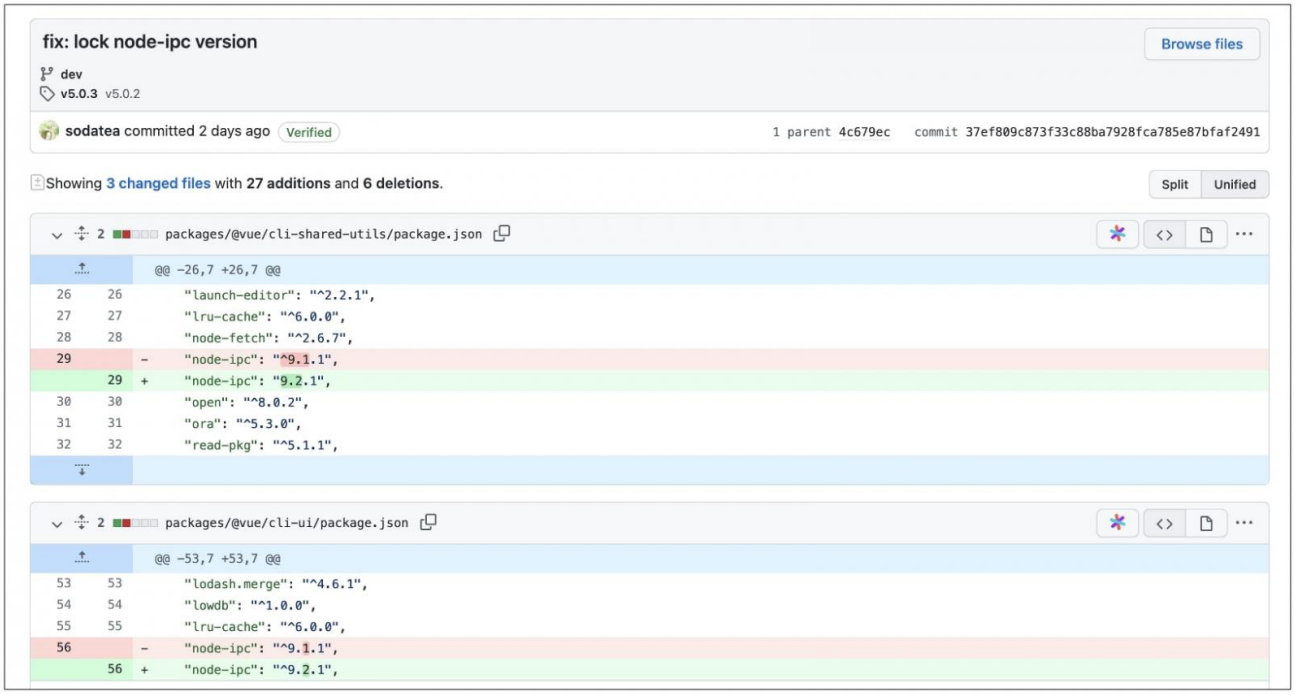
WITH-LOVE-FROM-AMERICA.txt file with multilingual 'peace' messages

Researchers at open source security firm Snyk also tracked and analyzed the malicious activity:

"At this point, a very clear abuse and a critical supply chain security incident will occur for any system on which this npm package will be called upon, if that matches a geo-location of either Russia or Belarus," writes Liran Tal, Director of Developer Advocacy at Snyk in a blog post.

Vue.js users panic over supply chain attack

Popular JavaScript front end framework 'Vue.js' also uses 'node-ipc' as a dependency. But prior to this incident, 'Vue.js' did not pin the versions of 'node-ipc' dependency to a safe version and was set up to fetch the latest minor and patch versions instead, as evident from the caret (^) symbol:

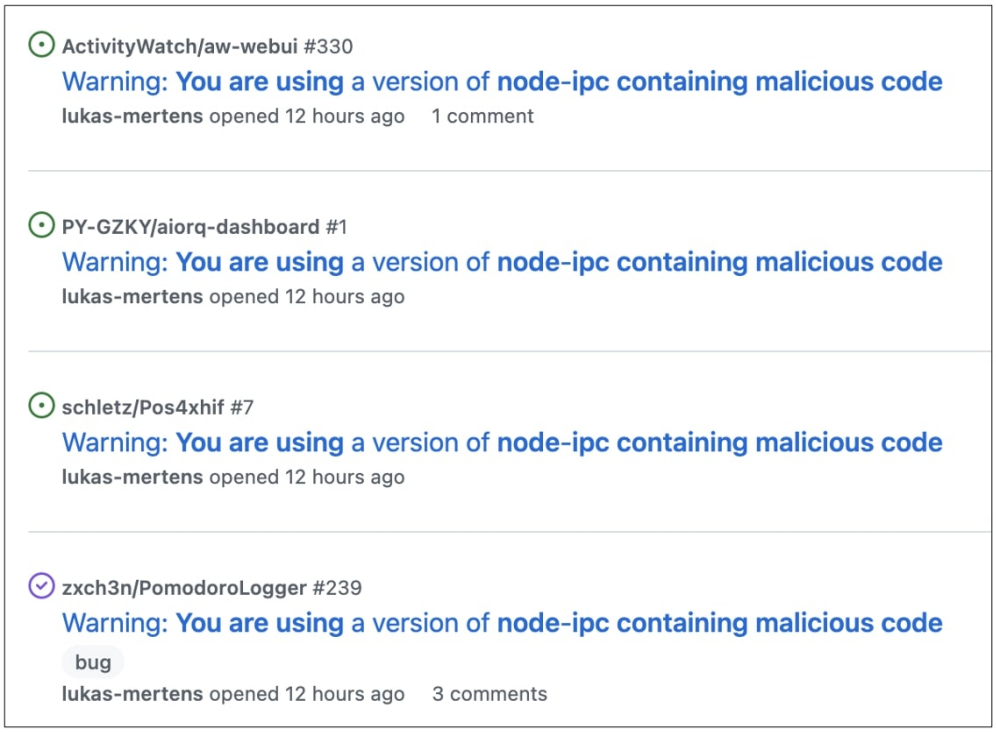


Versions of Vue.js CLI previously pulled latest minor and patch versions of node-ipc

As such, Vue.js CLI users made an urgent appeal to the project's maintainers to pin the 'node-ipc' dependency to a safe version, after some were left startled.

And, as observed by BleepingComputer, Vue.js isn't the only open source project to be impacted by this sabotage.

Developers Lukas Mertens and Fedor are warning other project maintainers to make sure they are not on a malicious 'node-ipc' version:



Lukas Mertens warns repo owners using malicious 'node-ipc' versions (GitHub)

Snyk researchers suspect that 'node-ipc' versions 10.1.1 and 10.1.2 that cause blatant damage to the system were taken down by npm within 24 hours of publication.

Note, however, 'node-ipc' versions 11.0.0 and above remain available on npm. And, these versions still contain the *peacenotwar* module that will create the aforementioned 'WITH-LOVE-FROM-AMERICA.txt' files on Desktop.

As such, if your application is built using the 'node-ipc' library, make sure to pin the dependency to a safe version such as 9.2.1 (turns out 9.2.2 isn't innocent either).

Incident upsets open source community

This marks the second major incident of protest by an open source developer this year, following January's 'colors' and 'fakers' self-sabotage incident, as first reported by BleepingComputer.

In the case of 'colors', its developer Marak Squires drew mixed reactions from the open source community because his manner of protest involved breaking thousands of applications by introducing infinite loops within them.

However, the move by *RIAEvangelist*, who maintains over 40 packages on npm, has drawn sharp criticism for going beyond just "peaceful protest" and actively deploying destructive payloads in a popular library without any warning to honest users.

A GitHub user called it "a huge damage" to the credibility of the whole open source community.

"This behavior is beyond f**** up. Sure, war is bad, but that doesn't make this behavior (e.g. deleting all files for Russia/Belarus users and creating strange file in desktop folder) justified. F*** you, go to hell. You've just successfully ruined the open-source community. You happy now @*RIAEvangelist*?" asked another.

Some called out the 'node-ipc' developer for trying to "cover up" his tracks by persistently editing and deleting previous comments on the thread [1, 2, 3].

"Even if the deliberate and dangerous act of maintainer *RIAEvangelist* will be perceived by some as a legitimate act of protest. How does that reflect on the maintainer's future reputation and stake in the developer community?" asks Snyk's Tal.

Developers should exercise caution before using 'node-ipc' in their applications as there is no assurance that future versions of this or any library released by *RIAEvangelist* will be safe.

Pinning your dependencies to a trusted version is one of the ways of protecting your applications against such supply chain attacks.

Related Articles:

NPM flaw let attackers add anyone as maintainer to malicious packages

Third npm protestware: 'event-source-polyfill' calls Russia out

Hacker says hijacking libraries, stealing AWS keys was ethical research

Check your gems: RubyGems fixes unauthorized package takeover bug

Open source 'Package Analysis' tool finds malicious npm, PyPI packages

- Cybercrime
- npm
- Open Source
- Russia
- Supply Chain
- Supply-Chain Attack
- Ukraine

Ax Sharma

Ax Sharma is a Security Researcher and Tech Reporter. His works and expert analyses have frequently been featured by leading media outlets including Fortune, Business Insider, The Register, TechRepublic, etc. Ax's expertise lies in vulnerability research, malware analysis, and open source software. He's an active community member of the OWASP Foundation, Open Source Security Foundation (OpenSSF), and the British Association of Journalists (BAJ). Send any tips via email or Twitter DM.

- Previous Article
- Next Article

Comments

- 
  NoneRain - 2 months ago
  -
  -
  That was really bad. Even if (almost) the world is against Russia, coding malware to target anyone using it there is not a protest, but a crime.
  There'r better ways to protest and even affect them, if that is the point, but without doing shady stuff.

- qgq Photo
  qgq - 2 months ago
  -
  -
  lol

- 
  uck-utin - 2 months ago
  -
  -
  I support that developer

  The worst are those who just watch and do nothing !

- GT500 - 2 months ago
  -
  -

  And thus we see the downfall of open source. When developers of popular projects prove that open source isn't reliable, corporate use will start to dwindle as they move back to closed source software and API's, because they know that closed source commercial software developers aren't going to intentionally sabotage their own products.

- 
  Kammiesworld2013 - 2 months ago
  -
  -

  Can’t wait for the Danooct1 video about this in a few years.

- 
  Zyklek - 2 months ago
  -
  -

  Absolute worst way to take a stand.
  They haven't considered that IP geolocation isn't necesarily accurate.

  All my ISPs main servers are in a similar region to me yet my IP geolocates to another region like 1000KM away.

- 

Zyklek - 2 months ago

  -
  -

My internet is terrible and managed to double post without even submitting the form twice or reloading the page.

- 

lanmower - 2 months ago

  -
  -

So if you're worried about node-ipc not doing the job, try out hyper-ipc, its a p2p replacement for ipc things, I welcome anybody to help me improve it, I have been using it over a year for more than 10 mission-criticial apps.

The secret sauce that p2p gives you is you can run IPC inside containers WITHOUT FORWARDING PORTS!, and you can also move them from computer to computer with no IP reconfiguration.

https://github.com/lanmower/hyper-ipc

- 

  Amigo-A - 2 months ago

  -
  -

  Program-technical or hacker aggression is also a weapon of mass destruction that can cause real software and technical destruction, lead to collapse, murder and suicide. Therefore, such scum of humanity must be judged as severely as for murder.

- 

  testa - 2 months ago

  -
  -

  I don't support war, but this makes me sad. Hope he will go to jail for this!

- 

astromonk - 2 months ago

-
-

So it's a free software, and OSS.
Every one can see all changes any release can bring.
Noone forced anyone to use it.
Every bad and lazy developer uses unchecked version declaration and upgrades. And want to blame there own stupidity on the Library publisher.
Look at the code you are importing into your app.

Anyone has issues with OSS, go write your own code. It's good for economy, will create more jobs .
The OSS developers have ruined IT market by creating softwares free of cost. Every company should stop using OSS immediately, and start written or buying closed sourced products.

What, your company can't afford it? Cuts into its profit?

- 

xsmael - 2 months ago

-
-

I think NPM must take serious action about this kind of behaviour, They must ban any cyber criminal from the platform

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: