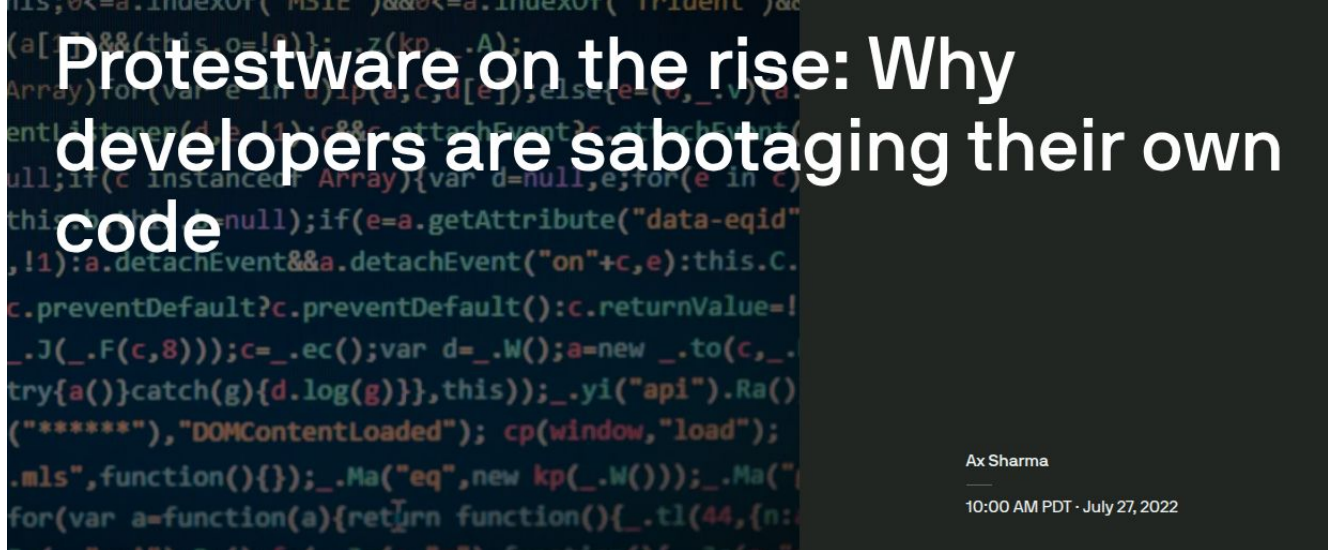


On the Characteristics and Impacts of Protestware Libraries

Tanner Finken, Jesse Chen, and Sazzadur Rahaman
University of Arizona





Threat Research | November 16, 2023

Protestware taps npm to call out wars in Ukraine, Gaza

ReversingLabs researchers have discovered npm packages that hide scripts broadcasting messages of peace related to the conflicts in Ukraine and in Israel and the Gaza Strip.



BLOG AUTHOR

Paul Roberts, Director of Content and Editorial at RL. [READ MORE...](#)

🕒 FEBRUARY 23, 2024

Is the future of open source software at risk due to protestware?

by Stuart Pallister, Singapore Management University



Editors' notes

Technology · 5 Min Read

Protestware and the Digital Battlefield: The rise of ideological code in a fragmented world

Protestware refers to open-source software that has been intentionally modified to express political or social protest. This can range from displaying messages to users, to more disruptive or destructive actions such as sabotaging software functionality or deleting data.



Srinivas G. Roopi · ETGovernment

Updated On May 9, 2025 at 11:24 PM IST

Protestware: Digital Protest

- 'Protestware' - new term for OSS protest
- Began during Russian-Ukrainian conflict (Feb 2022)
- Impactful example: node-ipc
- Although reported, not well studied or understood

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

By **Ax Sharma**

March 17, 2022 05:51 AM 12

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

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)

Protestware Related Work

- Cheong et al. proposed ethical guidelines for OSS

developers

Ethical Considerations Towards Protestware

Marc Cheong[†], Raula Gaikovina Kula*, and Christoph Treude[†]

[†]University of Melbourne, Australia, *Nara Institute of Science and Technology, Japan
marc.cheong@unimelb.edu.au, christoph.treude@unimelb.edu.au, raula-k@is.naist.jp

- Kula et al. gave short paper with 3 categories

In War and Peace: The Impact of World Politics on Software Ecosystems

Raula Gaikovina Kula
Nara Institute of Science and Technology, Japan
raulak@is.naist.jp

Christoph Treude
University of Melbourne, Australia
christoph.treude@unimelb.edu.au

- Fan et al. studied community reactions to protestware

with two samples (colors.js and es5-ext)

Developer Reactions to Protestware in Open Source Software: The cases of color.js and es5-ext

Youmei Fan ✉ · Dong Wang · Supatsara
Wattanakriengkrai · Hathaichanok
Damrongsiri · Christoph Treude · Hideaki
Hata · Raula Gaikovina Kula

Our Research Topic

- Analyze at a larger scale with a comprehensive dataset

Our Definition: “protestware is any open-source software that has been intentionally modified by its developers to express political messages or disrupt functionality as a form of protest.”

- Restrict our search to reusable libraries (SSC impact)

Our Research Questions

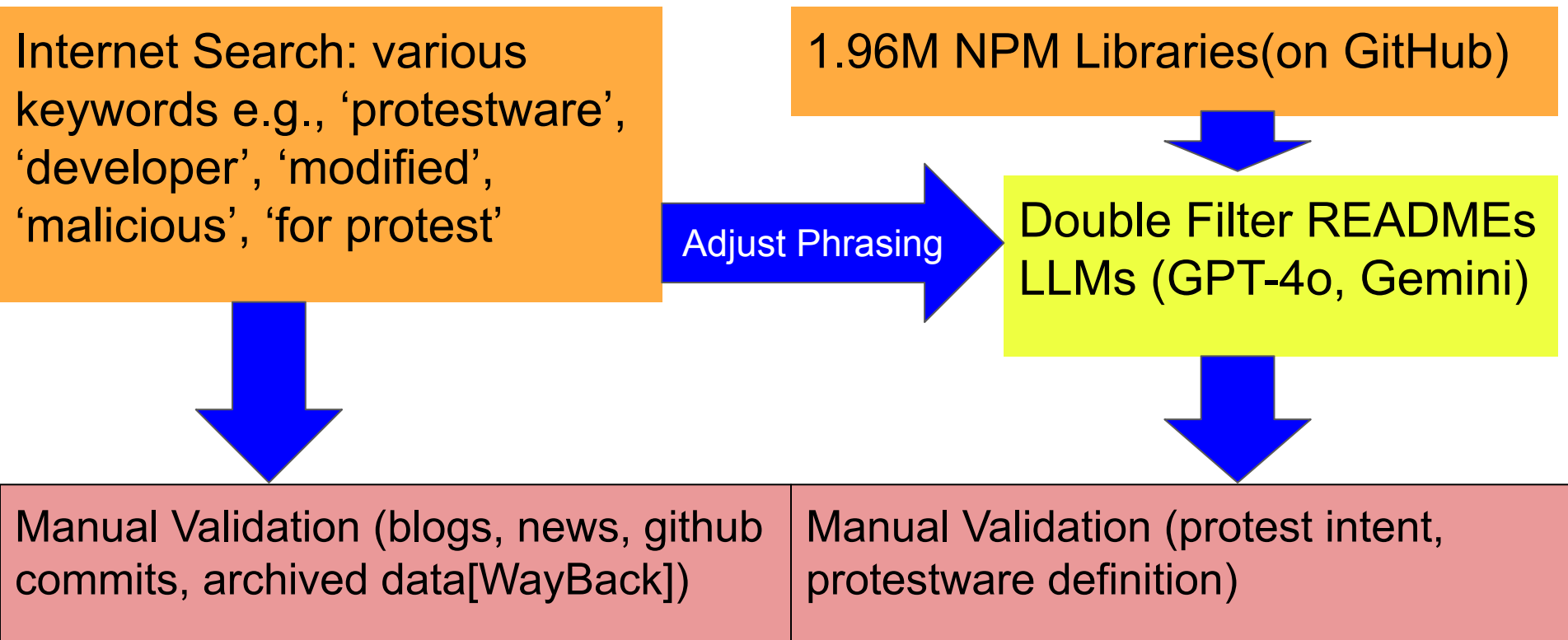
RQ1. What characteristics exist in protestware?

- Implementation, triggers, audience, transparency

RQ2. What happens after conversion?

- Disruption, sentiment, and usage trends

How We Collected Our Dataset



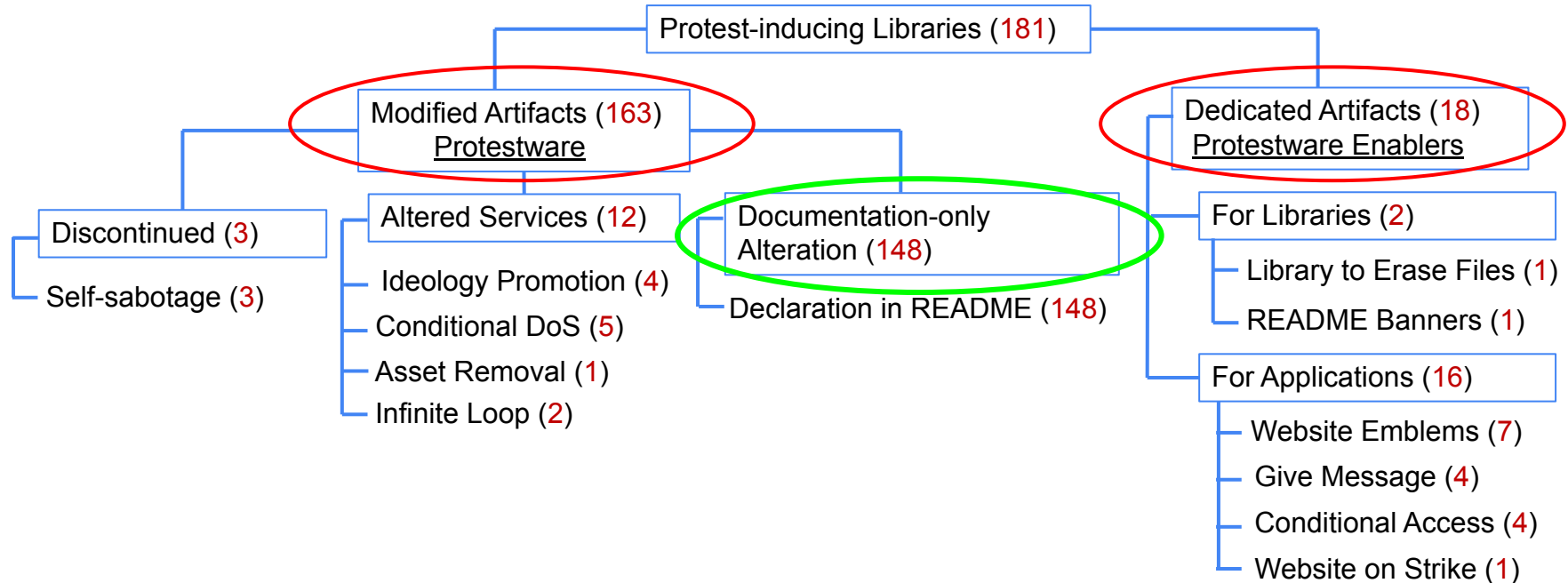
How We Collected Our Dataset

Result:

Total of 181 Protest related Libraries!

RQ1: Characteristics of Protestware


Protestware Taxonomy Result



Protestware Altered Documentation

- Nestjs-pino, Coral UI Core, angular-emojis

README Code of conduct MIT license



"Vovchansk (2024-06-02) 1513" by National Police of Ukraine (Liut Brigade) is licensed under CC BY 4.0.

This is Vovchansk, Ukraine, the city where the father of this library's author was born. This is how it looks now, after the Russian invasion. If you find this library useful and would like to thank the author, please consider donating any amount via one of the following links:

- [Armed Forces of Ukraine](#) • ["The Come Back Alive" foundation](#) •

Thanks for your support! 🇺🇦

NestJS-Pino

README License

Coral UI Core 🖐️

A collection of utility classes and components for building Coral UI.


Important

If you think that Elon Musk is cool, you are a racist, sexist, are homophobic, transphobic or a fascist, then you shouldn't use this software. It's only for cool people and you're not cool. You're a loser.

Examples with different Sizes

Black Lives Matter (I acknowledge that Black people have to fight for basic rights, against systemic racism, unequal opportunities and injustice across the 🌍. I know this is wrong and I am ❤️!)

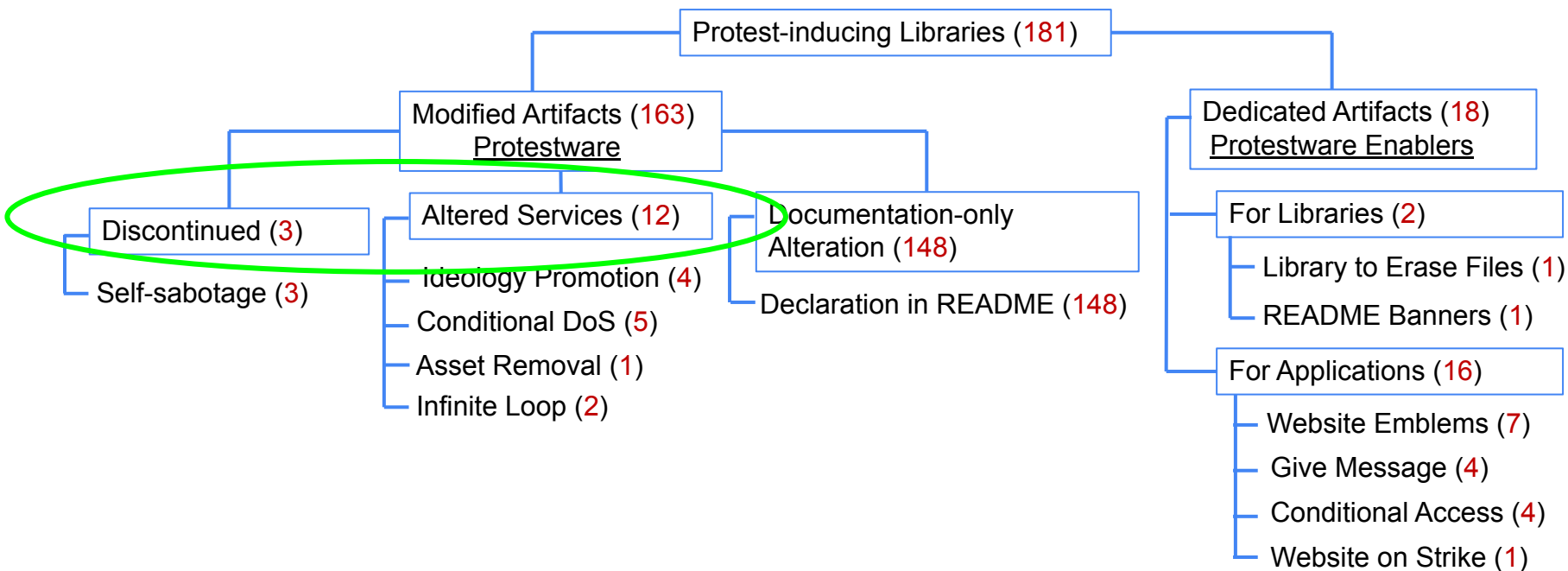
```
<angular-emojis [name]='black_heart' size='50'> </angular-emojis>
<angular-emojis [name]='black_medium_square' size='50'> </angular-emojis>
<angular-emojis [name]='waving_black_flag' size='50'> </angular-emojis>
<angular-emojis [name]='fist_1' size='50'> </angular-emojis>
<angular-emojis [name]='fist_2' size='50'> </angular-emojis>
```



What Issues Trigger Protestware?

Trigger	Frequency
Russo-Ukrainian war	121 (72%)
Black Lives Matter	19 (11%)
Israeli-Palestinian conflict	14 (8%)
Sexism	3 (2%)
Corporate Conflict	3 (2%)
Variety of Others	7 (4%)

Protestware Taxonomy



Target: Who Gets Affected?

- Specific: Targeted set of users
- Universal: All users impacted equally
- Raises questions of open-source fairness

Target: Specific

- Target users remove functionality
- Target users get different experience (message, delete files)

The screenshot displays a code editor interface with three main sections:

- Commit Message:** A text input field containing the message "drop k hujam support of russian language".
- File List:** A sidebar on the left showing a directory structure with "po" expanded, listing "LINGUAS" and "ru.po".
- Diff View:** The main editor area shows a diff for the "ru.po" file. It indicates "2 files changed" and "+0 -2430 lines changed". The diff table shows changes across various language codes, with the "ru" entry (line 10) highlighted in red, indicating a deletion.

Line	Change	Code
7	+	fr
8	+	it
9	+	pt_BR
10	-	ru
11	+	sk
12	+	uk
13	+	zh_TW

Below the diff view, a code editor shows a JavaScript snippet:

```
33 + <script>
34 +   if (!!navigator.language && ['ru', 'ru-ru', 'ru_ru'].includes(navigator.language.toLowerCase()) && window.location.pathname !== '/%F0%9F%96%95')
35 +     window.location = '/🚫'
```

At the bottom right, a message is displayed:

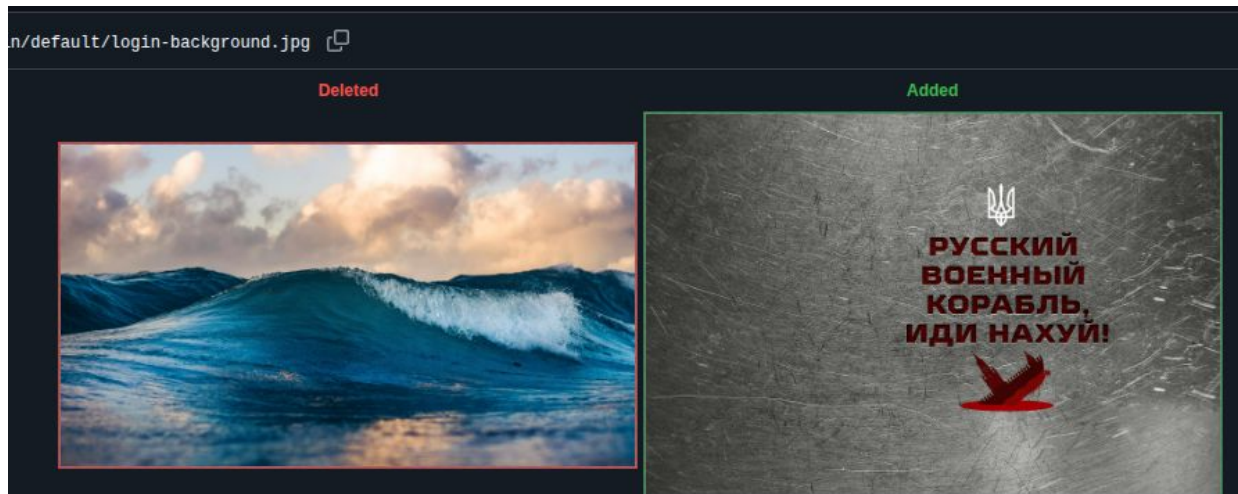
Forbidden to Russian people.

Please come back as soon as pease returns to Eastern Europe.

17

Target: Universal

- Message
- Removed Code
- Infinite Loop

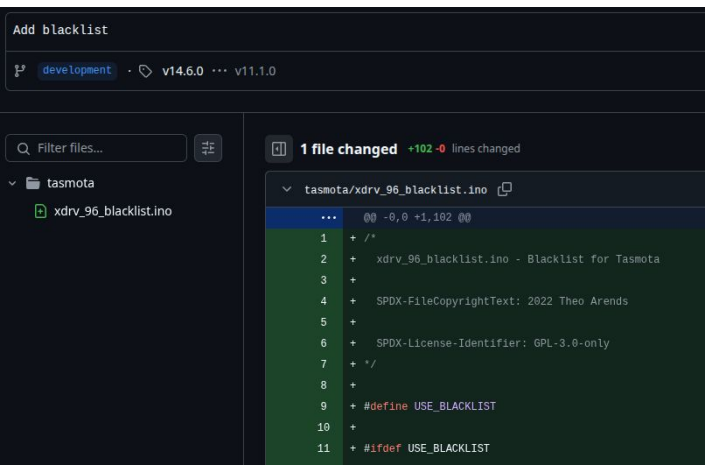


```
3 + String left pad.  
4 +  
5 + P.S: [I've unpublished it from NPM.](
```

```
16 + let am = require('../lib/custom/american');  
17 + am();  
18 + for (let i = 666; i < Infinity; i++;) {
```

'Transparency Isn't Always Respected'

- Only 3/15 altered functionality libraries disclosed their protest
- Others were silently removed or hidden in code
- Potentially undermines trust in OSS communities



```
1 //
2 // xdrv_96_blacklist.ino - Blacklist for Tasmota
3 //
4 // SPDX-FileCopyrightText: 2022 Theo Arends
5 //
6 // SPDX-License-Identifier: GPL-3.0-only
7 //
8 //
9 #define USE_BLACKLIST
10
11 #ifdef USE_BLACKLIST
```

Important notice about the usage of this software for `.ru`, `.su`, `.by`, and `.pф` domain zones

As a consequence of the illegal war in Ukraine, the behavior of this repository and related npm package [sweetalert2](#) is different for `.ru`, `.su`, `.by`, and `.pф` domain zones.

Including this software in any domain in `.ru`, `.su`, `.by`, and `.pф` domain zones will block the website navigation and play the national anthem of Ukraine.

This behavior is classified as [protestware](#) and this project is listed in [GitHub Advisory Database](#) and [Snyk Vulnerability DB](#).

RQ2: Aftermath of Protestware

Examples of Supply Chain Disruption

- Damaging software infrastructure: node-ipc
 - 30,000 messages and files lost by NGO server hosted in Belarus (Reddit)
- Failures due to self sabotage: left-pad
 - NPM stated “hundreds of failures per minute”
- Infinite loops causing apps to crash
 - Colors.js and faker.js
- Ripple effects through widely used frameworks

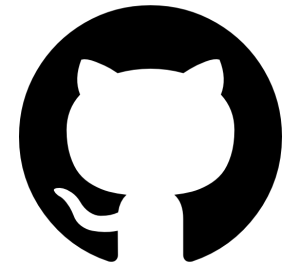
Reaction Analysis(GitHub+Reddit)



- GitHub Commits on insertion of protest
 - Looking at other developer's thoughts
- Reddit Comments
 - Looked at relevant threads to 'protestware'
 - Comparing general stances on protestware in general

[Content Warning- some comments have inappropriate language]

Developer Reactions(GitHub)



- GitHub Comments on Protestware Commits
 - Most reactions were negative (4/7 active)



TechStudent10 on Dec 26, 2022

Why did you do this?



EvelynSubarrow on Mar 12, 2022

This sort of action is deeply disappointing, I hope you reconsider on this. Holding ordinary enthusiasts to account for the actions of their government will not achieve anything useful for anyone.



6



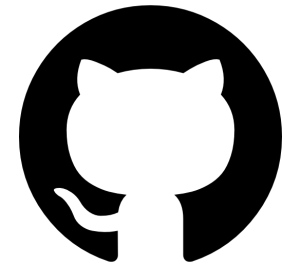
Comment on line R1032



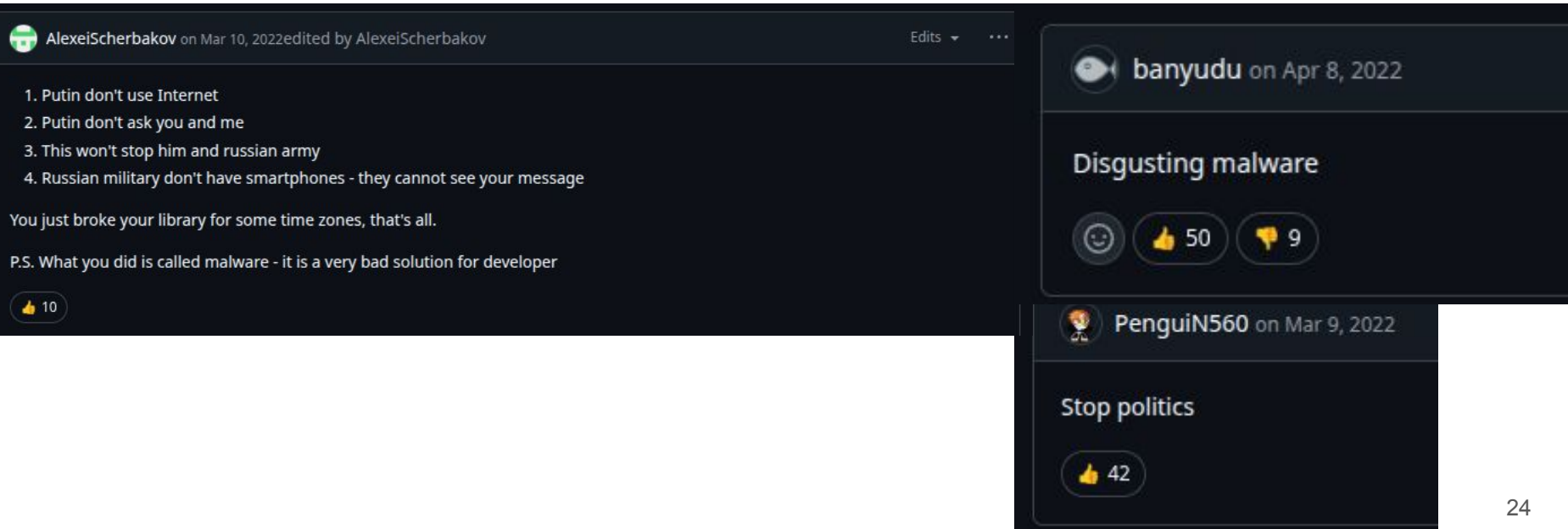
Lemonawa on Apr 9, 2022

what a stupid code here!

Developer Reactions(GitHub)



- GitHub Comments on Protestware Commits
 - Most reactions were negative (4/7 active)

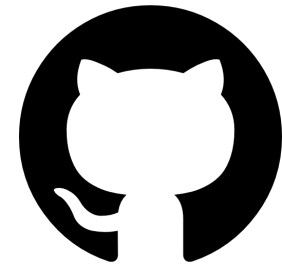


The screenshot shows a GitHub commit by AlexeiScherbakov from March 10, 2022. The commit message lists four points: 1. Putin don't use Internet, 2. Putin don't ask you and me, 3. This won't stop him and russian army, and 4. Russian military don't have smartphones - they cannot see your message. Below the list, it says 'You just broke your library for some time zones, that's all.' and 'P.S. What you did is called malware - it is a very bad solution for developer'. There is a thumbs up reaction count of 10.

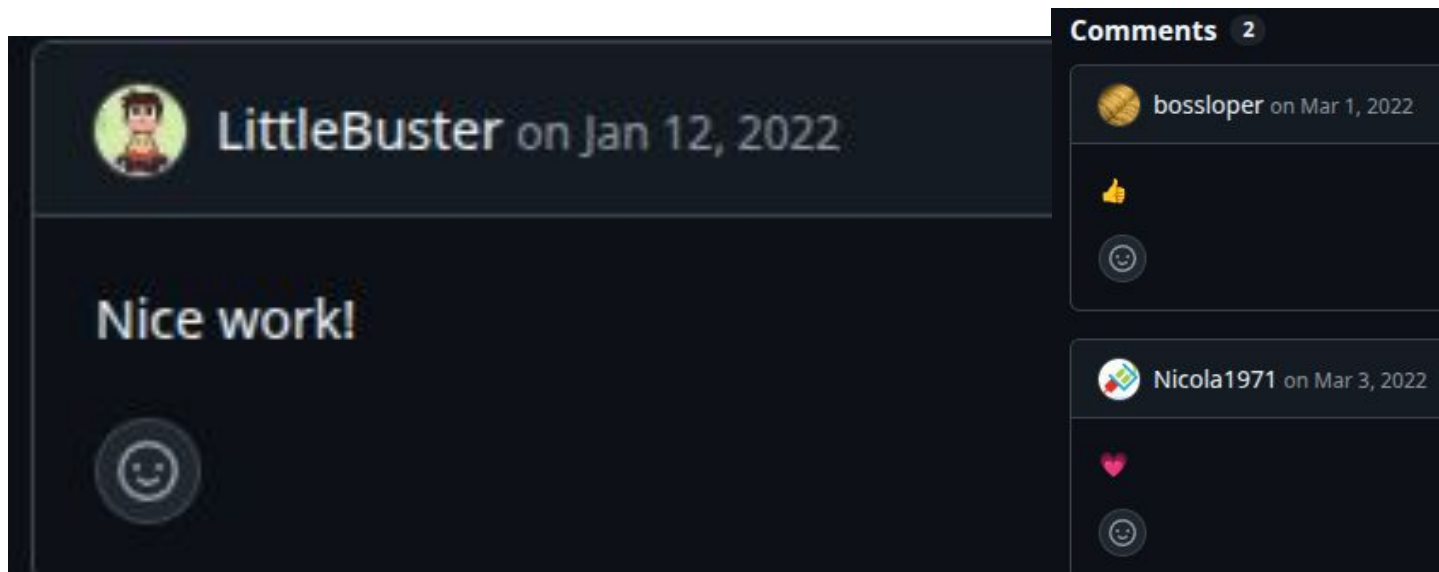
Comments on the commit:

- banyudu** on Apr 8, 2022: Disgusting malware. Reactions: 50 thumbs up, 9 thumbs down.
- Penguin560** on Mar 9, 2022: Stop politics. Reactions: 42 thumbs up.

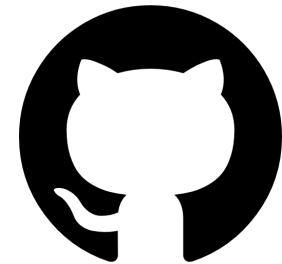
Developer Reactions(GitHub)



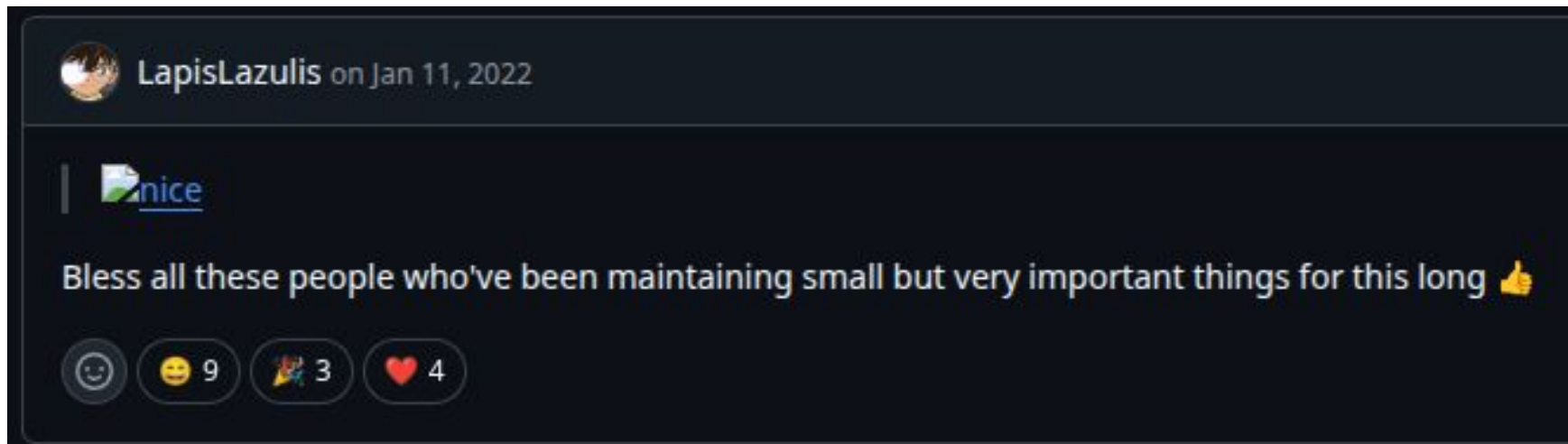
- Some political support for aligned causes
 - Typically lower engagement



Developer Reactions(GitHub)




- Some political support for aligned causes
 - Typically lower engagement




Broader Reactions(Reddit)




- Reddit Comments for general stances
 - More in opposition

 **0xC1A** · 3y ago
Self sabotage, good luck living with the consequences of your actions
↑ 35

 **Voltra_Neo** · 3y ago
In one word: *sigh*
↑ 5

 **faustoc5** · 3y ago
How is fucking with all your users a protest ?
More like fuckyouallware
↑ 5

 **AceSevenFive** · 3y ago
You mean malware?
↑ 7

Broader Reactions(Reddit)



- Reddit Comments for general stances
 - More in opposition



shevy-ruby • 3y ago

I always felt that politics should not be part of code respectively open source. If you want to be an engineer (and let's assume that software engineering is part of engineering) then there should be objective criteria - be it documentation, usability, efficiency.

Politics are always subject to bias.



2



Taldoesgarbage • 3y ago

The fact that other people have put time and effort into open source projects just for their creators to put shitty 'protestware' in them makes me really angry. If you make an open source project with dozens of contributors who have put time and effort into making your project good just to ruin it you are a dick.



0

Broader Reactions(Reddit)



- Reddit Comments for general stances
 - More in opposition



[deleted] · 3y ago

Protestware? Call Malware as Malware.



127



sik0fewl · 3y ago

It's not protestware, it's malware and the developers involved with malware should be blacklisted.



10

Broader Reactions(Reddit)



- Reddit Comments for general stances
 - Some for support ('it's their code')



[deleted] · 3y ago

I fully support this type of action. and in no way is this "vandalism" anybody who says it is can fuck right off.

If a person wrote the software, and has given it out for free without being paid. They have a right to do whatever they want, whenever they want with that said software. It's THEIR software, nobody should be able to tell them what they can and cannot do with it.

If businesses don't want to be caught off guard by open source software, then they should pay for software.



-5

Broader Reactions(Reddit)



- Reddit Comments for general stances
 - Some for support ('it's their code')



Intelligent-donkey · 3y ago

Everything is political, anyone who has every used a variation of the phrase "X is not political" can go fuck themselves.

If your message is good, then spread it whenever and wherever you can.

Of course it often does pay to be mindful of how people will respond to your message, and to avoid anything that will ultimately be counter productive. But I have no categorical opposition to any specific form of protest, only practical concerns.



Broader Reactions(Reddit)



- Reddit Comments for general stances
 - Others for conditional support ('if it doesn't hurt anyone')



[deleted] · 3y ago

If they're providing something of value for free, I don't have a problem with them posting a message. Hostile actions like deleting stuff are obviously over the line.



Siphyre · 3y ago

Posting messages is cool, actually deleting files is dumb. You are going to hit innocents by accident. IP > Country lists are not 100% accurate. VPNs also get used and can cause issues. Someone Russian, living abroad, researching the war back home to see what sort of lies are being told might get affected. Damaging people with code is ultimately malware and should be considered as such, along with being prosecuted for it. Posting a message though? That is cool and even encouraged.



18

Protestware Usage (NPM Usage Trends)

- Collected data from NPM using WayBack snapshots near protest insertion
- Comparing protestware to library with similar functions
- All collected samples had an increase in dependency count
- More variety in download counts
- Two popular (over 1M downloads) remained active

Library Name(s)	Dependency % Difference	Download Count % Difference
<u>node-ipc</u> Python-shell	+12.1% +45.0%	-48.0% +95.0%
<u>es5-ext</u> core-js-pure	+39.4% +122.6%	-24.8% -29.2%
<u>EventSource</u> faye-websocket	+40.5% +97.0%	-48.7% -15.0%
<u>sweetalert2</u> sweetalert	+104.7% +14.7%	+33.8% -14.1%
<u>colors.js</u> chalk	+16.7% +55.0%	-29.2% +89.2%
<u>faker.js</u> casual	+2.4% +6.5%	-7.4% +89.2%
<u>styled-components</u> react-base16-styling	+42.8% +50.0%	+38.1% +48.8%
<u>nestjs-pino</u> nest-winston	+405.7% +87.1%	+572.0% +66.4%
<u>left-pad</u> pad-left	N/A +407.1%	+226.6% +2,647.2%

Key Takeaways

- Protestware is a new form of digital protest
- Large disruptions caused by protestware
 - Many Negative views on this type of protest
 - Although, usage continued to increase
 - Supply chain integrity may be at risk again
- Various forms of digital protest
 - Pattern of expressing belief in non-disruptive manner

Conclusion + Q&A

- To know more about examples and our data, see our paper and replication package hosted on Zenodo (<https://zenodo.org/records/15279732>)
- Thanks to my coauthors: Jesse Chen and Sazzadur Rahaman
- And all others who have helped out with this project
- Thank you! I'm happy to take any questions.
- Or reach out to me at: finkent@arizona.edu

Supplemental Slides (For potential questions)

- Some methodologies(Taxonomy coding & Reaction Analysis) (skipped for brevity)
- Dataset LLM's validation method
- Also recommendations to deal with protestware or using appropriate libraries
- Additional reasoning behind choosing NPM and README

Protestware Taxonomy Methodology

- Assigned Code to each library based on behavior changed
 - Generalized codes and grouped common together

Reaction Analysis(Methodology)



- GitHub Commits found on insertion of protest
 - Manual analysis and aggregation of sentiment
- Reddit Comments (Reddit API)
 - Extracted relevant threads to 'protestware'
 - LLM filtering for relevant opinions (support or oppose)
 - Manual validation of comments
 - Additional Validation of LLM filter with 100 random samples (>80% accurate with similar ideas seen)

Dataset LLM validation

To validate the accuracy of the LLMs we performed the filtering of repos, we:

- Looked at 100 random samples
- Found over 80% agreed with the label (some false negatives)
- Types(protest idea) seen were mostly represented in our sample

General Developer Recommendations

- Most recent libraries seen with non-harmful protest (altering documentation/ README)

Although, to reduce chances of potential protestware affecting your system (typical recommendations seen):

- Pinning a known safe version (disable automatic updates, then updating when verified)
- Forking and having own repo (in case its removed)
- Pick libraries with strong contributor communities

Using NPM and READMEs for Dataset Collection

Looking at NPM

- Found multiple protestware libraries on NPM already
- Libraries have interconnected structure, meaning many dependencies and potentially higher affects

Using README

- We hypothesized that READMEs were a good way to express protest and indicate intent
- Limited resources used on README tokens rather than exploring large code bases and many commits