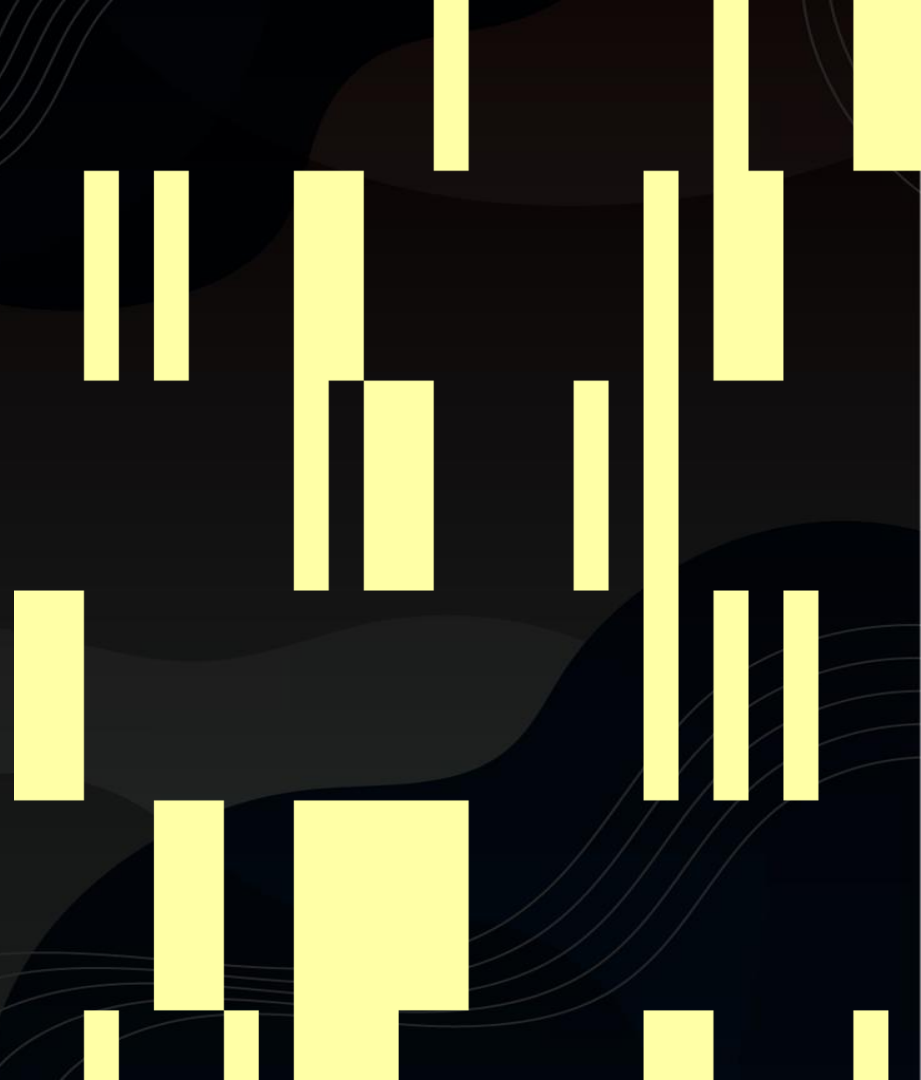


Токсичные репозитории

Что сейчас происходит
с OpenSource?





Алексей Казин

DevOps-инженер


Автор канала

Из сисадмина в DevOps

ГНИВЦ

это крупнейшие государственные
информационные системы,
миллионы пользователей, десятки
проектов, 1500+ сотрудников

О чем будем говорить?

- 
- Что такое protestware?
 - История создания toxic-repos
 - История с Node-ipc
 - Вернемся на 7 лет назад
 - Выводы
 - Что делать?
 - Первые попытки сопротивления

ВНИМАНИЕ!

Все нижеследующее является личным жизненным опытом автора. У Вас он другой, и это нормально. Тема провокационная, и обязательно вызовет жаркое обсуждение. Данный доклад не несет цели кого-либо оскорбить.

ЧТО ТАКОЕ PROTESTWARE?

Protestware — это универсальный термин, который используется для описания пакетов, которые каким-либо образом изменены для протеста против определенного события. В отличие от вредоносных пакетов, эти изменения вносятся не «хакерами» или другими злоумышленниками, а часто известными и уважаемыми членами сообщества открытого исходного кода, которые активно поддерживают или участвуют в крупномасштабных проектах с открытым исходным кодом.

Основные типы протестного ПО

- **Баннеры в репозиториях**
Обычно добавляются в README репозиторияев
- **Слоганы в логах и cli**
Вывод слоганов и лозунгов в лог-файлы, либо в командную строку.
Обычно происходит для определенного часового пояса и в зависимости от местоположения пользователя.
- **Исполнение не деструктивного кода**
Также использует «геолокационный вектор по часовому поясу», но могут создавать всплывающие окна, открывать браузеры или создавать/затирать файлы в ФС пользователя.
- **Деструктивные протесты**
Самый яркий пример деструктивного протеста это node-irc, о нем будет рассказано далее.
- **DDoS**

ИСТОРИЯ TOXIC-REPOS



Toxic-repos – проект создан в марте 2022 года и направлен на создание реестра свободного ПО с признаками protestware. Изначально список брался из “google” таблицы Техдирского клуба.



NODE-IPC

Node-irc обновляется до версии 10.1.1. В код добавляется таймер, который в рандомное время вызывает добавленный код. А новый код уже в свою очередь получает доступ к файловой системе и затирает содержимое файлов смайликом в виде сердца, но только при условии определения геопозиции России или Беларуси.

Через 10 часов выпускается версия 10.1.2. Это сделано в попытке запустить автоматическое обновление зависимостей.

Выходит версия **10.1.3** с откатом внесенных изменений. Таким образом версия с вредоносным кодом пробыла в реестре пртjс менее 24 часов, но из-за большого количества загрузок это определенно повлияло на проекты которые зависели от node-ipc. Но в этот же день появляется версия **11.0.0**. А в ней уже появилась и зависимость от модуля reasenotwar, и вывод политических слоганов в stdout.

15 марта 2022

Выходит версия **9.2.2**. Так как это была последняя стабильная версия и огромное количество проектов ссылалось на нее.

Изменения, которые были внесены:

- модуль `reascenotwar` добавлен как зависимость;
- добавлена зависимость от `colors@*`, который содержит деструктивный код;
- изменена лицензия с MIT на лицензию DBAD, которая содержит ненормативную лексику.

Примерно в то же время выходит версия **11.1.0**, которая содержит зависимость от `reascenotwar`, но при этом удаляется вывод лозунгов в `stdout`.

Взлом твиттер аккаунта Брендона Миллера.

В это же время Брендона и его жену полностью деанонят и выкладывают в общий доступ все их персональные данные.

Также есть информация, что в его дом была вызвана полиция и задержание проходило в довольно жесткой форме.

Самые известные жертвы инцидента с node-ipc

- Проект **Vue.js** оказался уязвимым для протестного ПО node-ipc
- **CLI Vue.js** зависел от node-ipc версии 9.*, которая добавляла модуль `reascenotwar`, записывающий файл `WITH-LOVE-FROM-AMERICA.txt` на рабочий стол пользователя.
- Игровой движок **Unity** также оказался уязвимым для протестного ПО node-ipc. Он также зависел от node-ipc версии 9.*

И ВСЁ?

Как «сломать» крупные сайты за 11 строк кода?

20 марта 2016 – разработчик npm пакета left-pad удалил все свои пакеты в знак протеста.

Один из затронутых пакетов, React, использовался крупными сайтами, такими как Facebook.

НЕКОТОРЫЕ ВЫВОДЫ

Какие выводы можно сделать?

- Вера в опенсорсные продукты была подорвана, т.к. люди начали себя некорректно вести.
- Многие разработчики теперь задумаются о рисках обновления до последних версий.

ЧТО ДЕЛАТЬ?

Будьте осторожны с протестным ПО

Текущая ситуация является нестабильной, и мы ожидаем, что в будущем мы увидим новые векторы угроз, связанные с протестным программным обеспечением.

Так что же нам делать?

- Продолжать предупреждать сообщество о появлении новых моделей угроз как можно быстрее.
- Вести диалог с сообществом ПО с открытым исходным кодом и стараться понять, как нам прийти к консенсусу в вопросе отношения и реакции на протестное ПО.
- В целом повышать культуру OSS.

КАК БОРОТЬСЯ?

Противодействие

На данный момент есть два решения от сообщества `toxic-repos`:

`toxic-repos-filter`

для `pip` и `npm`

и

`npm-toxic-filter`

исключительно для `npm`

Спасибо за внимание!

