Stony Brook University

Exploitation of Service Workers using Ad Push Notifications

Gauri Baraskar, Gagan Ganapathy, Piyush Mital

FAR BEYOND

Motivation

- Recently, there has been an increase in the popularity of service workers, leading to ad networks leveraging push notifications to deliver push based Ads.
- Such notifications cannot be easily detected by ad blocker software as they can be received even after the user stops the base website session.
- There is a lack of studies in analysing the impact of the malicious push based notifications while browsing websites.
- As web push notifications (WPNs) are relatively new, their role in ad delivery has not yet been studied in depth.

Problem Statement

Service worker is a thread separate from the main application thread which provides functionalities like caching, push notifications, etc for a better browsing experience.

Although, recently many websites use this functionality to push ads and generate revenue on their platform.

Through this study, we aim to understand the scale of deployment of service workers and their use for ad push notifications.

Finally, we present a proof of concept method to block ads received via these notifications.

Our contributions

- We perform a comprehensive analysis across thousands of websites that use this functionality to push ads.
    - An automatic collector system for large-scale crawling and push notification data aggregation.

- Additionally, we analyze if these ads are pushed from malicious sources.

- Finally, we propose a rudimentary solution to tackle the misuse of service workers to push malicious ads.

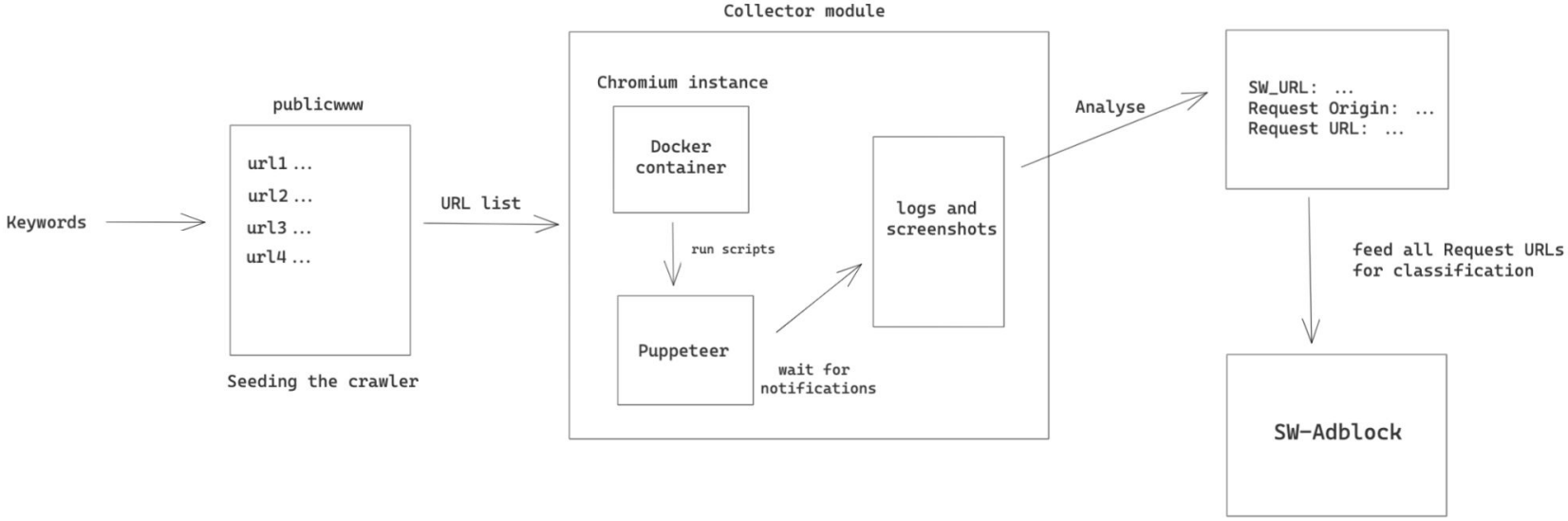
Approach

- We first manually seed a list of popular ad networks (such as Ad-Maven, OneSignal ...) and use their snippets to perform a source code search using publicwww.
- We gather a total of 14,000 websites that could potentially register service workers and publish WPN ads using this approach.
- We visited each URL and retained only those that actually make a request for a notification permission.
- We obtain 997 URLs that issued a notification permission request.

Approach

- We develop a data collection module leveraging a freshly instantiated chromium browser to automatically permit notifications.
- Once a website is loaded, we use a Puppeteer script to listen to service worker events such as *serviceworkercreated*
- SWs subscribe to push notifications via a Cloud Messaging Platform such as Firebase Cloud Messaging, our Puppeteer script logs these communications as well as.
- Further, we build a dataset of websites and ad networks for further analysis

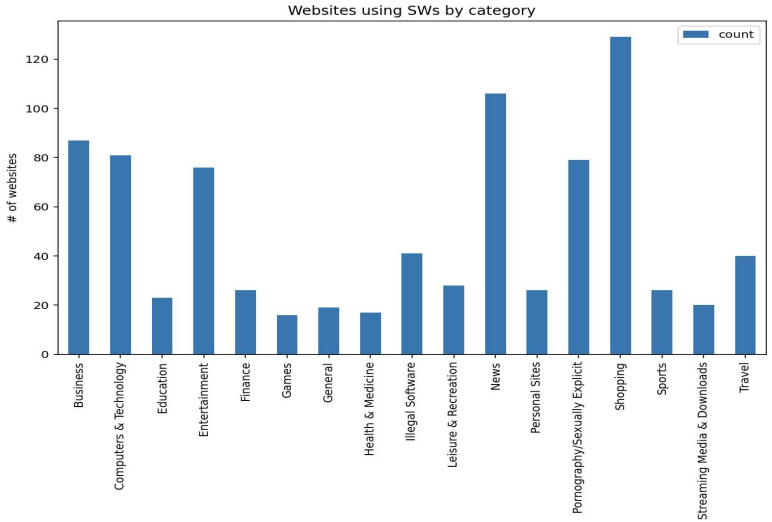
System overview

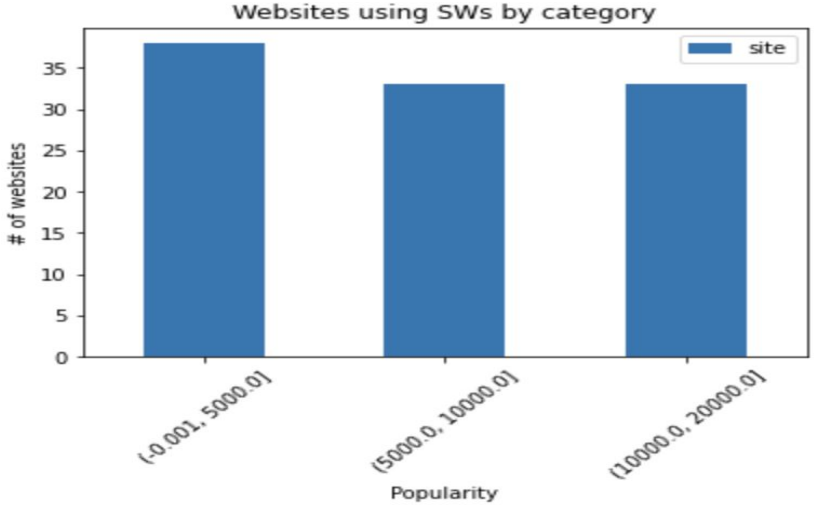


Logs

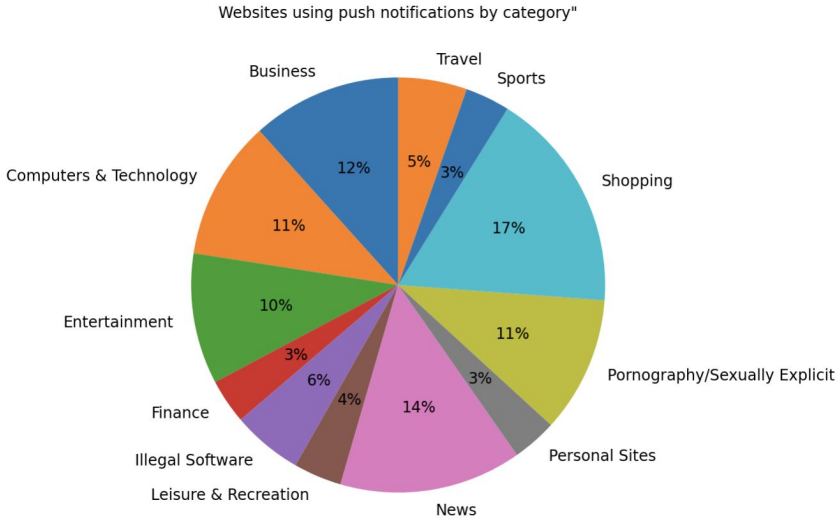
```
(venv) gaganganapathyas@Gagans-MacBook-Pro DataCollector % python3 docker_monitor.py
[Visiting Page started @ 2021-12-3 04:46:07 ]
        ID :: 1638506754.37936_vada_pav
        URL :: https://www.indiatoday.in/
        ||
                [Service Worker Registered @ 2021-12-3 04:46:39 ]
                SW URL :: https://www.indiatoday.in/service-worker.js
        ||
                SW Status :: New
        ***
                [Service Worker Request called @ 2021-12-3 04:46:41 ]
                Request Id :: 224.480
                Request Origin :: https://www.indiatoday.in/service-worker.js
                Request URL :: https://www.indiatoday.in/service-worker.js
        ***             Response file saved     ***
                [Service Worker Request called @ 2021-12-3 04:46:45 ]
                Request Id :: 224.517
                Request Origin :: https://www.indiatoday.in/service-worker.js
                Request URL :: https://cdn.izooto.com/scripts/workers/47d5a439dc84bb1630674aaff9947baeeb5e6f90.js
        ***             Response file saved
```

Evaluation

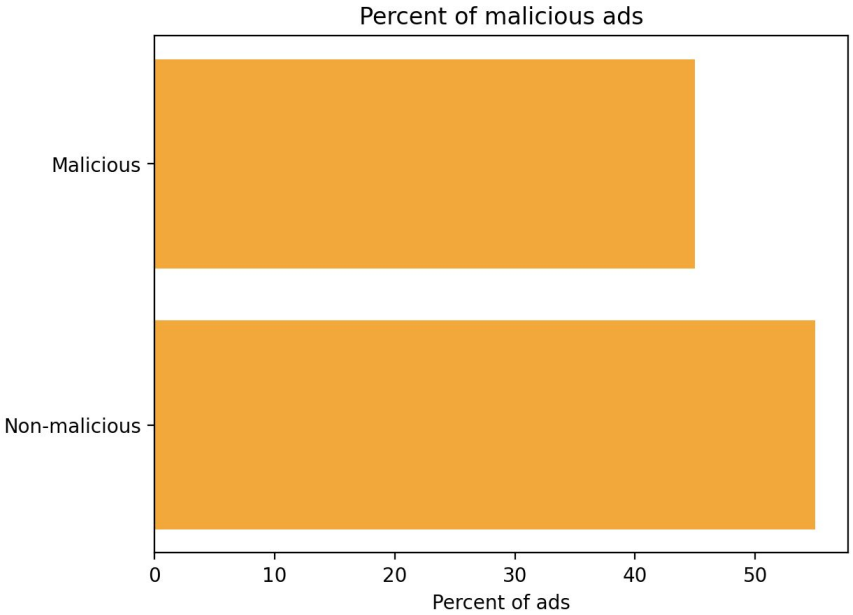

Websites using SWs by category
count
# of websites
0
20
40
60
80
100
120
Business
Computers & Technology
Education
Entertainment
Finance
Games
General
Health & Medicine
Illegal Software
Leisure & Recreation
News
Personal Sites
Pornography/Sexually Explicit
Shopping
Sports
Streaming Media & Downloads
Travel


Websites using SWs by category
site
# of websites
0
5
10
15
20
25
30
35
(-0.001, 5000.0]
(5000.0, 10000.0]
(10000.0, 20000.0]
Popularity

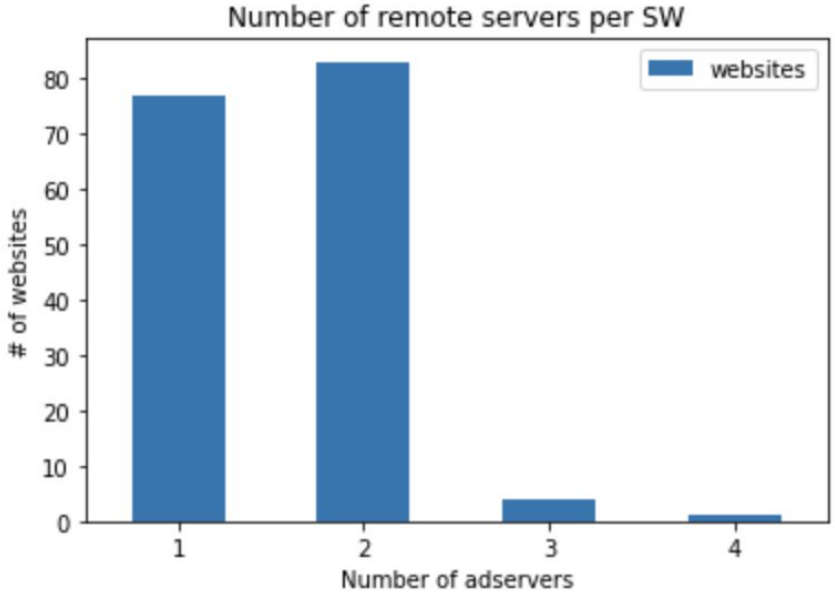
Evaluation


Websites using push notifications by category"
Business
Travel
Sports
Computers & Technology
Shopping
Entertainment
Pornography/Sexually Explicit
Finance
Personal Sites
Illegal Software
Leisure & Recreation
News
12%
5%
3%
17%
11%
10%
11%
3%
6%
4%
14%

Evaluation


Percent of malicious ads
Malicious
Non-malicious
0
10
20
30
40
50
Percent of ads

Evaluation


Number of remote servers per SW
websites
# of websites
0
10
20
30
40
50
60
70
80
1
2
3
4
Number of adservers

Conclusion

1. Out of 14,000 websites about 7% of the websites use service workers.
2. News and Shopping websites are the categories that use service workers the most.
3. Most top ranking websites deploy service workers presumably to provide better user experience.
4. Around 70% of the websites that use service workers also use push notifications. The static assets and network responses are stored in this cache.
5. Around 56% of the websites that use service workers also push ad notifications through third-party servers.
6. About 45% of the ads that are pushed are recognised to be malicious by Virua Total API.
7. Finally, we studied the number of 3rd party servers that a service worker connects to. Our observations state that most service workers connect to a maximum of two remote servers for push notification.