**Android Ads Test Summary**

**Device**: Android LG Stylo 4, LM-Q710ULM, Hardware Version Rev 1.0, Android 8.1.0

**Summary**:

Unable to see TSS ads type from 5 different types of apps tests performed

The tests for each apps were done 3 times for each ad networks with incognito mode

Total tests: 5 \* 3 \* 8 = 120 tests (least)

|  |  |  |
| --- | --- | --- |
| **Apps Installed (Browser)** | **Version** | **Ads types found** |
| Chrome | 78.0.3904 | Gaming sites, Notifications, Lottery, Adult sites, Scareware |
| Microsoft Edge | 42.0.2.4048 | Notifications mostly, followed by some legit ads (one of the ads has one of search query Ex. "How many luggage’s Lufthansa air allows”, adult site etc. |
| Brave | 1.5.1 | Gaming sites, Adult, Notifications |
| Firefox | 68.2.1 | Gaming sites, Adult, Notifications, Lottery, Scareware |
| UC Browser | 12.13.5.1209 | Scareware (Index, HTML, CSS, JS), Movies, Sample link Scareware 1, Scareware 2 |

**Current Publisher Account Balance Info of QuickWebchecker**

|  |  |
| --- | --- |
| **Ad Network** | **Amount Balance as of Nov 21, 2019** |
| Admaven | $0.007 |
| PopMyAds | $0.09 |
| HilltopAds | $1.78 |
| PopAds | $0.14 |
| Propeller | $0.001 |
| Revenue | $0.04 |
| PopCash | $0.03 |
| **Total** | **$2.151** |

**Mac OSx Ads Test Summary**

**OS Platform:** Mojave 10.14.6

**Summary Mac:**

* Surprising that Update Flash Player is the most common type of ad found.
* The second commonly found among other ad network were Notification attack.
* The third least common type were of TSS types (Mac OS Virus TSS)
* In PopMyAds: 2/3 ads that were found were more likely of TSS types
* In PopAds: 1/4 ads that were found were more likely of TSS types
* In Admaven: 1/6 ads that were found were more likely of TSS types
* Note: Hilltop Ads was giving me “Eat my cells” the generic page, perhaps could have identified as publisher? The Windows reports on below is quiet TSS supportive, this brings a suspicion of being detected of publisher account and always having “Eat my cells” ad being popped.

|  |  |  |  |
| --- | --- | --- | --- |
| **Browser** | **Browser Version** | **TSS Found Ad Network** | **Likelihood** |
| Safari | 13.0.3 | PopMyAds  PopAds | Highly (2/3)  More Likely (1/4) |
| Chrome | 78.0.3904.108 | PopMyAds | Highly (2/3) |
| Firefox | 70.0.1 | PopMyAds  Admaven | Highly (2/3)  Likely (1/6) |
| Brave | 1.0.1 Chromium 78.0.39 | No Ads of any type | None (0/all hosted page) |

**Windows Ads Test Summary**

**Platform: Windows 10**

Each browser exhibit differently for Windows. The breaking down of each browser experience as follows.

**Edge Summary:**

* In Hilltop ads (Edge): 5/5 tests consecutively with incognito gave TSS types (Windows TSS type)
* The second kinds of ads that were found were of Flash Player Download and Messenger2Go download (Facebook Messenger like)
* The third but few were of Adult ads type
* There was no notification ads target found as Edge does not support Notifications.

**Chrome Summary:**

* Notifications and extension download (Add Mega Music Search) were the most found type
* The second category were of adult types, Download (Messenger2go, Flash Player)
* Unable to see TSS attacks: Hilltop ads and PopAds were displaying more of Update Flash Player and Messenger2go Download types ads

**Firefox Summary:**

* Notifications and Flash Download were the most common types
* The second type were of “adds-on” / fake plugins download
* Unable to see TSS attacks: Hilltop ads and PopAds were serving mostly flash player, gaming ads and some adult sites

**Brave Summary:**

* Was able to block all ads in all hosted page

|  |  |  |  |
| --- | --- | --- | --- |
| **Browser** | **Browser version** | **TSS Found Ad Network** | **Likelihood** |
| Edge | 44.18362 | Hilltop | Highly |
| Chrome | 78.0.3904.108 | No TSS | None |
| Firefox | 70.0.1 | No TSS | None |
| Brave | 1.0.1 Chromium 78.0.3904.108 | No TSS | No Ads of any type |