Wireless Application Service Providers' Association

Report of the Adjudicator

Complaint number	#41413
Cited WASPA members	Marvel Media Sdn. Bhd (1514)
Notifiable WASPA members	n/a
Source of the complaint	WASPA Compliance Department
Complaint short description	Reasonable steps not taken to prevent fraudulent use of member's networks and systems.
Date complaint lodged	2019-05-28
Date of alleged breach	2019-04-17
Applicable version of the Code	v16.6
Clauses of the Code cited	4.11(a) and (b)

Related complaints considered	#39139
Fines imposed	Payment of R50 000 for contravention of clause 4.11(a) and R50 000 for contravention of clause 4.11(b).
Other sanctions	n/a
Is this report notable?	n/a
Summary of notability	n/a

Complaint

1. The Complainant initiated a complaint against the Member as a result of a fraud investigation conducted on behalf of WASPA on 17 April 2019 by Fraud Find.

2. The investigator downloaded and installed an application called *"EZ Cleaner Pro-Boost"* from a third party site onto a Samsung J5 cell phone.

3. After the application had been installed, the MSISDN used by the investigator was automatically subscribed to the Member's subscription service at a cost of R7 per day, without any explicit step being taken by the investigator in this regard.

4. As a result of the subscription, the airtime balance for the MSISDN was reduced from R46.00 to R33.00, i.e. a deduction of R13.

5. The Complainant alleged that the automatic subscription to the Member's service was fraudulent and that the Member had failed or omitted to take reasonable steps to prevent its systems from being used in a fraudulent manner.

6. The packet capture data obtained by the investigator detected that a malicious application known as *com.adflash.ezcleaner* had been used.

7. WASPA distributes a list of suspicious applications and sources to all its members from time to time (the ‘’Blocklist’’). All members are required to implement a system whereby any request emanating from applications listed on the Blocklist are blocked and do not get passed on to any Mobile Network Operator (MNO).

8. The Complainant alleged that an updated version of the WASPA Blocklist had been sent via email to the Member on 2 July 2018 and that this particular malware had been included in the Blocklist.

9. The Complainant alleged further that the Member had breached clause 4.11 of the WASPA Code of Conduct by failing or omitting to take reasonable steps to prevent its networks and systems from being used in a fraudulent manner.

10. In particular, the Member had not complied with WASPA's published best practices for fraud prevention, and the Member had failed to block interactions with a specific application as soon as reasonably possible upon notice from WASPA to do so, but in no later than twenty-four (24) hours (including weekends and public holidays) under any circumstances.

11. The evidence provided by the Complainant in support of its complaint included the following:

    a) a video displaying the installation of the malware and the auto subscription;

    b) a PDF document displaying images of the test results from the video;

    c) a packet capture data report displaying the HTTP header: *‘’X-Requested-With: com.adflash.ezcleaner’’*;

    d) The latest WASPA Blocklist, dated 13/05/2018; and

    e) email logs as proof that WASPA had emailed an updated Blocklist, which included the malware named *com.adflash.ezcleaner*, to the Member on 2 July 2018.

12. The complaint was initially referred to an emergency panel hearing due to the urgency and seriousness of the matter. However, the emergency panel could not make a conclusive finding and directed that the complaint be referred to formal adjudication and that the Member had to provide further and conclusive proof that the necessary blocks had been implemented correctly on its system.

Member's response

13. In its initial response to the complaint, the Member confirmed that it did update its systems to block applications appearing on the WASPA Blocklist as soon as it was received from WASPA.

14. The Member stated that it had run multiple stress-tests on its systems after receiving the complaint and found that the HTTP header: *''X-Requested-With: com.adflash.ezcleaner''* was not presented. The Member provided a txt.file with an extract from its own logs, which confirmed that the HTTP header was missing.

15. The Member submitted video evidence showing two scenarios, one where the block for this malware was implemented, and the other where it was not. The video demonstrated that when the block was activated, it operated correctly and the user was redirected to the Google home page. When the block was turned off, the user was redirected to the landing page for the subscription service.

16. The Member speculated that the malware may have penetrated its system in this particular case because of the free open-source PHP web framework used by the Member for the development of its web applications.

17. The Member confirmed that it since made a change to its systems to correctly implement the detection of ''X-Requested-With'' HTTP headers for each request made to its servers.

18. The Member also challenged the accuracy and completeness of the packet capture data reports provided by the Complainant. Firstly, the Member referred to the fact that the relevant HTTP header - *''X-Requested-With: com.adflash.ezcleaner''* - appeared and disappeared at various times throughout the HTTP request and response flow, as depicted on the logs provided by the Complaint. Secondly, the Member referred to the absence of a response body for certain requests in the logs provided by the Complainant, which meant that the request would not have been actioned any further.

19. The Member asked that the logs be checked and resubmitted by the Complainant to enable the Member to conduct further investigations into the matter.

Complainant's further response

20. The Complainant responded to the assertions made by the Member by categorically stating that the packet capture logs, MP4 video, and all supporting documents provided in support of the complaint against the Member were complete and had not been altered or tampered with.

21. The Complainant then went on to provide a detailed explanation for each of the requests and response data appearing on the logs provided.

22. In particular, the Complainant gave an explanation for why the *''X-Requested-With: com.adflash.ezcleaner''* HTTP header may not always appear for each of the requests on the logs.

23. The Complainant explained that when an application uses Google Android's ''WebView'' to request a web page, WebView attaches an extra header named ''X-Requested-With'' with the relevant app ID.

24. According to the Complainant, the "X-Requested-With" header script was designed to be used as a flag to mark AJAX (Asynchronous JavaScript and XML) requests. The header is non-standard, but it is used by many Javascript libraries. Most major Javascript

libraries and/or frameworks (like JQuery) will set the ‘’X-Requested-With’’ HTTP header for any AJAX requests.

25. However because Android’s WebView will set the ‘’X-Requested-With’’ HTTP header, it is possible that the returned results are JSON data, HTML body, or HTTP headers only with no body.

26. The packet capture logs in this case are based on server requests and responses, where the request method used is the *‘’GET’’* method. The GET method requests transfer of a current selected representation for the target resource[1].

27. The Complainant confirmed that the HTTP header - *‘’X-Requested-With: com.adflash.ezcleaner’’* - appears on the packet capture logs when the first request was made to a server controlled or managed by the Member (i.e. funious.com).

28. The Complainant argues that as this was the first interaction between the Android device making requests to a server controlled or managed by the Member, rules should have been implemented by the Member on its server to monitor and detect requests coming through from a package name included in the WASPA Block List (in this case the com.adflash.ezcleaner malware).

29. The Member’s server should then have terminated the connection and not returned anything back on the response to the Android device.

30. If the Blocklist was implemented at this first request, then the auto-subscription of R7/day would have been prevented as further requests would not have redirected to the aggregator’s server (api.netsmart.eu server).

31. The Complainant also highlighted on its logs that a further request was made to the Member’s server before a redirect request was sent to the aggregator’s server. The Complainant stated that this was a further opportunity for the Member to implement a block.

32. In response to the Member questioning the accuracy of the logs provided by the Complaint because there was no response body displayed for certain requests, the

[1] According to https://tools.ietf.org/html/rfc7231 ,

Complainant stated that it was possible not to have a response body returned on a HTTP request. It was also evident from the logs provided that the second request made to the Member's server with the HTTP header - *''X-Requested-With: com.adflash.ezclean''* - was returned with a response body. The returned HTML status code for this request was 302 Found, which meant that the request was redirected despite the HTTP header being present.

33. In responding to the Member's argument that the request forwarded to its aggregator was also missing the "X-Requested-With" HTTP header, the Complainant stated that this was irrelevant since the flow should already have been blocked on at least two occasions before any requests were forwarded to the aggregator's server.

34. In any event, the Complainant again pointed out that this was a redirection (HTTP 302) from the second request to the Member's server, which had displayed the HTTP header - *''X-Requested-With: com.adflash.ezclean''*. The Member failed to implement the blocklist on this second request too, even after returning with a response body with the extra parameter appended on the URL.

35. The Complainant also stated that the Member's reference to the logs for the traffic to the MNO's servers had no bearing on the complaint as those servers were outside of WASPA's jurisdiction. Nevertheless, the Complainant argued that the request to the MNO server was not a redirected page, which might explain why the ''X-Requested-With'' HTTP header could be seen again.

Member's further response

36. The Member was given a further opportunity to respond to the statements and arguments made by the Complainant.

37. The Member again reiterated that it had immediately implemented the Blocklist after it was received from WASPA on 2 July 2018 and that it had ensured that the necessary steps were taken by it to ensure that applications included on the Blocklist were blocked.

38. The Member repeated its previous statement that on this occasion the HTTP header - *''X-Requested-With: com.adflash.ezclean''* - was not presented when a request was made to its servers. The Member states that if the HTTP header in question had been presented, its system would have successfully blocked the application (as shown in the recorded video provided).

39. The Member also denied that it used AJAX for calling the request and therefore the missing response body shouldn't be an AJAX issue.

40. The Member again questioned a request being passed on if it was missing the response body. In the logs received for this complaint, there was no response body, but the request proceeded to the next stage.

41. The Member questioned how it could prove its execution of the Blocklist correctly if no ''X-Requested-With'' HTTP header was presented in this case.

Sections of the Code considered

42. The Complainant cited clause 4.11 of the WASPA Code of Conduct as the basis for its complaint.

43. Clause 4.11 states:

Members must take reasonable steps to prevent their networks and systems from being used in a fraudulent manner, including:

(a) complying with WASPA's published best practices for fraud prevention;

(b) blocking interactions with specific applications or sources as soon as reasonably possible upon notice from WASPA to do so, but in no later than twenty-four (24) hours (including weekends and public holidays) under any circumstances; and

(c) reporting any fraudulent activity identified on their networks or systems to WASPA within twenty-four (24) hours (including weekends and public holidays) .

44. The best practices referred to in clause 4.11(a) are contained in WASPA's Fraud Detection and Mitigation Best Practice Guidelines (version 2.1).

45. The relevant provisions of the Guidelines relating to the detection and mitigation of certain fraudulent activity (including ''toll fraud''[2]) are found in section 3, which reads as follows:

3.2 DETECTION

The X-Requested-With HTTP header is inserted by Android applications making HTTP requests, so web traffic from applications will potentially contain this header.

By logging and monitoring for these application headers, one can form a profile for suspicious applications. Application traffic showing zero or little declines and a high amount of 'already subscribed' notifications suggests abnormal behaviour and should be flagged as a suspicious application profile.

Analyse the user behaviour of subscribers. Multiple subscribe attempts to a service or services in a short period should be flagged as suspicious, as this is not normal subscriber behaviour.

The headers for these subscriptions can be inspected for application traffic. Once applications with suspect profiles or user behaviour are identified, attempt to locate the apps in official app stores, install and test them for malicious behaviour.

Apps that are found to be automatically subscribing to services should be blocked, and reported to the Fraud Prevention Task Team (fptaskteam@waspa.org.za).

[2] Section 3.1.3 of the Guidelines describes toll fraud as *an application that tricks users to subscribe or purchase content via their mobile phone bill. Toll fraud includes any type of billing except Premium SMS and premium calls. Examples of this include: Direct Carrier Billing, WAP (Wireless Access Point), or Mobile Airtime Transfer. WAP fraud is one of the most prevalent types of Toll fraud. WAP fraud can include tricking users to click a button on a silently loaded transparent WebView. Upon performing the action, a recurring subscription is initiated, and the confirmation SMS or email is often hijacked to prevent users from noticing the financial transaction.*

3.3 MITIGATION

3.3.1 Blocklist

WASPA maintains a blocklist of known malicious applications. The list is updated periodically, and distributed to members via email and API push as and when it is updated. Please ensure you are on the relevant mailing lists to receive these updates. Contact secretariat@waspa.org.za for more information.

Applications are added to the blocklist when malicious behaviour has been observed.

Subscription attempts containing the X-Requested-With HTTP headers with known malicious applications on the blocklist should be blocked by the member across all MNOs.

It is recommended to return HTTP 200 with no HTML content since the pages are not being displayed.

Report malicious apps found in official stores to the store owner. If you believe that any of the applications in the block list are incorrectly listed, please contact secretariat@waspa.org.za

3.3.2 Effective fraud detection and prevention solution

The blocklist alone is not sufficient, since bad actors are constantly adapting their strategies, and new malicious applications enter the market at a rapid pace.

For this reason, an effective fraud detection and prevention solution must be implemented by Members across all MNO's to validate subscription requests and block requests that do not originate from human users. The solution should validate all subscription requests in real time. An effective solution is able to adapt to new threats as they emerge.

46. No further clauses were assigned by WASPA.

Decision

47. The Member has admitted that it received the WASPA Blocklist on 2 July 2018, i.e. almost 10 months before the investigation was conducted in this matter.

48. The Member has not challenged the Complainant's evidence that the Blocklist sent to the Member on 2 July 2018 included the name of the malware in this case, i.e. *com.adflash.ezclean.*

49. I am therefore satisfied that the Member was properly notified by WASPA of the suspicious application header - *com.adflash.ezclean* – and that the Member then had an positive obligation in terms of clause 4.11(b) to monitor its systems for this malware.

50. The Member also did not challenge the Complainant's evidence that the malware that was installed on the investigator's Android device was able to access the Member's servers and automatically subscribe the MSISDN without any human interaction during the subscription process and in such a way that the process was hidden from the investigator.

51. The Member also did not challenge the Complainant's evidence that the airtime balance for the relevant MSISDN was reduced after the subscription was activated.

52. I am therefore satisfied that fraudulent activity actually took place on the Member's system.

53. Section 3.2 of the WASPA's Fraud Detection and Mitigation Best Practice Guidelines (version 2.1) provides that a Member can monitor for suspicious applications listed on the WASPA Blocklist by looking out for HTTP headers labelled *"X-Requested-With",* together with the name of the application, which are inserted by Android applications making HTTP requests the Member's servers.

54. The Complainant provided packet capture data logs showing that the HTTP header: *"X-Requested-With: com.adflash.ezclean"* was displayed when at least two initial requests were made by this particular malware to a server controlled or managed by the Member (i.e. funious.com) when the transaction was initiated.

55. The Member has stated that the HTTP header: *"X-Requested-With: com.adflash.ezclean"* was not presented when the first requests were made to its servers. The Member has questioned how it could be expected to block the malware if it was not initially detected on its system.

56. However, after considering the evidence presented by both parties, and the detailed explanation given by the Complainant, there is no reason for me to doubt the accuracy and completeness of the logs presented by the Complainant, which clearly show that the relevant HTTP header was displayed in respect of the two initial requests made to the Member's servers.

57. The Complainant has given a cogent explanation as to why the HTTP header appears and disappears from the logs at various stages of the transaction flow and for why no response body was displayed in the logs for the initial HTTP request made to the Member's servers and why it was still possible for the request to proceed to the next stage of the transaction flow. In doing so, the Complainant has successfully refuted the assertion made by the Member that the logs provided by the Complainant were not accurate or complete.

58. Based on all the evidence provided in this complaint, I find that the Member has failed to implement the detection and mitigation measures required in terms of section 3 of the WASPA's Fraud Detection and Mitigation Best Practice Guidelines (version 2.1) and is therefore in breach of clause 4.11(a) of the WASPA Code of Conduct.

59. I also find that the Member failed or omitted to block the interaction between its systems and this specific application, namely *com.adflash.ezclean,* which had appeared on the Blocklist sent by WASPA via email to the Member on 2 July 2018. The Member has therefore also breached clause 4.11(b) of the WASPA Code.

60. The complaint is accordingly upheld in both respects.

Sanction

61. Effective fraud prevention and mitigation is clearly in the best interests of all stakeholders in the industry. Toll fraud and other fraudulent activities pose particular concerns for members and consumers alike in the context of subscription services, where consumers continue to be subscribed to such services without their knowledge or express assent.

62. The detection and mitigation measures set out in section 3 of the Fraud Detection and Mitigation Best Practice Guidelines are easy and inexpensive to implement.

63. The Member's failure or omission to implement the required measures must be viewed in a serious light. An appropriate sanction must take into account the serious threat that fraud poses to the industry as a whole.

64. In mitigation, it has been noted that the Member did take steps to change its system in order to implement the required detection and mitigation measures.

65. In aggravation, it is noted that fraudulent activity actually took place on the Member's systems. It is also duly noted that a previous complaint has been lodged against the Member for a similar breach of clause 4.11 (see complaint #39139) and that this complaint was upheld against the Member.

66. Based on the aforegoing, and in line with the sanctions imposed in similar complaints of this nature against defaulting members, the Member is fined an amount of R50 000.00 for the contravention of clause 4.11(a) and R50 000 for its contravention of clause 4.11(b).

67. Both fines are payable within 7 (seven) days of publication of this report.