Detailed and Technical Response To Recent Articles Alleging Malware On the Propeller Ads Network

I. Introduction

Propeller Ads is one of the Internet's largest advertising networks and has, for years, serving advertisements online for the world's largest brands on countless websites of every form. For nearly a decade, Propeller Ads has operated a platform that connects publishers with advertisers and does everything in its power, as explained below, to make sure all advertisements that it helps advertisers place comply with industry standards and law in the best interest of internet browsers, the advertisers, and the publishers.

However, recently, two authors published reports alleging that Propeller Ads has been implicated in a scheme to serve malware to users who view advertisements served through its network. The allegations against Propeller Ads in these reports are, at their heart, false and libelous.

While Propeller Ads hesitates to provide more attention to these unprofessional and misleadding reports, Propeller Ads does not want to let the allegations in the articles pass without detailed response and refutation and so it must reference the reports. Specifically, on July 27, 2020, Robin Wright of TechTarget.com published a report titled "Digital ad networks tied to malvertising threats – again," which in turn referenced a prior article by Mr. Wright titled "'Master134' malvertising campaign raises questions for online ad firms" and a report by Eliya Stein on Confiant.com titled "Tag Barnakle: The Malvertiser That Hacks Revive Ad Servers, Redirects Victims To Malware."

The reports contain strong, yet unsupported, indictments of Propeller Ads and other advertising networks by accusing them of being involved in malicious advertising campaigns and of monetizing them by making redirects through advertisements served through the Propeller Ads network. Each of these reports contains false, misleading, and libelous statements regarding Propeller Ads, to which Propeller Ads will respond herewith. However, to understand why the allegations are false, first we must explain what exactly Propeller Ads does.

II. The Propeller Ads Network

Propeller Ads is a general-purpose self-serve advertising network that helps connect advertisers with publishers. When an advertiser wants to get its advertisements onto the internet, it can use Propeller Ads' automated network to find websites that are willing to publish advertisements. The automated network helps the publishers set up methods for advertisements to bid for spaces on the publishers' websites and, when an advertiser purchases advertising space, the network serves the advertisements provided by the advertiser to the publisher.

Through this network, Propeller Ads acts as nothing more than an automated intermediary to help advertisers find the best publishers to publish their advertisements, and to help publishers to get the greatest utilization out of their advertising space. Propeller Ads is not involved in the creation of the advertisements or the operation of the publishers. As noted, the network is a "self-serve" network that allows the advertisers and publishers to connect with each other themselves through its automated systems.

And because of the incredible value that Propeller Ads brings in connecting advertisers with publishers, Propeller Ads has become one of the most popular advertising networks on the internet, helping serve 10,000 new advertising campaigns each week. It is this very ecosystem of advertising networks, like the one operated by Propeller Ads, that allows the Internet as we know it exist.

Propeller Ads does not endorse, support, or encourage any advertisement on its network. More to the point, Propeller Ads has a strict policy of forbidding advertisers from using the network to help advertise or distribute viruses, malware, or other unlawful or damaging content, and has implemented measures to limit this kind of content.

However, the very nature of this system, and its incredible popularity, also make it impossible to police every single advertising campaign, despite Propeller Ads taking every reasonable step, and implementing state-of-the-art technological methods, to prevent abusive uses of the network. It is neither physically possible, nor legally required, for Propeller Ads to manually and individually review every single advertisement or publisher website. Again, Propeller Ads helps serve over 10,000 new advertising campaigns each week. And so, despite Propeller Ads' best efforts and technological systems, like with any other network of this kind, some bad actors do manage to get through Propeller Ads' security systems and procedures for short periods of time before they can be tracked down and removed.

III. Propeller Ads Actively Combats Malicious Actors and Activities

Notwithstanding the false allegations of the authors of the reports, Propeller Ads does not work with these bad actors, does not turn a blind-eye to these bad actors, and in fact has implemented various legal and technological means to prohibit, catch, and terminate these bad actors when they are found. The three pillars of Propeller Ads' methods of combatting bad actors are though technological measures, a notice and take-down system, and legal means. Considering each of these in turn:

A. Technological Procedures and Systems

Propeller Ads has implemented technical procedures and systems to anticipate and detect unlawful or malicious activities on or through its network, which can detect robots, scripts, spiders, adware, malware, viruses, phishing offers, trojans and more, including malicious activities that use cloaking methods and other tricks.

Propeller Ads is constantly working to improve its service quality controls, guidelines, and policies, and is constantly updating its technological systems to catch new vectors and attacks used by bad actors. As bad actors develop new methods of attacking systems like Propeller Ads and internet users, Propeller Ads identifies those methods and takes action to stop their use.

This system is what keeps nearly 100% of advertisements served through Propeller Ads safe and secure. Propeller Ads has systems in place to protect users, publishers, *and* advertisers. But as any security researcher should know, it is quite literally impossible to prophylactically protect against all methods of attack, especially before the methods of attack have even been developed. Nevertheless, Propeller Ads has managed, through its strenuous efforts, to minimize malicious activities on its network such that it is almost relatively nonexistent. This has been possible only because of Propeller Ads' devotion and determination to remove bad actors from its system, and its adoption of strict, precise, and comprehensive policies and internal requires that Propeller Ads follows without exception.

With regards to the specific allegations in the reports, the authors have either acted negligently or have been willfully malicious to insinuate that Propeller Ads has knowingly or intentionally worked with the bad actors in the cases referenced in the reports. First, the advertising malware at issue in the reports are not viruses. From a technical standpoint, it is nearly impossible to technically distinguish

advertising malware from legitimate traffic in an advertising network until the moment that it reaches the device of the end user and starts operating. It is even more difficult to identify when the advertiser redirects an end user from what appears to be a legitimate advertisement on the network to an illegitimate website off the network. Thus, the only sure-fire way to combat such bad actors is through a robust notice and takedown system, like the one that Propeller Ads has in place, described below.

As a result of Propeller Ads' efforts, we believe that Propeller Ads is one of the cleanest advertising networks available – and certainly among advertising networks of its size. If any malicious activities appear on or through the network, it is not a result of Propeller Ads' intention or neglect, but only through the extraordinary efforts of bad actors who work to circumvent Propeller Ads' efforts.

B. Notice, Takedown and Termination Procedures

For a tiny fraction of a percent of advertisements, advertiser websites, or publisher websites that contain malicious activities that get through Propeller Ads' technological measures, Propeller Ads has implemented a notice and takedown procedure that allows *any* person to report suspected malicious activity, which Propeller Ads acts on promptly.

Specifically, any person, whether it be an end user, a publisher, an advertiser, a researcher, a security professional, or an author for a security publication, can contact Propeller Ads through a variety of means to report any suspicious or malicious activities occurring on or through the Propeller Ads network. These reports may be made via email to contact.us@propellerads.com or through any of the other methods of contact which Propeller Ads has made available on its website and its network.

When Propeller Ads receives such a report of suspicious or malicious activity, it creates a ticket to make sure the report is properly tracked and immediately begins its process to attempt to resolve the alleged issue. In cases where it is clear that the advertiser or publisher is acting in violation of Propeller Ads' Terms and Conditions (see below) or is otherwise acting in violation of law, Propeller Ads immediately halts the malicious activity through its network.

In cases where Propeller Ads cannot clearly determine whether the activity is in violation of the Terms and Conditions or law, Propeller Ads immediately requires the accused advertiser or publisher to respond to the allegation. If

Propeller Ads does not receive a satisfactory and prompt response, it shuts down the advertising campaign. If there is any indication that the advertiser or publisher is repeatedly violating the Terms and Conditions, Propeller Ads terminates the advertiser or publisher from using the network entirely.

C. Legal Efforts and Procedures

From the legal perspective, Propeller Ads requires all publishers and advertisers to comply in all respects with its Terms and Conditions, which can be found at https://propellerads.com/terms/. The Terms and Conditions include a comprehensive list of prohibited activities on behalf of both publishers and advertisers, require them to provide wide-ranging representations and warranties, and subject them to significant liability in the event of their breach of the Terms and Conditions.

Specifically, but without limitation, the Terms and Conditions include provisions regarding the following:

1. Propeller Ads does not permit advertisers or publishers in a wide range of unacceptable activities and organizations, including terrorist organizations, military, arms and/or ammunition manufacture or sales, money laundering, criminal activities, sanctioned activities and organizations, or political organizations. Contrary to assertions made in the report by Rob Wright, Propeller Ads explicitly prohibits, and does not desire, pornographic advertisements or advertisers on its platform, which it believes is damaging to both its brand and its publishers, who do not desire such advertisements.

2. Propeller Ads reserves the right to forbid access to, suspend, ban, and close any account of any advertiser or publisher for any or no reason, including for violating any provision of the Terms and Conditions.

3. Propeller Ads requires publishers and advertisers to uphold the highest ethical and commercial standards. Each party must have all necessary rights and permissions for the advertising campaigns in which they participate, and holds each party responsible for their violations of the standards and rules.

4. Propeller Ads fully, unambiguously, and unquestionably prohibits any parties from engaging in any form of fraud, from disguising or cloaking ads with different content or landing pages, or from redirecting users. Any persons who engage in these activities are banned and can be subject to legal action.

5. Advertisements themselves may not contain pornography, illegal activities, racial, ethnic, political, hate-mongering or otherwise objectional content, or content that is violent or obscene. Advertisements may not contain or promote illegal substances, drugs or related paraphernalia. Advertisements may not contain adware, malware, viruses, or be a part of any phishing scene. Misleading ads are wholly prohibited.

Propeller Ads reserves the right to take legal action against all advertisers and publishers who violate the Terms and Conditions and may seek to hold the advertisers or publishers liable for injuries that they cause to third-parties as a result of their unlawful activities.

Propeller Ads also works cooperatively with law enforcement from around the world to curb abusive uses of its system including, where permitted and appropriate, disclosing information about advertisers and publishers who have violated law, all in an effort to halt their malicious activities and hold them responsible for their unlawful conduct. Propeller Ads works voluntarily with law enforcement from jurisdictions around the world, even those jurisdiction in which Propeller Ads is not obligated to cooperate because it is not subject to their laws. Propeller Ads does this because it is devoted to making sure that its network is clear from malicious activities and safe for users, advertisers, and publishers.

IV. Responses to Specific Allegations in the Reports

Given all of the foregoing, one may believe that Mr. Wright and Mr. Stein were simply uninformed about the allegations in their reports and that their false statements regarding Propeller Ads were simply made negligently. However, both Mr. Wright and Mr. Stein hold themselves out as experts in this field and should be knowledgeable about how Propeller Ads works, or at the very least should have reached out for comment to Propeller Ads before making their allegations. However, they did not contact Propeller Ads and made their misleading and false allegations, nonetheless. We will now respond directly to some of those allegations.

Mr. Stein alleges that Propeller Ads is "well documented to be a purveyor of malicious demand, including a large quantity of adware trojans that are disguised as fake Flash updated." This is false. Propeller Ads has a highly regarded reputation in the industry after operating for nearly a decade and offering the highest quality of services by establishing long-term relationships with its clients

and customers. Propeller Ads has never been subject to any lawsuits or governmental actions arising from any purported malware, adware, trojans, advertising fraud, or other malicious activities. As the only support for his statement, Mr. Stein cites solely to one of the reports by Mr. Wright (thereby engaging in circular citations) and another article acknowledging that Propeller Ads cannot control all malicious activity on the internet and must deal with advertising malware like other major companies like the New York Times. This certainly does not mean that Propeller Ads is a "well documented ... purveyor of malicious demand." Mr. Stein made this statement without any basis, and it is flatly false.

Mr. Wright, in his report, as part of the circular citations, attributes a few statements to Mr. Stein, who stated that malicious actors "worked with Propeller Ads because they could make money by redirecting traffic from the hijacked ad servers to Propeller," that Propeller Ads "is the monetization partner of the attacker," and that "a victim is going to get redirected to something nasty through the Propeller network." These statements are all wholesale misrepresentation and misdirection.

As described in detail above, Propeller Ads takes extraordinary effort to keep off and remove malicious actors from its network. But when one of these malicious actors does get through Propeller Ads' efforts, that does not mean that Propeller Ads is working with them, that Propeller Ads is their partner, or that Propeller Ads is knows or intends for any users to be redirected to malware. Yet that is exactly the implication made by Mr. Stein and Mr. Wright and the implication is absurd. It is like implying that, even though the government constructed a toll road, hires police officers to protect the toll road, and prosecutes people who violate laws on the road, the government is nonetheless "working with," "partnering with," and acting in concert with someone who gets drunk and hits another driver on the toll road. The implication is absurd and libelous.

Once again, Propeller Ads has implemented numerous systems and procedures to prohibit, track down, and remove malicious actors and content from its network. When malicious actors take extraordinary measures to circumvent Propeller Ads' efforts, it is in violation of everything that Propeller Ads works for and strives for, and not anything that Propeller Ads desires to be a part of.

Though Mr. Stein apparently acknowledges this by stating that Propeller Ads is "pretty far down the steam" and that it did not know about the hacking of advertising servers that made the malware attack possible, Mr. Wright quotes Mr.

Stein as stating that "Propeller Ads is 'known to look the other way on things like this' in the past." This is absolutely false. As detailed above, Propeller Ads has implemented a robust notice, takedown and termination procedure under which it does not "look away" from any allegations of malware. Quite tellingly, neither Mr. Stein nor Mr. Wright provide any support for this false allegation, because there is none. This is yet another false and libelous statement.

Mr. Wright continues to quote Mr. Stein as stating that "when you take a random Propeller ad tag and refresh it and four out of five times you get either porn or malware." This statement is simply and empirically false. As explained above, both porn and malware are prohibited from the Propeller Ads network. Aside from all the other reasons Propeller Ads would not have such content on its network, it does not serve Propeller Ads' interests to allow content that its publishers and end users find objectionable. Propeller Ads has become one of the biggest advertising networks on the Internet because publishers trust the advertisements served through its network. Propeller Ads simply could not exist if 80% of the advertisements were porn or malware, as Mr. Stein states. But to the extent does get past Propeller Ads' measures, it is a fraction of a percent of advertisements served through the network. There is no explanation or excuse for Mr. Stein making this false statement.

V. Conclusion

Propeller Ads stresses once more that it is a self-serve network acting as an intermediary between advertisers and publishers. It has implemented multiple systems and procedures to make malware and other undesirable content nearly non-existent through its network. However, to the extent any such content does find its way onto the system, Propeller Ads is not intentionally involved in it and is not responsible for it.

Mr. Wright and Mr. Stein however have intentionally and falsely implicated Propeller Ads in the activities of the very people that Propeller Ads takes much effort to remove from its network. The reports by Mr. Wright and Mr. Stein are accordingly misleading, false, and defamatory.

Propeller Ads does not intentionally, willfully, or knowingly work with malicious actors like the ones referenced in Mr. Wright and Mr. Stein's reports. When Propeller Ads learns of any such alleged activities, it takes prompt action thereon.

Propeller Ads requests that Mr. Wright and Mr. Stein immediately rescind their reports.

This document is not intended to constitute, nor shall it be deemed to constitute, a full statement of all facts, rights, or claims relating to this matter, nor is it intended, nor shall it be construed as, a waiver, release, or relinquishment of any defenses, rights, or remedies available to Propeller Ads, whether legal or equitable, all of which are hereby expressly reserved.