Tag Barnakle threat actor compromises over 120 more adservers

April 21 2021, by Sarah Katz

Credit: Confiant via Unsplash.com

Around one year ago, the security research company Confiant revealed a threat actor group called Tag Barnakle that targeted Revive Adserver instances on a mass scale. Now, however, Confiant has discovered that

their publicization of Tag Barnakle's activity hardly detracted from the group's confidence.

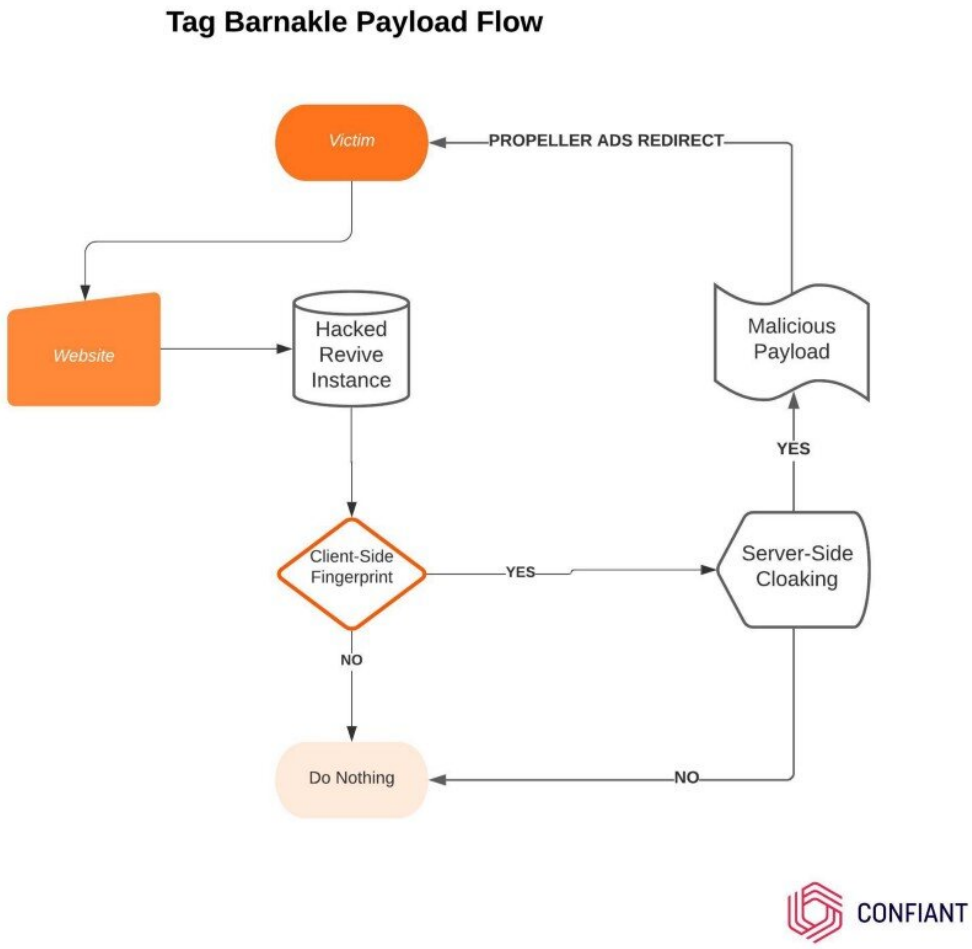
As a recap, the majority of malvertising groups operate mainly by targeting large advertising platforms by posing as media buyers with helpful tech expertise. In short, they aim to persuade these platforms to incorporate them into their infrastructure without inspecting the cloaked malicious entities too closely.

On the other hand, Tag Barnakle functions by directly compromising the ad serving infrastructures of these large platforms. This way, by skipping the step of running an ad campaign, they can typically manage to save a lot of money up front, thus increasing their ROI.

At that point, news of the attack spread across sources such as BleepingComputer and ZDNet regarding 60 ad servers compromised via malicious ads. Most recently, over the past 12 months, Tag Barnakle has migrated to mobile attacks.

From what Confiant can gather, the attack process goes as follows: Hacked Revive Adserver > Malicious Payload > Client-side Fingerprinting > Server-side Cloaking > Secondary Payload > Propeller Ads

This means that once the malicious payload communicates the Client fingerprint back to the attacker's server, the attacker relays new Javascript for the payload to execute. At this time, Tag Barnakle seems to be targeting mobile devices with WebGL parameters. This new server-side code only goes through if the targeting client parameters match.



Credit: Confiant

According to Confiant's research, these evil Propeller Ads look quite similar to the generic kind of malvertising to which many users are accustomed. These fake ads typically involve alerts about alleged compromised devices in order to persuade the user to install malicious software labeled as an antivirus or scanner. Moreover, many of these ads

might even lure users to the app store tools for Safety/Security/VPN apps that either use malicious ads themselves or include hidden subscription costs.

So far, in terms of reach, Tag Barnakle seems to have the most traction with long-tail websites and moderately trafficked ad publishers. Among these entities, many seem to host their technical stack on Revive servers.

When de-obfuscating such suspicious traffic in any kind of mobile forensics, researchers have determined that payloads tend to show calls to Propeller Ads, meaning that potential affected users and companies might want to keep those sorts of calls in mind when performing their own investigations.

More information: Stein, E. Tag Barnakle One Year Later: 120+ More Revive Adserver Hacks. Confiant, 19 Apr. 2021. blog.confiant.com/tag-barnakle … r-hacks-f3e5b3bc8e70