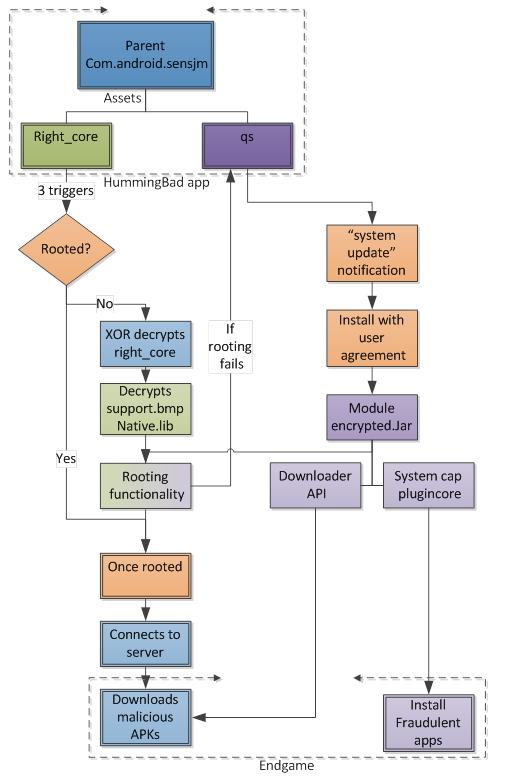
**HummingBad Malware:**

**What is HummingBad**: If you are an android user and you do download apps from 3rd party then you may have seen this or other from its family. HummingBad is a malware that uses known android exploits to display ads, download other malicious apps, and produce fake ratings on the internet. It was discovered by Checkpoint researchers in February 2016. This malware is a Trojan adware, it tries to root your device and gain system access. In the report of Checkpoint, it is told that this malware was created by a Chinese mobile and server company called Yingmob. This malware has helped generate them $300,000 every month.

**How it Works:** This malware takes the help of Android fragmentation. Google constantly updates its android OS. Mobile manufacturers and carriers may not provide these updates which leave behind the vulnerability that provides a way for these attack

**Fig:** Working of HummingBad malware. [2]

As shown in the figure this malware attacks in two different ways. When it gets access to your system as a Trojan, it looks for 3 events to fire its attack: BOOT\_COMPLETED, TIME\_TICK, or SCREEN-ON. Then malware checks if the device is rooted or not. If it is rooted it continuous if not it decrypts its file called right\_core.apk which launches multiple exploits to root a device. If secret rooting fails it tries to exploit social engineering and send notification of system update. The installed app will be a fraudulent app that will decrypt Module\_Increpted.jar which will have the same capabilities as right\_core. At this point, the malware has resources to connect with the advertising server and will throw all kinds of advertisements. It will also install lots of apps without your permission. If the root is successful it can be even dangerous. The root will give malware access to the system app; malware will seat on your device as a system app so even if your system reset your phone it can reinstall. With root access, it can also generate a fake IMEI number in the same device and redownload the same app and get paid for the referral.

**Why Was it Created:** According to checkpoint it was mainly created for making money. According to the article published by checkpoint and outlook here are some numbers:

“The apps display more than 20 million advertisements per day.

Yingmob achieves a high click rate of 12.5% with illegitimate methods, resulting in over 2.5 million clicks per day.

HummingBad installs more than 50,000 fraudulent apps per day.”

These all number translates to an average revenue per click of $0.00125, revenue from clicks- more than $3000 per day, revenue from a referral - $0.15 per app and over $7,500 per day. Which totals to $10,000 per day.

**Effects:**

**A screenshot of a cell phone

Description automatically generated**

**Fig:** Cumulative users effected from August 2015 to May 2016: [1]

**A picture containing accessory, text, umbrella, vector graphics

Description automatically generated**

**Fig:** Countries mostly affected by Hummingbad by the end of May 2016. [1]

**A close up of text on a white background

Description automatically generated**

**Fig:** Different OS versions affected by Hummingbad. [1]

The most recent Android operating system Marshmallow[4] of that time was also affected by the malware attack.

**Mitigation and Prevention:** The sad part is this malware or malware of these kinds are all over the internet, especially if you download a patched software from 3rd party. So, avoid downloading anything from 3rd party.

You might be thinking that if you download the app from the play store you will be saved, but this malware was found even in the apps inside the play store. Because of this new malware, Google had to change its whole policy and implement strict security checkups before one could publish an app in the play store.

The best way to Mitigate this malware will be to use a secured phone which regularly gives you updates like Motorola, Nexus, Pixel; all from google family. There are some Chinese makers like Xiaomi, Huawei, but these phones are not compatible with security features provided by our telecom so that can be another security loophole.

Reference

[1] “From HummingBad to Worse,” *Checkpoint Software*, Jul. 2016.

[2] “HummingBad: A Persistent Mobile Chain Attack,” *Check Point Software*, 04-Feb-2016. [Online]. Available: https://blog.checkpoint.com/2016/02/04/hummingbad-a-persistent-mobile-chain-attack/. [Accessed: 26-Jan-2020].

[3] “A spike in Shedun, also known as HummingBad,” *The Shield*. [Online]. Available: https://blog.lookout.com/a-spike-in-shedun-also-known-as-hummingbad. [Accessed: 26-Jan-2020].

[4] “Android version history,” *Wikipedia*, 23-Jan-2020. [Online]. Available: https://en.wikipedia.org/wiki/Android\_version\_history. [Accessed: 26-Jan-2020].