<http://blog.checkpoint.com/2016/02/04/hummingbad-a-persistent-mobile-chain-attack/>

Name: Hummingbad

Affected Platform: Android

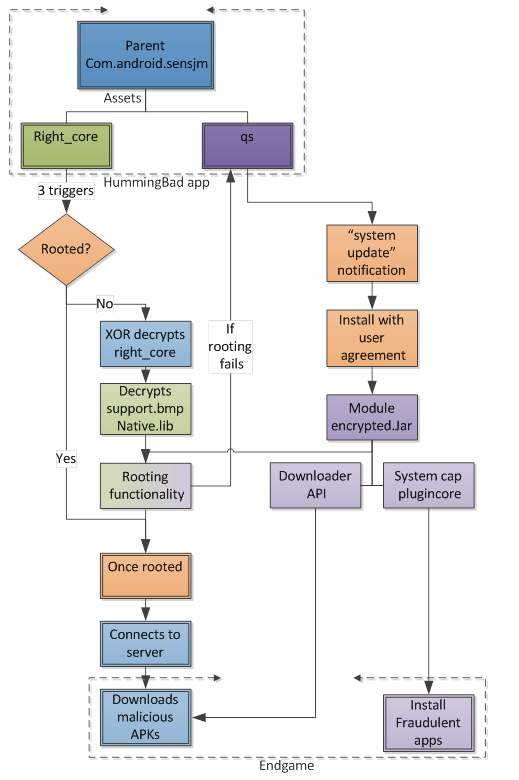
Found originally by: Check Point

Main Info:

* HummingBad, this malware establishes a persistent rootkit with the objective to generate fraudulent ad revenue for its perpetrator, similar to the BrainTest app discovered by Check Point earlier this year.
* HummingBad installs fraudulent apps to increase the revenue stream for the fraudster.
* CP's analysis of the HummingBad malware shows that multiple fraudster groups continue to evolve their methods, including assuring the persistency of the malware once the infection is successful.
* This campaign is the latest in a series initiated by various fraudster groups in the last 4 months.
  + This epidemic of Android malware includes BrainTest, PushGhost and Xinyinhe.
* Moreover, as the malware installs a rootkit on the device, it enables the attacker to cause severe damage if he decides to change his objectives, including installing key-logger, capturing credentials and even bypassing encrypted email containers used by enterprises.

HummingBad: A complex Malware:

* HummingBad starts a sophisticated chain attack that's interesting in a few respects.
  + First of all, the malware's malicious components are all encrypted.
    - This makes it much harder for security solutions to detect that it is malware since no malicious code is visible for inspection.
  + Second, the malware initiates a silent attack vector.
    - If this fails, the malware will initiate a second attach vector which has the same capabilities as the first one.
    - This is an interesting course of action for mobile threats because redundancy helps the perpetrator ensure the objective is met.
    - Finally each attack vector consists of several stages, including decrypting and unpacking the actual malicious codes.



The Two Attack Vectors:

* HummingBad contains within its assets two files, and each generates a separate attack.
* The first attack vector generates a silent operation triggered by one of three common events on the device:
  + BOOT\_COMPLETED - occurs after booting the device.
  + TIME\_TICK - occurs every time a minute passes
  + SCREEN\_ON - occurs when the screen is turned on
* The malware then checks if the device is rooted or not.
  + If the device is rooted, the malware continues straight to act on its objective.
  + If the device is not rooted, the parent malware XOR decrypts a file from its assets called right\_core.apk [every character is XORed against 85).
  + The right\_core.apk then decrypts a native library from a file called support.bmp.
  + This native library is used to launch multiple exploits in an attempt to escalate privileges and gain root access.
* Once elevated to root, the malware establishes communication with one of its C&C servers.
* From the server, the malware downloads a list of malicious APKs.
* The second attack vector, called qs, is initiated only if the first vector failed to gain root.
  + This attack vector uses social engineering in order to achieve its purpose.
  + The component "qs" is also XOR encrypted and needs to be decrypted by the parent malware.
* Once unpacked, the malware pops up a fake user notification regarding a system update.
* If the user opens the notification, he is required to authorize the installation of the "system update" which is actually a malicious APK.
* The malware then hides its own icon and DES decrypts a file called module\_encrypted.jar.
  + The module\_encrypted.jar component has the same capabilities as right\_core, in addition to several new exploits.
* At this stage, the malware will try to connect to its C&C servers for further commands.
* The server can initiate several actions by the malware:
  + Download apks from a URL provided by the server and install it.
    - Depending on if the root access was successfully established, the application will install the apk silently or show an install dialog containing text provided by the server.
  + Send referrer requests in order to create a google play advertisement revenue.
    - To achieve this purpose, the malware gets a list of packages and referrer ids from the server and then scans the applications running on a device.
    - Once it has collected this information the malware sends com.android.vending.INSTALL\_REFERRER intents with the corresponding referrer ID, in order to gain revenue.
  + Launch applications - the malware will get a list of packages from the server and try to launch them.
    - Send request to a URL provided by the server. In this case, the malware will get a URL from the server and will open a connection with the URL using a given user agent: Mozilla/5.0, Macintosh, Intel, Mac OS X 10.10, rv:38.0,Gecko/20100101, Firefox/38.0.
* It is interesting to note that all of the C&C servers are still alive and contain dozens of malicious APKs.
  + A few of the malicious binaries on the C&C servers have dropper capabilities of their own while others have rooting capabilities.

Other Info:

* Check Point's Mobile Threat Prevention identified the threat automatically by detecting exploitation attempts while examining the malware in the MTP emulators.
* The infection vector was a drive-by download attack, and indicates some adult content sites served the malicious payload.

List of C&C servers:

* hxxp://manage.hummerlauncher[.]com
* hxxp://cdn.sh-jxzx[.]com/z/u/apk
* hxxp://fget.guangbom[.]com
* hxxp://d2b7xycc4g1w1e.cloudfront[.]net
* hxxp://manage.hummerlauncher[.]com:10010/c/40
* hxxp://manage.hummerlauncher[.]com:10010/c/39
* hxxp://manage.hummerlauncher[.]com:10010/c/43
* hxxp://manage.hummerlauncher[.]com:10010/c/50
* hxxp://manage.hummerlauncher[.]com:10010/c/51
* hxxp://manage.hummerlauncher[.]com:10010/c/53
* hxxp://manage.hummerlauncher[.]com:10010/c/61
* hxxp://manage.hummerlauncher[.]com:10010/c/44
* hxxp://manage.hummerlauncher[.]com:10010/c/31
* hxxp://manage.hummerlauncher[.]com:10010/c/29
* hxxp://manage.hummerlauncher[.]com:10010/c/30
* hxxp://cdn.sh-jxzx.com/z/u/apk/SN-SDK-5002[.]apk
* hxxp://fget.guangbom[.]com:7012/getSSPDownUrl.do?cid=118
* hxxp://d2b7xycc4g1w1e.cloudfront[.]net/upload/apk/1435636098822.apk
* hxxp://fget.guangbom[.]com:7012/getSSPDownUrl.do?cid=119

Terms:

* **Media Transfer Protocol (MTP)**
* **Media Transfer Protocol Device Simulator (MTP Simulator)** - is a fully -featured, self-contained device simulator that emulates an MTP device.
  + Its primary purpose is to enable developers to exercise expected behavior based on the MTP specification by returning appropriate MTP response packets and generating MTP events.
* **Brain Test** - was a piece of malware masquerading as an Android app that tested the users IQ.
  + **Discovered by**: Check Point.
* **Ghost Push** - Is kind of malware which infects the Android OS by automatically gaining root access, downloads malicious software, converts to a system app and then loses its root access which makes it virtually impossible to remove the infection by factory reset unless the firmware is reflashed.
  + **Type**: Virus/Malware
  + **Discovered by**: Cheetah Mobile's CM Security Research Lab.
  + The malware hogs all system resources making it unresponsive and drains the battery.
  + Further investigation of Ghost Push revealed more recent variants, which, unlike older ones, employ the following routines that make them harder to remove and detect:
    - Encrypt its APK and shell code
    - Run a malicious DEX file without notification
    - Add a "guard code" to monitor its own processes.
    - Rename .apk files used to install the malicious apps.
    - Launch the new activity as the payload.
* **Xinyinhe** - Malicious adware family that allows for the complete takeover of an Android user's device.
  + **Discovered by**: FireEye
  + This attack is created by a mobile app promotion company called NGE Mobi/Xinyinhe.
  + Article: <https://www.fireeye.com/blog/threat-research/2015/09/guaranteed_clicksm.html>