Brain Test Re-Emerges: 13 Apps Found in Google Play

By Lookout

Published: 2016-01-06 · Archived: 2026-04-05 18:06:22 UTC

Summary

The malware family Brain Test, unfortunately, has made a comeback. Some variants attempt to gain root privilege, and persist factory resets and other efforts to remove it, especially on rooted devices.

Lookout consumer and enterprise users are protected.

In October 2015, we discovered several applications live in the Google Play Store that looked suspiciously like they were written by the developers behind the Brain Test malware family. Curiously, these apps had hundreds of thousands of downloads and at least a four star average review score -- indicating a satisfying app experience, not obtrusive adware. Not long before, in September, Google had removed two Brain Test samples after a report by Check Point.

It took more research, aided by the Lookout Security Cloud, to connect the dots, but on December 29 we confirmed our suspicions that additional apps containing Brain Test malware were in Google Play. We found 13 Brain Test samples in total, written by the same developers. We contacted Google, who promptly **removed these 13 apps from the Google Play Store.**

How did these apps appear in the Play Store? It seems likely that over 2-3 months, the malware authors used different names, games, and techniques to see what apps they could publish in Play while flying under the radar. Then, just before Christmas, a game called Cake Tower received an update. The update turned on functionality similar to the initial versions of Brain Test and included a new command and control (C2) server, which was the smoking gun we needed to tie together the apps.

The explanation for the apps' high ratings and hundreds-of-thousands of downloads is the malware itself. First off, some of the apps are fully-functioning games. Some are highly rated because they are fun to play. Mischievously, though, the apps are capable of using compromised devices to download and positively review other malicious apps in the Play store by the same authors. This helps increase the download figures in the Play Store. Specifically, it attempts to detect if a device is rooted, and if so, copies several files to the /system partition in an effort to ensure persistence, even after a complete factory reset. This behavior is very similar to several other malware families we've seen recently, specifically Shedun, ShiftyBug, and Shuanet.

Unfortunately, Brain Test is back, but Google worked quickly to remove the malicious apps we discovered, and we are continuing to monitor for new variants.

Removal

Unfortunately, a simple factory reset (in other words, using the 'Factory Reset' option from the Settings application on an Android device) is not enough to remove the malware, as factory resets do not clear the /system partition. The best option for most users would be to backup anything on their device they would like to save, and then re-flash a ROM supplied by the device's manufacturer. Users can check with their device manufacturer for the proper steps on flashing a factory ROM.

Technical Analysis

The technical analysis will focus on the most recent update to 'com.beautiful.caketower' (SHA1: 18b387c31797a23f558c67194cd2483dcf8cd033) that became made available on the Google Play Store on December 23, 2015. The behavior this sample exhibits closely follows the behavior observed in the initial batch of Brain Test samples. **Initial Launch** After the application is installed and initially executed, it does the following: 1) Starts a watchdog executable that reports to the C2 when the application has been uninstalled

2) Decrypts the asset located at 'assets/res/drawable/pw.png' and copies it to '/data/data/com.beautiful.caketower/app_cache' with a randomly generated filename (e.g. '11ya'). This decrypted asset is a malicious APK that is used for persistence (package name: "com.qualconm.power", SHA1: f52bc39bda66d347cc108f15e7efee52f7e7a112).

3) Writes a small shell script to '/data/data/com.beautiful.caketower/app_cache'. If the device is rooted, it executes the shell script, which will copy the previously dropped persistence APK to the '/system/priv-app' directory on the device, ensuring persistence even after a factory reset.

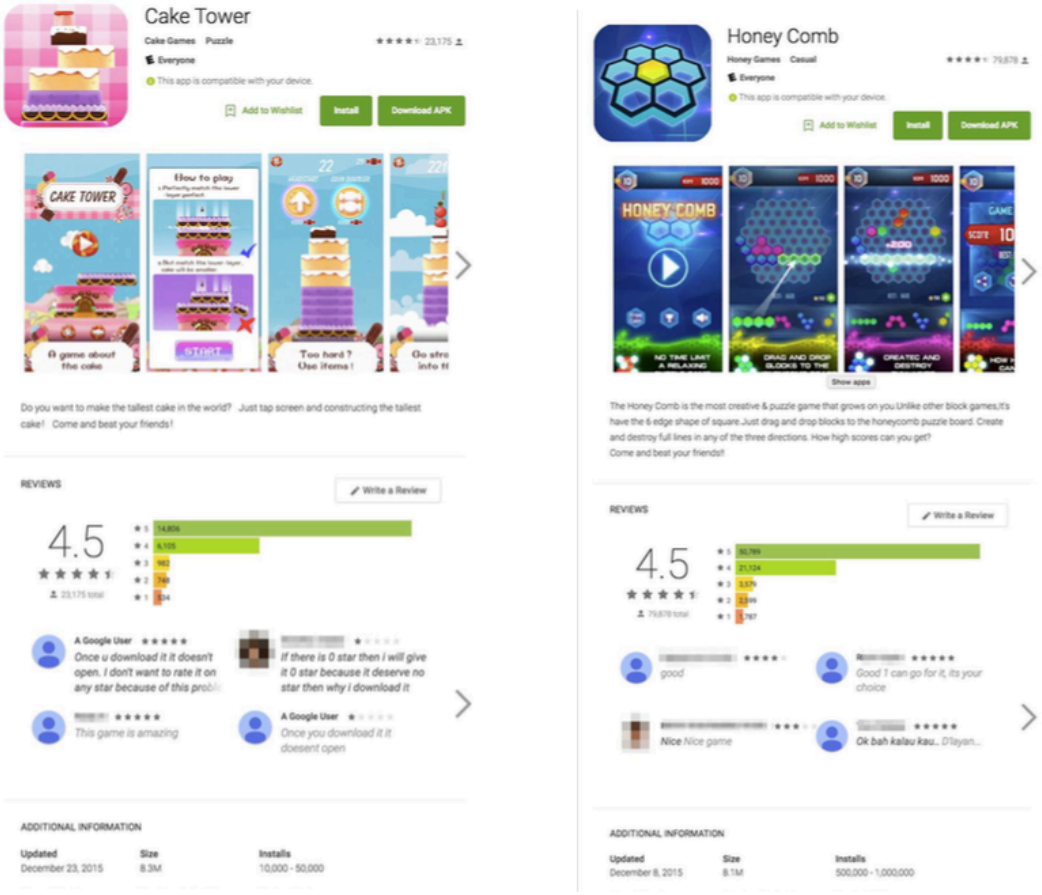
Subsequent Behavior

After the initial persistence routine completes, several background services continue to check-in with the command-and-control servers. Like the original Brain Test variants, the current version has the ability to download additional configuration parameters from the command-and-control server, as well as execute arbitrary commands as root or dynamically load and execute additional Java code.

It appears the primary goal of the malware is to download and install additional APKs as directed by the command-and-control server. The developers also used infected devices to download other malicious applications they had submitted to the Play Store, which would inflate the number of downloads each application received.

Additionally, the malware provided capabilities that allowed the developers to post positive reviews on their own malicious applications using compromised devices, which may explain why every sample we observed had a rating higher than 4.0. Their last malicious application to receive an update before removal, 'com.beautiful.caketower', had between 10,000 - 50,000 installs and a 4.5 average rating out of 23,175 reviews, according to the application's Google Play Store page (Figure 4), while another associated sample, 'com.sweet.honeycomb' (SHA1: edb88aea5f9ad489db5869ad49252a865d5cd9f0) had between 500,000 - 1,000,000 installs with an average 4.5 rating out of 79,878 reviews (Figure 5).

While the malware's primary motive is likely selling guaranteed application-installs, its flexible design could allow the developers to utilize infected devices for more nefarious purposes if they desired.



Conclusion

Brain Test's end goal has always been money. There has been an emergence of entities, primarily originating from China, that have been **selling guaranteed application-installs to developers**. In order to facilitate the installs, they rely on compromising a large number of devices and then pushing the installs to those devices. Similar tactics have been around for many years in the PC world, and we've seen multiple Android malware families take a similar approach.

What differentiates this particular situation, though, is the delivery mechanism: where PC malware is typically served through misleading advertisements or drive-by-downloads, this malware made it onto a mainstream app store, and in some cases, obtained over 500,000 downloads and an average 4.5 rating before removal. While it's definitely true that users are considerably safer when downloading only from a mainstream source like the Google Play Store, we recommend users remain cautious and use additional security software to ensure the safety of their device.

Appendix

Below is a list of applications that were removed from the Google Play Store:

Application Name	Package Name	SHA1
Cake Blast	com.zhtt.cakeblast	c146accd006bd4f2bdfe0557d1b3d2d547e74717
Jump Planet	com.galaxy.jumpplanet	997a36295076649a8154efe066f2849f2848b5b0
Honey Comb	com.sweet.honeycomb	edb88aea5f9ad489db5869ad49252a865d5cd9f0
Crazy Block	com.crazy.block	715c58c3e7834256637b29a951326c31ab0730b0
Crazy Jelly	com.crazy.sugar	b0734b52a12c30a882cf7df4ffcf85fb7fd0e9b7
Tiny Puzzle	com.dot.tinypuzzle	415b8f81c5f3ce2a767902e977cf83b510bd467e
Ninja Hook	com.sunshine.ninja	32acb811af288237605da2d19dc6f88d89f321ed
Piggy Jump	com.stupid.piggyjump	c54fb4038e1a06534404372538876d8863bfc507
Just Fire	com.tomtom.justfire	6e59fa627ae42486970e6f8249fca2e987174f04
Eat Bubble	com.fine.eatbubble	134a7e9741a1237f55a2c987d70148888b2ad3f9
Hit Planet	com.smile.hitplanet	89a8a39cd2e6a1567802a9210040c12a9eb63c7c
Cake Tower	com.beautiful.caketower	18b387c31797a23f558c67194cd2483dcf8cd033
Drag Box	com.block.dragbox	N/A

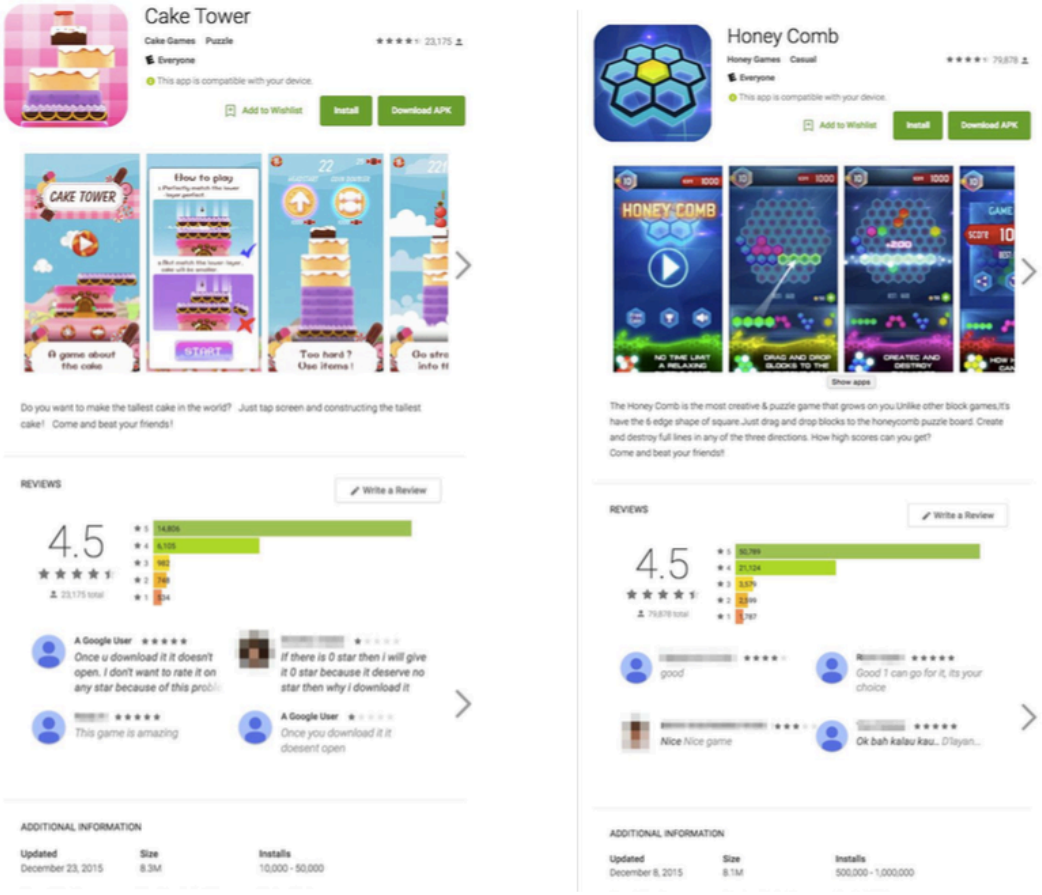
Subsequent Behavior

After the initial persistence routine completes, several background services continue to check-in with the command-and-control servers. Like the original Brain Test variants, the current version has the ability to download additional configuration parameters from the command-and-control server, as well as execute arbitrary commands as root or dynamically load and execute additional Java code.

It appears the primary goal of the malware is to download and install additional APKs as directed by the command-and-control server. The developers also used infected devices to download other malicious applications they had submitted to the Play Store, which would inflate the number of downloads each application received.

Additionally, the malware provided capabilities that allowed the developers to post positive reviews on their own malicious applications using compromised devices, which may explain why every sample we observed had a rating higher than 4.0. Their last malicious application to receive an update before removal, ‘com.beautiful.caketower’, had between 10,000 - 50,000 installs and a 4.5 average rating out of 23,175 reviews, according to the application’s Google Play Store page (Figure 4), while another associated sample, ‘com.sweet.honeycomb’ (SHA1: edb88aea5f9ad489db5869ad49252a865d5cd9f0) had between 500,000 - 1,000,000 installs with an average 4.5 rating out of 79,878 reviews (Figure 5).

While the malware's primary motive is likely selling guaranteed application-installs, its flexible design could allow the developers to utilize infected devices for more nefarious purposes if they desired.



Conclusion

Brain Test's end goal has always been money. There has been an emergence of entities, primarily originating from China, that have been **selling guaranteed application-installs to developers**. In order to facilitate the installs, they rely on compromising a large number of devices and then pushing the installs to those devices. Similar tactics have been around for many years in the PC world, and we've seen multiple Android malware families take a similar approach.

What differentiates this particular situation, though, is the delivery mechanism: where PC malware is typically served through misleading advertisements or drive-by-downloads, this malware made it onto a mainstream app store, and in some cases, obtained over 500,000 downloads and an average 4.5 rating before removal. While it's definitely true that users are considerably safer when downloading only from a mainstream source like the Google Play Store, we recommend users remain cautious and use additional security software to ensure the safety of their device.

Appendix

Below is a list of applications that were removed from the Google Play Store:

Application Name	Package Name	SHA1
Cake Blast	com.zhtt.cakeblast	c146accd006bd4f2bdfe0557d1b3d2d547e74717
Jump Planet	com.galaxy.jumpplanet	997a36295076649a8154efe066f2849f2848b5b0
Honey Comb	com.sweet.honeycomb	edb88aea5f9ad489db5869ad49252a865d5cd9f0
Crazy Block	com.crazy.block	715c58c3e7834256637b29a951326c31ab0730b0
Crazy Jelly	com.crazy.sugar	b0734b52a12c30a882cf7df4ffcf85fb7fd0e9b7
Tiny Puzzle	com.dot.tinypuzzle	415b8f81c5f3ce2a767902e977cf83b510bd467e
Ninja Hook	com.sunshine.ninja	32acb811af288237605da2d19dc6f88d89f321ed
Piggy Jump	com.stupid.piggyjump	c54fb4038e1a06534404372538876d8863bfc507
Just Fire	com.tomtom.justfire	6e59fa627ae42486970e6f8249fca2e987174f04
Eat Bubble	com.fine.eatbubble	134a7e9741a1237f55a2c987d70148888b2ad3f9
Hit Planet	com.smile.hitplanet	89a8a39cd2e6a1567802a9210040c12a9eb63c7c
Cake Tower	com.beautiful.caketower	18b387c31797a23f558c67194cd2483dcf8cd033
Drag Box	com.block.dragbox	N/A

Source: https://blog.lookout.com/blog/2016/01/06/brain-test-re-emerges/