A Whale of a Tale: HummingBad Returns

By bferrite

Published: 2017-01-23 · Archived: 2026-04-19 02:13:17 UTC

Check Point researchers have found a new variant of the HummingBad malware hidden in more than 20 apps on Google Play. The infected apps in this campaign were downloaded several million times by unsuspecting users. Check Point informed the Google Security team about the apps, which were then removed from Google Play.

This new variant, dubbed 'HummingWhale,' includes new, cutting edge techniques that allow it to perform ad fraud better than ever before.

HummingBad is a malware first discovered by Check Point on customer's devices in February 2016. HummingBad stands out as an extremely sophisticated and well-developed malware, which employed a chain-attack tactic and a rootkit to gain full control over the infected device. Later, in July 2016, Check Point unraveled the entire infrastructure behind the malware's activities and even managed to identify Yingmob, the group behind the campaign.

The malware was spread through third-party app stores and affected over 10 million victims, rooting thousands of devices each day and generating at least $300,000 per month. HummingBad was so widespread that in the first half of 2016 it reached fourth place in 'the most prevalent malware globally' list, and dominated the mobile threat landscape with over 72% of attacks.

It was probably only a matter of time before HummingBad evolved and made its way onto Google Play. HummingWhale malware first raised suspicions when Check Point researchers analyzed one of the apps. It registered several events on boot, such as TIME_TICK, SCREEN_OFF and INSTALL_REFERRER which was dubious in that context. Code similarity inspection revealed that this was only one app out of a series of apps with a common name structure – com.XXXXXXX.camera (e.g. com.bird.sky.whale.camera, com.color.rainbow.camera, com.fishing.when.orangecamera).

All of the apps were uploaded under the names of fake Chinese developers. In addition to the camera family, researchers were able to identify 16 additional, distinct package names related to the same malware, some of which were also found on Google Play.

However, the most suspicious property of these apps was a 1.3MB encrypted file called 'assets/group.png' – a suspiciously large file. Some later HummingBad samples disguised as an app called "file-explorer" had the exact same encrypted file with a similar size. The new samples of HummingWhale also match several other traits and identifiers seen in previous samples, such as registering to certain events and some identical strings in their code and certificates.

In addition, we identified several new HummingBad samples which operate as the previous version did and begun to promote the new HummingWhale version as part of their activity. This new malware was also heavily packed

and contained its main payload in the ‘group.png’ file, which is, in fact, an apk, meaning they can be run as executables.

This .apk operates as a dropper, used to download and execute additional apps, similar to the tactics employed by previous versions of HummingBad. However, this dropper went much further. It uses an Android plugin called DroidPlugin, originally developed by Qihoo 360, to upload fraudulent apps on a virtual machine.

First, the Command and Control server (C&C) provides fake ads and apps to the installed malware, which presents them to the user. Once the user tries to close the ad, the app, which was already downloaded by the malware, is uploaded to the virtual machine and run as if it is a real device. This action generates the fake referrer id, which the malware uses to generate revenues for the perpetrators.

This method has several advantages:

1. It allows the malware to install apps without gaining elevated permissions first.
2. It disguises the malicious activity, which allows it to infiltrate Google Play.
3. It allows the malware to let go of its embedded rootkit since it can achieve the same effect even without it.
4. It can install an infinite number of fraudulent apps without overloading the device.

HummingWhale also conducted further malicious activities, like displaying illegitimate ads on a device, and hiding the original app after installation, a trait which was noticed by several users. As can be seen in the image below, HummingWhale also tries to raise its reputation in Google Play using fraudulent ratings and comments, similar to the Gooligan and CallJam malware before it.

This is a prime example of malware developers learning from each other, as tactics that were introduced by one of them are quickly adopted by others. The fraudulent ratings left by such malware is another reminder that users cannot rely on Google Play for protection, and must apply further, more advanced means of security.

IOCs

C&Cs:

https://apis.groupteamapi.com

“/(.+)?app.blinkingcamera.com(.+)?/”

Package names:

- com.bird.sky.whalecamera – Whale Camera
- com.op.blinkingcamera – Blinking Camera
- com.fishing.when.orangecamera – Orange Camera
- com.note.ocean.camera – Ocean camera
- io.zhuozhuo.snail.android_snails -蜗牛手游加速器-专业的vpn，解决手游卡顿延迟问题
- com.cm.hiporn – HiPorn
- com.family.cleaner – Cleaner: Safe and Fast
- com.wall.fast.cleaner – Fast Cleaner
- com.blue.deep.cleaner – Deep Cleaner

- com.color.rainbow.camera – Rainbow Camera
- com.ogteam.love.flashlight – com.qti.atfwd.core
- com.wall.good.clevercamera – Clever Camera
- com.well.hot.cleaner – Hot Cleaner
- com.op.smart.albums – SmartAlbums
- com.tree.tiny.cleaner – Tiny Cleaner
- com.speed.top – Topspeed Test2
- com.fish.when.orangecamera – Orange Camera
- com.flappy.game.cat – FlappyCat
- com.just.parrot.album – com.qti.atfwd.core
- com.ogteam.elephanta.album – Elephant Album
- gorer – File Explorer
- com.with.swan.camera – Swan Camera
- com.touch.smile.camera – Smile Camera
- com.air.cra.wars – com.qti.atfwd.core
- com.room.wow.camera – Wow Camera-Beauty，Collage，Edit
- com.start.super.speedtest – com.qti.atfwd.core
- com.best.shell.camera – Shell Camera
- com.ogteam.birds.album – com.qti.atfwd.core
- com.tec.file.master – File Master
- com.bird.sky.whale.camera – Whale Camera
- cm.com.hipornv2 – HiPorn
- com.wind.coco.camera – Coco Camera
- global.fm.filesexplorer – file explorer
- com.filter.sweet.camera – Sweet Camera
- com.op.blinking.camera – Blinking Camera
- com.mag.art.camera – Art camera
- com.cool.ice.camera – Ice Camera
- com.group.hotcamera – Hot Camera
- com.more.light.vpn – Light VPN-Fast, Safe,Free
- com.win.paper.gcamera – Beauty Camera
- com.bunny.h5game.parkour – Easter Rush
- com.fun.happy.camera- Happy Camera
- com.like.coral.album – com.qti.atfwd.core
- com.use.clever.camera – Clever Camera
- com.wall.good.clever.camera – Clever Camera

SHA 256:
026d768bdaee3d9ba890493fcc71fa106df8c7319d2298e02845ccd73b08611d

91bb63ff99b5f00dc293d1b5c7fdc51ddddcdad4c306ab0eaaf0a1f6d9a5c651

0993f1a9572babec9971187735378fbf5eaae022f36958f3d992e0222a421e0e

ef5a2d495623f3f5498468f2a2cbee1d26dca78bb73b1fd873acffc7172a7756

d7ff6f5c272ca25e2dee716580b21ca506ab75faa2e599932ed8481ecdd922dd

9a9348d3a522b7292692f9babc773f01e5ff8e8225e00404a3b9664b4137d955

dfcbec620a8a53096a32b1da5fdf73008fc3ff5a228176c1b45b0fd95f8c61ce

948dfffd89be109671408343ea84978de0b3029367851879eadb86697cb6f2e0

47d3c854700663969913e1df437f65680c8e17c229dd6348ad3153211242058b

11b421f64fb5641919385caffb41c7594094fc2d0dd82fe7983ab3c39d5705a1

329c2b731e8e5b1ddd5adb88dd7658f6501cfd5be9a2e0ba1fdd5ca95133ce0e

f458e94bcf9e2d65e1ed047bb3179e03700fe200b896d4cafd24c9d6443fc80d

e649c79796735e35c54b7fe390f233825b11eb089564c135c3fe09ebb0eae20f

e02ba0934a21cf0f44e4d5daed39c56e0029c3d3e5896a3f75a7de01fb1ae574

34d3968010112a51ee6d72416e197067883e4cd4ca50e83e1cf52aa4469e0ddb

5f588bbe7932dd9d9f3780577d8aca0b913b0b3f8f471df06336bd637509fda9

48adf4a7b64f83d29cf98cc1370f4d5f4d34b40e5523bd391dc12a80537f125e

86300257a48e893cb7867596a2ff9eac1aa8aa89e01496d30e9f85a7d47c1023

954d004bb7174e886b49d7815e4ef4126627d044ba4c336fc0671ed777e8a47d

793a970e4fbb4e07f49020d4bda9887502b90dfff35efd93bef2131bfe7e6c45

359c9ba08ee2c508d57c933e1ac1bc0cb37dd78cb64339e446e3307882c04886

dee86e0006d58f9ab24698a73e609649e91a7f53e20ac495f20f2522503715da

9bd6f2ba13b3c447e3b8eb83c197c98da276a71f031c4d841c64addcb3ce6426

fc67adbba8570911a7c4db35401235ca5bbe7deb312a2171a831569c41668272

2d2ade60cee284392b54c7785a0612bbc45533905381c02b68741a989a779d99

32d9c801ffccad7d95f3eb256ca23c585329863a19d0316f7bedc556b5d59d8f

47fd258670c91edb29f24b244101be412667de01e0b52daf5f0901c846dbcf2b

49ff608d2bdcbc8127302256dc7b92b12ea9449eb96255f9ab4d1da1a0405a1b

777acf88669cf0ef8d22280333a73f77ae3b100b7c69d6e307501b8da51104fd

0df88d176f6390716e833f9fc96c82aa65740d7e02045c1f5a127499868384af

0aabea98f675b5c3bb0889602501c18f79374a5bea9c8a5f8fc3d3e5414d70a6

7ef91ac2ce9be16919e1dd52e5484352d2bb71d57cc694a11992a07b050a7822

84be18bb9e7d9b427acda81e2fba08f0828ba5e99e0c00cb1bbeb6a808c02119

55e186caeadda451451272877def3df5212101cb5eccdb1bb1d0058cbd734181

22c17c72517bfaed4c0aeacc0fdb95578f467ecc586e503de85e859b17e7e779

1ef3d2ee38005173e353eba06c440cfb73cfef40189e3567cddf0df7bd5f4d1e

79ec0fde7799bef5414efb33b24603b3267d4c679481c27e8485aafed008b925

9e567c1fee6c753dfbffc4d1af9e9debbf22f0d5f5ab78dc6b1f6b2b6eaa4574

772488e59f9c7727d0d6494ecd702371ce6de1df51471c779df33befa24bc097

9f4a2dfac381f0eb2e1633fb8d51d3ab6c8391a65050d781e0ce4a799b8d8236

188778069588711f4e7bcf8a8942e101fc21aab543bd84f6114501701a6df24e

208179cf3147b86c4fcf7c38baab67632607f89647f8e912c44eb79c92766b68

1455f59aca25ea52194c3ee0bc0f98bf890547dd519077339fabe76f4b4981d0

84b8fb9752605316e8c9ba39846abca43d302e779b1baa6967dbd021f5545d50

7fb98c12d376f2608edbdbc87304eb8d2880762b6c357050222130314986726b

bc0d9d24a5445ea11f898fb05366d2dc92112d82728206f1d6d27f2fe4631cbb

1d78cf86f5e5fccf3a6a87ea3fe5d7952dc15e76314442566298fb8b85237d1a

43bd2ea4c4ef1733cb9f306da5fab52d71f6a1b60f567c114ca24b6a6253be20

2b3c3d19191c686019d6ba957bc4fe7785c1c0537f5b4f2ac21c04e6a3eefcd6

3b9f5e7dcea7eb38383cc7cea09c1d4a0ca7caeef60e6071c41daa0142ca89e0

0738bee39fc612d4d9e8851bc20cd8ffa4e7a5b57a05754cc056780ce0da4ce5

767cb865ce2bff1304a835fbd84c5a66067e02f6a846d26e5db62610b13188a8

3858e922bfba7bb88f5ceedc627b4e6b8a6572e3184e2ef6b3e8f65d60194e66

06bf0142851108aa3dbc5da0110e9e8b268da4c17e4951e7056659b60e6a05e7

59adefed71cd819cbb6e4b785a125de6af57563b2d5faf96f998b0e01f7e5e18

7edaa7211b67efc5e8cc285020e6542569a2a393258aeb1eee0a130622fa5a2a

d7f30fa04b539fdbbf10ea0f0f5fd1db071c4caca1d07dec0a40673755f5b852

9b4d8b9ec284598cf51bef14fb73d1b72ee78b7182ad64479942b14cf5ca0381

d80258407a8d29705786d3e7dd38d7cbf08ffee751907b9d45d30c046df2c66d

672134399413f903bc66e87a6032fcb135f8e96d8f7c53255f45a08e61582ec6

be2ecc8094a9bfd118f280af0f170aebcaf90441e624a2b3af2dfda8591c25a9

5a135204b64d101bf9de25d65cc9335737d0ae3fb108f59c8f9c0a3d1feee65a

c8b744b80707a6a0e6b00215364cfbca4c29bec1d99abd67f0042eaa1d3cda5a

a80109ea1fe890458b917c341e44828701905e67dc690e60b90ad335c749d340

76e65a792be8b97e2d123e18b1310a751840f99198ba32292ad67ec8dcdae036

c879bec98b492331cb60449c533d2df630820a77b1f2fe52e0c749d9fbeba049

322be13cac68d265041cb0947df912d8496ee7422aebfe4ed65abfd04fe03b83

61109de12654526330ce31ba9e6fc40c9d38ac9c990367a9f8d2627b68017c16

15209d33e0370c513cdac2affbe175efa5fa07c725c08ccefc7c47d055f18764

23fcea247193648e4e51af46e054b7cb481ee0a92aa8d8bb50b5b97b040cfa3a

0f7d2fbe81860185a2955873ad0e7c4c68f42cc529ce66b8400277a9db79a83b

185c3059b9001de5887ed275e58d88ef585fe645a9ada3bc0ef880f8b5d05695

49fe0548c1deb22b5c58ab2ddd0fd93b5e975bd603454b1b990cefe46619bc51

4826fcaf14ea2d0bc9fab08caefd762baa7c3a7cb7f27cccf943de377b4f3688

b2ddbf1ce48cc1231a5dea698c4e46fa7268449d1f37c303a5b0532a8f075b04

4d4ec0daa5d5deb25de77bf1b149358547d21bc97449b0e1e3ffd4ff89e37ec3

c01f5727fd2c7bb735862f62fc484149ed8558a0fe503871d199b5b9c9ce7622

6ddbda7d1b7ab7f00cfad005d265ffccf36e5e19d5ebe350f8203d8342d66bc2

84d512c391077094f183ec1f881a3a566f4298e2171c90bf6b2601ebe5729012

b362febb7673a90ba26d7f763c0cdd77131233da1ddeefa4f61c5a75a422132c

a5442654e4bcfc25dbb9da605a66ea85bbd32c0df0c0e8182d569aa9cf1ac7e0

3cdbc2c0e91f73dbd5daee8a807d58f34cf49a21d6d2e3cf2764332c6a791e2f

be5020000ab6ec45a8e6c9d09857029116aaa80ecb4fc2a8bed39f4507682737

15d1347de925e55480160da7037136c918e5f977f281e488bc221f3c80f05e59

952acb85c7763fbd5c5d6632b29dd4f8339e327bb71b421530c93e88d2f986f8

beb3f9e15a865e28059ac692841af7b4f1bc5bbeb005e993d442e4ef9acf0adf

9cee668dd34e0449e2d6e447cf007af838d142014ea02374706e0b286b94c5b3

40abc7dd0edb1a3c3fb3a613a2239c707926247fd1c889d6a575538e548ddf3b

2e1259cc2289a0e980663e003df4230b96038151de7b3fd3aceb9794535ca4eb

90ee7f69ea6157d659596ad1959ad09af8a829aaca9504e0d339efee37706100

49f3e8d9ae94dd45281a55b20e9c784df947fa8f15bbc2bb9a2cd549eda9f326

31a701b9be2973e42f0750740546f65fd8e57e0afd81f4a508bb817c212d0c1a

a5224d1662053b2768d71ad511169c7a83c6855474560605aa8eaab0119a9fd1

7e610e48efd41fc24fac6d332fbc01934a4e3e8fc896b148647a34beda41b1a8

cbc370871328876cae6723db10eda3e7bbff1a0148cb3546c62b6ec1f4747f46

255433ed54a20f9d0e6fce27c4c3bcb2759b05db7c8b55ba7f61178366dbc435

1766595cf73e8555371e501e7f136d0b4969c2ac4d58f17c7f776b1b65ce0fc5

fb36975565b6b69cc5c90298f308429259b729266b1140babd16eec0b1a0523b

b3c125812b014545fc85affcd4b0dc4518bc1be8682ab79b61e575922c020c78

1f70d638367ec6c40ba8766d9cf025edf8de68559d725aee00101556d6e03037

863356c6cb09fbfae353769c659a64f6cd45f0d8e74ac63124c95117d542677b

4400ebc0f545d481992bb67b1e3f3766e969c4679915daefcedb7614b82e9fcb

6ab4d2c3bdb1e8a0d50df3e0ba164dbc0e339869d00ca919b2a9dc6bd0ff5735

65295d62f14558464f9ca85a0bac915040179a9e563f0617d63eb3e0984500dc

2106e9f21d1d08fb946ec5834e1f715f383b4c988fc6711a3b5350ec7b7cc026

b0fe985f7478bb841d062c0cd1a72861097459df64496db6e8b38cc01539283e

07d954330b32708d4df4faea3c7693ea626323b5f950ebef94d16d66cb1b3912

c86d7680332b074af05a022f22229bbe0bc45126fdbbb24ea4e96b1fa13dbdd5

878c5eddc9a9b251365417047b213956bf8562a85d9fa7a9f1a8b9248bd3379d

bfabd967119353eefab73486b47066181060a9a4d5129d6c6d607cde58b25f47

0a58a94e2670aed6d980b79dd50cf3c0bfd634056905cdcc6611729830fb0889

407ee462d9e85b8c253ed69c5feee7bb3a859bff9fa5cee2d784c12d513a529f

330724c5fcd1efa0552089e5690844c0c23408c8479485099bcabfbebff28dc9

d45a221d85210cef2edc5db0b41529b215de4f9f271f3b52f29d20708fbb58dd

52f7fffa17e6fc88906863bf9fa2384fbc64e017470bd889f367a5bd6c936e0e

9bd0acb0eb7b04bae2de31db0ed36a853f4639b1805ecb9ca51dcbdabeb5a1d6

5bca1b054baa6642d86cd311690d61458469b4a46c23d8d85d0a87e43e29c9fc

a75ca07568f39701040daf92e5d8ee8089287b3e6dae0eb42103c2b0ede248bf

b9a132e15b6bed52b032180d0b7a87dda7c611e78bef7aae9258574a7dab6359

6f47a8e8ec920860aac34cf5c68f351e5fee6838c47e8f908c007fe7e144915a

a8e4f14146fad6183fb69c7eaf133102072eeeb6f016a2079d015b7061d022ac

1f3397174e7fe932f49146d02dcf3845eb829b453d509fe46633ea32e7700889

928c46788d92b1e74f43c9a18c31aa7cde57c37a9bbb695af962b64cd6cfd201

201a6792208a6e1c2ef53d251412d5701a1b36ec740e578dfd4153fdc90a6b76

25e390f0442c3b8f02763e670a37ea26472c58153a90b65a3f3c6ffcf29ad832

389d1bd55f37f41f63f2429ef74ba4d41fd9eae70d432394199d6a586579292b

300a5404d5e1194a7cb2e3bdb167af02f1d059a5f4de934c13f23ad483459e4f

7a984e0ed17c7db35dd70ed51aff6725d87901151701f61b217ef614ce165fa2

49d0d2e07ea6c845700cb91f66d339c694ca746dba259fe2b97e4bc6fa6f9156

34e4c9d8404f33df89d4c1e92a43ea9293016d69c9aa460ea1a60ac70cbb1694

2a730dd301a8a34581a2d4534b72d609b51ab9276fd83689a220d85c4111e85c

5a366038d339813235a40053d0286e697798752dc45210a0011d9286d785346c

61fe29dadb7fb6ad19dd050e7e37c037da0e9de09a25da7cd28c6f4c601b2054

fa997f8280dc4fe2a56d47da4523a7d83ad661068a30719a4005dfc2e7f73134

6faf8bba0f0be9fa24e8afd199d795acb839abc47b7c2cda60f173897884da51

049508e8b8640a14ca6391ded601eef0be764363159fa2310aa9d737d6a76eff

147600aa3bb1b86654e0cf8b79cedefa5fb965437a37106929da5965794ed1d8

c7eb86efc34482bc27ca6a18e5bcaa6ef8ca2c18effd3854dbefb6e945780964

a3b685ebacb154c285a1796a1b46e8c8afd1d5ea3571116ed9646188dd7b6eba

397a09b9b39ba6be5d9fd02e8be714c0f905dbd5da6a048845aedbcb9756992b

f95919380b54d3b639e9006a6c5a081410d658f8617a1dabc572e1243e5d007e

bb8607e72ec71c2cdc0876bd1f818ff099888f6c7837c337bc2d560b148d199d

eb1cd908ce73827cf6fc7444100b911edd32d48e878550a31f99668925b89b0c

9257099a2fb84aeb3e674977f7c5143ae618e523a822c3e1f8255697d40a1ef9

3110550a14f379fcbdd36b8e51957998ac9c61faaf67ac694368d690983ba31e

59d78238bd041a22711733742f7836345c004856a8d4ac4e748b01ecedb56b73

cc9b67ed180522ad3a4402eb9e8f2d686a93af0619436c667dec9623b57b136e

e24e267724128b1d505e3e7e309e8e44a6f14990018dc4862cbec78100b8fa57

58b60d51a5a1f249021b4f5c8c18d195ff923db5ae0e97238a7f772f6c35003d

18090bf793be49c3481109d24fca95f97c3f47325d5658d0c6bf08a291701e62

57aaba0e69188ddf2c78cc7e5abf351e80b2fb2093a7868420bc915b072ddc10

0908a85853e1c472e9fe02b787c5e3bee4f42a448185a6e033797b5a0ee00f54

4d0adf91bef382c7f1828106c59059700753eeb1cf27fc5a9506b5f3d874c939

d95790b3fc4e1799f929180a2bcf106c25ac8a408ae3f15e592f8954909b86b2

7b212a010636117b2cf040530d34798fce696a8e46250ae31a5d13ae84f5a0b2

99cdc3779c5cf3cb79e5fa6662bd567af46c19601d5f3f3990c5cedab0d13846

b6f63861a7fffae140bc55e7d868eecbc5def568053cbb47f407088a6fb5fe7a

48efd52404246da3c18f698a6021acb01fc61be4de6083c2c189026fe64db819

56ccc9b1461d5fb91a4b0968c53cc6d6f7e1482e4ef13dcf4df8e96cb9fc8167

bb317ccdfadd55f2f49a08afe50c9b5d025dff83a54edf69799b5b43950c6c1a

0ad2ff0d4b5c6cb8aaa0b9ccb8aaa591701f777f10a6d4695d4431d8e6a8f96b

04eb032c2804c2a73ce8b183b2868fa6947da91698daeddde77df8c50b0aff2e

c2b0941f5ff6330e838cdc7e8e7778b736a342b3aefd8c0c3eeb085c142c3dbb

2d952cd6bd676b98cf3c995db12db61763c8b020fc952f5c6ec9dbbbf5291e87

001bca3d5b8309403b49801a7ef56c311dcdeee41ce23b5ada2f96bdcb4fe853

b40b0386dba34ac357a7b0524174f63c3566e64f3606331b247bf528b6aca875

c18bce7e6a3cd33136202d697d26e368e7f468238af1a923c0635c7fbe915d05

1cdcfa003d3f304e2dd870919a1cb702267a2d9b090e165af34f2ff5f64c6de6

bc9179b928269f188859a90c7366e1fec49571bcc2f60effef1383c6e4c2434f

c752d601de41b08d1a94eb719584ce7813984217c7417b27c4b2adaedaf760bc

11336505bcc14ab375e480b911e47317587bda109bc187ab117ceb614903cd04

0a85a5d14950c1bfc49c9af1aea6ac8b0390851f9d990a00dcd9930706cab33f

d644444e6a8c7033df94fbc4fb7303441067933dcb085fd47c60903055c33f98

0e53ee429ee6a9873f5f7eecfa83384e4b825328383b0689041de9ebdc9ae79d

---

Source: https://blog.checkpoint.com/2017/01/23/hummingbad-returns/