The Judy Malware: Possibly the largest malware campaign found on Google Play

By bferrite

Published: 2017-05-25 · Archived: 2026-04-05 21:52:32 UTC

Check Point researchers discovered another widespread malware campaign on Google Play, Google's official app store. The malware, dubbed "Judy", is an auto-clicking adware which was found on 41 apps developed by a Korean company. The malware uses infected devices to generate large amounts of fraudulent clicks on advertisements, generating revenues for the perpetrators behind it. The malicious apps reached an astonishing spread between 4.5 million and 18.5 million downloads. Some of the apps we discovered resided on Google Play for several years, but all were recently updated. It is unclear how long the malicious code existed inside the apps, hence the actual spread of the malware remains unknown.

We also found several apps containing the malware, which were developed by other developers on Google Play. The connection between the two campaigns remains unclear, and it is possible that one borrowed code from the other, knowingly or unknowingly. The oldest app of the second campaign was last updated in April 2016, meaning that the malicious code hid for a long time on the Play store undetected. These apps also had a large amount of downloads between 4 and 18 million, meaning the total spread of the malware may have reached between 8.5 and 36.5 million users. Similar to previous malware which infiltrated Google Play, such as FalseGuide and Skinner, Judy relies on the communication with its Command and Control server (C&C) for its operation. After Check Point notified Google about this threat, the apps were swiftly removed from the Play store.

Figure 1: A malicious Judy app on Google Play

How Judy operates:

To bypass Bouncer, Google Play's protection, the hackers create a seemingly benign bridgehead app, meant to establish connection to the victim's device, and insert it into the app store. Once a user downloads a malicious app, it silently registers receivers which establish a connection with the C&C server. The server replies with the actual malicious payload, which includes JavaScript code, a user-agent string and URLs controlled by the malware author. The malware opens the URLs using the user agent that imitates a PC browser in a hidden webpage and receives a redirection to another website. Once the targeted website is launched, the malware uses the JavaScript code to locate and click on banners from the Google ads infrastructure.

Upon clicking the ads, the malware author receives payment from the website developer, which pays for the illegitimate clicks and traffic.

The JavaScript code locates the targeted ads by searching for iframes which contain ads from Google ads infrastructure, as shown in the image below:

Figure 2: Searching for iframes containing Google ads

The fraudulent clicks generate a large revenue for the perpetrators, especially since the malware reached a presumably wide spread.

Who is behind Judy?

The malicious apps are all developed by a Korean company named Kiniwini, registered on Google Play as ENISTUDIO corp. The company develops mobile apps for both Android and iOS platforms. It is quite unusual to find an actual organization behind mobile malware, as most of them are developed by purely malicious actors. It is important to note that the activity conducted by the malware is not borderline advertising, but definitely an illegitimate use of the users' mobile devices for generating fraudulent clicks, benefiting the attackers.

In addition to the clicking activity, Judy displays a large amount of advertisements, which in some cases leave users with no option but clicking on the ad itself. Although most apps have positive ratings, some of the users have noticed and reported Judy's suspicious activities, as seen in the images below:

Figure 3: Comments made by suspicious users

As seen in previous malware, such as DressCode, a high reputation does not necessarily indicate that the app is safe for use. Hackers can hide their apps' real intentions or even manipulate users into leaving positive ratings, in some cases unknowingly. Users cannot rely on the official app stores for their safety, and should implement advanced security protections capable of detecting and blocking zero-day mobile malware.

Appendix 1 – list of malicious apps developed by Kiniwini

Package name	App name	Date	Min	Max
air.com.eni.FashionJudy061	Fashion Judy: Snow Queen style	24.3.17	100,000	500,000
air.com.eni.AnimalJudy013	Animal Judy: Persian cat care	14.4.17	100,000	500,000
air.com.eni.FashionJudy056	Fashion Judy: Pretty rapper	24.3.17	50,000	100,000
air.com.eni.FashionJudy057	Fashion Judy: Teacher style	24.3.17	50,000	100,000
air.com.eni.AnimalJudy009	Animal Judy: Dragon care	14.4.17	100,000	500,000
air.com.eni.ChefJudy058	Chef Judy: Halloween Cookies	10.4.17	100,000	500,000
air.com.eni.FashionJudy074	Fashion Judy: Wedding Party	7.4.17	50,000	100,000
air.com.eni.AnimalJudy036	Animal Judy: Teddy Bear care	16.4.17	5,000	10,000
air.com.eni.FashionJudy062	Fashion Judy: Bunny Girl Style	24.3.17	50,000	100,000
air.com.eni.FashionJudy009	Fashion Judy: Frozen Princess	7.4.17	50,000	100,000
air.com.eni.ChefJudy055	Chef Judy: Triangular Kimbap	10.4.17	50,000	100,000
air.com.eni.ChefJudy062	Chef Judy: Udong Maker – Cook	10.4.17	10,000	50,000

air.com.eni.FashionJudy067	Fashion Judy: Uniform style	24.3.17	10,000	50,000
air.com.eni.AnimalJudy006	Animal Judy: Rabbit care	14.4.17	100,000	500,000
air.com.eni.FashionJudy052	Fashion Judy: Vampire style	24.3.17	100,000	500,000
air.com.eni.AnimalJudy033	Animal Judy: Nine-Tailed Fox	18.4.17	100,000	500,000
air.com.eni.ChefJudy059	Chef Judy: Jelly Maker – Cook	10.4.17	50,000	100,000
air.com.eni.ChefJudy056	Chef Judy: Chicken Maker	10.4.17	50,000	100,000
air.com.eni.AnimalJudy018	Animal Judy: Sea otter care	14.4.17	100,000	500,000
air.com.eni.AnimalJudy035	Animal Judy: Elephant care	16.4.17	5,000	10,000
air.com.eni.JudyHappyHouse	Judy's Happy House	10.4.17	100,000	500,000
air.com.eni.ChefJudy036	Chef Judy: Hotdog Maker – Cook	29.3.17	50,000	100,000
air.com.eni.ChefJudy063	Chef Judy: Birthday Food Maker	10.4.17	50,000	100,000
air.com.eni.FashionJudy051	Fashion Judy: Wedding day	20.4.17	100,000	500,000
air.com.eni.FashionJudy058	Fashion Judy: Waitress style	24.3.17	10,000	50,000
air.com.eni.ChefJudy057	Chef Judy: Character Lunch	10.4.17	100,000	500,000
air.com.eni.ChefJudy030	Chef Judy: Picnic Lunch Maker	10.4.17	500000	1000000
air.com.eni.AnimalJudy005	Animal Judy: Rudolph care	14.4.17	100,000	500,000
air.com.eni.JudyHospitalBaby	Judy's Hospital:pediatrics	10.4.17	100,000	500,000
air.com.eni.FashionJudy068	Fashion Judy: Country style	24.3.17	10,000	50,000
air.com.eni.AnimalJudy034	Animal Judy: Feral Cat care	16.4.17	10,000	50,000
air.com.eni.FashionJudy076	Fashion Judy: Twice Style	20.4.17	100,000	500,000
air.com.eni.FashionJudy072	Fashion Judy: Myth Style	20.4.17	50,000	100,000
air.com.eni.AnimalJudy022	Animal Judy: Fennec Fox care	14.4.17	100,000	500,000
air.com.eni.AnimalJudy002	Animal Judy: Dog care	14.4.17	100,000	500,000
air.com.eni.FashionJudy049	Fashion Judy: Couple Style	24.3.17	100,000	500,000
air.com.eni.AnimalJudy001	Animal Judy: Cat care	14.4.17	100,000	500,000
air.com.eni.FashionJudy053	Fashion Judy: Halloween style	7.4.17	100,000	500,000
air.com.eni.FashionJudy075	Fashion Judy: EXO Style	7.4.17	50,000	100,000

air.com.eni.ChefJudy038	Chef Judy: Dalgona Maker	28.3.17	100,000	500,000
air.com.eni.ChefJudy064	Chef Judy: ServiceStation Food	10.4.17	10000	50000
air.eni.JudySpaSalon	Judy's Spa Salon	10.4.17	1,000,000	5,000,000
Total			**4,620,000**	**18,420,000**

Appendix 2 – list of apps developed by other developers

Package name	App name	Date	Min	Max	Developer
com.CoupleDday	커플디데이 (커플 기념일, 위젯)	2-Apr-17	100,000	500,000	Neoroid
com.DogSound	Dog Music (Relax)	29-Jun-16	10,000	50,000	Neoroid
com.kakaotalkchatanalyst.ks	카카오톡 대화분석기	25-Feb-16	1,000,000	5,000,000	DeepEnjoy
com.PeriodCalendar	황금기 알리미 (여성달력)	20-Apr-16	100,000	500,000	Neoroid
com.MoneyBook	100억 가계부	2-Apr-17	100,000	500,000	그린 스튜디오
com.lee.katocpic	KatocPic(카톡픽) – 카톡프로필	23-Aug-16	5,000	10,000	Wontime
com.appnapps.app77	필수추천 무료어플 77	5-Feb-17	1,000,000	5,000,000	App&Apps
com.sundaybugs.spring.free	Spring-It's stylish, it's sexy	30-Sep-16	1,000,000	5,000,000	Sundaybugs
com.lx5475.craftingbox2	Crafting Guide for Minecraft	4-May-17	500,000	1,000,000	JIZARD
Total			**4,215,000**	**18,060,000**	

Appendix 3 – list of SHA256

a7e2030649cca0651730d4bea6f9c03200aaa3a0da56f112bf7c5691c172fcde

a649293a9420afdd9c034f74bc501eef645af1ca940346a59d0fc7aef9028dc9

407e92a8c83a1fc9797c7047a5084ffc3ca8616779bd7eb829c1a0210a731356

3803ca279b007f10b9ca1eb5fa329bd87e5b40670805d57031971d7bd6d5fb77

0aba0b966df39f8e0bf5f93955827ea223c1bda4c167232f9805958aa6e66ec0

0f883861ce387f2e6336f68f040a6bb635fe8358b9eb6efe1398f887000a9351

11dc1c54f1c0f08bbc335c22e43f1d27e6ed05261c98facffd0a1c084021caf4

15d34a094515d7044194762650c0b0f77ec546025d555b09dd03c9e2d67532fd

1a652e3d37e6d5a67efff547de111d161c396a5619136244d7f0846558037674

1cd233cfedd87e15953138f82d78140ca4890161271542627e033f11225df181

1db8c76ead84322407d4d112c8ab855f4b4ea414c6e7379fcd1ad03e56fa975c

2117a776609b249436e448def0e6e0bfc5a6b3c176f101ff3f4411f4e2e14584

28785f3acd5f3b75ce9b919cb0549b41e24cf38f729b60f720d989f83406bcc0

37ae2e88dee816d7ed4036dced7b404c98d321de89faaedbbabd00fadfde65fa

3e96f9ff46708e5a70977dfbcfb5e90d3c5b1b6caeee36303c179b724c708be5

4d1503ef789d31047d39efe28e7abae3104e0b7d0ded9bf899fd92f814246718

5e086c84836ed931dd2650f29f27e8b43eaef67bf29b63d0c508fee04e4c339d

5fc2853fc986b1d6c41a99238ada777c188a1f204720760441f577a19d9030b6

71196796b8cc06d1fe563b18d94043905db92bf87309bc2690522198a7795203

744b6d454f70524b0962843551fb05bed8926fcb7e59e19b23fe63cdaf39b78f

79f43d95e7b90b21b6d00ed942327493c54d492103dcb815979d73593c14d14d

92965cb6e0ea88db6603f485dfdfe454ace7e23beda8e598f60b42179e12a926

97b82001836238d74505b83dac900029338ecc66008827ec62de18f6912e0007

99fb35fdcce4f4834780e29196df6e7d27cfa5d5a2d03ea16a4aae6aaec3541c

9c6ca77794bdd03a9ba76cbe8418a83c50261063b47fbd2d51e7c777f74492f1

9e8b51a18c0032fbb2ff84056dc353cafb03335253cf3864735f2b6231f9bcf9

b1629184416c15e00b446a533b552901a871ef923427042f6aa7f5509579c1a8

b8f3493cb2f37d7dca678e675edca280aac388baad8407b596202b2cdfb7d0f2

c2217f8324394c28b49a34f5012e59a6bd2f98c2d036678692c0d12c418ff593

c23cccc0e5b92c0a0971e6e93ee0652e4cc49996d08f9a389090a43620b2d529

d4d5ad8e8457b006c624f1163cd9a6839ff033ee05722eb2fa4693f6ea20ce1b

dcc4d9a47b9a09c705aed50062f99d0a498e62f10a7e615f9c541383bae72515

e2950cee820ee6fe3d879c0d3dfa43fa803475056e09f27f351713bb1630412b

e992e87b56b088a5d3a594388eada8c2573c974c85412bbf863e45027156fe0a

f3cca64c3c38307c013758a764e1001065dbd1a75e0b3b36f4997556740c1303

faedac8eb47265709f58cc6c91e939d149512fbf81f5eddd618dd9a9351d4e8f

4517d503c3d86e3fd25a929c7af705ed729981b900cd96603a36bb1e20abee3f

4c5f2897403fc3e4d2e0028e9becfece17b2613c8a0ec6b84c56ac2bf6baf0b4

d08dd9fd31862fad3e2a19333f74e9bc8dbc5eac0714f3a32c575329c82e3e4b

459e5fdef42d7007524d1ff2856ea5f218303c88d1cd83d00d38f5cf9645ba0f

5258f84d9f8cc4c1dc018e0ea4fbc8a56c1ec49eb934347b76f8d7bbe91f29cc

040e6d65749ab02446bbd012419cb6e00427201b261128df313daa87cea64abb

d5640bb77ed417bbfcd9e409b8653cac29eb78b0f86981fe4662893fd7b4be7c

32262e708e0467f91bbb86ee3c5955a04b942be4fb5561ea1d92332adc0cb79c

210f88eeb00fd3437cbb6de8da01ed6a027bcd5a4cd8865760baf65d4083f252

4d307d5e2783131eae8c8fba619054cdbe683c5cb6cc3401bf04b08d5b68e036

d08f63456fdd97e3b025bd9d0f41a2369fccc8303f3011d86aadde3d38a7caf8

a52a11928075e12de58794e05fd8d6ecafe49358f74b0734d2f1bb214125493f

a6e2e92d02572698b83f083d6b2c9d22073659644b91ca825b5c95cb3a3b892f

90b1ab2cce2cccd1a65b8242c39f778f723adf632122e26a0c10a970cffc73c3

dbb976d4880010e2d267cccda6d3ed745c35ce1c3310d65fe4cc5dab830fe03b

e9c22cfee3b9161c8677fc5f3e4808af845a7251c340ae226057d070551902e1

7968d34cd539d7e947315da9f39f42ccbfb782498a7362346ce83d5e9cacd374

dca641a91aa5600752c2d8f6cd8b751e655e714cd6ea0c8b247cf23bb9e671de

c70f268d549be552832722824c8150b62e0c9f32e08d11442a2c061a97bda131

b6e745d2f947ce521b425047739ecf206be862f5b8cef6118024084996c1ff38

79c574c4a628b8be8f29fd41f76007e303bbf02d609d1e3a62ca6c2ae7083e1d

564fe11fad80ef31ef067f02904d8db8afe636160fb00803537b275eea15bb67

35888a5fc383316c7ad504bf49653d18965aec49eb7cb8dcf2c27a52d4b0e292

f6628943a994b3a654cc2c04dce979a772c312d30cc9b57e7e87ebe355d88d47

2d78f8bc7a3fcf3f45efe96ca136e33ec74678da80d716e3c2c0c5e9fe61219f

24c96ae798113b454b352e672fd3188361edeecde0bdd78ec69abbfe2510c543

c350a7a3d3c9d142fa0f2f7ef7e8a0aeeb937ba684e2c4a14b363b4e3fb2dc44

406469b7d7c061a14dd3ee959d27ff2de7609ffee27556614f9ada55c9b4c105

887da9c7e2a2c5a86f531e8bb3a0a10d77829c6321ba26ab89398212e0516517

82b0441b97597cee80dcdf373bc77f7dd0ea51aca8268135baf31aef83ede4a9

42f03ce06e47ee7562707b666e3780fc260b211bf4b23021761f54598d731fff

4293c15a61b194cbf98c2cbb413e514931ada1a3b241a34e4cfda1b30c191c8a

37a7e7b390014fa314533cff462e733d2491ef50c18834e06ce8df0a2e7cf354

42e2f82baa67172643a0e285eaddc61e0190bee98cb6d11dfa6dc93ad4780d29

d5c0911a90ce75378065af7790ae94a49462b55c57ae71f49b3d1b3ec4a46bed

3974f21d025ff41edc5161b6b115a389509a607a51d47867d7f4bd8eb16a0506

45f3fbc9dea31761d3b0a7ceae28e1858495f5e0f2dd5fef3c1ab9954f2cbc5d

48b36f59091697e8053ec2b7a1b7e1d8ae41a1cd8fe0ebb30ef4cb32aa64cdd6

496445f3b2966b01edfd40458d27e6ecb85737aa035552958d83188069fc6533

3fa06d06ae072af0877bb8f52ff80d26e74153d1cd1b96b0bc0a428491af59d8

30b201ac258b70b9facd77f565c6704c8b99cee000afd2877ac88ffb8e424094

1fad3833e49aee029fad5089deb28301fbf8640fa97fa58452716bdab4f8c610

cd68e747b5f0c143ee006dbd4e545bd80540cfac03290d46416acb756ba2d986

c9aaefb6b3fb1c03b3a41afccc37561537146eefb51f7d498fbdad55bf2a8ff1

d180f55c5f9f8b6557d485ae8d09a31a52a6f827e8b41551fea9d07ff6b17739

6a26e97cf849e8631e2f6cf92f1c8839755a213cdd2b6ee500b640e38d73fc5c

434382ae159c0080dbd7dbb8c20a1ad842ab127c3f09f58bf6ef5547497dbca7

a76633d89e8dd4833c12be91175ee4af5744e9a4edc873a1349dd5be39bbac2d

83d97489848532aaad58df7d74a5ffc36ae0aad89196be99c4d6b0dcb350ed1a

bd45a96672a5dbd35a99ee3c9e12bacb99715771c59dc7071a0eaa1fcbdb379f

f9f1fbe3b68c1c465c781c33dd7b155f491444cdfa337b7f472bc03b86878361

b7121de02f2a5fe031988382ccad0a277f50fac7e27c006f1ca15e91973f6a78

39d54257f158b9b47f6d82e9e6f2427cfa4b629f355623930fa0627f59409ca3

501e81f133aedd99a8499182b5823efbbc3d5865f83c4c1de4fdbfa085924fc6

adca05fded0f8203fb79a3aaf7d33b6dbf80936f32c676f8f8bfef55103f6d6c

3c8caaee546077f1f477caa4492dd136c4c7b1884903a2065406b39877617689

f94022043e53ae7f89294a572fb66fe11ede2327547e5bcfdbec776e96fbef89

0cd304c9ff806002d9a763e0351e37e81493e723166e471c6bb8ff2acde29f43

4e62e6a4193ab91ce6630307fb62dd5d021251d206f09138aef4cb028b5aa0c8

adfc6449c4b7035b0a22d92d21dbdffde70b1eda0bf04b755a84ec47bc3965b7

fe571038b3457bc79669b5ade54223a03ab8bc85380f18f162f8df2ba83d08b2

fcbcfb6b2c31062008f7ec5efd363b532295790aa2c22220dfb21ab1e1db32f7

5600a01296c01d0059bc2db6eccf7b0079fdfb094cd8b1065d261f7a67e51b78

1f3a6a5e2a56ec8ad1afe22b5909e052b6085084b0a97076cf0697b9f854459b

5bf386540b73f41b76e68058f410094a7721d4cb1012cbeff0a49d96907a2c8f

f60eea8b71c6d95488b1a7ae93524471b7f8d5eeb7f14431be42d1956cd3338c

205ec303d5c7b2377ebef257cbfc0f21c8066e6b789f4cdf5eb3a97021586d5d

841a1950bea9acad0a6871026fb8e003b7eeecd3a8b73f2ca1e51aaec814fb2d

9488ea858098e67f7a70afca4c0aeb68e165f3db5fe1431bfd14cdd943620899

ce890aa7ff83d3b05ccb2b4cfc411d73fad7552d616d5ed950bb53072a7a4e62

1a8814ab87718639dd6603795b0155132e4b60117a9b310c1b85a548116ff446

51b650cb4160bf78637acc6b22c0996bbe1068688f20994bb8a9c7e1c4462a37

037bbd9f907338e0db3872a8ea5ba79b900368790b92885ddd8a350cc2b275a9

be7759dcb501880c63b45c61578dfd67d4014589581f2f43d1666ba38c1e63dd

92a72f36c1fce30fcf1b14e14ba868c4848b9f78d68c33ff8033f32f5f5f96fc

bcc39545c42276594a78c517e452befc5438ec93c92abc568c426677da0c684a

0b07e6dc9b5855833630bf45533320c8a2a8fdd685e9f3e0ebe62d502a391980

4ded00a4d12c4a045b681823182274a93b706b3c72f9905716b94cf03e954d02

ad56d33051d3ed4068c95e2033a3630504f3feb8bf96d3424785e697e57c0eb5

959b8403e989cd0a6d994906a09d9d210914c46d9ee10c8ee03c1fc2c6657e06

26f4ff8969543cac41b0c9a63c15f90fd4697a1f110a8df90c5f1fd9d1860d0e

0efd2d97dbe61bd9b5951180ae8979c01ef2e3bd0184dcdf850e11781531e5a4

15e5bf87fe854b3a1ecf0e8446cd39ceda429d6b6e7d78f2f78fbfea7eb5959c

---