Malware Displaying Porn Ads Discovered in Game Apps on Google Play

research.checkpoint.com/malware-displaying-porn-ads-discovered-in-game-apps-on-google-play/

January 12, 2018

January 12, 2018
Research By: Elena Root & Bogdan Melnykov

Check Point Researchers have revealed a new and nasty malicious code on Google Play Store that hides itself inside around 60 game apps, several of which are intended to be used by children. According to Google Play's data, the apps has so far been downloaded between 3 million and 7 million times.

How It Works

Dubbed 'AdultSwine', these malicious apps wreak havoc in three possible ways:

1. Displaying ads from the web that are often highly inappropriate and pornographic.
2. Attempting to trick users into installing fake 'security apps'.
3. Inducing users to register to premium services at the user's expense.

Apart from these current three main activities, the malicious code can use its infrastructure to broaden its goals to other purposes, such as credential theft.

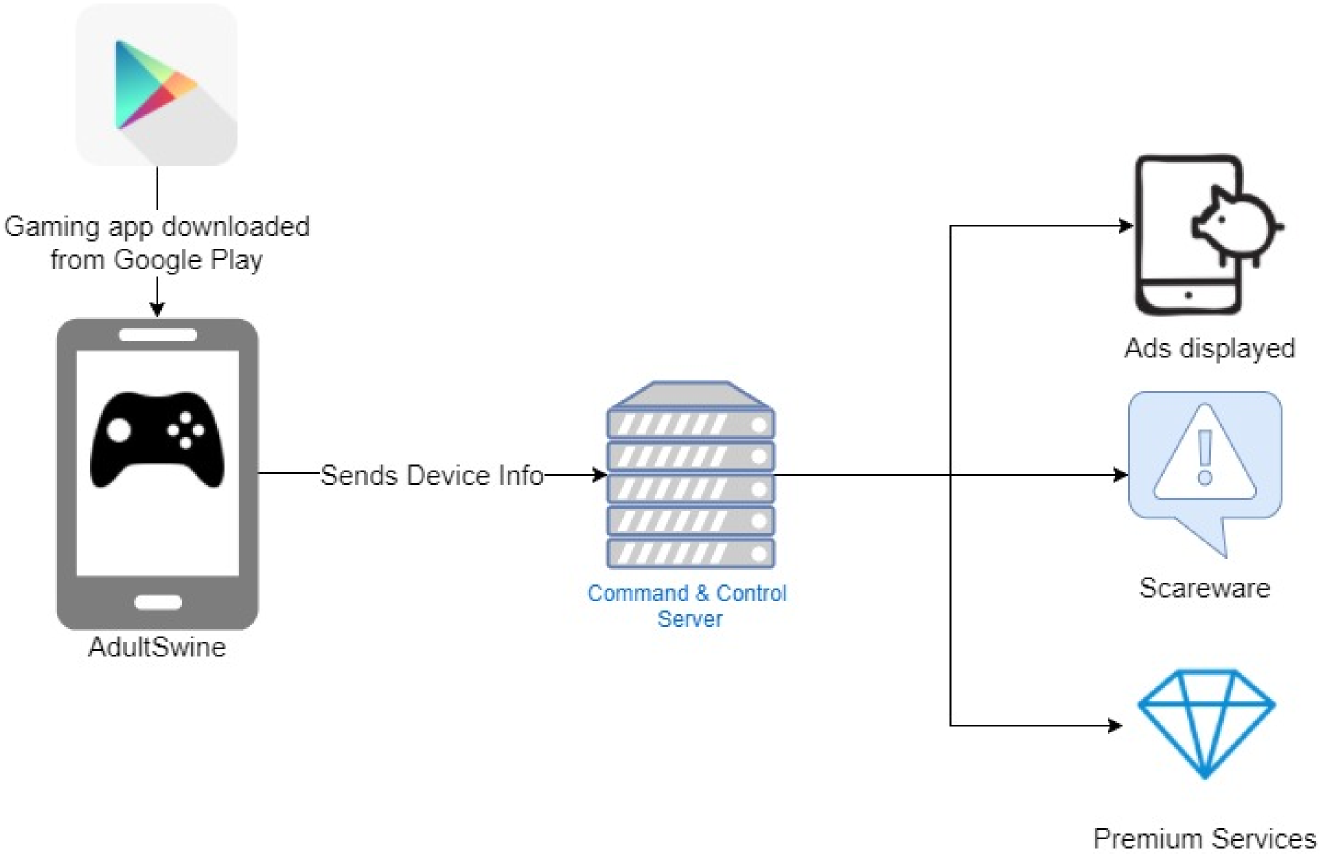


Figure 1: *AdultSwine operation flow*

Once the malicious app is installed on the device, it waits for a boot to occur or for a user to unlock his screen, upon which it initiates its malicious activity.

Illegitimate and Inappropriate Ads

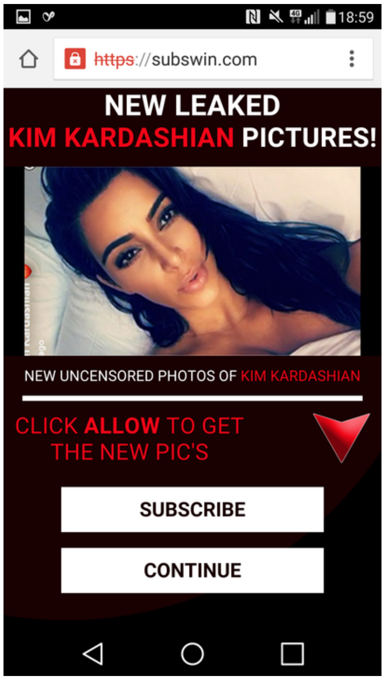
First, the malicious code contacts its Command and Control server (C&C) to report the successful installation, sends data about the infected device and then receives the configurations, which determine its course of operation. These configurations instruct it on whether to hide its icon (to encumber removal), which ads to display, over which apps and on what terms. It is interesting to note that the server however forbids ads to be displayed over certain apps such as browsers and social networks, in order to avoid suspicion.

The malicious code then verifies certain conditions regarding the device's status and checks which app is currently running on screen. Once all its terms are met, it begins to display the illegitimate ads outside of the app's context. If it is embedded inside a web browser app the ads will be displayed inside that browser, if not they will be displayed inside a designated web view.

As for the ads being displayed, they come from two main sources; the first is that of the main ad providers, which forbid such illegitimate display of their ads. The second is the malicious code's own ad library, which contains ads of an offensive nature, including pornographic ads.

All these are displayed to children while playing the game that the app is masquerading as.

Below is a mild example of the ads presented and a comment from one of the victims, whose son had an unfortunate experience.



NEW LEAKED
KIM KARDASHIAN PICTURES!

NEW UNCENSORED PHOTOS OF KIM KARDASHIAN

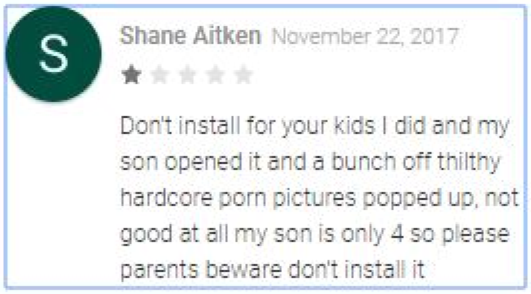
CLICK ALLOW TO GET
THE NEW PIC'S

Figure 2: *Examples of ad displayed and user reviews on Google Play*

Scareware – Deceptive App Install Tactics

Another course of action the malicious app pursues is scaring users into installing unnecessary and even harmful “security” apps.

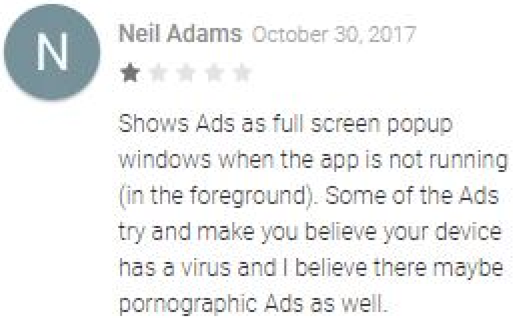
First, the malicious app displays an ad that claims the user’s device is infected by a virus. Should the user press the notification of “Remove Virus Now” he is redirected to an app in the Google Play Store with a somewhat questionable connection to virus removal. An experienced eye could easily foresee this tactic, though a child playing a game app is easy prey for such nefarious apps.



Shane Aitken November 22, 2017

★☆☆☆☆

Don't install for your kids I did and my son opened it and a bunch off thilthy hardcore porn pictures popped up, not good at all my son is only 4 so please parents beware don't install it



Neil Adams October 30, 2017

★☆☆☆☆

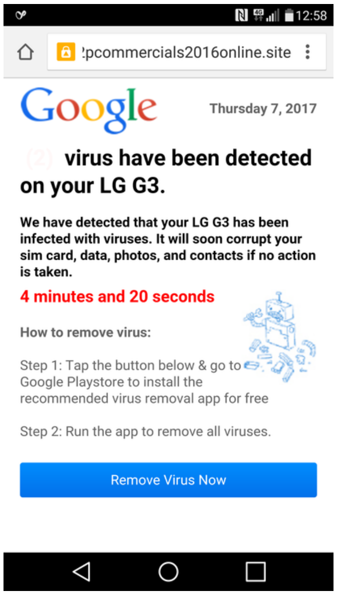
Shows Ads as full screen popup windows when the app is not running (in the foreground). Some of the Ads try and make you believe your device has a virus and I believe there maybe pornographic Ads as well.

Figure 3 *– Left image: Scareware Ad Displayed*
Centre image: The redirect ‘anti-virus’ app in Google Play.
Right image: User reviews in Google Play

Registering To Premium Services

Another technique used by the malicious app is registering to premium services and charging the victim’s account for fraudulent premium services they did not request to send or receive. In a similar way to the scareware tactic seen above, the malicious app initially displays a pop-up ad, which attempts to persuade the user to click through.

This time however, the ad claims that the user is entitled to win an iPhone by simply answering four short questions. Should the user answer them, the malicious code informs the user that he has been successful, and asks him to enter his phone number to receive the prize. Once entered, the malicious code then uses this number to register to premium services.



Thursday 7, 2017

(2) virus have been detected on your LG G3.

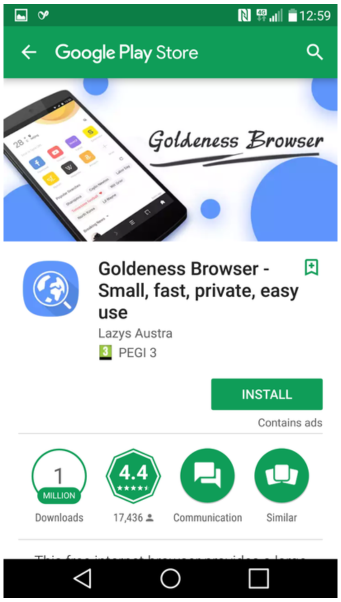
We have detected that your LG G3 has been infected with viruses. It will soon corrupt your sim card, data, photos, and contacts if no action is taken.

4 minutes and 20 seconds

How to remove virus:

Step 1: Tap the button below & go to Google Playstore to install the recommended virus removal app for free

Step 2: Run the app to remove all viruses.



Goldeness Browser - Small, fast, private, easy use

Lazys Austra

PEGI 3

The flow is presented in the images below.

Notification of Winning the iPhone *Request to Enter Phone Number*

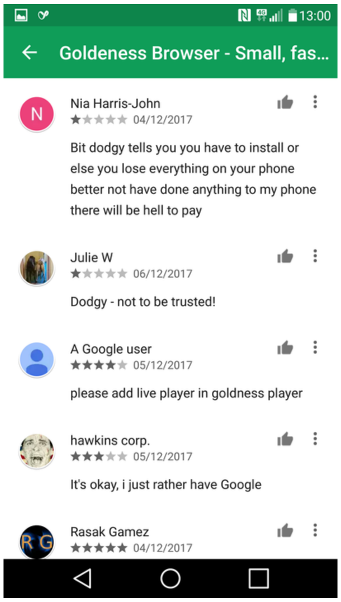
A Comprehensive Threat

Although for now this malicious app seems to be a nasty nuisance, and most certainly damaging on both an emotional and financial level, it nevertheless also has a potentially much wider range of malicious activities that it can pursue, all relying on the same common concept.

The malicious code simply receives a target link from its Command and Control server and displays it to the user. While in some cases this link is merely an advertisement, it could also lead to whatever social engineering scheme the hacker has in mind.

Indeed, these plots continue to be effective even today, especially when they originate in apps downloaded from trusted sources such as Google Play.

Appendix 1 – List of App Names



Goldeness Browser - Small, fas...

Nia Harris-John
★☆☆☆☆ 04/12/2017

Bit dodgy tells you you have to install or else you lose everything on your phone better not have done anything to my phone there will be hell to pay

Julie W
★☆☆☆☆ 06/12/2017

Dodgy - not to be trusted!

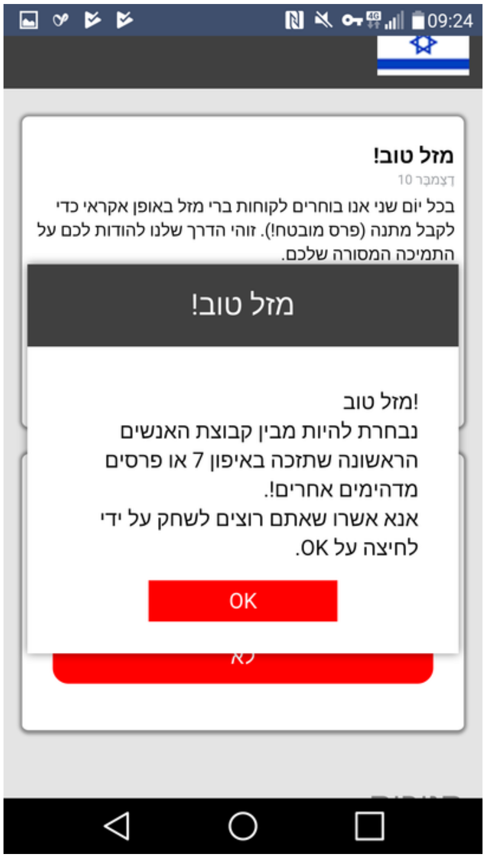
A Google user
★★★★☆ 05/12/2017

please add live player in goldness player

hawkins corp.
★★★☆☆ 05/12/2017

It's okay, i just rather have Google

Rasak Gamez
★★★★★ 04/12/2017



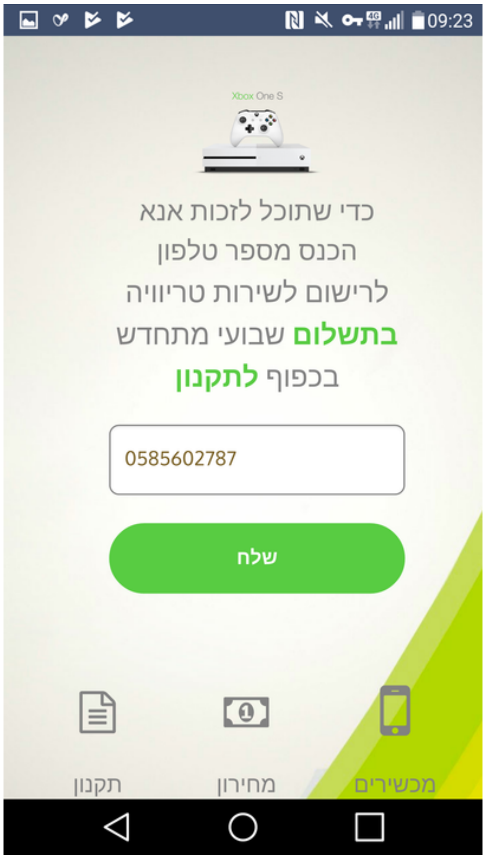
מזל טוב!

דצמבר 10

בכל יום שני אנו בוחרים לקוחות ברי מזל באופן אקראי כדי לקבל מתנה (פרס מובטח!). זוהי הדרך שלנו להודות לכם על התמיכה המסורה שלכם.

מזל טוב!

!מזל טוב
נבחרת להיות מבין קבוצת האנשים הראשונה שתזכה באיפון 7 או פרסים מדהימים אחרים!.
אנא אשרו שאתם רוצים לשחק על ידי לחיצה על OK.



כדי שתוכל לזכות אנא
הכנס מספר טלפון
לרישום לשירות טריוויה
בתשלום שבועי מתחדש
בכפוף **לתקנון**

0585602787

App Name	Minimum Downloads	Maximum Downloads
Five Nights Survival Craft	1,000,000	5,000,000
Mcqueen Car Racing Game	500,000	1,000,000
Addon Pixelmon for MCPE	500,000	1,000,000
CoolCraft PE	100,000	500,000
Exploration Pro WorldCraft	100,000	500,000
Draw Kawaii	100,000	500,000
San Andreas City Craft	100,000	500,000
Subway Banana Run Surf	100,000	500,000
Exploration Lite : Wintercraft	100,000	500,000
Addon GTA for Minecraft PE	100,000	500,000
Addon Sponge Bob for MCPE	100,000	500,000
Drawing Lessons Angry Birds	50,000	100,000

Temple Crash Jungle Bandicoot	50,000	100,000
Drawing Lessons Lego Star Wars	50,000	100,000
Drawing Lessons Chibi	50,000	100,000
Girls Exploration Lite	10,000	50,000
Drawing Lessons Subway Surfers	10,000	50,000
Paw Puppy Run Subway Surf	10,000	50,000
Flash Slither Skin IO	10,000	50,000
Invisible Slither Skin IO	10,000	50,000
Drawing Lessons Lego Ninjago	10,000	50,000
Drawing Lessons Lego Chima	5,000	10,000
Temple Bandicoot Jungle Run	1,000	5,000
Blockcraft 3D	1,000	5,000
Jungle Survival Craft 1.0	1,000	5,000
Easy Draw Octonauts	1,000	5,000
halloweenskinsforminecraft	1,000	5,000
skinsyoutubersmineworld	1,000	5,000
youtubersskins	1,000	5,000
DiadelosMuertos	500	1,000
Draw X-Men	500	1,000
Moviesskinsforminecraft	500	1,000
Virtual Family – Baby Craft	500	1,000
Mine Craft Slither Skin IO	500	1,000
Guide Clash IO	100	500
Invisible Skin for Slither IO app	100	500
Zombie Island Craft Survival	100	500
HalloweenMakeUp	100	500

ThanksgivingDay	100	500
ThanksgivingDay2	100	500
Jurassic Survival Craft Game	100	500
Players Unknown Battle Ground	100	500
Subway Bendy Ink Machine Game	100	500
Shin Hero Boy Adventure Game	100	500
Temple Runner Castle Rush	100	500
Dragon Shell for Super Slither	100	500
Flash Skin for Slither IO app	50	100
AnimePictures	50	100
Pixel Survival – Zombie Apocalypse	50	100
Fire Skin for Slither IO app	10	50
San Andreas Gangster Crime	10	50
fidgetspinnerforminecraft	10	50
Stickman Fighter 2018	10	50
Subway Run Surf	10	50
Guide Vikings Hunters	10	50
Woody Pecker	10	50
Pack of Super Skins for Slither	10	50
Spinner Toy for Slither	10	50
How to Draw Coco and The Land of the Dead	10	50
How to Draw Dangerous Snakes and Lizards Species	1	5
How to Draw Real Monster Trucks and Cars	1	5
How to Draw Animal World of The Nut Job 2	1	5
How to Draw Batman Legends in Lego Style	1	5

Appendix 2 – List of SHA256 hashes

08a595d274c5988a975a2746705422cbf110ce1de6e0b66fd798acc961a30687

d49b4359851e1bc4d66510412e111115fff19bbafc92fabee51229e1876b649d

952cccf1b4149110dbc336b8925c5d8e4a3d71c60969b2d6127a4bf9bb7ba08d

19566767d6b1e340436a520a30af7febf480e812443f435fc4800c7a1d27248e

14f1829a9d3c38a45c869c28ee8cde1e4e67cd5a637b22edb62de01e3faf7932

34d1a4a40a959d2c4219dfc5ca7e4b6aa9771ad1c577baf0a2fe16b655e9837d

89e0bfae364ce7e9319c4e7fe365eb68f8d590d5f3d81abad4b81ce78736d4a2

c12a75a55e6bd72945a74497b72f448eb8303605a8a1418a7e33abf25a447b48

e06a932be78bc9431c4cd876a45d504f30c3d9032fbfa2945eaf1a42c5b040f8

bfe453afb0afd92d42362bdc662c8cede2b35f004c9031ab6461fb765cf0c893

281db6373f5b40dffa88ce9cb054eb3744bc95d51089b067549f7166c1a3075d

a309d862ed007befa05cfd36a8ddb64fe4f39fd7298890d2c5f4c38d3a6fd39a

a571bb83695b79a4521e7a297b5b4cd04e3a18e2c4a58b796ba6ac68e0634f5f

3d3e8e48db16546f7c4d1195cd87c1c705f16e9208c5a91a36a9df8686e6bcd5

6dd8096ad8d8f4065153f20247e2391ca0bfd8d269e31523dd4907102527ee0b

73561c69d590f0a74528b3579581c9d2a157c36f6abfb90a1188bffd88549de9

4e4ca96b22aeb5e990548cbc3c9ac9266dce055b6a74ca8202b2a43f6a0945f2

f9bff59ed24bb8c873ce209239e18a3209cd311fd911ce9fd4ec4087e242ed27

31304f5387025f5016d4716ed0943193b9e58acf22dbf904db8a160864642309

b908f2c4163d7ce0b20581d65395c2ebc2b866dc0a709ef4deda2038a519e3ad

653e9fab85fda60460c4374666c9513ce85967eafd279a687b80b622c1631ff2

564313b6d07bc54482671b010e23095fcb35fd1402cbf8464bc2b3f9e4a5f3c6

67f93cc2fc5dd4df95618399afc3b7070310b88d9b7e1b817b97e493a1eac076

82f41c08c4d48960083c83625a77e6f8cae62e4c2548d3a21128b23c7abf570c

64da0f06b505a2dbe3f6516c117ffaa1af44593733b44a3a796400c5a4d982e5

f0921f0cbaaecd517f900988b2a220f71e28a67587c8a811c4a56397223dd7d6
a40d4621097afed5670c9c4da87603cb2f3a70da7d14d9b4340c58a67d9cf6f4
5302cf3afc9d16a9bcd6c05e2d6bdac54689f0119d61037fe53b0e02e1753e1b
8a94245757531eb074a0ac94b78871d161f87d46a36f0e8f8c62938e2a02ae84
8b2ec78b63e469129ae84cf23f3942d5e5b63fcc42348c5ffa4722a57355488d
ac5a0bec8e5b6e08649b40a67e6f9786f83c9e54b8d870bc8c5e4b0e0fb6e6c1
0d8d1eece839fa842f2bc6b8b3f6f15494f4e02a14f51fd7a4bf9971a87756d5
d33b27e37bd7c59e36bc7eabcc0e576f735d0bc39f7b3f1796926ba0e0745742