

Google Play apps with 150 million installs contain aggressive adware

NurPhoto | Getty Images

reader comments

35 with 30 posters participating

Share this story

Researchers have identified a massive adware campaign that invaded the official Google Play market with more than 200 highly aggressive apps that were collectively downloaded almost 150 million times.

The 210 apps discovered by researchers from security firm Checkpoint Software bombarded users with ads, even when an app wasn't open, according to a blog post published by the company on Wednesday. The apps also had the ability to carry out spearphishing attacks by causing a browser to open an attacker-chosen URL and open the apps for Google Play and third-party market 9Apps with a specific keyword search or a specific application's page. The apps reported to a command-and-control server to receive instructions on which commands to carry out.

Once installed, the apps installed code that allowed them to perform actions as soon as the device finished booting or while the user was using the device. The apps also could remove their icon from the device launcher to make it harder for users to uninstall the nuisance apps. The apps all used a

software development kit called RXDrider, which Checkpoint researchers believe concealed its abusive capabilities from app developers. The researchers dubbed the campaign SimBad, because many of the participating apps are simulator games.

“With the capabilities of showing out-of-scope ads, exposing the user to other applications, and opening a URL in a browser, SimBad acts now as an Adware, but already has the infrastructure to evolve into a much larger threat,” Checkpoint researchers wrote.

The top 14 apps were collectively downloaded a whopping 75 million times, with the No. 1 app receiving 10 million installs and the next 13 getting 5 million downloads each. The next 53 each received 1 million downloads. They are:

Package Name	App Name	# Installs
com.heavy.excavator.simulator.driveandtransport	Snow Heavy Excavator Simulator	10,000,000
com.hoverboard.racing.speed.simulator	Hoverboard Racing	5,000,000
com.zg.real.tractor.farming.simulator.game	Real Tractor Farming Simulator	5,000,000
com.ambulancerescue.driving.simulator	Ambulance Rescue Driving	5,000,000
com.heavymountain.bus2018simulator	Heavy Mountain Bus Simulator 2018	5,000,000
com.firetruckemergency.driver	Fire Truck Emergency Driver	5,000,000
com.farming.tractor.realharvest.simulator	Farming Tractor Real Harvest Simulator	5,000,000
com.carparking.challenge.parksimulator	Car Parking Challenge	5,000,000
com.speedboat.jetski.racing.simulator	Speed Boat Jet Ski Racing	5,000,000
com.watersurfing.carstunt.racing.simulator	Water Surfing Car Stunt	5,000,000
com.offroad.woodtransport.truckdriver	Offroad Wood Transport Truck Driver 2018	5,000,000
com.volumen.booster.equalizer	Volumen booster & Equalizer	5,000,000
com.ks.prado.Car.parking.race.drive.apps	Prado Parking Adventure	5,000,000

com.zg.offroad.Oil.tanker.transporter.truck.cargo.simulator	Oil Tanker Transport Truck Driver	5,000,000
com.monstertruck.demolition	Monster Truck Demolition	1,000,000
com.hummerlimotaxi.simulator.driving	Hummer taxi limo simulator	1,000,000
com.excavator.wreckingball.demolition.simulator	Excavator Wrecking Ball Demolition Simulator	1,000,000
com.offroad.gold.transport.truck	Offroad Gold Transport Truck Driver 2018	1,000,000
com.sea.animals.trucktransport.simulator	Sea Animals Truck Transport Simulator	1,000,000
com.water.surfingrace.motorbike.stunt	Water Surfing Motorbike Stunt	1,000,000
com.policechase.thiefpersecution	Police Chase	1,000,000
com.police.plane.transporter.game	Police Plane Transporter	1,000,000
com.ambulance.driver.extreme.rescue.simulator	Ambulance Driver Extreme Rescue	1,000,000
com.hovercraftracer.speedracing.boat	Hovercraft Racer	1,000,000
com.cars.transport.truckdriver.simulator	Cars Transport Truck Driver 2018	1,000,000
com.motorbike.pizza.delivery.drivesimulator	Motorbike Pizza Delivery	1,000,000
com.heavy.excavator.stonecutter.simulator	Heavy Excavator – Stone Cutter Simulator	1,000,000
com.bottle.shoot.archery.game	Bottle shoot archery	1,000,000
com.offroadbuggy.car.racingsimulator	Offroad buggy car racing	1,000,000
com.garbagetruck.city.trash.cleaningsimulator	Garbage Truck – City trash cleaning simulator	1,000,000
com.tanks.attack.simulator.war.attack	Tanks Attack	1,000,000
com.dinosaurpark.trainrescue	Dinosaur Park – Train Rescue	1,000,000
com.pirateshipboat.racing3d.simulator	Pirate Ship Boat Racing 3D	1,000,000
com.flyingtaxi.simulator.race	Flying taxi simulator	1,000,000
com.jetpackinwater.racersimualtor.danger	Jetpack Water	1,000,000
com.boostervolumen.amplifiersoundandvolumen	Volumen Booster	1,000,000

com.farmgames.animal.farming.simulator	Animal Farming Simulator	1,000,000
com.monstertruck.racing.competition.simulator	Monster Truck	1,000,000
com.simulator.offroadjeep.car.racing	Offroad jeep car racing	1,000,000
com.simulator.flyingcar.stunt.extremetracks.racing	Flying Car Stunts On Extreme Tracks	1,000,000
com.simulator.tractorfarming.driving	Tractor Farming 2018	1,000,000
com.impossible.farming.transport.simulator	Impossible Farming Transport Simulator	1,000,000
com.volumenbooster.equalizerboost	Volumen Booster	1,000,000
com.mustang.rally.championship.racingsimulator	Mustang Rally Championship	1,000,000
com.deleted.photo.recovery	Deleted Photo Recovery	1,000,000
com.race.boat.speedy	Speed Boat Racing	1,000,000
com.cycle.bike.racing.game	Super Cycle Jungle Rider	1,000,000
com.write.name.live.wallpaper.hd	My name on Live Wallpaper	1,000,000
com.maginal.unicorn.game	Magical Unicorn Dash	1,000,000
com.grafton.cycle.jungle.rider.race	Super Cycle Jungle Rider	1,000,000
com.lovecallingapps.lovecaller.Screen	Love Caller Screen	1,000,000
com.city.car.funny.racing.stunt.game.pro	Racing Car Stunts On Impossible Tracks	1,000,000
com.citycar.funny.racinggame.stunt.simulator	Racing Car Stunts On Impossible Tracks 2	1,000,000
com.urban.Limo.taxi.simulation.games	Urban Limo Taxi Simulator	1,000,000
com.cg.heavy.tractor.simulator.game	Tractor Farming Simulator	1,000,000
com.campervan.drivingsimulator.caravan	Camper Van Driving	1,000,000
com.bootleshoot.sniper	Bottle Shoot Sniper 3D	1,000,000
com.globalcoporation.fullscreenincomingcaller.app	Full Screen Incoming Call	1,000,000
com.mustache.beard.editor	Beard mustache hairstyle changer Editor	1,000,000
com.volumenbooster.increaservolumen	Volumen Booster	1,000,000
com.photoeditor.girlfriend.addgirlstophoto.pic	girlfriend photo editor	1,000,000

com.tracker.location.number.free.spy	Mobile Number Tracker & Locator	1,000,000
com.garden.editor.app	Garden Photo Editor	1,000,000
com.fortunewheel.game	Fortune Wheel	1,000,000
com.farming.transport.tractor.simulator	Farming Transport Simulator 2018	1,000,000
com.offroad.tractor.transport.drivingsimulator	OffRoad Tractor Transport	1,000,000
com.customwallpaper.mynameonlivewallpaper	my name on live wallpaper	1,000,000

The remainder received 500,000 or fewer downloads each. Checkpoint has a full list of all the apps [here](#).

Web searches found that many apps with similar or identical names were still available in Google Play at the time this story was being reported. This will make it harder for users to determine if an installed app is benign or abusive. One possibly useful method for determining abuse is to use the package name to search a phone for abusive apps. While Google has removed all the reported apps from Play, it wasn't immediately clear if those apps will automatically be uninstalled from infected devices or if users must do so manually. Company representatives didn't immediately respond to emails seeking comment for this post.

Malicious and abusive apps in Google Play have been an ongoing problem for years. The company is quick to remove bad apps once they're reported, but often, by that point, hundreds of millions of users have already been infected. While there's no sure-fire way to know if a Google Play app is safe, reading user reviews, scrutinizing requested permissions, and avoiding apps from unknown developers or with fewer than 10,000 downloads can often help. When in doubt, or in cases where apps have minimal benefit, it's best to steer clear.

<https://arstechnica.com/?p=1473183>