SimBad: A Rogue Adware Campaign On Google Play

By deugenio

Published: 2019-03-13 · Archived: 2026-04-06 03:09:24 UTC

March 13, 2019

Research by: Elena Root and Andrey Polkovnichenko

Check Point researchers from the Mobile Threat Team have discovered a new adware campaign on the Google Play Store. This particular strain of Adware was found in 206 applications, and the combined download count has reached almost 150 million. Google was swiftly notified and removed the infected applications from the Google Play Store.

Inside the SDK

The malware resides within the ‘RXDrioder’ Software Development Kit (SDK), which is provided by ‘addroider[.]com’ as an ad-related SDK. We believe the developers were scammed to use this malicious SDK, unaware of its content, leading to the fact that this campaign was not targeting a specific county or developed by the same developer. The malware has been dubbed ‘SimBad’ due to the fact that a large portion of the infected applications are simulator games.

The Infection Chain

Once the user downloads and installs one of the infected applications, ‘SimBad’ registers itself to the ‘BOOT_COMPLETE’ and ‘USER_PRESENT’ intents, which lets ‘SimBad’ to perform actions after the device has finished booting and while the user is using his device respectively.

After installation, the malware connects to the designated Command and Control (C&C) server, and receives a command to perform. ‘SimBad’ comes with a respected list of capabilities on the user’s device, such as removing the icon from the launcher, thus making it harder for the user to uninstall, start to display background ads and open a browser with a given URL.

Fig 1: *A list of the possible commands from the C&C server*

Fig 2: *Code that hides the application's Icon to make it harder to remove*

Fig 3: *The code that starts the background ads*

What Does SimBad Do?

'SimBad' has capabilities that can be divided into three groups – Show Ads, Phishing, and Exposure to other applications. With the capability to open a given URL in a browser, the actor behind 'SimBad' can generate phishing pages for multiple platforms and open them in a browser, thus performing spear-phishing attacks on the user.

With the capability to open market applications, such as Google Play and 9Apps, with a specific keyword search or even a single application's page, the actor can gain exposure for other threat actors and increase his profits. The actor can even take his malicious activities to the next level by installing a remote application from a designated server, thus allowing him to install new malware once it is required.

Fig 4: *An illustration of the attack vector*

The C&C Server

The C&C server observed in this campaign is 'www[.]addroider.com'. This server runs an instance of 'Parse Server' (source on GitHub), an open source version of the Parse Backend infrastructure, which is a model for providing web app and mobile app developers with a way to link their applications to backend cloud storage and APIs exposed by back-end applications, while also providing features such as user management, push notifications and more.

The domain 'addroider[.]com' was registered via GoDaddy, and uses privacy protection service. While accessing the domain from a browser you get a login page very similar to other malware panels. The 'Register' and 'Sign Up' links are broken and 'redirects' the user back to the login page.

Fig 5: *The login page of the domain*

Fig 6: *The WhoIS information on RiskIQ's PassiveTotal*

According to RiskIQ's PassiveTotal, the domain expired 7 months ago. As a result, it may be that are looking into a compromised, parked domain that was initially used legitimately, but is now participating in malicious activities.

Our Take

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.

Appendix 1 – List of Infected Applications:

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
com.flying.ambulance.emergency.rescue.simulator	Flying Ambulance Emergency Rescue	500,000
com.mustang.driving.car.race	Mustang Driving Car Race	500,000
com.waterpark.carracing.simulator	Waterpark Car Racing	500,000
com.impossibletrucks.extremetrucks.simulator	Impossible Tracks – Extreme Trucks	500,000
com.extreme.flying.motorbike.stuntsimulator	Flying Motorbike Stunts	500,000
com.emergency.firetruck.rescue.drivingsimulator	Fire Truck Emergency Rescue – Driving Simulator	500,000
com.snowplow.simulator.heavysnow.excavator	Heavy Snow Excavator Snowplow Simulator	500,000
com.waterskiing.simulator.games	Water Skiing	500,000
com.photomaker.editor.women.makeupandhairstyle	Women Make Up and Hairstyle Photo Maker	500,000
com.fortune.mountain	Mountain Bus Simulator	500,000
com.vanpizza.truckdelivery.simulator	Van Pizza	500,000
com.truck.simulator.transportandparking	Truck Transport and Parking Simulator	500,000
com.hoverboard.racing.spider.attacksimulator	Hoverboard Racing Spider Attack	500,000
com.moto.sport.championship.racingsimulator	Motorsport Race Championship	500,000
com.demolitionderby.simulator	Demolition Derby	500,000

com.lovecaller.free.loveringtones	Love Caller with love ringtones	500,000
com.house.transport.truck.movingvan.simulator	House Transport Truck – Moving Van Simulator	500,000
com.heavy.excavator.simulator.stonedriller	Heavy Excavator Stone Driller Simulator	500,000
com.cycle.downhill.game	Super Cycle Downhill Rider	500,000
com.extreme.rallychampionship.race	Extreme Rally Championship	500,000
com.missileattack.army.truck	Missile Attack Army Truck	500,000
com.mobile.caller.location.tracker.freecall	Caller Location & Mobile Location Tracker	500,000
com.mobilenumberlocator.tracker	Mobile number locator	500,000
com.mynameonlivewallpaper.animated.hd	My name on Live Wallpaper	500,000
com.spk.coach.offroad.School.bus.mountain.free	City Metro Bus Pk Driver Simulator 2017	500,000
com.fullscreen.incomingcaller.app	Full Screen Incoming Call	500,000
com.allsuit.man.casualshirt.photo.editor	Man Casual Shirt Photo Suit	500,000
com.americanmuscle.car.race	American muscle car race	500,000
com.offroad.nuclearwastetransport.truckdriver	Offroad Nuclear Waste Transport – Truck Driver	500,000
com.madcars.fury.racing.driving.simulator	Mad Cars Fury Racing	100,000
com.high.wheeler.speed.race.championship	High Wheeler Speed Race	100,000
com.colorbynumber.number.coloring.paint.game	Number Coloring	100,000
com.campervan.race.driving.simulator.game	Camper Van Race Driving Simulator 2018	100,000
com.unicornfloat.speedrace.simulator	Unicorn Float – Speed Race	100,000
com.dualscreenbrowser	Dual Screen Browser	100,000
com.harvest.timber.simulatorandtransport	Harvest Timber Simulator	100,000
com.racingsimulator.hot.micro.racers	Hot Micro Racers	100,000
com.lara.unicorn.dash.magical.raider.race	Lara Unicorn Dash	100,000

com.wingsuit.simulator.extreme	Wingsuit Simulator	100,000
com.foodtruck.driving.simulator	Food Truck Driving Simulator	100,000
com.dograce.competition	Dog Race Simulator	100,000
com.suvcar.parking.simulator.game	SUV car – parking simulator	100,000
com.clap.phonefinder.locator	Phone Finder	100,000
com.phonenumerlocator.findphonenumbers	Phone number locator	100,000
com.whatsapplock.gallerylock.ninexsoftech.lock	Gallery Lock	100,000
com.secret.screenrecorder.screenshotrecord	Secret screen recorder	100,000
com.facebeauty.makeup	Face Beauty Makeup	100,000
com.write.your.christmas.letter.santa.threewisemen	Christmas letters to santa and three wise man	100,000
com.deletedfiles.photo.audio.video.recovery	Deleted Files recovery	100,000
com.screndualbrowserdouble.app.android	Dual Screen Browser	100,000
com.crack.mobile.screen.prank	Broken Screen – Cracked Screen	100,000
photoeditor.Garden.photoframe	Garden Photo Editor	100,000
com.modiphotoframe.editor	Modi Photo Frame 2	100,000
com.callerscreen.lovecaller	Love Caller Screen	100,000
com.antitheftalarm.fullbatteryalarm.sound	Anti Theft & Full Battery Alarm	100,000
com.lovecaller.screen.custom	Love Caller Screen 2	100,000
com.sms.message.voice.reading	Voice reading for SMS. Whatsapp & text sms	100,000
com.photo.text.editor.nameonpic	Name on Pic-Name art	100,000
com.mtsfreegames.Speedboatracing	Speed Boat Racing	100,000
com.simulator.traindriving	Train Driving Simulator	100,000
com.grafton.Cycle.jungle.rider	Super Cycle Rider	100,000
com.gl.racinghorse.competition	Racing Horse Championship 3D	100,000
moveapptosd.tosdcard.freeapp	Move App To SD Card 2016	100,000

com.avatarmaker.poptoy.creator	Pop Toy Creator	100,000
com.myphoto.live.wallpaper.editor	Photo Live Wallpaper	50,000
com.messenger2.play.game.Unicorndashk	Magical Unicorn Dash	50,000
com.truck.wheelofdeath	Truck Wheel of Death	50,000
com.livetranslator.translateinlive	Live Translator	50,000
com.volumecontrol.widget.volumebooster	Volume Control Widget	50,000
com.worldcup2018football.shirt.maker.photoeditor	World cup 2018 football shirt maker	50,000
com.girlfriendphotoeditor.girlsinyourphoto	Girlfriend Photo Editor 2	50,000
com.myphoto.on.musicplayer.free	My Photo on Music Player	50,000
com.taxidriving.simulatorgame.race	taxi	50,000
com.garden.photoeditor.photoframe	Garden Photo Editor	50,000
com.fortunewheel.deluxe	Fortune Wheel Deluxe	50,000
com.motorcycle.extremeracing.simulator	Extreme Motorcycle Racer	50,000
com.offroad.snow.bike.christmas.racing	Offroad Snow Bike – Christmas Racing	50,000
com.Droidhermes.bottleninja	Bottle Shoot	50,000
com.Hadiikhiya.photochangebackground	Photo Background Changer 2017	50,000
com.offroad.christmas.treetransport.truck.driversimulator	Offroad Christmas Tree Transport	50,000
com.tank.transport.armytruck.simulator	Tank Transport Army Truck	50,000
com.flagteams.facepaint.editor.world2018cup	Flag face paint: World Cup 2018	10,000
com.russianworld2018cup.livewallpaper.flagsteam	World Cup 2018 Teams Flags Live Wallpaper	10,000
com.editor.selfie.camera.photo	Selfie Camera	10,000
com.desirepk.Offroad.transport.simulator.apps	Missile Attack Army Truck	10,000
massimo.Vidlan.maxplayer	Max Player	10,000

com.flashalerts.callandsms	Flash Alert – Flash on Call	10,000
com.photovideo.maker.withmusic	Photo Video Maker with Music	10,000
com.braingames.iqtest.skills	Brain Games & IQ Test	10,000
com.mix.audio.and.video	Audio Video Mixer	10,000
com.poptoy.creator.edityourpoptoy	Pop Toy Creator 2	10,000
com.flashalert.callandsms	Flash on Call and SMS	10,000
com.photoframe.of.heart	Heart Photo Frames	10,000
com.shayari.hindi.status.photo.text	Shayari 2017	10,000
com.happy.photo.birthday.cake	Photo on Birthday Cake	10,000
com.photoeditor.nature.photoframes	Nature Photo Frames	10,000
com.photoframe.calendar2018editor	Calendar 2018 Photo Frame	10,000
com.christmas.truck.transportsimulator.game	Christmas Truck Transport Simulator	10,000
com.christmas.vandrive.modern.santa	Modern Santa – Christmas van drive	10,000
com.anbrothers.voicechanger.app	Change your voice	10,000
com.monsters.vs.water.duel	Moster vs Water	10,000
com.flowers.editor.photo.frame	EDIT Flowers Photo Frames	10,000
videoeditor.musicvideo.Phototovideomaker.videoeditor	Photo Video Maker with Music	10,000
com.racing.games.toiletpaper.race	Toilet Paper Race	10,000
com.Zv.puppiesdog.racegame	Dog Crazy Race Simulator	10,000
com.luxury.photo.frame.photo.editor	Luxury Photo Frame	10,000
com.bike.wheelofdeath	Bike Wheel of Death	10,000
com.qbesoft.worldfamousphotoframes.app	World Famous Photo Frames	10,000
com.heavysnowexcavator.christmas.rescue	Heavy Snow Excavator Christmas Rescue	10,000
com.syor.deleted.photo.recovery.video.restore	Deleted Files Recovery	10,000

com.footballanalyzer.resultsandstats	Football Results & Stats Analyzer	5,000
com.photoframe.cube3d.live.wallpaper.hd	3D Photo Frame Cube Live Wallpaper	5,000
com.photoframe.geenhill	Green Hill PhotoFrame	5,000
com.christmas.magnetic.magicboard.drawandwrite	Christmas Magic Board	5,000
com.animalspart.photo.editor	Animal Parts Photo Editor	5,000
com.camera.blur.photoeffects	DSLR Camera Blur	5,000
com.quick.photo.frame.carphotoframe	Car Photo Frame	5,000
com.game.handsslap.manitascalientes.redhands	Hands Slap Game	5,000
com.maa.durga.live.wallpaper	4D Maa Durga Live Wallpaper	5,000
com.photomontage.men.sweatshirt.editor	Men Sweatshirt Photo Editor	1,000
com.wordsgame.connectletters	Connect Letters. Words Game	1,000
lanas.recover.deleted.pictures.photos	Recover Deleted Pictures	1,000
com.customized.radio.alarm.clock	Custom Radio Alarm Clock	1,000
com.antispamcalls.blockspamcaller	Anti-spam Calls	1,000
com.compatibilitytest.friends.couples	Compatibility Test	1,000
com.dualscreen.android.app.double	Dual Screen Browser	1,000
com.magic.glow.livewallpaper.animatedwallpaper	Magic Glow Live Wallpaper	1,000
com.game.virtualpet.porgy	Porgy Virtual Pet	1,000
com.explosiongame.taptheball	Tap the Ball	1,000
com.analog.digital.clock.live.wallpaper	Clock Live Wallpaper	1,000
com.royalestas.information	Royale Stats	1,000
com.editor.firetext.photo.frame	Fire text photo frame	1,000
editor.card.greetings.christmas.com.christmasgreetingscard	Christmas greetings card	1,000
com.bestappsco.bestapplock.free	Best App Lock	1,000
com.DJ.photoframe.editor	DJ Photo Frames	1,000

com.autocall.redial.automatic.recall	Auto Call redial	500
com.picquiz.guess.picture.game	Guess the picture	500
com.professionalrecorder.audio.call.record	ProfesionalRecorder	500

BLOGS AND PUBLICATIONS

- Check Point Research Publications
- Global Cyber Attack Reports
- Threat Research

February 17, 2020

“The Turkish Rat” Evolved Adwind in a Massive Ongoing Phishing Campaign

---