More Than 1 Million Google Accounts Breached by Gooligan

By bferrite

Published: 2016-11-30 · Archived: 2026-04-13 02:06:08 UTC

As a result of a lot of hard work done by our security research teams, we revealed today a new and alarming malware campaign. The attack campaign, named Gooligan, breached the security of over one million Google accounts. The number continues to rise at an additional 13,000 breached devices each day.

Our research exposes how the malware roots infected devices and steals authentication tokens that can be used to access data from Google Play, Gmail, Google Photos, Google Docs, G Suite, Google Drive, and more.

Gooligan is a new variant of the Android malware campaign found by our researchers in the SnapPea app last year.

Check Point reached out to the Google Security team immediately with information on this campaign. Our researchers are working closely with Google to investigate the source of the Gooligan campaign.

"We're appreciative of both Check Point's research and their partnership as we've worked together to understand these issues," said Adrian Ludwig, Google's director of Android security. "As part of our ongoing efforts to protect users from the Ghost Push family of malware, we've taken numerous steps to protect our users and improve the security of the Android ecosystem overall."

> Click here to read Adrian Ludwig's complete statement on Gooligan.

We are very encouraged by the statement Google shared with us addressing the issue. We have chosen to join forces to continue the investigation around Gooligan. Google also stated that they are taking numerous steps including proactively notifying affected accounts, revoking affected tokens and deploying SafetyNet improvements to protect users from these apps in the future.

In the following sections, we provide more answers regarding the campaign.

Who is affected?

Gooligan potentially affects devices on Android 4 (Jelly Bean, KitKat) and 5 (Lollipop), which is over 74% of in-market devices today. About 57% of these devices are located in Asia and about 9% are in Europe.

In our research we identified tens of fake applications that were infected with this malware. If you've downloaded one of the apps listed in Appendix A, below, you might be infected. You may review your application list in "Settings -> Apps", if you find one of this applications, please consider downloading an antivirus product such as Check Point ZoneAlarm to check if you are indeed infected.

We have noticed that hundreds of the email addresses are associated with enterprise accounts worldwide.

How do you know if your Google account is breached?

You can check if your account is compromised by accessing the following web site that we created: https://gooligan.checkpoint.com/.

If your account has been breached, the following steps are required:

1. A clean installation of an operating system on your mobile device is required (a process called “flashing”). As this is a complex process, we recommend powering off your device and approaching a certified technician, or your mobile service provider, to request that your device be “re-flashed.”
2. Change your Google account passwords immediately after this process.

How do Android devices become infected?

We found traces of the Gooligan malware code in dozens of legitimate-looking apps on third-party Android app stores. These stores are an attractive alternative to Google Play because many of their apps are free, or offer free versions of paid apps. However, the security of these stores and the apps they sell aren’t always verified. Gooligan-infected apps can also be installed using phishing scams where attackers broadcast links to infected apps to unsuspecting users via SMS or other messaging services.

How did Gooligan emerge?

Our researchers first encountered Gooligan’s code in the malicious SnapPea app last year. At the time this malware was reported by several security vendors, and attributed to different malware families like Ghostpush, MonkeyTest, and Xinyinhe. By late 2015, the malware’s creators had gone mostly silent until the summer of 2016 when the malware reappeared with a more complex architecture that injects malicious code into Android system processes.

The change in the way the malware works today may be to help finance the campaign through fraudulent ad activity. The malware simulates clicks on app advertisements provided by legitimate ad networks and forces the app to install on a device. An attacker is paid by the network when one of these apps is installed successfully.

Logs collected by Check Point researchers show that every day Gooligan installs at least 30,000 apps fraudulently on breached devices or over 2 million apps since the campaign began.

How does Gooligan work?

The infection begins when a user downloads and installs a Gooligan-infected app on a vulnerable Android device. Our research team has found infected apps on third-party app stores, but they could also be downloaded by Android users directly by tapping malicious links in phishing attack messages. After an infected app is installed, it sends data about the device to the campaign’s Command and Control (C&C) server.

Gooligan then downloads a rootkit from the C&C server that takes advantage of multiple Android 4 and 5 exploits including the well-known VROOT (CVE-2013-6282) and Towelroot (CVE-2014-3153). These exploits still plague many devices today because security patches that fix them may not be available for some versions of

Android, or the patches were never installed by the user. If rooting is successful, the attacker has full control of the device and can execute privileged commands remotely.

After achieving root access, Gooligan downloads a new, malicious module from the C&C server and installs it on the infected device. This module injects code into running Google Play or GMS (Google Mobile Services) to mimic user behavior so Gooligan can avoid detection, a technique first seen with the mobile malware *HummingBad*. The module allows Gooligan to:

- Steal a user's Google email account and authentication token information
- Install apps from Google Play and rate them to raise their reputation
- Install adware to generate revenue

Ad servers, which don't know whether an app using its service is malicious or not, send Gooligan the names of the apps to download from Google Play. After an app is installed, the ad service pays the attacker. Then the malware leaves a positive review and a high rating on Google Play using content it receives from the C&C server.

Our research team was able to identify several instances of this activity by cross-referencing data from breached devices with Google Play app reviews. This is another reminder of why users shouldn't rely on ratings alone to decide whether to trust an app.

Two examples of reviews left by users who were also found on the attacker's records as victims.

An example of fake reviews and comments to one of the fraudulent applications.

The same user discovered two different fraudulent apps were installed on his device, without his knowledge.

Similar to HummingBad, the malware also fakes device identification information, such as IMEI and IMSI, to download an app twice while seeming like the installation is happening on a different device, thereby doubling the potential revenue.

One of the apps downloaded from Google Play by Gooligan.

What are Google authorization tokens?

A Google authorization token is a way to access the Google account and the related services of a user. It is issued by Google once a user successfully logged into this account.

When an authorization token is stolen by a hacker, they can use this token to access all the Google services related to the user, including Google Play, Gmail, Google Docs, Google Drive, and Google Photos.

While Google implemented multiple mechanisms, like two-factor-authentication, to prevent hackers from compromising Google accounts, a stolen authorization token bypasses this mechanism and allows hackers the desired access as the user is perceived as already logged in.

Conclusion

Gooligan has breached over a million Google accounts. We believe that it is the largest Google account breach to date, and we are working with Google to continue the investigation. We encourage Android users to validate whether their accounts have been breached.

Appendix A: List of fake apps infected by Gooligan

- Perfect Cleaner
- Demo
- WiFi Enhancer
- Snake
- gla.pev.zvh
- Html5 Games
- Demm
- memory booster
- แข่งรถสุดโหด
- StopWatch
- Clear
- ballSmove_004
- Flashlight Free
- memory booste
- Touch Beauty
- Demoad
- Small Blue Point
- Battery Monitor
- 清理大师
- UC Mini
- Shadow Crush
- Sex Photo
- 小白点
- tub.ajy.ics
- Hip Good
- Memory Booster
- phone booster
- SettingService
- Wifi Master
- Fruit Slots
- System Booster
- Dircet Browser
- FUNNY DROPS
- Puzzle Bubble-Pet Paradise
- GPS
- Light Browser
- Clean Master

- YouTube Downloader
- KXService
- Best Wallpapers
- Smart Touch
- Light Advanced
- SmartFolder
- youtubeplayer
- Beautiful Alarm
- PronClub
- Detecting instrument
- Calculator
- GPS Speed
- Fast Cleaner
- Blue Point
- CakeSweety
- Pedometer
- Compass Lite
- Fingerprint unlock
- PornClub
- com.browser.provider
- Assistive Touch
- Sex Cademy
- OneKeyLock
- Wifi Speed Pro
- Minibooster
- com.so.itouch
- com.fabullacop.loudcallernameringtone
- Kiss Browser
- Weather
- Chrono Marker
- Slots Mania
- Multifunction Flashlight
- So Hot
- Google
- HotH5Games
- Swamm Browser
- Billiards
- TcashDemo
- Sexy hot wallpaper
- Wifi Accelerate
- Simple Calculator
- Daily Racing

- Talking Tom 3
- com.example.ddeo
- Test
- Hot Photo
- QPlay
- Virtual
- Music Cloud

Source: http://blog.checkpoint.com/2016/11/30/1-million-google-accounts-breached-gooligan/