Advanced Notification of Malware Campaign - Gooligan

Security Advisory AE-Advisory 16-045

Criticality High

Advisory Released On 5 December 2016

Impact

- Control of infected device without user's permission and rate apps on their behalf.
- Attempt to steal information to gain access to the user's sensitive data from Gmail, Google Photos, Google Docs, Google Play, Google Drive and G Suite.

Solution

Refer to the "Solution" section below

Affected Group

- Android 4 (Jelly Bean, KitKat)
- Android 5 (Lollipop)

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found out about a new malware campaign called Gooligan. "Gooligan" is a malware that has affected Android phone users, compromising over a million Google accounts. It disguises itself as a legitimate Android app to trick users into installing the app, which then infects the phone. It then installs unwanted apps on the phone which cannot be easily removed, even if a factory reset is done. Further information is explained in the "Threat Details" section below.

Threat Details

The phone is infected when a user downloads and installs a Gooligan-infected app on a vulnerable Android device or when the user clicks on malicious links in phishing messages. After the installation of the app, it sends data about the devices to the campaign's Command and Control (C&C) server. It then downloads a rootkit from the C&C server that uses multiple Android 4 and 5 exploits including the well-known VROOT and Towelroot exploits. Unfortunately, these exploits still exist on many Android devices because there are not security fixes for them or because the user does not install them. If the attempt of the malware to root the Android device is successful, the attacker will have full control of the device and can execute privileged commands remotely.

Once Gooligan achieves root access, it downloads a new, malicious module from the C&C server and installs it on the infected Android device. This module then injects code into running Google Play or GMS (Google Mobile Services) to mimic the user's behavior so that it can avoid detection. This technique allows Gooligan to do the following:

- 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 revenu

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. Below are screenshots proving what has been said:

Please refer to the list of fake apps below that are infected with 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

Solution

Checkpoint has offered a website service where a user can enter with their Android device https://gooligan.checkpoint.com/ and check whether their device is infected with Gooligan or not.

If your account has been breached, follow these steps:

1. Do a clean installation of an operating system on your mobile device is required (a process called “flashing”).
2. Change your Google account passwords immediately after this process.

Firmware re-flashing involves performing a clean installation of the operating system on the mobile device. As the process can be complicated for some users, it is recommended that affected users seek help from a certified technician or phone manufacturer to have the phone’s firmware re-flashed.

Re-flashing the firmware will wipe out all your data, therefore it is recommended that you back up important information such as contacts, SMS messages, chats and images before performing a firmware re-flash. The steps are as follows:

1. Back up all important information such as contacts, SMS messages, chats and images to your computer or an external device
2. Bring your phone to the service centre and request for the firmware to be flashed. **Note:** This may incur a cost.
3. Sign out of all synchronized accounts (Gmail, Yahoo, Hotmail, Facebook, etc) in the phone
4. Repeat Step 3 for all other devices for which these accounts are synchronised to
5. Using a clean computer or phone, log in to each of the accounts and change the respective passwords. Enable 2-factor authentication (2FA) where possible
6. Log back in to your account after the passwords have been changed

Prevention

- Only download and install apps from reputable app stores
- Use an antivirus/antimalware scanner to scan app before installing
- Do not click on suspicious links, web pages or advertisements

References

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

https://gooligan.checkpoint.com/

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel (+971) 4 230 0003
Fax (+971) 4 230 0100
Email info[at]aeCERT.ae

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae