COMPUTER SECURITY BULLETIN

Risk/Impact Rating: SERIOUS

< GOOLIGAN >

CSB17-003

Description:

Gooligan malware

- Breached the security of 1 million Google accounts
- Compromise about ***74 percent of Android devices*** (Android 4.2 Jellybean, Android 4.4 Kitkat and Android 5.0 Lollipop)
- Found in at least 86 applications at third-party app stores.
- Force users into downloading apps as part of a huge advertising fraud scheme, making as much as $320,000 a month.
- Gains a foothold on devices when users visit a website and download a third-party app (porn site, or a third-party app store)
- Once downloaded, it determines which Android phone it's infected and launches the appropriate exploits to "root" the device
- Once it has control of the phone, the victim's Google account token is siphoned off to a remote server and could be used to gain access to their Gmail, Docs, Drive, Photos and other data, even where two-factor authentication is turned on.

To prevent the Gooligan virus from affecting your android devices:

- Avoid installing a third-party app markets
- Disable the "Allow Unknown Source Installation" in the Settings of your devices

If your phone is infected:

- Back up data;
- Delete everything on the device; and
- Do a factory reset.

References:

https://www.rt.com/usa/368751-android-malware-gooligan-ghost-push/

http://www.forbes.com/sites/thomasbrewster/2016/11/30/gooligan-android-malware-1m-google-account-breaches-check-point-finds/#63bf5695470d

http://www.digitaltrends.com/mobile/android-gooligan/

https://www.xda-developers.com/gooligan-malware-compromises-more-than-a-million-google-accounts-on-android/

http://www.gamenguide.com/articles/80028/20161202/heres-how-to-prevent-gooligan-virus-in-infecting-your-android-phone.htm

http://www.latimes.com/business/technology/la-fi-gooligan-virus-20161208-story.html

http://www.sci-tech-today.com/news/Keep-Gooligan-Off-Android-Phones/story.xhtml?story_id=023002T7X6RW