Gooligan: The next generation of the Ghost Push family of malware

Nokia Threat Intelligence Labs

December 2016

The Gooligan attack breached the security of over one million Google accounts. Gooligan potentially affects devices on Android 4 (Jelly Bean, KitKat) and 5 (Lollipop), which is over 74 percent of in-market devices today. About 57 percent of these devices are located in Asia, and about 9 percent in Europe. The Nokia Threat Intelligence Center associated with Nokia’s NetGuard Endpoint Security solution has been detecting the various strains of the Ghost Push malware family. In recent months, there has been a major spike in activity associated with both downloads and general command and control communications.
What is Gooligan?

Gooligan is a type of Android malware (malicious application). It is the new name for one of the longest running family of Android malwares in existence, Ghost Push. More recent names or aliases for Ghost Push include ‘SnapPea’, ‘Qysly’ and ‘GingerMaster’. The Gooligan variant is believed to be delivered by phishing schemes offering free versions of paid apps, via third party app stores or downloads. Vulnerable devices include phones running both Android 4 and 5 (including Jelly Bean, KitKat and Lollipop).

What harm does it do?

After the malware is successfully installed on the phone, Gooligan will start to install additional apps without the user’s permission. These apps include adware and other apps from the Google Play store. The malware will then rate these apps in an attempt to improve their reputation; driving sales and increasing revenue for these apps. Gooligan will then proceed to collect email account and authentication token information from the phone - providing access to the Google Suite of tools include Gmail, Photos, Google Drive, etc.

Why do we think this was a phishing attack?

Nokia's NetGuard Endpoint Security has been detecting the various strains of the Ghost Push malware family for quite a while now. In recent months there has been a major spike in activity associated with both downloads and general command and control communications for the various Ghost Push variants. Spikes like this are not typical without the added influence of things like well-planned phishing campaigns. The following graphs illustrate activity around the most recent Gooligan events.
Additional Ghost Push communications, where device information is being sent to Command and Control Servers, can be seen and correlated by the following graph.
Where has my data been going?

There are a few destinations that can be associated with the Ghost Push malware. Although domains tend to change from time to time, the destinations remain quite constant. These destinations (IOC) include but are not limited to:

<table>
<thead>
<tr>
<th>Domains</th>
<th>Destinations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ddonqfq.com</td>
<td>139.162.59.172; 139.162.63.212</td>
</tr>
<tr>
<td>Appso.net</td>
<td>52.74.198.242; 52.76.67.42</td>
</tr>
</tbody>
</table>

These destinations are mostly owned by various web hosting companies and therefore cannot easily be tied to a specific entity. These destinations have a very poor reputation as can be seen in the associated Virus Total reports.

How do I know if I’m infected?

CheckPoint have provided a WebApp that can verify whether a device has been affected, in case an email address was associated with the Android phone. Visit: https://gooligan.checkpoint.com/ to check your device.

What can I do if my Android phone is infected?

Unfortunately, the only way to remove Gooligan from an infected phone is to perform a “wipe and clean”. You should remove all data from your phone and reinstall the operating system. This task can be complicated for most users so we suggest visiting your mobile carrier for assistance with this process. The next recommended step is to change your Google account password immediately. If part of your private data included other personal data, credentials or access details, your other accounts may be at risk. Consider changing those passwords immediately as well.