Cybersecurity Blog

Everything about threat intelligence, blue team, red team, pentesting, security audit, security review, testing and assessment.

Friday, September 16, 2016

Xiaomi's Analytics Application Security & Privacy Concern

You might have heard about the recent blogspot of Reverse Engineering Xiaomi's Analytics app at https://www.thijsbroenink.com/2016/09/xiaomis-analytics-app-reverse-engineered/ Summary - Basically there is an application called Analystics which is there by default on every MIUI user's phone. This application runs in background 24*7 and it also re appears without user interaction even if you delete it.

Xiaomi is one of the world's largest smartphone manufacturers, which has previously been criticized for spreading malware, shipping handsets with pre-loaded spyware/adware and forked version of Android OS, and secretly stealing users' data from the device without their permission.

Few readings for the same are referenced below:

1. http://thehackernews.com/2014/10/xiaomi-data-breach-hacker.html
2. http://thehackernews.com/2015/03/Xiaomi-Mi-4-malware.html
3. http://thehackernews.com/2014/08/xiaomi-phones-secretly-sending-users.html

Technical Summary:

Detailed technical specifications are provided on original researcher's blog at https://www.thijsbroenink.com/2016/09/xiaomis-analytics-app-reverse-engineered/

I am going to provide simplified technical summary.

Why it looks fishy?

There are couple of reasons for the same.

- Application runs 24*7 in background.
- It reappears after a while even after you delete it.
- It continuously checks for the new version of Analytics application on server.
- While making requests to the server it sendsIMEI, MAC address, Model, Nonce, Package name and signature to the server.
- If new version on server is available it gets downloaded **without user interaction**.
- Phone or user does not verifies new application installation and this is whole done via HTTP protocol.

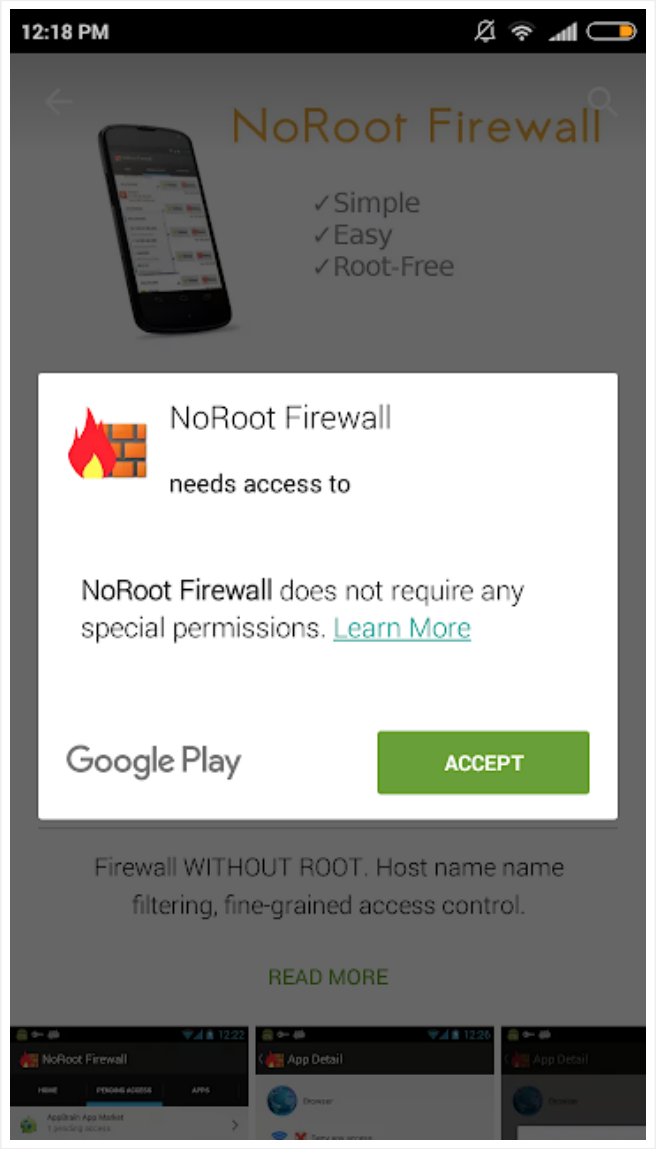
This all suggests that, any MiTM attacker can spoof his/her application name with Analytics.apk application and can install in your phone without user consent which is a security implication as well as privacy issue.

What Xiaomi says about this?
As of now there is no official sayings from them. We may listen in future.

Is there any workaround fix?
Yes. You can install NoRoot firewall application which does not ask for any permission. However, it will monitor your network traffic. So if you do trust this application which has 4.4 rating with 1 million download, then you are good to go :) .

Below picture shows it does not ask for any permission.

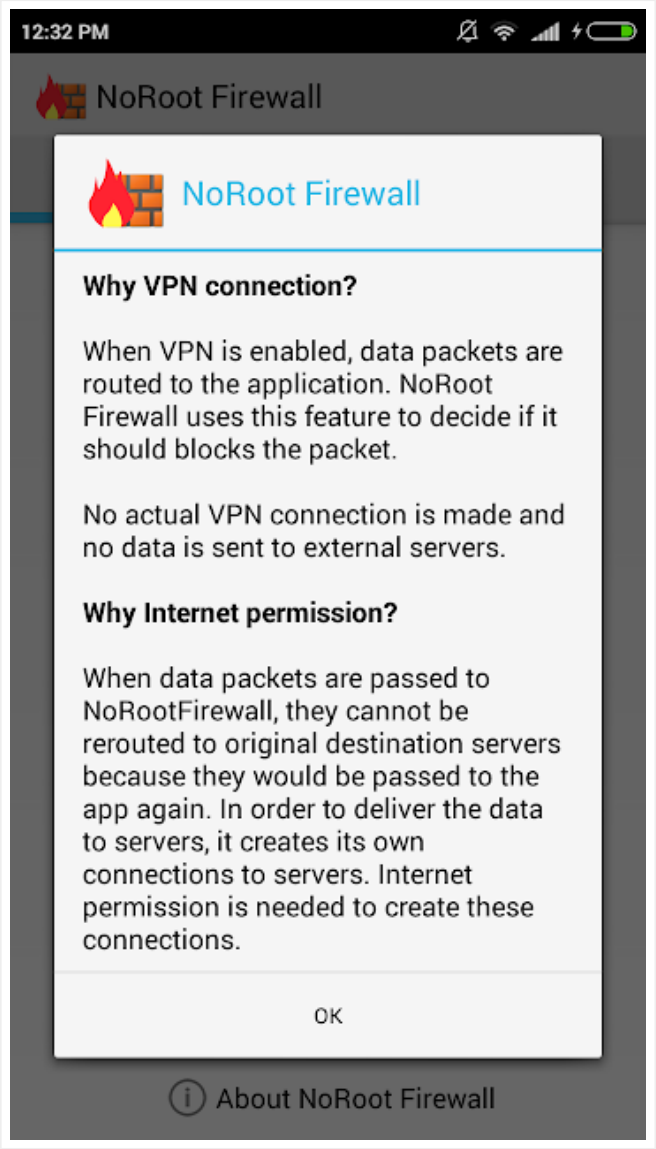
► May 1 (1)
► April 10 (1)
► April 3 (2)
► 2015 (4)
► 2014 (22)
► 2013 (58)



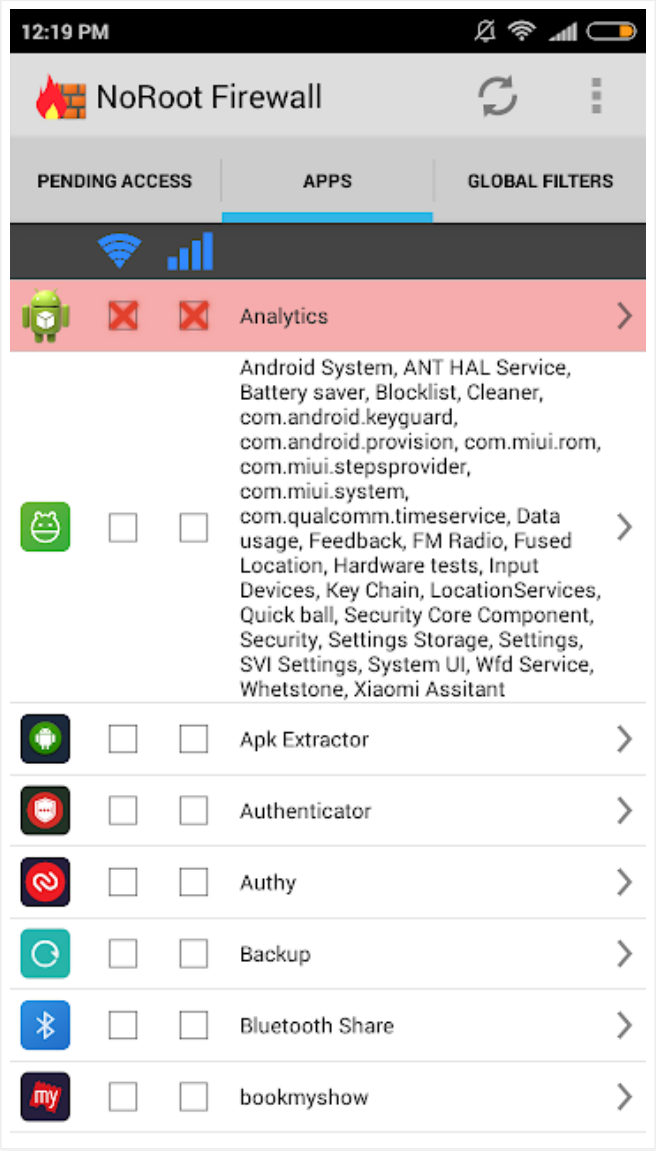
Start firewall post installation of the application.

It may ask you to accept that it will monitor your network connections. (Better you stop firewall or remove application while you are signing into any application even though you are on SSL.)

If you are wondering why VPN? then here is the reason.



Now navigate to the apps tab and double tab on checkbox in order to disable application to from making any external server connection.



Additionally you can block all Xiaomi domains through Adaway application. However it requires rooted device.

Domains to block within AdAway are as follows:

This hosts file contains exported entries from AdAway.
127.0.0.1 micloud.xiaomi.net
127.0.0.1 xiaomi.net
127.0.0.1 account.xiaomi.com
127.0.0.1 pdc.micloud.xiaomi.net
127.0.0.1 wifiapi.micloud.xiaomi.net

127.0.0.1 xiaomi.com
127.0.0.1 contactapi.micloud.xiaomi.net

References:

1. https://www.thijsbroenink.com/2016/09/xiaomis-analytics-app-reverse-engineered/
2. http://thehackernews.com/2016/09/xiaomi-android-backdoor.html

Posted by Frogy at 9/16/2016

Labels: android, application security, backdoor, firewall, mobile firewall, mobile security, Xiaomi

No comments:

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)