PRIVACYSENTRY
THREATREPORT

September 7, 2015

LEO Privacy Guard

How We Found LEO Privacy Guard

While evaluating applications in the mobile privacy space, we started getting alerts from SpyAware that one of the apps we were evaluating was making connections back to Singapore and China. It raised our curiosity enough to take a deeper look.

We fired up LEO Privacy Guard with some of our deep analysis tools. It can be very tricky to find and isolate where and when private data is being leaked. However, after just a couple minutes of analysis with LEO Privacy Guard, here's what we found.

Device Data Sent by LEO Privacy Guard

```
POSTed Device Data
POST /appmaster/release HTTP/1.1
device: “0001a” “d3b**********************b6d” “appmaster” “2.5”
“KTU8**********NJ4” “4.4.4” “samsung” “SAMSUNG-SGH-I337” “1920x1080”
“480” “en” “GMT-08:00” “356********918” “310*********061”
“40:**:**:**:**:3E” “9c3*********713”
Content-Length: 19
Content-Type: text/plain; charset=ISO-8859-1
Host: api.leomaster.com
Connection: Keep-Alive
User-Agent: Apache-HttpClient/UNAVAILABLE (java 1.4)
check-update-params
HTTP/1.1 200 OK
Server: nginx/1.6.2
Date: Fri, 31 Jul 2015 21:29:14 GMT
Content-Type: text/html;          =utf-8
Content-Length: 131
```

So right off the bat, LEO is sending almost every unique identifier available from my device, over an unencrypted connection, back to a server in Singapore.

What Data is LEO Privacy Guard Taking From Me?

Here are the pieces of data we have isolated so far from the sample above:

IMEI (International Mobile Equipment Identity)

The IMEI is a unique identifier for your phone.

In the posted device data above, the example data reads: “356*********918”

IMSI (International mobile subscriber identity)

The IMSI is a unique identifier which identifies you to your mobile service provider’s network.

In the posted device data above, the example data reads: “310*********061”

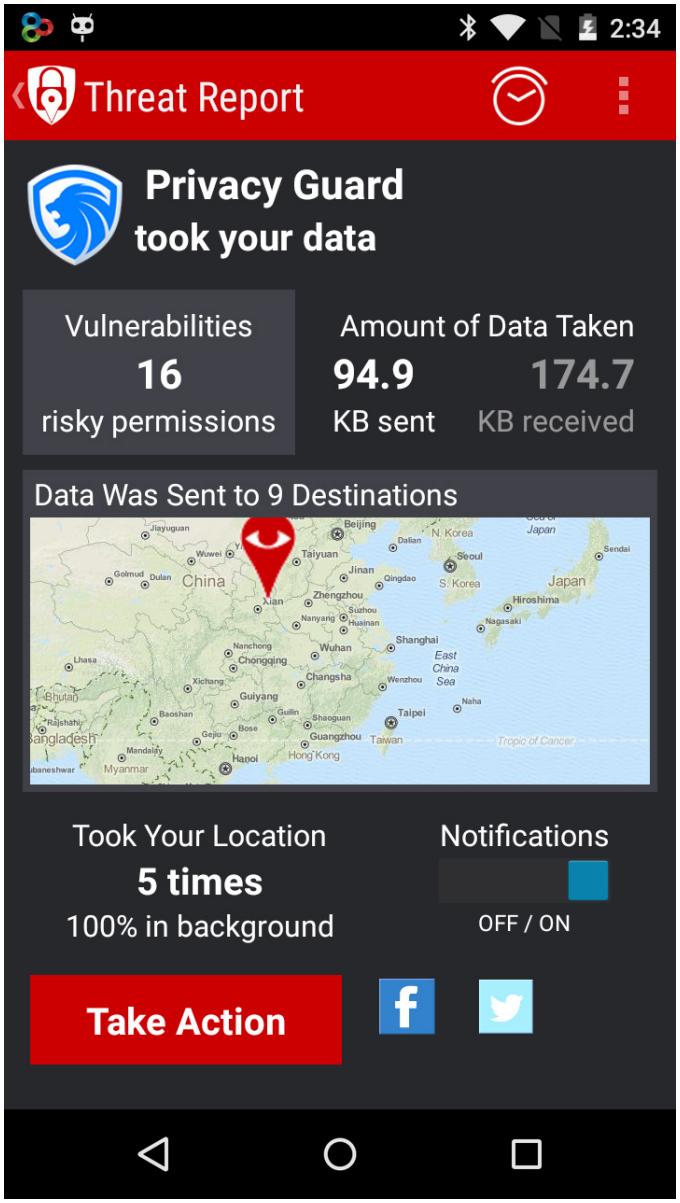
ICCID

The ICCID is the serial number/unique identifier for the SIM card itself.

In the posted device data above, the example data reads: “KTU8***********NJ4”

Wifi MAC Address

The MAC address is the unique identifier for a network device.



Screen Capture from SpyAware Showing Data taken and received, including location taken.

In the posted device data above, the example data reads: “40:**:**:**:**:3E”

Android.DEVICE_ID

This is a 16 character unique device identifier which can be used to identify which device made an app purchase.

In the posted device data above, the example data reads: “9c3**********713”

Device Make & Model Info

While this is not a direct export of private data, the make and model of your device can help an attacker identify known vulnerabilities & attack surfaces to exploit your device.

In the posted device data above, the example data reads: “4.4.4” “samsung” “SAMSUNG-SGH-I337”

Why Is This Bad?

Using IMEI to Blacklist or Impersonate a Device

1. Some hackers are interested in only the short-term play: changing the number of a stolen device to one that is not blacklisted, but the there is a strong long-term possibility of building inventories of these numbers to be re-sold to criminals attempting to bypass prepaid SIM card restrictions, thereby getting free cell service. [1]

2. Your IMEI is vitally important information. If a thief gets it, they can mark your phone lost or stolen and make your phone stop working, entirely. Then, they can switch it to their own account, which is often a fake identity, and make an claim for it being lost. You should never give out your IMEI unless you know you are on the phone with legitimate customer service. [2]

3. You can think of it as an equivalent to a MAC address on a network. The IMEI can be spoofed to impersonate you and your phone. Your phone service provider traces your IMEI in order to maintain your phone connection, so your phone could be tracked by criminals in the same way. The IMEI is also used to find stolen phones, by comparing it to the IMEI database of stolen phones maintained by the GSM Alliance, for example.

So, to protect your identity, and limit tracing to legitimate usages, it is extremely important to not spread the IMEI out in public. Why does Leo Privacy Guard need to collect and store such sensitive data? If their database was ever breached by hackers, any phone that has had Leo installed on it could be at risk. [3]

Using IMSI and ICCID to Duplicate a SIM Card

The IMSI and ICCID are the unique identifiers for the SIM account holder and physical SIM card, respectively. Using this information, hackers can use freely available tools and devices to clone your SIM, thereby using up your phone minutes for their own calls.[4]

1. http://www.zdnet.com/article/scammers-phishing-for-sensitive-iphone-data/
2. http://forum.xda-developers.com/showthread.php?t=2277733
3. http://security.stackexchange.com/questions/71794/why-do-i-need-to-hide-my-phones-imei
4. http://www.thehackerstore.net/2014/04/sim-card-cloning-make-duplicate-mobile.html

Spoofing MAC Address to Gain Access to White-Listed Resources

Some corporate networks use the MAC address of phones to decide which phones to allow connections from. By programming their phone to use your MAC address (spoofing), they could gain access to sensitive corporate data. While this kind of exploit usually requires that the attacker has access to the WIFI network, it's very easy to spoof a mac address.

User Location Taken

SpyAware has detected that Leo Privacy Guard also takes the user's location. Given the amount of data sent, there is a chance that it is also being sent to the remote server, but we can't say conclusively at this time. We are doing further research on this.

Unencrypted Transmission

As the icing on the cake, all of this data is being sent over an unencrypted connection. This means that it is in a very human, readable form. Not only is LEO Privacy Guard harvesting this information, they are also making it very easy for anyone with physical network access to easily harvest this information themselves.

The Power of Correlation

Each of these pieces of information presents a privacy risk in its own right, but put all together, this is nearly every piece of information that would be required to spoof a device and it's user. It's tantamount to posting up someone's full name, address, phone number, birthday, social security number and mother's maiden name in unencrypted text to a company's private database. Each piece of information on it's own is very low risk, but all together, it's everything an identity thief would need to steal someone's identity and start opening up credit accounts.

When this data is combined with information available to many data brokers, such as your phone's physical location, it means that they have a startlingly clear picture of you, your habits, and so on.

Beyond Reach

All of the data that Leo gathers is passed to servers in Singapore and China. This means that your identifying information is being held by the company that is under the laws of these respective countries. For those of you already living under that law, that is to be expected. However, many people around the world might be shocked to discover that if law enforcement or these governments required access to this data, they would be forced to provide it.

Why does Leo need this information?

We have reached out to Leo Privacy Guard's corporate leadership to ask:

- Why does your app collect this information?
- Why does it send this information to remote servers?
- Why does it do so unencrypted (in the clear)?

We have not received a reply as of the date of publication of this paper.