KRYPTOWIRE DISCOVERED MOBILE PHONE FIRMWARE THAT TRANSMITED PERSONALLY IDENTIFIABLE INFORMATION (PII) WITHOUT USER CONSENT OR DISCLOSURE

Tuesday November 15, 2016

Kryptowire has identified several models of Android mobile devices that contained firmware that collected sensitive personal data about their users and transmitted this sensitive data to third-party servers without disclosure or the users' consent. These devices were available through major US-based online retailers (Amazon, BestBuy, for example) and included popular smartphones such as the BLU R1 HD. These devices actively transmitted user and device information including the full-body of text messages, contact lists, call history with full telephone numbers, unique device identifiers including the International Mobile Subscriber Identity (IMSI) and the International Mobile Equipment Identity (IMEI). The firmware could target specific users and text messages matching remotely defined keywords. The firmware also collected and transmitted information about the use of applications installed on the monitored device, bypassed the Android permission model, executed remote commands with escalated (system) privileges, and was able to remotely reprogram the devices.

The firmware that shipped with the mobile devices and subsequent updates allowed for the remote installation of applications without the users' consent and, in some versions of the software, the transmission of fine-grained device location information. The core of the monitoring activities took place using a commercial Firmware Over The Air (FOTA) update software system that was shipped with the Android devices we tested and were managed by a company named Shanghai Adups Technology Co. Ltd.

Our findings are based on both code and network analysis of the firmware. The user and device information was collected automatically and transmitted periodically without the users' consent or knowledge. The collected information was encrypted with multiple layers of encryption and then transmitted over secure web protocols to a server located in Shanghai. This software and behavior bypasses the detection of mobile anti-virus tools because they assume that software that ships with the device is not malware and thus, it is white-listed.

In September 2016, Adups claimed on its web site to have a world-wide presence with over 700 million active users, and a market share exceeding 70% across over 150 countries and regions with offices in Shanghai, Shenzhen, Beijing, Tokyo, New Delhi, and Miami. The Adups web site also stated that it produces firmware that is integrated in more than 400 leading mobile operators, semiconductor vendors, and device manufacturers spanning from wearable and mobile devices to cars and televisions.

CAPABILITIES	Carrier IQ (2011)	ADUPS
SMS Recording	✔ * Partial as part of debug logs	✔
SMS Transmission	✔ * Partial to the carrier as part of debug logs	✔
IMEI Exfiltration	✔	✔
IMSI	✔	✔
Call Log Transmission	✔ * Partial as part of debug logs	✔
Call Contact Information Transmission	✔ * Partial as part of debug logs	✔
Location Collection & Transmission	✔	✔
Command Injection	✔	✔
Remote User App. Update	✖	✔
Remote User App. Install	✖	✔
Transmit List of installed Applications	✖	✔
Transmit order of application execution	✖ * Event information as part of the call process	✔
Programmatic Firmware Update	✖	✔
Remote Execution & Privilege Escalation	✖	✔ * This enables execution of remote code without permission and user consent
IP Address	✔	✔
Name	N/A	✔ *For contacts
Email Address	✔	✖
Key logging	✔ * Partial to the carrier as part of debug logs	✖

Figure 1: Comparison of Adups with 2011 CarrierIQ capabilities based on publicly available sources.

In Figure 1, we compare our findings with the data collection capabilities of Carrier IQ's software in November of 2011 that offered a comprehensive suite of analytics for wireless network and device performance. The CarrierIQ case created a lot of public debate and was the subject of an investigation by the FTC and other government agencies.[1]

We analyzed the Personally Identifiable Information (PII) collected and transmitted in an encrypted format to servers in Shanghai including one of the bestselling unlocked smartphones sold by major online retailers.

Moreover, some transmitted the body of the user's text messages and call logs to a server in located in Shanghai. All of the data collection and transmission capabilities we identified were supported by two system applications that cannot be disabled by the end user. These system applications have the following package names:

- com.adups.fota.sysoper
- com.adups.fota

The data collection and transmission capability is spread across different applications and files. The data transmission occurred every 72 hours for text messages and call log information, and every 24 hours for other PII data. The information was transmitted to the following back-end server domains:

1. **bigdata.adups.com (primary)**
2. bigdata.adsunflower.com
3. bigdata.adfuture.cn
4. bigdata.advmob.cn

All of the above domains resolved to a common IP address: 221.228.214.101 that belongs to the Adups company. During our analysis, bigdata.adups.com was the domain that received the majority of the information whereas rebootv5.adsunflower.com with IP address: 61.160.47.15 was the domain that can issue remote commands with elevated privileges to the mobile devices.

---

[1] Understanding Carrier IQ Technology - What Carrier IQ Does and Does Not Do - December 12th 2011 - http://www.franken.senate.gov/files/letter/111212_CarrierIQ_Attachment.pdf

Before the data transmission occurs the device checks in with a remote server using a REST API and is instructed on what to collect. It is worth noting that the REST endpoint differs for various phone manufacturers and even phone models. Below is an example of a check-in response:


```
{
   "json": {
      "keys": [{
         "given": "0",
         "keyword": "",
         "type": "1"
      }],
      "poll_cycle": "24"
   },
   "md5": " B865B089A298D529B4602A3D359FE4C8"
}
```


We have identified two important elements in the server's response: the "given" and "keyword" elements. Our analysis leads to the understanding that the "given" keyword could be used to identify messages from a specific phone number, while "keyword" could be used to retrieve messages containing a specific keyword. In the example above this server's response is set to transmit all the text messages on the device. The data transmission occurs using encrypted web protocol over a REST API. Figure 2. below is lists the files that were uploaded to bigdata.adups.com during our analysis:

Files	Description
DcApp.json	App's that the user has installed on the device.
DcAppOp.json	Android App Ops data
DcMobileStatus.json	Diagnostic data
DcRootInfo.json	A listing of files in the /system/bin and /system/xbin directories
DcTellMessage.json	The user's call log (and numbers people the user has texted)
dc_app_flow.json	The order in which a user uses apps
dc_msg_key.json	The content of the user's text messages

Figure 2. List of files uploaded to bigdata.adups.com during our analysis.

It is worth noting that user's text messages are encrypted using DES. Below is an example entry of the dc_msg_key.json file:


```
{
    "dc_date": "2016-09-13 17:01:07",
    "dc_type": "1",
    "keyword": "HUnrP/GTiH/aEPM8bVXmaw\u003d\u003d",
    "md5": "B865B089A298D529B4602A3D359FE4C8",
    "msg_date": "1473798497903",
    "msg_type": "1",
    "tell": "+1540XXXXXXX"
}
```


During our analysis we identified the necessary key to encrypt and decrypt these messages. The aforementioned entry in plaintext is: "Be there in 5"

As smartphones are ubiquitous and, in many cases, a business necessity, our findings underscore the need for more transparency at every stage of the supply chain and increased consumer awareness. Kryptowire has developed tools aimed at detecting non-compliant software that can violate privacy and security policies that are not necessarily classified as malware. In many cases, these applications are benign, but exhibit behavior non-compliant with organizational, industry, and government policies.

Kryptowire has communicated its findings with respect to the affected devices with Google, Amazon, and BLU Products, Inc.

Manufacturers that believe their devices may be affected can contact oem@kryptowire.com for additional information.

Consumers that believe their devices may be affected can refer to the manufacturer warranty or retailer terms of purchase for further instructions.

About Kryptowire

Kryptowire was jumpstarted by the Defense Advanced Research Projects Agency (DARPA) and the Department of Homeland Security (DHS). Kryptowire provides mobile application security analysis tools, anti-piracy technologies, mobile app marketplace security analytics, and Enterprise Mobility Management (EMM) solutions. Kryptowire was founded in 2011, is based in Fairfax, Virginia, and has a customer base ranging from government agencies to national cable TV companies.