

Elect 2012 Program Reverse Engineering Project

Saleh Alsanad

Computer Engineer

and

Abdulaziz Alazmi

Computer Engineer

Kuwait

January 17, 2012

Abstract

This report is a demonstration of what we have found in Elect 2012¹ iPhone application. We heard a lot about the privacy violation that this program committed and decided to take a look at it and write a report for IT guys (and maybe law guys) to look at.

Introduction

Active Media company did a great job at providing us with an iPhone application² that provides us with all news and information we need for elections of 2012 national assembly in Kuwait. But, Active Media did a very big mistake here. The application provides the information of people (Area, Job, Circle, Nationality number and Full name) just by providing part of the full name. That is a great violation of people's privacy. Plus, The information transfers non-securely to the application.

Setup and start working

I have setup my machines so that I can capture the packets that Elect 2012 application sends and got shocked that the application didn't use any kind of security. The application sends a normal GET request to a server called q8forlife.com. A 'whois' request gives me this output:

Registrant:

Waleed Abubaker
Kuwait
KUWAIT CITY, 13115
Kuwait

Registered through: Mad Dog Domains

Domain Name: Q8FORLIFE.COM
Created on: 09-Jun-09
Expires on: 09-Jun-12
Last Updated on: 21-Dec-11

Administrative Contact:

Abubaker, Waleed w_ab@msn.com
edit – Kuwait
Hawalli - block 12 - street 138
building 36 -Apartment 29
Hawalli, Hawalli 30233
Kuwait
(965) 65501648 Fax --

Technical Contact:

Abubaker, Waleed w_ab@msn.com
edit – Kuwait
Hawalli - block 12 - street 138
building 36 -Apartment 29
Hawalli, Hawalli 30233
Kuwait
(965) 65501648 Fax --

1 The real application name is in Arabic 'انتخب 2012' but I'll use Elect 2012 through out this report

2 <http://itunes.apple.com/us/app/id492499102>

Domain servers in listed order:
NS1.Q8FORLIFE.COM
NS2.Q8FORLIFE.COM

So, this server is registered by Waleed Abubaker who is the author of the Elect2012 program. I'm not sure of the relationship between him and Active Media company. Plus, the given address in the 'whois' request is probably the address of the company itself. Entering the the site hosted at q8forlife.com gives:



The screenshot shows a Chromium browser window with the address bar displaying 'q8forlife.com/counter'. The page content includes the ActiveMedia logo (PRODDYNAMIC SOLUTIONS) on the left. The main heading in Arabic is 'للتصويت الرجاء تحديث البرنامج'. Below this, there are four smartphones displaying the application interface. To the right of the phones, the text 'العدد الكلي للتحميل' is followed by the large number '23137'. Below the number, it says 'Release Date: January 9th 2012'. At the bottom right, there is an 'Available on the App Store' badge and a button that says 'اضغط للتحميل'. The website URL 'www.activemedia.com.kw' is visible at the bottom center of the page.

Then, I did a search by name using the application and watching the packets as it travels through the network. I detected that the application sends a GET request to q8forlife.com and the website returns a JSON object that contains the information of people containing the name you searched for.

Capturing from wlan0 [Wireshark 1.6.1 (SVN Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ip.addr eq 192.168.43.24 Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
4355	2061.459854	192.168.43.24	184.168.115.185	TCP	66	[TCP Dup ACK 4354#1] 49437 > http [ACK] Seq=1 Ack=1 Win=131760 Len=0 TSval=305742016 TSecr=17646296
4356	2061.483892	192.168.43.24	184.168.115.185	HTTP	509	GET /rest/citizen/fullname/%D9%85%D8%AD%D9%85%D8%AF%20%D8%B3%D8%A7%D9%84%D9%85%20%D8%A7%D8%AC%D9%88
4357	2061.483776	192.168.43.24	184.168.115.185	HTTP	509	[TCP Retransmission] GET /rest/citizen/fullname/%D9%85%D8%AD%D9%85%D8%AF%20%D8%B3%D8%A7%D9%84%D9%85%20%D8%A7%D8%AC%D9%88
4361	2062.696931	184.168.115.185	192.168.43.24	TCP	66	http > 49437 [ACK] Seq=1 Ack=444 Win=6912 Len=0 TSval=1764631051 TSecr=305742039
4362	2062.697107	184.168.115.185	192.168.43.24	TCP	66	[TCP Dup ACK 4361#1] http > 49437 [ACK] Seq=1 Ack=444 Win=6912 Len=0 TSval=1764631051 TSecr=305742039
4364	2063.618950	184.168.115.185	192.168.43.24	TCP	889	[TCP segment of a reassembled PDU]
4365	2063.618826	184.168.115.185	192.168.43.24	HTTP	71	HTTP/1.1 200 OK (application/json)
4366	2063.618856	184.168.115.185	192.168.43.24	TCP	889	[TCP Out-Of-Order] http > 49437 [PSH, ACK] Seq=1 Ack=444 Win=6912 Len=823 TSval=1764631960 TSecr=305742039
4367	2063.618921	184.168.115.185	192.168.43.24	TCP	71	[TCP Retransmission] [TCP segment of a reassembled PDU]
4370	2063.712790	192.168.43.24	184.168.115.185	TCP	66	49437 > http [ACK] Seq=444 Ack=824 Win=130944 Len=0 TSval=305744257 TSecr=1764631960
4371	2063.713005	192.168.43.24	184.168.115.185	TCP	66	[TCP Dup ACK 4370#1] 49437 > http [ACK] Seq=444 Ack=824 Win=130944 Len=0 TSval=305744257 TSecr=1764631960
4372	2063.713160	192.168.43.24	184.168.115.185	TCP	66	49437 > http [ACK] Seq=444 Ack=829 Win=130928 Len=0 TSval=305744257 TSecr=1764631977
4373	2063.713282	192.168.43.24	184.168.115.185	TCP	66	[TCP Dup ACK 4372#1] 49437 > http [ACK] Seq=444 Ack=829 Win=130928 Len=0 TSval=305744257 TSecr=1764631977
4374	2063.789996	192.168.43.24	184.168.115.185	HTTP	509	GET /rest/citizen/fullname/%D9%85%D8%AD%D9%85%D8%AF%20%D8%B3%D8%A7%D9%84%D9%85%20%D8%A7%D8%AC%D9%88
4375	2063.790236	192.168.43.24	184.168.115.185	HTTP	509	[TCP Retransmission] GET /rest/citizen/fullname/%D9%85%D8%AD%D9%85%D8%AF%20%D8%B3%D8%A7%D9%84%D9%85%20%D8%A7%D8%AC%D9%88
4376	2064.139135	184.168.115.185	192.168.43.24	TCP	66	http > 49437 [ACK] Seq=829 Ack=887 Win=7936 Len=0 TSval=1764632491 TSecr=305744333
4377	2064.139337	184.168.115.185	192.168.43.24	TCP	66	[TCP Dup ACK 4376#1] http > 49437 [ACK] Seq=829 Ack=887 Win=7936 Len=0 TSval=1764632491 TSecr=305744333
4379	2065.208924	184.168.115.185	192.168.43.24	TCP	888	[TCP segment of a reassembled PDU]
4380	2065.209054	184.168.115.185	192.168.43.24	TCP	888	[TCP Retransmission] http > 49437 [PSH, ACK] Seq=829 Ack=887 Win=7936 Len=822 TSval=1764633551 TSecr=305744333
4381	2065.214769	184.168.115.185	192.168.43.24	HTTP	71	HTTP/1.1 200 OK (application/json)
4382	2065.214841	184.168.115.185	192.168.43.24	TCP	71	[TCP Retransmission] [TCP segment of a reassembled PDU]

Hypertext Transfer Protocol

GET /rest/citizen/fullname/%D9%85%D8%AD%D9%85%D8%AF%20%D8%B3%D8%A7%D9%84%D9%85%20%D8%A7%D8%AC%D9%88%D9%87%D9%84%20%D9%85%D8%AD%D9%85%D8%AF%20%D8%A7%D9%84%D8%AC%D9%88%D9%87%D9%84%20%D9%85%D8%AD%D9%85%D8%AF%20%D8%B3%D8%A7%D9%84%D9%85%20%D8%A7%D8%AC%D9%88

Host: www.q8forlife.com\r\n

User-Agent: ummah/1.1 CFNetwork/548.0.4 Darwin/11.0.0\r\n

Accept: */*\r\n

Accept-Language: en-us\r\n

Accept-Encoding: gzip, deflate\r\n

Cookie: PHPSESSID=9a63cf0dee7583f95457b7fd4277c9b2\r\n

```

0000  00 16 ea b7 56 02 5c 59 48 82 f6 e5 08 00 45 00  ...V.Y H.....E.
0010  01 ef 0f e7 40 00 40 06 b0 ff c0 a8 2b 18 b9 a8  ..o.o. ....+...
0020  73 b9 c1 1d 00 50 1c 76 b1 72 fd e4 f5 e9 80 18  s...P.v .r.....
0030  20 2b e4 62 00 00 01 01 08 0a 12 39 40 d7 69 2e  +b.... ..90.i.

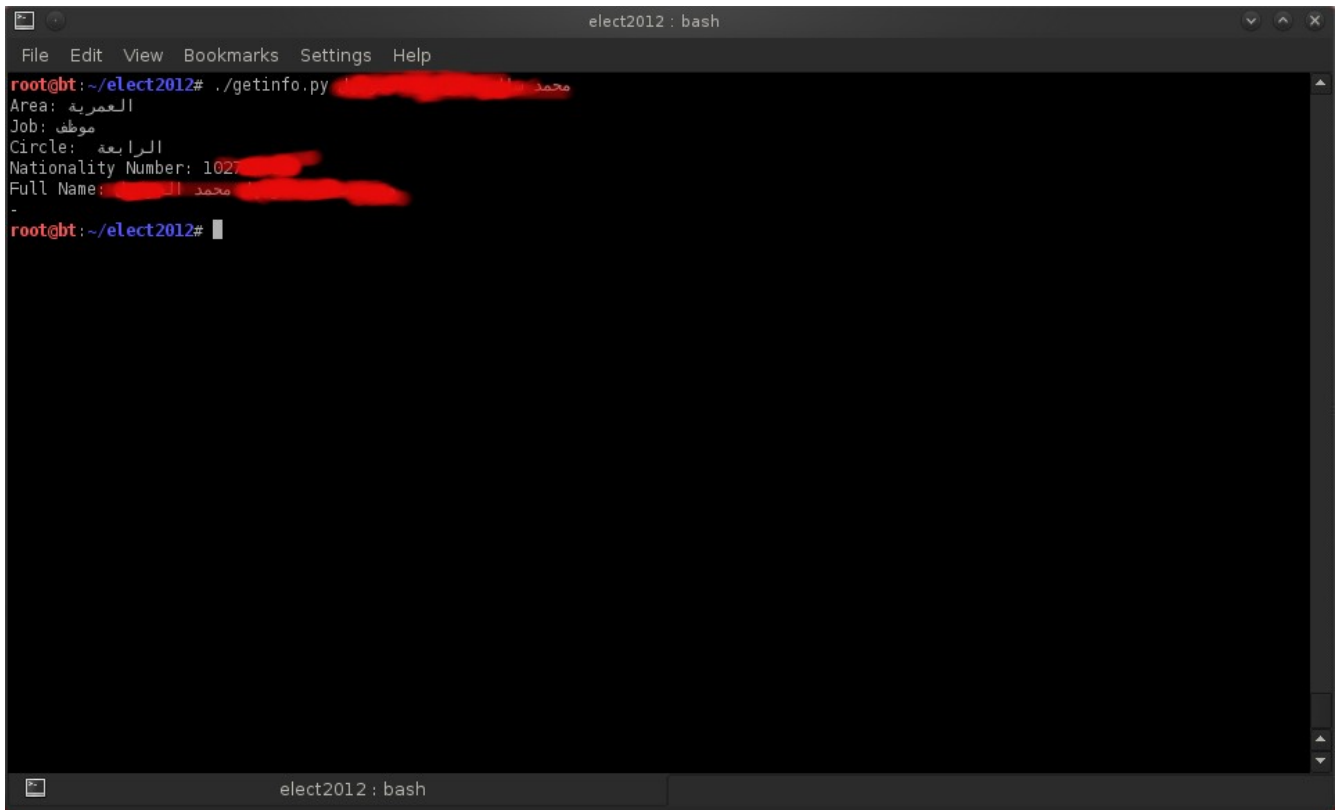
```

wlan0: <live capture in progress> F... Packets: 4461 Displayed: 734 Marked: 0 Profile: Default

Of course the connection is not secure.

The question is: How did he got the information of people through which he loaded his database with?

When I tried to search for a nationality number, the application crashed.
Finally, I wrote a python script³ to get the information of any given name:



```
elect2012 : bash
File Edit View Bookmarks Settings Help
root@bt: ~/elect2012# ./getinfo.py محمد بن محمد
Area: العمرية
Job: موظف
Circle: الرابعة
Nationality Number: 102
Full Name: محمد بن محمد
-
root@bt: ~/elect2012#
```

Conclusion

It's great to write programs that eases up our lives but it should not violate our privacy. Hackers are always there to look for faults and bugs to exploit it and get information from which they can move on. Last thing, my python script does what Elect 2012 application does exactly. So, don't tell me that I'm providing a tool to hack people's information. I'm not. q8forlife.com server is.

³ <https://gist.github.com/1628773>