



Universidade Federal do Rio de Janeiro
Instituto de Matemática
Departamento de Ciência da Computação
Grupo de Resposta a Incidentes de Segurança

Rio de Janeiro, RJ - Brasil

Segurança em Códigos QR

GRIS-2013-A-001

Rafael Oliveira dos Santos
rafaelsantos@gris.dcc.ufrj.br

A versão mais recente deste documento pode ser obtida na página oficial do GRIS: <http://www.gris.dcc.ufrj.br>.

GRIS - Grupo de Resposta a Incidentes de Segurança
Av. Brigadeiro Trompowski, s/nº
CCMN – Bloco F1 - Decanía
Cidade Universitária - Rio de Janeiro/RJ
CEP: 21949-900
Telefone: +55 (21) 2598-9491

Este documento é Copyright©2012 GRIS. Ele pode ser livremente copiado desde que sejam respeitadas as seguintes condições:

É permitido fazer e distribuir cópias inalteradas deste documento, completo ou em partes, contanto que esta nota de copyright e distribuição seja mantida em todas as cópias, e que a distribuição não tenha fins comerciais. Se este documento for distribuído apenas em parte, instruções de como obtê-lo por completo devem ser incluídas. É vedada a distribuição de versões modificadas deste documento, bem como a comercialização de cópias, sem a permissão expressa do GRIS.

Embora todos os cuidados tenham sido tomados na preparação deste documento, o GRIS não garante a correção absoluta das informações nele contidas, nem se responsabiliza por eventuais consequências que possam advir do seu uso.

Última atualização em: 17 de agosto de 2013

Sumário

1	Introdução	2
2	Desenvolvimento	3
2.1	Códigos QR?	3
2.1.1	Analisando a estrutura do Código QR	3
2.1.2	Código QR vs. Código de Barras	4
2.1.3	Como criar e ler?	5
2.1.4	Aplicações no dia-a-dia	5
2.2	É seguro escanear Códigos QR?	8
2.2.1	Por que me atacariam?	8
2.2.2	A nossa grande falha	8
2.2.3	Exemplos de possíveis ataques	8
2.2.4	Casos famosos	12
2.2.5	Security Quick Response Code - SQRC	16
2.3	Estudo de Caso: exemplo de ataque	18
2.3.1	Escolhendo uma vítima	20
2.3.2	Colhendo informações da vítima	21
2.3.3	Engenharia Social através da coleta	21
2.3.4	Resultados e coleta de informações	23
2.4	Boas práticas	23
2.4.1	Para os que escaneiam	23
2.4.2	Para os que criam os códigos	24
3	Conclusões	25
3.1	Projetos futuros	25
4	Referências Bibliográficas	26

1 Introdução

Desenvolvido no Japão em 1994 pela DENSO CORPORATION, os Códigos QR (Quick Response) são utilizados para transmitir qualquer tipo de dado através de uma simples captura de imagens em 2D.

Atualmente, os Códigos QR estão ganhando uma popularidade muito grande pela sua praticidade e devido ao mercado de dispositivos móveis, aparelhos capazes de lerem os códigos, estar crescendo muito!

Contudo, até que ponto é seguro escanear esses códigos? Será que existe um Código QR que possa executar códigos maliciosos? Ou mesmo um que, ao ser lido, roube todas as minhas informações pessoais?

Este artigo visa responder a todas essas perguntas e a entender minuciosamente os cuidados que devem ser tomados ao ler códigos QR. No final, apresentaremos uma cartilha com dicas de segurança para tecnologia móvel onde focaremos em códigos QR.



2 Desenvolvimento

2.1 Códigos QR?

Em 1994, a DENSO CORPORATION, um fabricante internacional de componentes automotivos, decidiu desenvolver uma espécie de simbologia em duas dimensões com o objetivo principal de "Ser um código de leitura fácil para o leitor".

Muitas versões do Código QR foram desenvolvidas até chegarmos em 2013 na versão de número 40. Seguem abaixo detalhes um pouco mais aprofundados sobre a estrutura do Código QR:

2.1.1 Analisando a estrutura do Código QR



É possível dividir a estrutura física de um Código QR em 8 grandes partes:

1) **Finder Pattern - Localizador de Padrão:** O Localizador de Padrão consiste em três grandes estruturas que ficam localizadas em todas as quinas, exceto a da direita em baixo do código. Cadaquina é baseada em uma matriz 3x3 de módulos negros coberta por módulos brancos que são novamente cobertos por módulos negros. O Localizador de Padrão permite ao programa decodificar e identificar a imagem como um Código QR e determinar sua orientação correta.

2) **Separators - Separadores:** Os separadores brancos possuem uma largura de um *pixel* e aumenta o reconhecimento do Localizador de Padrão por separá-lo da área de Dados em si.

3) **Timing Pattern - Temporização de Padrão :** Alternando entre módulos pretos e brancos, a Temporização de Padrão permite ao programa decodificar e determinar a largura de um padrão.

4) **Alignment Patterns - Alinhamento de Padrão:** A seção de Alinhamento de Padrão ajuda o Leitor dos Códigos QR a compensar algumas possíveis distorções na imagem. A primeira versão do Código QR não possuia a seção de Alinhamento de Modelos e com o crescimento do tamanho do código, mais seções de Alinhamento de Padrão foram adicionadas.

5) **Format Information - Informação de Formato:**

A Informação de Formato consiste em 15 *bits* próximos aos separadores e armazenam informação sobre o nível de correção de erro do Código QR assim como do modelo de máscara escolhido.

6) **Data - Dados:**

Aqui é onde ficam os dados propriamente dito. Eles são convertidos em um “fluxo de *bits*” para então serem guardados em partes de 8 *bits*.

7) **Error Correction - Correção de erros:** Semelhantemente com a seção de Dados, os códigos de Correção de Erros são armazenados em 8 *bits*.

8) **Remainder Bits - Bits restantes:**

Esta seção consiste em bits vazios caso os Dados e a Correção de erros não puderem ser divididos em 8 *bits* da forma apropriada.

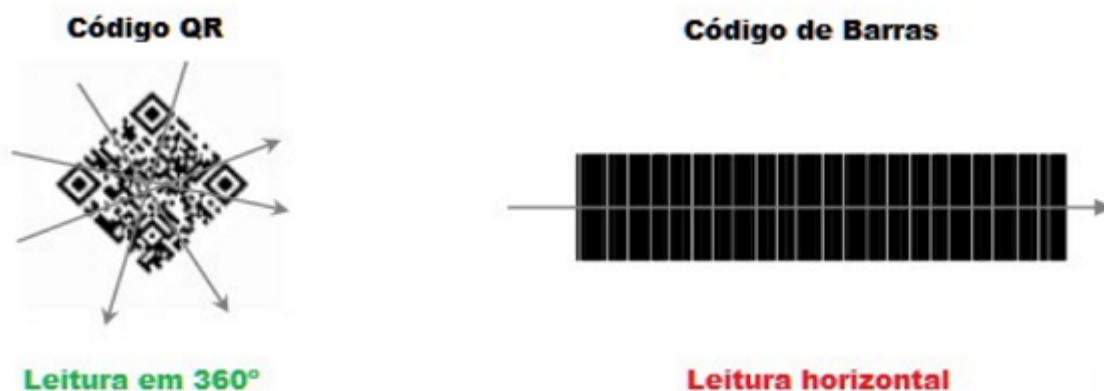
2.1.2 Código QR vs. Código de Barras

Ao conhecer um pouco o Código QR você deve se perguntar: "E os Códigos de Barras já não fazem isso?". Os Códigos de Barras são de grande utilidade para a humanidade atualmente, porém, com a criação dos Códigos QR, muitas outras funcionalidades foram inseridas:

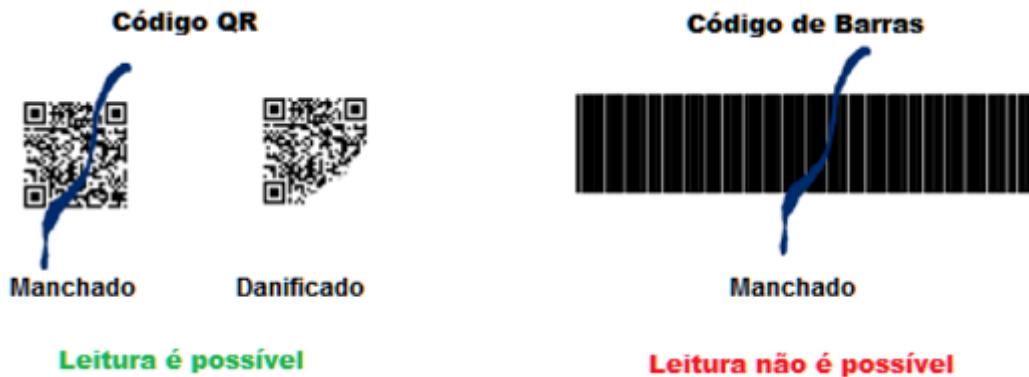
a) Posição onde são armazenados os dados



b) Leitura em alta velocidade



c) Durabilidade contra manchas e danos



d) Representação Kanji



2.1.3 Como criar e ler?

Para criar os códigos é necessária a utilização de um *QR Code Generator*, ou Gerador de Código QR em português, que é facilmente encontrado na Internet. Um exemplo seria o <http://qrcode.kaywa.com/>.

Algumas funcionalidades desses dados representados podem ser divididas em **URLs**, que levam à endereços da Internet, **Textos**, que mostram algum tipo de informação em texto puro, **Número de telefones**, que armazenam algum número de telefone, ou mesmo **SMS**, que automaticamente enviam uma mensagem de texto para um celular específico.

Com um código já criado, para que a leitura seja feita, você precisa de um dispositivo onde seja possível a instalação de um *QR Code Reader*, ou Leitor de Códigos QR em português. Um exemplo de leitor grátil pode ser encontrado em <http://barcode-scanner.softonic.com.br/android>.

2.1.4 Aplicações no dia-a-dia

Apesar de ser uma tecnologia não muito nova, atualmente, principalmente pelo fato do "boom" dos dispositivos móveis, no Japão e na Coréia do Sul a utilização de Códigos QR no dia-a-dia já é realidade. Nesses países, graças aos códigos QR, é possível efetuar compras até em estações de metrô! Nos EUA, as coisas estão avançando de uma forma estrondosa também. É muito comum andar pela 5th Avenue em Nova York e se deparar com um anúncio gigantesco com um Código QR, por exemplo. Aqui no Brasil, não estamos tão distantes disso. Muitas ações de marketing, ou mesmo os próprios bancos nacionais como veremos a seguir, já utilizam os códigos QR também.

A seguir, seguem alguns figuris para ilustrar as aplicações no dia-a-dia:

- a) Fazer compras
<http://www.youtube.com/watch?v=3Mqcb7RoN4Y>



b) Publicidade

<http://www.youtube.com/watch?v=SVjWBfVSbY4>



c) Armazenando dados de pacientes

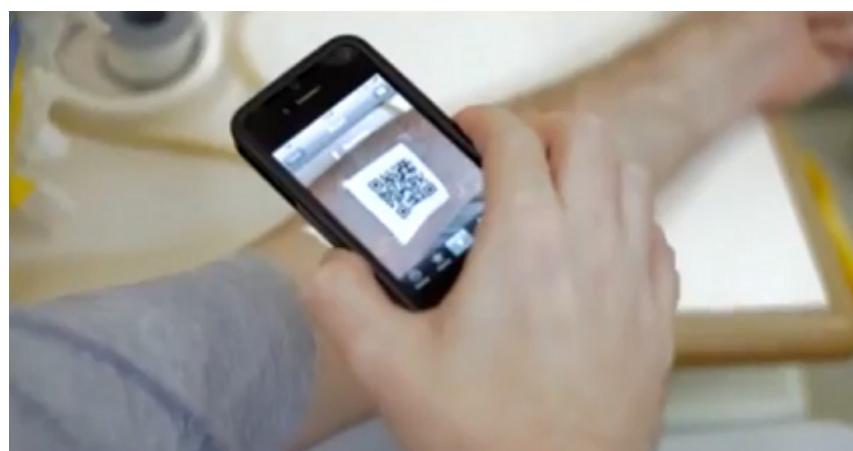


d) Pagamento de contas



e) Durante a doação de sangue

http://www.youtube.com/watch?v=rr8R-vr-Yqg&feature=player_embedded



f) Utilizando softwares de relacionamento

http://www.youtube.com/watch?v=8Y0St_Igp6M



2.2 É seguro escanear Códigos QR?

Depois de todas as novidades e coisas interessantes que podemos utilizar com os Códigos QR fica uma pergunta no ar: É seguro escanear esses Códigos? Será que alguém pode criar um código malicioso que consiga roubar meus dados? Será que algum deles pode instalar um aplicativo sem minha autorização em meu dispositivo?

2.2.1 Por que me atacariam?

O grande incentivo para um indivíduo malicioso praticar atividades maliciosas utilizando os Códigos QR é que os dispositivos móveis armazenam grande quantidade de informações pessoais. É uma verdadeira mina de ouro! Números telefônicos, conversas via aplicativos de comunicação, transações bancárias, e muito mais!

De posse dessas informações, um indivíduo com intenções maliciosas poderia praticar diversas atividades criminosas, como: extorsão, sequestro, furto, etc.

2.2.2 A nossa grande falha

O que alavanca a possibilidade de ataques bem sucedidos é a curiosidade das pessoas sem consciência dos perigos a qual estão expostas. Muitas delas escaneiam compulsivamente os códigos QR unicamente para desvendar seu significado, sem certeza alguma de sua origem ou segurança.

É essencial que você se controle e evite esse tipo de falha. Caso suspeite de um código onde a oferta é boa demais, não se arrisque! Mais à frente serão mostradas algumas dicas importantes sobre Boas Práticas ao escanear Códigos QR.

2.2.3 Exemplos de possíveis ataques

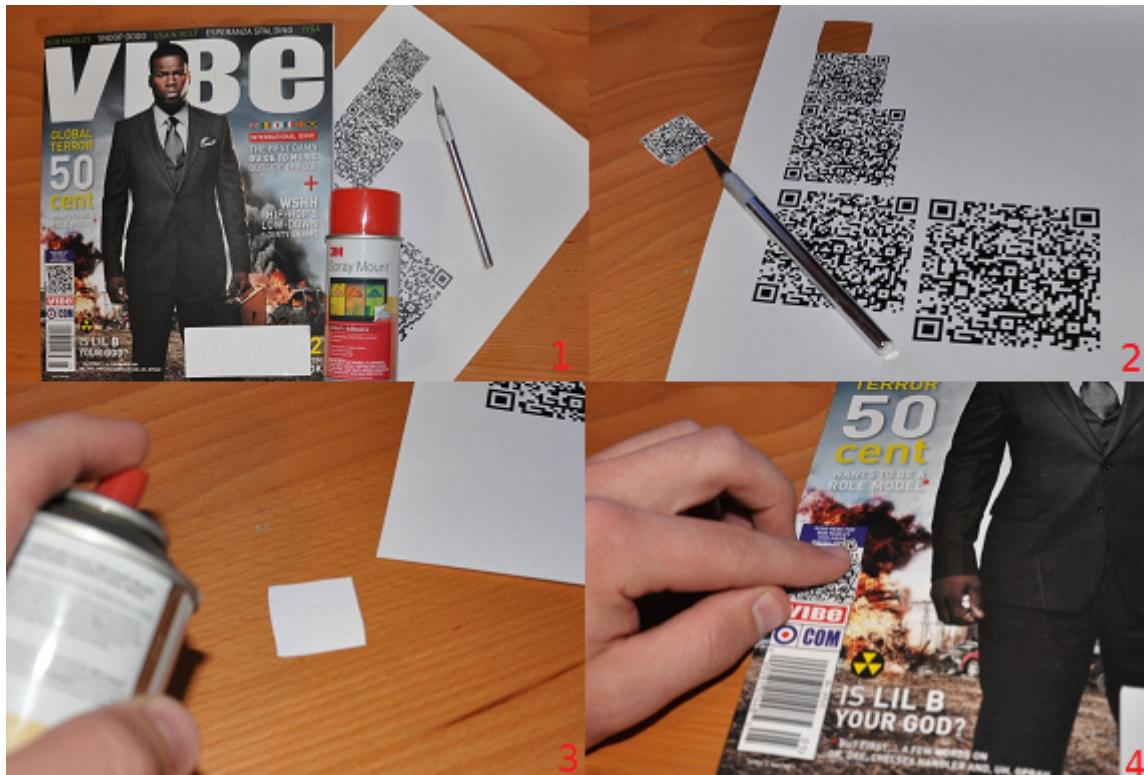
É muito difícil listar exatamente todos os possíveis ataques utilizando Códigos QR. A cada dia, *crackers* podem criar novos ataques, descobrirem novas vulnerabilidades, e explorar ainda mais a “má” utilização desses códigos. Contudo, segue uma lista de alguns já conhecidos tipos de ataques utilizando Códigos QR:

a) *QRJacking*

Este ataque funciona basicamente ao trocar um Código QR legítimo por um *sticker* redirecionando para outro malicioso. Um ataque muito simples mas que pode trazer consequências catastróficas.

Um exemplo, ilustrado a seguir, é de um ataque *QRJacking* em uma revista. O atacante cria um Código QR malicioso e imprime vários tamanhos até encontrar o exato ao do legítimo. Logo

em seguida ele cola por cima do original e o deixa para que pessoas escaneiem em uma sala de espera, por exemplo.



Fonte: <http://notdanwilkerson.wordpress.com/2011/05/03/qr-jacking/>

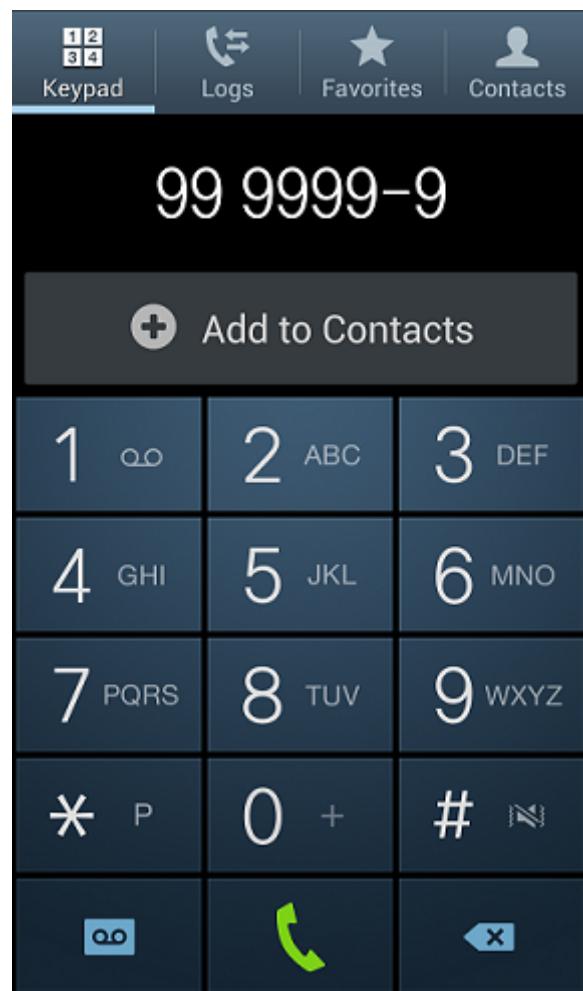
Podemos encontrar outros exemplos de **QRJacking**, sofisticados ou não, abaixo também:





b) *ScanJacking*

Neste ataque, caso o dispositivo móvel permita que se execute *JavaScript* sem prévia confirmação do usuário, uma pessoa mal intencionada conseguiria criar um código para fins maliciosos. Por exemplo, um código QR poderia direcionar para uma *URL* supostamente “inofensiva” mas que na verdade executa um *JavaScript* que mostra os *Logs*, Contatos, etc da vítima:



c) *Phishing*

É possível realizar também ataques de Engenharia Social, como o ***Phishing***, utilizando Códigos QR. Juntamente com um ataque de ***ScanJacking***, um atacante pode criar um código malicioso que leve a vítima à um *site* muito parecido com o legítimo.



Fique atento à site falsos! Esta imagem mostra um exemplo de Phishing do Paypal.

Imagine a seguinte situação: Uma empresa X decide criar um anúncio publicitário em uma revista de grande circulação na cidade. Porém, uma pessoa com intenções maliciosas cria um falso Código QR que leva à um *site* também falso muito parecido com o da empresa X. Lá, a vítima fornece todas as suas informações pessoais, senhas, etc. achando que está realizando um compra online, por exemplo, mas na verdade está sofrendo um ataque de ***Phishing*** muito poderoso!

d) Fraude de SMS

Você já deve ter ouvido em propagandas algo do tipo: "Quer receber notícias sobre seu time preferido? Mande um SMS para o número Y com a palavra TIME.". A empresa fornece as notícias esportivas para quem interessar assinar seu *feedback* e o usuário paga por isso, diariamente, semanalmente, etc. Esse tipo de serviço pode ser muito interessante para algumas pessoas, porém, o que aconteceria se o usuário pagasse por um serviço e não o recebesse? Se pagasse um preço extremamente elevado por esse serviço? Ou pior, se pagasse por um serviço que ele nem sabe que está pagando?

É assim que o ataque da Fraude de SMS funciona. Utilizando uma funcionalidade dos Códigos QR, que é a de enviar SMS para números telefônicos, atacantes podem criar códigos maliciosos que fazem pessoas assinarem algo que não desejavam ou pagarem por algo por um preço abusivo. Alguns leitores de Códigos QR avisam e mostram a mensagem de texto e o telefone a ser enviada a mensagem. Contudo, outros fazem esse processo automaticamente.



QR-Code da promoção

NOTÍCIAS SBT

Não fique sem saber o que ocorre no Brasil e no mundo! Envie um SMS com a palavra "NOTICIA" para 44644". Assinatura: R\$0,31 + imp/sms Operadoras participantes: Vivo, CTBC, Oi, TIM, Claro



► REGULAMENTO

Portal de Voz do Ratinho

Participe do Programa do Ratinho, ligue para 015 11 97424-0004 e dê sua opinião. "Custo de uma ligação para celular de São Paulo".

Serviço disponível para todas as operadoras de telefonia móvel e fixa.



► ACESSE O SITE



QR-Code da promoção

Promoção - Quem Sabe Ganhando Mais

Conheça o novo concurso de Perguntas e respostas! A cada resposta certa você ganha 2X chances de levar 10 mil reais! Envie MAIS para 44944 e Participe!

AVISO: NAO ENVIAMOS MENSAGENS SMS PARA INFORMAR GANHADORES
Para cancelar o serviço envie a palavra SAIR para 44944
Custo: R\$1,99 operadora Oi , R\$1,99 + impostos/mgs demais operadoras



► ACESSE O SITE



QR-Code da promoção

Promoção – Tenha Estilo

Envie MODA para 57550 e Participe!

AVISO: NAO ENVIAMOS MENSAGENS SMS PARA INFORMAR GANHADORES
Para cancelar o serviço envie a palavra SAIR para 57550
Custo: R\$1,99+imp por semana para operadoras Claro, Vivo e Tim e R\$1,99 por semana para operadoras Oi
Quiz: R\$0,31+imp/mensagem para operadoras Claro, Vivo, Tim e Oi.



MUNDO SBT - ENTRETENIMENTO

Exemplo de uso legítimo de SMS com QR Codes.

Imagine uma situação onde alguém cria um Código QR fraudulento e divulga no corredor do escritório onde trabalha. Além disso, coloca um anúncio ao lado do código dizendo: "Escaneie e concorra a um Iphone!". Apenas para exemplificar, imagine também que a cada mensagem recebida o sistema do atacante consegue ganhar R\$5,00. Salário extra garantido para a pessoa com intenções maliciosas, não?

e) Conectando-se em redes inseguras

É possível também utilizar os Códigos QR para se conectar automaticamente à redes sem fio. Uma situação para exemplificar essa funcionalidade seria quando uma pessoa chega em um aeroporto e deseja se conectar à Internet. Um cartaz com o código é divulgado e, assim que escaneado, configura o dispositivo automaticamente para se conectar à rede sem fio desejada.

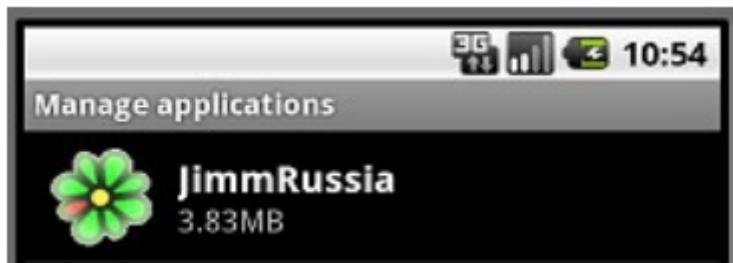
Esse conforto e rapidez é tão bom quanto perigoso. Caso a rede sem fio esteja sendo monitorada por um agente malicioso, ele pode capturar todos os dados que passam pela rede, roubar os dados bancários, informações pessoais, etc, e a partir disso realizar atividades ilegais como extorsão, criar perfil falso com seus dados, e muito mais...

2.2.4 Casos famosos

Recentemente ocorreram 2 ataques que ficaram famosos por utilizar um Código QR como ferramenta de ataque. Segue uma análise detalhada feita de cada um.

a) JimmRussia

Em meados de Setembro de 2011, um novo *malware* foi identificado em alguns fóruns e sites a Rússia utilizando um Código QR. Ele redirecionava para um site que continha um aplicativo chamado JimmRussia, que na verdade era um *trojan* que fingia ser um "Instant Messenger" do ICQ, para as pessoas baixarem em suas dispositivos móveis:



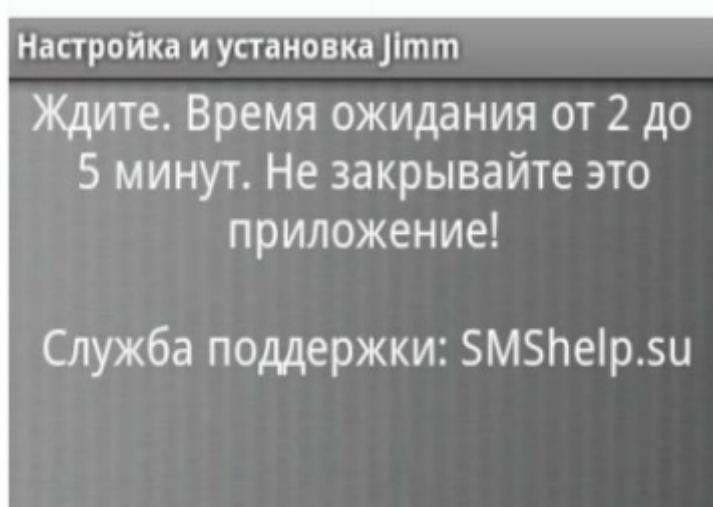
Analizando mais a fundo, era possível primeiramente notar o nome do pacote do *malware*:

```
package="appinventor.ai_russ_support.JimmRussia".
```

Logo em seguida, as permissões que ele possuia:

```
<uses-permission android:name="android.permission.SEND_SMS" />
<uses-permission android:name="android.permission.INTERNET" />
<uses-permission android:name="android.permission.RECEIVE_SMS" />
```

E, assim que abrisse o aplicativo, a seguinte mensagem aparecia:



Por fim, o aplicativo praticava o ataque Fraude de SMS, como mostrado anteriormente, para seus fins maliciosos. Eram enviadas várias mensagens para o número 2476 com um custo de 6 dólares cada uma para o indivíduo malicioso.



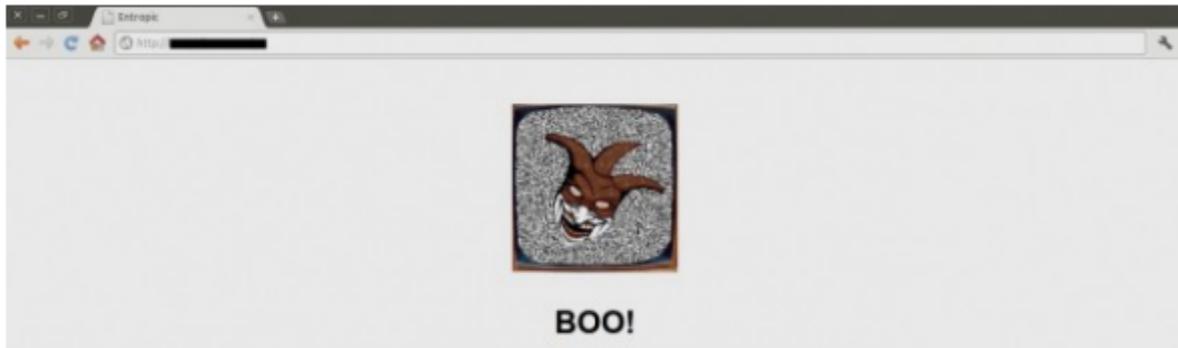
b) th3j35t3r

Em março de 2012, um *hacker* entitulado como th3j35t3r publicou em seu *blog* que tinha conseguido realizar um ataque com Códigos QR e obtido informações valiosas de algumas pessoas relacionadas a um grupo hacktivista. O ataque utilizava técnicas de *ScanJacking* explicadas acima e ,claro , contou com a curiosidade das pessoas em descobrir o que um Código QR fazia.

Tudo começou quando em sua conta do *Twitter* , th3j35t3r simplesmente trocou sua foto por um Código QR sem dar nenhuma breve explicação(o Código QR abaixo foi alterado e não é o malicioso!):



Ao escanear o código, a pessoa era redirecionada para uma *URL* que mostrava uma imagem de palhaço com a palavra "BOO!":



Juntamente com a imagem, existia um código *JavaScript* embutido que na verdade era um código de execução de um *shellcode*. Quando a pessoa escaneava o Código QR malicioso, o mesmo era executado. Este *shellcode*, na verdade, era uma versão atualizada e modificada de um *exploit* para *Webkit* já conhecido da CVE-2013-1807.

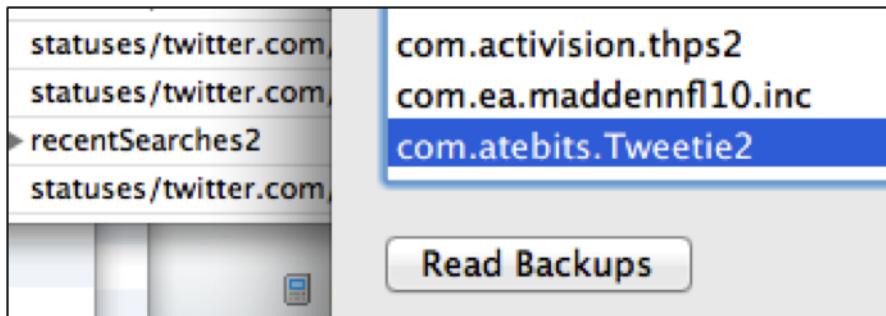
Exploits para *Webkit* nunca foram novidades e, de acordo com a análise do *malware* mostrada em seu *post*, este *exploit* executava um comando no *netcat* que enviava as credenciais do *Twitter* da vítima para ele.

Muitas pessoas não resistiram e acabaram caindo na falha de escanear o código malicioso. Porém, o *hacker* afirma não ter divulgado nenhuma informação sigilosa das vítimas, com uma exceção: a vítima não estar na “shit list” criada por ele.



Esta lista continha o usuário da conta do *Twitter* de vários “candidatos” à vítima: @alemarahweb, @HSMPress @AnonymousIRC, @wikileaks, @anonyops, @barretbrownlol, @DiscordiAnon, @RepDanGordon.

Ainda que a vítima utilizasse na época o IOS 5.1, o banco de dados *com.atebits.Tweetie2* continha o *com.atebits.Tweet2.plist* que detém o usuário do *Twitter*, pesquisas recentes feitas, UDID do aparelho (identificador único de cada *iphone*, dentre outras informações sigilosas da vítima).



Por fim, *th3j35t3r* elevou seus privilégios nos aparelhos infectados através do usuário/senha padrão já conhecidos do IOS (root/alpine) para analisar SMS, mensagens de voz, *logs* das chamadas, email no telefone, e muito mais da vítima. Para tal, seguem algumas *queries* simples em sqlite3 utilizadas:

```
th3j35t3r$ sqlite3 sms.db
SQLite version 3.7.9 2011-11-01 00:52:41
Enter ".help" for instructions
Enter SQL statements terminated with a ";"

sqlite> select address, text from message;
+15555551234| Where can I download LOIC?
+15555551234| Whats the new IRC Hivemind Server?
+15555551234| Where can I find a good attorney?
```

Algumas estatísticas sobre o ataque divulgados pelo *hacker*:

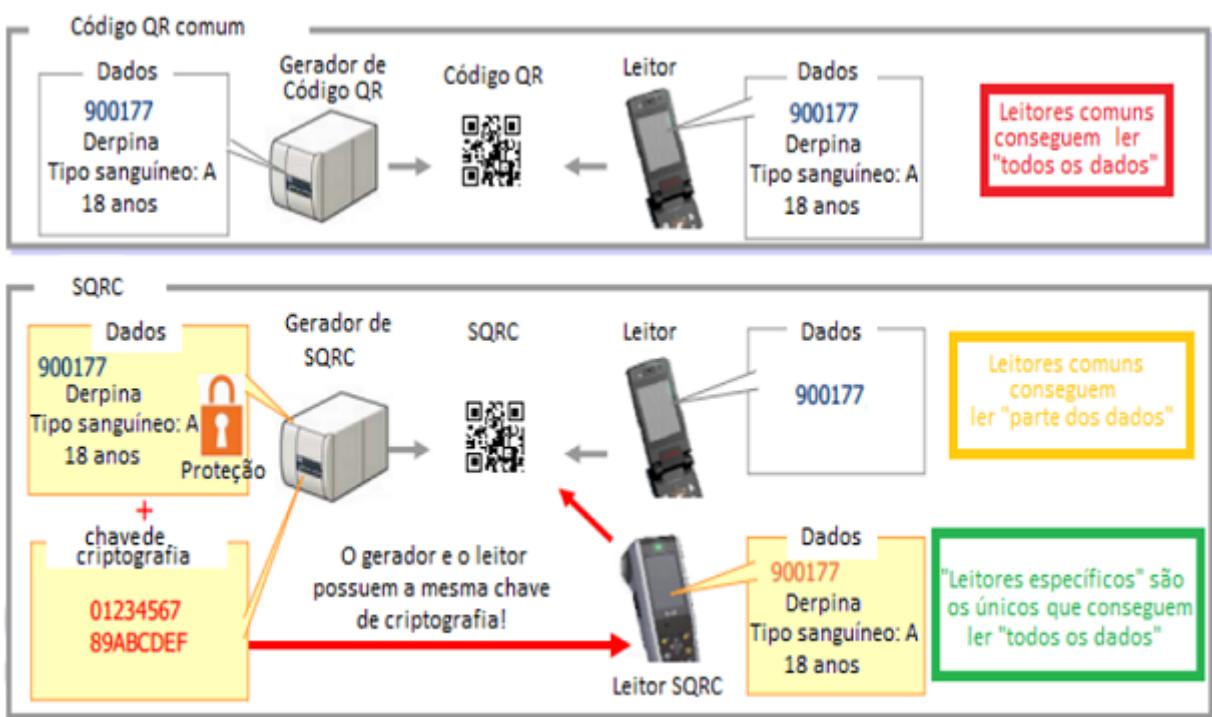
- Mais de 1200 pessoas escanearam o código malicioso;
- Desses, 500 conseguiram ser de fato atacados;
- E desses 500, um número significativo estava na “shit-list”;
- Um arquivo .txt com 146 MB foi divulgado com todas as informações das vítimas do ataque.

2.2.5 Security Quick Response Code - SQRC



Como uma forma de tentar proteger e amenizar o vazamento de informações pessoais através de Códigos QR, foi desenvolvido o SQRC - *Security Quick Response Code*. A sua utilização funciona da seguinte forma: Um gerador do código deve ser um especial, o Gerador de SQRC, onde o código é gerado utilizando uma criptografia que somente um determinado Leitor de SQRC é capaz de decifrar. Mesmo que uma pessoa consiga escanear o Código QR, em um leitor comum de celular, por exemplo, ela só conseguirá pegar parte dos dados por não utilizar o Leitor de SQRC.

A seguir segue um diagrama para exemplificar melhor sua utilização:



Dispositivo SQRC.

2.3 Estudo de Caso: exemplo de ataque

Primeiramente, é importante frisar que todo ataque aqui mostrado foi apenas uma **SIMULAÇÃO**. Nenhuma informação sensível foi resgatada durante a pesquisa e tudo que será mostrado a seguir foi manipulado em um ambiente totalmente controlado! Além disso, essa seção também não tem o intuito de ensinar minuciosamente como realizar um ataque utilizando Códigos QR. A missão maior do GRIS com essa pesquisa é conscientizar que ataques podem ser feitos!

A idéia desse estudo de caso é mostrar como uma pessoa maliciosa poderia realizar um ataque se aproveitando da curiosidade das pessoas em escanear seu código QR. Inicialmente, foi desenvolvido um código QR que levaria a seguinte URL: <http://gris.dcc.ufrj.br/qrcode.php>. Esse código foi impresso em um *banner* e colocado dentro do Centro de Tecnologia (CT) da UFRJ para tentar descobrir se as pessoas forneciam seus dados pessoais somente com um Código QR sem informações em volta. A figura a seguir mostra onde o *banner* foi colocado:



Dentro dessa URL, foi desenvolvido uma pequena simulação de aplicativo para celular, onde uma pesquisa falsa estava acontecendo:



Para confirmar sua escolha, a vítima deveria fornecer seu email pessoal. Todas essas informações eram enviadas para o email do "atacante":

Validação

Voltar

Nome	Seu nome
Email	Endereço email
Opção	<input type="text"/>

Confirmar Voto

2.3.1 Escolhendo uma vítima

Como primeiro passo, era preciso escolher uma vitima para o ataque. Analisando um dos emails, era possível encontrar as seguintes informações:

Subject : QRCode formulario - Novo
Formwidget-2 : Fulano
Formwidget-3 : fulano@email.com
Formwidget-6 : Iphone 5



[Generate Report here](#)
[Subscribe](#) | [Unsubscribe](#) from receiving this email

Além disso, analisando o *user agent* para saber os acessos da URL do código QR, foi possível identificar várias informações preciosas do dispositivo móvel em questão. As informações do último acesso (nossa vítima) está destacada abaixo:

```
AppleWebKit/534.30 (KHTML, like Gecko) Version/4.0 Mobile Safari/534.30
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like
Gecko) Version/6.0 Mobile/10A403 Safari/8536.25

Mozilla/5.0 (Linux; U; Android 2.3.6; pt-br; MB860 Build/4.5.2A-51_OLL-48)
AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1
Mozilla/5.0 (Linux; U; Android 2.3.6; pt-br; MB860 Build/4.5.2A-51_OLL-48)
AppleWebKit/533.1 (KHTML, like Gecko) Version/4.0 Mobile Safari/533.1
Mozilla/5.0 (iPhone; CPU iPhone OS 6_0 like Mac OS X) AppleWebKit/536.26 (KHTML, like
Gecko) Version/6.0 Mobile/10A403 Safari/8536.25
unknown AppEngine-Google; (+http://code.google.com/appengine; appid: qmksync)
unknown AppEngine-Google; (+http://code.google.com/appengine; appid: qmksync)
unknown AppEngine-Google; (+http://code.google.com/appengine; appid: qmksync)
Ewing (Android)
Mozilla/5.0 (SymbianOS/9.4; Series60/5.0 Nokia5230-1d/50.4.001; Profile/MIDP-2.1
Configuration/CLDC-1.1 ) AppleWebKit/533.4 (KHTML, like Gecko) NokiaBrowser/7.3.1.25
Mobile Safari/533.4 3gpp-gba
```

Concluindo nossa primeira parte de escolha da vítima, buscamos na *internet* por vulnerabilidades do sistema utilizado para ver se poderíamos explorá-las através da utilização de Códigos QR:

SecurityFocus™

Symantec Connect
A technical community for Symantec customers, end-users, developers, and partners.
Join the conversation >

Vulnerabilities

Vendor: ←

Title:

Version:

Search by CVE

CVE:
Submit

Nokia Web Browser for S60 Infinite Array Sort Denial of Service Vulnerability
2008-10-15
<http://www.securityfocus.com/bid/31703>

Nokia Browser HTML Denial of Service Vulnerability
2006-08-11

2.3.2 Colhendo informações da vítima

Com o email em mãos e realizando buscas pelas mídias sociais, era possível encontrar informações pessoas da vítima sem mesmo se logar no sistema:



2.3.3 Engenharia Social através da coleta

Com tais informações, foi confeccionado um email a fim de enganar a vítima mais uma vez. O *Phishing* em questão induzia a vítima a escanear em seu dispositivo móvel um Código QR que instalava um falso aplicativo, um *malware* para explorar a vulnerabilidade em questão:



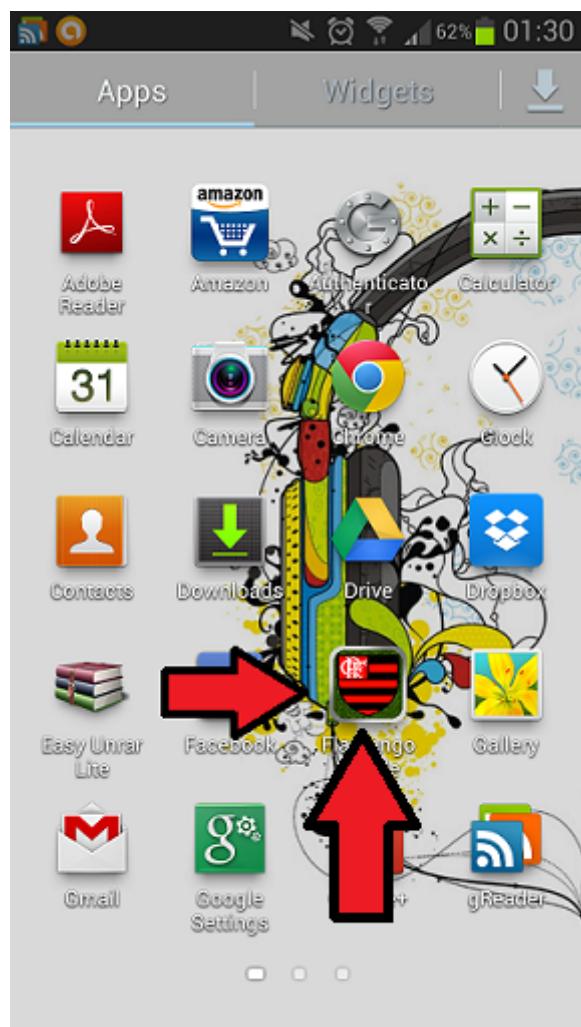
Quer receber notícias do Mengão no seu celular??

Instale agora o aplicativo Mengão Hexa em seu celular e receba diariamente notícias do Mais Querido do Brasil!!

Basta escanear o QR Code abaixo:



O interessante aqui é perceber que esse ataque de Engenharia Social realmente poderia dar certo. Como a vítima já possui o hábito de escanear Códigos QR em seu celular, como foi feito em primeiro momento, ela certamente poderia escanear mais uma vez e instalar um aplicativo sem noção do perigo que está correndo!



2.3.4 Resultados e coleta de informações

Não pretendemos entrar em detalhes de como criar *malwares* que podem explorar vulnerabilidades nos dispositivos móveis. Porém, depois que o aplicativo malicioso estiver instalado, em alguns casos, o controle total do celular pode estar no controle do *cracker!* Em nosso estudo de caso, nossa vítima já estaria correndo sérios perigos ao instalar o falso aplicativo do Flamengo mostrado acima.

Para concluir nosso estudo de caso, todas as informações da vítima então podem ser acessadas: mensagens de texto, agenda, acesso à email, mídias sociais, vídeos, fotos, etc:



Somente como título de curiosidade, tivemos vários acessos à nossa URL durante o período em que expomos o *banner*. O resultado da falsa pesquisa teve como mais votos o *Samsung Galaxy S3*, e 13 pessoas forneceram seus dados pessoais (nome e email).

2.4 Boas práticas

Após conhecer algumas ameaças fique sempre atento a partir de agora ao utilizar Códigos QR. Evite também criar uma preocupação extrema com eles, pois podemos tirar grandes proveitos ao utilizá-los corretamente. Para tal, seguem algumas boas práticas para o dia-a-dia:

2.4.1 Para os que escaneiam

- Utilize um bom leitor

É de extrema importância escolher um leitor bom. Bom no sentido de ser um *software* que se preocupa com segurança, disponibiliza atualizações com uma frequência boa, e que consiga realizar os *scans* de uma forma eficaz.

Existem no mercado vários leitores, famosos ou não, pagos ou não, que são muito bons nesses sentidos. Dessa forma, segue uma lista que pode ajudar na escolha de um bom leitor:

- Não deixe um Código QR agir sozinho!

Nunca permita que um Código QR faça suas atividades de forma automática. Se seu leitor ou dispositivo deixa ou possui essa configuração por padrão, **desabilite-a**. Infelizmente, alguns celulares permitem que o *javascript* seja executado camufladamente, porém, é crucial você saber tudo que um Código QR está prestes a realizar.

- Não forneça informações desnecessárias.

Sempre que um Código QR te levar para algum lugar, evite fornecer muitas informações. Sempre se pergunte, são realmente necessárias todas essas minhas informações para acessar

meu *Facebook*, por exemplo? Eu preciso de fato dar meu endereço de casa para ler um livro em um *site*?

Desconfie de tudo, **sempre!**

- Sempre verifique a URL

Seguindo na linha do segundo tópico, verifique sempre a URL para onde um Código QR vai. Muitas vezes pessoas maliciosas podem divulgar códigos maliciosos que levam à *sites* totalmente diferentes do divulgado.

Além disso, fique atento também aos endereços com *link* encurtado. O grande propósito de um Código QR é simplificar as coisas, simplificar *links*. Então, para que precisam encurtar um endereço para depois criar um Código QR? Esta técnica pode ser utilizada para esconder endereços maliciosos, fique atento!

- Verifique a integridade física do código

Um outro tópico importante também é a integridade física de um Código QR. Verifique se existe algum vestígio de que aquele código foi alterado, o ambiente onde ele está sendo publicado e se seria fácil alterá-lo com um ataque de *QRJacking*, por exemplo.

Isso tudo deve ser levado em conta para evitar a dor de cabeça depois.

2.4.2 Para os que criam os códigos

- Evite serviços de encurtamento de *link*

Como já foi dito, encurtamento de *link* com Códigos QR não combinam! Se você pretende utilizar um Código QR para levar à um endereço de *site* muito grande, pra que você precisa encurtá-lo? Esse é o grande barato do Código QR, ele simplifica tudo para você com uma simples imagem em 2D.

- Sempre mostre o endereço que seu Código QR redireciona

É essencial ao criar um Código QR e ao divulgá-lo que você coloque o endereço para onde ele está indo ao lado. Isso passa uma confiança para seu Código QR e a pessoa pode conferir a URL que está sendo mostrada em seu dispositivo com a que está ao lado de seu código.

- Não utilize Códigos QR para informações sensíveis

Nunca utilize os Códigos QR para armazenar informações sensíveis como senhas, número de CPF, etc. Esses códigos não foram desenvolvidos para esconder uma mensagem para que ninguém possa ver. Mesmo que seu código fique extremamente guardado, ninguém tem acesso à ele, etc, não use essa tecnologia. Procure por mecanismos de Criptografia se achar válido.

- Procure zelar pela integridade física do seu código

Sempre que desejar publicar um Código QR, verifique primeiramente o ambiente onde você vai fazê-lo. Veja quantas pessoas passam por ali, faça uma pesquisa de que tipo de público frequenta o local, e, acima de tudo, se a integridade física de seu código será preservada. Nunca deixe um Código QR “exposto” à ataques!

Você pode colocar um plástico por cima do código, plastificá-lo, ou até colocá-lo atrás de um vidro!

3 Conclusões

É notório que os Códigos QR e todas as novas tecnologias desonvolvidas para dispositivos móveis dia após dia são de extrema utilidade para todos nós. Porém, infelizmente devemos estar sempre atentos, não só aos Códigos QR, mas à toda tecnologia que utilizamos no ponto de vista da **Segurança da Informação**.

Com esse artigo, pretendi mostrar e conscientizar que os Códigos QR podem e são extramente perigosos se usados em uma forma maliciosa. *Crackers* podem tornar situações simples, corriqueiras, onde pessoas simplesmente ao escanear um código podem sofrer danos irreparáveis.

Vale ressaltar também que não pretendemos causar pânico e muito menos orientar às pessoas a não utilizarem mais Códigos QR! Os Códigos QR são muito bons! Basta seguir algumas boas práticas mostradas nas seções anteriores que você estará um pouco mais protegido.

3.1 Projetos futuros

Nós, do GRIS, não podemos dar por encerrado esse assunto. Muitas outras áreas da Segurança em Códigos QR não foram exploradas ainda. Dessa forma, decidimos colocar alguns pontos interessantes aqui para mostrar os possíveis projetos futuros relacionados ao tema:

- Pesquisa sobre SQRC

A utilização do SQRC ainda não é muito consolidada e é muito difícil encontrar documentos relacionados à ela. Um projeto interessante seria pesquisar mais sobre sua utilização e tentar buscar *hardwares* para a realização de testes.

- Listar vulnerabilidades recentes dos leitores de Códigos QR

Buscar pela *internet* matérias, notícias, ou documentos em geral que falem sobre vulnerabilidades recentes dos leitores de Códigos QR. Descobrir se existem novos métodos de ataques que conseguem burlar todo o sistema já consolidado dos leitores atuais.

- Conhecendo pixel a pixel o Código QR

Pesquisar como funciona pixel a pixel um Código QR. Se você for realizando alterações em um Código QR em um editor de imagem, por exemplo, e for apagando pixel a pixel o código, até quando ele consegue ser legível? Sabemos que internamente o código possuem seu algoritmo de correção, porém pesquisar mais sobre essa área seria muito interessante e desafiador.

- Utilização de Códigos QR no Brasil

Algumas pessoas comentam que os Códigos QR nunca darão certo em nosso país. As empresas de telefonia móvel ainda não conseguem cobrir de uma maneira ideal toda a área nacional a *internet* nos dispositivos móveis. De uma certa forma, mesmo que as pessoas queiram escanear Códigos QR, sem *internet* fica complicado aumentar a utilização dessa tecnologia no Brasil. Pesquisar mais sobre esse assunto e criar estatísticas seria muito importante também!

- Forense em dispositivos móveis com ataques de Códigos QR

A forense em dispositivos móveis é uma área da Segurança da Informação que cresce a cada dia. Muitas pessoas usam seus celulares, por exemplo, como próprios computadores. Estudar um pouco mais sobre um caso onde envolva um crime ao utilizar ataques com Códigos QR seria desafiador!

- Hacktivismo + Códigos QR

Vimos neste artigo um exemplo de ataque envolvendo Hacktivismo. Será que essa idéia "cola"? Entender um pouco mais dessa mistura e pesquisar sobre como esses grupos hacktivistas pensam sobre o tema seria bem legal.

- Entendendo os geradores de Códigos QR

Como os geradores de Códigos QR funcionam? Qual algoritmo ele usa? Em que linguagem? Tentar pegar o código fonte de um gerador de Códigos QR deveria ser bem interessante para ver detalhe a detalhe como ele funciona!

4 Referências Bibliográficas

- 1) <http://blog.mobilephonesecurity.org/2011/09/qr-codes-and-security-my-take.html>
- 2) <http://blog.mobilephonesecurity.org/2011/09/qr-code-security-tips-for-both.html>
- 3) <http://www.darkreading.com/mobile-security/167901113/security/news/232301147/qr-codemalware-picks-up-steam.html>
- 4) <http://mashable.com/2011/10/20/qr-code-security-threat/>
- 5) <http://threatpost.com/google-patches-qr-code-vulnerability-in-glass>
- 6) https://www.securelist.com/en/blog/208193145/Malicious_QR_Codes_Pushing_Android_Malware
- 7) <http://blogs.itbusiness.ca/2010/08/qr-code-security-are-we-ready-to-discuss-the-risks/>
- 8) http://www.sba-research.org/wp-content/uploads/publications/QR_Code_Security.pdf
- 9) <http://isc.sans.edu/diary.html?storyid=12760&rss>
- 10) <http://www.mobile-barcodes.com/qr-code-software/>
- 11) <http://www.gs1jp.org/pdf/001.pdf>
- 12) <http://www.milliontech.com/home/content/view/254/139/>
- 13) <http://vitreoqr.com/qr-code-Security-SQRC.php>
- 14) <http://beqrious.com/scanning-qr-codes-be-safe/>
- 15) http://aa-download.avg.com/filedir/press/AVG_Community_Powered_Threat_Report_Q4_2011.pdf
- 16) <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2013-1807>
- 17) <http://jesterscourt.cc/2012/03/09/curiosity-pwned-the-cat/>
- 18) <http://notdanwilkerson.wordpress.com/2011/05/03/qr-jacking/>