Codici QR infetti: nuova minaccia emergente

Attraverso i codici QR è possibile distribuire malware ai dispositivi mobili senza che l'utente ne sia consapevole.

Rossano Ferraris

Il crimine informatico ogni giorno trova tecniche e strumenti sempre più sofisticati per poter portare a termine le sue azioni senza che queste siano facilmente rilevate e bloccate. Questa volta è il caso dei codici QR che sembrano costituire un ottimo canale per la distribuzione del malware alla grande massa degli utenti possessori di dispositivi mobili.
Effettivamente, considerando l'enorme diffusione di smartphone, iphone, tablet e altri dispositivi di questo tipo, era inevitabile che qualcosa si muovesse anche su questo fronte.

Che cosa sono i "codici QR"

Pochi sono a conoscenza dei cosiddetti codici QR e di come questi siano usati anche se sempre più spesso si nota la loro presenza su giornali, blog, riviste, cartelloni pubblicitari, ecc.
Tecnicamente un codice QR (in inglese *QR Code*) è un codice a barre bidimensionale (o codice 2D), ossia a matrice, composto da moduli neri disposti all'interno di uno schema di forma quadrata.

Rossano Ferraris, senior research engineer per Total Defense Inc.

È impiegato per memorizzare informazioni generalmente destinate a essere lette tramite un telefono cellulare o uno smartphone. Il nome QR è l'abbreviazione dell'inglese quick response (risposta rapida), in virtù del fatto che il codice fu sviluppato per permettere una rapida decodifica del suo contenuto.
Il codice QR fu sviluppato nel 1994 dalla compagnia giapponese Denso Wave, allo scopo di tracciare i pezzi di automobili nelle fabbriche di Toyota.
In Giappone si diffuse anche l'utilizzo dei codici QR sui biglietti da visita per semplificare l'inserimento dei dati nella rubrica del cellulare. Dalla seconda metà degli anni 2000, divennero sempre più comuni le pubblicità che ricorrevano all'uso dei codici QR stampati sulle pagine di giornali e riviste, o sui cartelloni pubblicitari, per veicolare facilmente indirizzi e URL.
Oggi con la grande diffusione degli smartphone (soprattutto in Europa e in Asia), è possibile trovare applicativi che circolano sulla rete da installare sui dispositivi mobili e in grado pertanto di decifrare i codici QR. Si tratta in definitiva di lettori QR che possono essere comodamente scaricati da Internet e installati sul proprio smartphone, iphone o qualunque dispositivo mobile dotato di video camera. Una volta installato basta avvicinare il proprio dispositivo sul codice QR, inquadrarlo con la video camera e il gioco è fatto: il lettore QR decodifica automaticamente il codice e visualizza il risultato che nella maggior parte dei casi è un sito o un video pubblicitario.

Nella pratica

Di per sé la tecnologia è comoda perché evita all'utente di digitare un indirizzo di posta elettronica o un indirizzo Internet in quanto sono sufficienti due semplici operazioni: inquadrare la video camera sul

codice e confermare. Ma una domanda sorge spontanea: quanto è sicura questa funzione? In termini di sicurezza, effettivamente, ci sarebbero alcuni aspetti da considerare come per esempio: chi mi assicura che il codice QR non sia infetto?
Mostreremo ora come sia semplice creare un codice QR di un blog o in generale di un indirizzo Internet e distribuirlo e stamparlo ovunque in modo che gli utenti possessori di smartphone possano leggerlo ed essere indirizzati a tale sito.
Supponiamo di generare il codice QR del mio blog personale di sicurezza www.securitysurfer.com.
La procedura è molto semplice: copio l'indirizzo da cui voglio generare il codice e lo incollo sulla barra degli indirizzi di un applicativo chiamato bit.ly.
Clicco sul bottone "shorten" che letteralmente significa "abbreviazione" e ottengo la forma abbreviata del sito in questione (Figura 1).

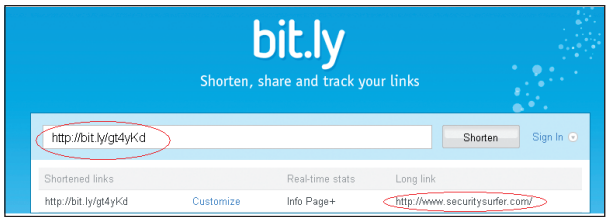

Figura 1 – "Shorten" del blog www.securitysurfer.com

Dopodiché aggiungo all'indirizzo abbreviato l'estensione ".QR" e ottengo il codice QR relativo (Figura 2).

Figura 2 – Codice QR del blog www.securitysurfer.com

A questo punto abbiamo generato il codice QR del mio blog di sicurezza che posso distribuire tranquillamente su giornali, riviste, cartelloni, ecc. L'operazione funziona molto bene e per gli increduli invito loro ad avvicinare il loro iphone (dotato di lettore QR) sul codice appena generato per verificarne il risultato.
Ma se il sito di cui devo generare il codice QR fosse un sito malevolo? Se, in qualità di cyber-criminale, volessi distribuire malware agli utenti di iphone usando questa tecnica? È possibile e fattibile anche perché l'utente è ignaro di quello che può nascondersi dentro un codice QR rivelandosi potenzialmente dannoso.

Conclusioni

Il diffondersi dei codici QR è già una realtà con la quale gli utenti dovranno interfacciarsi sempre di più. Data la ovvia incomprensibilità di un codice QR, gli utenti sono tenuti ad agire con la massima cautela. Si consiglia pertanto di seguire alcune semplici regole di comportamento che stanno alla base della sicurezza informatica:

- Mai fidarsi di ciò che è "sconosciuto": mantenere una certa forma di scetticismo verso la maggior parte dei codici QR che si trovano in giro per la rete o sui cartelli o addirittura sui muri della città in cui vi trovate. È consigliabile avvicinare la videocamera del proprio cellulare verso codici QR che si trovano in postazioni note, come musei, riviste, giornali conosciuti e altro che non sia sospetto.
- Installare una Security Suite sul dispositivo: quasi d'obbligo è l'installazione di un'applicazione di sicurezza sul proprio cellulare smartphone o iphone che sia.

Rossano Ferraris

Rossano Ferraris è laureato in Informatica e possiede le certificazioni SANS (GCIH, GCFA, GREM).
Attualmente ricopre il titolo di Senior Research Engineer per Total Defense Inc. (www.totaldefense.com) ex divisione di CA Tecnologies ISBU.
È membro e co-fondatore del team ISI (Internet Security Intelligence) all'interno del Dipartimento di Ricerca della ISBU (Internet Security Business Unit) con la responsabilità di guidare l'area EMEA nello studio, analisi e tracciamento delle minaccie emergenti. Consulente presso la Procura della Repubblica e le Forze dell'Ordine in materia di analisi forense e tematiche legate ai crimini informatici in Italia.
È inoltre socio AIPSI (capitolo italiano ISSA) e impegnato in attività di sensibilizzazione attraverso interventi pubblici e la scrittura di pubblicazioni sulle insidie provenienti dalla rete.
Rossano Ferraris è co-autore del libro "Qualcuno ci spia: spyware nel tuo pc", edito da Mondadori (2005) e ideatore del blog "SecuritySurfer" (www.securitysurfer.it).