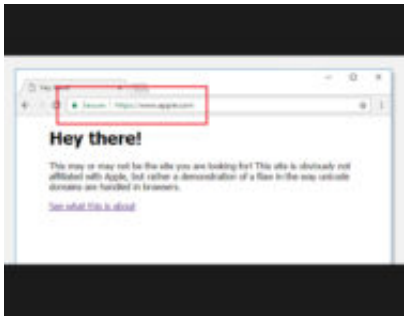
Attacco Phishing utilizza caratteri Unicode nei domini, rendendoli quasi impossibili da identificare

Date : 21 aprile 2017



La recente vulnerabilità evidenziata in alcuni browser, grazie alla quale è possibile realizzare attività di phishing in grado di ingannare anche gli utenti più smaliziati, è il sintomo di alcuni problemi di fondo che affliggono l'attuale implementazione di Internet (e delle tecnologie digitali in generale).

Tale implementazione è avvenuta nel giro di pochi anni, tumultuosamente, spesso frettolosamente, per lo più in modalità "bottom-up", e per queste sue modalità di realizzazione oggi Internet nel suo compesso soffre di un gran numero di lacune dal punto di vista della sicurezza, particolarmente difficili da risolvere in quanto parti integranti del sistema.

Nel caso specifico la lacuna risiede nel fatto che, in base ad una particolare RFC (la 3492 del preistorico 2003), i nomi di dominio composti da caratteri non-ASCII (Unicode) possono essere rappresentati in ASCII (utilizzando un meccanismo di codifica chiamato Punycode).

Questa feature, introdotta a suo tempo in assoluta buona fede, consente ad un soggetto malizioso di forgiare dei nomi di dominio che, una volta visualizzati nella barra degli indirizzi di alcuni browser, sono graficamente indistinguibili da quelli di brand conosciuti (homographic attack). La frode in oggetto si realizza dunque innanzi tutto tramite un'attività di typosquatting (registrazione di un dominio in caratteri non ASCII, che codificato in ASCII sembri un altro dominio).

Nell'esempio, utilizzando la codifica Punycode dei caratteri cirillici, si può mostrare all'utente l'url "apple.com", mentre in realtà il dominio registrato è "xn--80ak6aa92e.com". Di conseguenza, una volta carpita la buona fede dell'utente impersonando il sito Apple (phishing), è possibile applicare tecniche di social engineering per farsi consegnare le credenziali di accesso al sito stesso, con tutte le conseguenze del caso (furto di identità, furto di dati, estorsione, etc).

Cosa ci insegna questo ennesimo esempio di abuso di una delle features sulle quali si basa il buon funzionamento di Internet?

Per una serie di ragioni storiche abbiamo costruito una intera civiltà digitale su fondamenta che non sono adeguate agli scopi ed all'importanza che essa ha assunto nel tempo, perchè sono state pensate ed implementate in tempi completamente diversi, nei quali le minacce erano diversi ordini di grandezza inferiori rispetto ad oggi.

Dobbiamo urgentemente rimettere mano a tutto quanto fatto negli ultimi 30 anni, ripensarlo a fondo e in molti casi rifarlo da capo, ed allo stesso tempo introdurre regole molto più stringenti (per esempio sulla registrazione dei domini).

A cura di: **Andrea Zapparoli Manzoni**