Euroconference NEWS
L'INFORMAZIONE QUOTIDIANA DA PROFESSIONISTA A PROFESSIONISTA
Direttori: Sergio Pellegrino e Giovanni Valcarenghi

Edizione di martedì 4 novembre 2014

SOLUZIONI TECNOLOGICHE

Sicurezza, come funzionano i cavalli di Troia

di **Teamsystem.com**

Installare un buon antivirus, creare password diverse per ognuno dei servizi che utilizziamo online, non aprire allegati e non rispondere mai alle email sospette e così via. Sono alcuni dei consigli che dovremmo tenere sempre presenti quando accendiamo il computer, eppure, quello che solitamente si fa fatica a comprendere, è l'attinenza di queste pratiche alla vite reale. Sembra quasi che queste precauzioni siano teoriche, perché in fondo non è mai capitato che qualcuno abbia
rubato i nostri dati. Statisticamente è così, solo una piccola parte delle persone che navigano su Internet subisce un'infezione di qualche virus o un attacco da parte di un hacker, ma è anche vero, che tanti hanno il proprio computer infetto, trasformato in quello che in gergo viene chiamato "
zombie" ovvero sotto il controllo totale di qualche cyber criminale e neanche lo sanno.

Il mercato del crimine

Il mercato della criminalità informatica fattura svariati miliardi di euro ogni anno. Si tratta di un sistema collaudato e molto efficiente, che si basa principalmente sul furto dei dati delle carte di credito. Una vera miniera d'oro che la malavita utilizza per rubare denaro a banche, istituti di credito e persone comuni. Secondo
Kaspersky Lab, ogni giorno compaiono circa
315.000 nuovi esempi di software dannosi e non esiste sistema operativo che oggi possa essere considerato sicuro.

Quando si parla di
cyber-crimine, bisogna aver ben presente che abbiamo a che fare con organizzazioni molto complesse e legate al crimine organizzato. Oggi i pirati informatici attivi sono professionisti che usano strumenti molto evoluti e fanno di tutto per mettere le mani sulle informazioni che gli interessano.

Primo passo: il cavallo di Troia

Lo strumento preferito dai cyber criminali è un codice maligno chiamato
trojan horse, ovvero cavallo di Troia. Si tratta di un codice che viene installato nel computer

nei modi più svariati, soprattutto via posta elettronica e magari servendosi di quella che apparentemente può sembrare un normale documento o una foto. La tecnica più semplice consiste nell'
aggiungere una doppia estensione a un file.

Immaginiamo di ricevere un allegato che si chiama "
RicevutaPagamento.jpg". A prima vista sembra una foto e siamo portati a pensare che sia innocua. In realtà quel file si chiama "
RicevutaPagamento.jpg.vbs" dove
.vbs è la vera estensione che però Windows ha nascosto. Quel
.jpg che vediamo, fa parte del nome del file, ma non è affatto la sua estensione! Se facciamo clic su quella falsa immagine, partirà il programma contenuto nel file che installa nel computer il cavallo di Troia. Non ci accorgeremo di nulla, magari faremo più volte clic sul file perché l'immagine non si apre e alla fine penseremo semplicemente che non funziona. Eppure, ormai il danno è fatto perché, inconsapevolmente, abbiamo installato nel nostro computer un codice maligno che apre un varco verso l'esterno e permette a chi lo ha programmato di fare quello che vuole. Una volta colpiti da un "cavallo di Troia", è molto difficile rilevarlo. Questi virus, infatti, usano delle tecniche particolari per nascondersi e spesso si servono di strumenti avanzati per bloccare l'attività dell'antivirus. Accorgersi della loro presenza è molto difficile: non rallentano il computer e non modificano nessuna delle impostazioni visibili del sistema operativo.

Secondo passo: il keylogger

I cavalli di Troia di per sé non causano danni al computer, ma la prima cosa che fanno è installare un programma chiamato
keylogger, che è in grado di registrare tutto ciò che viene digitato sulla tastiera. I keylogger più efficienti si attivano solo quando ci colleghiamo a un sito Internet che i pirati informatici ritengono "interessante". Per esempio un portale di e-commerce o il nostro servizio di Internet banking. In questo modo hanno la certezza di catturare solo le informazioni che gli servono, senza perdere tempo a controllare un gran numero di dati per estrarre quello che gli interessa. Il keylogger registra il codice della nostra carta durante un acquisto e legge le credenziali per accedere al sito della banca, dopodiché invia i dati a chi lo ha programmato. Non servirà a nulla cambiare i codici se il nostro computer è infetto, perché tutto ciò che viene digitato sulla tastiera, sarà registrato!

Come difendersi

Come abbiamo detto prima, un trojan horse è difficile da individuare una volta installato perché sa benissimo come nascondersi e mimetizzarsi. Dobbiamo quindi evitare di installarlo,

aggiornando sempre il nostro antivirus e facendo una scansione di ogni file che ci sembra sospetto, prima di fare clic e cercare di aprirlo.

Per scoprire gli allegati di posta che si nascondono con il trucco della doppia estensione, basta
impostare Windows in modo da fargli visualizzare sempre l'estensione completa dei file. Se notiamo un file, come l'esempio riportato prima, eliminiamo immediatamente la mail.

C'è anche un trucco per essere più sicuri quando inseriamo dati sensibili all'interno di un sito. Ricordiamoci che i keylogger registrano le comunicazioni fra la tastiera fisica e il computer, se invece usiamo
la tastiera virtuale di Windows o di OS X potremmo digitare senza essere tracciati, anche in presenza di software maligno nel computer. L'utilizzo della tastiera virtuale è una buona prassi che dovremmo adottare tutte le volte che eseguiamo operazioni delicate.