Alla ricerca di immagini: attenti alla truffa

Anche una semplice ricerca di immagini su Internet può esporre ad attacchi di tipo Fraudtool. La soluzione? Secondo TG Soft occorrono un buon software antivirus, ma soprattutto prudenza e buon senso.

Il trend dell'evoluzione dei malware negli ultimi mesi vede senza dubbio una notevole crescita di fenomeni orientati a truffare gli utenti, più che a danneggiare i loro computer, in uno scenario nel quale tecniche di social engineering vengono utilizzate sempre più massivamente per questi scopi. A differenza delle tecniche di attacco tradizionali, con le quali 'chi' attacca cerca di sfondare le difese con attacchi brute force o sfruttando falle di sicurezza, le tecniche di social engineering portano l'utente stesso a garantire l'accesso a informazioni personali sensibili o addirittura al proprio computer volontariamente, naturalmente come vittima di una frode o di tranelli studiati per raccogliere informazioni sulla vittima, che possano essere utili per gli scopi della frode stessa.

I falsi antivirus (Fraudtool o Fake AV in inglese) sono un ottimo esempio dell'utilizzo di queste tecniche per riuscire a farsi consegnare volontariamente i dati della carta di credito, subendo una vera e propria truffa. Oltre al danno c'è anche la beffa di essere convinti che si sta acquistando un software per eliminare virus dal proprio computer, mentre il software stesso è un malware e il suo unico scopo è quello di acquisire numeri di carte di credito attraverso un modulo di acquisto.

Generalmente questi malware richiedono una notevole quantità di interazione da parte dell'utente, che deve scaricare il programma, eseguirlo sul suo computer e addirittura essere convinto ad acquistarlo in seguito. È proprio qui che entra in gioco il social engineering; il file malevolo, infatti, generalmente è presentato con un nome allettante, che ne invoglia l'esecuzione. Il programma stesso, poi, è graficamente curatissimo e del tutto simile a un vero antivirus, per dare quel tono di serietà e per ingenerare nell'utente un senso di fiducia e di familiarità che lo porterà ad essere più facilmente convinto a fare quello che propone il malware.

Recentemente è stato scoperto un nuovo metodo di attacco mirato, per ridurre al minimo le operazioni che l'utente deve eseguire per 'autoinfettarsi'. Questo tipo di attacco sfrutta la funzione di autoanteprima di uno dei più noti motori di ricerca, quando si utilizza la funzionalità di ricerca di immagini. Quando si clicca su un'immagine trovata tramite questo servizio, infatti, il motore di ricerca visualizza l'immagine di interesse, più l'anteprima della pagina nella quale è inserita. Alcuni domini malevoli, sfruttando questa caratteristica, utilizzano dei particolari siti che reindirizzano l'utente verso altre pagine, nel caso in cui la pagina reindirizzatrice sia raggiunta tramite l'anteprima del motore di ricerca. Se invece si dovesse raggiungere la stessa pagina direttamente tramite browser (uno qualsiasi), si viene reindirizzati verso un sito 'pulito'. Per questo motivo questi tipi di attacchi sono molto difficili da individuare e di conseguenza da prevenire.

Nel caso in cui uno di questi siti sia visitato tramite la funzione di autoanteprima del motore di ricerca, l'utente è immediatamente reindirizzato verso un dominio malevolo che propone una finta scansione al-

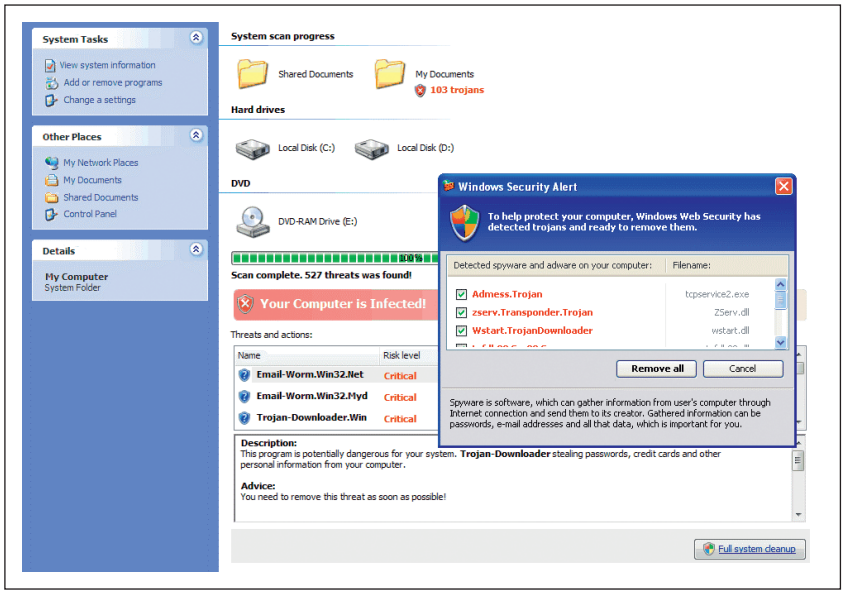

Fig. 1 - Esempio di sito malevolo che simula una scansione del computer del visitatore

l'interno del browser per attirarlo verso la trappola, ovvero scaricare il falso antivirus che viene proposto alla fine della scansione fittizia per rimuovere le minacce trovate. A seconda del browser in uso verrà visualizzata una pagina 'esca' differente, ma lo scopo sarà sempre quello di far scaricare il malware al visitatore (vedi fig. 1). Scaricare ed eseguire il file proposto porta inevitabilmente a ritrovarsi in esecuzione sul computer il classico Fraudtool (vedi Fig. 2), che impedisce l'utilizzo di qualsiasi altro programma sostenendo che sia infetto o che sia un malware e che propone l'acquisto di una fantomatica versione completa per rimuovere le minacce (inesistenti) rilevate. In questo modo, spaventando l'utente e utilizzando le sopracitate tecniche di social engineering, il falso antivirus lo porta proprio a infettare il suo stesso computer e in seguito a fornire volontariamente il proprio numero di carta di credito, credendo di acquistare qualcosa che lo aiuterà a risolvere problemi che invece proprio lui sta creando.

Proprio per le difficoltà a risalire alla fonte degli attacchi e per quanto i software antivirus come Vir.IT eXplorer, la cui versione gratuita ricordiamo essere scaricabile direttamente dal sito http://www.tgsoft.it, siano sempre aggiornati e pronti a combattere queste crescenti minacce, il ruolo dell'utente consapevole sta diventando sempre più importante. Le tecniche illustrate finora, infatti, si basano fortemente sull'interazione che l'utente deve avere con il malware affinché l'attacco vada a buon fine e lo scopo dell'attaccante sia raggiunto. Fortunatamente questi tipi di attacchi si possono prevenire agendo direttamente dal principio,

Fig. 2 - Esempio di fraudtool all'opera

utilizzando un po' di prudenza e di buon senso, ad esempio evitando di fornire il proprio numero di carta di credito al primo software sconosciuto che lo chiede oppure evitando di cliccare su ogni messaggio (o presunto tale) che può essere presentato da qualsiasi tipo di sito o software.

www.tgsoft.it

G.C.

Il NOC a garanzia dei servizi

Reti, sistemi e applicazioni sempre sotto controllo grazie al Network Operations Center di Test.

Il controllo di reti e sistemi è, per un'azienda, un'attività veramente impegnativa che richiede non solo skill elevati, ma sempre più spesso anche disponibilità H24. TEST Spa, azienda specializzata nella progettazione e fornitura di infrastrutture, soluzioni tecnologiche, prodotti e servizi nel settore ICT, ha costituito il Network Operations Center (NOC), una struttura specialistica dedicata che svolge con continuità 24x7x365 attività di monitoraggio, di controllo proattivo delle applicazioni, di gestione e supporto per i sistemi ICT dei clienti e le attività di monitoring e management dei vari servizi che TEST fornisce con la propria infrastruttura in modalità 'as a service'. La struttura, ubicata a Padova, è costituita da un team di operatori specializzati nel monitoraggio sulle principali piattaforme HW/SW, applicazioni e servizi di rete, affiancati da sistemisti certificati che operano dal livello di infrastruttura all'applicazione.

Il servizio di monitoraggio effettuato dal NOC consiste nel controllo continuativo nelle 24 ore della corretta funzionalità dell'infrastruttura di rete, server, apparati, sistemi operativi, servizi di rete, applicazioni, procedure, reti private virtuali, a supporto del servizio IT dell'azienda cliente. Tale attività permette di cogliere in tempo condizioni di errore o anomalie che possono preludere all'insorgere del disservizio e di intraprendere tempestivamente le opportune azioni correttive concordate (diagnostiche, segnalazioni, chiamate a centri di assistenza, interventi diretti di ripristino), consentendo quindi di ridurre al minimo le situazioni e i tempi di fermo utente.

www.testspa.com

A.C.R.