Nuovo attacco informatico al nostro sito

23 Maggio 2015

Nella giornata del 22 maggio 2015 abbiamo subito un nuovo attacco informatico che, nonostante le misure di sicurezza adottate, hanno oscurato il nostro sito web.

Tale oscuramento è durato poche ore avendo ripristinato in tempo record l'agibilità del sito. Purtroppo, però, sono stati cancellati alcuni file ed immagini che saranno ripristinate entro pochi giorni.

Si sente parlare molto di crimine informatico, o anche cybercrime, ma in cosa consiste esattamente? In realtà si tratta di un argomento complesso.

Analogamente al crimine tradizionale, quello informatico può assumere varie forme e essere perpetrato praticamente sempre e ovunque. I criminali che commettono questo tipo di crimini utilizzano una serie di metodi a seconda delle proprie capacità e scopi. Ciò non dovrebbe sorprendere: il crimine informatico è, dopotutto, semplice 'crimine' con l'aggiunta di qualche sorta di componente 'informatico'.

Nel trattato del Consiglio d'Europa sulla criminalità informatica viene utilizzato il termine "cybercrime" per definire reati che vanno dai crimini contro i dati riservati, alla violazione di contenuti e del diritto d'autore [Krone, 2005]. Tuttavia, altri [Zeviar-Geese, 1997-98] suggeriscono una definizione più ampia che comprende attività criminose come la frode, l'accesso non autorizzato, la pedopornografia e il "cyberstalking" o pedinamento informatico. Il manuale delle Nazioni Unite sulla prevenzione e il controllo del crimine informatico (The United Nations Manual on the Prevention and Control of Computer Related Crime) nella definizione di crimine informatico include frode, contraffazione e accesso non autorizzato [Nazioni Unite, 1995].

Come si può vedere da queste definizioni, il crimine informatico può coprire una gamma molto ampia di attacchi. È importante comprendere le differenze tra i vari tipi di crimine informatico, in quanto ciascuno richiede un approccio diverso per migliorare la sicurezza del computer.

Prendendo spunto dalle varie definizioni, Symantec descrive concisamente il crimine informatico come *un crimine commesso utilizzando un computer, una rete o un dispositivo hardware*. Il computer o il dispositivo può essere l'agente, il mezzo o l'obiettivo del crimine.Un crimine può avere luogo sul solo computer o in combinazione con altre posizioni e luoghi.Per meglio comprendere l'ampia gamma di crimine informatico esistente è possibile dividerlo in due categorie definendolo, per lo scopo di questa ricerca, come crimine informatico di Tipo 1 e di Tipo 2.

Il crimine informatico di Tipo 1 presenta le seguenti caratteristiche:

- Si tratta generalmente di un singolo evento se visto dalla prospettiva della vittima. Ad esempio, la vittima scarica inconsapevolmente un Trojan Horse che installa sul suo computer un keystroke logger, ovvero un programma che registra quanto viene digitato sulla tastiera. In alternativa, la vittima può ricevere un'e-mail contenente quello che sembra un collegamento a un sito noto, ma che è in realtà un sito ostile.
- Il crimine informatico viene facilitato da programmi crimeware quali keystroke logger, virus, rootkit o Trojan Horse.
- I difetti e le vulnerabilità dei software offrono spesso un punto di appoggio all'aggressore per perpetrare l'attacco. Ad esempio, i criminali che controllano un sito Web possono sfruttare una

vulnerabilità del browser Web per introdurre un Trojan Horse nel computer della vittima.

Esempi di questo tipo di crimine informatico includono, tra gli altri, il phishing, il furto e la manipolazione di dati o servizi tramite azioni di hacking o virus, il furto di identità e le frodi bancarie o legate all'e-commerce.

Il crimine informatico di Tipo 2 comprende attività quali il cyberstalking e le molestie, le molestie ai minori, l'estorsione, il ricatto, la manipolazione dei mercati finanziari, lo spionaggio e le attività terroristiche, ma non si limitano solo a queste.Le caratteristiche del crimine informatico di Tipo 2 sono le seguenti:

- È caratterizzato solitamente da una serie continua di eventi che prevedono ripetute interazioni con l'obiettivo.Ad esempio, la vittima viene contattata in una chat da qualcuno che, nel corso di un certo periodo di tempo, tenta di stabilire qualche tipo di relazione.Alla fine, il criminale sfrutta il legame che si è stabilito con la vittima per commettere un crimine.Un altro caso si verifica quando i membri di una cellula terroristica o di un'organizzazione criminale utilizzano messaggi in codice per comunicare in un forum pubblico e, ad esempio, pianificare attività criminose o concordare luoghi di riciclaggio di denaro sporco.
- Tali attività vengono facilitate generalmente da programmi che non rientrano nella definizione di crimeware. Ad esempio, le conversazioni possono avvenire tramite client di messaggistica istantanea e i file possono essere trasferiti mediante FTP.

Si ringraziano i "naviganti" per il disagio che si è arrecato.