Hacking e crimini informatici

Hacker nella lingua inglese sta ad indicare una persona che utilizza le proprie competenze informatiche per esplorare i dettagli dei sistemi programmabili. La parola deriva dal verbo "To hack" che indica l'attività di comporre insieme vari programmi, senza tener conto dei metodi e procedure usati nella scrittura del software "ufficiale". Lo scopo è quello di migliorare l'efficienza e la velocità del software. In realtà il verbo to hack significa tagliare, sfrondare, sminuzzare, e quindi "aprirsi un varco" fra le righe di codice che istruiscono i programmi software.

Le origini del termine risale alla seconda metà del XX secolo. Successivamente è stato utilizzato in senso generale anche per indicare individui che studiano e sperimentano la materia, per conoscerne i segreti ed analizzarla in profondità, quindi una persona esperta di informatica ed utilizza le proprie competenze per risolvere problemi Dal punto di vista informatico, non è da confondere con i cracker, o pirati informatici, il cui scopo è prettamente violare e danneggiare un sistema cui si riferisce impropriamente il mondo giornalistico con il termine *hacker*.

Un pò di storia

Nel 1958/1959, si definirono hacker un gruppo di studiosi del club del Massachussetts Istitute of Tecnology che si preoccupava di porre le basi per le comunicazioni informatiche. Nel 1961 gli hackers lavorarono per un programma che simulava la battaglia stellare, lo Spaceware, progetto molto ambizioso per l'epoca ma che mostrava la potenzialità dei calcolatori. Nello stesso anno fu inventato il primo microcomputer, il Pdp1 utile per la ricerca scientifica e per la matematica. Nel 1963, un famoso hacker Stewart Nelson scoprì che alcune note potevano essere utilizzate per entrare nel sistema telefonico e riuscì in questo modo a

mettere in comunicazione tutte le università americane. Nelson fece anche una dichiarazione importante: “per un Hacker una porta chiusa è un insulto, e una chiusa a chiave è un oltraggio”. Negli anni settanta nasce nel mondo informatico un altro hacker David Silver che già da piccolo mostrava inclinazioni verso l’informatica e la tecnologia; all’età di dieci anni Silver ideò con un’antenna radar, uno specchio parabolico con microfono in grado di captare conversazioni a centinaia di metri di distanza. Silver fondò i primi negozi informatici segreti dove si poteva acquistare ciò che serviva a pochi soldi. Iniziò l’evoluzione informatica che portò alla costruzione di macchine sempre più complesse e sofisticate.

Gli hacker in Italia

In Italia i primi hacker nacquero intorno agli anni ottanta dopo l’arrivo del Commodore 64 ed erano dotati di sani principi; si proposero infatti di non arrecare danni ai sistemi informatici che andavano ad esplorare. Il primo gruppo di hacker famoso fu DTE222 ed erano fondamentalmente di Milano. Negli anni seguenti, gli hacker italiani aumentarono tantissimo e non tutti seguirono i sani ideali e principi iniziali; un notevole gruppo indirizzò gli interessi verso atti vandalici. Un altro gruppo nel 1986, dedicò le proprie conoscenze per ideare il videotel progetto che decollò lentamente a causa di mancanza di clientela per gli alti prezzi della Sip. Fu in questo periodo che gli hacker iniziarono a pensare di violare password e username per bypassare i prezzi ed accedere al servizio gratuitamente. Gli utenti colpiti erano le grandi industrie ed evitavano di danneggiare i cittadini privati; qualche hacker riusciva ad accedere anche ad account militari americani.

Nel 1988 nacque la GARR Gruppo per ‘Armonizzazione delle Reti di Ricerca; nel 1990 con la nascita dei floppy disc, iniziò la diffusione dei primi virus che portò nel 1993 all’arresto di Joseph Lois Popp. Quest’ultimo aveva ideato un virus che bloccava i pc dopo 90 accensioni;

una delle peggiori conseguenze fu la cancellazione di 10 anni di dati dell'università di Bologna.

Il crimine informatico

Il crimine informatico è un abuso che coinvolge l'informazione in tutte le sue parti hardware e software. Per crimini informatici si intende l'accesso non autorizzato, l'intercettazione e la trasmissione di dati, il danneggiamento, deterioramento o cancellazione ed interferenza di dati, l'uso improprio di dispositivi e i reati, il furto di identità, la pirateria o la diffusione di materiale illecito.
Dal 2017 i crimini informatici sono aumentati in tutto il mondo colpendo oltre un miliardo di persone e causando danni per oltre 500 miliardi di dollari.
Gli attacchi informatici avvengono spesso tramite software detti in generale malware che vengono spesso chiamati virus. In realtà i malware vengono classificati nel seguente modo:

- Virus: sono parti di codice che si diffondono copiandosi all'interno di altri programmi, o in una particolare sezione del disco fisso, in modo da essere eseguiti ogni volta che il file infetto viene aperto. Si trasmettono da un computer a un altro tramite lo spostamento di file infetti ad opera degli utenti.
- Worm: questi malware non hanno bisogno di infettare altri file per diffondersi, perché modificano il sistema operativo della macchina ospite in modo da essere eseguiti automaticamente e tentare di replicarsi sfruttando per lo più Internet. Per indurre gli utenti ad eseguirli utilizzano tecniche di ingegneria sociale, oppure sfruttano dei difetti (Bug) di alcuni programmi per diffondersi automaticamente. Il loro scopo è rallentare il sistema con operazioni inutili o dannose.
- Trojan horse: software che oltre ad avere delle funzionalità "lecite", utili per indurre l'utente ad utilizzarli, contengono istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore. Non possiedono

funzioni di auto-replicazione, quindi per diffondersi devono essere consapevolmente inviati alla vittima. Il nome deriva dal famoso cavallo di Troia.

- Backdoor: letteralmente "porta sul retro". Sono dei programmi che consentono un accesso non autorizzato al sistema su cui sono in esecuzione. Tipicamente si diffondono in abbinamento ad un trojan o ad un worm, oppure costituiscono una forma di accesso lecita di emergenza ad un sistema, inserita per permettere ad esempio il recupero di una password dimenticata.
- Spyware: software che vengono usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato. Le informazioni carpite possono andare dalle abitudini di navigazione fino alle password e alle chiavi crittografiche di un utente.
- Dialer: questi programmi si occupano di gestire la connessione ad Internet tramite la normale linea telefonica. Sono malware quando vengono utilizzati in modo illecito, modificando il numero telefonico chiamato dalla connessione predefinita con uno a tariffazione speciale, allo scopo di trarne illecito profitto all'insaputa dell'utente.
- Hijacker: questi programmi si appropriano di applicazioni di navigazione in rete (soprattutto browser) e causano l'apertura automatica di pagine web indesiderate.
- Rootkit: i rootkit solitamente sono composti da un driver e a volte, da copie modificate di programmi normalmente presenti nel sistema. I rootkit non sono dannosi in sé, ma hanno la funzione di nascondere, sia all'utente che a programmi tipo antivirus, la presenza di particolari file o impostazioni del sistema. Vengono quindi utilizzati per mascherare *spyware* e *trojan*.
- Scareware: non sono altro che porte di accesso che si nascondono sui manifesti pubblicitari e installano altri malware e spesso c'e il pericolo che facciano installare malware che si fingono antivirus tipo il famoso "rogue antispyware".
- Rabbit: i rabbit sono programmi che esauriscono le risorse del computer creando copie di sé stessi (in memoria o su disco) a grande velocità.
- Adware: programmi software che presentano all'utente messaggi pubblicitari durante l'uso, a fronte di un prezzo ridotto o nullo.

Possono causare danni quali rallentamenti del PC e rischi per la privacy in quanto comunicano le abitudini di navigazione ad un server remoto.

- Malvertising: malicious advertising, sono degli attacchi che originano dalle pubblicità delle pagine web.
- File batch: hanno estensione ".bat". I file batch non sono veri e propri malware, ma solo semplici File di testo interpretati da Prompt dei comandi di microsoft windows. In base ai comandi imposti dall'utente, il sistema li interpreta come "azioni da eseguire", e se per caso viene imposto di formattare il computer, il file esegue l'operazione imposta, perché eseguire i file inoltrati al processore è un'operazione di routine. Questo rende i file batch pericolosi. I file batch sono spesso utilizzati nel ciberbullismo.
- Keylogger: I Keylogger sono dei programmi in grado di registrare tutto ciò che un utente digita su una tastiera o che copia e incolla rendendo così possibile il furto di password o di dati che potrebbero interessare qualcun altro. La differenza con gli Adware sta nel fatto che il computer non si accorge della presenza del keylogger e il programma non causa rallentamento del pc, passando così totalmente inosservato. Generalmente i keylogger vengono installati sul computer dai trojan o dai worm, in altri casi invece il keylogger viene installato sul computer da un'altra persona che può accedere al pc o attraverso l'accesso remoto (che permette a una persona di controllare un altro pc dal suo stesso pc attraverso un programma) oppure in prima persona, rubando così dati e password dell'utente. Esistono anche i Keylogger Hardware, che possono essere installati da una persona fisica, e poi, sfruttando la rete Internet inviano informazioni al malintenzionato quali password, email, ecc...
- Rogue antispyware: malware che si finge un programma per la sicurezza del PC, spingendo gli utenti ad acquistare una licenza del programma.
- Ransomware Virus che cripta tutti i dati presenti su un disco, secondo una chiave di cifratura complessa; poi, per ottenerla e decrittografare il computer, bisogna pagare il cracker che ha infettato il pc e quindi ottenere la chiave di cifratura per "tradurre" i dati. Questi software sono pericolosi in modo direttamente proporzionale alla quantità e

alla riservatezza dei dati presenti sul disco. Una volta questi virus erano presenti in Windows con diffusione ristretta, mentre oggi la diffusione è aumentata, anche su sistemi operativi mobili.

- "A comando", cioè vengono attivati secondo le volontà del cracker nel momento che ritiene opportuno.
- "Automatici", che si dividono in altre due sottocategorie:
  - "Da esecuzione", cioè vengono eseguiti e quindi si attivano quando l'utente li avvia;
  - "Da avvio", cioè si attivano quando si spegne/accende il device.
- Bomba logica: è un tipo di malware che "esplode" ovvero fa sentire i suoi effetti maligni al verificarsi di determinate condizioni o stati del PC fissati dal cracker stesso.
- Bomba a decompressione è un file che si presenta come un file compresso. Deve essere l'utente ad eseguirlo. All'apparenza sembra un innocuo file da pochi Kilobyte ma, appena aperto, si espande fino a diventare un file di circa quattro Petabyte, occupando quindi tutto lo spazio su disco rigido.