

## Relazione del dott. Roberto Paleari

(Membro della squadra che ha vinto nel 2008 i campionati mondiali di Hacking. Attuale esperto per la Sicurezza e Reti del Dipartimento di Informatica e Comunicazione dell'Università degli Studi di Milano)

### “IL BISCOTTO PREFERITO DI UN HACKER (confessioni un “pentito”)

Martedì 30 novembre 2010



La parola hacker è un termine risalente agli anni Settanta che, inizialmente, era collegato ad un complimento piuttosto che a qualcosa di dispregiativo: gli hacker erano quelle persone esperte in un determinato settore (non necessariamente di quello informatico) che volevano dimostrare le proprie competenze e le proprie capacità tecniche. Nel corso degli anni, soprattutto a causa della pubblicità negativa fatta dai media, ha assunto una connotazione negativa andando ad indicare un criminale informatico.

Al giorno d'oggi, nel settore dell'informatica si fa riferimento a due classi di hacker:

> i cosiddetti “*Black hat*” che sono i “cattivi” perché conducono attività illegali, tra questi si annoverano i veri e propri criminali informatici (quelli che ad esempio “bucano” i sistemi informatici delle banche per fare soldi) e gli autori di malware (virus, worm ecc ...) da diffondere su Internet;

> e i “*White hat*” che sono i “buoni”. Sono esperti di sicurezza che lavorano per aziende o enti di ricerca il cui obiettivo è quello di cercare di violare la sicurezza dei sistemi ma non a scopi illeciti quanto per poi sviluppare nuovi sistemi di protezione e di difesa.

Il mondo dell'hacking è cambiato molto negli ultimi anni, perché da attività non organizzata né coordinata (“hack for fun”) il crimine informatico è diventata un'attività molto complessa connessa ad organizzazioni criminali con fine di lucro (“hack for profit”).

### Aspetti di sicurezza in Internet

Dal 2002 al 2009 si è verificata una crescita esponenziale dei crimini commessi su Internet motivata dalla possibilità di lucro. Oggi i crimini informatici sono attività molto redditizie tali da coinvolgere molte persone che investono del denaro in queste attività.

Come si fa a “fare soldi” su Internet e come sono organizzati i crimini informatici? Semplificando al massimo il fenomeno la situazione è questa: da computer infetti vengono inviati messaggi di posta indesiderata (“spam”) con l'obiettivo di fare in modo che l'utente clicchi sul collegamento in essi contenuto indirizzandolo ad una risorsa che contiene contenuto maligno che viene scaricato infettando a sua volta il computer dell'utente che, inconsapevole, compie attività illecite su istruzione del malware che vi si è insinuato.

I gestori dei grandi provider stimano che il 90% dei messaggi che circolano è posta indesiderata.

L'obiettivo è dunque quello di sottrarre dal computer infetto tutta una serie di informazioni (dati sensibili riferiti a conti correnti, numero della carta di credito, ecc...) e poi di rivenderle sul mercato nero oppure di attivare vere e proprie compravendite di macchine infette e di sistemi compromessi.

Quali sono gli obiettivi di un attaccante, di un hacker cattivo?

1. massimizzare il numero di sistemi compromessi, per rubare il maggior numero di informazioni e, conseguentemente, ricavare denaro sia dall'affitto di macchine infette sia dalla vendita di informazioni;

2. massimizzare la durata dell'infezione per mantenere il più a lungo possibile il controllo della macchina infetta ed evitare che qualcun altro possa “rubarla”.

## **Come si fa ad infettare una macchina?**

Il metodo più diffuso per infettare un computer è attraverso il **phishing**: siti fasulli appositamente predisposti che assomigliano in tutto e per tutto ad un sito reale con l'obiettivo di rubare le credenziali del conto.

Un'altra tipologia di truffa è lo **scam**. È una lieve variante del phishing, in cui arrivano dei messaggi di posta elettronica che cercano di vendere prodotti (nella maggior parte dei casi viagra, cialis, copie di orologi Rolex, ...) col fine di far inserire all'acquirente il numero di carta di credito per poi prelevare dalla stessa denaro.

Oggi, però, la tendenza per assumere il controllo di molte macchine è quella di compromettere dei siti famosi. Gli hacker riescono a modificare il codice sorgente di un sito in modo tale che tutte le persone che visitano il sito e hanno sul proprio PC un sistema vulnerabile (non protetto) possano essere infettate da **malware**. Il malware è dunque una sequenza di codice progettata per danneggiare intenzionalmente un sistema, i dati che contiene o comunque alterare il suo normale funzionamento, all'insaputa dell'utente.

## **I Captcha**

La posta indesiderata consiste in messaggi pubblicitari contenenti link maligni. Per inviarla è necessario attivare indirizzi mail creati appositamente da criminali informatici con nomi casuali e fasulli. Per evitare questo problema di creazione di indirizzi mail fasulli, sono stati introdotti i Captcha, immagini con scritte poco nitide e distorte che solo l'occhio umano è in grado di decifrare. Questo significa che per poter registrare un nuovo indirizzo di posta è necessario decifrare l'immagine e digitarla manualmente nell'apposito spazio.

Gli hacker, in teoria, non dovrebbero più essere in grado di registrare automaticamente indirizzi di posta elettronica per effettuare lo spamming. In realtà sono nate delle società il cui business è basato proprio sulla risoluzione dei captcha, dove delle persone passano tutto il giorno a risolverli fornendo, a pagamento, le soluzioni agli hacker che ne fanno richiesta. Per ovviare al pagamento è anche stato inventato un sistema assai originale che prevede la risoluzione dei captcha in forma gratuita. Sono gli stessi utilizzatori dei siti pornografici che per passare da un'immagine all'altra digitano il captcha inconsapevoli di fornire un "servizio" agli hacker.

## **I Social network**

L'utilizzo dei social network espone gli utenti ai pericoli tecnologici sopraesposti quali il phishing, lo spamming e il cosiddetto Likejacking. Ma anche la privacy dei dati personali è a rischio: Facebook, ad esempio, tratta una quantità enorme di informazioni sensibili, ma sono pochissimi gli utenti che sono a conoscenza del trattamento di questi dati personali; basti pensare che l'accordo di apertura di un profilo Facebook è più lungo della costituzione americana. E nessuno lo legge... Vi è un vero e proprio trasferimento di diritti su informazioni e foto che diventano così di pubblico dominio.

Il Likejacking (termine che corrisponde al pulsante "Mi piace" di facebook per condividere un determinato contenuto) è un sistema che invia spam con link dal contenuto maligno. Una volta aperta, la pagina esegue un codice equivalente ad un click su "Mi piace". L'obiettivo? Pubblicità! Questo fa sì che il sito visitato compaia tra le prime inserzioni pubblicitarie visto l'alto (fasullo) gradimento ottenuto.

## **I Giochi on-line**

Sempre più diffusi, i giochi online non garantiscono però l'equità del gioco stesso perché manca un vero e proprio garante al di sopra delle parti che vigili sulla correttezza dello svolgimento. Durante una partita di videopoker, ad esempio, dietro pagamento, è infatti anche possibile vedere in anticipo le mani degli avversari.

Altre truffe con i giochi online sono i virus camuffati da programmi per giocare a poker gratuitamente che, comunque, richiedono il numero di carta di credito e poi scambiano i dati con un complessa rete di affiliati.

## **La sicurezza nelle reti locali**

Le reti wireless, proprio perché senza fili, possono esporre l'utilizzatore ad una serie di pericoli perché chiunque si trova all'interno dell'area di copertura può collegarsi alla rete all'insaputa del proprietario! Nei casi più gravi vengono commesse attività illecite su Internet in modo anonimo ed è molto difficile accorgersi e risalire all'intruso.

Fondamentale diventa quindi proteggere e “chiudere a chiave” la rete. Con una chiave segreta per la cifratura del traffico solo chi la conosce può collegarsi alla rete.

Le reti protette possono comunque essere esposte ad attacchi con tentativi di autenticazione con chiavi diverse soprattutto se la chiave è semplice.

### **La sicurezza nelle reti mobili**

I telefoni cellulari di terza generazione sono dei veri e propri PC tradizionali che permettono l'installazione di applicazioni aggiuntive e che sono dunque soggetti ad attacchi informatici proprio come i computer. Esempi ne sono i giochi con inclusi malware che effettuano chiamate internazionali o comunque non autorizzate, oppure l'accesso da parte di terzi ai dati (foto, numeri della rubrica, video, ecc..) contenuti nel cellulare. Come per i computer, anche i telefoni cellulari devono quindi essere protetti con sistemi di difesa.

### **Conclusioni**

L'elettronica è in definitiva un campo libero per gli hacker che potrebbero addirittura controllare i sistemi elettronici delle automobili e aggirarne i controlli di sicurezza con conseguente controllo dei freni, del cruscotto, ecc... e “attaccare” anche quei Pacemaker controllabili via radio regolando o spegnendo da remoto il dispositivo!

Perché tanti problemi?

1. C'è poca consapevolezza degli aspetti legati alla sicurezza.
2. La sicurezza costa, e non ha un ritorno immediato.
3. Il mercato spinge per anticipare il rilascio dei prodotti.
4. Sono forti gli incentivi economici a compiere attività illecite.

Oggi il crimine informatico è un business; le nuove tecnologie hanno prodotto nuovi problemi e nuove minacce.

Serve dunque una maggiore conoscenza e attenzione al problema attraverso un minimo di formazione perché conoscere i problemi è già un importante passo avanti!

*Altre informazioni relative alla conferenza si trovano sul sito [www.tangram.it](http://www.tangram.it)*