[BACKDOOR]

Una **backdoor** è un metodo, spesso segreto, per bypassare la normale autenticazione in un prodotto, un sistema informatico, un crittosistema o un algoritmo.

Le backdoor sono spesso scritte in diversi linguaggi di programmazione e hanno la funzione principale di superare le difese imposte da un sistema, come può essere un firewall, al fine di accedere in remoto a un PC.

In questo modo si può ottenere per mezzo di un sistema di crittografia un'autenticazione prendendo il completo o parziale possesso del computer ‘vittima’.

Una backdoor può celarsi segretamente all'interno di un programma di sistema, di un software separato, o può anche essere un componente hardware malevolo come: apparati di rete, sistemi di sorveglianza e alcuni dispositivi di comunicazione che possono avere celate al loro interno backdoor maligne permettendo l'intrusione di un eventuale criminale informatico (craker).

[UTILIZZI]

In alcuni casi sono volute e create appositamente, per esempio da un gestore di sistema informatico (amministratori di rete o sistemista) permettendo una più agevole opera di manutenzione dell'infrastruttura informatica, agendo sul sistema software del computer da remoto oppure per ripristinare password dimenticate dagli utenti.

Tuttavia alcune password di default, possono funzionare da backdoor se non vengono fatti i giusti controlli e le appropriate modifiche di sicurezza, così come alcune funzionalità di debugging possono anche agire come falla per aggirare il sistema se non vengono rimossi nella versione ufficiale.

I requisiti di una backdoor sono:

- Trasparenza, cioè la capacità di eseguire comandi senza che l'utente principale se ne accorga e fixi il problema;
- Versatilità, cioè la capacità di superare diversi sistemi di sicurezza.

[STRATEGIE DI ATTACCO]

Vi sono diversi tipi di attacchi:

- Port binding - rivela dove e come i messaggi vengono trasmessi e consegnati all'interno della rete.

- Connect-back - consente una connessione dai server alla piattaforma ‘vittima’ attraverso porte non protette dal firewall.

- Connect availability use - implica l'uso di diversi campioni di malware per violare la rete e che non sono individuabili per molto tempo. Questo permette agli hacker maggiori possibilità di rubare dati sensibili al bersaglio. Il primo malware o "prima linea backdoor", funge da piattaforma per scaricare il secondo, la "seconda linea di backdoor", che esegue il furto effettivo di informazioni.

- Legitimate platform abuse - In questa strategia, i criminali informatici abusano di una piattaforma valida ben consolidata come potrebbe essere un blog e lo utilizzano per la memorizzazione dei dati inviata dal server malevolo precedentemente creato per l'attacco o in questo caso raccolta informazioni.