

*Come può, l'aggiunta di una semplice periferica, permettere ad un hacker di accedere ai dati contenuti all'interno di un computer connesso ad Internet? Se il sistema operativo è XP e se è attivo il servizio "Universal Plug and Play Device Host" allora è possibile*

Mi ricordo la prima volta che si è parlato di plug n' play: un meccanismo standard per l'installazione di nuove periferiche. Ripensando al tempo perso, in ambiente DOS, nell'installare una scheda di rete o una scheda sonora, questo nuovo modo di lavorare rendeva molto più comodo ed efficace qualsiasi aggiornamento hardware. Il tempo passa e passando da un'evoluzione all'altra, ecco spuntare nei nostri computer un nuovo meccanismo: UPnP, acronimo di Universal Plug and Play.

### UPNP: DI COSA SI TRATTA

Questo meccanismo di riconoscimento delle periferiche si basa su un semplice concetto: se esiste una periferica di rete compatibile a UPnP è possibile configurarla ed utilizzarla appena una macchina viene connessa ad una rete.

L'effetto di questo meccanismo è quello di poter utilizzare da subito delle periferiche presenti in rete, senza doverle forzatamente cercare. Tutti sappiamo però che, dove c'è un automatismo, c'è sempre qualcuno che prova a sfruttarlo a proprio fine...

### DEFAULT O NON DEFAULT

UPnP è un meccanismo che trova la sua implementazione in numerosi sistemi operativi Microsoft. Windows 98 e 98SE lo in-



## PLUG N'... PRAY!

stallano solo a richiesta, Windows ME lo installa, ma di default non lo attiva, Windows XP lo installa e lo attiva. L'attivazione di default ha solleticato la mente di alcune persone che si sono subito date da fare per verificare l'effettiva stabilità di UPnP e ovviamente hanno scoperto alcuni problemi.

La prima scoperta è stata quella di capire come poter provocare un buffer overflow tramite un pacchetto TCP/IP. Questo tipo di errore permette, ad una persona con le giuste conoscenze, di eseguire dei programmi nella macchina dov'è avvenuto tale errore.

Il secondo problema scoperto è legato invece al protocollo che si occupa di scoprire queste periferiche: SSDP, acronimo di Simple Service Discovery Protocol.

SSDP manda, tramite TCP/IP, un pacchetto UDP in broadcast. Teoricamente le macchine in grado

di rispondere a SSDP, rispondono a tale macchina avvisando la disponibilità di una certa risorsa.

Il problema in questo caso è dato dal fatto che è possibile creare un pacchetto UDP di risposta, da mandare alla macchina che ha un servizio UPnP attivo, che avvisa che una certa macchina ha delle risorse utilizzabili. Ipotizziamo che un certo hacker sia in grado di trovare alcune macchine con UPnP attivo e di confezionare ad arte dei pacchetti UDP contenenti l'indirizzo di una certa macchina presente in rete: ecco che è stato appena realizzato un DDoS, cioè un attacco distribuito.

### E ORA COME FACCIAMO?

La cosa più veloce che si possa fare è quella di disabilitare il servizio UPnP dalle vostre macchine; fatta questa semplice operazione, passate subito ad aggiornare la vostra versione di Windows, lanciando la procedura di Windows Update e scaricando gli aggiornamenti consigliati.

Una volta riavviata la macchina potete riattivare il servizio UPnP, sempre che ne sentiate l'esigenza, o lasciare il servizio disabilitato e riattivarlo solo quando se ne presenti l'occasione.

Per chi volesse approfondire il discorso consiglio di recarsi nel sito dell'azienda che ha trovato il problema: <http://www.eeye.com/html/Research/Advisories/AD20011220.html>; alle persone più pigre consiglio invece di scaricare "UnPlug n' Pray", un tool visuale in grado di disabilitare UPnP: <http://grc.com/UnPnP/UnPnP.htm>; infine, agli smettoni consiglio di cercare e scaricare XPl0it.c di Gabriel Maggiotti, un tool per "verificare" il problema.