Il worm Code Red

Simone Bassani
sbassani92@gmail.com

Simone Falvo
smvfal@gmail.com

Indice

1 Introduzione

2 Dettagli incidente

3 Diffusione e sistemi coinvolti

4 Conseguenze e impatto economico

I principali effetti del worm Code Red furono il degradamento delle prestazioni e la perdità di stabilità dei sistemi coinvolti. Il costo globale complessivo stimato fu di 2.6 miliardi di dollari [fonti: Sans, Computereconomics] , di cui 1.1 miliardi impiegati nell'ispezione ed il recupero dei server ed i restanti 1.5 miliardi riguardarono le perdite di produttività a seguito dell'indisponibilità dei sistemi. Quest'ultimi comprendevano non soltanto le macchine server degli utenti finali, ma anche vaste porzioni dell'infrastruttura di rete che furono completamente disabilitate, molte compagnie provider di dispositivi di rete sperimentarono un'indisponibiltà media di ben 36 ore [fonte Sans institute].
Il processo di propagazione del worm ha generato un'enorme quantità di pacchetti. Sebbene il volume di questi pacchetti era relativamente piccolo rispetto al normale traffico di rete, l'ingente quantità ha causato congestionamento e gravi problemi ad alcuni ruoter, specialmente quelli con risorse limitate. Per esempio, a causa della generazione randomica degli indirizzi IP, molti pacchetti non venivano inoltrati poiché la destinazione risultava sconosciuta, finendo così per riempire le cache ARP, esaurire la memoria e provocare il riavvio dei dispositivi [fonte-cisco].
La figura X mostra il costo complessivo di Code Red in relazione agli incidenti più rilevanti del periodo [fonte-computereconomics].

5 Contromisure

6 Conclusioni

Riferimenti bibliografici

[1] James F. Kurose & Keith W. Ross: *Reti di calcolatori e internet. Un approccio top-down.* Pearson (2013)