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 [1, 2], 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 [2].
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 [3].
La figura 1 mostra il costo complessivo di Code Red in relazione agli incidenti più rilevanti del periodo [1].

Analysis by Incident

Year	Code Name	Worldwide Economic Impact ($ U.S.)	Cyber Attack Index
2001	Nimda	$635 Million	0.73
2001	Code Red(s)	2.62 Billion	2.99
2001	SirCam	1.15 Billion	1.31
2000	Love Bug	8.75 Billion	10.00
1999	Melissa	1.10 Billion	1.26
1999	Explorer	1.02 Billion	1.17

Figura 1: Confronto danno economico

Il sito web della Casa Bianca riuscì ad evitare conseguenze sostanzialmente "disattivando" l'indirizzo IP bersaglio dell'attacco DDoS, ovvero reindirizzando tutte le richieste non malevole verso altri indirizzi associati, questo è stato possibile perché il worm è stato progettato per inviare traffico verso un unico indirizzo IP, invece dell'intero blocco di indirizzi relativi al dominio della Casa Bianca.

5 Contromisure

6 Conclusioni

Riferimenti bibliografici

[1] *"Malicious Code Attacks Had $13.2 Billion Economic Impact in 2001."* Computer Economics. September, 2002
https://www.computereconomics.com/article.cfm?id=133

[2] Schauer, Renee C.. *"The Mechanisms and Effects of the Code Red Worm."* Sans Institute. 2001
https://www.sans.org/reading-room/whitepapers/dlp/the-mechanisms-and-effects-of-the-code-red-worm-87

[3] *"Code Red Worm - Customer Impact."* Cisco. July 20, 2001
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010720-code-red-worm