LOGIC BOMB

MONICA VENTURELLI

Logic bomb

- Sono formate da una porzione di codice che si attiva in determinate condizioni
  - Presenza/assenza di alcuni file
  - Una particolare data
  - Uno specifico utente che usa il programma

Logic bomb

- Possono essere contenute all'inteno di singoli programmi o di software dannosi (virus-worm)
- Rimangono ignote fino a quando non vengo attivate
  - Cancellano o modificano file e dati
  - Bloccano l'intero sistema
- Una particolare tipo di bomba logica è la bomba a tempo

Bomba a tempo

- Si attiva in un determinato momento
  - Data o ora prefissata
- Disattiva tutto il funzionamento del programma
- La prima è stata scritta in Scribe

Il 20 marzo 2013 fu lanciato un attacco informatico contro la Corea del Sud ed una bomba logica colpì i computer cancellando il contenuto dei rispettivi dischi di almeno 3 banche e 2 società di media. Symantec dichiarò che il malware conteneva un componente capace di colpire anche i sistemi Linux.

Nel mese di febbraio del 2000 Tony Xiaotong fu accusato di aver inserito una bomba logica nel sistema della ditta per cui lavorava, la Deutsche Morgan Grenfell. La bomba, inserita nel 1996, avrebbe dovuto attivarsi il 20 luglio 2000 ma altri programmatori dell'azienda la scoprirono prima che "esplodesse". Per ripulire il sistema occorsero diversi mesi.

Il 29 ottobre 2008 una bomba logica fu scoperta nei sistemi di Fannie Mae. La bomba era stata inserita da Rajendrasinh Babubhai Makwana, un cittadino Indiano che lavorava presso la sede di Urbana, in Maryland. La bomba era stata programmata per attivarsi il 31 gennaio 2009 ed avrebbe potuto colpire tutti i 4.000 server di Fannie Mae. Makwana era stato licenziato il 24 ottobre 2008 ed aveva progettato di inserire la bomba nella rete di computer prima che il suo account fosse cancellato. Makwana fu processato e condannato a 41 mesi di prigione il 17 dicembre 2010.