Sécurité - CM

19 septembre 2018

1 Introduction

Adresse du prof : j2m@unistra.fr.

1.1 Historique

- 1988, Ver morris, exploitation d'une faille de sendmail et de la commande finger sur UNIX ($\approx$ 6000 (10%) machines contaminées).
- Travail pour résoudre le problème $\Rightarrow$ Création du CERT (Computer Emergency Response Team).
- Années 90 :
  - Démocratisation d'internet
  - Kevin Mitnick est le 1er hacker recherché par le FBI
  - Premières exploitations de vulnérabilités par dépassement de tampon, injection SQL, XSS.
- Début 2000 :
  - Apparition de DDOS et des premiers botnets
  - Premiers vers informatiques (I Love You, Code Red, ...)

1.2 Industrialisation

- Cybercriminalité
  - Apprition de gangs de hacker, notamment dans les pays de l'Est.
  - Organisations criminelle sévissent sur Internet.
    - Ex : Silk Road fermé en 2013 par le FBI (vente drogue et arme)
    - Ex : rançon logiciels (ransomware)
  - Pertes estimés à plusieurs centaines de millions d'euros par an
    - Agissent à partir de paradis numérique
  - Commerce d'armes d'intrusion ou de destruction numérique
    - Ex : location de botnets, achat de 0-day