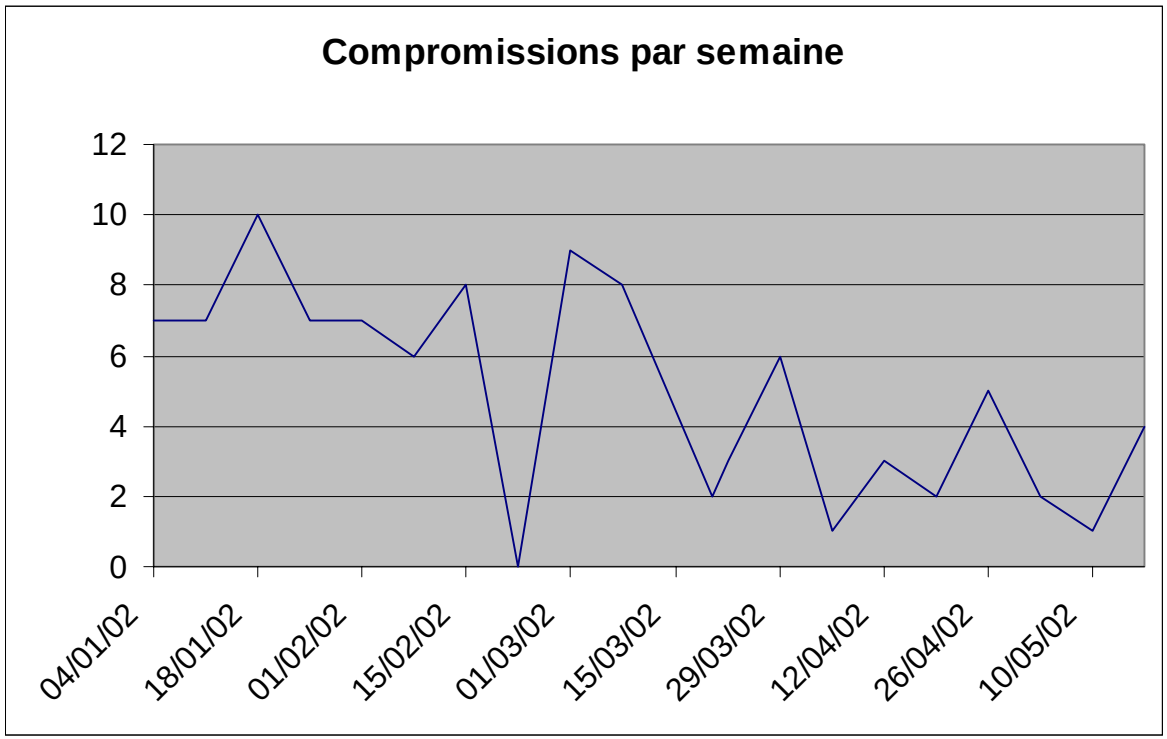
RéSIST

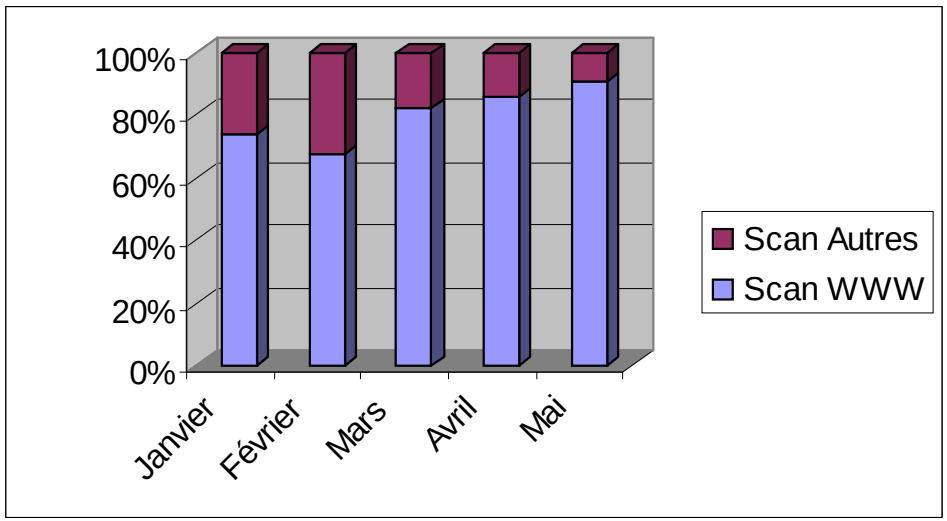
Tour d ’horizon

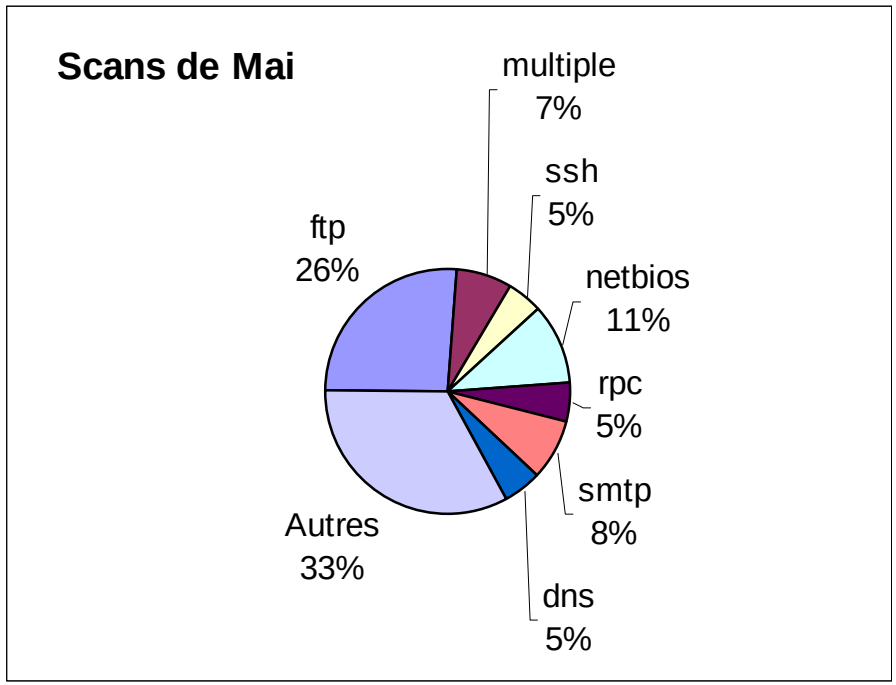
- Statistiques
- Agressions
  - Faille, Virus/Ver, Rootkit/Trojan
- Utiles
  - Outil, service WWW, jugement
- Mini-thème
- Actualités

Statistiques : compromissions

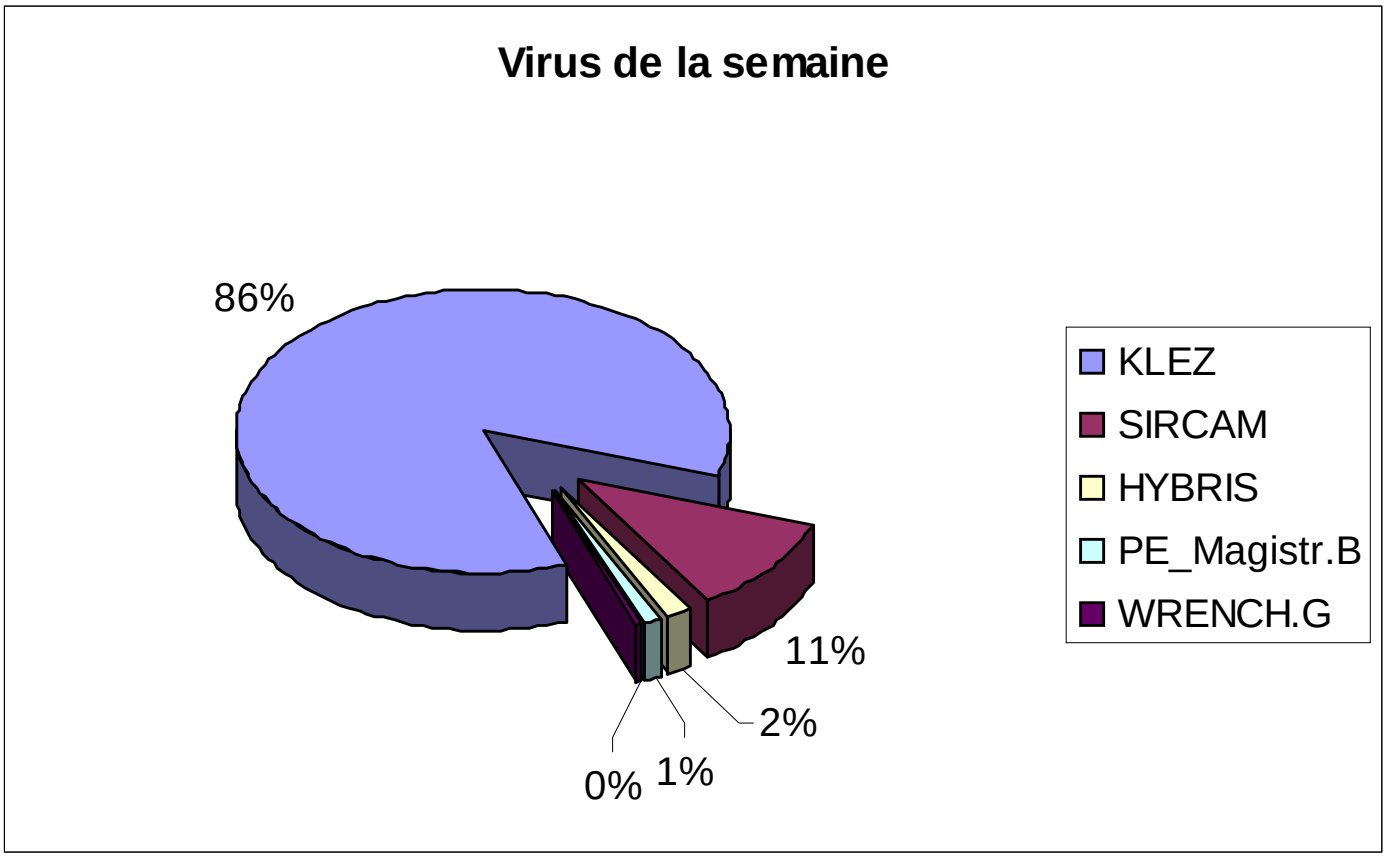


Statistiques : Scans





Statistiques : virus



Agressions

Faille : MS-SQL

Virus/Ver : KLEZ

Rootkit/Trojan : Optic Kit

Faille : MS-SQL

- OS : Microsoft
- Logiciel SQL Server 6.5 7.0 et 2000
- Conditions :
  - authentification en « mixed mode »
  - pas de mot de passe pour le « service account »
- Principe :
  - exécution distante de SQL XP_CMSHELL

Faille : MS-SQL

- Utilisation
  - Un ver existe et se propage très rapidement
- Parades
  - Bloquer le port 1433 sur les pare-feux
  - Mettre un mot de passe au compte SA

Source CERT-A

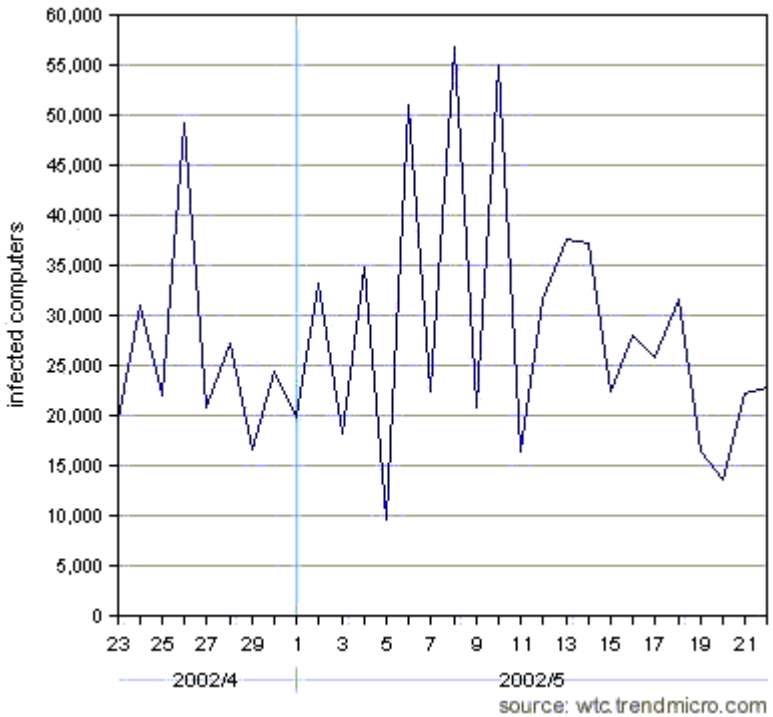
Virus/Ver : KLEZ

- Nom : KLEZ
- Découvert 17 avril 2002
- Type : Virus + Ver
- Nombreuses variantes : KLEZ.I
- Propagation par
  - email (carnet d ’adresses, fichiers divers dont html)
  - partage réseau

Virus/Ver : KLEZ

- Spécificités :
  - Email d ’expéditeur dans le carnet d ’adresses
  - SMTP embarqué
  - Désactivation des antivirus
- Actions
  - Destruction de documents

Virus/Ver : KLEZ



RootKit : Optic Kit

- Nom : Optic kit (tux)
- Découverte : 22 Jan 2002 ?
- Symptômes
  - Répertoire /dev/tux
  - Port ouvert 14859
  - Login console impossible
- ircd, stacheldrath, sshd, synscan, ps modifié

Utiles

Outil : honeyd

Serveur WWW : www.dshield.org

Economie & Loi : Ecole de Chimie

Outil : Honeyd

- Programme de création d'un honeynet
  - Plusieurs machines
  - Plusieurs OS (En fingerprint nmap uniquement)
- Manque de maturité
  - Simulation de services insuffisante (2 scripts)
- http://www.citi.umich.edu/u/provos/honeyd

Serveur WWW : Dhield

- http://www.dshield.org
  - Base de données de scans en ligne
  - Indique si un site a déjà été agresseur
  - Fournit un client pour de nombreux systèmes
  - Nombreuses statistiques

RéSIST

Economie & Loi

- Retour sur le jugement de l ’école de Chimie
  - Administrateurs condamnés MAIS :
  - Autorisation pour des besoins de services
  - Interdiction de communiquer les informations
  - ***Un jugement n’est <u>jamais</u> définitif***

RéSIST

Le mini-thème

La presse UnderGround

RéSIST

Les revues underground

- Phénomène récent en France 2 ans
- 4 types
  - Sensationnel ou décalé
    - NetBug,Virus, Zataz
  - Sensationnel/Pirate
    - Hacker Magazine,Le journal du pirate, Pirate Mag'
  - Pirate
    - Hackerz voice (et surtout le HS)
  - Sécurité
    - MISC

RéSIST

Les revues underground

- Hackerz Voice
  - Groupe DMPFRANCE
  - Mensuel, n°10, 3€
  - Hors Série 5,90€ Bimestriel n° 6
  - Pirate : une « hackademy »
  - Codes utilisables directement
  - Le « niveau » est en augmentation régulière
  - http://www.hackerzvoice.com

RéSIST

Les revues underground

- Virus Magazine
  - Editeur ACBM
  - Trimestriel, n° 19, 2€
  - Canard enchaîné de l ’informatique
  - http://www.acbm.com

Les revues underground

- Pirate Mag ’
  - Editeur ACBM
  - Trimestriel, n° 10, 2€
  - Pirate
  - http://www.acbm.com

Les revues underground

- Hacker news magazine
  - Editeur Hagal Aria
  - Trimestriel, n°5, 2€
  - Mi sensationnel/ Mi pirate
  - http://www.hackermag.com

Les revues underground

- Le journal du Pirate
  - Editeur Hagal Aria
  - Bmestriel, n°1, 2.99€
  - Mi sensationnel/ Mi pirate

RéSIST

Les revues underground

- NetBug
  - Groupe Posse Presse
  - Bimestriel, n°4, 2€
  - Sensationnel
  - http://www.posse-press.com

RéSIST

Les revues underground

- MISC
  - Groupe Diamond Editions (Linux Mag)
  - Trimestriel, n°2, 7,45€
  - Orienté sécurité
  - Articles complets, souvent originaux
  - Inutilisable pour un « script kiddy »
  - http://www.miscmag.org

RéSIST

Actualités : REMIP 2000

RéSIST

Actualités : REMIP 2000

- Réseau de Recherche & d ’Enseignement Toulousain
- 37 Sites
- Tout optique
- Anneau Gigabit
- Connexion 1Gbit/s ou 100 Mbit/s