Introduction aux antivirus et présentation de ClamAV

Un antivirus libre pour un système libre

Antoine Cervoise

ClamAV : http://www.clamav.net/

Plan

- Le monde des malwares
  - Historique
  - Les logiciels malveillants
  - Nouvelles tendances et actualités
- La réponse des antivirus
  - Fonctionnement des antivirus
  - Pourquoi avoir un antivirus sous Unix
  - ClamAV
  - Les limites

Plan

- Le monde des malwares
  - Historique
  - Les logiciels malveillants
  - Nouvelles tendances et actualités
- La réponse des antivirus
  - Fonctionnement des antivirus
  - Pourquoi avoir un antivirus sous Unix
  - ClamAV
  - Les limites

Un peu d'histoire

- Théorie
  - Années 40
- Premier virus/vers
  - Années 60
- Première utilisation du terme « virus informatique »
  - 1986
- Apparition des premiers botnets
  - 1998/1999
- Première utilisation du terme « robot »
  - 2002

Plan

- Le monde des malwares
  - Historique
  - Les logiciels malveillants
  - Nouvelles tendances et actualités
- La réponse des antivirus
  - Fonctionnement des antivirus
  - Pourquoi avoir un antivirus sous Unix
  - ClamAV
  - Les limites

Les logiciels malveillants

- Programmes simples
  - Cheval de Troie et porte dérobée (*Trojan, backdoor*)
  - Bombes logiques
  - Outils de captation d'information (*spyware*)
  - Numérotateur furtif (*dialer*)

Les logiciels malveillants

- Programmes auto-reproducteurs
  - Virus
    - Programme
    - Système
    - Interprétés (Macro, Java, JavaScript, etc.)
  - Ver
    - Réseaux locaux, Messagerie, Internet, Poste à poste, Autres (mIRC, DNS)

Les logiciels malveillants

- Botnet (roBOT NETwork)
  - Dirigé par un *botmaster* via un *Command & Control*
  - La classification s'appuie sur le mode de communication
    - Centralisé : IRC, HTTP, Web 2.0
    - Résiliant : P2P
  - Utilisation :
    - Relais de SPAM
    - Attaque par déni de service distribué (*DDoS*)
    - Fraude au clic
    - Camouflage (*single-flux, double-flux, RockPhish*) [8-1]

Fonctionnalités

- Désactivation des mises à jour
  - Antivirus
  - OS
  - Autres
- Suppression des autres *malware*
- Furtivité (*rootkit*)
- Obfuscation du code
- Chiffrement du binaire

Les logiciels potentiellement indésirables

- PUP (Potentially Unwanted Program)
  - Ne sont pas des programmes malveillants
  - Notamment
    - *Adware*
    - *Jokes*
    - Outils de piratage

Plan

- Le monde des malwares
  - Historique
  - Les logiciels malveillants
  - Nouvelles tendances et actualités
- La réponse des antivirus
  - Fonctionnement des antivirus
  - Pourquoi avoir un antivirus sous Unix
  - ClamAV
  - Les limites

Les nouvelles tendances

- Diminution des PUPs
- Orientation vers les mobiles
  - *Malware* sous Android : Multiplié par 33 en 2011 [12-1]
  - Retour des *dialer*
  - Malware bancaire *in the mobile*
    - Zeus In The Mobile (ZITMO) [12-2]
    - SpyEye In The Mobile

L’actualité

- Stuxnet
  - Ver informatique
  - Vise les infrastructures nucléaires Iranienne
- Duqu
  - Vol d’information
  - Essentiellement en Iran
- sKyWIper/Flame [13-1] [13-2] [13-3]
  - Vol d’information
  - Principalement au Moyen Orient

Plan

- Le monde des malwares
  - Historique
  - Les logiciels malveillants
  - Nouvelles tendances et actualités
- La réponse des antivirus
  - Fonctionnement des antivirus
  - Pourquoi avoir un antivirus sous Unix
  - ClamAV
  - Les limites

Les Antivirus

- Ils détectent
  - Logiciels malveillants
  - PUP
  - Fichiers potentiellement malveillants
    - Ex. : AntiVir détecte les fichiers HTML servant au phishing

Les Antivirus

- Modes de fonctionnement
  - Statique
    - la détection est effectuée sur commande
    - exemples :
      - Poste de travail : inspection d'un disque
      - Serveur mail : analyse d'une pièce jointe
      - Serveur mandataire : analyse d'un fichier téléchargé
  - Dynamique
    - logiciel actif en permanence

Les Antivirus

- Techniques de détection
  - Analyse de forme
    - Base de signatures
    - Recherche générique
    - Analyse heuristique
    - Analyse spectrale
  - Contrôle d'intégrité (liste blanche)
  - Analyse comportementale

Plan

- Le monde des malwares
  - Historique
  - Les logiciels malveillants
  - Nouvelles tendances et actualités
- La réponse des antivirus
  - Fonctionnement des antivirus
  - Pourquoi avoir un antivirus sous Unix
  - ClamAV
  - Les limites

Un antivirus sous Unix, pourquoi ?

- Les menaces sont présentes
  - Windows : Conficker (MS08-067 - *CVE*-2008-4250)
  - Mac : Flashback (CVE-2012-0507)
  - Linux : UNIX/Admw0rm
  - Solaris : SunOS/BoxPoison.worm [20-1]

Un antivirus sous Unix, pourquoi ?

- Tout les systèmes sont vulnérables
  - Plus de 5000 CVE sur 2011 !
    - CVE : *Common Vulnerabilities and Exposures* [19-3]

Un antivirus sous Unix, pourquoi ?

- Tout les systèmes sont vulnérables
  - Mises à jours des produits sur 2011
    - Microsoft : 100 bulletins (MS11)
    - Apple : 14 bulletins CERTA [19-1]
    - Linux Debian : 236 bulletins DSA
      - DSA : *Debian Security Advisories* [19-2]
  - Plus de 5000 CVE sur 2011 !
      - CVE : *Common Vulnerabilities and Exposures* [19-3]

Un antivirus sous Unix, pourquoi ?

- Les utilisateurs sont vulnérables
  - Windows : DNSChanger [21-1]
  - Mac : Mac Defender, DNSChanger
  - Linux : Fake 0-day in OpenSSH [21-2]
  - Android : Trojan.AndroidOS.Dogowar.a [21-3]

Un antivirus sous Unix, pourquoi ?

- Détecter les logiciels malveillants visant d'autres plateformes
  - Exemples :
    - Serveur Web,
    - Serveur mail,
    - Serveur mandataire (*proxy*),
    - Serveur de fichier
    - Serveur CVS ou SVN

Plan

- Le monde des malwares
  - Historique
  - Les logiciels malveillants
  - Nouvelles tendances et actualités
- La réponse des antivirus
  - Fonctionnement des antivirus
  - Pourquoi avoir un antivirus sous Unix
  - ClamAV
  - Les limites

ClamAV, présentation

- Présentation du projet
  - Projet open source (GPL)
  - Racheté par SourceFire en 2007
  - Depuis 2011, plus d'un million de signatures

ClamAV, présentation

- Présentation du projet
  - Moteur antivirus sur analyse de forme
    - Multi-thread
    - Scan sur demande
    - MAJ des signatures automatisée
  - Disponible sur de nombreuses plateformes
    - Linux, Windows, AIX, OSF, Solaris, HP-UX, OpenVMS

ClamAV, présentation

- Différents modes de fonctionnement
  - Clamscan : ligne de commande
  - Daemon
  - GUI : ClamTK ou Klam
  - Logiciel de messagerie

Plan

- Le monde des malwares
  - Historique
  - Les logiciels malveillants
  - Nouvelles tendances et actualités
- La réponse des antivirus
  - Fonctionnement des antivirus
  - Pourquoi avoir un antivirus sous Unix
  - ClamAV
  - Les limites

ClamAV, les limites

- Pas de gestion centralisée des machines
- Possible lenteur de mise à jour sur chaque distribution
  - Ecart de version entre les sources officielles et le paquet non officiel
- Projets indépendants
- SourceFire et l'avenir du libre ?

Limites antivirus ?

- Un seul antivirus sur un SI n'est pas suffisant !
- Moteurs différents pour [29-1] :
  - Postes de travail
  - Serveurs
  - Passerelles Internet

Limites des antivirus

- Ils ne sont qu'une brique de la sécurité d'un SI, ne sont pas fait pour détecter :
  - de flux illégitimes,
  - du spam,
  - une attaque ciblée,
  - un rootkit,
  - l'exploitation d'une faille
- Ils ne se substituent pas à une sensibilisation de l'utilisateur

La fin des antivirus ?

- Stuxnet, Duqu, Flame découverts tardivement

- L'AV reste indispensable
  - Dernier maillon sur le poste
  - Protègent des botnets, des PUPs
  - Réduisent la propagation

Pour aller plus loin

- Les virus informatiques : théorie, pratique et applications, Eric Filiol, 2009
  - ISBN 978-2-287-98199-9, Collection IRIS
- Les virus informatiques, Club de la Sécurité de l'Information Français (CLUSIF), , 2005
  - http://www.clusif.asso.fr/fr/production/ouvrages/pdf/virusinformatiques.pdf
- Bots et Botnets, Club de la Sécurité de l'Information Français (CLUSIF), 2009
  - http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-2009-Bots-et-Botnets.pdf
- Programmes Potentiellement Indésirables, Club de la Sécurité de l'Information Français (CLUSIF), 2008
  - http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-Spyware.pdf
- What Biology Can (and Can't) Teach us about Security, David Evans
  - Parallèle entre informatique et biologie
  - http://www.cs.virginia.edu/~evans/usenix04/usenix.pdf

Questions ?

- Me contacter :
  - Mail : antoine.cervoise@gmail.com
  - Twitter : @acervoise