Computer Emergency Response Team
Industrie Service Tertiaire

EdelWeb
Groupe On-x

Lutte Anti-Virus

Limites des techniques de détection et d'éradication

Philippe.Bourgeois (à) cert-ist.com

Jerome.Rochcongar (à) edelweb.fr

Agenda

- Les faiblesses connues des anti-virus
- Cas des archives malformées : Etude Cert-IST
- Eradication de virus “persistants” : Retour d’expérience et recommandations EdelWeb
- Recommandations Cert-IST

Nota : "Virus" est utilisé ici pour désigner tout type de code malveillant : virus, ver, trojan, rootkit, …

Faiblesses connues des anti-virus

- Fonctionnent essentiellement par signature
  - Reconnaissent facilement les virus déjà connus
  - Mais sont souvent aveugles face à des variantes de ces attaques

Faiblesse intrinsèque (par conception)

- Doivent traiter de multiples formats et encodages
  - Archives (ZIP, RAR, TGZ, etc…)
  - Encodage Mime
- Ne sont pas exempts de bugs (ex : Buffer overflow)
  - Les antivirus ne sont que des logiciels …
  - Certains bugs impactent la sécurité :
    - Mise en défaut de l'antivirus (non détection de virus)
    - Ou même mise en danger de la plate-forme hôte (exécution de code)

Faiblesse de construction

Faiblesses connues des anti-virus

- Les antivirus sont une cible d'attaque pour les codes malveillants :
  - Désactivation des anti-virus
  - Dissimulation au moyens de « rootkits » ou de fonctions avancées de la plate-forme (exemple : ADS)

Cible activement attaquée

- Synthèse des "stratégies" d'attaques :
  - Neutralisation (stopper l'antivirus)
  - Contournement (échapper à la détection)
  - Tremplin (utiliser l'anti-virus pour infecter le système)

Evolution du nombre d'avis Cert-IST sur les produits anti-virus

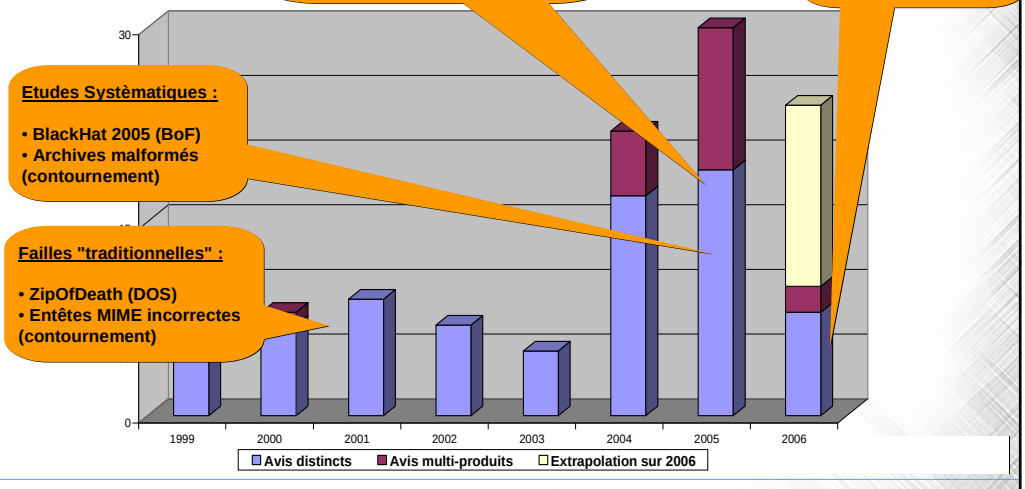
- Une augment… …uis mi 2004
  - Les anti-virus i… …illes ?

Emission d'une pré-alertes Cert-IST :
• CERT-IST/DG-2005.006 (07/10/05)

Virus utilisant les archives malformées :
• **Sober-X**

Etudes Systèmatiques :
• **BlackHat 2005 (BoF)**
• **Archives malformés (contournement)**

Failles "traditionnelles" :
• **ZipOfDeath (DOS)**
• **Entêtes MIME incorrectes (contournement)**



Recherches connues sur la vulnérabilité des anti-virus (1/2)

- Etude 2005 par des chercheurs de ISS : (Liste)
  - Première étude systématique dans ce domaine (reverse engineering de code)
  - Vulnérabilités de type « Buffer/Heap overflow » identifiées dans les anti-virus :
    - Computer Associate, ClamAV, F-Secure, Kaspersky, McAfee, Panda, Sophos, Symantec, Trend Micro

- Etudes sur les archives malformées
  - IDefense (octobre 2004) : CAN-2004-0932 à CAN-2004-0936, CVE-2004-2442
    - Indiquer une taille de zéro dans l'entête ZIP
  - fRoGGz (octobre 2005) ; CVE-2005-3210 à CVE-2005-3235
    - Ajouter un marqueur "MZ" en tête d'un fichier d'archive (RAR, CAB, ARJ)
  - Andrey Bayora (octobre 2005) : The Magic of magic byte
    - Ajouter un marqueur "MZ" en tête de fichiers ".hmtl", ".bat" ou ".eml"

Recherches connues sur la vulnérabilité des anti-virus (2/2)

- Thierry Zoller :
  - 17/10/05 : RAR - Evasion of Anti Virus Detection
  - 03/11/05 : F-Prot/Frisk Anti Virus bypass - ZIP Version Header
  - 28/12/05 : New AV-Evasion Methods - Summary
    - New Methods of Evasion : 5
    - AV Products currently affected : 22
    - Gateway Solutions affected : 2
  - 19/01/06 : F-Secure AV - Anti-virus Bypass and Buffer Overflow

Agenda

- Les faiblesses connues des anti-virus
- Cas des archives malformées : Etude Cert-IST
- Eradication de virus “persistants” : Retour d’expérience et recommandations EdelWeb
- Recommandations Cert-Ist

Principe d'une archive malformée

- Un fichier archive "normal" est légèrement déformé (Illustration)
  - Ex : ajouter "MZ" en tête d'un fichier "ZIP"
- Le fichier malformé contient un virus :
  - Il n'est plus détecté comme infecté par l'anti-virus (du fait de la malformation)
  - Mais l'outil de décompression (WinZip, WinRar) est capable d'extraire le virus (il n'est pas gêné par la malformation)
- Risque ?
  - Permet de contourner une protection périmétrique (passerelle antivirus)
  - Mais sera normalement stoppé sur le poste utilisateur lorsque le virus sera extrait de l'archive malformée (analyse "à l'accès")

Etude réalisée par le Cert-IST

- Prolongement d'une étude publiée par "Froggz" en octobre 2005
- Construction d'un jeu de test systématique
  - Trois malformations : MZ, MZ+, Null
  - Seize formats d'archive : 7Z, ACE, ARJ, BZ2, CAB, CPIO, ISO, JAR, LHA, LZH, RAR, TAR, TGZ, UUE, XXE, ZIP
- Test de :
  - Sept antivirus :
    Avast, ClamWin, F-Secure, Kaspersky, McAfee, Sophos, Trend Micro
  - Quatre outils de manipulation d'archive
    WinZip 9.0, PowerArchiver 9.26.02, WinRAR 3.51, Windows XP

Résultats de l'étude

- Résultats : 92 anomalies identifiées (Détails)
  - 15 anomalies sont préoccupantes.
    Exemple : Fichier ZIP malformé extractible par WinZip
  - Les autres anomalies sont mineures.
    Exemple : Fichier LZH malformé extractible par WinRar.
- Conclusion :
  - Il est facile de trouver des anomalies qui permettent de contourner une protection antivirale périmétrique;

Recommandations Cert-IST

- Pourquoi l'antivirus est-il mis en échec ?
  - Hypothèse 1 : L'AV fait entièrement confiance aux octets d'entête pour déterminer la nature du fichier

    MZ = Exécutable ⇨ le fichier n'est pas une archive ZIP.
    Quid des archives auto-extractibles, alors ?
  - Hypothèse 2 : L'AV ne comprend pas la structure du fichier et décide qu'il n'est pas dangereux

    Pourquoi ne pas émettre un avertissement : fichier non compris = fichier suspect
- Comment améliorer la détection ?
  - Emettre un avertissement (ou mise en quarantaine) sur détection d'une anomalie
    - Contradiction entre l'entête du fichier ("MZ") et son extension (".ZIP")
    - Ou toute autre anomalie dans la structure du fichier

Réaction des éditeurs anti-virus

- Résultats mitigés
  - 3 ont corrigé les anomalies dans le mois qui suivait le rapport d'anomalie.
  - 2 ont corrigé dans les 6 mois suivants, après relances.
  - 2 n'ont pas pris en compte les anomalies signalées (ils sont toujours vulnérables).

Agenda

- Les faiblesses connues des anti-virus
- Cas des archives malformées : Etude Cert-IST
- Eradication de virus “persistants” : Retour d’expérience et recommandations EdelWeb
- Recommandations Cert-IST

Qu'est-ce qu'un virus "persistant" ?

- Tout type de code malveillant (virus, ver, troyen,…)
- Utilise des techniques de furtivité pour se cacher
- Utilise des techniques sophistiquées afin d'empêcher sa suppression

DIFFICULTES de DETECTION et d'ERADICATION

Exemple du ver Brontok (1/3)

- Ver apparu fin 2005
- Propagation par
  - **messagerie** (pièce jointe au mail)
  - copie sur les **partages réseau** et **supports USB**
- Caractéristiques
  - **Processus non interruptibles** par les moyens propres au système :
    - ✓ lancés au démarrage (même en mode sans échec)
    - ✓ utilisent le nom de processus systèmes (smss, lsass, ...) → considérés comme légitimes, critiques et ininterruptibles par Windows
  - Utilisation de la **ligne de commande et de Regedit impossible**
  - **Fichiers infectés et clés de registre recréés** en permanence

Exemple du ver Brontok (2/3)
Difficultés d'éradication

- Avec un anti-virus en mode scan
  → Brontok détecte le lancement d'un antivirus et effectue un **redémarrage du poste**
- Avec des outils spécifiques fournis par des éditeurs
  → **Inefficaces** sur la version du ver testée
- Manuellement
  → **Impossible** par les moyens standard Windows car :
  - *éditeur de registre désactivé*
  - *pas d'accès à la ligne de commande*
  - *processus non interruptibles via taskmgr ou mode sans échec*
  - *...*

Exemple du ver Brontok (3/3)
Solutions d'éradication

- Utilisation d'outils tiers
  - Arrêt des processus
  - Modification des valeurs de la base de registre

  Rq: Le lancement de certains outils tiers entraîne un reboot
- Utilisation de la console de récupération de Windows
  - Accès au système sans que les processus du ver ne soient lancés
  - Suppression des fichiers infectés
- Réinstallation du poste

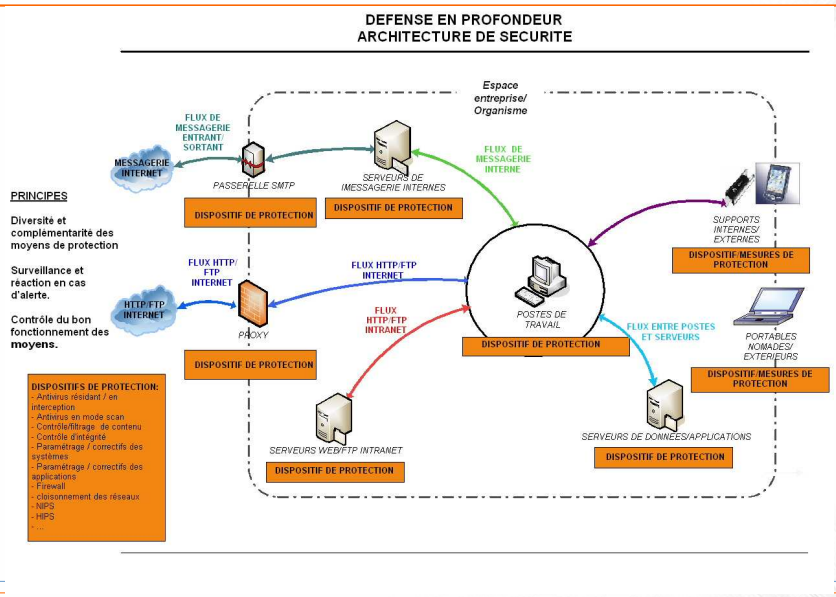
Bilan sur les virus “persistants”

- Impacts
  - **Indisponibilité** des postes (mise en quarantaine)
  - **Interventions** sur les postes infectés (éradication ou réinstallation)
  - Remise en état du SI **coûteuse**
- Tendance
  - **Développement de ce type de codes**

Recommandations : Prise en compte de ce type de code

- **Prévention**
  - intégrer les évolutions des virus “persistants” à la **veille antivirale** et **aux tests des capacités d’éradication** des logiciels antivirus
- **Protection**
  - Mettre en oeuvre une **Protection multi-niveaux** du SI
  - **Utiliser des Moyens de protection différents** et **complémentaires** (plusieurs antivirus, filtrage, contrôle d’intégrité, paramétrage des systèmes, des applications, ...)
- **Réaction**
  - Adapter la **gestion de crise et les procédures** / scénarios critiques (ex: association code de type Blaster et capacités de persistance)

Prise en compte de la menace liée au code malveillant



Recommandations :Prise en compte de la menace liée au code malveillant

- Mise en oeuvre d'une politique antivirale
  - identification des besoins, des moyens, des responsabilités
- Veille technique
  - Anticiper les principales crises
- Application régulière des correctifs
  - Diminuer la vulnérabilité des postes
- Contrôles multi-niveaux (Passerelles HTTP, SMTP, Messagerie interne, Serveurs de données, postes de travail)
- Antivirus, Firewall, contrôle d'intégrité, NIPS, HIPS
  - Assurer l'administration et l'exploitation des moyens déployés
- Contrôle des ordinateurs portables et supports

Agenda

- Les faiblesses connues des anti-virus
- Cas des archives malformées : Etude Cert-IST
- Eradication de virus “persistants” : Retour d’expérience et recommandations Edelweb
- Recommandations Cert-IST

Constat

- Le poste utilisateur est devenu la cible Nº 1 des attaques
  - Opportunistes (constitution de "botnets")
  - Ou ciblées (espionnage industriel)
- L'anti-virus est une protection indispensable, mais pas infaillible
  - Il ne protège que contre une menace déjà identifiée
  - Il peut être parfois contourné
  - Ses capacités de désinfection peuvent être mises en défaut
- De plus en plus de "chercheurs" s'intéressent aux failles des anti-virus
  - Nota : la "mode" n'est plus à publier des avis de sécurité sur Bugtraq, mais plutôt à garder secret ses trouvailles.

Conclusion

Pas de solution miracle ☹

Mais une prise de conscience commune permet de maintenir/renforcer les défenses

- Pour les organismes de veille et les experts
  - Vigilance pour identifier les nouvelles menaces
  - Adapter les outils et procédures à ces menaces
- Pour les éditeurs de solutions anti-virus
  - Réceptivité (vigilance) face aux "nouvelles" attaques
  - Réactivité
- Pour l'entreprise : une défense en profondeur
  - Ne pas se limiter à une protection périmétrique
  - Sensibiliser les utilisateurs
  - Protéger l'information au sein de l'entreprise