JSSI 2004

La "mobilité" du code malveillant

Nicolas RUFF
EdelWeb / Groupe ON-X
nicolas.ruff@edelweb.fr

Plan

- Plan
- Introduction
- Les risques
- Les conséquences
- Scénario catastrophe
- L'état de l'art de la protection
- Conclusion

Introduction (1/3)

- **Définition du "code malveillant"**
  - Virus de messagerie (@MM)
    - Code autoreproducteur se propageant sous forme de pièce jointe
    - Exécution manuelle ou automatique à la prévisualisation
  - Ver réseau
    - Code autoreproducteur exploitant une faille dans un logiciel réseau
    - Avec (ex. Blaster) ou sans (ex. Slammer) charge finale
  - Spyware (terme très générique)
    - Programme espion destiné à collecter des données sur le poste de l'utilisateur et à les retransmettre
      - Établit généralement un "profil" marketing
    - Parfois actif
      - Affichage de popups, modification du navigateur, etc.
    - Généralement furtif et difficile à éradiquer
  - Backdoor
    - Logiciel ouvrant des services supplémentaires non désirés
      - Connexion à distance au poste
      - Relais SMTP
      - Zombie DDoS
    - Implique une exploitation manuelle ultérieure

Introduction (2/3)

- "Phising"
  - N'est pas un "code" malveillant mais peut exploiter des failles du client
  - Récupération de données sensibles (ex. n°CB) grâce à de faux messages destinés à leurrer l'utilisateur
- Autres codes (virus compagnons, virus de boot, etc.)
  - Aujourd'hui marginaux
- Spam
  - N'est pas un "code" malveillant (sauf lorsque le spam contient des scripts !)
  - Mais souvent un but pour les auteurs de code malveillant (source de revenus)

❑ Évolution de la menace

- A l'origine
  - Deux sources d'infection principales
    - Virus infectant le boot ou les applications échangés par disquette
    - Diffusion de logiciels "pirates" possédant une backdoor
  - Propagation lente
  - Charge finale = perte de données
- Aujourd'hui
  - Principal vecteur d'infection : Internet
    - Tout moyen de communication numérique rapide et standardisé pourrait être utilisé
  - Propagation très rapide
  - Charge finale = intérêt financier (vol d'informations ou spam)

❑ Remarque

- Aujourd'hui seule la plateforme "WinTel" est prise pour cible

Introduction (3/3)

- **Qui crée du code malveillant ?**
  - Quelques exemples …
    - Sociétés de marketing "on-line"
      - Installation de spywares
      - Ex. Famille "Trojan.Downloader" (cf. Swizzor alias MP3Search)
    - Sociétés de mass-mailing ("spam")
      - Déploiement de relais SMTP, collecte d'adresses email
      - Ex. Famille "TrojanProxy"
    - Escrocs
      - Vol de données financières, réseaux de zombies pour DDoS
      - Ex. Racket du site de Webcast lors de la finale du SuperBowl
    - Sociétés de surveillance domestique
      - Implantation de backdoors, surveillance des enfants et des conjoints
      - Ex. Evil Eye Software
  - Remarque : forte compétition entre les créateurs de virus
    - Cf. messages "cachés" dans Netsky et Bagle

Les risques (1/2)

- **L'accès Internet**
  - Toute entreprise possède une adresse email
  - Développement de l'accès Internet chez les particuliers
    - Accès haut débit et toujours allumés (ADSL)
  - Soutenu par le gouvernement (administration numérique)
  - Soutenu par les grandes entreprises (ex. Microsoft)

- **Les équipements nomades**
  - Toute une famille : portable, téléphone, PDA, clés USB, juke-boxes numériques, etc.
  - Ils (re)créent une passerelle entre de nombreux réseaux
  - Les schémas de défense actuels sont périmétriques (Firewalls, Proxies, etc.)
    - Cf. discours Microsoft sur le SP2
  - Or le "périmètre" de l'entreprise est de plus en plus flou
    - Internet, Intranet, clients, fournisseurs, enfants, etc.

Les risques (2/2)

- **L'utilisateur**
  - Aucune sensibilité à la sécurité chez les particuliers et dans les PME/PMI
    - Le danger de l'outil informatique n'est pas perçu
    - Pas d'attitude "défensive" vis-à-vis des risques
    - L'éducation est faite par les vendeurs de produits …
  - Le code malveillant est banalisé
    - Il devient presque "normal" d'être infecté
  - L'image actuelle de l'informatique est le "tout ouvert"
    - Logiciels libres, "sharewares" crackés, téléchargements illégaux, …
    - Ex. 77% des sociétés américaines hébergent des clients P2P
      - http://news.com.com/2100-1027_3-1026184.html
- **Facteurs aggravants**
  - Professionnalisation de la menace
  - Dépendance croissante vis-à-vis de l'informatique
  - Les logiciels distribués actuellement sont une menace
    - Abondance de fonctionnalités inutiles
    - Configuration par défaut non sécurisée
    - Besoin de mise à jour constant et manuelle
    - (Souvent) présence de code malveillant intégré

Les conséquences (1/1)

- **Conséquences immédiates**
  - Déni de service sur les ressources (réseau / stockage)
  - Destruction de données
    - Attention aux filtres mal configurés
  - Coût important
    - Direct : perte d'exploitation
    - Indirect : traitement des incidents

- **Conséquences à long terme**
  - Banalisation de l'incident de sécurité
  - Diffusion d'informations à l'extérieur de la société
    - Rediffusion de messages, collecte d'information sur les postes …
  - Remarque : peu de jurisprudences concernant des affaires de code malveillant

- **Bien souvent de manière indétectable et intraçable !**

Scénario catastrophe (1/3)

- **Tout moyen de communication numérique rapide et standardisé peut être vecteur de code malveillant**
  - Exemple : extension de la menace au réseau GSM
  - D'autres scénarios sont envisageables à moyen terme
    - Ex. démodulateurs TV+ADSL, magnétoscopes reliés à Internet, etc.

- **Réception d'un SMS malveillant**
  - Un SMS/MMS peut contenir tout type de données
    - Texte, application Java, animation, vidéo, etc.
  - Exécution du contenu sans confirmation si :
    - Le code est signé
      - CA préinstallées : Thawte, Verisign, etc.
    - L'entête du message indique un SMS "opérateur"
      - Exemples bien connus : logos, sonneries, mise à jour de la carte SIM
  - Sinon l'utilisateur doit cliquer sur "oui" …
- **Exécution locale d'une application Java**
  - Plateforme unique : MIDP 1.0 (maintenant 2.0)
  - Machine Java native
    - Sécurité allégée (problème de performance)
    - Versions anciennes et boguées (ex. 1.3.1 sur mon téléphone)
  - Certains téléphones "haut de gamme" possèdent de plus un OS
    - Symbian ou Windows CE

Scénario catastrophe (2/3)

- **"Autorun"**
  - Les cartes SIM "phase 2+" (dites "SIM Toolkit") peuvent contrôler le téléphone
    - Ex. installation de services "opérateur" (météo, trafic, etc.)
    - Ces services sont basés sur l'envoi de SMS en tâche de fond
  - Les commandes sont fournies par la carte à l'allumage du téléphone

- **Propagation GSM**
  - L'application Java peut accéder au carnet d'adresses et se propager par SMS
- **Propagation IP**
  - Développement des services WAP / GPRS
  - Il existe souvent un filtrage de ports très restrictif
  - Mais SMTP, POP, HTTP, HTTPS sont autorisés
- **Propagation PC**
  - La quasi-totalité des téléphones exigent Outlook pour leur synchronisation
    - Exploitation de bogues Outlook/IE
    - Ex. "buffer overflow" dans le traitement des vCard (MS01-012)
    - En créant une entrée dans le carnet d'adresses, il est possible d'exécuter du code sur PC
  - Il est possible d'envoyer des SMS en local (ex. Bluetooth)
  - Il est possible d'envoyer des SMS via une adresse email (ex. tel@opérateur)

Scénario catastrophe (3/3)

- **Charge finale**
  - Déni de service
  - Collecte des IMEI
  - Collecte des carnets d'adresse
  - Suppression du code PIN (ou code PIN aléatoire)

- **Solutions de protection ?**
  - Capacité de réaction des opérateurs inconnue
  - Il n'existe pas de logiciel côté téléphone permettant de filtrer un SMS "malveillant"
  - Mise à jour logicielle (Firmware, OS et/ou JVM) complexe (retour usine)

État de l'art de la protection (1/4)

- **Challenge : les technologies nomades sont …**
  - … multiformes
    - Matériel : PC, PocketPC, PDA, Téléphone, Jukebox, …
    - Système : Windows CE, PalmOS, Symbian, propriétaire, …
    - Processeur : Intel, Motorola, StrongARM, …
  - … personnelles
    - L'utilisateur mélange données professionnelles et usage personnel de son appareil
    - Il établit un lien affectif et refuse d'être limité
  - … sensibles
    - Les données contenues sont en général les plus sensibles de l'entreprise (messagerie, documents de travail, configuration VPN)
  - … exposées
    - Connexion à des réseaux non maîtrisés
    - Absence de sensibilité de l'utilisateur aux problèmes de sécurité
  - … vulnérables
    - Pas d'administration centralisée lorsque le poste n'est pas connecté ou connecté via une liaison lente au réseau de l'entreprise
    - Pas de gestion des risques spécifiques à la technologie employée

État de l'art de la protection (2/4)

- **Solutions actuelles contre le code malveillant**
  - Configuration robuste du poste de travail
    - Limitation des droits utilisateur
  - Suivi des correctifs de sécurité
  - Sensibilisation des utilisateurs
  - Contrôle des entrées / sorties de données
    - Filtrage des pièces jointes
    - Contrôle des logiciels installés
  - Protection réseau
    - Firewall personnel
  - Recherche de codes malveillants
    - Antivirus
    - Recherche de Spywares (logiciels Ad-Aware, Spybot)
  - Contrôle de cohérence
    - Contenu des clés sensibles (Run, etc.)
    - Processus démarrés

- **Limites**
  - Pas toujours appliqué …
  - Ces techniques sont connues des attaquants
  - Les bases de connaissance n'évoluent pas toujours aussi vite que la menace

État de l'art de la protection (3/4)

- **Axes de développement**
  - Configuration "tout interdit" par défaut
    - Le nombre de questions adressées à l'utilisateur est réduit
    - Cf. Windows XP SP2
  - Frontières de l'entreprise floues => évolution de la défense périmétrique vers une défense en profondeur
    - Intégration et coopération des outils de protection locale
    - Contrôle via des dispositifs réseau externe
      - Service de quarantaine de Windows 2003
      - Solution Cisco
      - Solution Checkpoint
    - Remarque : quelle est la validité d'un contrôle effectué par le nomade sur lui-même ?

État de l'art de la protection (4/4)

- Coordination des moyens de lutte et centralisation de l'administration
  - Prise en compte de la variabilité des configuration
  - Adaptation dynamique des règles de sécurité à l'environnement
    - Définition de "profils"
    - Autodétection du profil le mieux adapté
- Prise en compte des menaces spécifiques
  - Ex. Bluetooth, téléphones Java, assemblies .NET
  - Les outils sont-ils disponibles / adaptés / efficaces ?

Conclusion

- **Le "code malveillant" est devenue une notion fourre-tout regroupant des attaques très variées**
- **Les technologies de protection actuelles ne protègent que contre les attaques connues et exploitées**
  - Problème du coût de R&D sur une menace inexistante
  - Les attaques "marginales" ne sont pas répertoriées
- **La menace croit en étendue et en technicité**
  - Les attaques techniquement possibles sont nombreuses
  - Le nombre de chercheurs augmente également
  - Les concepteurs de code malveillant en retirent un bénéfice financier
- **Les solutions techniques sont insuffisantes**
  - Il est nécessaire d'anticiper les risques et de mettre en place une organisation de veille/réaction
  - Exemple le plus trivial : le filtrage des pièces jointes par extension