Malwares
La menace de l'intérieur

Nicolas RUFF (EADS-CCR)
nicolas.ruff@eads.net

Eric DETOISIEN
eric_detoisien@hotmail.com

Plan

1. Introduction
2. Panorama de la menace actuelle
3. Progrès des techniques rencontrées "dans la nature"
4. Analyse des défenses existantes
5. Nouvelles techniques de protection
6. Conclusion
7. Références

Introduction

- Sécurité depuis toujours limitée au périmètre extérieur du SI (protection des serveurs sur Internet)
- Pourtant la menace des chevaux de Troie est toute aussi réelle et ancienne mais souvent ciblée
- Aujourd'hui ce danger devient massif et opportuniste au travers des spywares
- Les malwares sont une réalité, efficaces et en constante évolution ils demandent de nouveaux types de protection

Panorama de la menace actuelle

- 3 tendances lourdes
  - Explosion de la malveillance informatique
    - Spam/spim, phishing/pharming, vol d'identité, malwares, etc.
  - Profits importants générés par ces activités
  - Absence de solution à l'échelle de l'Internet
    - Législations, normes techniques, outils
- Conclusion : la malveillance organisée sur Internet est une activité durable (car rentable)
- Note : les spywares qualifiés de "menace de l'an 2005" par les administrateurs … mais pas par les décideurs (étude WatchGuard)

Progrès des techniques rencontrées "dans la nature"

- Une idée forte : les activités de recherche sont désormais financées
- Exemples d'outils et de techniques rencontrées dans la nature
  - "Rootkits" Windows indétectables
    - Hacker Defender "Rootkit Golden" (390 €)
    - EvilEyeSoftware "RAT" (entre $200 et $300)
  - Techniques anti-analyse
    - Initialement : des versions modifiées de UPX
    - Maintenant : protection par des outils spécialisés type ASPACK, détection de VMWare
      - Ex. Mydoom.P, LovGate.AJ, Litmus.AS
  - Virus "professionnels"
    - Ex. collaboration des virus Bagle / Zafi / Netsky
      - http://www.kaspersky.com/news?id=160377972

Progrès des techniques rencontrées "dans la nature"

- Motivation des attaquants
  - Capturer des données sur le poste
    - En général financières
      - Mots de passe PayPal, banques en ligne, etc.
    - Le vol d'identité est également à la hausse
  - Utiliser le poste en rebond ("bot")
    - *Cf. "tracking botnets" du HoneyNet Project*
    - DDoS
    - Émission de spam
    - Compromission d'autres machines
    - Manipulation des revenus publicitaires (Adwares et Google AdSense)
    - Manipulation des sondages en ligne

Progrès des techniques rencontrées "dans la nature"

- Les cibles du vol d'information
  - Courant :
    - Mots de passe applicatifs
      - Keylogging
      - Écoute du trafic réseau (très courant aujourd'hui)
      - Pour contourner le SSL, il est possible d'intercepter l'API Winsock
  - Moins courant :
    - Données de formulaires mémorisées
    - Mot de passe Windows
    - Clés privées des certificats
    - *En général lié à une attaque ciblée*

Progrès des techniques rencontrées "dans la nature"

- Démo
  - SSLug
    - Proof of Concept d’un malware avancé
    - Man-in-the-Middle SSL transparent pour l’utilisateur
    - Développé pour Internet Explorer
    - Utilisation d’injection de code par API Hooking
    - Récupération en clair du flux chiffré via HTTPS
    - Présentation à l’utilisateur du "vrai" certificat

Analyse des défenses existantes

- Une panoplie bien rodée …
  - Sur le poste de travail
    - Antivirus
    - Antispyware
    - Firewall personnel
    - HIDS/HIPS
  - Aux frontières de l'entreprise
    - Antivirus de passerelle / de messagerie
    - Filtrage d’extension
    - Proxy filtrant (par URL ou par contenu)

Analyse des défenses existantes

- Ces outils "traditionnels" deviennent inefficaces
  - Les techniques à base de signatures ne suivent plus
    - Très forte réactivité des auteurs de malwares (parfois 15 minutes entre 2 mises à jour)
    - Utilisation de "0day"
    - Attaques via des scripts/objets dynamiques dans le navigateur, la machine Java, les plugins Flash/PDF
  - Les "black lists" d'URLs ne sont plus suffisantes
    - Utilisation de machines compromises pour relayer des attaques en "phishing" (pas d'adresse IP fixe)

Analyse des défenses existantes

- Ces outils "traditionnels" deviennent inefficaces (suite)
  - Les canaux cachés se font de plus en plus furtifs vis-à-vis du firewall personnel
    - Utilisation de connexions IE légitimes via scripting OLE
    - Utilisation de Browser Helper Objects (BHO) ou de plugins
  - Les moteurs de détection et/ou les évaluations de risques s'avèrent incomplets
    - Utilisation de nouveaux vecteurs d'attaque (ex. bogue JPEG)
  - Les outils de protection eux-mêmes sont attaqués
    - Ex. nombreux bogues dans les moteurs de décompression LHA / ARJ / ZIP / …
    - Ex. Ver Witty

Nouvelles techniques de protection

- Des évolutions sensibles du marché
  - Frontières de plus en plus floues entre les outils
    - Suites "tout-en-un"
    - Bases de signatures par type de menace (payantes)
    - Détecteurs de rootkits
      - F-Secure, Symantec, SysInternals, Microsoft (projet Strider GhostBuster), etc.
    - Technologies anti-"buffer overflow" et anti-"0 day"
      - McAfee, Cisco, Symantec, etc.
    - Moniteurs comportementaux
  - Entrée de Microsoft dans le jeu
    - Firewall de XP SP2
    - Analyse des BHO de XP SP2
    - Outil "Stinger-like" mis à jour tous les mois
    - Rachat de Giant Antispyware
    - Rachat de Antigen et GeCAD (antivirus)

Nouvelles techniques de protection

- Sur le poste de travail
  - Protections spécifiques des cibles traditionnelles
    - BHO
    - Clés de base de registre "sensibles"
  - Moniteurs de comportements
    - "Profiling" applicatif (avec phase d'apprentissage ou non)
    - Accès à des ports sensibles (ex. TCP/25)
    - Lancement de code depuis des répertoires sensibles (ex. Temporary Internet Files)
    - Détection d'API hooking
    - Etc.

- Aux frontières
  - Détection des canaux cachés HTTP par analyse comportementale
    - Connections régulières et uniformes dans la journée
    - Ratio upload/download anormal
    - Accès à une URL unique

Nouvelles techniques de protection

- Outils OpenSource
  - Protection du poste : aucun ?
  - Détection aux frontières
    - Cctde (plugin SNORT)
    - Tcpstatflow
- Outils commerciaux
  - Détection aux frontières
    - BlueCoat
    - WatchGuard
  - Blocage des "0day"
    - McAfee Entercept
    - Symantec Enterprise Firewall
    - Cisco CSA
    - Primary Response (Sana Security)
    - StormShield (SkyRecon)
  - Etc. etc. (un marché vraiment dynamique !)

Conclusion

- Menace professionnelle donc potentiellement redoutable et très efficace
- Solutions classiques du marché obsolètes ou du moins insuffisantes
- Nouvelles solutions à peine émergentes (mais très dynamiques)
- Une nouvelle menace, dans des cas extrêmes difficile à stopper, mais qui ouvre aussi un nouveau marché bien juteux pour les éditeurs …

Références

- Les directions générales sous-estiment les "spywares"
  - http://www.vulnerabilite.com/actu/20050125102942etude_watchguard_spywares.html
- "Covert Channel and Tunneling over the HTTP protocol Detection"
  - http://www.gray-world.net/projects/papers/html/cctde.html
- TcpStatFlow
  - http://www.geocities.com/fryxar/
- Benjamin Caillat - Backdoors en environnement Windows
  - http://benjamin.caillat.free.fr/