Le "Peer to DoS"

Nicolas RUFF
EADS-CCR DCR/STI/C
nicolas.ruff (at) eads (dot) net

Plan

- Introduction
- P2P
  - Logiciels et protocoles
  - Contournement des filtres périmétriques
- Botnets
  - Evolutions et besoins actuels
- Convergence
  - Exemple des réseaux eDonkey et Skype
- Conclusion
- Références

Introduction

- Deux phénomènes parallèles
  - Fort développement des réseaux P2P
    - S'adaptent aux contre-mesures
    - Avantages techniques indéniables du P2P
      - Mutualisation des ressources, diminution de la latence
  - Forte activité dans le domaine des botnets
    - Activité lucrative en pleine expansion
    - Les plus gros réseaux atteignent les 100,000 bots
- Ces activités vont-elles converger ?

P2P

- Logiciels et protocoles
  - 1ère génération : N clients -> 1 serveur
    - Ex. Napster
  - 2ème génération : N clients -> M serveurs
    - Ex. ed2k
  - 3ème génération : N clients sans serveur
    - Ex. Gnutella, Kad, Skype, …
  - 4ème génération : N clients + anonymat
    - Ex. Hamachi, Freenet , …

P2P

- Contournement des filtres périmétriques
  - 1ère génération
    - Connexion TCP/UDP directe
  - 2ème génération
    - Traversée de NAT (STUN, TEREDO, etc.)
  - 3ème génération
    - Encapsulation dans HTTP
    - Traversée des proxies
  - 4ème génération
    - Encapsulation dans SSL / chiffrement intégral

Botnets

- Evolution
  - Cheval de Troie : connexion pirate -> machine
  - Bot : connexion machine(s) -> pirate
    - Nécessaire vu la taille des réseaux de bots
      - Jusqu'à 100,000 machines …
- Besoins actuels
  - Canal de contrôle
    - Résilience
    - Anonymat / discrétion
  - Logiciel client
    - Furtivité des connexions
    - Résistance à l'analyse

Convergence

- Plusieurs pistes de développement
  - Le réseau P2P comme canal de contrôle
  - Le client P2P comme bot

EADS

Convergence

- IRC comme canal de contrôle
  - Inconvénients
    - La connexion est difficile à masquer chez la victime
    - Le canal peut être compromis (chan et/ou serveur)
    - La connexion du pirate peut être tracée
- Le réseau P2P comme canal de contrôle
  - Avantages
    - Les données de contrôle sont noyées dans le flot
    - L'envoi de commandes est "anonyme"
    - Le canal de communication peut être "caché"
      - Ex. fichier possédant un hash particulier, etc.

EADS

Convergence

- Logiciel spécifique comme bot
  - Inconvénients
    - Peut être identifié par les antivirus
    - Peut être analysé en cas de compromission
- Le client P2P comme bot
  - Avantages
    - Les logiciels clients sont toujours autorisés à contourner les sécurités locales
    - Le fichier est "légitime"
    - L'analyse *post mortem* ne révèle rien de particulier

EADS

Convergence

- Exemples d'utilisation du client P2P comme bot
  - Scénario #1 : serveur eMule "hostile"
    - Le lancement d'une attaque DDoS se fait en ajoutant la cible comme source de tous les téléchargements
    - Les clients firewallés ("LowID") sont pilotés "en direct" par le serveur
  - Faisabilité : totale
  - Furtivité : totale
    - Aucune trace sur le client, sauf à journaliser tout le trafic réseau

Convergence

- Scénario #2 : attaque sur le client eMule
  - Exploitation d'une faille binaire ou faille protocolaire
  - Injection d'une commande de connexion vers la cible
- Faisabilité : forte
- Furtivité : forte
  - Aucune trace sur le client si l'exécution se fait en mémoire uniquement
  - Nécessité de mettre en place des eMulePots ?

Convergence

- Scénario #3 : "plug-in" Skype
  - Virus installant un plug-in basé sur l'API Skype
  - Pilotage de la victime via le réseau Skype
- Faisabilité : totale
  - Cf. plug-in Timbuktu pour Skype
- Furtivité : forte
  - Le binaire peut être capturé
  - Mais le canal de contrôle est anonyme, totalement chiffré, et noyé dans le trafic Skype

EADS

Conclusion

- La convergence P2P / Botnets ne présente que des avantages pour les attaquants
- Cette convergence est à craindre dès que le niveau des attaquants aura progressé
- Le pire (to pire) reste à venir
  - Evolution de tous les logiciels "grand public" vers un modèle P2P
  - Service P2P natif Windows
    - Déjà disponible en v0.3 dans XP SP2

Références

- Magazine MISC n°24
  - L'utopie du parfait malware (Georg Wicherski)

- Remerciements à toute l'équipe DCR/STI/C du centre de recherche EADS
  - Et en particulier :
    - Kostya Kortchinsky
    - Philippe Biondi
    - Fabrice Desclaux