

# Les FAI face aux virus et aux vers

#### Nicolas FISCHBACH

Senior Manager, IP Engineering/Security - COLT Telecom nico@securite.org - http://www.securite.org/nico/

version 1.0



### Plan

- » Introduction
- » Virus et vers
  - > Quelques exemples
  - > Les intentions (cachées)
- » Détection
  - > Flux réseaux (Netflow)
  - > Syphon ("Sinkhole")
  - > Serveurs SMTP/DNS
  - > Pot de miel
- » Filtrage
  - > ACLs, BGP, etc.
  - > Couches applicatives (réseau et système)
  - **Conclusion**





### Virus et vers

#### » Quelques exemples

- > Anciens
  - . Code Red (IIS), Nimda (Mail)
  - . Slammer (SQL)
- > Récents [Microsoft+logiciels de "masse"]
  - . NetSky: Mail (moteur intégré)+part. rés., vuln. IE Mime Header
  - . Witty: vuln. ICQ (ISS), propagation aléatoire (UDP)
  - . Autres [déni de service]: NTP, Zonelabs+TAT14, CRL Verisign
  - . B[e]agle: Mail (moteur intégré)+part. rés., shell 8866/tcp
  - . (Mimail), MyDoom: Mail+Kazaa, DDoS SCO, shell 3127-3198/tcp
  - . Welchia/Nachi: vuln. DCOM/WebDAV, payload via TFTP, shell 666-765/tcp
  - . Sobig: Mail (moteur intégré)+part. rés., payload via HTTP
  - . Blaster: vuln. DCOM, payload TFTP, shell 4444/tcp, DDoS MSWU
  - . Depuis ce week-end: Sasser (vuln. LSASS, vers, shell 9996/tcp, charge FTP 5554/tcp)



### Virus et vers

#### » Les intentions (cachées)

- > Zombie/agent pour déni de service mutualisé (\*bot)
- > Relais ouvert (open proxy)
- > Client/Serveur/Relais de messagerie (SMTP agent)
- > Calcul distribué, etc.

#### » Ce qui a changé

- > "Ingénierie sociale"
  - Messagerie (types "sûrs" ? ZIP, PDF, BMP, MP3: failles clients)
  - Phishing
- > Ce n'est plus que pour le "fun"
- > Collaboration/copier&coller entre les auteurs
- > Prise de conscience des différents acteurs (efforts de certains FAI "grand public")

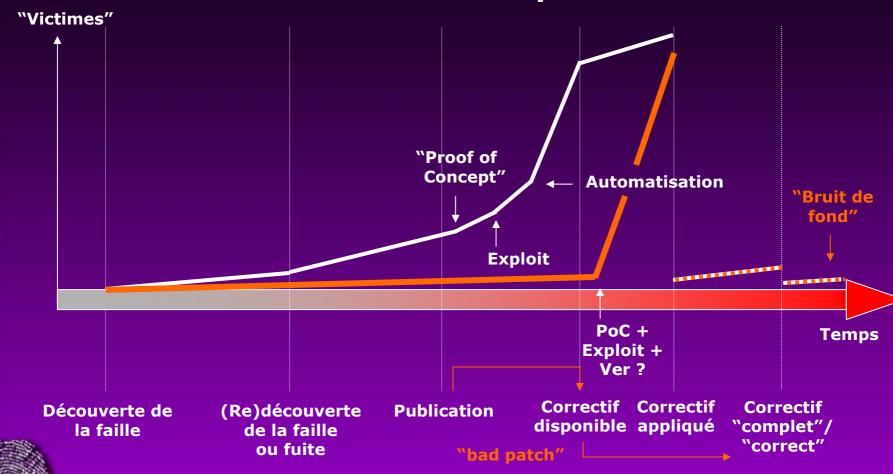




### Virus et vers

المجام المالية المالية

Evolution d'une vulnérabilité: le potentiel "ver"



> Facteur clé: exploit "générique" ? [Messenger vs LSASS]



#### **» MEECES**

- > Money
- > Ego
- > Entertainment
- > Cause
- > Entrance into social groups
- > Status

### Max Kilger (Honeynet Project)

- > S'applique à "l'underground"/pirates/"chapeaux noirs"
- > Référence à MICE (Money, Ideology, Compromise, Ego) agences de (contre) espionnage [INTEL]





- » Les activités "courantes"
  - > Cause/Hacktivism:
    - Dégradation de sites web
    - DDoS (SCO, WU/MSFT, etc)
  - > Ego/Status:
    - "I have more (network) power than you"
    - "I'm not going to loose that item in <online game>"
  - > Entertainment
    - "Hey look, I just DoSed <favorite IRC user/website>"
  - > Entrance into a social group
    - "Wanna trade this botnet?"



#### » Les activités "courantes"

- > [Virtual] Money:
  - Routeurs "BGP"
  - SPAM, botnets, relais ouverts, etc.
  - Numéros de CB, comptes eBay, etc.

#### » Et aujourd'hui ? L'argent !

- > "Pay or get DDoSed"
- > Vers pour diffuser du courrier non sollicité
- > Crime organisé/organisations mafieuses appliquant des techniques ancestrales à l'Internet (racket)
- > Cibles: commerce en ligne, sites de gaming, gambling, betting



### » Ce qui a changé

- > Perdre un botnet n'est pas une tragédie
- > Des outils d'acquisition en masse sont nécessaires
- > Les auteurs protègent leur propriété (hôte et canal de communication)
  - IRC/P2P/protocoles méconnus/IPv6 (anonyme)
  - Sécurisation de l'hôte pour éviter les infections multiples
- > Plus pour le plaisir et pour tuer le temps (connaissances en réseau et techniques/technologies de filtrage)
- > Les connaissances, le niveau, l'organisation et la hiérarchie ne sont pas différents/moins bons dans le monde "underground"... tout sauf le monde chaotique auquel on pourrait s'attendre



### » Ce qui a changé

- > Quelques centaines d'euros correspondent à un salaire annuel dans des pays pauvres
- > L'AP et l'AdS sont les sources principales (en plus de .ro)
- > Le profil idéal: bonne éducation, habite dans un pays avec un fort taux de chômage, ...
- > La majorité des communications se fait en ligne (Internet), les communications "hors bande" se limitent à des réunions de "hackers" ou des appels locaux
- > Avez-vous les ressources nécessaires pour analyser des To de journaux IRC provenant d'hôtes compromis/pots de miel (en x différentes langues) ?



### » Acteurs impliqués

- > Editeur
- > CERT
- > Anti-virus
- > FAI
- > Entreprise
- > Utilisateur



### » Acteurs impliqués

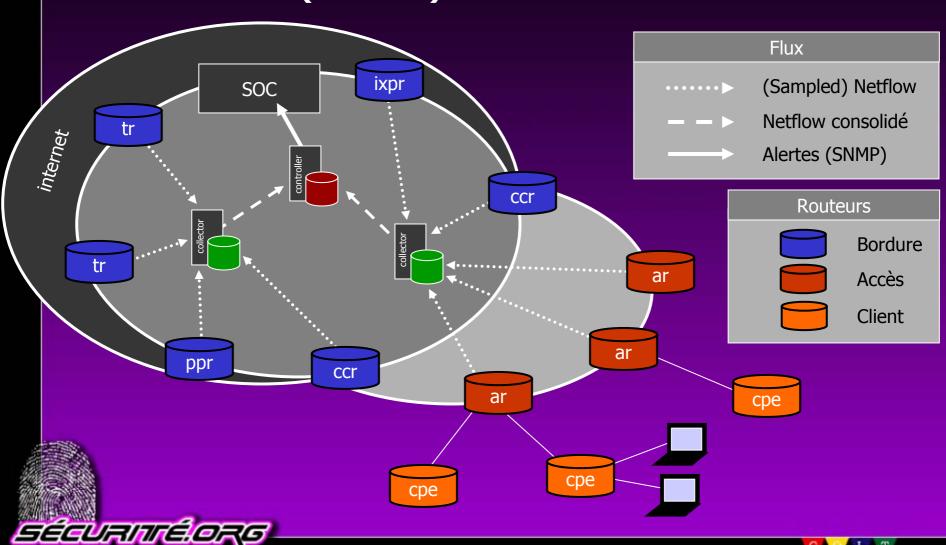
- > FAI
  - Réseau
  - Systèmes
  - (Sécurité): accès "full" IP, sans filtrage
- > Entreprise
  - Réseau
  - Systèmes
  - Sécurité
    - . Pare-feu: souvent qualifié de ligne Maginot et/ou d'aveugle
    - . Sécurité du poste client: pare-feu, antivirus, privilèges, failles, ...
- > Bien souvent les éléments, comme le réseau, souffrent plus côté entreprise!
- > Mobilité: le ver du lundi matin/retour de vacances

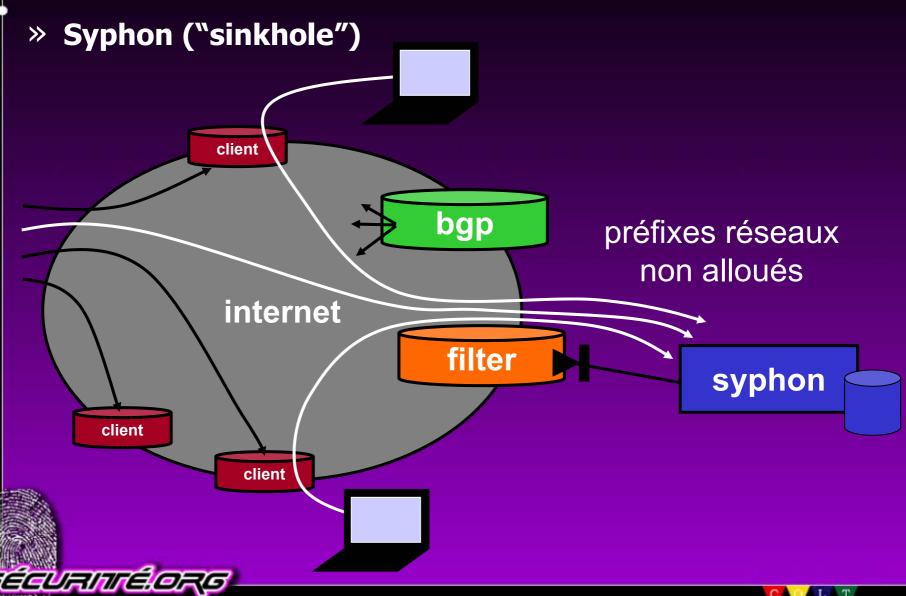


- » Un challenge!
  - > Quels sont les moyens de détecter virus et vers ?
  - > Comment détecter un nouveau vers/virus ayant un impact conséquent rapidement ?
    - moins d'une heure
    - en tenant compte du jour et de l'heure
- » Ces techniques s'appliquent également aux réseaux bureautique/IT internes!



» Flux réseaux (Netflow)





### >> Serveurs SMTP/DNS

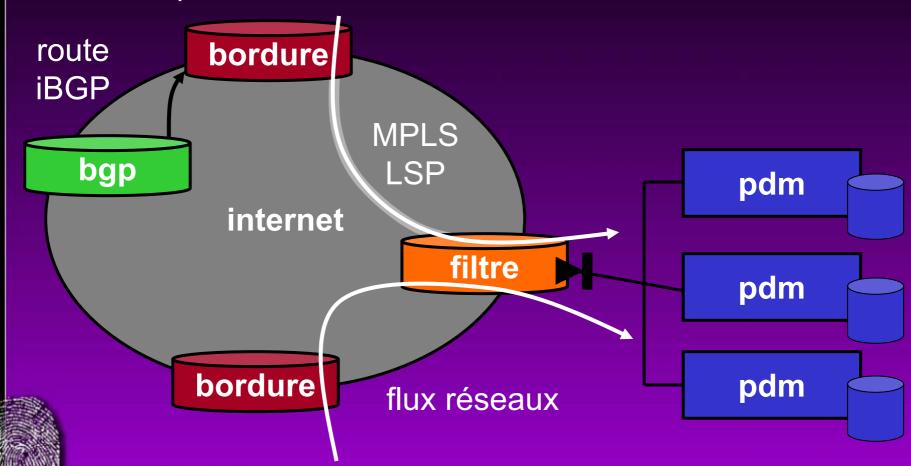
- > Statistiques
- > Journaux
- > SMTP: "Analyser" le contenu (en transit)
  - Mots-clés
  - Fichiers attachés (extension et type)
  - Filtre Bayésien
  - Vipul Razor/DCC (vérification de condensats de messages)
  - Anti-virus "en détection seulement"



» Pot de miel

VAITITÉ!O:

> Pour plus d'interactivité



### >> Tous les FAI ne sont pas égaux face au filtrage

- > Fournisseur de transit international (Tier 1)
- > Opérateur local ou d'infrastructure (Tier 2)
- > FAI avec une base de clients majoritairement du type particuliers/PME (Tier 3)
  - xDSL, cable, dial-in, hotspot wifi, etc.

#### Filtrage: politique et impact

- > Ports "Microsoft"
- > Protégez les utilisateurs ?
- > Donnez du temps pour mettre à jour ?
- > Ne rien faire tant que l'infrastructure ne souffre pas ?
- > Protéger l'utilisateur de l'Internet ou l'inverse ?



### » Filtrage par le réseau

- > ACLs (Access Control Lists)
  - Filtrage sur une partie de l'en-tête
  - Problématique de gestion
- > BGP (Border Gateway Protocol)
  - Routage par rapport à la destination
- > PBR (Policy Based Routing)
  - Routage par rapport à la source (et une partie de l'en-tête)
- > NBAR (Network Based Application Recognition)
  - Identification de l'application (flexibilité)



### » La mise en cage

- > Système identifié comme infecté ou pas à jour (niveau de "patch")
- > Accès limité à l'Internet



- » Couches applicatives (réseau)
  - > L'évolution risque de "sauver" les FAI :-)
  - > "Anything on top of IP" -> "Anything on top of HTTP"
    - SOAP, XML, Web Services
    - Chiffrement
  - > VPN SSL vs IPsec
    - exploit PCT
    - "Attaque" TCP ReSeT
  - > Effet de bord du Service Pack 2 pour WindowsXP



- » Couches applicatives (système) Messagerie
  - > Approche?
    - Marquer
      - . Dossier séparés (POP3 ?)
    - Filtrer/Détruire
  - > Relais de messagerie
    - Pas de filtrage
    - Comment gérer une file qui "déborde"?
  - > Serveur de messagerie
    - Webmail
    - Client



### Conclusion

- » Conclusion
- » A lire également
  - > Backbone and Infrastructure Security
    - http://www.securite.org/presentations/secip/
  - > (Distributed) Denial of Service
    - http://www.securite.org/presentations/ddos/
- » Q&R
- Merci: French Honeynet Project, MISC, SSTIC (Rennes, Juin 2004), experts



