

Evolution des dénis de services et du phishing

v1.1

Nicolas FISCHBACH

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

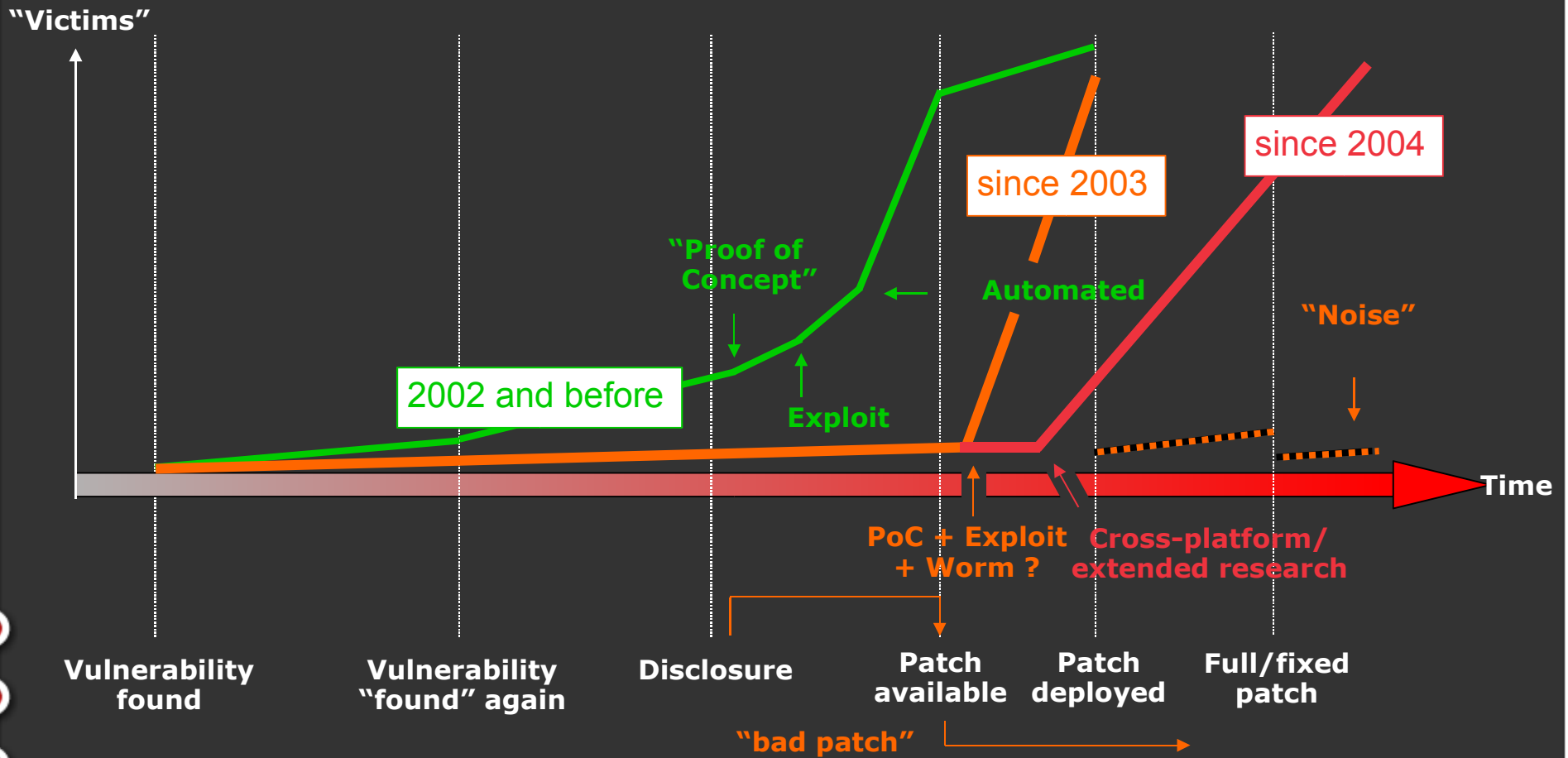
Agenda

- Introduction
- Cycle de vie d'une vulnérabilité
- Les dénis de services
- Les "botnets"
- Le phishing
- Les acteurs
- Conclusion

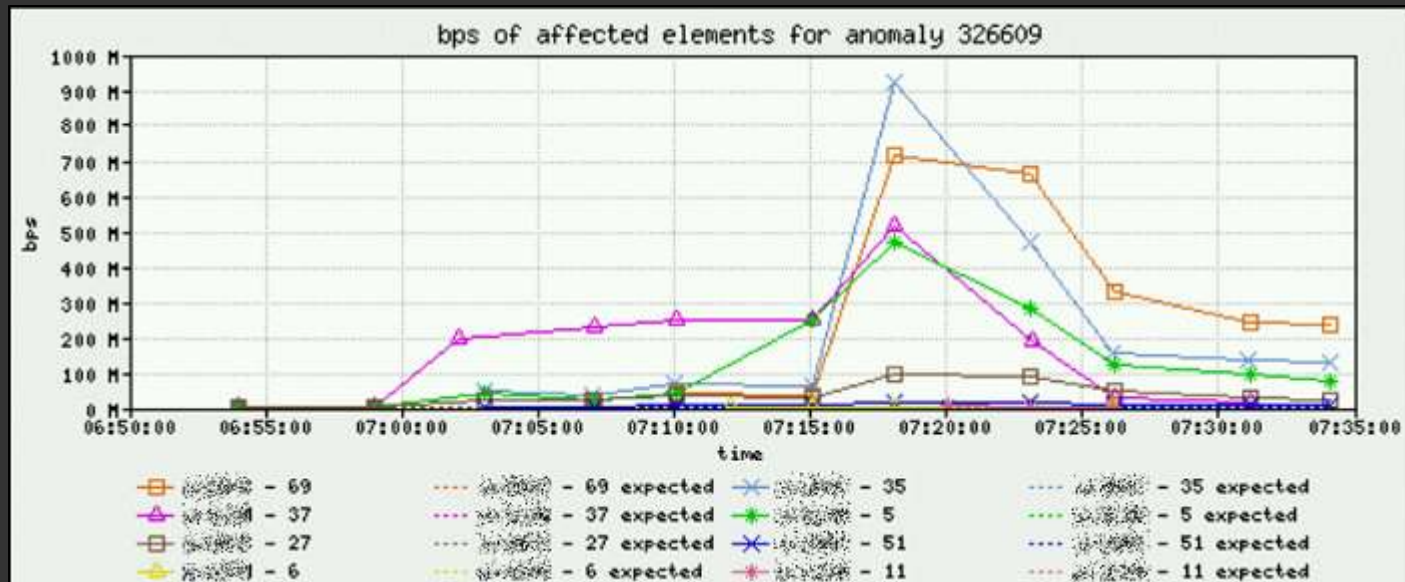


Cycle de vie

EUROSEC 2005



Exemple de DDoS

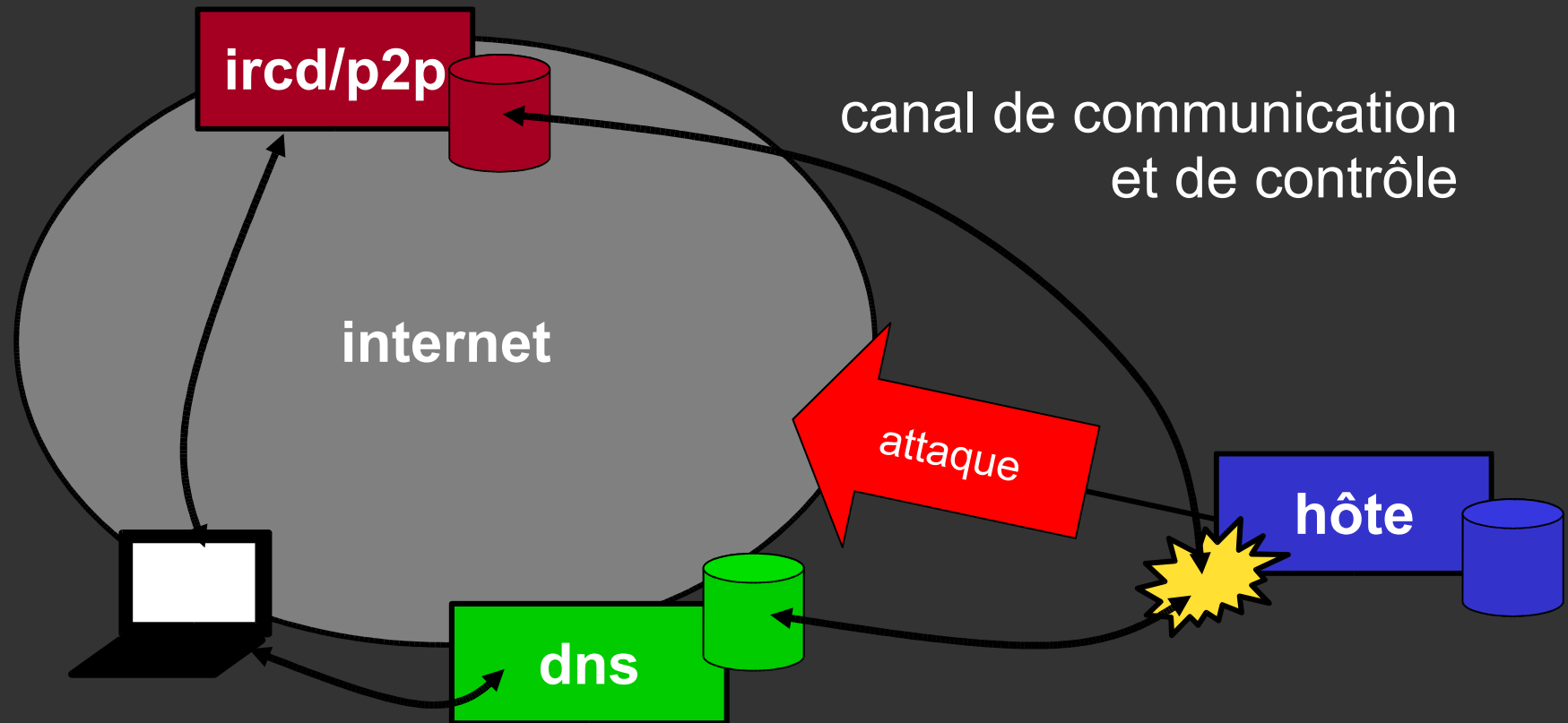


- Environ 3Gb/s de bande passante
- Destination: un hôte, 0/udp

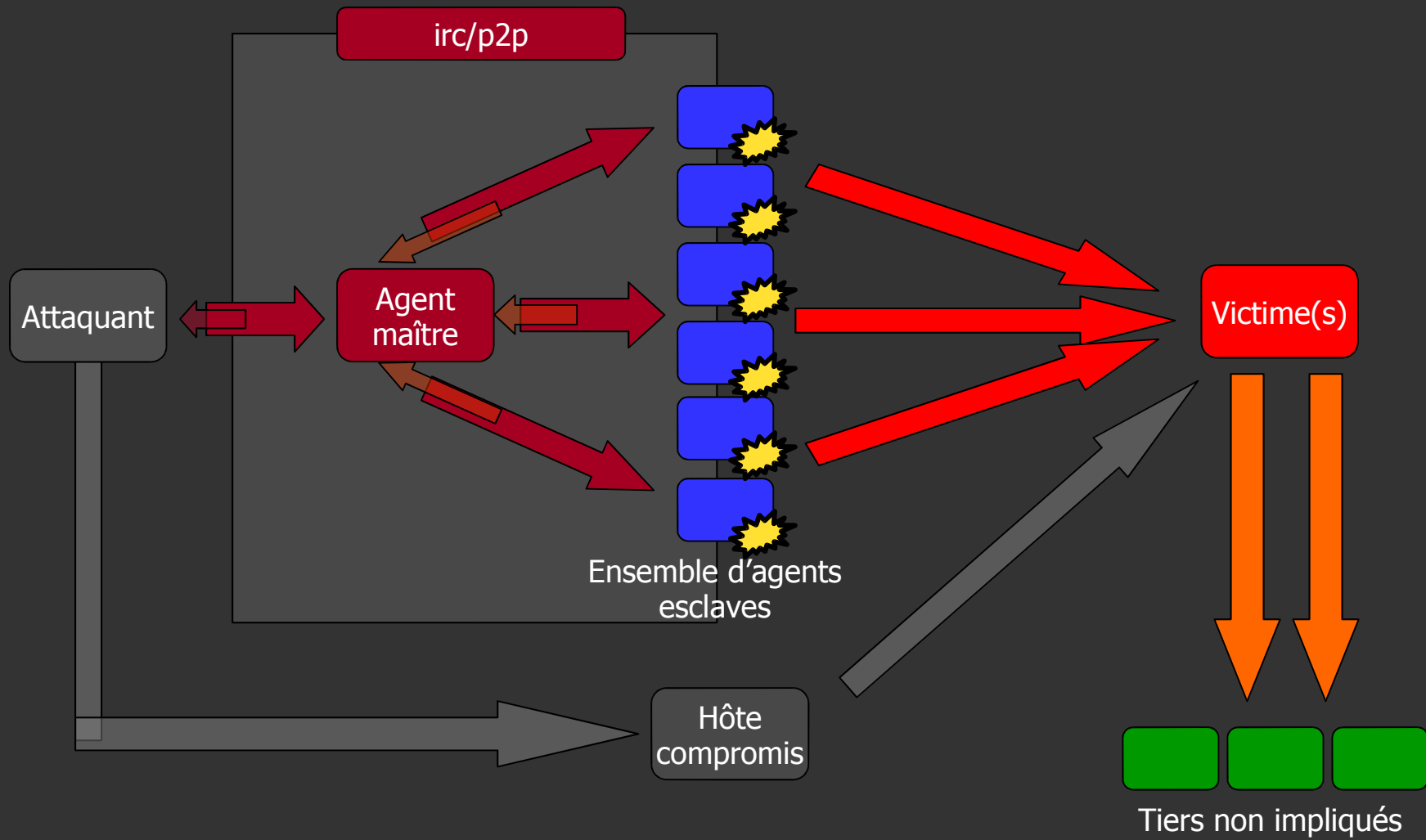
Exemple de DDoS

- Sur 4 mois: 21962 anomalies détectées
 - 5302 High (anomalies traitées)
 - 15513 Medium
 - 1147 Low
- Par jour:
 - ~40 anomalies sont affichées au NMC/NOC
 - Une partie est composée de doublons et de faux positifs
 - En moyenne 20 attaques par jour
 - Un tiers/quart a un impact "important" chez un client

Botnet



Botnet



Botnet

- Quelques chiffres:
 - Environ 600 réseaux "surveillés et connus"
 - Estimation: 2000 à 5000 réseaux
 - De 100 a 5000 agents en moyenne
 - Rarement plus de 10000 agents
 - Prix: de moins de 0.10EUR à plus de 40EUR par agent
 - Mono-infection courante (mais des cas de multi-infection se voient toujours)
 - Puissance de feu moyenne par agent: de 128 à 256Kb/s
- Serveur IRC modifiés et utilisation de *dyndns-like*
- Partage d'empreintes d'attaques

Phishing

- Activité en plein boom
- Anglophone en majorité
- Serveurs "piratés"
 - Exploitation directe
 - Réseau
 - Application web
 - Exploitation indirecte
 - "Google Hacking"
 - "Zombies" reconvertis
 - SPAM via SMTP
 - Cheval de Troie
 - Serveur HTTP

Phishing

- Beaucoup de serveurs en colocation mal protégés
- Répartition 50/50 UNIX/Win32
- 50% des UNIX avec un "renifleur" et un "rootkit"
- Applications: awstat, phpbb, mailman, etc.
- Site principal rarement modifié (sous-répertoires)
- Script basique (PHP, ASP) avec un mail() vers courriel yahoo-like
- Protection: arrêt du service/serveur, "trou noir" réseau, "trou noir" DNS, ... avec des implications légales et de service
- Problème d'autorité: FAI, FAI tiers, PTT, NHTCU, attaqué (banque, entreprise), juge, etc.

Phishing

- Côté client
 - Exploitation de la crédulité et du manque de connaissances
 - Exploitation du navigateur
 - Failles dans le navigateur
 - Utilisation des langages de script (champs cachés ou "surimpression") et objets "actifs" (BHO)
 - Failles dans des librairies (images)
 - Sites à fort trafic piratés (via des tiers: publicité)
 - Détournement de fonctionnalités
 - client: IDN
 - serveur: URL externe encodée dans l'URL principale (via iframe, principe du XSS)
 - Impact des collisions MD5/SHA-1 sur les certificats ?

Les acteurs

- Le gamin boutonneux ?
- L'organisation mafieuse ?
- Diversification (DDoS-for-hire, SPAM, phishing, etc)
- Peu de créateurs, beaucoup de copieurs/profiteurs
- IRC reste le canal de communication principal, mais les plus malins savent rester discrets
- On assiste de plus en plus à des tentatives de vol: les méchants commencent à protéger et défendre leur propriété

Conclusion

- Les nouveaux téléphones portables comme proie de choix ?
- “Offline” phishing: CLI modifié (VoIP)
 - Appel avec CLI de la banque: social engineering
 - Appel avec le CLI du client: mécanisme d’authentification
- Evolution des dénis de services
 - Quelles (propositions de) solutions ?
- Evolution du phishing
 - Quelles (propositions de) solutions ?
- Questions/Réponses