



HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet



ENST Paris
8 mars 2007

L'insécurité du spam

Raphaël Marichez
<Raphael.Marichez@hsc.fr>

- **Origine et impacts du spam**
 - Les victimes
 - Les acteurs
 - L'armement
- **Les stratégies de la lutte dans l'Histoire**
 - L'approche technique
 - Briser la chaîne
 - Rester réaliste

- **Disponibilité**

- Temps gâché
- Difficile à chiffrer
- Evaluer les coûts
 - Taille de la structure
 - « Appliance » dédiée ou compétences internes
 - Risque induit : dépendance; compétence
 - Surestimation des compétences ? (universités)

- **Confidentialité**

- Attaques non ciblées

- **Pourquoi** : auto-alimentation du spam

- **Comment** : carnet d'adresses Outlook

- Hégémonie d'un unique logiciel

- Adresses générées pour l'occasion et... spammées !

- **Confidentialité**

- Attaques ciblées

- **Pourquoi** : piratage, intelligence économique

- **Comment** : le virus destructeur n'existe plus

- L'ère est au cheval de Troyes discret

- La messagerie est le point d'entrée toujours présent






- Les coûts peuvent être démesurés

- Intégration à la politique de sécurité de l'organisme

- **Le mythe du *hacker bulgare***
- **C'est un mythe !**

The 10 Worst ROKSO Spammers

As at
07 March 2007

Rank	Photo	Spammer or Spam Gang	Country
1		<p>Alex Blood / Alexander Mosh / AlekseyB / Alex Polyakov</p> <p>So many Alex & Alexey spamming! Alex Blood tied to Pilot Holding & bbasafehosting.com long ago, then Alex Polyakov posted he owned them. Massive botnet and child-porn spam ring, also pharma, mortgage, and more. May work with Kuvayev and Yambo.</p>	Ukraine
2		<p>Leo Kuvayev / BadCow</p> <p>Russian/American spammer. Does "OEM CD" pirated software spam, copy-cat pharmaceuticals, porn spam, porn payment collection, etc. Spams using virus-created botnets and may be involved in virus distribution.</p>	Russia
3		<p>Amichai Inbar</p> <p>Full scale criminal operation. Spamming porn, illegal drugs and pump-&-dump stock using botnets. Partnered with many of the worst US and Russian ROKSO spammers.</p>	Israel
4		<p>Ruslan Ibraqimov / send-safe.com</p> <p>Stealth spamware creator. One of the larger criminal spamming operations around. Runs a CGI mailer on machines in Russia and uses hijacked open proxies and virus infected PCs to flood the world with spam.</p>	Russia
5		<p>Michael Lindsay / iMedia Networks</p> <p>Lindsay's iMedia Networks is a full-fledged spam-hosting operation serving bulletproof hosting at high premiums to well known ROKSO-listed spammers. His customers spam via botnet zombies</p>	United States California

spamhaus.org

The 10 Worst Spam Origin Countries		As at 07 March 2007
Rank	Country	Number of Current Known Spam Issues
1	United States	<u>2034</u>
2	China	<u>386</u>
3	Russia	<u>277</u>
4	United Kingdom	<u>181</u>
5	Japan	<u>172</u>
6	South Korea	<u>161</u>
7	Germany	<u>137</u>
8	Canada	<u>127</u>
9	Netherlands	<u>127</u>
10	Hong Kong	<u>121</u>

- **Statistiques (polytechnique.org)**
 - Population essentiellement française
 - Cadres et dirigeants
 - Résultats entre le 20 février et le 7 mars 2007 :

USA (tout opérateur confondu)

1er Europe : Proxad (jusqu'en février 2007)

Japon, Taïwan

Wanadoo (5è), Club-Internet

tpnet.pl (Pologne)

Thaïlande, Inde

Italie, Allemagne

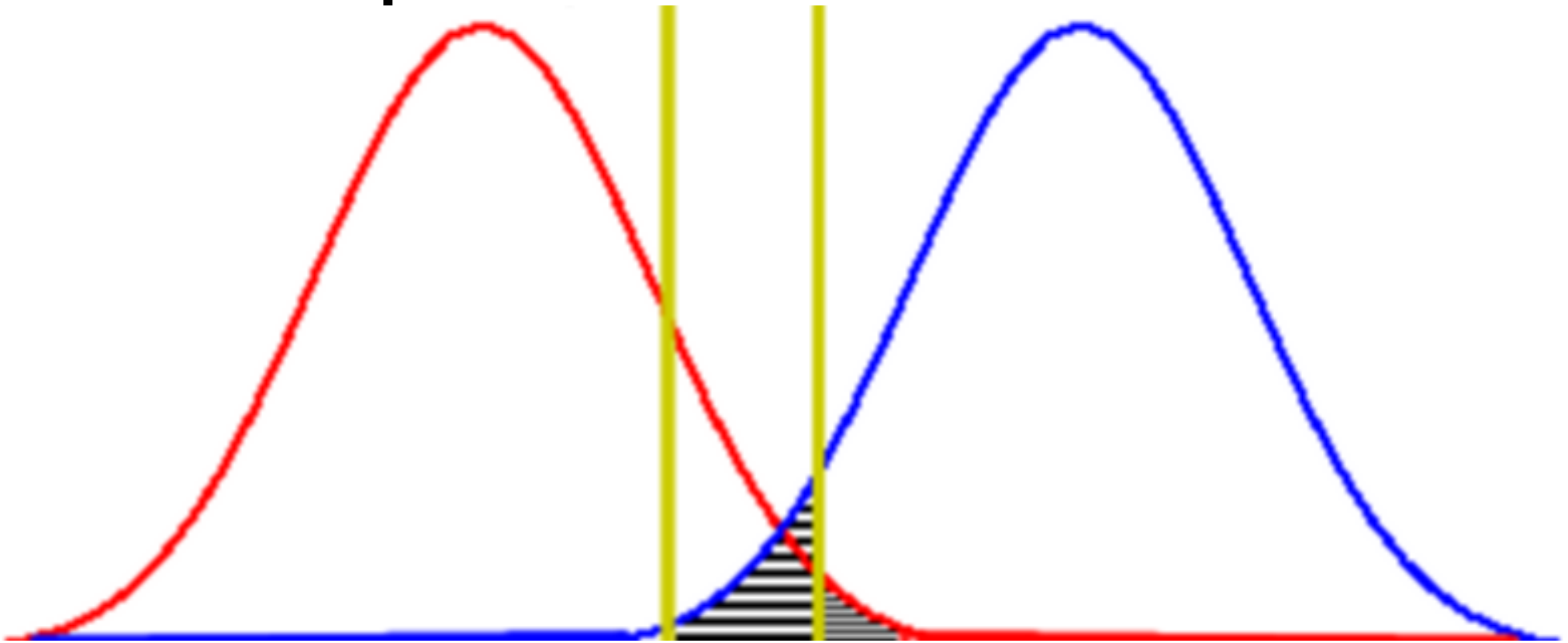
...

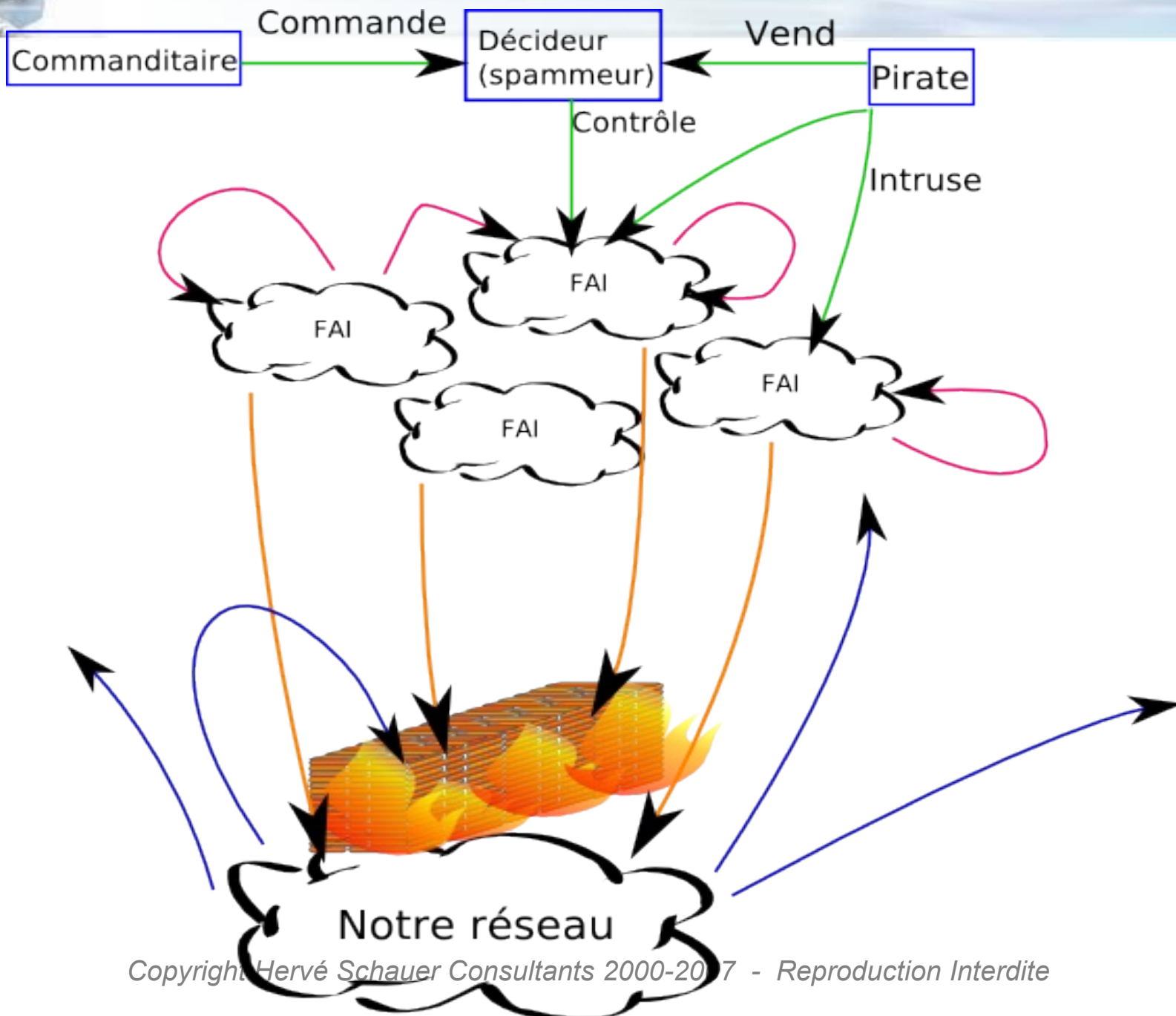
Chine très en retard

- Analyse de signal

spam

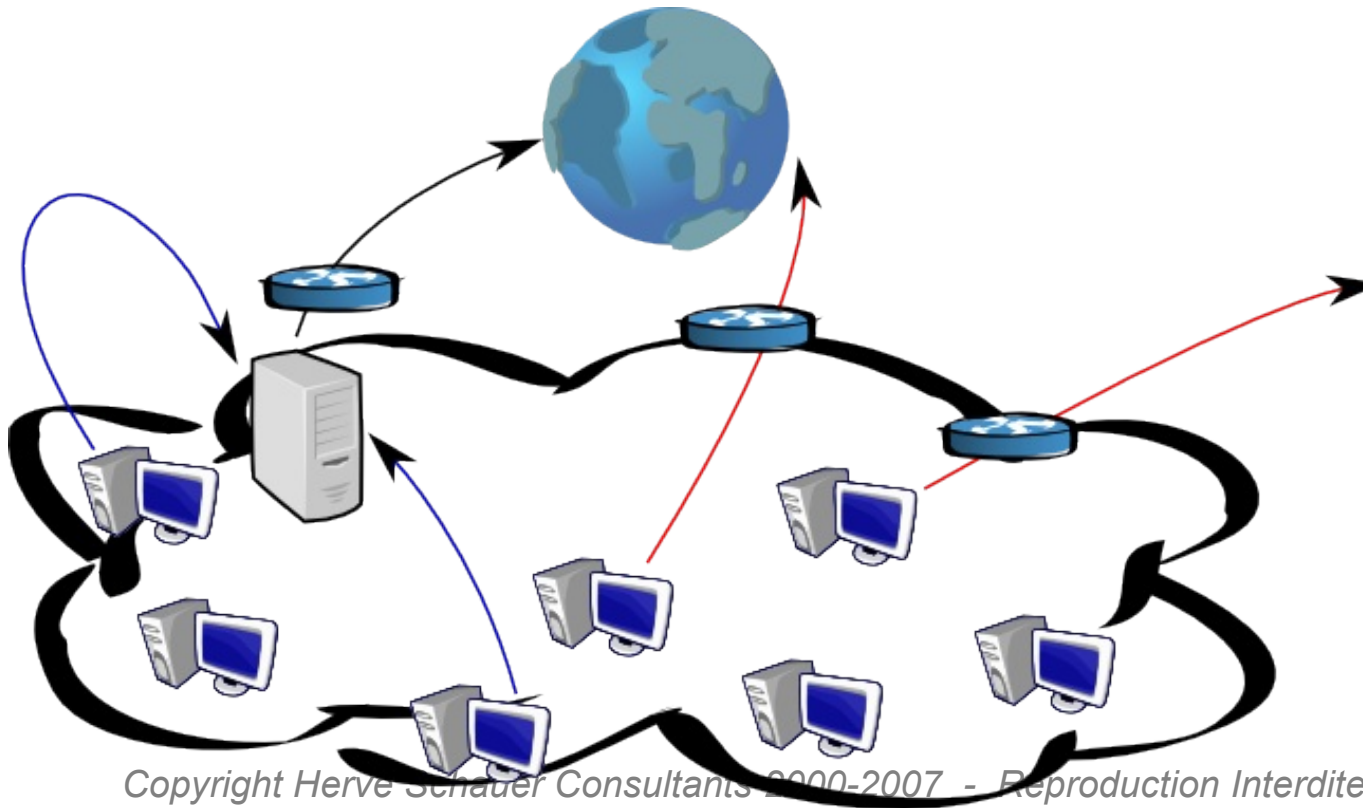
ham





Aujourd'hui on commence à filtrer ce qu'on émet

- Les contre-mesures des autres durcissent et nous affectent
- Nous sommes notre propre spammeur
- Nous contrôlons mieux les émetteurs !



- **Bilan très sombre des dernières années**
 - A cause de l'évolution du paysage Internet
 - Par manque d'évolution de la stratégie de lutte
- **Intégrer cette évolution par le filtrage en sortie**
 - Les premières impressions sont positives
 - Enfin une **légère** diminution sur Polytechnique.org
 - Législation sur un filtrage en sortie ?
 - Serait plus efficace que contre les spammeurs
 - On a bien des réglementations sur la pollution !