



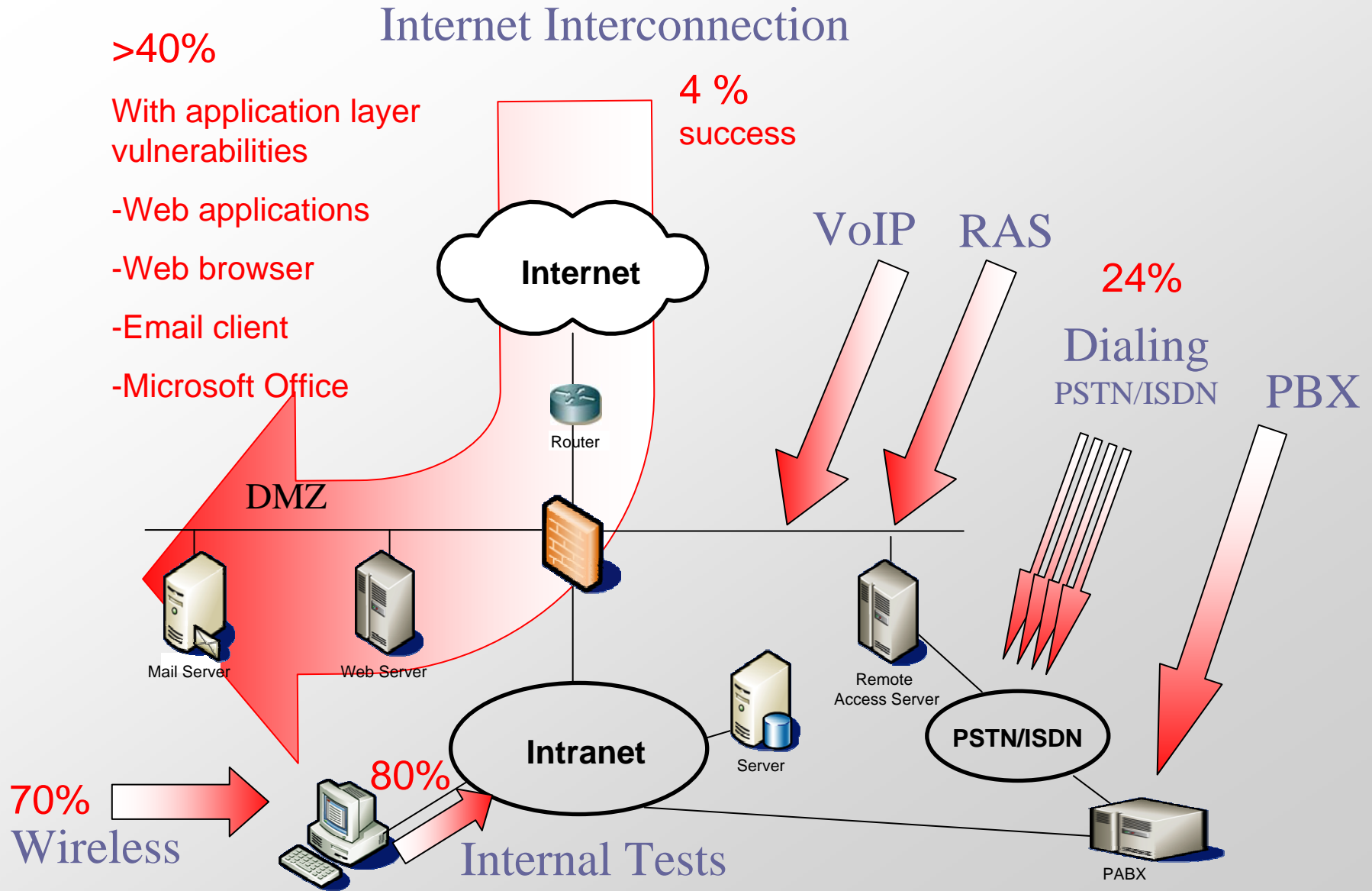
CLUSIR - Les nouvelles menaces

<hr/>	
Cedric GENOYER	
Directeur SRC	
  <small>branche CONSEIL & FORMATION</small>	Telindus Security Research Centre
	GSM +33 (0)6 14 17 17 01
	E-MAIL cedric.genoyer@telindus.fr

DÉMONSTRATIONS D'INTRUSION

17 mai 2006

SRC Statistics : Successful Intrusive Tests



DÉMONSTRATIONS/PRÉSENTATION

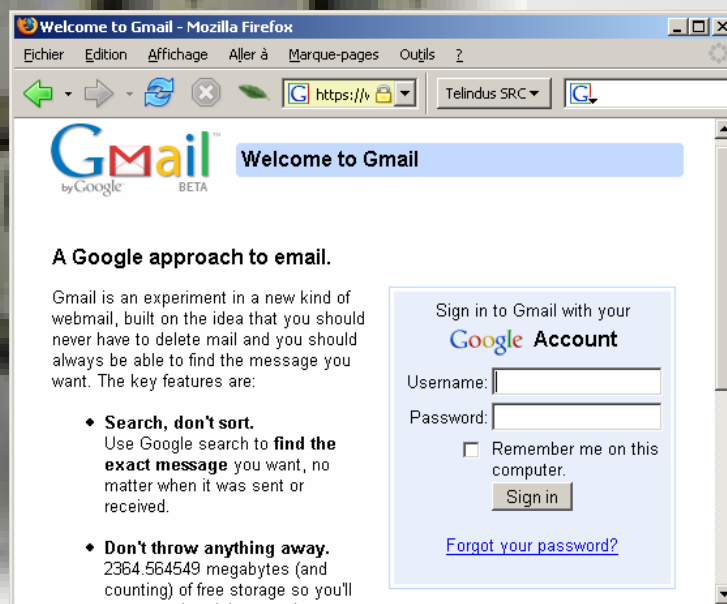
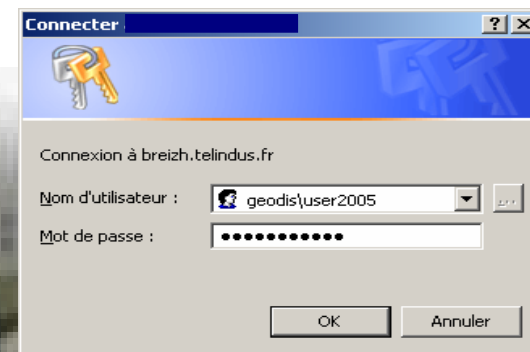
> Les attaques purement réseau depuis Internet sont de plus en plus contrées:

- > Firewall & IDS entre Internet et LAN
- > Flux autorisés limités (ex: blocage P2P, accès Web par proxy, etc...)

> Les pirates, comme les virus et vers s'attaquent

- > aux "faiblesses" humaines (utilisateurs et/ou administrateurs)
 - > Droits des utilisateurs trop importants (demo 1 = boot CD, boot USB, boot réseau)
 - > Complexité des mots de passe (demo 2 = crack base SAM + base Rainbow)
 - > Utilisation du même mot de passe sur plusieurs systèmes (explication attaque DC)
 - > Manque de sensibilisation / Espionnage (visuel, matériel, logiciel) (**demo 3 = keylogger physique**)
- > aux couches applicatives:
 - > Faiblesses de Windows (demo 2 = base Rainbow expliquée)
 - > Vulnérabilités des outils Office (ex: Microsoft Office) (demo 3 = ajout compte utilisateur)
 - > Vulnérabilités du browser Internet (**demo 4 Serveur Web Malicieux – « keylogger » logique**)
 - > Exploitation des flux applicatifs autorisés (**demo 5 = Cheval de Troie**)

ESPIONNAGE / KEYLOGGER



VULNERABILITES DES APPLICATIONS

> **Les outils de bureautique courants:**

- > Microsoft Office
- > Web Browser
- > Client Mail
- > Etc...

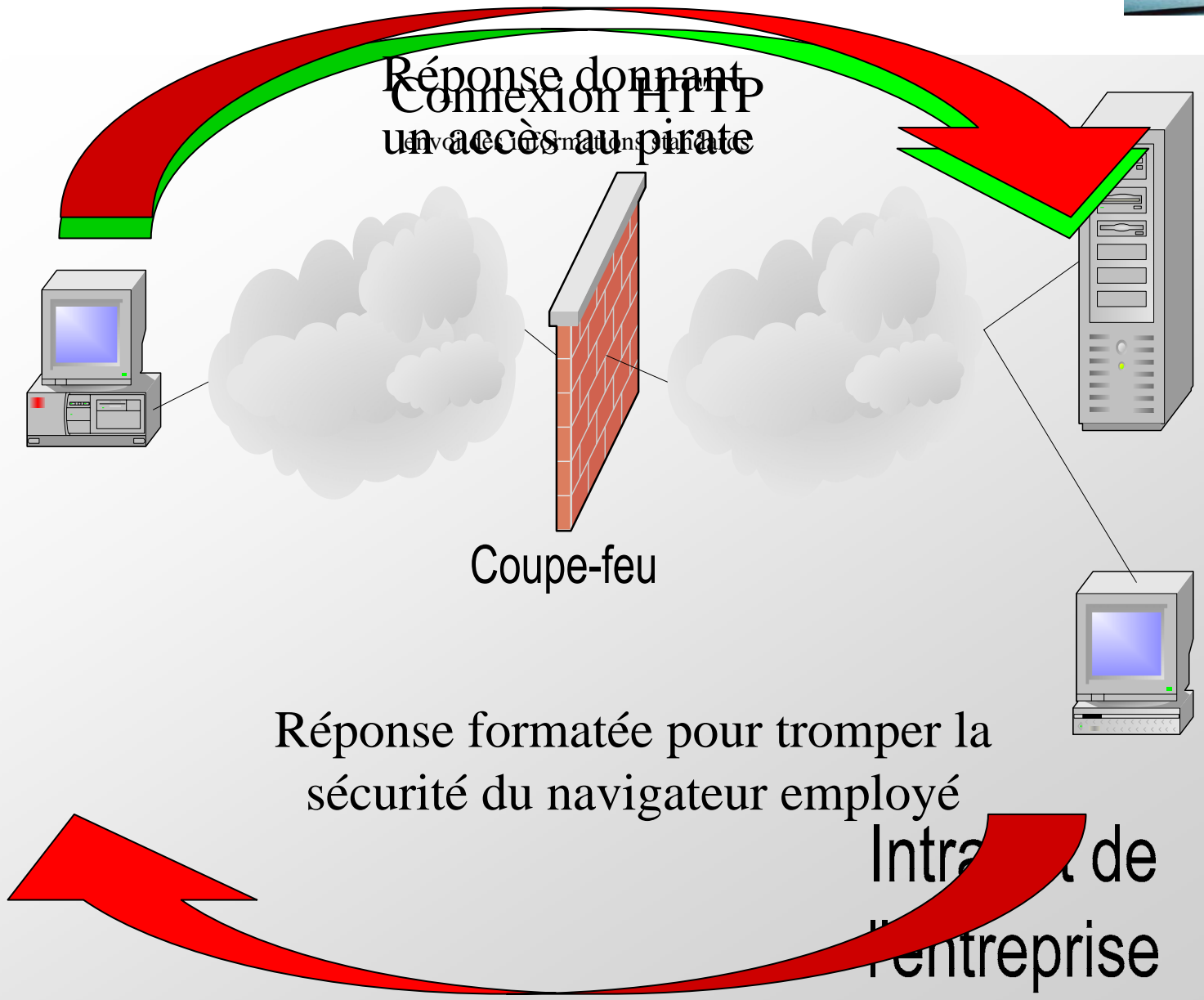
> **Les applications de sécurité**

- > Antivirus
- > Firewalls personnels
- > Anti spywares
- > Etc...



- > Si le navigateur contient des failles de sécurité non corrigées, un simple click sur une page web peut aboutir à :
 - > La manipulation des champs visibles dans le browser
 - > Adresse (URL) d'un Lien cliquable
 - > Adresse (URL) de la page courante
 - > L'espionnage des données saisies dans une autre fenêtre du browser
 - > Le vol de fichiers de la victimes
(ex: fichier de comptes et mots de passe / base SAM)
 - > L'installation d'outils d'attaque / d'un cheval de Troie sur la victime
 - > La prise de contrôle à distance du poste victime
 - > L' attaque de l'Intranet à travers la victime

SERVEUR WEB MALICIEUX



Navigation sur Internet & intrusion



8



> **A noter :**

- > La connexion provient à l'origine de l'utilisateur lui-même
- > Attaque pouvant contourner les systèmes de coupe-feu (firewalls)
- > Le navigateur le plus employé (Microsoft Internet Explorer) est aussi celui contenant le plus de failles de sécurité
- > Un utilisateur peut s'infecter ainsi en navigant depuis son domicile, puis apporter le même ordinateur au bureau et ainsi infecter le réseau interne

STRATÉGIES D'ATTAQUE

- > **Toutes ces faiblesses peuvent être combinées pour créer des scénarios d'attaques plus complexes pour:**
 - > Obtenir un contrôle plus important
 - > Obtenir un résultat plus rapidement
 - > Réduire la visibilité de l'attaque

- > **De plus, les points d'accès permettant d'entrer sur le réseau interne sont nombreux...**

Merci de votre attention.

