Université
De Boumerdes

Université
De Limoges

Département d'informatique
M2

Menaces (failles de sécurité, Attaques et vulnérabilités)

Réalisé par : Dr RIAHLA
Docteur de l'université de Limoges (France)
Maitre de conférences à l'université de Boumerdes

Objectif

- Comprendre les différents types de menaces présentes
- Comprendre comment se protéger efficacement
- Mieux savoir juger l'impact d'une nouvelle menace.

Université
De Boumerdes

Université
De Limoges

Département de physique/Infotronique
IT/S6

Introduction

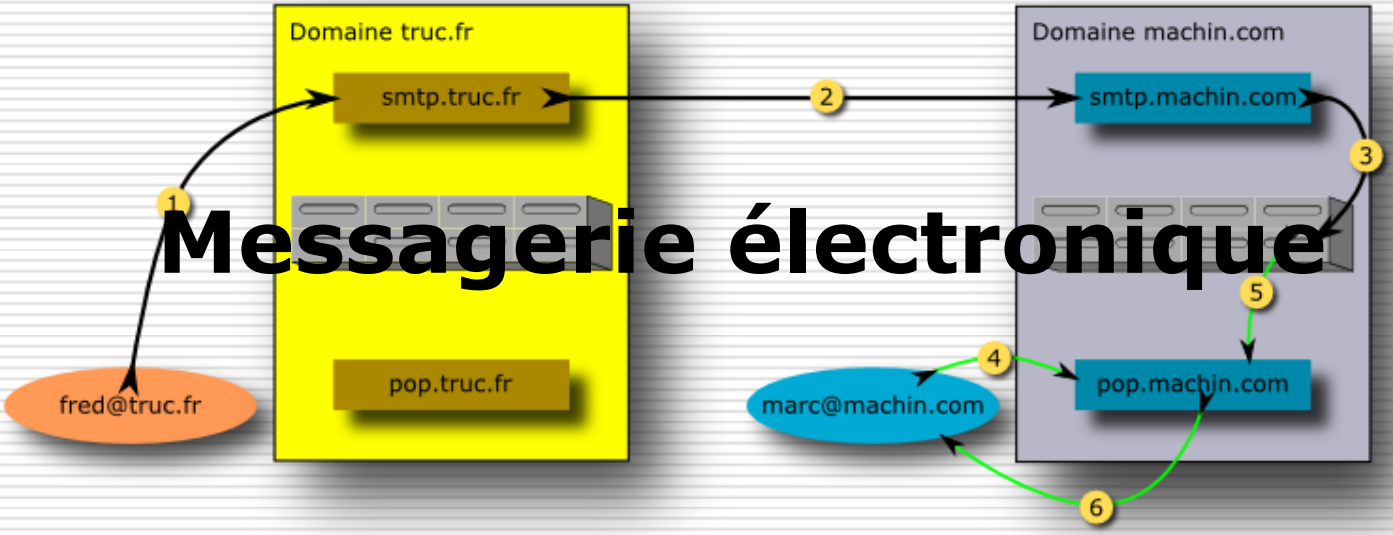
Réalisé par : Dr RIAHLA
Doctorant a l'université de limoge (France)

Université
De Boumerdes

Université
De Limoges

Département de physique/Infotronique
IT/S6

Messagerie électronique



Réalisé par : Dr RIAHLA

2008/2009

Messagerie électronique

La messagerie électronique constitue un véritable outil de travail et de productivité pour les organisations, elle est le plus souvent considéré comme une application stratégique, voir critique.

Messagerie électronique

- De par la conception du système de messagerie, le contenu des messages circule en clair sur le réseau. Cela doit en limiter l'usage au transfert de données non confidentielles.

- Dans ce contexte, il est impératif de savoir protéger le système de messagerie et d'en garantir sa sécurité.

Messagerie électronique (Risques)

- La perte, l'interception, l'altération et la destruction de messages.
- L'infection des systèmes par le biais de messages contenants des virus, vers ou cheval de Troie par des pièces jointes.
- Inondation de messages.
- L'usurpation d'identité des utilisateurs

Messagerie électronique (Risques)

- Des messages peuvent être introduits, rejoués, mélangés, supprimés ou retardés
- Refus de service par défection d'un élément de la chaine du système de messagerie
- La divulgation d'informations confidentielles.
- La répudiation (un acteur du système nie avoir envoyé ou reçu un message)

Messagerie électronique (Forgé un mail)

SMTP utilise des connexions TCP sur le port 25

Il connaît quelques simples commandes comme :

HELO (annonce d'un serveur)

Mail From: (définition expéditeur)

Rcpt To: (définition destinataire)

Data: (définition du contenu)

telnet mail1.epfl.ch 25
Trying 128.178.7.12...
Connected to mail1.epfl.ch.
Escape character is '^]'.
220 mail1.epfl.ch ESMTP
HELO batcave.com
250 mail1.epfl.ch
MAIL FROM: batman@batcave.com
250 ok
RCPT TO: philippe.okamp@epfl.ch
250 ok
DATA
354 go ahead
Is it a bird? Is it a plane?
or is it just a forged e-mail?
.
250 ok 1004541790 qp 14607
QUIT
221 mail1.epfl.ch
Connection closed by foreign host.

Messagerie électronique (Spams ou pourriel)

- E-mail non-sollicité, non-ciblé, à très grand tirage
- L'adresse source est toujours falsifiée
- Un message est déposé dans une centaine de serveurs SMTP avec une liste de >10k destinations chaque fois
- Les serveurs abusés envoient fidèlement une copie à chaque destinataire
- Recherche aléatoire de destination

Messagerie électronique (*Spam: Dégâts*)

- Les serveurs abusés sont surchargés (souvent plus de 24h)
- Les disques se remplissent de logs et de messages (risque de blocage)
- La bal de l'admin est inondée de messages d'erreurs (adresses invalides)
- L'ISP peut menacer de couper la ligne
- Inclusions dans listes noires

Messagerie électronique (*Spam: Dégâts*)

- Encombrer inutilement une partie de la bande-passante

- Le spam induit des coûts supplémentaires pour les fournisseurs d'accès à internet (FAI)

- Ces frais supplémentaires se répercutent sur les abonnés

Messagerie électronique (*Spam: Dégâts*)

Mettre en place une plus grande largeur de bande

Acheter des serveurs supplémentaires pour gérer le spam

Disposer d'un plus grand espace disque

Engager du personnel supplémentaire pour traiter les réclamations

Messagerie électronique (*Attention de :*)

- Répondre au spam, car cela peut permettre aux spammeurs de savoir que votre adresse électronique est valide ;

- Menacer les spammeurs, cela ne ferait que les énerver.

- Bombarder les spammeurs de courrier électronique.

- Spammer les spammers (dépourvu de bon sens).

Messagerie électronique (*Spam: Protection*)

Serveur:

- interdire le relais

Source:

- Liste noire de serveurs

Contenu: Filtre anti-spam

- Mots-clés, format
- Données annexes (temps de transit, nombre de destinataires…)
- Listes noires de spams connus

Messagerie électronique
Spam: évolution

Botnets

- Les hackers utilisent des vers et des virus pour installer des robots sur les machines infectées
- Les hackers louent des réseaux de zombies à des spammers (5'000 bots x 1 semaine = 350$)

Messagerie électronique
Spam: évolution

Les lois deviennent efficaces:

- PW Marketing a été condamné à $2mio d'amende en Californie
- Jeremy Jaynes condamné à 9 ans de prison en Virginie

Nb: il gagnait 400'000$ par mois avec un taux de retour de 1 sur 30'000

Université
De Boumerdes

Université
De Limoges

Département de physique/Infotronique
IT/S6

Virus, vers, chevaux de Troie et autres

Réalisé par : Dr RIAHLA

2008/2009

Virus

- fragment qui se propage à l'aide d'autres Programmes
- Portion de code inoffensive ou destructrice capable de se reproduire et de se propager.

Types:

Virus boot

Virus dissimulé dans les exécutables

…

– Échange de disquettes
– Pièces jointes au courrier électronique
– Exécutables récupérés sur Internet

Vers

- Programme autonome

- Proches des virus mais capables de se propager sur d'autres ordinateurs à travers le réseau.

- Un moyen courant de propagation: le carnet d'adressesd'outlook (ex: "I Love you": déni de service sur les serveurs web).

Exemples: (code red, blaster)

Cheval de Troie
troyen, trojan horse, trojan :

- Dérivée de la mythologie grecque.
- Comme les Grecs cachaient des soldats dans le ventre d'un cheval en bois lors de la guerre contre Troie, cette malware (troyen) en fait de même.
- Le "troyen" est un programme malicieux (ou utile) qui en cache un autre.
- Le programme caché est en principe un "keylogger".

Cheval de Troie
troyen, trojan horse, trojan
Exemple

- Le premier programme malicieux (principal) ouvre les ports de communication.

- Le deuxième programme malicieux, le “keylogger” copie toutes ces données , elles seront envoyées et connues par le programmeur de ce code malicieux.

- Ordinateur téléguidé donc botnet

Virus, Vers et autres malwares

Backdoor: Accès caché à un ordinateur pour gérer un ordinateur à distance (Installés par des chevaux de Troie):

Taille: plus il est petit, plus il est facile à installer

Fonctionnalités: téléchargement d'autres programmes, espionnage réseau, écran, clavier.

Mode de communication: Attente sur un port TCP ou UDP prédéfini.

Virus, Vers et autres malwares

- **Rootkit**: logiciel qui masque la présence d'un intrus.

- **Spyware**: logiciel qui transmet des informations privées, Il modifient le comportement des browsers

- **Autres** (hoax, bombes logiques, DOS,…)

Effet des Virus et malwares

- Perte de données
- Perte de temps de travail
- Perte d'image de marque
- Perte de fonctionnalité (e-mail ou systèmes bloqués)
- Intrusion, vol
- Perte de confidentialité

Virus Modernes

- Les virus modernes utilisent Internet pour se propager activement
- Il peuvent infecter la planète en quelques heures
- Efficaces, car ils se propagent plus vite que les anti-virus peuvent être mis à jour

Bugbear (septembre 2002)

- Virus qui se propage comme attachement d'e-mails

- Il utilise une faille de MS-IE (outlook, outlook-express) pour s'exécuter automatiquement -> activemail

- Il se propage automatiquement par e-mail en faisant des forwards ou des reply à des mails qu'il trouve sur son hôte.

- Il se propage se copiant dans le répertoire d'autres PCs qui partagent leurs disques -> ver.

Bugbear (septembre 2002)

- Il installe un backdoor sur les machines infectées (transfert de fichiers, exécution de programmes)
- Il désactive tous les antivirus et firewalls qu'il connaît
- Il envoie une copie de tous les mots de passe que vous avez enregistrés à une série de bals sur Internet
- Il installe un espion de clavier (keylogger)

Exemples

- SQL-Slammer
- Le Canular
- Joke
- Publicité virale (idem)

Merci