Contexte

Les solutions actuelles

Une solution

Les critères pour une autre solution

La détection

La mise en quarantaine

La sortie en quarantaine

Conclusion

Quarantaine automatique de postes infectés

Fabrice Prigent

Université Toulouse 1 Sciences Sociales

25 avril 2007

Du nomadisme

Le nomadisme s'étend

- la généralisation des portables
- les possibilités d'accès sans-fil accrues
- les procédures administratives et logistiques simplifiées (Eduroam, etc.)
- les modes de vie changent

Une compétence minime

Les utilisateurs sont exigeants, et en même temps peu compétents. Cela a trois conséquences

- la quasi-totalité des services "courants" doit être proposée
- l'accès doit être facilité (préférer les portails captifs au 802.1x)
- les procédures de sécurité minimales ne sont pas respectées

Des possibilités d'interventions réduites

Les postes nomades sont rarement manipulables par les équipes informatiques car

- Ils ne sont pas propriété de l'établissement
- L'utilisateur ne peut/veut pas venir au service informatique
- L'utilisateur n'a pas forcément les droits administrateurs

Des possibilités d'interventions réduites

Et même quand ils le sont, ils ne sont bien évidemment

- pas prêtés au fiston pour récupérer le dernier jeu à la mode sur un site avec 40 spywares par minute,
- pas emprunté par la fille pour chater de choses terrrrrrriblement importantes
- pas utilisés pour visiter des sites russes pour âmes esseulées avec trojan en bonus

Des risques accrus

Le tableau sécuritaire d'Internet se noirci

- Des vulnérabilités de plus en plus rapidement exploitées
- Des répercussions juridiques de plus en plus courantes

Le portable est isolé

La solution consiste parfois à isoler les portables quasiment comme s'ils étaient extérieurs.

- Efficace vis à vis de l'interne
- Mais seuls les services publics sont accessibles
- Quid des risques juridiques

Le NAC

Les solutions Network Access Control ont pour but de vérifier l'adéquation des postes avec la politique de sécurité de l'établissement.

- présence d'un firewall
- présence d'un antivirus
- des signatures à jour
- clés de registre positionnées.

Le poste reste en quarantaine tant que la politique n'est pas respectée. Installation, activation, mises à jour des process de sécurité sont cependant autorisées.

Le NAC : les problèmes

Mais ces solutions ont plusieurs défauts

- Comment sont traités les postes Linux, Mac OS ?
- Il faut un client logiciel
  - qui doit être installé et géré (solution par module java)
  - qui pose parfois des problèmes de compatibilité
  - qui n'est pas toujours installable
- Avoir un antivirus à jour n'a jamais empêché d'avoir un virus (2 cas "explosifs" en 3 ans).
- Ils sont (très) payants

Les critères

Plusieurs points sont apparus nécessaires avec les années. Ils concernent

- Les postes
- L'attaque
- La solution dans sa globalité

Les critères sur le poste

- Aucune intervention ne doit être nécessaire sur les postes
- Aucun postulat sur le poste : la solution est agnostique. Microsoft n'est pas toujours responsable, (après tout, même une horloge arrêtée a raison 2 fois par jour).
- L'utilisateur ne doit pas voir la protection en temps normal

Les critères sur l'attaque

- Le moins de postulats possible sur l'attaque : elle peut venir de n'importe quel service

Les critères sur la solution

- Le système doit être automatique : les administrateurs ne sont pas forcément présents
- La solution doit être d'un coût raisonnable quelque soit le nombre de postes
- La protection doit prévenir l'utilisateur (afin de prévenir toute agressivité).

Détecter le problème

Des critères précédents, on déduit rapidement que l'on doit détecter le problème de l'extérieur du poste. Nous disposons donc de tous nos équipements pour celà.

Que fait un attaquant (automatique ou non) ?

Il utilise de manière anormale et généralement répétée un service pour obtenir une action profitable pour lui.

Prenons quelques exemples.

Détecter un virus par mail, spammeur, etc.

Quarantaine automatique de postes infectés

Fabrice Prigent

Contexte

Les solutions actuelles

Une solution

Les critères pour une autre solution

La détection

La mise en quarantaine

La sortie en quarantaine

Conclusion

Son comportement va occasionner des tentatives de connexions répétées sur les services de courrier. On le repère donc par :

- Les journaux du firewall qui interdit les sorties SMTP ne provenant pas du serveur officiel
- Le serveur SMTP officiel qui détecte une trop grande fréquence d'envois
- Le serveur SMTP officiel qui détecte un trop grand nombre d'expéditeurs pour une même machine

Détecter un ver microsoft , etc.

Son comportement va occasionner des tentatives de connexions répétées sur les services de partage. On le repère donc par :

- Les journaux du firewall qui interdit les sorties Netbios
- Le firewall interne qui interdit les communications Netbios
- Les firewall des serveurs qui bloquent les communications Netbios

Détecter un ver PHP, ASP, etc.

Quarantaine automatique de postes infectés

Fabrice Prigent

Contexte

Les solutions actuelles

Une solution

Les critères pour une autre solution

La détection

La mise en quarantaine

La sortie en quarantaine

Conclusion

Il s'attaque au serveur Web. On le repère donc par :

- Un trop grand nombre d'erreurs 404
- Une anormalité de paramètres sur les requêtes standard

On voit là qu'il est particulièrement intéressant d'avoir un détecteur d'anomalies, et donc de caractériser la normalité. Pour nous c'est

- 50 lignes de perl (deviator)
- 800 lignes d'expressions régulières
- moins de 1% de CPU

Détecter un brute-forcer.

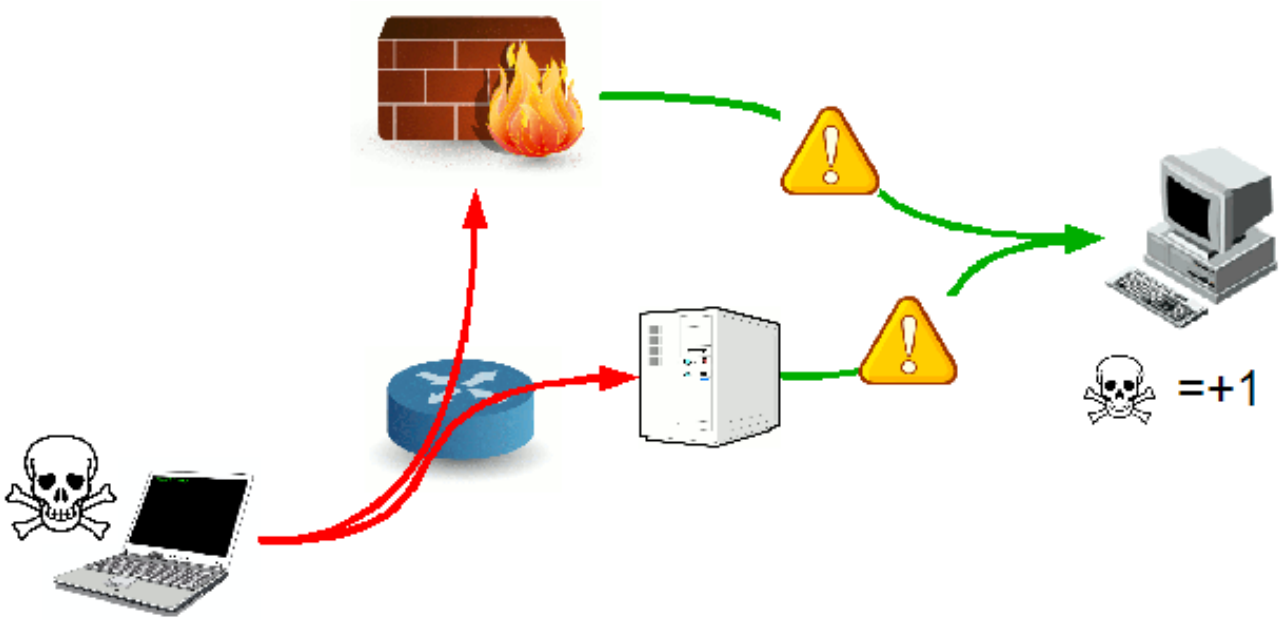
Il s'attaque aux serveurs avec authentifications. On le repère donc par :

- Un trop grand nombre de connexions
- Un trop grand nombre d'erreurs de login
- Un trop grand nombre d'erreurs de mot de passe

De manière générale

On détecte la répétition d'un événement anormal. On prendra garde de ne pas réagir trop rapidement : les utilisateurs ont le droit de se tromper.
Chaque serveur, firewall, équipement, doit donc remonter l'information en un point central de corrélation.

Schéma de la détection



Le coordonateur

La machine responsable du monitoring doit être capable de réagir aux incidents. Cela peut être fait de plusieurs manières, mais nous ne détaillerons que la solution actuellement déployée

- Le coordonateur envoie à chaque serveur une liste des machines en quarantaine
- Chaque serveur exécute alors le protocole de quarantaine associé
  - Blocage pur et simple
  - Blocage avec avertissement
- Le firewall intercepte toutes les communications web et les renvoie vers un serveur web interne.
- Si la requête est à destination d'un serveur de désinfection, la communication est autorisée.

L'avertissement

Il est évident qu'un utilisateur bloqué réagira mal. Sauf si

- Il est clairement averti du problème
- Il est averti immédiatement du problème (celà lui permet de savoir qu'il vient de faire une conn....une ane...une erreur)
- Une solution de décontamination lui est proposée (d'où l'intérêt de laisser sortir les requêtes vers les serveurs antiviraux).
- Le correspondant informatique dont il dépend est lui aussi au courant.

Schéma de la quarantaine

Quarantaine automatique de postes infectés

Fabrice Prigent

Contexte

Les solutions actuelles

Une solution

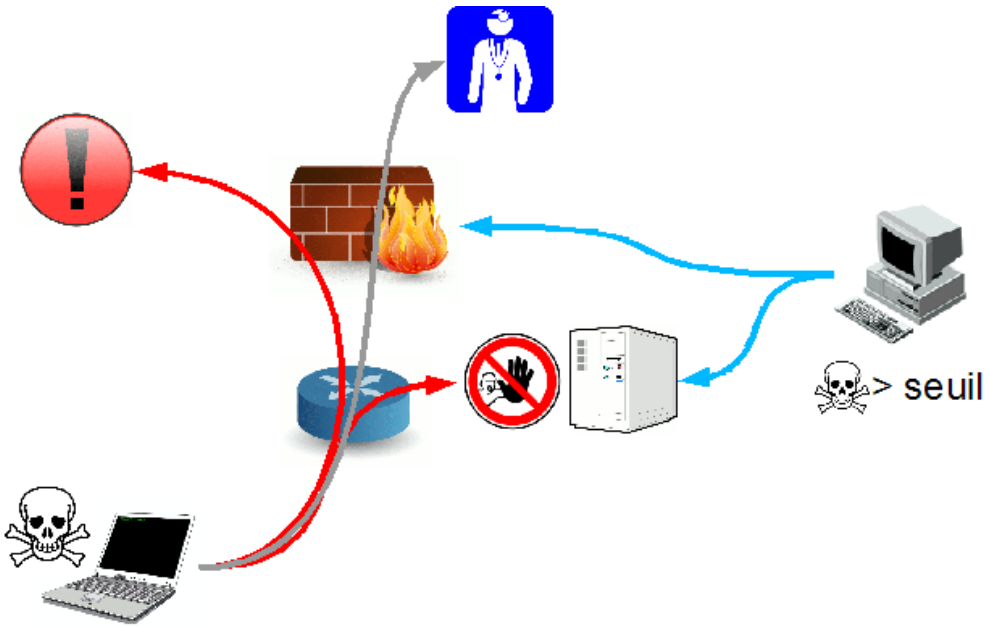
Les critères pour une autre solution

La détection

La mise en quarantaine

La sortie en quarantaine

Conclusion



Le coordonateur

Le dernier point est la sortie de la quarantaine. Celle-ci doit être automatique, le service informatique n'étant pas nécessairement présent.
Elle ne doit avoir lieu que si la quarantaine n'a plus lieu d'être. C'est à dire si l'incident est clos.

Une journée ordinaire de quarantaine

Quarantaine automatique de postes infectés

Fabrice Prigent

Contexte

Les solutions actuelles

Une solution

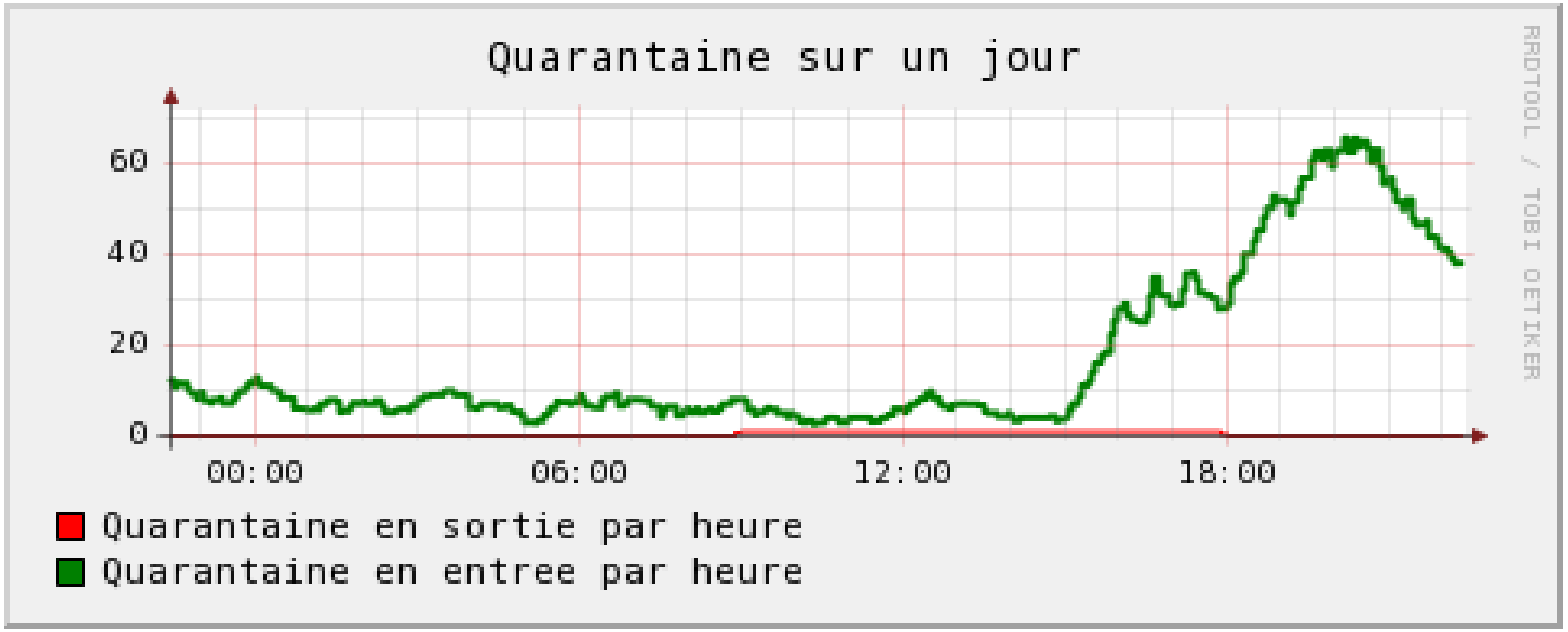
Les critères pour une autre solution

La détection

La mise en quarantaine

La sortie en quarantaine

Conclusion



Conclusion

Après 3 ans d'utilisation, les résultats sont probants :

- Les postes infectés (2-3 postes WiFi par semaine) sont isolés très rapidement.
- Aucune infection généralisée depuis 3 ans (2 par an avant)
- Les faux positifs concernent... 1 mac avec SMTP embarqué.
- Un calme important de nos utilisateurs (à la limite du "si je ne suis pas bloqué c'est que tout va bien").
- Assez grande confiance dans la sécurité du réseau des utilisateurs (action très visible).

Contexte

Les solutions actuelles

Une solution

Les critères pour une autre solution

La détection

La mise en quarantaine

La sortie en quarantaine

Conclusion

...

Des questions ?