CAPITOUL : La quarantaine interne

Fabrice Prigent

Université Toulouse 1 Capitole

Jeudi 21 Février 2013

L'université Toulouse 1 Capitole

- Université en droit, économie et gestion, avec une petite UFR informatique,
- 21000 étudiants,
- 2100 personnels (dont 1000 vacataires),
- très forte centralisation (2 entités semi-indépendantes),
- forte consommation de terminaux personnels (15000-17000)
  - ordinateurs
  - smartphones
- forte sensibilité au "hype"

Les ordinateurs à l'UT1

- Les ordinateurs inventoriés et gérés
  - OS verrouillés (Windows XP ou Windows 7)
  - Antivirus à jour,
  - Firewall mis en place
  - De plus en plus dans l'AD et sans droit administrateur.
- Les terminaux inventoriés non gérés
  - Achetés sur le marché de l'université
  - Ordinateurs professionels mais grande variété
  - OS variés
  - Maintenance "aléatoire".
- Le reste (étudiants, chercheurs avec budget propre, etc.)
  - PC "assembleurs" ou "distributeurs"
  - Ci-dessus, en moins bien maintenus.

Les postes professionnels ludiques

Tu leur dis pour les portables professionnels avec Call Of Duty dessus ?

Les croyances

- J'ai un antivirus gratuitement livré avec mon PC acheté il y a 3 ans, donc je ne crains rien,
- J'ai un mac, monsieur, je ne peux avoir été infecté,
- J'ai un antivirus symentacafbitdef de la mort qui tue à 20€ par an.
- Mon fils est un expert en informatique, vous verriez ce qu'il trouve sur internet !

Des malwares ?

Les faits

- Piratage du New York Times
  - 45 malwares repérés après analyse par Mandiant
  - 1 seul était détecté par Symantec !
- Un malware non détecté dans les 2 mois ne le sera jamais.

Les faits

- On ne peut toucher aux postes non gérés
  - pas le temps (trop d'étudiants)
  - pas le droit (pas de droits administrateurs)
  - pas envie (PEBKAC)

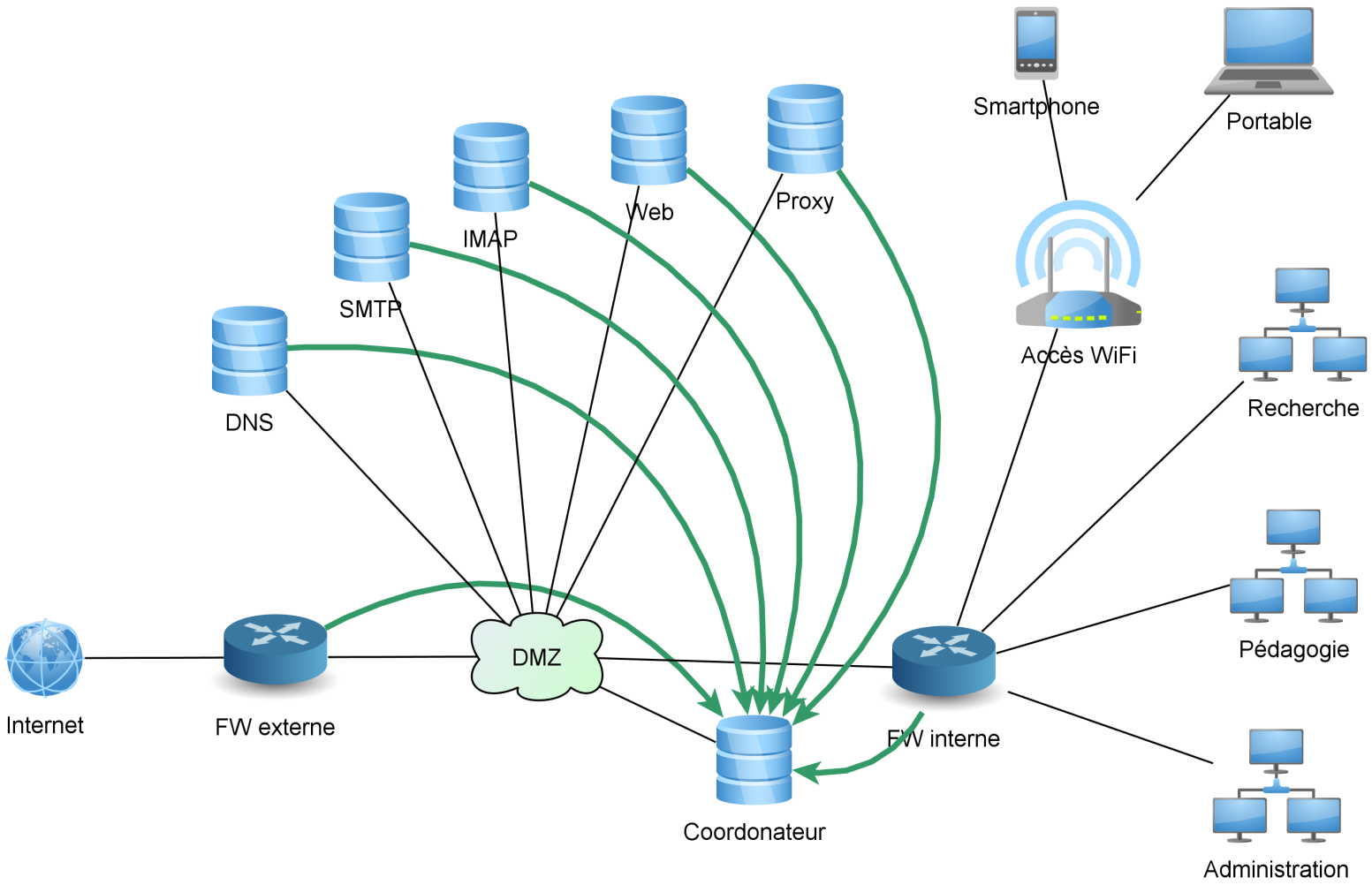
La quarantaine

Détecter les comportements déviants et mettre les postes infectés en quarantaine.

Détecter les comportements déviants

Cela va supposer le déploiement de sondes sur l'ensemble des processus qui ont une capacité à voir les choses anormales.

- Les attaques sortantes
  - web
  - IDS
- Les scans de port
- Les scans de comptes/mots de passe
- Les comportements abusifs
  - en fréquence
  - en volume
- Les comportements anormaux
- La connexion à des ressources "hostiles"
  - connexions à des sites webs référencés
  - résolution dns de sites "hostiles"


Smartphone
Portable
Web
Proxy
IMAP
SMTP
DNS
Accès WiFi
Recherche
Pédagogie
Internet
FW externe
DMZ
FW interne
Coordonateur
Administration

Un collecteur

Point central de l'architecture

- Il reçoit les journaux de toute l'infrastructure (1000 lignes par minute)
- Il détecte, en temps réel, les attaques
- Il analyse les remontées d'attaques
  - chaque 2 secondes pour les 5 dernières minutes,
  - chaque 5 minutes pour la dernière heure,
  - en évitant les attaques non dispersives (accès réseau ou imprimante d'un externe)
- Il met en quarantaine si le nombre d'attaques dépasse un seuil.
  - sur le proxy
  - sur les serveurs
  - sur les firewalls

Un firewall externe

Il doit bloquer, et journaliser les protocoles inutiles

- SMTP,DNS,SNMP
- Netbios, Rdesktop
- etc.

Doté d'un IDS

- il journalise les attaques qu'il repère.

Il classifie le trafic en 4 zones

- Libre (les serveurs internes ou externes connus)
- forte latence, débit moyen (ftp, pop, imap, etc. et certains serveurs non prioritaires)
- faible latence, petit débit (SSH)
- forte latence, très faible débit (le reste)

Un firewall interne

- Il logue les violations aux règles de sécurité
- Il redirige les consultations web vers le proxy transparent
- Il logue les nouvelles connexions trop fréquentes (P2P)

Un proxy

Basé sur squid et squidguard, il filtre en redirigeant sur un site web technique

- Les sites adultes (indicateur, si l'utilisateur proteste, d'une infection)
- Les sites malware
- Les machines infectées

Précautions à prendre

- 2 squid tournent en simultané (monothread)
- 2 ports pour chacun : sain et infecté
- le rechargement des iptables est plus léger que celui de squid.

Un web technique

Plusieurs fonctions

- fournir un wpad pour l'autoconfiguration des postes.
- fournir les pages de refus et loguer les accès aux pages malware.

Un serveur DNS / DHCP

La fonction DHCP

- fournir le plus de renseignement utile pour les postes (syslog, wpad, smtp, etc.)

La fonction DNS, qui a une notion de seuil local.

- détecter de très nombreuses requêtes DNS,
- détecter de nombreuses requêtes DNS nouvelles,
- détecter de nombreuses requêtes DNS sans résolution,
- détecter des requêtes sur des sites hostiles,
- expérimentalement : détecter des requêtes DNS à forte entropie.

Les serveurs web

Un analyseur de logs repère les requêtes anormales et les logue

- url inconnue
- paramètre inconnu
- format du paramètre incompatible avec l'existant

Les serveurs authentifiants

On peut y mettre les CAS, serveurs pop, imap, ftp, etc.

- Journalise une alerte à chaque échec

Les serveurs SMTP

- Analyse le nombre d'expéditions par machine,
- Analyse le nombre d'expéditions par expéditeur,
- Quand un seuil est dépassé, on journalise une alerte.

Les serveurs

Ils réagissent aux ordres du coordinateur

- en bloquant,
- en journalisant la tentative comme "persiste à ...".

L'évolution avec le temps

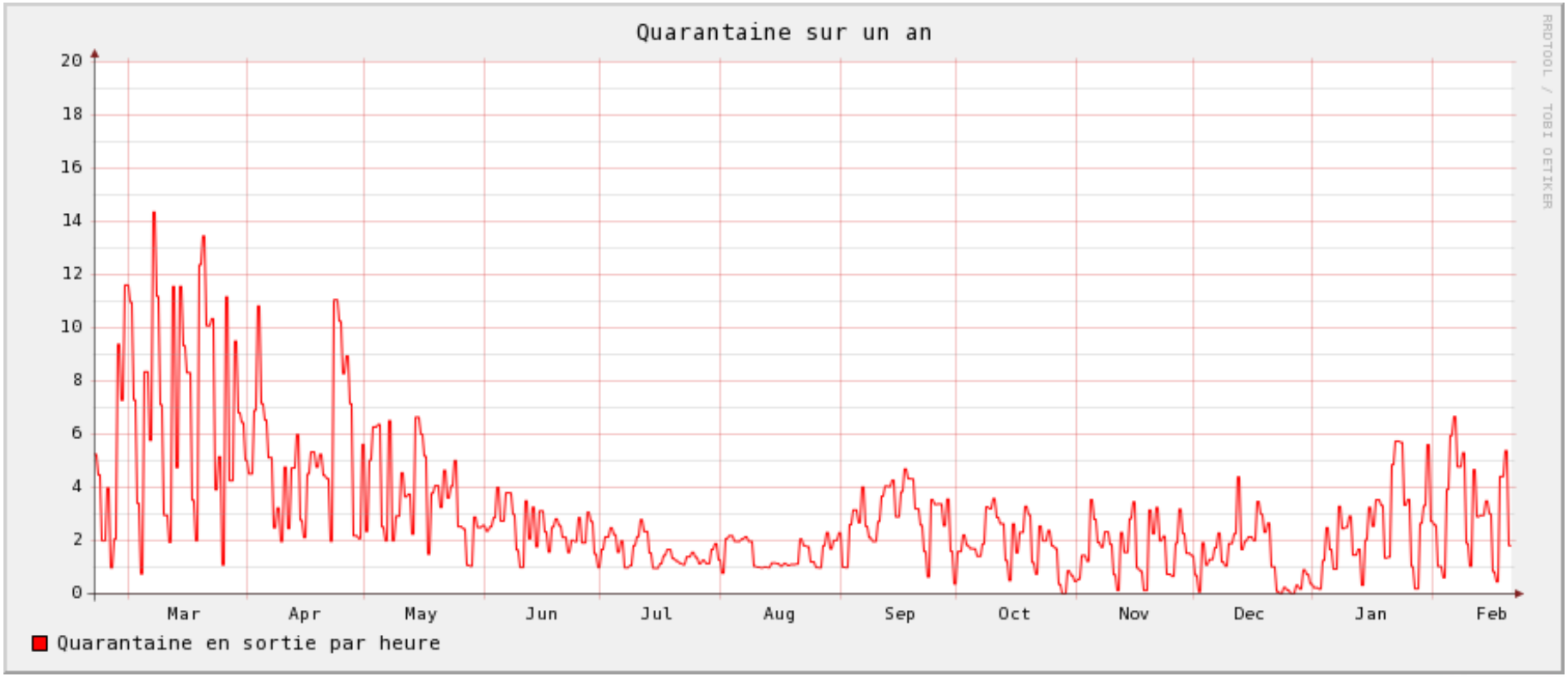
Les usages ont évolué avec le temps, et comme le système date de 2006, il en a vu passer.

- Les virus n'envoient plus de spams directement
- Les propagations par netbios sont beaucoup plus rares.
- Les tests de mots de passe touchent maintenant pop, imap, sql, etc.

L'évolution avec le temps

- Skype est détecté comme P2P, enclenchant des mises en quarantaine
  - Blocage mais sans mise en quarantaine (mais plus pour longtemps)
- Les requêtes HTTPS se généralisent, empêchant
  - La détection de certaines urls,
  - L'avertissement "propre" des victimes dans certains cas.
- Certains outils persistent dans les échecs d'identifiant (thunderbird)
- Les étudiants étrangers génèrent des "explosions" de nouveaux domaines DNS,
- L'IDS doit être régulièrement re-paramétré
- Certains sites référencés comme malware doivent être audités pour vérification

Résultats


Quarantaine sur un an
20
18
16
14
12
10
8
6
4
2
0
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec
Jan
Feb
Quarantaine en sortie par heure
RRDTOOL / TOBI OETIKER

Résultats

Quarantaine horaire

Date d'execution : **Jeudi 21 Février 2013 a 10:10:12**

Machines Internes repérées

DNS	IP	Attaque	Nb
dhcp-12-1-199.univ-tlse1.fr	10.12.1.199	Persiste :Sortie Netbios	3277
dhcp-7-7-89.univ-tlse1.fr	10.7.7.89	Persiste :Domaine infectieux	356
dhcp-7-3-106.univ-tlse1.fr	10.7.3.106	Persiste :malware web http://ads.alpha00001.com/cg	166
dhcp-7-11-173.univ-tlse1.fr	10.7.11.173	Persiste :Domaine infectieux	104
dhcp-7-15-253.univ-tlse1.fr	10.7.15.253	Persiste :malware web http://ads.clicksor.com/newS	94
dhcp-7-7-89.univ-tlse1.fr	10.7.7.89	Persiste :malware web http://ads.alpha00001.com/cg	73
dhcp-7-3-106.univ-tlse1.fr	10.7.3.106	Persiste :Domaine infectieux	48
dhcp-7-15-253.univ-tlse1.fr	10.7.15.253	malware web http://ads.clicksor.com/newServing/sho	12

Qualitativement

Le résultat, malgré les années, reste très positif

- Le système est agnostique,
- Plus aucune infection virale massive depuis 2005,
- Les antivirus de poste détectent 50 fois moins d'infections que l'infrastructure,
- La quantité de travail occasionnée par les faux positifs est très inférieure au gain,
- Tout est automatique : entrée en quarantaine et sortie (au bout d'une heure),
- Les utilisateurs mis en quarantaine font le lien avec leur erreur.