

RESIST

29/01/2008

Faits techniques et retour d'expérience d'une cellule d'expertise dans la lutte contre le code malveillant

Cathy Noiret

cathy.noiret (à) edelweb.fr

Anne Mur

anne.mur (à) edelweb.fr

EdelWeb / Groupe ON-X



Sommaire

- I. Présentation de la mission de la cellule
- II. Périmètre technique couvert
- III. Moyens de protection en place
- IV. Fonctionnement et organisation de la cellule
- V. Moyens d'expertise de la cellule
- VI. Cas concrets d'analyse
- VII. Evolution de la menace sur un an
- VIII. Evolution de nos outils
- IX. Limites des antivirus
- X. Difficultés rencontrées par la cellule
- XI. Conclusion



I. Présentation de la mission de cette cellule

❑ **Objectif : Assister le client dans la définition et l'application de leur politique de lutte antivirale**

❑ **Nos actions**

✓ Assistance à Maîtrise d'Ouvrage

- Veille technique sur les codes malveillants et les moyens pour s'en protéger
- Définition des spécifications techniques de besoins
- Qualification et choix de solutions
- Elaboration de cahiers de recette

✓ Assistance à Maîtrise d'Œuvre

- Réalisation de solutions spécifiques pour la lutte
 - ✓ Kit de contrôle basé sur plusieurs outils, avec remontée de traces
- Traitement des problèmes notifiés par les clients
 - ✓ Incidents non répertoriés (code malveillant inconnu)
 - ✓ Anomalies (dysfonctionnement des outils)



II. Périmètre technique couvert (1/3)

- ❑ **Plusieurs sites distants géographiquement**
- ❑ **Quelques chiffres : 3000 postes de travail, 300 serveurs**
- ❑ **Systemes utilisés : Windows (majoritaire), Linux, Unix**



II. Périmètre technique couvert (2/3)

□ Les biens à protéger

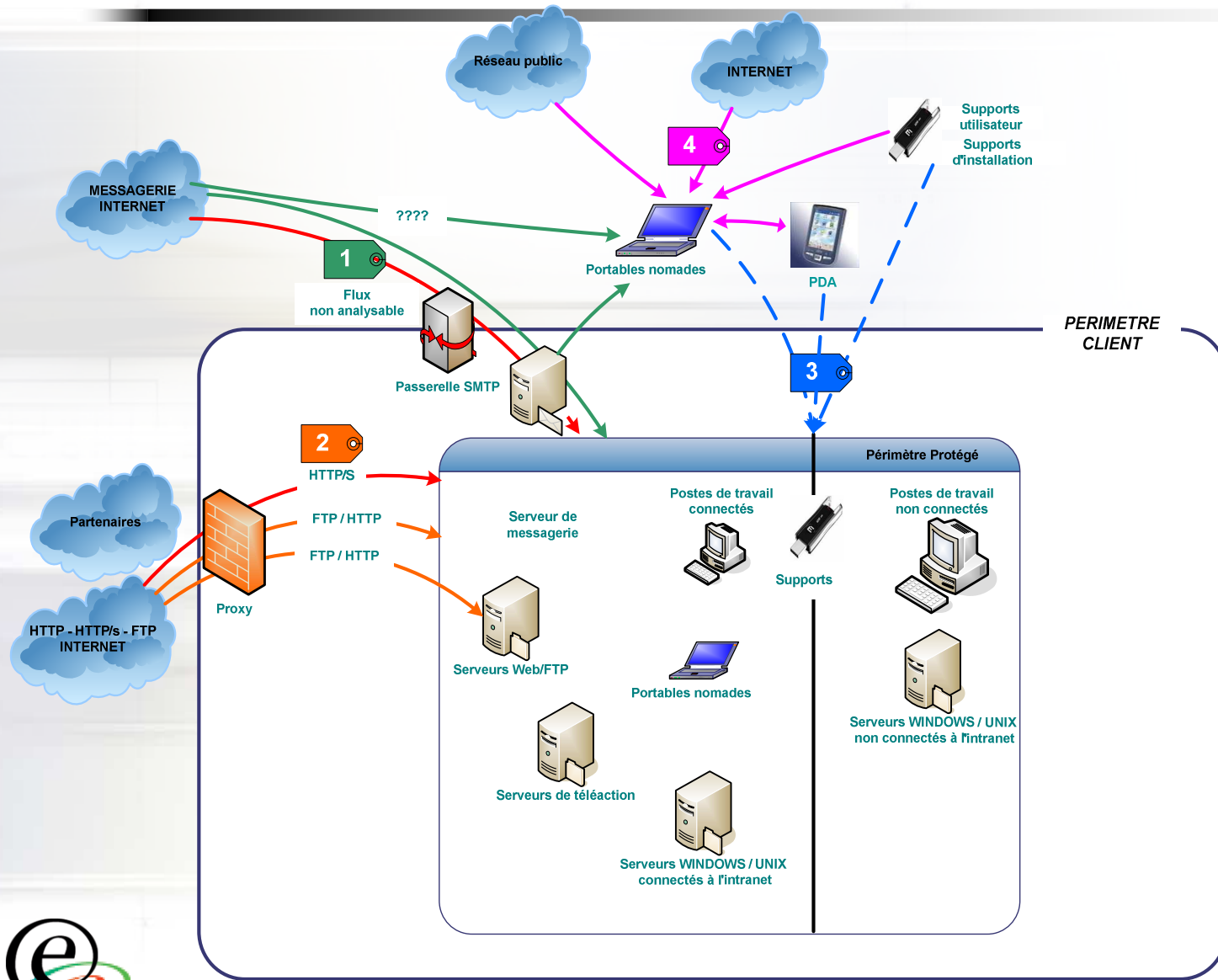
- ✓ Serveurs
- ✓ Postes de travail fixes et nomades
- ✓ Supports transportant des fichiers

□ Les flux de données

- ✓ Flux entre l'extérieur et l'intérieur du SI
 - HTTP, HTTPS, FTP
 - Mail externe
 - Supports (clés USB, CDROM, ...)
 - ...
- ✓ Flux internes au SI
 - Mail interne
 - Echanges de fichiers entre serveurs et postes de travail
 - Supports
 - ...



II. Périmètre technique couvert (3/3)



III. Moyens de protection (1/3)

□ Application des principes de défense en profondeur

- ✓ Indépendance des moyens de protection lorsqu'ils sont placés sur des lignes de défense différentes
- ✓ Complétude : moyens adaptés aux niveaux de gravité des menaces
- ✓ Surveillance et réaction en cas d'alerte
- ✓ Contrôle du bon fonctionnement des moyens

□ Ces principes de défense en profondeur sont appliqués

- ✓ dans l'organisation
- ✓ dans les technologies, et en particulier la défense ne doit pas reposer uniquement sur un produit ou une technologie quelle que soit sa qualité
- ✓ dans la mise en œuvre



III. Moyens de protection (2/3)

□ Principes de protection des flux

- ✓ Contrôle par au moins deux antivirus de chaque flux
- ✓ Détection d'un code malveillant au plus près de son arrivée dans le SI
- ✓ Alerte immédiate suite à la détection d'un code malveillant, pour assurer une réactivité maximale
- ✓ Mise en quarantaine
- ✓ Pas de désinfection automatique

III. Moyens de protection (3/3)

FLUX	Emplacement	Antivirus
Messagerie externe	Serveur mail	AV1 – AV2
	Poste de travail	AV4
Messagerie interne	Serveur mail	AV3 – AV2
	Poste de travail	AV4
Données	Serveurs de fichiers	AV2 – AV3
	Poste de travail	AV4
	Kit d'analyse	AV4 – AV3 – AV2
	Kit d'analyse utilisateur	AV3
Supports	Stations dédiées au contrôle de support	AV2 – AV3
	Poste de travail	AV4
Web/FTP	Proxy HTTP	AV5
	Poste de travail	AV4

IV. Fonctionnement et organisation de la cellule (1/2)

❑ Scénario type du traitement d'un incident

1. Détection d'un code malveillant par le client
2. Réception des détails de l'infection et des souches
3. Réalisation d'une analyse de risques adaptée au contexte du client
4. *Intervention si nécessaire (récupération des souches)*
5. Contact des éditeurs si souche non détectée
6. Analyse des souches et création d'une procédure de désinfection
7. *Désinfection sur site sur demande du client*
8. Validation et envoi de la procédure au client
9. Fermeture du problème (après désinfection)

IV. Fonctionnement et organisation de la cellule (2/2)

□ **Fonctionnement de la cellule**

1. Astreinte chaque jour ouvré de 9h00 à 18h00
2. Réception des appels téléphoniques et des éléments de diagnostic (logs, souches virales,...)
3. Assistance du client dans le recueil des éléments de diagnostic
4. Reproduction des problèmes sur la plate-forme technique du laboratoire
5. Rédaction et qualification des procédures palliatives et correctives
6. Diffusion aux établissements des procédures
7. Support auprès des établissements pour l'application des procédures
8. Diffusion des fiches et procédures au client

V. Moyens d'expertise d'EdelWeb (1/2)

□ Matériel

- ✓ Reproduction de l'architecture de protection du client
- ✓ Serveurs de virtualisation
 - Images des systèmes utilisés chez le client
 - Images de tests des différents systèmes d'exploitation Microsoft

□ Humain

- ✓ Equipe répartie sur deux sites géographiques
- ✓ Matière grise ;-)

□ Logiciel

- ✓ Outils
 - Sysinternals Tools, Malware Analysis Pack, ...
- ✓ Outils maison
 - Analyse de logs systèmes, analyse de trafic réseau, pot de miel, ...



EdelWeb



V. Moyens d'expertise d'EdelWeb (2/2)

□ Tâches

- ✓ Analyse de codes malveillants (plus de 10 analyses/mois depuis plus de 5 ans)
- ✓ Qualification bimestrielle des outils (qualité de détection et fonctionnalités)

□ Expertise

- ✓ Expertise forte en sécurité Windows
- ✓ Gestion de crise

□ Veille sur la menace virale et les solutions

- ✓ Sources d'informations : mailing-lists, éditeurs AV, CERTs, sites web, ...
- ✓ Réalisations
 - Bulletin de veille bimestriel adapté à l'environnement du client
 - Notes techniques



VI. Cas concrets d'analyse

□ Trois cas types

□ **Virut A (virus)**

- ✓ Infection des fichiers exécutables accédés par d'autres programmes
- ✓ Ouverture d'une backdoor IRC

□ **Brontok (ver complexe)**

- ✓ Redémarre la machine lorsqu'un titre de fenêtre contient (cmd, exe, sophos, virus...)
- ✓ Processus créés reconnus comme non interruptibles
- ✓ Propagation via lecteurs réseaux et supports amovibles

□ **Downloader BAI (trojan)**

- ✓ Très nombreuses variantes
- ✓ Télécharge via HTTP d'autres codes malveillants



VII. Evolution de la menace sur un an

□ Tendances constatées

- ✓ Infections de médias amovibles en nette hausse
- ✓ Majorité de trojans, de moins en moins de virus, vers
- ✓ Nombreux adwares / spywares
- ✓ Augmentation des codes complexes
 - Fonctionnalités de rootkit
 - Modifications importantes du système
 - Infection de nombreux fichiers
- ✓ Beaucoup de variantes de certains codes (type dropper)



VIII. Evolution de nos outils

□ 2002

- ✓ Machines physiques pour l'analyse de codes malveillants (images Ghost)

□ 2004

- ✓ Machines de virtualisation « VMware Workstation » multi-utilisateurs (Windows 2003 Server)

□ 2006 - Pot de miel

- ✓ Basé sur un système Linux
- ✓ Récupération des fichiers téléchargés

□ 2007

- ✓ Améliorations des outils « maisons »
- ✓ Tableau de comparaison de détection des moteurs antivirus
- ✓ Analyse simple de l'impact d'un code sur le système
- ✓ Exécution dans un environnement fermé



IX. Limites des antivirus

- ❑ **Décalage permanent / apparition de nouveaux codes**
- ❑ **Couverture partielle / types de codes**
 - ✓ Rootkits très mal détectés
 - ✓ Spyware/Adware (en fonction de l'éditeur)
- ❑ **Régression du niveau de détection / codes antérieurs**
- ❑ **Nombreuses variantes des codes**
 - ✓ Le délai de prise en compte par les éditeurs est variable
 - ✓ Augmentation de la fréquence de mise à jour des signatures

X. Difficultés rencontrées par la cellule

- ❑ **Prise en compte des éditeurs parfois longue**
- ❑ **Faux-positifs pouvant avoir des répercussions importantes**
- ❑ **Récupération des souches pas toujours possible**
 - ✓ Utilisateur a supprimé la souche
 - ✓ Souches sur un média amovible plus disponible
- ❑ **Manque parfois de visibilité sur le SI du client**
 - ✓ Intervention sur site nécessaire pour obtenir les informations
- ❑ **Difficultés pour la désinfection**
 - ✓ Trop nombreux fichiers infectés ou altérés
 - ✓ Reproduction de l'infection impossible (site non disponible, souches effacées, ...)

XI. Conclusion (1/2)

□ Pistes d'améliorations techniques

- ✓ Renforcement de la configuration des serveurs et postes de travail
 - Ex. de paramétrage : désactivation du service Server sur les postes de travail
 - Etude de mise en œuvre de pare-feux sur les postes de travail
- ✓ Protection spécifique aux équipements portables
 - Analyse de risque sur les PC portables pour le choix de solutions complémentaires
 - Etude des menaces pesant sur les PDA / Smartphone
 - Contrôle des PC portables et mise en quarantaine si non-conformité à la reconnexion (NAC / NAP)
- ✓ Détection au niveau du réseau
 - Mise en œuvre d'une sonde de détection de codes malveillants (IDS) éventuellement en coupure (IPS)

XI. Conclusion (2/2)

□ Pistes d'améliorations organisationnelles

- ✓ Sensibiliser les utilisateurs (toujours) aux évolutions de la menace
 - Exemple concret : connexion d'un disque dur externe USB infecté sur un poste de travail du SI par un utilisateur
- ✓ Améliorer les procédures de gestion de crise virale
 - Disposer de scénarios concrets de gestion de crise et de procédures de gestion de crise
 - Disposer et maintenir à jour les éléments nécessaires à la maîtrise d'une propagation virale
 - ✓ Description de l'architecture antivirale
 - ✓ Identification des composants critiques
 - ✓ Etat de configuration des antivirus, des moyens de surveillance et des procédures
 - ✓ Identification des supports et experts
 - ✓ Identification des moyens d'intervention : techniques et humains

Questions ?

