

Affaire suivie par :
CERTA

NOTE D'INFORMATION DU CERTA

Objet : Retour d'expérience du ver ILOVEYOU

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2000-REC-001>

Gestion du document

Référence	CERTA-2000-REC-001
Titre	Retour d'expérience du ver ILOVEYOU
Date de la première version	16 mai 2000
Date de la dernière version	–
Source(s)	
Pièce(s) jointe(s)	Aucune

TAB. 1 – *gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

Résumé

Les récents dégâts provoqués par le virus ILOVEYOU, ont montré une nouvelle fois que la sécurité reposait en grande partie sur le comportement des utilisateurs et en particulier sur leur capacité à respecter les règles élémentaires de protection.

1 Généralités

Les dégâts provoqués par le ver ILOVEYOU ont entraîné une prise de conscience plus aigüe, du risque de nuisance des virus. Selon de nombreux observateurs, le risque de propagation dans les prochains mois, de ver encore plus virulents qu'ILOVEYOU ou encore d'attaques classiques (dénier de service par exemple), est élevée. Cette analyse de la situation sur Internet est la conséquence des phénomènes suivants :

1° Les technologies d'attaque les plus performantes sont disponibles et utilisées simultanément.
Par exemple dans le cas d'ILOVEYOU le pirate a utilisé à la fois :

- un langage de script Microsoft ;
- la contamination par carnet d'adresses ;
- la contamination par IRC.

- 2° La quantité de machines connectées sur le réseau a augmenté. Celles-ci sont souvent peu ou mal protégées et offrent donc des cibles d'attaque de plus en plus nombreuses.
Le nombre de machines disposant d'un accès permanent à Internet et à forte bande passante (câble, ADSL, LS) explose. Ces dernières sont utilisables pour des attaques par déni de service distribué de façon d'autant plus efficace que la sécurité n'est pas ou peu prise en compte.
- 3° La période d'été a toujours été propice aux attaques.
La vie étudiante et scolaire ralentie en fin d'année, les techniques sont aussi mieux maîtrisées et les groupes s'animent !

Cette analyse nous engage à réagir :

1. Revoir le paramétrage des barrières de sécurité (« firewall ») et en particulier la règle classique qui consiste à ne pas filtrer les flux de l'intérieur vers l'extérieur (par exemple pour l'IRC). Dans le même domaine d'action la règle par défaut d'une barrière de sécurité doit-être : « *tout ce qui n'est pas autorisé est interdit* » (ce qui n'est pas l'option par défaut de certains produits commerciaux).
2. Revoir ou prévoir des plans de parade et de réaction : conduite à tenir, personnes à prévenir, diffusion de l'alerte, etc.
3. Mise à jour des logiciels (navigateur, anti-virus, application du type bureautique).
4. Sauvegarde régulière des données et stockage de ces dernières dans des lieux isolés.
5. Exploitation et sauvegarde des journaux de log.

2 Aspects techniques

- Il est nécessaire de définir, dans votre entité, une configuration type des logiciels de navigation et de messagerie. A titre d'exemple il ne semble pas indispensable que tous les postes de travail aient besoin de pouvoir exécuter des script en Visual basic ou encore que les ActiveX ou mIRC soient disponibles pour tous :

1. Supprimer WScript.
2. Supprimer l'exécution automatique des fichiers htm :
 - (a) dans l'explorateur Windows ;
 - (b) menu « Affichage » ;
 - (c) sous-menu « Options » (ou « Options des dossiers » selon la version de Windows) ;
 - (d) onglet « Type des fichiers ».

Supprimer la ligne associée à l'extension hta.

3. Supprimer tous les ActiveX :
 - (a) menu « Démarrer » ;
 - (b) menu « Paramètres » ;
 - (c) menu « Panneau de configuration » ;
 - (d) icône « Options Internet » ;
 - (e) onglet « Sécurité » ;
 - (f) sélectionner l'icône « Internet » ;
 - (g) bouton « personnaliser le niveau » ;
 - (h) options « contrôles ActiveX et plugins ».

Désactiver tous les ActiveX.

Manipulation identique pour les applets java avec l'option « script » dans l'étape (3h).

4. Désinstaller mIRC (logiciel de relais chats).

- **Le ver ILOVEYOU a mis en évidence l'exploitation des carnets d'adresses.** Il est ainsi apparu que des services partageaient des carnets d'adresses Outlook pour faire leur annuaire interne. Dans ces carnets partagés apparaissent toutes les informations souhaitables pour un pirate (nom, e-mail, téléphone, etc.). Ce partage d'adresse est évidemment un outil indispensable mais il est préférable, sur le plan de la sécurité, de l'installer dans une page web de votre Intranet. Il est ainsi présent à une adresse donné ce qui sera plus difficile à retrouver pour un pirate.
- La contamination par carnet d'adresses avait été démontrée par MELISSA et exploitée par ILOVEYOU. Il peut être judicieux d'inscrire d'office dans le carnet d'adresses de chaque poste de travail le mél du responsable sécurité : ainsi dans ce type d'attaque, ce dernier sera immédiatement et massivement alerté.

3 Conclusion

Il est aujourd'hui impératif de sensibiliser les utilisateurs sur la faiblesse des paramètres par défaut, de ne pas leur livrer des postes de travail sur lesquels des exécutables dont ils n'ont pas besoin sont disponibles et de vérifier les choix de filtrage des barrières de sécurité. Enfin, il faut vérifier que les règles relatives aux sauvegardes et à leur stockage sont bien appliquées.

Gestion détaillée du document

16 mai 2000 version initiale.