



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 05 juillet 2000
N° CERTA-2000-ALERTE-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Alerte de virus LOVE-LETTER-FOR-YOU

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-ALE-001>

Gestion du document

| | |
|-----------------------------|-------------------------------------|
| Référence | CERTA-2000-ALE-001 |
| Titre | Alerte de virus LOVE-LETTER-FOR-YOU |
| Date de la première version | 05 mai 2000 |
| Date de la dernière version | 05 juillet 2000 |
| Source(s) | code source du virus |
| Pièce(s) jointe(s) | Aucune |

TAB. 1 – gestion du document

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

1 Résumé

Un ver se répand actuellement très vite sur le réseau internet par le biais de la messagerie et de l'IRC. Il infecte de nombreux fichiers qu'il détruit.

Ce ver écrit en VISUAL BASIC est déjà recensé chez des partenaires du CERTA.

2 Origine

- Source du ver donnée par un de nos partenaire.
- groupe de news fr.comp.securite.
- Avis du CERT IST.
- Avis SYMANTEC <http://www.symantec.com/avcenter/venc/data/vbs.loveletter.a.html>.

3 Risque

- Risque élevé.
- Faille officielle.
- Écrasement de fichiers.

- Le mode de propagation peut entraîner une grande surcharge des réseaux.
- Probablement un cheval de Troie (reste à confirmer).

4 Systèmes impactés

Tous les systèmes Windows (NT, 2000 et 9x) sont concernés.

5 Symptômes

5.1 E-mail

Arrivée d'un e-mail aux caractéristiques suivantes :

Objet : ILOVEYOU

Corps du message kindly check the attached LOVELETTER coming from me.

Fichier attaché LOVE-LETTER-FOR-YOU.TXT.vbs.

5.2 IRC

Réception d'une page HTML LOVE-LETTER-FOR-YOU.HTM ayant pour titre « LOVELETTER - HTML » dès que l'on se connecte à un canal IRC sur lequel une personne infectée est présente.

5.3 Fichiers infectés

5.3.1 Faux fichiers systèmes

Les fichiers suivants sont créés

- Dans le répertoire de windows (WINDOW ou WINNT): Win32DLL.vbs
- Dans le répertoire système de Windows : MSKernel32.vbs et LOVE-LETTER-FOR-YOU.TXT.vbs (c'est ce dernier qui sert d'attachement aux e-mail), LOVE-LETTER-FOR-YOU.HTM (servant pour l'infection sur IRC) et WinFAT32.exe.

5.3.2 Configuration

Internet Explorer Modification de la page de démarrage d'Internet Explorer de manière à télécharger un exécutable WIN-BUGSFIX.exe au prochain lancement du navigateur. L'exécutable est rangé dans le répertoire de téléchargement d'Internet Explorer.

mIRC Écrasement du fichier de configuration script.ini qui s'exécute à chaque fois qu'un interlocuteur entre sur le canal IRC où vous êtes connectés.

5.3.3 La base de registre

Elle est modifiée pour relancer le ver (et WIN-BUGSFIX.exe) à chaque démarrage :

- dans le chemin HKLM\Software\Microsoft\Windows\CurrentVersion\Run création des clefs MSKernel32 et WIN-BUGSFIX ;
- dans le chemin HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices création d'une clef Win32DLL.

5.3.4 Fichiers écrasés

Tous les fichiers aux extensions suivantes situés sur des disques fixes locaux ou sur des disques réseaux sont potentiellement infectés :

- *.vbs, *.vbe : contenu écrasé par le code du ver ;
- *.js, *.jse, *.css, *.wsh, *.sct, *.hta : le contenu est écrasé par le code du ver et l'extension est remplacée par .vbs. Par exemple toto.css devient toto.vbs.
- *.jpg, *.jpeg : le contenu est écrasé par le code du ver et l'extension .vbs est ajoutée à la fin.
- *.mp2, *.mp3 : sont cachés (attribut caché) et des fichiers *.mp2.vbs ou *.mp3.vbs sont créés avec le contenu du ver. Par exemple : toto.mp3 devient caché et un fichier visible toto.mp3.vbs est créé.

6 Solution

6.1 Antivirus

Mettre à jour l'antivirus.

6.2 Firewall

Le temps de l'alerte bloquer les chargements http depuis le site `www.skyinet.net/~young1s/` ou `~angelcat/` ou `~chu/` ou `~koichi/`.

6.3 Configuration d'Internet Explorer

Dans les paramètres de sécurité, il faut demander au moins l'avis de l'utilisateur avant d'exécuter du code dans une page HTML.

6.4 Configuration de mIRC

Décocher « Autoaccept DCC send request » dans les paramètres de votre connexion/profil, afin de ne plus accepter automatiquement les fichiers envoyés par dcc send.

Ne **JAMAIS** accepter les fichiers que l'on vous envoie.

6.5 E-mail

Ne **JAMAIS** exécuter une pièce jointe.

6.6 Option de l'explorateur de Windows

Désactiver le lien entre les fichiers *.vbs et l'interpréteur WSH (`wscript.exe`).

6.7 Faire le ménage

6.7.1 Nettoyer la base de registre

Supprimer les Entrées citées précédemment au paragraphe 5.3.3.

6.8 mIRC

Détruire le fichier `script.ini` s'il contient la chaîne `LOVE-LETTER-FOR-YOU.HTM`.

6.9 Internet Explorer

Vérifier dans le panneau de configuration que la page de garde ne pointe pas sur l'un des sites `www.skyinet.net`.

6.10 Nettoyer les fichiers systèmes

Supprimer les fichiers .vbs et .htm cités précédemment au paragraphe 5.3.1. Vérifier l'origine du fichier `WinFAT32.exe`.

6.11 Nettoyer le répertoire de téléchargement d'internet explorer

Supprimer le fichier WIN-BUGSFIX.exe.

6.12 Analyser tous les fichiers .vbs et .vbe

Détruire tous les fichiers à l'extension *.vbs et *.vbe contenant le ver. Par exemple, tous les fichiers .vbs ou .vbe contenant la chaîne ispyder@mail.com.

Gestion détaillée du document

1.1 05 juillet 2000 modifications de mise en page.

1.0 05 mai 2000 version initiale.