Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 mars 2004
N° CERTA-2004-ALE-003

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Propagation du ver Phatbot

Gestion du document

Référence	CERTA-2004-ALE-003
Titre	Propagation du ver Phatbot
Date de la première version	19 mars 2004
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.

1 Risque

- Compromission du système ;
- déni de service.

2 Systèmes affectés

- Microsoft Windows 2000 ;
- Microsoft Windows XP.

3 Résumé

Un ver nommé `Phatbot` (ou `Gaobot` ou `Agobot` ou encore `Polybot` selon les éditeurs d'antivirus) semble se propager actuellement.

4 Description

Un ver nommé `Phatbot` semble se propager de plusieurs façons différentes. Il semble exploiter de nombreuses vulnérabilités affectant Microsoft Windows, telles que `RPC DCOM` (CERTA-2003-AVI-111 et CERTA-2003-AVI-149-001), `Dameware Miniremote` (CERTA-2003-AVI-214), `Microsoft Locator Service`

(CERTA-2003-AVI-009), WebDAV (CERTA-2003-AVI-050), Windows Workstation Services (CERTA-2003-AVI-185). Le ver semble aussi se propager via les partages réseau protégés par un mot de passe faible, ainsi que par la porte dérobée laissée par le ver MyDoom (normalement filtrée par le pare-feu).

Il aurait des fonctionnalités d'écoute de trafic réseau, dans le but de voler des noms d'utilisateur et des mots de passe ftp et irc, ainsi que des cookies http. Il aurait également des fonctionnalités de spam, et pourrait voler les clés CD de produits Microsoft ou de jeux. Il pourrait lancer un proxy HTTP.

Il serait capable d'éliminer certains virus, tels que Sobig, Welchia ou Blaster. Il serait surtout capable de terminer des processus liés à des produits de sécurité tels que des antivirus et des pare-feux personnels.

Phatbot aurait la possibilité de lancer des dénis de service. Les commandes seraient adressées aux machines infectées par Phatbot par l'intermédiaire d'une version modifiée du protocole WASTE (protocole P2P). Il utiliserait le port 4387/tcp.

Il ajouterait les clés de registre suivantes :
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Generic Service Process
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Generic Service Process
D'autres clés de registre pourraient être ajoutées.

Ce ver serait polymorphique, ce qui compliquerait sa détection par les antivirus.

5 Solution

- Appliquer tous les correctifs de Microsoft ;
- utiliser des règles de filtrage appropriées et des mots de passe forts pour le partage réseau ;
- se référer à l'avis CERTA-2003-AVI-084.

6 Documentation

Analyse du ver Phatbot par Lurhq :
http://www.lurhq.com/phatbot.html
Analyse du ver W32/Agobot-FG par Sophos :
http://www.sophos.com/virusinfo/analyses/w32agobotfg.html
Analyse du ver Phatbot par Network Associates :
http://vil.nai.com/vil/content/v_101100.htm
Analyse du ver Agobot par TrendMicro :
http://fr.trendmicro-europe.com/enterprise/security_info/ve_detail.php?id=58041&VName=BKDR_SPYBOT.Z

Analyse du ver Agobot par F-Secure :
http://www.f-secure.com/v-descs/agobot_fo.shtml
Analyse du ver Polybot par Symantec :
http://www.symantec.com/avcenter/venc/data/w32.hllw.polybot.html
Avis CERTA-2003-AVI-084 :
http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-084/
Avis CERTA-2003-AVI-111 :
http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-111/
Avis CERTA-2003-AVI-149-001 :
http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-149/
Avis CERTA-2003-AVI-214 :
http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-214/
Avis CERTA-2003-AVI-009 :
http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-009/
Avis CERTA-2003-AVI-050 :
http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-050/
Avis CERTA-2003-AVI-185 :
http://www.certa.ssi.gouv.fr/site/CERTA-2003-AVI-185/

Gestion détaillée du document

19 mars 2004 version initiale.