

# ACTU NEWS ANTIVIRUS, ANTISPAM, CYBER CRIMINALITÉS

## Bootkit 2009

Kaspersky Lab, éditeur reconnu de solutions de sécurité informatique contre toutes les formes de menaces cybercriminelles (botnets, escroqueries, phishing, spams, etc.), publie « Bootkit 2009 », un article consacré à Backdoor.Win32.Sinowal. Rédigé par Sergey Golovanov, Senior Malware Analyst chez Kaspersky Lab, et Vyacheslav Rusakov, Responsable de l'analyse des codes malicieux les plus complexes chez Kaspersky Lab, ce rapport analyse la nouvelle modification du bootkit, considéré comme l'application malveillante la plus sophistiquée à ce jour.

Identifiée à la fin du mois de mars 2009, la nouvelle version du bootkit se propage via des sites, pornographiques ou encore qui proposent au téléchargement des applications piratées. La grande majorité des serveurs impliqués dans l'infection des utilisateurs peut être reliée d'une manière ou d'une autre à des éléments russophones : ils fonctionnent dans le cadre de « programmes de coopération », dans lesquels les propriétaires de sites travaillent avec les auteurs d'applications malveillantes.

Comme dans ses formes précédentes, le bootkit recourt à une méthode fondée sur l'infection du MBR, qui permet le chargement de son pilote avant le démarrage du système d'exploitation. Cependant, à la différence de ses versions antérieures, Backdoor.Win32.Sinowal utilise désormais une technologie plus sophistiquée, qui lui permet de dissimuler sa présence dans le système. La majorité des fonctions clés qui installent des intercepteurs avec des fonctions systèmes sont modifiées, ce qui complique sensiblement la procédure d'analyse du code malveillant.

L'activité récente du bootkit Backdoor.Win32.Sinowal démontre la nécessité d'améliorer les technologies antivirales actuelles, non seulement afin de combattre avec efficacité les tentatives d'infection des ordinateurs, mais aussi pour détecter les menaces plus complexes, capables d'intervenir à chaque niveau du système d'exploitation.

.../....

<http://www.viruslist.com/fr/analysis?pubid=200676198>

<http://www.kaspersky.com/fr/news?id=207217165>



Copyright : sergey - 2009-07-26 18:27:22

Creative Commons Deed

Paternité - Pas d'Utilisation Commerciale - Pas de Modification 2.5

Vous êtes libres :

- \* de reproduire, distribuer et communiquer cette création au public

Selon les conditions suivantes :

Paternité. Vous devez citer le nom de l'auteur original.

Pas d'Utilisation Commerciale. Vous n'avez pas le droit d'utiliser cette création à des fins commerciales.

Pas de Modification. Vous n'avez pas le droit de modifier, de transformer ou d'adapter cette création.

\* A chaque réutilisation ou distribution, vous devez faire apparaître clairement aux autres les conditions contractuelles de mise à disposition de cette création.

\* Chacune de ces conditions peut être levée si vous obtenez l'autorisation du titulaire des droits.

Ce qui précède n'affecte en rien vos droits en tant qu'utilisateur (exceptions au droit d'auteur : copies réservées à l'usage privé du copiste, courtes citations, parodie...)

Ceci est le Résumé Explicatif du Code Juridique (la version intégrale du contrat).

<http://creativecommons.org/licenses/by-nc-nd/2.5/>