ICEBOX : analyse de Malwares par introspection de machine virtuelle

Benoit Amiaux, Luca Farey, Jean-Marie Borello

ThalesGroup Rennes
{nom.prenom}@thalesgroup.com

Résumé

Cet article présente un projet d'introspection de machine virtuelle extensible et performant, dénommé IceBox, offrant non seulement les fonctionnalités de reporting classiques des sandboxes actuelles mais aussi un contrôle total du système d'exploitation invité via une modification du projet open-source VirtualBox[1]. De part sa furtivité liée au fait qu'aucun agent ne tourne dans l'invité, ce projet se prête particulièrement bien à l'analyse dynamique de malwares.

[1] *https ://www.virtualbox.org/*

Keywords:
introspection, machine virtuelle, malware, analyse dynamique