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 2013
N° CERTA-2013-ACT-027

Affaire suivie par :
CERTA

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTA-2013-ACT-027

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-2013-ACT-027`

1 Contre-mesures aux attaques de vols d'identifiants

Dans le cadre de sa mission de traitement des attaques informatiques, le CERTA est régulièrement confronté aux attaques de type « Pass-the-Hash ».

Après la compromission d'un poste du système d'information, l'attaquant cherche à élever ses privilèges, c'est-à-dire passer d'un simple compte utilisateur à celui d'un administrateur du domaine ou équivalent.

Pour cela l'attaquant cherche à récupérer les identifiants de tout utilisateur se connectant à la machine qu'il a compromise :

- en interceptant les phases d'authentification NTLM entre un client et un serveur ;
- en récupérant le condensat dérivé du mot de passe stocké dans la base SAM ;
- en récupérant le condensat dérivé du mot de passe dans la mémoire du processus LSASS de Windows.

Dans le cadre des mesures de défense en profondeur, il est essentiel d'appliquer des mesures spécifiques afin d'atténuer ce risque particulier. À cette fin, le CERTA recommande l'application des préconisations du guide de Microsoft « Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques », dont principalement :

- restreindre et protéger l'accès aux comptes d'administration du domaine ;
- restreindre et protéger l'accès aux comptes d'administrateurs locaux ;
- limiter les connexions à distance aux seuls comptes qui en ont besoin (pour les équipes de support, par exemple) ;
- ne pas utiliser de session d'administration pour naviguer sur l'Internet ou accéder à sa messagerie ;
- rendre exceptionnel l'ajout de droits administrateur à des utilisateurs standards ;
- ne pas utiliser de comptes de services bénéficiant de privilèges d'administration du domaine ;
- vérifier régulièrement que LAN Manager est bien désactivé dans les stratégies de groupe du domaine.

Documentation

- Guide Microsoft :
  http://www.microsoft.com/en-us/download/details.aspx?id=36036
- Guide d'hygiène informatique de l'ANSSI :
  http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf

2 Compromission des sites légitimes

Google publie depuis le 26 juin des relevés dynamiques au sujet des sites malveillants sur sa page "Transparence des informations". Ces données montrent que 90% des sites malveillants identifiés par Google s'avèrent être des sites Web légitimes compromis. Le CERTA partage ce constat au regard des incidents qu'il a traité ces dernières années.

Pour compromettre un maximum de sites, les attaquants scannent automatiquement l'Internet à la recherche de sites exposés à des vulnérabilités connues et non corrigées, comme par exemple les sites avec un gestionnaire de contenu (CMS) non maintenu à jour.

Une fois ces vulnérabilités exploitées, les attaquants ajoutent sur le site vulnérable des codes qui vont rediriger de manière transparente la victime vers des sites distribuant des charges malveillantes.

Le CERTA observe régulièrement, lors du traitement de sites défigurés par exemple, que la même vulnérabilité est utilisée par d'autres attaquants pour héberger sur le serveur compromis des charges malveillantes ou créer des redirections malveillantes.

Il convient donc d'être particulièrement vigilant sur ce type de menaces. L'accès à un site légitime peut toujours être une source de compromission. La surveillance des accès doit donc intégrer cette réalité. Par ailleurs, le CERTA recommande aux administrateurs de sites de s'assurer du meilleur niveau de mise à jour de tous les composants de leurs sites et de s'assurer régulièrement de l'intégrité des fichiers de leurs serveurs.

Documentation

- Rapport « Transparence des informations » de Google :
  http://www.google.com/transparencyreport/safebrowsing/

3 Compromission d'une mise à jour Opera

Le 19 juin 2013 *Opera* a été victime d'une attaque informatique. L'attaquant a réussi à modifier le système de mise à jour d'*Opera* pour diffuser un logiciel malveillant à la place d'une mise à jour officielle. Les postes Windows ayant mis à jour *Opera* entre 01h00 et 01h36 UTC peuvent donc être affectés par ces codes malveillants.

Le CERTA recommande de rechercher dans les journaux proxy d'éventuelles mises à jour ayant eu lieu durant cet intervalle pour identifier des postes impactés.

L'activation des mises à jours automatiques reste conseillée par l'ANSSI. Il convient cependant de pondérer cette recommandation selon le niveau de maturité du système d'information (SI). Sur un vaste SI maîtrisé, il est conseillé de récupérer les mises à jour sur des machines d'évaluation afin de réaliser des tests de non régression. Lors de cette phase, une étude de comportements anormaux de l'application devra être réalisée, afin d'éviter tout impact sur le SI après son déploiement.

Le CERTA rappelle que les attaques informatiques sont de plus en plus ciblées et que l'implémentation de cycles de validation des applications externes peut prévenir de nombreuses menaces.

Documentation

- Bulletin d'information sur la compromission d'Opera :
  http://my.opera.com/securitygroup/blog/2013/06/26/opera-infrastructure-attack

4 Rappel des avis émis

Dans la période du 28 juin au 04 juillet 2013, le CERTA a émis les publications suivantes :

- CERTA-2013-AVI-380 : Multiples vulnérabilités dans Citrix XenServer PV
- CERTA-2013-AVI-381 : Multiples vulnérabilités dans Adobe Photoshop Camera Raw
- CERTA-2013-AVI-382 : Multiples vulnérabilités dans WordPress
- CERTA-2013-AVI-383 : Vulnérabilité dans F5 BIG-IP et FirePass
- CERTA-2013-AVI-384 : Vulnérabilité dans Ruby
- CERTA-2013-AVI-385 : Vulnérabilité dans Atlassian Crowd
- CERTA-2013-AVI-386 : Multiples vulnérabilités dans HP ProCurve, H3C, 3COM

- CERTA-2013-AVI-387 : Multiples vulnérabilités dans Oracle Solaris
- CERTA-2013-AVI-388 : Multiples vulnérabilités dans Symantec Security Information Manager
- CERTA-2013-AVI-389 : Vulnérabilité dans Alcatel-Lucent OmniTouch
- CERTA-2013-AVI-390 : Multiples vulnérabilités dans Barracuda SSL VPN
- CERTA-2013-AVI-391 : Multiples vulnérabilités dans le noyau Linux de Ubuntu

Gestion détaillée du document

05 juillet 2013 version initiale.