

Vulnérabilités des postes clients

Un constat s'impose depuis quelques années dans le domaine de la sécurité des postes clients : la surface d'exposition de ces systèmes a sensiblement diminué ce qui a modifié les méthodes d'attaques.

Les systèmes d'exploitation les plus populaires comme Windows, ont fait le choix, dans leurs dernières versions, d'imposer dans leur configuration par défaut les mises à jour automatiques et l'activation d'un pare-feu. Ce dernier a rendu plus complexe les attaques directes visant des services vulnérables en écoute car la plupart des flux entrants sont dorénavant filtrés. Le temps des compromissions massives à l'aide de vers exploitant directement des failles de sécurité distantes semble révolu. Des vulnérabilités Windows récentes comme la MS08-001 [1] [2] ont néanmoins démontré qu'il était encore possible d'exploiter un service vulnérable protégé par le pare-feu Windows dans sa configuration par défaut. La généralisation des mises à jour automatiques a aussi contribué à réduire sensiblement les risques mais elles ne concernent par défaut que les composants du système d'exploitation (dont Internet Explorer sous Windows). Les mises à jour de logiciels tiers même très répandus (Microsoft Office, Mozilla Firefox, etc.) sont laissées au

Références

- [1] <http://www.microsoft.com/france/technet/security/bulletin/ms08-001.msp>
 [2] Cf. Retour sur la vulnérabilité MS08-001 du numéro 31

bon vouloir de chaque programme.

Ces évolutions n'ont pas échappé aux personnes malveillantes et de plus en plus de vulnérabilités exploitant les navigateurs Web populaires ont fait leur apparition. Il en va de même pour les extensions incontournables et multi-plate-forme comme Adobe Flash. Ces navigateurs représentent une cible de choix car ils sont disponibles dans beaucoup d'environnements et sont souvent l'un des uniques moyens de communication autorisés vers l'extérieur.

La compromission des postes clients repose en grande partie sur le maillon le plus faible : l'utilisateur. C'est en effet lui qui, en ouvrant des fichiers ou des liens douteux, va permettre la compromission de son poste (et parfois bien plus...). Un nombre croissant de compromissions sont réalisées en exploitant des vulnérabilités dans des

logiciels courants par le biais de fichiers jugés à tort inoffensifs. C'est le cas par exemple des suites bureautiques, des outils de gestion de documents (PDF entre autres), des logiciels de compression de fichiers, des lecteurs multimédias, etc. Ces logiciels, très largement répandus, disposent rarement des mises à jour de sécurité adéquates. Les vulnérabilités y étant découvertes sont en nette progression, ce qui montre bien l'intérêt croissant qui leur est porté. L'actualité récente montre aussi des cas d'attaques ciblées d'entreprises reposant sur l'exploitation de failles „0-day” dans ce type d'applications. On notera néanmoins qu'un certain nombre de logiciels tiers adoptent une politique de mise à jour de sécurité semblable à celle de Microsoft en invitant automatiquement les utilisateurs à installer une nouvelle version dès sa disponibilité. C'est à mon sens la seule solution viable pour améliorer globalement la sécurité du poste client.

La limitation des privilèges octroyés aux utilisateurs et donc aux applications qu'ils exécutent permet aussi de restreindre les impacts d'une compromission. Cette approche du moindre privilège a aussi été adoptée depuis peu dans la dernière version de Windows destinée aux postes clients même si elle repose en grande partie sur un mécanisme (UAC) basé sur la décision de l'utilisateur... et on sait bien que celui-ci a tendance à cliquer sur „Oui” sans même prendre le temps d'analyser la situation.

Ces navigateurs représentent une cible de choix car ils sont disponibles dans beaucoup d'environnements.



À propos de l'auteur

Guillaume Lehembre est un consultant sécurité français travaillant pour le cabinet HSC (Hervé Schauer Consultants - <http://www.hsc.fr>) depuis 2004. Il a travaillé sur différents audits, études et tests d'intrusion et s'intéresse de près à des sujets comme la sécurité des réseaux sans fils et la voix sur IP. Il a réalisé des interventions publiques sur ces sujets et a publié plusieurs articles, dont un article dans le numéro 14 de Hakin9 intitulé Sécurité Wi-Fi - WEP, WPA et WPA2. Il rédige un éditorial dans Hakin9 depuis Janvier 2007. Guillaume peut être contacté à l'adresse suivante : Guillaume.Lehembre@hsc.fr