Des ‘hackers’ pirates se paient des liens sponsorisés sur Google

Attention les pirates du Net viennent de mettre au point une nouvelle méthode pour nous inciter à visiter des sites contenant du code malveillant. Pour mener leurs actes de malveillance, ces cyber-délinquants n’hésitent pas à utiliser le moteur de recherche Google.

« En achetant des mots clés sur le géant de la recherche, les « black hats » redirigent les internautes vers des URL modifiées et contenant du code malveillant » explique Roger Thompson, CTO de Exploit Prevention Labs, une société spécialisée dans la sécurité,

« Ce « complot » utilise les liens sponsorisés de Google qui apparaissent en marge des résultats de recherche du moteur, et des ‘malwares’ capables de voler des informations confidentielles. La grande nouveauté c’est que cette technique induit un investissement, un paiement de la part des hackers », poursuit Thompson. *» Au lieu de simplement pirater les sites, ils doivent acheter des mots clés. »*

Tout compte fait, cette méthode est logique puisque ces mots clés font que les liens sponsorisés des cybercriminels sont très bien classés dans les résultats d’une recherche. Les ingénieurs des laboratoires d’Exploit Prevention expliquent comment ils ont découvert ce piratage :

« En lançant une requête contenant les termes « betterbusinessbureau » ou » modern cars airbags required » nous avons remarqué qu’un lien sponsorisé redirigeant vers le site associatif ***smartrack.org*** *apparaissait. Ce site malveillant utilisait un ‘exploit’ dans le MDAC (Microsoft Data Access Components » de Windows pour dissimuler une « backdoor » et un « post logger » sur le PC cible. »*

Rappelons que le MDAC a profité de trois correctifs (patchs) ces trois dernières années, le dernier remonte au mois de février 2007, quand la vulnérabilité a été jugée *« critique »* par la majorité des éditeurs de sécurité.

Une fois le ‘malware’ installé sur l’ordinateur non patché, le site smarttrack.org redirige discrètement l’internaute vers le véritable lien à l’origine de sa recherche.*« Une centaine de sites bancaires ont été la cible de ce type de détournement, »* constate Thompson.

« Ce schéma d’attaque a été découvert pour la première fois le 10 avril 2007, mais sa durée de vie est limitée. Dans le cas de smartrack.org le nom de domaine a été enregistré le 2 avril 2007. Google a retiré du réseau une vingtaine de ces liens sponsorisés malveillants dont smarttrack.org », précise Thompson.