Outlook Web App ciblé par des attaques de phishing sophistiquées – Le Monde Informatique

	Outlook Web App ciblé par des attaques de phishing sophistiquées

Selon les chercheurs de Trend Micro, un groupe de pirates sévit à l'encontre d'agences militaires, ambassades et d'entreprises liées à la défense nationale et des médias internationaux utilisant Outlook Web App d'Office 365.

Afin de voler les identifiants de messagerie des employés de nombreuses organisations publiques, parapubliques mais également privées, un groupe d'espions a mis en place des techniques de phishing avancées.
Selon des chercheurs de l'entreprise de sécurité Trend Micro, qui ont baptisé cette campagne Operation Pawn Storm dans un document publié la semaine dernière, le groupe à l'origine de ces attaques opèrerait depuis au moins 2007. Au cours de ces années, ils ont utilisé différentes techniques pour atteindre leurs objectifs, notamment des campagnes de phishing pour propager des malwares sous forme de pièces jointes Microsoft Office malveillantes, l'installation de backdoors type SEDNIT ou Sofacy, ou des exploits plus sélectifs pour infecter des sites légitimes.

Dans ses dernières attaques de phishing, le groupe a utilisé une technique particulièrement intéressante, ciblant les organisations qui utilisent Outlook Web App (OWA), une composante du service Office 365 proposé par Microsoft. Pour chaque attaque, le groupe a créé deux faux domaines : un premier, qui reproduit un site Web tiers connu des victimes – par exemple le site d'une conférence dans un secteur de l'industrie qui les intéresse – et un second, similaire au domaine utilisé pour le déploiement d'Outlook Web App par l'organisation visée. Les attaquants ont ensuite créé des courriels contenant un lien vers le faux site tiers sur lequel ils hébergeaient un code JavaScript non malveillant dont le but était double : ouvrir le site légitime dans un nouvel onglet et rediriger l'onglet déjà ouvert du navigateur Outlook Web App vers une page de phishing. « Le code JavaScript faisait croire aux victimes que leur session OWA était close, et la page malveillante leur demandait de se reconnecter en tapant à nouveau leurs identifiants », ont écrit les chercheurs de Trend Micro dans leur document.
« Les attaquants ont réussi à rediriger les victimes vers de fausses pages Outlook Web App en agissant sur les propriétés d'ouverture des pages de leurs navigateurs ».

Une technique de phishing multi-navigateurs
Selon les chercheurs, cette technique n'exploite aucune vulnérabilité et fonctionne avec tous les navigateurs courants dont Internet Explorer, Mozilla Firefox, Google Chrome et Safari d'Apple. Cependant, il faut deux conditions pour que ce mode opératoire fonctionne : « Les victimes doivent utiliser OWA et ils doivent cliquer sur les liens intégrés au volet de prévisualisation OWA », ont-ils expliqué. L'attaque est redoutable parce que l'onglet du navigateur ne permet pas aux victimes de voir que leur session OWA est illégitime et ils ont peu de chance de se rendre compte que l'URL a été usurpée avant de rentrer leurs identifiants. « De plus, les attaquants ont pris soin d'utiliser des noms de domaine très similaires à ceux choisis par les organisations ciblées pour leurs pages de log in OWA, et dans certains cas, ils ont même acheté des certificats SSL légitimes, de sorte que les navigateurs des victimes affichent aussi les indicateurs de connexion sécurisée HTTPS pour les sites de phishing », ont encore ajouté les chercheurs de Trend Micro.

Parmi les personnes visées, on trouve des employés de l'entreprise militaire privée américaine Academi, anciennement connue sous le nom de Blackwater ; l'Organisation pour la sécurité et la coopération en Europe (OSCE) ; le Département d'État des États-Unis ; le fournisseur du gouvernement américain Science Applications International Corporation (SAIC) ; une société multinationale basée en Allemagne ; l'ambassade du Vatican en Irak ; des médias de radiodiffusions de plusieurs pays ; les ministères de la Défense de la France et de la Hongrie ; des responsables militaires pakistanais ; des employés du gouvernement polonais et des attachés militaires de différents pays. Parmi les appâts utilisés par les assaillants, les chercheurs ont identifié des événements et des conférences bien-connus pour lesquels les victimes pouvaient avoir un intérêt.
« Mais, ce n'est pas tout : les assaillants ont combiné leur tactique de phishing à diverses attaques éprouvées afin de compromettre les systèmes et entrer dans les réseaux pour y voler des données », ont déclaré les chercheurs de Trend Micro.
« Les variantes de SEDNIT utilisées ont été semble-t-il très efficaces car elles ont permis aux pirates de voler des informations sensibles sur les ordinateurs des victimes en évitant de se faire repérer ».

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.lemondeinformatique.fr/actualites/lire-outlook-web-app-cible-par-des-attaques-de-phishing-sophistiquees-59081.html