Microsoft Outlook sous la menace d'assauts liés à une vulnérabilité 0-Day

La suite **Microsoft Office**, et particulièrement **Outlook**, serait sous la menace d'une vulnérabilité 0-Day. Autrement dit, une faille de sécurité non colmatée dans le logiciel de l'éditeur susceptible de servir de point d'entrée pour une cyberattaque.

Sophos pointe en effet un défaut du protocole Dynamic Data Exchange (DDE) de Microsoft.

DDE permet d'envoyer des messages et partager les données entre les applications. Selon le chercheur Mark Loman, un attaquant pourrait exploiter cette vulnérabilité pour exécuter un malware sans utiliser de macro.

Si le protocole existe depuis 1993, la faille qui l'accompagne n'a été mise en évidence qu'à l'occasion du bulletin de sécurité du mois d'octobre.

Depuis, *« de nombreux attaquants utilisent l'astuce pour déployer des chevaux de Troie d'accès à distance »*, déclare le chercheur de Sophos.

Attaque depuis une invitation Outlook

Le mode de propagation reste le même qu'habituellement. Les attaquants envoient un e-mail avec une pièce jointe sous forme d'un fichier Word ou Excel qui contient une macro infectieuse.

Tant que l'utilisateur n'exécute pas cette macro, il reste protégé.

Mais avec la faille DDE, même si l'exécution de macro est désactivée par défaut, l'attaquant peut mener sa tentative d'infection à bien.

Il est également possible de déclencher des attaques DDE dans Outlook via des courriels ou, directement, des invitations formatées avec Microsoft Outlook Rich Text Format.

« En plaçant le code dans le corps même du message, l'attaque est de plus en plus possible alors que faire tomber une personne ciblée dans le piège devient plus facile », considère Sophos dans son alerte.

Sauvé par les boîtes de dialogue

Par chance, l'exploitation de la faille DDE n'affranchit pas l'affichage des boîtes de dialogue invitant à valider, ou pas, l'action requise. L'utilisateur y trouvera là son salut s'il reste attentif au message alors affiché.

Celui-ci prévient notamment que certaines données ne sont pas accessibles et propose de lancer l'invite de commande pour les exécuter.

Une formulation suffisamment inhabituelle pour mettre la puce à l'oreille de l'utilisateur ciblé. Il en aura besoin.

Sauf à disposer d'une solution de sécurité stoppant ce type d'attaque, Microsoft n'a, pour l'heure, pas indiqué s'il comptait corriger la faille de son protocole.

Lire également
Esteemaudit : une zero day sur RDP de Windows XP et 2003 inquiète
Un vieux piratage de session Windows remis au goût du jour
Microsoft corrige encore Windows Defender en toute discrétion

(crédit photo : GlebStock-Shutterstock)