Cyberattaque Exchange : l'Europe touchée dans l'ombre des États-Unis

Combien de victimes… et combien d'assaillants ? Une semaine après les révélations sur les attaques visant les serveurs Exchange, il reste difficile de donner des estimations. À plus forte raison, du fait que les failles qui ont permis ces attaques sont désormais publiques – et facilement exploitables.

En l'état, les cibles semblent localisées essentiellement aux États-Unis. Mais l'Europe n'est pas épargnée. Sur place, une victime de marque s'est signalée : l'Autorité bancaire européenne. Elle a dû couper ses systèmes de messagerie. Ses investigations n'ont révélé, affirme-t-elle, ni exfiltration de données, ni propagation sur son réseau.

> *Most targets are located in the US but we've seen attacks against servers in Europe, Asia and the Middle East. Targeted verticals include governments, law firms, private companies and medical facilities. 3/5 pic.twitter.com/kwxjYPeMlm*
>
> *— ESET research (@ESETresearch) March 2, 2021*

De la CISA à l'ANSSI en passant par le CERT-EU, même consigne : dans la mesure du possible, patchez vos serveurs Exchange locaux sans attendre. À défaut, mettez en place les mesures de contournement provisoires que propose Microsoft. Mais gardez à l'esprit qu'elles ont un impact sur la fonctionnalité des serveurs Exchange, en plus de ne pas garantir une protection complète.

> *CISA urges ALL organizations across ALL sectors to follow guidance to address the widespread domestic and international exploitation of Microsoft Exchange Server product vulnerabilities; see CISA's newly released web page for details. https://t.co/VwYqAKKUt6. #Cyber #InfoSec*
>
> *— US-CERT (@USCERT_gov) March 9, 2021*

> *Zero-Day Vulnerabilities in Microsoft Exchange (CERT-EU Security Advisory 2021-013) – https://t.co/X33ges46Cx*
>
> *— CERT-EU (@CERTEU) March 3, 2021*

> *Alerte CERT-FR*
>
> *Mise à jour de l'alerte CERTFR-2021-ALE-004 concernant les vulnérabilités critiques dans Microsoft Exchange Server : Ajout des informations communiquées par Microsoft et des recommandations du CISA. https://t.co/mqi0jN8pW5*
>
> *— CERT-FR (@CERT_FR) March 8, 2021*

Un *webshell* à l'ancienne ?

En première ligne des accusés, la Chine. Et plus particulièrement un groupe cybercriminel dit à la solde de Pékin. On le connaît sous le nom de Hafnium.
Parmi ses compatriotes apparemment impliqués figurerait notamment LuckyMouse, aussi appelé Emissary Panda ou APT27. Parmi ses faits d'armes, une attaque « à la SolarWinds » au sens où elle se fondait aussi sur l'infection de mises à jour d'un logiciel. Son nom : Able Desktop. Sa fonction : la messagerie instantanée. Il fait partie d'une suite bureautique populaire en Mongolie, en particulier auprès de l'administration. On y a trouvé une *backdoor* et plusieurs chevaux de Troie.

Sur les serveurs Exchange, la porte dérobée prend la forme d'un *webshell*. Il semble s'agir d'une variante de China Chopper, utilisé au moins depuis 2013. Son canal d'entrée : les OAB (carnets d'adresses en mode hors connexion), grâce à une faille qui permet des écritures arbitraires.

Plusieurs indices illustrent le caractère hautement automatisé des attaques. Par exemple, le fait que des serveurs compromis aient fait l'objet de multiples tentatives ultérieures de compromission.

Qu'y a-t-il au-delà du *webshell* ? Microsoft recense, entre autres activités malveillantes survenues sur les serveurs touchés :

- Le vol d'identifiants par copie de la mémoire du processus LSASS, qui assure l'authentification
- L'utilisation des *snap-in* de PowerShell pour exfiltrer le contenu des boîtes mail
- L'exploitation d'outils comme Covenant, Nishang et PowerCat pour les accès à distance

Illustration principale © Julien Eichinger – Fotolia