Un malware sur Lambda : quel modèle de sécurité chez AWS ?

A-t-on trouvé le « premier *malware* ciblant spécifiquement Lambda » ? Tout du moins, le premier révélé au public, assure Cado Security. La start-up anglaise affirme qu'on lui doit cette découverte.

L'annonce intervient au moment où sa plate-forme de détection et de réponse aux menaces s'étend officiellement aux environnements *serverless*. Plus précisément ceux d'AWS : Fargate… et Lambda.

> *Today we're excited to announce that the Cado Response platform now supports #serverless environments, offering customers extended visibility and analysis of #AWSFargate and #Lambda https://t.co/0bCirs7GNU*
>
> *— Cado (@CadoSecurity) April 5, 2022*

Concours de circonstances ou communication orchestrée ? C'est en tout cas l'occasion de se rappeler le « modèle de responsabilité partagée » en place sur Lambda. AWS sécurise l'environnement d'exécution, mais le client est responsable du code de ses fonctions comme de la gestion des identités et des accès.

Denonia : vraiment rien que pour Lambda ?

Cado Security a donné au *malware* en question le nom de Denonia, en référence à l'une des URL qu'il tente de joindre. Le premier échantillon découvert* date de fin février 2022. Écrit en Go, il semble abriter une variante de XMRig (cryptomineur).

Comment Denonia est-il déployé ? Cado Security reconnaît l'ignorer. Quant à savoir s'il vise uniquement Lambda, là aussi, ce n'est pas certain. Plusieurs indices semblent toutefois confirmer qu'il s'agit au moins de sa cible principale. En tête de liste, un message d'erreur qui s'est affiché lors de l'analyse : le *malware* avait cessé de fonctionner à défaut de variables d'environnement Lambda.

Autres indicateurs : diverses bibliothèques embarquées. Permettant, entre autres, d'écrire des fonctions Lambda en Go et de retrouver des éléments contextuels dans des requêtes API.

Une autre bibliothèque a attiré l'attention. Elle implémente le protocole DoH, qui opère la résolution DNS sur HTTPS. Soit, dans le cas de Denonia, une façon de passer sous davantage de radars au moment de communiquer avec ses serveurs de commande et de contrôle.

** Les investigations ont mené à la découverte d'un autre échantillon, daté de janvier. Cado Security ne fait pas de commentaire à son propos.*

Illustration principale © Murrstock – Adobe Stock