Un malware, c'est quoi au juste ? AWS suscite le débat

Le *malware* que Cado Security dit avoir détecté sur Lambda en est-il vraiment un ? En s'y reprenant à deux fois, AWS s'est inscrit en faux.

La start-up britannique a expliqué avoir trouvé deux échantillons dudit *malware* – qu'elle a appelé Denonia en référence à une des URL qu'il tente de joindre. Le plus ancien (daté de janvier) n'a fait l'objet d'aucun commentaire de sa part. L'autre (de fin février) abritait semble-t-il une variante du cryptomineur XMRig.

D'après Cado Security, il s'agit, *texto*, du « premier *malware* ciblant spécifiquement Lambda ». Ou tout du moins du premier révélé au public.

Effet d'aubaine ? On aura noté que l'annonce est intervenue au moment même où la plate-forme de détection et de réponse aux menaces de Cado Security s'étendait officiellement aux environnements *serverless*. Plus précisément, ceux d'AWS : Fargate… et Lambda.

Pour AWS, Denonia n'est pas un *malware*

Le groupe américain n'a pas manquer de dénoncer un « sensationnalisme » contrastant avec la réalité d'une découverte « plutôt banale ». Et d'assurer, dans un premier temps, qu'on n'avait pas affaire à un *malware*. La raison ? Le logiciel en question s'appuie sur des informations de connexion obtenues frauduleusement ; il n'est pas capable par lui-même d'accès indésirables.

Cette position n'a pas fait l'unanimité dans le monde de la cyber. On a notamment fait remarquer que la plupart des programmes qu'on qualifie de *malwares* n'ont pas la capacité en question. Autre argument souvent invoqué : l'intention malveillante suffit à considérer un logiciel comme tel.

Denonia ne peut se propager automatiquement entre instances Lambda. Et sur chacune de celles qu'il cible, il a besoin d'informations de connexion. Pour AWS, cela suffit à dire que Lambda n'est pas vulnérable. C'est dans ce sens que la branche cloud d'Amazon a orienté son « deuxième jet » : Denonia n'exploite aucune vulnérabilité dans son offre de calcul sans serveur. Pour le reste, elle ne s'est pas complètement dédite : le code ne réalise « aucune des actions communément incluses dans la définition d'un *malware* ».

Photo d'illustration © ZinetroN – Adobe Stock