Cloud : quelles sont les menaces les plus dangereuses et comment s'en protéger ?

Le paysage de la cybersécurité est en perpétuelle évolution, et il est impératif de se tenir au courant des nouvelles techniques et surfaces d'attaque. Alors que les entreprises continuent de se tourner vers le cloud pour stocker leurs données et accéder à des services, les menaces liées à ces nouvelles technologies ne cessent d'augmenter.

Voici un résumé des techniques d'attaque les plus dangereuses observées à ce jour.

1. Vulnérabilités des services

L'une des attaques les plus fréquemment observées dans les réseaux cloud est la compromission par des services vulnérables.

Il est, par conséquent, essentiel de mettre à jour ces systèmes pour limiter les risques. Ce qui menace particulièrement les services cloud, ce sont les actions post-compromission, comme le déplacement latéral vers les principaux systèmes et ressources d'entreprise hébergés dans un réseau cloud. Le défi majeur pour les victimes est donc de répondre efficacement et rapidement.

Beaucoup d'entreprises concernées, qui s'appuyaient sur les scanners de vulnérabilités pour identifier et se protéger de ce type de failles, ont été exposées à un risque accru sur leurs réseaux, la vulnérabilité ayant été exploitée une semaine avant sa découverte.

Un exemple bien connu est Apache Log4J, qui une fois découvert, a eu un impact massif dans le monde entier. La gravité des attaques qui se sont produites à la suite d'une telle vulnérabilité montre à quel point il est vital pour les entreprises de détecter les activités malveillantes avant qu'un service ne soit identifié comme vulnérable.

2. Mauvaises configurations du cloud

Les erreurs de configuration sont la cause la plus courante des fuites de données dans le cloud, les entreprises laissant accidentellement les données de leurs clients accessibles au public, et les rendant ainsi facilement exploitables par les cybercriminels.

Ces erreurs ont entraîné une augmentation des fuites de données au fil des années. Encore une fois, ce phénomène n'est pas propre au cloud mais il est de plus en plus courant, lié notamment à la complexité des configurations dans le cloud.

En outre, la vigilance sur ces configurations ne vise pas qu'à prévenir les fuites de données. Dans de nombreux cas, il a également été constaté que les hôtes du cloud ont pu être infectés par des malwares ou par un accès supplémentaire au réseau, sans doute lié à des modifications du système opérées par un attaquant.

Le groupe de hackers TeamTNT a ainsi accédé à des Docker Daemon non sécurisés pour installer et exécuter ses propres images malicieuses, infectant les victimes via un botnet ou par minage de crypto-monnaie. Il s'agit d'une technique simple mais très efficace contre les entreprises dont les services cloud sont mal configurés.

La variété d'applications liées aux réseaux cloud qui peuvent être compromises lorsqu'elles sont mal configurées est trop vaste pour être abordée ici. Cependant, il faut retenir qu'un oubli de configuration permet non seulement de potentiellement générer une compromission des services cloud, mais également de devenir un vecteur d'intrusion extrêmement simple pour un cybercriminel compétent.

3. Attaques sur la chaîne logistique

Les attaques sur la chaîne logistique continuent à se multiplier. Certaines sont clairement identifiées, notamment Solarwinds attribuée à une APT russe, toutefois, il en existe beaucoup d'autres qui sont isolées dans les réseaux et services cloud.

Une méthode d'attaque sur la chaîne d'approvisionnement de plus en plus courante est la compromission des images Docker Hub.

TeamTNT, dont il a été question précédemment, a compromis et continue de compromettre les images Docker Hub, entraînant la compromission pour toute personne installant et mettant à jour ces images.

Leurs objectifs principaux incluent une fonctionnalité de botnet plus générique et le recours au minage. Les administrateurs de Docker doivent faire preuve de prudence lorsqu'ils intègrent de nouvelles images et qu'ils installent des logiciels externes sur leur réseau.

Une télémétrie appropriée des endpoints, exécutant de telles images, permet de s'assurer que rien de malveillant ne s'active après un certain délai.

En ce qui concerne la chaîne d'approvisionnement des logiciels, il existe de nombreuses opportunités pour l'attaquant. Comme observé lors de la compromission de l'outil d'envoi de rapports Bash uploader de Codecov en 2021, les logiciels peuvent être compromis aussi simplement qu'efficacement.

Cet outil – couramment utilisé dans le cycle de vie du développement logiciel – a été modifié par une mise à jour, incluant une seule ligne de code, qui n'a pas été découverte pendant des mois. Ce code a permis à l'attaquant d'extraire des identifiants stockés dans les environnements et processus d'intégration continue des clients.

À l'heure actuelle, impossible de se prononcer sur les véritables intentions de ces hackers mais de telles attaques continueront à être plus fréquentes, en particulier via des logiciels libres utilisés dans le monde entier.

4. Accès à la plateforme de gestion du cloud

De tels exemples nous amène à conclure qu'une grande partie des menaces liées au cloud vise à accéder à la plate-forme de gestion du cloud, en particulier aux comptes cloud privilégiés. Il est essentiel de se défendre contre les menaces liées au cloud car elles offrent à l'attaquant la possibilité de franchir la barrière de l'accès aux informations ou du contrôle d'un service puissant et normalement fiable.

Un hacker disposant d'un accès privilégié à la plateforme de gestion d'un service cloud, qu'il s'agisse d'AWS GCP ou d'Azure, peut se faufiler dans de nombreux endroits difficiles à identifier.

Grâce à l'utilisation d'outils open source tels que Purple Panda, un attaquant, disposant d'informations d'identification volées, peut automatiser l'escalade de privilèges et identifier les possibilités de mouvement latéral.

Les moyens utilisés par les attaquants afin d'obtenir un tel accès sont encore assez nombreux, telle que l'analyse des référentiels de code et d'images en ligne (Github, Docker Hub) qui permet de trouver des clés divulguées par erreur. Cela a permis de lancer des attaques sur la chaîne d'approvisionnement et des vols de données en masse.

En outre, des hackers très compétents et disposant de ressources importantes, comme APT29, recherchent ce type d'accès pour des missions commanditées par des Etats. L'hyper vigilance est donc de rigueur car ce niveau d'accès est, en général, particulièrement convoité par les cybercriminels.

Les attaquants ciblent de plus en plus fréquemment les vulnérabilités des applications, des logiciels libres et des technologies dans le cloud. Bien que les techniques utilisées lors de ces attaques soient variées, elles reposent généralement sur le fait que les réseaux cloud sont vastes, complexes et difficiles à gérer.

Les solutions de sécurité des agents et des conteneurs sont donc essentielles pour protéger les entreprises contre les menaces qui pèsent sur tout type de plateforme cloud.