Le vols des identifiants persiste et Ã©volue en ! 2018
Internet
PostÃ© par : JulieM
PubliÃ©e le : 20/12/2017 13:00:00

La rÃ©cente rÃ©vÃ©lation dâ□□Uber, sur le vol des donnÃ©es personnelles de 57 millions de ses clients, vient sâ□□ajouter Ã une longue liste de cyberattaques auxquelles les entreprises ont encore fait face cette annÃ©e.

Les techniques des pirates informatiques Ã©tant chaque fois plus sophistiquÃ©es, 2018 sâ□□annonce tout aussi menaÃ§ante pour les organisations qui ne sont pas prÃ©parÃ©es. Les innovations technologiques, qui permettent aux entreprises dâ□□amÃ©liorer et de varier leurs stratÃ©gies, offrent les mÃªmes opportunitÃ©s aux individus malveillants. 2018 promet ainsi une utilisation accrue de l'automatisation et de l'expansion des environnements hybrides cloud et DevOps.

Ces derniers crÃ©eront un terrain fertile pour les attaquants, du fait dâ□□un nombre croissant de comptes Ã privilÃ¨ges, associÃ©s Ã des utilisateurs humains ou non. Ces droits dâ□□accÃ¨s concernent des employÃ©s, des fournisseurs distants, des comptes de service, des clÃ©s d'accÃ¨s, des machines, des clÃ©s SSH (Secure Shell), ou encore des mots de passe intÃ©grÃ©s.

Selon Lavi Lazarovitz, Cyber Security Research Team Leader, chez CyberArk, les attaques et exploitations basÃ©es sur le vol des identifiants vont sâ□□accÃ©lÃ©rer pour dominer les cybermenaces en 2018, en particulier pour trois raisons :

Les pirates informatiques cachÃ©s derriÃ¨re des identitÃ©s machine

Les identitÃ©s fÃ©dÃ©rÃ©es, soit le fait de lier tous les droits dâ□□accÃ¨s dâ□□une personne Ã un identifiant unique, tendent Ã augmenter pour simplifier lâ□□expÃ©rience utilisateur. Or dâ□□un point de vue sÃ©curitaire, cette simplification accroit les vulnÃ©rabilitÃ©s, les identifiants devenant alors identiques.

De plus, lâ□□adoption croissante d'environnements basÃ©s sur les services augmente

automatiquement le nombre d'identitÃ©s ; il en dÃ©coule une surface d'attaques Ã©tendue, dans laquelle les pirates informatiques ne ciblent plus en prioritÃ© les identifiants de l'administrateur de domaine. Les Ã©quipes de sÃ©curitÃ© doivent donc Ãªtre prÃ©parÃ©es Ã dÃ©terminer quels utilisateurs et quelles machines sont dignes de confiance.

En volant les identitÃ©s des machines, les pirates peuvent en effet faire profil bas sur le rÃ©seau, tout en utilisant les droits dâ□□accÃ¨s associÃ©s pour contrÃ´ler les procÃ©dures et rÃ¨gles de sÃ©curitÃ©. Les outils dâ□□intÃ©gration et de livraison continues peuvent devenir alors les atouts les plus sensibles du rÃ©seau : lorsque leurs identifiants sont exploitÃ©s par une personne malveillante, cette derniÃ¨re peut en effet prendre le contrÃ´le de l'intÃ©gralitÃ© du workflow DevOps, et y intÃ©grer du code ou des configurations nuisibles.

Le chaos des clÃ©s SSH, source de consÃ©quences inattendues

Les clÃ©s SSH sont souvent utilisÃ©es pour accÃ©der aux ressources cloud, ce qui signifie que le protocole de connexion impose un Ã©change de clÃ©s de chiffrement en dÃ©but de connexion. Seulement, beaucoup dâ□□entreprises ne dÃ©ploient pas les infrastructures nÃ©cessaires pour sÃ©curiser les environnements DevOps. Cette absence de gestion engendre un "chaos de clÃ©s", et augmente le risque quâ□□elles soient exposÃ©es et compromises via des erreurs simples ou humaines.

Les Ã©quipes de sÃ©curitÃ© doivent donc amÃ©liorer la supervision pour Ã©viter que ces clÃ©s ne deviennent des cibles faciles pour les attaquants. Les principales prÃ©occupations associÃ©es concernent la multiplication des identifiants de machines et dâ□□humains, qui offrent des opportunitÃ©s de vols de privilÃ¨ges. Par exemple, un utilisateur, ayant accÃ¨s Ã un rÃ´le assignÃ© Ã une machine et dotÃ© de privilÃ¨ges, pourrait dÃ©rober l'identitÃ© de cette machine et nuire au compte cloud associÃ©.

De plus, les jetons d'authentification temporaires, employÃ©s en complÃ©ment ou Ã la place d'un mot de passe pour prouver lâ□□identitÃ© de lâ□□utilisateur, se rÃ©vÃ¨lent parfois Ãªtre une arme Ã double tranchant. En effet, bien quâ□□ils constituent une amÃ©lioration par rapport aux clÃ©s statiques, quâ□□ils expirent gÃ©nÃ©ralement aprÃ¨s un certain temps et quâ□□ils offrent des privilÃ¨ges dynamiques, ils ne fournissent une meilleure sÃ©curitÃ© que s'ils sont gÃ©rÃ©s correctement et surveillÃ©s en continu.

Security as a Target (SaaT) : l'authentification dans la ligne de mire des attaquants

Le cloud pousse au renforcement de l'identitÃ© Ã mesure que nous utilisons davantage de services, et moins de technologie brute ; cela entraine plus de possibilitÃ©s pour les hackers dâ□□effectuer des mouvements latÃ©raux entre les services, et une compromission plus facile au niveau de l'authentification, ce qui signifie une perte totale de l'identitÃ© pour lâ□□entreprise. Les mÃ©thodes actuelles d'authentification, telles que celle Ã deux facteurs et SSO (Single Sign On, soit une authentification unique), doivent alors s'adapter pour se protÃ©ger contre les menaces Ã©mergentes et afin de ne pas devenir des cibles.

Car si ces outils sont compromis, ils permettent aux attaquants une flexibilitÃ© sans prÃ©cÃ©dent, et leur offrent la capacitÃ© de compromettre les rÃ©seaux en profondeur. D'un point de vue dÃ©fensif, la technologie blockchain pourrait Ãªtre adoptÃ©e pour supprimer le seul point de confiance et d'Ã©chec qui favorise les techniques dâ□□attaques Golden Ticket et SAML. Elle pourrait en effet Ãªtre utilisÃ©e pour dÃ©placer la "confiance absolue" de l'Active Directory, par exemple, vers l'ensemble du rÃ©seau. Les pirates seraient alors forcÃ©s de compromettre une quantitÃ© significative d'actifs avant de pouvoir s'authentifier.

Les cyberattaques dont nous avons Ã©tÃ© tÃ©moins en 2017, telles que WannaCry et NotPetya, et celles des annÃ©es prÃ©cÃ©dentes, sont souvent liÃ©es Ã une adoption trop rapide de

technologies qui ne sont pas complÃ¨tement sÃ©curisÃ©es. Lâ□□intÃ©gration de toute innovation doit en effet sâ□□aligner Ã des stratÃ©gies de gestion des risques. Pour de nombreuses organisations, le dÃ©fi rÃ©side donc dans le fait que les nouvelles technologies nâ□□ont pas le niveau de maturitÃ© en matiÃ¨re de sÃ©curitÃ© que celles plus anciennes.

Les entreprises se retrouvent par consÃ©quent vulnÃ©rables aux attaques, en particulier celles qui visent les comptes administrateurs, voie royale des hackers vers leurs systÃ¨mes et leurs donnÃ©es. Le risque est donc bien rÃ©el, avec pour consÃ©quence des milliards dâ□□identifiants clients disponibles sur le Dark Web. En mai 2018, le RÃ¨glement GÃ©nÃ©ral de la Protection des DonnÃ©es (RGPD) entrera en vigueur en Europe et obligera les organisations Ã se conformer Ã un certain nombre de rÃ¨gles strictes en matiÃ¨re de cybersÃ©curitÃ©.

Bien que contraignant au premier abord, il permettra aux entreprises de mieux apprÃ©hender la gestion de leurs donnÃ©es et la protection de leurs systÃ¨mes pour lutter contre les cyberattaques, toujours plus agressives et vouÃ©es Ã se dÃ©velopper au rythme des innovations technologiques.