CyberArk publie un rapport sur les nouvelles tendances en matière d’attaques ciblées avancées – Global Security Mag Online

	CyberArk publie un rapport sur les nouvelles tendances en matière d’attaques ciblées avancées – Global Security Mag Online

CyberArk annonce la publication d'un nouveau rapport qui détaille les tendances actuelles des cyberattaques ciblées avancées, lesquelles ont communément adopté comme signature clé l'exploitation malveillante des comptes à privilèges.

L'étude intitulée « Privileged Account Exploits Shift the Front Lines of Security » apporte une expertise sur les récentes tendances des attaques ciblées, à partir de l'expérience de terrain des analystes les plus réputés au monde en matière de menaces informatiques et de résolution des attaques de sécurité les plus dévastatrices. Les participants à cette analyse incluent :

· Groupe de renseignements de sécurité et de recherche Cisco Talos
· Service de consultance financière Deloitte LLP – Equipe de recherche informatique
· Deloitte & Touche LLP – Services en matière de risques informatiques
· Mandiant, une entreprise FireEye
· RSA, Division Sécurité d'EMC
· L'équipe RISK de Verizon

« Cette coalition rassemble certains des analystes des menaces informatiques les plus brillants, expérimentés et réputés au monde. C'est en comparant et en comprenant les points communs de nos recherches respectives que nous avons pu dresser un aperçu approfondi des modes de fonctionnement des attaques ciblées, explique Udi Mokady, PDG de CyberArk. Cette étude nous a permis de découvrir que presque chaque attaque avancée implique une exploitation de comptes à hauts pouvoirs, raison principale pour laquelle elles sont si difficiles à déceler et à stopper. Ces comptes permettent en effet aux assaillants d'accéder à des réseaux et bases de données sécurisés, d'effacer toute trace d'infraction, d'éviter toute détection et de créer des portes de sortie rendant leur éviction des réseaux quasi impossible. La sécurisation des comptes à privilèges est devenue la nouvelle priorité des systèmes de défense dans la bataille que les entreprises mènent actuellement face à la cybercriminalité. »

Les comptes à privilèges, qui se composent notamment des identifiants utilisés pour l'administration informatique des mots de passe par défaut et codés en dur ainsi que de backdoors d'applications, offrent aux pirates informatiques un véritable laissez-passer qui leur permet de se rendre où ils le souhaitent et de traverser le réseau sans le moindre obstacle. Ces comptes permettent également aux hackers d'effacer leurs traces et de soutirer des données en tous genres. Et dès que ceux-ci parviennent à obtenir un accès privilégié aux systèmes et applications critiques, il est extrêmement difficile de les arrêter et d'atténuer les risques de perte de données et de préjudice commercial.

Parmi les principales découvertes du rapport :
· Chaque secteur et chaque entreprise est aujourd'hui une cible : Les pirates informatiques ont élargi leur champ d'action et **ciblent aujourd'hui les entreprises de toutes tailles**, dans tous les secteurs confondus. Chaque attaque a souvent une cible bien déterminée, et les **pirates visent fréquemment leurs partenaires et fournisseurs**. Les analystes en sécurité ont étudié des attaques visant des cibles non-traditionnelles, telles que des **sociétés de transport par camion** et de nombreux autres prestataires de services professionnels (**conseillers en gestion, auditeurs, avocats spécialisés dans les contentieux, etc.**), lesquelles constituent une étape clé dans le processus d'attaque d'un partenaire commercial.
· La résistance de périmètre est futile : Les pirates parviendront tout de même à s'introduire dans le périmètre de sécurité, et les employés constitueront le point d'infection le plus probable. L'attaque par hameçonnage est la technique la plus répandue et ne fait que gagner en sophistication, ce qui a rendu les connexions des employés beaucoup plus simples à infiltrer que les réseaux ou autres logiciels.
· Les pirates restent cachés pendant plusieurs mois ou années : Lors de leur détection, la plupart des attaques étaient en cours depuis au moins 200 jours. Les attaques financières sont quant à elles décelables plus rapidement, en règle générale en moins de 30 jours. Les assaillants peuvent dissimuler leurs traces par le biais des comptes à privilèges, en supprimant l'historique des connexions ainsi que les autres preuves.
· Les pirates convoitent les accès à hauts pouvoirs : Dans presque chaque cyberattaque ciblée, des comptes à privilèges ont été piratés. D'après leurs recherches, les analystes de la sécurité déclarent qu'entre 80 et 100% des incidents de sécurité les plus graves avaient pour « signature » une exploitation malveillante de comptes à hauts pouvoirs au cours de leur processus d'attaque.

· Les menaces liées aux comptes à privilèges largement sous-estimées : Les risques et les failles de sécurité que présentent les comptes à privilèges sont bien plus importants que les entreprises ne le réalisent. Les sociétés sous-estiment grandement le nombre de comptes à hauts pouvoirs qu'elles possèdent et ignorent quels systèmes les hébergent. Les recherches de CyberArk ont démontré que les organisations comptent aujourd'hui au minimum trois à quatre fois plus de comptes à privilèges que d'employés.

· Les cyberattaques contre les comptes à privilèges sont de plus en plus sophistiquées : Les analystes de la sécurité ont recensé plusieurs types d'infractions au niveau des comptes à hauts pouvoirs, qui vont de l'attaque répétée des comptes de service à la violation des appareils embarqués de l' « Internet des objets », en passant par la création d'identités multiples dans Microsoft Active Directory afin d'assurer la redondance des points d'accès et des portes dérobées.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.globalsecuritymag.fr/CyberArk-publie-un-rapport-sur-les,20141120,48898.html
par CyberArk