Combattre le vol dâ□□identifiants avec lâ□□automatisation
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 18/11/2022 14:00:00

Plus de 24 Milliards dâ□□identifiants volÃ©s sont disponibles sur Internet et le Darkweb.Leur exploitation par les groupes de cybercriminels reprÃ©sente le premier vecteur dâ□□attaque, loin devant le phishing et lâ□□exploitation de vulnÃ©rabilitÃ©s, dixit JÃ©rÃ´me BEAUFILS, dirigeant de la sociÃ©tÃ© SASETY.

En utilisant ces identifiants, les attaquants prennent le contrÃ´le des comptes utilisateurs et exposent les organisations Ã des violations, Ã des ransomwares et au vol de donnÃ©es.

Bien que les CISOs soient conscients de cette menace et disposent souvent dâ□□outils pour rÃ©duire ce risque, lâ□□actualitÃ© dÃ©montre que leur application sâ□□avÃ¨re largement insuffisante.

Une dÃ©marche structurÃ©e et continue permet de rÃ©duire lâ□□exposition au risque mais elle reprÃ©sente une charge trop importante pour des Ã©quipes sÃ©curitÃ© souvent limitÃ©es. Lâ□□automatisation de la dÃ©tection et de lâ□□identification des risques rÃ©els pour lâ□□organisation constitue la seule rÃ©ponse adaptÃ©e Ã la dynamique des cybermenaces.

Nature du risque

80% des violations d'applications Web impliquent des identitÃ©s compromises. Les attaquants utilisent des techniques comme l'ingÃ©nierie sociale, la force brute et l'achat d'identifiants sur le Darkweb pour compromettre les identitÃ©s et obtenir un accÃ¨s aux ressources des organisations.

Ils tirent souvent parti des faiblesses suivantes :

â□¢ Mot de passe unique entre plusieurs applications
â□¢ Mot de passe commun entre applications personnelles et professionnelles
â□¢ Mots de passe stockÃ©es dans les navigateurs
â□¢ RÃ©utilisation de mots de passe ou durÃ©e de vie importante
â□¢ Identifiants non utilisÃ©s (collaborateurs ayant quittÃ© lâ□□entreprise, prestataires, comptes de service, etc.)
â□¢ Mots de passe partagÃ©s entre diffÃ©rents utilisateurs

Le principal dÃ©fi pour l'organisation est que les attaquants n'ont besoin que d'un seul identifiant valide pour s'introduire.

Mitigation du risque

Pour rÃ©duire leur exposition au risque, les organisations doivent se concentrer sur ce qui est exploitable du point de vue des attaquants.

Une mÃ©thodologie efficace repose sur les Ã©tapes suivantes :

1. Collecter les identifiants dÃ©robÃ©s

Pour commencer Ã rÃ©soudre le problÃ¨me, les Ã©quipes sÃ©curitÃ© doivent collecter des

donnÃ©es sur les identifiants qui ont Ã©tÃ© dÃ©robÃ©s Ã divers endroits du Web et sur le Darkweb. Des outils comme HaveIBeenPwned ou celui de lâ□□Institut Hass-Platner sont utiles. Cette Ã©tape permet dâ□□obtenir un premier Ã©tat de la situation et dâ□□identifier les comptes individuels qui doivent Ãªtre mis Ã jour.

2. Identifier le risque dâ□□exposition rÃ©el

Une fois les donnÃ©es collectÃ©es, les Ã©quipes sÃ©curitÃ© doivent dÃ©terminer quels identifiants peuvent Ãªtre rÃ©ellement exploitÃ©s.

Pour ce faire, elles doivent utiliser des techniques similaires Ã celles des attaquants :

â□¢ VÃ©rifier si les identifiants permettent l'accÃ¨s aux ressources externes, tels que les services Web et les bases de donnÃ©es
â□¢ Tenter de dÃ©chiffrer les hachages de mots de passe capturÃ©s
â□¢ Valider les correspondances entre les identifiants dÃ©robÃ©s et les outils de gestion des identitÃ©s de l'organisation, tels que lâ□□Active Directory
â□¢ Tester des variantes pour identifier de nouvelles identitÃ©s qui pourraient Ãªtre compromises : les utilisateurs utilisant gÃ©nÃ©ralement les mÃªmes modÃ¨les de mot de passe

3. RÃ©duire le risque dâ□□exposition

AprÃ¨s avoir validÃ© les identifiants dÃ©robÃ©s qui exposent rÃ©ellement lâ□□organisation, les Ã©quipes sÃ©curitÃ© doivent prendre des mesures ciblÃ©es pour attÃ©nuer le risque.

Par exemple :

â□¢ Supprimer les comptes inactifs divulguÃ©s de lâ□□Active Directory
â□¢ Initier des changements de mot de passe pour les utilisateurs actifs
â□¢ Revoir les processus et la politique de gestion des mots de passe (durcissement, cycle de vie)

4. Mettre en place une dÃ©marche de validation continue

Les techniques des attaquants tout comme la surface d'attaque des organisations Ã©voluent en permanence, en particulier en termes de comptes utilisateurs. Par consÃ©quent, un effort ponctuel pour identifier, vÃ©rifier et rÃ©duire le risque dâ□□exposition des identifiants est insuffisant.

Pour combattre durablement ce risque, les organisations doivent adopter une dÃ©marche de traitement continu. Cependant, la charge que reprÃ©sente ces actions manuelles est trop importante pour des Ã©quipes de sÃ©curitÃ© aux ressources limitÃ©es.

La seule faÃ§on de gÃ©rer efficacement la menace est d'automatiser le processus de validation.

Automatisation

Depuis 2021, le cabinet Gartner a introduit cette automatisation au travers des concepts Â« Automated Penetration Test and Red Team Tool Â» et Â« External Attack Surface Management Â». Ces concepts rassemblent des techniques visant Ã identifier de faÃ§on continue les risques exposant la surface dâ□□attaque des organisations afin de concentrer le travail de remÃ©diation sur les risques avÃ©rÃ©s.

Parmi les acteurs, la sociÃ©tÃ© Pentera constitue aujourdâ□□hui le leader de la cybervalidation automatisÃ©e.

Utilisant les derniÃ¨res techniques dâ□□attaques les plus avancÃ©es, leur solution permet de

rÃ©aliser de faÃ§on automatique et continue des attaques Ã©thiques afin de mettre en Ã©vidence les vulnÃ©rabilitÃ©s statiques et dynamiques. Ces tests sont exÃ©cutÃ©s aussi bien depuis lâ□□extÃ©rieur que depuis lâ□□intÃ©rieur de lâ□□organisation, permettant de couvrir toute la surface dâ□□attaque.

Parmi les fonctionnalitÃ©s, le module Â« Leaked Credentials Â» automatise les Ã©tapes de dÃ©couverte des identifiants dÃ©robÃ©s et la vÃ©rification de lâ□□exposition quâ□□ils reprÃ©sentent pour lâ□□organisation :

â□¢ Sur les services externes (SaaS, sites Web, messagerie)
â□¢ Sur les services internes (applications, postes de travail, serveurs, Ã©lÃ©ments dâ□□infrastructure).

Le rÃ©sultat de ces investigations prÃ©sente les vecteurs dâ□□attaques complets ainsi que la description des actions de remÃ©diation Ã rÃ©aliser par les Ã©quipes sÃ©curitÃ©. La communication avec des outils de type SIEM ou ITSM permet dâ□□intÃ©grer ce processus dans le processus global de gestion du risque de cybersÃ©curitÃ©. Ces solutions correspondent Ã lâ□□avenir de la surveillance, de la dÃ©tection et de la prÃ©vention des menaces.