Rapport de veille : Janvier 2025

Introduction

Le mois de janvier 2025 a été marqué par une intensification des cybermenaces, touchant divers secteurs tels que la santé, l'éducation, les télécommunications et les infrastructures critiques. Les attaques ont varié en nature, incluant des ransomwares, des violations de données massives et des campagnes d'ingénierie sociale sophistiquées. L'utilisation croissante de l'intelligence artificielle (IA) par les cybercriminels a également été une tendance notable, posant de nouveaux défis en matière de cybersécurité.

1. Les incidents de sécurité majeurs

a. Frederick Health Medical Group (États-Unis)

Le 27 janvier, un ransomware a compromis les données de 934 326 patients, incluant des informations sensibles telles que les numéros de sécurité sociale et les dossiers médicaux. Bien qu'aucun groupe n'ait revendiqué l'attaque, il est suspecté que l'organisation ait payé une rançon pour éviter la publication des données volées. (TechRadar)

b. TalkTalk (Royaume-Uni)

Le 26 janvier, un pirate utilisant le pseudonyme "b0nd" a revendiqué le vol des données personnelles de plus de 18,8 millions de clients actuels et anciens de TalkTalk, incluant des noms, adresses e-mail et numéros de téléphone. TalkTalk a contesté ces chiffres, affirmant que le nombre réel de clients est d'environ 2,4 millions. (SOCRadar® Cyber Intelligence Inc.)

c. PowerSchool (États-Unis)

Le 7 janvier, PowerSchool a confirmé une violation de données affectant potentiellement 62,4 millions d'élèves et 9,5 millions d'enseignants. L'attaque a exploité des identifiants volés pour accéder aux bases de données, exposant des informations personnelles et académiques sensibles. (SOCRadar® Cyber Intelligence Inc.)

d. Phemex (Plateforme de cryptomonnaie)

Phemex a subi une attaque entraînant la perte de plus de 69 millions de dollars en actifs numériques, incluant des Ethereum, Bitcoin et Binance Coin.

L'incident a conduit à une suspension temporaire des opérations de la plateforme. (SOCRadar® Cyber Intelligence Inc.)

e. Marks & Spencer et Co-op (Royaume-Uni)

Des cybercriminels ont utilisé des techniques d'ingénierie sociale pour tromper les services informatiques et réinitialiser les mots de passe des employés, permettant un accès non autorisé aux réseaux internes. Le groupe "Scattered Spider" est suspecté d'être à l'origine de l'attaque. (Latest news & breaking headlines)

2. Les Vulnérabilités critiques (CVE)

a. CVE-2025-0282 – Ivanti VPN

Une vulnérabilité zero-day dans les VPN Ivanti a été exploitée pour compromettre les réseaux de Nominet, le registre officiel des domaines .UK. Cette faille a permis un accès non autorisé aux systèmes internes. (Formation Cybersécurité UK)

b. CVE-2025-21298 – Exécution de code à distance via Windows OLE

Cette vulnérabilité permet à un attaquant d'exécuter du code arbitraire sur le système cible en incitant l'utilisateur à ouvrir un fichier RTF malveillant ou à prévisualiser un e-mail spécialement conçu dans Microsoft Outlook. L'exploitation réussie peut conduire à une compromission complète du système.

3. Les outils et techniques d'attaque

a. Ingénierie sociale avancée

Les attaquants ont utilisé des techniques sophistiquées, telles que le hameçonnage par QR code via WhatsApp, pour compromettre les comptes de responsables gouvernementaux. Le groupe APT russe "Star Blizzard" est suspecté d'être derrière ces attaques. (DigitalXRAID)

b. Exploitation de l'IA par les cybercriminels

L'utilisation de modèles d'IA générative par les attaquants a introduit de nouvelles menaces, telles que les injections de commandes et l'exfiltration de données. Les

experts recommandent l'adoption de contre-mesures basées sur l'IA pour détecter et prévenir ces attaques. (Business Insider)

4. Les Tendances observées

- **Ciblage du secteur de la santé** : Les établissements de santé continuent d'être des cibles privilégiées pour les ransomwares, en raison de la nature sensible des données qu'ils détiennent.
- **Montée en puissance des attaques par ingénierie sociale** : Les cybercriminels perfectionnent leurs techniques pour manipuler les individus et obtenir un accès non autorisé aux systèmes.
- **Utilisation croissante de l'IA par les attaquants** : Les modèles d'IA sont de plus en plus exploités pour automatiser et sophistiquer les attaques, rendant leur détection plus complexe.