Rapport de veille : Février 2025

1. Incidents de sécurité majeurs

a. Marks & Spencer (Royaume-Uni)

Le détaillant britannique a subi une attaque majeure orchestrée par le groupe Scattered Spider. Les attaquants ont utilisé des techniques d'ingénierie sociale pour tromper le support informatique et obtenir des réinitialisations de mots de passe, accédant ainsi aux réseaux internes. Ils ont déployé le ransomware "DragonForce", entraînant des perturbations dans les opérations en ligne et en magasin. (Latest news & breaking headlines)

b. Orange Romania

Le groupe Orange a été victime d'une cyberattaque menée par le hacker "Rey", affilié au groupe HellCat. Plus de 600 000 enregistrements, incluant des adresses e-mail, des données clients et des détails partiels de cartes de paiement, ont été exfiltrés. L'attaque a exploité des vulnérabilités dans les systèmes internes, notamment Jira. (PKWARE®)

c. Zacks Investment Research (États-Unis)

Un cybercriminel utilisant le pseudonyme "Jurak" a divulgué des informations sensibles concernant environ 12 millions d'utilisateurs, incluant des noms, adresses e-mail et numéros de téléphone. Il a également revendiqué l'accès au code source de plusieurs sites internes de Zacks. (SOCRadar® Cyber Intelligence Inc.)

d. Hewlett Packard Enterprise (HPE)

HPE a signalé une violation de données impliquant l'accès non autorisé à des informations sensibles, telles que des noms, numéros de sécurité sociale et permis de conduire. L'entreprise collabore avec des experts en cybersécurité pour enquêter sur l'incident. (BreachFin)

2. Vulnérabilités critiques (CVE)

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

- **Score CVSS** : 9.8 (Critique)
- **Composant affecté** : Technologie OLE de Windows
- **Description** : Permet l'exécution de code arbitraire via des fichiers RTF malveillants ou des e-mails piégés.
- **Correctif** : Mise à jour de sécurité publiée par Microsoft.(Wikipedia)

b. CVE-2025-XXXX – Vulnérabilité dans Jira

- **Score CVSS** : Élevé
- **Composant affecté** : Jira
- **Description** : Exploitation de vulnérabilités dans Jira ayant permis l'accès non autorisé aux systèmes internes d'Orange Romania.
- **Correctif** : Mises à jour de sécurité recommandées pour Jira.(PKWARE®)

3. Outils et techniques utilisés par les attaquants

- **Ingénierie sociale avancée** : Utilisation de techniques telles que le "SIM swapping" et l'usurpation d'identité pour tromper les services informatiques et obtenir des accès privilégiés. (Latest news & breaking headlines)
- **Exploitation des LLMs (Large Language Models)** : Des vulnérabilités ont été identifiées dans des modèles d'IA tels que DeepSeek-R1 et Gemini AI, exposant des risques de "prompt injection" et de manipulation de la mémoire à long terme. (Wikipedia)
- **Ransomwares émergents** : Le ransomware "Sarcoma" a ciblé Unimicron, un fabricant de circuits imprimés, en exfiltrant 377 Go de données et en menaçant de les divulguer. (blog.synergyit.ca)

4. Tendances observées

- **Augmentation des attaques par ransomware** : Des entités telles que Lee Enterprises et le Sault Tribe ont subi des attaques perturbant leurs opérations, soulignant la menace persistante des ransomwares. (blog.synergyit.ca)
- **Exploitation des vulnérabilités des API** : Une entreprise technologique a révélé qu'une vulnérabilité dans son API avait permis l'accès non autorisé aux données de plus de 5 millions de comptes utilisateurs. (BreachFin)
- **Menaces liées à l'IA** : L'utilisation de l'IA par les cybercriminels pour automatiser et amplifier les attaques a été une préoccupation majeure, nécessitant des défenses basées sur l'IA pour contrer ces menaces. (Business Insider)