Rapport de veille : Mars 2025

1. Incidents de sécurité majeurs

a. Ministère de la Santé de Palaos

Le 1er mars, le ministère de la Santé de Palaos a été victime d'une attaque par le ransomware Qilin, perturbant les services médicaux et compromettant des données sensibles. (Formation Cybersécurité UK)

b. Oracle Cloud

Des cybercriminels ont revendiqué l'accès à plus de 6 millions de dossiers clients d'Oracle Cloud, mettant en lumière des failles potentielles dans les systèmes de sécurité du fournisseur de services cloud. (cshub.com)

c. Agence spatiale polonaise (POLSA)

Le 2 mars, l'agence spatiale polonaise a détecté un accès non autorisé à son infrastructure informatique. Les autorités soupçonnent une implication d'acteurs étatiques, notamment en raison des tensions géopolitiques régionales. (Reuters)

d. GitHub Actions

Une attaque sophistiquée a ciblé GitHub Actions, exploitant des failles dans les pipelines CI/CD pour injecter du code malveillant dans des projets open source, compromettant ainsi la chaîne d'approvisionnement logicielle. (SOCRadar® Cyber Intelligence Inc.)

2. Vulnérabilités critiques (CVE)

a. CVE-2025-22224 – VMware ESXi

- **Score CVSS** : 9.8 (Critique)
- **Description** : Vulnérabilité de type "out-of-bounds write" affectant VMware ESXi, permettant une exécution de code arbitraire.
- **Exploitation** : Activement exploitée dans la nature.
- **Correctif** : Patchs disponibles via VMware. (Tenable®, Formation Cybersécurité UK)

b. CVE-2025-24984 – Microsoft Windows

- **Score CVSS** : Élevé
- **Description** : Nécessite un accès physique pour être exploitée, permettant une fuite d'informations sensibles.

- **Correctif** : Incluse dans le Patch Tuesday de mars 2025. (strobes.co, Zero Day Initiative, Tenable®)

c. CVE-2025-26630 – Microsoft Windows

- **Score CVSS** : Critique
- **Description** : Vulnérabilité zero-day activement exploitée, permettant une élévation de privilèges.
- **Correctif** : Corrigée dans le Patch Tuesday de mars 2025. (Arctic Wolf, crowdstrike.com)

3. Outils et techniques utilisés par les attaquants

- **Arcane** : Un nouveau malware voleur d'informations, capable de dérober des identifiants VPN, des données de clients de messagerie et des informations stockées dans les navigateurs web. (Formation Cybersécurité UK)
- **Atlantis AIO** : Plateforme automatisée de credential stuffing ciblant plus de 140 services en ligne, facilitant les attaques par force brute à grande échelle. (Formation Cybersécurité UK)
- **Exploitation des LLMs** : Les cybercriminels utilisent des modèles de langage avancés pour mener des attaques sophistiquées, telles que l'injection de commandes et l'exfiltration de données. (Business Insider)

4. Tendances observées

- **Augmentation des attaques ciblant les infrastructures critiques** : Les secteurs de la santé, de l'énergie et des télécommunications ont été particulièrement visés, soulignant la nécessité de renforcer la résilience de ces infrastructures.
- **Exploitation des chaînes d'approvisionnement logicielles** : Les attaques sur GitHub Actions démontrent la vulnérabilité des pipelines CI/CD et l'importance de sécuriser l'ensemble du cycle de développement logiciel. (SOCRadar® Cyber Intelligence Inc.)
- **Adoption croissante des solutions sans mot de passe** : À l'occasion de la Journée mondiale du mot de passe 2025, l'industrie a mis en avant les alternatives telles que les passkeys et l'authentification biométrique pour améliorer la sécurité des identifiants. (TechRadar)