Attribution des cyber-attaques : Analyse forensique et apprentissage non supervisé pour l'identification des familles de ransomware

CONTEXTE

- Les attaques par ransomware représentent une **menace majeure** pour les infrastructures critiques, causant des pertes financières considérables.
- Ces attaques exploitent des techniques avancées pour **chiffrer les données** des victimes et exiger **une rançon**. La détection et l'analyse des ransomwares sont cruciales pour renforcer la cybersécurité. [1]
- Actuellement, **les approches traditionnelles** basées sur les binaires des ransomwares, signatures ou encore leur comportement en exécution, sont **limitées face aux variants et aux attaques « zero-day »**, nécessitant le développement de **méthodes indépendantes de ces données et automatisables.** [2]

ÉTAT DE L'ART

Il existe **différents types d'analyses de ransomwares** :
✓ **Analyse statique, dynamique et hybride** → Permettent d'extraire des caractéristiques exploitables mais ne constituent pas en elles-mêmes des méthodes de classification.

Ces différents types d'analyses permettent d'établir les **méthodes actuelles de classification de ransomwares** :
✓ **Méthodes de classification : comportementale, heuristique et ML supervisé** → Exploitation des caractéristiques extraites. [3]

📌 **Problème** : Les ransomwares modernes **suppriment leurs binaires** après l'attaque et utilisent des techniques d'évasion et d'obfuscation de plus en plus élaborées, rendant ces analyses inefficaces. **Les artefacts Windows constituent alors une source d'information précieuse** pour une classification post-attaque sans accès aux fichiers malveillants.

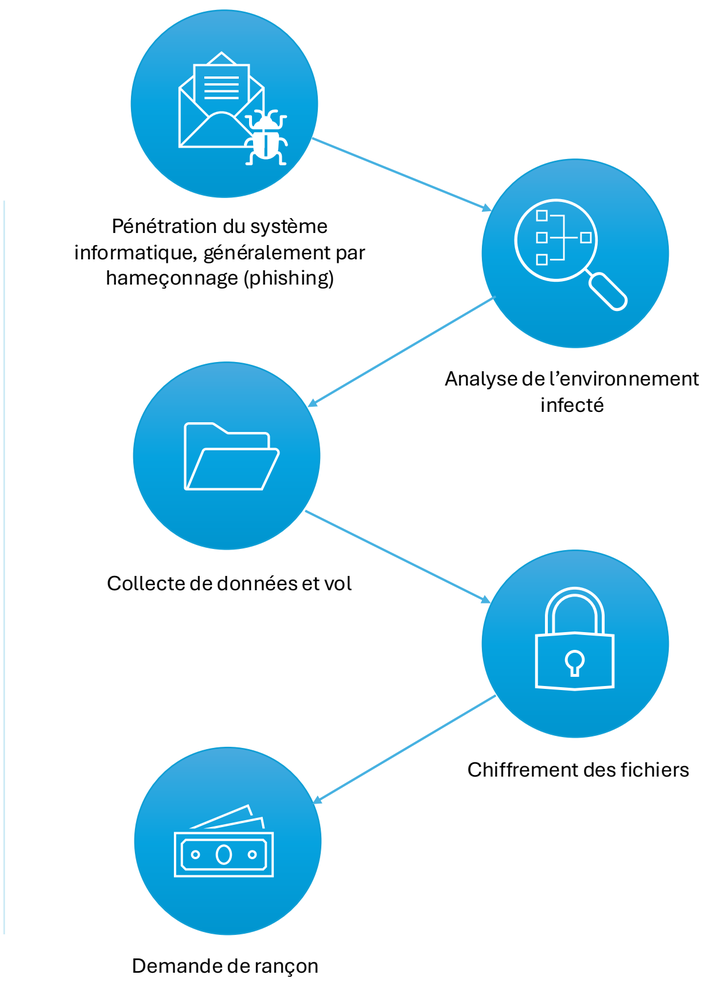

Figure 1 : Représentation des étapes d'une attaque par ransomware

OBJECTIFS

L'objectif de cette recherche est de développer une **approche avancée de classification des ransomwares** en s'appuyant sur des **techniques d'apprentissage non supervisé sur des artefacts Windows**. [4]

Les contributions attendues sont :

- Une **collecte de données** issue d'environnements variés.
- L'élaboration d'un **modèle d'apprentissage non supervisé** pour automatiser la classification. **[5]**
- Développer des approches pour **identifier les auteurs et l'origine des attaques par ransomwares**.

Ces travaux permettront d'apporter une **meilleure compréhension des ransomwares** et d'**améliorer l'analyse forensique des attaques par les forces de l'ordre**.

Références :

[1] Comparitech, "Ransomware roundup 2024 : End-of-year report," 2024.

[2] S. Razaulla, C. Fachkha, C. Markarian, A. Gawanmeh, W. Mansoor, B. C. M. Fung, and C. Assi, "The age of ransomware : A survey on the evolution, taxonomy, and research directions," IEEE Access, vol. 11, pp. 40698–40723, 2023.

[3] A.-R. Belea, "Methods for Detecting Malware Using Static, Dynamic and Hybrid Analysis," International Conference on Cybersecurity and Cybercrime, vol. 10, pp. 258–265, May 2023.

[4] S. Zhang, C. Hu, L. Wang, M. J. Mihaljevic, S. Xu, and T. Lan, "A Malware Detection Approach Based on Deep Learning and Memory Forensics," Symmetry, vol. 15, p. 758, Mar. 2023. Number : 3 Publisher : Multidisciplinary Digital Publishing Institute.

[5] J. Ispahany, M. R. Islam, M. Khan, and M. Islam, "Ransomware Detection Using Machine Learning : A Review, Research Limitations and Future Directions," IEEE Access, vol. PP, pp. 1–1, Jan. 2024.

Étudiante : Anais Moussouni
Superviseurs : Nga NGUYEN, Frédéric FAUBERTEAU

Laboratoire : DVRC et IFT