Analyse et reverse engineering d'outils de hacking du dark web

- Réalisé par :
- Ilias Belharda, Chihab Medagheri Alaoui, Salma Faris, Aya Fdail

- Supervisé par : Othmane Cherqi

- Année académique : 2024 / 2025

Introduction

- **Contexte :**
- Le dark web est un espace caché d'internet où des outils de cybercriminalité sont échangés.
- **Problématique :**
- Quels sont les outils disponibles et leurs impacts sur la cybersécurité ?
- **Objectifs :**
- - Identifier des forums.
- - Analyser les outils malveillants.
- - Étudier les comportements en environnement sécurisé.

Méthodologie

Étapes principales :

1. Navigation et identification des forums d'exploit.

2. Analyse des outils via le reverse engineering.

3. Utilisation de sandboxing pour observer les comportements.

Exploration et Préparation

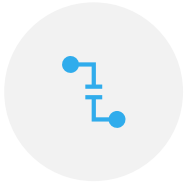
WEB SELFLESS :

- RÉSEAUX ANONYMES ACCESSIBLES VIA TOR.

- FOCUS SUR LES FORUMS ACTIFS.

PRÉPARATION :

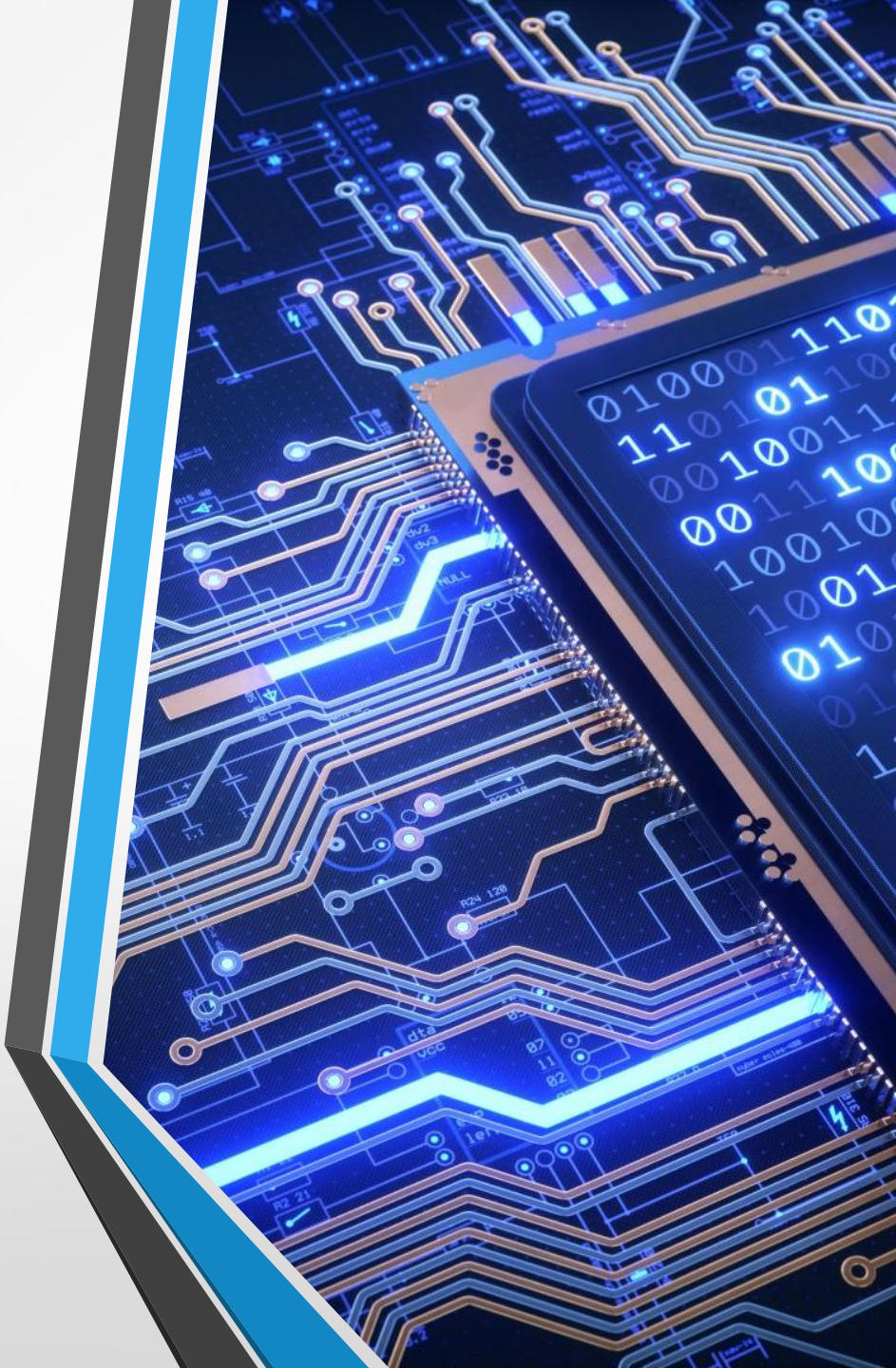
- DÉSACTIVATION DES FONCTIONNALITÉS À RISQUE.



- UTILISATION D'UN FIREWALL ET D'ANTIVIRUS (CLAMAV).

Magic Bytes et Analyse

- Magic Bytes : Signatures permettant d'identifier le type de fichier.
- Méthodes :
- - Commande 'file' : Identifie le type de fichier.
- - Commande 'strings' : Extrait les chaînes de caractères.
- - 'binwalk' : Analyse les structures cachées dans les fichiers.



Reverse Engineering et Sandboxing

- Reverse Engineering : Comprendre le fonctionnement des fichiers suspects.
- Sandboxing : Tester les fichiers dans un environnement isolé.
- Outils : HybridAnalysis, VirusTotal.

Implications et Défis

- Risques :
- - Propagation de logiciels malveillants.
- - Vol de données sensibles.
- - Escroqueries.

- Défis :
- - Accès limité aux forums fiables.
- - Analyse d'un échantillon réduit.

Conclusion et Perspectives

Résumé :

Cette étude a permis de renforcer notre maîtrise des techniques d'analyse de fichiers malveillants tout en explorant les outils disponibles sur le dark web. Les résultats ouvrent la voie à des recherches plus approfondies et à des solutions de cybersécurité innovantes.

Perspectives :

- Automatisation des analyses.

- Collaboration en cybersécurité.