Analyse forensic de malware et impact contre la cybercriminalité

TABLE DES MATIÈRES

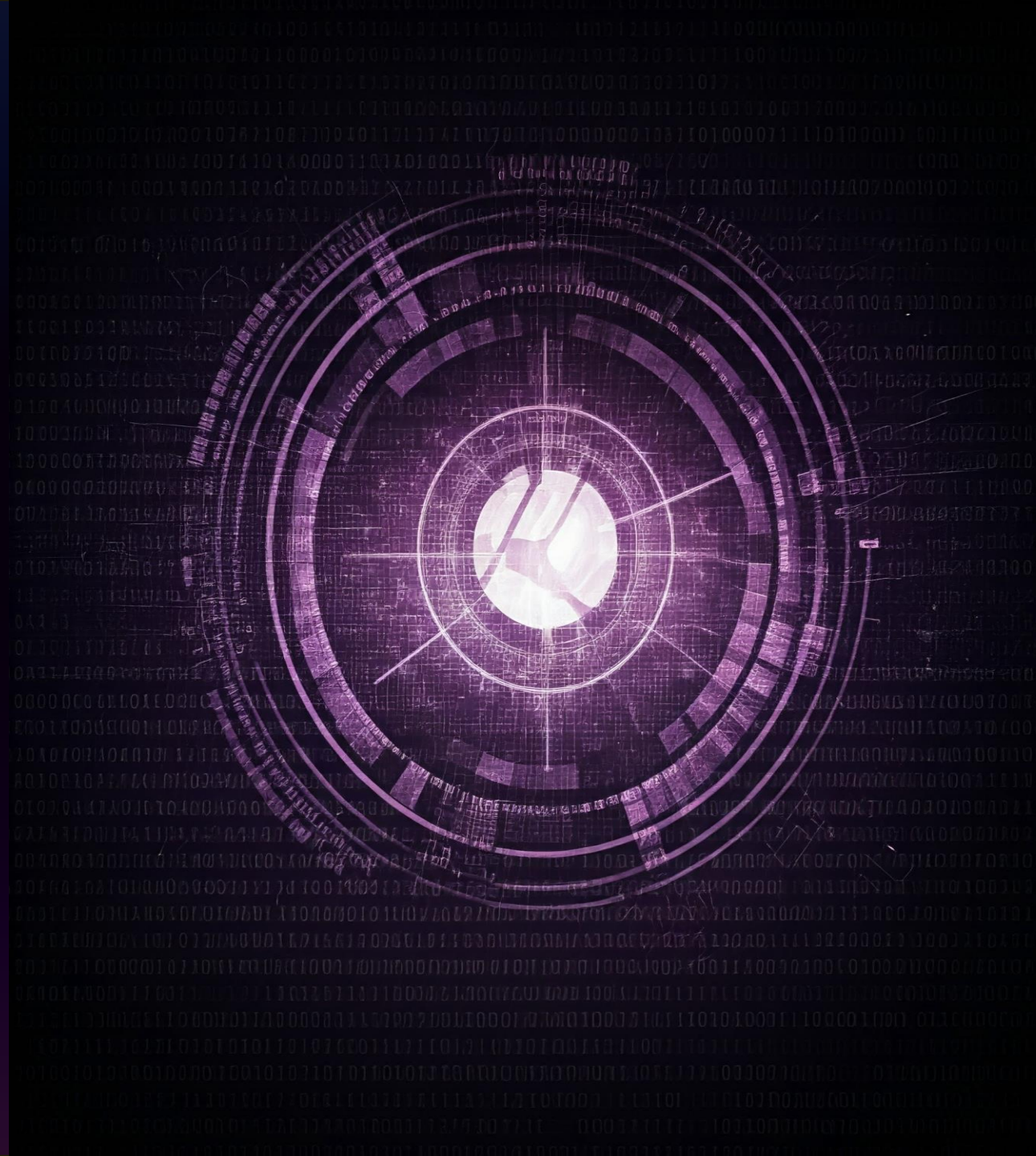
1) INTRODUCTION

FORENSIC

- DOMAINE SCIENTIFIQUE

- RÉCUPÉRATION ET ANALYSE DE SUPPORTS SUSPICIEUX

- DIFFÉRENTS TYPES D'ANALYSES



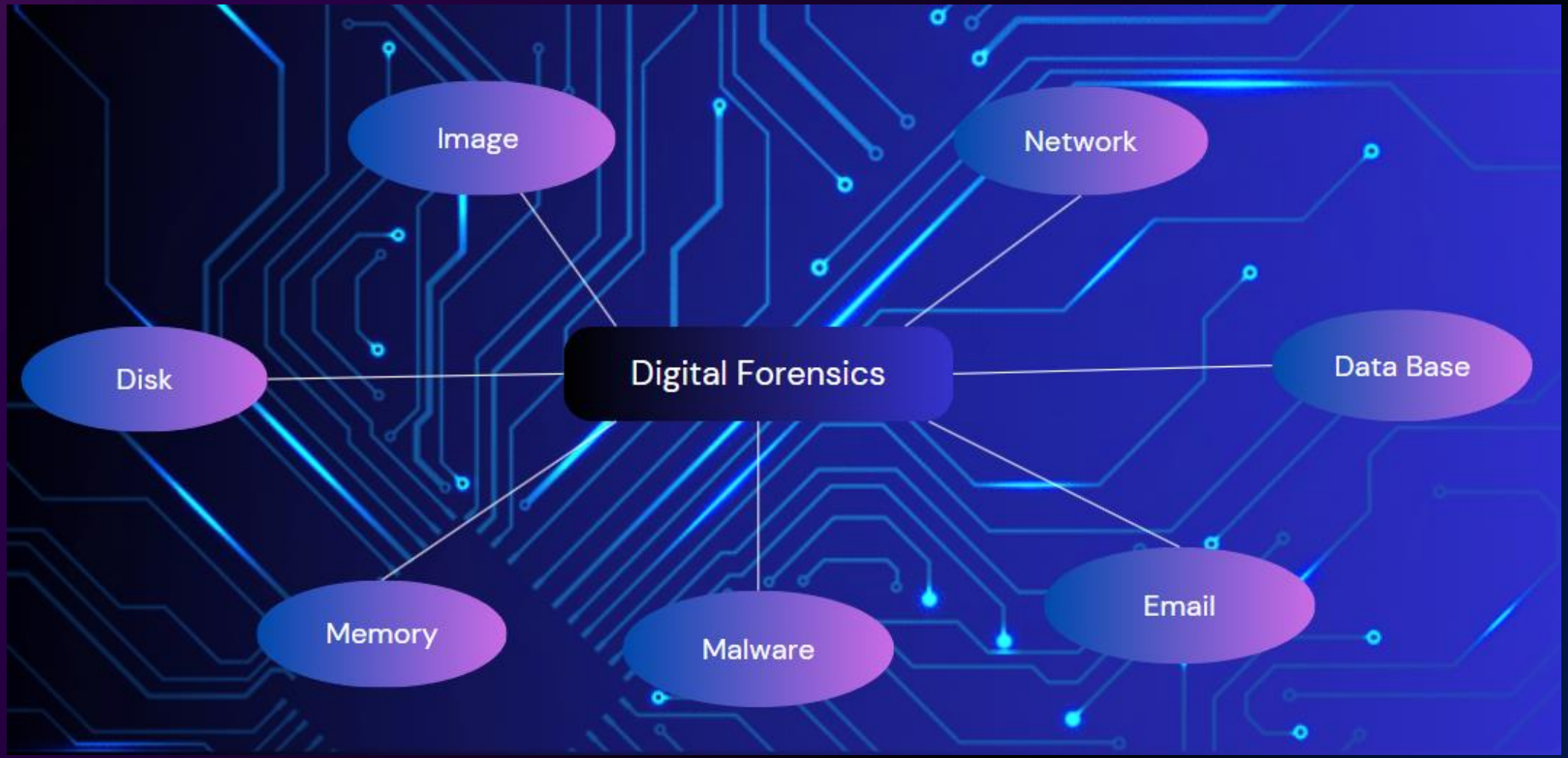


Image
Network
Disk
Digital Forensics
Data Base
Memory
Malware
Email

MALWARE

- PROGRAMME/CODE À BUT MALVEILLANT
- UTILISATION DE MOYENS DIVERS POUR INFECTER UN SYSTÈME
- BUTS DIFFÉRENTS EN FONCTION DE L'ATTAQUANT

TYPES DE MALWARE

- VIRUS 
- VER 
- RANSOMWARE 
- SPYWARE 

REVERSE INGENEERING

- DÉSASSEMBLAGE/ANALYSE
- COMPÉTENCES TECHNIQUES NÉCÉSSAIRES
- PLUSIEURS APPLICATIONS POSSIBLES
- QUESTIONS LÉGALES ET ÉTHIQUES

2) Forensic de Malware

POINTS IMPORTANTS

1. IDENTIFICATION ET CLASSIFICATION DU MALWARE
2. ANALYSE STATIQUE
3. ANALYSE DYNAMIQUE
4. EXTRACTION DES INDICATEURS DE COMPROMISSION (IOC)
5. TRAÇAGE DE L'ORIGINE, DE LA PROPAGATION ET ATTRIBUTION

3) OUTILS

IDA PRO/GHIDRA

- OUTILS DE REVERSE INGINEERING
- PROPRIÉTAIRE/OPEN-SOURCE
- SUPPORT PROFESSIONNEL/COMMUNAUTÉ
- DÉCOMPILATEUR PLUS PRÉCIS CHEZ IDA PRO

THE ZOO

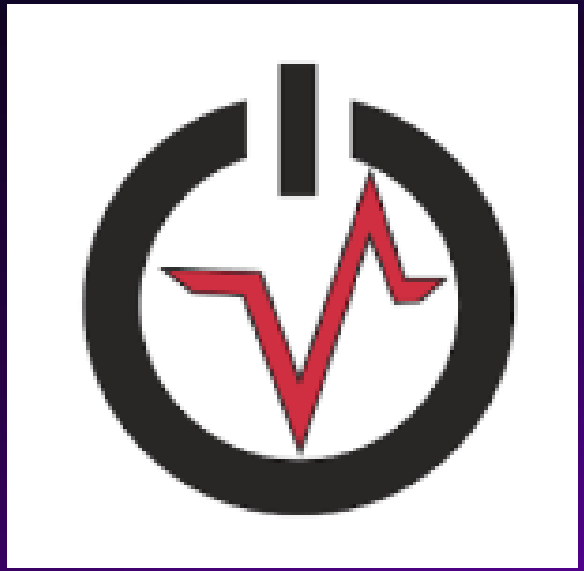
- RÉFÉRENCIEL OPEN-SOURCE DE MALWARE

- ÉCHANTILLONS DE MALWARE POUR L'ANALYSE, LA RECHERCHE, L'EDUCATION

- LA COMMUNAUTÉ PEUT SOUMETTRE DE NOUVEAUX ÉCHANTILLONS

VOLATILITY

- OUTIL OPEN-SOURCE ORIENTÉ FORENSIC
- ANALYSE DE LA MEMOIRE VIVE
- EXTRACTION DE DONNÉES
- DÉTECTION DE MALWARE DANS LA MÉMOIRE VIVE



4) Démonstration

Ghidra x Wannacry

ATTENTION: CETTE SÉQUENCE A ÉTÉ RÉALISÉE PAR UN PROFESSIONNEL

NE REPRODUISEZ PAS CELA CHEZ VOUS

WANNACRY

- RANSOMWARE + VER

- PROPAGATION SMB V1

- CVE-2017-0144 (ETHERNALBLUE)

5) Cybercriminalité et impact

DÉFINITION

- ACTIVITÉS CRIMINEL DANS LE CYBERESPACE/AVEC DES TECHNO NUMÉRIQUES

- DIFFÉRENTES FORMES

- UTILISATION DE MALWARES, VULNÉRABILITÉS, LOGICIELS

- UTILISÉ PAR DIVERS PROFILS

IMPACTS RECHERCHÉS

- REMONTER À LA SOURCE
- COMPRENDRE LE COMPORTEMENT DU MALWARE
- ÉLABORATION DE CONTRE-MESURES
- COLLECTE DE PREUVES POUR POURSUITES JUDICIAIRES
- PRÉVENTION

IMPACTS RÉELS

- PARFOIS COMPLIQUÉ EN FONCTION DU PAYS
- COMPRENDRE LE COMPORTEMENT DU MALWARE
- ÉLABORATION DE CONTRE-MESURES
- PREUVES SOUVENT INSUFFISANTES OU ATTAQUANT DANS UNE AUTRE LÉGISLATION
- PRÉVENTION

6) Conclusion


Kahoot!

7) Bibliographie

- Julien B.
- https://github.com/ytisf/theZoo
- https://github.com/NationalSecurityAgency/ghidra?tab=readme-ov-file
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144
- EC-Council C|HFI Module 0 et 1
- CyberOps Cyber_Sec_M0-2024

MERCI POUR VOTRE ÉCOUTE