

Atelier/Jeu n° 2 : « WannaCry Nightmare Puzzle »

Puzzle cryptographique

Se joue à 5 étudiants

Difficulté 3/5



« En 2017, le monde a été frappé par une attaque de ransomware sans précédent appelé WannaCry, qui a infecté des centaines de milliers d'ordinateurs dans plus de 150 pays. Le ransomware était particulièrement dangereux, car il utilisait un **assemblage cryptographique** redoutablement efficace pour chiffrer les fichiers des victimes, rendant ainsi la récupération des données impossible sans la clé de déchiffrement correcte.

Sauras-tu reconstruire cet assemblage ? »



1

Remplir correctement le puzzle vide avec les 21 étiquettes Crypto WannaCry

2

Numéroter chacune des étapes dans le petit cercle gris

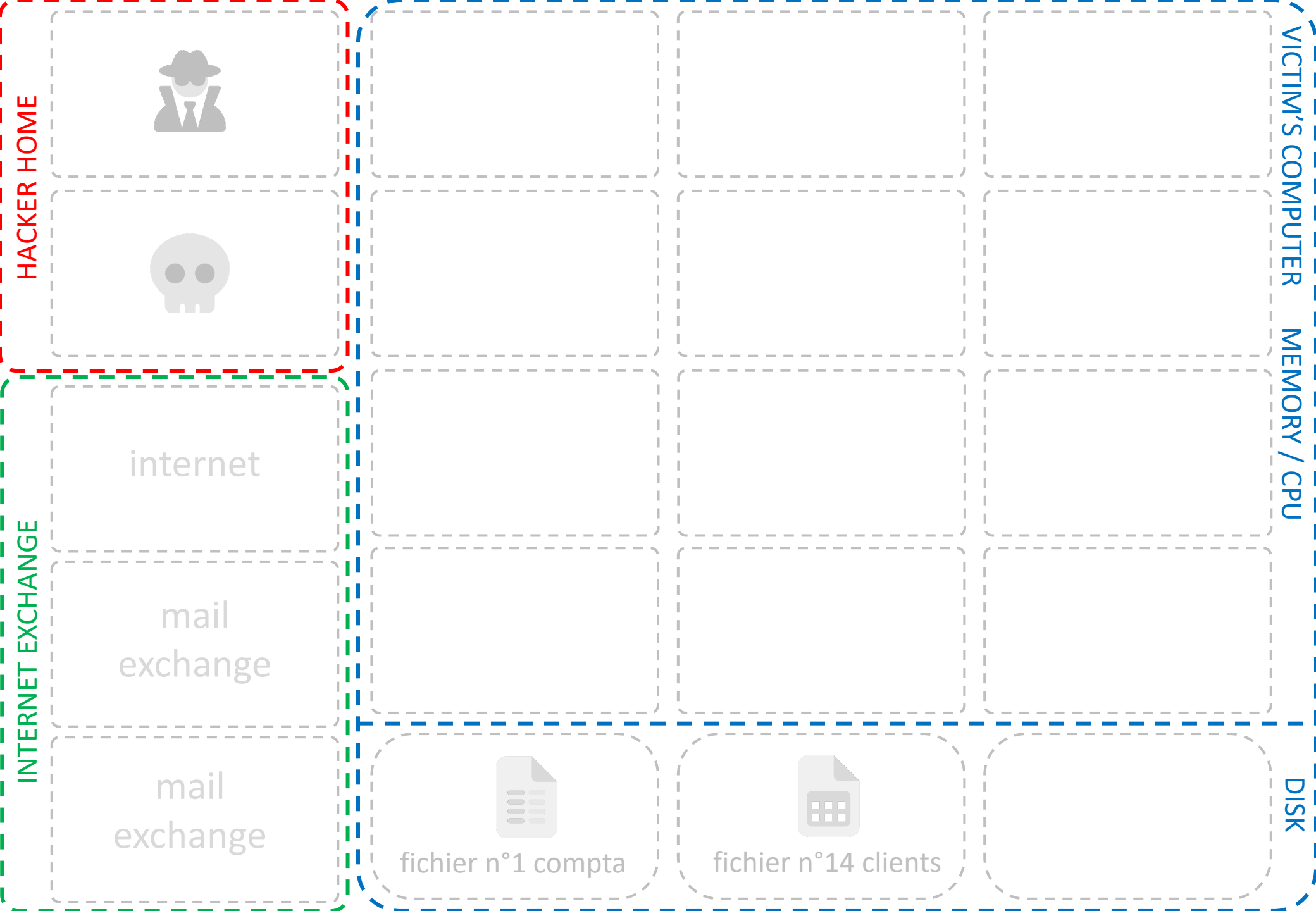
3

L'assemblage cryptographique doit être optimal : rapide, centralisé, facile et sûr




« WannaCry Nightmare Puzzle »
{EGE-2023-Stelau-Cryptographie Moderne}

© Stelau 2023 - Benoit LEGER-DERVILLE – Nicolas CHALANSET – Loïc PERRY – Quentin ROPELE







Cyberattaque : malware sur poste Victime (par phishing)




Païement Rançon




Remplacement fichier n°1
compta chiffré + K_1 chiffré




Déchiffrement du fichier
n°1 de compta avec clé K_1




Génération de K_1 puis
Chiffrement du fichier n°1
de compta avec clé AES K_1




**Suppression mémoire
de KVs**



Chiffrement de K_{14} avec KVp +
Suppression mémoire de K_{14}



**Renvoi de KVs en
clair vers Victime**




Déchiffrement de K_1 avec KVs




Chiffrement de KVs avec KAp



Déchiffrement du fichier
n°14 clients avec clé K_{14}



Génération KAs + KAp




**Stockage de KVs
chiffré sur disque dur**



**Envoi de KVs chiffrée
vers Attaquant**




Chiffrement de KVs avec KVp




Remplacement fichier n°14
clients chiffré + K_{14} chiffré




Déchiffrement de K_{14} avec KVs




Chiffrement de K_1 avec KVp +
Suppression mémoire de K_1



Génération KVs + KVp



Génération de K_{14} puis
Chiffrement du fichier n°1
de compta avec clé AES K_{14}



Déchiffrement de KVs avec KAs