

R5.B.09 – CYBERSÉCURITÉ

PARTIE I

Edward Staddon

Edward.Staddon@univ-ubs.fr

Université Bretagne Sud, IUT de Vannes, Département Informatique



PLAN DU COURS

- Introduction à la cybersécurité
- Les risques de la cyber espace
- Les cyberattaques
- Protection préventive
- Protection active et anticipative
- Architectures de sécurité et architectures sécurisés
- Introduction à l'analyse de risque

PLAN DU COURS

- Introduction à la cybersécurité
 - Les risques de la cyber espace
 - Les cyberattaques
 - Protection préventive
 - Protection active et anticipative
 - Architectures de sécurité et architectures sécurisées
 - Introduction à l'analyse de risque
- 
- PARTIE I



INTRODUCTION À LA CYBERSÉCURITÉ

LE « CYBERESPACE »

Espace de communication créé par l'interconnexion mondiale des ordinateurs (→ Internet) et par les données qui y sont traitées ; espace, milieu dans lequel naviguent les internautes. (→ cybermonde)



The space of virtual reality; the notional environment within which electronic communication (esp. Via the internet) occurs.

LE « CYBERESPACE »

ANSSI → Agence Nationale de la Sécurité des Systèmes d'Information

- Crédit 7 juillet 2009 → responsabilité de la sécurité informatique Française

Q cyber.gouv.fr

Espace constitué par les infrastructures interconnectées relevant des technologies de l'information, notamment l'Internet.

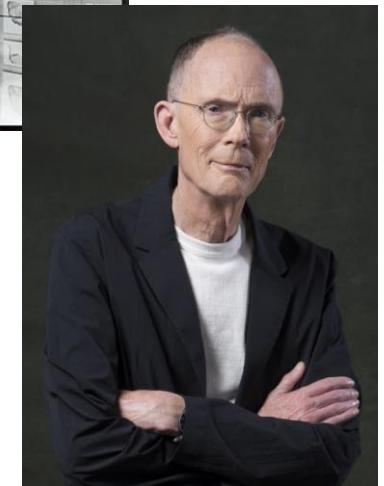


Perçu comme un nouveau territoire, le cyberspace est un espace difficile à définir car il repose sur un ancrage à la fois physique et informationnel.

LE « CYBERESPACE »

Beaucoup d'origines

- Fin 1960 → Artiste Danoise Susanne Ussing
 - Création d'un « Atelier Cyberspace »
 - Espaces sensoriels, la gestion d'espace artistique
- Début 1980 → Auteur American William Gibson
 - Science-fiction cyberpunk
 - Première apparition 1980 → *Gravé sur Chrome* (*Burning Chrome*)
 - Deuxième apparition 1984 → *Neuromancien* (*Neuromancer*)



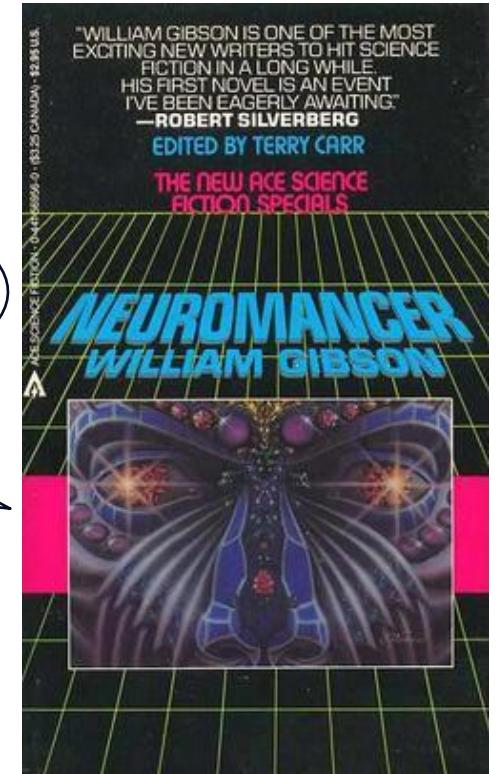
LE « CYBERESPACE »

Le terme a progressivement été associé avec les réseaux informatiques « en-ligne »

“Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding.”

- Terme critiqué par Gibson

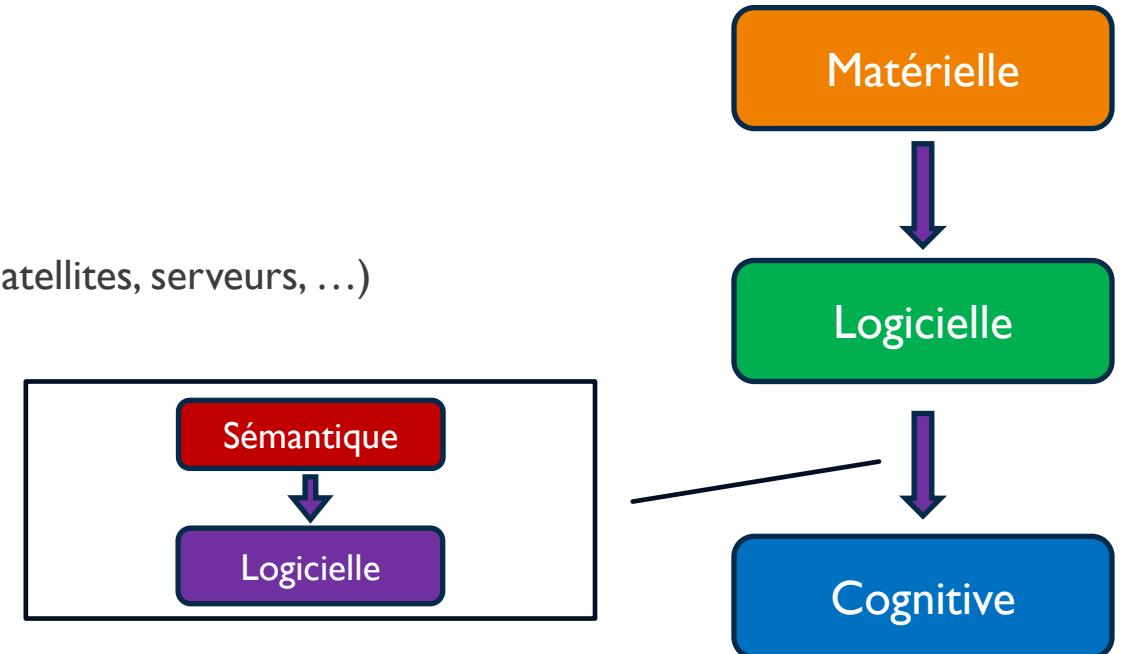
Hum ... un mot évocateur et qui ne veut rien dire ...
« Cyberespace » ? C'est un bon buzzword !



LE « CYBERESPACE » AU XXI^E SIÈCLE

Terme représente le monde numérique de l'informatique

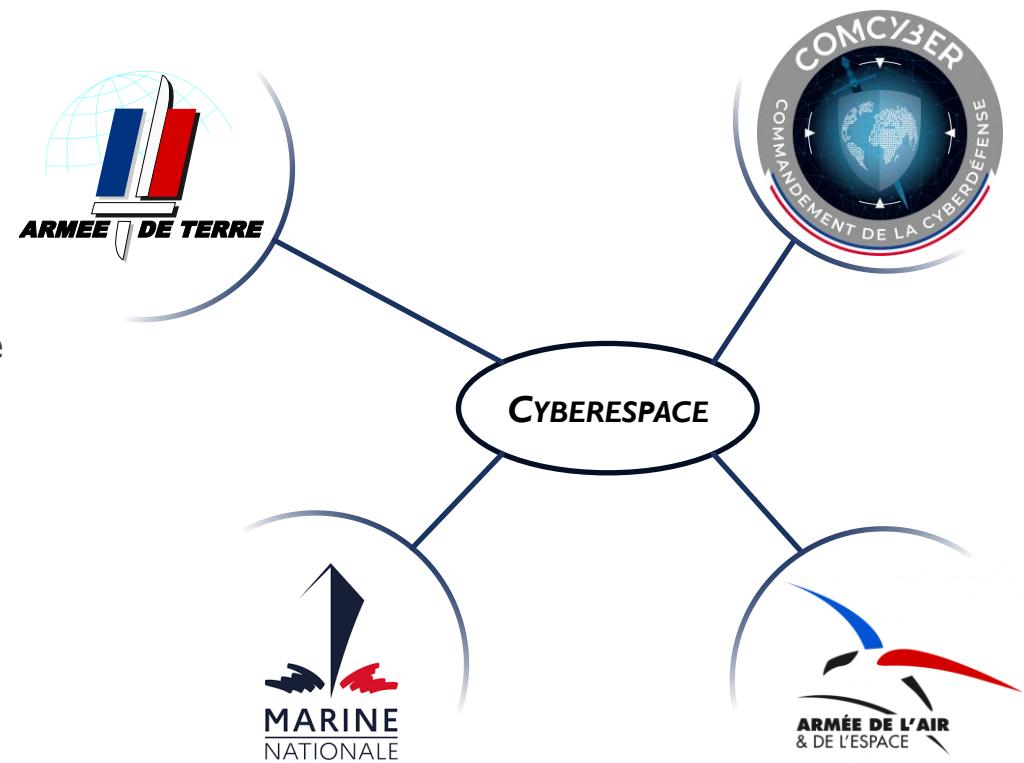
- Couverture mondiale des équipements connectés
- Modèle 3 couches couramment utilisé
 - **Matérielle** → Infrastructure (ordinateurs, câbles, clés USB, satellites, serveurs, ...)
 - **Logicielle** → Fonctionnalité (code, protocoles, ...)
 - **Cognitive** → Données
- Version 5 couches créé en 2010 d'origine Française
 - Ajout de deux couches supplémentaires
 - **Sémantique** → Stockage et administration
 - **Service** → Entreprises publics, commerciaux, opérationnels (banque), médias (YouTube), ...



LA GUERRE DE LA CYBERESPACE



- Reconnu comme la 5^{eme} domaine de guerre
 - Electronique → Cyberdéfense
 - Géré par le COMCYBER → Commandement de la cyberdéfense
- Dimension horizontale supplémentaire
 - Non seulement domaine propre à part
 - Tous les domaines militaires en dépendent de plus en plus



LES DOMAINES DU CYBERESPACE

Cyberespionnage



Cyberdéfense



Cybersécurité



CYBERESPIONNAGE

Ensemble d'actions menées dans le cyberspace consistant à infiltrer, clandestinement ou sous de faux prétextes, les systèmes informatiques d'une organisation ou d'un individu, et à s'emparer de données pour les exploiter.



Le cyberespionnage se pratique notamment par le biais de logiciels malveillants ou espions, de cyberattaques persistantes, ou en mettant à profit les vulnérabilités des systèmes informatiques.



CYBERESPIONNAGE

Obtenir des « secrets » et de l'information sans la permission et la connaissance du propriétaire

- Utilisation de techniques sur Internet, les réseaux ou les ordinateurs individuels
 - Proxy, logiciel malveillant, cheval de Troie, logiciel espion, ...
- Plusieurs méthodes couramment utilisées **capture de positionnement** **mouchard** **keylogger** **compromission de smartphone** **réPLICATION** **capture d'écran** **camera** **scan de données**
- Premier espionnage en 1996 → développement de l'activité de l'Internet



Stuxnet (découvert 2010 / dev 2005 ?)
Responsable dégâts projet nucléaire Iranien ?
Coordination US / Israël ? → « Opération Jeux Olympiques »



Le cyberespionnage constitue l'une des menaces les plus redoutées par l'ANSSI. Les auteurs utilisent souvent des méthodes très pointues, pouvant rester tapis très longtemps dans un système sans jamais se faire repérer. Les conséquences peuvent être désastreuses pour la ou les organisations victimes.

CYBERDÉFENSE

Ensemble des moyens mis en place par un État pour défendre dans le cyberespace les systèmes d'information jugés d'importance vitale, qui contribuent à assurer la cybersécurité.



La cyberdéfense met notamment en œuvre la lutte informatique défensive et la lutte informatique offensive.



CYBERDÉFENSE

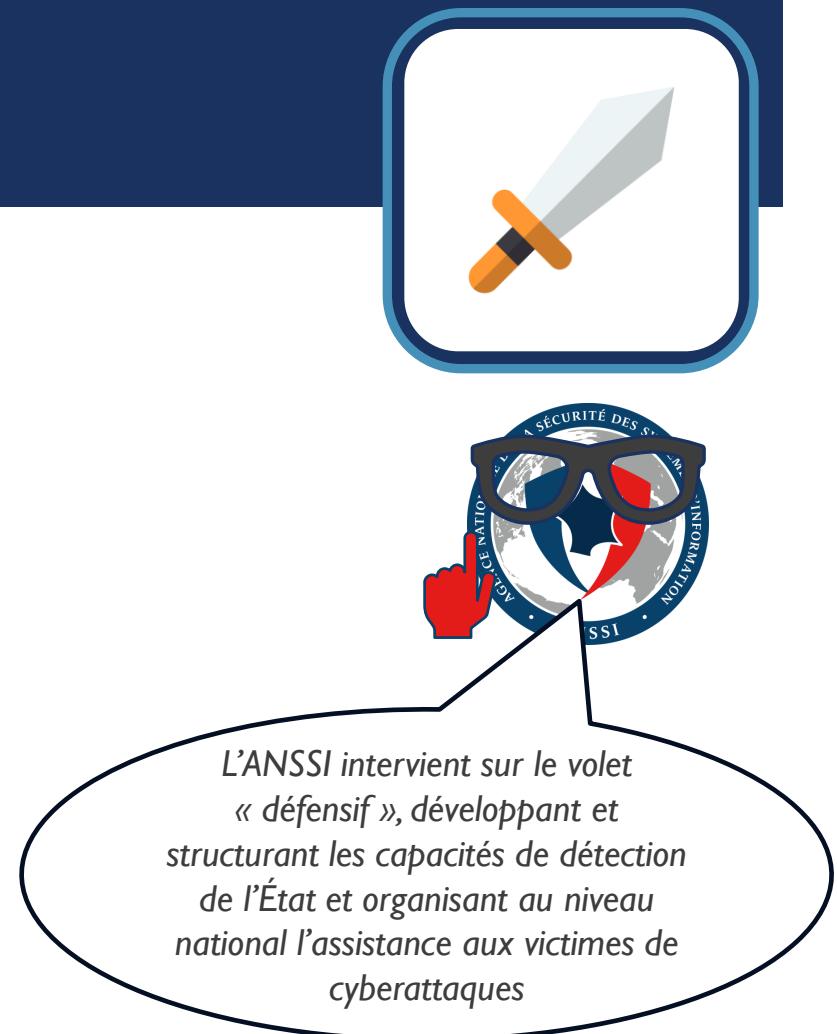
Regroupe tous les moyens mis en place par un pays dans la « guerre informatique » menée dans le cyberespace

- Dépasse la « sécurité informatique »
 - Conséquences directes sur la sécurité nationale
- Deux méthodologies de lute informatique
 - Défensive → LID
 - Offensive → LIO



Prise en charge par l'**ANSSI**, répondant au premier ministre et DGA MI

- Plusieurs écoles militaires / ingénieurs



CYBERSÉCURITÉ



État d'un système d'information qui résiste aux cyberattaques et aux pannes accidentelles survenant dans le cyberspace.



La cybersécurité est assurée par la cyberprotection ainsi que, dans le cas d'un Etat, par la cyberdéfense.

CYBERSÉCURITÉ

Terme néologiste désignant tout ce qui peut être utilisé pour protéger les personnes et les actifs informatiques des États et des organisations

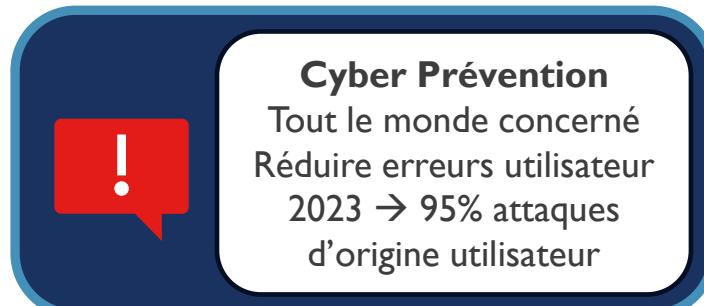
lois outils concepts de sécurité dispositifs de sécurité mécanismes de sécurité formations
politiques de sécurité technologies actions méthodes de gestion des risques bonnes pratiques

Contraste avec la cyberdéfense

- Défense → répondre à une menace
- Sécurité → prévenir et agir

Plusieurs zones liées à la sécurité

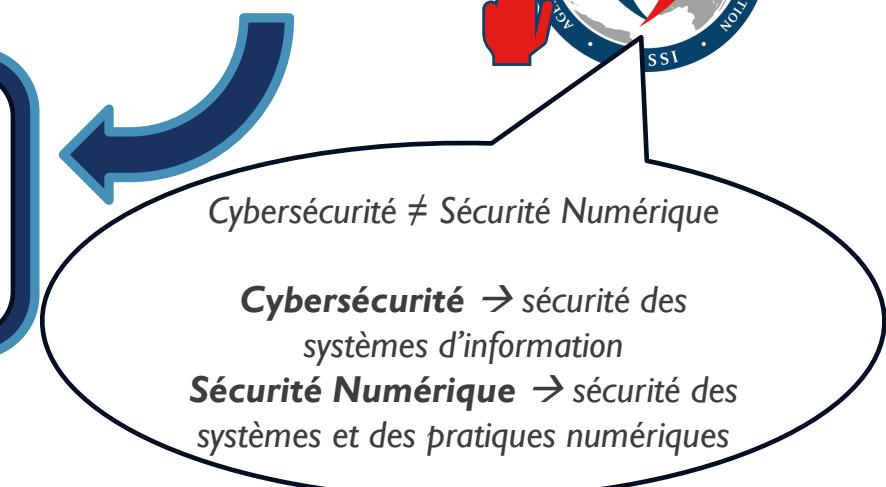
cloud systèmes
réseaux applications



Internet

IoT

.....



TRIAD CIA

- Modèle commun constituant la base du développement des systèmes de sécurité
 - Permet d'identifier les vulnérabilités & méthodes de création de solutions
- Trois idées essentielles au fonctionnement d'une entreprise ➡ Si respecté → mieux équipe pour gérer les incidents



Confidentialité



Intégrité



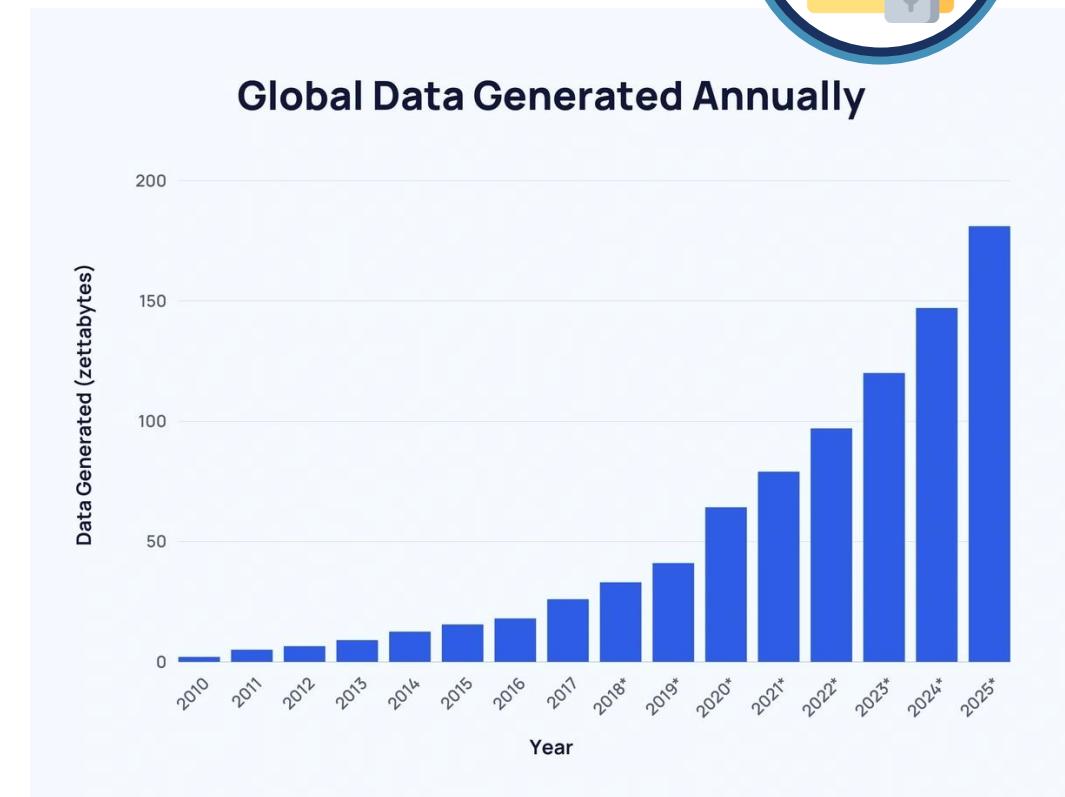
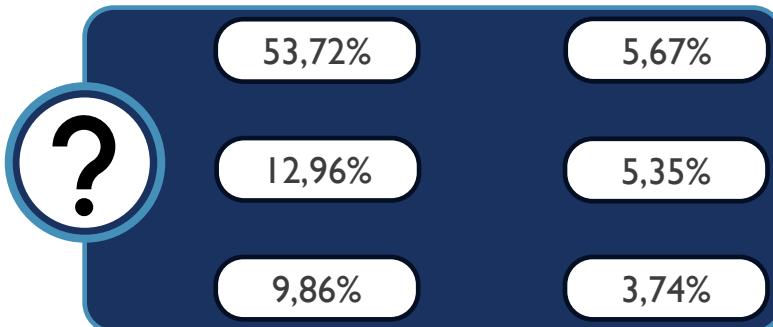
Disponibilité

CONFIDENTIALITÉ



Enorme quantité de données créée et partagé sur Internet

- 147 Zo créée en 2024
- Estimation de 181 Zo en 2025 **i** 1 Zo = 402,74 millions To
- Croissance exponentielle de données créées
 - 90% des données existants créées dans les 2 dernières années
 - + 50% du Traffic d'origine ... ?



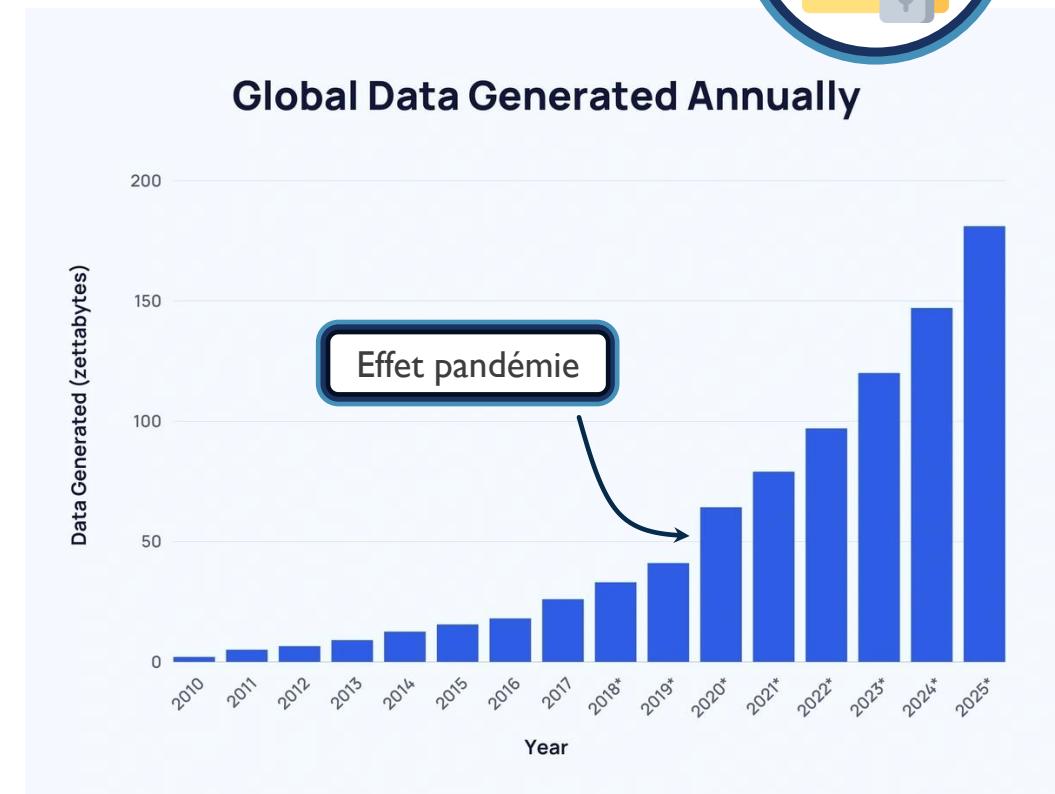
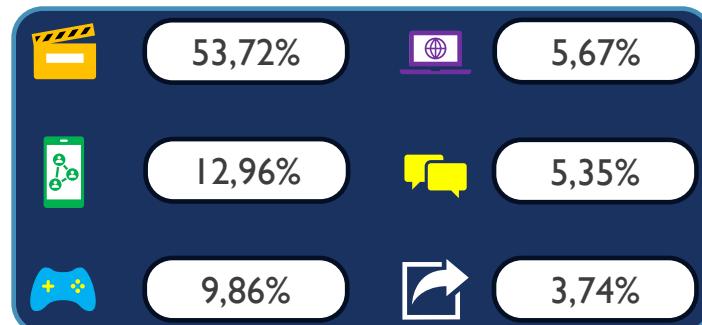
Source: <https://explodingtopics.com/blog/data-generated-per-day>

CONFIDENTIALITÉ



Enorme quantité de données créée et partagé sur Internet

- 147 Zo créée en 2024
- Estimation de 181 Zo en 2025 i 1 Zo = 402,74 millions To
- Croissance exponentielle de données créées
 - 90% des données existants créées dans les 2 dernières années
 - + 50% du Traffic d'origine vidéo



CONFIDENTIALITÉ



→ Assurer que les données sont gardées secrètes ou privées

- Plusieurs méthodes possibles
 - **Gestion d'accès** → authentification (ex: CAS UBS → ENT/PARTAGE)
 - **Protection des données** → chiffrement (ex: RSA, AES, hachage, etc...)
- Empêcher tout accès non autorisé
- Assurer l'accès aux personnes nécessaires
 - Enseignants → accès aux notes des étudiants
 - Étudiants → pas d'accès aux notes



Whatsapp

- Accès aux groupes régulé
→ Control d'accès par ajout des personnes
- Protection des messages
→ Chiffrement de bout-en-bout

INTÉGRITÉ



- Informations fiables et valides
 - Information sur le site de l'IUT **DOIT** être à jour et correct
 - Question de confiance en la source / l'entreprise

- Plus d'entreprises tournent vers le dématérialisé
 - Plus de papier (youpi...)
 - Gestion décentralisée et désynchronisé
 - Plus de signatures papier
 - Comment vérifier l'origine ?

Informations pour l'année en cours

Date de mise à jour valide

– Rentrée universitaire 2024-2025

⇒ **découvrez toutes les dates de rentrée (MAJ du 20 août)**

⇒ **découvrez le Guide pratique de l'étudiant***

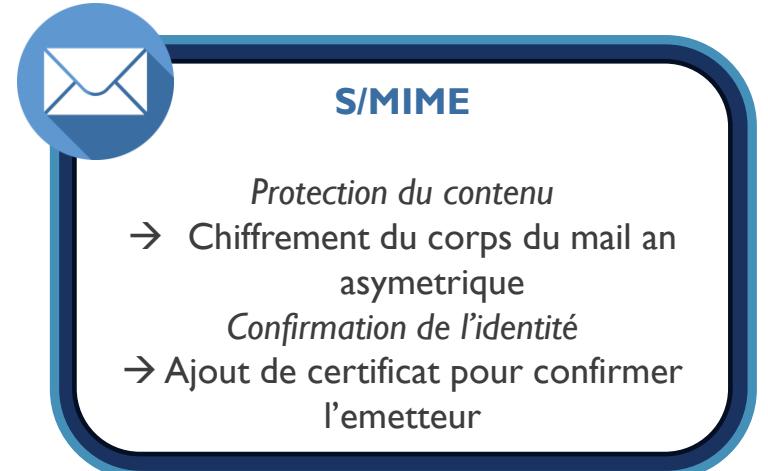
* ce guide vous détaille toutes les bonnes adresses, les bons plans et les principaux services utiles lors de votre année universitaire (logement, réseau bus, aide sociale...).

INTÉGRITÉ



→ Assurer que les données sont authentiques, fiables et exemptes de falsification

- Plusieurs méthodes possibles
 - **Mêmes que la confidentialité**
 - **Certificats** → Confirmer l'authenticité et fiabilité de la source (ex: SSL/TLS → HTTPS)
 - **Signatures numériques** → Confirmer l'identité de la signature et détecter les modifications



DISPONIBILITÉ



- Monde plus en plus connecté
 - Besoin d'une connexion Internet pour tout faire
 - Banques, assurance, université, etc...
- Disponibilité des entreprises mais également des services
 - FAI, EDG, GRDF, etc...
- Dépend de facteurs parfois sans control
 - Catastrophe naturelle → orage novembre 2023

franceinfo:

09/12/2023

« Il y a un peu plus d'un mois, la tempête Ciaran provoquait de nombreux dégâts en Bretagne. Près de 600.000 clients d'Orange ont été privés de téléphone et d'internet. Aujourd'hui encore, il en reste 12.500 dans toute la Bretagne et le retour complet à la normale n'est pas prévu avant fin février. 3.000 techniciens sont à pied d'œuvre mais face à l'ampleur des dégâts, les réparations prennent du temps [...]»

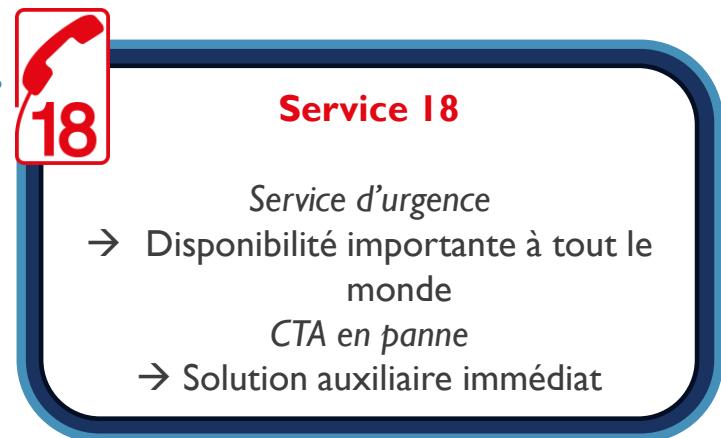
Source: franceinfo: Tempête Ciaran. Ces clients toujours privés d'internet et de téléphone dans le Morbihan

DISPONIBILITÉ



→ Assurer l'accès rapide aux informations a ceux qui ont le besoin

- Plusieurs méthodes possibles
 - **Solutions auxiliaire** → systèmes redondants (ex: réseau → fibre + 5G)
 - **Mises à niveau** → réduction des dysfonctionnements / bugs (update, patch, ...)
 - **Reprise après sinistre** → réduire le temps de remise en état
 - R6.B.07
- Souvent inévitable lors d'opérations de maintenance



QUELQUES DATES IMPORTANTS ...

1970

Premier virus « Creeper », programme réplicant sur ARPANET
« I'm the creeper, catch me if you can! »

Création du premier anti-virus
« Reaper »

1976 - 2006

Pendant 30 ans, plus de \$2M de documents aérospatiaux de Boeing donnés à la Chine par Greg Chung

Plus grande attaque interne impactant les US

2013

Edward Snowden du CIA a fuité des informations classifiées du NSA

L'attaque interne avec le plus gros impact sociétal → perte de confiance dans le gouvernement US

2013 – 2014

Attaque de Yahoo!, 3M de comptes utilisateurs atteints (noms, mdp, questions de sécurité, ...)

Yahoo a reçu une amende de \$35m pour ne pas avoir informé de l'attaque → baisse du prix de vente d'environ \$350m

2015

4,2m de données personnelles volé du bureau du gestion du personnel US, dont 21,5m agents sécurité et 5,6m empreintes digitales

Un des plus grosses fuites de données gouvernementales US

2017

« NotPetya » virus ciblant des vulnérabilités chez Windows a atteint plus de 12 500 machines, purgant banques, aéroports, gouvernements, ...

Plus dangereux qu'un rançongiciel classique, a empêché les machines de fonctionner

2017

« WannaCry », rançongiciel crypto-verre ciblant les machines Windows avec paiement en Bitcoin

Premier « rançon-verre » du monde, plus de 230 000 ordinateurs infectés dans plus de 150 pays en 1 journée

2017

« Equifax », n'a pas patché une faille Apache Struts, env. 143m US compromis avec 209 000 cartes de crédits

Plus grande fuite de données bancaires



LES RISQUES DE LA CYBER ESPACE

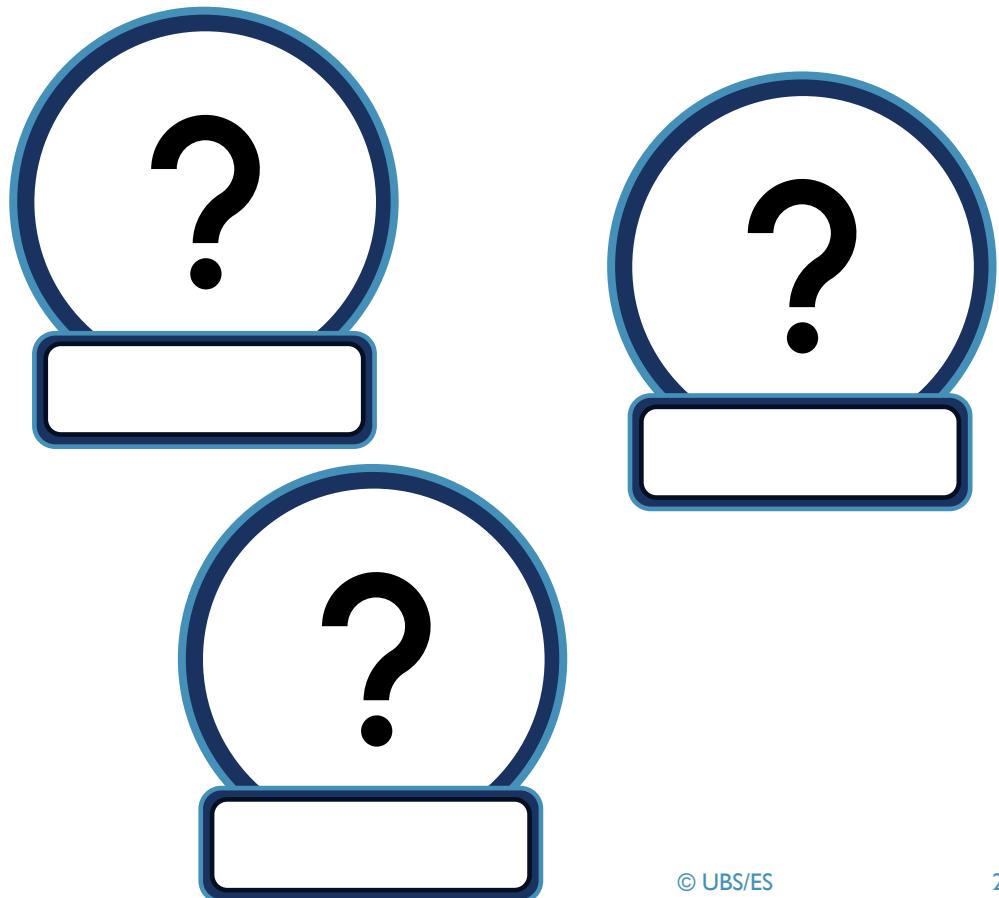
LE « CYBER RISQUE »

Le risque cyber concerne l'exposition ou les pertes potentiels d'une attaque

L'étude des risques permet d'identifier les menaces et les vulnérabilités

- Quantifier la probabilité d'une attaque
- Qualifier les conséquences

La Cybersécurité est un élément PRIORITAIRE



LE « CYBER RISQUE »

Le risque cyber concerne l'exposition ou les pertes potentiels d'une attaque

L'étude des risques permet d'identifier les menaces et les vulnérabilités

- Quantifier la probabilité d'une attaque
- Qualifier les conséquences

La Cybersécurité est un élément PRIORITAIRE

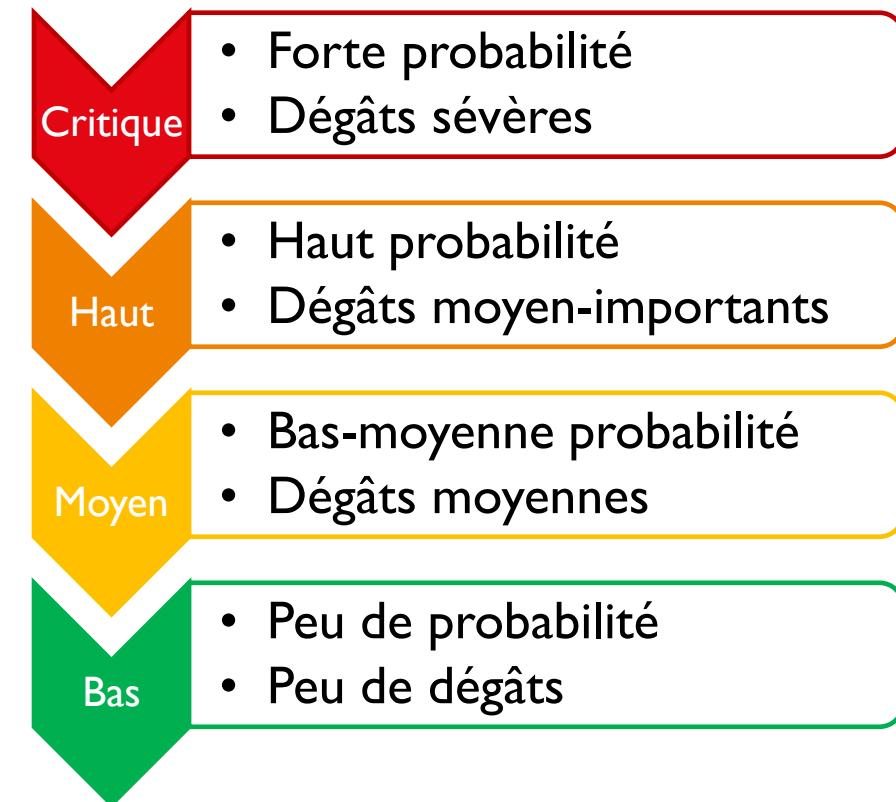


CLASSEMENT DES RISQUES

Un grand nombre de risques peuvent exister
Important de les « classifier »

- Plusieurs méthodes existent
 - Domaine ciblé
 - **Probabilité**
 - **Dégâts**
- Classements propres aux entreprises
 - Discrétion du RSSI

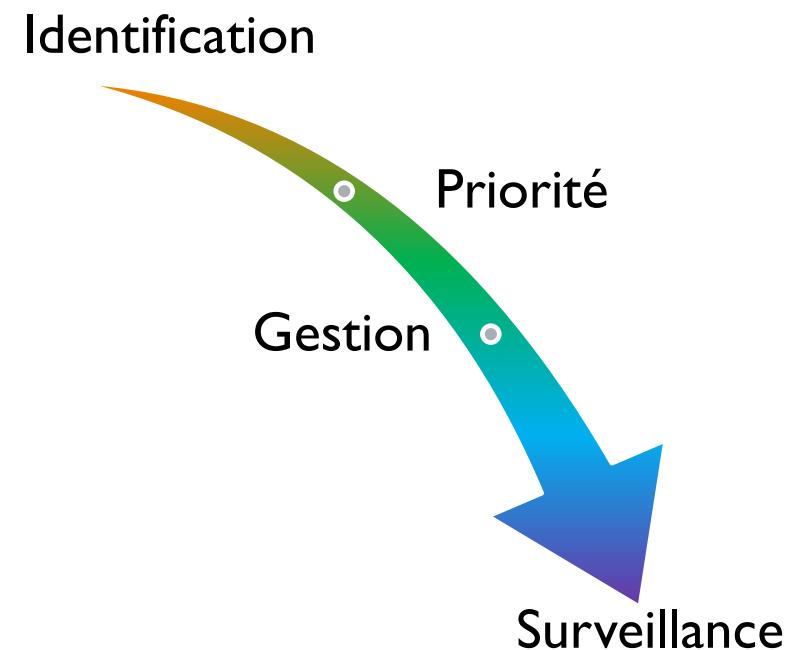
Les plus fréquents



LA GESTION DES RISQUES CYBER

L'évolution constante des méthodes de gestion des risques est importante

- Processus de plusieurs étapes
 - **Identification** → lister les risques potentiels contre le SI
 - **Priorité** → Ordonner selon un classement défini
 - **Gestion** → Traiter les risques un par un et mettre en place une protection
 - **Surveillance** → Observer les risques traités et non traités pour identifier d'éventuels attaques
- Les risques ne peuvent pas être éliminés
→ réduire leur impact et probabilité des menaces



MENACES VS VULNÉRABILITÉS VS CONSÉQUENCES

Menace

Couvre toute type d'attaques

Ex: Ingénierie sociale, DDoS, analyse de traffic, écoute, intrusion, etc...

Diversité de menaces dont les origines peuvent être également diverse et variés

Vulnérabilité

Concerne les failles, faiblesses ou lacunes pouvant être exploités

Ex: logiciel/system non à jour, mauvaise configuration, pas de patch de sécurité

Vérification constante, protection active (installation des mјj, patch) ou configuration précise

Conséquence

Les dégâts réels subis d'une intrusion réseau ou système

Peuvent être directes (financiers), ou indirectes (réputation)

Possibilité de conséquences légales selon l'attaque/vulnérabilité

Sévérité liée à l'attaque et la gestion de la réponse

COMMENT ÉVALUER UN RISQUE CYBER

- Les attaquants ciblent généralement les actifs critiques d'une entreprise
 - Composés de plusieurs ressources (ex: data, systèmes, réseaux, etc...)
 - Il est important de les identifier
- Ces actifs peuvent posséder des vulnérabilités qui doivent être identifiées
 - Utilisation de Framework d'évaluation des risques (NIST, FAIR, COSO, TARA, ...)
 - 3 types d'évaluations primaires
 - Mise en place d'audits réguliers sont également utiles (internes/externes)

Risque de référence

Information d'identification et de priorité des risques

- Exemple: pas de système de surveillance sur une porte
- Identifie l'impact sur d'autres secteurs / personnels de l'entreprise (salaires, RH, travaux, etc...)

Risqués liés aux problèmes

Prise en compte de l'effet domino des risques de référence

- Exemple: La porte non surveillée a été utilisé pour un cambriolage. Cette évaluation identifie des changements (entrée sortie du personnel, ouverture prolongé, système de surveillance existent en panne, etc...)
- Permet la mise en place des changements plus facilement, en confiance et de manière renseigné

Évaluation continue

Surveillance 24h/7j pour identifier de nouveaux risques

- Exemple: mise en place d'un système de badge sur la porte, réparation du système de surveillance, etc...
- Permet de mitiger les risques avant leur exploitation et les rendre plus efficace

COMMENT AMÉLIORER LA SÉCURITÉ DES SYSTÈMES

Une implication active de l'entreprise et des personnels est importante

- Mise en place d'une stratégie de défense multicouche



Première ligne
de défense

- Mise en place de pare-feu robustes
- Mise à jour logiciel réguliers
- Cyber prévention auprès du personnel de l'entreprise



Défense
proactive

- Surveillance des activités réseaux
- Mise en place de technologies de chiffrement des données sensibles stockés et transmis
- Gestion d'accès renforcé (MFA, droits utilisateurs, etc...)

→ Ces méthodes apportent une protection contre les menaces et une résilience cyber sur le long-terme

POURQUOI LA RÉPONSE À INCIDENTS ?

- La réponse à incidents joue un rôle cruciale
 - Définit le plan de mitigation d'une attaque
 - Actions à mener, liens de communications, étapes de récupération
 - Détermine la rapidité et l'efficacité de la réponse
- Testes et mises à jour régulier
 - Évolution des menaces → plan périmé
 - Intégration des leçons apprises des précédents attaques
- Formation du personnel dans les procédures de réponse
 - Minimiser l'impact d'un incident



Pas une question de « **si** »
Mais de « **quand** » ...

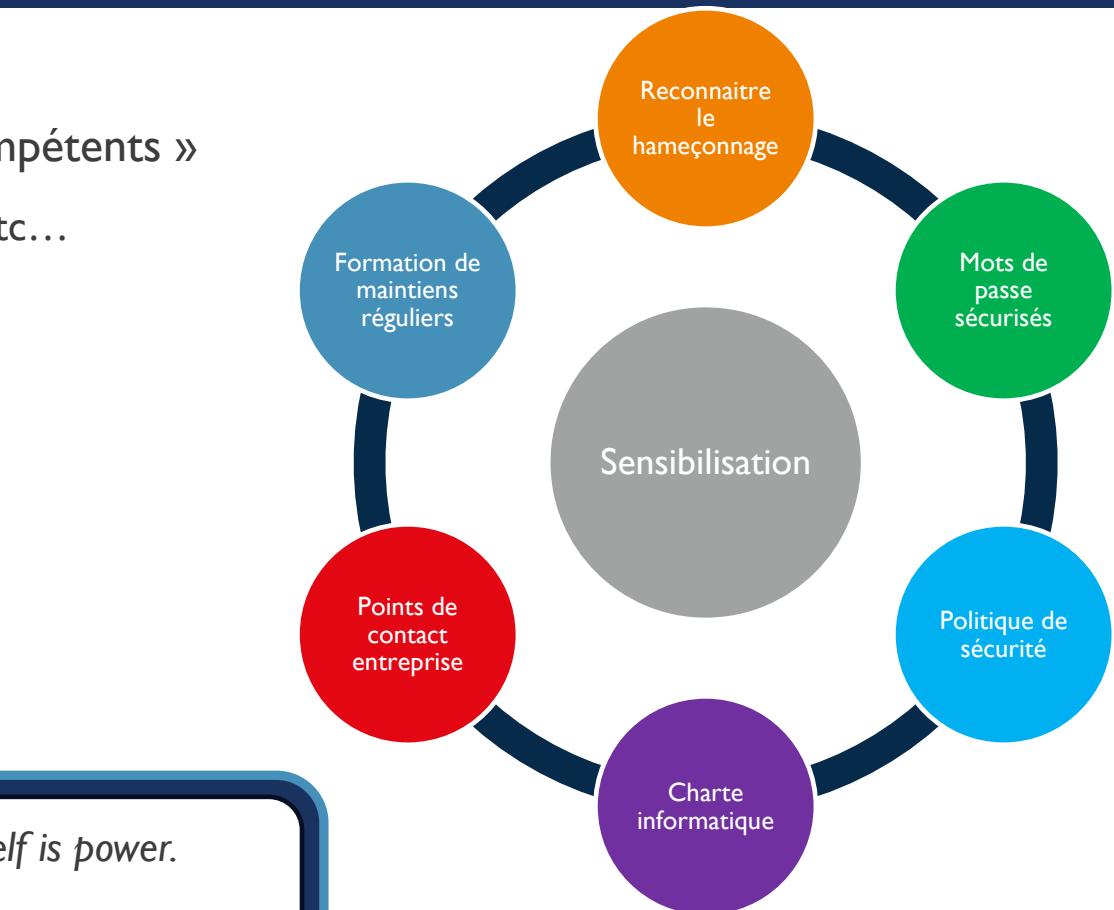
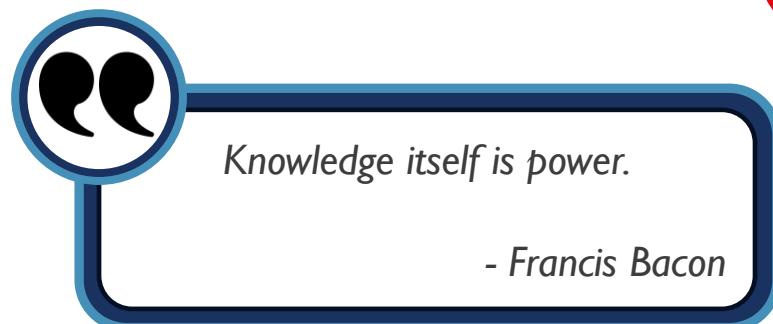
L'IMPORTANCE DE LA FORMATION

Beaucoup de formations sont réservés aux personnes « compétents »

- Formations sécurité RSSI, DSI, ingénieurs de maintenance, etc...
- **Mauvaise idée**

Tout le monde est impliqué dans la protection

- Les premières personnes ciblées → personnel classique
- *Formation* → première ligne de défense proactive
 - Formations de maintien réguliers pour suivre les tendances



QUELQUES RISQUES COURANTS

Les risques se présentent sous plusieurs formes

- Variant d'un domaine à un autre
- Évolution constante

Présentation des risques les plus courants



Fournisseurs tiers



Employés et entrepreneurs (menaces internes)



Manque de conformité



Propriété intellectuelle / informations sensibles mal sécurisés



Acteurs tiers

FOURNISSEURS TIERS



Risque

Incorporation de fournisseurs tiers dans le fonctionnement d'organisations

- Soulagement financier
- Efficacité opérationnelle
- Représentent un risque significatif
 - Ont accès à des données sensibles
 - Informations personnelles des clients

Mitigation

Posséder une vue d'ensemble complète et continue des entités dans le réseau

- Surveillance constante des activités et potentiels vulnérabilités
- Maintien de protocoles de sécurité pour tous
- Accès limités et ciblés aux informations nécessaires pour les fournisseurs

MENACES INTERNES



Risque

Les employés et entrepreneurs jouent un rôle important dans la sécurité de l'entreprise

- Formations cybersécurité sont importants
- Pouvoir identifier les risques et savoir y répondre
- Employés souvent ciblés d'attaques
 - Vol d'identité où infection virale, etc...

Mitigation

Mise en place d'un modèle de sécurité zéro-confiance

- Tous les accès administrés et paramétrés
- Champ de vision selon le travail de chacun
 - Un RH n'a pas besoin d'un accès aux données comptables
 - Réduction des opportunités d'actions malicieuses ou d'erreurs

MANQUE DE CONFORMITÉ



Risque

Le respect des données privées est de plus en plus important et régulé

- Existence de plusieurs normes à suivre
- RGPD, PCI, HIPPA, etc...

- Conformité avec ces normes est important
- **Ce n'est pas une garantie de sécurisation**

Mitigation

Audits réguliers des autorités pour valider la conformité

- Temps élevé entre les audits
- Possibilité de perte de conformité accidentelle

- Mise en place de surveillance de l'écosystème cyber
 - Vérification de la conformité
 - Identifications des évolutions de l'entreprise

DONNÉES MAL SÉCURISÉES



Risque

De plus en plus de collection de données utilisateur

- (avec et sans autorisation)
- Données « importantes » pour améliorer l'expérience client
- Augmentation du risque d'attaque
 - Données mal sécurisés → cible parfaite au vol et revente

Mitigation

Sécurisation des plateformes de stockage et d'analyse

- Augmenter la protection des données
- Vérification des processus d'analyse
- Organisation d'audits réguliers
 - Confirmation du niveau de sécurité / conformité
 - Mises à jour et adaptation des protocoles de sécurité

ACTEURS TIERS



Cybers criminels

- Motivation financière
- Multiples méthodes (ransomware, vol de données, fraude, etc...)
- Évolution constante des méthodes pour contourner les mesures de sécurité

États étrangers

- Motivation politique / stratégique
- Cyber espionnage (données gouvernementales, infrastructures critiques)
- Méthodes sophistiqués → menace importante

Hacktivists

- Motivations politiques ou sociales
- Ciblant disponibilité et intégrité (modifications web, vol de données, DDoS, etc...)
- Mise en avant de leur cause (manifestation)

Autres acteurs émergeants

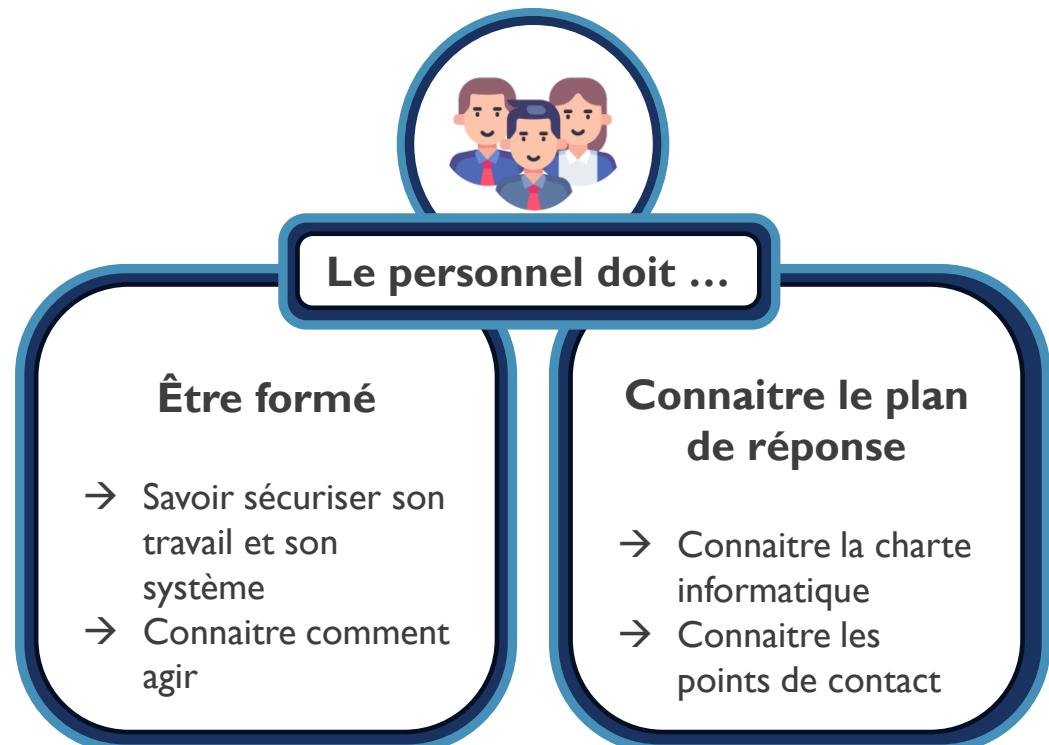
- Espionnage industrielle
- But de gain compétitive (infiltration)
- Perturber les opérations, voler des informations propriétaires

QUI EST RESPONSABLE ?

Généralement → responsabilité des équipes informatique et sécurité

En réalité → tout le monde est responsable

- Il est important d'avoir un plan de réponse à incident complet
 - Définir les responsabilités de chacun
 - Quand ils sont à réaliser
 - Les étapes de chaque utilisateur / département en cas d'attaque



LES CYBERATTAQUES

CYBERATTAQUE

Ensemble coordonné d'actions menées dans le cyberspace qui visent des informations ou les systèmes qui les traitent, en portant atteinte à leur disponibilité, à leur intégrité ou à leur confidentialité.



Une cyberattaque peut être ponctuelle ou s'inscrire dans la durée.

LES GRANDES FAMILLES DE CYBERATTAQUES

L'ANSSI identifie quatre grandes familles de cybermenaces. Selon la motivation de l'attaquant et le mode opératoire adopté, chaque cyberattaque pourra être associée à l'une de ces menaces.



Visée lucrative



Espionnage



Déstabilisation



Sabotage



L'APPÂT DU GAIN



- Génération d'un gain financier
 - **Directe** → Apport court terme (vol, détournements de fonds, etc...)
 - **Indirecte** → Apport long terme (vol et vente de données privés, investissement bourses, impact réputation, etc...)
- Généralement réalisée par des groupes de cybercriminels organisés
 - Sélection de cibles généralement opportuniste

ESPIONNAGE



Sous sa propre catégorie « Cyberespionnage » → Renseignement

- Plusieurs objectifs en vue, 2 très communs
 - **Étatique** → Informations gouvernementales, secret défense, etc...
 - **Économique** → Informations financiers, montants bancaire, revenue, etc...
- Mise en place et conservation d'un accès discret et durable
 - Peut prendre longtemps avant d'être aperçu → années ...
- Plusieurs secteurs exposés
 - **Industriels** → armement, spatial, aéronautique, pharmaceutique, énergie, etc...
 - **État** → économie, finances, affaires étrangères, défense, etc...

DÉSTABILISATION

Existe sous plusieurs formes



- **Perception**
 - diffusion de données légitimes lors de campagnes de fausses informations (boites mails, sites internet, etc...)
- **Décrédibiliser**
 - défiguration d'un site web, saturation connexions,
 - D'origine employés mécontents, organisations étatiques, souvent des « hacktivistes »
- **Sabotage**

SABOTAGE

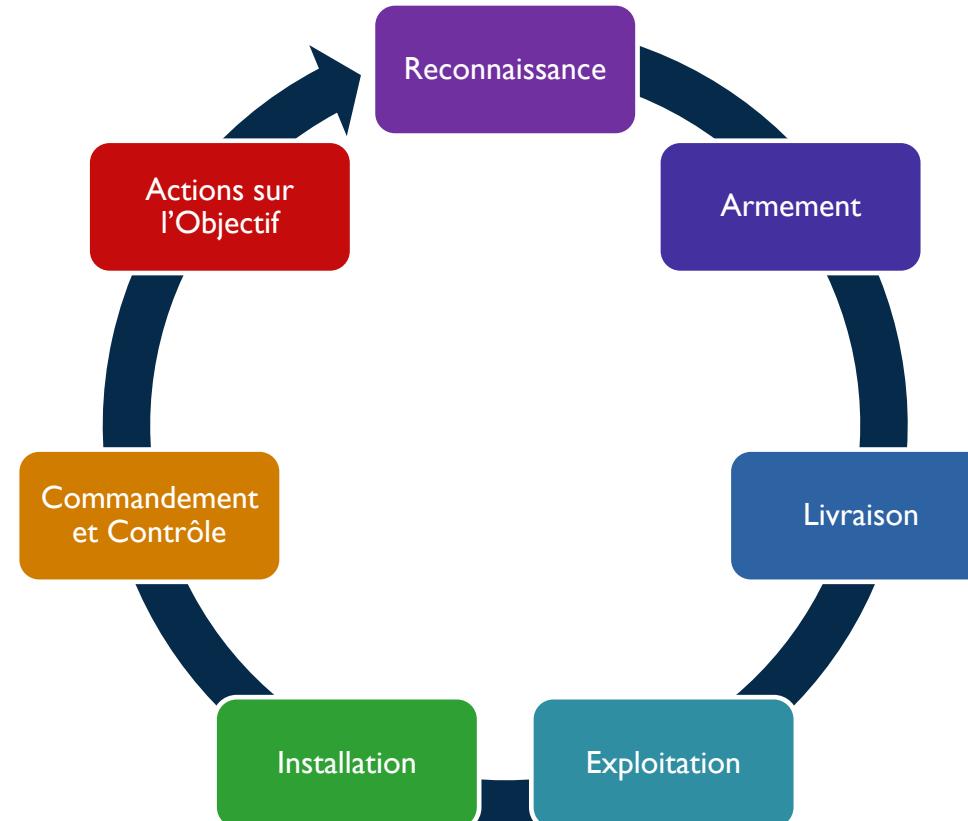


Ne pas atteindre que l'image de la cible

- Toucher au fonctionnement elle-même
- Rendre inopérant le SI
 - Tout ou une partie
 - Système d'informations classique / systèmes industriels
- Effectué **VIA** une cyberattaque → comment ?

LES ÉTAPES D'UNE CYBERATTAQUE

- Pas aussi simple que « viser → tirer »
- Plusieurs étapes pour une attaque réussie
 - Basée sur le « Kill Chain » militaire
- « Kill Chain Intrusion » défini sur 7 étapes



LES ÉTAPES D'UNE CYBERATTAQUE

Reconnaissance

- Sélection de la cible, la recherche et l'identification des vulnérabilités du réseau

Armement

- Création du moyen d'attaque (virus, ver, logiciel malveillant, etc...) donnant accès à distance à la cible via les vulnérabilités

Livraison

- Transmission de l' « arme » à la cible (via des pièces jointes, sites web, clé USB, etc...)

Exploitation

- Déclenchement de l'infection en agissant sur le réseau cible pour exploiter la vulnérabilité

Installation

- Installation d'un point d'accès utilisable par un attaquant externe

Commandement et Contrôle

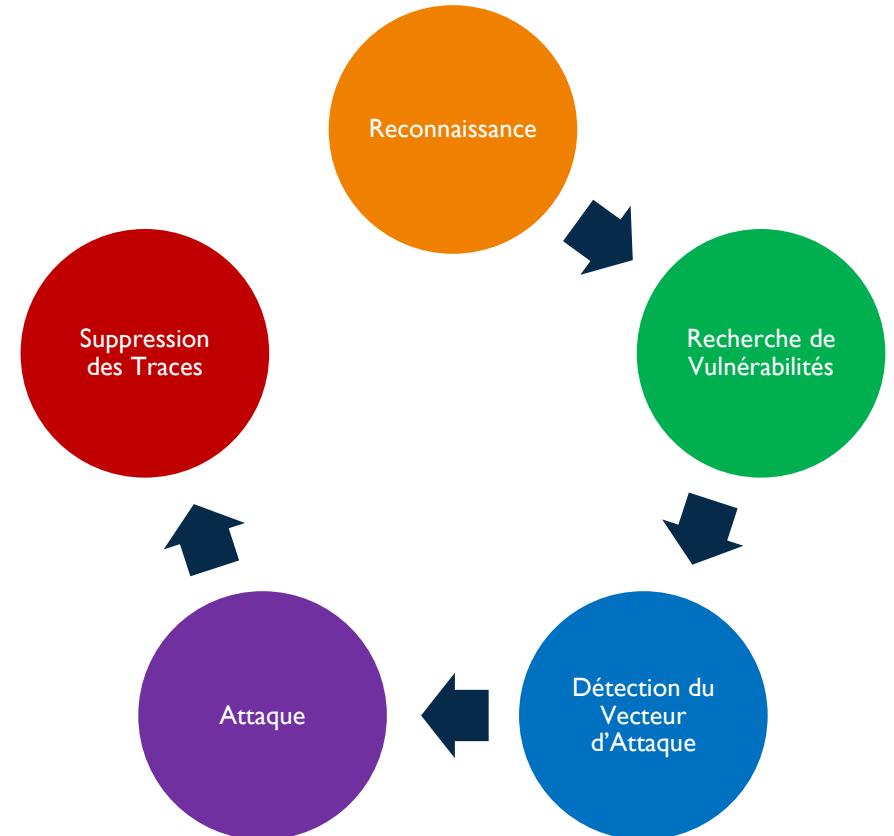
- Accès permanent au réseau cible via le logiciel malveillant

Actions sur l'Objectif

- Prise de mesures pour atteindre l'objectif (ex. Exfiltration ou destruction de données, chiffrement contre rançon, etc...)

LES ÉTAPES D'UNE CYBERATTAQUE

- Récemment, une revue des étapes a été fait
 - Plus de précision
 - Regrouper certaines phases
 - Ajout de l' « extraction » de l'attaquant
- Approche de 5 étapes dans lesquels les 7 autres peuvent être regroupés



LES ÉTAPES D'UNE CYBERATTAQUE

Reconnaissance

« Reconnaissance »

- Analyse et exploration de la cible : topologie du réseau, OS, logiciels, équipements physiques, informations importants (IP, noms d'utilisateurs), informations sur le personnel (adresse personnel et numéros de téléphone pro et perso), système pare-feu, etc...

Recherche de Vulnérabilités

« Reconnaissance » | « Armement »

- Analyse de la reconnaissance pour identifier des failles dans le réseau, OS, logiciels, employés, etc...

Détection du Vecteur d'Attaque

« Reconnaissance » | « Armement » | « Livraison »

- Basé sur les vulnérabilités et la reconnaissance réseau et système, on identifie par ou « pénétrer » dans la cible (numérique, personnel, physique, etc...)

Attaque

« Armement » | « Livraison » | « Exploitation » | « Installation » | « Commandement et contrôle » | « Actions sur l'objectif »

- Pas de méthodologie « fixe » pour mener une attaque car dépendant des spécifications de la cible mais peut être précisé et entraîné via les précédentes étapes

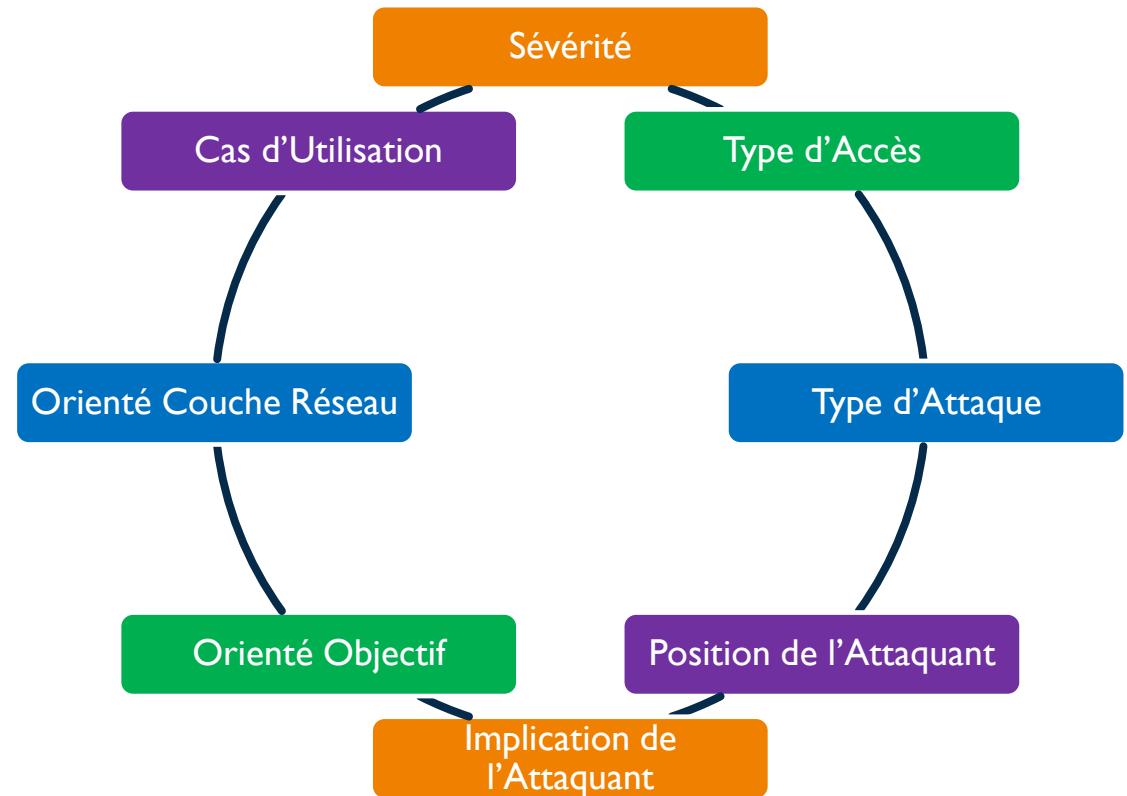
Suppression des Traces

- Nettoyage de la cible via la manipulation ou suppression des logs (manipulation préférable), pour réduire la probabilité de détection et retarder une réponse

CATÉGORISATION DES ATTAQUES

La catégorisation est un facteur important

- Permet de trier les attaques
- Plus pertinent aujourd'hui avec beaucoup de méthodologies
- 8 méthodologies de catégorisation
 - Chacun possédant leur propre approche



CATÉGORISATION DES ATTAQUES

Sévérité

Organisé selon la sévérité de l'attaque ou le niveau de la menace

- Utilisé par le « UK National Cyber Security Centre » → 6 niveaux de menaces allant de « localisé » à « Urgence National Cyber »

Type d'Accès

Organisé selon le type d'accès utilisé pendant l'attaque

- Séparation selon le moyen d'accès → Physique / Cyber

Type d'Attaque

Organisé selon le type de l'attaque

- Plusieurs méthodes existent
- DoS, Probing, R2L, U2R | DoS, MitM, Brute Force | Scan et Probing | etc...

Position de l'Attaquant

Organisé selon la position de l'attaquant par rapport à sa victime

- Séparation selon la position sur le réseau et système ciblé → Externe / Interne

CATÉGORISATION DES ATTAQUES

Implication de l'Attaquant

Organisé selon l'interaction entre l'attaquant et la victime

- Séparation selon l'implication de l'attaque → Passive / Active

Orienté Objectif

Organisé selon l'objectif final et l'attaque utilisé

- Plusieurs méthodes existent
- Reconnaissance, Accès, Malicieux, Non-Malicieux, Cybercriminalité, Cyberespionnage, Cyberterrorisme, Cyberguerre | Matériel, Réseau | Facteur Humain | etc ...

Orienté Couche Réseau

Organisé selon la couche du modèle OSI sur laquelle l'attaque réside

- Couches 1-4 et 7

Cas d'Utilisation

Organisé selon le cas d'utilisation spécifique

- Plusieurs cas → plusieurs approches
- IoT → Modèle IoT couches Perception, Réseau, Application | CPS-Smart Grids → Couches Energie et Alimentation, Informatique, Communication | etc ...

Categorisation	Approach
Attack Severity	Six threat levels: Localised, Moderate, Substantial, Significant, Highly Significant and National Cyber Emergency
Access Type	Physical, Cyber
	DoS, Probing, R2L, U2R
	DoS, MitM, Brute Force
Attack Type	DoS, Replay, Deception
	Active Eavesdropping, Scanning, Probing
	Physical, Network, Software, Encryption
Attacker Position	Outside, Inside
Attacker Implication	Active, Passive
	Privacy
	Reconnaissance, Access, Malicious, Non-Malicious, Cyber Crime, Cyber Espionage, Cyber Terrorism, Cyber War
Objective Oriented	Disconnection and Goodput Reduction, Side-Channel Exploitation, Covert-Channel Exploitation
	Hardware, Network, Human Factor
	Interception, Interruption, Fabrication, Modification
	Access Control, Authentication, Availability, Confidentiality, Integrity
Network Layer Oriented	OSI model, Layers 1–4 and 7
	CPS-NCS
	Attacks on Physical Components, Attacks on Communication Network
	CPS-Smart Grids
	Power and Energy Layer, Computer/IT Layer, Communication Layer
Use-Case Specific	Wireless Ad-Hoc Networks
	Attacks on MANET, Attacks on WSN
	IoT
	Low-Level, Intermediate-Level, High-Level Security Issues
	IoT Stack Layers-Perception, Network, Application
	SDN
	SDN Architecture-Application Layer, Application-Control Interface, Control Layer, Control-Data Interface, Data Layer

MENACE VS ATTAQUE

Terminologie souvent utilisé pour la même chose

Menace	Attaque
Intentionnelle ou involontaire	Intentionnelle
Peuvent ou ne peuvent pas être malicieuses	Malicieuse
Des circonstances qui peuvent causer des dégâts	L'objectif est d'infliger des dégâts
Les informations peuvent ou ne peuvent pas être modifiés ou endommagés	La probabilité de modification et de dégâts des informations est très forte
Difficile à détecter en comparaison	Facile à détecter en comparaison
Peuvent être bloqués en contrôlant les vulnérabilités	Ne peuvent pas être bloqués en contrôlant QUE les vulnérabilités
Peuvent être initiés par le système ou par une entité tierce	Toujours initié par une entité tierce (système ou utilisateur)
Peuvent être classifié comme Physiques, Interne, Externes, Humaine et Non-Physiques	Peuvent être classifiés comme Virus, Spyware, Phishing, Vers, Spam, Botnets, DoS, Ransomware et Intrusion

TYPES DE MENACES

Il existe plusieurs types de menaces

- **Non structurés** → utilisation d'outils facile d'accès (scripts shell, casseur de mdp)
 - Peuvent causer des dégâts significatifs a une entreprise
- **Structurés** → attaque organisée pour atteindre un réseau ou une organisation spécifique
 - D'origine d'hackers très motivés et très compétents
- **Externes** → utilisation non autorisée des accès informatique et réseau via l'Internet
 - D'origine individuelle ou d'organisations externe a l'entreprise
- **Internes** → utilisation non autorisée des accès réseau via un accès direct ou un compte utilisateur
 - Généralement d'origine d'un employé

MENACES EN 2024

- Évolution constante des attaques
 - Menaces suivent également
- Par deuxième trimestre 2024
 - Plus de 1636 attaques par organisation
 - PAR SEMAINE
- Présentation des 16 menaces les plus présente en 2024

→ 16. Procédures post-attaque insuffisant

- Environ 67% des entreprises ayant subi une attaque sont attaqués une deuxième fois en moins d'un an
- Environ 10% de ces entreprises subissent au moins 10 attaques par an

→ 15. Mauvaise gestion de données

- Beaucoup trop de données à gérer
- Des données en surplus donc mal organisés

MENACES EN 2024

→ 14. Internet des Objets

- Augmentation du nombre d'équipements suite à la pandémie
- En 2022 plus de 112m attaques
 - En 2018 seulement 32m

→ 13. Vulnérabilités équipements mobiles

- Forment une couche de sécurité supplémentaire à cause de la quantité de données
- Des méthodes MFA souvent liés au smartphone

→ 12. Vulnérabilités Cloud

- Augmentation du nombre d'environ 154% dans la dernière année
- Souvent lié à une mauvaise configuration
 - 2023 → Toyota, 260000 clients impactés

→ 11. Mauvaise hygiène Cyber

- Manque de formation ou de prévention cyber
- Environ 2/3 d'entreprises US n'utilisent pas de gestionnaire de MDP
- 54% de pro. Informatique n'utilisent pas le MFA

MENACES EN 2024

→ 10. « Drive By Attack »

- Passage par un site web infecté → téléchargement d'un logiciel malicieux
- Souvent caché comme Pop-Up

→ 09. Chevaux de Troie

- Un des premiers attaques → Encore utilisé aujourd'hui
- Couramment utilisé dans les guerres et l'espionnage → guerre Israël - Hamas

→ 08. Rançongiciel

- Entre 2023-2024, augmentation du prix moyen de plus de 500%
 - \$400000 → \$2m
- En 2023, temps moyen de récupération est de 136h / 17 jours ouvrés

→ 07. Attaques « sponsorisées » par des États

- Très coutant en période de tension / guerre
- Attaques des deux côtés pendant l'invasion de l'Ukraine

MENACES EN 2024

→ 06. Menaces Internes

- Couvrent les menaces intentionnels ou involontaires
- En 2018, un salarié de Tesla s'est vu refuser une promotion
 - Partagé des informations sensibles à des entreprises tiers

→ 05. DNS Tunneling

- Cacher du traffic dans des requêtes DNS pour passer les pare-feux
- Très efficace → pas facile à comprendre

→ 04. Menaces Cyber basés sur l'IA

- Utilisation de l'IA pour identifier des vulnérabilités
- Est également utilisé pour automatiser l'attaque
 - Plus sophistiqués et plus fréquents
- En 2023, 85% des pro. Cybersécurité pensent que la croissance des attaques est due à l'utilisation de l'IA
 - 90% des startups sont inquiets des dégâts des attaques IA

MENACES EN 2024

→ 03. Erreurs de Configuration

- Malheureusement très fréquent → personne n'est parfait
- En 2023, plus de 8000 serveurs étaient vulnérables à cause d'une mauvaise configuration
- Les causes les plus communs
 - Ne pas changer la configuration par défaut
 - Pas de segmentation réseau
 - Ne pas faire de māj / patch des logiciels / OS
 - Utilisation de mots de passe faibles

→ 02. Exposition au risque des tiers

- Exploitation de systèmes vulnérables de partenaires / fournisseurs tiers
 - Accès privilégié au système ciblé
 - Permet de contourner un système sécurisé
- Début 2024, AT&T impacté par une intrusion via fournisseur
 - Plus de 70m clients concernés (données SMS, appel, mdp, etc)
- 2023, 29% des intrusions ont eu lieu via un tiers

MENACES EN 2024

→ 01. Ingénierie Sociale

- Considéré comme la menace la plus dangereuse
 - Se repose sur l'exploitation des erreurs humaines que des vulnérabilités techniques
- En 2023, 74% des intrusions ont inclus une forme d'interaction humaine
 - Entre 75% et 91% des attaques ciblés ont commencé par **MAIL**
- Menace de plus en plus sophistiqués grâce à l'IA (IA générative, deepfake, etc...)

■ Les types les plus fréquents

- **Filoutage** (hameçonnage / phishing)
 - Tromperie par message
- **Spoofing**
 - Déception par création de faux contenu (mail / site web)
- **Whaling**
 - Cibler des personnes importantes dans les entreprises pour extraire de grosses sommes d'argent
- **Provocation**
 - Attirer des personnes à cliquer sur de fausses publicités avec des malwares ou des demandes d'informations personnels

LES TYPES DE CYBERATTAQUE

Pour rappel → Une cyberattaque est une action délibérée sur un système ou un actif

- Une attaque possède généralement
 - Un objectif précis
 - Une motivation
- Elle suit une méthodologie particulière et précise lorsque l'opportunité apparaît

- Il existe deux types d'attaques
 - **Actives** → Manipuler des ressources système ou impacter leur opération
 - **Passives** → Extraire des informations sensibles sans impacter leurs ressources

QUELQUES ATTAQUES PASSIVES



Écoute Clandestine



Analyse de Traffic



Empreintes



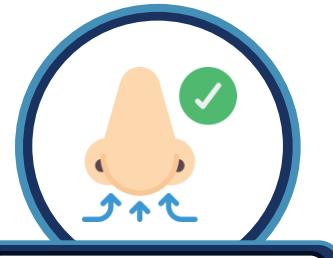
Espionnage



Wardriving



Plongée dans les
poubelles



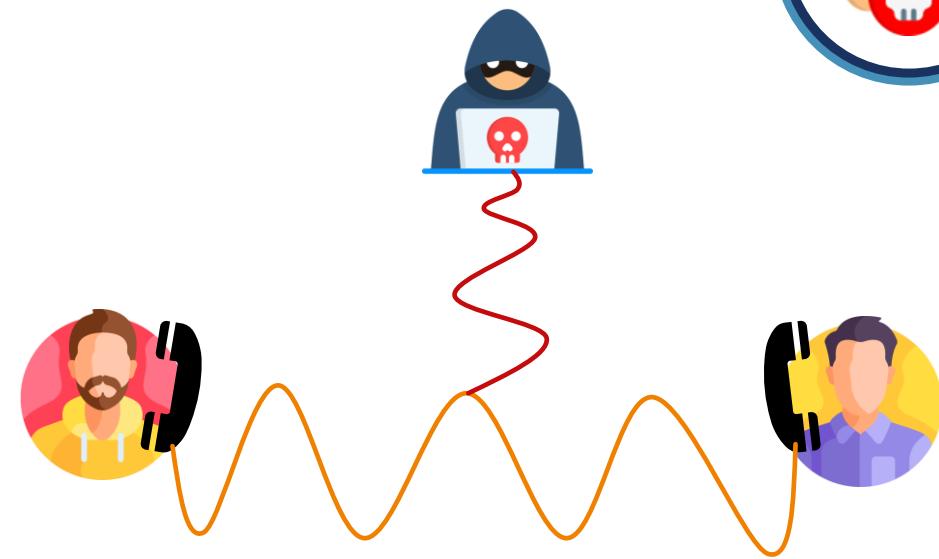
Reniflage de
Paquets

ÉCOUTE CLANDESTINE

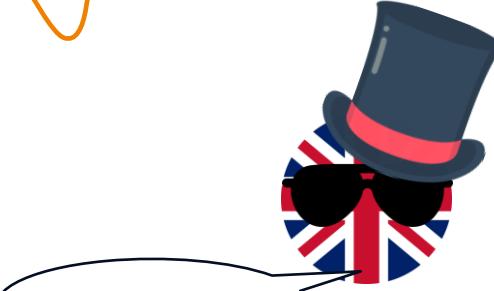


Écoute en temps réel des communications

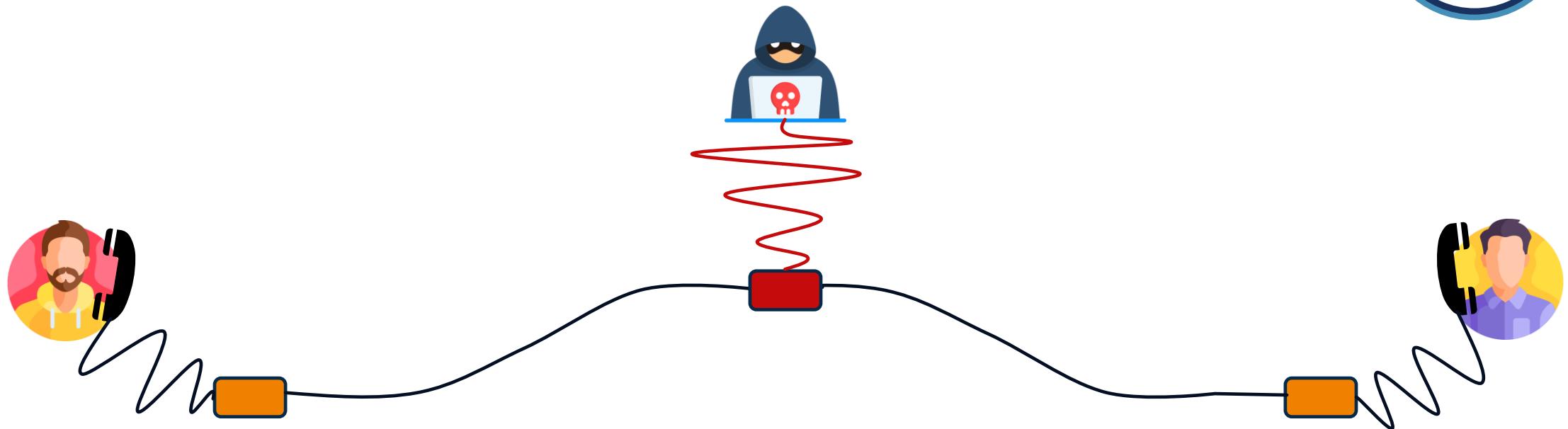
- Vol d'informations partagé sur un moyen non sécurisé
 - Wi-Fi publique, téléphone, etc...
 - Seulement l'information recherché est gardée
-
- Distinction avec « Snooping »
 - Données stockées pour analyse antérieur



TCPDump, Wireshark, etc...



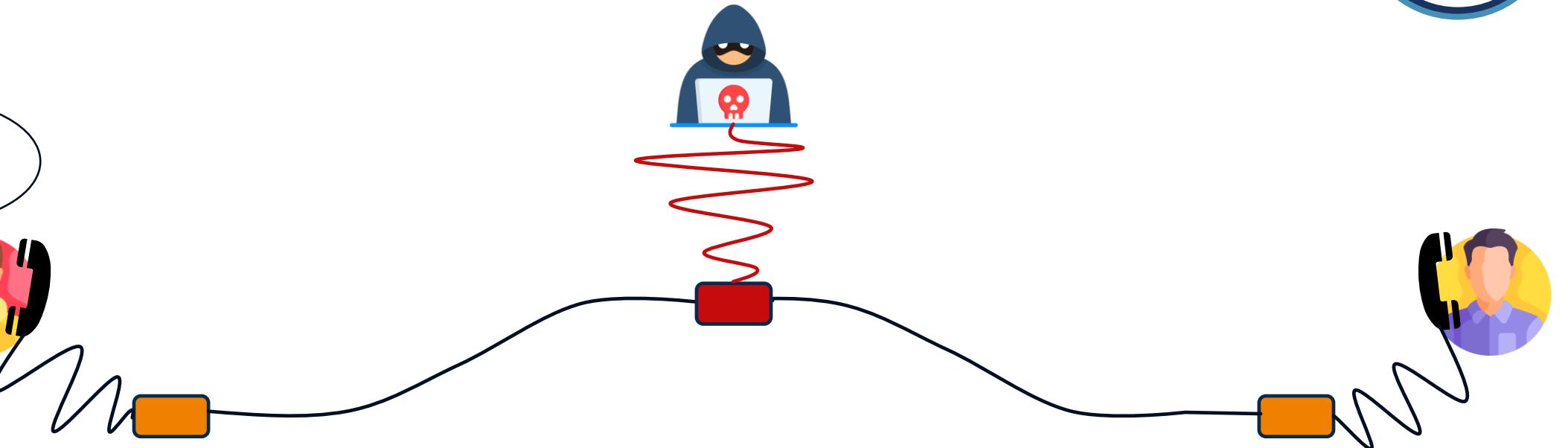
ÉCOUTE CLANDESTINE



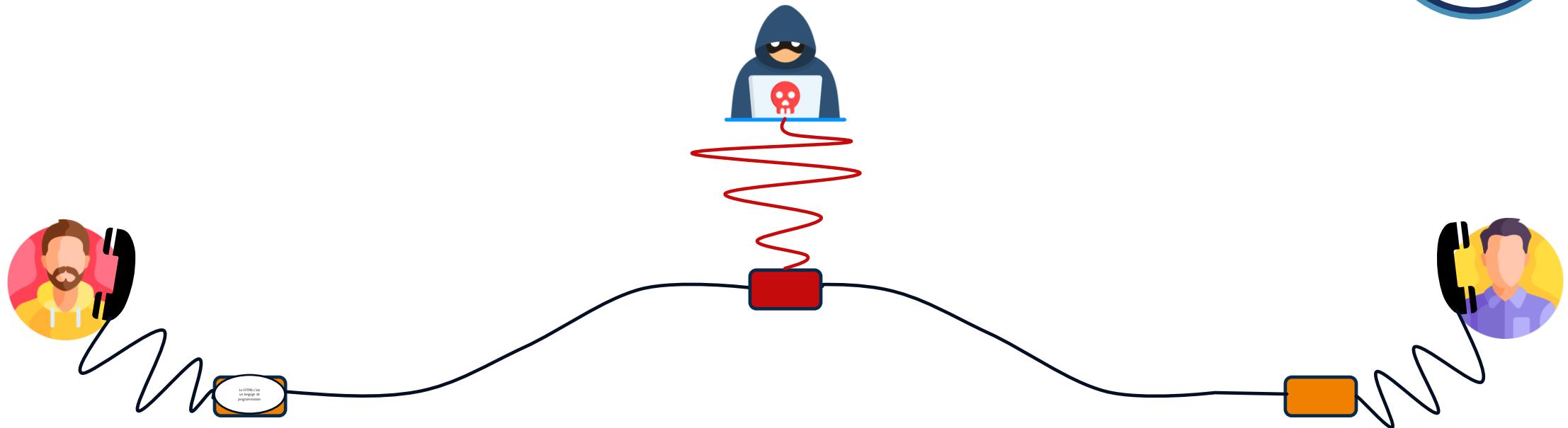
ÉCOUTE CLANDESTINE



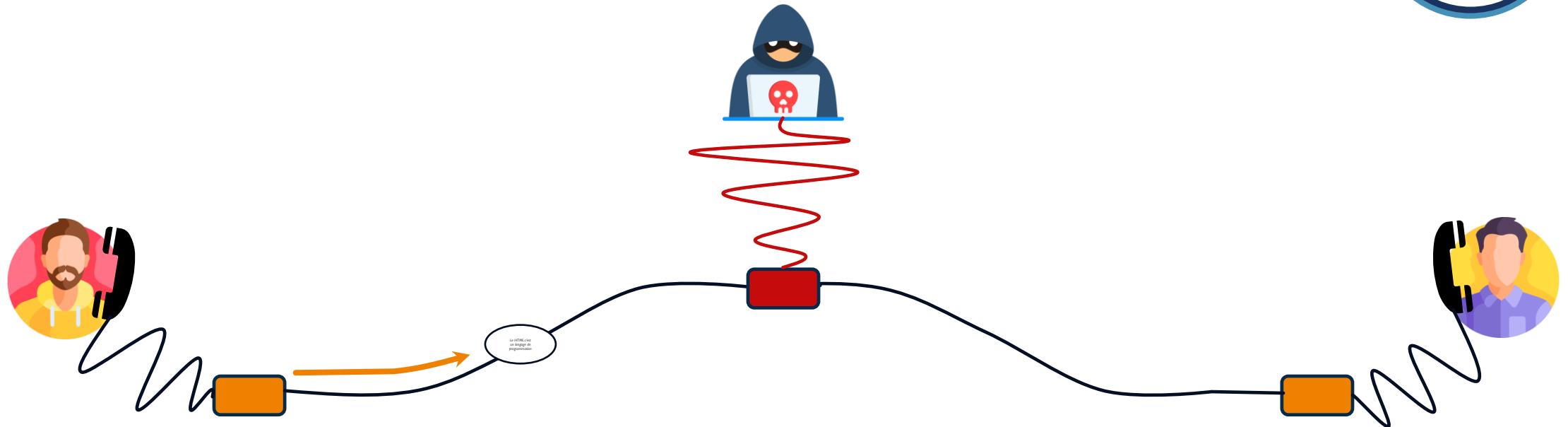
Le HTML c'est
un langage de
programmation



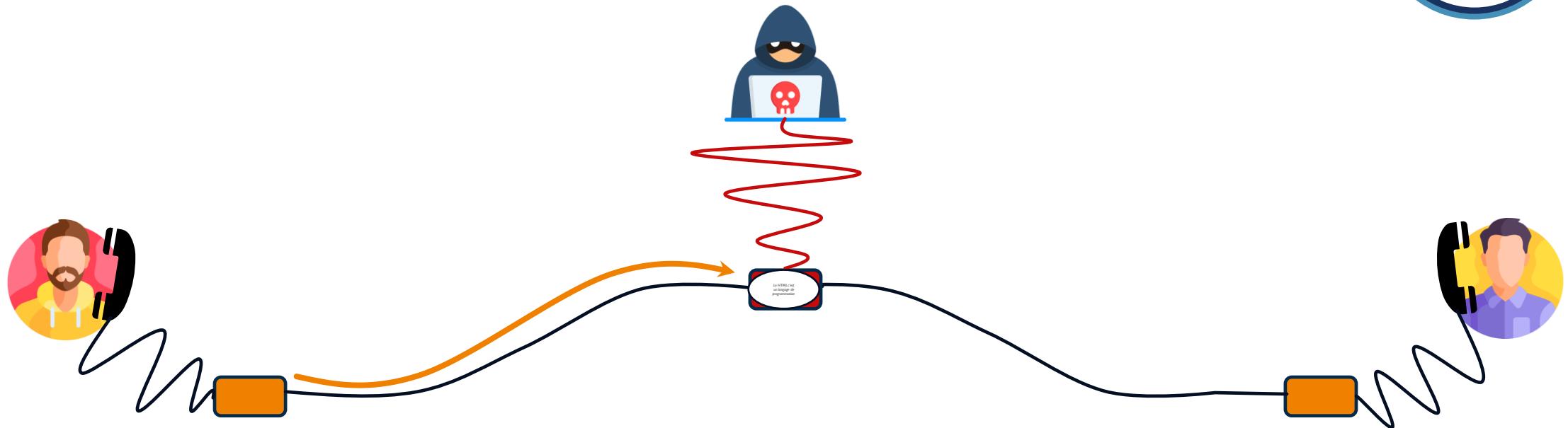
ÉCOUTE CLANDESTINE



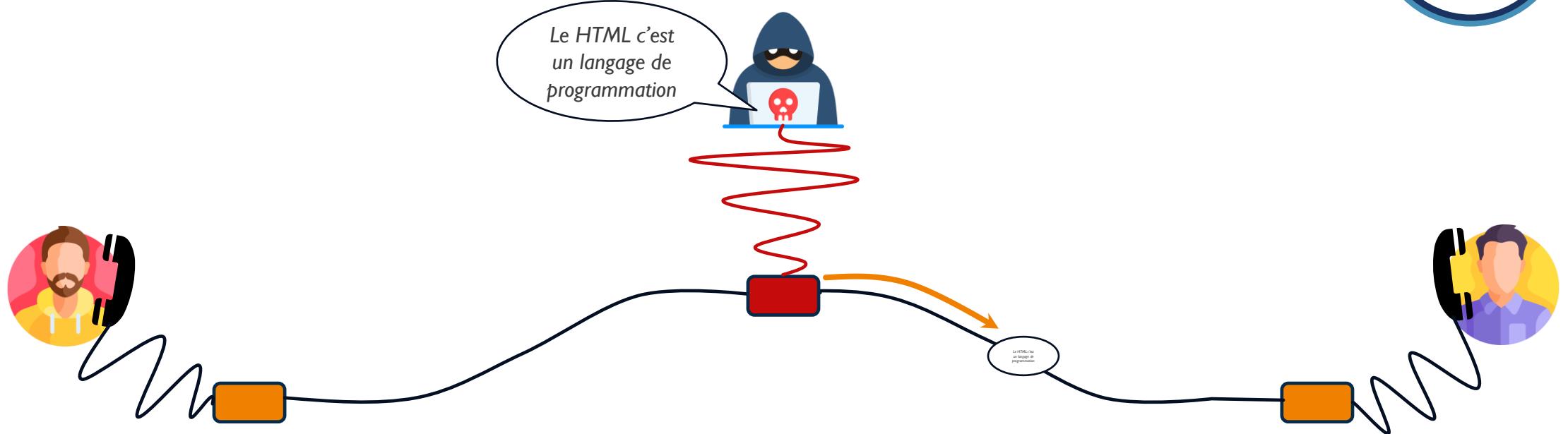
ÉCOUTE CLANDESTINE



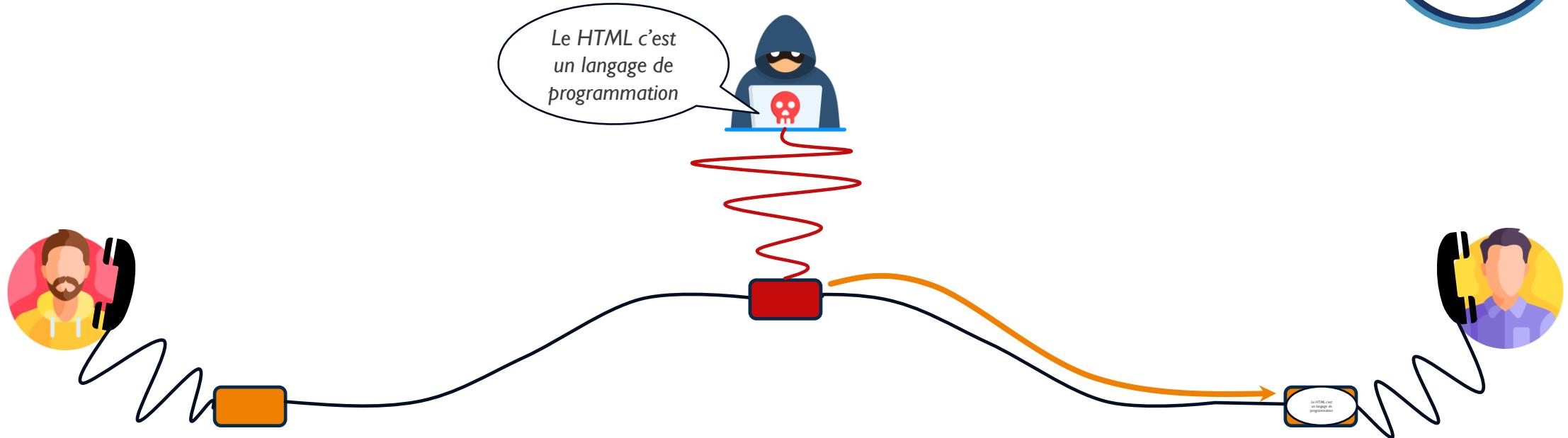
ÉCOUTE CLANDESTINE



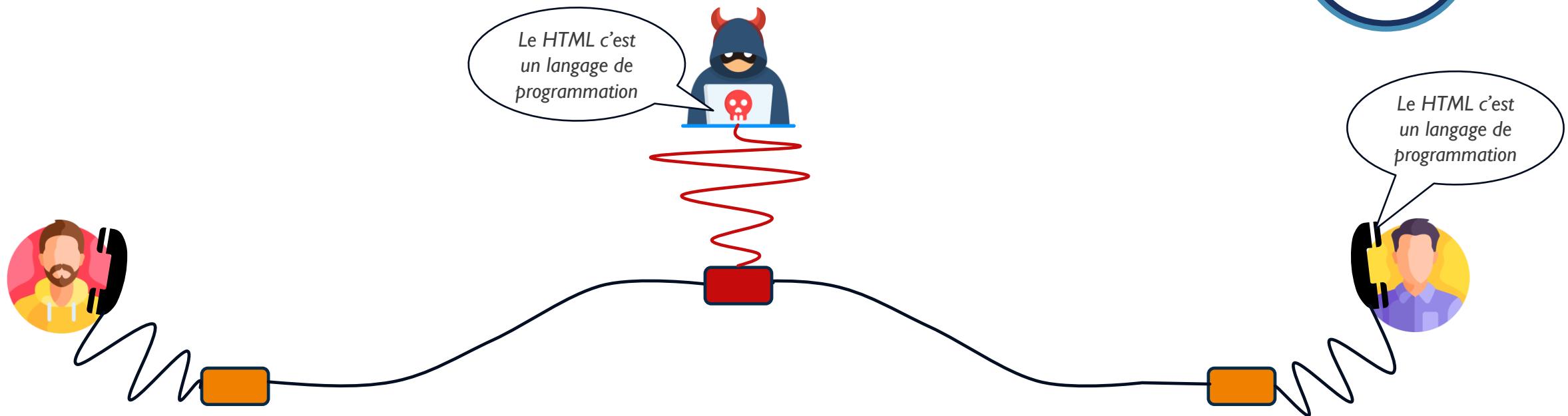
ÉCOUTE CLANDESTINE



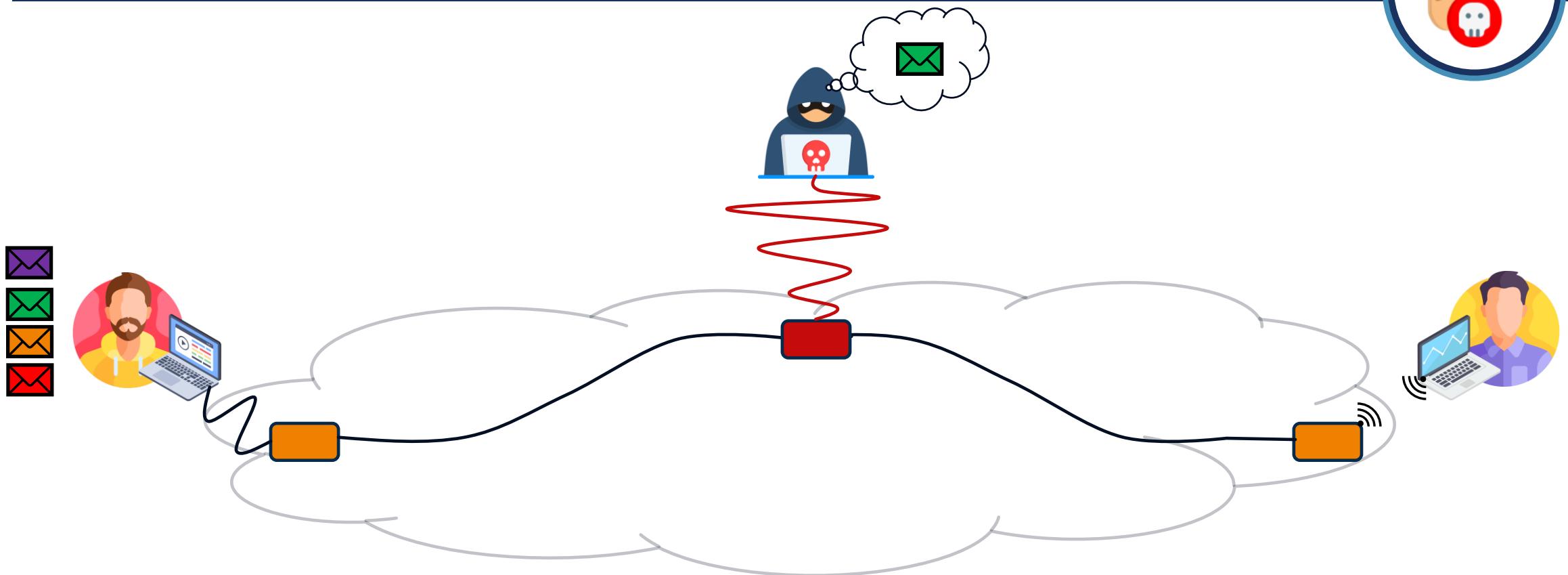
ÉCOUTE CLANDESTINE



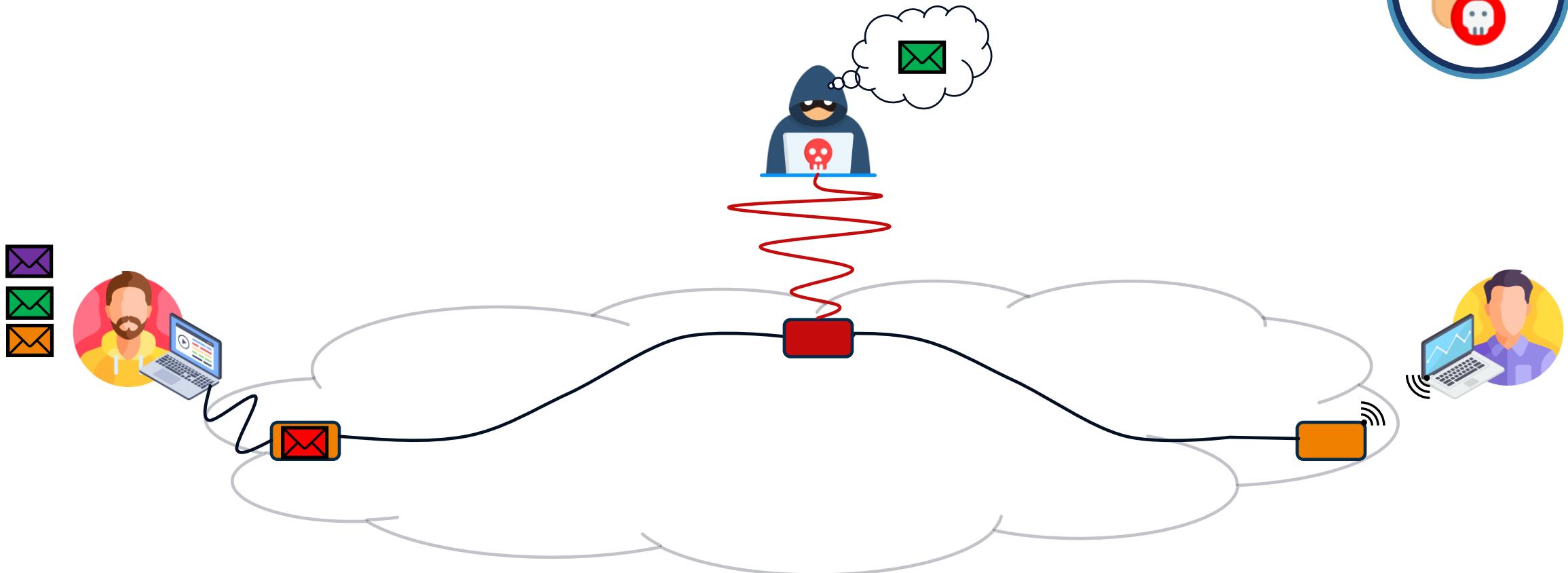
ÉCOUTE CLANDESTINE



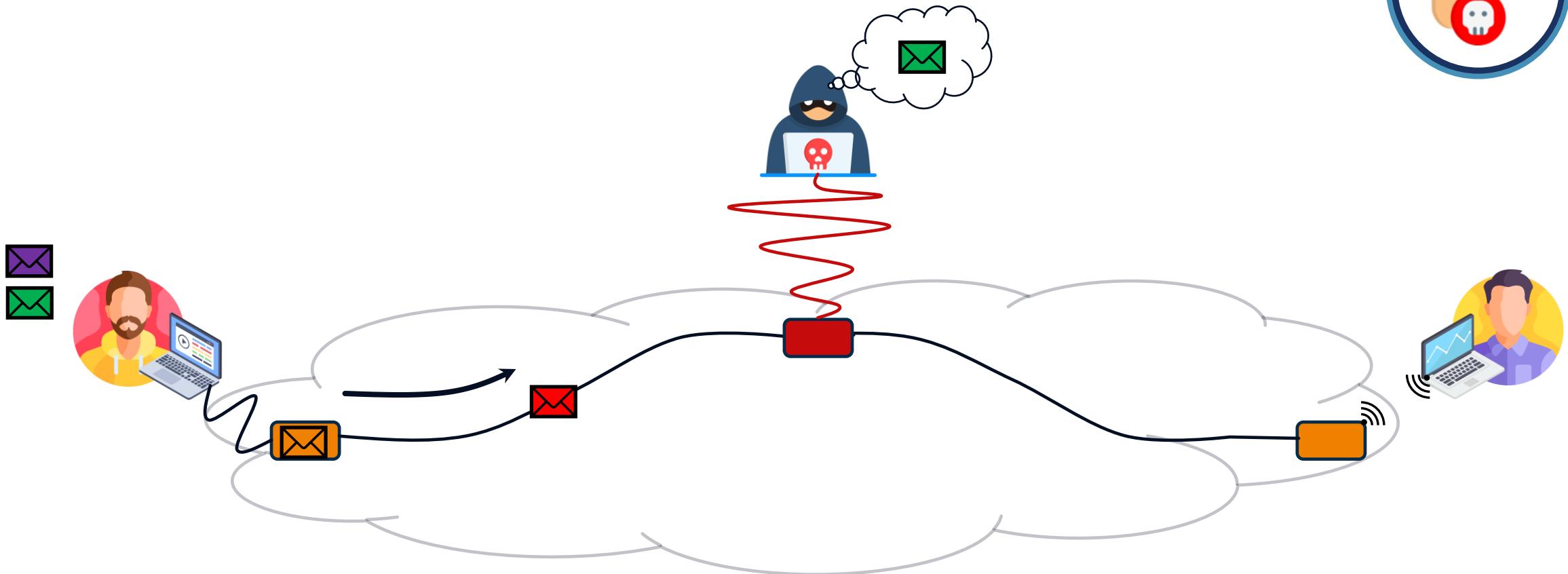
ÉCOUTE CLANDESTINE



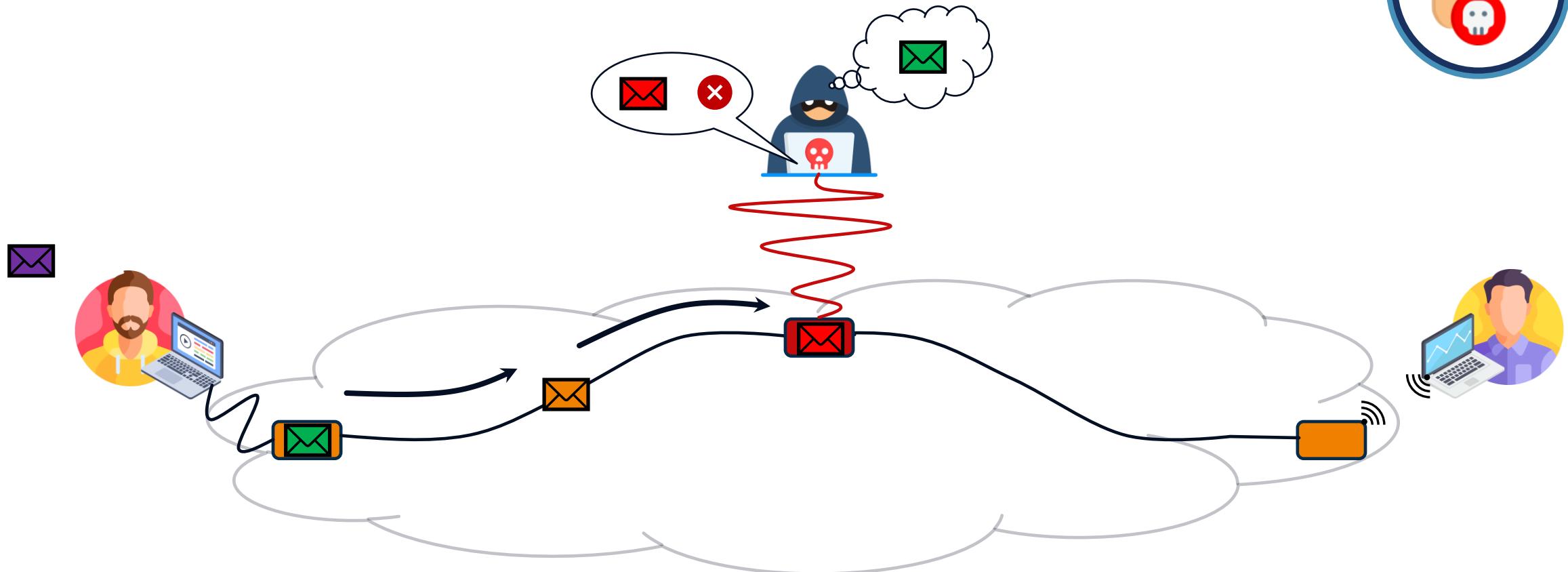
ÉCOUTE CLANDESTINE



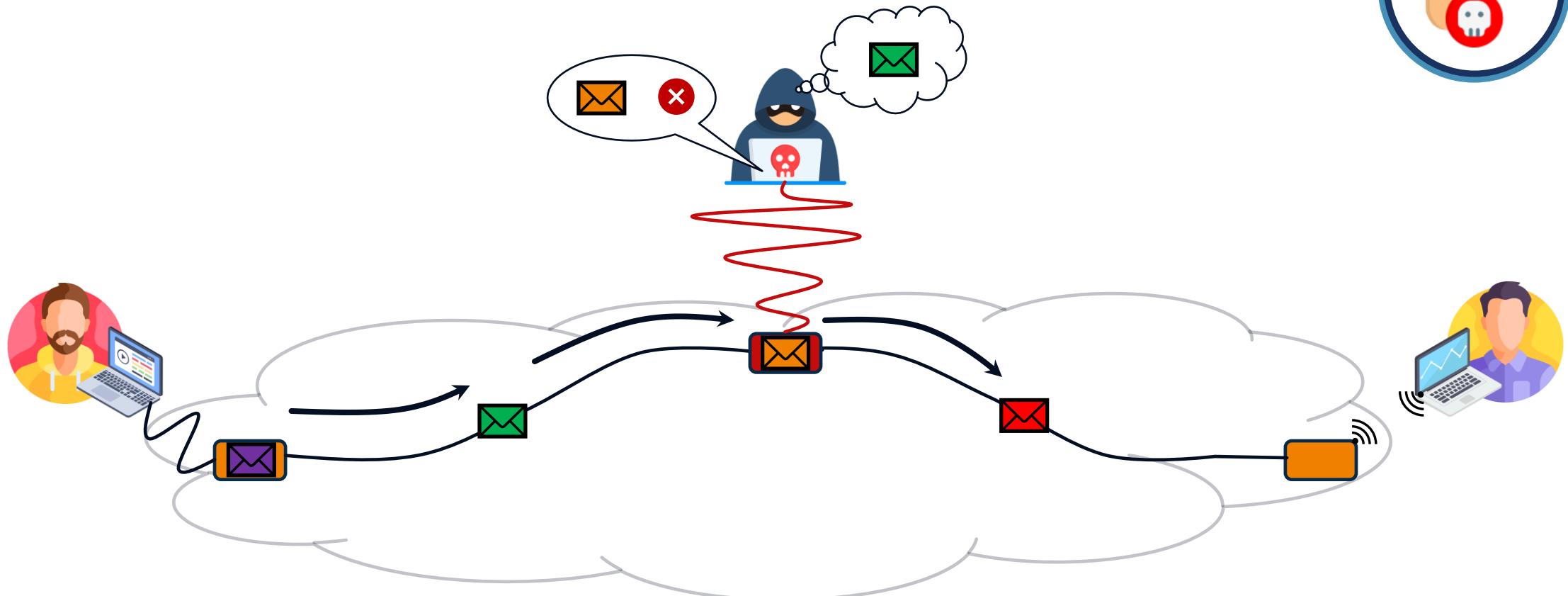
ÉCOUTE CLANDESTINE



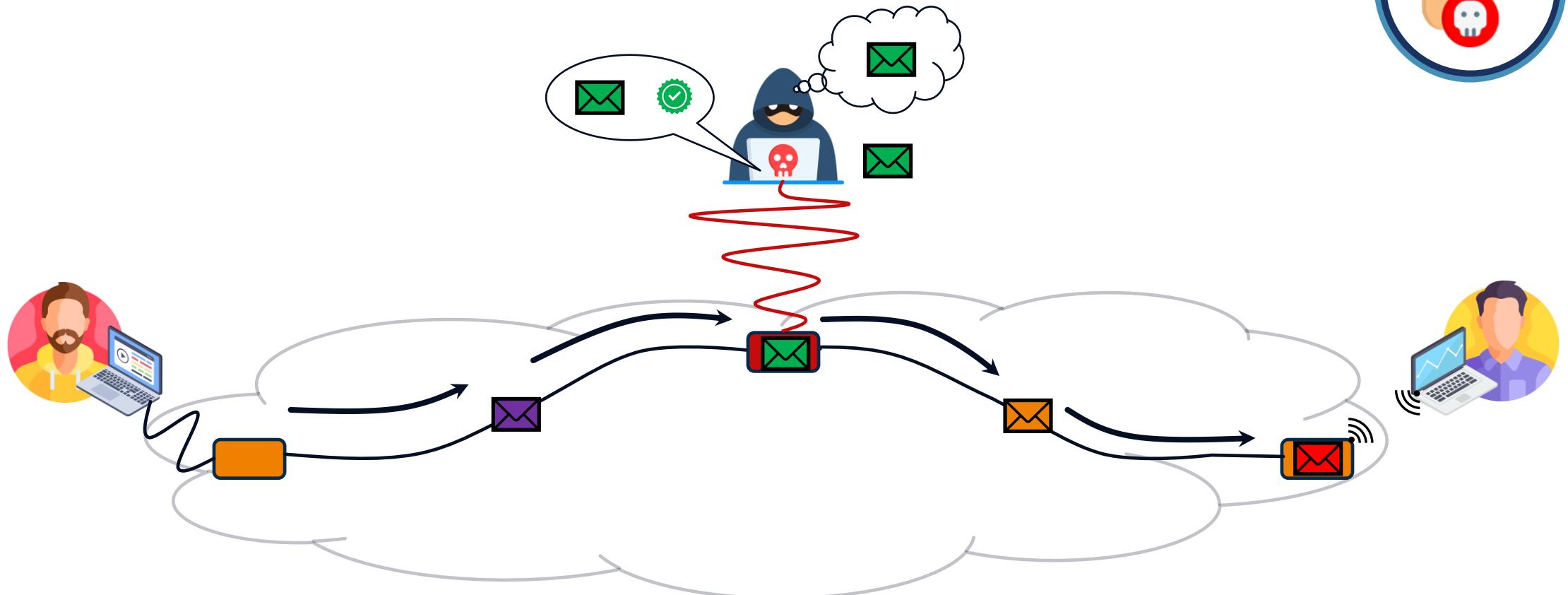
ÉCOUTE CLANDESTINE



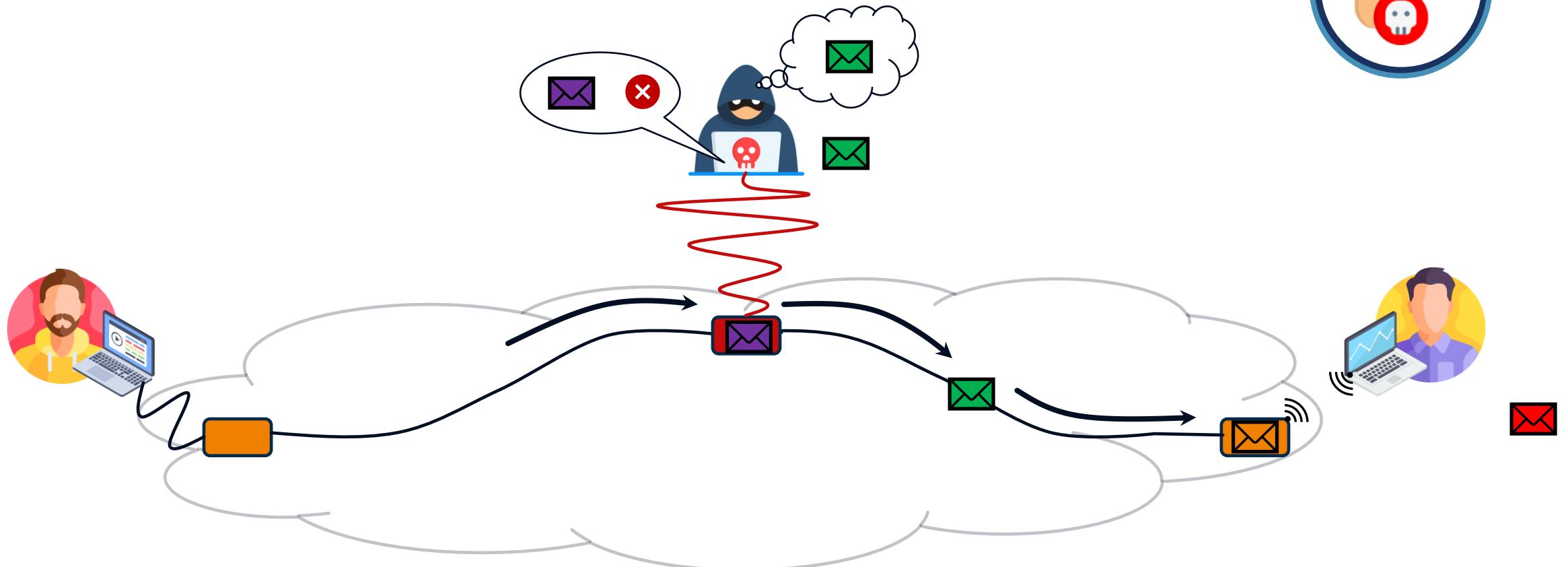
ÉCOUTE CLANDESTINE



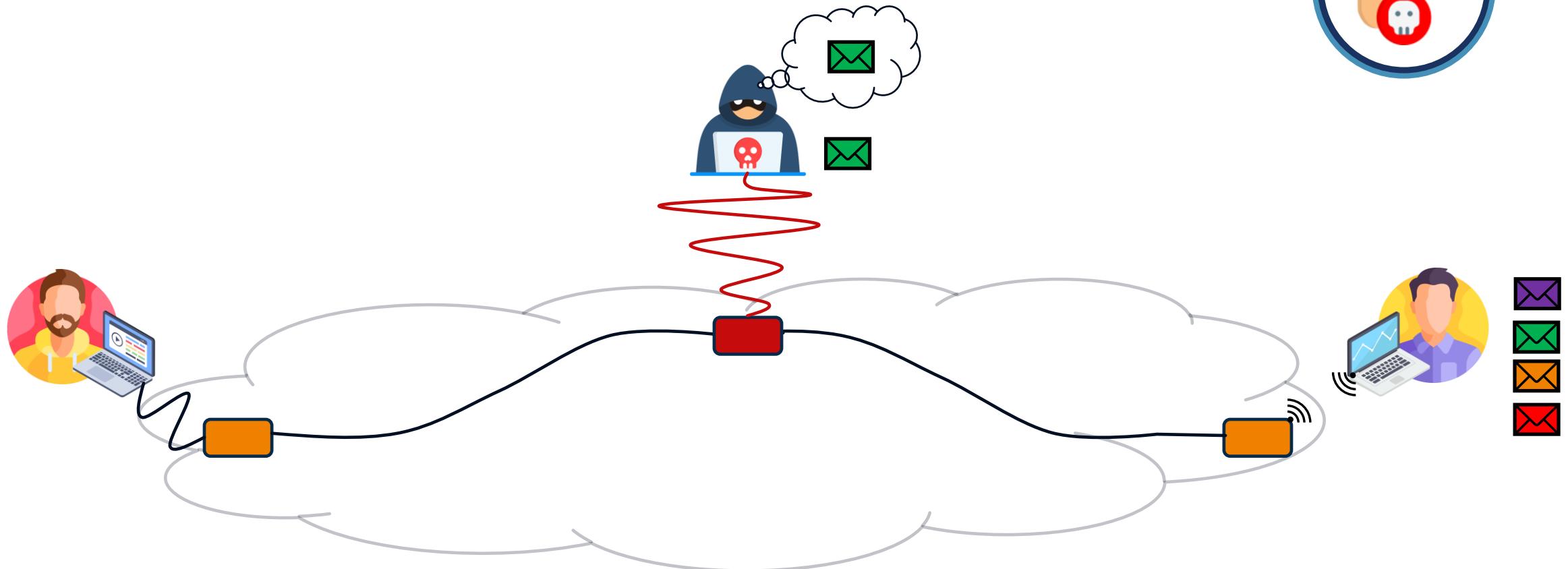
ÉCOUTE CLANDESTINE



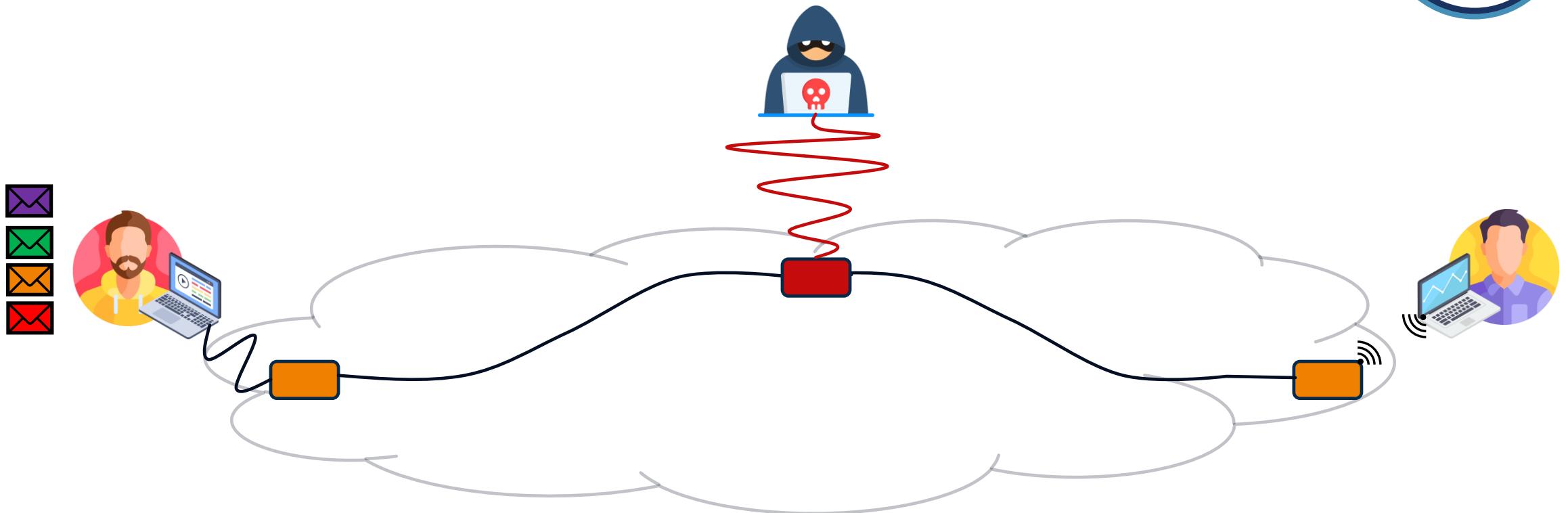
ÉCOUTE CLANDESTINE



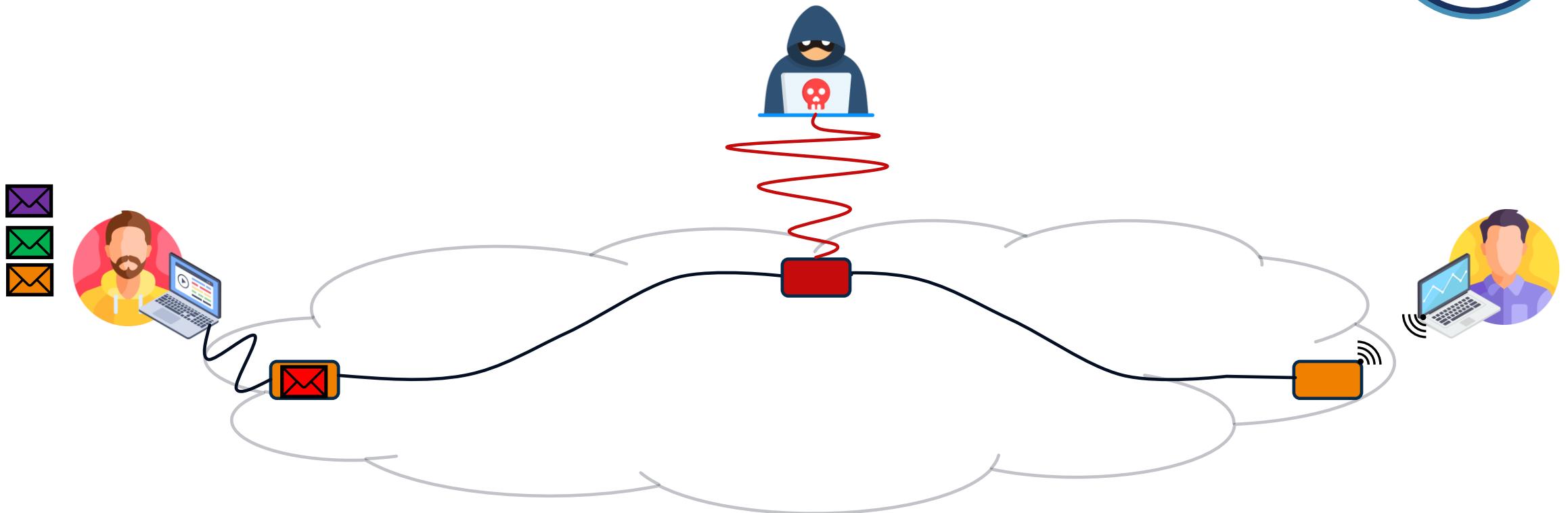
ÉCOUTE CLANDESTINE



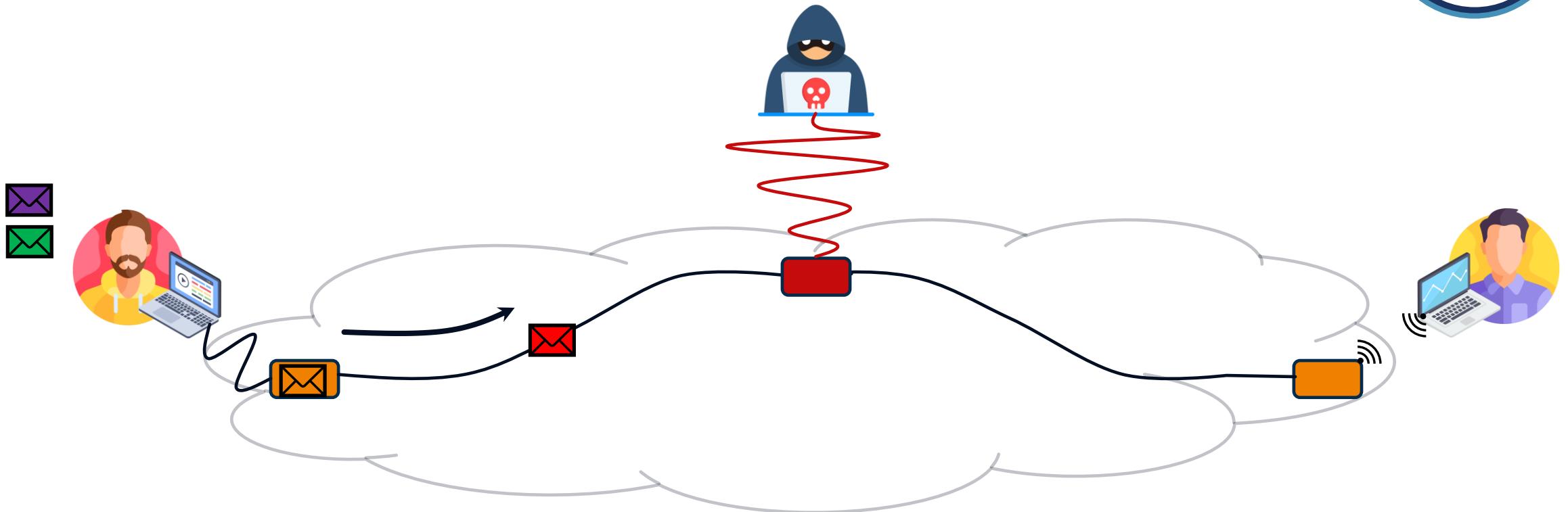
DISTINCTION « SNOOPING »



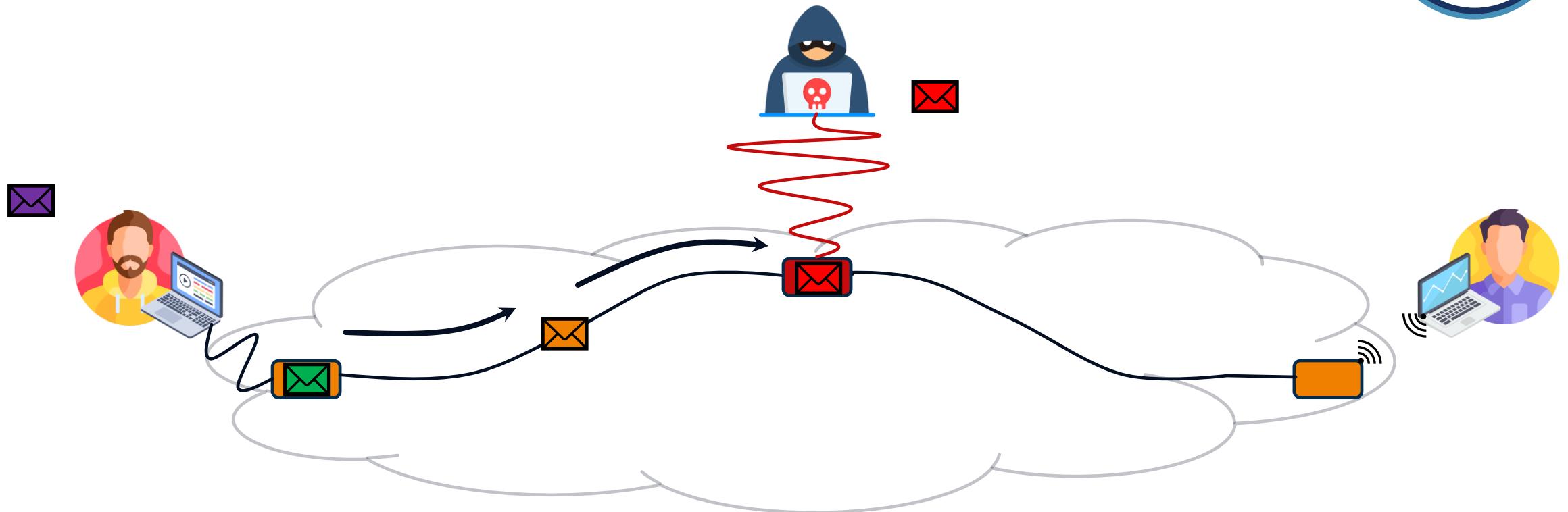
DISTINCTION « SNOOPING »



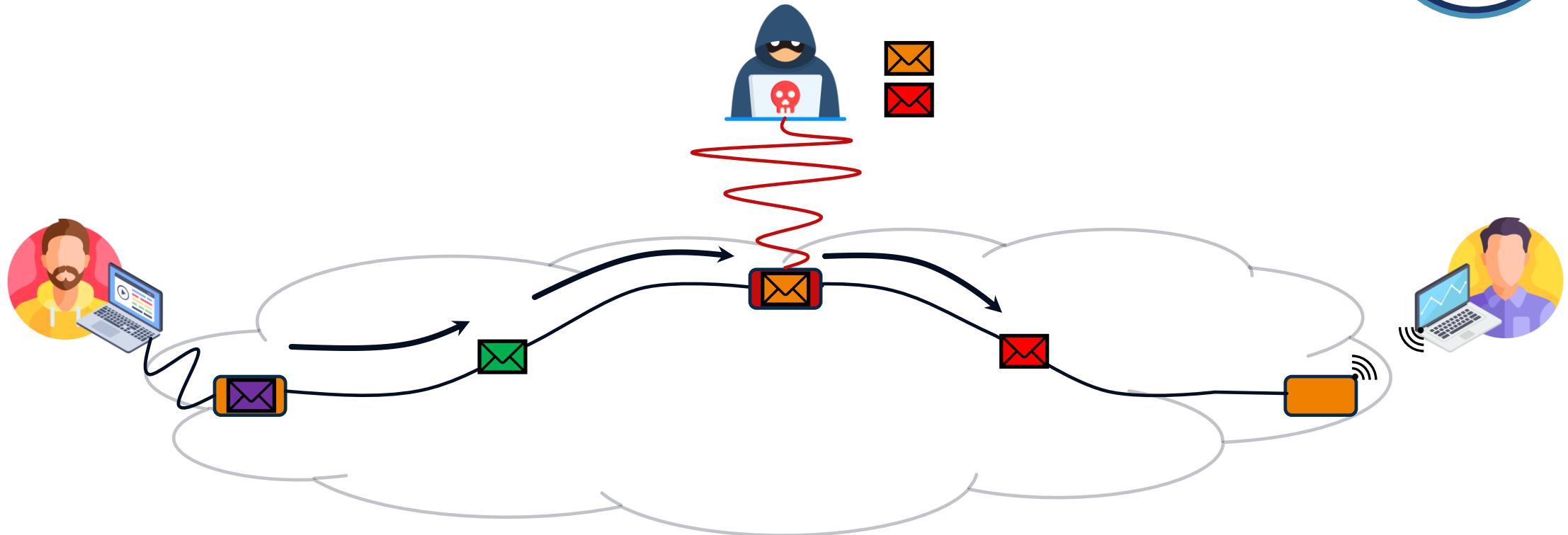
DISTINCTION « SNOOPING »



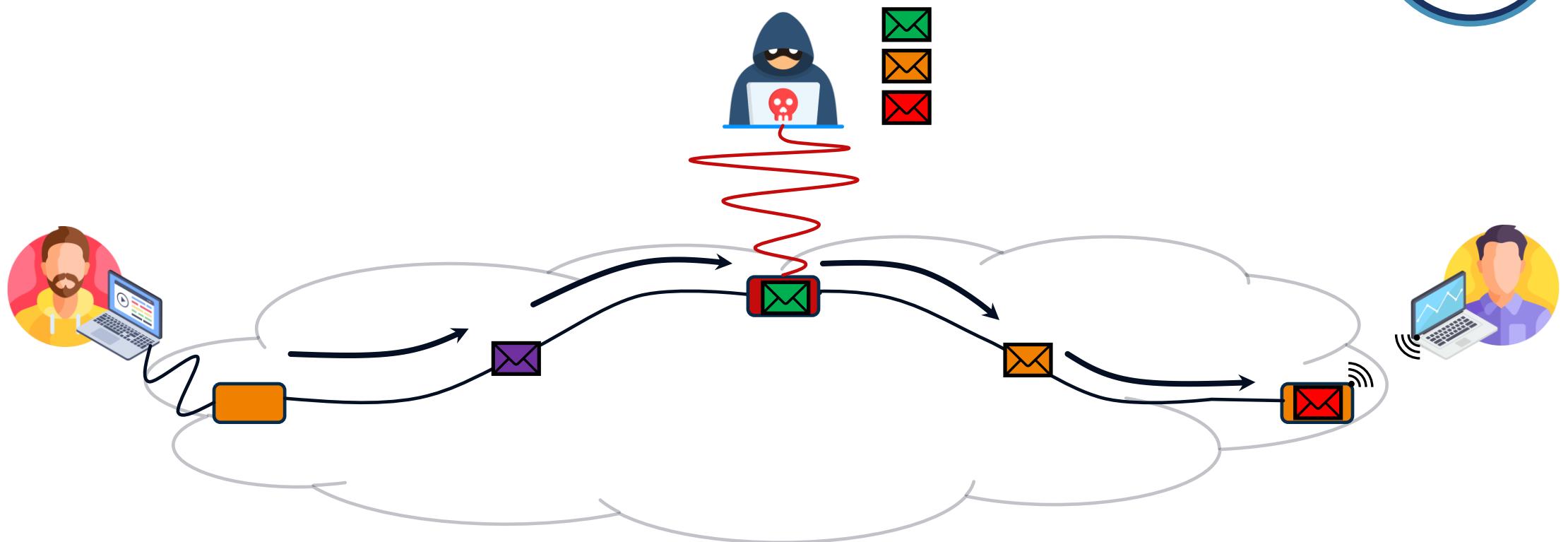
DISTINCTION « SNOOPING »



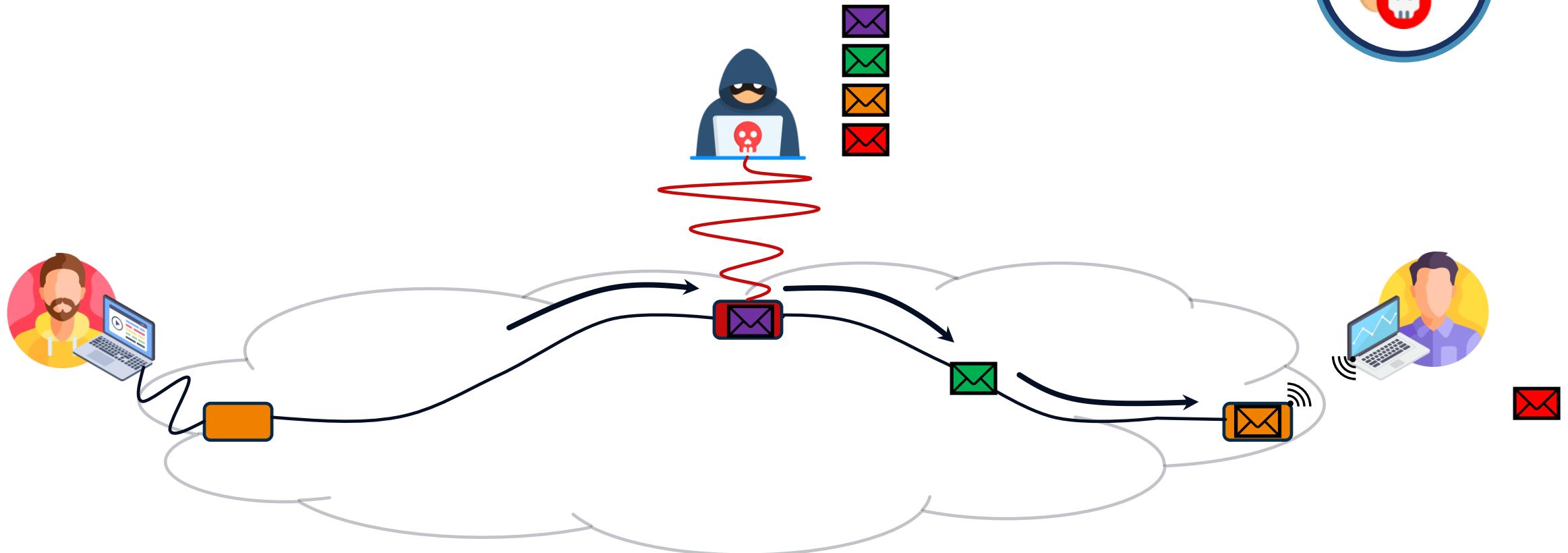
DISTINCTION « SNOOPING »



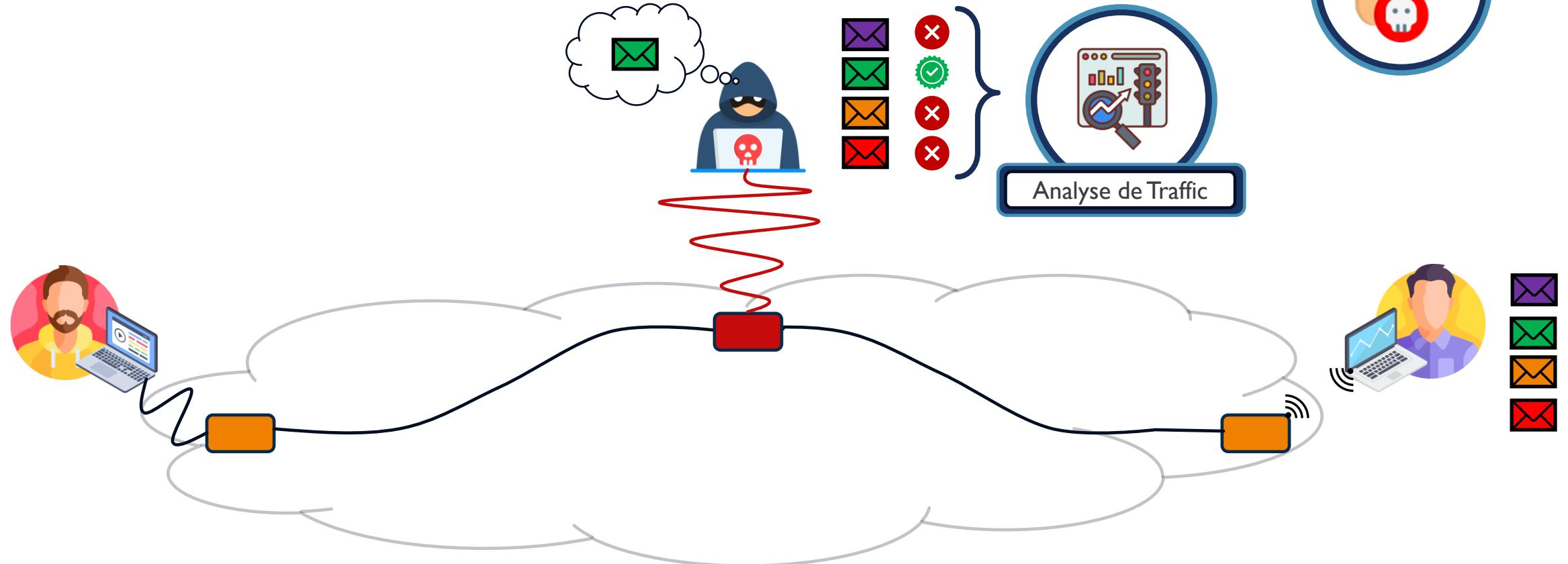
DISTINCTION « SNOOPING »



DISTINCTION « SNOOPING »



DISTINCTION « SNOOPING »



ANALYSE DETRAFFIC

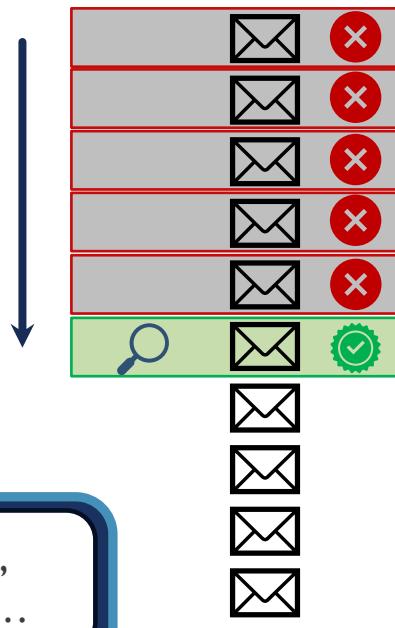


Observation et analyse des communication réseau

- Faite à partir de données capturés (« Snooping »)
- Recherche d'éléments particuliers
 - Extraction de logins et mdp
- Analyse comportementale
 - Analyse statistique des communications
 - Permet de construire un « profile d'utilisateur »
- Fourni une compréhension des activités, envies, vie personnelle d'un utilisateur



TCPDump, Wireshark,
Analyse statistique, etc...



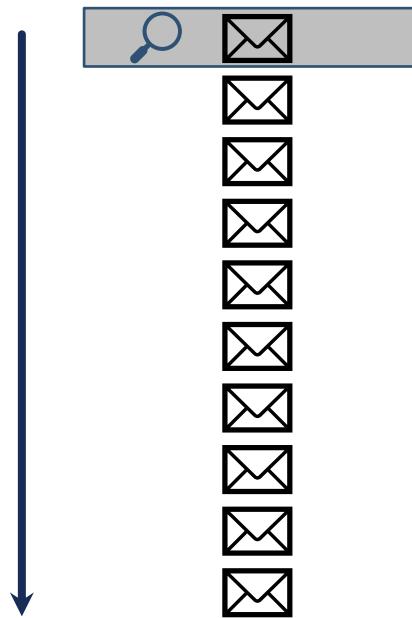
Traffic Analysis



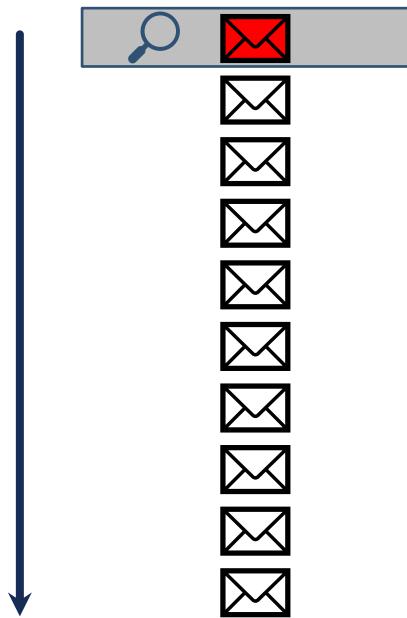
ANALYSE DE TRAFFIC



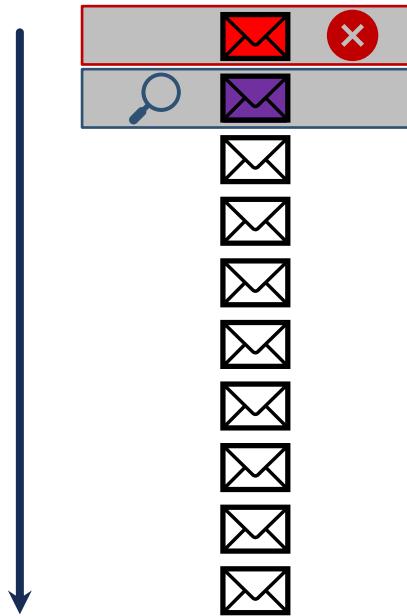
ANALYSE DE TRAFFIC



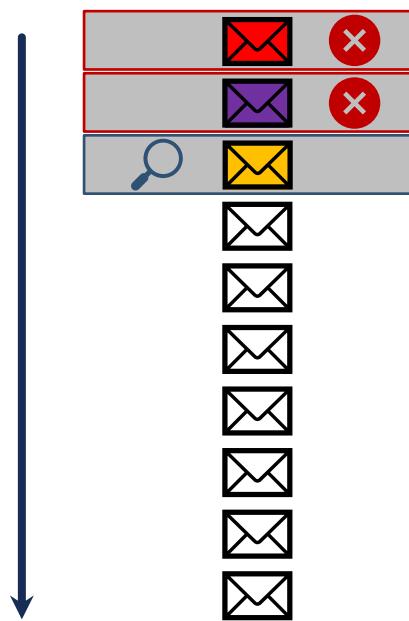
ANALYSE DE TRAFFIC



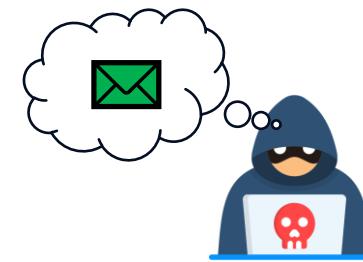
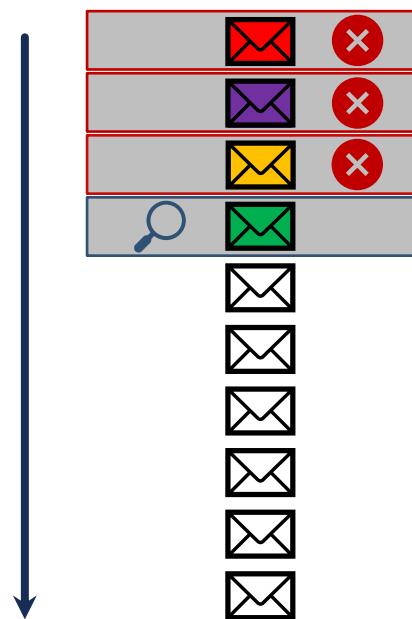
ANALYSE DETRAFFIC



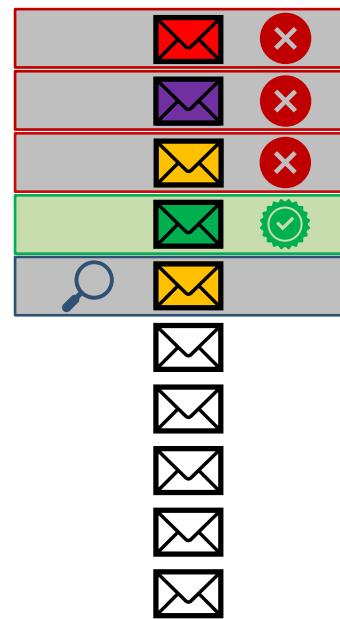
ANALYSE DETRAFFIC



ANALYSE DETRAFFIC



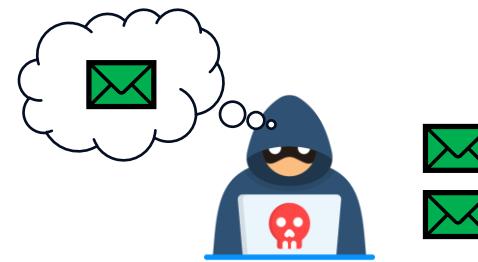
ANALYSE DE TRAFFIC



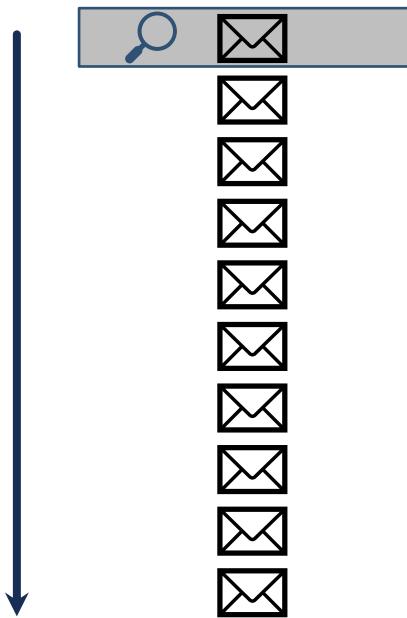
ANALYSE DETRAFFIC



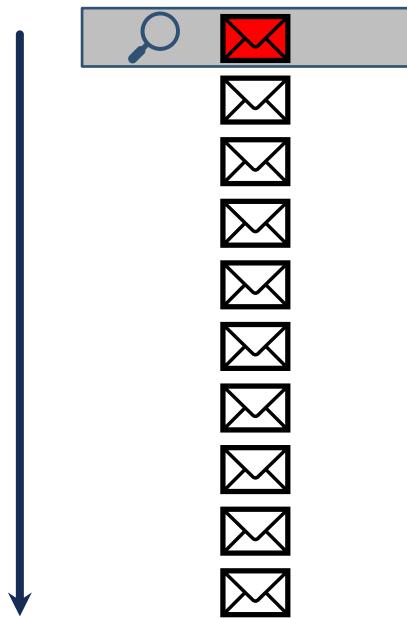
✉️	✗
✉️	✗
✉️	✗
✉️	✓
✉️	✗
✉️	✗
✉️	✗
✉️	✗
✉️	✓



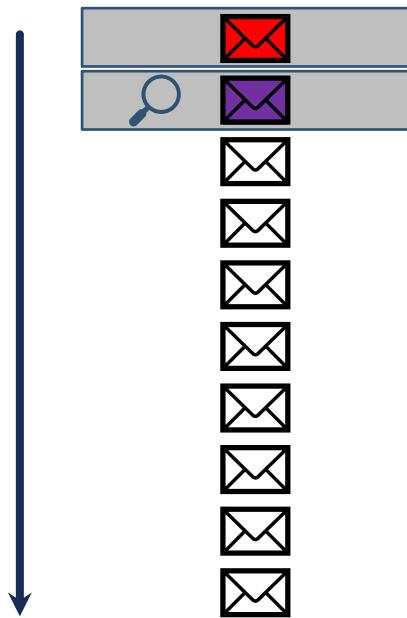
ANALYSE DE TRAFFIC



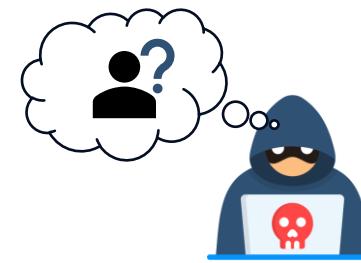
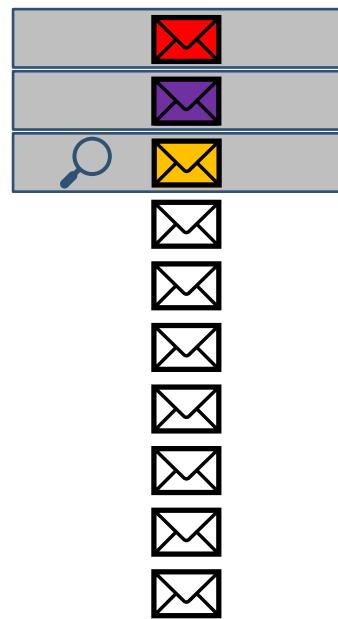
ANALYSE DE TRAFFIC



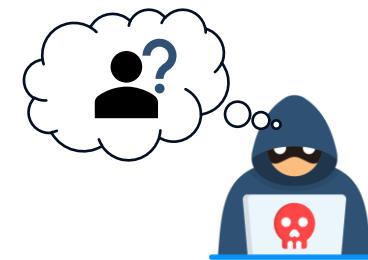
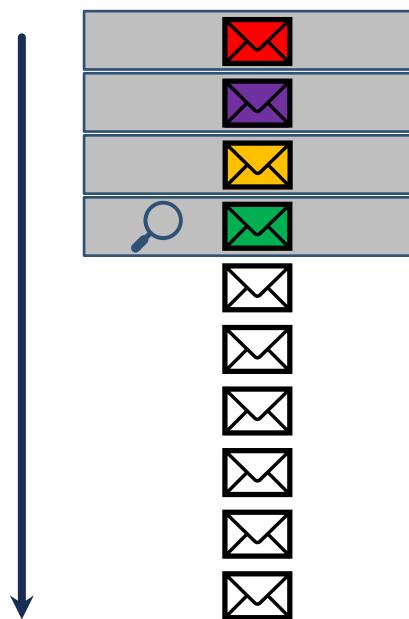
ANALYSE DE TRAFFIC



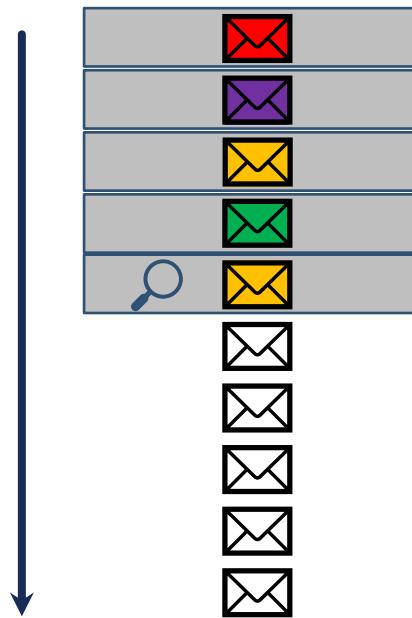
ANALYSE DE TRAFFIC



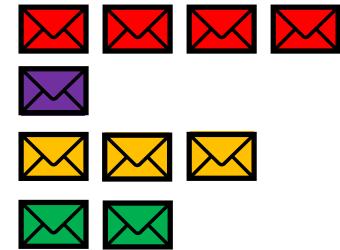
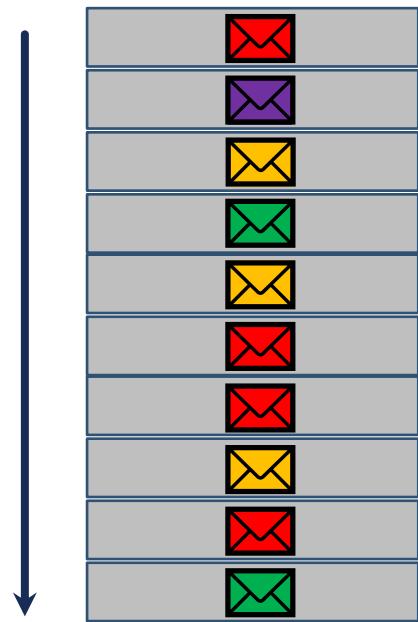
ANALYSE DE TRAFFIC



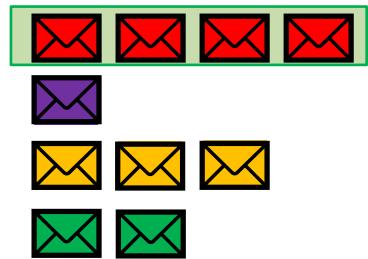
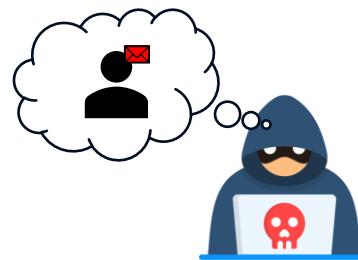
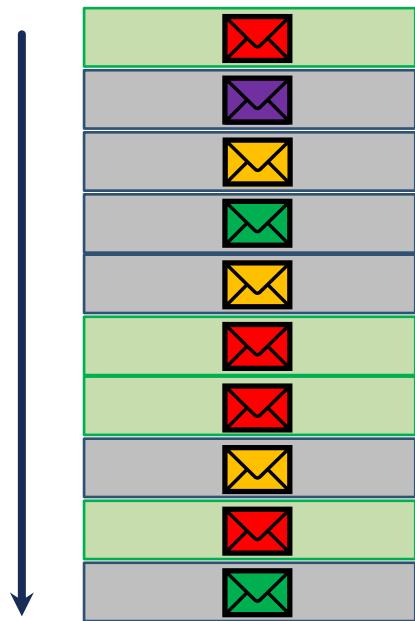
ANALYSE DE TRAFFIC



ANALYSE DETRAFFIC



ANALYSE DETRAFFIC

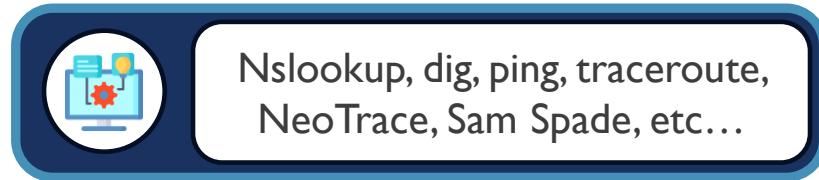


EMPREINTES

Observer et apprendre le maximum d'informations sur a cible

- **Équipements** → système, réseau, OS
- **Fonctionnement réseau** → IP, DNS, pare-feu, ports, etc...
- **Employés** → logiciels, noms d'utilisateur, mdp, numéro d'employé, etc...

- Plusieurs approches possibles
 - **Requêtes DNS, requêtes réseau, scan de port, balayage ping, etc...**



EMPREINTES – REQUÊTES DNS



- Interroger les nameservers DNS
 - Identifier les autorités sur les domaines des cibles
- Interroger les nameserveurs cibles
 - Mail
 - Nameserver, CNAME
 - IPv4, IPv6



Nslookup, Dig
Who.is

```
staddon@pc-mna-68:~$ nslookup -type=ns iutvannes.fr
Server:      193.52.48.66
Address:     193.52.48.66#53

Non-authoritative answer:
iutvannes.fr      nameserver = ns-31-c.gandi.net.
iutvannes.fr      nameserver = ns-242-b.gandi.net.
iutvannes.fr      nameserver = ns-24-a.gandi.net.

Authoritative answers can be found from:
ns-31-c.gandi.net      internet address = 217.70.187.32
ns-24-a.gandi.net      internet address = 173.246.100.25
ns-242-b.gandi.net      internet address = 213.167.230.243
ns-31-c.gandi.net      has AAAA address 2604:3400:aaac::20
ns-24-a.gandi.net      has AAAA address 2001:4b98:aaaa::19
ns-242-b.gandi.net      has AAAA address 2001:4b98:aaab::f3
```

```
staddon@pc-mna-68:~$ dig iutvannes.fr NS
; <>> DiG 9.18.28-1~deb12u2-Debian <>> iutvannes.fr NS
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38877
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 7
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 9149923767b54b331a85804866ec2fec4c92cf50dad13fb0 (good)
;; QUESTION SECTION:
;iutvannes.fr.           IN      NS

;; ANSWER SECTION:
iutvannes.fr.        2735    IN      NS      ns-242-b.gandi.net.
iutvannes.fr.        2735    IN      NS      ns-31-c.gandi.net.
iutvannes.fr.        2735    IN      NS      ns-24-a.gandi.net.

;; ADDITIONAL SECTION:
ns-31-c.gandi.net.   446     IN      A       217.70.187.32
ns-24-a.gandi.net.   446     IN      A       173.246.100.25
ns-242-b.gandi.net.  446     IN      A       213.167.230.243
ns-31-c.gandi.net.   446     IN      AAAA    2604:3400:aaac::20
ns-24-a.gandi.net.   446     IN      AAAA    2001:4b98:aaaa::19
ns-242-b.gandi.net.  446     IN      AAAA    2001:4b98:aaab::f3

;; Query time: 0 msec
;; SERVER: 193.52.48.66#53(193.52.48.66) (UDP)
;; WHEN: Thu Sep 19 16:06:36 CEST 2024
;; MSG SIZE  rcvd: 277
```

EMPREINTES – SCAN DE PORTS



- Evaluer les équipements ciblés
 - Identifier les « trous » dans le pare-feu
 - Avoir une idée des services qui tournent
- Identification de potentiels vulnérabilités
 - Service SSH non sécurisé
 - Service GIT activé mais non utilisé
 - Etc...



nmap

```
staddon@pc-mna-68:~$ sudo nmap www.iutvannes.fr
Starting Nmap 7.93 ( https://nmap.org ) at 2024-09-19 16:29 CEST
Nmap scan report for www.iutvannes.fr (188.165.155.194)
Host is up (0.014s latency).
rDNS record for 188.165.155.194: ns-serge.id-interactive.fr
Not shown: 973 filtered tcp ports (no-response), 5 filtered tcp ports (admin-prohibited)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
110/tcp   closed pop3
119/tcp   closed nntp
143/tcp   closed imap
443/tcp   open  https
587/tcp   closed submission
873/tcp   closed rsync
993/tcp   closed imaps
995/tcp   closed pop3s
1521/tcp  closed oracle
2200/tcp  closed ici
2222/tcp  closed EtherNetIP-1
2401/tcp  closed cvspserver
3333/tcp  closed dec-notes
3389/tcp  closed ms-wbt-server
3690/tcp  closed svn
5432/tcp  closed postgresql
5999/tcp  closed ncd-conf
8443/tcp  closed https-alt
8888/tcp  closed sun-answerbook
9418/tcp  closed git

Nmap done: 1 IP address (1 host up) scanned in 4.29 seconds
```

EMPREINTES – REQUÊTES RÉSEAU



- Evaluer les équipements ciblés
 - Identifier les logiciels, OS
- Identifier et évaluer topologie réseau
 - Identifier nombre de équipements intermédiaires
 - Noms, IP, position
 - Examiner équipements propres à la cible



nmap, ping, traceroute

```
staddon@pc-mna-68:~$ sudo nmap -O -v www.iutvannes.fr
Starting Nmap 7.93 ( https://nmap.org ) at 2024-09-19 16:17 CEST
Initiating Ping Scan at 16:17
Scanning www.iutvannes.fr (188.165.155.194) [4 ports]
Completed Ping Scan at 16:17, 0.05s elapsed (1 total hosts)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.11 - 4.1
Uptime guess: 131.900 days (since Fri May 10 18:41:57 2024)
TCP Sequence Prediction: Difficulty=260 (Good luck!)
IP ID Sequence Generation: All zeros
```

```
staddon@pc-mna-68:~$ sudo traceroute -I www.iutvannes.fr
traceroute to www.iutvannes.fr (188.165.155.194), 30 hops max, 60 byte packets
 1 gw-v55.univ-ubs.fr (172.17.0.249)  0.409 ms  0.388 ms  0.383 ms
 2 fw-ubs-va-x5.univ-ubs.fr (193.52.32.43)  0.234 ms  0.229 ms  0.225 ms
 3 vlan1510-be3-ren-nr-rennes-rtr-091.noc.renater.fr (193.51.176.14)  3.135 ms  3.205 ms  3.319 ms
 4 et-5-2-1-ren-nr-paris1-rtr-131.noc.renater.fr (193.51.177.174)  9.236 ms  9.233 ms  9.228 ms
 5 et-4-0-1-ren-nr-paris2-rtr-131.noc.renater.fr (193.55.204.193)  9.413 ms  9.408 ms  9.404 ms
 6 par-th2-pb3-nc5.fr.eu (57.128.121.26)  10.412 ms  12.300 ms  12.259 ms
 7 * * *
 8 * * *
 9 * * *
10 be103.rbx-g3-nc5.fr.eu (54.36.50.227)  12.947 ms  12.708 ms  12.790 ms
11 * * *
12 * * *
13 * * *
14 ns-serge.id-interactive.fr (188.165.155.194)  20.476 ms  19.396 ms  19.390 ms
```

ESPIONNAGE

Vol d'informations sans être remarqué

- Usurpation d'identité d'un utilisateur légitime
- Vol d'informations de la cible
 - Par accès physique aux locaux
 - Par accès numérique aux systèmes
- Accès physique plus rare
 - Pas facilement détecté
 - Mettre en place **Écoute Clandestine et Analyse de Traffic**



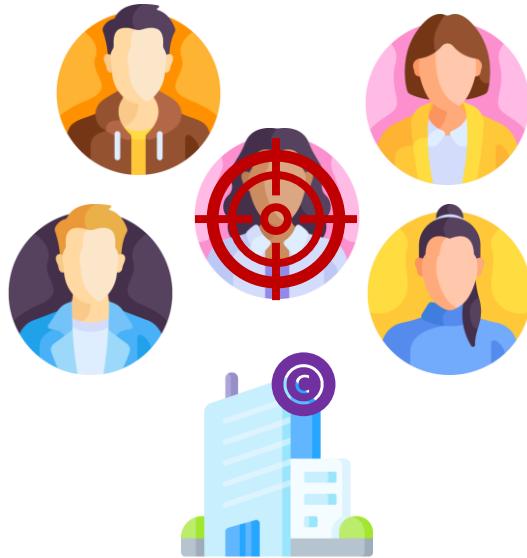
ESPIONNAGE



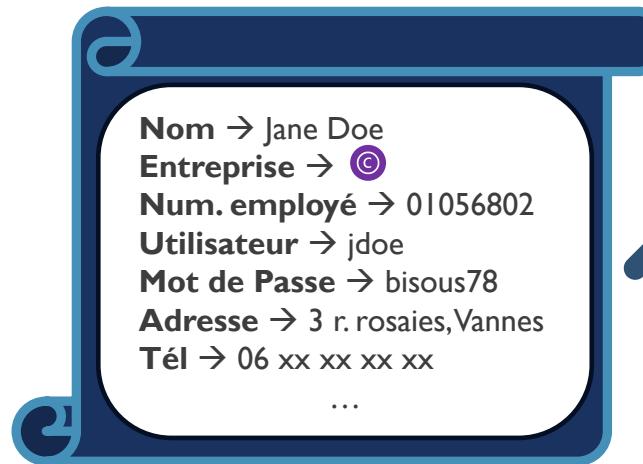
ESPIONNAGE



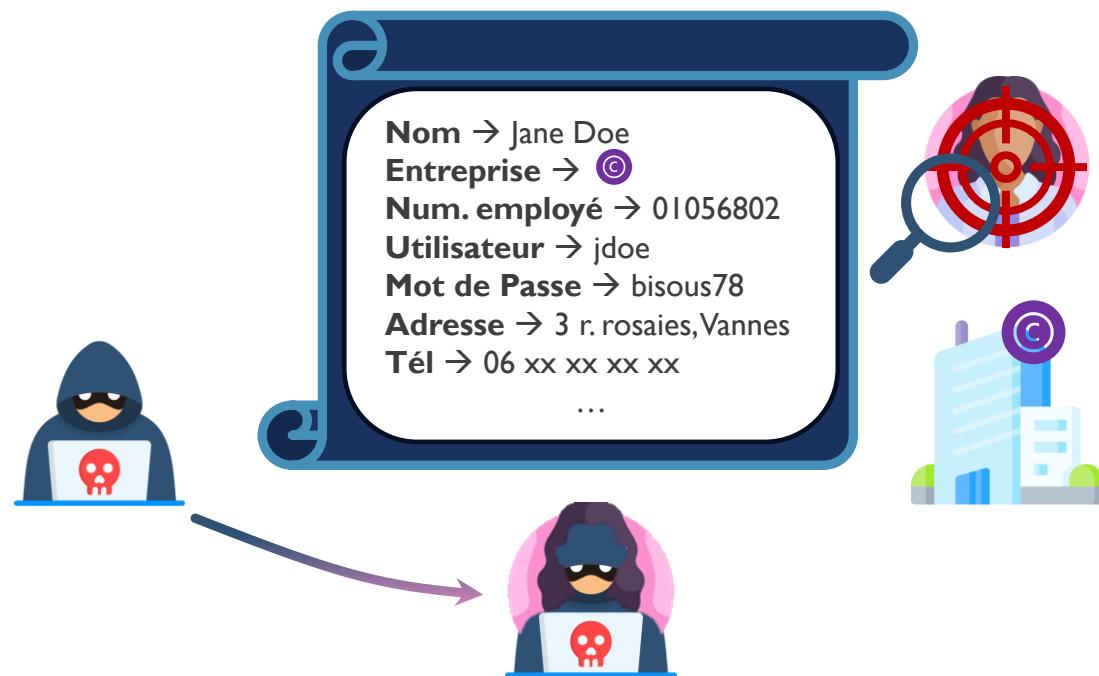
ESPIONNAGE



ESPIONNAGE



ESPIONNAGE



ESPIONNAGE



ESPIONNAGE



1



2

ESPIONNAGE

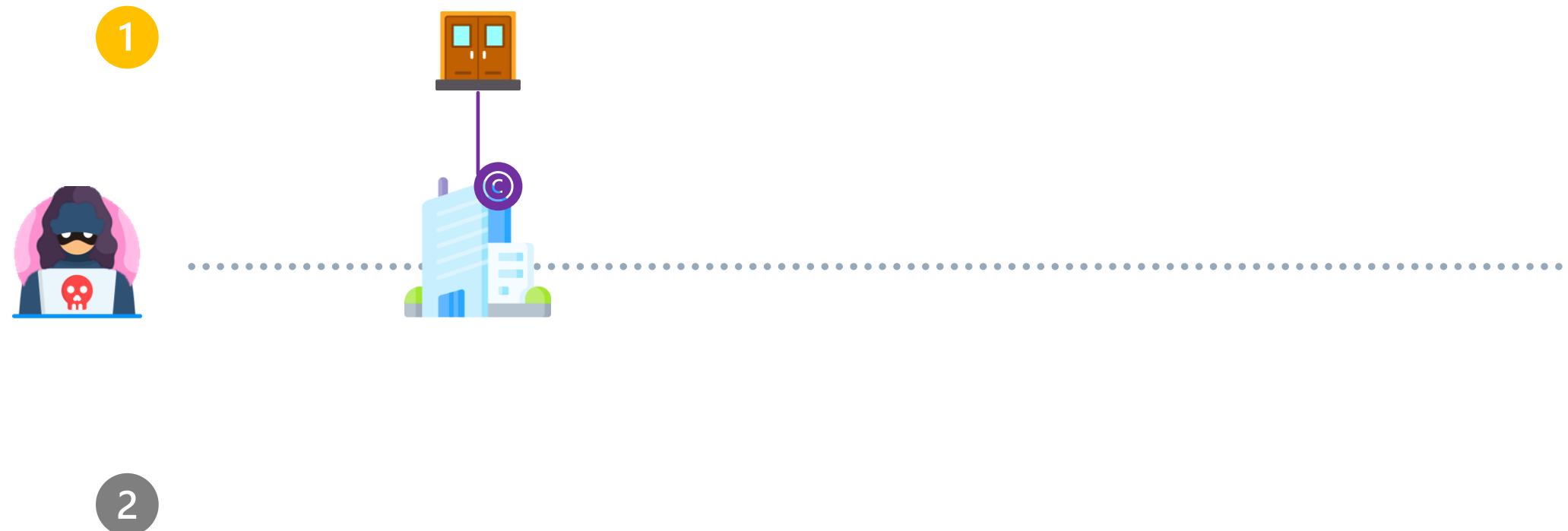


1

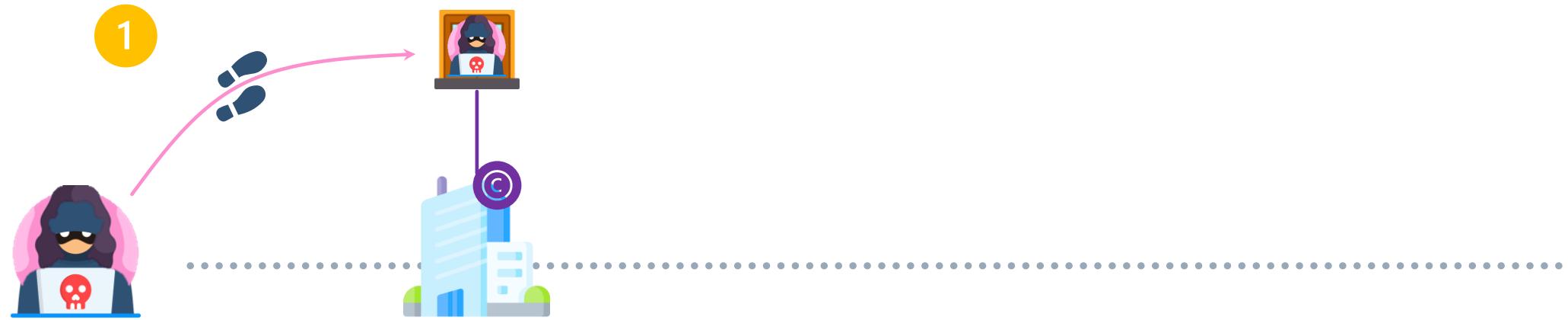


2

ESPIONNAGE



ESPIONNAGE

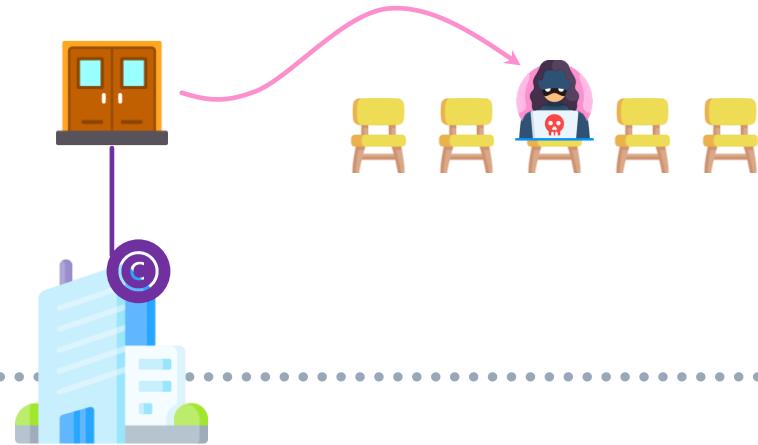


2

ESPIONNAGE

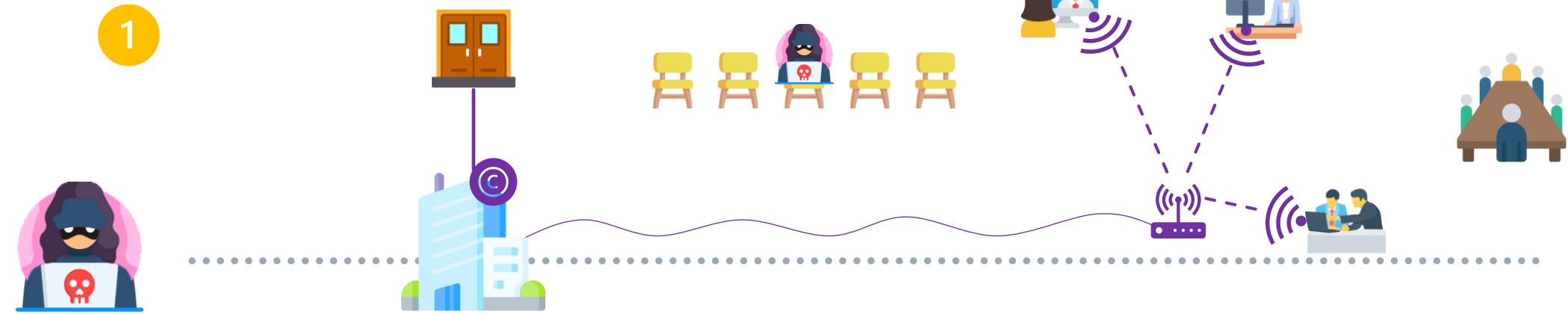


1



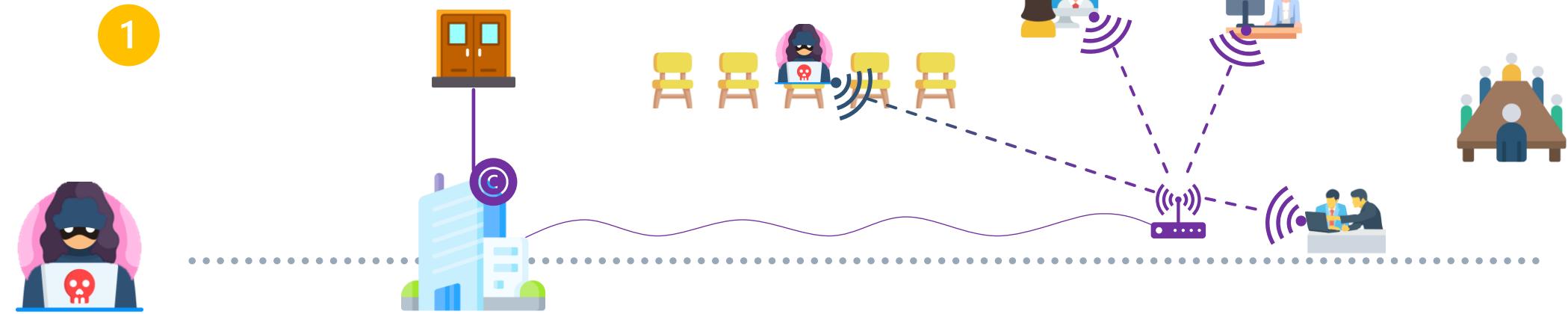
2

ESPIONNAGE

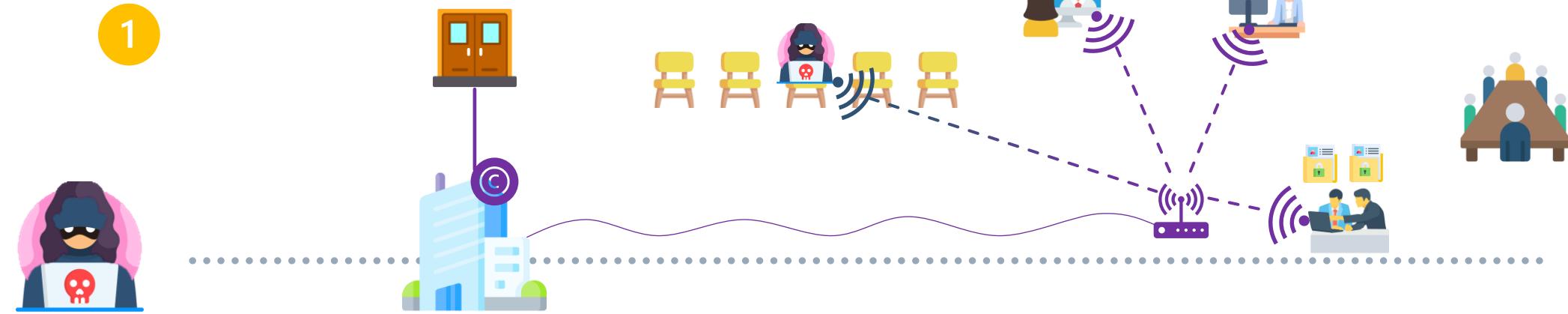


2

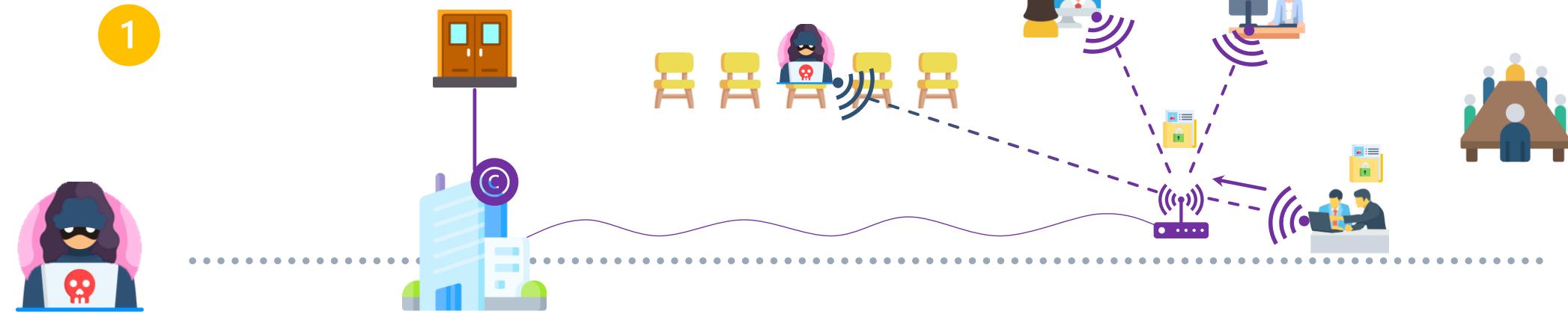
ESPIONNAGE



ESPIONNAGE

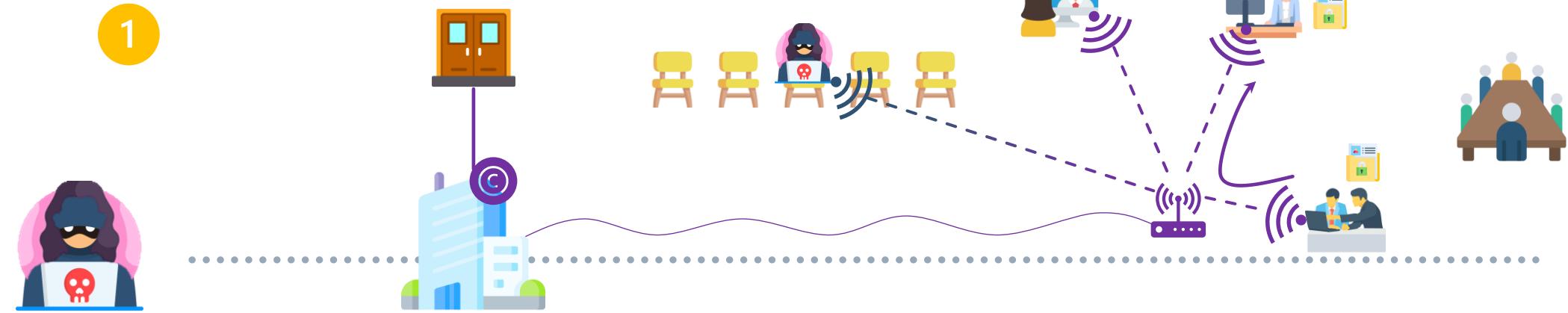


ESPIONNAGE



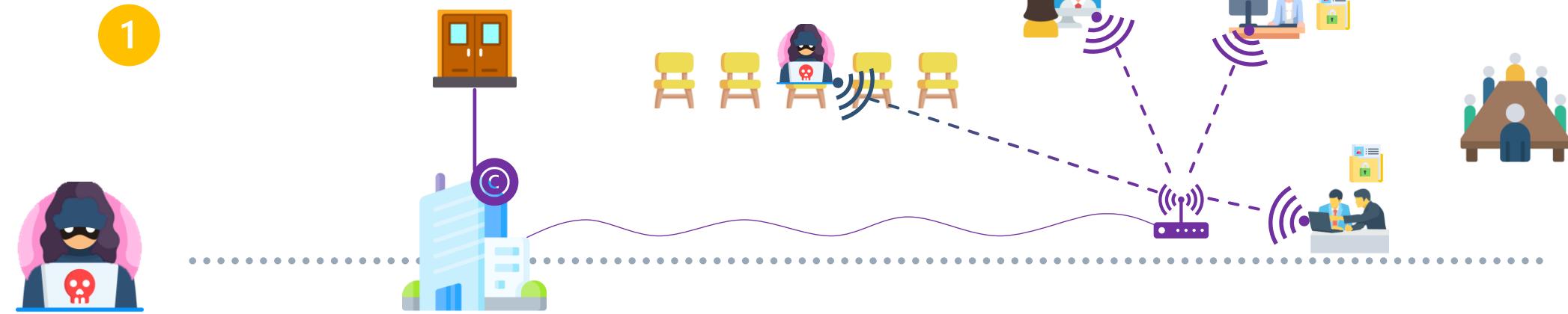
2

ESPIONNAGE



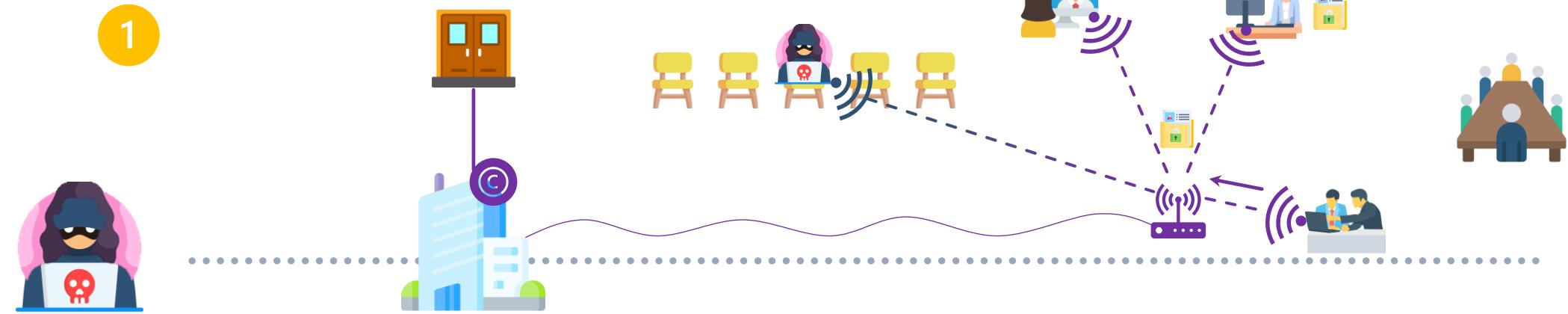
2

ESPIONNAGE



2

ESPIONNAGE

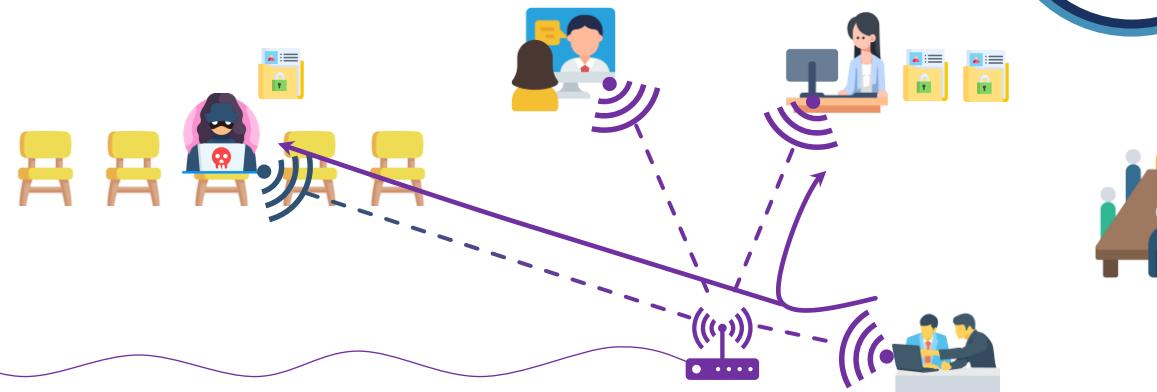


2

ESPIONNAGE

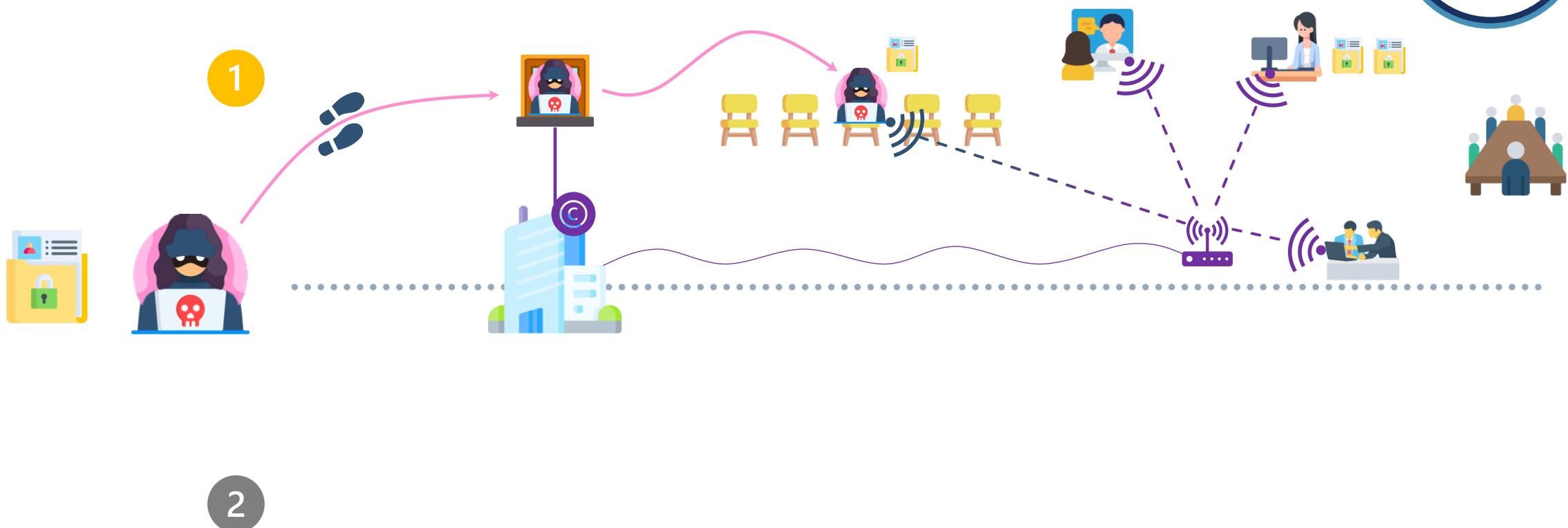


1

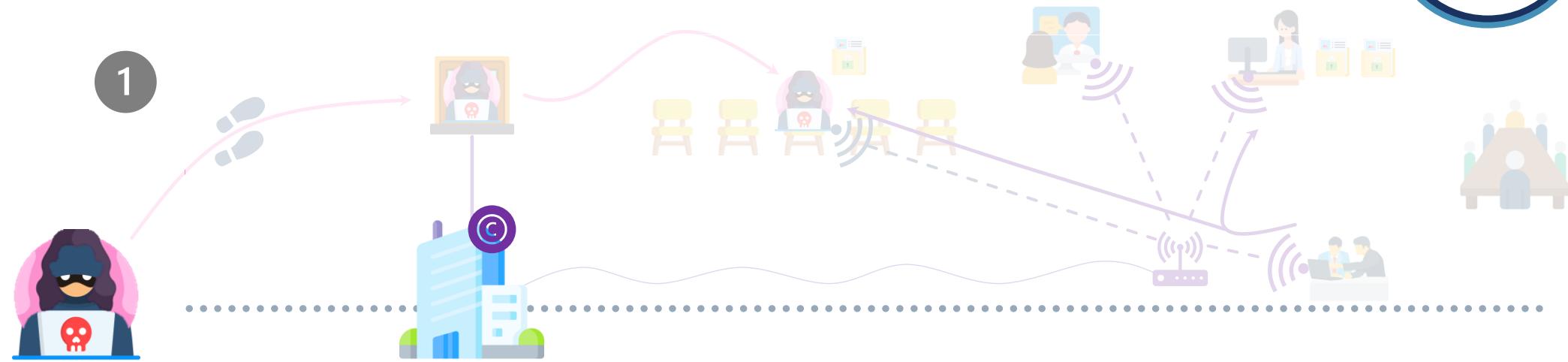


2

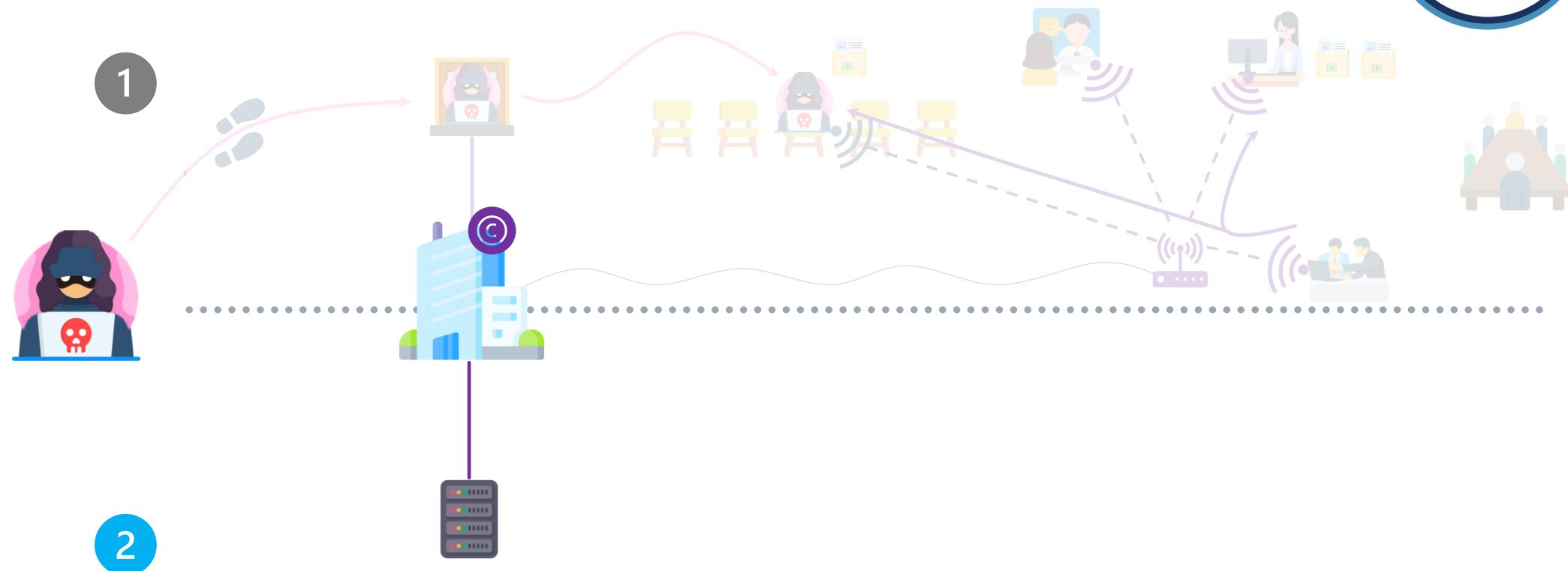
ESPIONNAGE



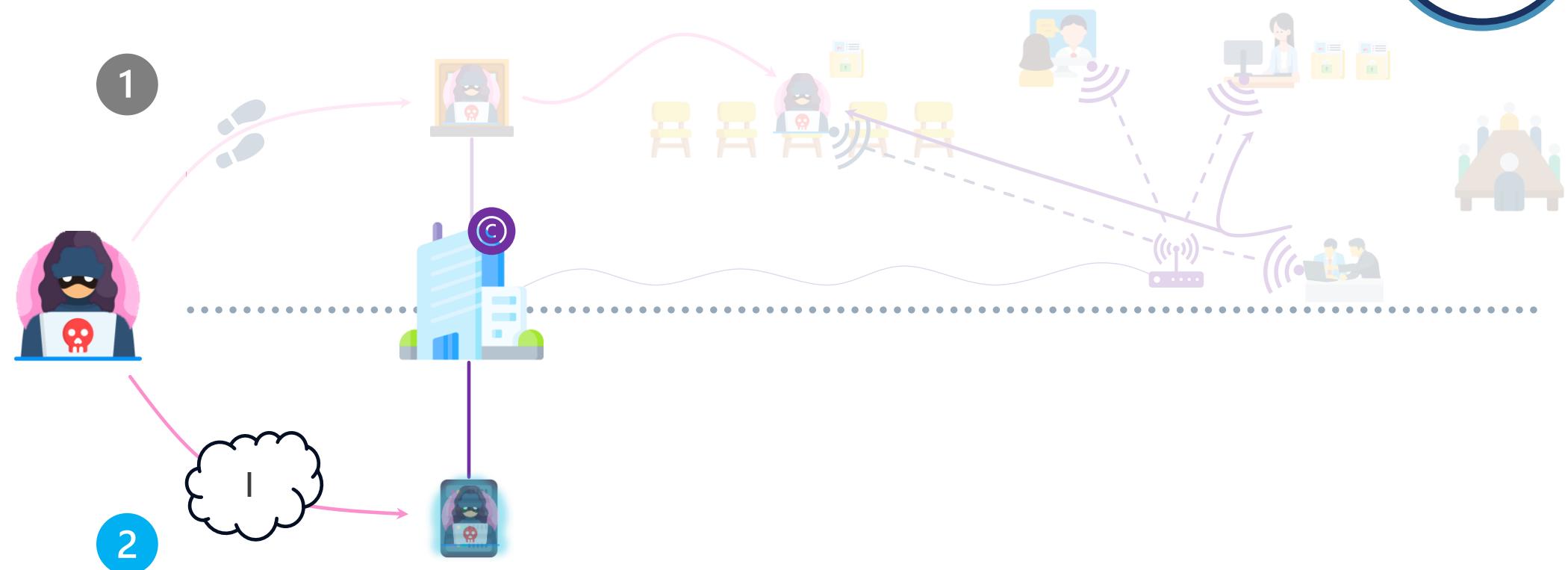
ESPIONNAGE



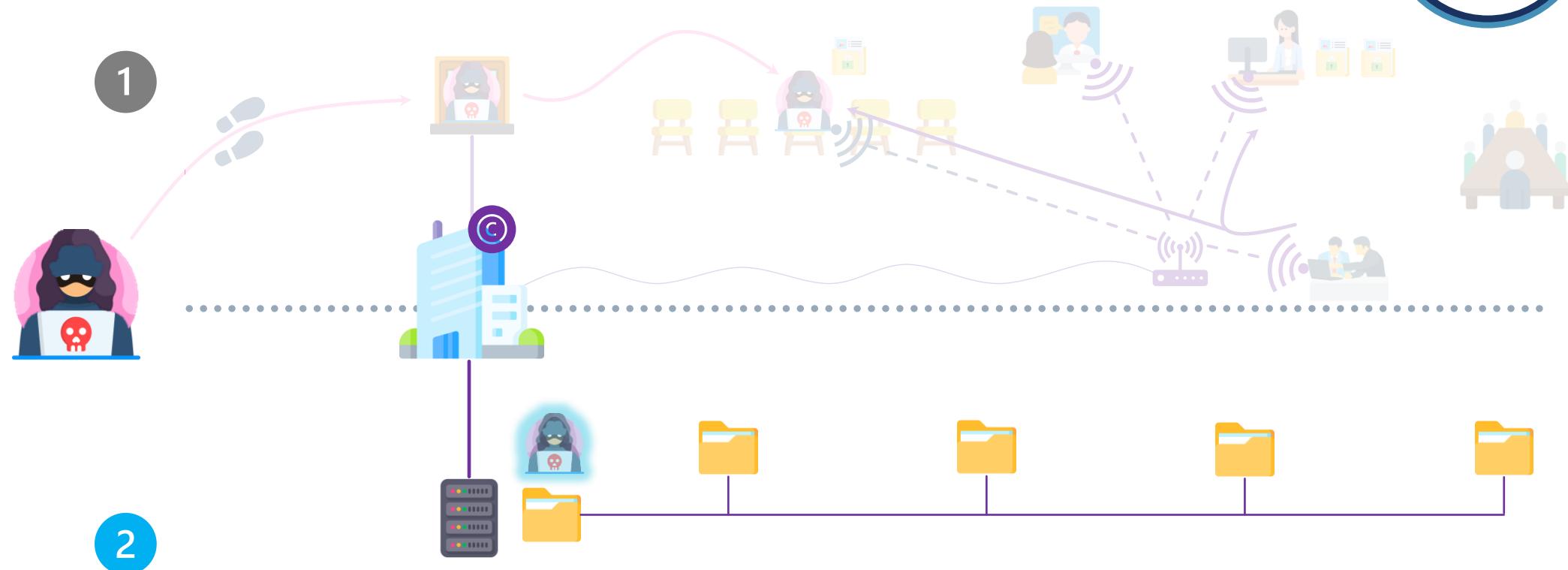
ESPIONNAGE



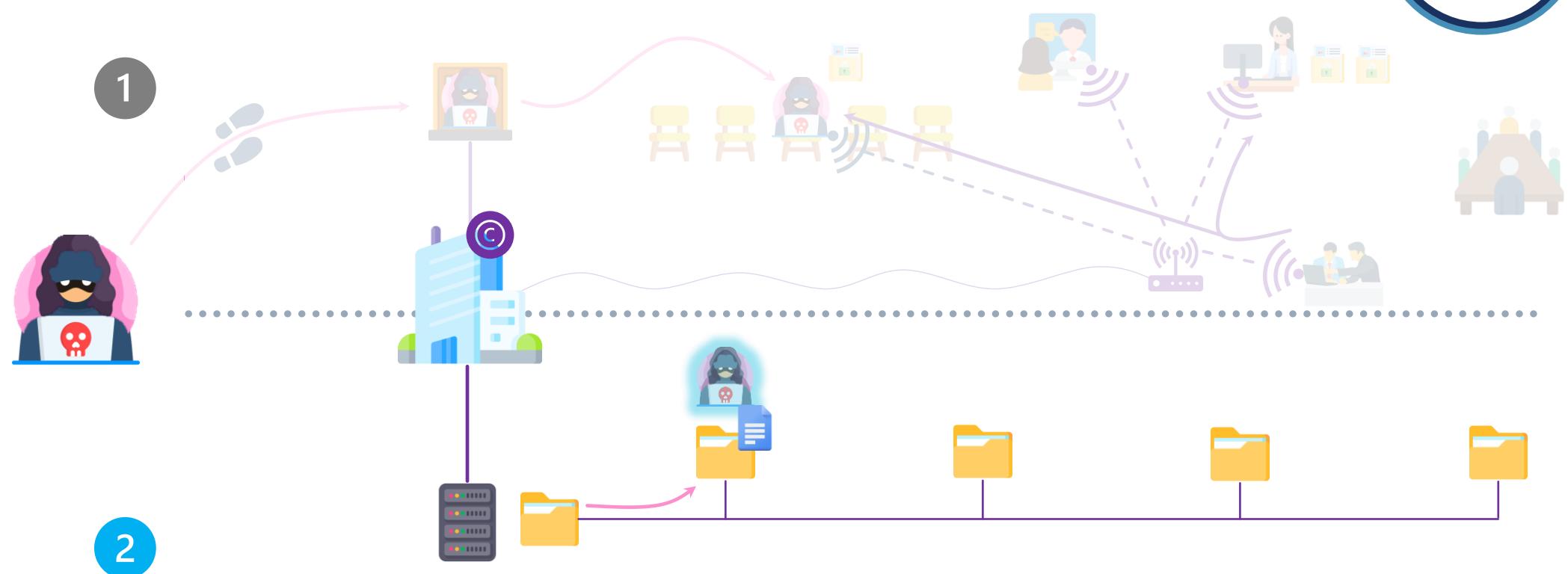
ESPIONNAGE



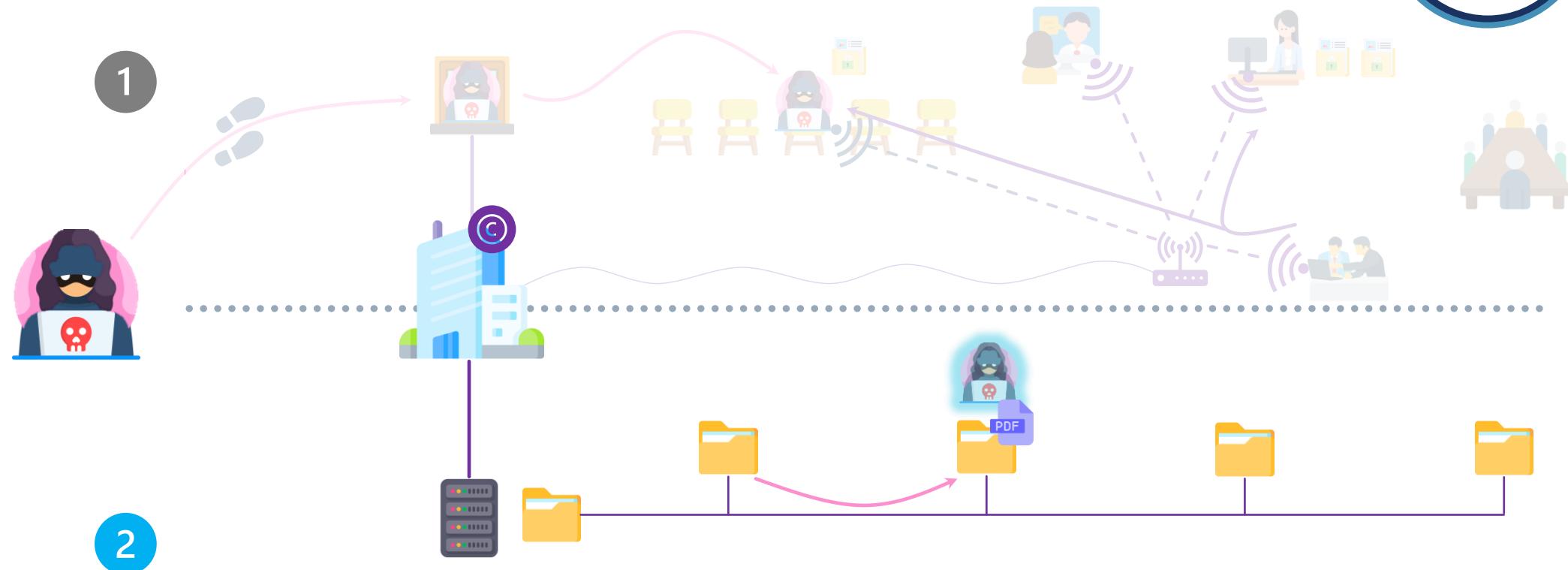
ESPIONNAGE



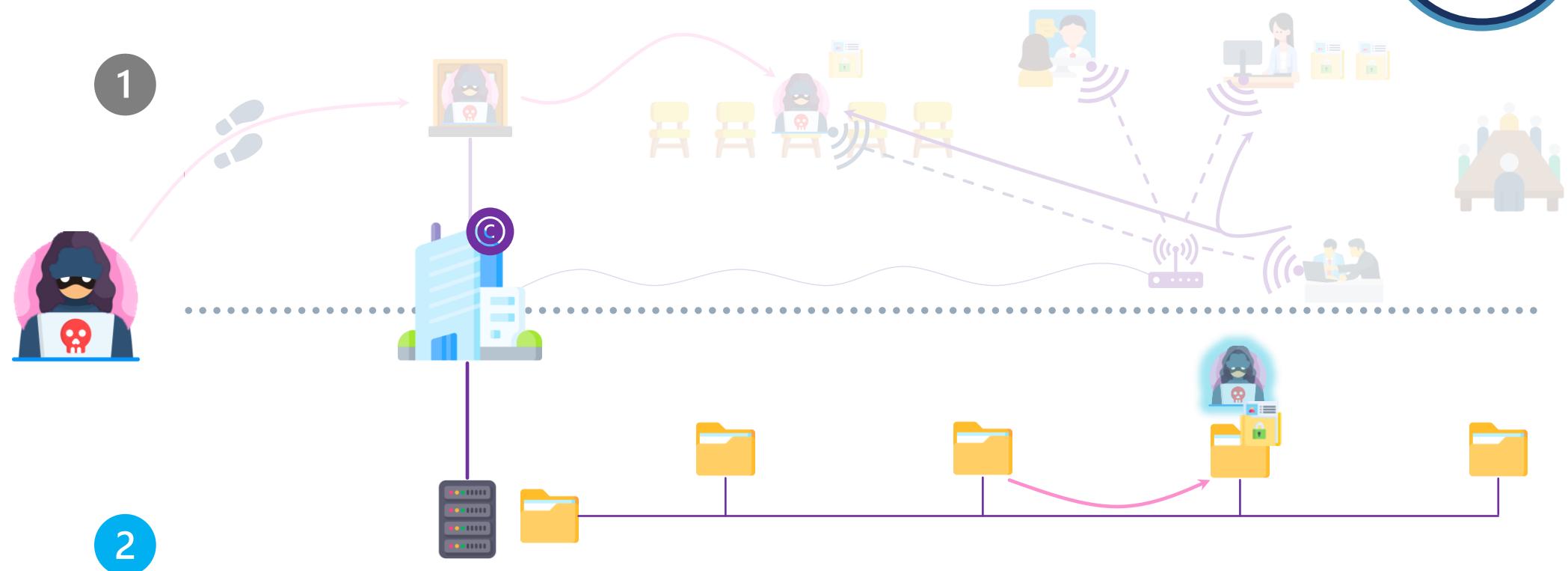
ESPIONNAGE



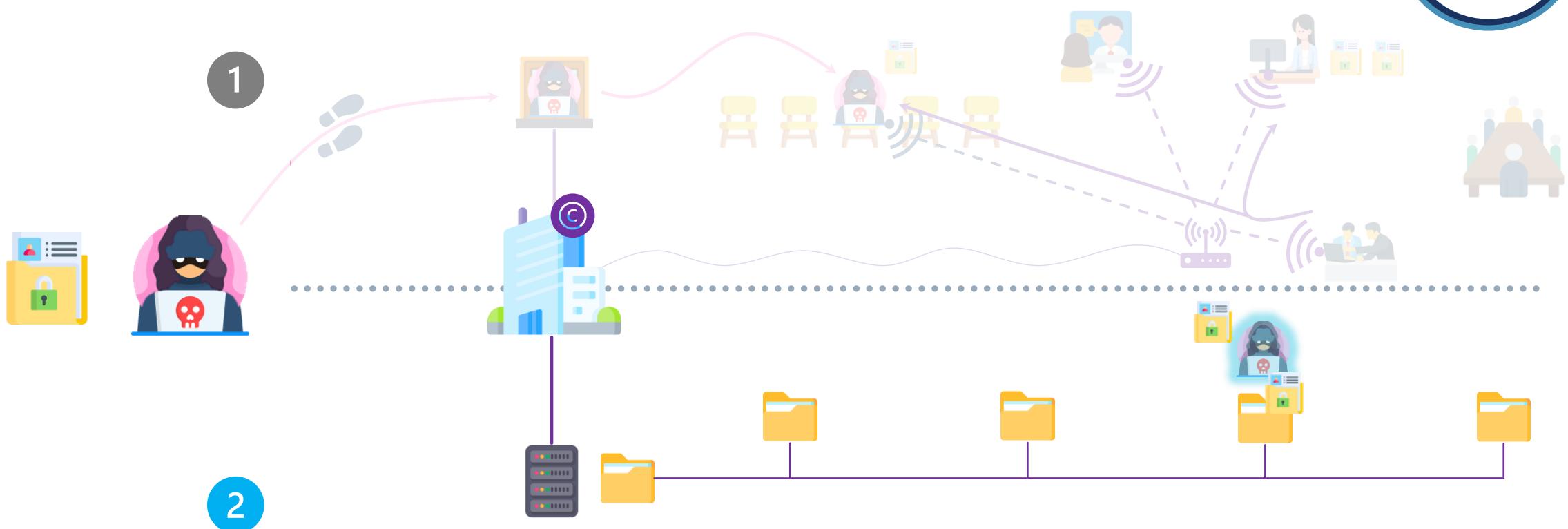
ESPIONNAGE



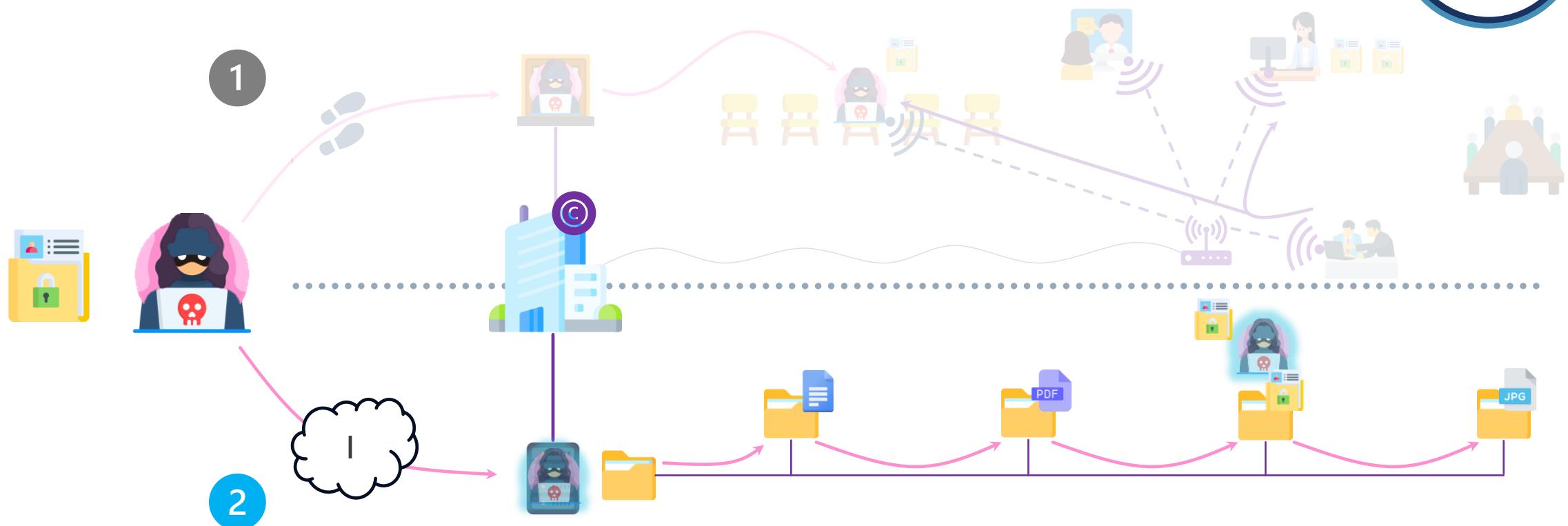
ESPIONNAGE



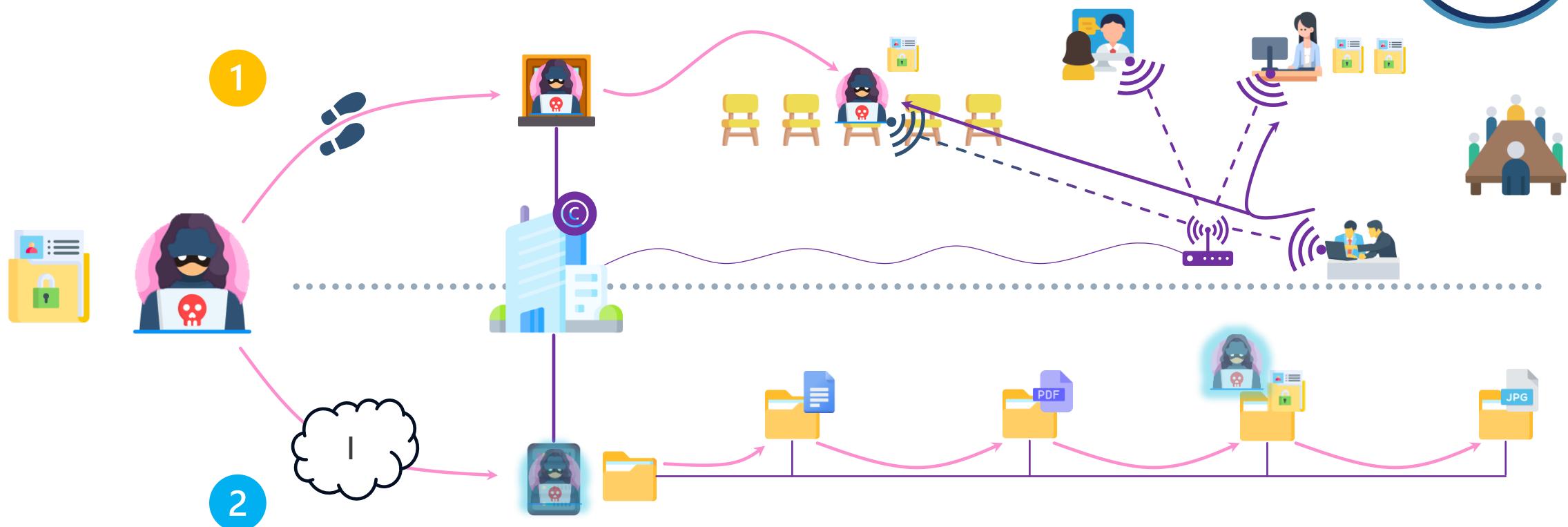
ESPIONNAGE



ESPIONNAGE



ESPIONNAGE

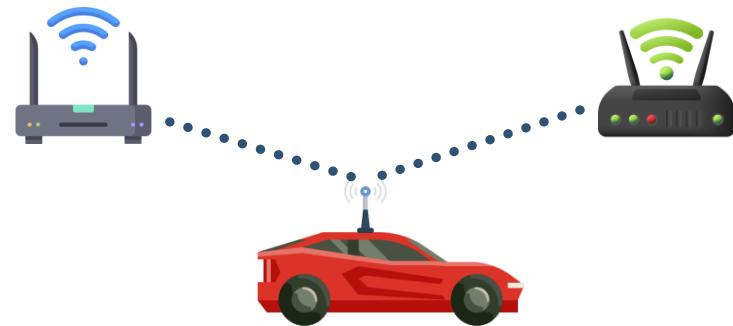


WARDRIVING

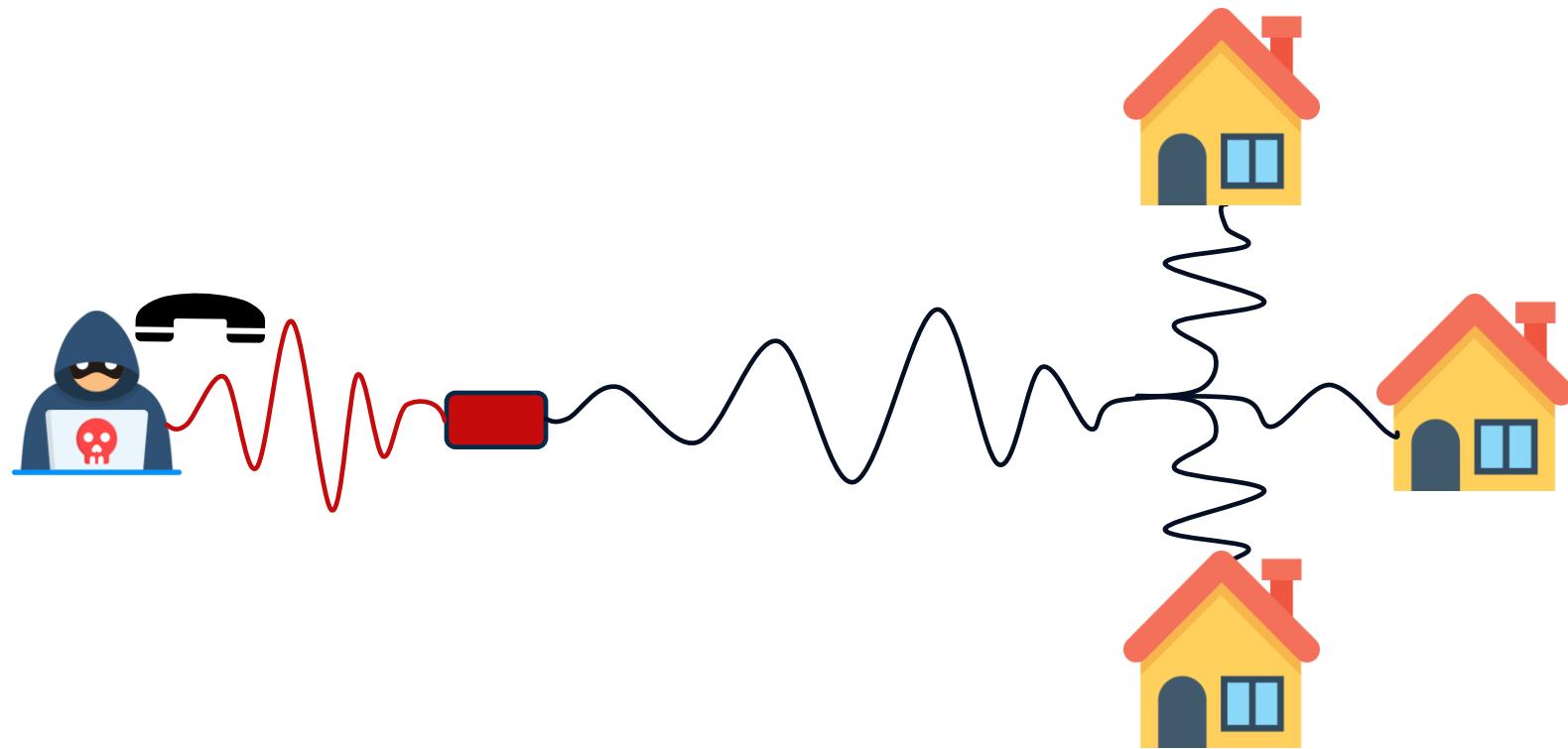


Scan des réseaux Wi-Fi à proximité

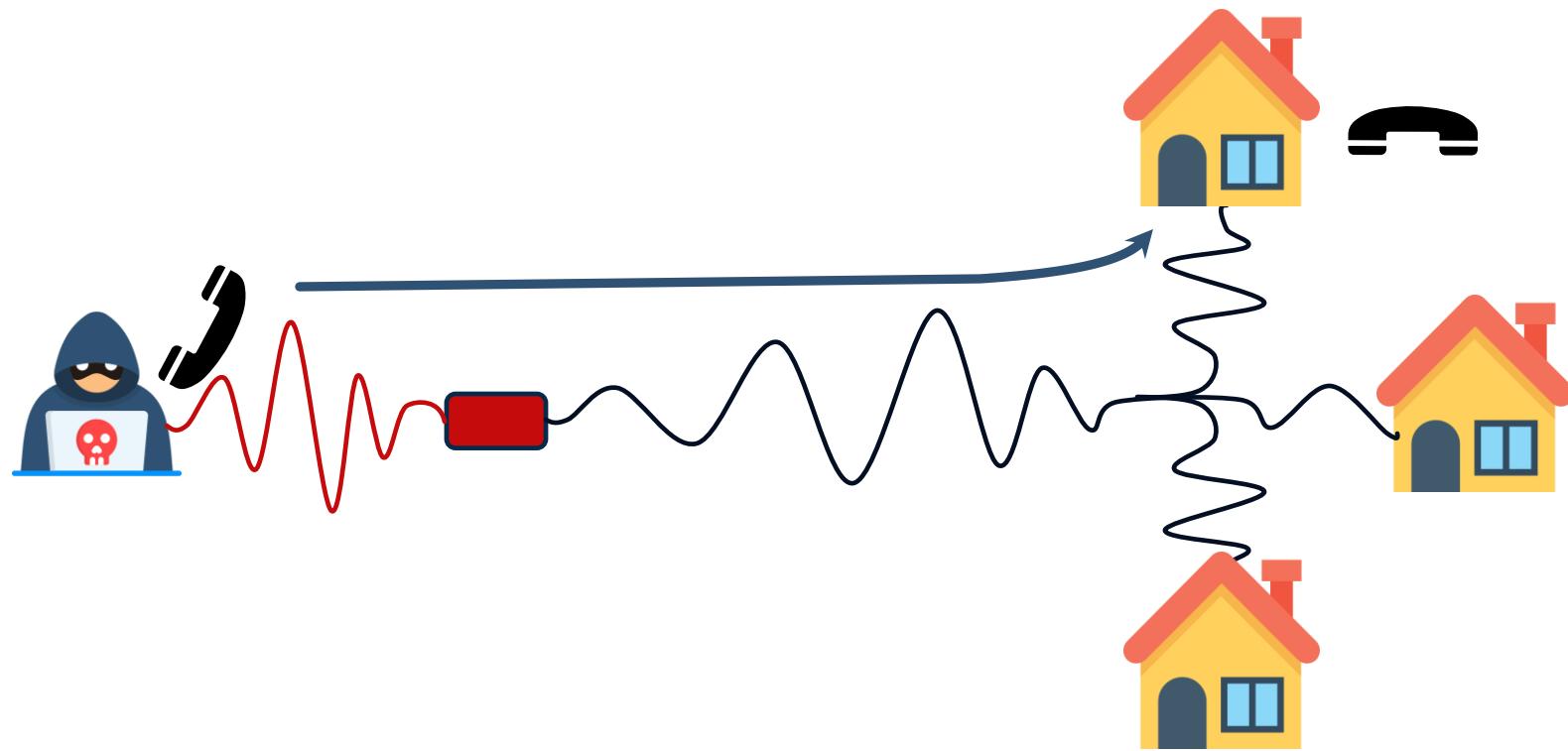
- Identifier réseaux non sécurisés / sécurité faible
- Scan fait en mouvement
 - Généralement en voiture
 - Peut se faire d'autre manières (Warbiking → vélo)
- D'origine Wardialing
 - Processus d'appeler tous les numéros dans une gamme donnée
 - Identifier l'existence d'un modem



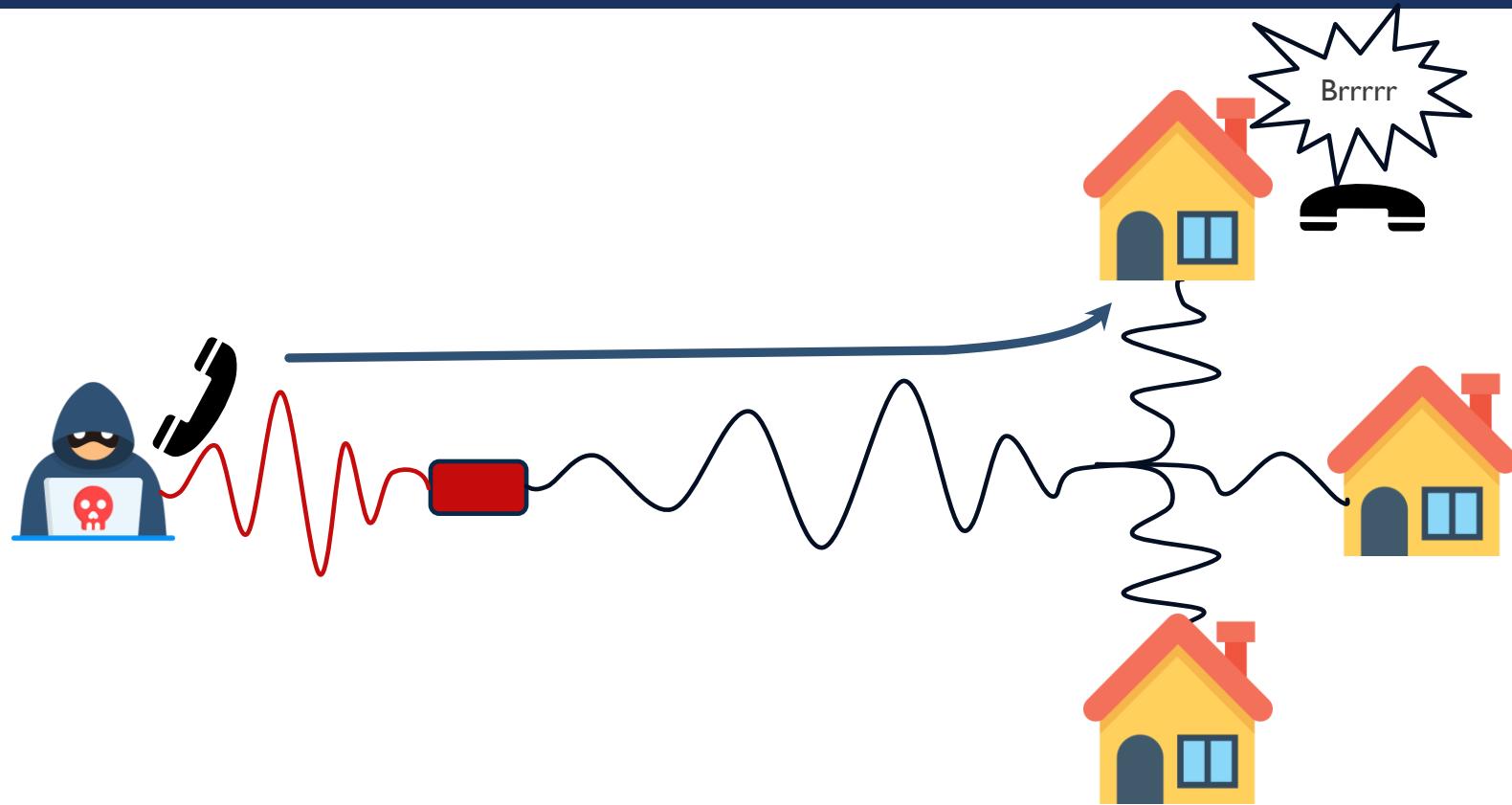
WARDIALING



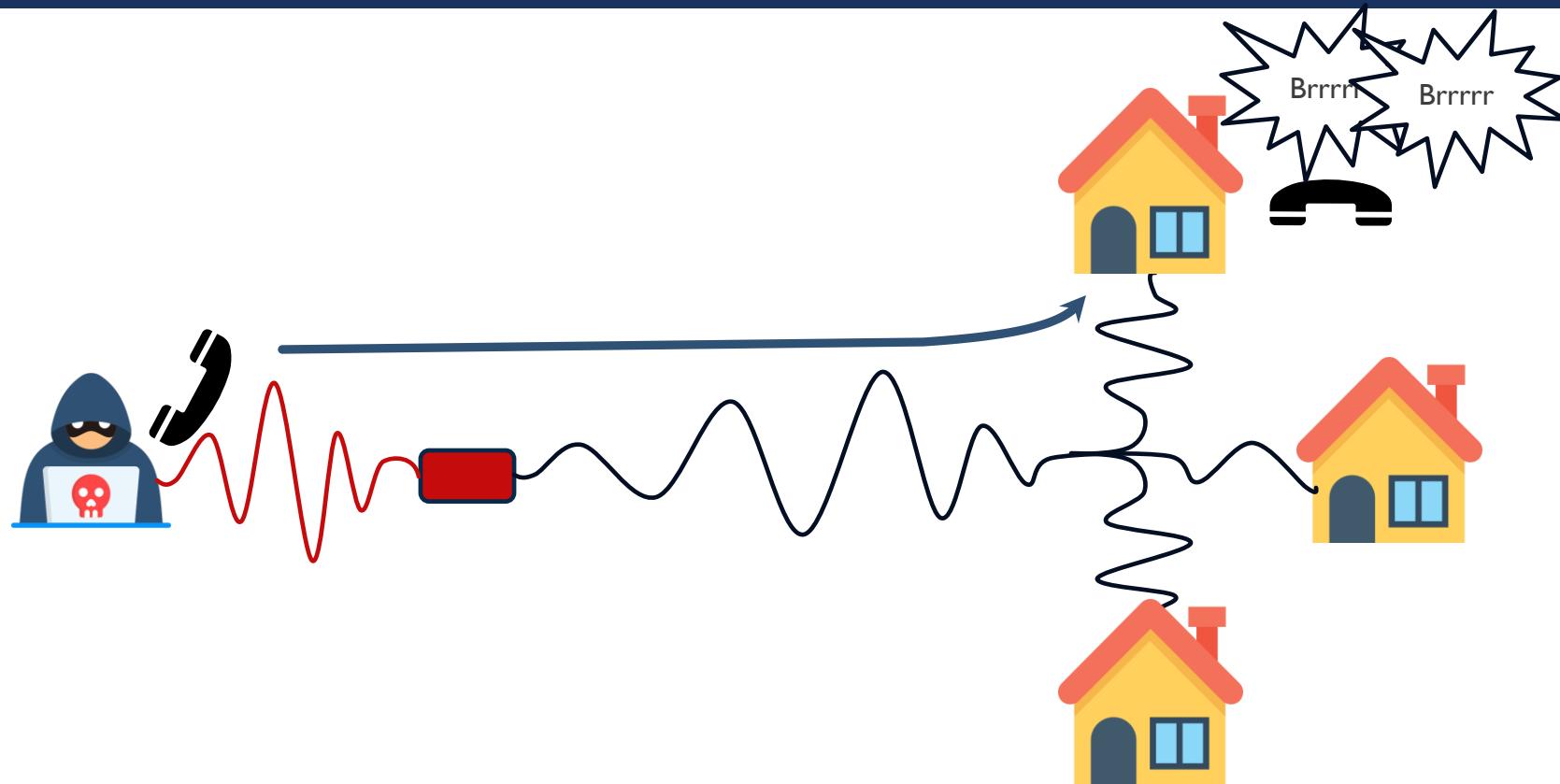
WARDIALING



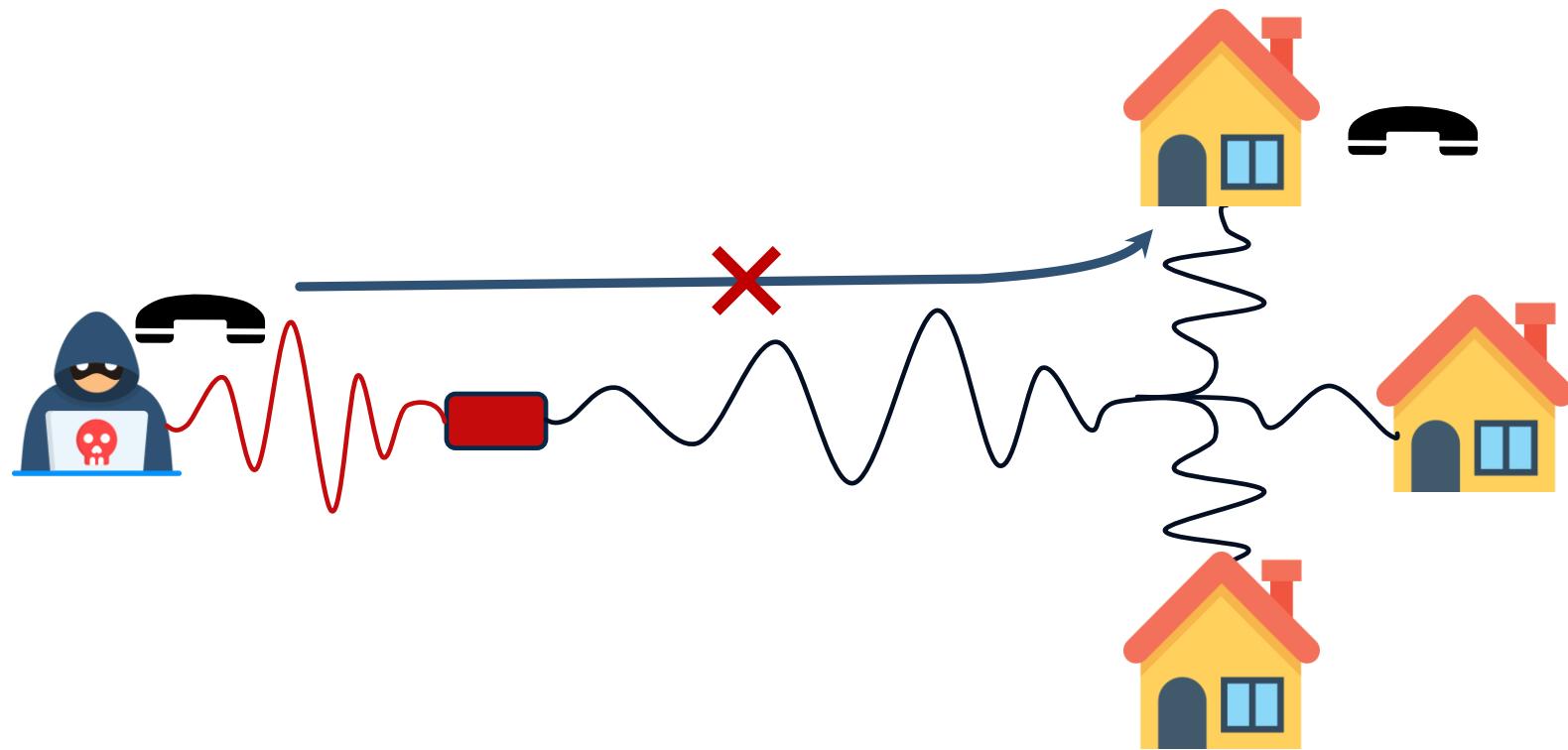
WARDIALING



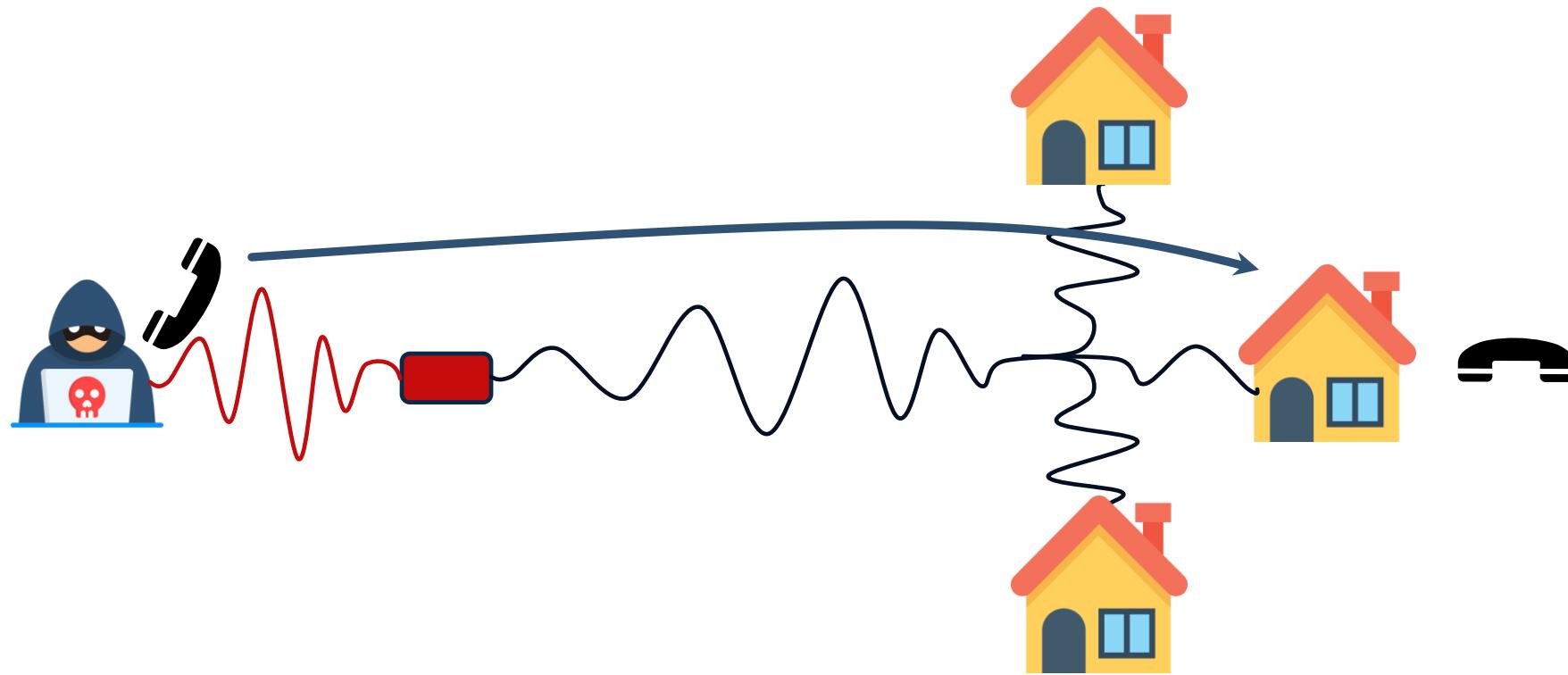
WARDIALING



WARDIALING



WARDIALING



WARDIALING



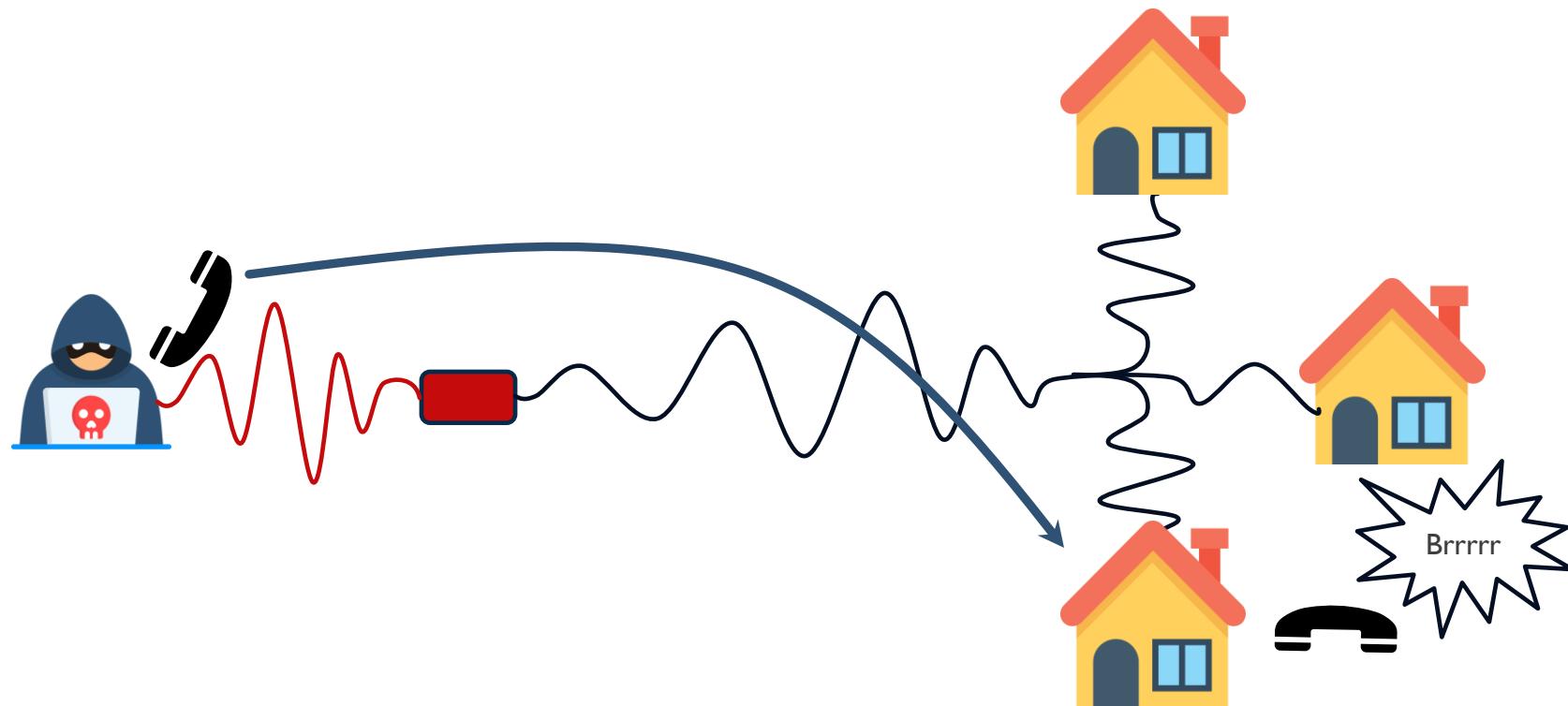
WARDIALING



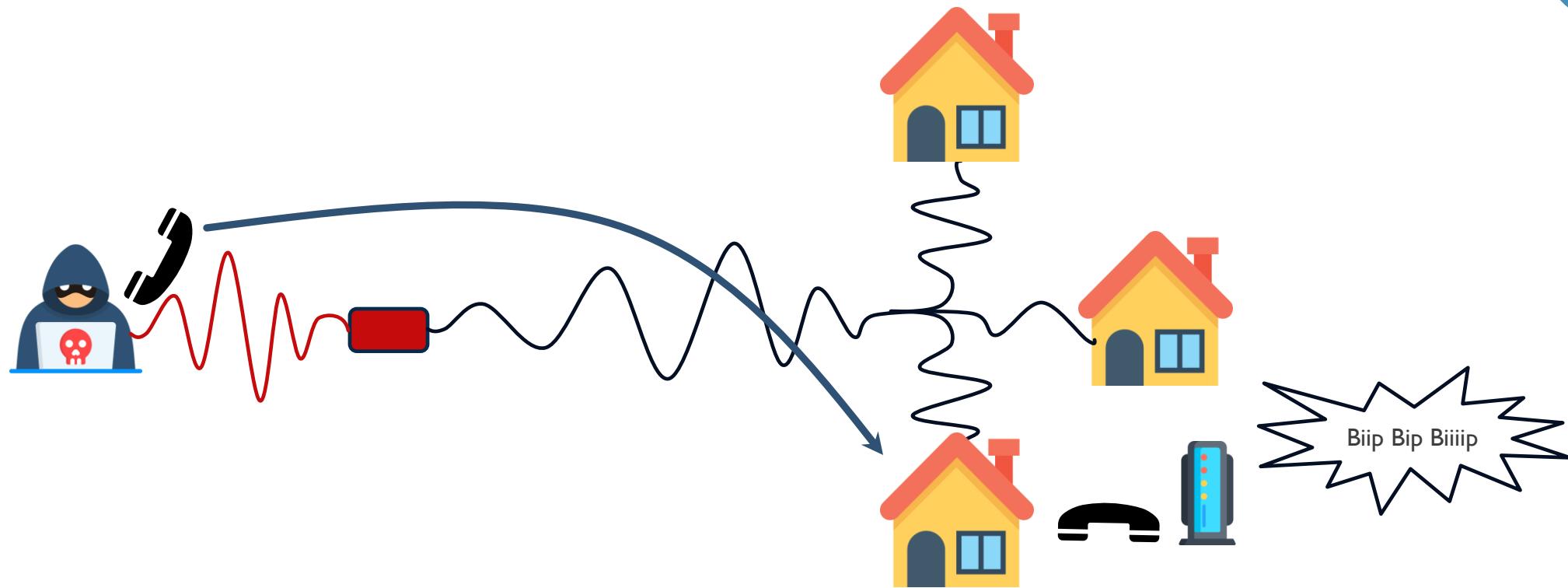
WARDIALING



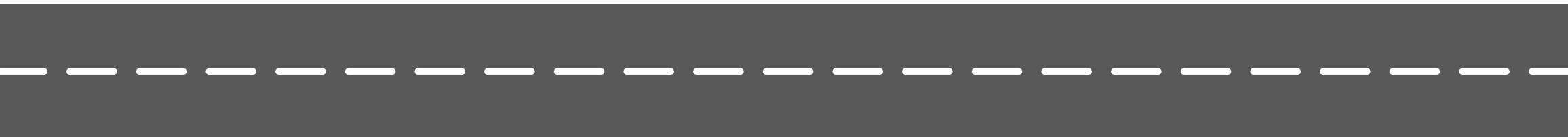
WARDIALING



WARDIALING



WARDRIVING



WARDRIVING



WARDRIVING



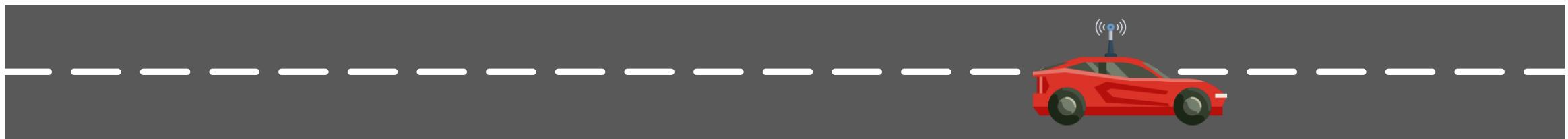
WARDRIVING



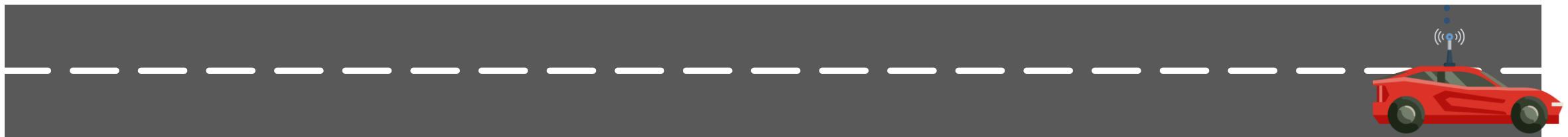
WARDRIVING



WARDRIVING



WARDRIVING



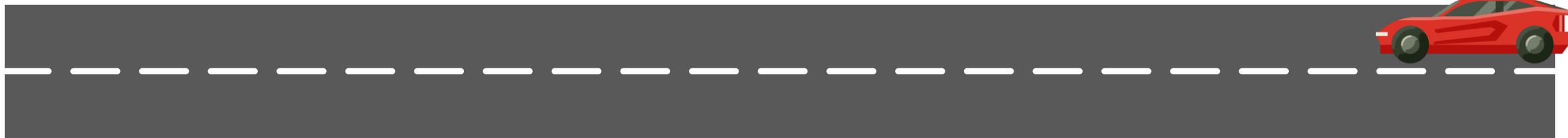
WARDRIVING



WARDRIVING



WARDRIVING



WARDRIVING



WARDRIVING



WARDRIVING



PLONGÉE DANS LES POUBELLES



Fouille des déchets ménagers et électronique

- Rechercher des informations personnelles jetés
- Mots de passe, identifiants, etc...
- Récupération de déchets électronique
 - Extraction d'identifiants non supprimés
 - Login/mot de passe, clés de session, cookies, etc...



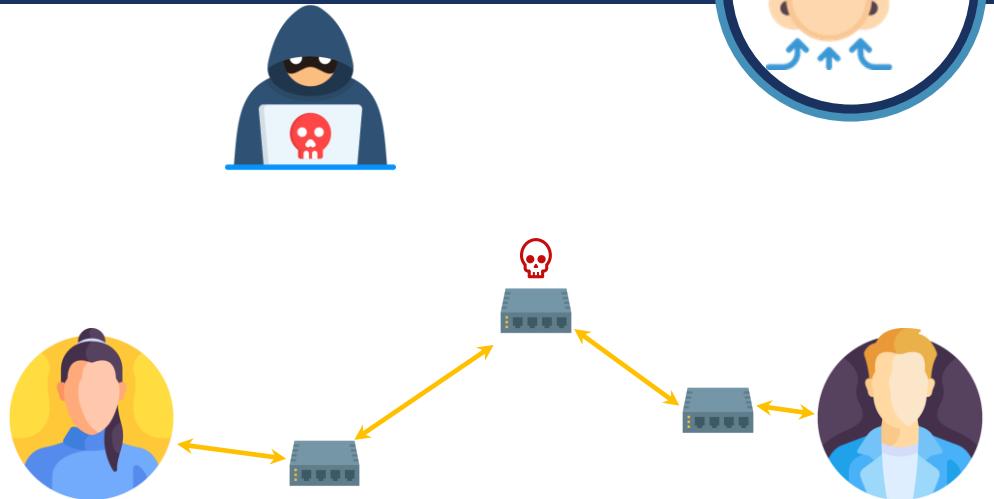
Dumpster Diving

RENIFLAGE DE PAQUETS

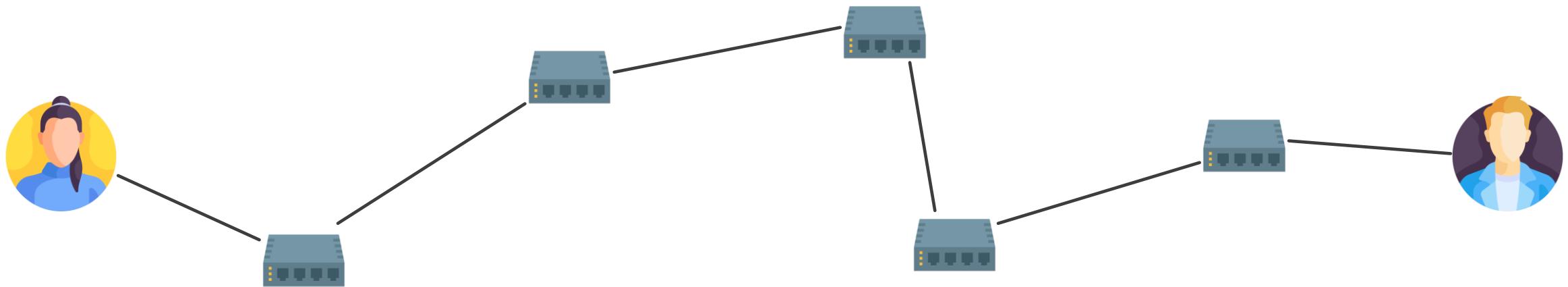


Surveillance et récupération du trafic réseau

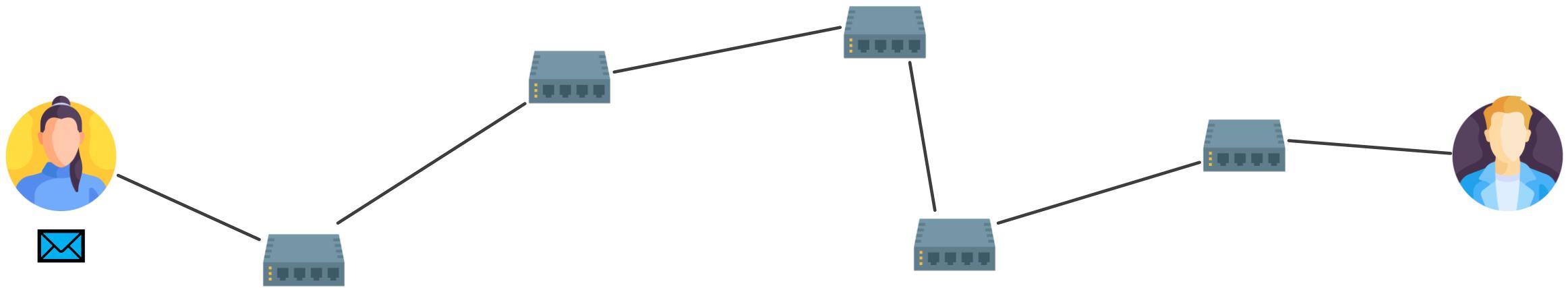
- Installation d'un système de surveillance
 - Équipement ou logiciel
 - N'impacte pas le fonctionnement
-
- Le même principe est utilisé comme technique de protection
 - Vérification du traffic
 - Identification de communications anormales



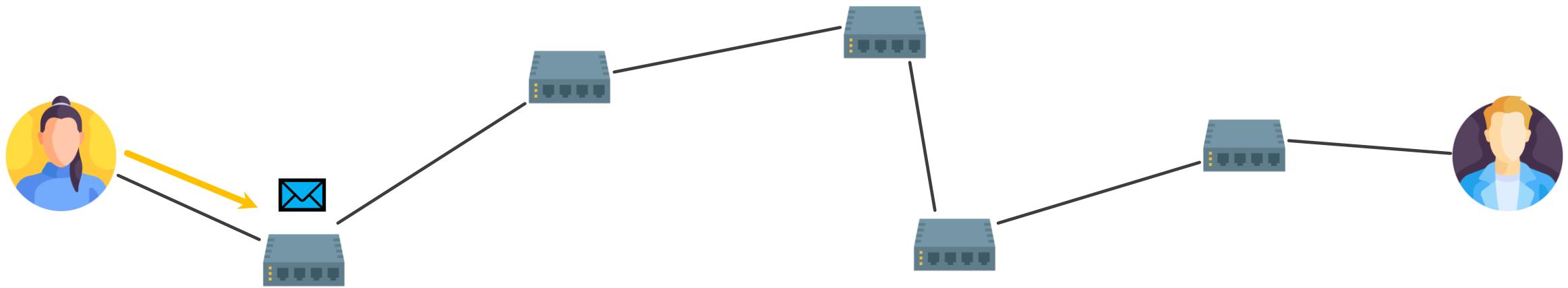
RENIFLAGE DE PAQUETS



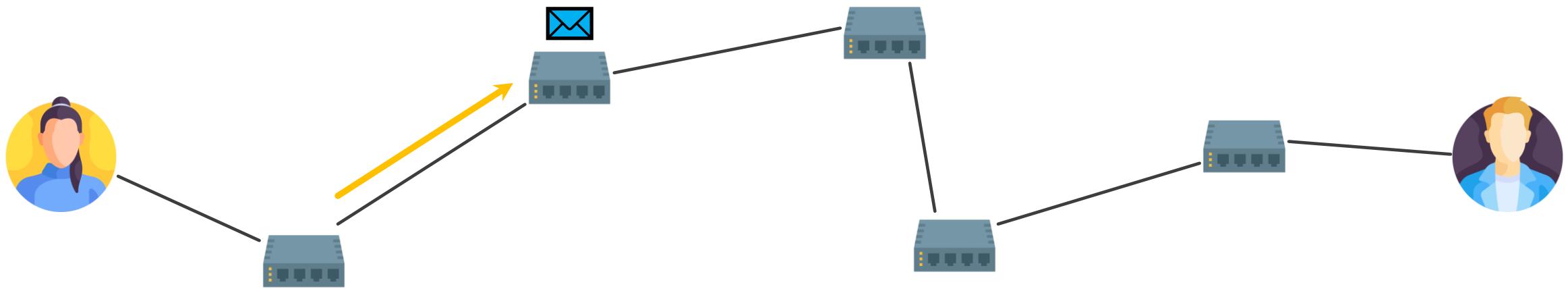
RENIFLAGE DE PAQUETS



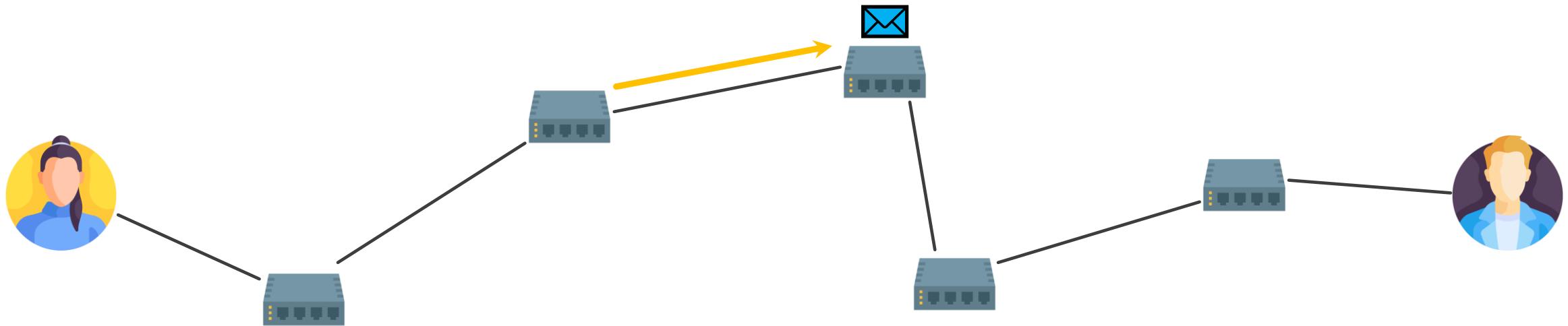
RENIFLAGE DE PAQUETS



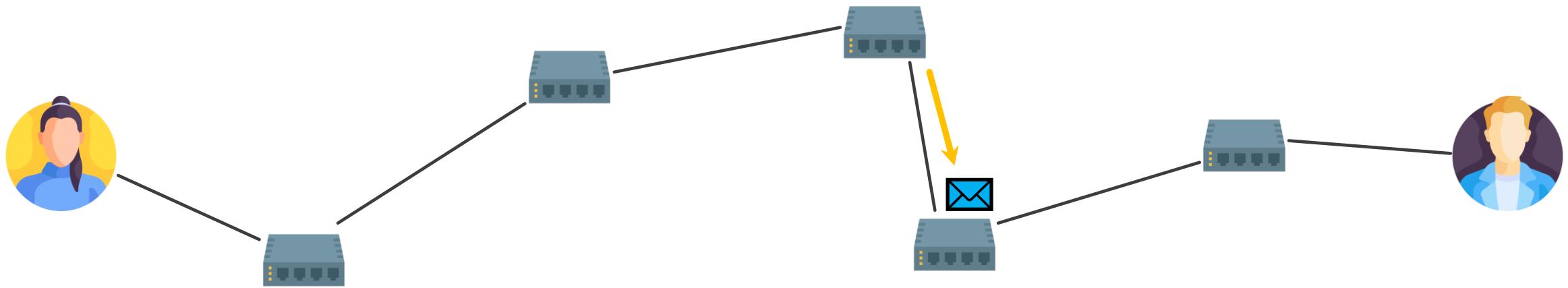
RENIFLAGE DE PAQUETS



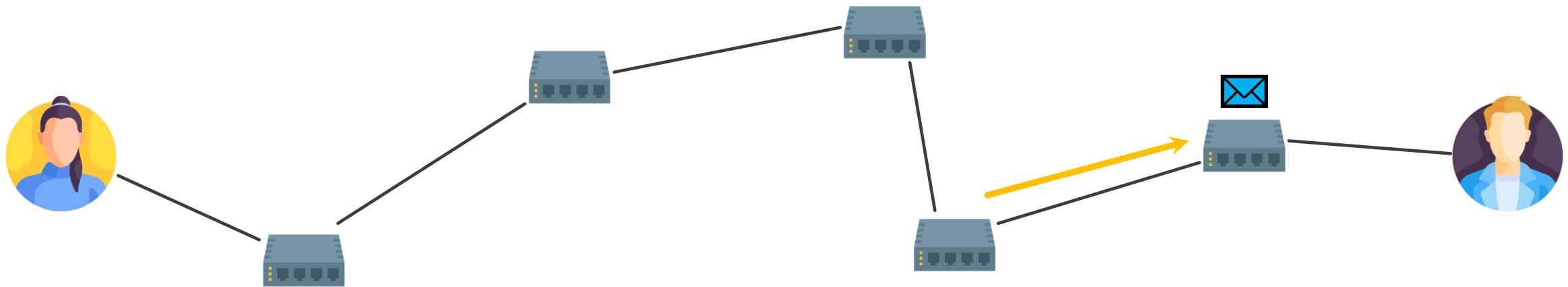
RENIFLAGE DE PAQUETS



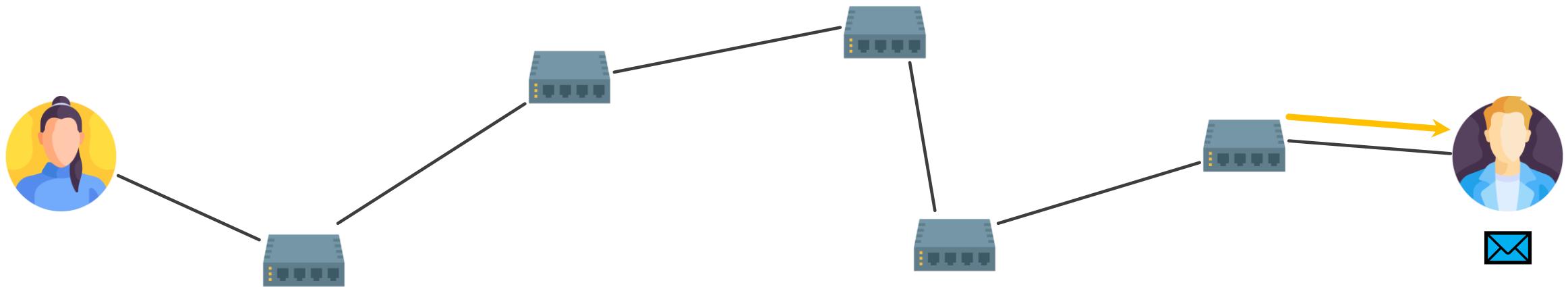
RENIFLAGE DE PAQUETS



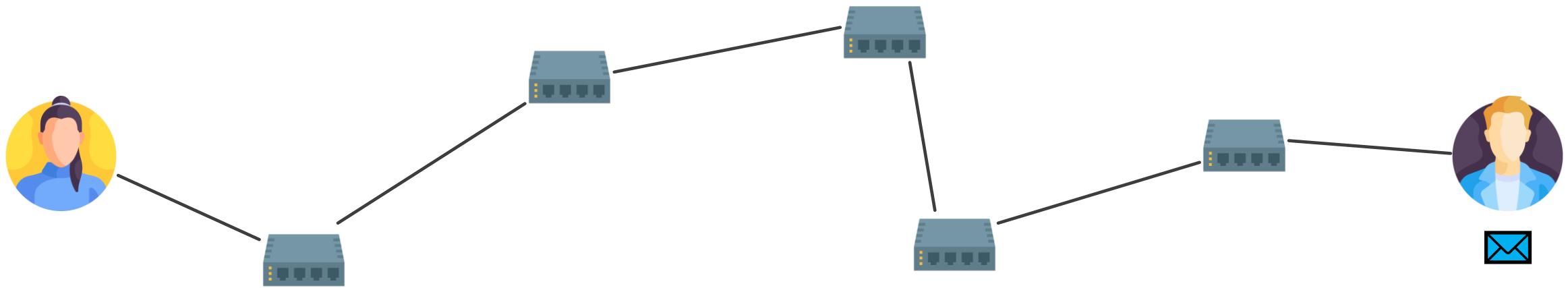
RENIFLAGE DE PAQUETS



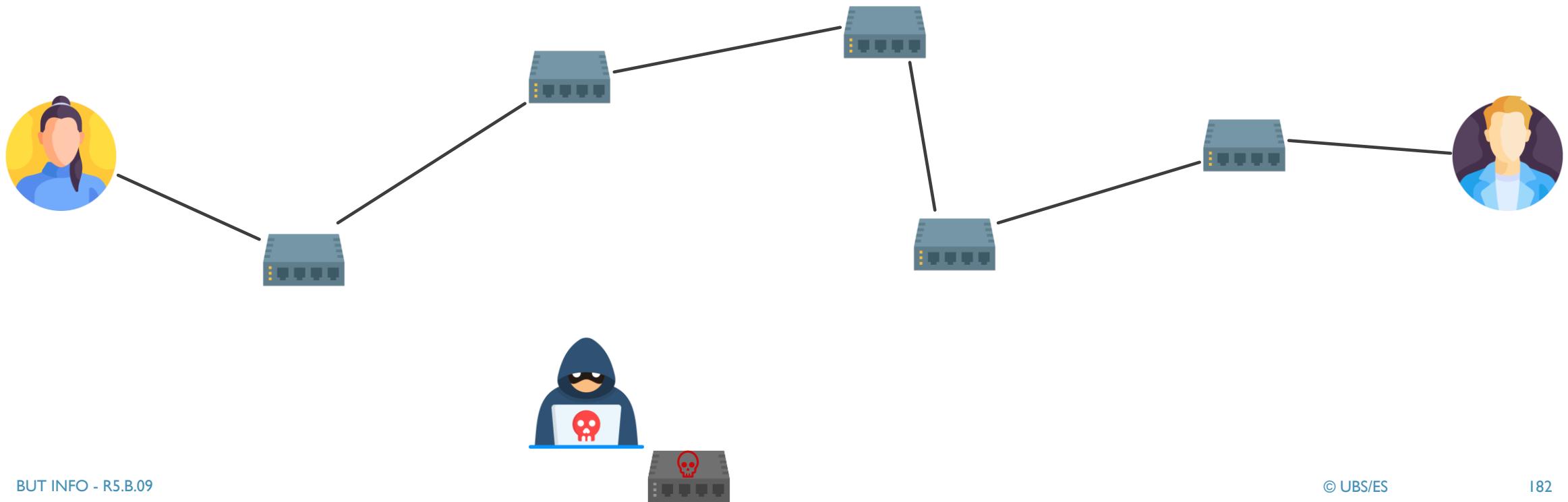
RENIFLAGE DE PAQUETS



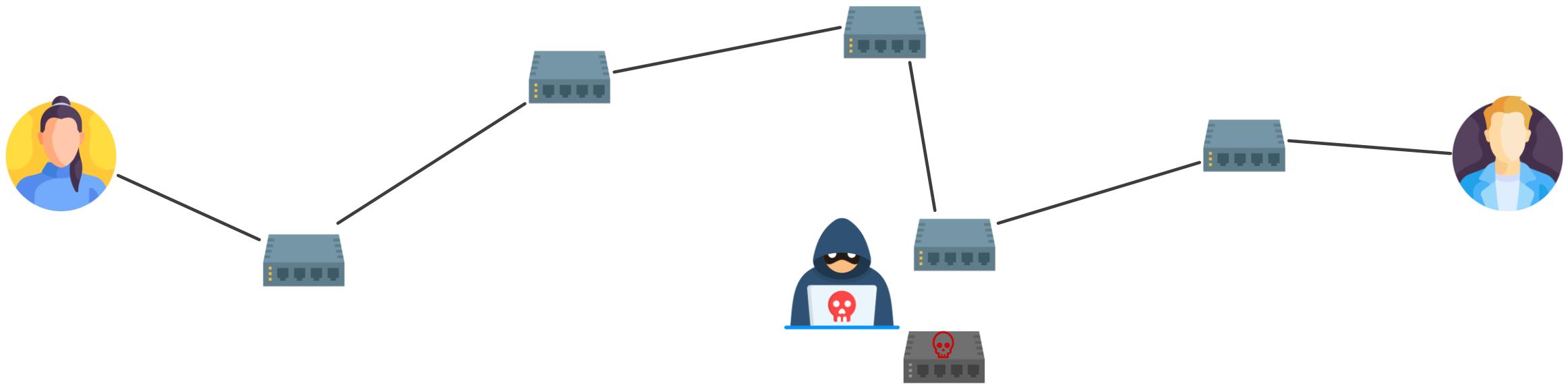
RENIFLAGE DE PAQUETS



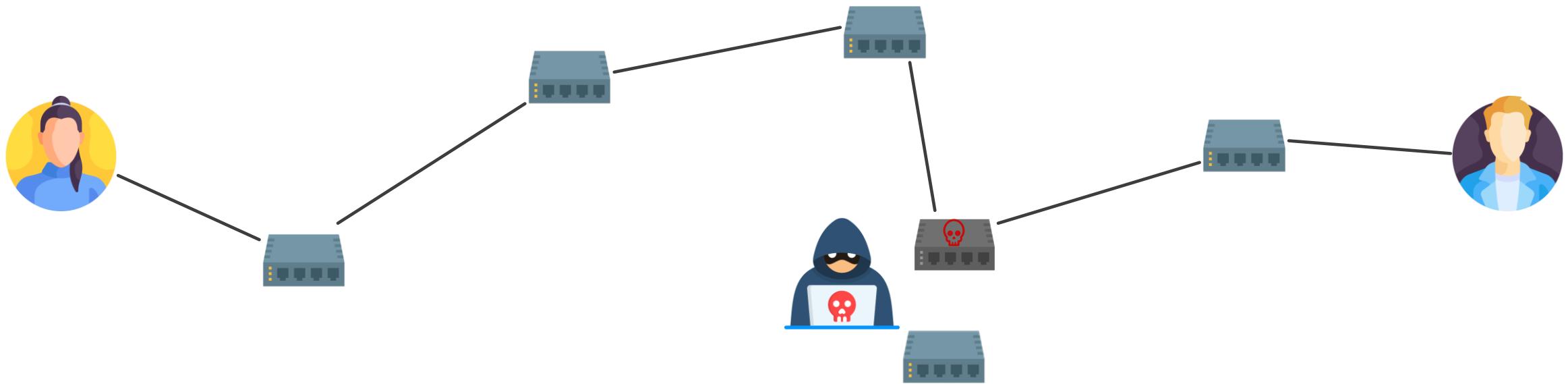
RENIFLAGE DE PAQUETS



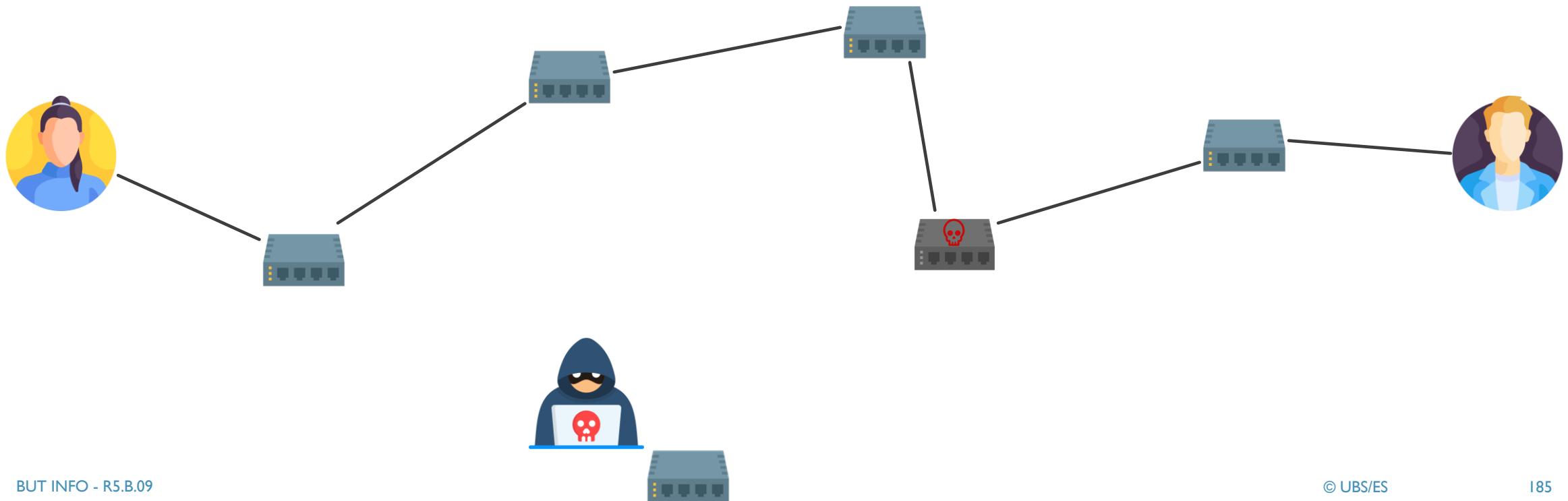
RENIFLAGE DE PAQUETS



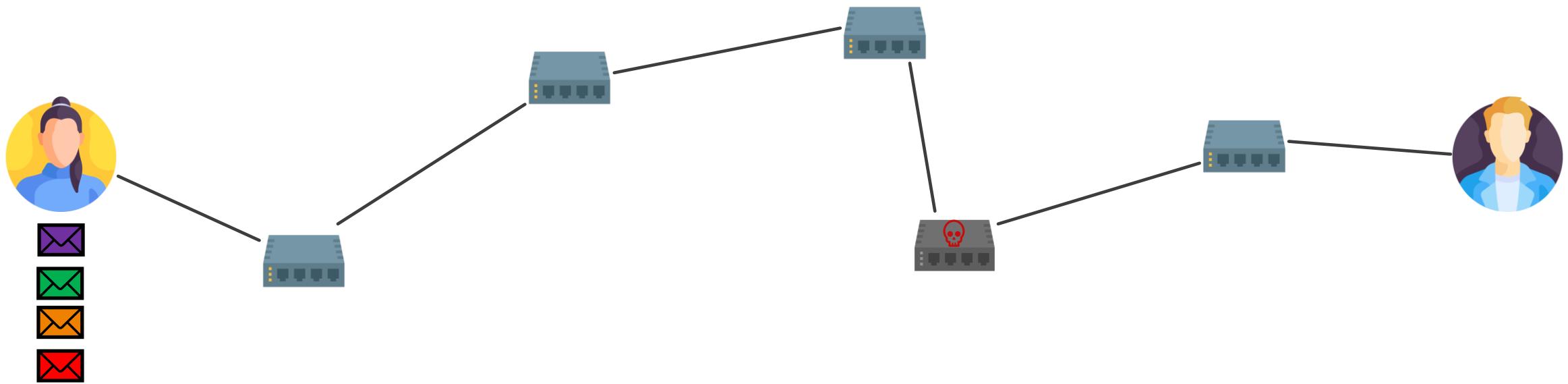
RENIFLAGE DE PAQUETS



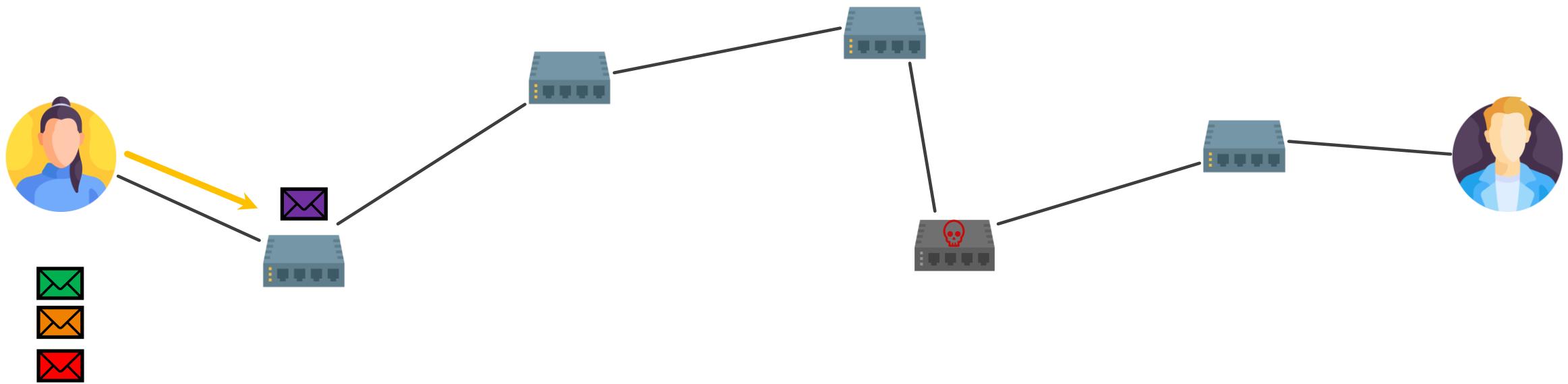
RENIFLAGE DE PAQUETS



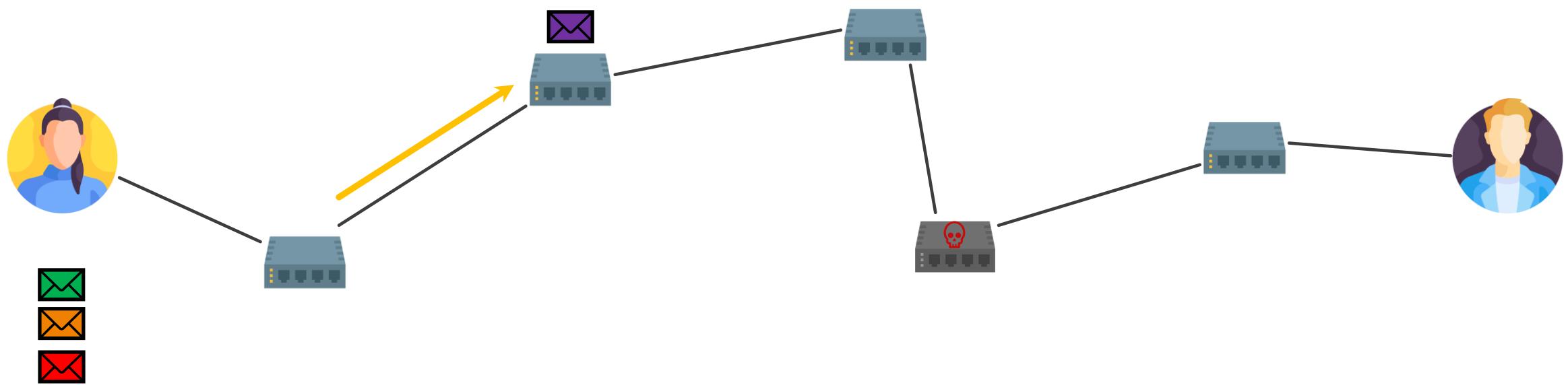
RENIFLAGE DE PAQUETS



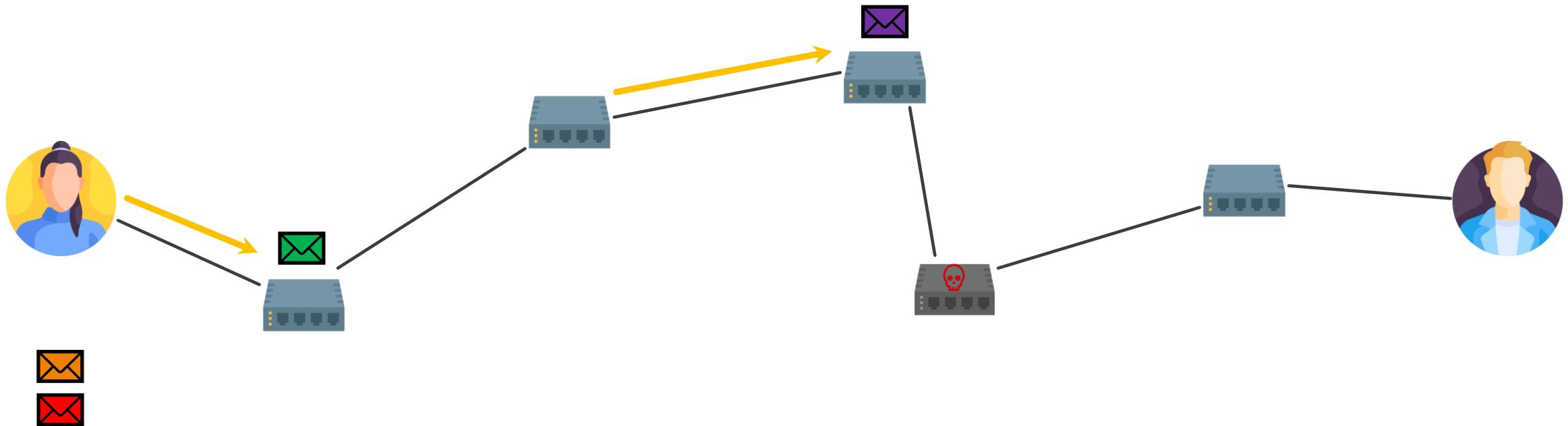
RENIFLAGE DE PAQUETS



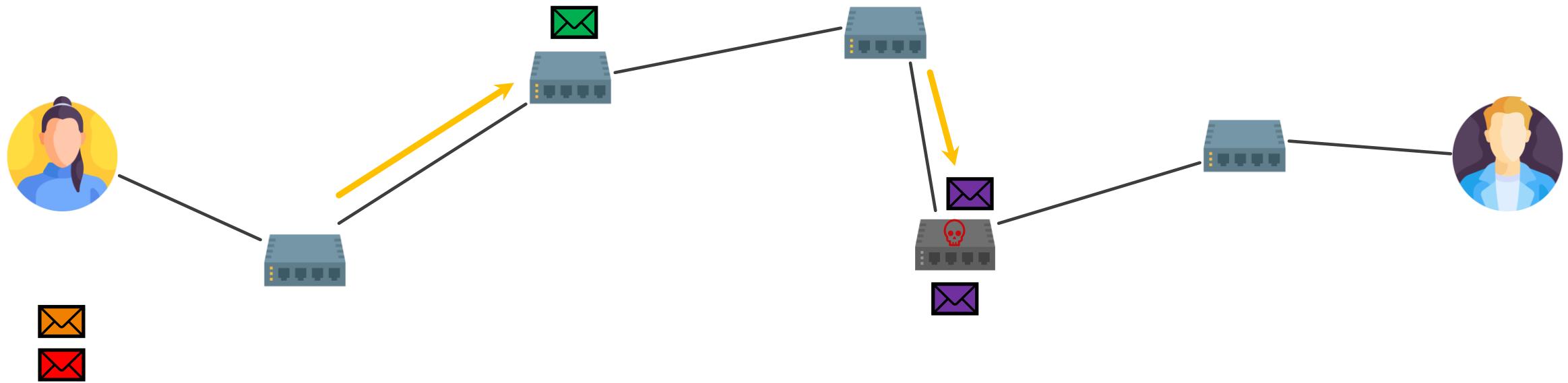
RENIFLAGE DE PAQUETS



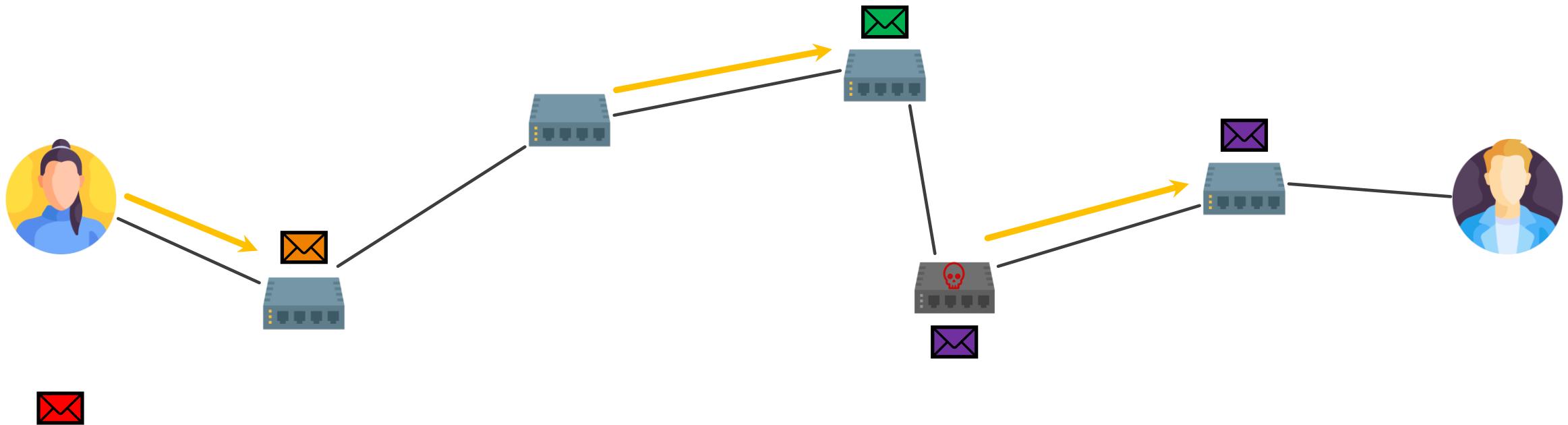
RENIFLAGE DE PAQUETS



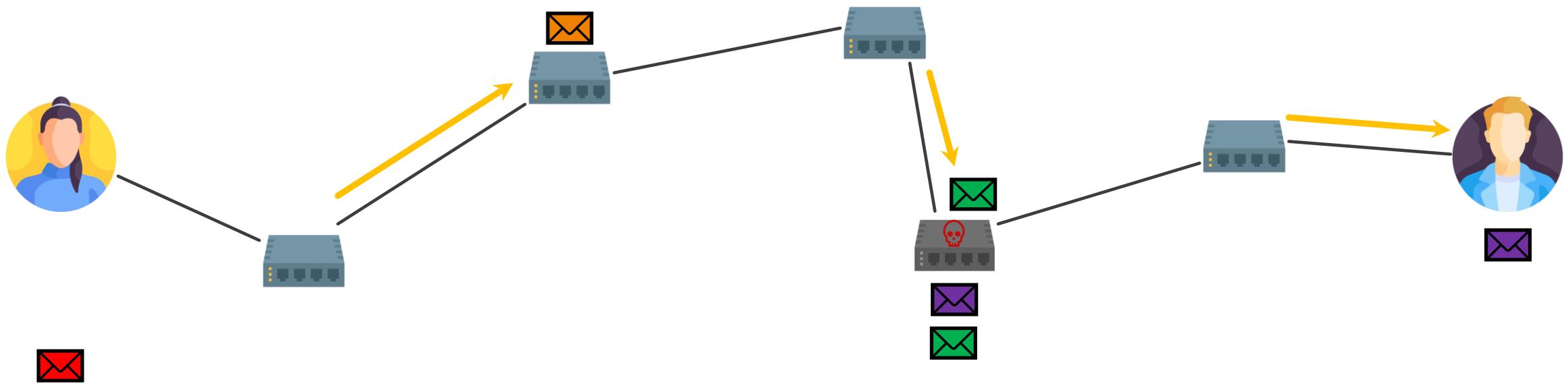
RENIFLAGE DE PAQUETS



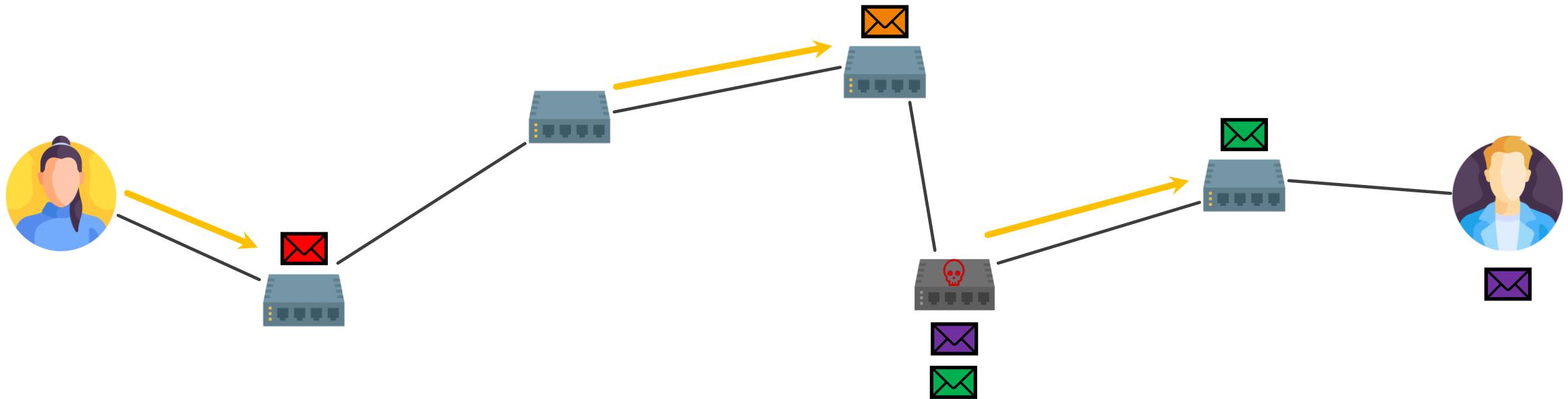
RENIFLAGE DE PAQUETS



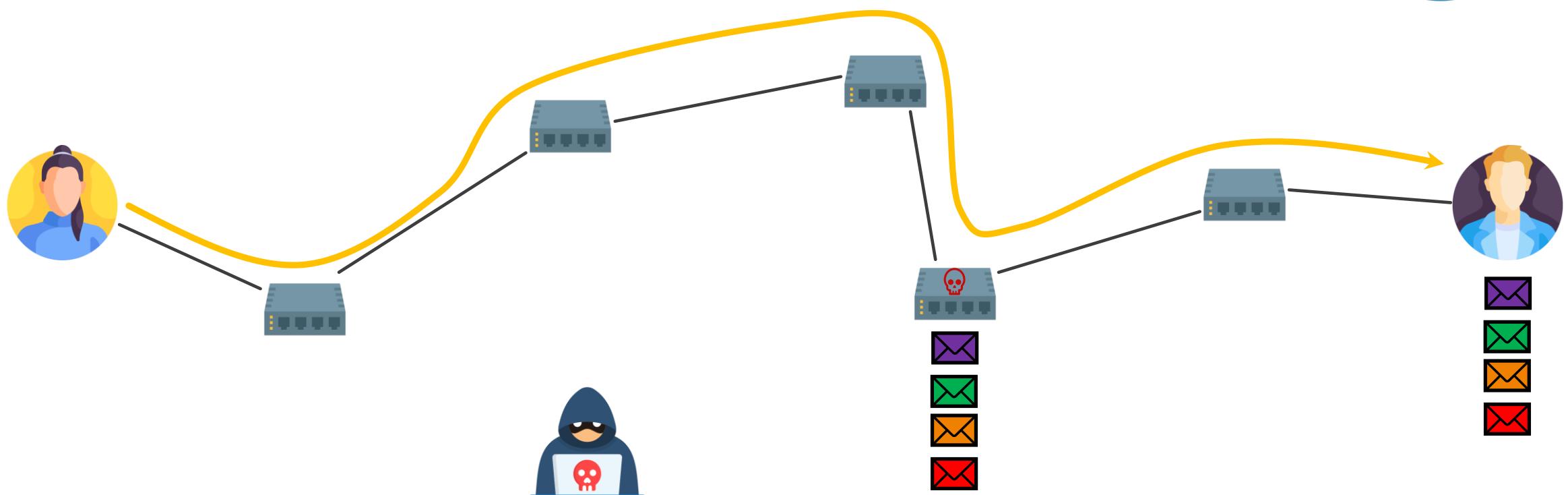
RENIFLAGE DE PAQUETS



RENIFLAGE DE PAQUETS



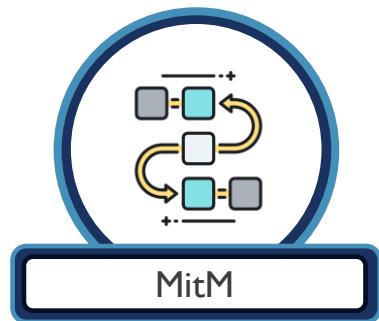
RENIFLAGE DE PAQUETS



QUELQUES ATTAQUES ACTIVES



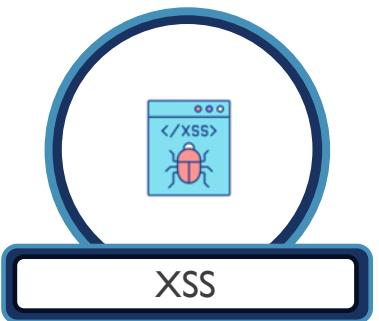
DoS / DDoS



MitM



Ingénierie Sociale



XSS



Drive-by-Attack



Logiciel Malveillant



Cheval de Troie



Rançongiciel



DNS Tunneling



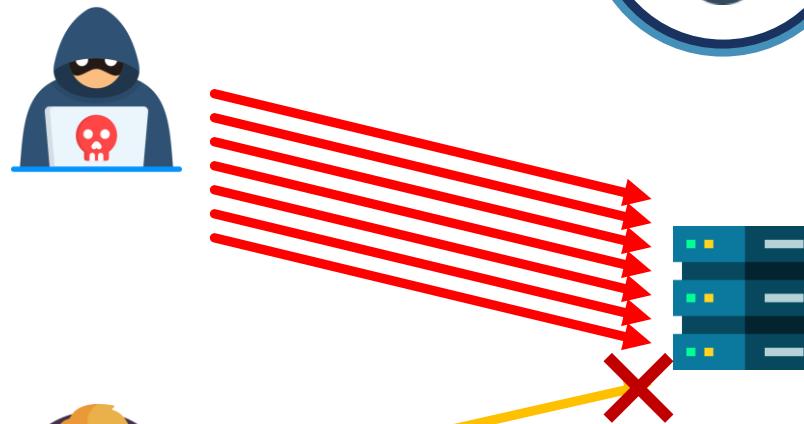
Jumeau Maléfique

DÉNIS DE SERVICE



Impacter la disponibilité d'un système

- Saturation des ressources, impossibilité de communiquer
 - Inondation réseau
- Empêcher tout accès au système cible
- Version Distribué DDoS
 - Plus efficace
 - Plus de conséquences



DÉNIS DE SERVICE



DÉNIS DE SERVICE



DÉNIS DE SERVICE



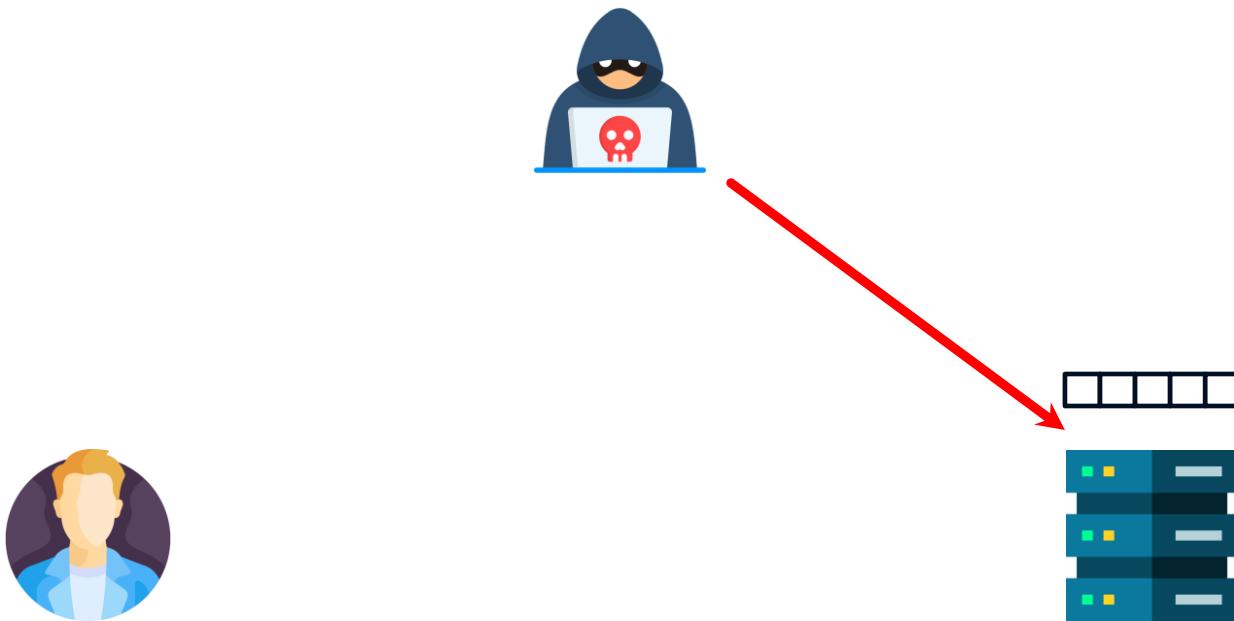
DÉNIS DE SERVICE



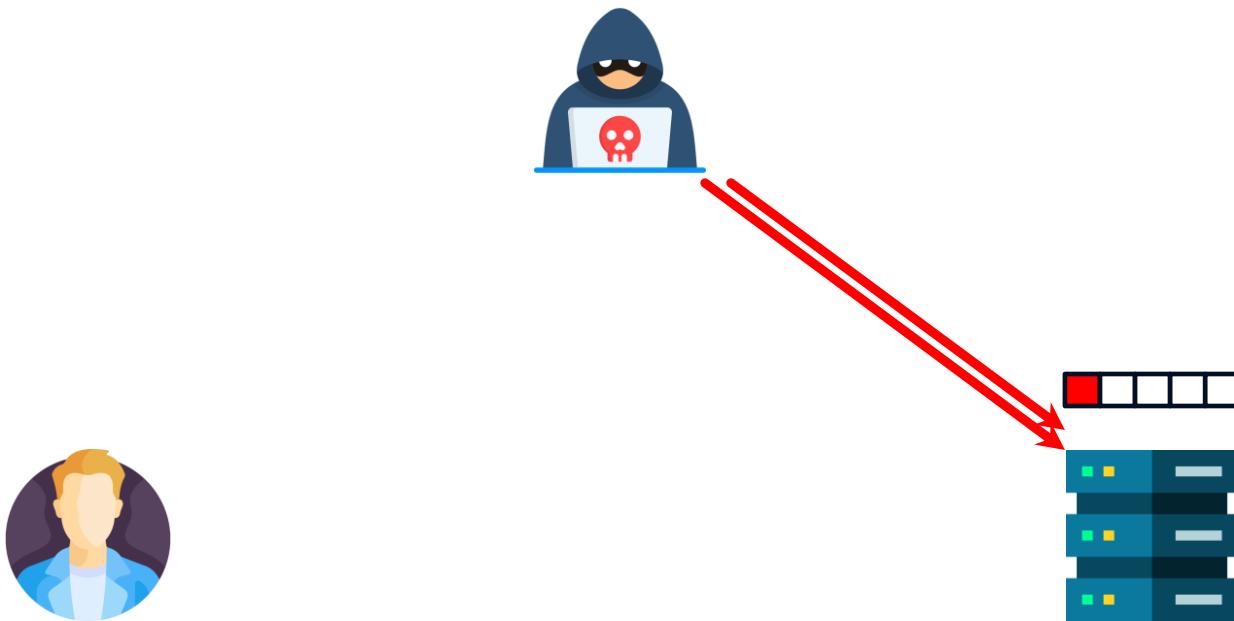
DÉNIS DE SERVICE



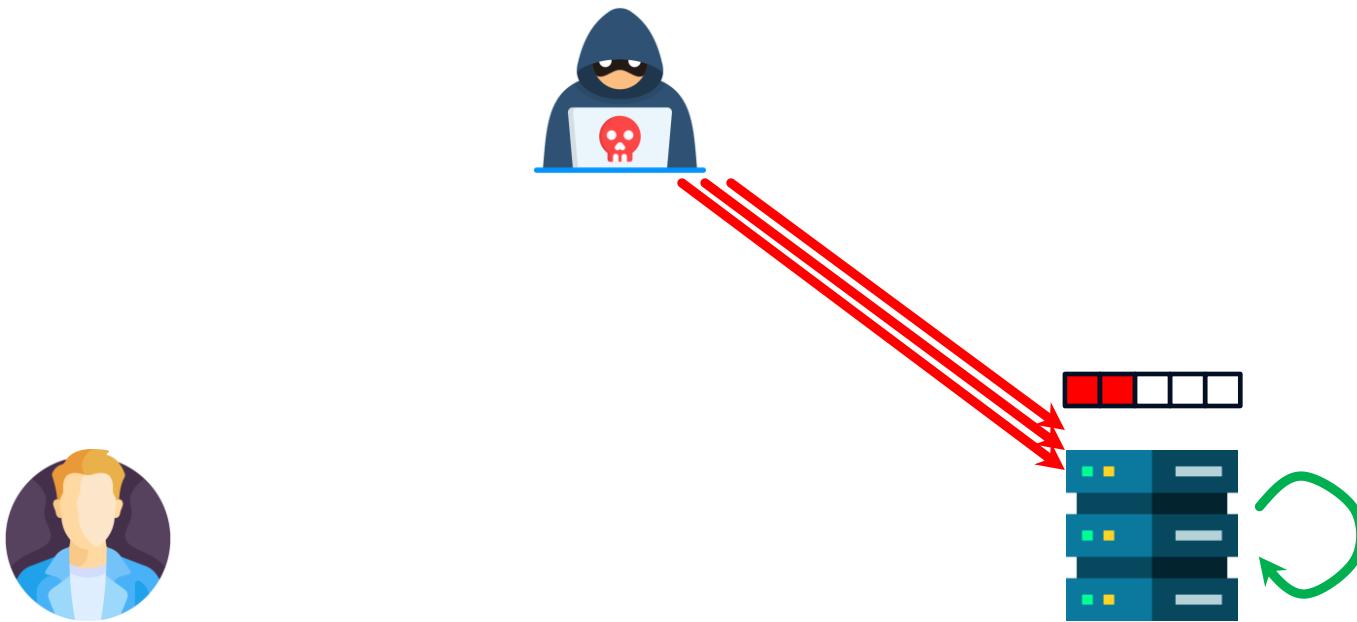
DÉNIS DE SERVICE



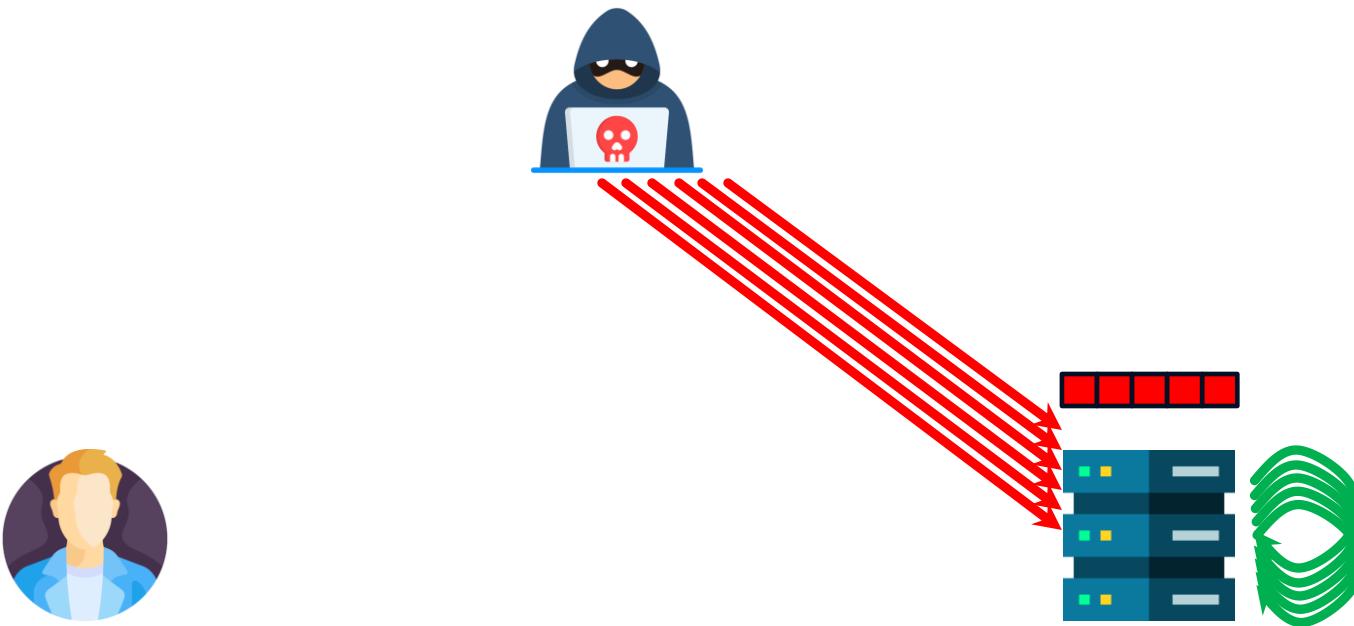
DÉNIS DE SERVICE



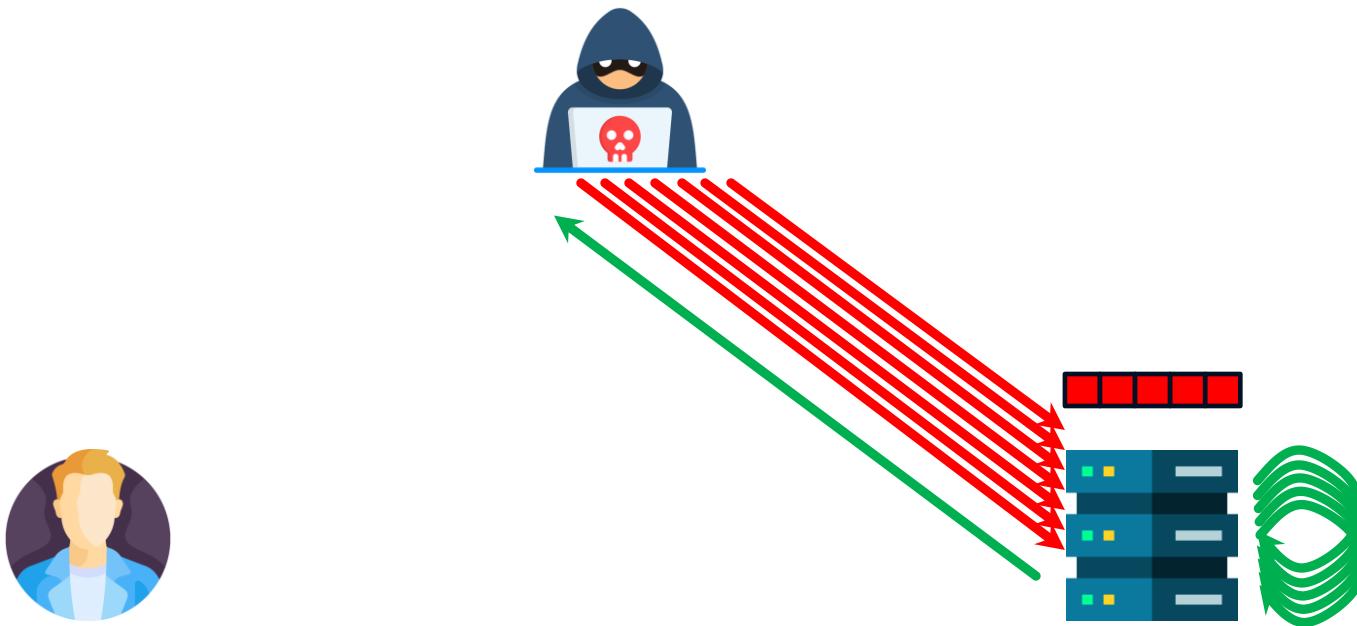
DÉNIS DE SERVICE



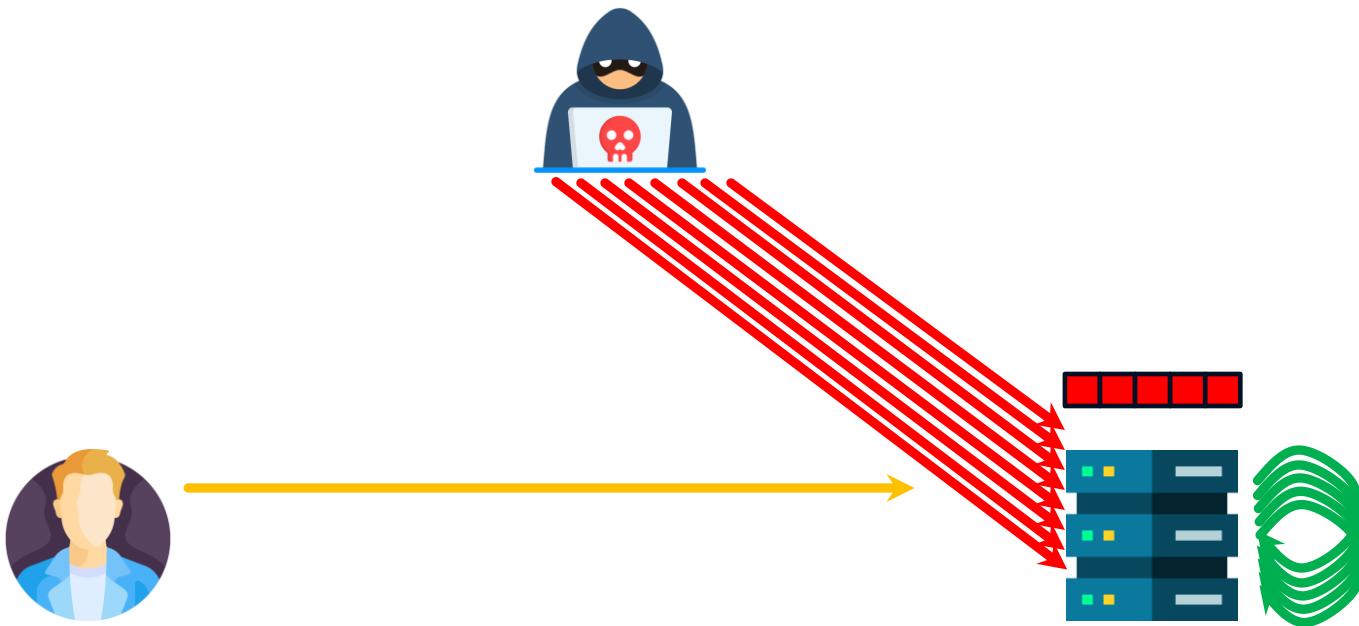
DÉNIS DE SERVICE



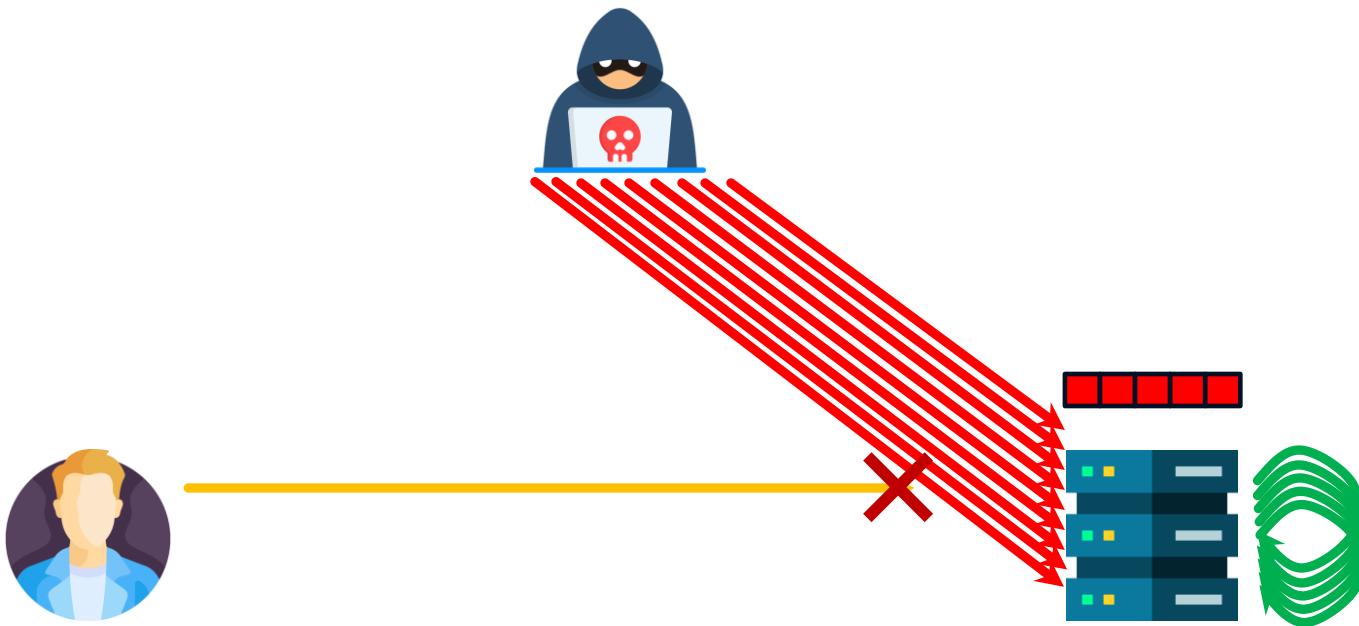
DÉNIS DE SERVICE



DÉNIS DE SERVICE



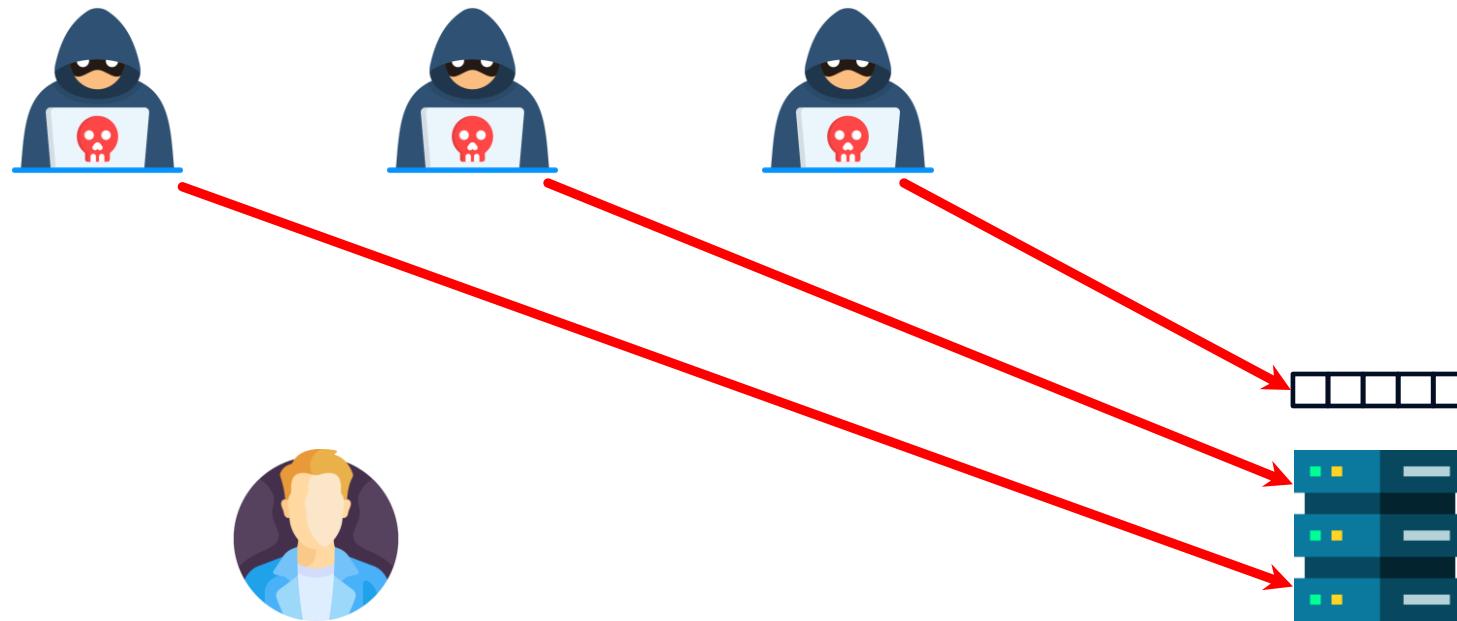
DÉNIS DE SERVICE



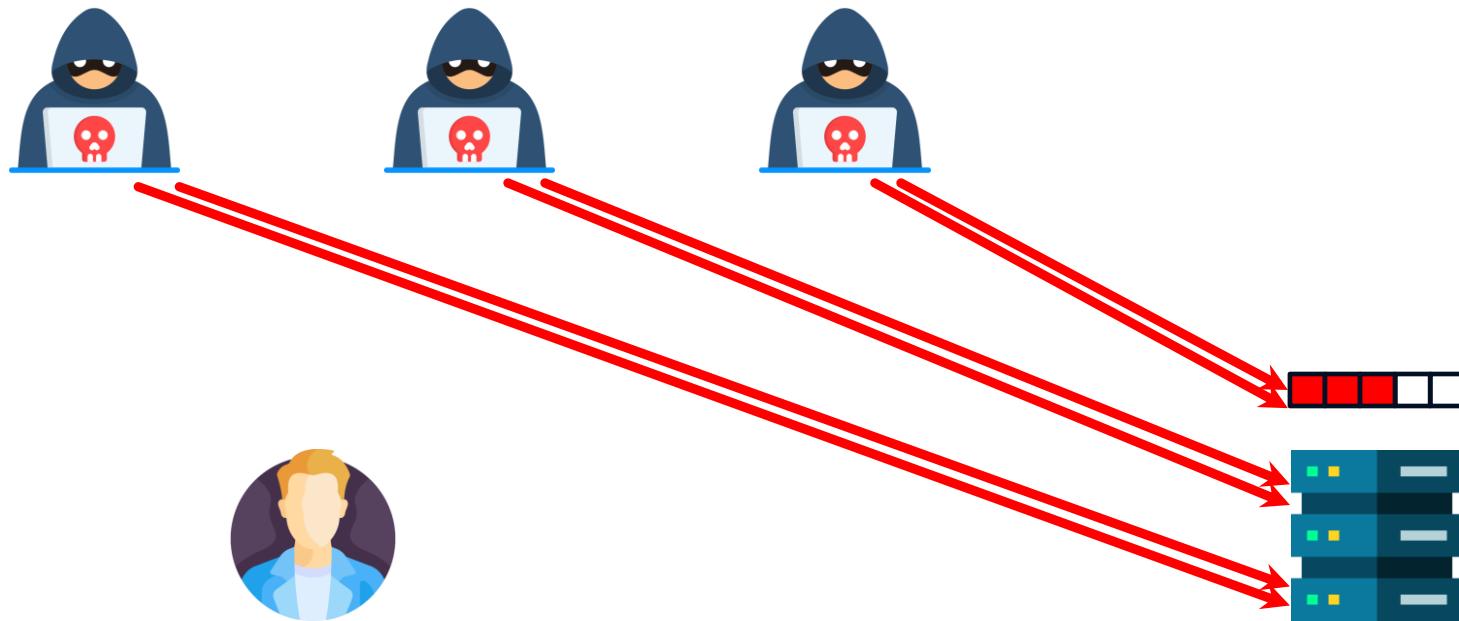
DÉNIS DE SERVICE DISTRIBUÉ



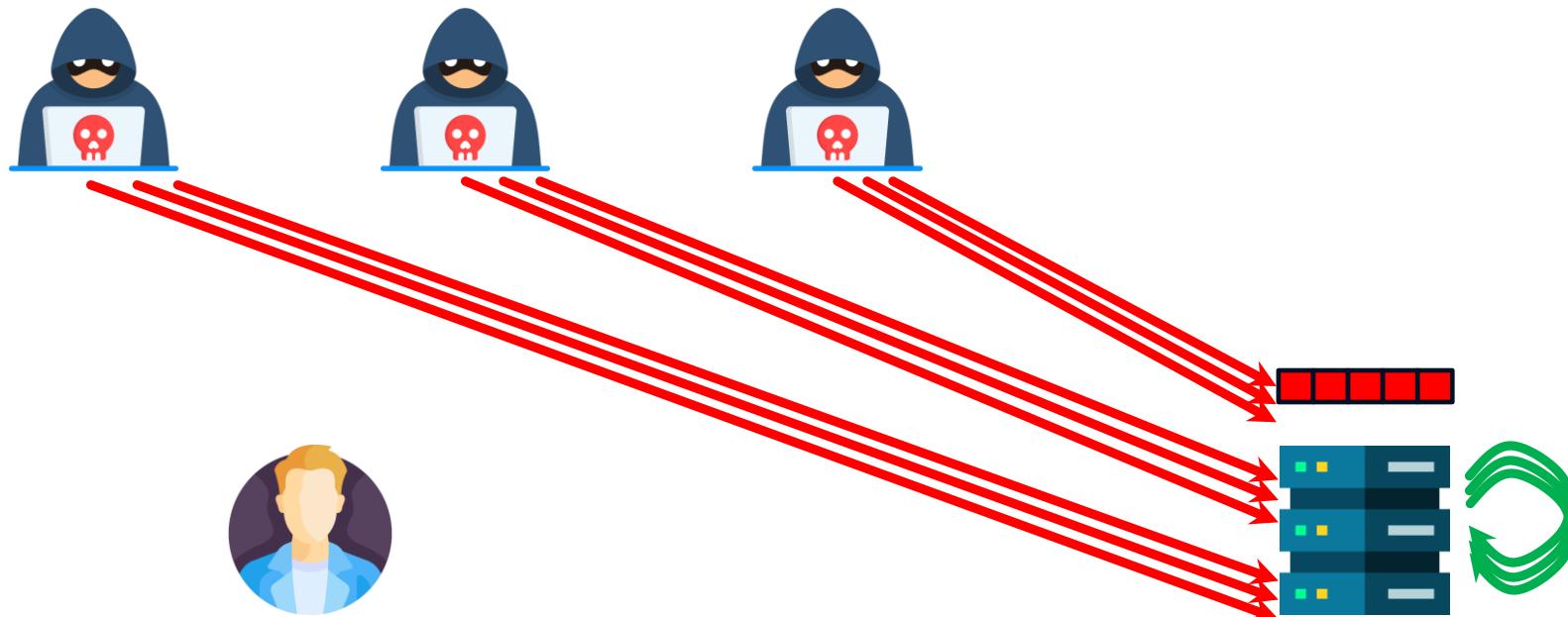
DÉNIS DE SERVICE DISTRIBUÉ



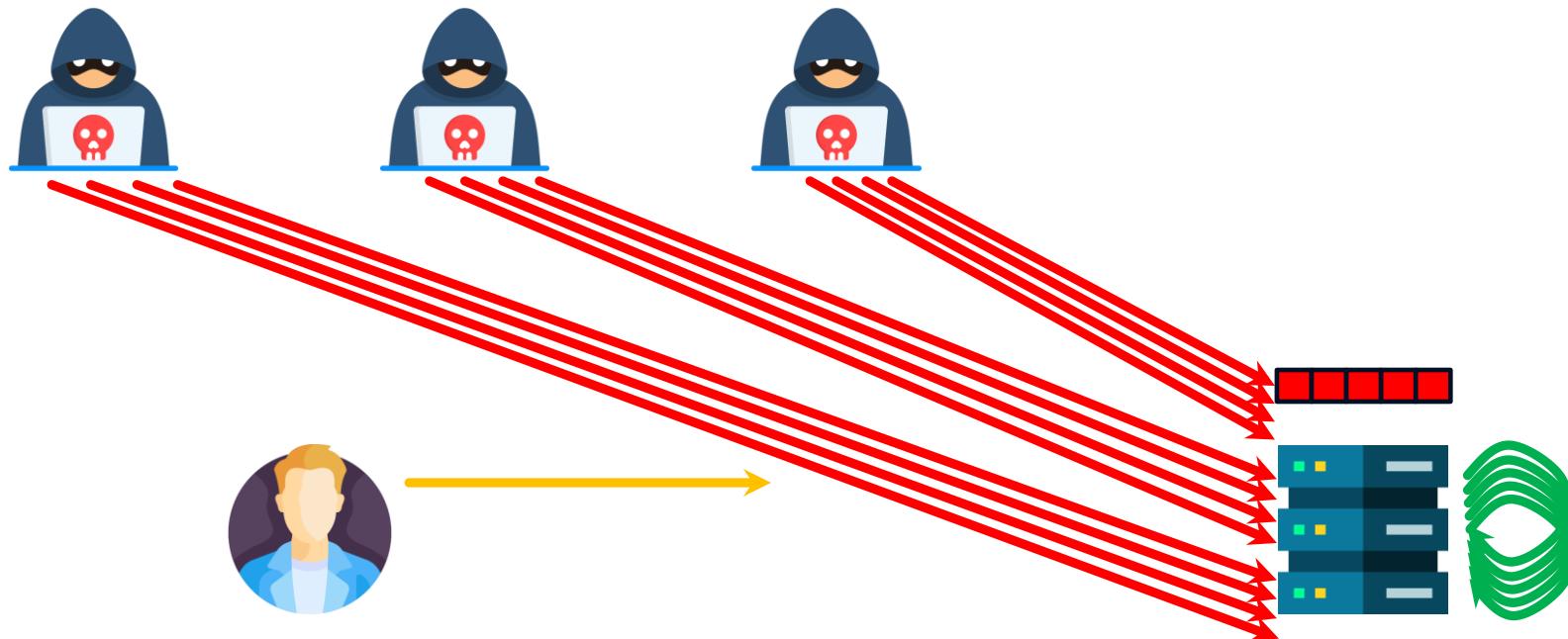
DÉNIS DE SERVICE DISTRIBUÉ



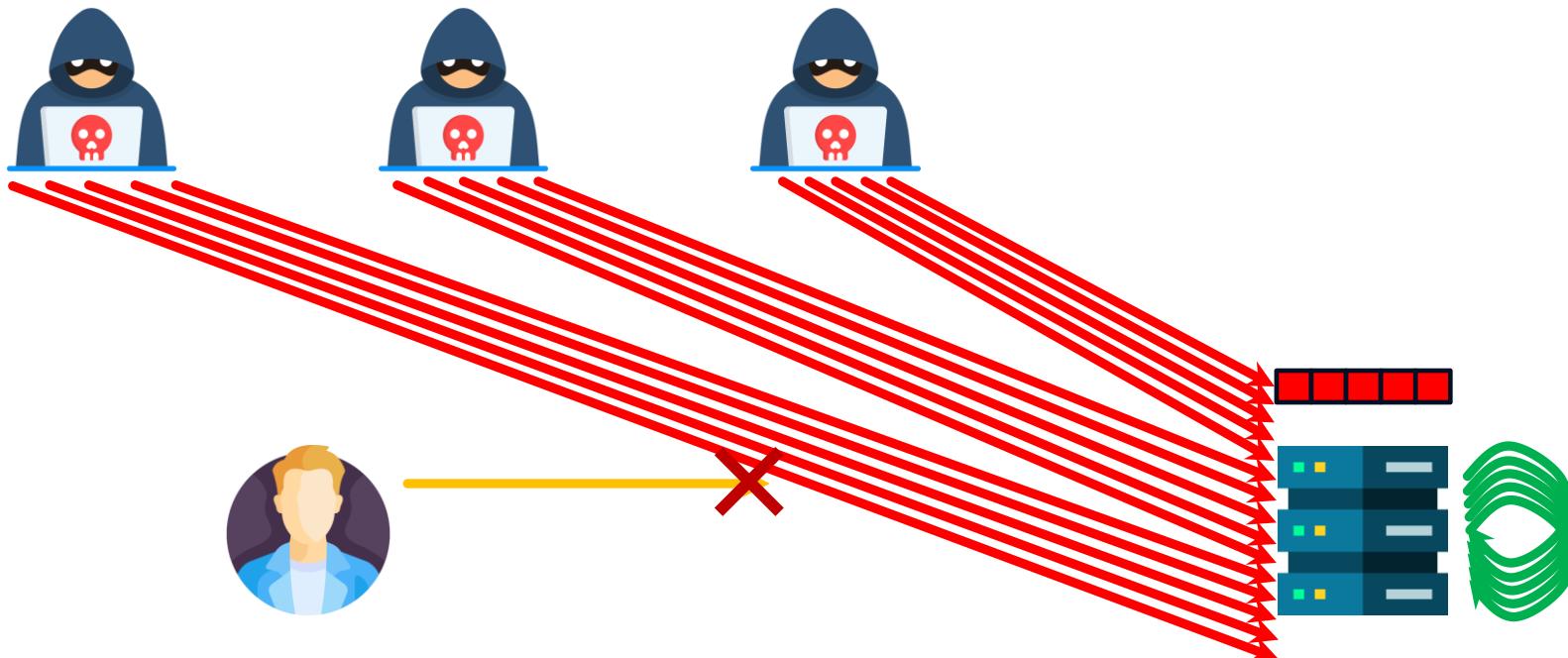
DÉNIS DE SERVICE DISTRIBUÉ



DÉNIS DE SERVICE DISTRIBUÉ



DÉNIS DE SERVICE DISTRIBUÉ



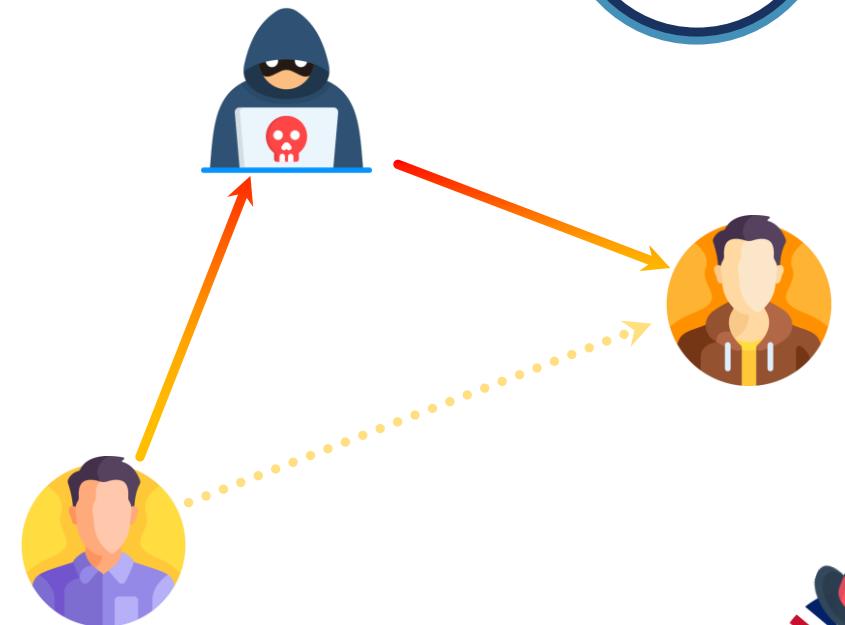
MAN-IN-THE-MIDDLE



S'implanter entre deux entités en communication

- Tromper les participants à communiquer via l'attaquant
 - Complètement transparent pour les deux participants
- Accès direct au traffic

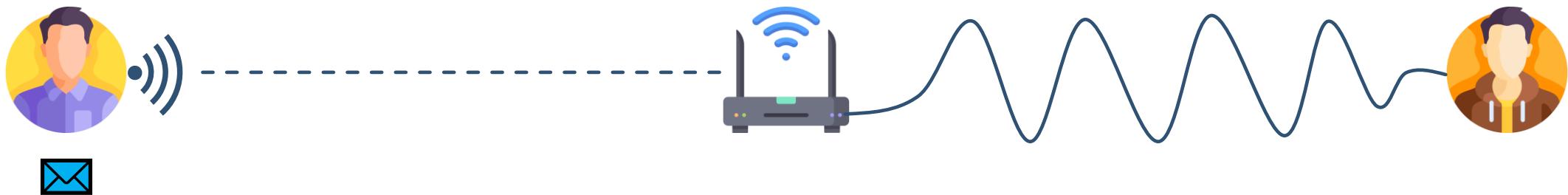
- Possibilité d'agir sur le flux
 - Retirer le chiffrement → SSLStrip
 - Modifier ou supprimer certaines données



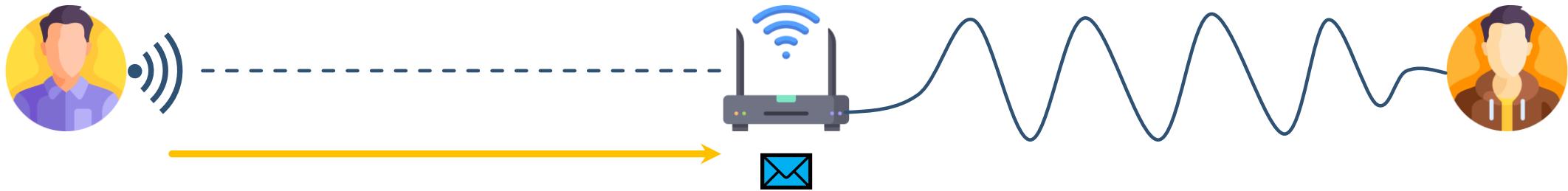
MAN-IN-THE-MIDDLE



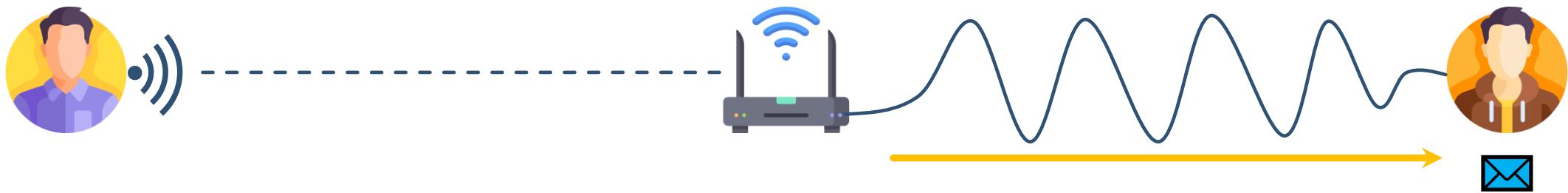
MAN-IN-THE-MIDDLE



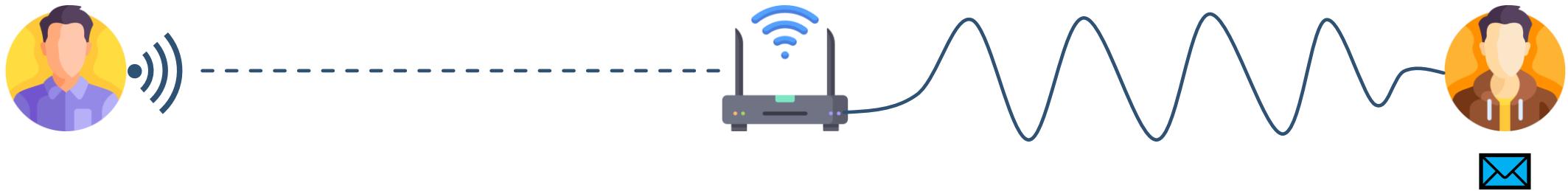
MAN-IN-THE-MIDDLE



MAN-IN-THE-MIDDLE



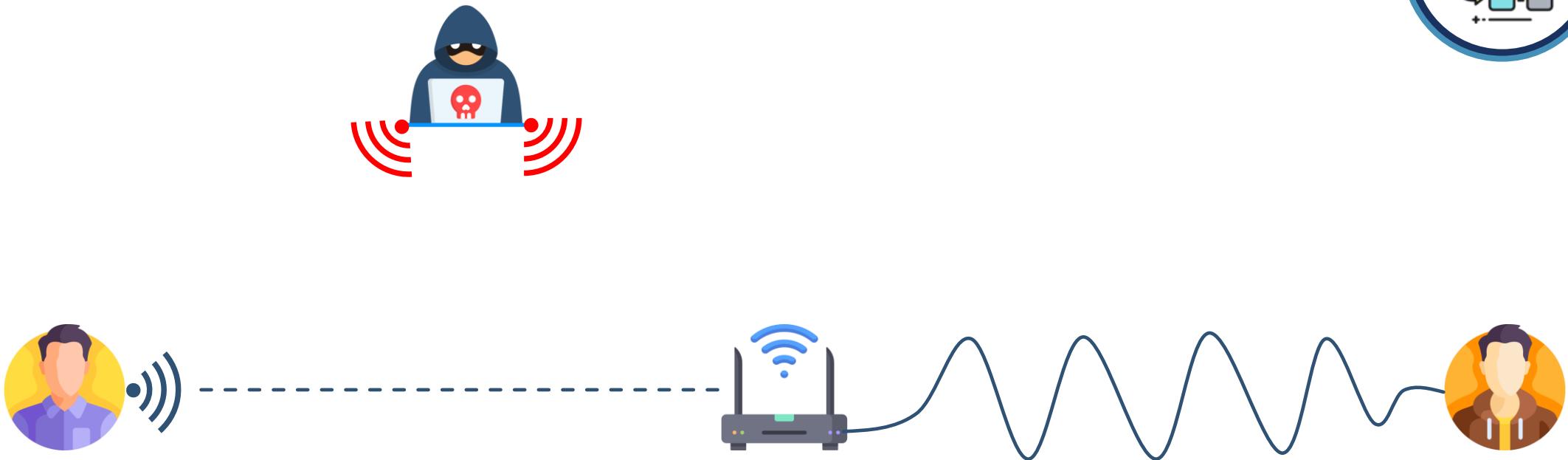
MAN-IN-THE-MIDDLE



MAN-IN-THE-MIDDLE



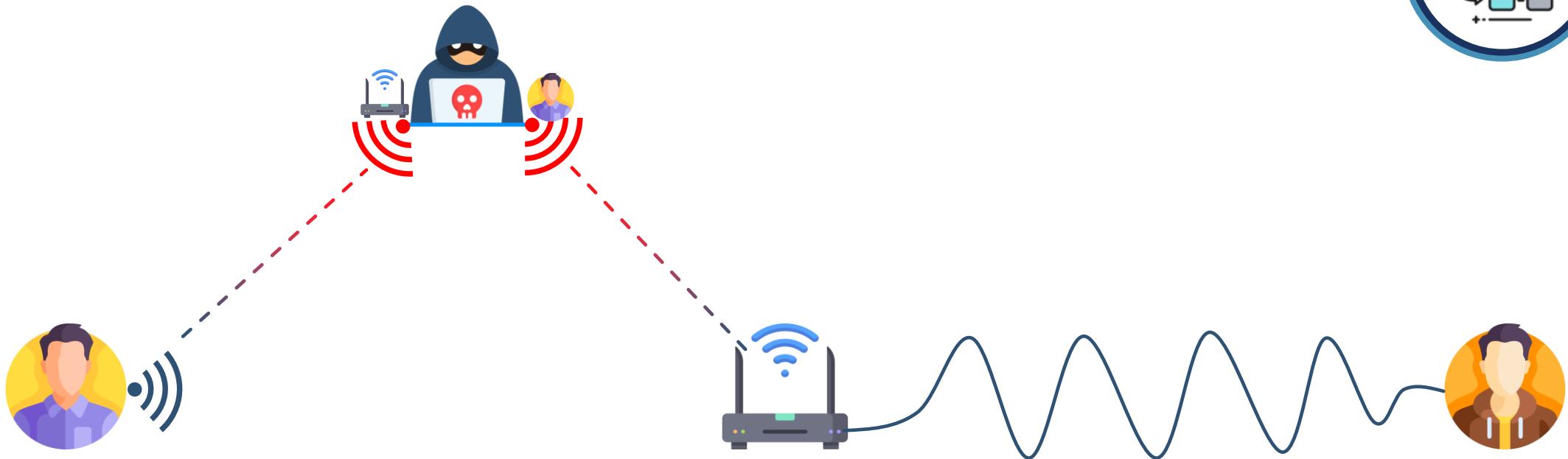
MAN-IN-THE-MIDDLE



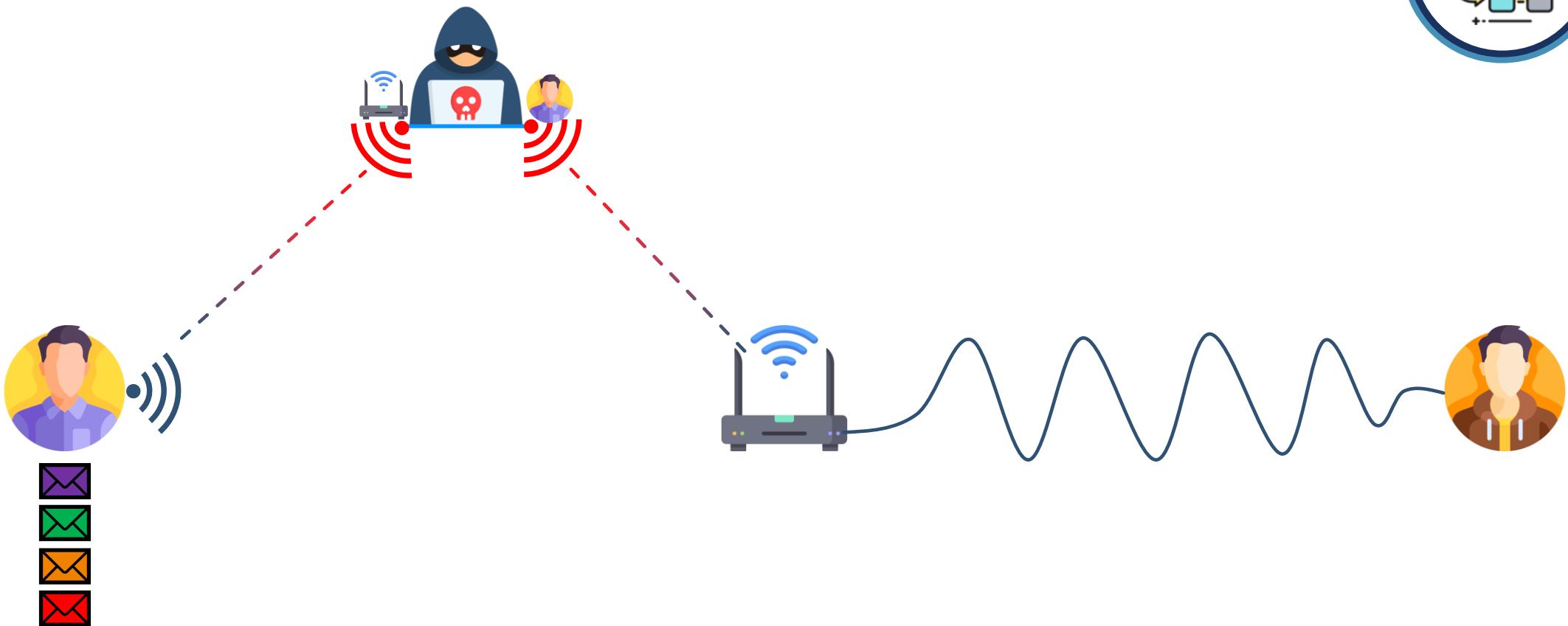
MAN-IN-THE-MIDDLE



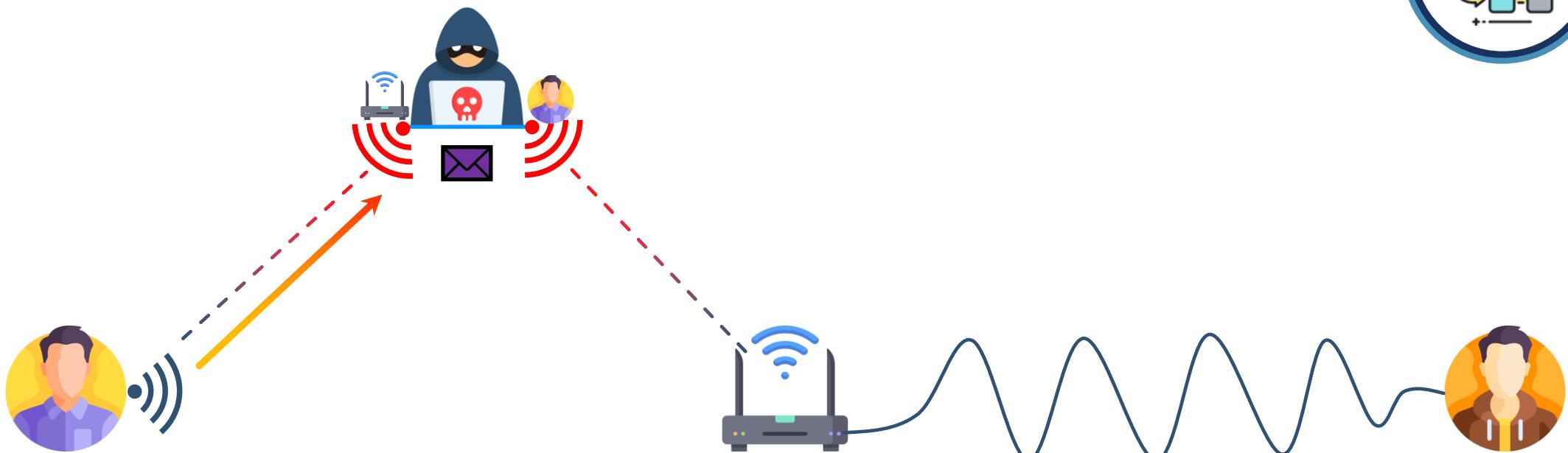
MAN-IN-THE-MIDDLE



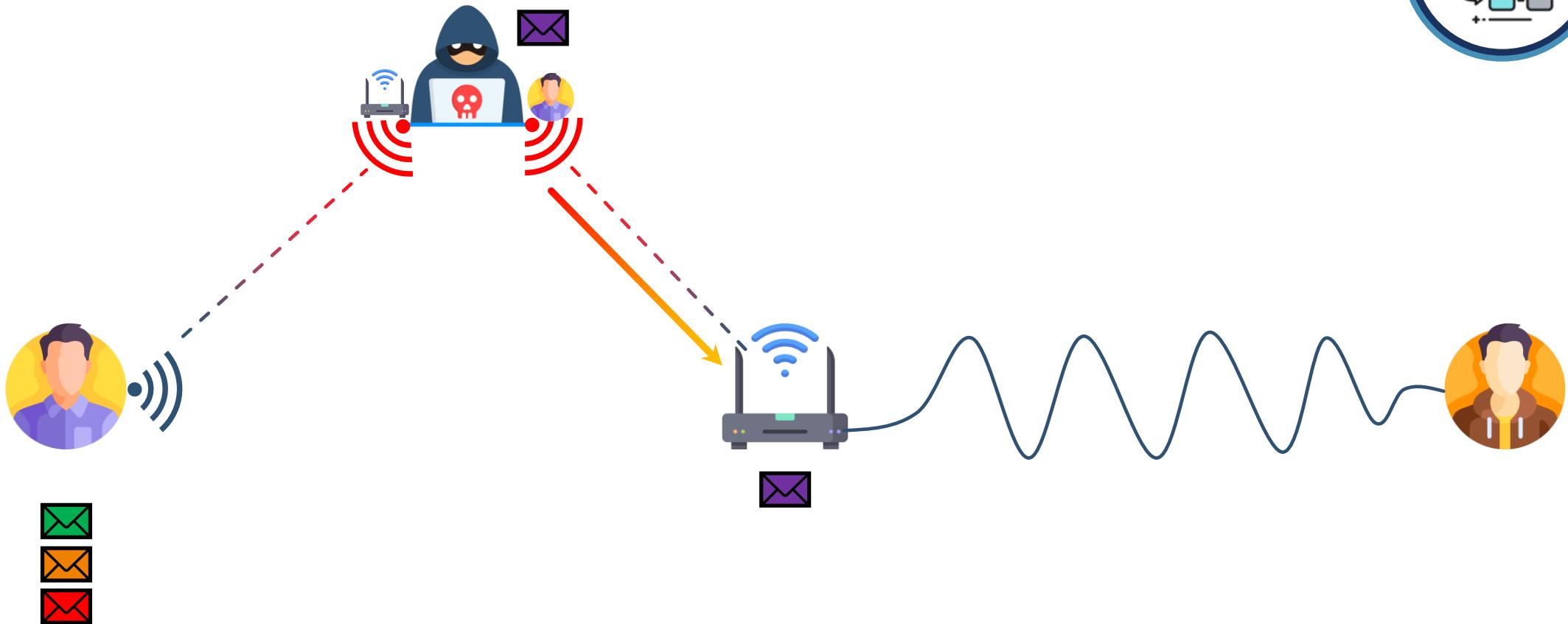
MAN-IN-THE-MIDDLE



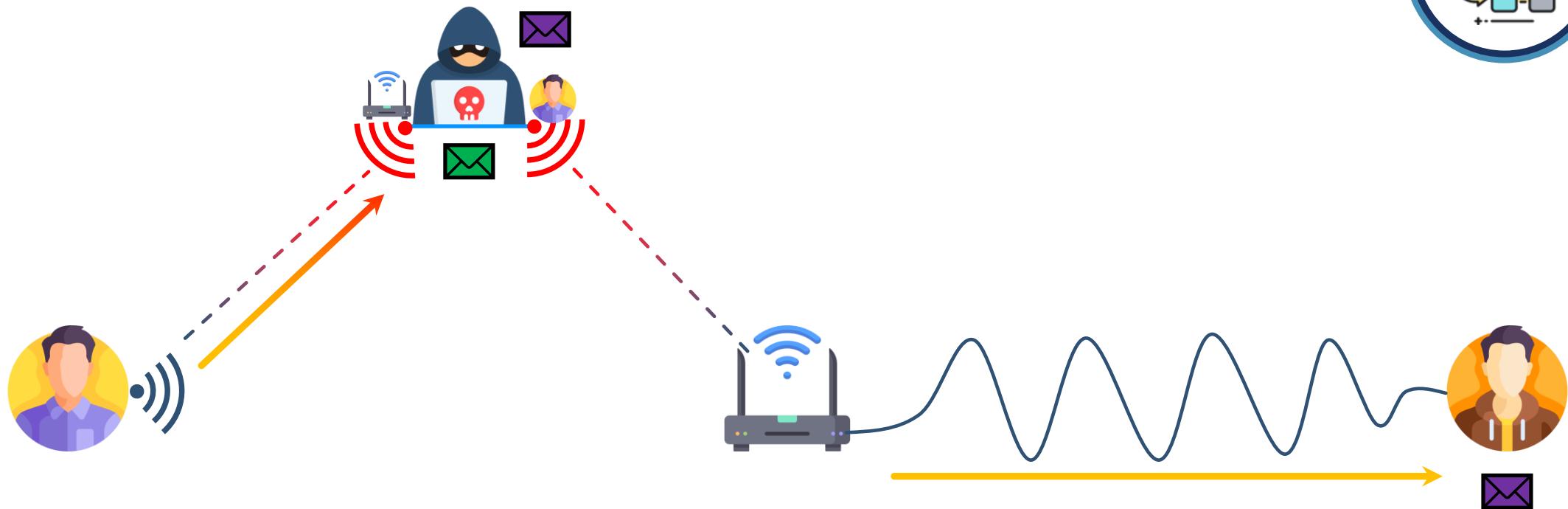
MAN-IN-THE-MIDDLE



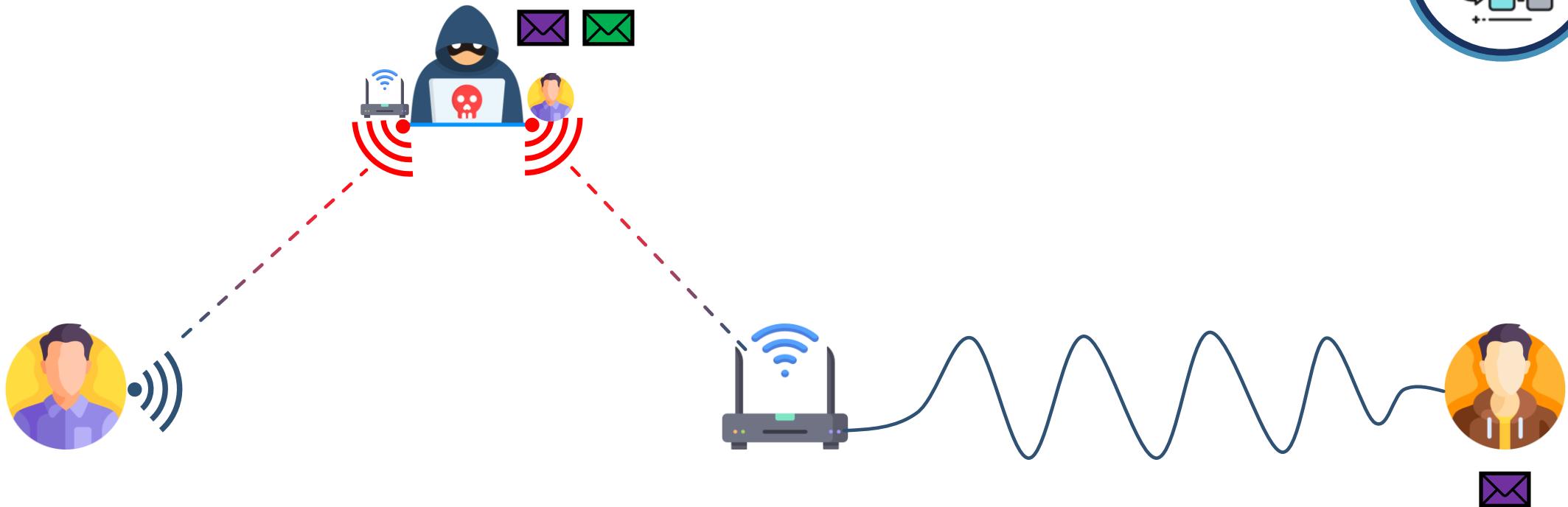
MAN-IN-THE-MIDDLE



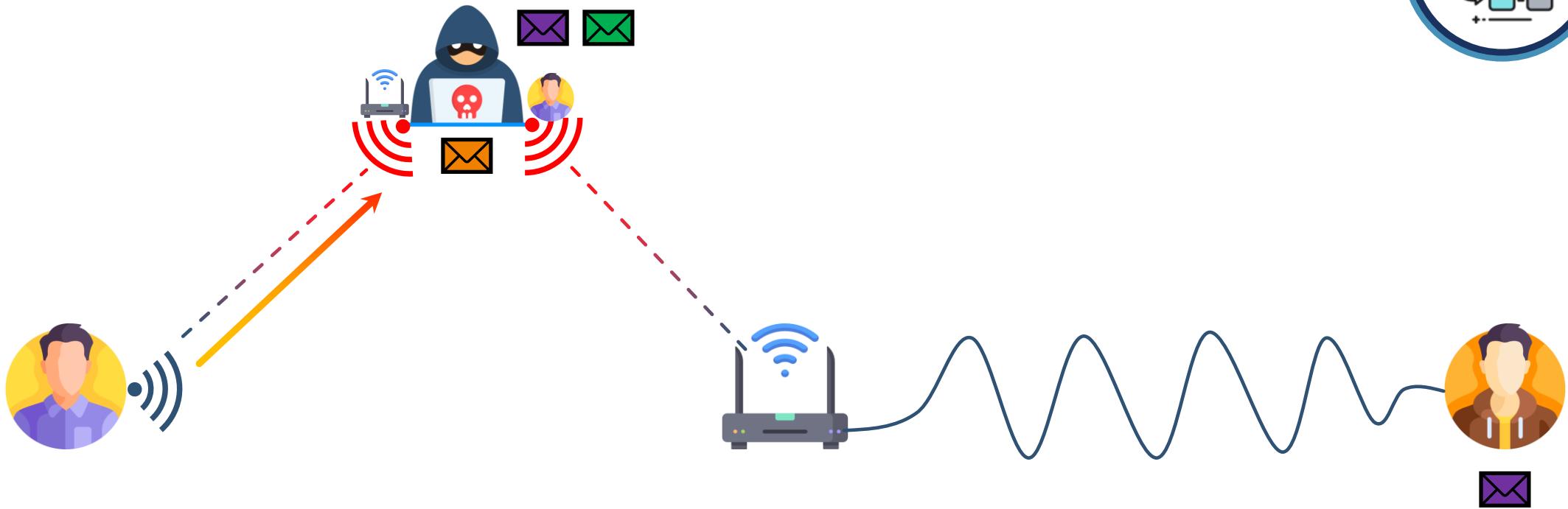
MAN-IN-THE-MIDDLE



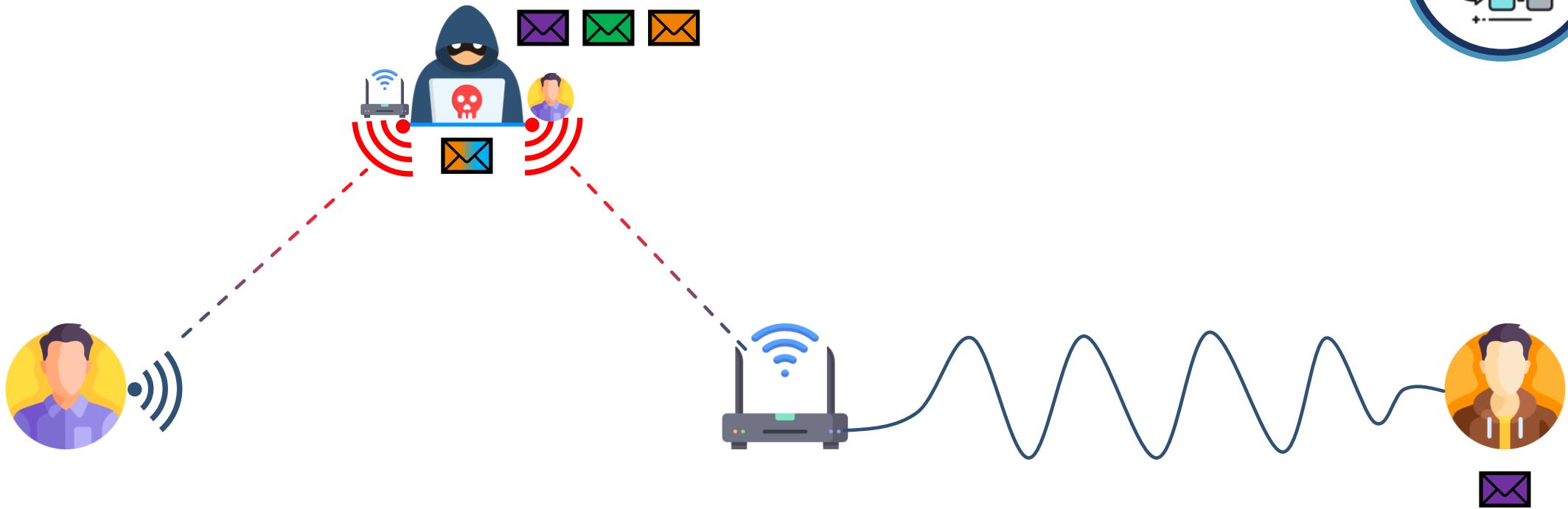
MAN-IN-THE-MIDDLE



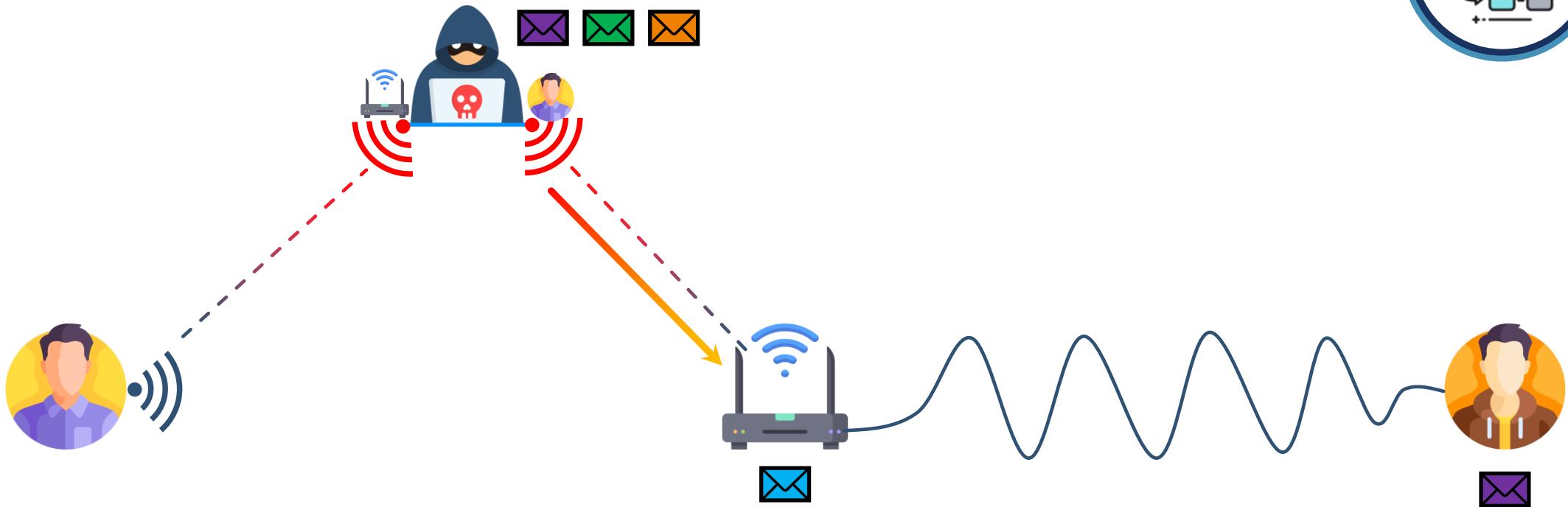
MAN-IN-THE-MIDDLE



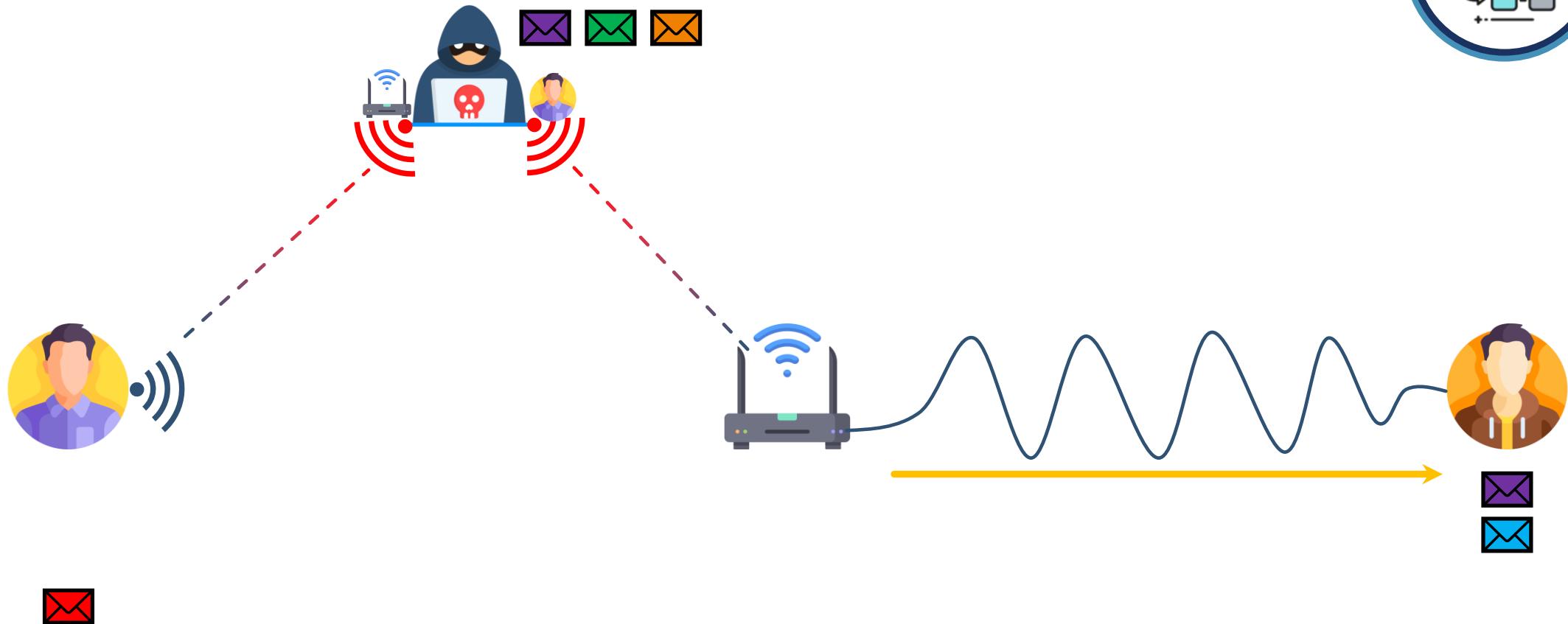
MAN-IN-THE-MIDDLE



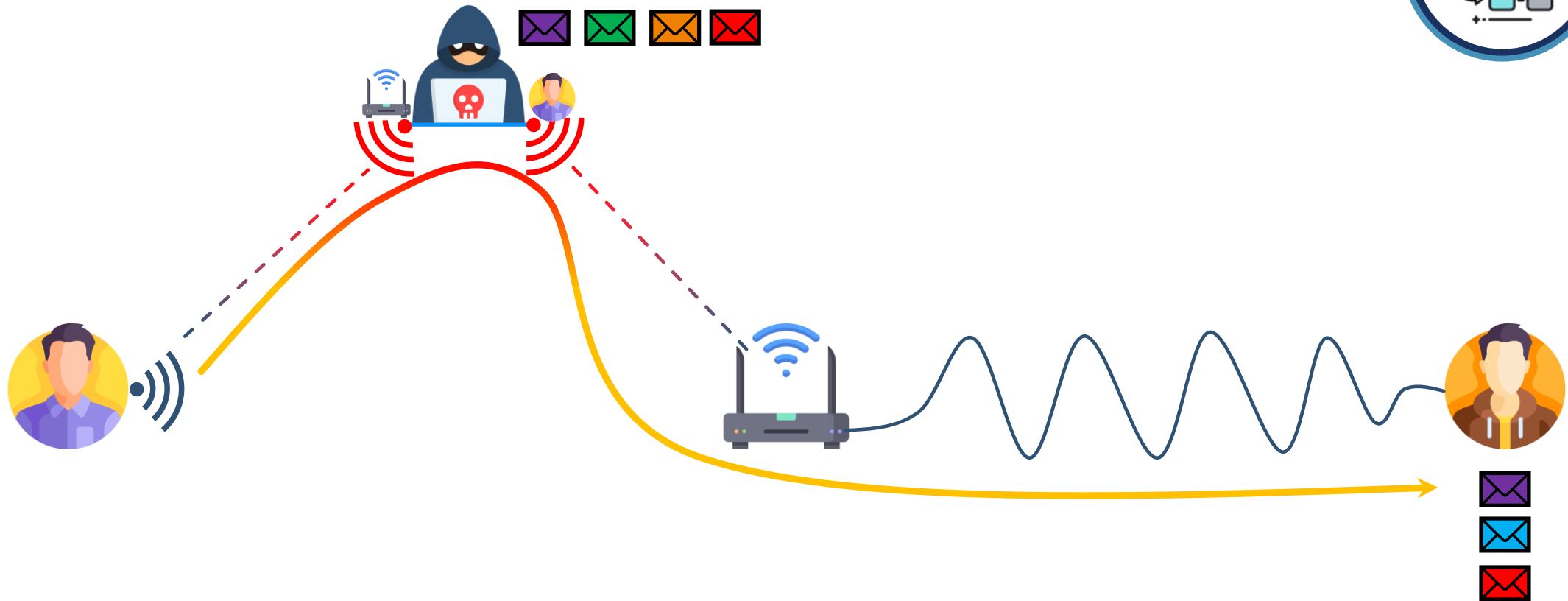
MAN-IN-THE-MIDDLE



MAN-IN-THE-MIDDLE



MAN-IN-THE-MIDDLE

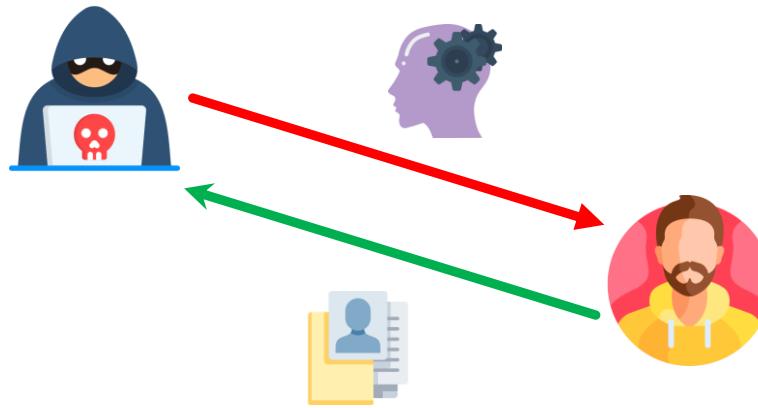


INGÉNIERIE SOCIALE



Manipulation psychologique pour escroquerie

- Tromper sa cible pour extraire des informations
 - Personnels ou Professionnels
 - Voler les identifiants de sa cible pour continuer le cycle
- Plusieurs méthodes existent
 - Filoutage, Spoofing, Whaling, Provocation, Prétexte, Attaque de point d'eau, etc...



INGÉNIERIE SOCIALE – FILOUTAGE

Attaque le plus commun – Hameçonnage

- Technique de fraude
- Effectuer de l'usurpation d'identité
- Faire croire à la victime de s'adresser à une entité de confiance
 - *Spoofing*
- Peut être adapté à la cible → *Whaling*
- Plusieurs moyens disponibles
 - Mail → Plus commun et méthode le plus ancien
 - SMS → Plus récent et devient de plus en plus utilisé (*SMiShing*)



INGÉNIERIE SOCIALE – FILOUTAGE



"Administration Universitaire" <prenom.nom@etu.sorbonne-universite.fr>

Vérifiez vos informations pour l'annuaire 2024 2 August, 2024 04:26

From: Administration Universitaire

Bonjour à toutes et à tous,

Dans le cadre de la mise à jour de l'annuaire universitaire pour l'année 2024,

Nous vous invitons à cliquer sur le lien ci-dessous pour procéder à la mise à jour de vos informations :

Mise à jour de l'annuaire 2024

Nous vous remercions pour votre confiance.



URL pas universitaire → utilisation du service qrcod pour cacher le vrai lien



INGÉNIERIE SOCIALE – PROVOCATION



Promettre quelque chose en retour d'informations sensibles

- Jouer sur la cupidité des personnes
- Attaque très couramment fait par mail, mais également en personne
- Ex: Arnaque nigériane – Fraude 419
 - Réception d'un mail / courrier d'un prince nigérian
 - Promettre une grosse somme d'argent en retour d'une « aide » financière afin de le débloquer

PRINCE JONES DIMKA
52/54 SHASHA ROAD, P.A.
DOPEMU - AGEGE
LAGOS - NIGERIA.
FAX: 234-1-521075

ATTENTION: THE MANAGING DIRECTOR

DEAR SIR,

URGENT BUSINESS PROPOSAL

WE HAVE THIRTY MILLION U.S. DOLLARS WHICH WE GOT FROM OVER INFLATED CONTRACT FROM CRUDE OIL CONTRACT AWARDED TO FOREIGN CONTRACTORS IN THE NIGERIAN NATIONAL PETROLEUM CORPORATION (NNPC). WE ARE SEEKING YOUR ASSISTANCE AND PERMISSION TO REMIT THIS AMOUNT INTO YOUR ACCOUNT. YOUR COMMISSION IS THIRTY PERCENT OF THE MONEY.

PLEASE NOTIFY ME YOUR ACCEPTANCE TO DO THIS BUSINESS URGENTLY. THE MEN INVOLVED ARE MEN IN GOVERNMENT. MORE DETAILS WILL BE SENT TO YOU BY FAX AS SOON AS WE HEAR FROM YOU. FOR THE PURPOSE OF COMMUNICATION IN THIS MATTER, MAY WE HAVE YOUR TELEFAX, TELEX AND TELEPHONE NUMBERS INCLUDING YOUR PRIVATE HOME TELEPHONE NUMBER.

CONTACT ME URGENTLY THROUGH THE FAX NUMBER ABOVE.

PLEASE TREAT AS MOST CONFIDENTIAL, ALL REPLIES STRICTLY BY DHL COURIER, OR THROUGH ABOVE FAX NUMBER.

THANKS FOR YOUR CO-OPERATION.

YOURS FAITHFULLY,

Elieben
PRINCE JONES DIMKA
3-4-95

Baiting



INGÉNIERIE SOCIALE – ATTAQUE DE POINT D'EAU



Observation des habitudes des utilisateurs pour identifier un point « commun »

- Basé sur les méthodes d'observation animalier
 - Difficile d'attraper un animal sauvage dans la nature
 - Identification d'un point d'eau à proximité fréquenté par les animaux
 - Attendre à côté que l'animal ciblé arrive
- Méthodologie adaptée à l'informatique
 - Identification d'un site web fréquenté par une entreprise cible
 - Infection du site → infection du visiteur → infection de l'entreprise

2011 – Opération Torpille

Saisie et modification de 3 sites web Tor par le FBI pour afficher l'adresse IP des visiteurs
→ Ajout d'un code intégré à Adobe Flash pour ping le serveur FBI hors réseau Tor

2017 – CCleaner

Introduction de malware dans l'exe officiel
L'environnement de dev / build a été infecté
→ signature des exe avec le certificat officiel du développeur



CROSS-SITE SCRIPTING



Injection de contenu dans une page web – XSS

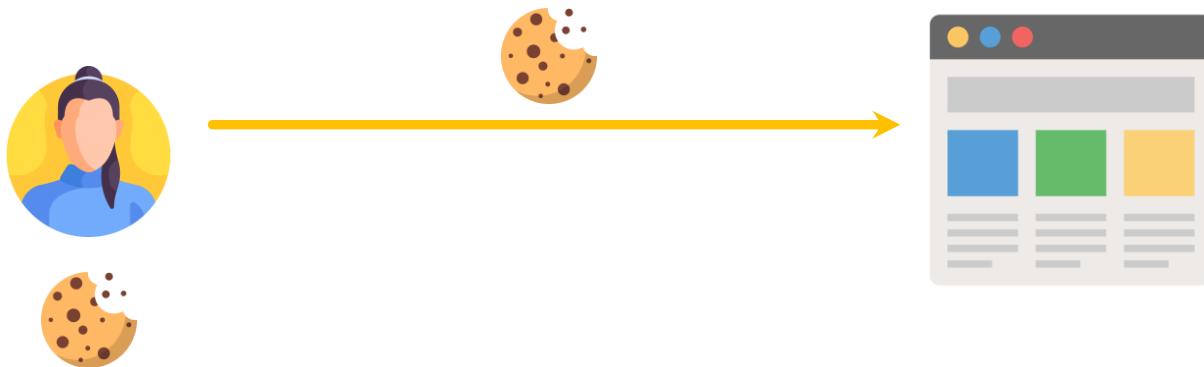
- Exploitation d'une faille de protection
 - Pas de sécurisation des entrées
 - Code exécuté par les navigateurs visiteurs
- Plusieurs possibilités avec HTML5, javascript, etc...
 - Redirection vers un site web pour de l'hameçonnage
 - Voler des cookies de session



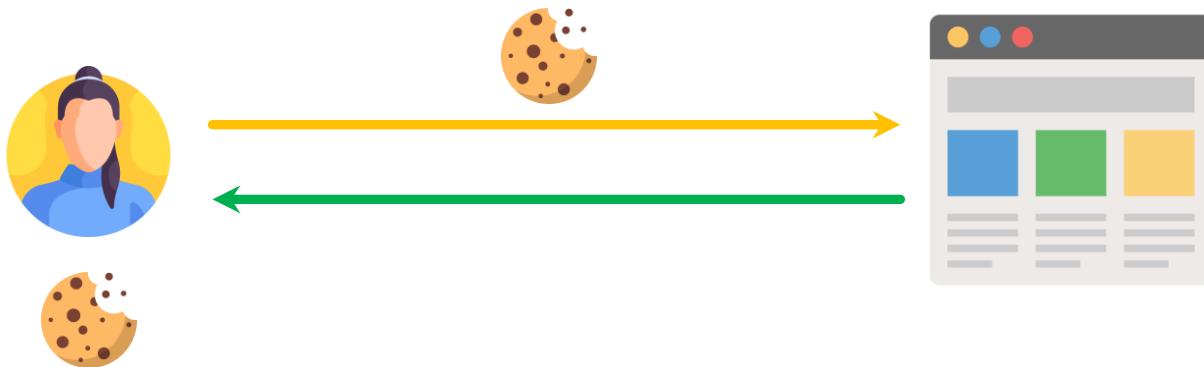
CROSS-SITE SCRIPTING



CROSS-SITE SCRIPTING



CROSS-SITE SCRIPTING



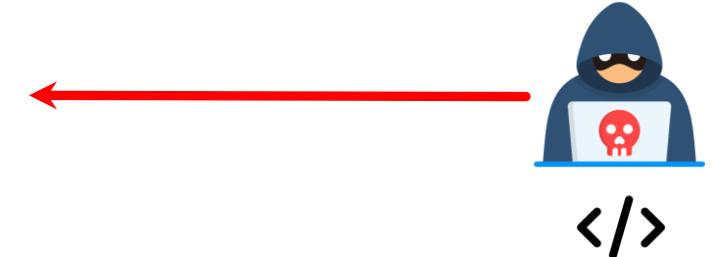
CROSS-SITE SCRIPTING



</>



CROSS-SITE SCRIPTING



CROSS-SITE SCRIPTING



</>

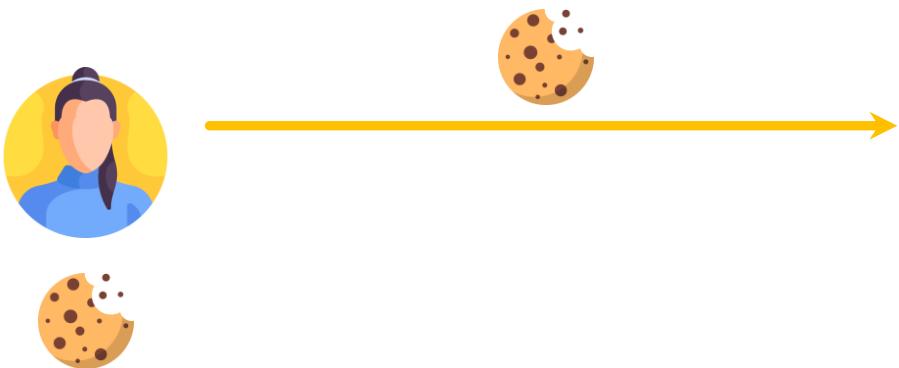


CROSS-SITE SCRIPTING

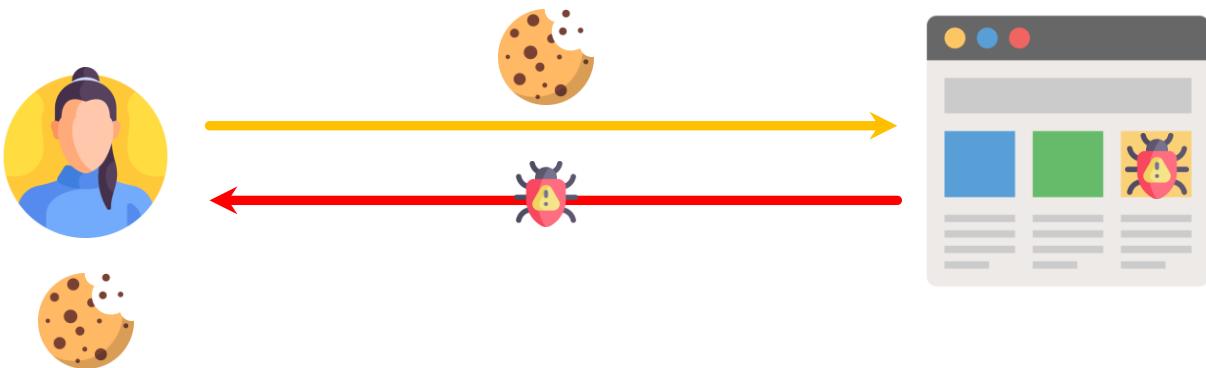


</>

CROSS-SITE SCRIPTING



CROSS-SITE SCRIPTING



CROSS-SITE SCRIPTING



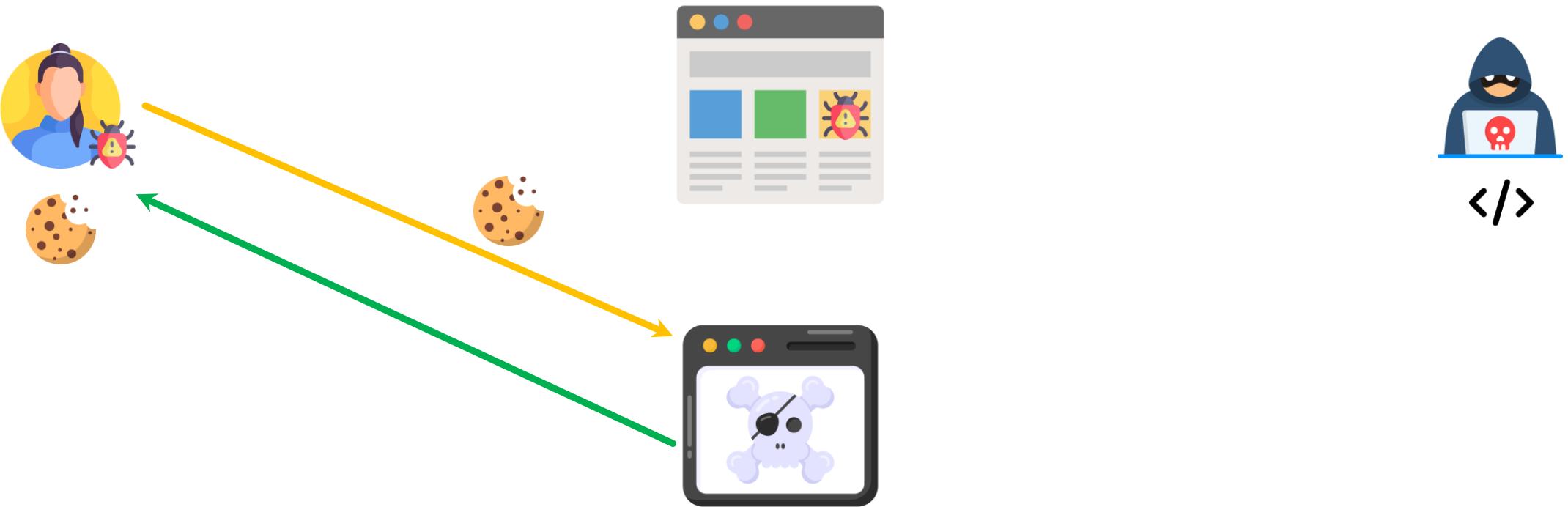
</>



CROSS-SITE SCRIPTING



CROSS-SITE SCRIPTING



CROSS-SITE SCRIPTING



</>

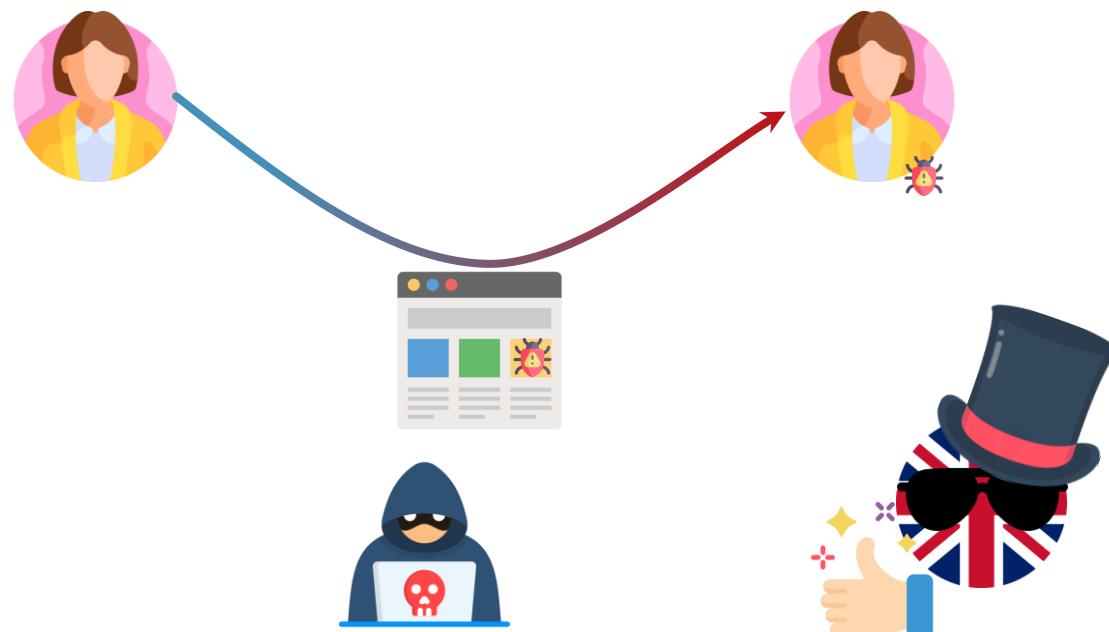
A large red arrow points from the smartphone icon towards the hacker icon.

DRIVE-BY-ATTACK



Téléchargement d'un logiciel inaperçu → Drive-by-Download

- Plusieurs méthodologies
 - Visiter un site web
 - Ouvrir une pièce jointe dans un mail
 - Cliquer sur une publicité inattendue, etc...
- Existence d'une approche d'installation → Drive-by-Install
 - Même méthodologie mais avec installation du logiciel
- Malware, Rançongiciel, Cheval de Troie, etc...



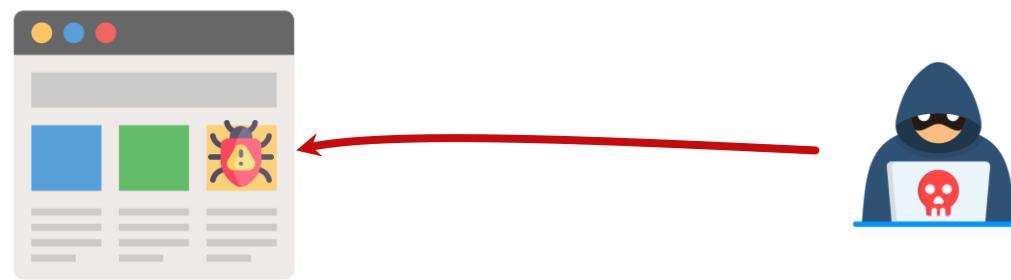
DRIVE-BY-ATTACK



DRIVE-BY-ATTACK



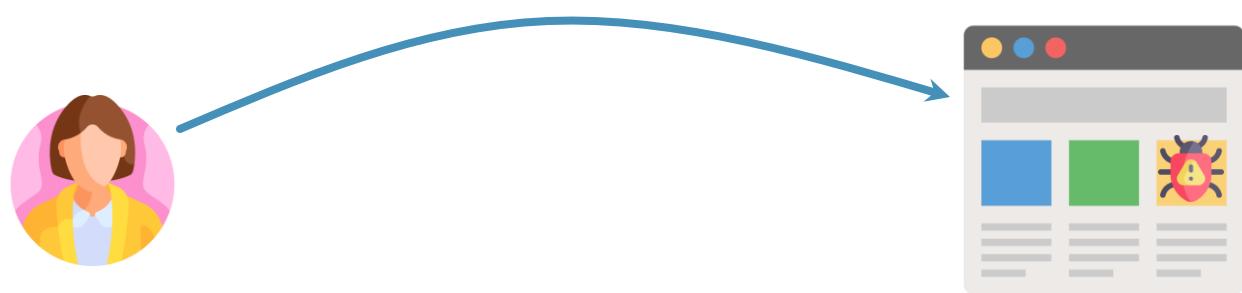
DRIVE-BY-ATTACK



DRIVE-BY-ATTACK



DRIVE-BY-ATTACK



DRIVE-BY-ATTACK



DRIVE-BY-ATTACK



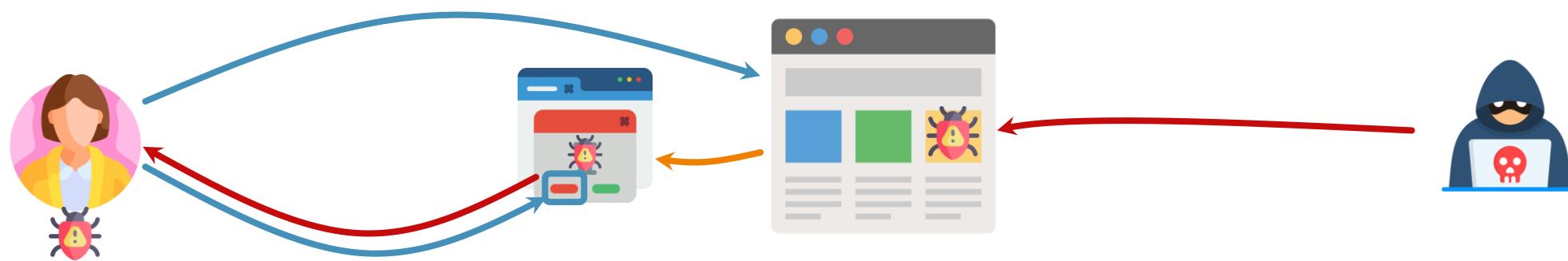
DRIVE-BY-ATTACK



DRIVE-BY-ATTACK



DRIVE-BY-ATTACK



LOGICIEL MALVEILLANT



Programme développé dans le but de nuire à un système informatique

- Sans autorisation de l'utilisateur
- Souvent mélangé avec les « virus »
- Trois mécanismes de classement
 - **Propagation** → ex. ver – se propage sur un réseau informatique
 - **Déclenchement** → ex. bombe logique – se déclenche sur un évènement particulier (i.e. vendredi 13)
 - **Charge utile** → ex. virus Tchernobyl – essaye de supprimer des parties importantes du BIOS
- Plusieurs sous-types (virus, vers, **cheval de Troie**, **rançongiciel**, keyloggers, etc...)

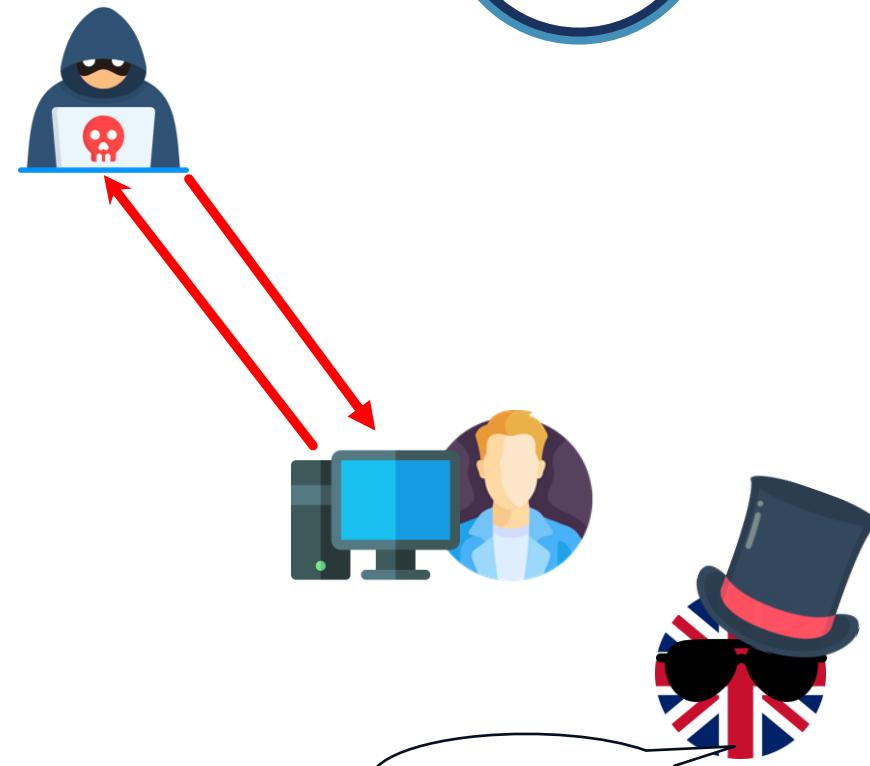


CHEVAL DETROIE



Type de logiciel malveillant qui se « déguise » en logiciel standard

- Dérivé de l'antiquité grecque
 - La chute de la cité de Troie
- Esquive les vérifications de sécurité pour fonctionner sans problème
- N'est pas un virus ou verre → ne se propage pas / n'infecte pas d'autres fichiers
- Généralement utilisé pour fournir un accès à distance
 - Utilisé légalement dans les enquêtes numériques
- Souvent utilisé pour les attaques rançongiciel

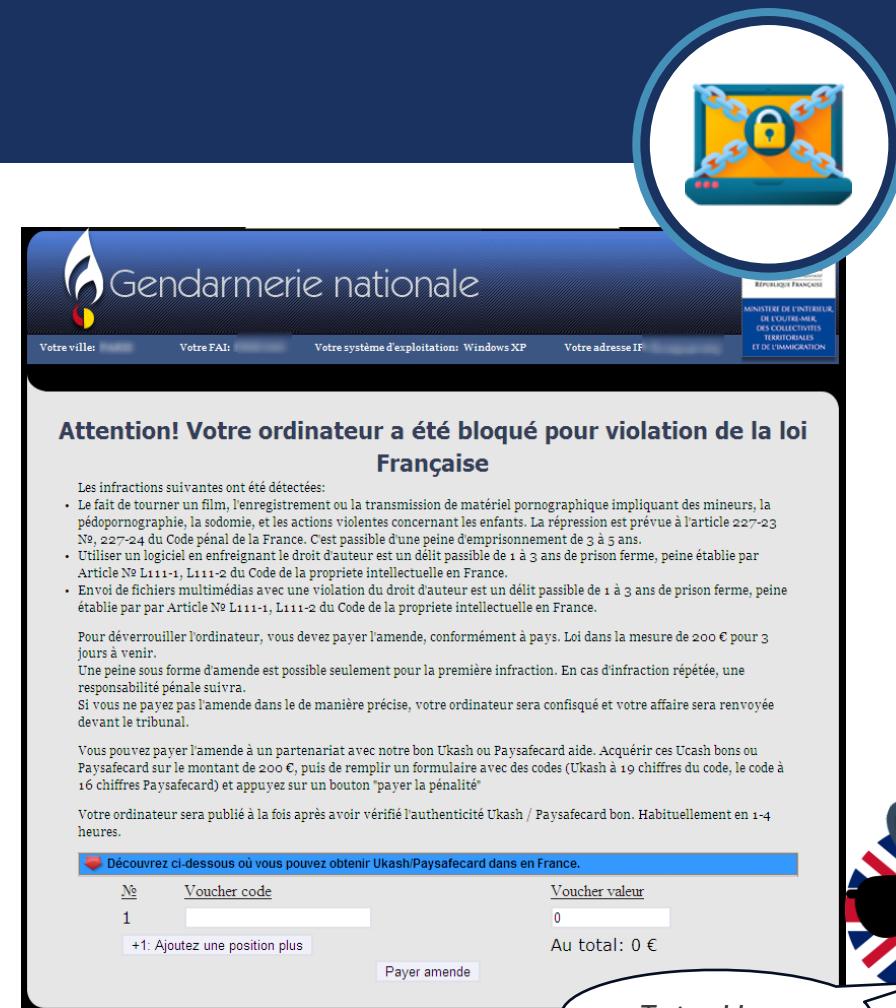


RANÇONGICIEL

Type de logiciel malveillant qui prend en « otage » les données personnelles

- Utilisation de chiffrement pour bloquer l'accès
- Réclame une somme d'argent en échange pour la clé
 - Migration vers crypto → Bitcoin
- Attaque très dévastatrice
 - Attaque **WannaCry**

Attention : Ne jamais payer le rançon → très peu de chance de récupérer une clé qui fonctionne



RANÇONGICIEL -- WANNACRY



Attaque mondiale en mai 2017

- Utilisation d'un rançongiciel ver auto-répliquant
- Ciblant des machines Windows
- Chiffrant tous les données en demandant du Bitcoin
- Propagation via EternalBlue
 - Exploit développé par la NSA
 - Utilisant une faille dans SMBv1
 - Publié par le groupe de hackers « **The Shadow Brokers** »
- Infection très prononcée chez les anciennes versions de Windows
 - XP, Server 2003

Patch existant depuis mars 2017

Première publication de patch pour des systèmes non maintenues



Carte estimative des pays infectés

RANÇONGICIEL -- WANNACRY



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>. But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled. Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>. Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>. And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
GMT from Monday to Friday

Send \$300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Contact Us

Check Payment

Decrypt

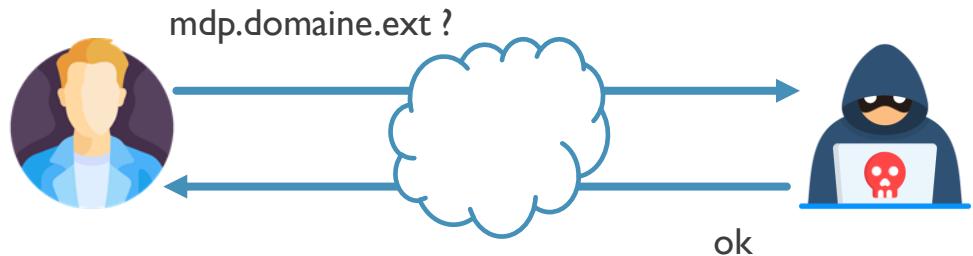
The screenshot shows a Windows-style dialog box titled "Wana Decrypt0r 2.0". It displays a message: "Ooops, your files have been encrypted!". The interface is primarily red and white. It contains several sections of text and two large rectangular boxes on the left side. Each box has a title, a date and time, a progress bar, and a "Time Left" indicator. The top box is for payment due on 5/16/2017 at 00:47:55, with 2:23:57:37 left. The bottom box is for file loss on 5/20/2017 at 00:47:55, with 6:23:57:37 left. At the bottom, there are links for "About bitcoin" and "How to buy bitcoins?", a "Contact Us" button, and two main action buttons: "Check Payment" and "Decrypt". A "Send \$300 worth of bitcoin to this address:" field contains the Bitcoin address 12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw, which is also copied to the clipboard.

DNS TUNNELING

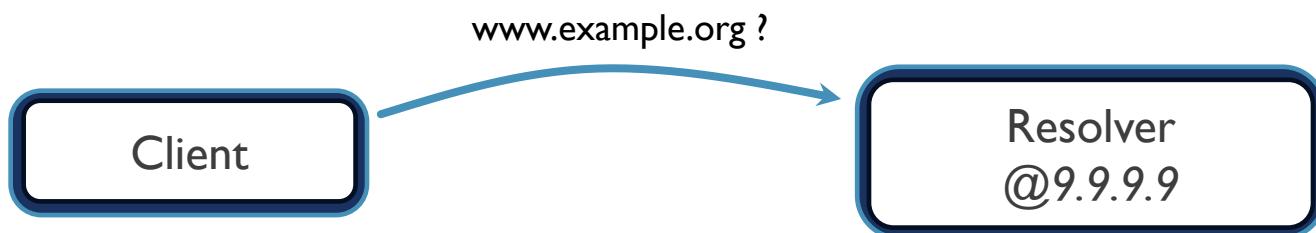


Exploitation de l'échange DNS pour transmettre des données

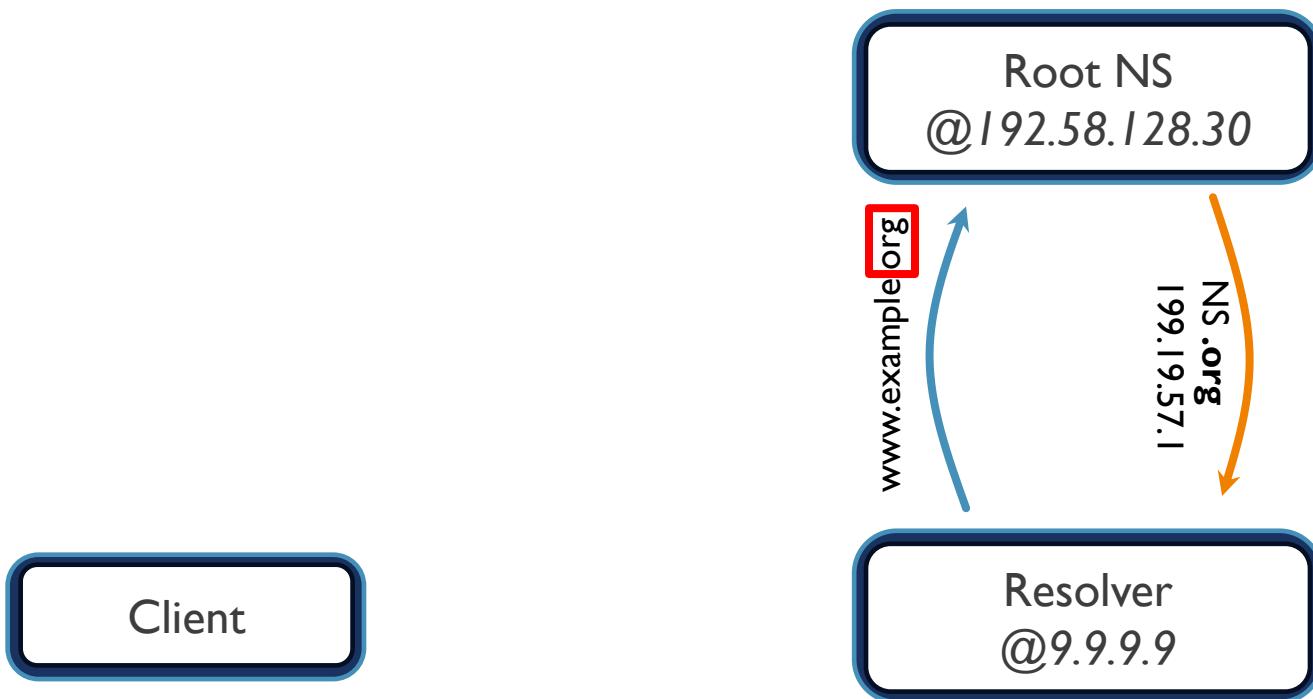
- Utilisation du mécanisme client-serveur préexistant
- Permet de contourner des systèmes de protection
 - DNS élément fondamental en réseau
- Utilisation de « sous-domaines » comme méthode de transport
 - Requêtes DNS orientés automatiquement vers domaine de l'attaquant
 - Réponses orientées automatiquement vers la victime



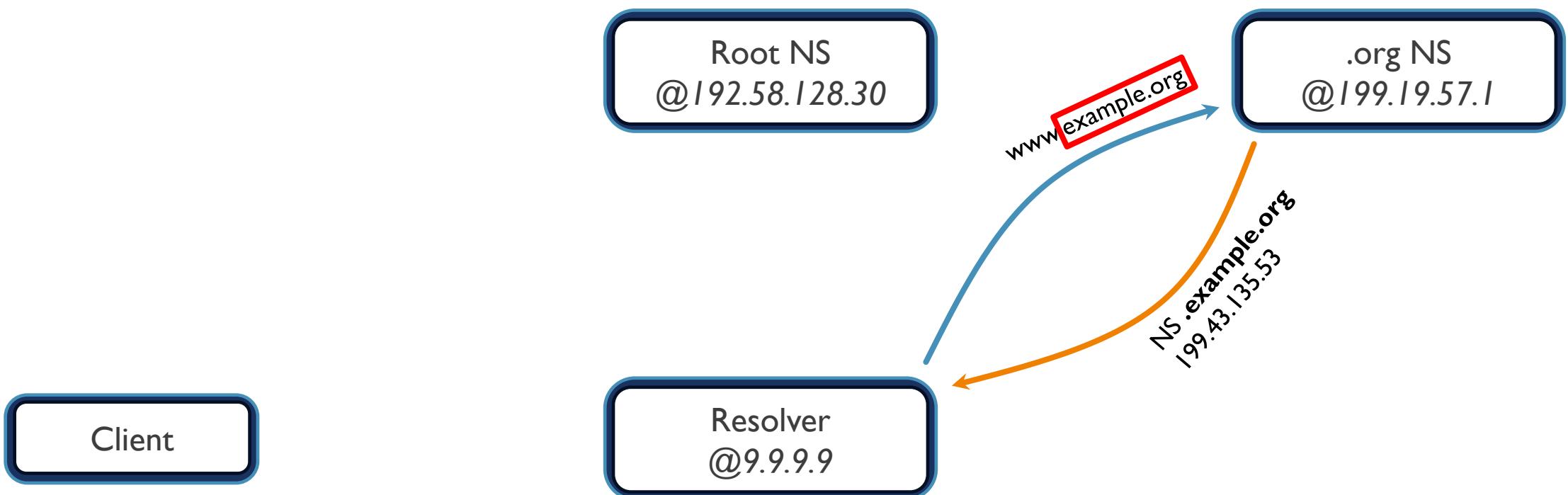
RAPPEL DNS



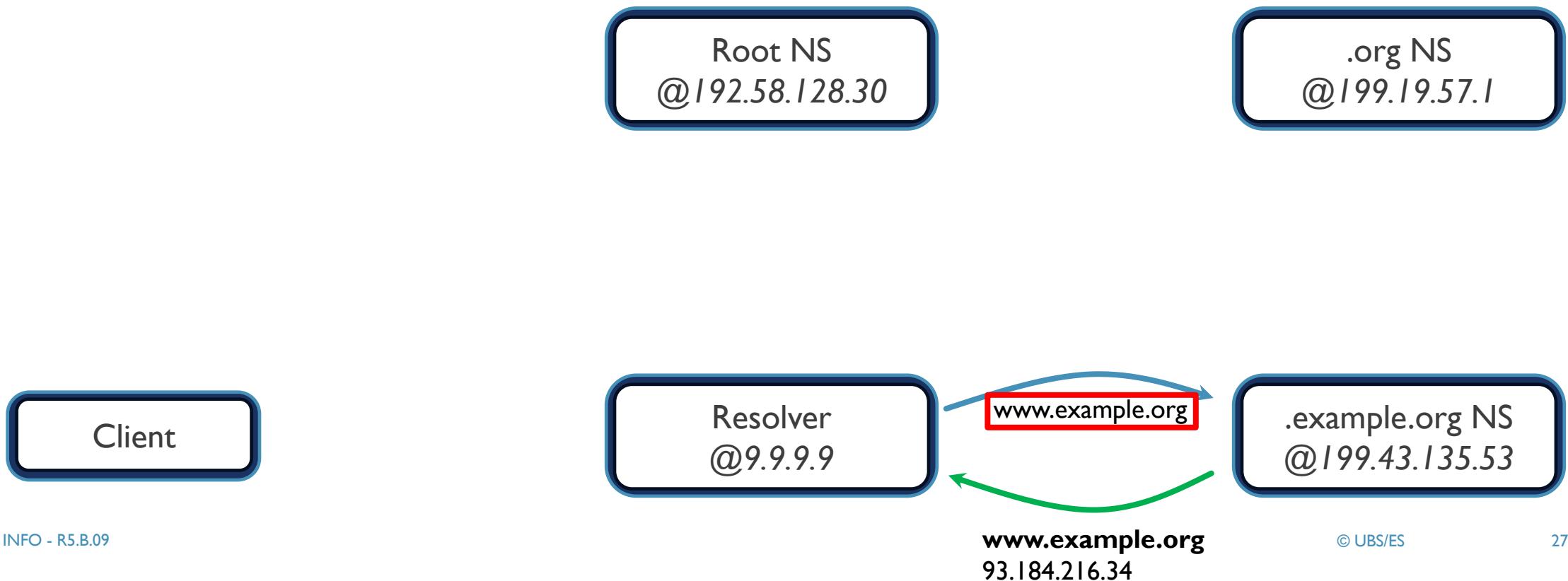
RAPPEL DNS



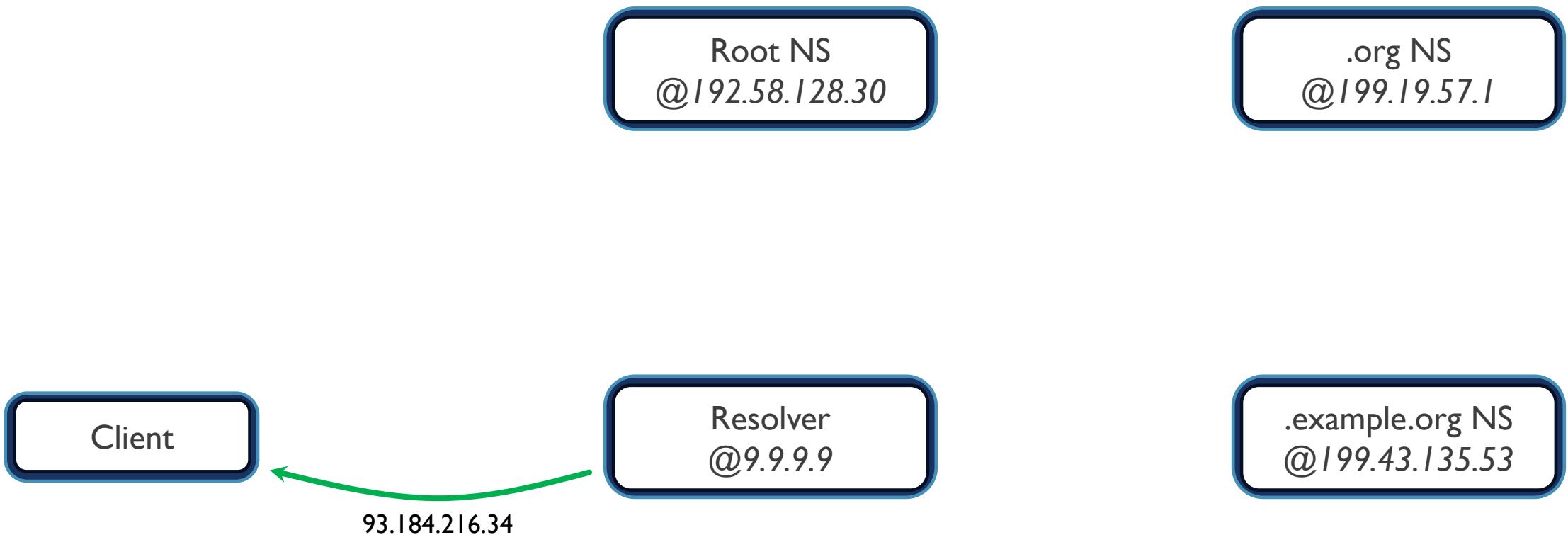
RAPPEL DNS



RAPPEL DNS



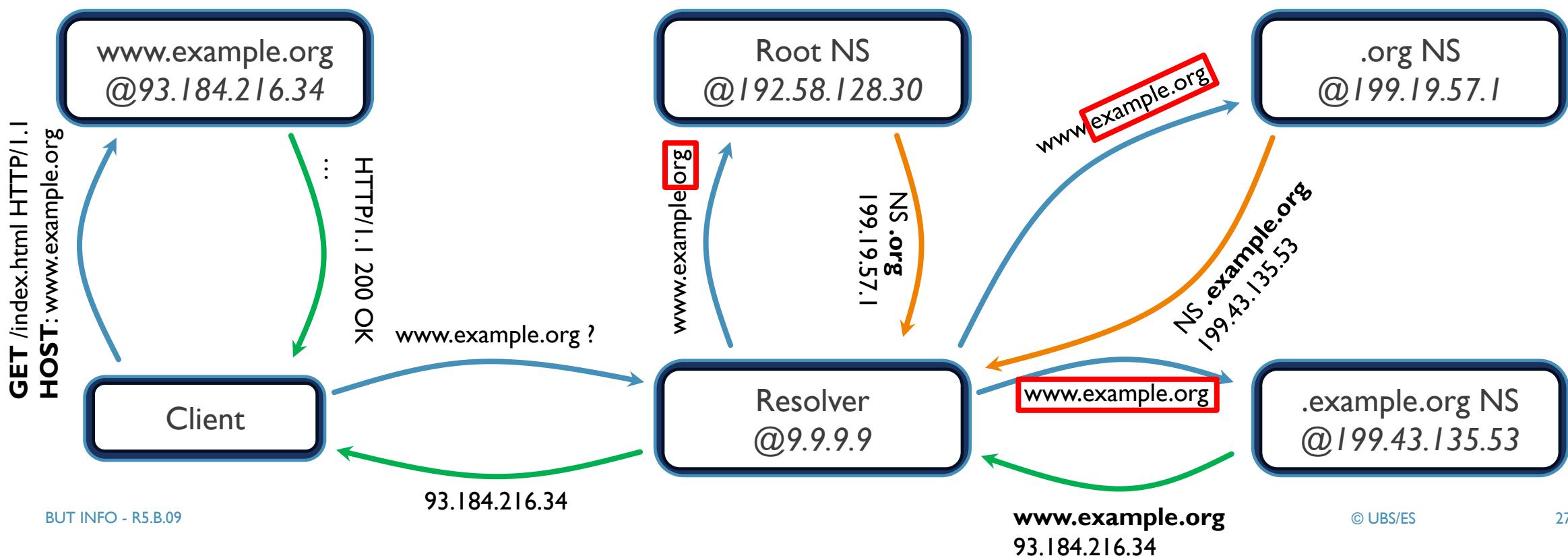
RAPPEL DNS



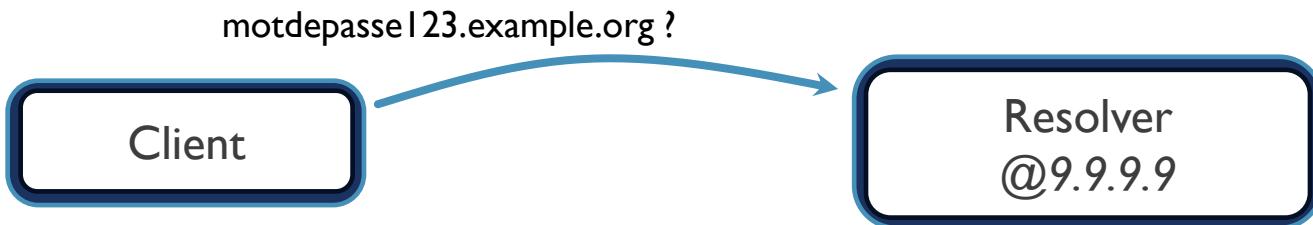
RAPPEL DNS



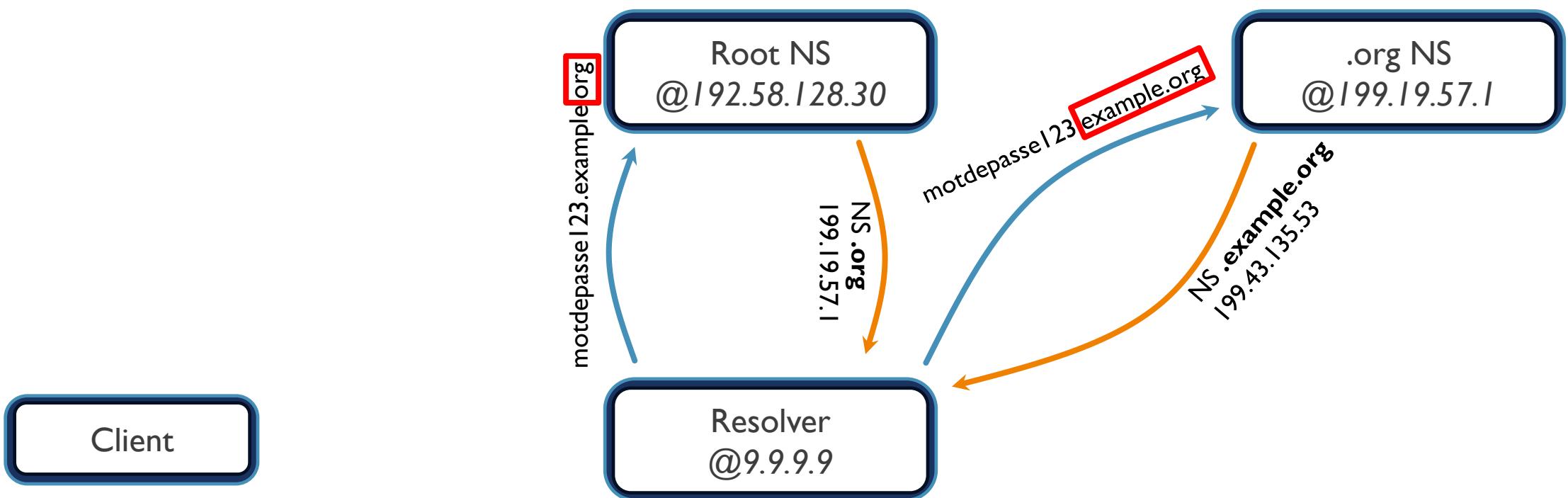
RAPPEL DNS



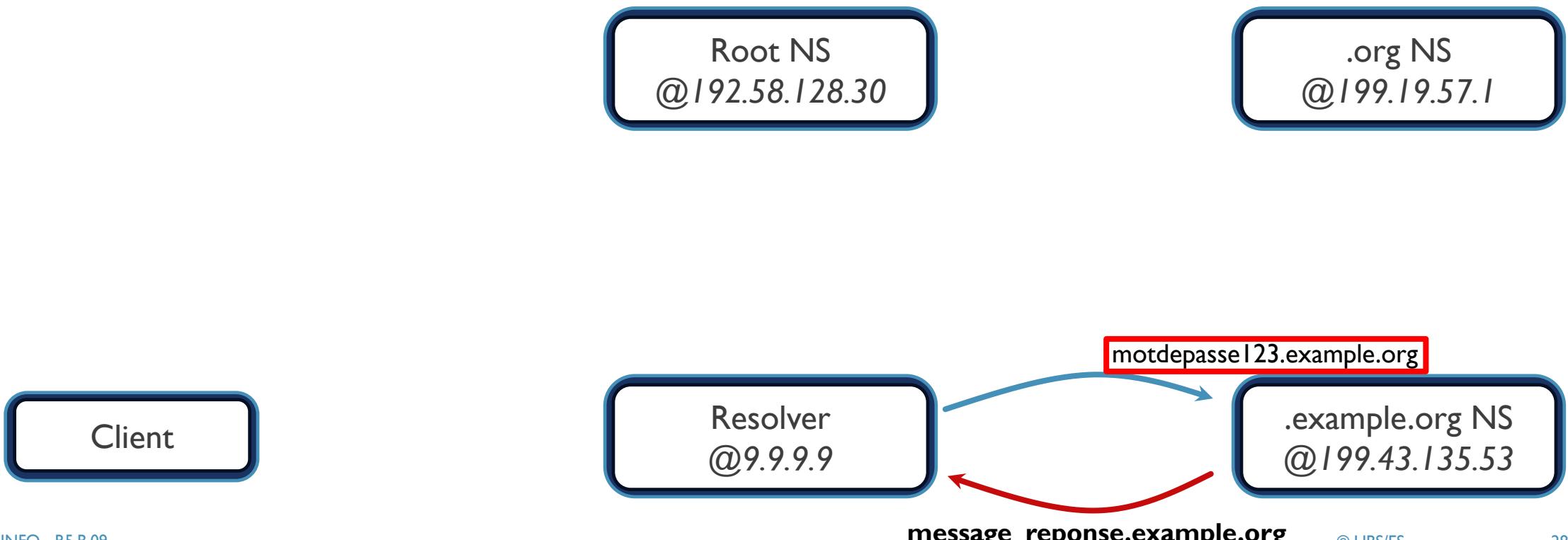
DNS TUNNELING



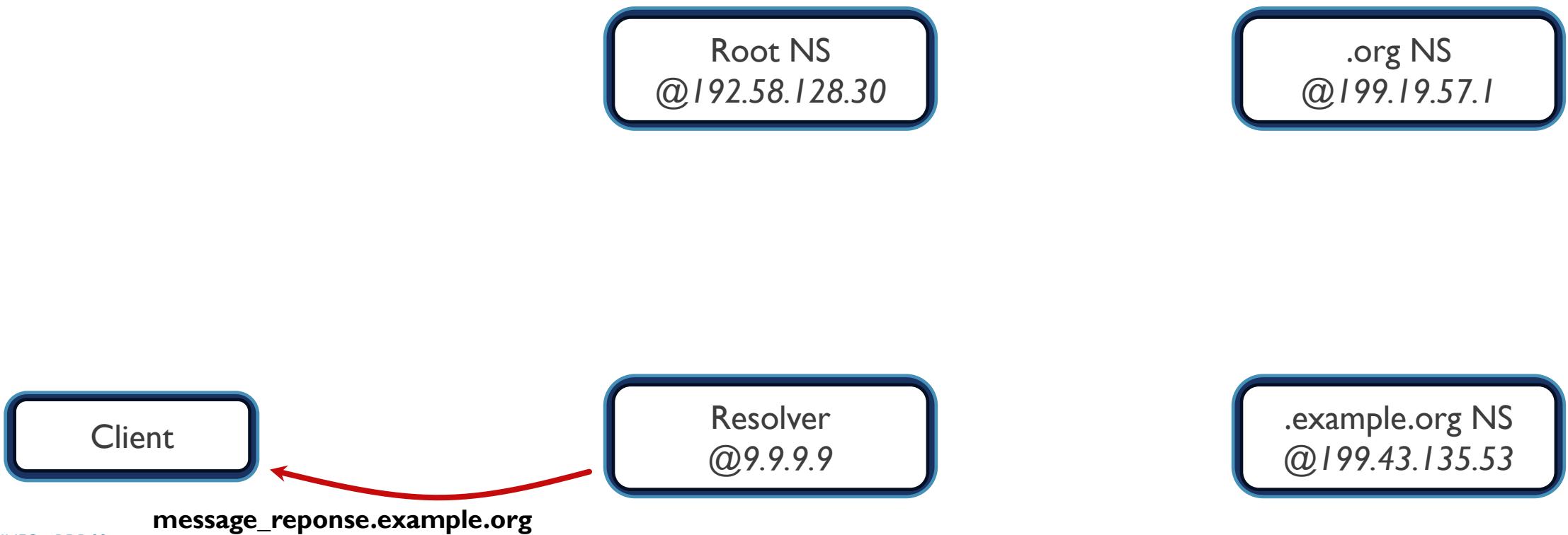
DNS TUNNELING



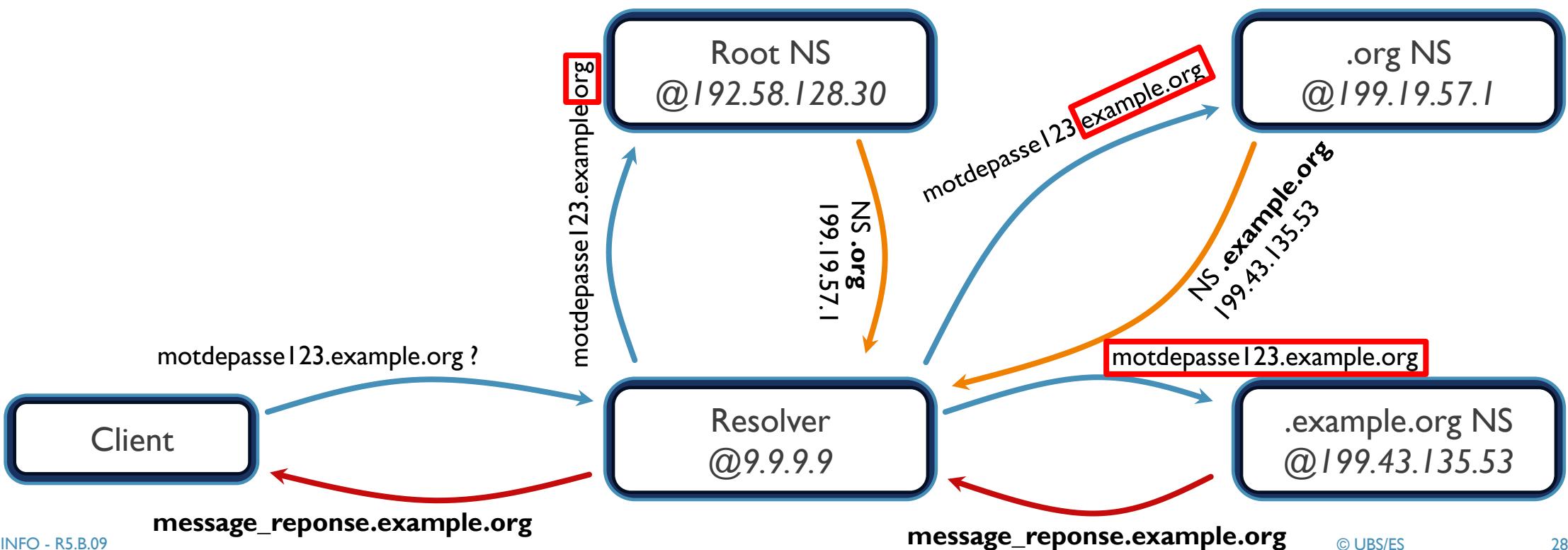
DNS TUNNELING



DNS TUNNELING



DNS TUNNELING



JUMEAU MALÉFIQUE



Attaque de point d'accès Wi-Fi (AP)

- Déploiement d'un faux AP en copie d'un vrai
- Inciter les utilisateurs à l'utiliser → *Eduroam*
- Tout trafic transit via le système de l'attaquant

- Possible de déployer des pages portail captive faux
 - Inciter les utilisateurs à renseigner leurs infos de connexion
- Très dangereux dans des zones avec beaucoup de réseaux Wi-Fi
- Nuance avec un AP malveillant → AP illégitime sur un réseau existant
 - Contourner la sécurité sur le réseau légitime

