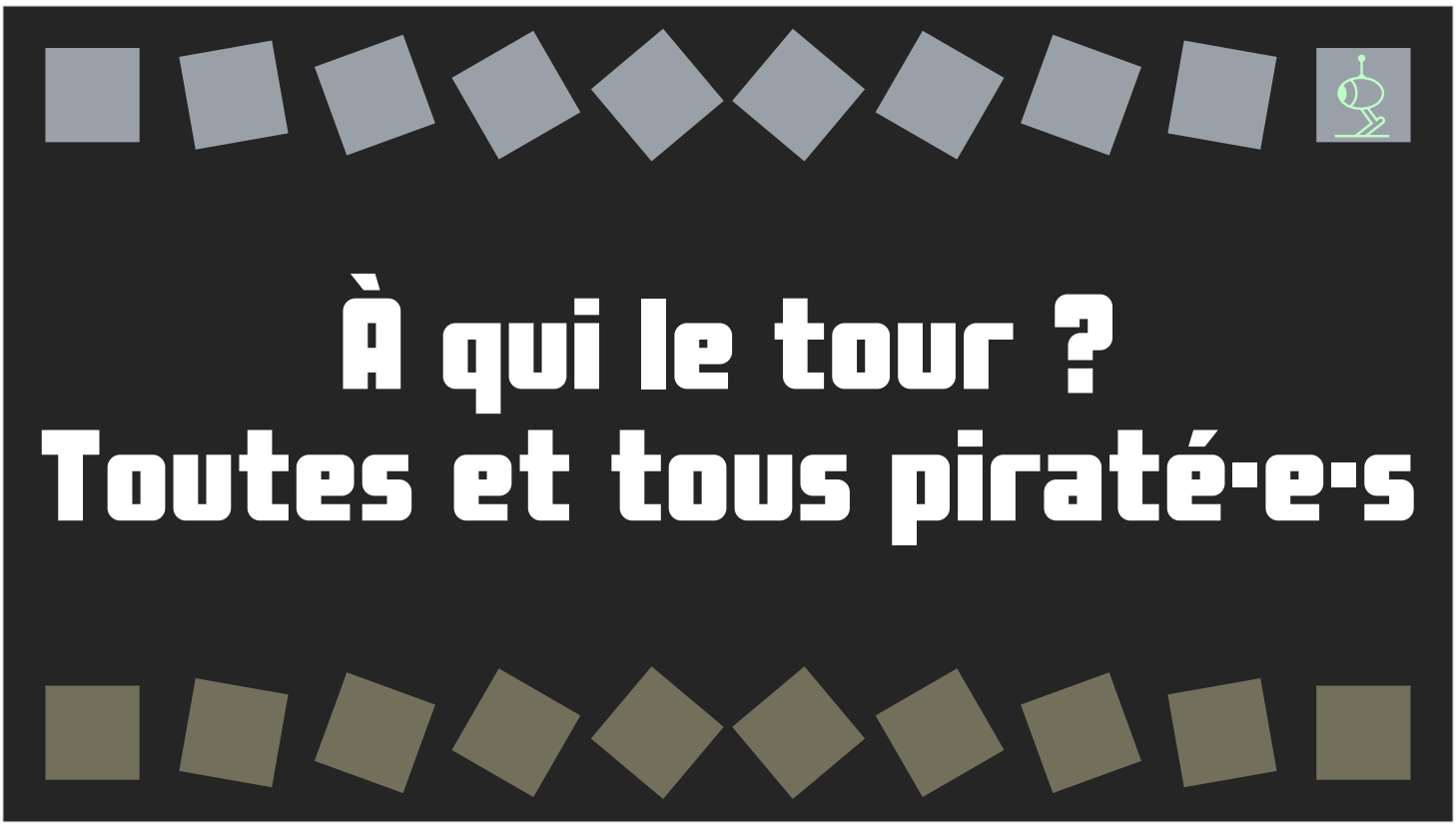


Bonjour !

Je m’appelle Frédéric BISSON, je suis développeur et je travaille à Rouen (Normandie).

L’actualité de ces dernières années regorge de reportages et d’interviews parlant de cyberattaque.

À chaque fois, le discours est le même : on parle d’attaque de grande ampleur, de coupure réseau, d’indisponibilité, des données exfiltrées etc.

Les collectivités font désormais régulièrement la une dès qu’elles subissent une cyberattaque.

- Un PDF avec
  - Les diapos
  - Les notes

zigazou.dev/download/cyberattaques-notes.pdf

Un PDF regroupant à la fois les diapositives et les notes est disponible au téléchargement à l'adresse :

https://zigazou.dev/download/cyberattaques-notes.pdf

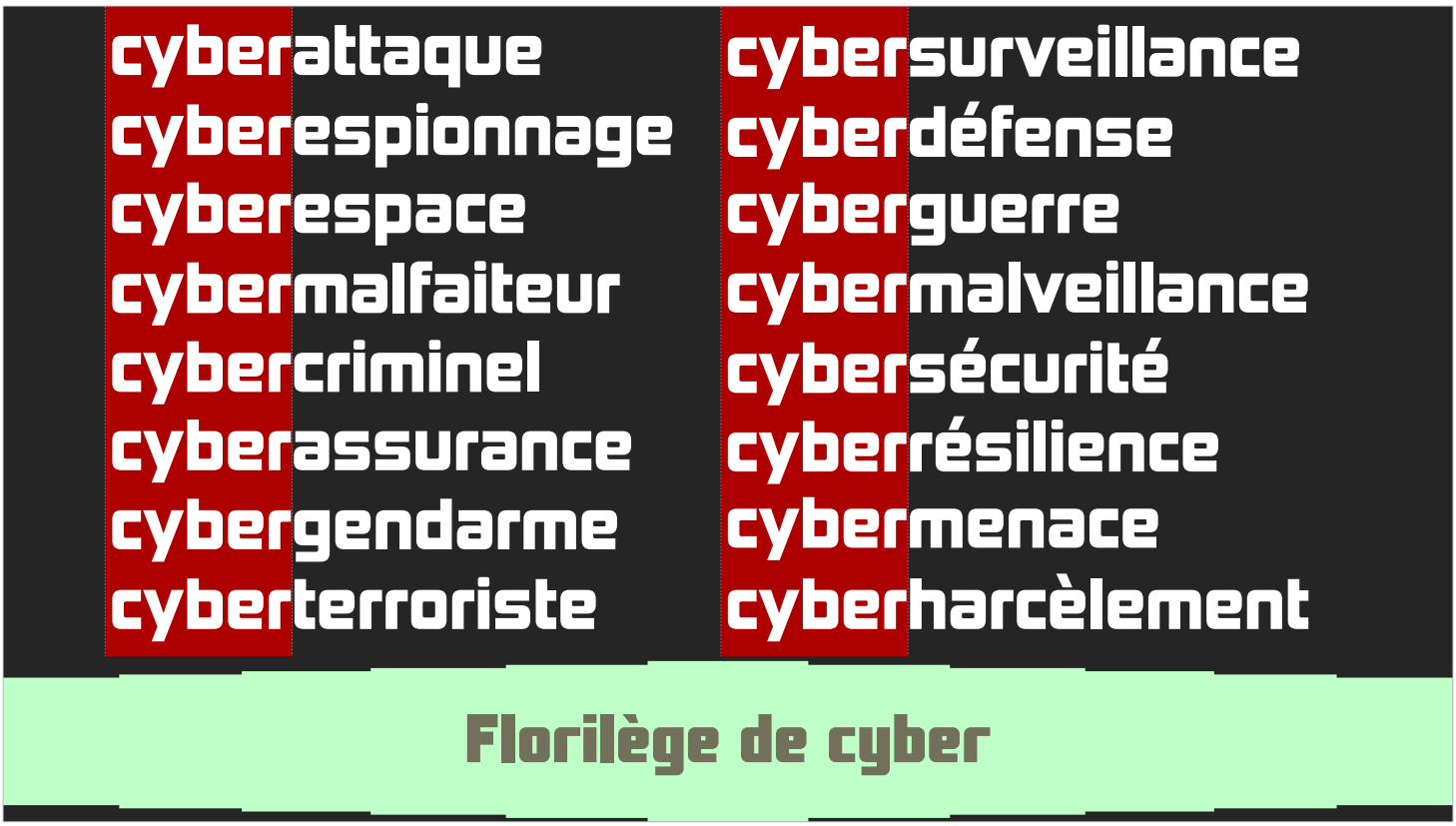
Sur les ruines du futur.

2022 : l’année de tous les e·dangers ? 4674 ransomwares confirmés. Plus de 300000 sites web infiltrés et modifiés. Plus de 20 milliards d’identifiants de connexion diffusés. L’ambiance malveillante sur le réseau des réseaux aura été particulièrement présente en 2022.

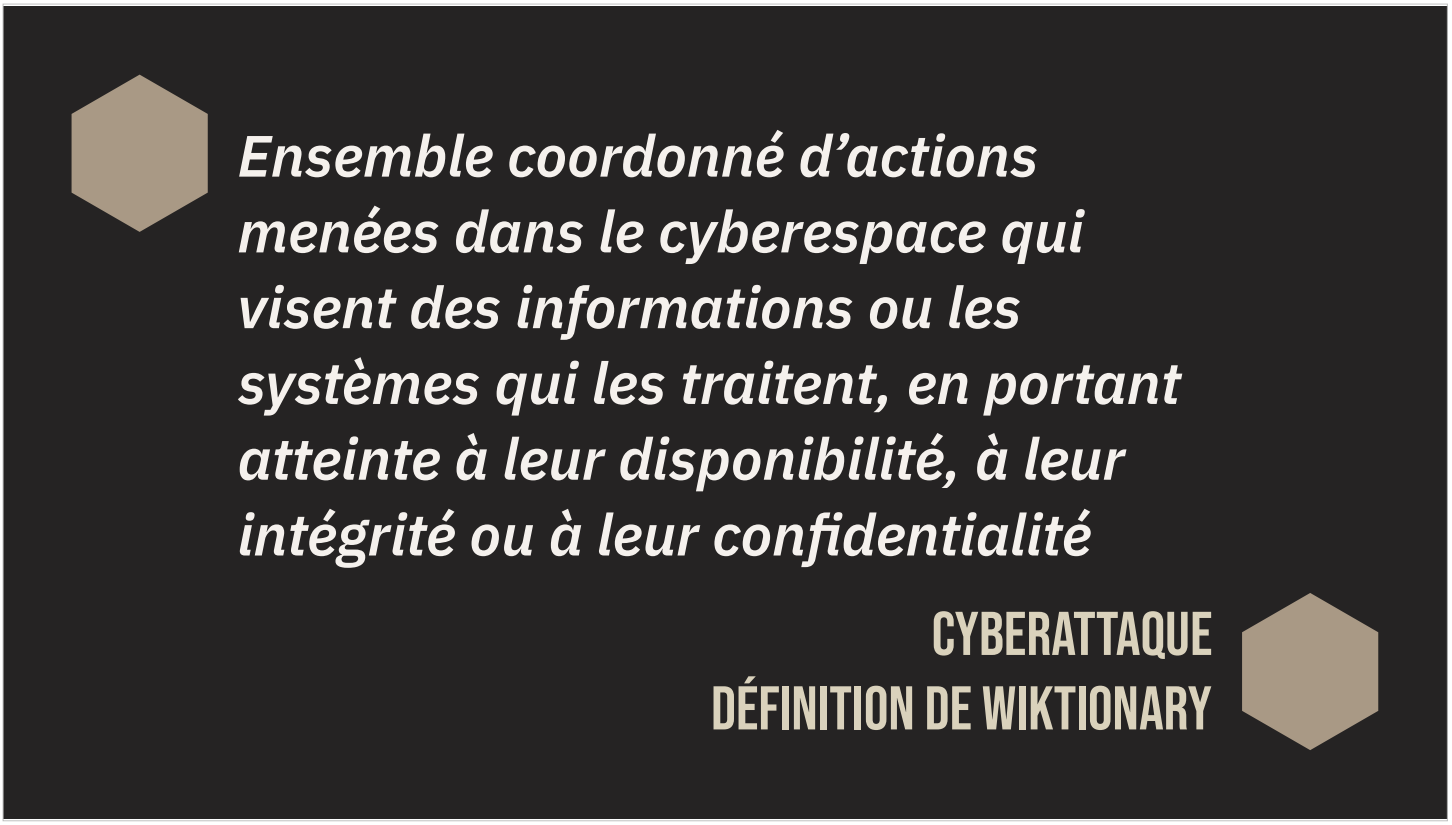
Nous commençons notre périple par une simple constatation.

Le mot « cyber » est maintenant un préfixe utilisé pour susciter la peur.

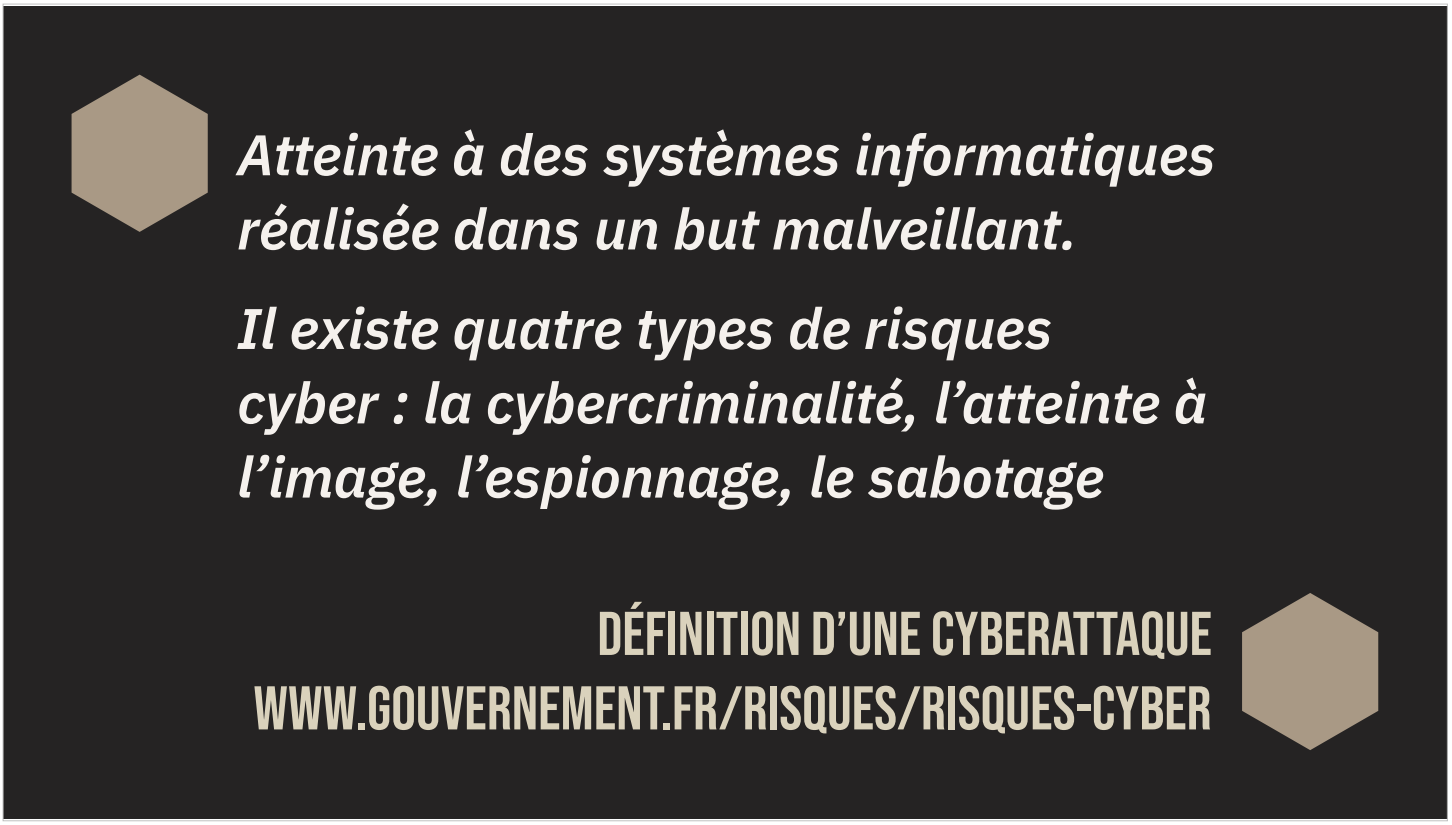
Selon Wikipédia, cyber est un préfixe à la mode à partir de la moitié du XXe siècle, son usage étant consécutif au développement de l'informatique, de la robotique et à l'avènement du réseau internet.



Il suffit de le rajouter à n’importe quel mot du réel pour en faire un terme dédié à internet.



Selon Wiktionary, une cyberattaque est un ensemble coordonné d'actions menées dans le cyberespace qui visent des informations ou les systèmes qui les traitent, en portant atteinte à leur disponibilité, à leur intégrité ou à leur confidentialité.



Une autre définition de la cyberattaque est donnée par l'État :

Il s'agit d'une atteinte à des systèmes informatiques, réalisée dans un but malveillant. Il existe quatre types de risques cyber : la cybercriminalité, l'atteinte à l'image, l'espionnage, le sabotage.

La première cyberattaque de l'histoire ?

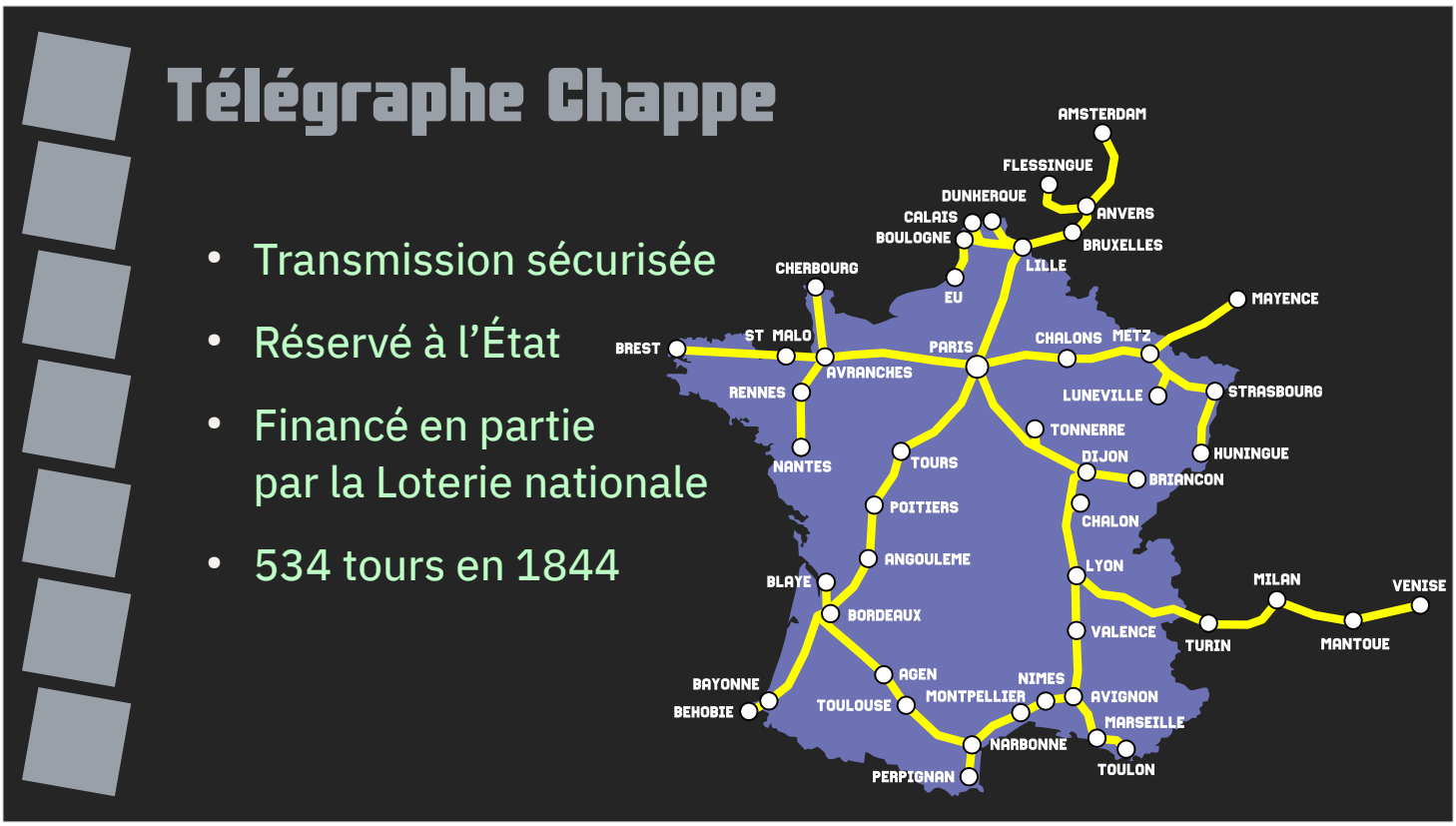
Selon vous à quand remonte la première cyberattaque ?

Un négociant qui, pour se procurer des nouvelles de Bourse, afin de jouer sur les fonds publics, obtient à prix d'argent certains signaux d'un employé de l'administration des télégraphes, se rend-il coupable du crime de corruption ?

LA GAZETTE DES TRIBUNAUX
10 DÉCEMBRE 1836

En extrapolant, on peut considérer que la première cyberattaque a eu lieu en 1834.

Au sujet de cette affaire, la Gazette des Tribunaux indiquait en 1836 : « Un négociant qui, pour se procurer des nouvelles de Bourse, afin de jouer sur les fonds publics, obtient à prix d’argent certains signaux d’un employé de l’administration des télégraphes, se rend-il coupable du crime de corruption ?



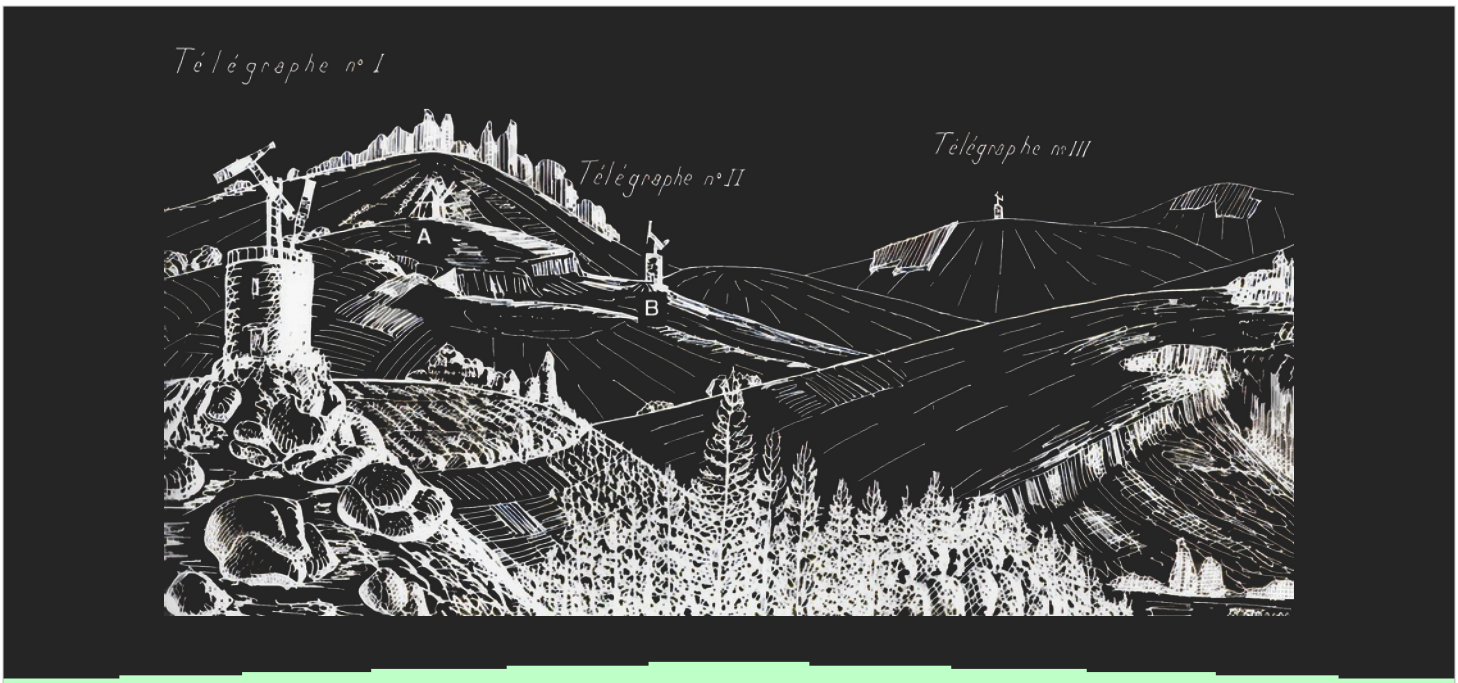
Le télégraphe Chappe a été créé en 1794.

Comme tous les télégraphes il permet de transmettre des informations à distance.

Il était sécurisé et réservé à l'État.

La loterie nationale a d'ailleurs été créée pour financer son fonctionnement.

En 1844, il comptait 534 tours relayant les messages à travers un réseau qui couvrait toute la France et plus encore.

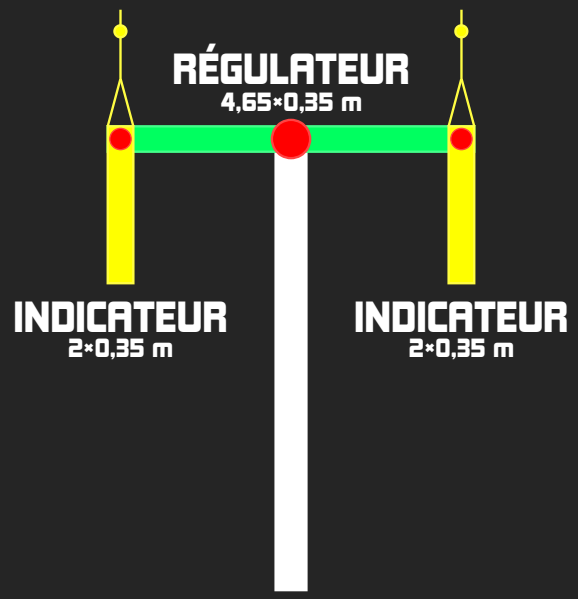


Des tours espacées de 25 km environ

Les tours dont on parle sont des bâtiments installés tous les 25 km environ de façon qu’une tour pouvait observer la tour précédente et la tour suivante.

Des sémaphores

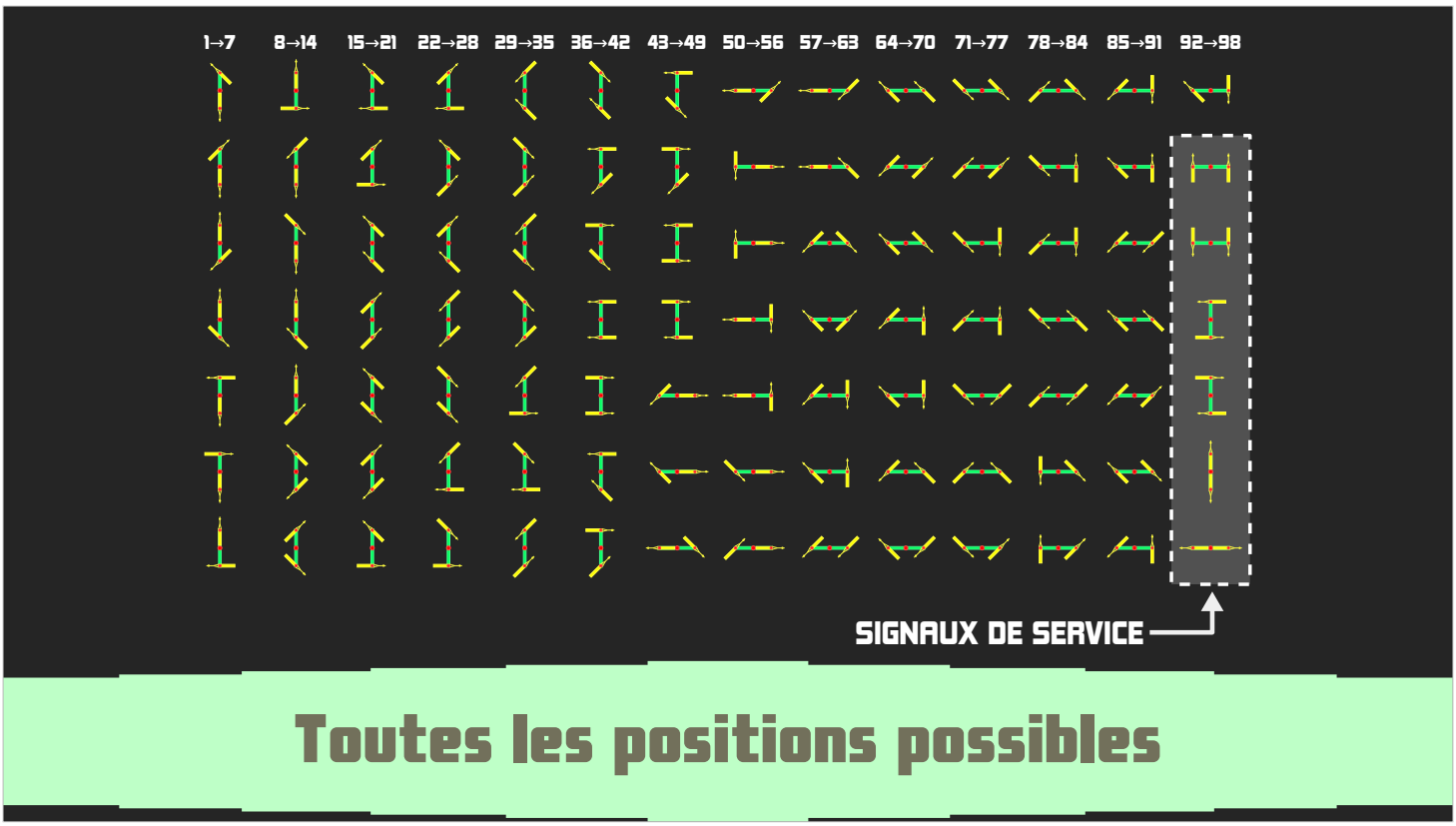
- Un système optique
- La position du régulateur et des indicateurs correspond à un numéro
- Les signaux sont transmis de tour en tour



Car le télégraphe Chappe était un système optique.

Il utilisait des sémaphores basés sur la position de planches de bois articulées qu'on appelait régulateur et indicateurs.

À chaque position correspondait un numéro.

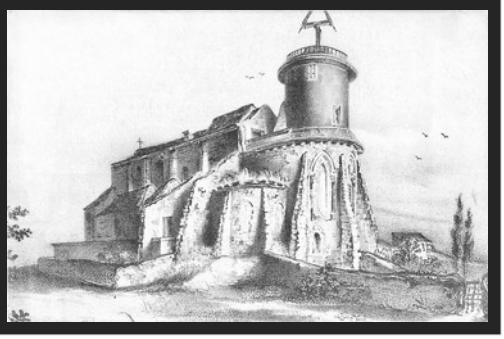


Il y avait en tout 98 positions valides.

6 d’entre elles correspondaient à des signaux de service.

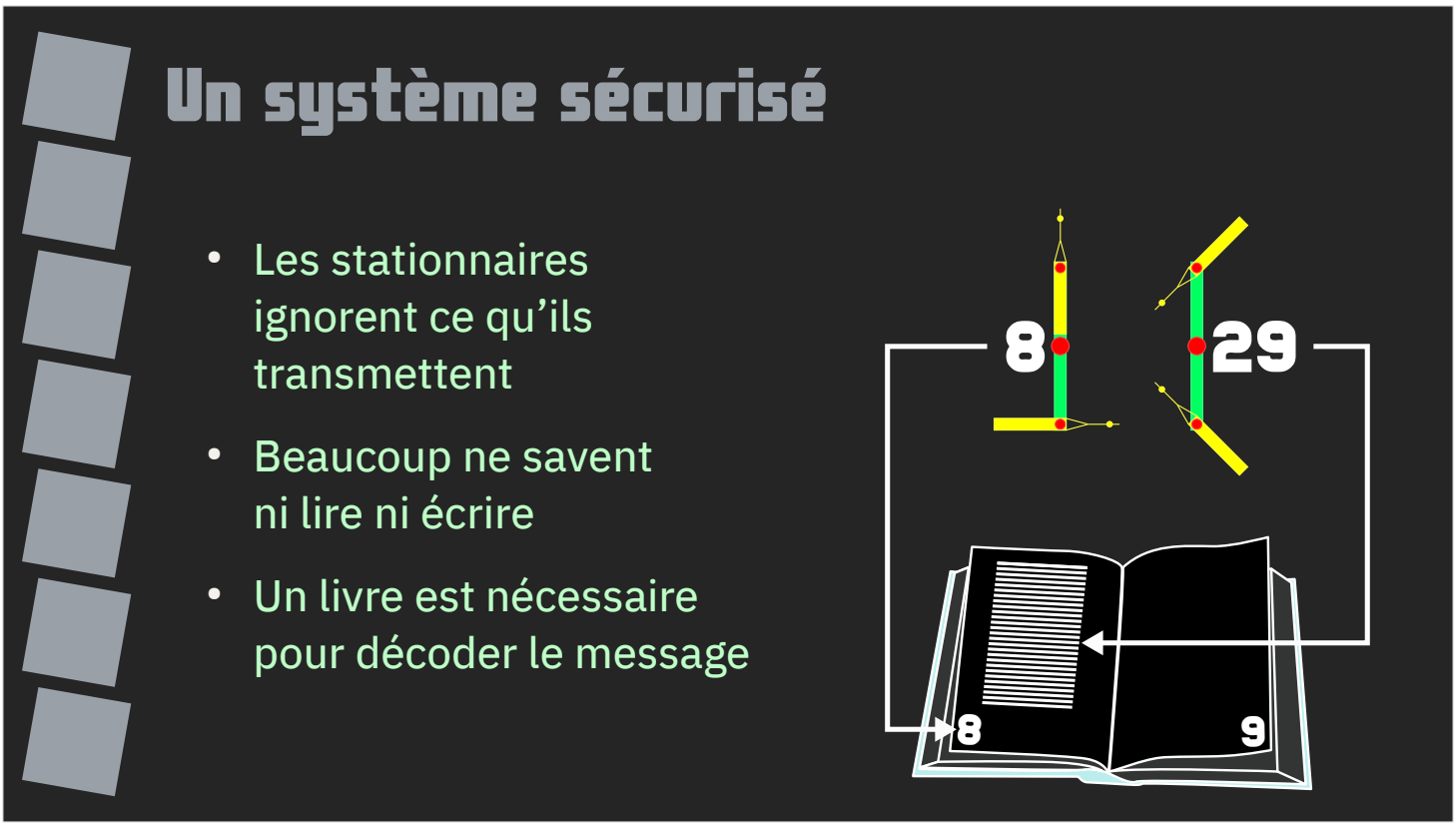
Trois catégories de personnel

- Directeurs
  - Encodent et décodent les messages
  - Travaillent sur certaines villes (Paris, Tours, Bordeaux…)
- Inspecteurs
  - Surveillent les divisions (~12 stations)
- Stationnaires
  - Transmettent les messages



Le réseau était animé par trois catégories de personnel :

- Les directeurs, situés aux nœuds stratégiques du réseau et qui étaient les seuls à pouvoir encoder et décoder les messages
- Les inspecteurs qui surveillait le bon fonctionnement du réseau, chacun étant affecté à un groupe d'environ 12 tours
- Et enfin les stationnaires qui passaient leurs journées à surveiller les tours et à retransmettre les messages qu'ils captaient.



Comme les stationnaires ne savaient pas ce qu'ils retransmettaient, beaucoup ne sachant ni lire ni écrire, le système était considéré sécurisé, à l'instar des équipements réseau d'aujourd'hui qui transmettent des paquets de données sans avoir besoin de connaître leur contenu.

Un livre était nécessaire pour décoder un message, le premier code donnant la page du livre et le second la position du mot sur cette page.

La faille du télégraphe Chappe

- Un signal de régulation pour annuler un message
  - Indique que le dernier message doit être ignoré
  - Signal propagé par les stationnaires
  - Nettoyage effectué par les directeurs
- Une personne peut être soudoyée…
- Il est possible d'insérer des messages privés ! 

Alors où est la faille de ce système ?

Elle réside dans l'existence d'un signal de régulation permettant d'annuler un message. Quand un stationnaire pensait s'être trompé dans ses signaux, il envoyait le signal d'annulation pour indiquer que le message qu'il venait d'envoyer devait être annulé.

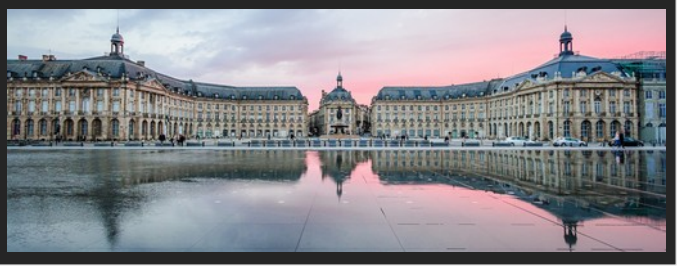
Le stationnaires suivants propageaient ce signal si eux-mêmes avaient déjà transmis le message erroné avant de recevoir le signal d'annulation.

De plus, comme dans toute organisation humaine, une personne peut être soudoyé.

Tout cela permettait d'insérer des messages privés dans le réseau en les faisant passer pour des messages erronés.

Les bourses de France

- Lyon, Marseille, Bordeaux, Nantes, Lille, Nancy, Rouen
- État de la bourse transmis par voie postale
- 3 jours de décalage entre Paris et Bordeaux
- En transmettant une info plus vite, on peut spéculer !



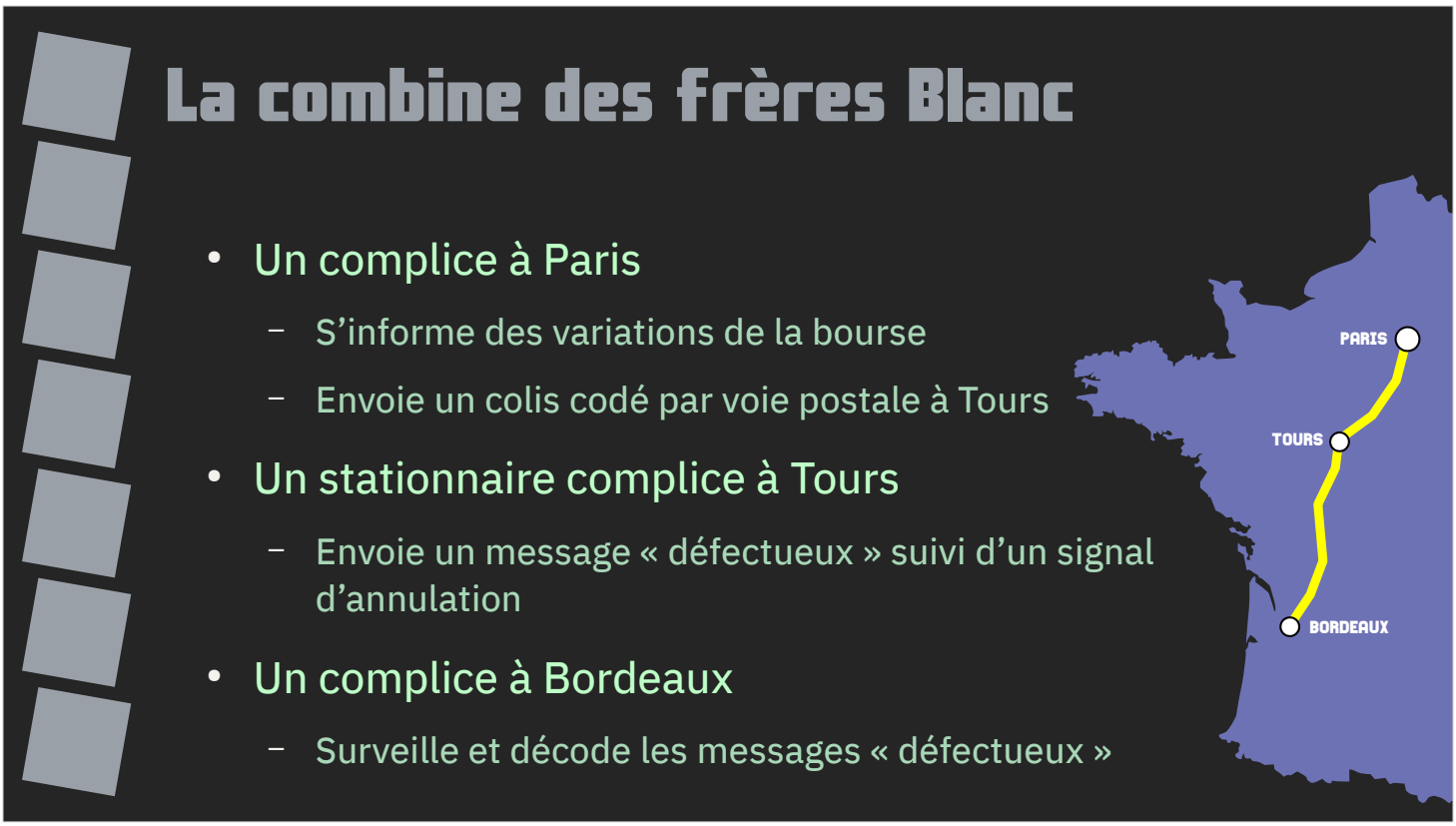
Pour comprendre l'intérêt de cette faille, il faut se replacer dans le contexte de l'époque.

Il y avait plusieurs bourses en France (il n'y en a plus qu'une aujourd'hui, celle de Paris).

L'état de la bourse de Paris était transmis par voie postale aux autres bourses, ce qui pouvait entraîner des décalages de plusieurs jours.

Entre Paris et Bordeaux, le décalage était de 3 jours.

Si on pouvait transmettre les évolutions du cours de la bourse plus rapidement, il devenait possible de spéculer.



Les frères Blanc, qui habitaient à Bordeaux, ont monté une petite organisation pour exploiter cette combine.

Cela nécessitait :

- Un complice à Paris, pour transmettre les variations de la bourse en envoyant un message codé par voie postale à Tours.
- Pourquoi Tours ? Tout simplement parce qu'il y avait un directeur à Tours ! Tout message erroné émis depuis Paris aurait été arrêté à Tours. Il y fallait donc un complice pour insérer les messages « défectueux » dans le réseau.
- Et un complice à Bordeaux, dans une chambre d'hôtel ayant vue sur la tour Chappe, pour détecter les messages à destination des frères Blanc.

Même avec la perte de temps entre Paris et Tours, les frères Blanc étaient informés en avance des fluctuations de la bourse.

La fin d’une belle aventure

- De 1834 à 1836
- La bonne étoile des frères Blanc attire la suspicion
- Les frères Blanc s’en sortent bien
  - Absence de cadre légal autour des télécommunications
- Monopole public des télécommunications
  - Loi de 1837 à la suite de l’affaire
  - Se terminera en 1998 !

Leur combine a duré 2 ans.

Leur étonnante capacité d’anticipation ainsi que le décès de leur complice à Tours, ont attiré la suspicion.

Ils s’en sortent toutefois bien car il n’y avait pas de cadre légal à l’époque autour des télécommunications. Hormis une corruption d’agent de l’État, sans grand impact sur leur fortune.

C’est de cette époque que le monopole des télécommunications de l’État a été instauré. Monopole qui tiendra jusqu’en 1998 !

Les collectivités, cibles de cyberattaques

Même si cette primo-attaque d'un réseau de télécommunications ne peut pas être réellement qualifiée de cyberattaque, il n'en demeure pas moins que la criminalité dans le domaine des télécommunications ne date pas d'hier.

Si on revient à aujourd'hui, les dernières actualités donnent l'impression que les collectivités sont de plus en plus la cible de cette criminalité, le tout dans un contexte de Brexit, de covid, de guerres, de dérèglement climatique etc.

De juillet 2021 à juillet 2022, les administrations publiques ont totalisé 24,21 % des incidents signalés.

ENISA THREAT LANDSCAPE 2022
TARGETED SECTORS PER NUMBER OF INCIDENTS

Le rapport Enisa threat landscape 2022 (soit l’Agence de l'Union européenne pour la cybersécurité) a évalué que les administrations publiques ont totalisé 24,21 % des incidents signalés de juillet 2021 à juillet 2022.

Recrudescence des attaques

Qté	Type de collectivité	Population
124	commune	5 800 000
38	intercommunalité	-
9	département	8 800 000
5	région	24 000 000

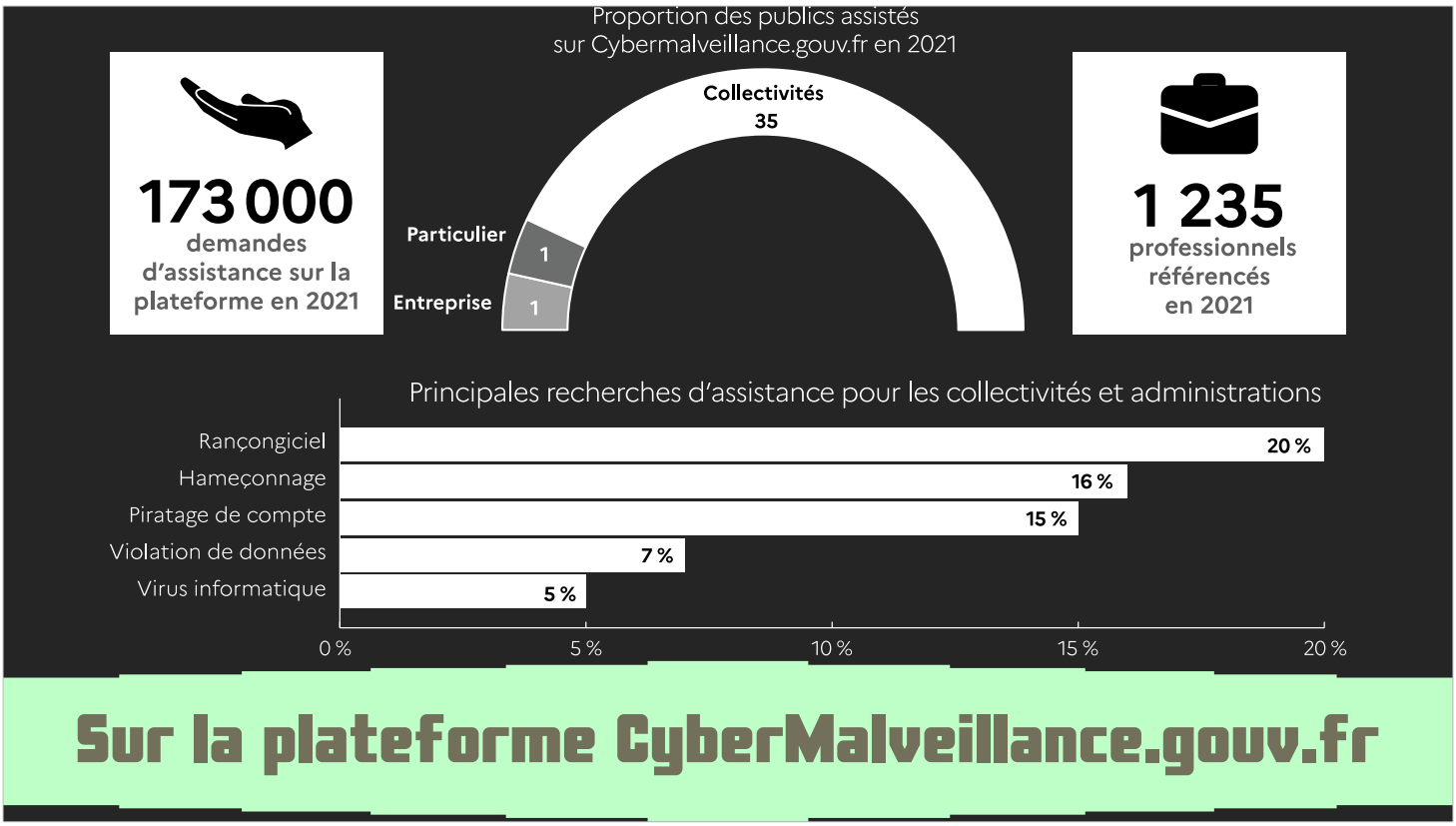
Attaques constatées, pour lesquelles il existe au moins un article signalant l'attaque sur la période 2018-2023

Sur les six dernières années, de 2018 à 2023, j'ai pu recenser 124 cyberattaques sur des communes, 38 sur des intercommunalités, 9 sur des départements et 5 sur des régions.

On peut citer notamment

- Les régions Normandie, Centre Val-de-Loire et Guadeloupe
- Les départements de Seine-Maritime, Seine-et-Marne et des Alpes-Maritimes
- Les villes de Caen, les Mureaux et Aix-les-Bains

On a un spectre très large qui va de la commune de 150 habitants à la région de 12 millions d'administrés.

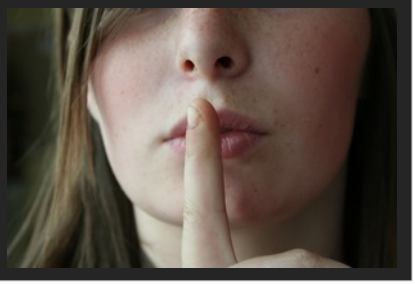


Selon Cybermalveillance.gouv.fr, leur plateforme a enregistré 173000 demandes d'assistance en 2021, très majoritairement en provenance de collectivités.

Ces demandes tournaient principalement autour des rançongiciels.

De la difficulté d'avoir des chiffres

- Pas de chiffre officiel
- Les cyberattaques peuvent être
  - déclarées mais passées sous silence
  - non déclarées par les collectivités
  - non déclarées par la supply-chain
  - non détectées



Ces chiffres doivent être vus comme des minimum. Il s'agit seulement des collectivités pour lesquels on peut trouver les traces des cyberattaques dans la presse et les médias.

Il n'existe pas encore de chiffre officiel permettant d'avoir des statistiques précises.

En dehors des collectivités référencées, il y a donc une amplitude large laissant la possibilité à :

- Des cyberattaques déclarées mais passées sous silence
- Des cyberattaques non déclarées par les collectivités
- Des cyberattaques non déclarées par la supply-chain (les fournisseurs et prestataires des collectivités)
- Ou encore des cyberattaques non détectées

Il y a quelques années, les pirates rentraient dans le système informatique et volaient des données sans faire de bruit.

Autrement dit, les villes étaient piratées sans le savoir.

DAMIEN BANCAL – ZATAZ
INTERVIEW FRANCE 3, 04/11/2022

Un premier indice qui explique la recrudescence des cyberattaques est le fait qu'auparavant les attaques se concentraient sur le vol de données.

Aujourd'hui, les rançongiciels rendent ces mêmes données inutilisables.

On peut également envisager l'amélioration progressive des systèmes de détection et une plus grande vigilance.

Le privé moins touché ?

- Activité > sécurité
- Confiance, image
  - Clients
  - Investisseurs
  - Actionnaires
- Plus de moyens

- 2022
  Über, Nvidia, Twitter
- 2021
  Microsoft Exchange, Axa Partners, Acer
- 2020
  Amazon Web Services, Bouygues Construction

Le privé est-il moins touché que le public ? Pas vraiment !

Moins médiatisé, sûrement.

Les entreprises doivent tout d'abord maintenir leur activité car pas d'activité signifie pas d'argent, quitte à sacrifier la sécurité. L'impact sera donc moins visible que pour une collectivité qui bloque tout pendant plusieurs jours voire semaines.

Elles doivent également conserver la confiance et l'image qu'elles ont auprès de leurs clients, de leurs investisseurs ou de leurs actionnaires, quitte à garder sous silence certains problèmes.

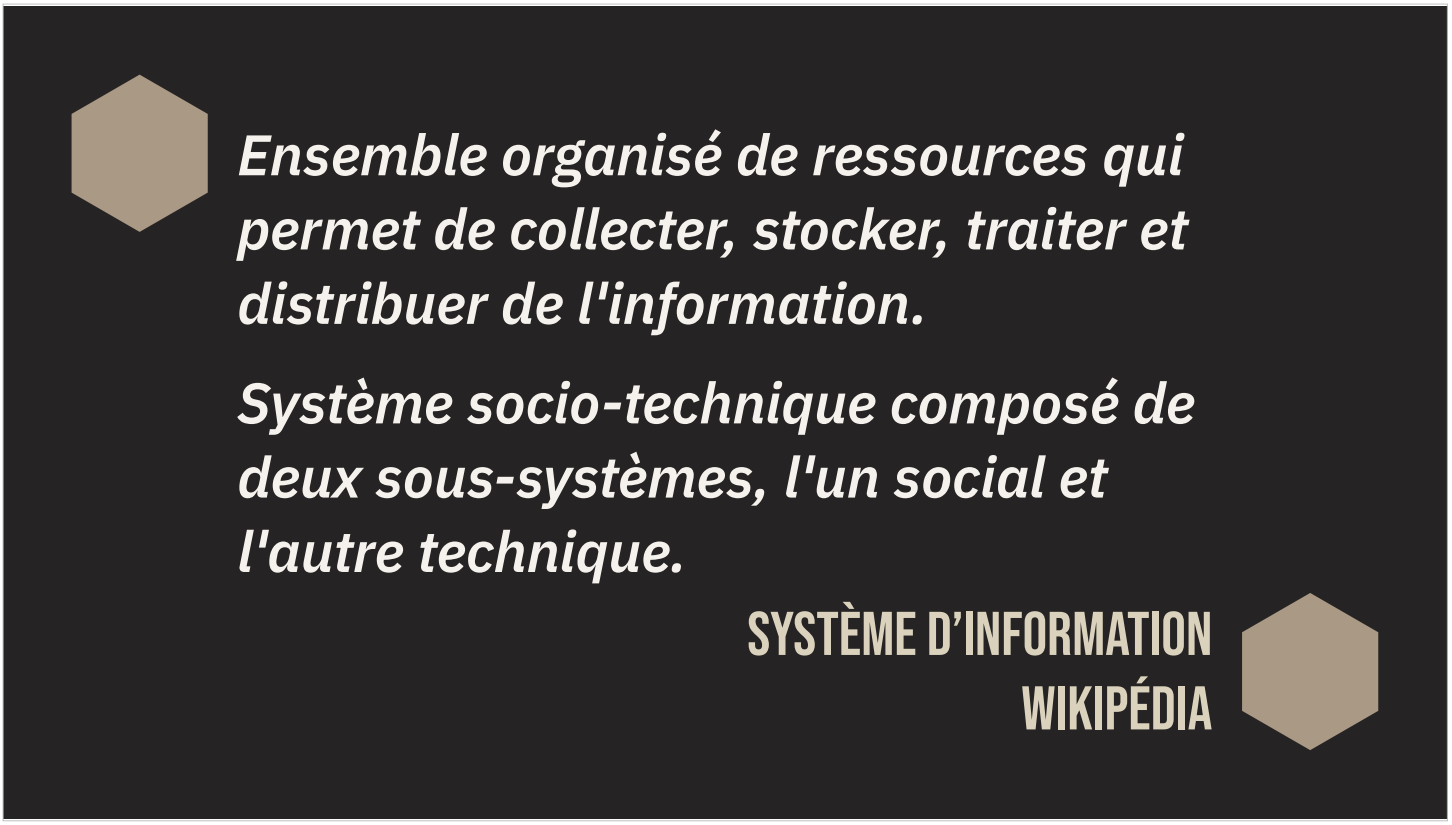
Et elles ont plus de moyens pour y parvenir.

Même les plus grandes subissent des cyberattaques. On peut citer Amazon Web Services et Bouygues Construction en 2020, Microsoft Exchange, Axa Partners et Acer en 2021, ou Über, Nvidia et Twitter en 2022.

Un système d'information

La notion de système informatique n'est pas suffisante quand on parle de cybersécurité. Elle doit être élargie à la notion de système d'information.

Comprendre ce qu'englobe la notion de système d'information est essentielle pour pouvoir se défendre au mieux



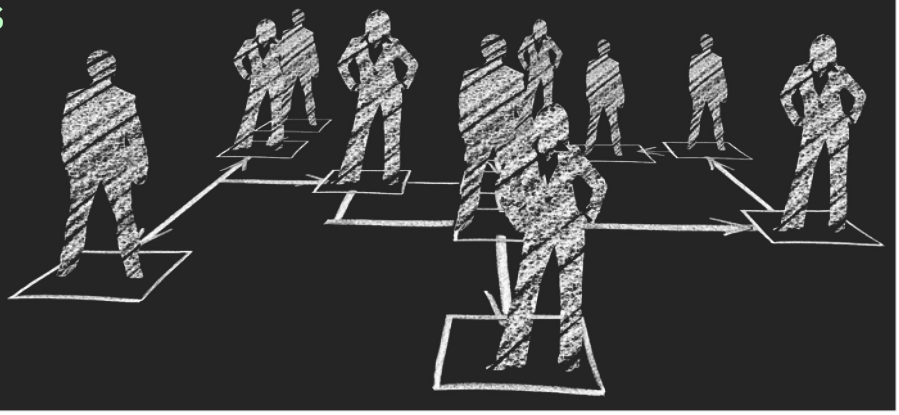
Selon Wikipédia, un système d'information est un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information. Il s'agit d'un système socio-technique composé de deux sous-systèmes, l'un social et l'autre technique.

QUE RETROUVE-T-ON DANS UN SI ?

Ceci étant posé, que va-t-on retrouver dans un SI ? (parce que système d’information, c’est un peu long à prononcer)

Une organisation

- Une hiérarchie
- Des personnes
- Des procédures



Tout d’abord, on retrouve une organisation humaine, avec sa hiérarchie, ses personnes et ses procédures : qui commande à qui, qui fait quoi, quel chemin doivent prendre les décisions etc.

Du matériel

- Dispositifs de sécurité
- Postes de travail fixe/portable
- Serveurs physiques/virtuels
- Réseau interne/externe
- Téléphones fixes, mobiles, fax...

On retrouve aussi du matériel comme des dispositifs de sécurité, des postes de travail fixe ou portable, des serveurs physiques ou virtuels, des réseaux internes ou externes, des téléphones fixes, des téléphones mobiles, des fax, des imprimantes en réseau etc.

De l’intangible

- Applis métier
- Bases de données
- Fichiers
- Gestion des accès
- Accès internet, intranet ou extranet
- Système de paiement
- Outils collaboratifs, agendas, espace de partage, forums, carnet d’adresses, chat, visioconférence

Et de l’intangible qui comprend des logiciels, des données, des droits, des APIs...

Cela peut se traduire sous forme d’applications métier, de bases de données, de fichiers, de gestion des accès (mots de passe, permissions...), d’accès internet, intranet, extranet, de systèmes de paiement, d’outils collaboratifs, d’agendas, d’espaces de partages, de forums, de carnets d’adresses, de chat, de visioconférence etc.

Surface d’attaque

Dans le cadre des cyberattaques, la notion de SI entraîne inévitablement la notion de surface d’attaque.

Somme des différents points faibles par lesquels un utilisateur non autorisé pourrait potentiellement s'introduire dans un environnement logiciel et en soutirer des données.

SURFACE D'ATTAQUE

HTTPS://FR.WIKIPEDIA.ORG/WIKI/SURFACE_D%27ATTAQUE

Toujours selon Wikipédia, il s'agit de la somme des différents points faibles par lesquels un utilisateur non autorisé pourrait potentiellement s'introduire dans un environnement logiciel et en soutirer des données.

Notez bien que la surface d'attaque ne se concentre pas sur l'aspect informatique des cyberattaques.

Surface d’attaque et SI

- Chaque élément du SI intervient dans la surface d’attaque
- Cyberattaque et points faibles
  - Plusieurs faiblesses sont nécessaires pour une cyberattaque
  - À grande surface d’attaque, grand nombre de faiblesses
- Hétérogène ou homogène ?

Chaque élément du SI intervient dans la surface d’attaque.

Plus le SI est complexe, plus il est difficile de circonscrire sa surface d’attaque.

Mais cela implique aussi que le pirate va devoir enchaîner les faiblesses afin d’atteindre ses objectifs.

Se pose aussi la question de savoir s’il est préférable d’avoir

- un SI hétérogène, qui va être plus difficile à maîtriser et maintenir
- ou un SI homogène, plus facile à maîtriser et maintenir mais qui va présenter la vulnérabilité des platanes au bord des routes : tous issus de la même souche, ils sont alors tous vulnérables à la même maladie.

Bien comprendre son SI

- Pour éviter de faire de la sécurité inutile
- Pour sécuriser chaque point faible

Il est très important de bien cerner ce que recouvre un SI afin :

- d’éviter de faire de la sécurité inutile
- et de sécuriser chaque point faible.

Points faibles de l'organisation

- Humain
  - Corruption
  - Disponibilité
  - Biais et états psychologiques
  - Obéissance
  - Méconnaissance du danger
- Procédures
  - Attaques temporelles
  - Attaques par perturbation
- Autorité
  - Identification
  - Authenticité

En reprenant les trois éléments d'un SI, on peut dégager des listes de faiblesses génériques.

Dans le cas de l'organisation, l'humain est l'une des plus grandes faiblesses. Il est corruptible, a une disponibilité limitée voire variable. Il est soumis à des biais et états psychologiques. Il a une notion variable de l'obéissance et peut méconnaître le danger.

Les procédures mises en place sont sensibles à des attaques temporelles (comme pour l'organisation des bourses françaises avec l'attaque du télégraphe Chappe) ou aux attaques par perturbation (le déni de service en fait partie).

L'autorité, elle, est source de difficultés quant à l'identification ou l'authenticité d'une personne ou d'un message émanant d'elle.

Toutes ces faiblesses sont exploitées par les pirates.

Alain, agriculteur, fait faire des travaux sur une remorque. Montant de la facture : 3300€. Il reçoit par mail la facture et la paie avec le RIB en pièce jointe. Son garagiste n'a jamais reçu l'argent.

Il a été victime d'un piratage de sa boîte mail.

VRAIE FACTURE MAIS FAUX RIB
LE MAINE LIBRE - 07/09/2021

Pour illustrer ces faiblesses, on peut prendre le cas des faux RIB.

Le Maine Libre citait l'exemple d'Alain, agriculteur qui a fait faire des travaux sur une de ces remorques.

Il y en avait pour 3300€ et son garagiste lui a envoyé la facture et un RIB par mail pour le règlement.

Ce dernier n'a malheureusement jamais reçu l'argent que lui devait l'agriculteur car Alain s'était fait pirater sa boîte mail.

Le RIB du garagiste avait été remplacé par le RIB du criminel.

Alain a en toute bonne foi payé.

Points faibles du matériel

- Des bugs matériels
  Failles Meltdown, Spectre
- Des bugs logiciels
- Des bugs inhérents
  Attaques par relais, capacité de traitement
- Attaques par perturbation
  Sensibilité à un contexte physique
- Attaques temporelles
  Cartes bleues
- Interconnexions

À l'instar des logiciels, le matériel a aussi ses points faibles

Par exemple, il y a eu les failles Meltdown et Spectre affectant les processeurs Intel voire AMD. Comme il est impossible de « corriger » le matériel (à part en le remplaçant), des patchs ont été développés pour les systèmes d'exploitation avec comme conséquences des pertes de performances.

Le matériel, effectuant des tâches de plus en plus complexes, embarque des logiciels qui peuvent aussi avoir leurs failles.

Il y a aussi des bugs dûs à la conception ou aux limitations techniques. L'IoT, par exemple, embarque souvent des circuits aux capacités de traitement faibles pour limiter consommation et prix. Difficile d'avoir des protections élaborées dans ces conditions.

Les attaques par perturbation ou temporelles sont elles-aussi pertinentes pour le matériel.

« Ils se déplacent par trois ou quatre, se collent aux gens et détournent leur attention d'une manière ou d'une autre. »

Au mois d'août 2019, la Police Nationale a mis en garde les touristes à Nice contre un gang. Les malfrats, munis d'un TPE, se positionneraient près des serviettes de vacanciers pour débiter les cartes.

ESCROQUERIE AU PAIEMENT SANS CONTACT
UFC QUE CHOISIR - 03/06/2021

L'UFC Que Choisir en juin 2021 évoquait le cas d'escroqueries au paiement sans contact pour lesquels un gang en 2019 se déplaçait en petit groupe sur les plages, se collait aux gens, détournait leur attention pour lancer un paiement avec un terminal de paiement électronique portable.

Ce type d'attaque ne requiert pas de connaissances particulières en informatique.

Points faibles de l'intangible

- Mauvaise configuration
  - Configuration par défaut
  - Méconnaissance
- Code source
  - Complexité
  - Mises à jour, zero-day
  - Provenance
- Mots de passe
  - Par défaut
  - Trop simples
  - Stockés en clair
  - Partagés

Enfin, on parle souvent des failles des logiciels mais ils ne sont pas les seules à avoir des faiblesses dans le monde de l'intangible.

Une mauvaise configuration des logiciels peut amener des failles.

Il en va de même pour les mots de passe, qu'ils soient par défaut, trop simples, stockés en clair, partagés ou utilisés plusieurs fois.

Pour revenir aux logiciels, la complexité des programmes est telle qu'il est particulièrement difficile de garantir qu'un logiciel ne présente aucune faille. Cette complexité force à recourir à des bibliothèques, qu'on connaît encore moins que son propre code.

Si une mise à jour suffit généralement à corriger une faille de sécurité, il existe des failles qui posent problème : les failles zero-day. Ce sont des failles pour lesquelles l'éditeur ne sait pas encore qu'elles existent. Elles vont être exploitées de façon discrète ou bien être vendues sur le marché noir.

Les mots de passe par défaut de vos objets connectés se trouvent facilement sur Google !

Des chercheurs ont découvert que de nombreux propriétaires de périphériques IoT ne changent jamais les mots de passe par défaut.

MOTS DE PASSE PAR DÉFAUT DES OBJETS CONNECTÉS
SOPHOS - 29/03/2018

Une étude de Sophos en mars 2018 précisait que les mots de passe par défaut des objets connectés se trouvaient facilement sur Google.

Malheureusement, de nombreux propriétaires de ces objets ne changent jamais les mots de passe par défaut, faisant de ces objets des proies faciles pour les pirates.

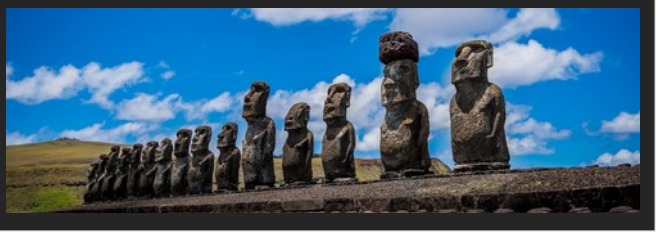
L'Angleterre dispose déjà de lois imposant les mots de passe uniques.

SURFACE D'ATTAQUE DES COLLECTIVITÉS

Concentrons-nous sur les collectivités pour esquisser leur surface d'attaque.

Des organismes complexes

- **Hiérarchies profondes**
  Distance hiérarchique importante N+1… N+10,
  prise de décision reposant sur l'autorité
- **Formes juridiques variées et entremêlées**
  CCAS, Offices de Tourisme, Communautés de Communes, Écoles,
  Collèges, Lycées, Services mutualisés, partenariats public-privé…



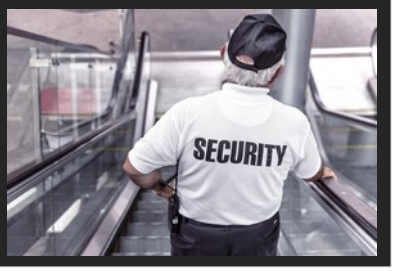
Les collectivités sont des organismes complexes.

Tout d'abord par leurs hiérarchies profondes. Il n'est pas rare de trouver des agents qui soient à un niveau N+10 de la direction générale des services.

Elles présentent des formes juridiques variées et entremêlées. On peut citer les CCAS, les offices de tourisme, les communautés de communes, les écoles, collèges et lycées, les services mutualisés, les partenariats public-privé…

Des humains faillibles

- Nombreux agents et diversité des métiers
  Angers + Métropole + CCAS = 4600 agents permanents, +200 métiers
- Manque de compétences
  Absence de bonnes pratiques, de configurations adéquates
- Manque de sensibilisation, de formation
  Entraîne des pratiques à risque
- Nombreux prestataires externes
  Différences de pratiques de sécurité



Les collectivités ont recours à beaucoup de personnels sous diverses formes : fonctionnaires, contractuels, Atsem, prestataires, police municipale etc. Rien qu'à Angers en incluant la ville, la métropole et le CCAS, cela représente 4600 agents permanents pour plus de 200 métiers.

Maintenir un niveau de sécurité dans ces conditions est un défi car la sécurité peut être mise à mal par un manque de sensibilisation et de formation.

Enfin, la nature sans cesse évolutive de la menace cyber nécessite de disposer de compétences en interne pour sécuriser le SI, ce qui peut être facilement hors de portée de nombreuses collectivités.

Un grand nombre de compétences 1/4

SÉCURITÉ	ACTION SOCIALE, SANTÉ	EMPLOI, INSERTION PRO
Circulation, stationnement, salubrité publique, gardes champêtres…	CCAS, aide sociale facultative, centres d'accueil, EHPAD, logement, campagne de vaccination, salubrité, alerte et veille sanitaire, participation aux ARS…	Maisons de l'emploi, missions locales, siège à Pôle Emploi…
ENSEIGNEMENT	**ENFANCE, JEUNESSE**	**SPORTS**
Gestion des écoles, des personnels TOS, ATSEM, scolarisation, cantines, périscolaire, logement étudiant, sectorisation des écoles, obligation scolaire…	Crèches, haltes garderies, jardins d'éveil, relais d'assistants maternels…	Piscine, patinoire, stade, gymnase, camping, équipements sportifs, subventions aux clubs, mise à disposition pour les écoles…

La multiplicité des compétences des collectivités augmente d'autant plus la surface d'attaque ainsi que l'intérêt des pirates pour ces structures.

En prenant le cas d'une mairie, ses compétences couvrent la sécurité, l'action sociale et la santé, l'emploi et l'insertion professionnelle, l'enseignement, l'enfance et la jeunesse, les sports…

Un grand nombre de compétences 2/4

ACTION CULTURELLE	TOURISME	FORMATION, APPRENTISSAGE
1 % culturel, écoles de musique, de danse, d'art dramatique, des Beaux-arts, inventaire, bibliothèques, musées, archives, archéologie préventive…	Office de tourisme, promotion	Mise en relation avec les employeurs, reconversion, création ou reprise d'entreprise…

ÉCONOMIE	POLITIQUE DE LA VILLE	URBANISME
SRDEII, aides à la création d'activités, à l'immobilier, aux entreprises en difficultés, aux professionnels de santé, aux cinémas, au maintien de services en milieu rural…	Contrat de ville…	PLU, permis de construire, droit de préemption urbain, ZAD, ZAC, protection des espaces agricoles et naturels…

… l'action culturelle, le tourisme, la formation et l'apprentissage, l'économie, la politique de la ville, l'urbanisme…

Un grand nombre de compétences 3/4

AMÉNAGEMENT	LOGEMENT	DÉCHETS
Aménagement du territoire, amélioration du cadre de vie, SRADT, chartes interco. d'aménagement, aménagement rural…	Financement du logement, PLH, PDH, attribution des logements sociaux, OPH, aides à la pierre, droit au logement opposable, OPAH…	Collecte et traitement des ordures ménagères, déchets des ménages…
EAU, ASSAINISSEMENT	**RÉSEAUX, TÉLÉCOM.**	**ÉNERGIE**
Distribution de l'eau potable, schéma de distribution, zonage d'assainissement, raccordements, eaux pluviales, milieux aquatiques, prévention, canaux…	Infrastructures, réseaux, services de télécommunication, télévision locale…	Distribution d'électricité, gaz, énergie renouvelables, performance énergétique, installations pour véhicules électriques, réseaux de chaleur…

… l'aménagement, le logement, les déchets, l'eau et l'assainissement, les réseaux et télécommunications, l'énergie…

Un grand nombre de compétences 4/4

AÉRODROME	TRANSPORTS PUBLICS	TRANSPORTS SCOLAIRES
Conventions, aménagement, entretien, exploitation des aérodromes civils d'intérêt local, expérimentation, services infra/ interrégionaux…	Transports publics, covoiturage, autopartage, location de vélos, transport de marchandises, logistique urbaine, PDU, routes express, chemins ruraux…	Financement, organisation et fonctionnement des transports scolaires

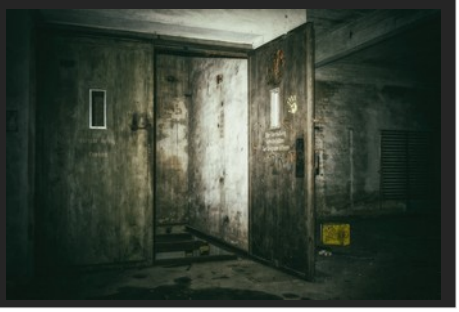
ÉTAT CIVIL	PORTS, VOIES D'EAU, LIAISONS
Naissance, mariage, décès, fermeture de cercueil, cimetières, inhumations, exhumations, crémations, concessions…	Police des ports maritimes, ports intérieurs, de plaisance, maritimes de commerce et de pêche, desserte des îles côtières…

… les aérodrome, les transports publics, les transports scolaires, l'état civil, les ports, voies d'eau et liaisons les concernant.

Je vous laisse imaginer les quantités de données personnelles et qualifiées que les collectivités peuvent détenir. On parle de données qualifiées dans le sens où ce sont des données avec des informations précises et vérifiées contrairement à une simple liste de mails.

Des infrastructures hétérogènes

- Manque de moyens, d’investissements
  - Renouvellement retardé
  - Matériel plus supporté ou mis à jour
- Accès physique faiblement sécurisé
- Éléments non maîtrisés
  - BYOD
  - Télétravail



Du côté du matériel, le grand nombre de compétences se mêle au manque de moyens ou d’investissements, le tout aboutissant à des infrastructures hétérogènes.

Le renouvellement des équipements est souvent retardé et il n’est pas rare d’y trouver du matériel ancien qui n’est plus supporté par son fabricant.

Les accès physiques peuvent également y être plus faiblement sécurisés.

L’évolution des pratiques (BYOD, bring your own device, apportez votre propre matériel) ainsi que le télétravail forcé amené par le confinement du Covid ont introduit dans le SI des équipements que la DSI ne maîtrise absolument pas.

De l'intangible hétéroclite

- Applications, services
  - Mauvaises configurations
  - Mauvaise utilisation du logiciel libre
- Applications métiers
  - Mises à jour, maintenance
  - Éditeurs spécialisés
- Données
  - Incompatibilités d'encodage, de format
  - Mots de passe en clair
  - Infractions au RGPD

Côté logiciel, on va retrouver des mauvaises configurations ou des mauvaises utilisations du logiciel libre. Par exemple, Des collectivités décident parfois d'adapter des logiciels libres.

Il s'agit d'une mauvaise pratique car les correctifs et évolutions du logiciel original ne sont souvent pas transposées sur le logiciel adapté, entraînant l'impossibilité d'appliquer les mises à jour.

Qui dit grand nombre de compétences, dit aussi grand nombre de logiciels souvent développés par des éditeurs spécialisés. De nombreux éditeurs encore présents aujourd'hui se sont créés dans les années 80 ou 90 et ont du mal à s'adapter à la transition du client-serveur au web imposée par les années 2000, que ce soit en termes d'ergonomie ou de sécurité.

Côté données, on va retrouver des problèmes d'incompatibilités d'encodage ou de format, des mots de passe en clair dans les bases de données et bon nombre d'autres infractions au RGPD.

Les raisons d'une cyberattaque

De façon générale, quelles sont les raisons qui poussent les pirates à mener des cyberattaques ?

Pour l'argent !

- Échange clé de déchiffrement contre cryptomonnaie
- Revente
  - Données exfiltrées
  - Portes dérobées
  - Accès initiaux
- Minage de cryptomonnaies
- Fraude au président/RIB

La raison première, c'est l'argent bien sûr !

Que ce soit via le rançonnage, la revente de données exfiltrées, la revente de portes dérobées, le minage de cryptomonnaies, la fraude au président etc.

Il y a quand même des limites : le retour sur investissement et le risque.

Par exemple, il y a très peu de braquage de banque de nos jours parce que le risque est trop grand (forces de l'ordre, caméra de surveillance...) pour peu de retour (les agences de banque ont de moins en moins d'argent liquide dans leurs coffres).

Quelques exemples.

La cyberattaque d'Aix-les-Bains permettait au pirate de faire du minage de cryptomonnaie.

Les données récupérées dans le SI du département de l'Ardèche ont revendues.

On voit aussi que les rançons peuvent se transformer en revente de données sur le marché noir quand la victime ne veut/peut pas payer.

Même si les victimes ayant payé sont plutôt discrètes, les cyberattaques rapportent des millions chaque année aux pirates.

Pour des raisons stratégiques

- Préparation d’une cyberattaque
- Atteinte à l’image
- Espionnage
- Sabotage
- Hacktivisme

Pirater peut aussi se faire pour des raisons stratégiques.

Une attaque peut être perpétrée dans le but de préparer d’autres cyberattaques ou de préparer des opérations militaires.

Cela peut être pour porter atteinte à l’image d’une organisation ou d’une entreprise, pour espionner, saboter ou faire du militantisme.

Ce sont souvent les États qui ont recours aux cyberattaques à but stratégique.

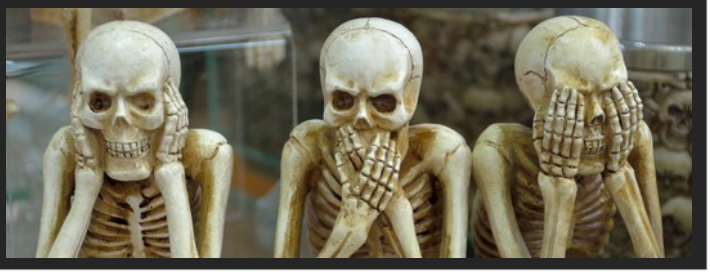
Dans la presse déchaînée, on peut apprendre que la Corée du Nord a peut-être hacké Sony à cause d'un film potache sur Kim Jong Un, que les États-Unis et Israël ont développé Stuxnet pour saboter le nucléaire iranien ou encore que le Vatican et le Parlement européen ont été visés pour leurs positions sur la guerre en Ukraine.

Déroulement d'une cyberattaque

Savoir comment se déroule une cyberattaque permet de mieux se préparer mais aussi d'être plus efficace lorsqu'on en subit une.

La (Unified) Kill chain

- Phases successives d'une cyberattaque
- Du point de vue de l’attaquant
- Première version en 2011 (Lockheed Martin)
- Outil de sensibilisation et d’évaluation



Les phases d’une cyberattaque sont dénommées « kill chain » ou cinétique d’attaque.

Cette notion a d’abord été développée par Lockheed Martin en 2011 mais il en existe plusieurs versions.

C’est un outil qui permet d’évaluer la progression d’une attaque et aussi de sensibiliser.

La version que je vais vous présenter s’appelle Unified Kill Chain et a été établie par Paul Pols en 2017.

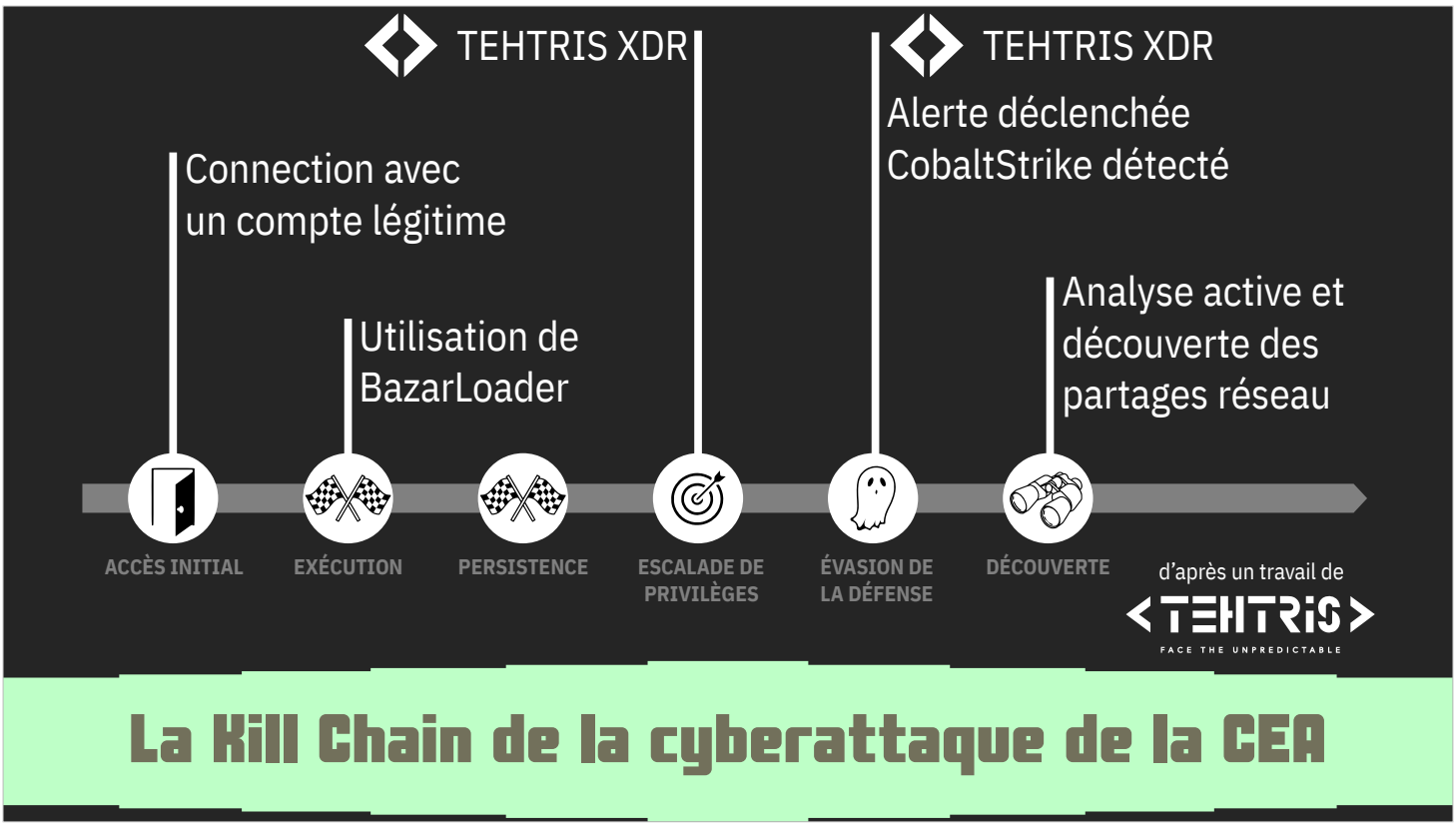
La capacité à corréler des événements qui proviennent de multiples sources grâce à la partie SIEM de Tehtris nous a permis de recréer la Kill Chain dans des délais très courts. [...]
Nous étions clairement plus près de la fin de cette Kill Chain que du début !

JÉRÉMIE PIAZZA, RSSI COLL. EUROP. D'ALSACE
LE MAG-IT - 18/04/2023

Le 28 septembre 2022, la Collectivité Européenne d'Alsace (fusion des départements du Haut-Rhin et du Bas-Rhin) subissait une cyberattaque.

Jérémie Piazza, le RSSI de cette collectivité, est revenu sur cet épisode dans Le Mag-IT en avril 2023.

Il précise que l'usage de l'EDR de Tehtris leur avait permis de recréer la Kill Chain rapidement pour finalement s'apercevoir que l'attaquant avait bien progressé !

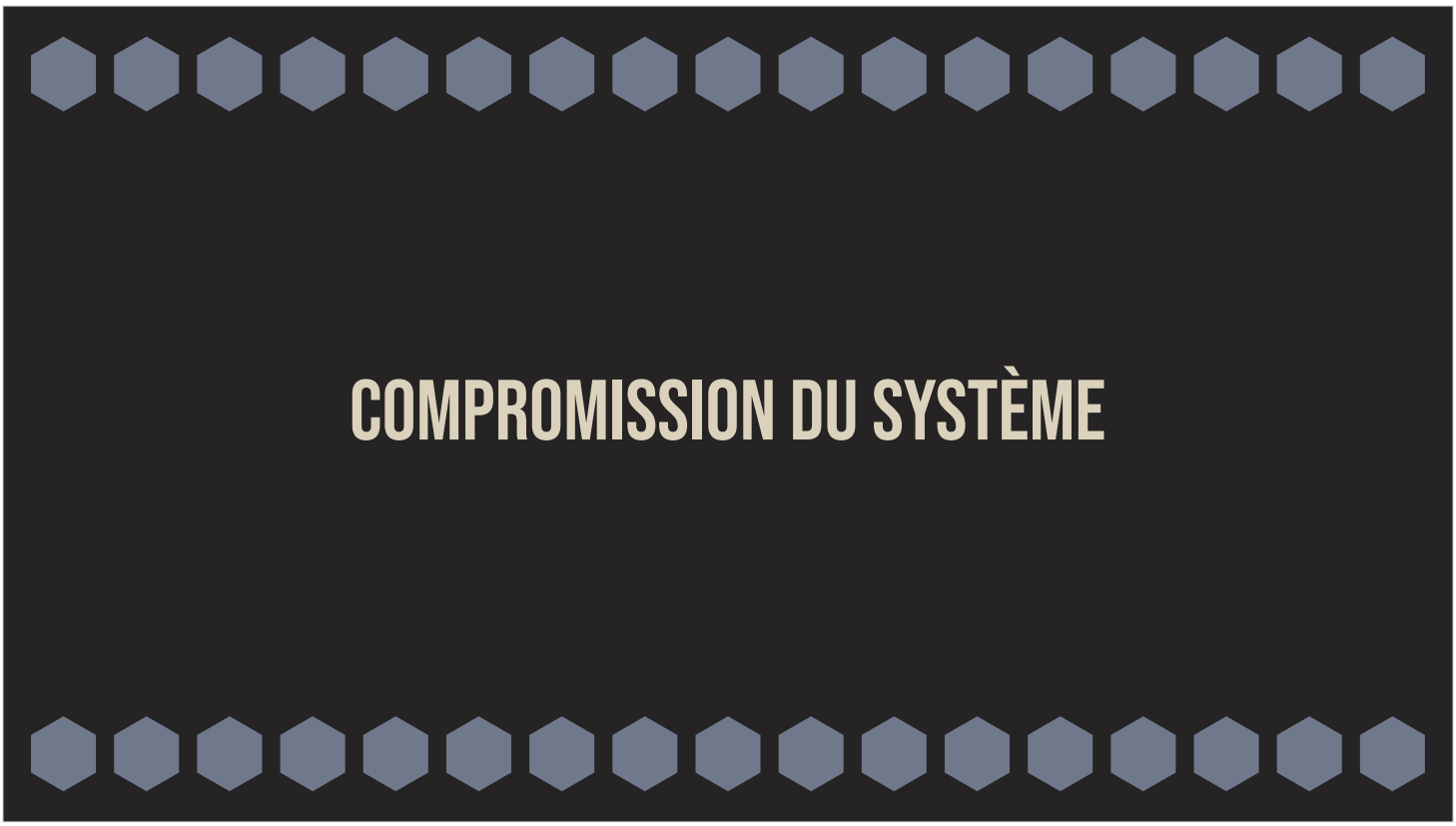


Une Kill Chain peut comporter de nombreuses étapes.

Elles ne sont cependant pas toutes nécessaires pour mener à bien une attaque.

Leur ordre n'est également pas gravé dans le marbre.

Dans un retour d'expérience sur la cyberattaque de la Collectivité Européenne d'Alsace, Tehtris a dégagé les étapes d'accès initial, d'exécution, de persistance, d'escalade des privilèges, d'évasion de la défense et de découverte.



La chaîne d’attaque unifiée se décompose en 3 parties.

Il y a tout d’abord la compromission du système.

Reconnaissance

- Recherche, identification et sélection des cibles
  - Informations disponibles publiquement (OSINT)
  - Renseignement sur les systèmes utilisés (versions, failles…)
  - Scan d’adresses IP
  - Recours au marché noir (mails, mots de passe, failles zero-day…)
- Reconnaissance active ou passive

Chaque partie se décompose en étapes.

En premier, il y a la reconnaissance.

À cette étape, il n’y a souvent aucun contact entre le pirate et sa cible.

Le but va être de rechercher, identifier et sélectionner des cibles. Le pirate peut faire de l’OSINT, c’est-à-dire récolter des informations disponibles publiquement pour profiler sa cible.

Une fois ces informations collectées, il est possible de dresser une liste de failles potentiellement utilisables pendant l’attaque, voire de chercher sur le marché noir.

Armement

- Mise en place d’une infrastructure nécessaire à l’attaque
  - Achat de noms de domaines similaires à la cible
  - Récupération de malware prêts à l’emploi
  - Développements spécifiques
  - Compromission de serveurs
  - Location de botnet
  - Etc.

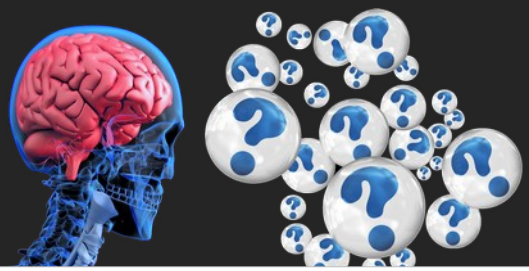
Il est alors temps de s’armer, de mettre en place l’infrastructure nécessaire à l’attaque.

Cela passe par de l’achat de noms de domaines similaires à celui de la cible, la récupération de malwares prêts à l’emploi, de développements spécifiques, de location de botnets etc.

Les botnets sont des réseaux d’ordinateurs ou d’appareils connectés à internet qui ont été piratés afin d’agir sur commande d’un pirate. De tels réseaux permettent d’envoyer du spam, de faire des attaques par déni de service ou de miner de la cryptomonnaie.

Ingénierie sociale

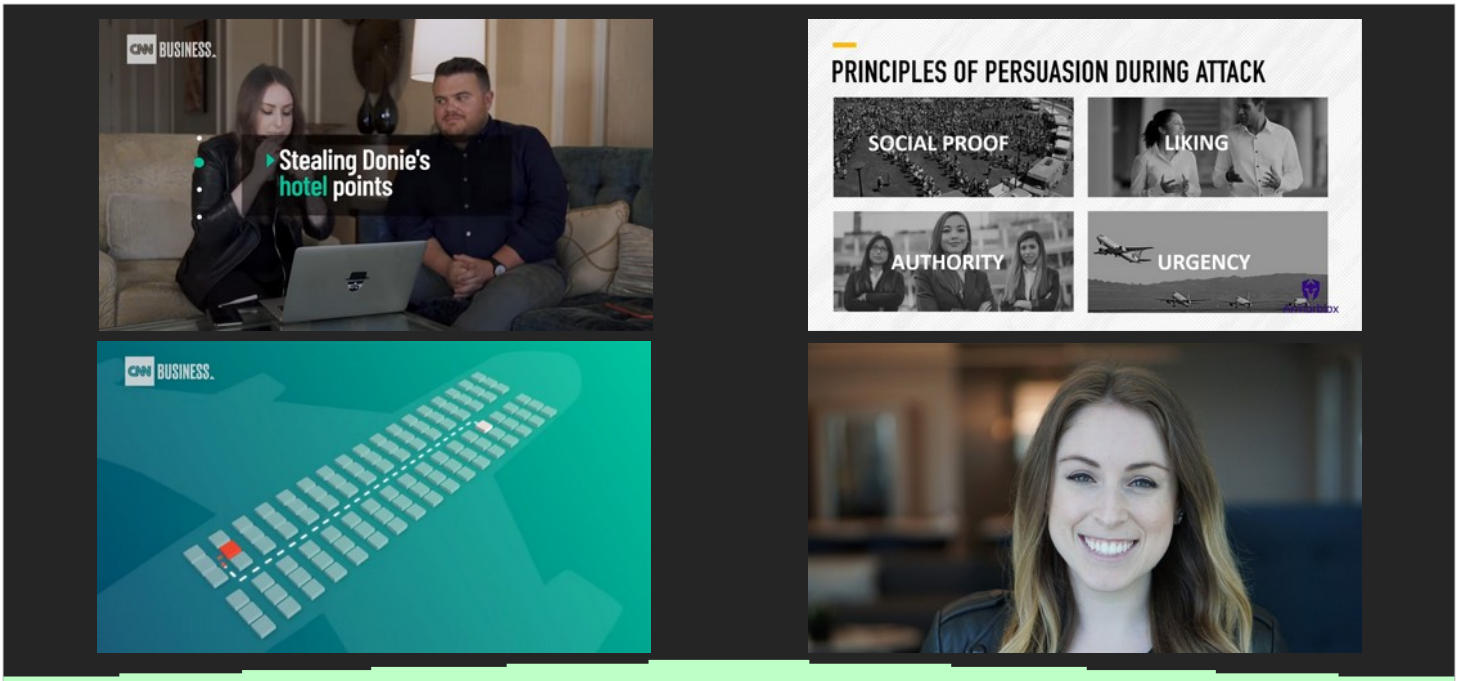
- Manipuler…
  - Preuve sociale
  - Empathie
  - Autorité
  - Urgence
- … pour faire faire des actions dangereuses
  - Visite de site malveillant
  - Clic sur un lien malveillant
  - Ouverture de fichier piégé



La cible identifiée, l'ingénierie sociale va permettre d'amener la victime à faire un faux pas, la flouer ou récupérer des accès.

L'ingénierie sociale ne requiert pas de compétences informatiques particulières, seulement de savoir manipuler des personnes en utilisant des biais cognitifs.

Les principaux sont la preuve sociale, l'empathie, l'autorité et l'urgence.



Rachel Tobac et l'ingénierie sociale

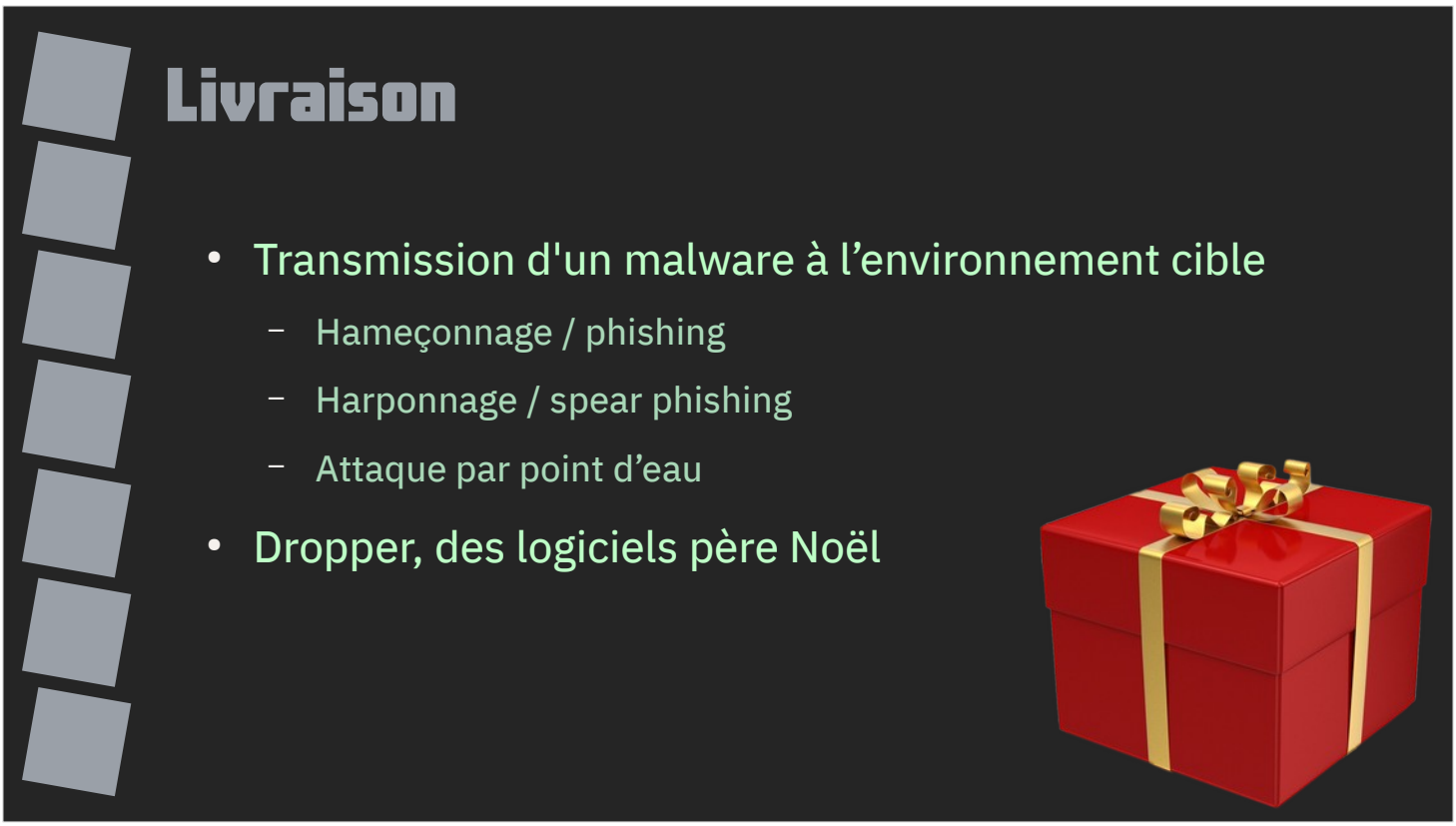
Pour illustrer l'ingénierie sociale, tapez « Rachel Tobac » sur YouTube.

Vous tomberez probablement sur une vidéo dans laquelle elle exerce ses techniques sur un journaliste de CNN.

En parcourant les réseaux sociaux et en passant quelques coups de téléphones, elle parvient à :

- Voler 90000 points d'hôtel du journaliste (l'équivalent de 1000 à 2000 dollars)
- Changer une bonne place dans l'avion de retour du journaliste contre une place peu intéressante (au fond de l'avion entre deux sièges)

Côté look, on est très loin du cliché sur les pirates !



La livraison consiste à transmettre un malware à l’environnement cible, que ce soit par phishing (spam à l’aveugle), harponnage (spam ciblé) ou par attaque par point d’eau.

Dans une attaque par point d’eau, la victime ne reçoit rien. Elle sera piégée alors qu’elle utilise un site sur lequel elle se rend régulièrement comme des espaces de discussions dédiés à son cœur de métier.

La livraison passe souvent par un paquet cadeau appelé « dropper », un logiciel générique capable d’installer n’importe quel logiciel sur un ordinateur cible.

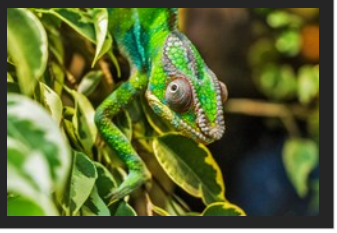
Exploitation

- Exploitation des failles d’un système
  - Faille connue non corrigée ou inexploitable en théorie
  - Faille inconnue (zero-day)
- Dans le but de
  - Pénétrer le système
  - Exécuter des malwares
  - Analyser le système

Un premier pied a été mis chez la victime, il est temps d’exploiter les failles du système dans le but de le pénétrer complètement, d’exécuter des malwares et de l’analyser encore plus.

Persistance

- Conserver l’accès au système cible
- Empêcher la suppression des malwares
  - Faire passer le malware pour un service légitime
  - Modifier la base de registre
  - S’installer sur le boot
  - Etc.



Maintenant que le pirate a pénétré le système, il doit s’assurer de pouvoir y rester.

Cela va passer par des techniques empêchant la suppression des malwares comme les faire passer pour des services légitimes, en modifiant la base de registre de Windows, en les installant sur le secteur d’amorce du disque dur de l’ordinateur afin d’être exécuté à chaque démarrage etc.

Évasion de la défense

- Échapper aux systèmes de détection
  - Désactiver la sécurité (anti-virus, pare-feu…)
  - Désactivation des rapports de crash, des dumps
- Échapper à l’analyse des systèmes infectés
  - Effacement périodique des journaux d’événements
  - Modification de l’horodatage des fichiers

L’objectif de l’attaque étant encore loin d’être atteint, il est primordiale de s’assurer qu’on passera incognito.

Il faut par exemple désactiver les anti-virus, les pare-feux, les rapports qui permettraient de détecter un comportement anormal, de faire comme si rien ne s’était passé en changeant les dates de dernière modification des fichiers infectés.

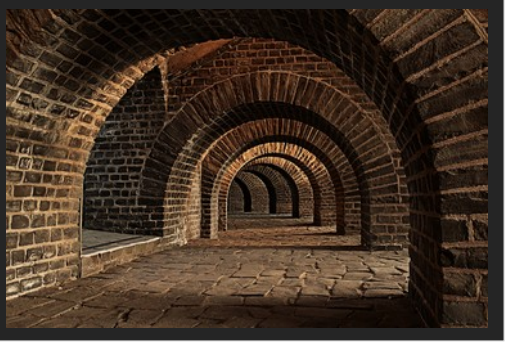
Commande et contrôle

- Commande à distance des éléments piratés
  - Installation d’une porte dérobée (backdoor)
  - Mise en place d’un canal de communication (direct, proxy, mail…)

Le pirate est dans la place pour longtemps, personne ne détecte sa présence, il est temps d’installer une porte dérobée ou un canal de communication qui permettra de contrôler l’ordinateur à distance afin de faciliter l’attaque.

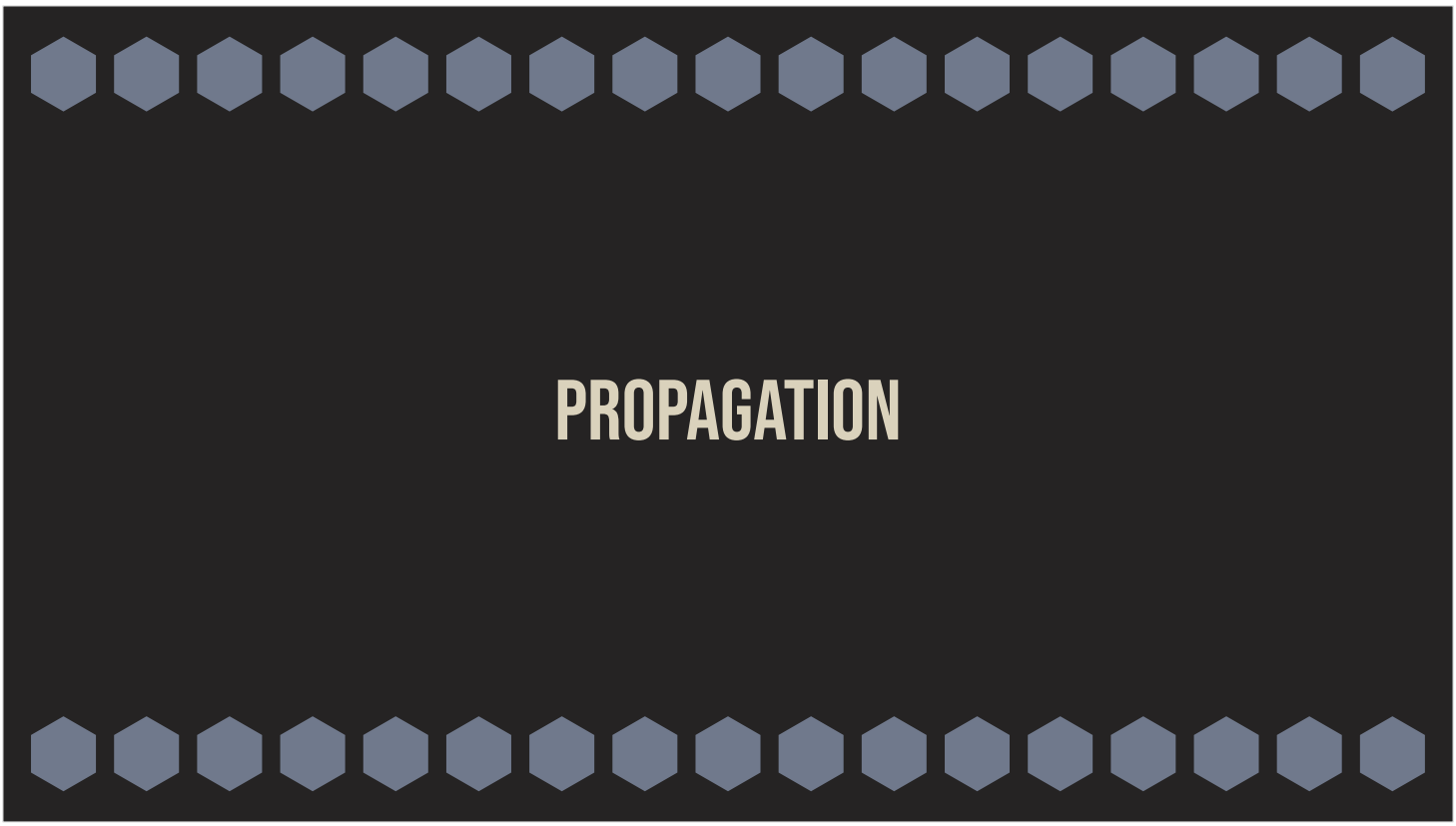
Pivotement

- Mise en place d’un tunnel vers des systèmes inaccessibles
  - Accès instantané
  - Accès différé
- Prépare les phases
  - Découverte
  - Mouvement latéral



Le point d’entrée dans le SI de la victime est bien installé, il faut mettre en place des chemins vers les systèmes internes, normalement inaccessibles de l’extérieur.

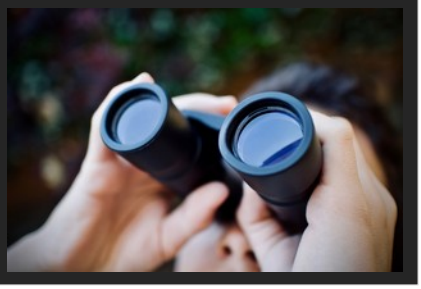
Cela permet de préparer les phases de découverte et de mouvement latéral.



Place à la propagation !

Découverte

- Recueil d’informations détaillées sur le système infecté
  - Emplacement physique de l’ordinateur
  - Liste de processus en cours d’exécution
  - Analyse du réseau interne



Pour optimiser la portée de son action, le pirate doit recueillir le maximum d’informations sur le système infecté : où se situe physiquement l’ordinateur au sein de l’organisation, la liste des tâches qu’il effectue et analyser le réseau interne.

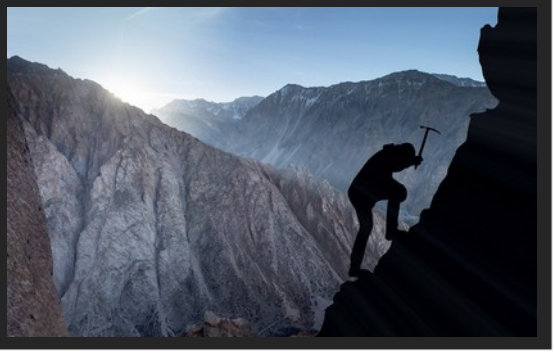
Exécution

- Téléchargement, exécution de modules supplémentaires

Si besoin, avec les informations supplémentaires récupérées, le pirate peut télécharger et exécuter des modules supplémentaires.

Escalade de privilèges

- Obtention d’autorisations plus élevées sur le système
- Utilisation de failles existantes
- Amélioration de la persistance du malware



De grandes ambitions nécessitent de grands privilèges, le pirate doit obtenir plus de droits sur le système que ceux dont dispose le compte qu’il a usurpé.

Cette phase fait appel à l’utilisation de failles existantes.

Vol d’infos d’identification

- Messagerie
  - Récupération des contacts, de l’annuaire
  - Envoi de messages piégés
- Utilisation de failles de sécurité
  - Analyse de la mémoire
  - Lecture de fichiers protégés
- Utilisation d’un keylogger

Ça peut toujours servir : voler des infos d’identification.

Les messageries en regorgent, le carnet d’adresses ou l’annuaire de l’entreprise étant de bons points de départ. Des messages piégés peuvent également être envoyés de façon totalement officielle depuis le compte usurpé.

Un keylogger, logiciel capturant les touches tapées au clavier branché sur la machine, permettra de récupérer les identifiants et mots de passe de chaque personne l’utilisant. En espérant tomber sur un administrateur système.

Mouvement latéral

- Accéder à des éléments de plus grande valeur
  - Active Directory
  - Bases de données
  - Sauvegardes
  - Équipements réseau
- En prendre le contrôle

Les ordinateurs piratés pour pénétrer les SI ont rarement une grande valeur stratégique.

Le pirate a besoin d'accéder à des éléments de plus grande valeur comme les Active Directory (serveurs contrôlant l'accès aux ressources du SI), les bases de données, les sauvegardes (pour pouvoir limiter la récupération des données ou récupérer des données de systèmes trop résistants) ou les équipements réseau.

Et bien sûr, d'en prendre le contrôle.

Le pirate a bientôt atteint ses objectifs.

Collecte

- Identifier et recueillir des données
  - Fichiers (PDF, Word, Excel...)
  - Mails, communications
  - Bases de données
- Dans le but de
  - Exfiltrer les données
  - Chiffrer les données

Il doit procéder à la collecte des fichiers (PDF, Word, Excel...), des mails, des communications, des bases de données etc.

Dans le but d’exfiltrer et/ou de chiffrer les données.

Exfiltration

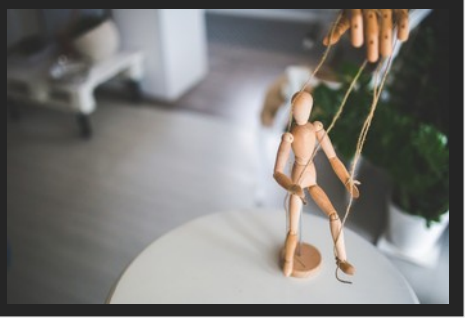
- Transfert des données du système vers un autre réseau
- Principe de la double extorsion
  - Demander une rançon
  - Et revendre les données sur le marché noir

Exfiltrer les données, quand cela est possible, est très intéressant.

Cela permet de faire d’une pierre deux coups : demander deux rançons, la première pour déchiffrer les données, la deuxième pour ne pas revendre les données au marché noir.

Manipulation de la cible

- Atteindre l'objectif de l'attaque
  - Chiffrement des données
  - Déni de service
  - Mise hors service



Le pirate peut maintenant s’en donner à cœur joie et chiffrer les données.

La manipulation de la cible peut aussi se traduire par un déni de service voire une mise hors service du SI.

Objectifs

- Objectifs de l'attaque visant à atteindre un but stratégique
  - Atteinte à l’image, décrédibilisation
  - Déstabilisation
  - Etc.

Les objectifs sont désormais atteints !

La cybersécurité

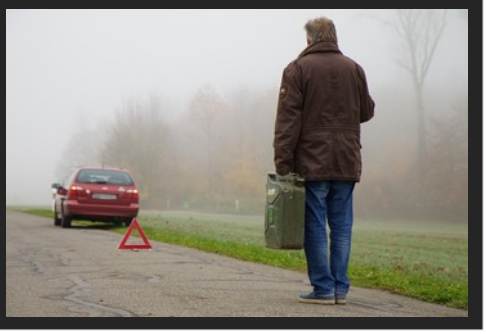
Maintenant que l’on sait comment opèrent les pirates pour mener leurs attaques, comment se dessine le paysage de la cybersécurité ?

Au premier abord, il apparaît plutôt terne.

Lors du Forum internationale de la cybersécurité de 2022, Guillaume Poupard, alors directeur général de l'Anssi (Vincent Strubel occupe ce poste depuis janvier 2023), déclarait que le sujet RH était ce qui allait nous limiter dans les années à venir.

Pénurie de talents

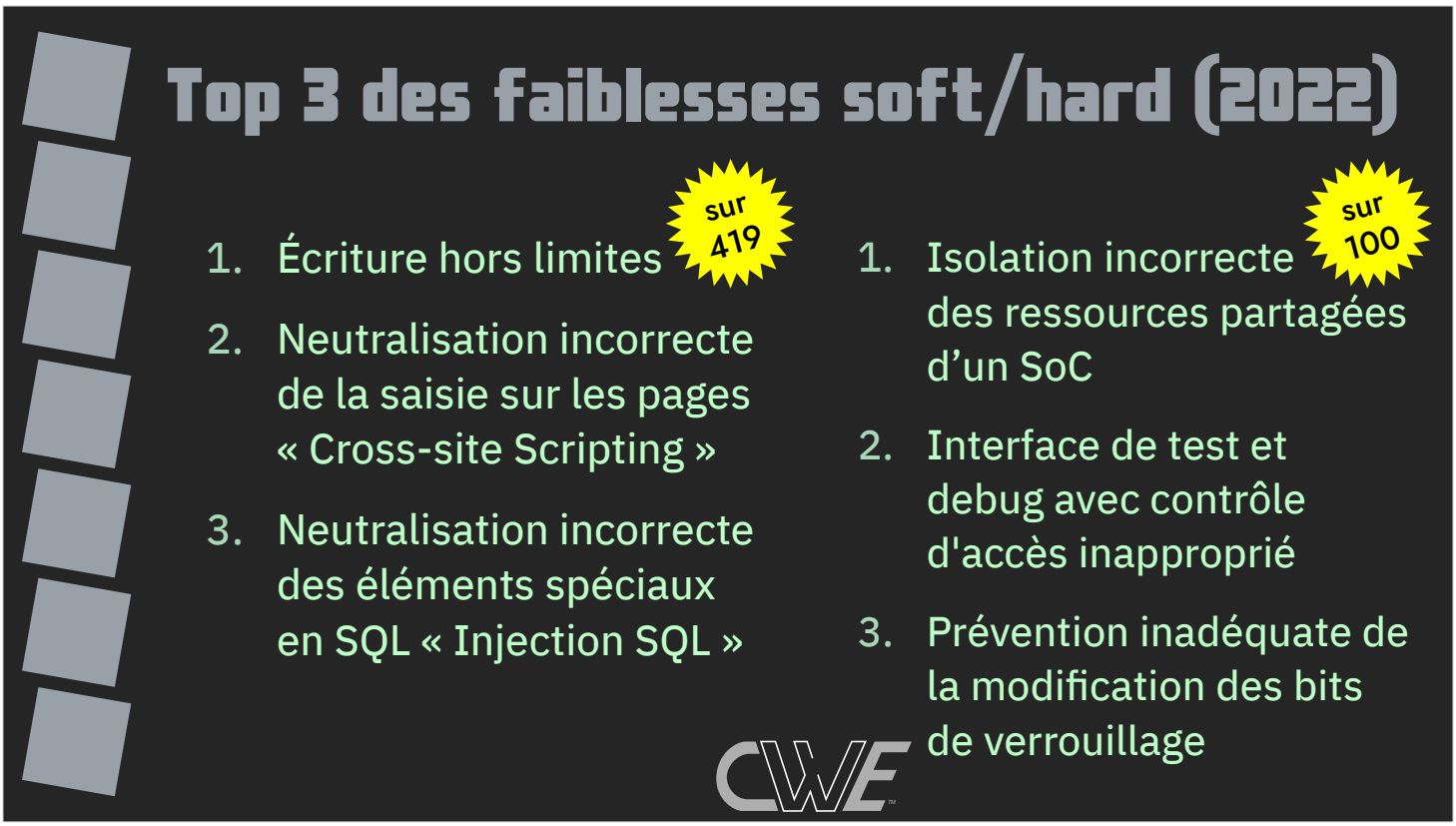
- 3 millions de personnes qualifiées manquent à l'appel
  700000 aux États-Unis, 15000 en France
- Un salaire médian inférieur à celui du privé
  Les grosses structures payent plus que les petites
- Surveillance H24 ?
  Recours à un SOC externalisé mutualisé



Car il y a actuellement une pénurie de talents : 3 millions de personnes qualifiées manquent à l'appel, dont 700000 rien qu'aux États-Unis et 15000 en France.

Pour les collectivités, la tâche de recrutement de profils spécialisés va être d'autant plus ardue que le salaire médian est traditionnellement inférieur à celui du privé. Et les grosses collectivités ont plus de moyens que les petites.

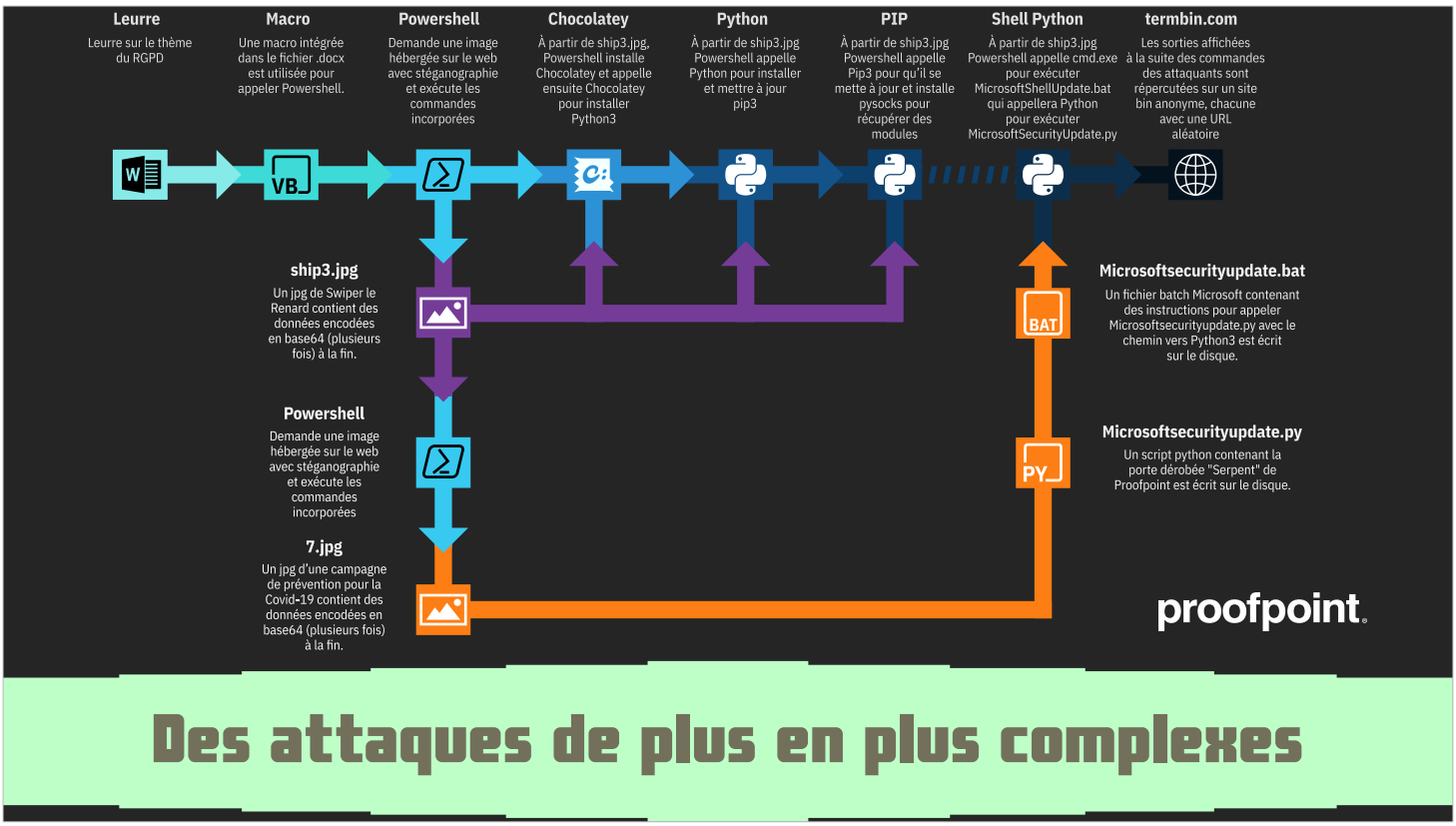
D'autant que les SI nécessitent aujourd'hui une surveillance H24.



La CWE (Common Weakness Enumeration ou énumération des faiblesses communes recense 419 types de faiblesse dans les logiciels et 100 pour le matériel.

Ce TOP3 est un extrait du TOP25 des faiblesses les plus couramment utilisées qu'elle dresse chaque année.

Le nombre de faiblesses est tellement grand qu'il est peu probable que les développeurs d'applications ou de matériels les connaissent tous.



Les attaques quant à elles sont de plus en plus élaborées et complexes.

Cela est dû à l'évolution de l'informatique et des réseaux :

- Des ordinateurs, des smartphones ou des tablettes avec toujours plus de mémoire, de disques, de puissance de calcul
- Des réseaux toujours plus rapides
- Des protocoles et standards toujours plus complexes

Ce schéma décrit la séquence d'actions menées par un malware pour installer un logiciel permettant de contrôler une machine à distance. Elle montre notamment l'utilisation de la stéganographie pour masquer l'existence du malware aux EDR potentiellement installés. Il ne s'agit que de la cinquième phase de la chaîne d'attaque unifiée, « Commande et contrôle ».

Des cybercriminels toujours plus pro

- Société de services
  - Ransomware as a Service
  - Malware as a Service
  - Location de botnet
  - SAV
- Marché noir
- International

Geek à capuche chez ses parents

Les cybercriminels, eux, sont plus professionnels que jamais !

Tout un écosystème de la cybercriminalité existe avec des spécialisations de plus en plus fines des acteurs.

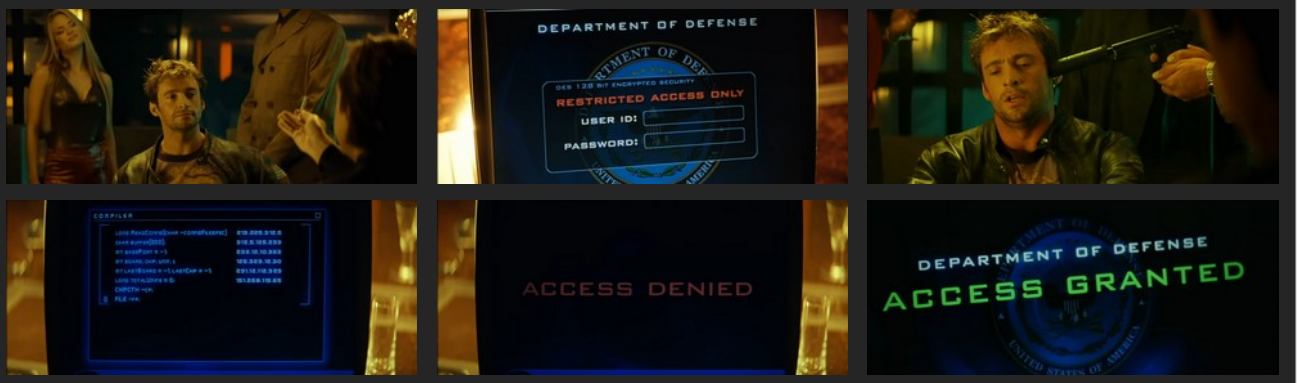
On peut accéder à des Ransomware as a Service, des Malwares as a Service etc. moyennant un pourcentage des recettes ou une somme fixe. Il est ainsi possible d'attaquer en ayant finalement très peu de ressources matérielles puisqu'elles sont fournies.

On peut louer des botnets à la journée, à la semaine, pour faire du déni de service, des campagnes de spam. Certains proposent un service après-vente ou des garanties « satisfait ou remboursé ».

Le marché noir est très développé et on peut y trouver des données volées, des malwares, des kits prêts à l'emploi etc.

Le système d'affiliation offre le travail à l'international en full-remote. Oubliez le geek à capuche dans la cave de ses parents !

Dans la culture populaire



Opération Espadon (2001) – Scène du recrutement
Stanley, ancien hacker qui n'a plus touché d'ordinateur depuis son passage en prison, parvient à cracker un chiffrement « DES 128 bits » en 60 secondes chrono, sous la menace, sur un ordinateur qu'il touche pour la première fois

L'un des clichés les plus risibles en la matière est le film Opération Espadon de 2001, dans la scène du recrutement.

Des mercenaires ont à tout prix besoin du hacker ultime.

Stanley est un ancien hacker qui n'a plus touché d'ordinateur depuis son passage en prison.

Lors de l'entretien, il parvient à cracker un chiffrement « DES 128 bits » en 60 secondes chrono, sous la menace, sur un ordinateur qu'il touche pour la première fois.

Tout d'abord, le DES 128 bits n'existe pas, ce qu'on peut pardonner aux scénaristes. Mais l'algorithme DES, en 2001, était déjà obsolète.

Ensuite, quand on arrive sur un ordinateur qu'on n'a jamais touché, avec des outils qu'on ne connaît pas, il est difficile de faire quoi que ce soit de productif en 60 secondes.

Alors tout n’est pas gris dans le paysage.

De nombreux acteurs officiels s'organisent, qu'ils soient historiques ou créés en réponse à la cybercriminalité.

On peut citer :

- l'Enisa, l'agence européenne,
- l'Anssi, l'agence nationale,
- Europol,
- les Csirt régionaux, qui sont très récents,
- l'initiative Cybermalveillance.gouve.fr
- ou encore la Cnil.

Lutte contre la cybercriminalité

- **STRJD**
  Service technique de recherches judiciaires et de documentation
- **IRCGN**
  Département informatique et électronique de l'institut de recherche criminelle de la Gendarmerie nationale
- **Formation N-TECH**
- **SR**
  Sections de recherches
- **BDRIJ**
  Brigade départementale de renseignements et d'investigations judiciaires
- **C3N**
  Centre de lutte contre les criminalités numériques

En matière de cybercriminalité, des cellules sont organisées par les services de l'Étatcomme le STRJD, l'IRCGN, les sections de recherches, la BDRIJ, le C3N...

La formation N-TECH qui s'adresse aux membres des forces de l'ordre.

Formations (1/2)

- Bac
  Bac pro, spécialité Cybersécurité, informatique et réseaux, électronique (2023)
- Bac + 2
  BTS Systèmes Numériques Informatique et réseaux, cyberdéfense (2017)
- Bac + 3
  Licence pro administration et sécurité des réseaux, sécurité des applications et des réseaux informatiques – Licence pro administration et sécurité des systèmes et des réseaux, cyberdéfense, anti-intrusion des SI – Licence d'informatique, parcours cyberdéfense – Bachelor Sécurité Informatique

Plus généralement, il existe maintenant des formations diplômantes allant du bac pro à bac + 5 et plus.

Si le bac pro spécialité cybersécurité a été créé en 2023, les formations existent depuis plus longtemps comme avec le BTS systèmes numériques informatique et réseaux, parcours cyberdéfense créé en 2017.

Plus on avance dans les études, plus de diversité s'offrent aux futures diplômés et diplômées.

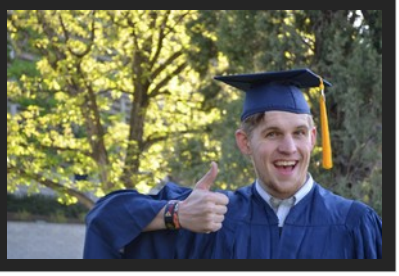
Formations (2/2)

- Bac + 5
  Master Cyberdéfense et sécurité de l'information – Master Ingénierie des réseaux de communications mobiles et sécurité – MBA management de la sécurité des données numériques – Mastère spécialisé cybersécurité – MSc Cybersécurité
- Labels SecNumEdu et SecNumEdu-FC de l'Anssi

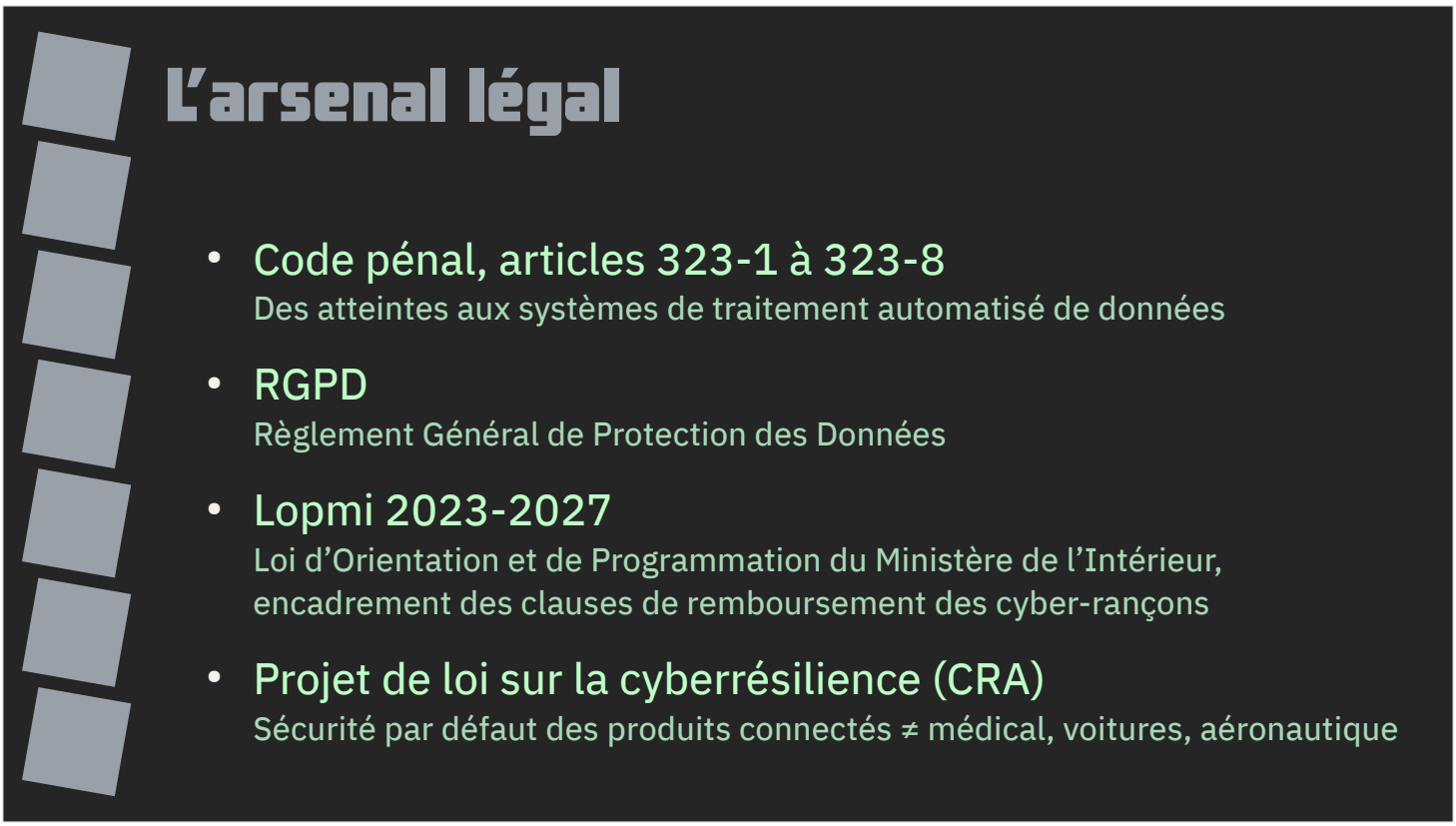
L'Anssi a créé les labels SecNumEdu et SecNumEdu-FC qui permettent de garantir un niveau de formation en matière de sécurité informatique.

Certifications

- Certifications de sécurité (Anssi)
  - Certification Critères Communs (CC)
  - Certification de Sécurité de Premier Niveau (CSPN)
- Prestataire de Vérification d'Identité à Distance (PVID)
- ISO/IEC 27001
  - Management de la sécurité de l'information



Des certifications ont été créées comme les certifications de sécurité de l'Anssi, les prestataires de vérification d'identité à distance, la norme ISO 27001 en management de la sécurité de l'information.



L'arsenal légal s'est étoffé.

Le code pénal dispose d'article concernant les atteintes aux systèmes de traitement automatisé de données.

L'Europe a créé le Règlement Général de Protection des Données, le RGPD, et travaille actuellement sur la loi sur la cyberrésilience qui va imposer le principe de sécurité par défaut pour les systèmes informatiques (à l'exception des dispositifs médicaux, de l'aéronautique et des voitures car soumis à d'autres textes).

La Lopmi 2023, loi d'orientation et de programmation du ministère de l'intérieur, a été votée le 24 janvier 2023. Elle encadre notamment les clauses de remboursement des cyber-rançons par les assurances. Une des conditions est le dépôt d'une plainte de la victime dans les 72 heures après connaissance de la cyberattaque.

Quelques acteurs du marché

- ESN certifiées
  www.ssi.gouv.fr/uploads/liste-produits-et-services-qualifies.pdf
- Plateforme de bug bounty
  YesWeHack, Open Bug Bounty, Hackerone, Bugcrowd, SafeHats...
- Programme CVE
  Identifier, définir et cataloguer les failles divulguées publiquement
- Google Project Zero
  Chercheurs en sécurité de Google étudiant les failles 0-day

Le marché s'organise lui aussi petit à petit.

L'Anssi propose toute une liste d'ESN certifiées qui pourront répondre aux sollicitations des collectivités pour gérer les cyberattaques.

Des plateformes de bug bounty se sont montées. Elles mettent en relation des entreprises ou collectivités avec des hackers. Quand ceux-ci découvrent des failles, ils touchent alors une prime.

Les failles de sécurités sont depuis longtemps identifiées et cataloguées dans une liste de référence appelée CVE (pour common vulnerabilities and exposures).

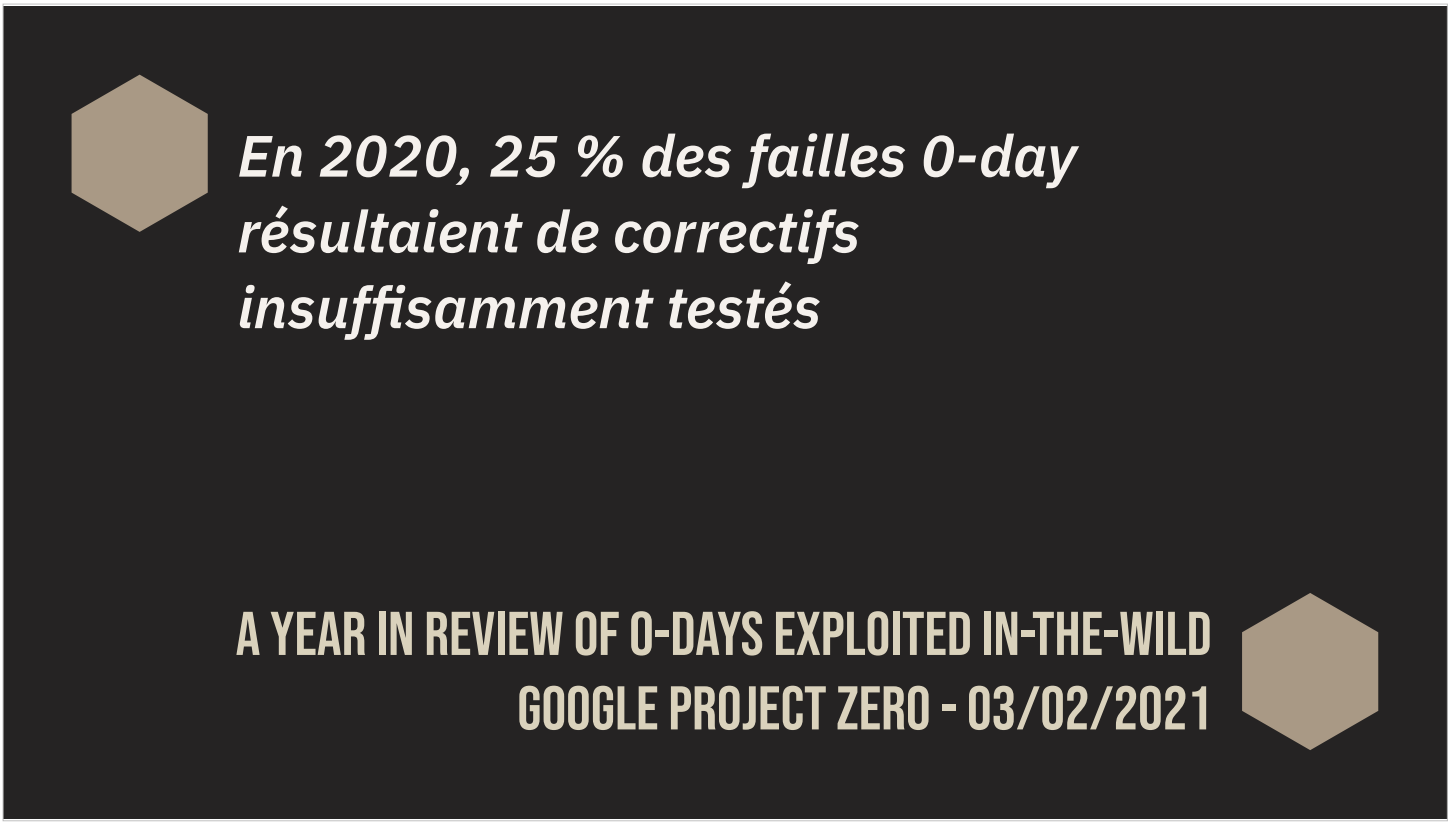
Google a lancé l'initiative Google Project Zero, une équipe de chercheurs en sécurité qui étudie et cherche des failles zero-day.

Adobe - Airbnb - Alibaba - Aliexpress - Amazon Web Services - Android – Apache
Apple - Asus - AT&T - Avast! - BASF - Bing - Blogger - Bosch - Cisco – Cloudflare
Cobalt - Deliveroo - Dell - Deutsche Telekom - Docker - Drupal - Dyson – eBay
Electronic Arts - Facebook - Github - Google - HTC - Huawei - IBM - IKEA – Intel
League of Legends - Lenovo - LinkedIn - MailChimp - Massachusetts Institute of
Technology - MasterCard - Matomo - Mattermost - McAfee - Microsoft – Motorola
Mozilla - Netflix - Netgear - Nokia - Nvidia - Oath - Open Office - OpenSSL – Opera
Oracle - Orange - OVH - OWASP - Panasonic Avionics - Paypal - Philips – PHP
Pinterest - Samsung - SAP - Slack - Sony - Sophos - SoundCloud – Spotify
Starbucks - Symantec - Synology - Telegram - Tinder - Tumblr - Twitch – Twitter
Typo3 - Uber - United Airlines - Verizon - Viadeo - Vimeo - Vodafone - Western
Union - WordPress - Xiaomi - Yahoo - Yandex - YouTube - Zimbra

De nombreux programmes de bug bounty

De nombreuses entreprises ont leur propre programme de bug bounty.

Toutes ces initiatives sont les bienvenues mais la tâche est colossale.



Le Google Project Zero a remarqué qu'en 2020 les correctifs développés pour corriger des failles zero-day n'étaient pas toujours complètement efficaces. 25 % corrigeaient insuffisamment la faille.

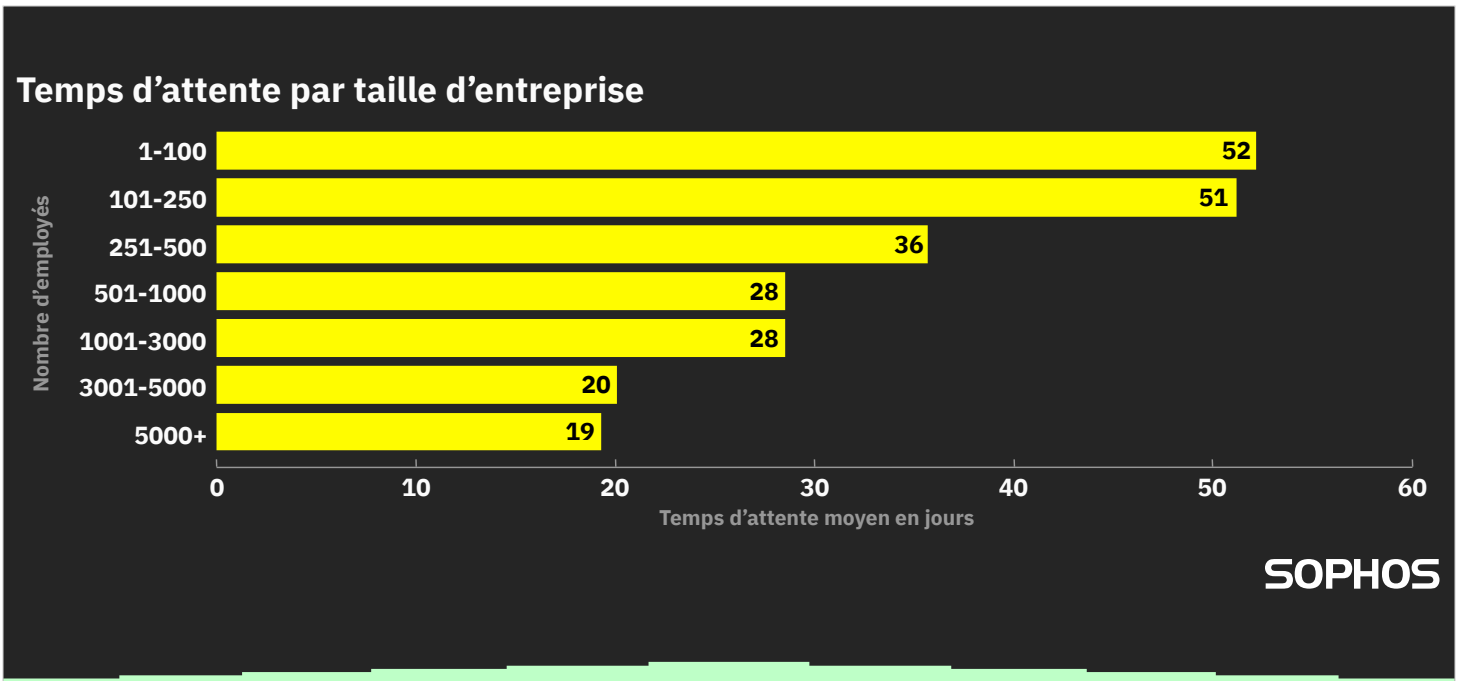
On a d’ailleurs vu en 2022 le cas d’une faille zombie qui touchaient les navigateurs Safari d’Apple. Un bug corrigé en 2013 avait été réintroduit par mégarde en 2016. Il est resté ouvert jusqu’en 2022, année de sa redécouverte et de sa correction.

Fenêtre d’exposition

- [Faille 0-day]
- Découverte de la faille
- Prise en compte par l’éditeur
- Développement du correctif
- Diffusion du correctif
- Installation du correctif

La fenêtre d’exposition mesure le temps pendant lequel un système est exposé à une faille.

Entre la découverte d’une faille zero-day par les pirates, la découverte de cette faille par des équipes spécialisées en cybersécurité, la prise en compte par l’éditeur, le développement du correctif, la diffusion de ce correctif et l’installation par les utilisateurs, la fenêtre d’exposition peut se compter en années.



Temps d'attente avant détection en 2021

Le temps d'attente avant détection mesure quant à lui le temps entre le début de la compromission du système et sa détection.

D'après une étude de Sophos sur 2021, le temps d'attente dépend de la taille de l'entreprise (plus précisément de ses moyens). Jusqu'à 250 personnes, une entreprise mettra une cinquantaine de jours à s'apercevoir qu'elle a été piratée.

Le temps de détection le plus court revient aux grosses entreprises de plus de 3000 personnes mais reste néanmoins autour de la vingtaine de jours.

Qui contrôle quoi ?

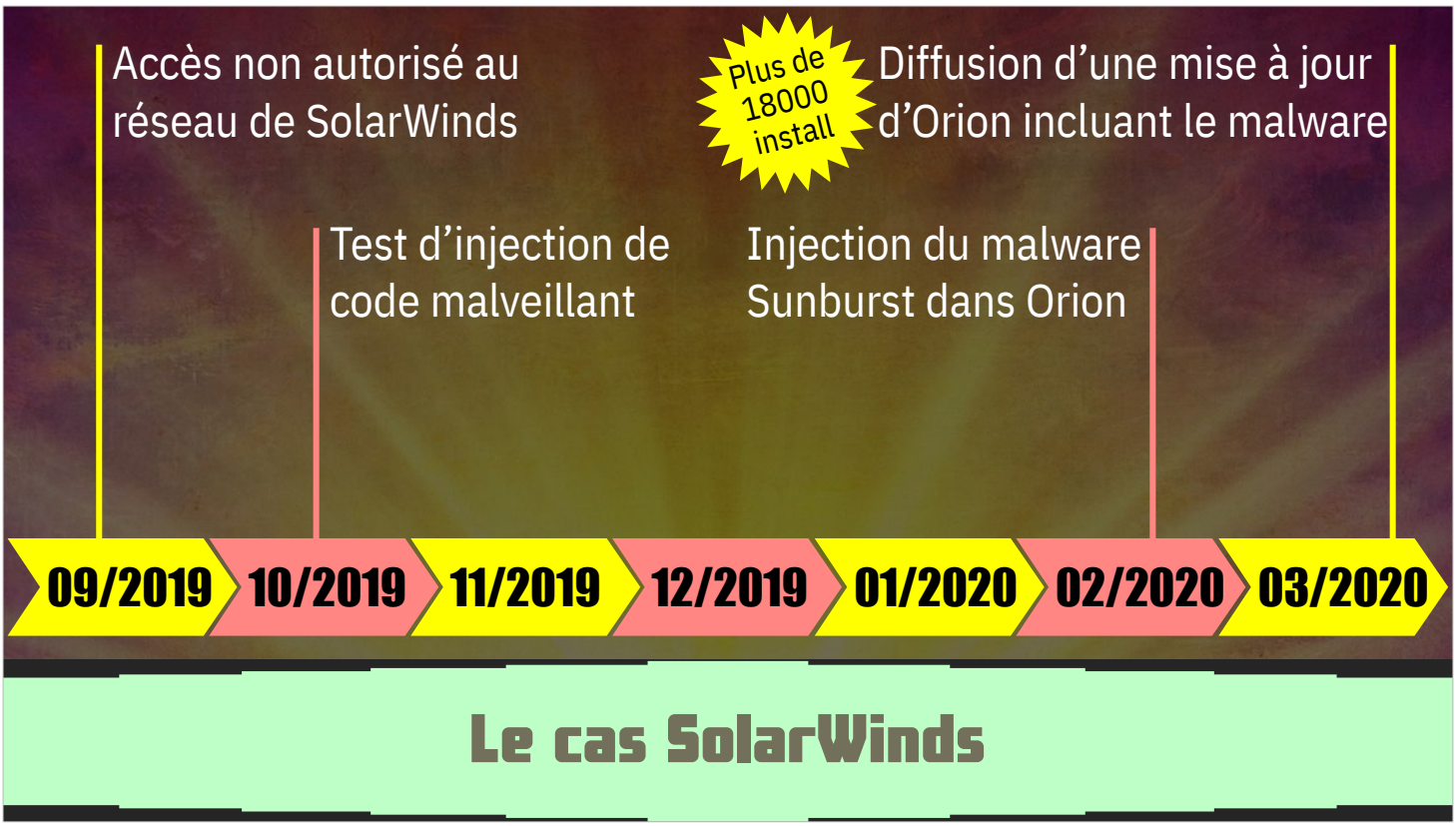
	serveur	ordinateur	réseau	logiciel	donnée	droit
DSI	?	?	?	?	?	?
service	?	?	?	?	?	?
agent	?	?	?	?	?	?
prestataire	?	?	?	?	?	?
usager	?	?	?	?	?	?
développeur	?	?	?	?	?	?

- Impossibilité de maîtriser complètement un SI
  BYOD, cloud, télétravail, supply-chain…

Savoir qui contrôle quoi dans un SI n’est pas aisé.

Que ce soit le DSI, le service responsable, les agents, les prestataires, les usagers ou les développeurs, tous ont une forme de contrôle sur le SI d’une collectivité.

Avec la montée du cloud et des systèmes *-as-a-service, il est particulièrement difficile de contrôler son SI car les collectivités, en tant que clientes, ont peu accès à l’infrastructure et aux logiciels utilisés par leurs prestataires.



Pour illustrer cet aspect, prenons le cas SolarWinds, une entreprise américaine développant des logiciels de supervision comme Orion.

Orion est un logiciel permettant la surveillance de la disponibilité et de l'utilisation d'un réseau.

En septembre 2019, des pirates ont obtenu une accès non autorisé au réseau de SolarWinds. En octobre, ils testaient l'injection d'un code malveillant dans les logiciels de SolarWinds.

4 mois plus tard, ils injectaient un malware, dénommé Sunburst, dans Orion. En mars 2020, SolarWinds distribuait une mise à jour d'Orion incluant le malware à tous ses clients.

Cette mise à jour a été installée plus de 18000 fois ! C'est une attaque particulièrement rentable pour les pirates qui ont eu accès au réseau d'un très grand nombre d'entreprises.

Plus proche de nous, il y a ce cas relaté par Le Télégramme en décembre 2022. Beaucoup de mairies ne jettent pas leur matériel informatique en fin de vie et chargent des associations ou des prestataires de leur donner une seconde vie.

La mairie de Montreuil-le-Gast avait chargé son prestataire d'effacer le contenus de ses disques. Celui-ci ne l'a pas fait et des données personnelles se sont donc retrouvées dans la nature.

Du château-fort à l'aéroport

Les collectivités doivent réussir leur transition du modèle château-fort au modèle aéroport.

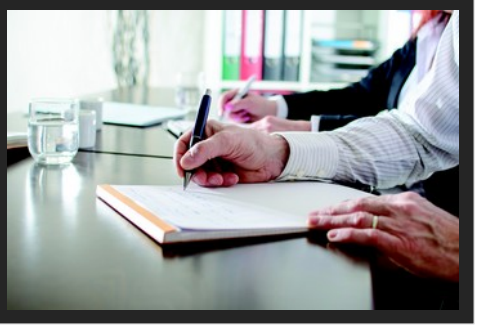
Le modèle château-fort fonctionne sur le principe d'une protection forte à l'entrée du système, mais faible une fois le système pénétré.

Le modèle aéroport impose quant à lui des contrôles de plus en plus poussés à mesure qu'on accède à des zones ou données sensibles.

Non seulement cette transition doit être réalisée par la DSI, elle doit en plus être accompagnée d'une conduite de changement quant aux habitudes des agents.

Former les agents (mais pas que)

- Agents
  Accès à des données sensibles, structure, organisation, droits…
- Usagers
  Équipements en dehors du périmètre de la DSI
- Élus
  Prise en compte des coûts, investissements…
- Piqûres de rappel indispensables !



Agents qui doivent être formés et sensibilisés régulièrement, étant donnée l'obsolescence des connaissances et les difficultés de l'être humain à garder un niveau d'attention élevé sur le long terme.

Les usagers doivent être sensibilisés car ils peuvent être vecteurs d'attaques à leur insu. La sécurité de leurs données dépend aussi d'eux.

Les élus doivent être sensibilisés car la sécurité a un coût non négligeable et une prise de conscience est nécessaire pour investir sur des postes qui n'ont pas de retour direct sur leurs actions politiques. Et puis « Pas besoin d'augmenter les budgets, tout va bien, on ne s'est jamais fait pirater ».

L'histoire sans fin

Il s'agit malheureusement d'une histoire sans fin.

Les plus vieux ont peut-être connu ça : dans les années 80, sur les ordinateurs familiaux Amstrad CPC, la copie des jeux sur disquettes était monnaie courante (internet n'existait pas encore et les réseaux de l'époque étaient lents).

Les éditeurs de jeux développaient des protections pour éviter qu'on puisse copier les jeux.

Il existait des logiciels dédiés à ce genre de cas comme Discology. Chaque fois que de nouvelles protections apparaissaient, une nouvelle version de Discology sortait qui permettait de quand même réaliser la copie.

Cyberattaque dans une collectivité

Concentrons-nous maintenant sur les cyberattaques dans les collectivités.

Comment se passent-elles ?

Tiens ? Ça ne marche pas !

- Dysfonctionnements étranges
- Connexion impossible
- Billetterie arrêtée
- Assistance prise d’assaut
- Sites web indisponibles
- Impossibilité de réaliser des démarches
- Panne ou attaque ?

Ça commence généralement par un « Tiens ? Ça ne marche pas ! »

Ça peut être des dysfonctionnements étranges : lenteurs inhabituelles, erreurs lors d’ouverture de fichiers…

Une connexion impossible à un logiciel métier, une billetterie arrêtée, une assistance prise d’assaut, des sites web indisponibles, l’impossibilité de réaliser des démarches.

La première question qui se pose : est-ce une panne ou une attaque ? La panne ayant une plus grande probabilité que l’attaque.

Réflexe de la DSI

- Arrêt des applications
- Coupure du réseau
  - Exfiltration de données
  - Double extorsion
  - Attaques supplémentaires
- Affichage agents
- Cellules de crise
- Contact Anssi, Cnil...
- Prestataires spécialisés
  - Recommandés par l'Anssi

Toute DSI suspectant une attaque va chercher à l'arrêter. Cela se traduit par l'arrêt des applications.

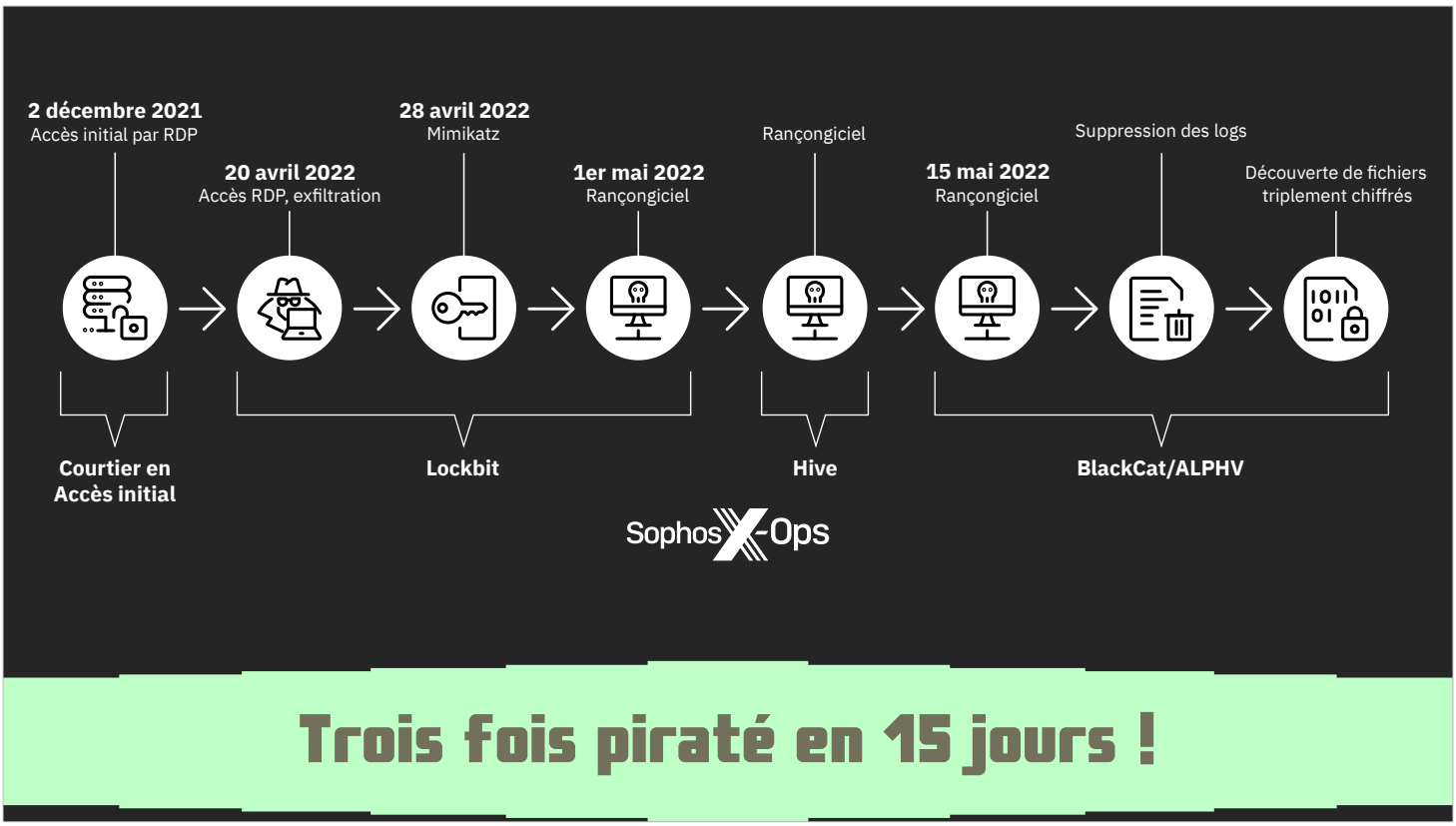
La coupure du réseau est un grand classique. Cela permet de limiter ou d'éviter l'exfiltration de données, des attaques supplémentaires ou que l'attaque se poursuive au cas où l'attaquant aurait besoin de la piloter manuellement comme se fut le cas pour le CHU de Rouen en 2019.

L'État est rapidement contacté par le biais de l'Anssi et de la Cnil.

Des cellules de crise se montent pour coordonner la réponse.

Les agents sont informés par un affichage papier, ou quelques coups de téléphone, leur intimant l'ordre de ne pas utiliser leurs ordinateurs et de les laisser éteints.

Pour sortir de la crise, les collectivités recourent à des prestataires spécialisés et rompus à l'exercice, recommandés par l'Anssi.



Une réponse rapide est impérative si on veut éviter la surenchère.

La société Sophos a relaté le cas d'un équipementier automobile anglais qui a été piraté trois fois de suite en 15 jours !

Un premier accès non autorisé avait été effectué en décembre 2021 par un courtier en accès initial, des pirates spécialisés qui revendent des accès à des SI au marché noir.

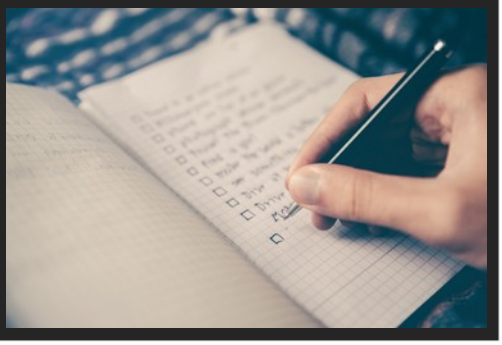
En avril 2022, le groupe Lockbit profite de cet accès pour installer son rançongiciel, immédiatement suivi par le groupe Hive, imités moins de 15 jours plus tard par le groupe BlackCat/ALPHV.

Les fichiers de l'entreprise ont été chiffrés 3 fois.

Cela a été rendu possible par la réaction de l'équipementier qui n'a pas jugé opportun de fermer tout son réseau.

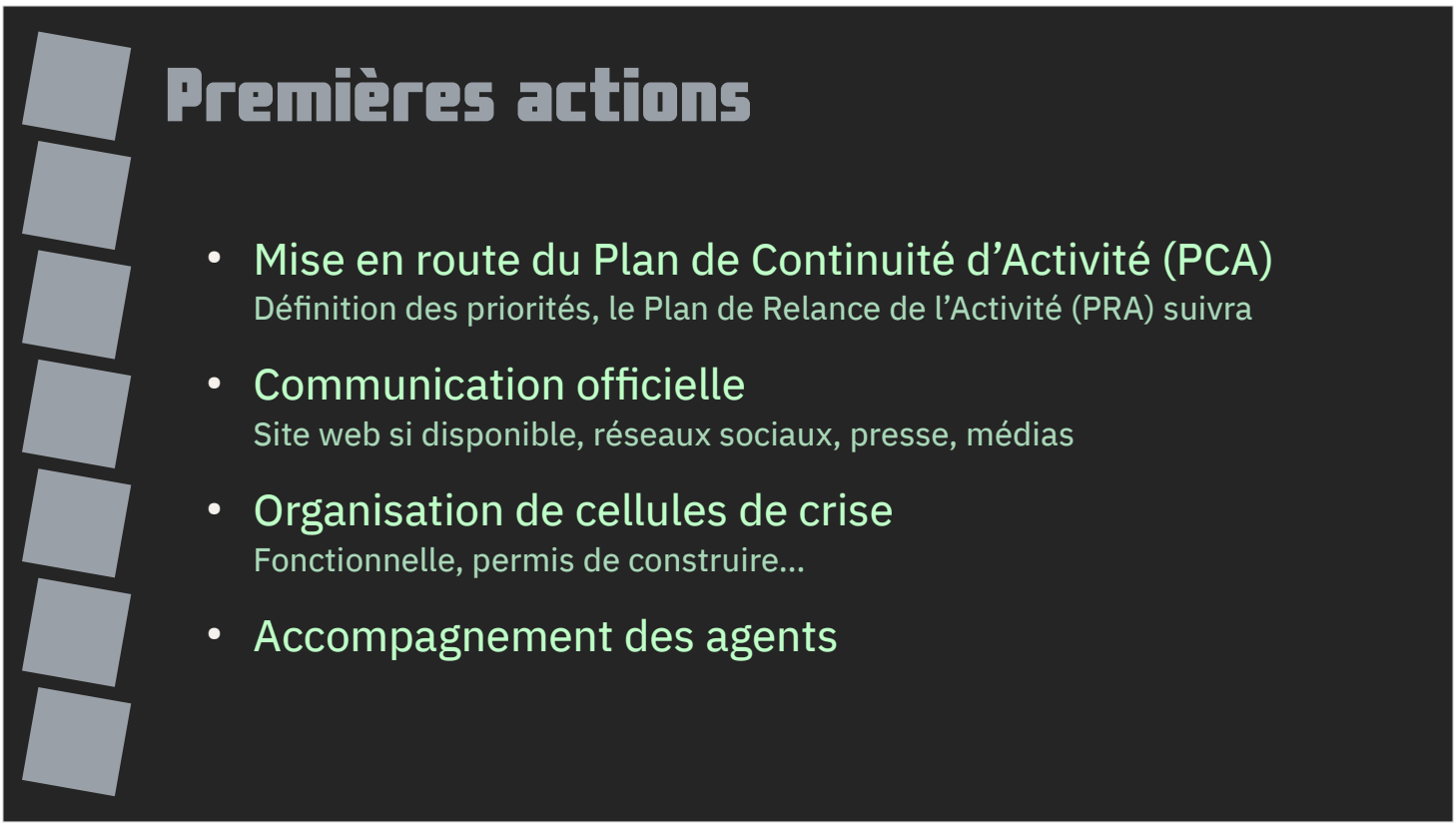
Que se passe-t-il ?

- Évaluer
  - Type d'attaque
  - Éléments impactés
  - Force de l'attaque
  - Actions à entreprendre
  - Possibilité de remise en ligne
- Informer les cellules de crise



La stupeur passée, les équipes de la DSI et des prestataires vont évaluer ce qu'il s'est passé : quel est le type d'attaque, les éléments impactés, l'ampleur, les actions à entreprendre, l'éventualité d'une remise en ligne etc.

Ce travail alimentera les cellules de crise pour qu'elles décident des suites à donner et de l'organisation des agents dans les jours et semaines qui vont suivre.



Parmi les premières actions, on peut recenser la mise en route du plan de continuité d'activité ou PCA, s'il existe, qui définit les priorités et ouvre la voie pour le plan de relance de l'activité ou PRA.

Une communication officielle est établie, en fonction de la disponibilité du site web, sur les réseaux sociaux, avec des communiqués voire des conférences de presse.

Les agents doivent aussi être accompagnés.

Déréférencement de caen.fr

- Des sites trompeurs…
  - « accompagnent »
  - Demandent ~30 €
- … mais légaux !
  - N'endossent aucune image
  - Font réellement la démarche
  - Un avertissement discret

L'indisponibilité du site web de la collectivité peut avoir des conséquences sur son référencement et pour les usagers qui chercheraient à effectuer des démarches.

Dans le cas de la ville de Caen, le déréférencement du site a fait remonter dans les résultats de recherches des sites trompeurs qui se proposent d'accompagner les usagers, moyennant finance.

Les collectivités ne peuvent malheureusement rien faire d'autre que prévenir la population par d'autres canaux car ces sites, tout trompeurs qu'ils soient, restent légaux : ils ne se font pas passer pour les collectivités, font réellement la démarche et affiche un avertissement (discret).

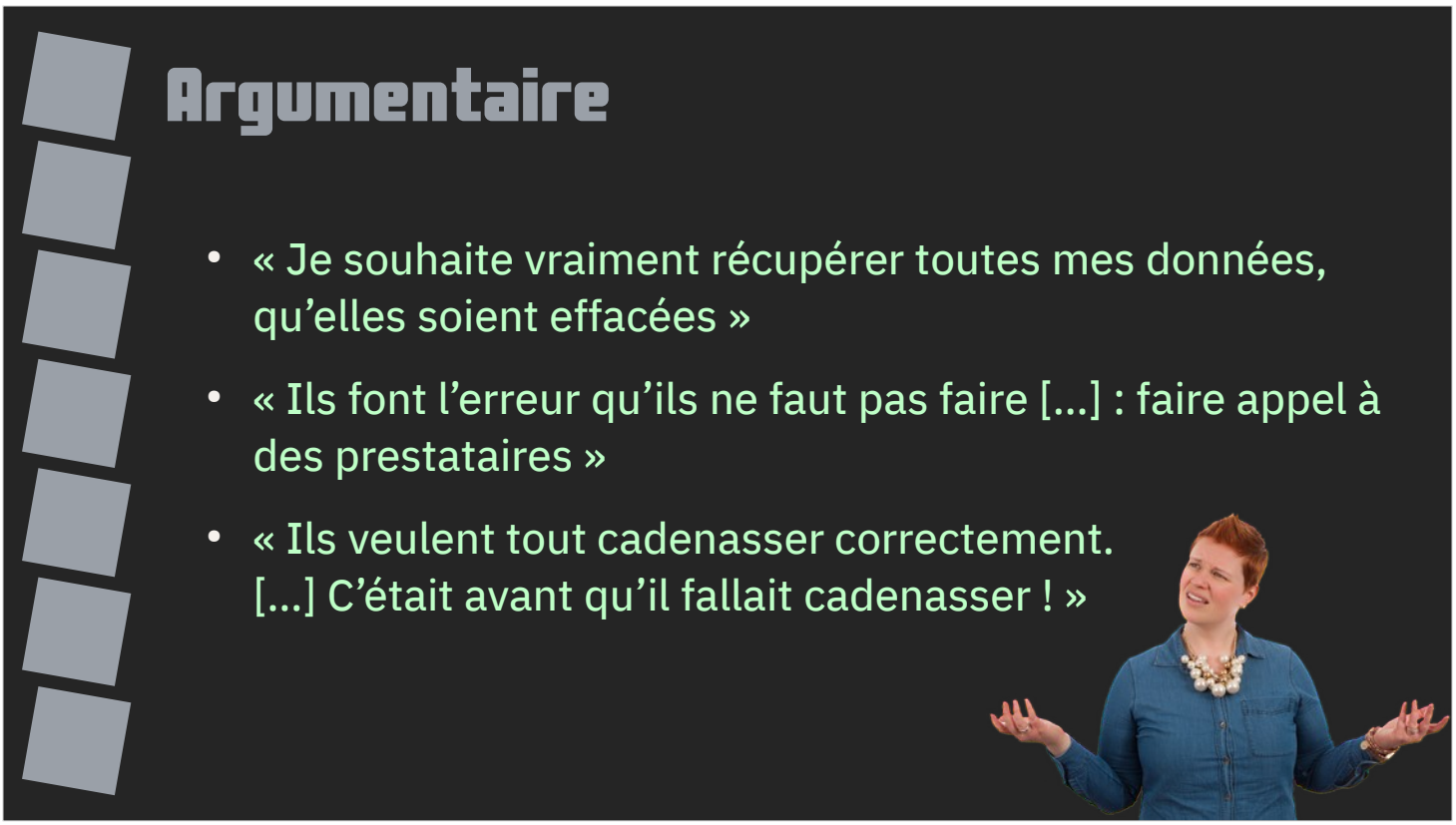
Des personnes peu informées peuvent se faire avoir.

« Cybersécurité : Ville de Caen piratée » Problèmes administratifs (Caen/Normandie)

Ne pas communiquer ou communiquer insuffisamment sur la situation et son évolution peut amener des usagers à imaginer ce qu'il se passe.

Exemple avec le compte Problèmes administratifs.

Le compte a produit une suite à sa première vidéo.



Il souhaite par exemple récupérer toutes ses données, qu'elles soient effacées, ce qui ne pourra jamais arriver et qu'aucune loi ne lui permettra de faire.

Faire appel à des prestataires serait une erreur. Les banques et assurances font elles-mêmes appel à des prestataires. Les prestataires ne sont pas le problème.

C'était avant qu'il fallait cadenasser ? Les budgets informatiques des collectivités sont souvent serrés. Difficile d'avoir un niveau de sécurité rendant impossible toute attaque dans ces conditions. De plus, l'informatique n'est pas la seule faille d'un SI et les failles zero-day, donc encore inconnue peuvent difficilement être anticipées, au mieux leur périmètre d'action peut être limité.

Retour au papier

- Ce qui est écrit devra être remis sur informatique !
- Obligation sur certaines démarches
  État civil, permis de construire…
- Gestion des usagers mécontents
- Préparation physique
- Réunions de couloir

Pour les agents, une cyberattaque se traduit par un retour au papier, sachant que tout ce qui aura été écrit devra être rebasculé dans les applications métiers quand elles seront à nouveau accessibles.

Impossible aussi d'arrêter l'activité en attendant le retour à la normale car certaines démarches comme l'état civil ou les permis de construire ne peuvent être retardées.

Il faut gérer les usagers mécontents. Ou se préparer physiquement car l'habitude de manipuler des registres d'état civil, par exemple, s'est perdue.

Les plus anciennes des assistantes, qui avaient commencé à travailler en mode papier, ont repris des habitudes qu'elles avaient eues.

Leurs collègues plus jeunes, qui n'ont connu que le mail et l'agenda informatique, étaient en panique totale.

CAROLINE FEL 15/06/2021
ADJOINTE ÉDUCATION ET FAMILLE, MAIRIE D'ANGERS

En juin 2021, Caroline Fel, adjointe éducation et famille à la mairie d'Angers racontait que les plus anciennes assistantes, qui avaient commencé à travailler en mode papier, avaient repris des habitudes qu'elles avaient eues tandis que leurs collègues plus jeunes, qui n'avaient connu que le mail et l'agenda informatique étaient en panique totale.

On a vu fleurir des Post-it de plein de couleurs.

Post-it a fait son mois avec la ville d'Angers.

CAROLINE FEL 15/06/2021
ADJOINTE ÉDUCATION ET FAMILLE, MAIRIE D'ANGERS

Elle notait également le retour de l'usage des Post-it.

Le matin, on a mis en place un atelier d'éveil musculaire pour les agents car au bout de trois jours on avait des agents qui avaient mal partout.

CAROLINE FEL 15/06/2021
ADJOINTE ÉDUCATION ET FAMILLE, MAIRIE D'ANGERS

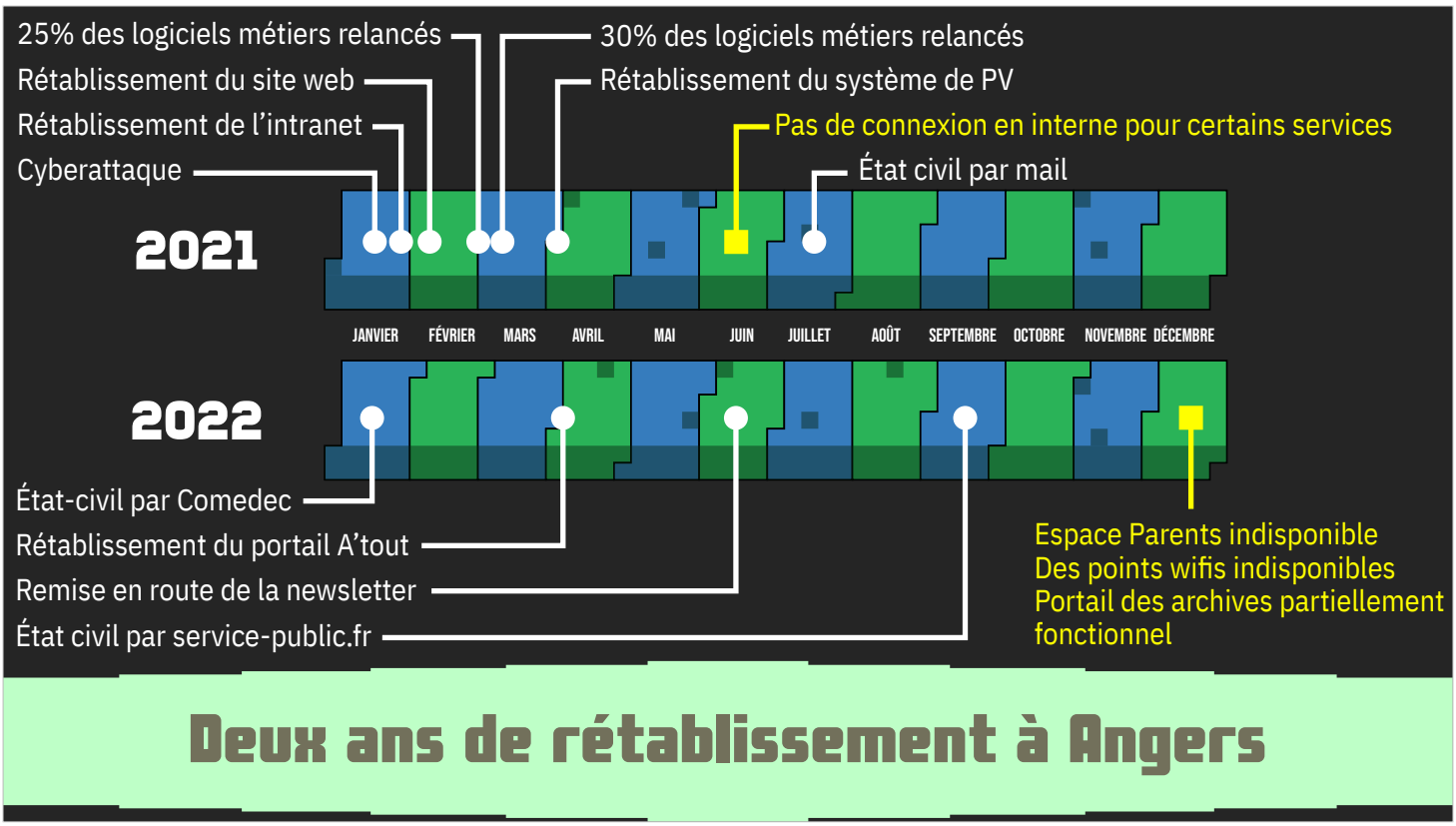
Ainsi que la mise en place d'un atelier d'éveil musculaire le matin pour les agents car au bout de trois jours, des agents avaient mal partout.

Retour à la normale

- 2 jours, 2 mois, 2 ans
  - **2 jours** pour s'organiser, gérer l'urgence
  - **2 mois** pour rétablir les fonctions principales
  - **2 ans** pour revenir à la situation précédant l'attaque

Le retour à la normale s'opère généralement en trois étapes, en fonction de l'ampleur de l'attaque :

- 2 jours sont nécessaires pour s'organiser et gérer l'urgence
- 2 mois pour rétablir les fonctions principales
- Et enfin 2 ans pour revenir à la situation précédant l'attaque.



Cela semble exagéré mais c'est bien ce qu'il s'est passé dans le cas d'Angers. Attaquée en janvier 2021, le site web est revenu un mois plus tard. 2 mois plus tard, seuls 30 % des logiciels métiers avaient été relancés.

En juin, des services n'avaient pas encore de connexion en interne.

En juillet 2021, on pouvaient faire les demandes de copie d'acte d'état civil par mail, à partir de janvier 2022 pour les demandes entre mairies.

Le portail A'tout, le portail des démarches et des paiements, n'est revenue qu'en avril 2022. La newsletter est réapparue en juin.

Ce n'est que depuis septembre 2022, qu'on peut utiliser service-public.fr pour les demandes de copie d'acte d'état civil.

Fin 2022, l'espace Parents, des points wifis ainsi que des parties du portail des archives sont encore indisponibles.

Payer la rançon ?

- Pourquoi pas ?
  « Il fallait qu'on récupère [nos données]. On a dû payer l'équivalent de 10 000 euros. » – Alain Letellier (CdC des Sablons) pour France 3 Hauts-de-France
- Non !
  « Ne payez pas la rançon. Le paiement ne garantit en rien le déchiffrement de vos données » – Anssi
- Les criminels ne lâchent pas un bon client
- Interdit dans le cadre du terrorisme
  Article 421-2-2 du Code pénal

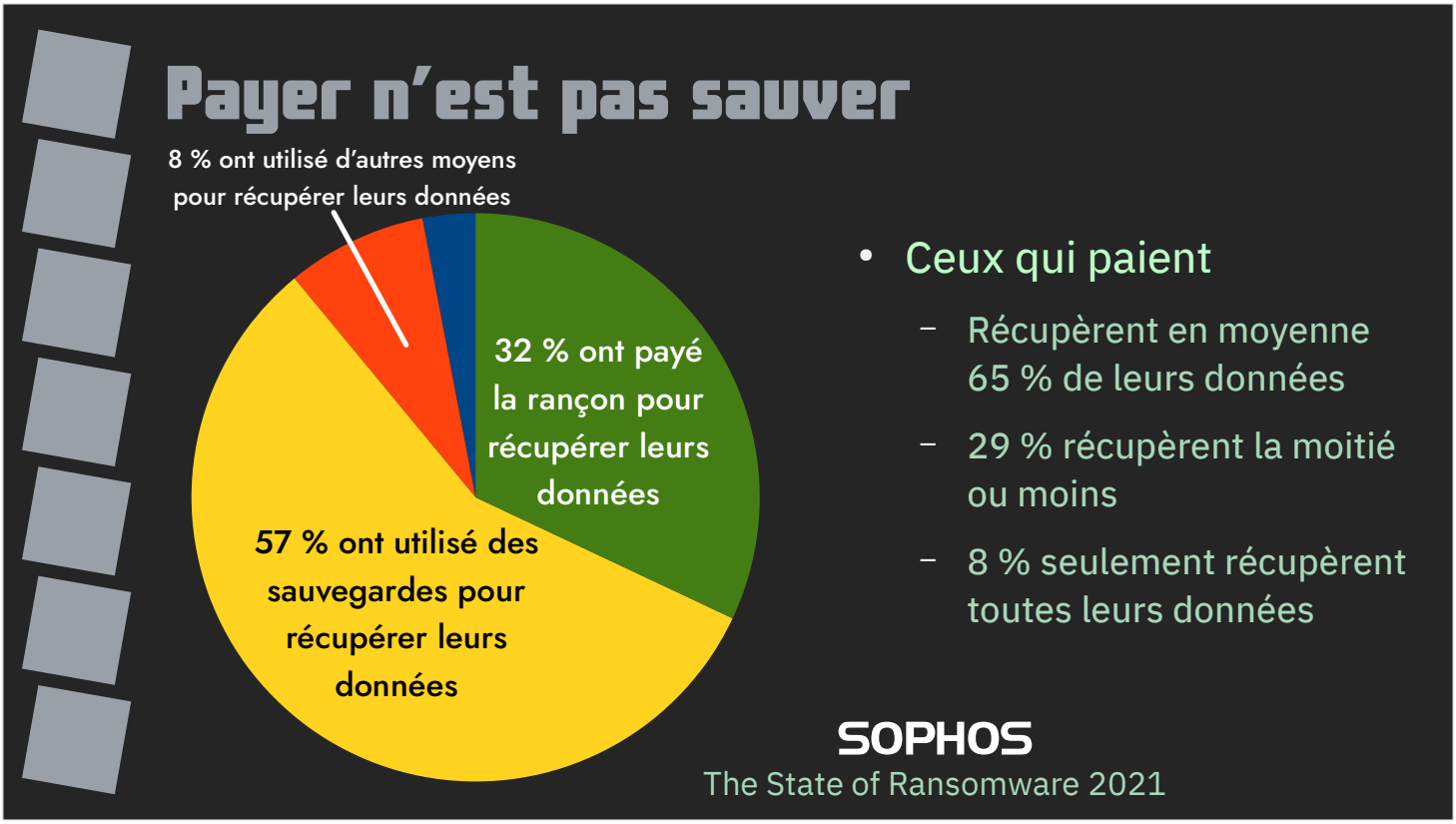
Pour les collectivités attaquées se pose inévitablement la question : doit-on payer la rançon ?

La communauté de communes des Sablons a fait le choix de payer l’équivalent de 10000 € pour récupérer ses données.

L’Anssi insiste fortement sur le fait de ne pas payer la rançon d’autant que le paiement ne garantit en rien le déchiffrement des données.

Il faut ajouter à cette position que les pirates aiment les bons payeurs.

On pourrait penser que les collectivités n’ont pas le droit de payer de rançon, il n’en est rien. C’est uniquement interdit dans le cadre du terrorisme (article 421-2-2 du Code pénal). La seule difficulté à éliminer reste alors le paiement, les collectivités n’ayant pas de carte bleue pour acheter de la cryptomonnaie.



De plus, payer n'est pas sauver.

Selon Sophos, si 32 % des organisations victimes de cyberattaques ont payé la rançon pour récupérer leurs données, seules 8 % récupèrent leurs données dans leur intégralité. Elles récupèrent en moyenne seulement 65 % de leurs données.

Il est préférable de s'en remettre à ses sauvegardes pour effectuer son retour à la normale.

Les sauvegardes, l'arme ultime ?

- **Indispensables** pour limiter les pertes
- Faiblesses
  - Elles sont aussi la cible des pirates
  - Sensibles aux défaillances matérielles
  - Obsolescence
  - Elles devraient être testées...
- Elles ne corrigent pas les failles du SI

Mais si les sauvegardes sont indispensables pour limiter les pertes, elles présentent de grosses faiblesses qu'il est important d'éliminer.

Elles sont aussi la cible des pirates. Selon leur fréquence, les données qu'elles contiennent peuvent être obsolètes. Elles sont sensibles aux défaillances matérielles comme un support mal enregistré. Surtout, elles devraient être régulièrement testées. Beaucoup de structures ne vérifient pas leurs sauvegardes.

Enfin, elles ne sont pas une protection. Elles ne corrigent pas les failles du SI.

Tout reconstruire

- Nettoyer
  - Ordinateurs fixes
  - Ordinateurs portables
  - Smartphones
  - Serveurs/applications
- Colmater les failles
- Augmenter la sécurité
- Répercuter les données à terme
- Tout en continuant d'assurer les missions !

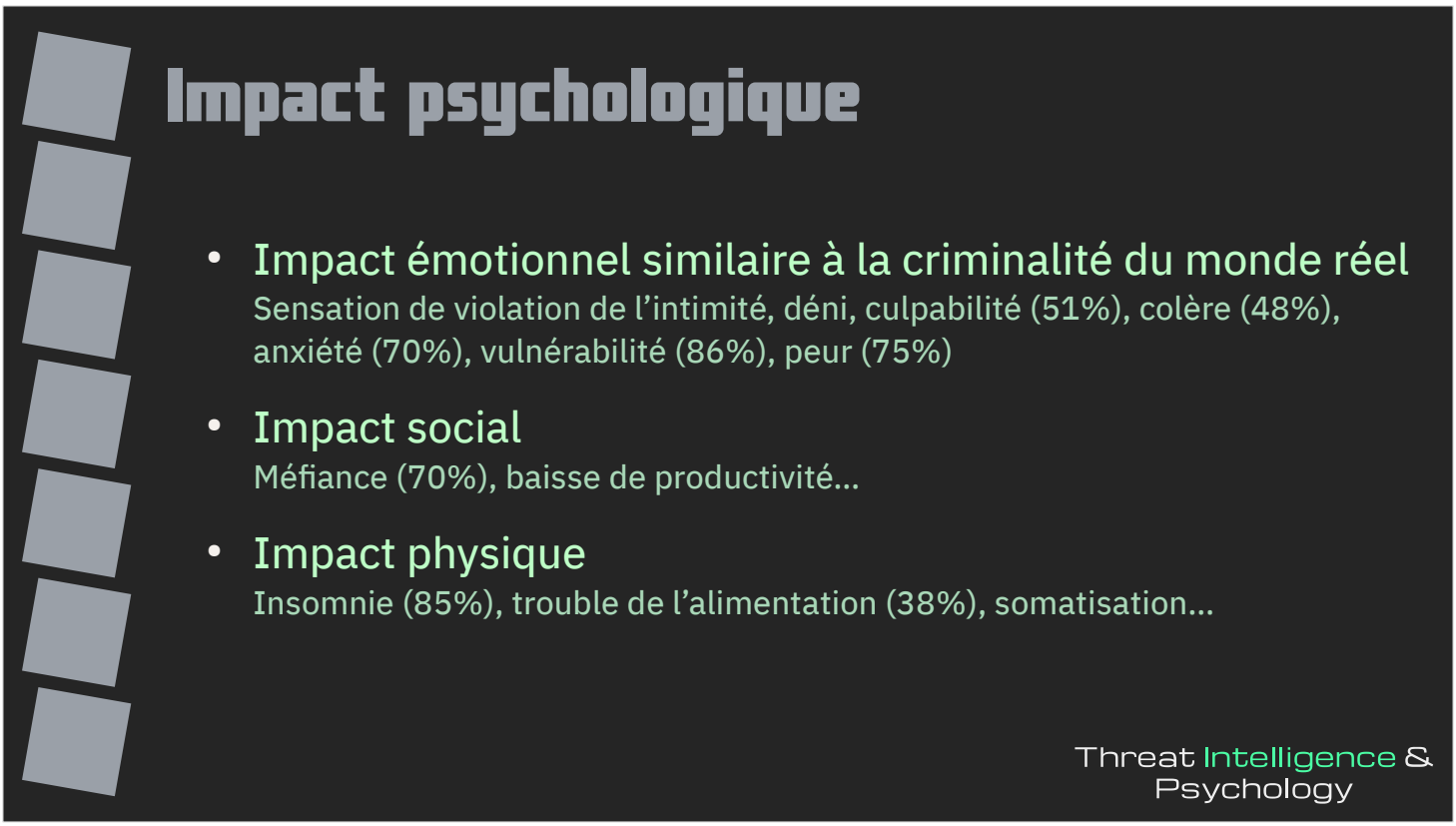
La crise passée, il est temps de tout reconstruire.

Dans les premières semaines, les équipes de la DSI ont du pain sur la planche car ils doivent s'assurer que les pirates n'auront pas la possibilité de revenir. Les ordinateurs fixes, portables, les smartphones ainsi que les serveurs et les applications doivent tous être nettoyés.

Rien qu'en postes de travail, cela représente plusieurs milliers de machines pour des villes comme Angers.

Les DSI en profitent pour débloquer des budgets en urgence afin d'augmenter le niveau de sécurité du SI.

Les agents devront aussi répercuter toutes les données papier sur informatique.

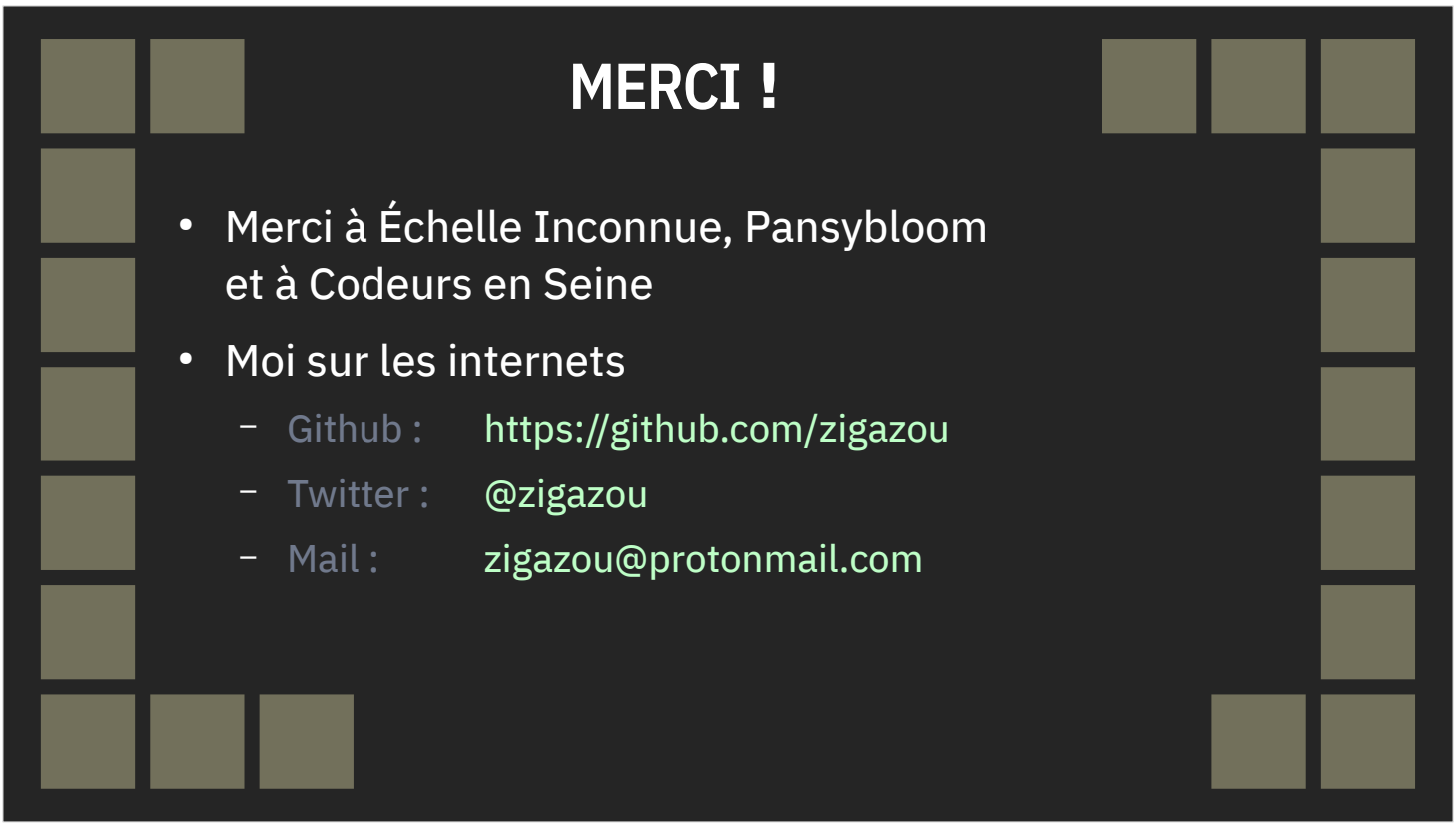


L'impact psychologique, quant à lui, est trop souvent négligé.

Des études ont montré que l'impact émotionnel d'une cyberattaque était similaire à la criminalité dans le monde réel comme le vol de son logement.

Cela peut même avoir des conséquences sociales et physiques.

Il s'agit d'un aspect que les RH des organisations devraient prendre en compte.



Merci de votre attention !

Merci à Échelle Inconnue, Pansybloom et à Codeurs en Seine.

Vous pouvez me retrouver sur les internets sur Github, Twitter ou par mail.