À qui le tour ?
Toutes et tous piraté-e-s

- Un PDF avec
  - Les diapos
  - Les notes

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.

Damien Bancal / Zataz

Cyber anywhere

Préfixe à la mode à partir de la deuxième moitié du XX^{e} siècle.

Usage consécutif au développement de l'informatique, de la robotique et à l'avènement du réseau internet.

CYBER

HTTPS://FR.WIKIPEDIA.ORG/WIKI/CYBER

cyberattaque
cyberespionnage
cyberespace
cybermalfaiteur
cybercriminel
cyberassurance
cybergendarme
cyberterroriste

cybersurveillance
cyberdéfense
cyberguerre
cybermalveillance
cybersécurité
cyberrésilience
cybermenace
cyberharcèlement

Florilège de cyber

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

CYBERATTAQUE
DÉFINITION DE WIKTIONARY

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

DÉFINITION D'UNE CYBERATTAQUE
WWW.GOUVERNEMENT.FR/RISQUES/RISQUES-CYBER

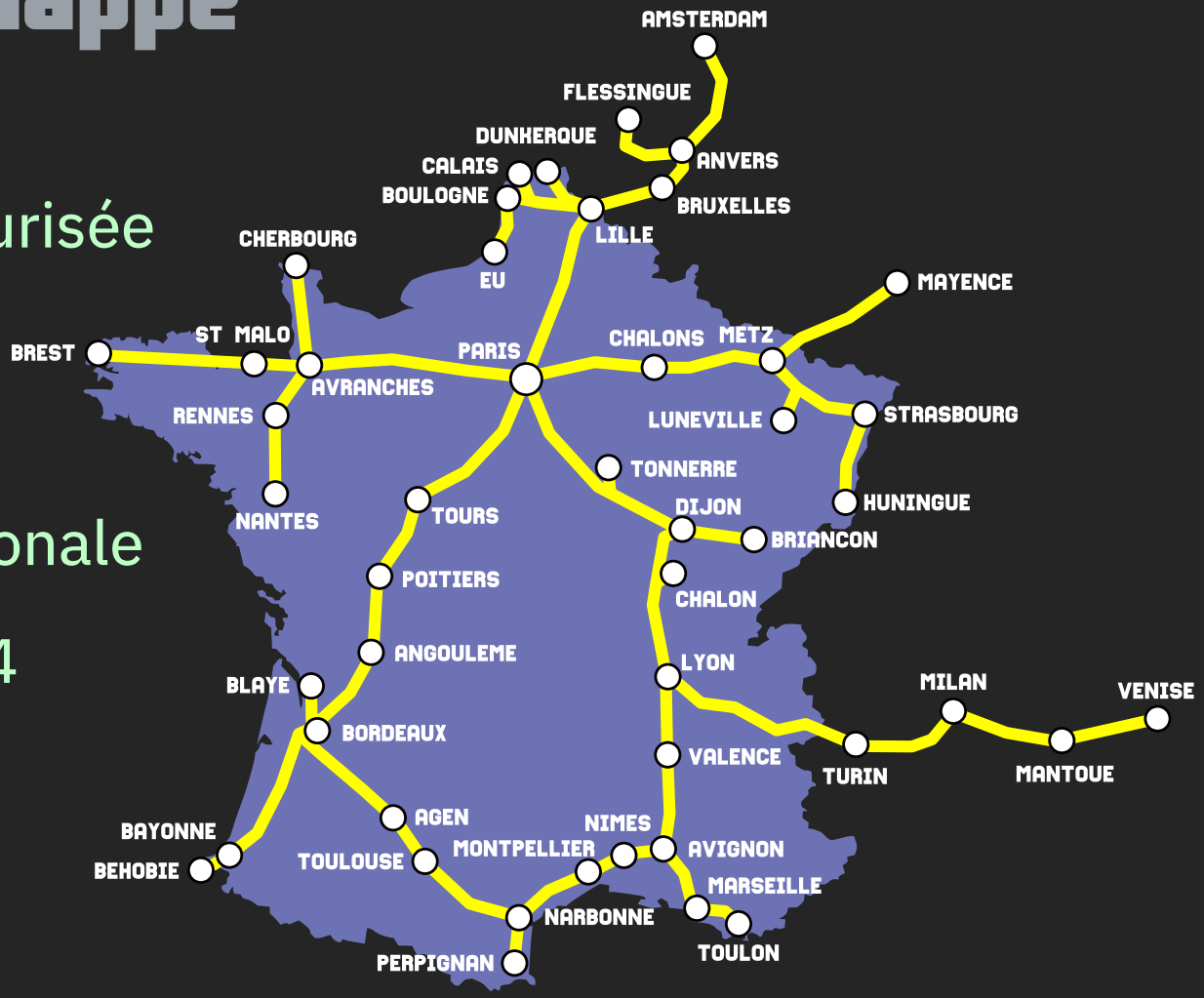
La première cyberattaque de l'histoire ?

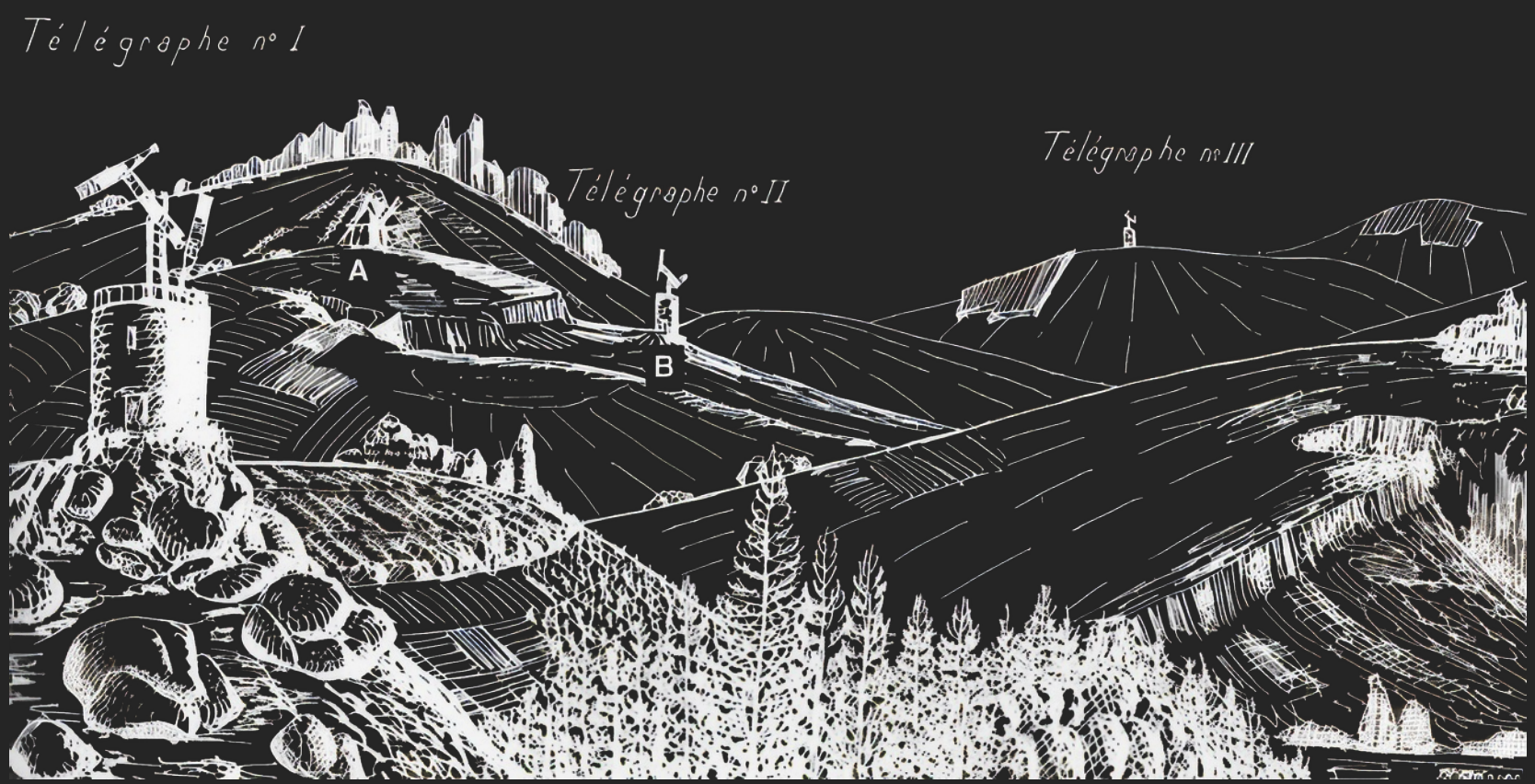
Un négociant qui, pour se procurer des nouvelles de Bourse, afin de jouer sur les fonds publics, obtient à prix d'argent certains signaux d'un employé de l'administration des télégraphes, se rend-il coupable du crime de corruption ?

LA GAZETTE DES TRIBUNAUX
10 DÉCEMBRE 1836

Télégraphe Chappe

- Transmission sécurisée
- Réservé à l'État
- Financé en partie par la Loterie nationale
- 534 tours en 1844

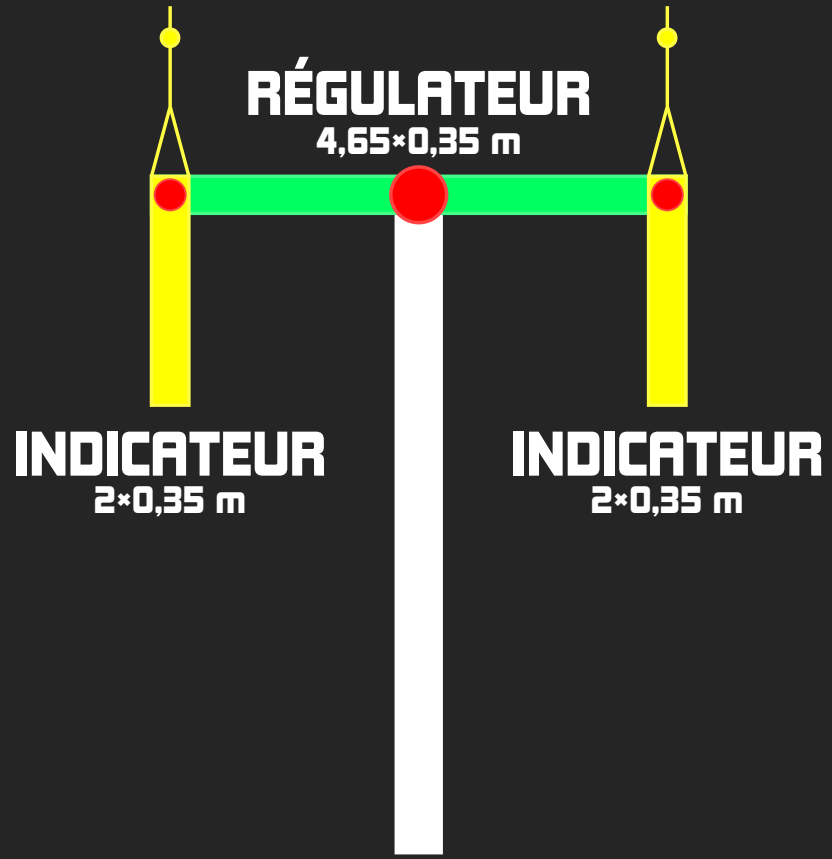


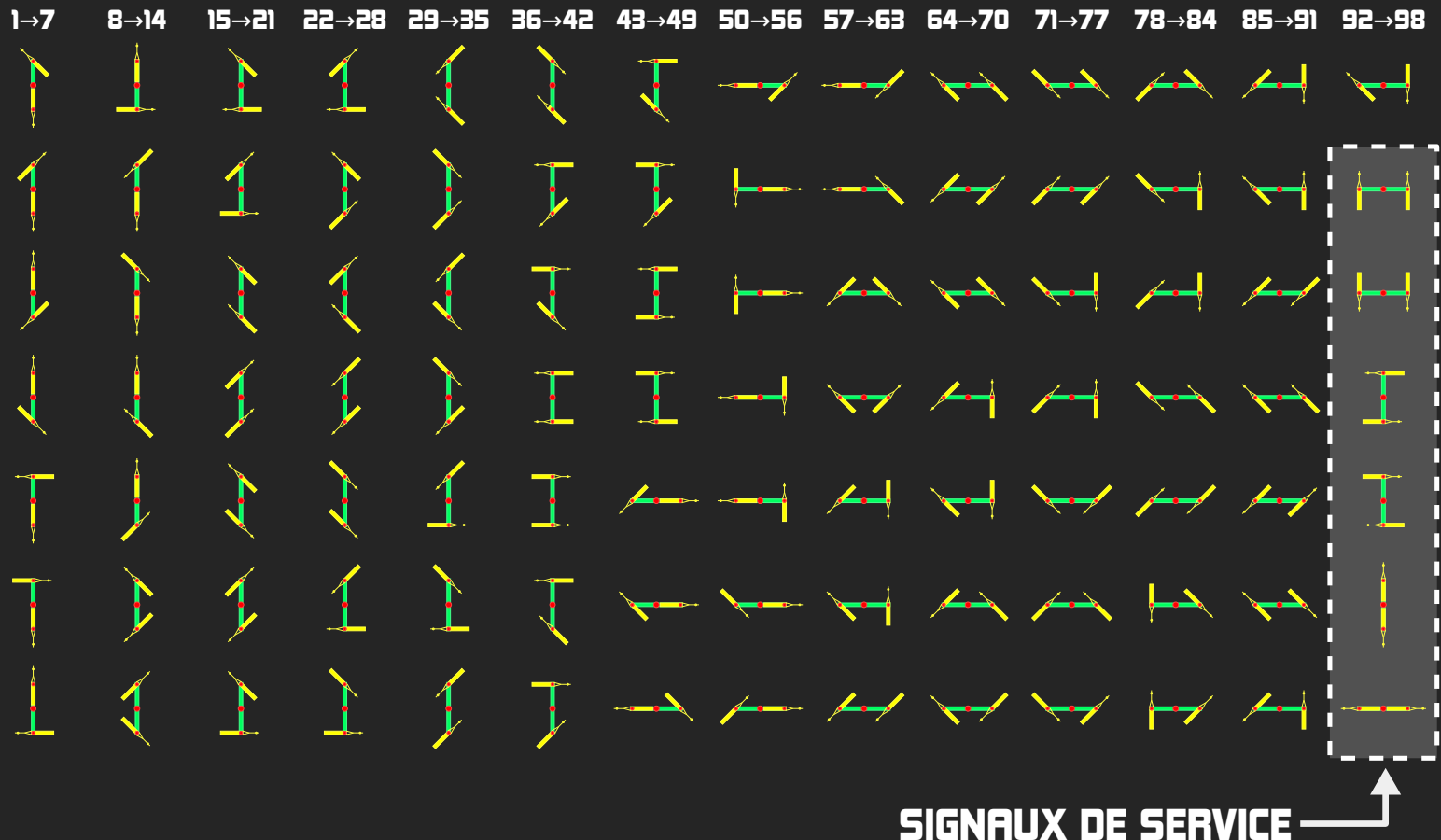


Des tours espacées de 25 km environ

Des sémaphores

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

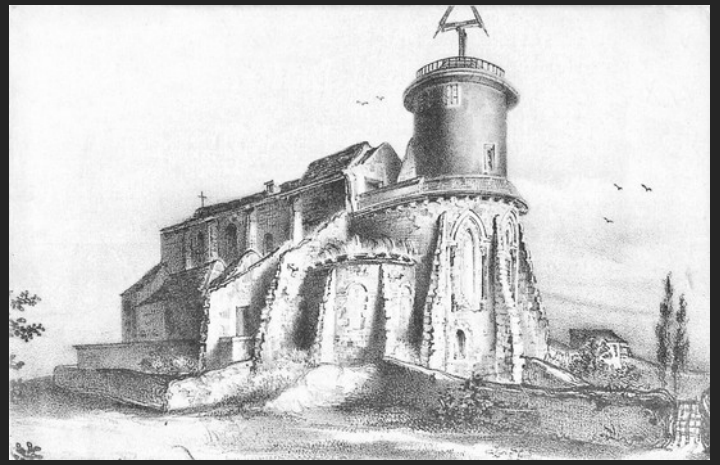




Toutes les positions possibles

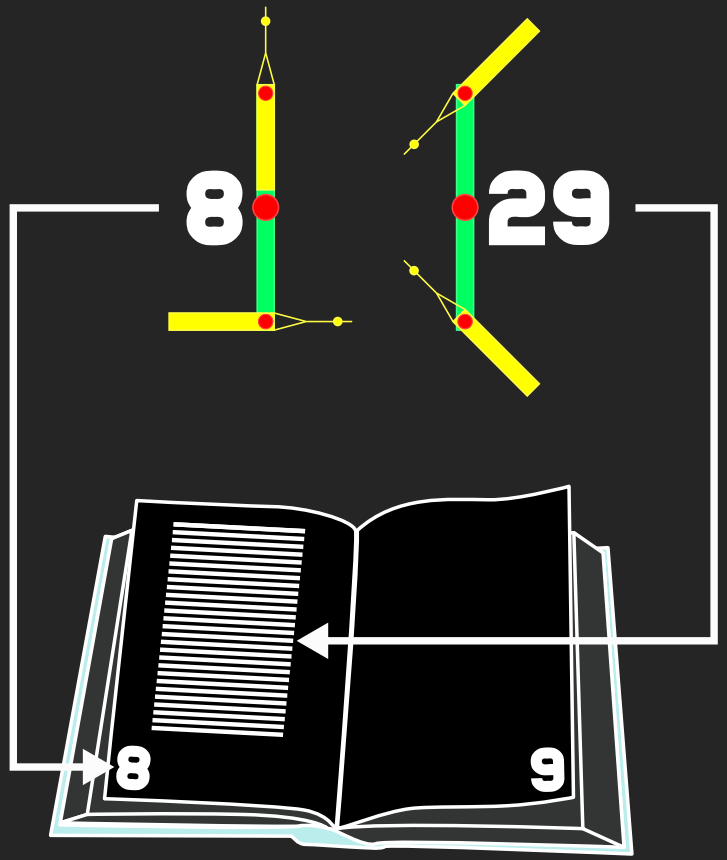
Trois catégories de personnel

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



Un système sécurisé

- Les stationnaires ignorent ce qu'ils transmettent
- Beaucoup ne savent ni lire ni écrire
- Un livre est nécessaire pour décoder le message



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 ! 

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 !

La combine des frères Blanc

- Un complice à Paris
  - S’informe des variations de la bourse
  - Envoie un colis codé par voie postale à Tours
- Un stationnaire complice à Tours
  - Envoie un message « défectueux » suivi d’un signal d’annulation
- Un complice à Bordeaux
  - Surveille et décode les messages « défectueux »

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 !

Les collectivités, cibles de cyberattaques

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

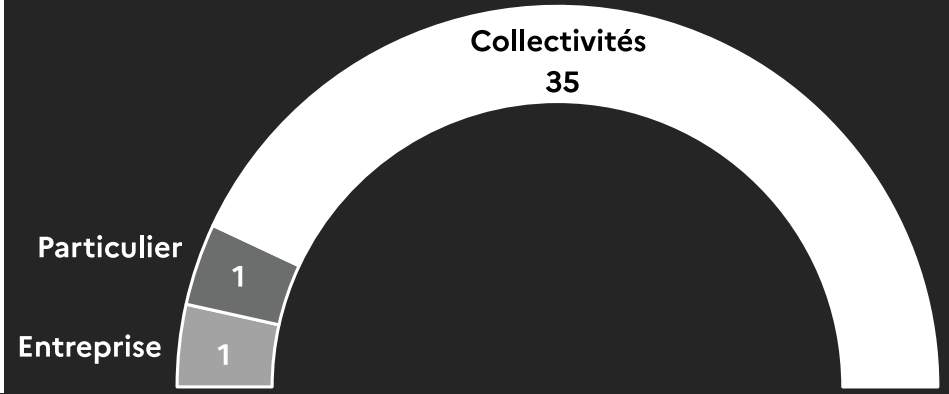
Recrudescence des attaques

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

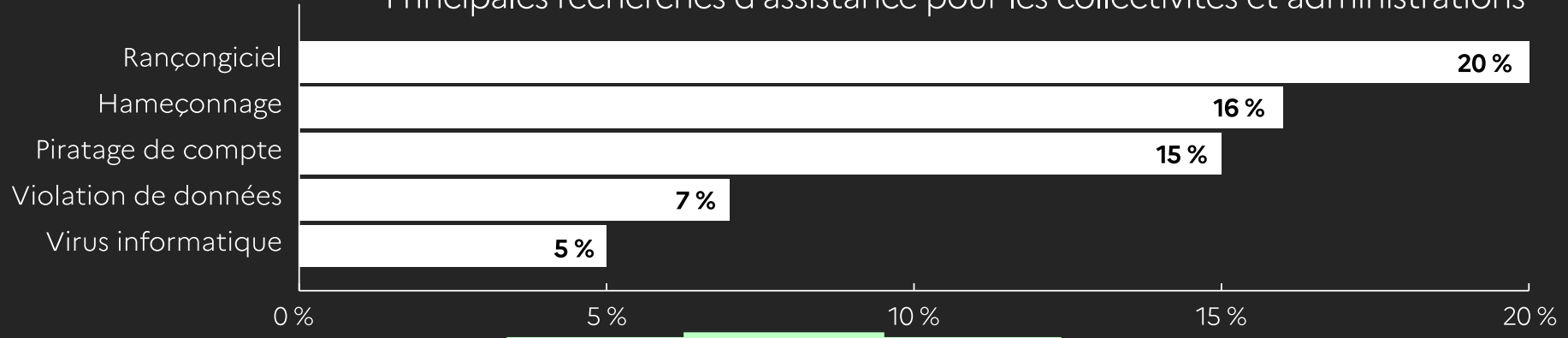
173 000
demandes d'assistance sur la plateforme en 2021

Proportion des publics assistés sur Cybermalveillance.gouv.fr en 2021



1 235
professionnels référencés en 2021

Principales recherches d'assistance pour les collectivités et administrations



Sur la plateforme CyberMalveillance.gouv.fr

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

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

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

Un système d'information

Ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information.

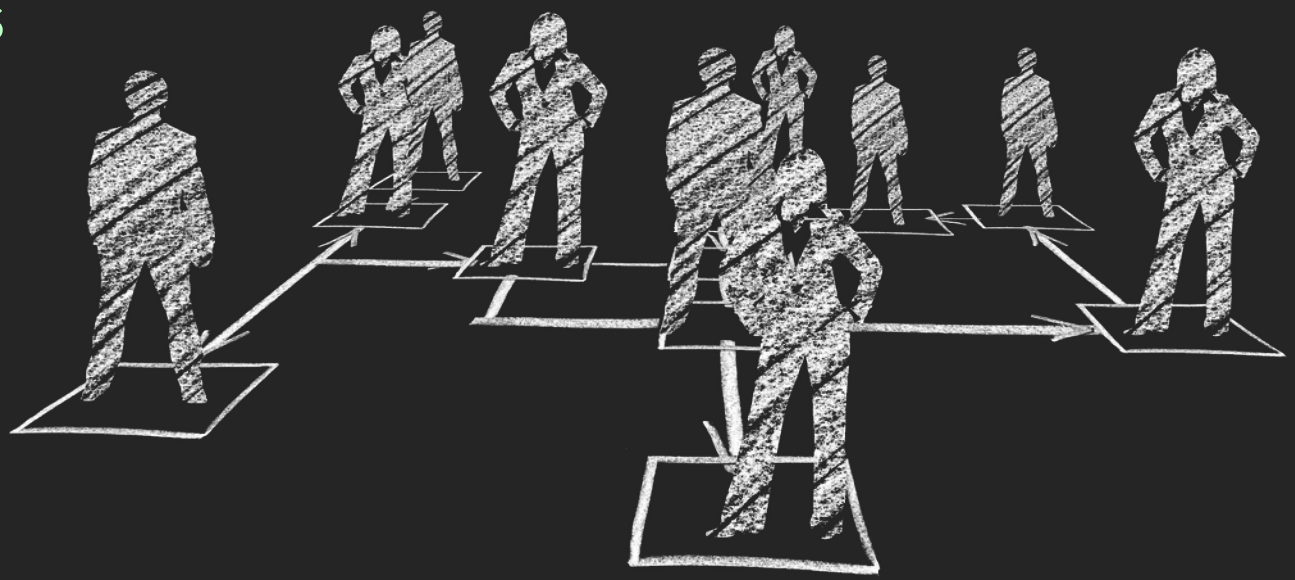
Système socio-technique composé de deux sous-systèmes, l'un social et l'autre technique.

SYSTÈME D’INFORMATION
WIKIPÉDIA

QUE RETROUVE-T-ON DANS UN SI ?

Une organisation

- Une hiérarchie
- Des personnes
- Des procédures



Du matériel

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

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

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.

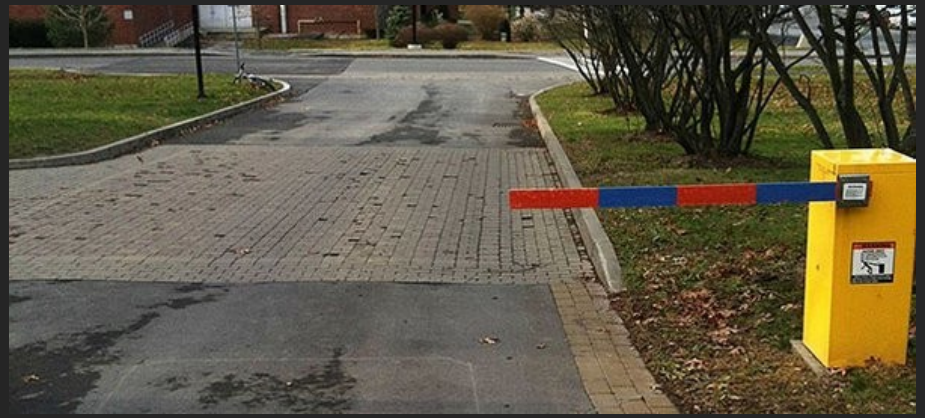
SURFACE D'ATTAQUE

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

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 ?

Bien comprendre son SI



- Pour éviter de faire de la sécurité inutile
- Pour 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

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

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

« 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

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

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

SURFACE D'ATTAQUE DES COLLECTIVITÉS

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…

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

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…

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…

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…

Un grand nombre de compétences 4/4

AÉRODROME

Conventions, aménagement, entretien, exploitation des aérodromes civils d'intérêt local, expérimentation, services infra/ interrégionaux…

TRANSPORTS PUBLICS

Transports publics, covoiturage, autopartage, location de vélos, transport de marchandises, logistique urbaine, PDU, routes express, chemins ruraux…

TRANSPORTS SCOLAIRES

Financement, organisation et fonctionnement des transports scolaires

ÉTAT CIVIL

Naissance, mariage, décès, fermeture de cercueil, cimetières, inhumations, exhumations, crémations, concessions…

PORTS, VOIES D'EAU, LIAISONS

Police des ports maritimes, ports intérieurs, de plaisance, maritimes de commerce et de pêche, desserte des îles côtières…

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

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

Les raisons d'une cyberattaque

Pour l'argent !

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

Cyberattaque à Aix-les-Bains :
le virus fabriquait de la cryptomonnaie

28/03/2022 LE DAUPHINÉ libéré

Les pirates de Lockbit diffusent des milliers
de données volés au Département de l'Ardèche

13/04/2022 ZATAZ

Une communauté de communes [...] Tous les élus ont acheté des bitcoins. [...] ils se sont arrangés avec le trésorier.

29/09/2022 LeMagIT

Avaddon : un butin d'au moins un million de dollars depuis début mai

27/05/2021 LeMagIT

Visé par une cyberattaque, le département de Seine-et-Marne refuse de payer la rançon exigée

17/11/2022 ouest france AFP

Le pirates et l'argent dans la presse

Pour des raisons stratégiques

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

La Corée du Nord a-t-elle hacké Sony à cause d'un film potache ?

17/12/2014 Le Journal du Dimanche

Stuxnet : comment les États-Unis et Israël ont piraté le nucléaire iranien

08/10/2015 L'OBS

Le site du Parlement européen visé par une cyberattaque après un vote sur la Russie

23/11/2022 franceinfo:

L'opérateur nucléaire ukrainien ciblé par une cyberattaque russe "sans précédent"

17/08/2022 L'USINE DIGITALE

Le Vatican victime d'une cyberattaque, orchestrée par Moscou selon l'Ukraine

01/12/2022 ouest france

En toute amitié

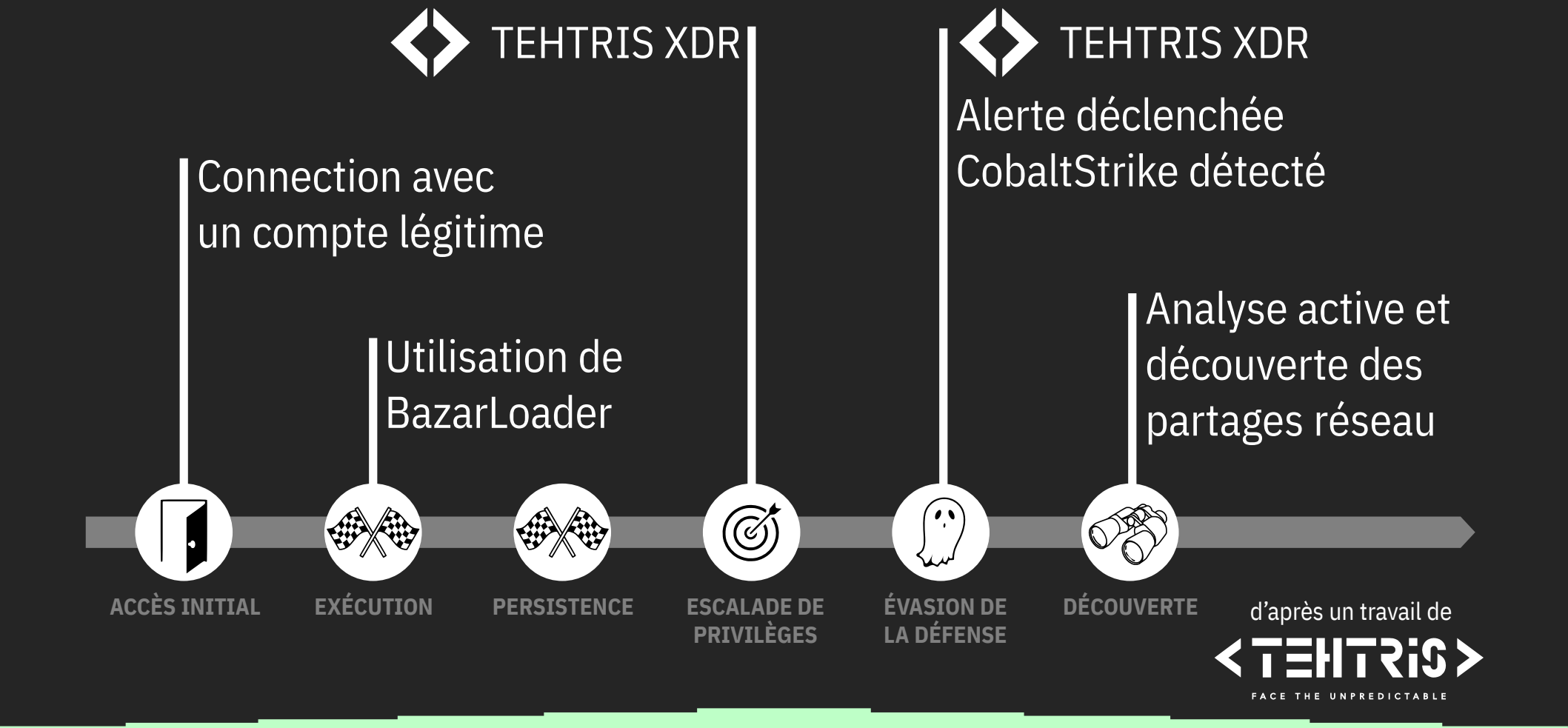
Déroulement d'une cyberattaque

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

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



La Kill Chain de la cyberattaque de la CEA

COMPROMISSION DU SYSTÈME

Reconnaissance

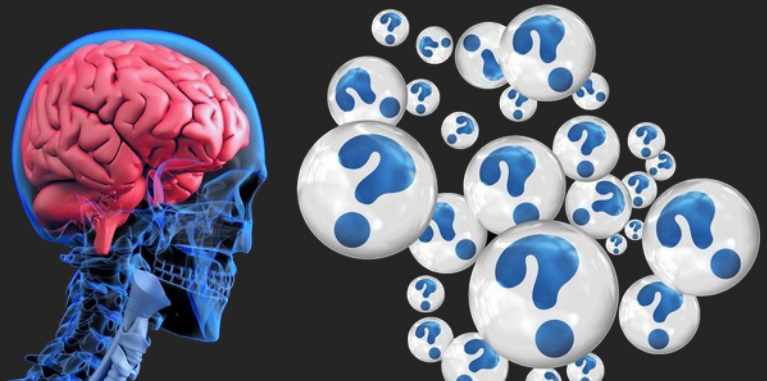
- Recherche, identification et sélection des cibles
  - Informations disponibles publiquement (OSINT)
  - Renseignement sur les systèmes utilisés (versions, failles…)
  - Scan d’adresses IP
  - Recours au marché noir (mails, mots de passe, failles zero-day…)
- Reconnaissance active ou passive

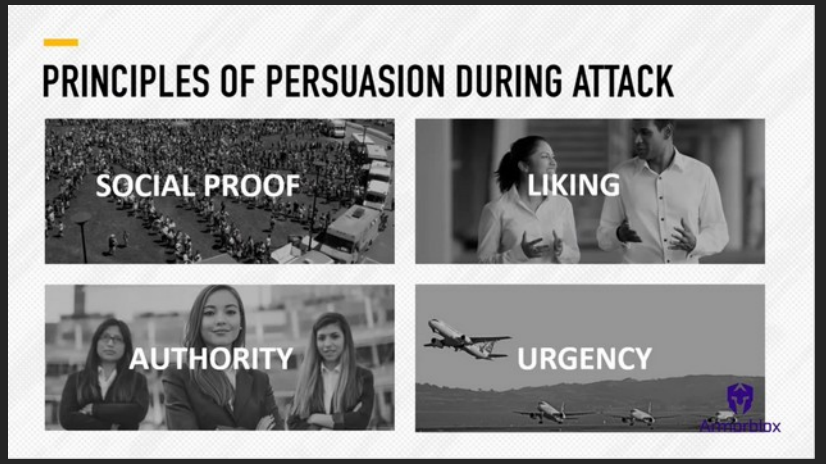
Armement

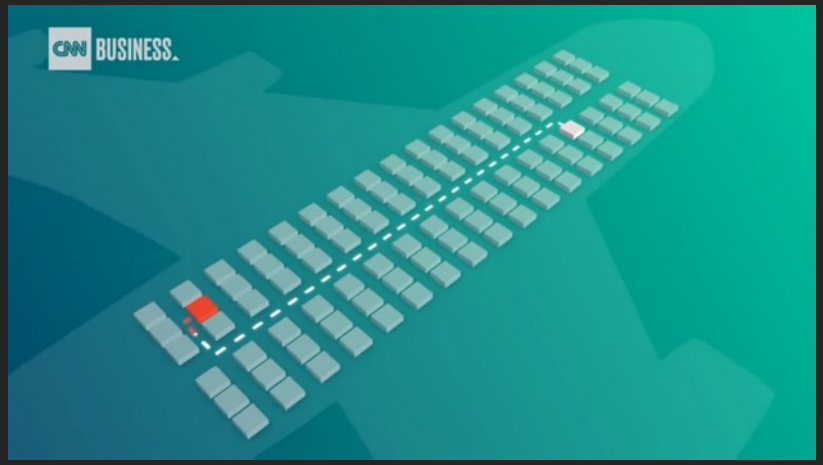
- Mise en place d’une infrastructure nécessaire à l’attaque
  - Achat de noms de domaines similaires à la cible
  - Récupération de malware prêts à l’emploi
  - Développements spécifiques
  - Compromission de serveurs
  - Location de botnet
  - Etc.

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







Rachel Tobac et l'ingénierie sociale

Livraison

- Transmission d'un malware à l’environnement cible
  - Hameçonnage / phishing
  - Harponnage / spear phishing
  - Attaque par point d’eau
- Dropper, des logiciels père Noël

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

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.

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

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…)

Pivotement

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

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

Exécution

- Téléchargement, exécution de modules supplémentaires

Escalade de privilèges

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

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

Mouvement latéral

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

ATTEINTE DES 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

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

Manipulation de la cible

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

Objectifs

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

La cybersécurité

UN AVENIR TERNE

Le sujet RH est ce qui va nous limiter dans les années à venir.

GUILLAUME POUPARD, DIRECTEUR GÉNÉRAL ANSSI
FORUM INTERNATIONAL DE LA CYBERSÉCURITÉ 2022

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

Top 3 des faiblesses soft/hard (2022)

sur 419

1. Écriture hors limites
2. Neutralisation incorrecte de la saisie sur les pages « Cross-site Scripting »
3. Neutralisation incorrecte des éléments spéciaux en SQL « Injection SQL »

sur 100

1. Isolation incorrecte des ressources partagées d'un SoC
2. Interface de test et debug avec contrôle d'accès inapproprié
3. Prévention inadéquate de la modification des bits de verrouillage

CWE™

Leurre

Leurre sur le thème du RGPD

Macro

Une macro intégrée dans le fichier .docx est utilisée pour appeler Powershell.

Powershell

Demande une image hébergée sur le web avec stéganographie et exécute les commandes incorporées

Chocolatey

À partir de ship3.jpg, Powershell installe Chocolatey et appelle ensuite Chocolatey pour installer Python3

Python

À partir de ship3.jpg Powershell appelle Python pour installer et mettre à jour pip3

PIP

À partir de ship3.jpg Powershell appelle Pip3 pour qu'il se mette à jour et installe pysocks pour récupérer des modules

Shell Python

À partir de ship3.jpg Powershell appelle cmd.exe pour exécuter MicrosoftShellUpdate.bat qui appellera Python pour exécuter MicrosoftSecurityUpdate.py

termbin.com

Les sorties affichées à la suite des commandes des attaquants sont répercutées sur un site bin anonyme, chacune avec une URL aléatoire

ship3.jpg

Un jpg de Swiper le Renard contient des données encodées en base64 (plusieurs fois) à la fin.

Powershell

Demande une image hébergée sur le web avec stéganographie et exécute les commandes incorporées

7.jpg

Un jpg d'une campagne de prévention pour la Covid-19 contient des données encodées en base64 (plusieurs fois) à la fin.

Microsoftsecurityupdate.bat

Un fichier batch Microsoft contenant des instructions pour appeler Microsoftsecurityupdate.py avec le chemin vers Python3 est écrit sur le disque.

Microsoftsecurityupdate.py

Un script python contenant la porte dérobée "Serpent" de Proofpoint est écrit sur le disque.

proofpoint.

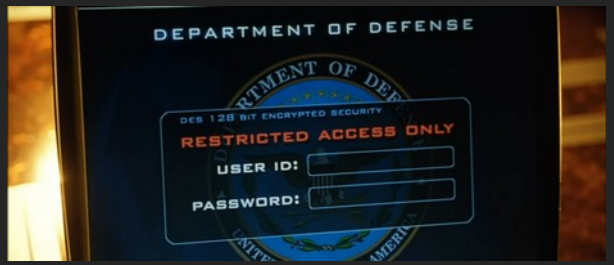
Des attaques de plus en plus complexes

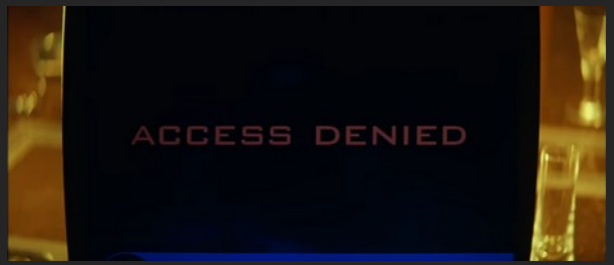
Des cybercriminels toujours plus pro

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

Geek à capuche chez ses parents

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

LA RÉPONSE S'ORGANISE

Quelques acteurs officiels

- Enisa
  European Union Agency for Cybersecurity
- Anssi
  Agence Nationale de la Sécurité des Systèmes d'Information
- Europol
- Csirt national/régional
  Computer Security Incident Response Team
- Cybermalveillance
- Cnil
  Commission Nationale Informatique et Liberté

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

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

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

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

L'arsenal légal

- Code pénal, articles 323-1 à 323-8
  Des atteintes aux systèmes de traitement automatisé de données
- RGPD
  Règlement Général de Protection des Données
- Lopmi 2023-2027
  Loi d'Orientation et de Programmation du Ministère de l'Intérieur, encadrement des clauses de remboursement des cyber-rançons
- Projet de loi sur la cyberrésilience (CRA)
  Sécurité par défaut des produits connectés ≠ médical, voitures, aéronautique

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

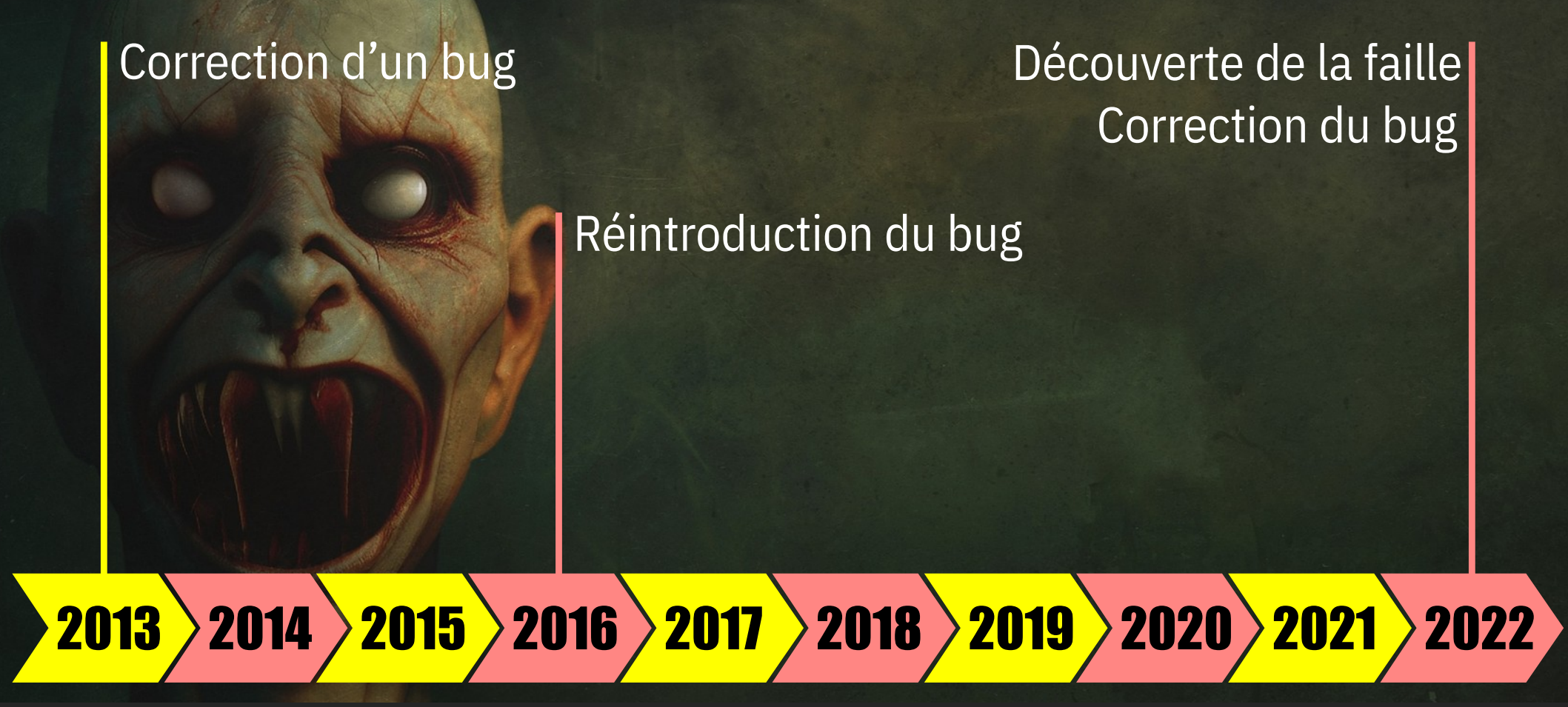
Adobe - Airbnb - Alibaba - Aliexpress - Amazon Web Services - Android – Apache
Apple - Asus - AT&T - Avast! - BASF - Bing - Blogger - Bosch - Cisco – Cloudflare
Cobalt - Deliveroo - Dell - Deutsche Telekom - Docker - Drupal - Dyson – eBay
Electronic Arts - Facebook - Github - Google - HTC - Huawei - 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

MAIS LA TÂCHE EST DANTESQUE

En 2020, 25 % des failles 0-day résultaient de correctifs insuffisamment testés

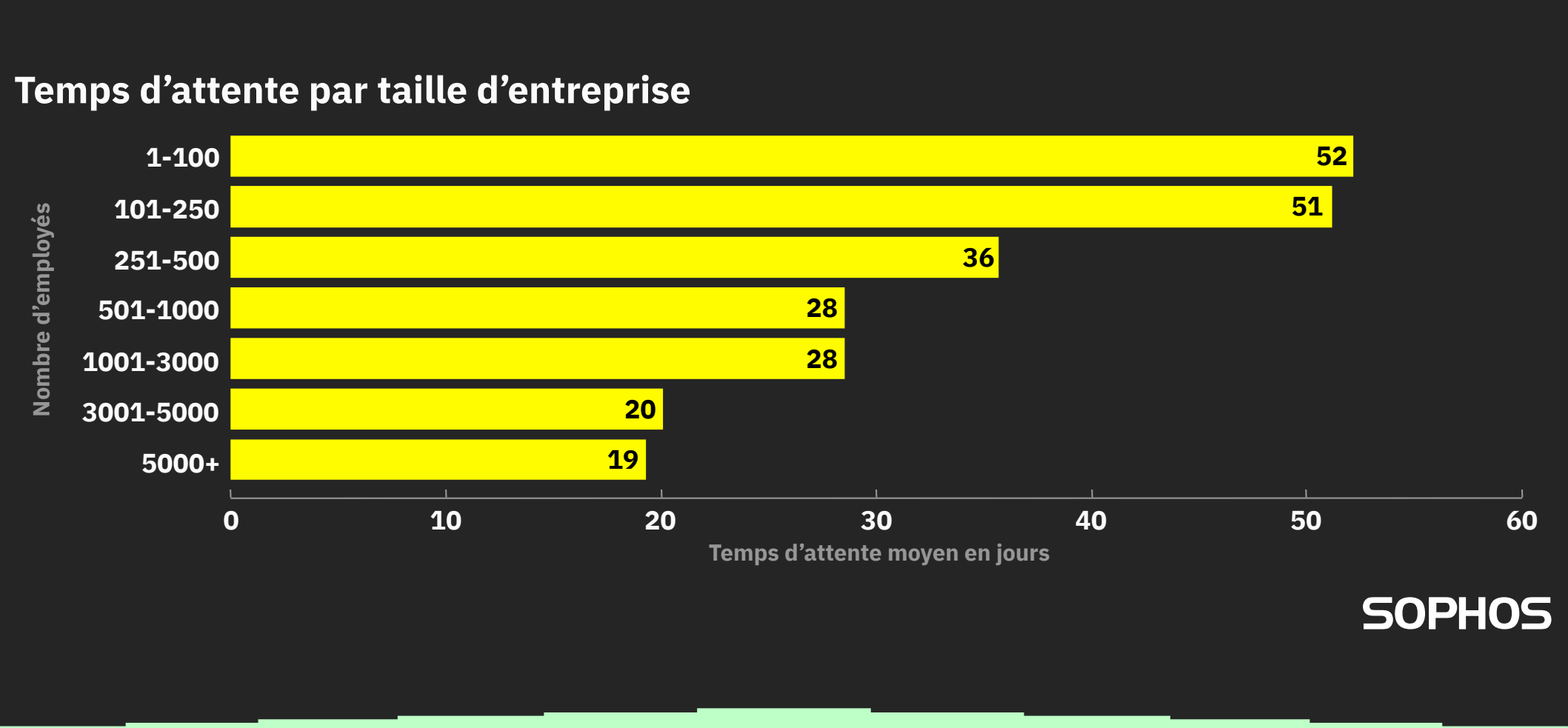
A YEAR IN REVIEW OF 0-DAYS EXPLOITED IN-THE-WILD
GOOGLE PROJECT ZERO - 03/02/2021



Chronologie de la faille CVE-2022-22620

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

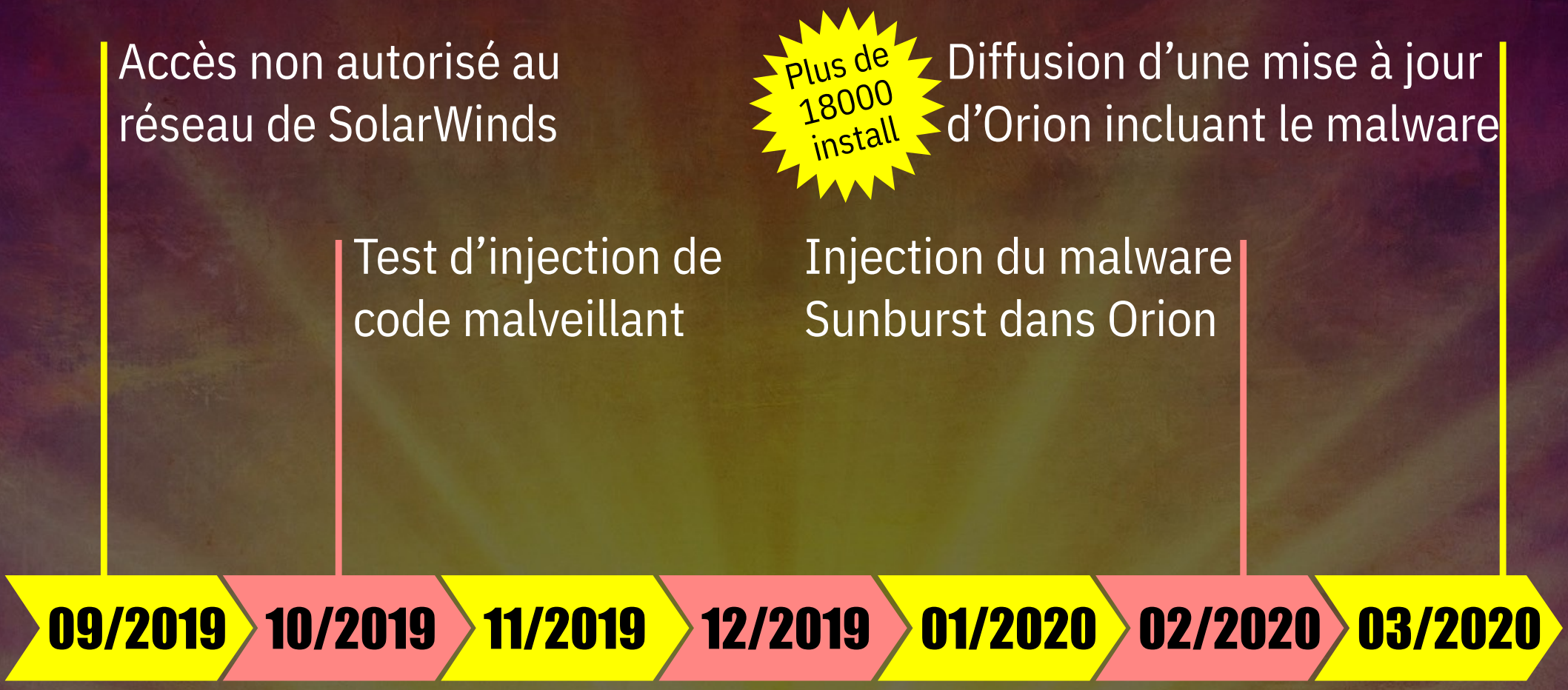


Temps d’attente avant détection en 2021

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…



Le cas SolarWinds

Sur 6 disques durs rachetés à la boutique EuroCash [...], 3 se sont avérés contenir des sauvegardes d'ordinateurs municipaux provenant du prestataire informatique de Montreuil-le-Gast. [...]

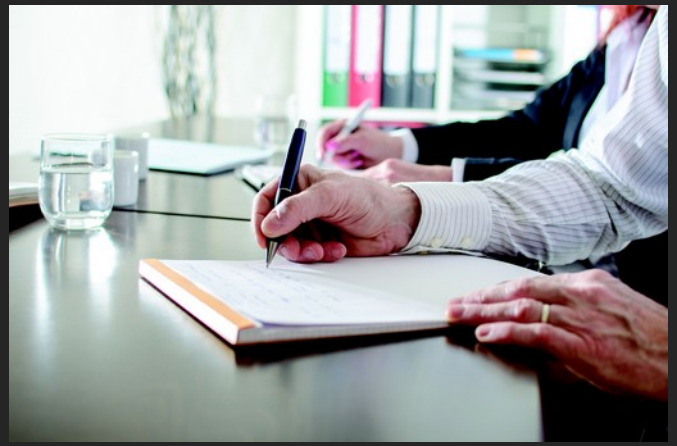
Des dizaines de milliers d'e-mails internes, les coordonnées personnelles d'élus et de responsables associatifs, des photos d'enfants d'employés...

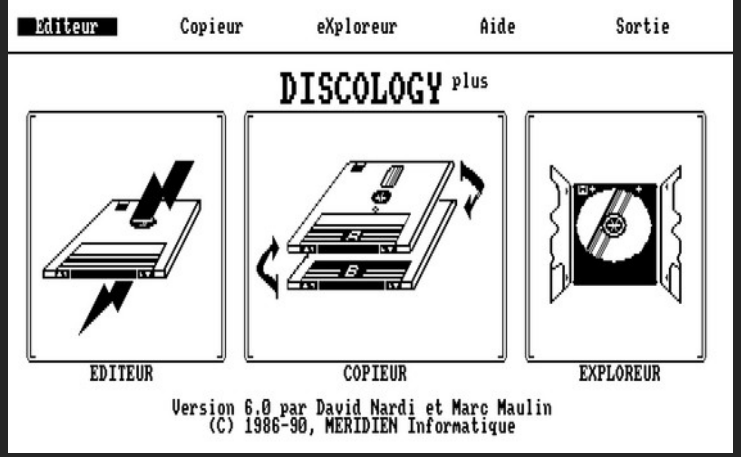
COMMENT NOUS AVONS ACHETÉ LES DISQUES DURS D'UNE MAIRIE - LE TÉLÉGRAMME 02/12/2022

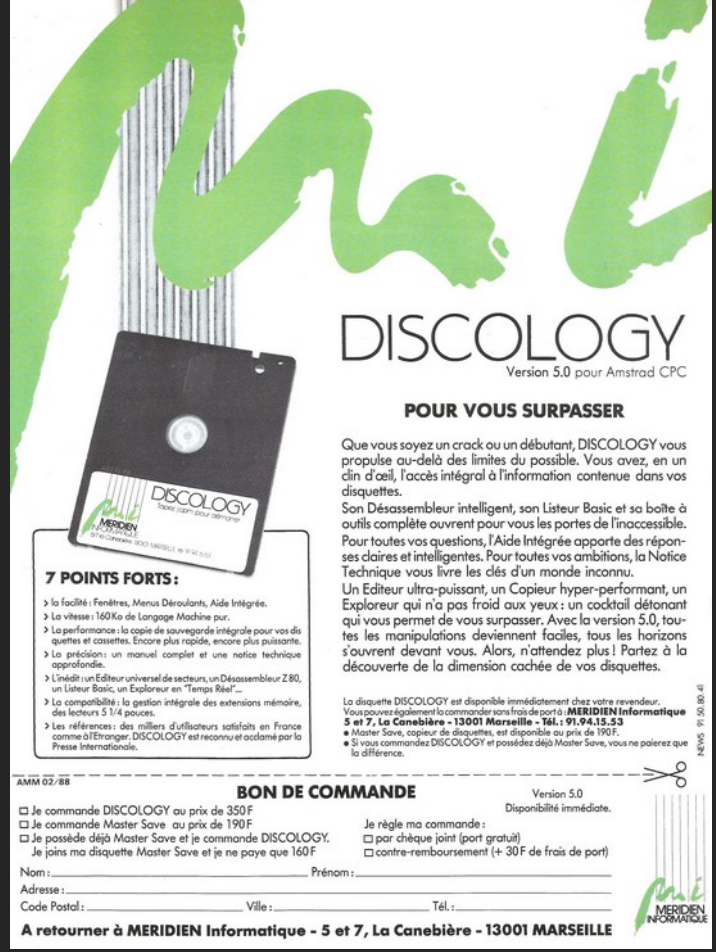
Du château-fort à l'aéroport

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 !







L'histoire sans fin

Cyberattaque dans une collectivité

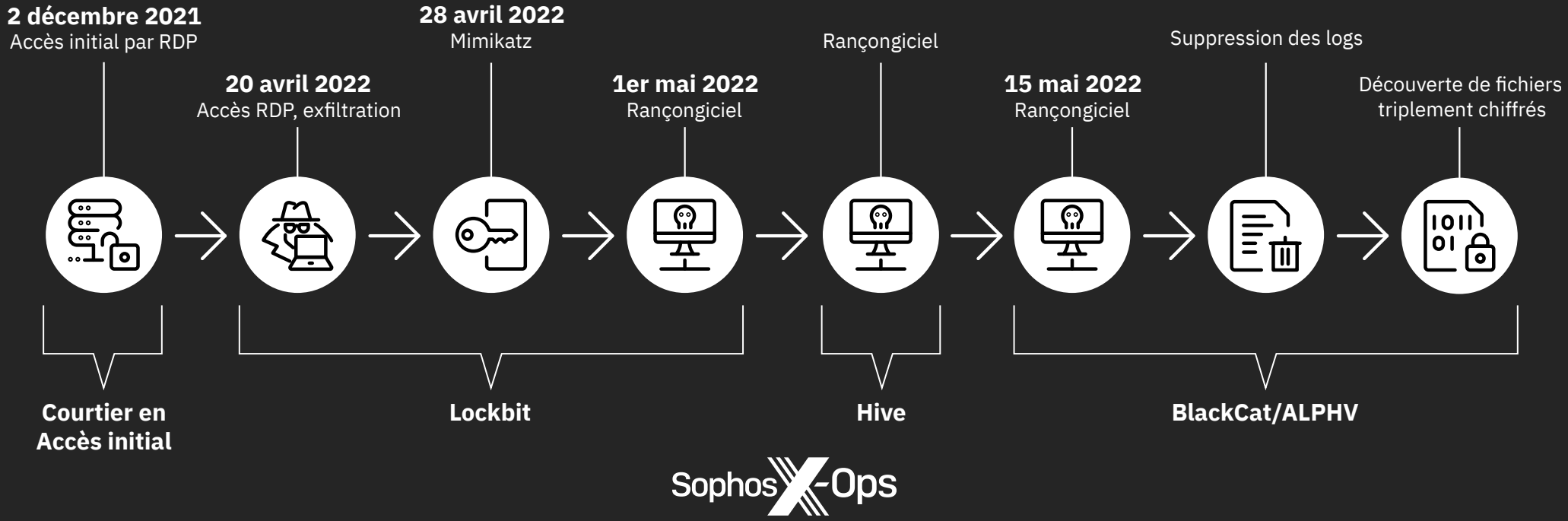
Tiens ? Ça ne marche pas !

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

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



Trois fois piraté en 15 jours !

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

Premières actions

- Mise en route du Plan de Continuité d’Activité (PCA)
  Définition des priorités, le Plan de Relance de l’Activité (PRA) suivra
- Communication officielle
  Site web si disponible, réseaux sociaux, presse, médias
- Organisation de cellules de crise
  Fonctionnelle, permis de construire…
- Accompagnement des agents

Déréférencement de caen.fr

CAEN NORMANDIE

Caenlamer NORMANDIE COMMUNAUTÉ URBAINE

Alerte cyberattaque : Sites non disponibles

Les sites internet officiels de la Ville de Caen et de la Communauté urbaine Caen la mer sont actuellement indisponibles suite à une cyberattaque.

Nous vous invitons à redoubler d'attention pour ne pas tomber dans le piège de sites frauduleux.

En cas de doute, contactez directement nos services par téléphone :

- Ville de Caen : 02 31 30 41 00
- CCAS de la Ville de Caen : 02 31 15 38 38
- Caen la mer : 02 31 39 40 00

VOS-DEMARCHES.com

Site privé indépendant de l'administration française

ETAT CIVIL | PASSEPORT | CARTE GRISE | CERTIFICAT DE NON GAGE | URBANISME | CARTE D'IDENTITÉ | PERMIS | FORMULAIRES ADMINISTRATIFS

Carte d'identité (CNI) : formulaire prédemande

Sélectionnez une sous-catégorie...

Accueil > Carte d'identité

Formulaire demande Carte nationale d'Identité en ligne

Délivrée aux personnes de nationalité française, la **Carte nationale d'identité** est valide 15 ans pour les adultes et 10 ans pour les mineurs. La CNI permet de se rendre sans passeport dans l'ensemble des pays de l'Union européenne et de l'espace Schengen. Vous avez besoin de faire établir une première carte d'identité ou de faire renouveler votre CNI expirée, perdue, volée ou détériorée ? Vous pouvez formuler une prédemande en quelques clics à l'aide du formulaire en ligne ci-dessous.

Une fois le formulaire complété, vous recevrez un mail de confirmation contenant la liste des mairies proches de chez vous, habilitées à traiter votre demande de CNI. Votre numéro de dossier de prédemande et un timbre fiscal vous sera aussi envoyé. Il vous faudra présenter ces documents accompagnés des pièces justificatives mentionnées dans le message à la mairie de votre choix.

1. Informations sur la carte d'identité | 2. Adresse de réception | 3. Vérification et validation

Retrouvez également dans ce dossier :

- État civil
- Passeport
- Carte Grise
- Certificat de non gage

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

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

[Enquête] Caen. Cyberattaque : et maintenant ?

Informatique. La Ville de Caen a été victime d'une cyberattaque lundi 26 septembre. Quels enseignements faut-il en tirer ? Comment réagir ? Éléments de réponse.

Publié le 05/10/2022 à 12h30

Quels enseignements la Ville de Caen tire-t-elle de la cyberattaque dont elle a été victime lundi 26 septembre ? Quelques éléments de réponse.

« Nouvelles du hacking de la Ville de Caen » Problèmes administratifs (Caen/Normandie)

Argumentaire

- « Je souhaite vraiment récupérer toutes mes données, qu'elles soient effacées »
- « Ils font l'erreur qu'ils ne faut pas faire [...] : faire appel à des prestataires »
- « Ils veulent tout cadenasser correctement. [...] C'était avant qu'il fallait cadenasser ! »

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

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

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

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

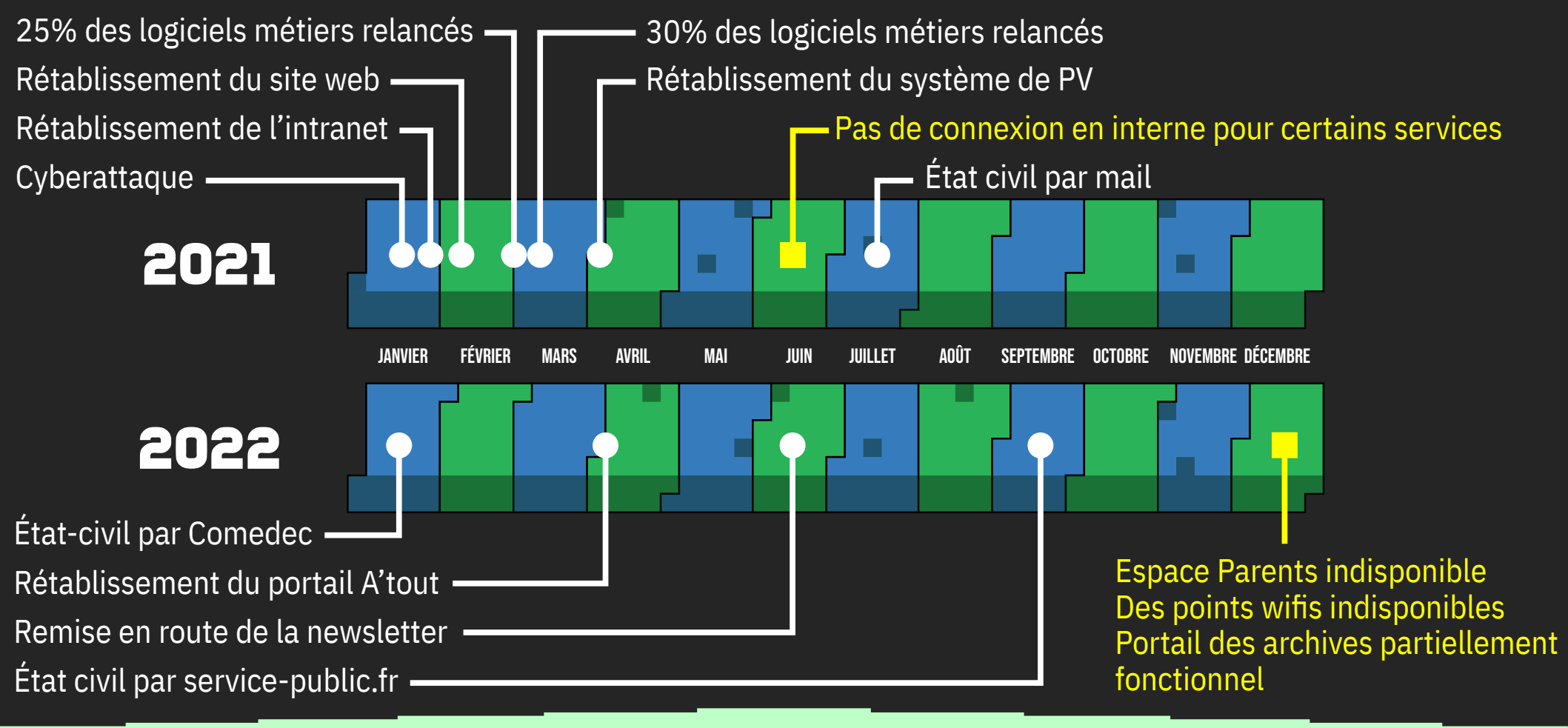
CAROLINE FEL 15/06/2021
ADJOINTE ÉDUCATION ET FAMILLE, MAIRIE D'ANGERS

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

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

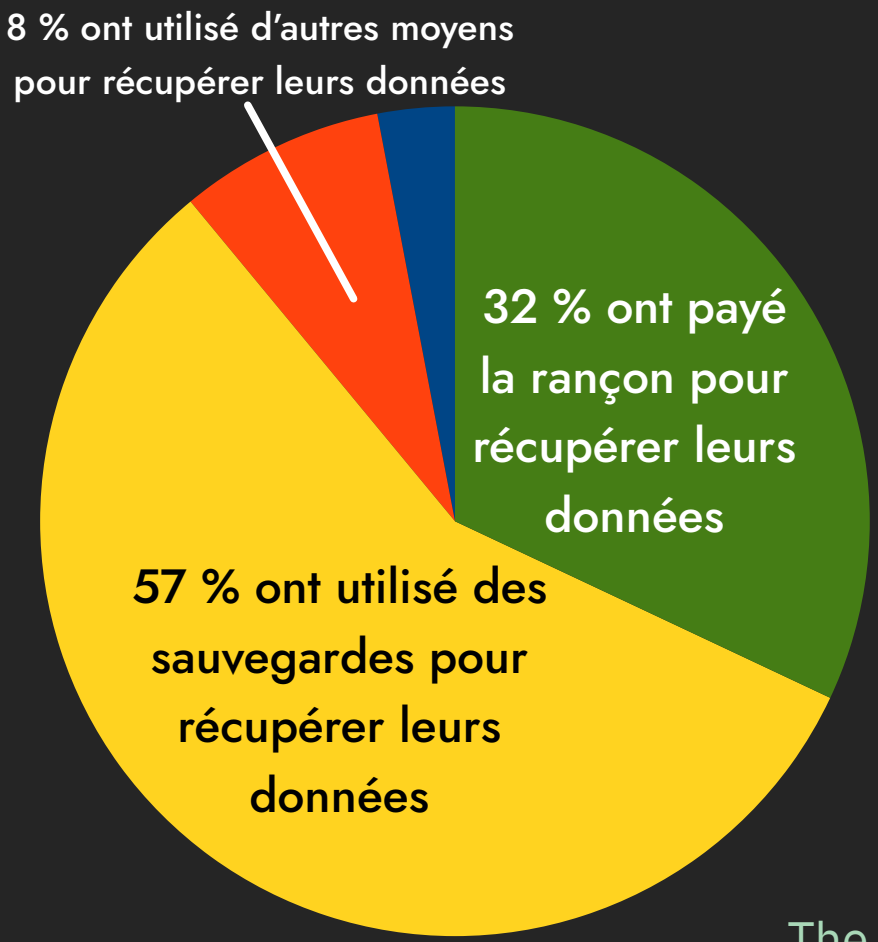


Deux ans de rétablissement à Angers

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

Payer n'est pas sauver



- Ceux qui paient
  - Récupèrent en moyenne 65 % de leurs données
  - 29 % récupèrent la moitié ou moins
  - 8 % seulement récupèrent toutes leurs données

SOPHOS

The State of Ransomware 2021

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

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 !

Impact psychologique

- Impact émotionnel similaire à la criminalité du monde réel
  Sensation de violation de l'intimité, déni, culpabilité (51%), colère (48%), anxiété (70%), vulnérabilité (86%), peur (75%)
- Impact social
  Méfiance (70%), baisse de productivité...
- Impact physique
  Insomnie (85%), trouble de l'alimentation (38%), somatisation...

MERCI !

- Merci à Échelle Inconnue, Pansybloom et à Codeurs en Seine
- Moi sur les internets
  - Github : https://github.com/zigazou
  - Twitter : @zigazou
  - Mail : zigazou@protonmail.com