Intégration de Sécurité dans les Projets

Introduction

VUE GLOBALE

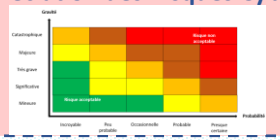
LOI REGLEMENT

NORMES

POLITIQUE RISQUES CONTROLES

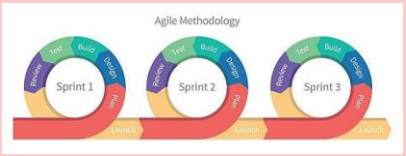
Politique & pilotage de la Cyber

Appréciation des Risques Cyber

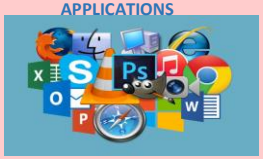


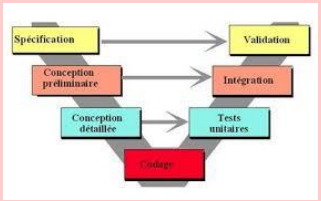
Contrôle & audit Cyber

SECURITE DANS LES PROJETS

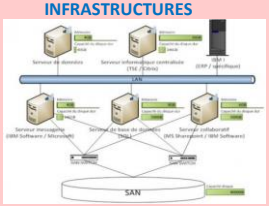


APPLICATIONS

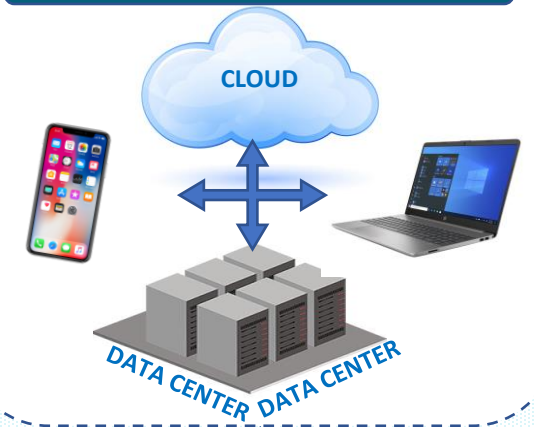




INFRASTRUCTURES



SYSTÈME D'INFORMATIONS



MESURES DE SECURITE

Gestion des identités et des accès au SI

Protection des informations

Cloisonnement et Robustesse du SI

Surveillance du SI

Gestion des vulnérabilités

MENACES


Etat de la menace

Etat de la menace

- ⇨ Les fondamentaux
- ⇨ Les principales attaques
- ⇨ Impacts natures & chiffres
- ⇨ Décryptage de quelques attaques

Les Fondamentaux

⇨Les critères de sécurité

⇨Les types de risques Cyber

⇨Les types de traitement de risques Cyber

Les Fondamentaux

La sécurité informatique vise à intégrer des mesures technico-organisationnelles à un dispositif IT afin de répondre à des exigences basés sur **3 critères** :

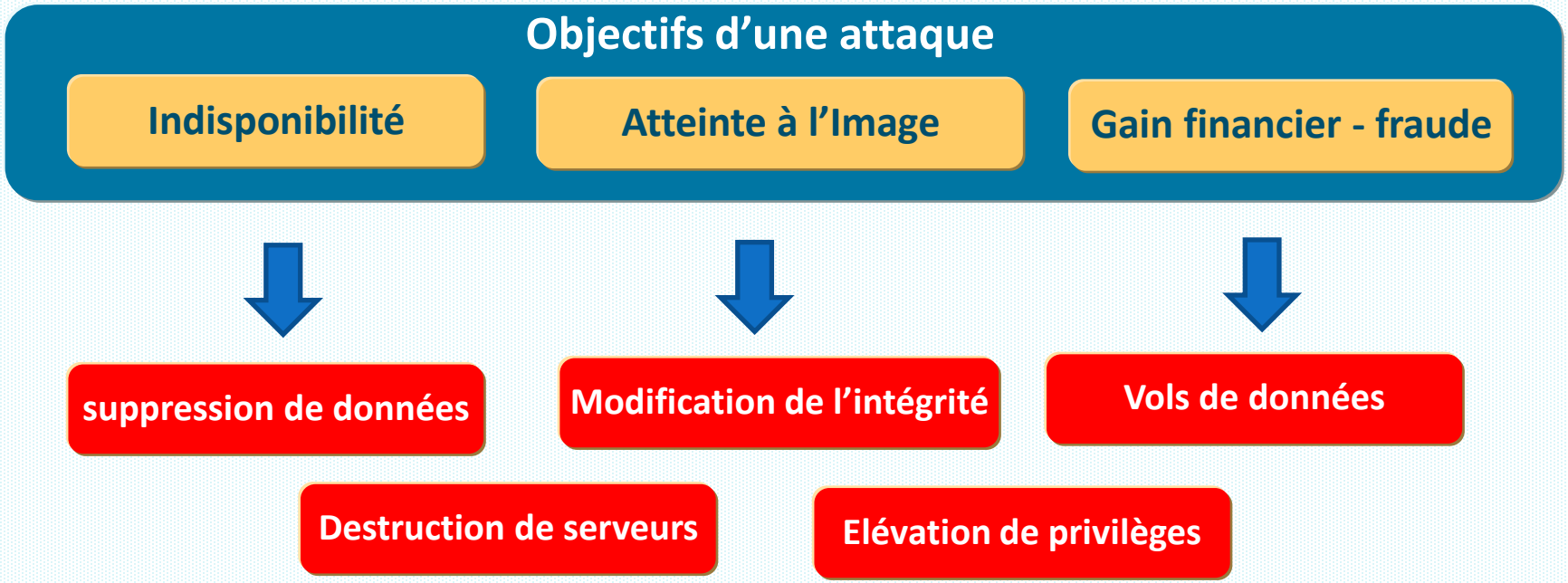
- **Disponibilité**: l'accès aux ressources du système d'information doit être permanent et sans faille durant les plages d'utilisation prévues
- **Intégrité**: garantie que le système et l'information traitée ne peuvent être modifiés que par une action volontaire et légitime
- **Confidentialité**: propriété d'une information qui n'est ni disponible ni divulguée aux personnes, entités ou processus non autorisés

Les Fondamentaux

Les Risques … cinq types possibles :

- **La cybercriminalité** : les nouvelles “mafias” en ligne dont le but est de gagner de l’argent au travers d’arnaques, de chantages ou de vols
- **La négligence** : résulte de la désinvolture des collaborateurs ou partenaires quant aux régles de sécurité internes et mettent l’entreprise en situation de risque
- **L’atteinte à l’image** : elle contribue à la campagne de déstabilisation d’une personne ou d’une entité dont les effets sont amplifiés par l’importance actuelle des réseaux sociaux
- **L’espionnage** : Sous couvert d’intelligence économique, certains concurrents ou États utilisent les vulnérabilités informatiques pour espionner les secrets d’une entreprise
- **Le sabotage** : ciblé, il est réalisé à des fins de déstabilisation (économique ou politique) ou pour des raisons idéologiques (activisme).

Les Fondamentaux



Les Fondamentaux

Le traitement du risque - quatre grandes familles de solutions pour traiter les risques :

- **l'évitement** en supprimant l'activité ou la condition qui mène au risque
- **le transfert** ou partage avec un tiers (assureur par exemple)
- **l'acceptation** du risque en mettant en place des mesures techniques ou organisationnelles pour diminuer l'impact ou la potentialité – souvent accompagné d'une provision financière

Les Principales attaques

⇨Les différents types d'attaques

- Spam
- Social Ingénierie
- Ddos
- Phishing
- Malware

⇨Zoom sur les attaque Malware - ransomwares

Types d'attaques - Spam

Le spam est un courrier électronique indésirable, non sollicité par le destinataire

- Il est souvent envoyé simultanément à un très grand nombre d'adresses électroniques.
- La plupart du temps les mails contiennent des fautes d'orthographes, une syntaxe douteuse, un contenu incohérent et ne vous sont pas explicitement destinés (mailing de masse).
- Les thèmes principaux que l'on retrouve dans les spams sont les services pornographiques, la spéculation boursière, la vente de médicaments, drogues, ou des propositions indécentes.
- Le spam peut contenir des liens ou pièces jointes frauduleuses et peut devenir une voie d'infection.

Types d'attaques - Spam

Les plus récents servent de support au phishing

- Ils proposent des remboursements de la part d'organismes publics, des faux avis de livraison, des gains à des concours, ...
- Ils peuvent vous êtes adressés nominativement, ou faire état de votre métiers ou de votre situation professionnelle.

Vigilance

- Toujours avoir un esprit critique sur les mails reçus
- Vérifier la cohérence de l'entête, de l'émetteur et de son adresse.
- « Dois-je recevoir ce mail ? »
- « M'est-il réellement destiné »
- Garder la maitrise de votre adresse e-mail
- Ne pas répondre au Spam et le supprimer
- Mettre en place des mécanismes anti-spam

Types d'attaques – Social ingénierie

L'ingénierie sociale est une manipulation psychologique, humaine qui consiste à obtenir un bien ou une information, en exploitant la confiance, l'ignorance ou la crédulité de tierces personnes.

- Une personne se faisant passer pour un personnel du support pour soutirer votre mot de passe … « suite à une panne »,…
- Une personne se faisant passer pour un personnel d'une autre direction ou d'une société en prestation pour votre entreprise pour collecter des informations sur un projet, une architecture technique, …
- La classique fraude au président
- Une personne se fait passer pour un agent des forces de l'Etat, ou de votre banque afin de soutirer des informations bancaires

Types d'attaques – Social ingénierie

Vigilance

- Ne pas communiquer d'informations par des canaux non prévus pour une prétendue urgence.
- Ne pas communiquer des informations confidentielles (login, mot de passe,…) si elles n'ont pas à l'être ou hors procédure/processus.
- Confirmer l'origine légitime d'une demande (émetteur, type de demande,…).

Dans le doute : s'abstenir !

Types d'attaques – Fraude au président

Elle consiste à convaincre le collaborateur d'une entreprise d'effectuer un virement important à un tiers pour obéir à un prétendu ordre du dirigeant

⇨ Les escrocs opèrent de manière sophistiquée après s'être très bien renseignés

- Appel de l'escroc en se faisant passant pour un président d'agence ou de groupe
- Basée sur 4 Principes : Peur , Incertitude Doute, Précipitation.
- Usurpation de Mail et coups de fil téléphoniques
- Création d'un scénario d'escroquerie amenant l'employé(e) à une sensation de confidentialité, de promotions, ou rétrogradation
- Demande d'un virement confidentiel et « secret »

⇨ Fraude estimée à 700 millions d'euros pour les entreprises française depuis 2010

⇨ +20 000 entreprises (de toutes tailles) victimes de cette arnaque

Arnaque « inventée » par le français Gilbert Chikli.

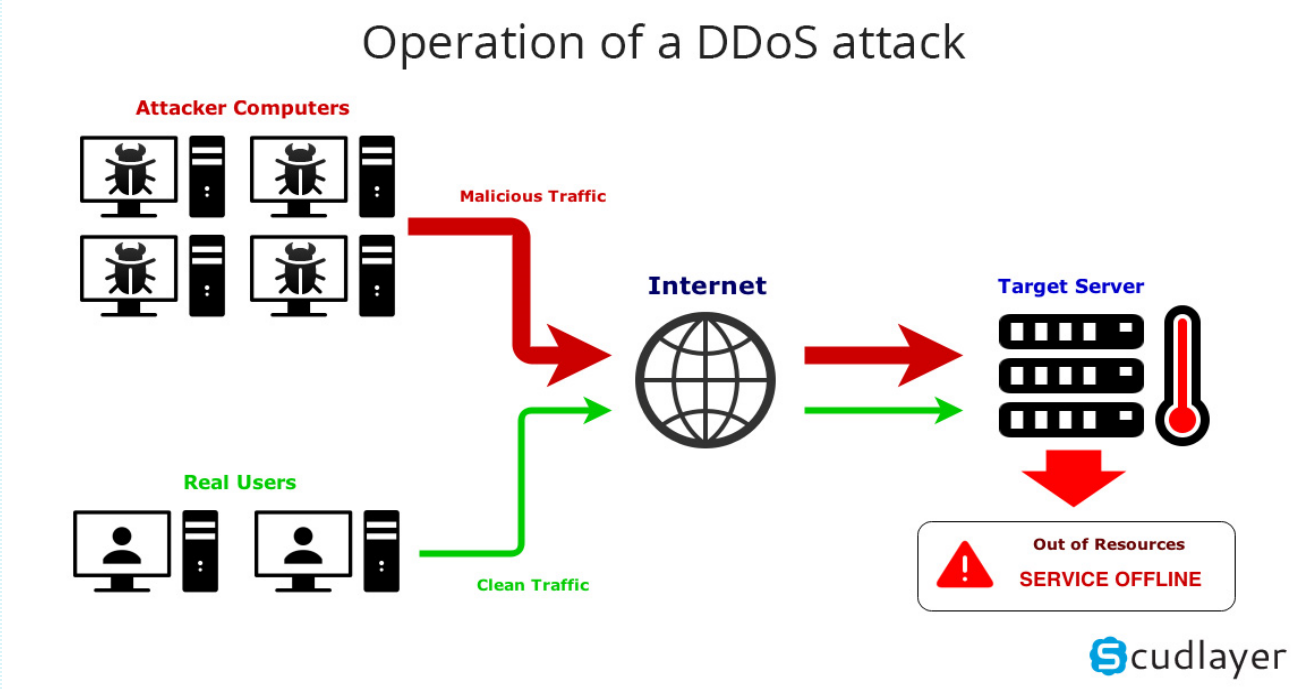
Types d’attaques – DDOS

Une attaque DDoS vise à rendre un serveur, un service ou une infrastructure indisponible en surchargeant la bande passante du serveur, ou en s’accaparant ses ressources jusqu'à épuisement)

- ⇨ OVH, l’un des hébergeurs les plus importants en Europe, a été victime d’une attaque par déni de service avec un débit supérieur au térabit par seconde.

- ⇨ Cette attaque est due à un botnet* qui est constitué de 145 00 caméras de surveillances IP, non protégées, qui ont été capables de lancer une attaque DDoS de plus de 1,5 térabit par seconde.

Types d'attaques – DDOS



Vigilance

- Ne pas forcer et relancer les connexions, vous participerez alors au déni de service
- Souscrire à des offres de protections offerts par les hébergeurs et/ou les opérateurs telecom

Types d'attaques – Phishing

Le phishing est une forme d'attaque dans laquelle le cybercriminel se fait passer pour un organisme ou une personne dans le but de voler des informations privées. Cette attaque se fait généralement par mail.

⇨Formulaire à remplir

⇨Redirection vers un faux site

⇨Les informations recherchées sont :

- Identifiants & mots de passe
  - Numéro de sécurité sociale
  - Numéro de cartes bancaires
  - Numéro de compte bancaire
  - Date de naissance
  - PINs (Personal Identification Numbers)

Types d’attaques – Phishing

Vigilance

- Ne pas cliquer sur les liens associés à un mail suspect.
- Ne pas télécharger sur les pièces jointes du mail.
- Mettez à jour votre système d’exploitation et votre navigateur web.
- Ne pas transférer le mail à ses collègues.
- Communiquer au service sécurité la réception d’un mail douteux.
- Supprimer le mail.

Types d'attaques – Malware

Un malware est un programme malveillant développé dans le but de nuire à une entreprise, un système d'information ou une personne.

⇨ **Le virus** est un programme qui a pour but de s'auto-reproduire en infectant d'autres programmes

⇨ **Les vers** sont installés directement sur les ordinateurs de leurs victimes à partir d'un code indépendant, avant de trouver des opportunités pour se répandre ou se faufiler dans d'autres systèmes. A la différence du virus qui se multiplie sur la machine de la victime, le vers se propage sur le réseau.

Types d'attaques – Malware

- **Les chevaux de Troie** sont des programmes qui ne se dupliquent pas, qui prétendent être légitimes, mais qui sont réellement conçus pour mener des actions à l'insu de leurs victimes. Ces logiciels n'ont qu'un seul but : **La prise de contrôle à distance** d'un ordinateur de façon discrète à travers un Remote Access Tool/Trojan (RAT). Ils sont généralement déployés avec des modules keyloggers (enregistrement de frappes), Screenshot, parcours de disque et exfiltration de données.

- **La Porte dérobée (ou backdoor)** : Elle est une voie d'accès illégitime insérée dans un logiciel, un système, un matériel à l'insu de l'utilisateur permettant de maintenir un accès dans le temps.

- **Le rootkit** est un ensemble de logiciels permettant généralement d'obtenir les droits root sur une machine, d'installer une backdoor, et d'effacer les traces laissées par l'opération.

Types d'attaques – Malware

Vigilance

- Ouvertures régulières de fenêtres de pop-up ou de publicités
- Modification de la configuration du navigateur web : Modification de votre page d'accueil ou du moteur de recherche …
- Surconsommation des ressources : Réduction de l'espace libre sur disque sans raison, surcharge du processeur
- Antivirus ou pare-feu désactivés sans intervention
- Mises à jour système ou antivirus chouant systématiquement

Types d'attaques – Ransomware

Les ransomware sont des malwares qui visent à extorquer de l'argent en chiffrant les données des postes de l'utilisateur ou de l'entreprise puis exige une rançon afin de les déchiffrer

En quoi un ransomware est différent d'un malware traditionnel ?

- Les ransomwares ne volent pas d'informations, ils n'exploitent pas l'ordinateur hôte
- Ils bloquent l'accès à l'utilisateur en verrouillant logiquement l'accès à sa machine et/ou à ses documents
- Ils demandent une rançon (la plupart du temps en bitcoin)
- Ils permettent une monétisation directe pour un coût de mise en œuvre limité

Types d'attaques – Ransomware

Comment opèrent-ils ?

⇨ Chaque ransomware est conçu pour agir différemment, mais ils sont tous programmés pour être furtifs et éviter d'être détectés par un antivirus classique

- **Techniques de l'obfuscation** : complication volontaire du code de manière à brouiller les pistes afin de passer au travers des niveaux de protection de l'antivirus classique
- **Chiffrement des communications** avec leur centre de commande : les communications chiffrées étant alors quasiment intraçables
- **Méthodes de chiffrement des données très robustes** : méthodes de chiffrement améliorées grâce à des crypto-bibliothèques qui utilisent un chiffrement puissant

Types d'attaques – Ransomware

Eléments observer par l'utilisateur …

Blocage de l'écran de l'appareil (ordinateur, smartphone ou tablette) en affichant une image détaillant le processus de récupération du contrôle de la machine, précisant le montant de la rançon et la procédure de paiement

Types d'attaques – Ransomware

Comment est-on infecté par un ransomware ?

⇨ Infection principalement par le biais d'une pièce jointe piégée
- mails infectés, déguisés en factures UPS, FedEx ou de banques américaines
- email provenant en apparence d'un prestataire envoyant une simple facture ou un récapitulatif de commande

⇨ Infection via un clic sur une fenêtre pop-up

Nouvelles variantes : diffusion par une simple clé USB ou via les messageries instantanées sous la forme d'une image dissimulant la charge utile

Types d'attaques – Ransomware

Vigilance

- Sauvegarder régulièrement vos données sur un support externe, hors ligne
- Ne pas cliquer sur les liens envoyés dans un mail par une personne inconnue
- Ne pas télécharger et ne pas ouvrir les pièces jointes à un mail douteux.
- En cas d'infection, ne pas payer la rançon.
- Déclarer tout incident au service compétent ou à votre correspondant sécurité.
- En cas de comportement suspect, débrancher le réseau Ethernet et Wi-Fi.

- Maintenir son anti-virus/anti-malware à jour

Types d'attaques – Ransomware

A votre avis, quel est le moyen de lutte prioritaire ?

Moyens de lutte possible

- Antivirus fonctionnel et à jour
- Installer les mises à jour de sécurité
- Maitrise et filtrage des points de connexion à internet
- La sauvegarde
- La sensibilisation

Types d'attaques – Ransomware

A votre avis, quel est le moyen de lutte prioritaire ?

Moyens de lutte possible

- Antivirus fonctionnel et à jour
- Installer les mises à jour de sécurité
- Maitrise et filtrage des points de connexion à internet
- ✓ **La sauvegarde**
- La sensibilisation

Types d'attaques – Ransomware

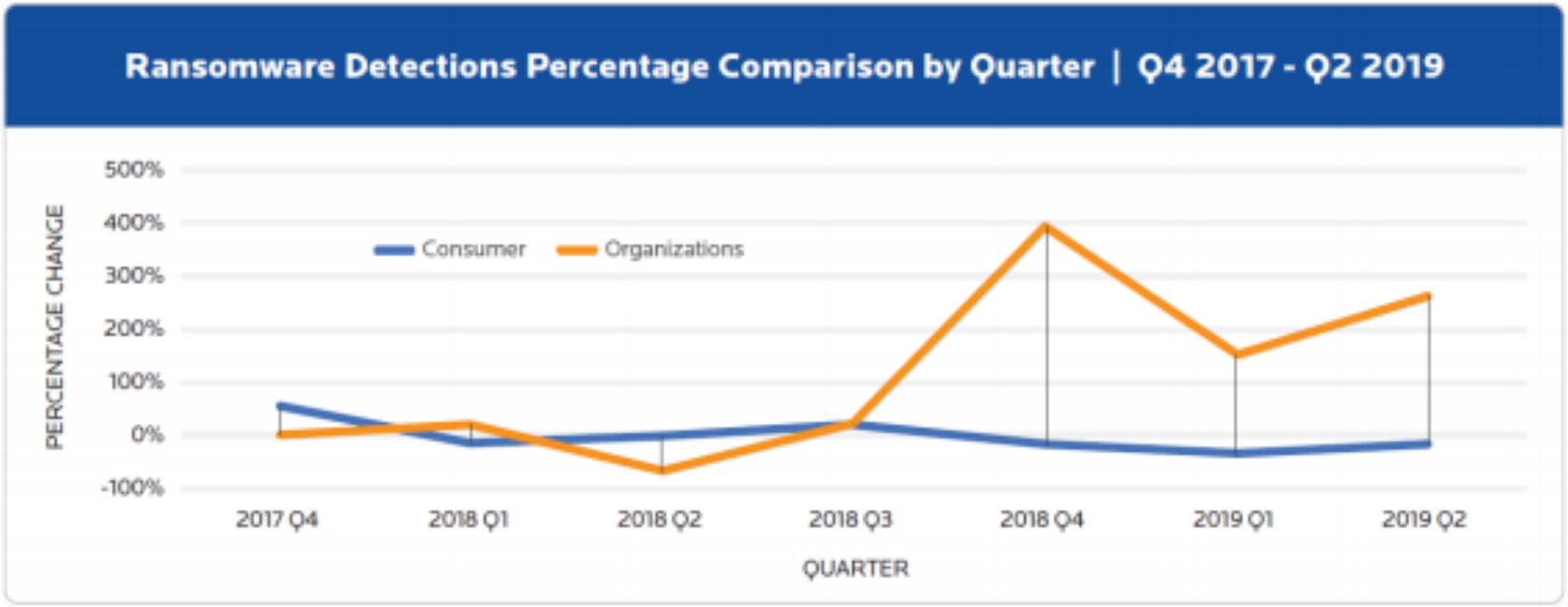


Fig. 3.2 : Comparatif de l'évolution du nombre d'attaques par rançongiciels impactant les particuliers et les entreprises. Source : MalwareBytes

Types d'attaques – Ransomware

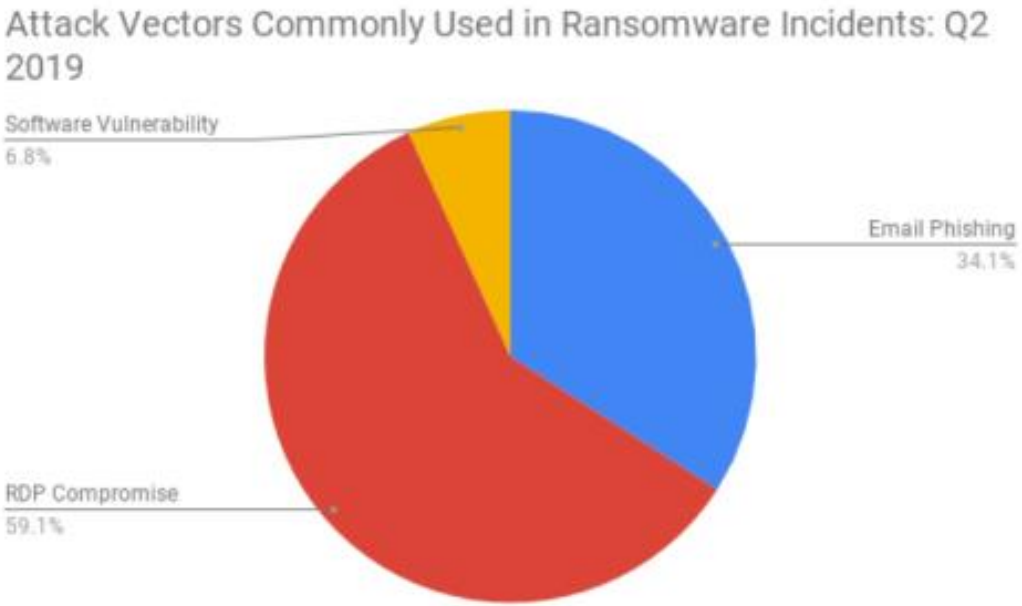


Fig. 3.5 : Vecteurs d'attaques utilisés pour délivrer des rançongiciels au 2ème trimestre 2019. Source : Security Boulevard

RDP : Remote Desktop Protocol *protocole qui permet à un utilisateur de se connecter sur un serveur exécutant Microsoft Terminal Services.*

Types d'attaques – Ransomware

Fig. 4.2 : Recensement des attaques par rançongiciels sur des entités gouvernementales américaines. Source : PCMatic.

Types d'attaques – Ransomware

Les groupes criminels sont désormais en mesure de préparer leurs opérations d'extorsion plusieurs mois à l'avance et ciblent spécifiquement des grandes entreprises ou institutions capables de payer de larges sommes d'argent.

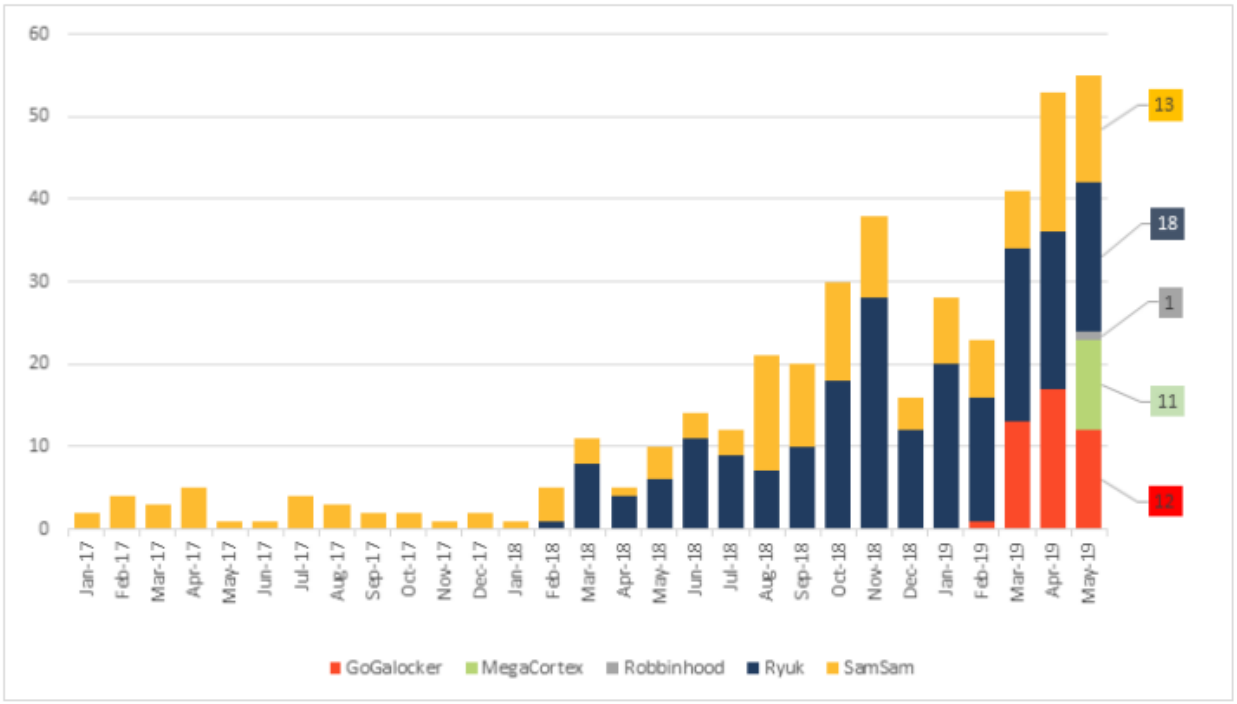


Fig. 3.4 : Multiplication des attaques impliquant certains rançongiciels utilisés pour du Big Game Hunting.
Source : Symantec

Types d'attaques – Ransomware

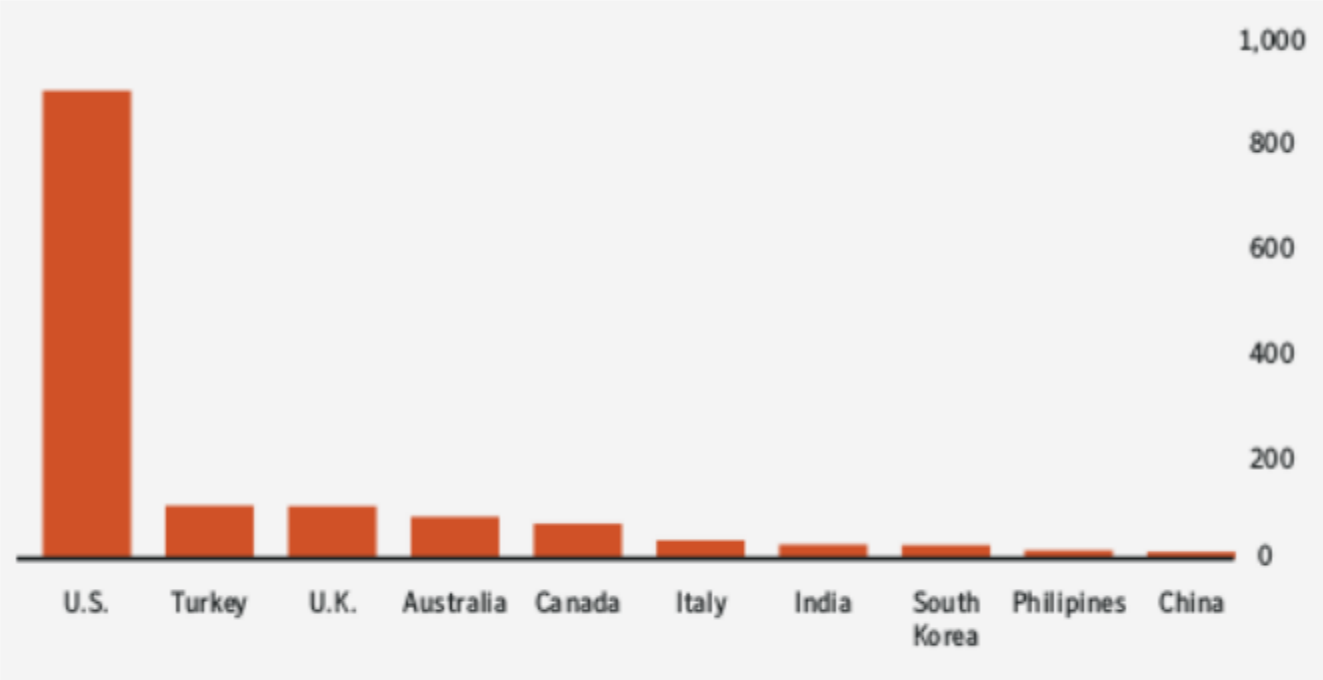
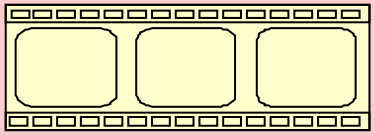


Fig. 4.1 : Répartition par pays des attaques « Big Game Hunting » détectées par Symantec ces dernières années.
Source : Symantec

Types d’attaques – Phishing

Rien ne vaut un petit film …



⇨ **Exercice :** Identifier ***les principales vulnérabilités*** qui ont été exploités par l’attaquant

Attaque : Impacts & chiffres

- ⇨ **Principaux impacts**
- ⇨ **Principaux chiffres en France et dans le monde**

Attaques: les principaux impacts

EFFETS D'UNE CYBERATTAQUE ET COÛTS LIÉS

	IMPACT INITIAL - PIC DE LA CRISE *premiers jours*	EFFET DE SOUFFLE *dans les mois qui suivent : de 1 à 3 mois*	RÉPLIQUES *effets rebonds de 6 mois à 3 ans*
PERTES D'EXPLOITATION	• Arrêt du fonctionnement normal de l'entreprise, voire interruption d'activité sévère • Pertes de données indispensables au bon fonctionnement de l'entreprise • Arrêt des canaux de communication avec les clients/ fournisseurs • Perte de temps des équipes, démobilisation • Perte de clients, perte d'opportunités commerciales	• Dysfonctionnent interne • Activité en mode dégradé, ralentissement (désorganisation, rattrapages) • Frais de dédommagement	Révélation dans les médias, impacts dus aux changements organisationnels internes. Facteurs aggravants pour les activités B2C : visibilité négative de la marque, suite juridique GDPR
COÛTS LIÉS À LA GESTION DE CRISE INFORMATIQUE	• Investigation, mobilisation d'expertise • Achat de matériel • Frais opérationnels de renfort (intérimaires métiers, saisies de données *a posteriori*, reconstruction de bases de données)	• Coût de reconstruction, de correction (peut monter jusqu'à 15 % du budget de la DSI) • Effet de rattrapage avec impact sur les pratiques internes - évolution des méthodes d'accès, conduite de changement qui peut être complexe...	
COÛTS LIÉS À LA COMMUNI-CATION	• Définition des messages, de la posture, communication auprès des collaborateurs, des clients, de l'écosystème, des autorités, des médias • Temps consacré à gérer les différentes interrogations	• Possibles rebonds à gérer en cas de fuite d'éléments nouveaux • Impact sur l'image dans le temps à suivre	
COÛTS JURIDIQUES	• Étude des impacts juridiques possibles • Gestion du dépôt de plainte de l'entreprise	• Premières requêtes ou demandes des autorités • Audits complémentaires	• Suite des affaires judiciaires/juridiques • Coûts liés aux conseils et au temps consacré • Coûts des amendes éventuelles

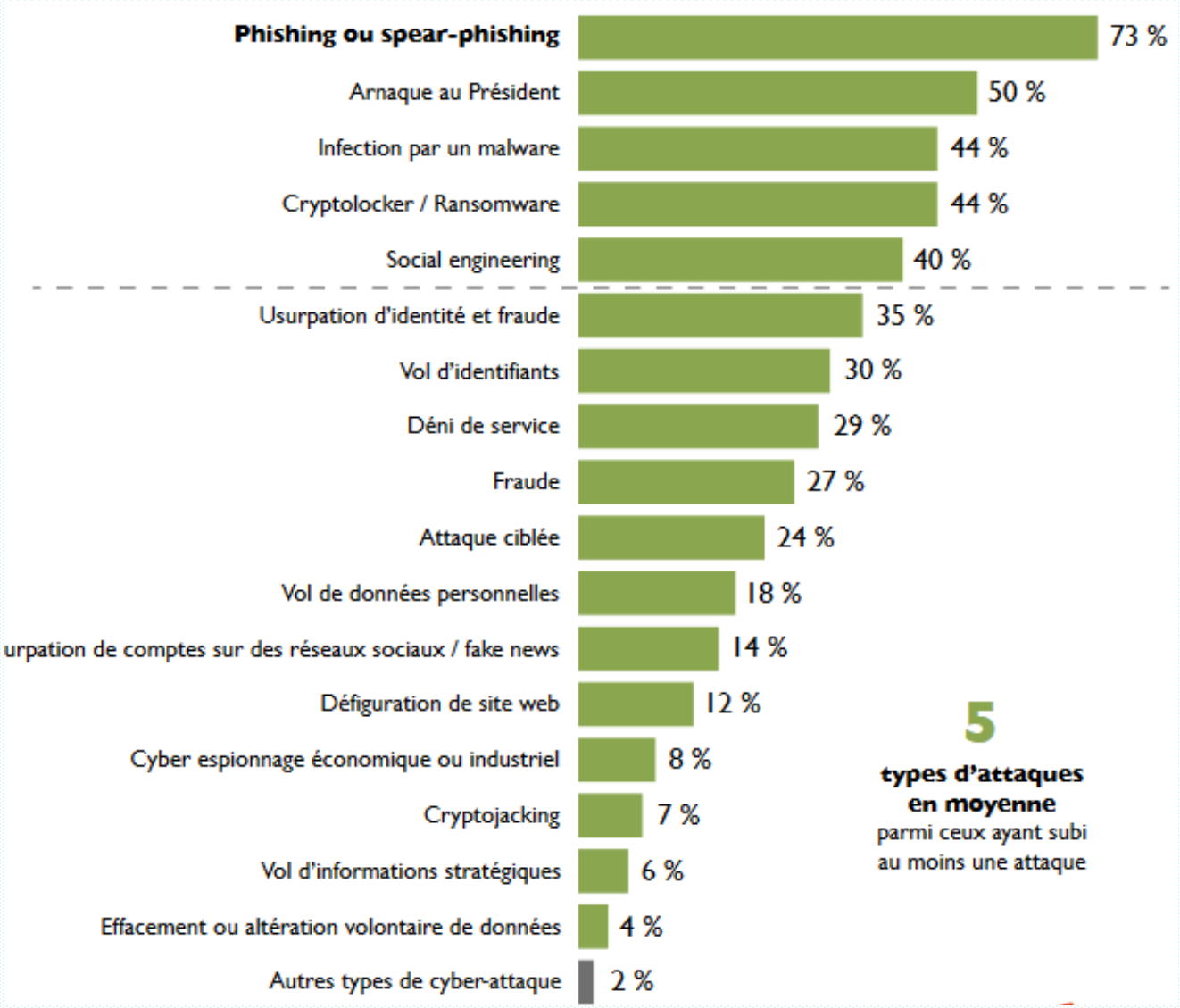
Source *: rapport du Ceidig 2021*

Les attaques en chiffre - France

- ⇨ Effet Pandémie : Hôpitaux, Agence du médicament, …
- ⇨ Collectivités locales
- ⇨ Premier redressement judiciaire suite à une attaque

Source *: rapport du Ceidig 2021*

Les attaques en chiffre - France



Les attaques en chiffre - France

Les cyberattaques les plus courantes contre les entreprises

Types d'attaques les plus constatés par les entreprises françaises en 2019 *

79 %	Phishing ou spear-phishing
47 %	Arnaque au président
43 %	Exploitation d'une vulnérabilité
40 %	Tentatives de connexion
35 %	Ingénierie sociale
31 %	Acquisition de noms de domaines illégitimes
29 %	Exploitation d'un défaut de configuration
28 %	Attaque en déni de service

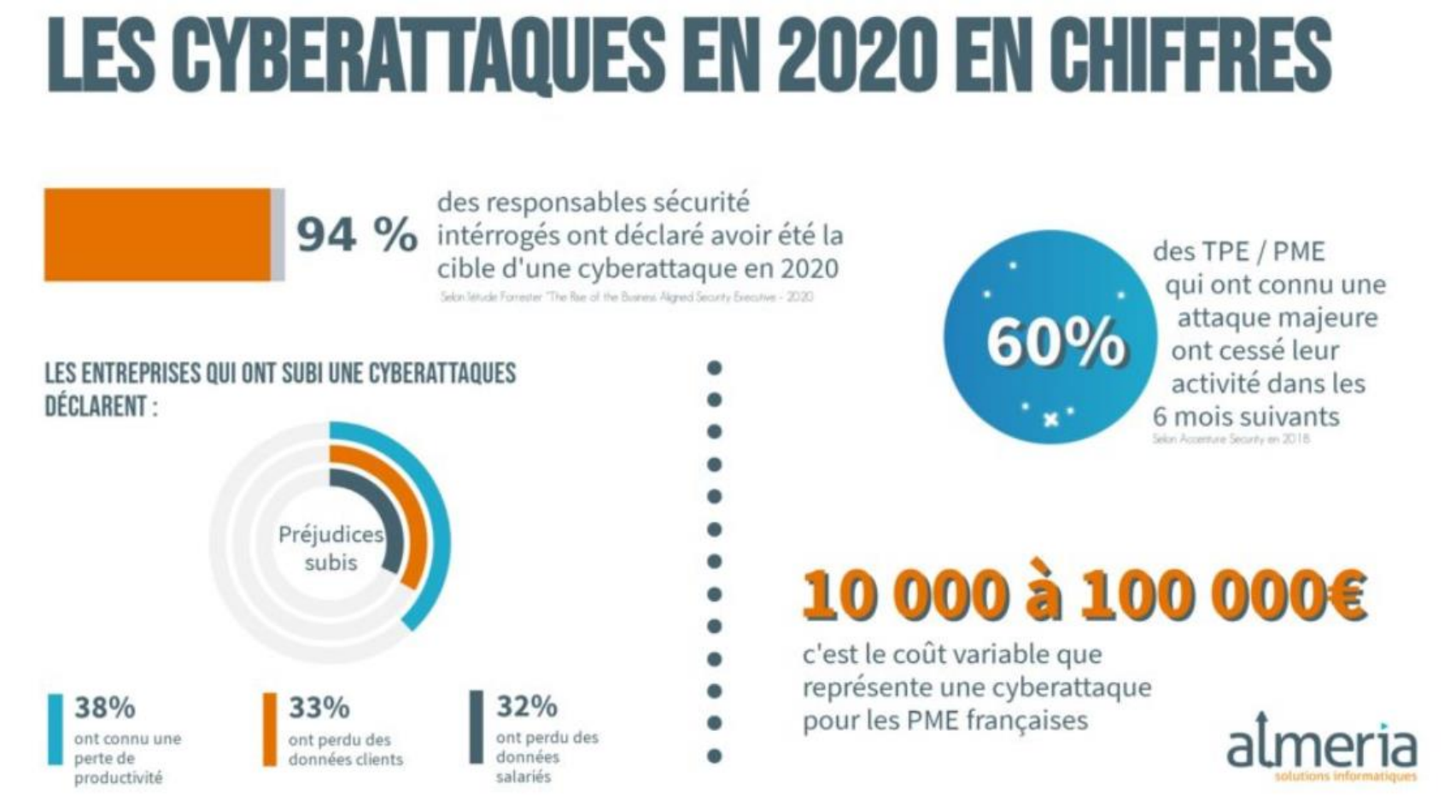
* Plusieurs réponses possibles, sélection des résultats supérieurs à 20 %.
En moyenne : 3,9 types d'attaques constatés parmi les entreprises ayant subi au moins une attaque.

Sources : CESIN, OpinionWay

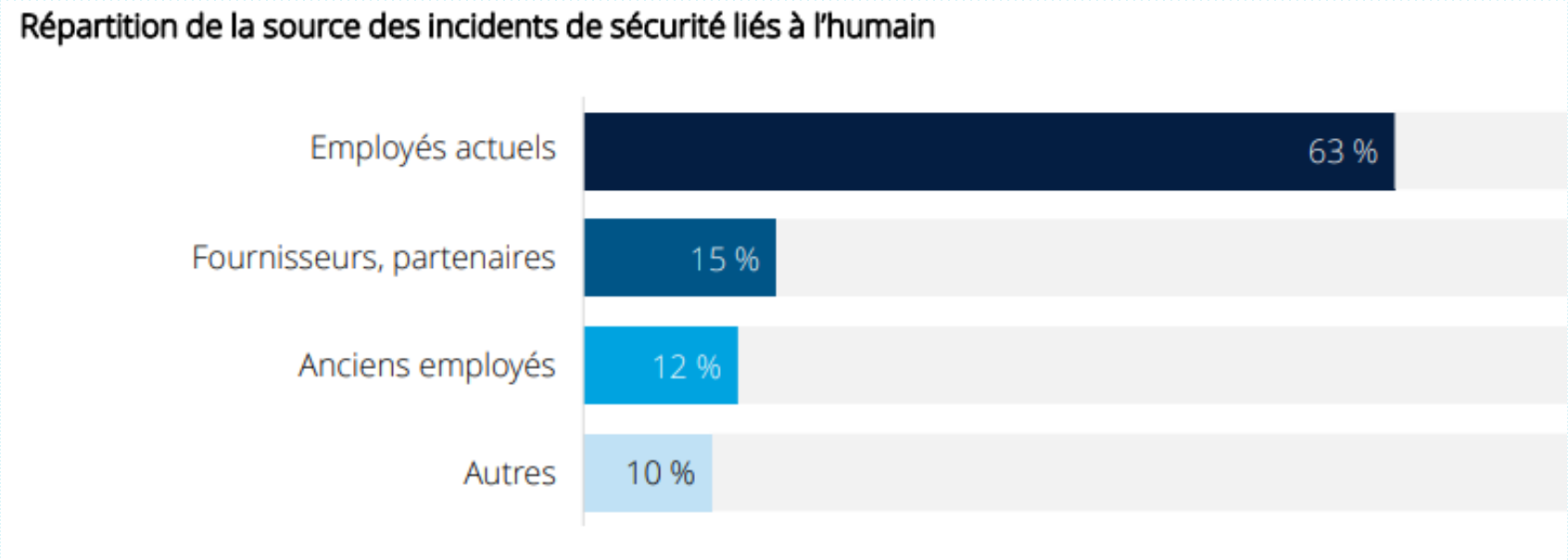
Les attaques en chiffre - France

- **8 entreprises sur 10** sont touchées par des cyber attaques chaque année.
- **En 2018**, le phishing (ou hameçonnage) est le mode d'attaque le plus fréquent avec **73%** d'entreprises touchées.
- **60%** des entreprises interrogées affirment que les cyber attaques ont eu un impact sur l'activité de leur entreprise. Les conséquences de ces attaques sont multiples :
  - **26% Ralentissement** de la production pendant une période significative
  - **23% Indisponibilité** de leur site Internet pendant une période significative
  - **12% Retards** de livraison auprès des clients
  - **11% Pertes** de chiffre d'affaires
  - **9% Arrêt de la production** pendant une période significative
  - **22% A**utres effets négatifs : augmentation de la charge de travail, baisse de productivité des collaborateurs, mauvaise réputation de l'entreprise

Les attaques en chiffre - France

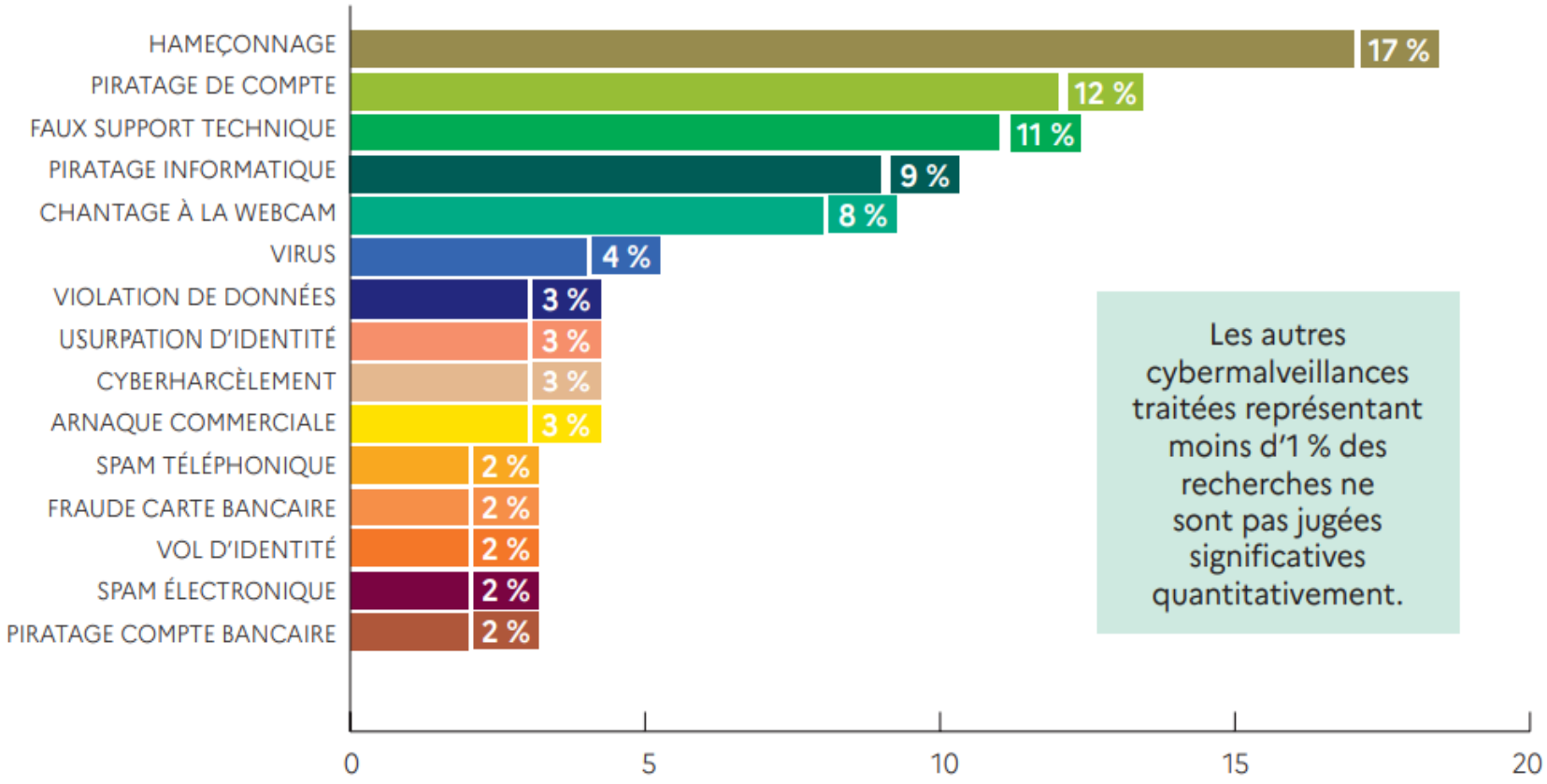


Les attaques en chiffre - France



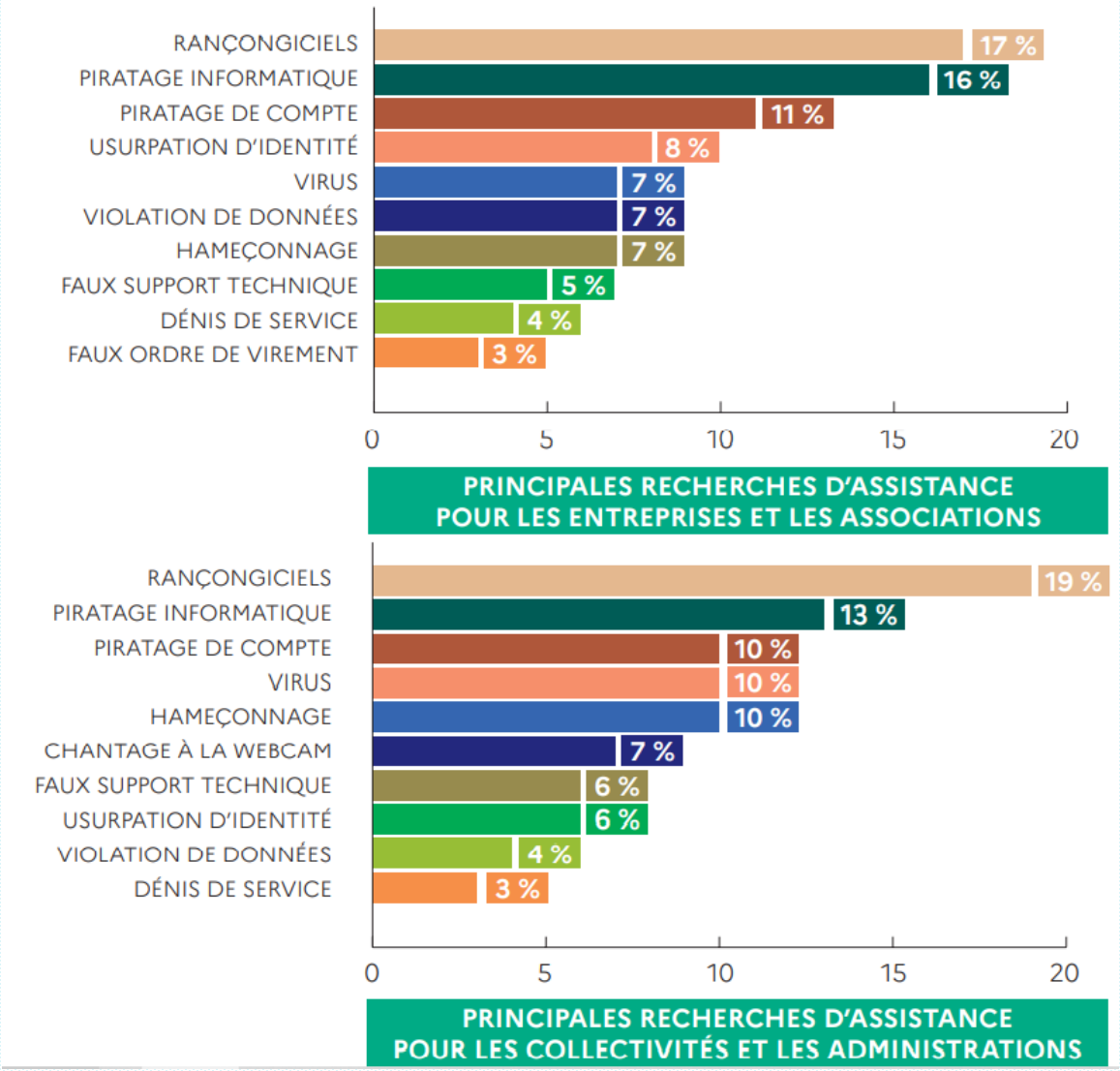
Les attaques en chiffre - France

LES 15 PRINCIPALES CYBERMALVEILLANCES SUR LESQUELLES ONT PORTÉ LES RECHERCHES D'ASSISTANCE DES PARTICULIERS EN 2020



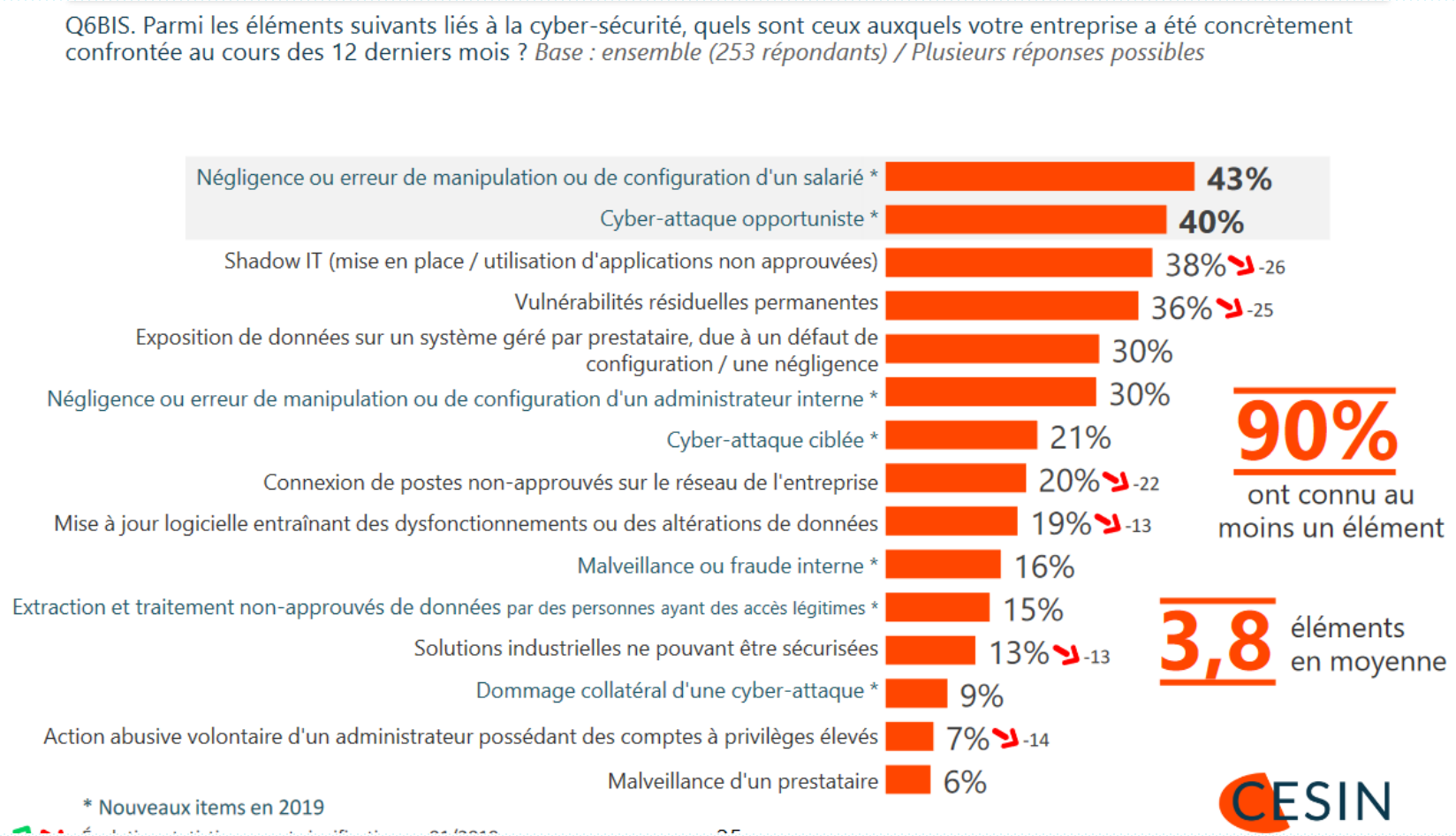
SOURCE CYBERMALVEILLANCE.GOUV.FR

Les attaques en chiffre - France



SOURCE CYBERMALVEILLANCE.GOUV.FR

Les attaques en chiffre - France



Les attaques en chiffre - France

Les PME aussi victimes des cyberattaques

- **43% des cyberattaques** visent les petites entreprises
- **4 PME sur 10** ont déjà subi une ou plusieurs attaques ou tentatives d'attaques informatiques.
- Les principales attaques :
  - *Phishing (24 %)*
  - *Malware (20 %)*
  - *Ransomware (16 %)*
  - *Fraude au président (6 %)*

Les attaques en chiffre - France

Vu par la Gendarmerie et la Police :

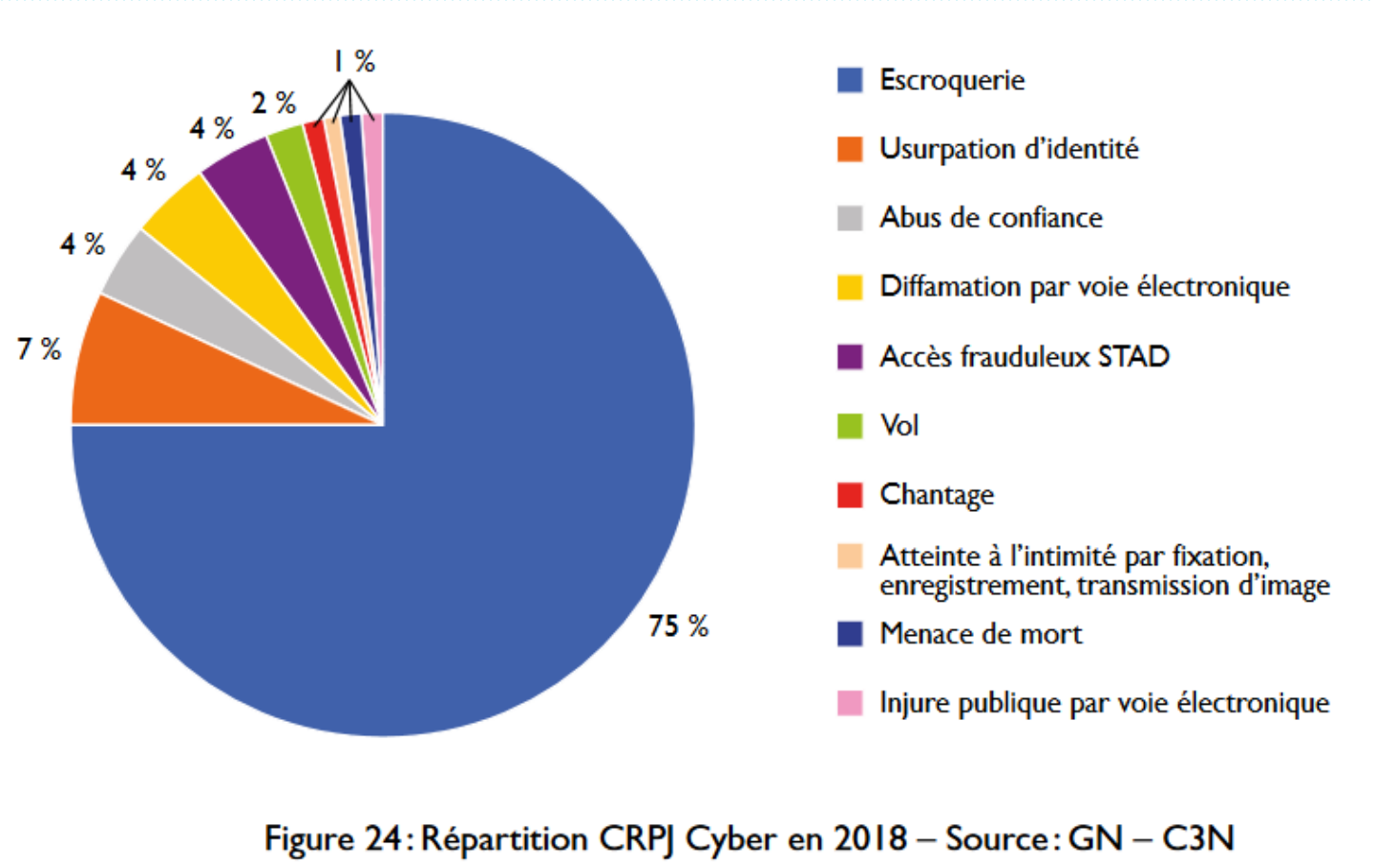
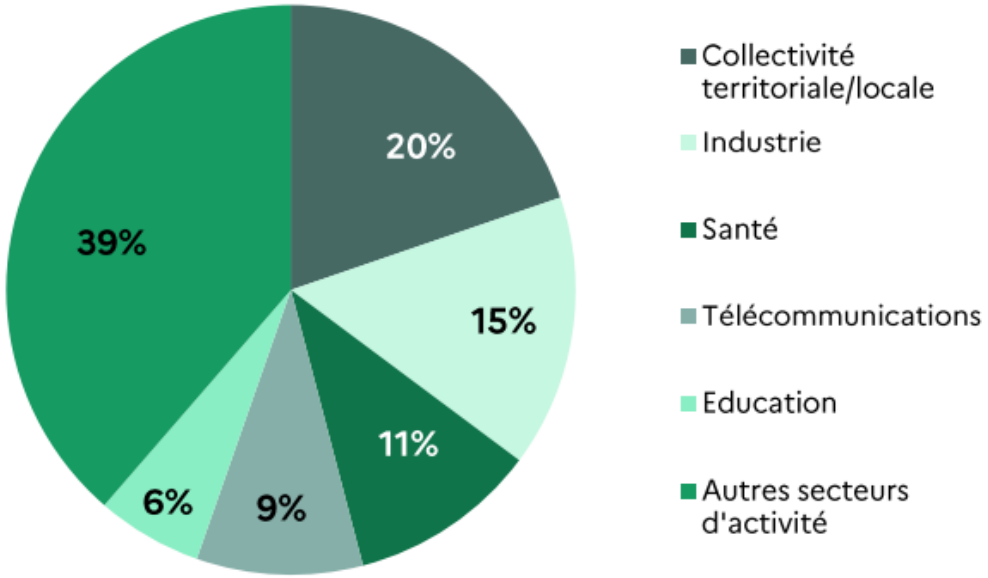


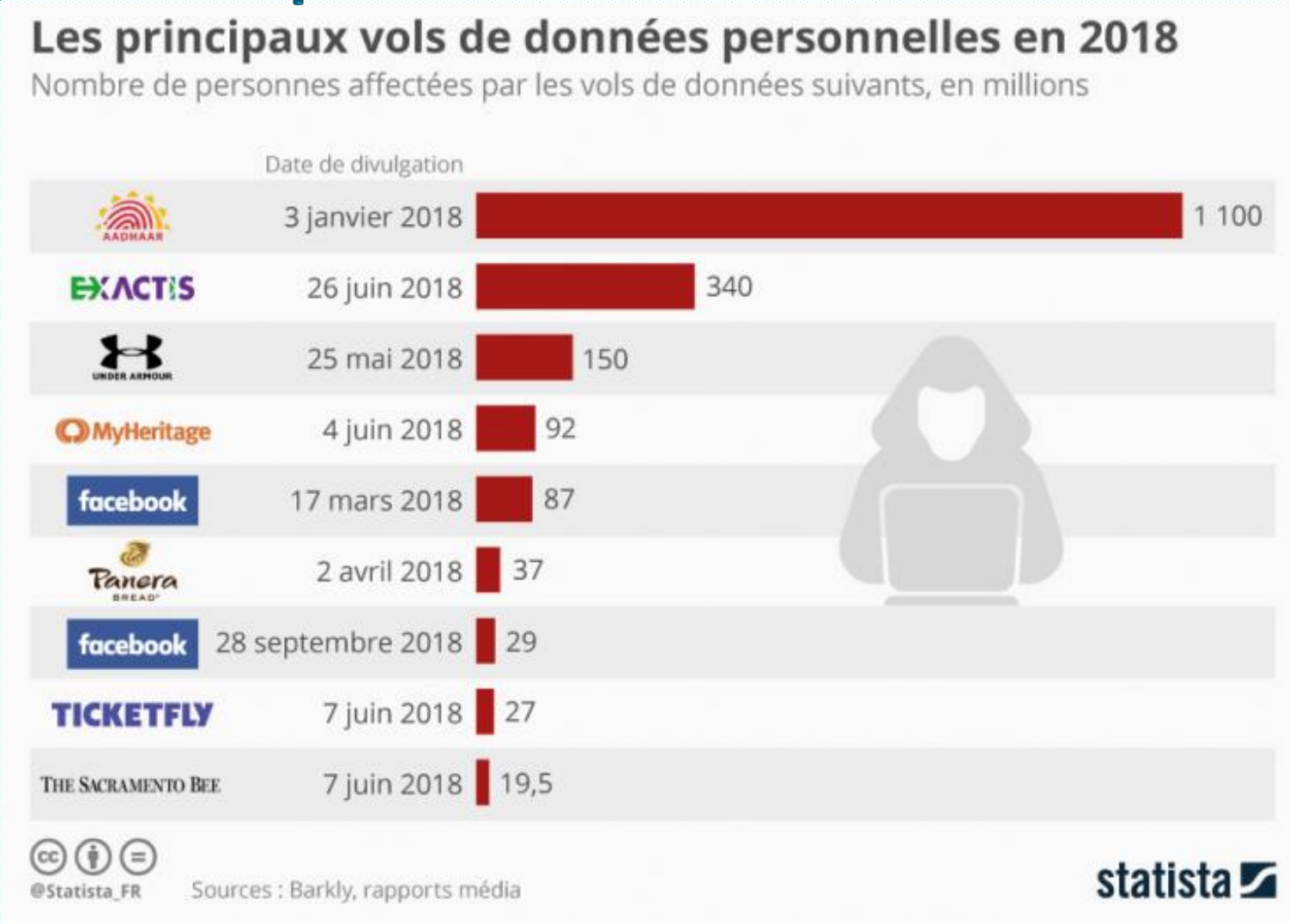
Figure 24 : Répartition CRPJ Cyber en 2018 – Source : GN – C3N

Les attaques en chiffre - France

Graphique : Secteurs d'activité touchés par les rançongiciels en 2020 en France



Les attaques en chiffre - Monde



AADHAAR : système d'identification de la population de l'Inde fondé sur la biométrie.

Les attaques en chiffre - Monde

- En 2017, **le coût moyen** d'une attaque de malware était **de 2,4 millions de dollars**
- En 2019, les coûts des dommages causés par un rançongiciel (ransomware) vont atteindre **11,5 millions de dollars par entreprise**
- Une entreprise sera victime **d'une attaque par un rançongiciel** toutes **les 14 secondes cette année**

Décryptage

⇨ DRIDEX

⇨ WANNACRY

⇨ STUXNET

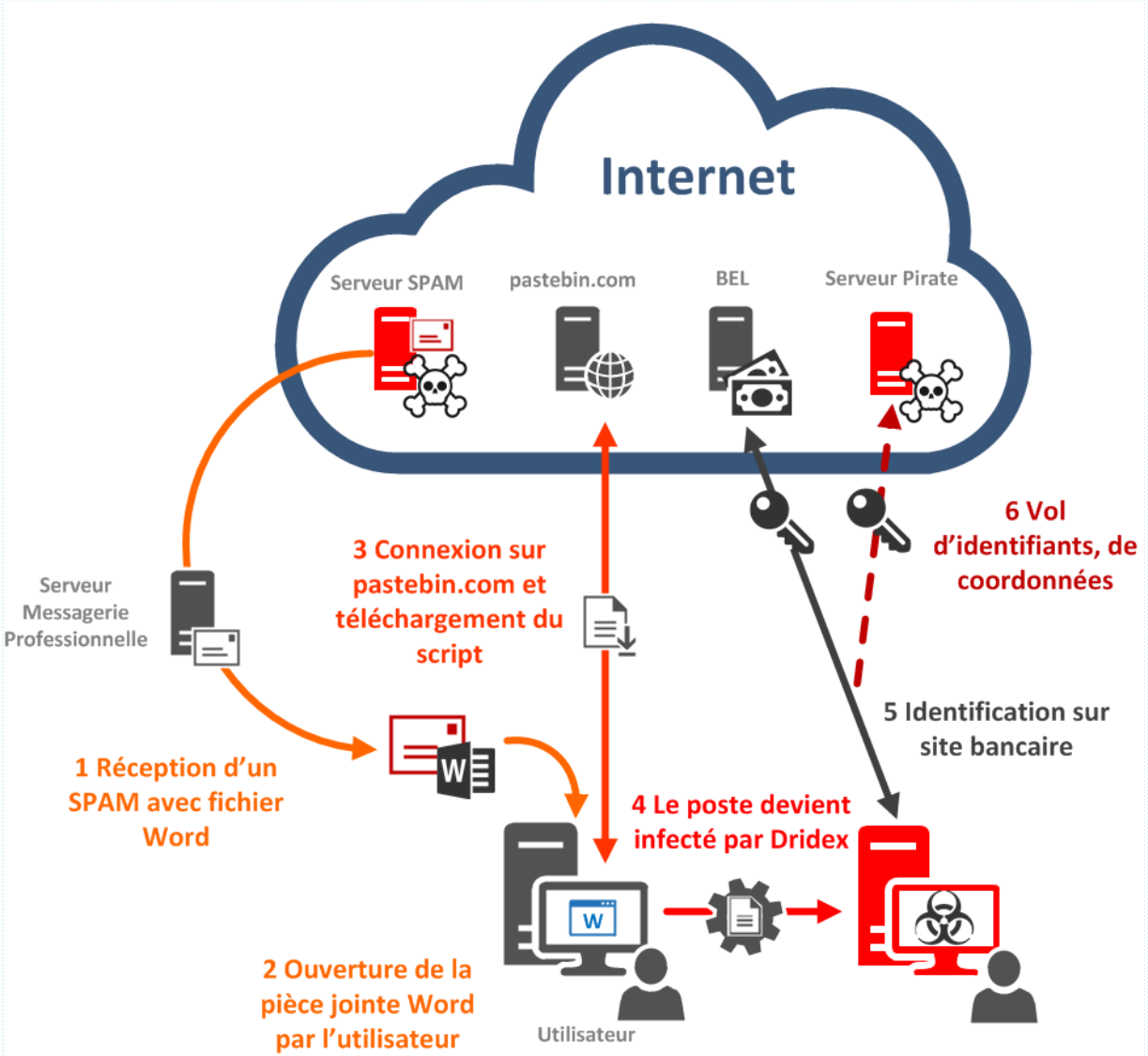
⇨ Et toutes les autres

Malware Star - Dridex

2014

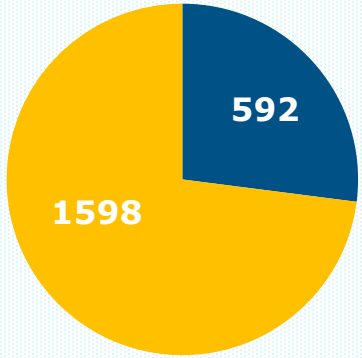
- L'utilisateur reçoit un mail avec une pièce jointe piégée au format Word
- L'utilisateur ouvre la pièce jointe ce qui déclenche l'exécution d'une macro
- La macro télécharge un fichier sur Internet contenant un script malveillant et l'exécute.
- Ce script télécharge à son tour un fichier exécutable (sur un serveur malveillant) et le lance.
- Cet exécutable (nommé « botnet 120 ») une fois installé reste persistant sur la machine et télécharge le malware Dridex
- Le malware Dridex surveille les actions de l'utilisateur notamment les navigations sur les sites bancaires ou de réseaux sociaux. Si une connexion sur l'un de ces sites est effectuée, les identifiants utilisés sont alors envoyés sur un serveur malveillant.

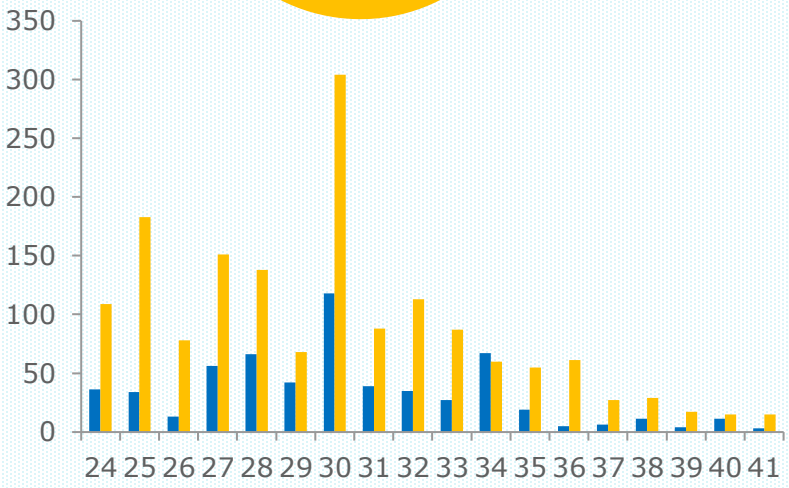
Malware Star - Dridex



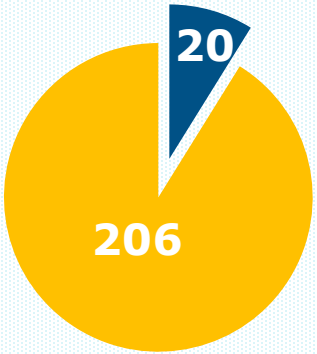
Malware Star - Dridex

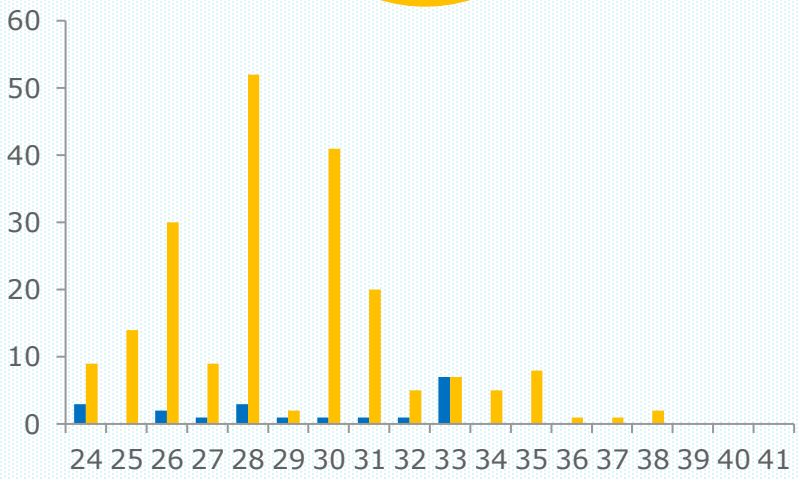
Détections des fichiers « factures » .doc (semaines 24 à 41)





Détections des scripts liés à Dridex .vbs (semaines 24 à 41)





Malware Star - WANNACRY

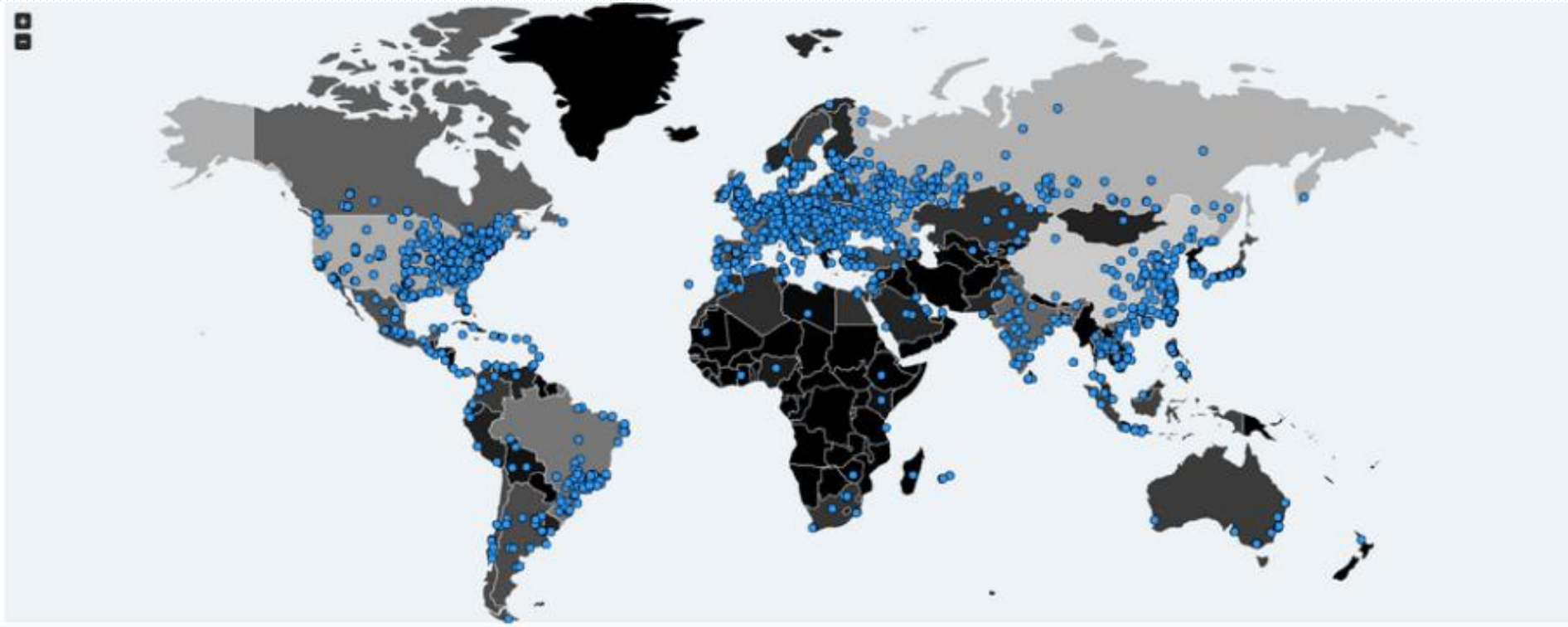
2017

- ***La plus grande infection de type Ver-Ransomware de l'histoire d'Internet***
- Cyberattaque mondiale massive faisant plus de 300 000 victimes
- 15 pays touchés
- Entreprises touchées : Vodafone, FedEx, Renault, Telefonica, le ministère de l'intérieur russe,…

Principales étapes de l'attaque …

- Exploitation d'une faille nommée ETERNALBBLUE dans le système Windows, plus précisément sur le service SMB (Server Message Block)
- Chiffre le contenu du poste de travail pour le rendre inaccessible à son propriétaire
- Déploiement d'un cheval de Troie nommé DoublePulsar afin de corrompre les copies automatiques de récupération de Windows pour rendre toute récupération de fichiers impossible.
- Réclamation d'une rançon allant de de 300 à 600 dollars

Malware Star - WANNACRY



Source : Malwaretech

Malware Star - WANNACRY

Impacts

- ⇨ Des millions de machines vulnérables car non mises à jour
- ⇨ Des entreprises touchées de manière automatique, distante, sans aucune interaction utilisateurs , dû à des failles d'exposition de leurs services SMB.
- ⇨ Des milliards de fichiers chiffrés
- ⇨ Un test grandeur mondiale du Patch management et des Sécurisations réseaux.
- ⇨ Une évolution et une mutation du code malveillant permettant de le rendre plus agressif

Malware Star - STUXNET

2010

- ⇨ Malware possédant plusieurs modules : Ver / Raccourci Fichier / Rootkit.
- ⇨ Dédié à l'attaque du programme nucléaire iranien.
- ⇨ Spécifique à des systèmes SCADA, et plus particulièrement les contrôleurs logiques programmables (PLCs).
- ⇨ Embarque l'exploitation de 4 failles 0-Day.

  - Infection initiale d'un système Windows via les 0-day présents dans le ver
  - Diffusion par Clé USB, et scan réseau interne
  - Recherche d'un logiciel « Step7 » de Siemens sur les PC infectés.
  - Infection du PLC relié
  - Modification des fréquences PLC et vitesse de rotation des moteurs

Malware Star - STUXNET

Impacts

- ⇨ Un cinquième des centrifugeuses nucléaires iraniennes détruites.
- ⇨ Perte de contrôle de la puissance virale. Infection de PC hors périmètre initial (Installation de Natanz).
- ⇨ 200,000 PC infectés, provoquant une dégradation physique de 1000 machines.
- ⇨ Impacts cyber dans le monde physique.

Attaque - Décryptage

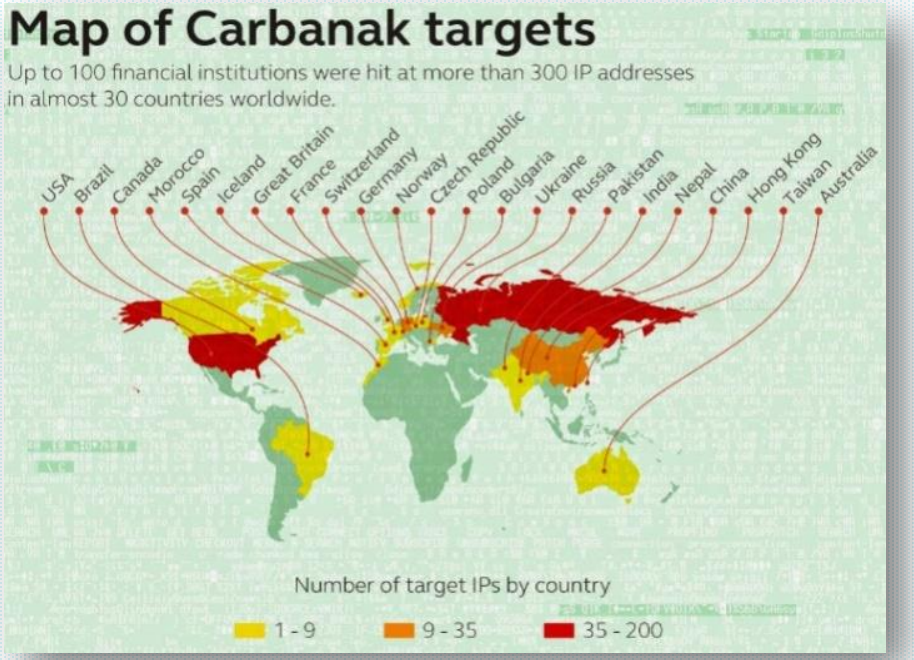
- CARBANAK
- TV5 Monde
- Hôpital US
- SWIFT
- VODAPHONE
- TF1
- CODE SPACE
- ORANGE
- TARGET

Décryptage : CARBANAK

2013

Décryptage : CARBANAK

- ⇨ 100 banques impactées (Russie, USA, Allemagne, Chine et Ukraine) en 2014
- ⇨ Pirates situés en Russie et en Chine
- ⇨ Espionnage des procédures internes des Banques pour procéder aux transferts
- ⇨ **1 Milliard** de dollars volés
- ⇨ Durée de la campagne entre 2 et 6 mois
- ⇨ ….

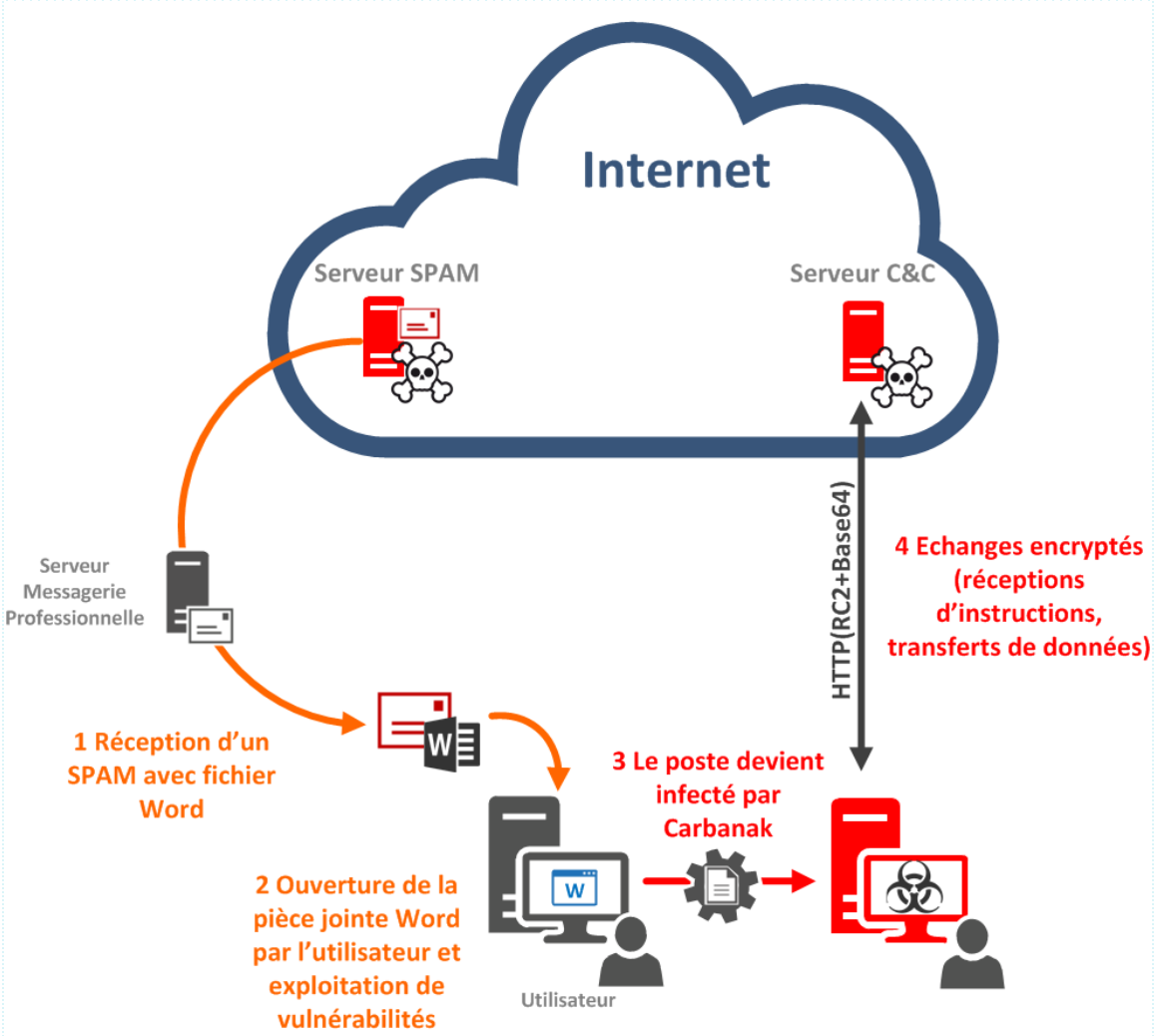


Décryptage : CARBANAK

Méthodes d'infection: 1 Campagne de SPAM

- ⇨ L'utilisateur reçoit un mail d'apparence légitime avec une pièce jointe piégée au format Word ou une avec une archive WinRAR (contenant un fichier CPL – applet du panneau de configuration)
- ⇨ L'utilisateur ouvre la pièce jointe qui exploite alors des vulnérabilités connues (ex: dans Microsoft Office)
- ⇨ La vulnérabilité exploitée permet l'exécution de code distant qui installe la Backdoor Carbanak
- ⇨ La machine infectée peut alors dialoguer avec un serveur de Command & Control (C&C) par l'intermédiaire de requêtes HTTP encryptées (RC2+Base64) et obfusquées pour recevoir ses instructions.

Décryptage : CARBANAK

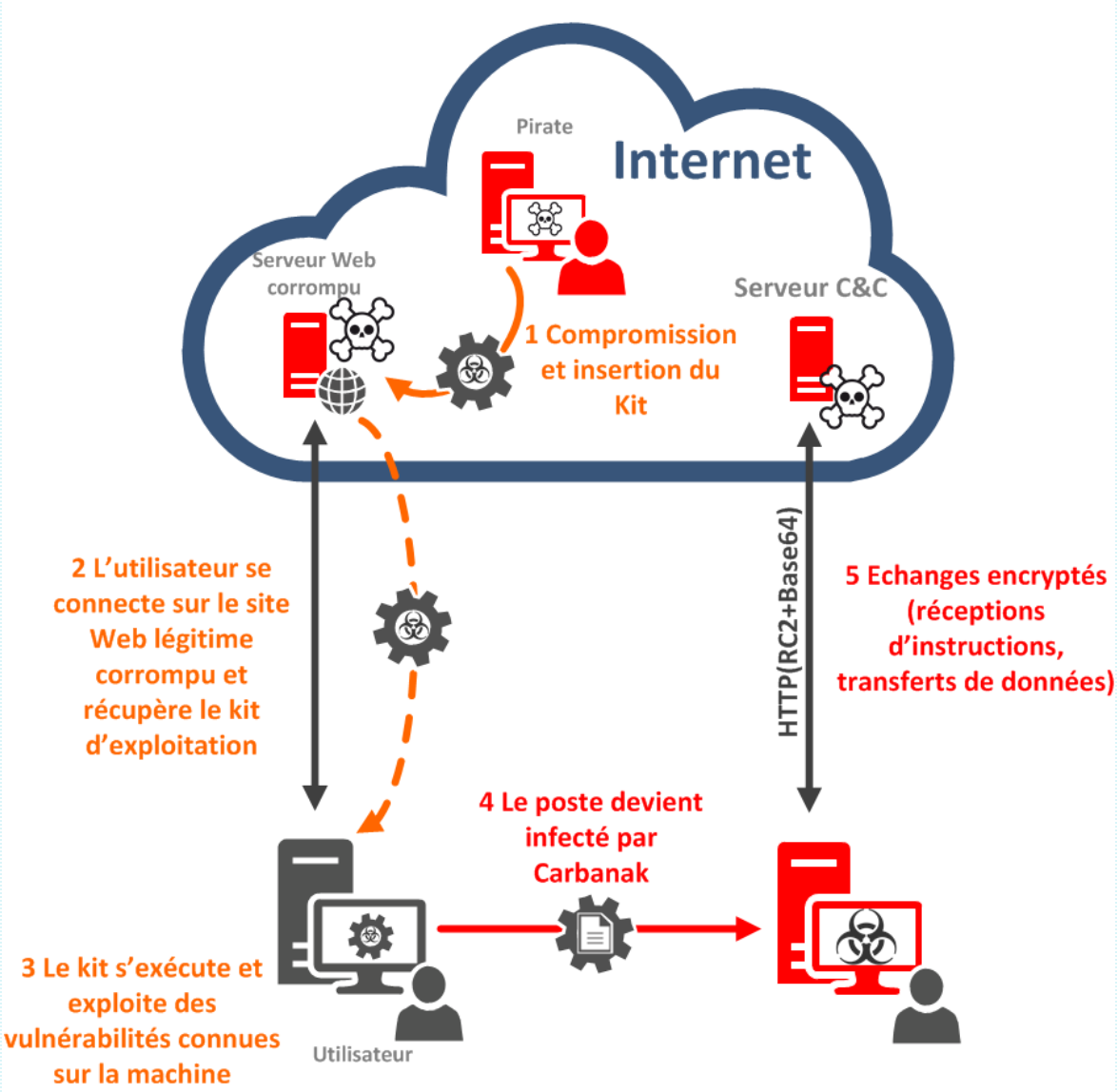


Décryptage : CARBANAK

Méthodes d'infection: 2 Téléchargement intempestifs

- ⇨ Compromission par les pirates de sites Web légitimes pour y insérer un Kit d'exploitation (RedKit)
- ⇨ L'utilisateur surfe sur le site web compromis et télécharge le kit à son insu
- ⇨ Le kit s'exécute et exploite alors des vulnérabilités connues
- ⇨ La vulnérabilité exploitée permet l'exécution de code distant qui installe la Backdoor Carbanak
- ⇨ La machine infectée peut alors dialoguer avec un serveur de Control &Command (C&C) par l'intermédiaire de requêtes HTTP encryptées (RC2+Base64) et obfusquées pour recevoir ses instructions

Décryptage : CARBANAK



Décryptage : CARBANAK

1. *Renseignements & Reconnaissance*

2. *Phishing*

3. *Collecte d'informations*

4. *Prise de contrôle de composantes du SI*

5. *Modification des systèmes anti-fraude*

Décryptage : CARBANAK

Impacts

⇨ **Compromission des bases de données Oracle** utilisées par les applicatifs SWIFT

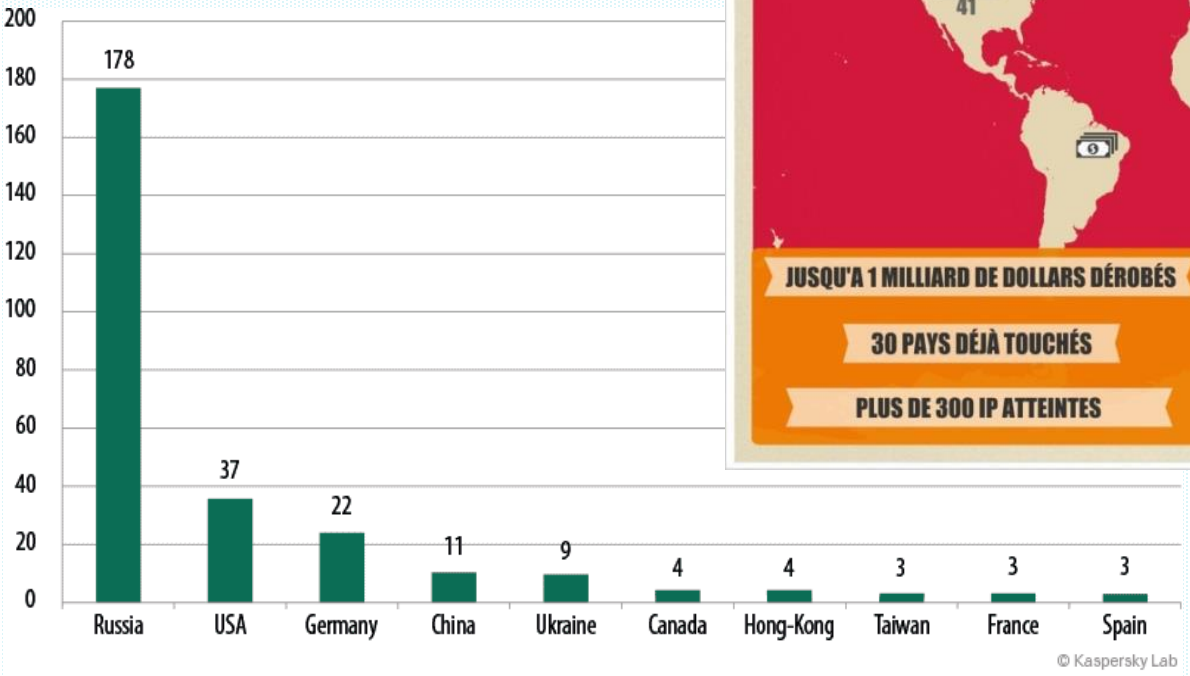
- Génération de transactions fictives en aval des étapes de vérification, création de transactions frauduleuses …
- Envoi des fonds sur des comptes ouverts frauduleusement, puis de ces comptes vers d'autres plus nombreux, puis vers des comptes de carte de crédit (de 600 à 7000 transactions par victime)

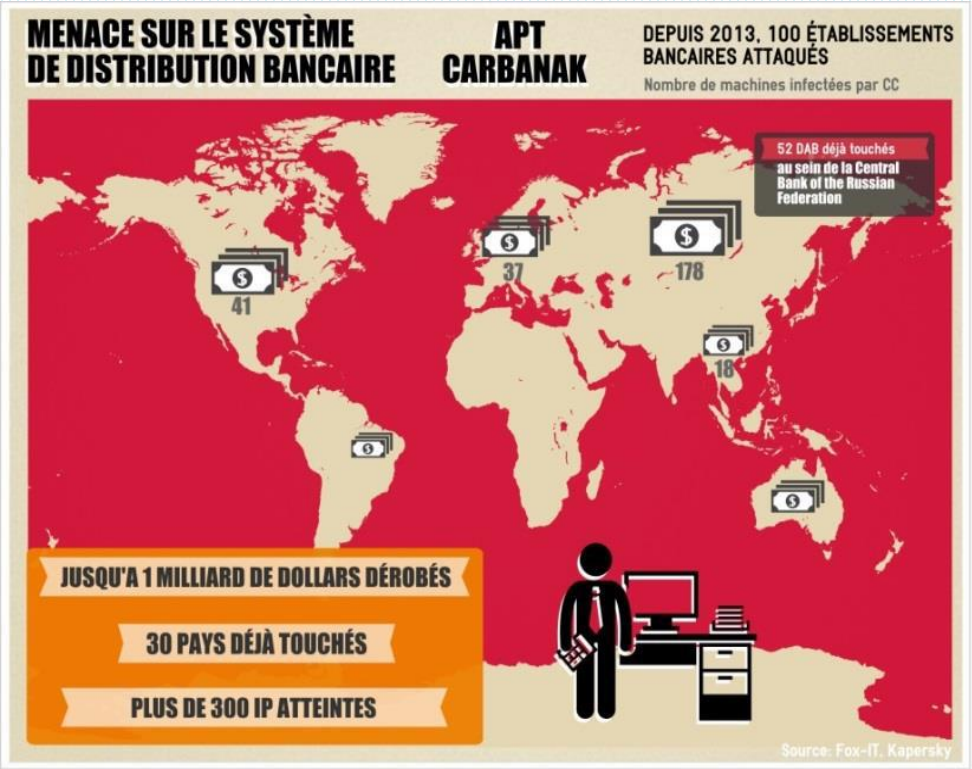
⇨ **Compromission des systèmes d'exploitation** des distributeurs de billets

- WINCOR: exploitation d'une faille permettant d'inverser l'index des montants des billets contenus dans les cassettes (100 roubles vs 5000 roubles) : 52 appareils piratés en Russie pour 50 M roubles (1 € = 70 roubles)
- Ejection de billets des distributeurs à heure fixe et récupération par des « mules »

Décryptage : CARBANAK

Situation





Décryptage : TV5 monde

2015

Décryptage : TV5 monde

Constats & premières actions

Le 08 Avril 2015 au soir:

- ⇨ Piratage des comptes de réseaux sociaux : Facebook, Twitter, Google+…
- ⇨ Défaçage du site Web
- ⇨ Diffusion de messages de menaces sur les intérêts Français et publication de données (en partie publique) de divers mairies
- ⇨ Arrêt de diffusion de la chaîne dans le monde entier
- ⇨ Perte de la messagerie
- ⇨ Sollicitation immédiate des experts de l'ANSSI pour confinement et enquête forensic
- ⇨ Reprise partielle des activités le 09 Avril vers 18h

Décryptage : TV5 monde

Origines

- ⇨ Attaque revendiquée par le groupe « CyberCaliphate » apparemment affilié à Daesh
- ⇨ Plus tard une deuxième piste désignerait un groupe de pirates russes: « APT28 » ou « Pawn Storm » car les méthodologies employées étaient semblables aux leurs
- ⇨ « CyberCaliphate » pourrait être une diversion

Décryptage : TV5 monde

Objectifs visés

- ⇨ Détruire la chaîne de télévision
- ⇨ TV5 Monde est diffusé dans plus de 200 pays dont certains du Maghreb et du Moyen-Orient,
- ⇨ Contrôler un média pour y véhiculer de la propagande : vu par 260 Millions de foyers
- ⇨ Cibler TV5 permet de menacer la France (contester les opérations militaires, …)

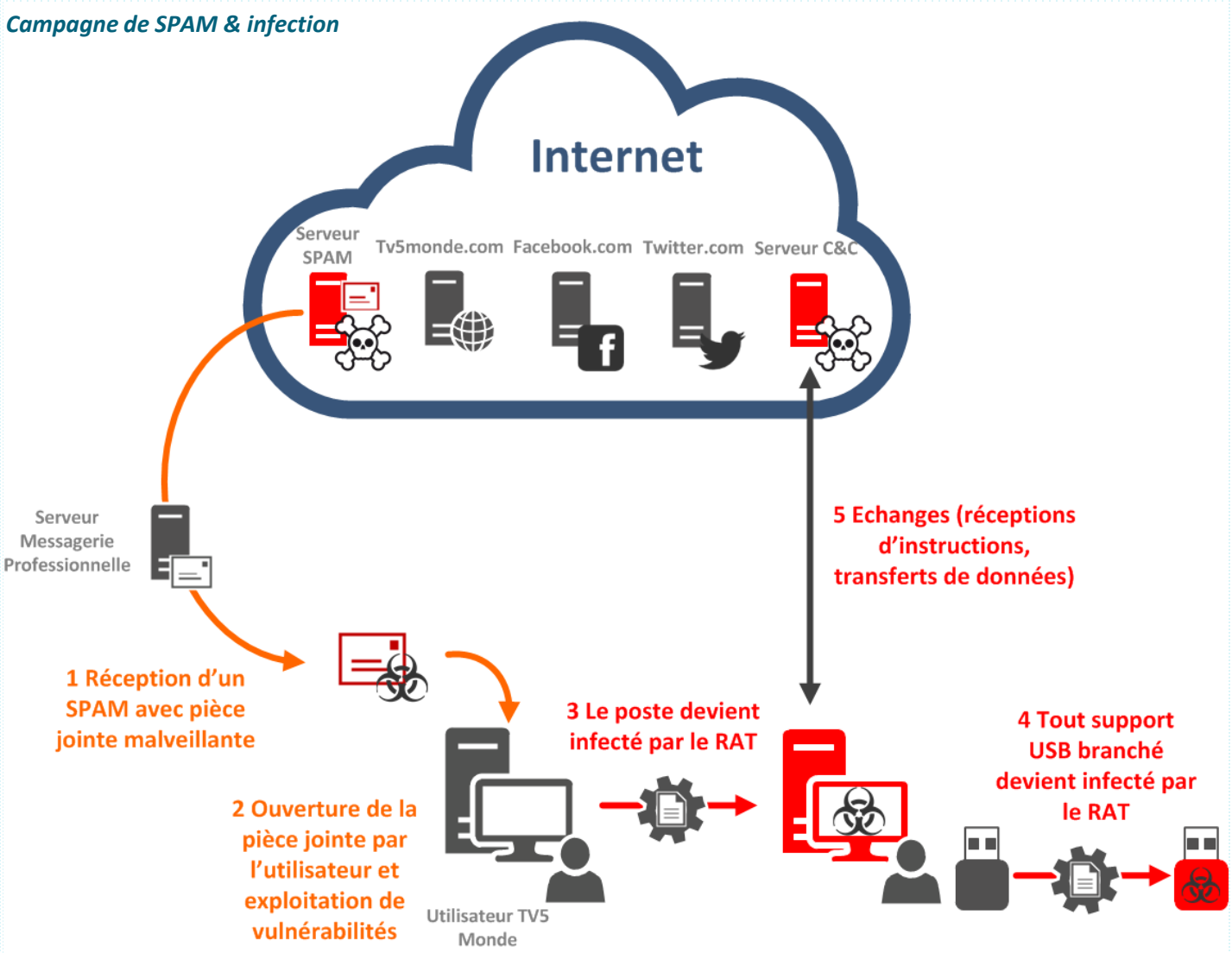
Décryptage : TV5 monde

Déroulement de l'attaque

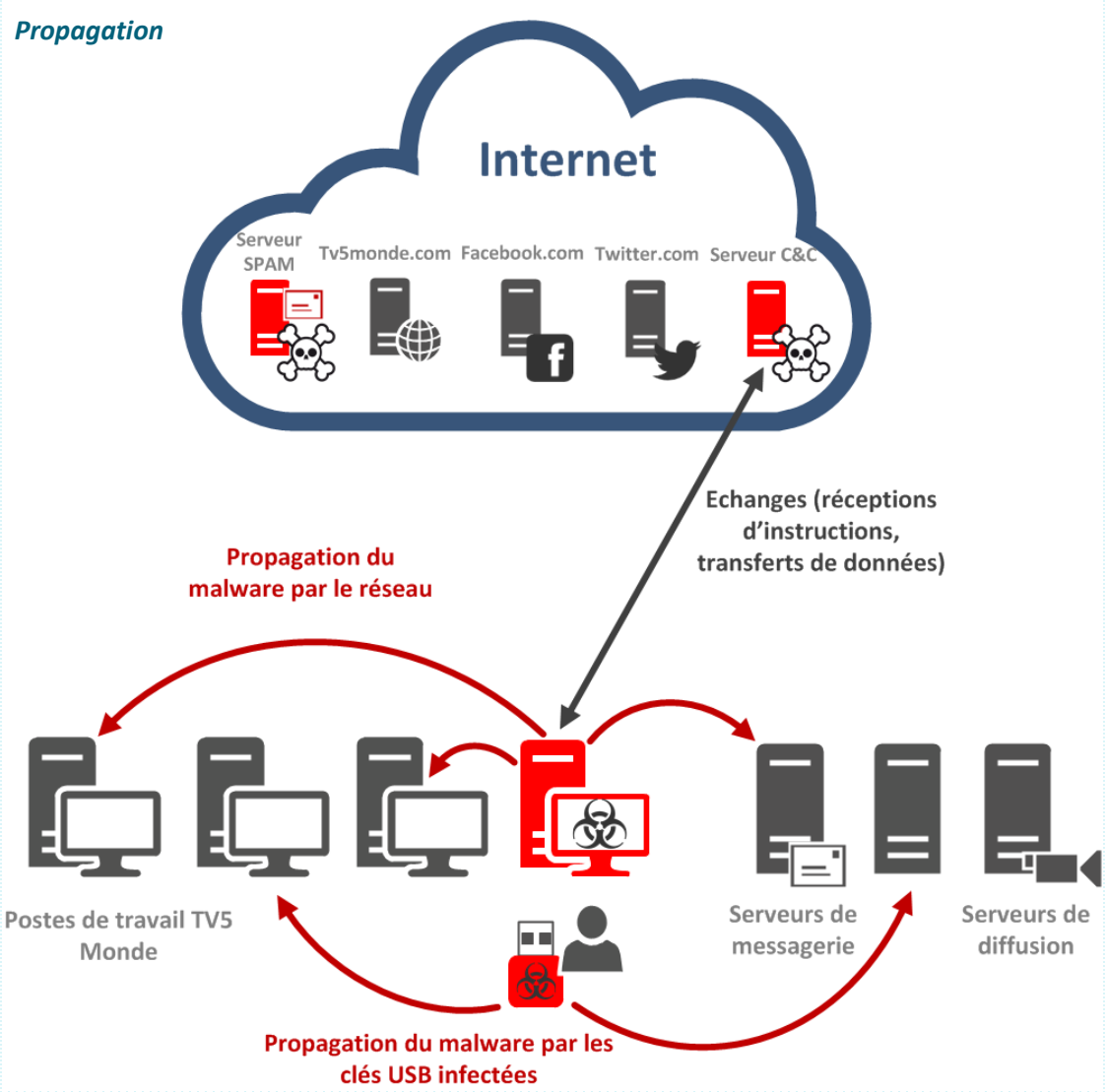
- Campagne de SPAM avec pièces jointes malveillantes à destination des journalistes et collaborateurs de TV5 Monde
- La pièce jointe serait un RAT - Remote Access Trojan - propagé dans tout le SI de la chaîne, récoltant au passage bon nombre d'informations (Adresses IP, OS, comptes, mots de passe etc…). Le malware se diffusait également par le biais des clés USB.
- Piratage des comptes de réseaux sociaux de la chaîne par les pirates eux-mêmes (après exfiltrations de données, ingénieries sociales ou encore attaques par brute force…)
- infection du cœur du SI, les serveurs de diffusion de la chaîne et provoqué un dénis de service de transmission
- Dénis de service de la messagerie interne, suppression des mails (forte probabilité d'exfiltration de mails et de comptes)

Décryptage : TV5 monde

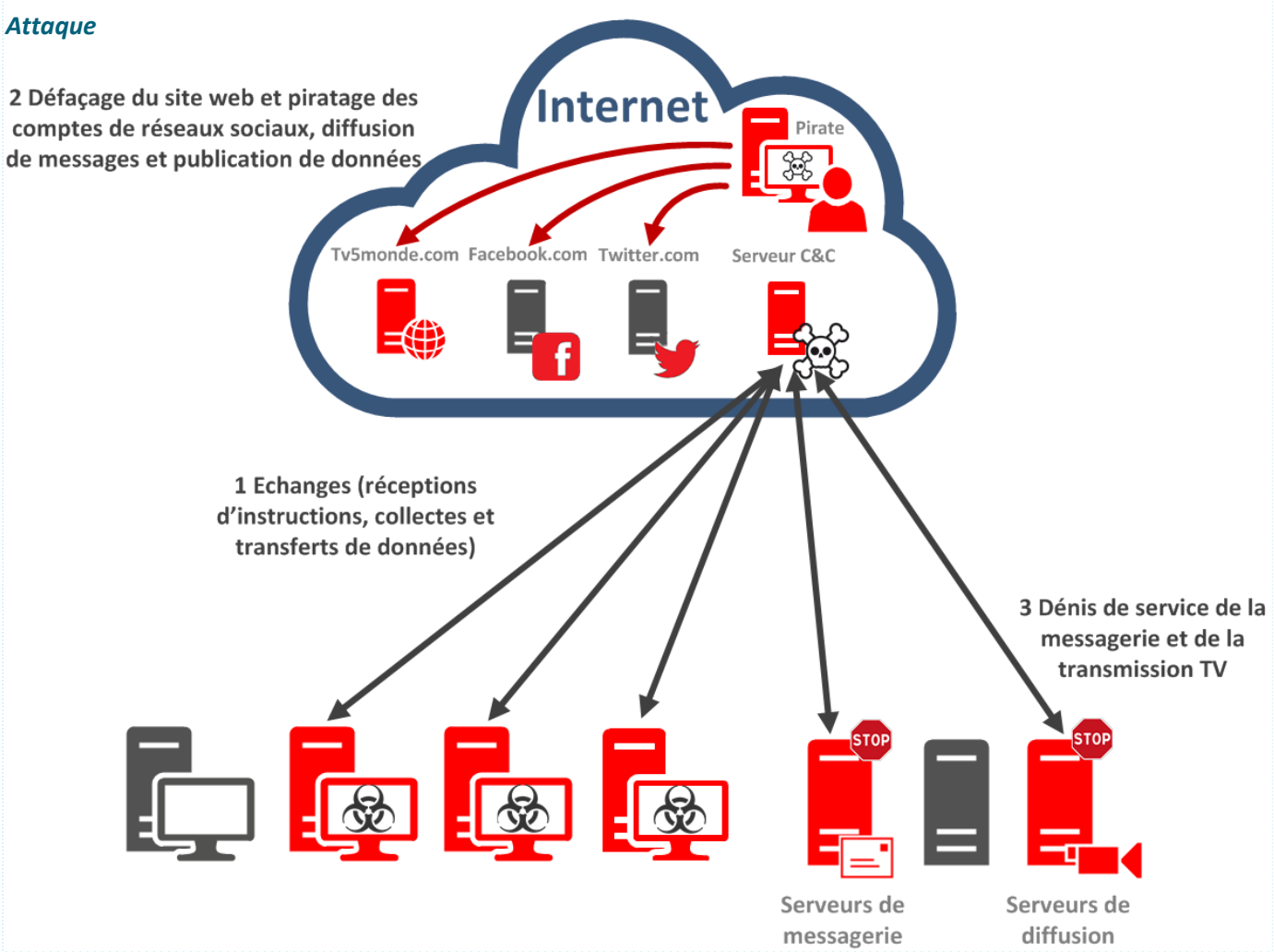
Campagne de SPAM & infection



Décryptage : TV5 monde



Décryptage : TV5 monde



Décryptage : TV5 monde

Points de faiblesses

- ⇨ Utilisateurs mal sensibilisés aux problématiques de sécurité : Campagne de SPAM ciblée
- ⇨ Politique de mots de passe inadaptée: Mots de passe faibles affichés sur les murs de la chaîne (ex: « lemotdepassedeyoutube »)
- ⇨ Faible cloisonnement du SI, ne disposant que d'un seul pare-feu
- ⇨ La chaîne n'applique pas les principes de défense en profondeur
- ⇨ Non prise en compte des avertissements de présences de failles:
  - ANSSI 15 jours auparavant
  - ZATAZ 9 alertes depuis 2013

Décryptage : TV5 monde

Impacts entreprises

- ⇨ Impact Business: Pertes de contrat
  - Des contrats (USA, Japon…) imposaient une continuité H24 des diffusions
  - Dès la première heure d'interruption, le canal TV5 Monde a été réattribué à une autre chaîne

- ⇨ Impact financier: Investissement dans la sécurité
  - 5 Millions d'euros en 2015
  - 3 Millions en 2016
  - 2 Millions récurrent à partir de 2017

Décryptage : Hôpital US

Cryptolocker dans l'hôpital (US)

Impact

- ⇨ Retour aux échanges par fax !!!
- ⇨ Hôpital paralysé pendant 10 jours qui avait dû envoyer ses patients vers d'autres centres de soin,

Mode opératoire

- ⇨ Pièce jointe dans un mail professionnel contrefait
- ⇨ Chiffrement des annuaires permettant l'échange des dossiers médicaux

Décryptage : SWIFT

SWIFT …

Impact

- ⇨ Détournement de 81 Millions de $
- ⇨ Perte de confiance dans l'établissement bancaire

Mode opératoire

- ⇨ Des identifiants internes ont été compromis et utilisés pour accéder aux systèmes liés au transfert d'argent (SWIFT)
- ⇨ Modification du logiciel de Swift sur les serveurs de la banque pour dissimuler des transactions frauduleuse
- ⇨ Malware pour modifier les rapports d'émission (au format PDF) afin de masquer les activités

Décryptage : SWIFT

- Mars 2016 : on apprend par les médias que 81 millions de dollars en provenance du Bangladesh ont disparu de la circulation.

- 15 mai 2015 : ouverture de 4 comptes bancaires à la RBC (Philippines) sous de fausses identités .
- 4 et 5 Février 2016, 35 transactions SWIFT sont frauduleusement exécutées par la Banque Centrale du Bangladesh à destination de la RCBC. 30 de ces transactions sont bloquées, mais 5 finissent par «passer».
- Les attaquants ont utilisé un Malware avancé qui ciblait spécifiquement l'établissement. Il a été créé sur mesure, les attaquants avaient une connaissance approfondie du logiciel SWIFT.
  - Un Malware personnalisé a été injecté dans le SI de la Banque Centrale du Bangladesh
  - Introduction dans le système, et observation des actions pendant plusieurs semaines.
  - Envoi de fausses instructions de Paiement pour effectuer les transferts
  - Effacement des traces de transferts.

Décryptage : VODAPHONE

Indélicatesse chez un prestataire : Vodaphone

Impact

- ⇨ Septembre 2013 : Un prestataire des systèmes de Vodafone exfiltre 2 millions de données clients et bancaires. 6% des clients (Allemagne) sont touchés !
- ⇨ Octobre 2015 : Une seconde attaque via un fournisseur touche 1827 clients

Mode opératoire

- ⇨ Les données contenues dans les bases de données sont exfiltrées via des supports externes, pour à terme être revendues sur le marché.

Décryptage : TF1

Vulnérabilité Site WEB : TF1

Impact

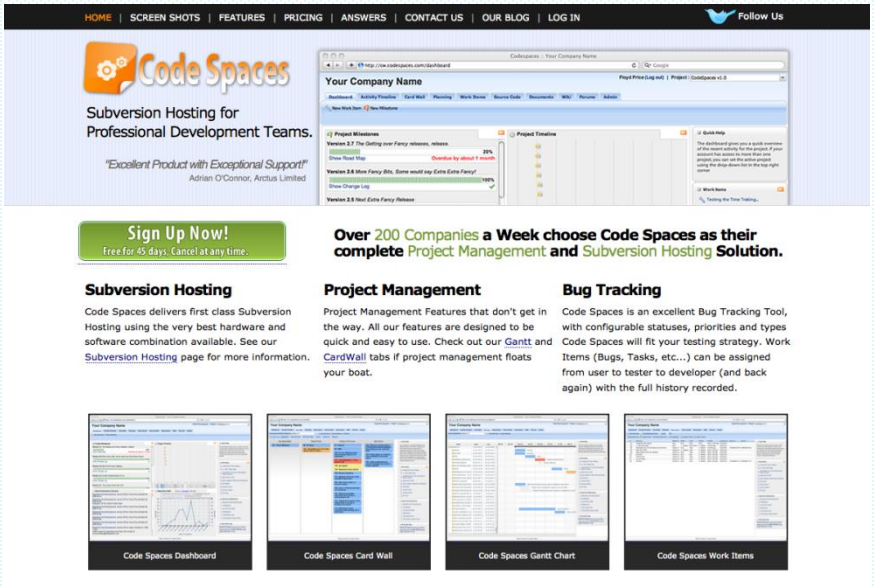
- ⇨ Vol de 1,9 millions de données clients
- ⇨ TF1 doit se mobiliser pour expliquer l'attaque à travers une forte mobilisation en matière de communication

Mode opératoire

- ⇨ Janvier 2015 : Des pirates trouvent 2 failles SQL sur le site TF1.fr, notamment sur une partie gérée par leur partenaire ViaPresse.

Décryptage : Code Space

Service Cloud : Code Spaces



Impact

⇨ Quasi disparition de la société Code Spaces en quelques semaines.

Mode opératoire

⇨ Juin 2014 : le Cloud de Code Spaces ciblé et les attaquant prennent le contrôle du S.I. (Administration).

⇨ Après chantage: suppression des données clients ainsi que les backups internes/externes…

Décryptage : Orange

Service de marketing externalisé : Orange

Impact

- ⇨ Les données personnelles de 1,3 millions de clients dérobées
- ⇨ La CNIL met en avant un défaut d'encadrement des sous-traitants…

Mode opératoire

- ⇨ Une simple modification d'adresse Internet (URL) a permis l'accès aux données

Décryptage : Target

Accès au SI par des tiers : Target

Impact

- ⇨ Vol de 40 millions de données cartes bancaires et de 70 millions d'identités clients
- ⇨ Plus de 250 M$ de coût pour la chaîne de magasins, une forte dégradation de l'image de marque

Mode opératoire

- ⇨ Décembre 2013 : les attaquants cherchent à pénétrer le SI de Target en utilisant son sous-traitant gérant la climatisation : Fazio Mechanical Services
- ⇨ Le portail de gestion des achats protégé par un mot de passe, facilement volé chez FMS, a servi de porte d'entrée