WAVESTONE

Cyberattaques en France : quelle situation sur le terrain ?

CERT-Wavestone

Septembre 2018 – Août 2019

Dans un monde où la capacité à se transformer est la clé du succès, nous éclairons et guidons nos clients dans leurs décisions les plus stratégiques

Des clients leaders dans leur secteur

3 000 collaborateurs dans 8 pays, dont 500 dédiés à la cybersécurité

Parmi les leaders du conseil indépendant en Europe, n°1 en France

Paris | Londres | New York | Hong Kong | Singapour* | Dubaï* | São Paulo*
Luxembourg | Madrid* | Milan* | Bruxelles | Genève | Casablanca | Istanbul* | Edimbourg
Lyon | Marseille | Nantes

* Partenariats

Analyse des cyberattaques touchant les grandes organisations

40

incidents de sécurité majeurs

ayant mené à l'interruption d'activités métiers ou une compromission avancée du système d'information

Parmi les plus grandes entreprises et institutions Françaises

- ✓ Industrie
- ✓ Technologies de l'information
- ✓ Secteur Public
- ✓ Finance
- ✓ Agroalimentaire
- ✓ Services

Une étude réalisée sur la base des interventions de **l'équipe de réponse à incidents de sécurité de Wavestone** entre Septembre 2018 et Août 2019

CERT

Le CERT-Wavestone

40 experts cyber crise

Investigation numérique

Gestion de crise

Analyse de malware

Analyse de la menace cyber

Mobilisable en 24/7

Organisation en 3x8 lors des crises cyber de grandes envergures

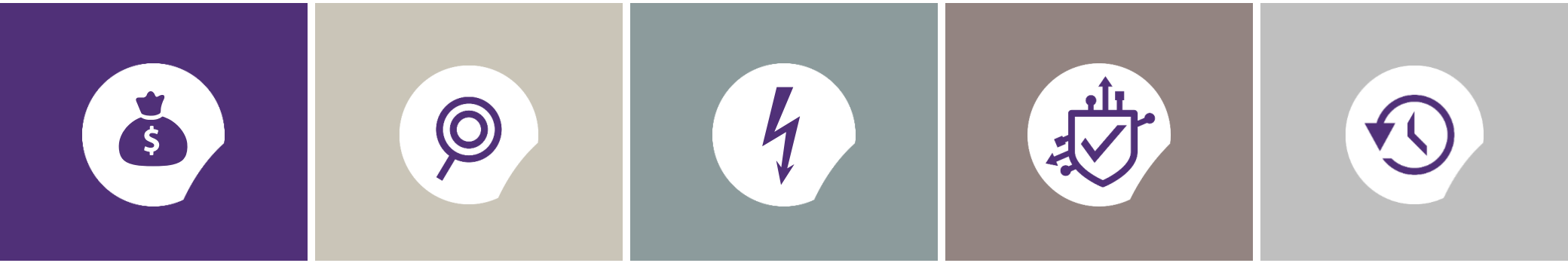
Multi-clients

+25 grandes organisations abonnées

Expert gestion de crise pour plusieurs cyber-assurances

Benchmark des réponses à incidents de sécurité

Une volonté d'éclairer sur l'état de le menace cyber en France
et de partager les clés pour une meilleure anticipation et réaction



Quelles sont les motivations des cyberattaquants ?

Quand et comment ont-ils été découverts ?

Comment se sont-ils introduits dans les systèmes ?

Comment les affronter et gérer la crise ?

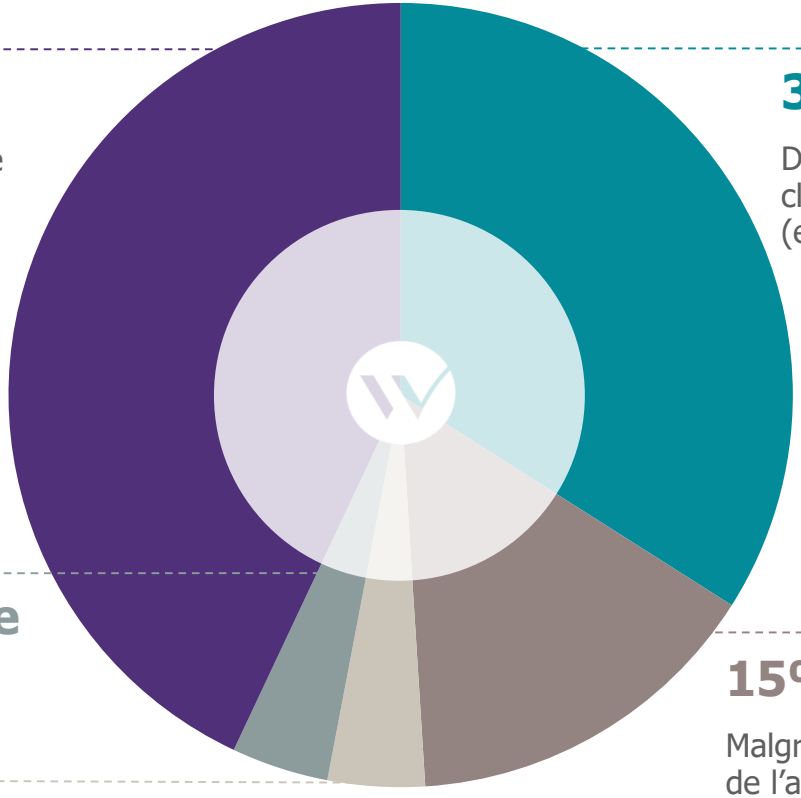
Comment se préparer en amont ?

L’appât du gain financier, le moteur principal des cybercriminels

Répartition des incidents de sécurité par motivation des attaquants

43% Gains financiers

Dont 36% d’attaques par ransomware et 7% de fraudes



34% Vol de données

Données métiers (e.g. coordonnées de clients, données bancaires…) et techniques (e.g. liste de comptes utilisateurs)

4% Nuisance à l’image

Défiguration de site web, vol de comptes sur des réseaux sociaux

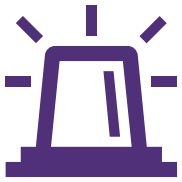
15% Indéterminée

Malgré la compromission, les motivations de l’attaquant n’ont pas pu être identifiées (attaque abandonnée, interrompue, compromission de systèmes sans actions ultérieures…)

4% Gains de capacité d’attaque

Détournement d’informations ou de ressources pour mener une attaque sur une autre cible

Des capacités de détection très hétérogènes parmi les grandes entreprises accompagnées



167 jours

Temps moyen écoulé entre une intrusion et sa détection

Mais encore…

50%

des entreprises détectent l'intrusion **dans les deux jours**

35%

des entreprises ne détectent l'intrusion que **dans les 6 à 9 mois**

6 ans

le **délai maximum** observé entre le début d'une attaque et sa détection par l'une des entreprises du panel…

Plus de 50% des attaquants ne disposent pas de compétences techniques avancées

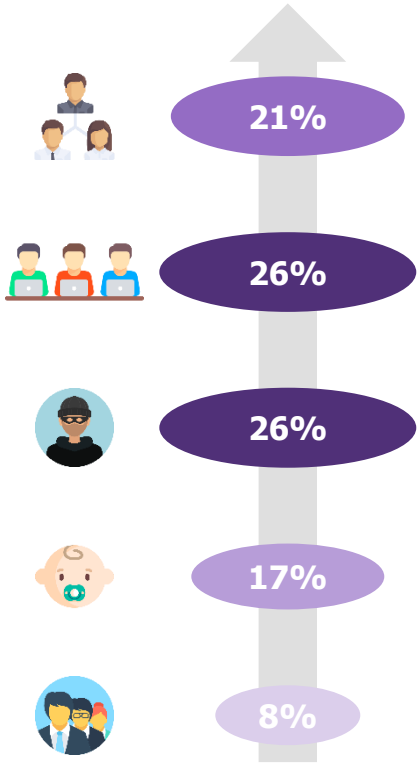
Quels types de menaces ?

65% menaces opportunistes : ne relèvent souvent pas d'un haut niveau de technicité ; ne visent pas une organisation en particulier, aussi si l'une est plus sécurisée qu'une autre, les attaquants passeront leur chemin pour se jeter sur la proie la plus facile.

30% menaces ciblées : visent des informations sensibles et précises dans l'organisation. Les attaquants sont mandatés avec un objectif clair. Ils mettent tous les moyens à disposition pour arriver à leurs fins.

5% menaces diffuses : correspondent aux habituelles infections virales ou encore au spam ; ne visent pas une organisation en particulier et ont un effet limité sur le SI : déni de service, perte de données utilisateurs…

Quels profils attaquants ?



Organisations rodées
e.g. groupe mafieux développant ses propres outils offensifs pour mener à bien ses attaques

Groupes d'individus
e.g. équipe de pirates capables de dérouler une méthodologie offensive en utilisant des outils du marché

Cybercriminel
e.g. individu achetant des services de piratage sur étagère

Script kiddies
e.g. étudiants réutilisant des codes d'exploitation et outils publics

Internes
e.g. Collaborateurs malveillants

Les mêmes portes d'entrée sont régulièrement utilisées par les attaquants

1 cas sur **10**

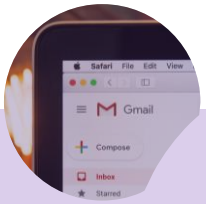
L'attaquant s'est infiltré dans le SI en exploitant un **service RDP exposé**

RDP est un mécanisme standard permettant l'accès à distance à des systèmes informatiques

1 cas sur **3**

L'attaquant a exploité une **application web vulnérable**

100% des applications web sont vulnérables selon le benchmark audit de Wavestone (wavestone.com)



1 cas sur **10**

L'attaquant s'est infiltré dans le SI par **un spear-phishing**

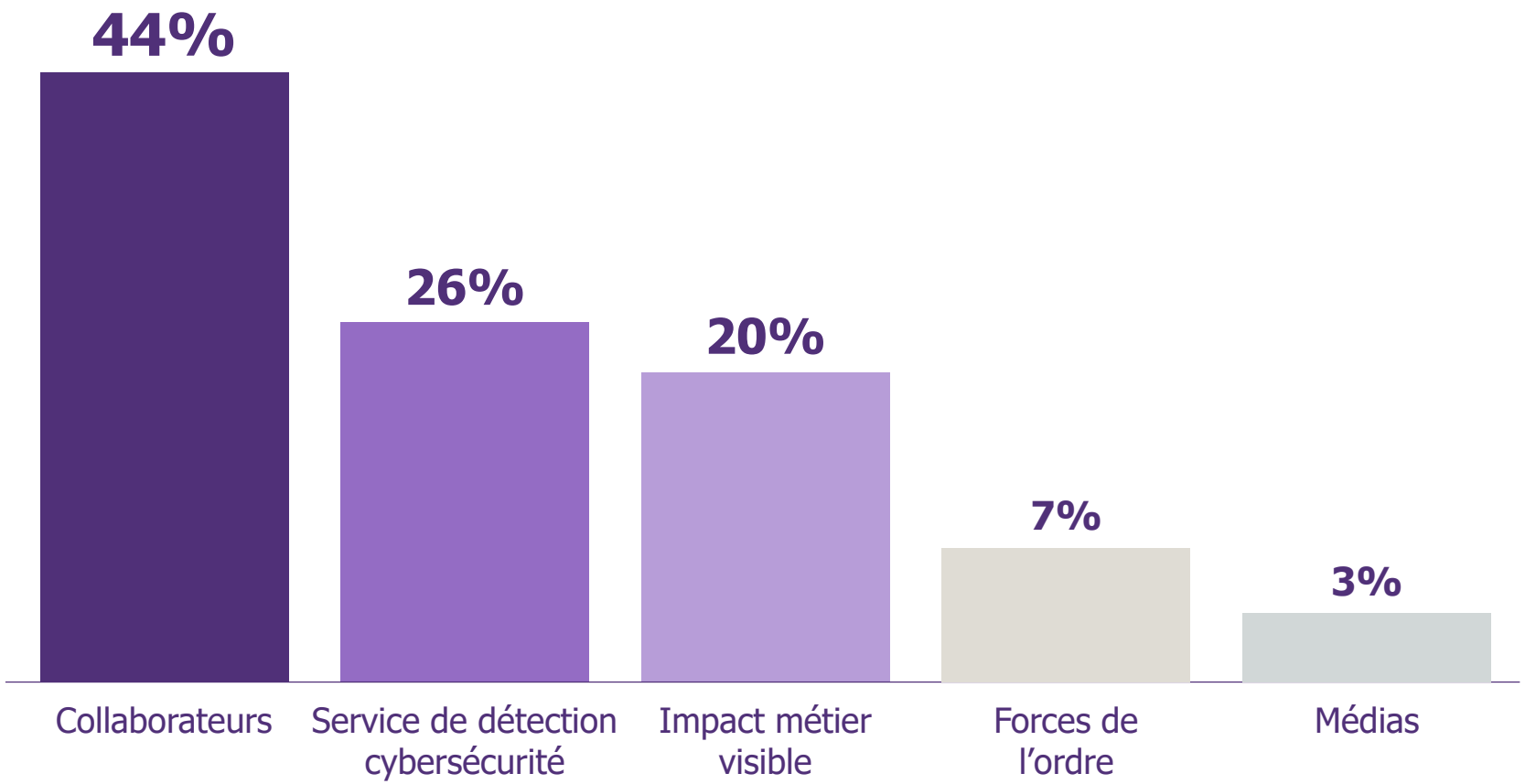
Un spear-phishing est un phishing ciblé : il vise une entreprise précise ou un groupe d'utilisateurs particuliers

Dans **20%** des cas, l'identification du vecteur d'intrusion n'a pas été possible :

- **Traces techniques insuffisantes**
- **Systèmes décommissionnés ou détruits**
- **Manques de ressources locales**

Les utilisateurs finaux : la clé de voute de la détection des attaques

Répartition par source de détection des incidents de sécurité



Les équipes pour piloter la résolution de la crise

12
personnes en moyenne

440
personnes au maximum

Dont
25%
de prestataires en moyenne

Combien de temps pour un retour à une **situation technique normale ?**

1 semaine

Pour un ransomware « simple » (i.e. sans propagation)

3,5 semaines

Pour une attaque ou un ransomworm ayant détruit une partie importante du système d'information

Et au moins 6 semaines pour une reconstruction saine, avec deux actions clés :

Reconstruction du cœur de confiance du SI pour bascule vers un nouvel environnement sain sur un week-end
Nettoyage et réimportation des données métiers créées pendant la crise

Un frein majeur au cœur de la crise !

Des difficultés notoires à récupérer des données sauvegardées… due à une indisponibilité du serveur de sauvegarde (destruction et perte du catalogue des sauvegardes) ou une perte d'intégrité des sauvegardes (infection antérieure à la sauvegarde la plus ancienne)

Le serveur de sauvegarde n'est jamais sauvegardé…

Comment éviter de devenir une cible ?

65%
des attaques sont opportunistes

Être au-dessus de la moyenne en cybersécurité permet de limiter fortement son attractivité auprès des cybercriminels

TOP 5 des actions pour se préparer à faire face à une attaque

Protéger les actifs les plus critiques en adoptant les bonnes pratiques de sécurité (correctifs de sécurité, gestion des droits, gestion des administrateurs…)

Améliorer l'efficacité de la détection des attaques avec un service spécialisé (surveillance 24/7, périmètre de détection adapté à la menace…)

Savoir gérer une crise majeure (équipe 24/7, moyens de communication spécifiques…) **et reconstruire en urgence** (procédures, matériel spécifique…)

S'entrainer grâce à des exercices de crise (répéter les efforts en différentes situations pour favoriser le développement de réflexes)

Souscrire une cyber-assurance et un contrat auprès d'une équipe spécialisée (s'entourer des experts pouvant accélérer la résolution de l'incident)

WAVESTONE

Contacter le CERT-Wavestone

+33 (0)1.49.03.27.26

cert@wavestone.com
PGP : 1CFEDF1D

Notre équipe de réponse à incidents de sécurité et de gestion de crise disponible en 24/7

https://www.securityinsider-wavestone.com/

wavestone.com
@wavestone_

PARIS

LONDRES

NEW YORK

HONG KONG

SINGAPOUR *

DUBAI *

SAO PAULO *

LUXEMBOURG

MADRID *

MILAN *

BRUXELLES

GENEVE

CASABLANCA

ISTANBUL *

LYON

MARSEILLE

NANTES

* Partenariats

WAVESTONE