Cyberattaques en France : les ransomwares, toujours menace n°1

Par le CERT-Wavestone

Octobre 2021

The Positive Way

WAVESTONE

Wavestone

Nous accompagnons les grandes entreprises et organisations dans leurs transformations les plus critiques

Business & technologie

13 bureaux
dans 8 pays

CA
418 M€

+3 000
collaborateurs

Le CERT-Wavestone :
40 experts en crise cyber

En 24/7 durant une attaque...

- **Investigation numérique / Forensics**
  Analyses système, réseau, de code malveillant
- **Gestion de crise cyber et métier**
  Pilotage, anticipation, support à la communication interne et externe, appui aux notifications réglementaires
- **Défense du SI**
- **Remédiation & Reconstruction**
- ***Threat Hunting***

... mais aussi en amont

- **Organisation d'exercices de crise**
- **Simulation d'attaques cyber**
  red-team / purple-team
- **Définition, animation et formation CERT et SOC**
- **Veille cybercriminalité** Watch & Learn
- **Évaluation de l'attractivité de l'entreprise**
- **Analyse et décryptage d'attaques**

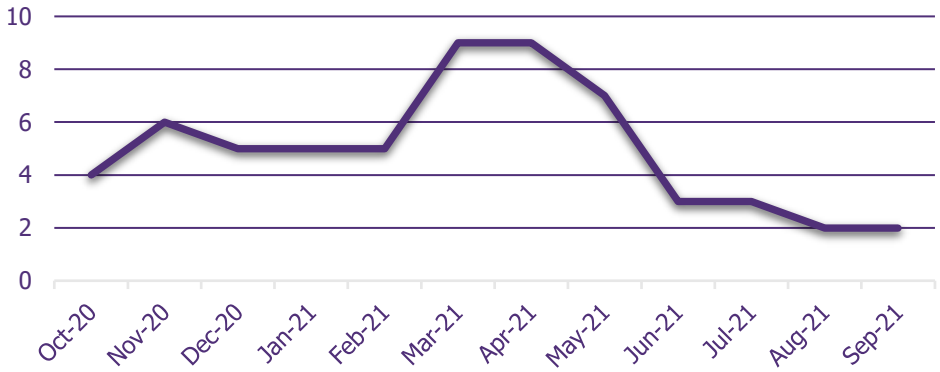
VISA DE SÉCURITÉ

Wavestone est la première entreprise à obtenir la qualification **Prestataire de Réponse aux Incidents de Sécurité** (PRIS) par l'ANSSI.

Qualification N°1443 |
Durée de 3 ans à compter du 29/06/2020

Bilan des cyberattaques gérées par le CERT-W

Nombre d'incidents majeurs par mois



Une **baisse sensible de l'activité** entre Juin et Septembre 2021

60 incidents de sécurité majeurs

(+15% de volume en nombre de jours vs 2020)

ayant mené à l'interruption d'activités métiers ou une compromission avancée du SI, dont 17 crises nécessitant un dispositif organisationnel spécifique

CERT

Une étude réalisée sur la base des interventions de l'équipe de réponse à **incidents de sécurité** de Wavestone entre Octobre 2020 et Septembre 2021

Benchmark
CERT - 2021

Benchmark des réponses à incident de sécurité

UNE VOLONTÉ D'ÉCLAIRER ET MONTRER L'ÉVOLUTION DE L'ÉTAT DE LA MENACE CYBER EN FRANCE, TOUT EN PARTAGEANT LES CLÉS POUR UNE MEILLEURE ANTICIPATION ET RÉACTION

Qui sont les attaquants et quelles sont leurs motivations ?

Comment se sont-ils introduits dans les systèmes ?

Quand et comment ont-ils été découverts ?

Combien de temps dure une crise majeure ?

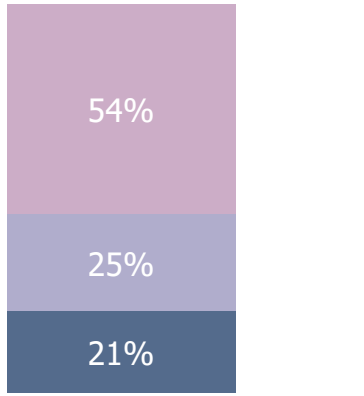
Comment se préparer pour limiter les impacts ?

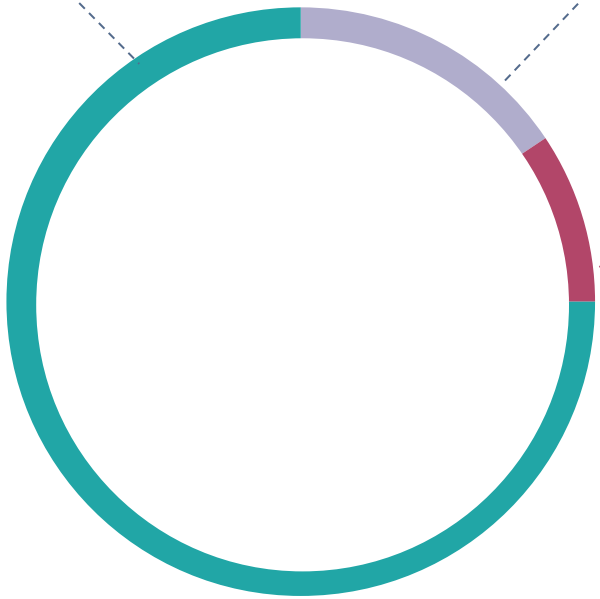
Le gain financier reste la première motivation des attaquants

RÉPARTITION DES INCIDENTS DE SÉCURITÉ PAR MOTIVATION DES ATTAQUANTS

Gains financiers (75%)

Les gains financiers peuvent être obtenus par des rançons pour débloquer le système d'information, des chantages à la non-divulgation des données ou par revente de données volées





Indéterminée (15%)

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

Gains de capacité d'attaque (10%)

Détournement d'informations ou de ressources pour mener une attaque sur une autre cible (spam/phishing, DDoS, supply-chain…)

Benchmark CERT - 2021

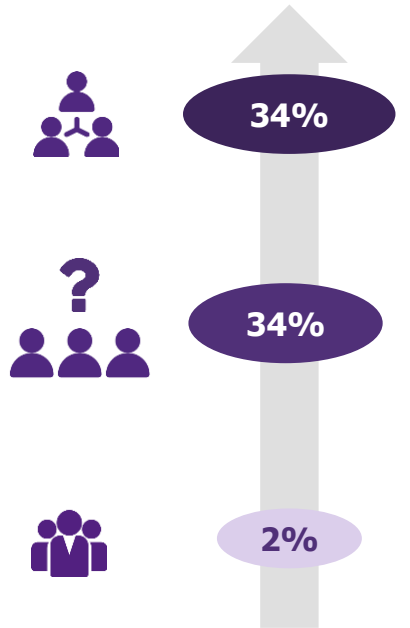
Des attaques très largement opportunistes menées par des groupes organisés

Quels types de menaces ?

57%

des attaques sont opportunistes, c'est-à-dire sont des attaques ne visant pas une organisation particulière.

Quels profils d'attaquants ?



Groupe organisé et connu
e.g. Conti, Ryuk, Revil…
(+4% vs 2020)

Groupe non déterminé ou cybercriminel seul
(-10% vs 2020)

Internes
e.g. (ex-) collaborateur malveillant
(-1% vs 2020)

Dans **30% des cas** **(+8% vs 2020)** il n'a pas été **possible de déterminer le profil**, généralement par manque de données à analyser;

Benchmark
CERT - 2021

Toujours les mêmes portes d'entrée pour s'introduire dans les systèmes

20%
Email frauduleux pour voler des 1ères informations ou piéger un ordinateur (phishing…)

-5% vs 2020

23%
Utilisation de comptes valides pour s'introduire dans le SI (vol de mot de passe, réutilisation…)

+5% vs 2020

18%
Service d'accès distant en utilisant des failles de sécurité ou des défauts de configuration
(Citrix, VPN…)

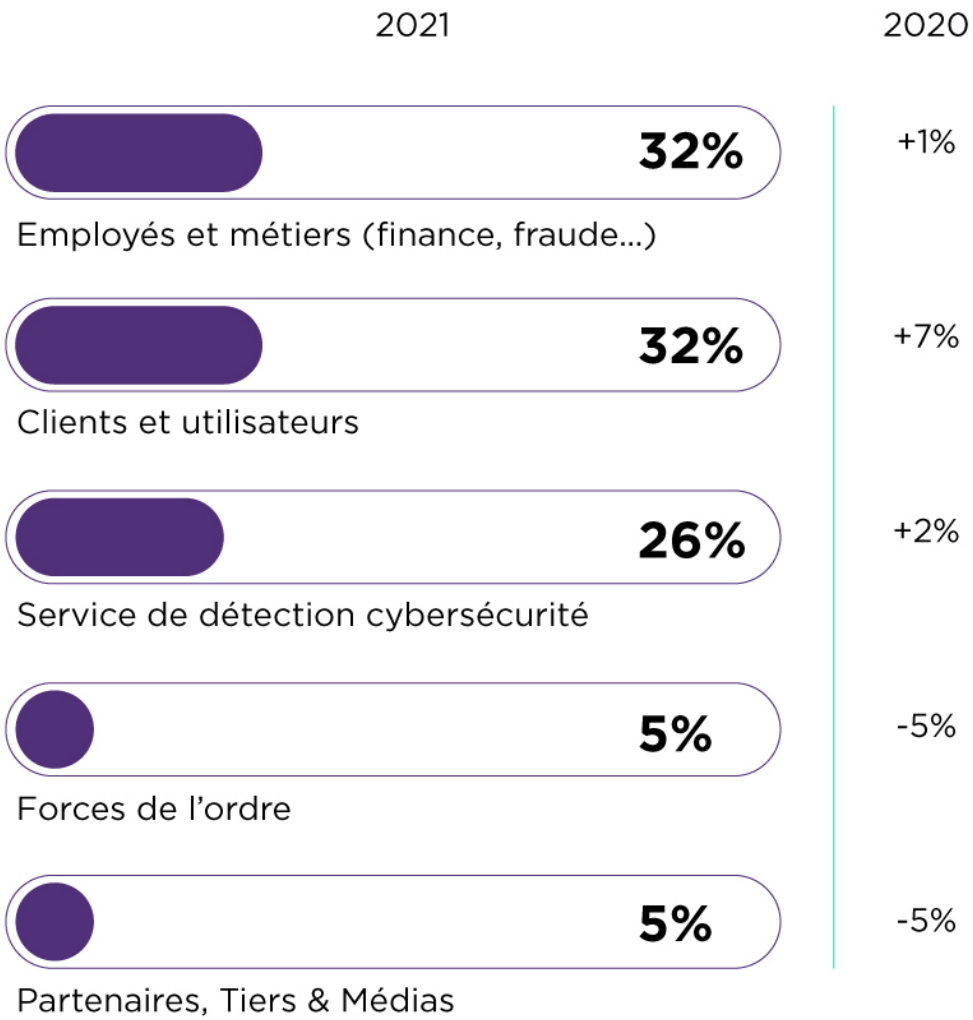
+2% vs 2020

Benchmark
CERT - 2021

Seulement **26% des incidents majeurs** ont été identifiés par les services de détection des entreprises

Dans **5%** des cas, Wavestone a pu stopper l'attaque avant son impact final

RÉPARTITION PAR SOURCE DE DÉTECTION DES INCIDENTS DE SÉCURITÉ

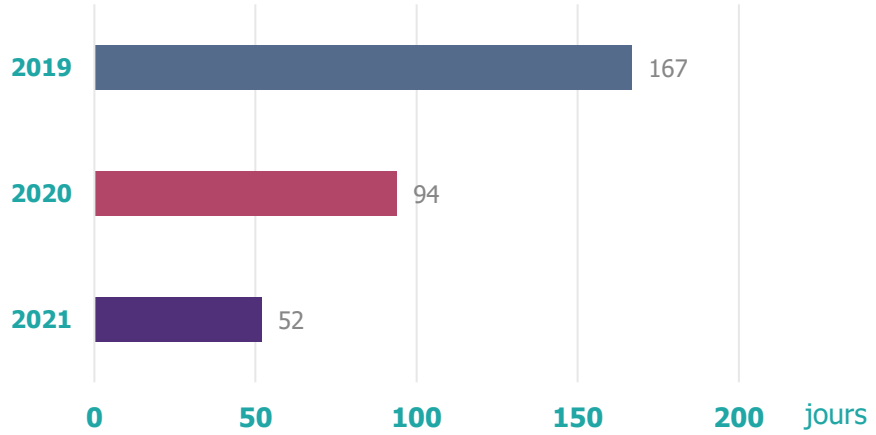


Benchmark
CERT - 2021

Une réduction de près de moitié du temps moyen écoulé entre une intrusion et sa détection

52
jours

Temps moyen écoulé entre une intrusion et sa détection ***contre 94 jours (-45%) en 2020***



Benchmark
CERT - 2021

Ransomware : le type d'attaque le plus fréquent et le plus impactant

60% des incidents sont causés par une attaque de type ransomware (89% des crises gérées sont des ransomwares)

1/3 des attaques ransomwares combinent vol de données et blocages du SI

Dans **90%** des attaques par ransomware, des données ont été perdues irrémédiablement

Dans **21%** des attaques par ransomware, les systèmes de sauvegarde ont été ciblés, jusqu'à être rendus inutilisables

GO FASTER

Des attaquants toujours plus rapides

3

jours seulement entre l'accès initial et le déploiement du ransomware pour l'attaque la plus rapide
(25 jours en moyenne)

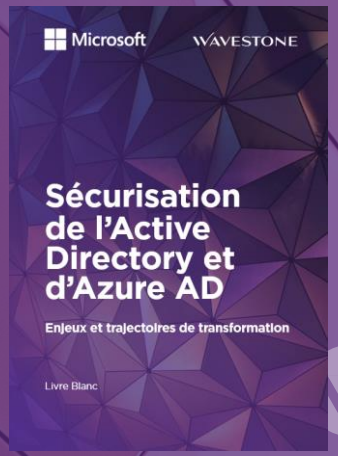
Un dénominateur commun de toutes les crises ransomwares gérées par le CERT-W

ACTIVE DIRECTORY compromis

L'attaquant possédait des comptes d'administration du domaine dans...

100% des crises

Pour aller plus loin :
Consultez notre Livre blanc Microsoft / Wavestone sur la sécurisation de l'Active Directory et d'Azure AD



Crises ransomware d'ampleur :

DES DÉLAIS INCOMPRESSIBLES… MAIS EN AMÉLIORATION

2
jours
pour mobiliser la crise sur un rythme de croisière

2
semaines
pour retrouver une situation métier en fonctionnement dégradé

2
mois
pour un retour complet à la normale

Benchmark
CERT - 2021

60
personnes en moyenne

250
personnes au maximum

10
prestataires en renfort en moyenne

Des rançons moins payées ?

Le montant des rançons est très variable…

Des rançons qui oscillent entre

100.000 €

et

2.000.000 €

en fonction de l'ampleur de l'attaque et de la taille de l'entreprise

Moins de

5%

des victimes ont payé la rançon.

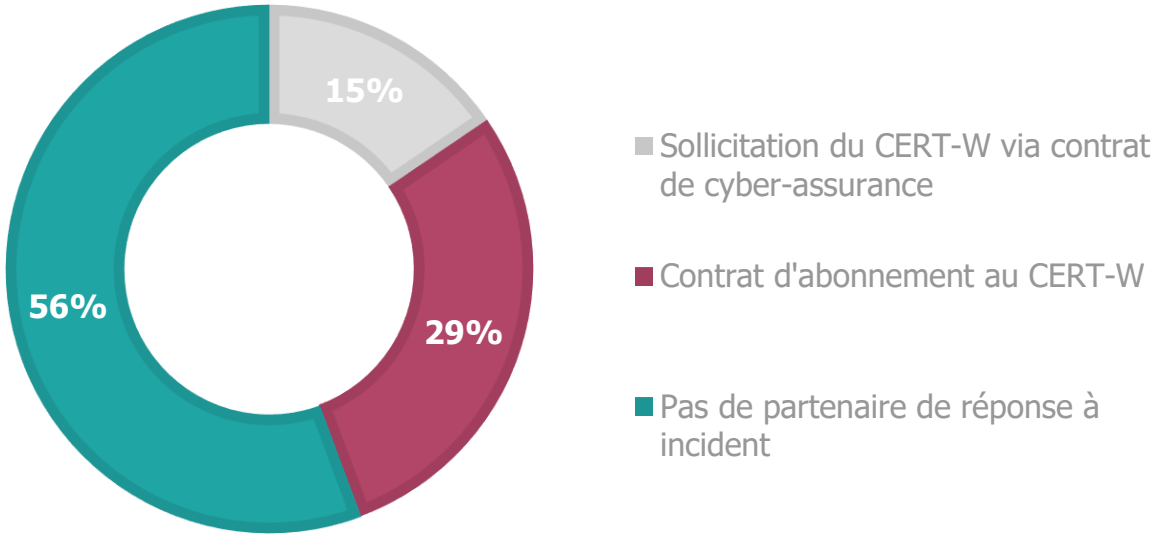
(Vs 20% en 2020)

…mais leur paiement est peu fréquent

Le paiement de la rançon n'accélère en rien le temps de résolution de la crise.

Benchmark
CERT - 2021

56% des incidents majeurs n'ont pas été anticipés par les victimes



42 %

des victimes n'avaient pas mené de projet de cyber résilience
(exercice de crise, sécurité des backups, tests de reconstruction…)

La majorité des victimes n'avait **pas de partenaire de réponse à incident** avant l'attaque

Benchmark
CERT - 2021

Comment ne pas être une cible facile ?

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, EDR…)

Savoir gérer une crise majeure (équipe 24/7, moyens de communication spécifiques…) grâce à des exercices de crise sur des scénarios variés (blocage du SI, vol de données ciblées, vol massif de données…)

Renforcer la sécurité des sauvegardes (durcissement, droits d'accès, isolation…) et s'entrainer à reconstruire en urgence (procédures, matériel spécifique…)

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

Envie de connaître votre degré de résistance ?
Evaluez-vous en utilisant le W-CyberBenchmark

En cas d'urgence pour les investigations ou la gestion de crise

Contactez le CERT-W cert@wavestone.com

Des attaques toujours en augmentation avec des impacts de plus en plus forts

Le nombre d'incidents majeurs traités par Wavestone augmentent en volume dans l'année (+15%). **La motivation du gains financiers** reste très majoritaire (75%).

Les ransomwares constituent **la menace numéro 1.** **La combinaison du blocage du SI avec un vol de données** est de plus en plus fréquente. **Les systèmes de sauvegardes** sont spécifiquement détruits dans 21% des cas.

Les attaquants mènent des attaques **toujours plus rapides** (réduction de 45% de la durée entre l'intrusion et le déclenchement de l'attaque avec des attaques qui réussirent en moins de 3 jours).

La durée des crises se réduit en moyenne **de 2 semaines d'interruption** et les rançons sont **de moins en moins payées.** Vers une meilleure préparation des entreprises ?

Benchmark
CERT - 2021

Wavestone, leader dans le domaine de la cybersécurité

Les **600 consultants cybersécurité** Wavestone allient expertises fonctionnelles, sectorielles et techniques, pour couvrir **plus de 1000 missions par an** dans une vingtaine de pays (notamment la France, le Royaume-Uni, les Etats-Unis, Hong Kong, la Suisse, la Belgique, le Luxembourg, ou encore le Maroc).

Une expertise éprouvée **de la stratégie à la mise en place opérationnelle** :

/ Management du risque & stratégie
/ Conformité numérique
/ Cloud & sécurité nouvelle génération
/ Tests d'intrusion et audits de sécurité
/ Réponse à incidents
/ Identité numérique (pour les utilisateurs et les clients)

En particulier dans le domaine des services financiers, de l'industrie 4.0, de l'IoT et des biens de consommation.

Contactez nos experts

Gérôme BILLOIS
Partner Cybersecurity & Digital Trust
gerome.billois@wavestone.com
(+33) 6 10 99 00 60
@gbillois

Nicolas GAUCHARD
Senior Manager CERT-Wavestone
nicolas.gauchard@wavestone.com
(+33) 667396570