WAVESTONE

COMMUNIQUE DE PRESSE *Paris, le 12 octobre 2021*

Cyberattaques : Le ransomware, menace numéro 1 en France

- **60% des attaques** observées par le CERT-Wavestone sont des ransomwares
- **30% des attaques ransomwares observées combinent le blocage du SI et le vol de données**
- **90% des victimes ont perdu irrémédiablement des données** mais le paiement des rançons diminue
- **56%** des victimes **n'avaient pas anticipé être la cible potentielle d'une cyberattaque**
- Des **attaques de plus en plus rapides** : un minimum de **3 jours** et une **moyenne de 25 jours entre l'intrusion et la demande de rançon**

A l'occasion du mois européen de la cybersécurité et dans le cadre des Assises de la Sécurité (13 au 16 octobre 2021), le cabinet Wavestone dévoile la nouvelle édition de son Benchmark des incidents de cybersécurité. Les enseignements qui y sont répertoriés proviennent d'une analyse complète des interventions de l'équipe CERT-Wavestone, en charge de l'aide aux victimes en cas de cyberattaques, réalisées entre septembre 2020 et octobre 2021… Soit, 60 incidents de sécurité majeurs ayant mené à une interruption d'activités ou à une compromission avancée du Système d'Information et ce, dans des secteurs très variés : industrie, secteur public, agroalimentaire, technologies de l'information, finance, etc. L'objectif de ce Benchmark est d'apporter des clés de lectures et de compréhension, tout en montrant l'évolution de l'état de la menace cyber en France.

Une forte prépondérance des ransomwares dans le panorama des cyberattaques

Les ransomwares représentent **60%** des cyberattaques rencontrées par le CERT-W chez les clients. De plus en plus nombreux, les attaquants sont également plus organisés et mieux outillés pour mener des attaques toujours plus efficaces.

« *Les groupes de cybercriminels ont réussi leur transformation numérique et leur organisation en plateforme a permis de massifier et de rendre plus efficaces et rapides leurs attaques* » indique **Gérôme Billois, Partner Cybersécurité**.

Au-delà du simple blocage du SI, **la combinaison avec un vol de données devient de plus en plus présente**. En effet, **30% des attaques ransomwares observées combinent le blocage du SI et le vol de données,** ce dernier constituant un levier supplémentaire pour obtenir des gains financiers.

Des attaques ransomwares plus rapides et plus ciblées

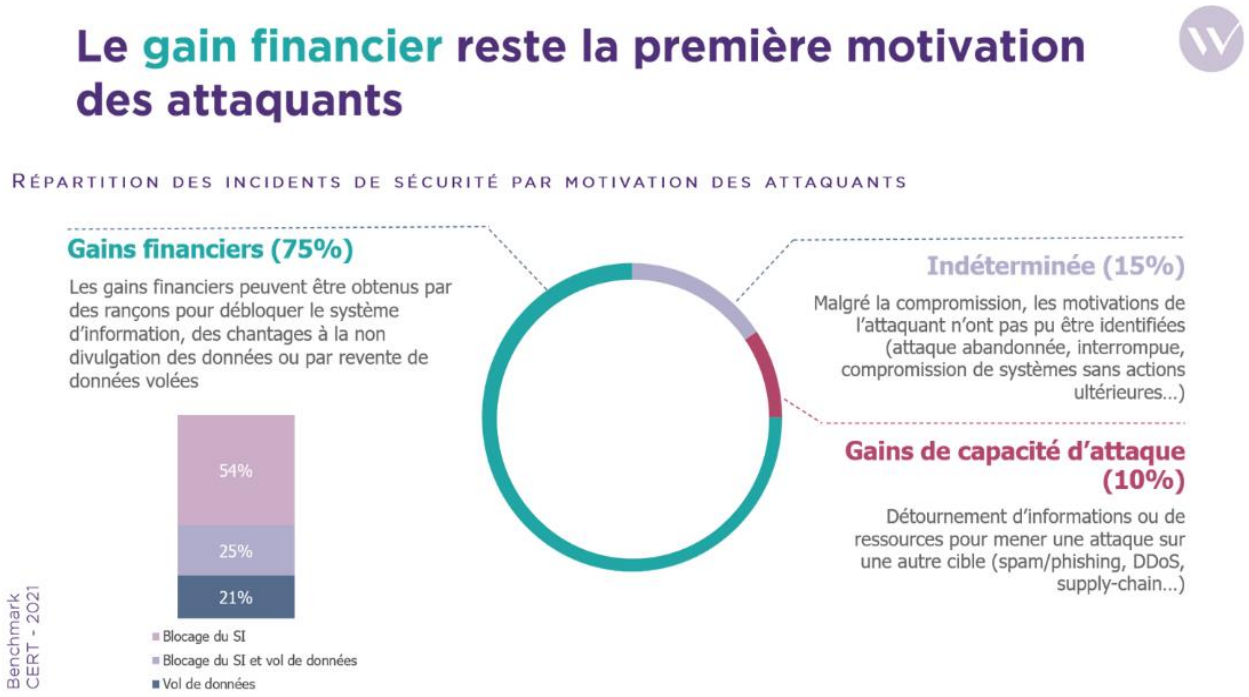
L'analyse révèlent une réduction du temps moyen entre l'accès initial et le déploiement du ransomware dans le système avec **un minimum de 3 jours pour l'attaque la plus rapide et une moyenne de 25 jours** sur les cas gérés. Les attaquants sont **de plus en plus déterminés à nuire à leurs victimes.** En effet, désormais, ils vont jusqu'à cibler et détruire les mécanismes de sauvegarde pour forcer le paiement de la rançon (**21% des cas**).

Le Benchmark permet de constater que dans **90% des cas des données ont été perdues irrémédiablement.** A noter la baisse significative du paiement des rançons cette année (**de 20% des victimes l'année précédente à 5%**). De multiples facteurs peuvent expliquer cette baisse : de la meilleure compréhension du faible intérêt à payer (le paiement de la rançon n'accélérant en rien le temps de résolution de la crise) aux actions de sensibilisation et de pression sur les intermédiaires de paiement par les différentes autorités.

D'autres types d'attaques sévissent toujours en toile de fond…

La menace ransomware ne doit pas faire oublier les attaques de **vols de données, de fraude et le gain de capacité d'attaques** qui restent bien présentes (**25%** des interventions) même si celles-ci sont moins fréquentes.

En ce qui concerne les canaux d'accès pour s'introduire dans les systèmes, les principales portes d'entrée restent **l'utilisation de comptes valides préalablement découverts/volés (23%), les emails frauduleux/*phishing* pour obtenir un accès (20%) et les services d'accès distants en utilisant des failles de sécurité ou des défauts de configuration (18%).**



Comment ne pas être une cible facile ? Quelques conseils du CERT-W

56% des victimes n'avaient pas anticipé être la cible potentielle d'une cyberattaque… Elles n'étaient ni dotées d'un contrat de réponse à incident, ni d'une cyber assurance et **42% des victimes n'avaient pas réfléchi à leur résilience en cas d'indisponibilité du système d'information.**

« *Même si des actions diplomatiques et judiciaires ont permis d'affaiblir l'écosystème cybercriminels, il ne s'agit pas de stopper les efforts, il faut se préparer dès maintenant grâce à des actions simples à mettre en place*. » souligne **Nicolas Gauchard, responsable du CERT-W**.

Les actions les plus importantes à mettre en place sont désormais connues :

- Identifier et protéger les systèmes et les données les plus critiques, sans oublier les systèmes techniques comme l'Active Directory ;
- Améliorer l'efficacité de la détection des attaques avec un service spécialisé 24/7 ;
- Savoir gérer une crise majeure en s'entrainant grâce à des exercices de gestion de crise ;
- Renforcer la sécurité des sauvegardes et s'entraîner à travailler sans informatique et reconstruire les systèmes en urgence ;
- Souscrire à une cyberassurance et un contrat auprès de service spécialisé en cas de crise.

Présentation en avant-première du Livre blanc Microsoft/Wavestone

Sécurisation de l'Active Directory et d'Azure AD : Enjeux et trajectoires de transformation

Présentation du Livre blanc **le Jeudi 14 octobre à 14h** lors de l'atelier de Microsoft aux Assises de la Sécurité « *Comment réussir l'implémentation de votre démarche Zéro Trust ?* »

Dans l'objectif de lutter contre les groupes de cybercriminels, un actif clé doit être au cœur de la stratégie de sécurisation : l'Active Directory (AD). Ce dernier joue un rôle central dans la gestion des accès aux ressources numériques et est régulièrement ciblé par les cybercriminels.

C'est pour cette raison que Microsoft et Wavestone se sont associés pour rédiger un livre blanc consacré à la sécurisation de l'Active Directory et d'Azure AD, aux enjeux et trajectoires de transformation.

Ce livre blanc analyse les tendances observées sur le terrain, identifie les limites actuelles et donne les bonnes pratiques pour sécuriser les briques essentielles du SI.

Les experts du cabinet Wavestone seront présents aux Assises de la Sécurité (Stand 183)

Intervention de Gérôme Billois et Matthieu Garin lors de l'atelier Wavestone sur le thème :
« Fighting back ransomware : comment le CAC 40 s'organise ?»

Intervention lors de l'atelier Microsoft intitulé :
« Comment réussir l'implémentation de votre démarche Zéro Trust ? »

Méthodologie du Benchmark

Ce Benchmark est issu de la consolidation des données de 60 réponses à incidents menés par le CERT-Wavestone entre Septembre 2020 et Octobre 2021 auprès de 50 organisations appartenant au Top 200 des entreprises françaises, issus de 10 secteurs d'activités différents : Banque, Assurance, Distribution, Industriel, Public, Santé, Service, Sport, Télécom, Transports. Les données de ce Benchmark ont été rendues anonymes : la collecte est uniquement statistique.

A propos de Wavestone

Dans un monde où savoir se transformer est la clé du succès, Wavestone s'est donné pour mission d'éclairer et guider les grandes entreprises et organisations dans leurs transformations les plus critiques avec l'ambition de les rendre positives pour toutes les parties prenantes. C'est ce que nous appelons « The Positive Way ».

Wavestone rassemble plus de 3 400 collaborateurs dans 8 pays. Il figure parmi les leaders indépendants du conseil en Europe, et constitue le 1er cabinet de conseil indépendant en France.

Wavestone est coté sur Euronext à Paris et labellisé Great Place To Work®.

Plus d'informations sur www.wavestone.com // @wavestoneFR

Contact le CERT-W : cert@wavestone.com

Wavestone

Mélodie Lauque

melodie.lauque@wavestone.com

Wellcom PR Agency

Sonia El Ouardi

sonia.elouardi@wellcom.fr

Donna Clément

donna.clement@wellcom.fr

Tel. : + 33 1 46 34 60 60