DÉPÔT DE PLAINTE

Avec Constitution de Partie Civile

Pour Piratage Informatique, Espionnage Industriel et Vol de Secrets de Fabrication

À :

Monsieur / Madame le Procureur de la République

Tribunal Judiciaire de [VILLE]

[Adresse complète du Tribunal]

[Code postal] [VILLE]

À [Ville], le [DATE]

I. Identité du plaignant

La présente plainte est déposée par :

Raison sociale / Nom et Prénom : _____

Forme juridique (si société) : _____

SIRET / N° RCS (si société) : _____

Représenté par (Nom, Qualité) : _____

Adresse du siège social / Domicile : _____

Code postal / Ville : _____

Téléphone : _____ Email : _____

Ci-après désigné(e) : « le Plaignant » ou « la Société Victime »

II. Identité des personnes mises en cause

Dans la mesure du possible, le Plaignant désigne comme auteurs présumés des faits :

Nom / Dénomination :

_____

Adresse connue :

_____

Qualité / Lien avec le Plaignant : _____

À défaut d'identification précise, la plainte est déposée contre X.

III. Exposé des faits

3.1 Contexte général

Le Plaignant est une entreprise spécialisée dans [décrire l'activité principale], employant [nombre] salariés, dont le savoir-faire et les secrets de fabrication constituent des actifs stratégiques essentiels à sa compétitivité sur le marché.

C'est dans ce contexte que le Plaignant a découvert, à compter du [DATE DE DÉCOUVERTE], des faits graves constitutifs d'atteintes à ses systèmes informatiques, de vol de données confidentielles et d'espionnage industriel, dont les circonstances sont exposées ci-après.

3.2 Faits de piratage informatique

À une date que les investigations permettront de déterminer, le ou les auteurs se sont introduits frauduleusement dans le système d'information du Plaignant. Les faits constatés sont les suivants :

- Intrusion non autorisée dans les serveurs internes de la société via [décrire le vecteur : phishing, exploitation de faille, accès interne frauduleux, etc.] ;
- Extraction et copie non autorisées de fichiers sensibles stockés sur [serveur / cloud / poste informatique] ;
- Installation de logiciels malveillants (malware, keylogger, cheval de Troie) permettant une surveillance continue des activités de la société ;
- Altération et / ou destruction partielle de données informatiques ;
- Exfiltration de données à caractère confidentiel vers des adresses IP ou serveurs extérieurs identifiés / non encore identifiés.

3.3 Faits d'espionnage industriel et de vol de secrets de fabrication

Les données subtilisées comprennent des informations de nature hautement confidentielle, protégées au titre du secret des affaires en application de la Loi n° 2018-670 du 30 juillet 2018. Il s'agit notamment :

- Des formules, procédés et méthodes de fabrication [décrire brièvement les produits concernés] constituant le cœur du savoir-faire industriel du Plaignant ;
- Des plans techniques, schémas, prototypes et cahiers des charges relatifs aux produits / technologies [à préciser] ;
- Des bases de données clients, fournisseurs et partenaires stratégiques ;
- Des études de marché, stratégies commerciales et informations financières confidentielles ;
- Des informations couvertes par des accords de confidentialité (NDA) conclus avec des tiers.

3.4 Préjudices subis

Les faits susvisés ont causé au Plaignant des préjudices importants, notamment :

- Préjudice économique direct évalué à ce stade à [MONTANT] euros, susceptible d'être réévalué ;
- Atteinte grave à la compétitivité et à la position concurrentielle de la société ;
- Atteinte à la réputation et à l'image de marque ;
- Coûts de remédiation informatique et de sécurisation des systèmes.

IV. Qualification juridique des faits

Les faits exposés sont susceptibles de recevoir les qualifications pénales suivantes :

Sur le piratage informatique :

- Accès frauduleux à un système de traitement automatisé de données (STAD) : article 323-1 du Code pénal (peine : 3 ans d'emprisonnement et 100 000 € d'amende) ;
- Maintien frauduleux dans un STAD : article 323-1 alinéa 2 du Code pénal ;
- Entrave au fonctionnement d'un STAD : article 323-2 du Code pénal (peine : 5 ans et 150 000 €) ;
- Introduction frauduleuse de données dans un STAD / modification ou suppression : article 323-3 du Code pénal.

Sur l'espionnage industriel et le vol de secrets de fabrication :

- Violation du secret des affaires : articles L. 151-1 et suivants et L. 152-1 du Code de commerce, issus de la Loi n° 2018-670 du 30 juillet 2018 ;
- Vol de fichiers et données informatiques : articles 311-1 et suivants du Code pénal ;
- Divulgation non autorisée d'informations protégées et violation de clauses de confidentialité ;
- Recel de bien provenant d'un délit : article 321-1 du Code pénal ;
- Le cas échéant : espionnage économique au profit d'une puissance étrangère (article 411-6 du Code pénal).

V. Éléments de preuve

À l'appui de la présente plainte, le Plaignant produit les pièces suivantes :

Pièce n° 1 : Rapport technique de l'expert en cybersécurité mandaté le [DATE] ;

Pièce n° 2 : Journaux (logs) des systèmes informatiques démontrant les intrusions ;

Pièce n° 3 : Constat d'huissier sur les systèmes et données affectés ;

Pièce n° 4 : Copie des documents et fichiers dérobés identifiés ;

Pièce n° 5 : Accords de confidentialité (NDA) conclus avec les mis en cause ou tiers concernés ;

Pièce n° 6 : Échanges de courriels / messageries documentant les faits ;

Pièce n° 7 : Évaluation du préjudice économique établie par [expert-comptable / cabinet conseil].

VI. Demandes

En conséquence des faits exposés, le Plaignant a l'honneur de vous demander :

- D'ouvrir une enquête préliminaire ou d'ordonner une information judiciaire sur les faits dénoncés ;
- De saisir l'unité compétente (BEFTI, C3N ou OCLCTIC) pour investigation numérique approfondie ;
- D'ordonner toute mesure de séquestre, de perquisition ou de conservation utile pour préserver les preuves ;
- De poursuivre les auteurs, coauteurs et complices des infractions commises ;

- D'admettre le Plaignant à se constituer partie civile afin d'obtenir réparation de l'intégralité des préjudices subis.

VII. Constitution de partie civile

Par la présente, le Plaignant entend se constituer partie civile et demande à être tenu informé de toute décision relative aux suites données à la présente plainte. Il sollicite l'indemnisation de l'ensemble de ses préjudices — matériels, économiques, concurrentiels et moraux — qui seront justifiés et chiffrés en cours de procédure.

À cet effet, le Plaignant élira domicile auprès de Maître [NOM AVOCAT], Avocat au Barreau de [VILLE], [ADRESSE CABINET].

Je soussigné(e), [Nom et Prénom], [Qualité], certifie l'exactitude des faits exposés dans la présente plainte et m'engage à informer les autorités judiciaires de tout élément nouveau susceptible de compléter ces déclarations.

Fait à [Ville], le [DATE]

Signature et cachet :

_____

[Nom, Prénom, Qualité]

Pièces jointes

Pièce n° 1 : Rapport d'expertise en cybersécurité

Pièce n° 2 : Journaux de connexion (logs)

Pièce n° 3 : Constat d'huissier

Pièce n° 4 : Inventaire des données dérobées

Pièce n° 5 : Accords de confidentialité

Pièce n° 6 : Correspondances pertinentes

Pièce n° 7 : Évaluation du préjudice économique