[Prénom] [Nom]

[Société]

[Adresse]

[Code postal] [Commune]

[Téléphone]

[Adresse électronique]

Monsieur le Procureur de la République

Tribunal judiciaire de [Ville]

[Adresse]

[Code postal]

À [Commune], le [Date]

**Objet** : Dépôt de plainte à la suite d’une attaque informatique par rançongiciel

Monsieur le procureur de la République,

J'ai l'honneur de vous informer des faits suivants :

**Présentation de la société victime**

*Présenter la société victime, son domaine d'activité, son chiffre d'affaire, la masse salariale et ou le nombre de sous-traitants dépendant de son activité.*

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

*Présenter le déclarant : Identité complète (Nom, prénom, date de naissance) et coordonnées postales, téléphoniques et électroniques.*

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

*Détailler l’infrastructure informatique de la société*

*Adresse IP publique, nom de domaine ou sous domaine*

*- Type d'infrastructure informatique et sa cartographie rapide : - Nombre de serveurs, localisation*

*- Nature des systèmes impactés :*

*- Précisez le système d’exploitation (Windows XP/7/10\*\* Windows Server 2008 R2 ou 2012 R2\*\*. Linux (redhat – debian- Centos…)*

*Serveurs physique ou virtuels*

*- Existence d'accès à distance sur le réseau : Précisez la technologie utilisée par les collaborateurs de l’entreprise pour se connecter à distance*

*Indiquez s’il y a utilisation d’un VPN (marque et version)*

*Eléments de sécurité au moment de l'attaque :*

*Type d’antivirus, Firewall*

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

**SUR LES FAITS :**

Sur l’attaque informatique

*Préciser l’objet de la plainte, la date à laquelle les faits ont été découverts et les circonstances de l'attaque*

*…………………………………………………………………………………………………..............................................................*

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

*Préciser pour cette attaque informatique, les coordonnées de contact de la personne qui sera l'interlocuteur technique (RSSI/CERT/ intervenant) et lister les sociétés externes intervenantes, en donnant leur point de contact.*

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

*Indiquer le nombre de postes/serveurs impactés sur le système ? (Système d’exploitation et sa version) et préciser la nature des données présentes sur ces postes notamment s’il y a des données sensibles, personnelles, de santé, classifiées ?*

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

*Décrire l’impact sur l’activité et Indiquer les mesures de remédiation prises, le cas échéant et notamment s’il y réinstallation des sauvegardes ?*

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

*Préciser, s’il est connu, le nom du rançongiciel ayant infecté le système et de quelle manière a t’il été déterminé*

…………………………………………………………………………………………………..............................................................

**SUR LES TRACES TECHNIQUES DE L’INFECTION**

*Préciser si le premier poste infecté de l’infrastructure a été découvert et s’il a été conservé.*

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

*Indiquer s’il est connu le vecteur de l’infection.*

*- Courriel contenant une pièce jointe (Préciser la langue de rédaction, communiquer les entêtes techniques, et la pièce jointe à transmettre au sein d’une archive au format .zip avec le mot de passe "infected" qui sera placée sur un CD ROM)*

*- Fichier téléchargé sur Internet (précisez requête effectuée au sein d’un moteur de recherche, adresse du site Internet, communiquer le fichier à transmettre au sein d’une archive au format .zip avec le mot de passe "infected" qui sera placée sur un CD ROM)*

*- Un accès à distance compromis – Quel compte utilisateur ? de quels droits disposait-il ?*

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

*Dans le cas de la découverte d’un un fichier contenant des instructions (appelée note de rançon) avec des adresses mails pour contacter les attaquants, un identifiant et/ou lien internet, le joindre à plainte, et mentionner la nouvelle extension des fichiers chiffrés, le cas échéant.*

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

*Précisez si les journaux de connexion (logs) relatifs à cette attaque ont été conservés, ainsi que la souche virale.*

*A transmettre au sein d’une archive au format .zip avec le mot de passe "infected" qui sera placée sur un CD ROM*

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

**---SUR LA PRISE DE CONTACT AVEC LE OU LES AUTEURS DE L'ATTAQUE---**

*Indiquer si un contact avec le ou les auteurs de cette attaque informatique a été effectué, et dans l'affirmative communiquer l’échange.*

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

*Préciser si le payement de la rançon a été envisagé ou non et si une négociation a eu lieu.*

*Rappel : il n’est pas conseillé de payer la rançon : Cela ne garantit par la récupération des données, ne prémuni pas contre une nouvelle attaque, et contribue à financer l’écosystème cybercriminel*

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

*En cas de payement communiquer les détails de la transaction (date, montant, adresse de payement) et les coordonnées de la personne l’ayant réalisée. Indiquer si vous avez été en mesure de récupérer vos données, et si oui préciser l’outil.*

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

---SUR LE PREJUDICE ET LA PLAINTE : ---

Indiquer une évaluation du préjudice

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

…………………………………………………………………………………………………..............................................................

En conséquence, je souhaite porter plainte contre X pour ces faits qui pourrait être qualifiés des chefs de

* Accès frauduleux à un STAD (Système de traitement automatisé de données.)
* Maintien frauduleux au sein d’un STAD
* Introduction frauduleuse au sein d’un STAD
* Modification frauduleuse d’un STAD
* Entrave à un STAD
* Extorsion en bande organisée
* *(si la victime est un service public)* Atteinte a un système de traitement automatise de données à caractère personnel mis en œuvre par l’État, commise en bande organisée

Je vous remercie de considérer ce courrier comme un dépôt de plainte.

Dans l'attente des suites que vous donnerez à ce courrier, je vous prie d'agréer, Madame, Monsieur le procureur de la République, l'expression de ma plus haute considération.

[Prénom] [Nom]