Dépôt de plainte

Vous êtes victime d'une compromission de votre système d'information par un rançongiciel.

Le but de cette fiche est de fluidifier les rapports entre La Justice, les services enquêteurs, les victimes et leurs prestataires, face à cette menace importante.

Les éléments que vous pouvez récupérer dans le cadre des analyses de cette compromission font de vous un acteur central pour améliorer l'efficacité de la réponse face à des criminels, par la détection rapide des éléments techniques pouvant être utiles aux investigations, et par l'assistance que vous pourrez apporter dans la judiciarisation des faits.

Vous trouverez ci-dessous les conseils pour vous aider dans ces démarches.

Préservation des traces

Cette préservation ne fait souvent pas partie des priorités lors de la gestion d'une crise liée à un ransomware, face à celles de la détection de l'étendue de la compromission et de la remise en production.

Pourtant, cette étape est essentielle pour permettre au service enquêteur de pouvoir réaliser plus sereinement ses investigations.

Il est donc indispensable d'avoir à l'esprit, dès les premiers actes de remédiation, les bonnes pratiques de conservation des traces, et notamment de :

- Travailler au maximum sur des copies en préservant le support originel afin de ne pas polluer les traces (date d'accès.) ou d'en supprimer afin d'assainir le système ;
- Sauvegarder les fichiers de logs bruts (EventX windows, logs Firewall, logs d'authentification...) avant tout redémarrage de la machine ou réinstallation du système, ils seront demandés en plus de votre rapport technique contenant les éléments extraits ;
- Préserver tous les éléments liés à l'infection : message électronique avec entête technique, note de rançon, exemplaire de fichiers chiffrés, adresse de crypto monnaie, fichiers malveillants (dropper, Payload) ;
- Préserver le disque dur de la machine primo infectée, ou à défaut en faire une copie physique (bit à bit).

Si des éléments techniques importants sont découverts lors de la phase de remédiation (serveur actif de Command & Control, IP des serveurs d'attaques des auteurs), un contact pourra être pris avec le CSIRT-PJ pour leur communiquer ces informations, même avant la phase du dépôt de plainte (mail : csirt-pj@interieur.gouv.fr, Tchap, …).

Dépôt de plainte

Réaliser votre dépôt de plainte

Plus **de 80 investigations sur des familles de ransomware** sont en cours au sein des services de Police Judiciaire spécialisés en cybercriminalité.

Ces enquêtes sont **regroupées, au sein des services de Police Judicaire spécialisés, par famille de rançongiciel**, et ce pour plus d'efficacité. Elles sont diligentées **sous l'autorité de la section J3 (cybercriminalité) du Parquet de Paris**, qui dispose d'une compétence nationale concurrente.

La plainte est donc très utile pour permettre de **communiquer des éléments enrichissant les enquêtes et nécessaire pour connaitre l'actualité de l'activité d'un groupe criminel sur le territoire national.**

Voici les éléments qui à rassembler en vue de la plainte.

- ✓ *Un extrait KBIS et un pouvoir du représentant légal pour déposer plainte, le cas échéant.*
- ✓ *Impact de l'infection sur l'activité de l'entreprise*
- ✓ *Coordonnées du RSSI, CERT et tous les partenaires intervenants*
- ✓ *Rapport des prestataires et leurs pièces jointes*
- ✓ *Vecteur et date d'infection*
- ✓ *Les logs d'infection (du système primo infecté, du pare feu)*
- ✓ *Disque de la machine primo-infectée*
- ✓ *Extension ajoutée après le chiffrement*
- ✓ *Type de fichier chiffré (bureautique, image)*
- ✓ *Type et sensibilité des données chiffrées*
- ✓ *Souche virale*
- ✓ *Note de rançon*
- ✓ *Si prise de contact avec le ou les auteurs : échanges et en-têtes techniques de courriel(s)*
- ✓ *Tous les fichiers transmis par la victime devront préalablement avoir été mis dans une archive au format .zip avec le mot de passe 'infected'*

Le dépôt de plainte peut se réaliser dans un commissariat ou une gendarmerie de votre choix.

Le site https://www.pre-plainte-enligne.gouv.fr/, permet de prendre un rendez-vous.

Il est également possible de le faire par lettre plainte, sur le modèle du canevas joint, qui devra être adressée pour une plus grande réactivité dans un premier temps **par mail au CSIRT-PJ** (csirt-pj@interieur.gouv.fr).

Son original devra ensuite être transmis par courrier au parquet local.

La question du paiement de la rançon

- Il est fortement déconseillé de payer la rançon. En effet cela ne garantit pas la récupération des données, ne prémunit pas contre une nouvelle attaque, et contribue à financer l'écosystème cybercriminel.

- En outre, les sociétés assistant la victime dans le paiement de la rançon peuvent être poursuivies pénalement en France sur le fondement de la complicité d'atteinte au STAD et de Blanchiment.

- En cas de prise de contact avec les auteurs, il est fortement recommandé de le faire avec l'assistance d'un service de police spécialisé qui dispose d'un cadre légal pour ce faire.