RENSEIGNEMENTS SUR LE SIGNALEMENT, DEUXIÈME ÉTAPE

A. Renseignements sur l'intervention à la suite de l'incident (renseignements supplémentaires)

1. Dans la mesure du possible, veuillez fournir des renseignements plus précis connus à ce stade sur la *chronologie de l'incident*, c'est-à-dire l'intrusion initiale, l'identification et les points clés relatifs à l'étendue de la compromission.

2. Dans la mesure du possible, veuillez fournir des renseignements connus à ce stade sur les caractéristiques de l'intrusion (p. ex. les indicateurs de compromission, les tactiques, les techniques et les procédures utilisées aux fins d'accès et d'infiltration). S'il est trop tôt pour fournir ces renseignements, vous pourrez le faire plus tard.

3. Dans la mesure du possible, veuillez fournir des copies de tous les fichiers journaux du réseau relatifs à cet incident. S'il est trop tôt pour fournir ces renseignements, vous pourrez le faire plus tard.

4. Si vous vous sentez à l'aise de le faire, veuillez fournir tous les rapports d'intervention disponibles concernant l'incident, qu'ils aient été générés à l'interne ou fournis par une tierce partie. Vous pourrez également les fournir plus tard.

B. Renseignements sur l'auteur de la menace (renseignements supplémentaires)

1. Avez-vous des renseignements sur les méthodes utilisées pour obtenir l'accès ou sur tout autre élément lié à l'intrusion dans le système?

2. Pouvez-vous fournir des renseignements supplémentaires sur l'auteur de la menace d'après les interactions que vous avez eues jusqu'à présent?

3. L'auteur de la menace a-t-il fourni des renseignements sur les comptes ou des instructions relatives aux transactions?

4. Y a-t-il des attributions précises qui peuvent être associées à l'auteur de la menace?

5. Y a-t-il des adresses et des activités de monnaie virtuelle clés liées à l'incident qui méritent d'être mentionnés?

6. Avez-vous d'autres renseignements qui pourraient permettre de comprendre qui pourrait avoir agi ainsi contre votre organisation?

C. Renseignements sur un incident de rançongiciel

1. Est-ce qu'il y a d'autres artéfacts de données liés à l'incident qui méritent d'être mentionnés?

2. Une rançon a-t-elle été versée?

i. Si oui, pouvez-vous fournir des renseignements sur la procédure de paiement qui a été utilisée?

ii. Si un paiement est envisagé, pouvez-vous fournir des renseignements sur la procédure qui sera utilisée?

D. Autres renseignements sur l'incident qui n'ont pas encore été fournis

1. Y a-t-il d'autres renseignements sur les processus ou techniques qui n'ont pas encore été mentionnés et qui seraient, selon vous, importants pour les forces de l'ordre à ce stade pour mieux comprendre l'incident?

2. Y a-t-il d'autres tierces parties externes impliquées à ce stade qui n'ont pas encore été identifiées et avec qui vous croyez que les forces de l'ordre devraient discuter?

3. Y a-t-il des services de soutien externe aux victimes dont votre organisation et/ou ses employés pourraient bénéficier pour mieux gérer les répercussions de l'incident?