RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

# KIT EXERCICE « SUR TABLE »

# Scénario «  Enseignement Supérieur Recherche Innovation »

# 1ERE PARTIE (25/12/24)

*(*) Table Top Exercice*

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

1

# Briefing

# Présentation des modalités de l'exercice (1/2)

**Objectifs de l'exercice :**

- Être sensibilisé aux grands principes de la gestion de crise cyber ;
- **Identifier les documents et procédures manquants pour traiter des incidents de sécurités**
- Réfléchir aux actions à mener en temps de crise / aux acteurs à mobiliser
- Développer son dispositif de gestion de crise

Pendant la séance, les joueurs sont invités à :

- **se projeter dans leur rôle respectif** au sein de la cellule de crise
- **réfléchir et partager sur les différentes actions à mener pour répondre aux différentes situations présentées**

- **Conseil aux joueurs : être aussi synthétique que possible afin de réussir à dérouler l'ensemble du jeu !**

# Présentation des modalités de l'exercice (2/2)

**Animateur : Nicolas**
**Observateurs : Martin et Kyrian**
**Coordinateurs: Edouard, Gérald et Mickael**

**Rôle des coordinateurs :**
Ils reçoivent à tour de rôle un stimulus. Les autres participants doivent demander la parole au coordinateur en levant la main.

**Déroulement d'un stimulus:**
Nicolas présente le stimulus. Le coordinateur donne sa première analyse et organise les interventions des participants qui lèvent la main ou celui à qui il donne la parole (pas de conversations croisées).Nicolas met fin au stimulus.

1. Présentation des modalités d'exercice
2. Réflexion sur les stimuli
3. 3 phases :
   - ALERTE/MOBILISATION - Stimuli 1-3
   - MAINTIEN DE LA CONFIANCE / COMPRENHENSION DE L'ATTAQUE - Stimuli 4-6
   - RELANCE DES ACTIVITES / DURCISSEMENT - Stimuli 7-9
   - RETEX à chaud / débrief

☑ **Nota bene : Des stimuli fictifs et sans corrélation entre eux**

# Tour de table des rôles joués

| Oliver MARCHAND DSI | [illegible] MOREAU | Olivier DURAND DSI | Charlie BARON DSI | Thierry SCHREINER DSI | Azizz EL KHIATI DSI | Franck GONNAUD DSI | Martin MIE & Kyrian PAINAULT |
|---|---|---|---|---|---|---|---|
| •Participant | •Coordinateur | •Participant | •Participant | •Participant | •Participant | •Participant | •Obervateur *(prise de note)* |

| Gérald SAILLY P' | Mickael BARON Lias | Hervé DOREAU P' | Mathis HEIN P' | Nicolas HERVE Animateur |
|---|---|---|---|---|
| •Coordinateur | •Coordinateur | •Participant | •Participant | •Animateur |

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

2

# Exercice

# PHASE 1 : ALERTE/MOBILISATION

# Stimulus 1

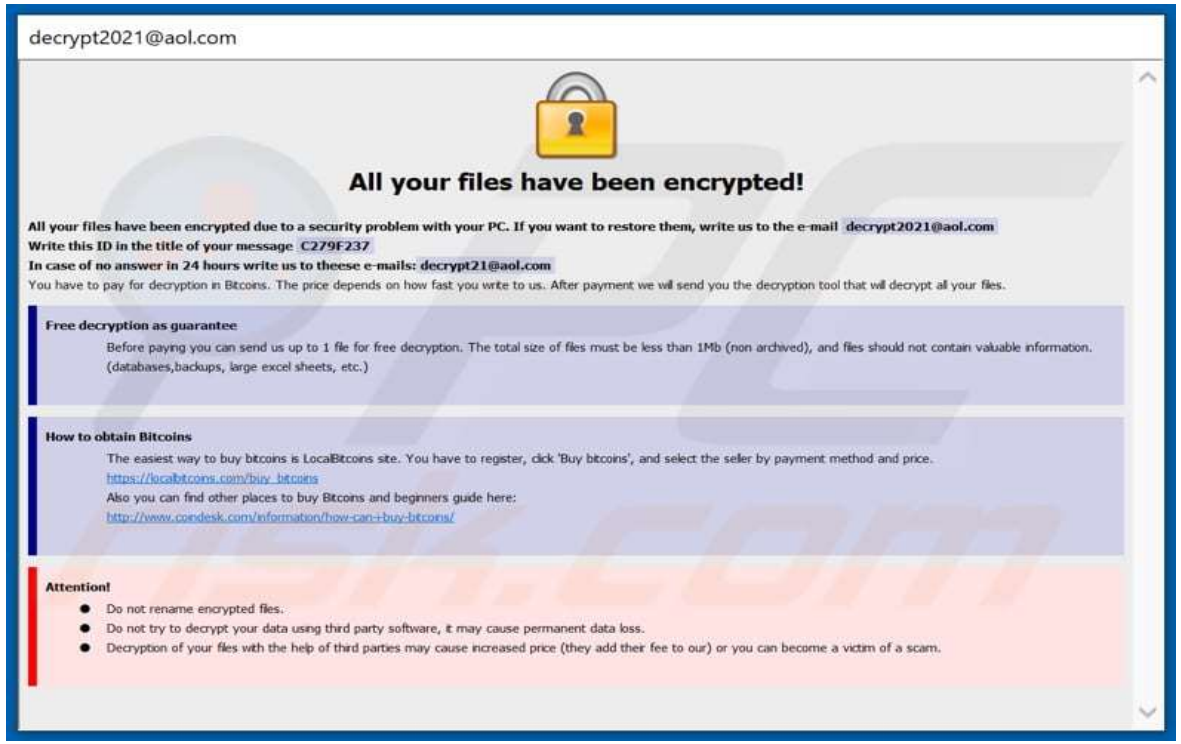
- **Nous sommes en fin d'année académique. Les vacances estivales approchent. Il existe une recrudescence des attaques dans le secteur, notamment permises par le vol des données identifiantes des populations étudiantes, enseignantes, de recherche et de l'administration (programmes malveillants « infostealers »).**

Fil conducteur :

- Quels sont les risques que vous identifiez ?
- Comment vous organisez-vous afin de diminuer le niveau de menace ?
- Quels sont les projets à mener et outils dont la cellule de crise et l'établissement ont besoin ? Sont-ils déjà en place ou à mettre dans votre plan de travail ? Pour quelles échéances ?

# Stimulus 2

**Un nombre croissant de personnels administratifs indiquent rencontrer des difficultés avec leurs ordinateurs. Certains voient apparaitre sur l'écran le message suivant :**



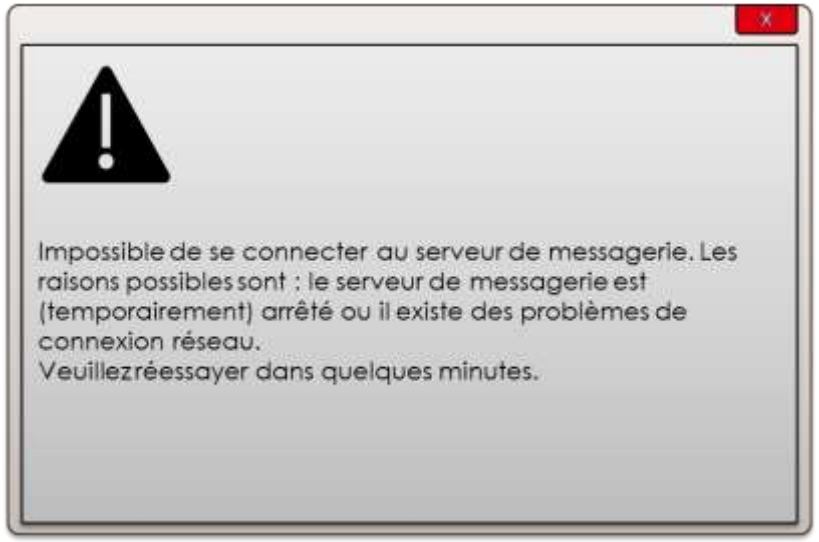

## Fil conducteur :

- Quelles actions prioritaires allez-vous mener ?
- Est-il nécessaire d'activer une cellule de crise ?

# Stimulus 3

**La direction des systèmes d'information a été informée que le chercheur participant au projet ERC AI-Generativ-Web n'a plus accès à sa messagerie ni à ses dossiers de recherche hébergés sur les infrastructures numériques collaboratives de l'établissement, depuis plusieurs jours maintenant.**

**Ce chercheur est *Project Investigator* pour le projet ERC : Les chercheurs avec qui il travaille sont affiliés à 3 autres établissements européens ainsi qu'à une université de premier plan américaine.**



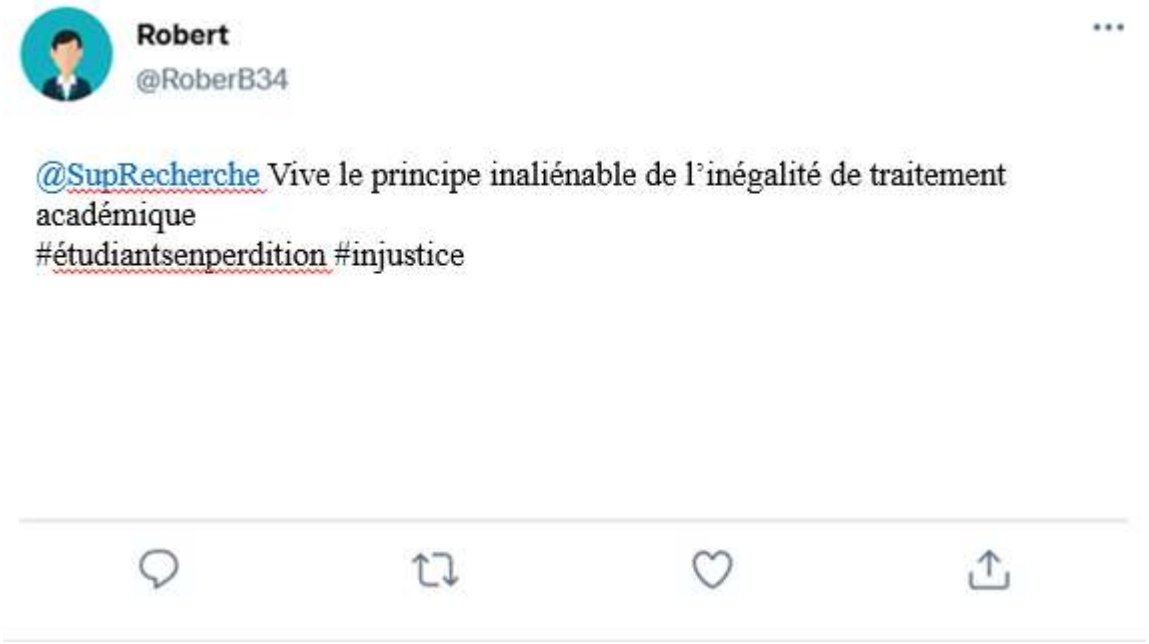

## Fil conducteur :

- Identifier l'ensemble des impacts métiers possibles
- Quelle serait la composition de votre cellule de crise ?
- Quelle serait la posture de l'établissement vis-à-vis de ses partenaires et personnels ?
- Disposez-vous de premiers éléments de langage clé en main ? Quels sont les outils de communication à votre disposition ? Ont-ils besoin d'être créés / enrichis / améliorés ?

# PHASE 2 : MAINTIEN DE LA CONFIANCE / COMPREHENSION DE L'ATTAQUE

# Stimulus 4

**Vous constatez de nombreux messages sur les réseaux sociaux commentant l'attaque ayant conduit à la modification de certaines évaluations de vos étudiants et dont vous avez été victime. Cette attaque éveille des problématiques juridiques que votre établissement pourrait potentiellement rencontrer.**




## Fil conducteur :

- Quelles actions prioritaires allez-vous mener ?
- Quels sont les risques de dégradation de la situation que vous anticipez ?
- Quelles sont les actions de communication que vous avez besoin de mettre en place ? Comment se déroule la validation de vos communications éventuelles ? Le cas échéant, qui est responsable de leurs émissions et des éventuelles réponses à réaliser ?

# Stimulus 5

**Vous êtes alertés que votre système de visioconférence est de temps à autre contrôlé par un attaquant qui s'emploie à diffuser des messages politiques et à mener des actions perturbantes pendant certains enseignements et certains colloques de recherche.**

**Depuis la crise sanitaire, une grande partie de vos enseignements sont délivrés en distanciel via cet outil. L'établissement prépare la venue d'une personnalité politique de premier plan et vous craignez pour la bonne tenue de l'évènement qui doit impérativement être aussi diffusé en ligne. Cet outil est le seul à vos yeux à passer l'échelle en termes de nombre de connexion.**

Fil conducteur :

- Quelles actions prioritaires allez-vous mener ?
- Qui est parties prenantes de votre plan d'action ?

# Stimulus 6

**Un chercheur signale qu'il est victime d'un vol de données de recherche sensibles qu'il a déposé sur l'entrepôt de recherche de l'établissement. Il vous reproche de « ne pas l'avoir suffisamment sécurisé ». Il a été menacé par l'attaquant sur sa messagerie personnelle d'un réseau social grand public : sa base de données de recherche et les résultats de sa recherche (qui doivent faire l'objet de plusieurs dépôts de brevet dans les prochains mois) seront revendues sur le darknet si une rançon de 10 bitcoins n'est pas payée dans les 24h.**

## Fil conducteur :

- Quelles actions prioritaires allez-vous mener ?
- Quelles sont les différents niveaux de responsabilités en jeu ? Disposez vous d'une charte numérique ou équivalente explicitant les responsabilités dans les sphères privées et publiques des populations ?
- Comment qualifiez-vous la finalité de cette attaque : Cyber ? Entrave au fonctionnement Situation d'ingérence ? Espionnage ? Lucratif ? Pré-positionnement stratégique ? Défi ? Amusement ? Autre ?
- Identifiez-vous les points de contact à mobiliser et signalements aux autorités à réaliser ?

# PHASE 3 : RELANCE DES ACTIVITES / DURCISSEMENT

# Stimulus 7

**Après signalement à la chaîne de gestion des incidents organisée par votre Ministère de tutelle, celle-ci contacte votre RSSI afin de disposer d'éléments sur l'attaque en cours. Elle souhaite savoir si l'établissement reçoit l'aide d'un prestataire technique (type PRIS, remédiation, avocat, etc.).**

## Fil conducteur :

- La cellule de crise a-t-elle connaissance du fonctionnement de la chaîne de signalement et gestion de crise ministérielle de tutelle ?
- Quelles actions prioritaires allez-vous mener ?
- Comment sont-elles réparties ?

# Stimulus 8

**L'attaque a conduit à éteindre l'ensemble du SI. Le RSSI constate que certains chercheurs affiliés à d'autres organismes de recherche ont rallumé des postes de travail contrairement au plan défini avec votre PRIS.**


## Fil conducteur :

- Quelles actions prioritaires allez-vous mener ?
- Comment sont-elles réparties ?
- Décidez-vous d'échanger avec :
  - les organismes tutelles des laboratoires de recherche impliqués ? A quel niveau ?
  - les directeurs et directrices des unités de recherche concernés ?
  - l'ensemble des populations concernées ?

# Stimulus 9

**Un agent vous contacte en se présentant comme agent de l'ANSSI, du CERT-FR précisément. Il vous indique vouloir vous accompagner et organiser une réunion avec toute votre cellule de crise. Il vous précise que le CERT-FR a été informé de l'attaque par la cellule de crise cyber de votre ministère de tutelle et évalue la gravité de l'attaque à un niveau maximal. Vos unités de recherche les plus sensibles et vos ZRR sont en effet touchées et le risque de latéralisation est critique.**


Fil conducteur :

- Répondez-vous favorablement à la demande ? Comment ?

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

3

# Fin d’exercice/débriefing

# Débriefing

**Présentation par les joueurs des points positifs et axes d'amélioration vis-à-vis de leur expérience**

Orientations :

- Avez-vous trouvé votre place et compris votre rôle dans cet exercice ?
- Qu'est ce qu'une crise pour vous ? Combien de crises avez-vous identifiées dans cette expérience ?
- Comment avez-vous vécu l'exercice ? Quels sont vos ressentis vis-à-vis des actions entreprises ?
- Quelles sont les 2/3 grandes décisions que vous avez prises ?
- Pensez-vous que votre gestion de crise d'origine cyber puisse se rapprocher de votre gestion de crise générale (Vigipirate, etc.) ?

# Quels enseignements à retenir d'une gestion de crise cyber ?

Organiser et préparer la cellule de crise (niveau stratégique et opérationnel)

Organiser la remontée d'information et l'outiller

Bien se préparer et s'outiller pour se donner les capacités (en particulier techniques) de réagir efficacement

Prendre des décisions (parfois incertaines)

Savoir communiquer en interne et avec les parties prenantes

RÉPUBLIQUE FRANÇAISE

*Liberté*
*Égalité*
*Fraternité*

# MERCI DE VOTRE PARTICIPATION !