Exercice PSSI

ISAE-ENSMA

Ecole Nationale Supérieure de Mécanique et d'Aérotechnique

Téléport 2 – 1 avenue Clément Ader BP 40109
86961 Futuroscope Chasseneuil Cedex
Tel. 05 49 49 80 80

www.isae-ensma.fr

Aéronautique – Espace – Transport - Energie

Ecole Nationale Supérieure de Mécanique et d'Aérotechnique
Téléport 2 - 1 avenue Clément Ader
BP 40109
86961 Futuroscope Chasseneuil Cedex
Tél : +33 (0)5 49 49 80 80

KIT EXERCICE " SUR TABLE "

1. Briefing

- Déroulement en 3 phases, deux fois 9 stimulus
- Pas de paroles croisées
- Qu'est-ce qu'il faut faire, qui contacter, quelles mesures, prévenir,
- Evaluation de la gravité
- Identification des procédures

2. Exercice

PHASE 1 : ALERTE/MOBILISATION

1er stimulus : 14m 30s

Fin année académique, recrudescence d'attaques dans le secteur = infostealers

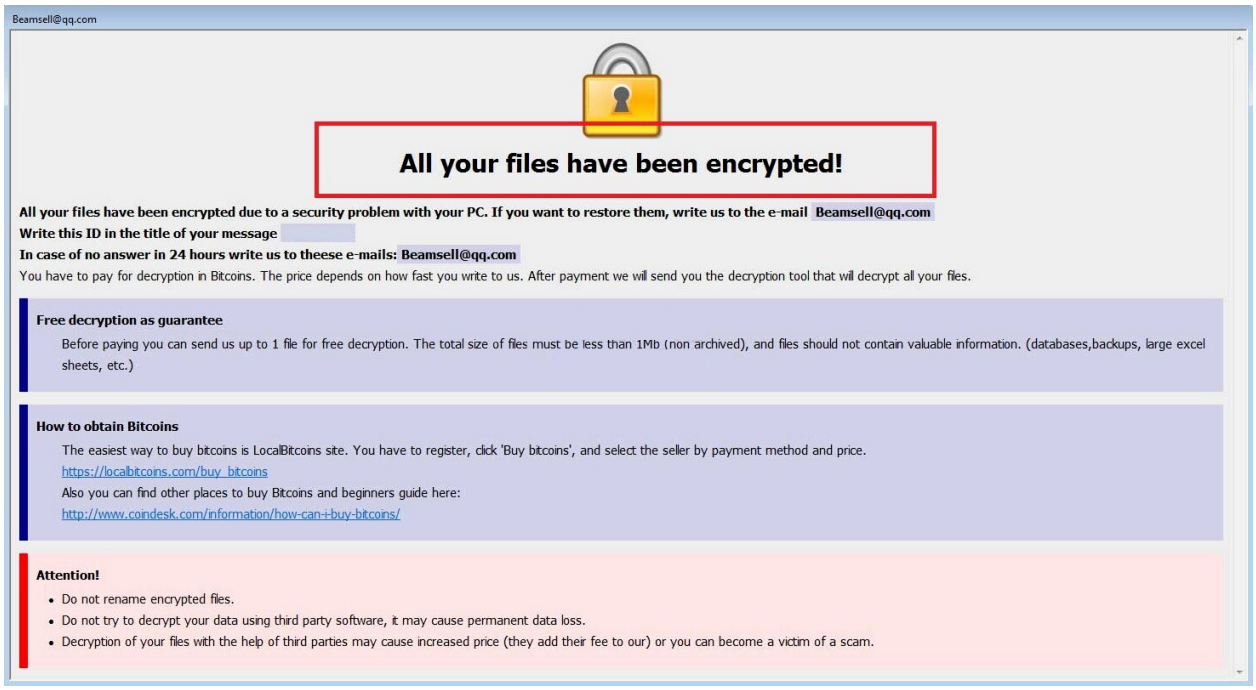
- Risques ?
  - Connection à dist. pour sessions VPN avec credentials volés (Infostealer)
  - Plus simple utlisateur présente risques par conséquence de la connexion
  - Enorme risque métier (examens...) et impact image de marque ENSMA, destructeur
- Organisation ?
  - Pour diminuer niveau menaces : diminuer risque, changer mot de passe mais personne pour le faire (étudiants...) donc limiter le nombre de connexions (déjà fermeture de Guacamole dans le passé)...
  - Réinstallation d'infra et isolation (confinement)
  - Préparation de fiche d'actions pour virus, fiche réflexe
  - Projets prévention, protection (pas assez...), conteneurisation des comptes, main courante => pas assez connu, identifier infra (DMZ, segm. réseau) pour être connue des infos
  - Prévenir RSSI, RENATER => qui prévenir si empêchement ?
  - Couper interconnexions ? (Poitiers... si niveau d'élévation trop élevé), pas forcément car ces connexions sont limitées dans le scope (faible nb de ports...)
    - => forward RSSI, Dir. DSI
  - Détection d'intrusion (déjà par Darktrace sur Teams)

- Anticipation du risque (nv PC, DSI blancs)

– Quels sont les projets à mener et outils dans la cellule crise ?
  - Alerte, Mobilisation, Conjointement avec PSSI (gestion de crise cyber)

2e stimulus : 22m

Nombre croissant de perrsonnels administratifs indiquent rencontrer des difficultés avec leurs oridnateurs. Certains voient apparaitre sur l'écran le message suivant: *pop-up "All your files have been encrypted !"*



– Actions prioritaires ?
  - Contact Edouard/Olivier
  - Evaluation de la gravité + se renseigner sur l'origine
  - Contact sur Teams RSSI, DDSI => oui mais avec quel info (diag Ordi(s), OS, sauvegarde existante ?)
    - Réponse graduée, également en fonction de la taille du secteur interne affecté
  - Débrancher le(s) PC(s)
  - Version de navigateur ? (plug-ins)
  - Réalité du chiffrement ?, car si vrai très important
  - Tableau de bord DSI (realtime), affichage ENT (et en fonction de la sévérité choisir le canal)

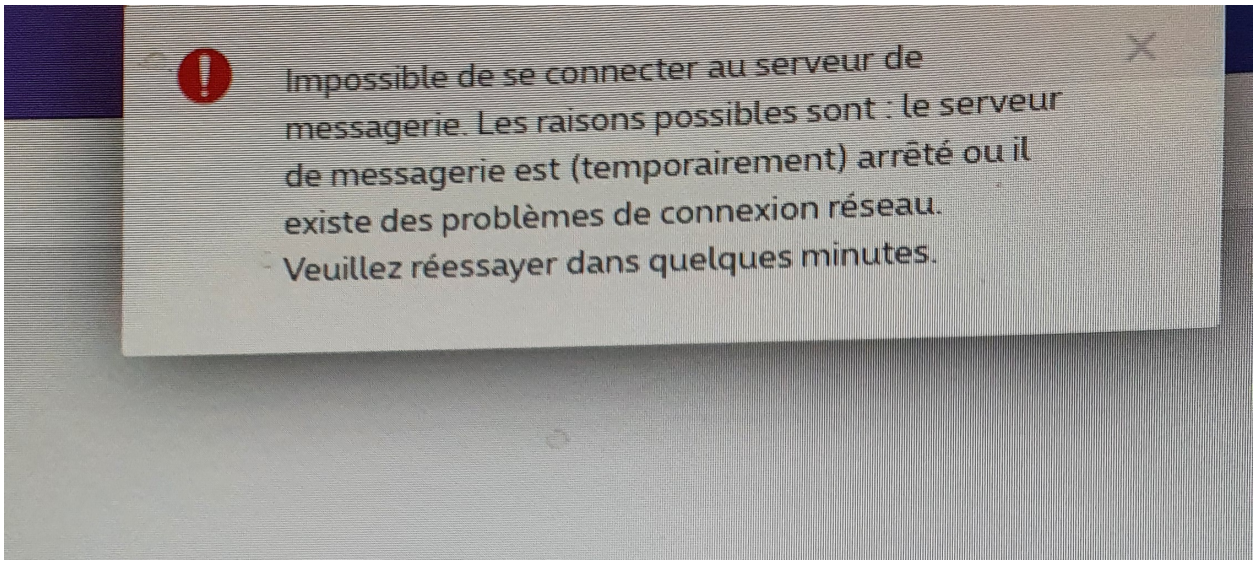
– Cellule de crise ?
  - Cyber, pas encore remontée à établissement si gravité plutôt faible
    - Si grave => directeur
    - Impact sur le travail
  - Fiche réflexe (limiter les dégats, alerter, évaluer...) qui peut la déclencher
    - Checklist de la situation (exemple armée), poids de la décision selon n'importe quel personnel qui peut dépasser décisions du supérieur et bilan (RETEX)

- Crise non préparée = catastrophe
- Décision en fonction de la politique (DSI ou direction, droits du RSSI [ex. couper réseau unilatéralement, etc.], différent côté humain ou technique car peut-être manque de compétences)
    - partage de la PSSI (utilisation des chartes déjà existantes)
    - livret de procédures pas assez exploité => procédures infra (ex. antivirus Mac et Linux, isolation VLANs)
    - matrice de compétences
    - limiter les coupures, car peut avoir impact collatéral
    - annuaire de crise

3e stimulus : 21m

La DSI 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 infrastrucutres 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.



confusion générale

- Impacts métiers ?
    - Impact ENSMA ?
        - Cloud de l'ENSMA ? MITM ?
        - Image de l'établissement ou chercheur
    - Niv de gravité ?

        - A-t-il juste oublié son MDP ? Serveur up ?
- Composition de cellule de crise ?
    - Cell de crise nécessaire ? oui car projet important bloqué
        - Pb purement technique : pas au dela d'aspect tech dont pas de cellule de crise et juste appel à la DSI (checklist...)
        - Gestion avec partenaires
        - Main courante (Excel)
    - Com de crise doit être maîtrisée "on a peut-être un pb ?..."
        - Non, personne communique, le préfet conférence de crise avec vrais éléments
        - Sévérité ? selon le personnel, et avis extérieur "il manque des gens" selon l'aspect
    - Kit de survie (clé USB, papier...)
- Posture de l'établissement vis-à-bis des partenaires et personnels ?
    - Situation politique selon le partenaire
    - Mesures conservatoires, pas forcément besoin de com ? => cadre éclairé et explication
- Eléments de langage clé en main ? Outils de com à disposition ? Ont-ils besoin d'être créés / enrichis / améliorés ?

PHASE 2 :

4e stimulus : 6m

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.

- Quelles actions prioritaires allez-vous mener ?
    - "Couper le feu" => com technique qui passe vers la direction
- Quels sont les risques de dégradation de la situation que vous anticipez ?

- Mauvaise com: message type pour ne pas donner infos erronées

– Quelles sont les actions de com que vous avez besoin de mettre en place ? Validation des coms éventuelles ? Le cas échéant, qui est reponsables de leurs émissions et des éventuelles réponses à réaliser ?
    - Action indirecte ?

5e stimulus : 6m 30s

Vous êtes alertés que votre système de visio est de temps à autre attaquée : messages politiques et actions perturbantes pendant certains enseignements et colloques de recherche.

Depusi la crise sanitaire, une grande partie de vos enseginements sont délivrés en distanciel via cet outil. L'étab. prépare la venue de personnalité pol. 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 tremes de nombre de connexion.

– Action prioritaires ?
    - Empêcher => deadline?
        - Planning prévisionnel, changement d'outil ? sauf que contraint
    - Trouver source
    - Veille techno (ex. Teams)
        - Injonction de l'ANSSI sur Pulsecure (VPN) : Eduvpn en attendant => redondance

- Se renseigner sur sec. de l'outil

– Qui est partie prenante de votre action ?
  - DSI, Direction

6e stimulus : 10m

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 brevets dans les prochains mois) seront revendues sur le darknet si une rançon de 10 bitcoins n'est pas payée dans les 24h.

– Actions prioritaires ?
  - Couper accès ?
    - Mais aucune preuve du vol donc vérif validité => trouver logs, enquêter
  - Contacter, diagnose
  - Vérif si sauvegarde, car si le cas que pb de vol de datas et réduction de la surface d'incident
  - Remonter à FSSI et ANSSI
    - Paiement de rançon interdit => si un seul utilisateur pas imp.

        - Chercheur risque de payer à titre indépendant
- Niveaux de resp. en jeu ? Disposez vous d'une charte num. ou équivalente explicitant les resp. dans les sphères privées et publiques des pop. ?
    - DSI ? Direction ?
- Comment qualifiez-vous la finalité de cette attaque : Cyber ? Entrave au fct ? Situation d'ingérence ? Espionnage ? Lucratif ? Pré-positionnement stratégique ? Défi ? Amusement ? Autre ?
    - Ingérence peu probable mais à ne pas écarter
    - Espionnage peu probable mais à ne pas écarter
    - Lucratif évident
    - Pré-positionnement stratégique à ne pas écarter
    - ...
- Indentifiez-vous les poins de contact à mobiliser et signalement aux autorités à réaliser ?
    - Chaîne SSI

PHASE 3 :

7e stimulus : 2m

Après signalement à la chaîne de gestion des incidents orgainsée 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'établisssement reçoit l'aide d'un prestataire technique (type PRIS, remédiation, avocat, etc.)

- La cellule de crise a-t-elle connaissance du fct de la chaîne de signalement et gestion de crise ministérielle de tutelle ?
    - Fiche prévention du RSSI etc.
    - A-t-on l'aide de qqn ?
        - Contact avocat OK
        - Pas de PRIS mais possible d'en contacter un et procédure
- Actions prioritaires ?
- Comment sont-elles réparties ?

8e stimulus : 10m

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 par votre PRIS.

image concertation

- Actions prioritaires ?
  - Isolation, bloquage ?
    - Risque d'aggravement de la situation
  - Référer à la direction
- Comment sont-elles réparties ?
  - Procédure de constatation d'infraction
  - Sanctions
- Décidez-vous d'échanger avec:
  - les organismes tutelles des labos de recherche impliqués ? A quel niveau ?
    - oui
  - les directeurs et directrices des unités de recherche concernés ?
    - oui
  - l'ensemble des pop. concernées ?
    - oui, expliquer à la pop.

9e stimulus : 5m

Un agent vous contacte en se présentant comme agent de l'ANSSI, du CERT-FR précisément. Il vous indique vouloir vous accompagner et organsier 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.

- Répondez-vous favorablement à la demande ? Comment ?
    - Vérifier que vraiment ANSSI (ex. appel téléphonique)
        - Traçabiliser

3. Débriefing

Tour de table :

- Azziz : identification et déclenchement d'actions qui ont un impact variable, avec un cadre éclairé, avec feedback
    - Procédures (fiches), checklists et indicateurs
- Mathis : Procédures au sein de la crise
- Gerald : attaque ciblée qui peut s'agrandir (ex. impact sur UP), pas assez de procédures de prévention
- Hervé : prévoir com autrement que par SI (ex. Teams qui peut être sur mobile, sauf si coupure totale)
- Franck : anticipation et info des utilisateurs (éviter les mauvaises manip.) sur les risques => prévention
- Charlie : identification des crises majeures et fiches
- Olivier (Durand): Qualité des procédures => et possiblement certifiées (ISO, AFNOR...), mesure du temps à mobiliser
- Thierry : trop loin dans le détail ? identifier des points de travail
- Niveau de sévérité, doc, chaîne de resp., com interne externe, faire vivre les procédures (RETEX...)
- Nicolas : gros travail