

# Cybersécurité et Communication de crise

Judicaël Blanc  
Directeur Général  
AlphaXData



Alexandra Salou  
Département Informatique  
IUT d'Aix-en-Provence  
Laboratoire Imsic



# POURQUOI ?



## Piratage de la Métropole Aix-Marseille-Provence, les pirates sont de retour

Posted On 28 Août 2020 By : Damien Bancal Comments: 4 Tag: fuite, leak, Métropole Aix-Marseille-Provence, pysa, rançongiciel

Après le piratage de la Métropole Aix-Marseille-Provence, en mars 2020, les pirates diffusent, six mois plus tard, des milliers de données volées à l'institution territoriale.

Nouveau piratage, et nouvelles données diffusées par des pirates informatiques. Cette fois c'est la Métropole Aix Marseille Provence qui a été malmenée.

Souvenez-vous, **14 mars 2020**. Malgré les efforts et efficacité des équipes informatiques, un **rançongiciel (ransomware)** se répand comme une traînée de poudre dans les systèmes de la mairie de Marseille et de la Métropole Aix-Marseille-Provence.

Six mois plus tard, les pirates du groupe **Pysa** sortent de l'ombre. Ces terroristes numériques ont diffusé les données volées en mars. Selon ce que j'ai pu découvrir, deux espaces cloud sur le web regroupant 40Go de documents volés par les malveillants. « **Nos vieux amis**. Indiquent les pirates. **Jolie province au sud de la côte française. Notre coopération a été très longue et fructueuse, et**

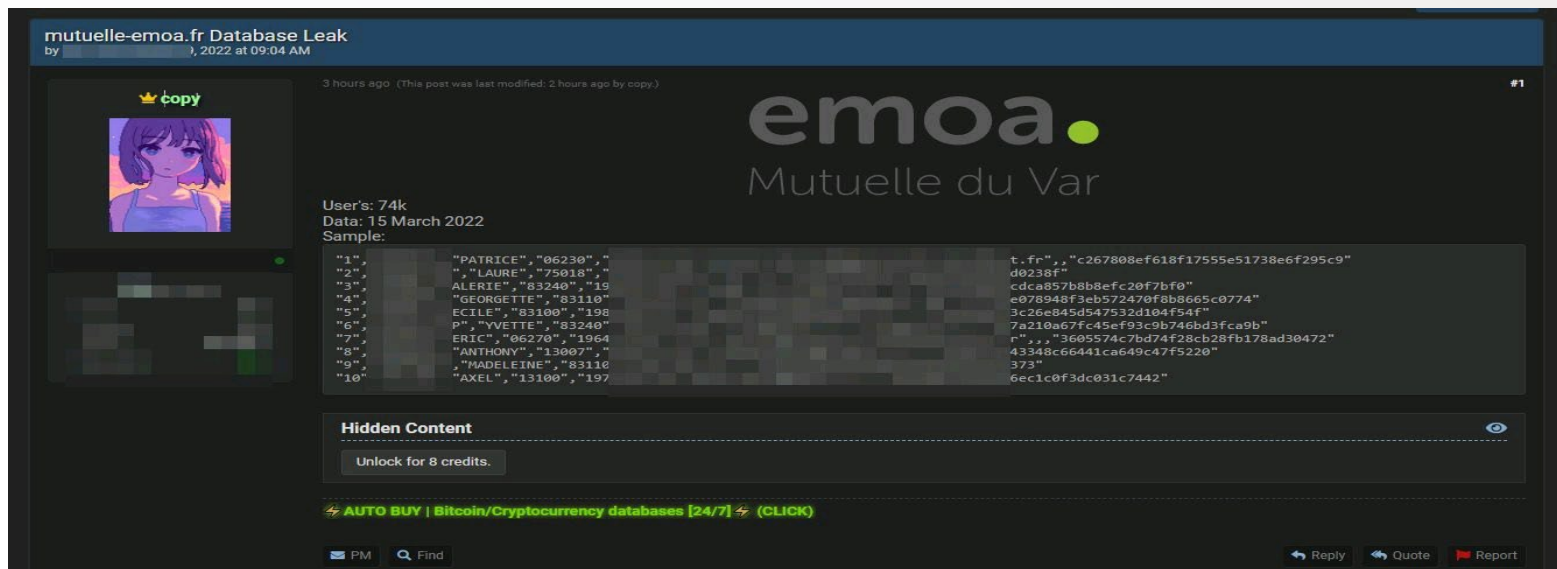
## Résident d'Aix-Marseille-Provence ?



**Ce sont vos informations !**

# POURQUOI ?

## Adhérent à la Mutuelle Var ?



The screenshot shows a forum post on a dark-themed website. The post title is "mutuelle-emoa.fr Database Leak" and it was posted by "by" on "1, 2022 at 09:04 AM". The user's profile picture is a character with purple hair. The post content includes the text "emoa. Mutuelle du Var" and a list of 10 entries, each with an index number and a name/ID pair. A "Hidden Content" section is visible below the list, with a button that says "Unlock for 8 credits." At the bottom of the post, there is a link: "AUTO BUY | Bitcoin/Cryptocurrency databases [24/7] (CLICK)".

mutuelle-emoa.fr Database Leak  
by 1, 2022 at 09:04 AM

3 hours ago (This post was last modified: 2 hours ago by copy.)

emoa.  
Mutuelle du Var

User's: 74k  
Data: 15 March 2022  
Sample:

```
"1", "PATRICE", "06230", "t.fr", "c267808ef618f17555e51738e6f295c9"  
"2", "LAURE", "75918", "d0238f"  
"3", "ALERIE", "83240", "15", "edca857b8b8efc20f7bf0"  
"4", "GEORGETTE", "83110", "19", "e078948f3eb572470f8b8665c0774"  
"5", "ECILE", "83100", "198", "3c26e845d547532d104f54f"  
"6", "YVETTE", "83240", "P", "7a210a67fc45ef93c9b746bd3fca9b"  
"7", "ERIC", "06270", "1964", "r", "3605574c7bd74f28cb28fb178ad30472"  
"8", "ANTHONY", "13097", "43348c66441ca649c47f5220"  
"9", "MADELEINE", "83116", "373"  
"10", "AXEL", "13100", "197", "6ec1c0f3dc031c7442"
```

Hidden Content

Unlock for 8 credits.

AUTO BUY | Bitcoin/Cryptocurrency databases [24/7] (CLICK)

PM Find Reply Quote Report

**Vos données sont vendues librement !**

# Communication de crise

Plusieurs actions possible :

- Initier un dialogue avec les équipes cyber et IT hors période de crise
- Anticiper les scénarios de crise
- Construire une stratégie de crise en amont
- Communiquer auprès des collaborateurs sur l'état de la situation et les consignes à appliquer
- Identifier les parties prenantes externes
- Travailler les argumentaires, les postures de communication et les messages clés
- Préparer une trame de communication de risque
- Identifier des porte-paroles potentiels
- Anticiper les éventuelles questions de crise
- Créer une boîte à outils dédié à la gestion d'une crise
- Former les équipes à la gestion du volet communication



# Communication de crise

Le rôle de la communication dans une crise cyber :

1. Préserver la réputation et l'image de son organisme pendant et en sortie de crise.
2. Rassurer rapidement les publics concernés sur le fait qu'un dispositif de crise a été mobilisé et gérer « l'impact émotionnel » de la crise
3. Modérer les impacts de la crise (court terme et long terme)
4. Montrer la mobilisation de l'organisme pour trouver une solution rapide au problème.



# Communication de crise

Au sein d'une cellule de crise, la communication de crise cyber sert à :


1. Définir la stratégie de communication au regard du contexte (posture pro-active ou réactive ?).
2. Préparer les messages adaptés à chaque cible, ce qui comprend la vulgarisation d'éléments techniques et les décliner en fonction des canaux de communication.
3. Trouver des canaux de communication alternatifs en cas d'indisponibilité des outils de communication.
4. Analyser et faire évoluer les postures de communication en fonction de l'évolution de la crise et de sa perception par les publics.
5. Assurer la cohérence et la coordination des différents types de communication qui sortent de l'organisme : la communication technique, institutionnelle et politique.





# Communication de crise

Quelques recommandations pour une communication de crise efficace :

- Être dans la transparence maîtrisée, respecter les faits, ne pas mentir ou indiquer les suppositions faites.
  - Être accessible, utiliser un vocabulaire simple et pédagogique.
  - Être concret, ne pas rassurer sans éléments de fond.
  - Éviter d'adopter un ton et un vocabulaire trop anxiogène.
  - Garder de la cohérence, ne pas se contredire dans la durée et d'un point d'émission d'information à l'autre.
  - Être complet, s'adresser à toutes les cibles, de l'organisation qui sont en droit d'attendre des éléments sur la situation.
  - Éviter le « Pas de commentaire » ;
  - Éviter une attitude négative tout en reconnaissant les problèmes.
- 

# Communication de crise

Quelques recommandations pour une communication de crise efficace :

- Donner de la visibilité sur les actions mises en œuvre sans s'engager sur des dates trop précises.
- Ne pas se précipiter : respecter et expliquer le temps long des investigations techniques.
- Ne pas attendre d'avoir l'exhaustivité des informations afin d'éviter qu'un tiers ne communique avant l'organisme.
- Ne pas chercher à désigner un coupable, ne pas faire d'attribution, qui reste une décision particulièrement complexe et politique.
- Faire prévaloir la solidarité.
- Conserver un contact régulier avec les différentes cibles.
- Être réactif, essayer de conserver un objectif de temporalité.
- En cas de judiciarisation, limiter sa communication pour respecter le secret de l'instruction.



# Communication de crise

Liste (non-exhaustive) des sources et références :

- ISO/IEC 27001
- ISO/IEC 22301
- ANSSI Guide gestion crise cyber
- AFNOR SPEC 2208



# L'assurance des risques cyber en crise

## L'assurance des risques cyber en crise



Pour Olivier Wild, président de l'Amrae, « le marché de la cyberassurance n'existera peut-être plus l'an prochain »

LEMAGIT



## Assuré contre les menaces cyber ?

# La clé c'est l'anticipation !

## Merci !

Judicaël Blanc  
Directeur Général AlphaXData  
☎ : 07 80 99 93 15  
contact@alphaxdata.com

Alexandra Salou  
Département Informatique  
IUT d'Aix-en-Provence  
Laboratoire Imsic  
alexandra.SALOU@univ-amu.fr

