Armateurs de France

ENSM
ÉCOLE NATIONALE SUPÉRIEURE MARITIME

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Ministère de l'Environnement, de l'Énergie et de la Mer

GICAN

Cluster Maritime Français
Le Faire-Savoir Maritime
The Maritime Voice

MARINE CYBERSÉCURITÉ

Consulter le guide maritime de l'ANSSI :

https://www.ssi.gouv.fr/actualite/guide-des-bonnes-pratiques-de-securite-informatique-a-bord-des-navires/

Section de recherches de la Gendarmerie maritime
67, rue de Buzenval 78800 Houilles
tél. : **01 30 86 10 87** – Email : **srgmar.houilles@gendarmerie.defense.gouv.fr**

CYBERGEND INVESTIGATION & CRIMINALISTIQUE

Prépresse de la marine – N° 17636 – 05-2017 - ©JM-Leroutier

CYBERMALVEILLANCE

Guide sur la **préservation** des **traces** et **indices**

Escroquerie, phishing, skimming, atteinte aux systèmes de traitement automatisé de données, chantage, faux ordres de virement, deni de service, apologie du terrorisme,… tel est le visage de la cybermalveillance.

La cybersécurité est l'affaire de tous.

Le traitement judiciaire de la cybermalveillance contribue à la sécurisation des échanges par voie numérique. La préservation des traces et indices numériques est alors fondamentale pour identifier les technologies employées par les malfaiteurs et les neutraliser. En effet, ces données sont par nature délicates, volatiles et périssables dans le temps. De fait, il convient d'agir rapidement et avec méthode, avant que les enquêteurs judiciaires en nouvelles technologies n'interviennent.

Section de recherches de la Gendarmerie maritime
67, rue de Buzenval 78800 Houilles

VOUS **ÊTES** SUR PLACE

ET CONSTATEZ L'ATTAQUE OU LA COMPROMISSION

1. Consignez par écrit le plus vite possible les raisons pour lesquelles vous pensez avoir été victime d'un piratage ou d'une attaque informatique. Ne cherchez pas à user de termes techniques, soyez surtout précis et concis.
2. Si possible, après avis de votre SSI, isolez le poste informatique concerné du réseau.
   Ne touchez à rien et surtout ne débranchez pas le poste informatique.
3. Si ce dernier est connecté à un réseau via un serveur, récupérez un maximum d'éléments comme l'adresse IP du poste ou des postes compromis, les logs serveurs, les adresses IP extérieures ayant sollicité l'entrée sur le système, les trames IP si cela est possible.
   Notez la date et heure de l'attaque.
   Si le poste possédait l'autorisation d'accéder à l'Internet à temps complet ou durant une période, précisez le.
4. Ne pas activer les stratégies dédiées à une restauration système automatique du poste attaqué ou contaminé.
   Récupérez les informations liées au(x) compte(s) utilisateur(s), les dernières actions réalisées si elles sont consultables en dehors du périmètre du poste informatique concerné.
5. Si l'attaque a consisté à l'adressage d'un ou de mails avec pièces jointes ayant été détecté par la suite par l'antivirus installé, pensez à identifier le mail, son expéditeur (mail et IP) mais fournissez également le nom de votre solution antivirus, sa version, ses options.

VOUS **N'ÊTES PAS** SUR PLACE

ET CONSTATEZ L'ATTAQUE OU LA COMPROMISSION

1. Consignez par écrit le plus vite possible les raisons pour lesquelles vous pensez avoir été victime d'un piratage ou d'une attaque informatique.
   N'usez pas de termes techniques, soyez surtout précis et concis.
2. Si possible, faites des captures écrans de ce que vous observez depuis votre poste, notez les dates et heures, les actions en cours.
   MAIS NE MODIFIEZ RIEN en supprimant des documents ou en répondant à des sollicitations via des fenêtres. Laissez les messages qui apparaissent.
3. N'éteignez pas votre poste, isolez ce dernier du réseau en déconnectant le PC au WIFI ou en ôtant le câble RJ45 (Ethernet). Laissez votre PC alimenté électriquement s'il s'agit d'un portable.
4. Notez votre nom d'utilisateur, votre session, les actions que vous avez réalisées, les mails lus et/ou répondus. Si votre antivirus/firewall s'est déclenché pour vous signaler un problème, mentionnez-le. Précisez la version de votre antivirus si possible.

CONTACTEZ
LE PLUS RAPIDEMENT POSSIBLE
LES SERVICES DE LA GENDARMERIE MARITIME
AUX NUMÉROS SUIVANTS :

Atlantique :	+ 33 2 98 22 22 17
Manche Mer du Nord :	+ 33 2 33 92 54 00
Méditerranée :	+ 33 4 22 43 71 65
Outre-mer/International :	+ 33 6 72 95 90 17

CONTACTEZ
LE PLUS RAPIDEMENT POSSIBLE LES SERVICES
DE LA GENDARMERIE MARITIME

Du respect des règles énoncées, de votre action de préservation des traces et indices que vous aurez effectuée, dépendent l'identification des auteurs et la judiciarisation des infractions commises.