

FICHE CYBER

Fraude au faux dépannage informatique

Statut : **En cours**

Secteurs affectés : **Tous**

Zones géographiques touchées : **Monde**

Objectif : **Lucratif**

Affiche une fausse alerte
et se fait passer pour
un support informatique



Attaquant



Utilisateur

Récupère l'accès de
l'ordinateur de la victime



Attaquant

SYNTHÈSE

La fraude au faux dépannage informatique, dite aussi à la réparation informatique ou au faux support technique, est une escroquerie qui consiste à faire apparaître dans le navigateur de la victime un message lui indiquant que son ordinateur est infecté par un logiciel malveillant. La victime est incitée à appeler un support téléphonique et à effectuer un paiement.

Si ce phénomène cybercriminel n'est pas nouveau, il connaît une recrudescence depuis ces derniers mois. Plusieurs milliers de victimes sont ciblées chaque année sur le territoire national français.

EN QUOI CONSISTE CE PHÉNOMÈNE CYBERCRIMINEL ?



Techniquement, il s'agit d'une **fenêtre de type « pop-up »** qui apparaît subitement sur le navigateur de la victime.

Dans la majeure partie des cas, ce genre de message s'affiche lorsque la victime consulte un site *web*, sur lequel les cybercriminels ont ajouté une ligne de codes malveillants.

L'objectif du message malveillant est de **créer un sentiment de panique chez la victime afin qu'elle appelle un numéro de téléphone d'assistance** qui est en réalité géré par des cybercriminels.

Dans certains cas, les malfaiteurs demandent à la victime d'installer un logiciel de prise de contrôle à distance, sous prétexte de dépanner son ordinateur.



Dans les faits, les malfaiteurs en profitent pour **dérober des informations personnelles ou bancaires afin de les exploiter ou de les revendre ultérieurement**.

En termes de logistique, les cybercriminels agissent en bande organisée et se regroupent dans des centres d'appel dédiés à ce type d'activité.

LEVIERS DE PRESSION UTILISÉS

Gravité



La fenêtre du navigateur *web* indique que **l'ordinateur de la victime est compromis**.

Urgence



La fenêtre est **intrusive et bloque la navigation** de la victime en indiquant un numéro à contacter.

Manipulation

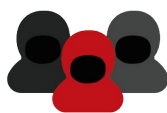


La victime **entre en contact** avec un malfaiteur qui prétend qu'il va dépanner son ordinateur, mais qui va **l'escroquer**.

QUE DIT LA LOI ?

Dans le Code pénal, les fraudes à la réparation informatique peuvent être qualifiées de la manière suivante :

- ✓ Article 313-1 et 313-2 : Escroquerie en bande organisée
- ✓ Article 323-1 à 323-7 : Atteintes à un système de traitement automatisé de données (STAD)
- ✓ Article 312-1 : Extorsion de fonds



1. PRÉPARATION

Les malfaiteurs se regroupent dans des centres d'appels et ils diffusent des messages frauduleux en masse afin de piéger de potentielles victimes.



2. MESSAGE D'ALERTE

L'utilisateur navigue sur internet de manière habituelle. Une fenêtre malveillante s'affiche indiquant que son ordinateur est infecté.



3. SOUTIEN FICTIF

La fenêtre affiche un numéro de téléphone à contacter pour joindre un support informatique en apparence légitime.



4. PRISE DE CONTACT

L'utilisateur appelle le numéro indiqué. Il communique alors sans le savoir avec des malfaiteurs qui souhaitent lui soutirer une somme d'argent.



5. COMPROMISSION





Le malfaiteur fait payer le service d'un prétendu dépannage en faisant installer un logiciel qui lui donne en réalité un accès aux données de l'ordinateur de la victime.



6. ACTIONS FRAUDULEUSES

Le malfaiteur récupère puis exploite ou revend les données personnelles et financières de la victime.

COMMENT S'EN PRÉMUNIR ?

-  Téléchargez vos logiciels sur des sites officiels.
-  En cas de doute, renseignez-vous auprès de cybermalveillance.gouv.fr. Des infographies et conseils vous permettront de connaître les démarches à suivre.
-  N'appellez pas le numéro qui s'affiche, redémarrez votre ordinateur et déposez plainte.
-  Ne donnez pas accès à votre ordinateur sous la pression ou la contrainte. Aucun service d'assistance légitime ne vous demandera vos coordonnées bancaires.