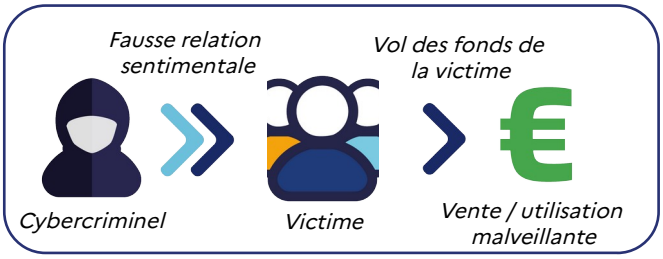
MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

COMCYBER-MI

FICHE CYBER

Escroqueries liées à la fausse romance
(Pig butchering)

Statut : **En cours**
Secteurs affectés : **Tous**
Zones géographiques touchées : **Monde**
Objectif : **Vol de fonds, cryptoactifs, escroquerie**



SYNTHÈSE

Le "*pig butchering*" est une méthode d'escroquerie à la romance en ligne très élaborée consistant à créer une fausse relation sentimentale pour inciter les victimes à verser des sommes d'argent importantes. Cette pratique tire son nom d'une analogie avec l'équarrissage d'un cochon, illustrant la façon dont les escrocs amadouent leurs victimes avant de les dépouiller complètement de leurs ressources financières.

I. De quoi parle-t-on ?

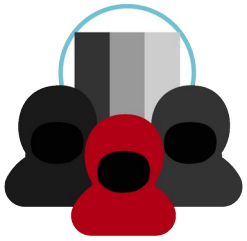
Il s'agit d'un ensemble d'escroqueries dans lesquelles un criminel initie une romance fictive avec une victime afin de l'escroquer et de récupérer des fonds sous couvert de faux investissements, de jeux en ligne ou d'appels aux dons pour des prétextes fallacieux (frais de santé par exemple).

Les auteurs obtiennent les numéros de téléphone et les informations personnelles de leurs cibles via des bases de données volées, puis les contactent par diverses applications de messageries. Ils se présentent souvent comme une jeune femme, ou plus rarement comme un jeune homme, et parviennent à convaincre la victime d'investir des sommes de plus en plus importantes. Une fois les fonds récupérés, les escrocs coupent brutalement tout contact.

Ce phénomène, en pleine expansion, touche plusieurs millions de victimes chaque année et représente un préjudice total de plusieurs milliards d'euros.

II. Profils et objectifs des cybercriminels

La majorité de ces infractions sont commises par des cybercriminels provenant principalement : **:**



- d'Afrique subsaharienne (« brouteurs »),
- d'Asie du Sud-Est, où, dans certains pays comme le Cambodge, les escrocs sont eux-mêmes victimes de trafic d'êtres humains, et forcés de travailler sous contrôle strict de groupes criminels organisés.

Motivation principale :

- l'appât du gain : les fonds volés servent à financer d'autres activités criminelles telles que le trafic de stupéfiants, le trafic d'être humains et les jeux illicites, ainsi qu'à rémunérer les membres des organisations.

III. Modes opératoires

Les escrocs utilisent des stratégies bien rodées pour séduire leurs victimes et leur soutirer de l'argent :

- **prise de contact :** Les escrocs contactent leurs cibles via des applications de messagerie en prétextant une erreur (mauvais numéro, mauvais destinataire). Ils entament ensuite une conversation amicale qui peut rapidement devenir plus intime.
- **mise en place de l'emprise :** pendant plusieurs jours ou semaines, les escrocs instaurent une relation de confiance en échangeant régulièrement des messages, des photos et des informations personnelles. Ils exploitent souvent l'isolement et/ou la vulnérabilité émotionnelle de leurs victimes.

Une fois la relation « sentimentale » avancée, l'escroquerie commence :

Carte PCS

- **la victime est convaincue d'envoyer de l'argent sous prétexte d'investissements ou pour régler des frais urgents.** Les moyens de paiements utilisés incluent :
  - les cartes prépayées (PCS, Neosurf, Transcash),
  - les mandats cash (Western Union) ;
  - les cryptoactifs : notamment les stablecoins comme l'USD Tether permettant de transférer des fonds rapidement et sans fluctuations importantes.


Stablecoin USDT Tether

- Une fois la confiance établie, les escrocs peuvent orienter la victime vers d'autres formes d'escroquerie, telles que :
  - la fraude à l'investissement (fausses plateformes d'achat de cryptoactifs),
  - la fraude à l'emploi en ligne (tâches prétendument rémunérées).

- Lorsque la victime commence à douter ou réalise qu'elle a été dupée, les escrocs **coupent tout contact** et disparaissent avec les fonds.

Comment s'en protéger ?

Soyez vigilant face aux messages suspects : méfiez-vous des messages provenant d'inconnus prétendant vous connaître sans que vous puissiez les identifier clairement.

Repérez les signes d'escroquerie : soyez attentif aux mauvaises traductions et aux fautes d'orthographe dans les messages, qui peuvent indiquer une tentative de fraude. De plus, les escrocs refusent généralement les visioconférences et sont réticents à envoyer des preuves d'identité.

Vérifiez la légitimité des plateformes d'investissement : n'effectuez des transferts de fonds que vers des plateformes reconnus et conformes à la réglementation.

Restez méfiant face aux offres trop alléchantes : si une opportunité semble trop belle pour être vraie, elle est probablement frauduleuse.

Ne cédez pas à la pression : méfiez-vous des incitations à investir rapidement sous prétexte de ne pas manquer une opportunité.

Soyez attentif aux frais de retrait élevés : des frais anormalement importants peuvent indiquer une arnaque.

SOURCES

Rapport sur la cybercriminalité 2024 – CCMI :
https://www.interieur.gouv.fr/actualites/actualites-du-ministere/rapport-annuel-sur-cybercriminalite-2024
Cybermalveillance.gouv.fr :
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/programmes-malveillants-virus-2023-ra