LE CHANTAGE À LA VIDÉO PORNOGRAPHIQUE

Category: Sécurité informatique
Tag: Enquête

Nos messageries sont inondées de scams portant sur un chantage à la vidéo suite à l'installation d'un virus.

Nancy, le 14/05/2020 :

Attention !!!!

Nous avons reçu plusieurs spams recommençant le chantage à la vidéo porno suite à l'installation d'un virus !

La menace est identique à celle communiquée ci-dessous.

NE DONNEZ PAS UN SOU !

Nous en recevons régulièrement car nous avons plusieurs adresses publiques. Nous publions quelques exemples sachant que nous en avons reçu en anglais et en espagnol (!). Il est demandé de payer en crypto monnaie. Une adresse est fournie dans le mail.

Les scams au chantage à la vidéo

Les recherches que nous avons effectuées montrent qu'il s'agit d'une arnaque à très grande échelle au vu du nombre de consommateurs qui nous contactent ou qui témoignent !

Nancy, le 13/09/2019 :

Nous avons reçu un mail de l'un de nos adhérents qui nous a fait plaisir ! Un de ces escrocs a été arrêté ! Nous avions reçu plusieur spams de cette personne. Nous publions l'article dans le lien ci-dessous :

https://bit.ly/2GdQ6Vp

Le contenu :

Il est toujours construit de la même façon. L'escroc vous annonce :

- Avoir installé un virus qui au choix lui a transmis le contenu de votre messagerie ou de votre ordinateur. Une autre option est l'activation de la webcam quand vous êtes allé sur des sites porno !
- Qu'il est inutile de vouloir nettoyer l'ordinateur ou de le formater car il a volé les données
- Que vous devez lui verser des sommes en crypto monnaies dans un délai de 48H maximum faute de quoi, vos données seront rendues publiques.
- Il vous promet qu'il effacera les données si vous payez

Il est à noter que les prix sont variables. Nous en avons qui demandent 520 € d'autres 2000 $!

Les recherches de l'ADC Lorraine :

Les adresses :

Les adresses mails ne donnent aucun résultat. Le contenu ne permet pas non plus d'exploiter la moindre information.

Par contre l'article de VAR MATIN publié ci-dessous donne la clé. Il s'agit d'un vol massif d'adresses mails (770 millions d'adresses) ! Cet article donne aussi de bons conseils qu'il fait suivre.

"Ne payez pas de rançon!"

Cela explique l'explosion d'envoi de ces faux messages.

Les adresses IP :

A partir d'un mail, nous avons réussi à identifier une adresse IP. Le site traceroute permet de constater que l'émetteur utilise une adresse d'un site colombien dénommé cable.net.co !

Un de ces mails a été envoyé de Croatie. Un troisième est parti d'Indonésie !!!!

Les forums :

Nous publions plusieurs forums ou articles qui montrent clairement le problème : Niort : la police lance un appel à la vigilance après des tentatives de "ransomware"

Le site zataz donne des informations précises. Il a recensé 301 versions (!) : Chantage par mail : NON vous n'avez pas été piraté

Le site bitcoinabuse.com permet de voir l'origine de l'adresse donnée pour le paiement : Bitcoin

Abuse Database

Nous publions une autre recherche qui est plus riche encore que la première : Base de données d'abus de Bitcoin

Un de ces mails a été envoyé de Croatie. Un troisième est parti d'Indonésie !!!!

Vérifier si on est concerné !

Nous publions un lien qui donne des précisions : 773 millions de mails piratés, comment savoir si vous êtes concernés

Il est indique que le site 'ai-je été pwned? permet de vérifier si votre adresse mail est concernée.

Dans ce cas, changez d'urgence le mot de passe. Nous vous déconseillons d'effectuer le moindre paiement suite à réception de ces mails. En outre, rien n'interdit à ce hacker de recommencer !!!

Par contre, nous vous conseillons de changer les mots de passe et d'installer un outil gratuit dénommé mailwasher qui permet de bloquer et de détruire à distance les mails non sollicités. C'est vous qui décidez ou non de garder les mails. La version payante permet le filtrage d'un nombre illimité de comptes mails.