AGENCE NATIONALE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Centre d'Alerte et de Réponse et
Aux Incidents de Sécurité Informatique

NATIONAL AGENCY FOR INFORMATION AND COMMUNICATION TECHNOLOGIES

Computer Incident Response Team

ALERTE DE SECURITE

SEXTORSION : chantage à la vidéo

Contenu

I. Contexte et Définition

Internet permet de converser anonymement et sans engagement avec des personnes du monde entier, par écrit, par un service de téléphonie ou par webcam. Or, la sextorsion le montre bien : à l'autre bout de la ligne se cache parfois quelqu'un dont les visées sont criminelles et préméditées. Sa cible craint dès lors de se trouver dans l'embarras vis-à-vis de sa famille, de ses amis ou de ses connaissances. En réalité, nos activités sur Internet sont souvent moins anonymes que nous le pensons.

La sextorsion est une méthode de chantage exercée sur une personne à partir de photos ou de vidéos la montrant nue ou en train d'accomplir des actes sexuels. Le terme anglais sextorsion est une contraction des mots sex et extortion (terme anglais qui désigne le chantage).

II. Modes opératoires

Variante classique : Les cibles sont contactées sur les réseaux sociaux (Facebook ou site de rencontre) par une séduisante inconnue qui souhaite être admise dans leur liste d'amis. Si la cible accepte, sa nouvelle amie virtuelle la retrouve sur un tchat. Au cours de la conversation, l'amie propose de poursuivre en mode vidéo (sur Skype par exemple). La cible est alors invitée à se déshabiller, ou à adopter des postures lascives. Les actes accomplis par la cible devant la webcam sont enregistrés à son insu. Peu après, elle sera contactée par des maîtres-chanteurs qui lui demanderont de l'argent, sous peine de voir les images diffusées (mise en ligne sur Youtube avec mention du nom, envoi par courriel à des proches, à des amis ou à l'employeur ou publication d'un lien sur Facebook).

Variante malware : dans ce cas de sextorsion, les ordinateurs, tablettes et smartphones des personnes qui surfent sur des sites à contenus pornographiques spécialement préparés sont infectés par un logiciel malveillant, ou malware. Ce dernier active la webcam de la cible pendant qu'elle regarde de la pornographie sans qu'elle ne se doute de rien. Ces vidéos souvent compromettantes sont transmises aux criminels qui font alors chanter la victime en la menaçant de publier la vidéo ou de l'envoyer à la liste d'amis qu'ils ont pris soin de lui voler.

Variante spam : il arrive aussi que ces tentatives de chantage soient envoyées à de nombreuses personnes sous forme de « menaces creuses » dans des spams. Les malfaiteurs espèrent en effet que parmi les destinataires se trouvent des personnes qui ont récemment regardé de la pornographie et que, intimidées par la menace, elles payent ce qui leur est réclamé. Dans ces cas-là, l'ordinateur des personnes touchées n'est pas infecté et les malfaiteurs ne possèdent aucun matériel compromettant.

III. Victimes et circonstances

La grande majorité des victimes de chantages à la vidéo sexy sont des hommes, adolescents ou adultes. La conversation a souvent lieu dans un français, un allemand ou un anglais approximatif. Les malfaiteurs opèrent depuis l'étranger et les paiements doivent être effectués

sur des comptes qui se trouvent eux aussi à l'étranger. Il arrive régulièrement que le matériel compromettant soit publié, même si la victime a payé, ou qu'un second paiement soit exigé.

IV. Comment se protéger ?

Pour éviter de tomber dans le piège :

- N'acceptez jamais des propositions d'amitié ou de rencontre en ligne de personnes que vous ne pouvez pas identifier clairement ou que vous n'avez jamais rencontrées dans la vie réelle.
- Ayez toujours à l'esprit que toute conversation par webcam est susceptible d'être enregistrée. Par conséquent, renoncez à tout acte qui pourrait vous mettre dans l'embarras.
- Désactivez toujours votre webcam quand vous n'êtes pas en discussion vidéo et collez un papier sur l'objectif.
- Faites les mises à jour régulières du système d'exploitation, du navigateur et de l'antivirus de vos appareils électroniques pour les protéger des malwares.
- Informer votre entourage sur cette méthode de chantage.

Si vous êtes victime d'une sextorsion :

- N'entrez pas en matière sur les exigences des maîtres-chanteurs. Ne payez pas !
- Rompez immédiatement tout contact avec la personne qui a servi d'appât et avec les maîtres-chanteurs. Supprimez-les de votre liste d'amis et ne réagissez à aucun message (courriels, SMS, etc.).
- Si les maîtres-chanteurs ont publié du matériel photo ou vidéo, signalez-le sans tarder à la plate-forme concernée (Youtube, Facebook, etc.) et exigez que tout soit effacé.
- Activez une alerte Google personnalisée. Vous serez ainsi averti dès qu'une photo ou une vidéo à votre nom sera publiée sur Internet.
- Conservez toutes les preuves (matériel photo et vidéo utilisé pour vous faire chanter, coordonnées des maîtres-chanteurs et de l'appât, messages qu'ils vous ont envoyés – historique des conversations en ligne, courriels, etc. – informations sur les transactions) et avisez les services compétents.
- Parlez-en à une personne de confiance et recherchez un soutien psychologique si cette situation vous pèse