[Transcript] Monde Numérique - Actu Technologies / [Interview] Benoit Grünemwald (Eset) : le phénomène de sextorsion en augmentation

Au premier trimestre 2023, comparé au dernier trimestre 2022, il y a eu une augmentation de 200% de cette catégorie de menaces que l'on va appeler s'extorsion, basée principalement sur des e-mails d'amsonnage, contenant ou pas d'ailleurs des vrais photos.
C'est le rendez-vous mensuel consacré à la cyber sécurité en partenariat avec EZ.
On va parler cette semaine d'un phénomène visiblement en augmentation, la s'extorsion, autrement dit l'extorsion de données à caractère sexuel ou simplement intime.
Bonjour, Benoît Grenemvalde.
Bonjour, Jérôme.
Expert cyber sécurité chez EZ.
Récemment, le FBI a mis en garde contre une pratique qui semble se développer.
Ce sont des pirates qui mettent la main sur des photos liées à des chirurgies esthétiques et le but du jeu, c'est de dévoiler des photos intimes.
C'est donc un phénomène à part entière.
Effectivement, sous la catégorie s'extorsion, on va retrouver plusieurs types de menaces et les fuites de données et où les attaques sur des hôpitaux et en particulier sur des cabinets de radiologie ou sur des cabinets de chirurgies esthétiques,
permettent d'obtenir un très grand nombre d'informations très sensibles et intimes,
à la fois les coordonnées des patients, mais également dans un très grand nombre de cas,
également des photos personnelles intimes qui vont permettre aux praticiens de travailler,
mais malheureusement, quand elles sont dans la nature, elles vont permettre à des cybercriminels de venir nous faire chanter.
Et alors, il y a différents cas de figure, Benoît, c'est ça qu'il faut préciser.
Oui, il y a des cas de figure qui sont complètement inventés par les cybercriminels et des cas de figure qui sont malheureusement réels.
Dans les cas réels, on peut bien entendu citer celui du vol d'information et de photos notamment intimes dans des établissements de santé. On peut également citer malheureusement l'utilisation de nos photos tout à fait non intimes, par exemple des photos de profils sur les réseaux sociaux, qui vont être utilisées pour créer soit des photos à caractère sexuel, soit directement avec l'intelligence artificielle, modifier une vidéo pornographique pour intégrer le visage de la personne et faire croire qu'elle est dans cette vidéo. Et c'est encore une fois un moyen de faire de faire chanter les différentes victimes.
Alors comme d'habitude, c'est une histoire à plusieurs niveaux. Il y a d'abord la récupération de ces données-là, quelquefois par amsonnage, c'est ça ?
Effectivement, l'amsonnage fait partie d'un moyen très courant. Alors l'amsonnage d'ailleurs fait partie tellement et tellement le moyen le plus courant d'obtenir des informations qu'il est un peu considéré comme la mère de toutes les attaques, on va dire qu'une attaque sur deux est partie peu ou prou d'amsonnage. Et ça me fait penser à cette attaque qui a été nommée Varenki, qui a été opérée, alors le procès est en cours à Paris, donc ils sont considérés suspects, présumés innocent pour l'instant, et ce sont deux Français qui auraient mené des campagnes d'amsonnage de
s'extorsion sur des ressortissants français ici, alors à la fois depuis le territoire français, mais à un moment ils se sont également exilés en Ukraine, et ces deux ressortissants sont en ce moment jugés pour cette affaire. Dans leur mode opératoire, ils avaient notamment donc cet

email d'amsonnage et de s'extorsion qui soi-disant annonçaient qu'il nous avait capturé en vidéo ou en photo depuis notre ordinateur en train de consulter des sites pornographiques, et donc au début ils avaient pour objectif de créer un logiciel qui allait effectivement faire ces photos ou vidéos, et puis ils se sont aperçus que le développement du logiciel était plus ou moins compliqué, et puis que finalement malheureusement les gens mordaient à l'amsonnage sans même avoir
ces preuves, parce que quand on est victime de s'extorsion, malheureusement généralement on est pris de panique, même si on n'a rien à se reprocher, ça c'est vraiment un effet très très comment dire, malheureusement très efficace de la part des cinématiques, c'est vraiment un réflexe, même si on n'a rien fait, on est tenté, et puis comme l'email, le message va nous mettre le doute, et bien malheureusement ils ont réussi à dérober un certain volume d'argent,
assez conséquent le procès dira combien exactement.
Alors on l'a dit donc des vrais images, parfois des fausses, parfois pas d'images du tout aussi, ça arrive également.
Exactement, dans le cas présent de Varunki, il n'y avait pas d'images, c'était vraiment de la pression mise sur les victimes, et puis quand on sait que les sites pornographiques sont parmi les plus visités de toute façon, ils avaient quand même assez de chance de tomber sur les consommateurs.
C'est assez effrayant, donc ça veut dire que notamment avec la fabrication de fausses images, on peut se retrouver demain, on va dire dans un film pornographique, acteur, alors que c'est totalement faux.
Exactement, et ça c'est la puissance de l'intelligence artificielle, encore une fois un double tranchant utilisée pour des choses magnifiques et qui font avancer le progrès et nos sociétés,
puis également détourner, pas pour des usages tout à fait illégaux et légitimes.
Dans cette utilisation, encore une fois on s'aperçoit que la victime est assez pronte à payer parce qu'elle a peur, et qu'une fois que le mal est fait, si les informations sont diffusées, si les photos ou les vidéos sont diffusées, que ça soit vrai ou pas, au final ça va être très compliqué de démontrer à son entourage, voire même on n'a pas envie de démontrer à son entourage que ce n'est pas nous qui sommes dans ces vidéos ou ces photos pornographiques.
C'est un phénomène vraiment d'une ampleur significative, sa benoît.
Oui, on le voit, alors il y a plusieurs raisons à cela.
Nous on l'a vu de manière tout à fait formelle, on a des chiffres sur les différents spam et ou type de messages que reçoivent à la fois nos clients mais également ceux que on peut arrêter plus globalement.
Et on a vu qu'au premier trimestre 2023, comparé au dernier trimestre 2022, il y a eu une augmentation de 200% de cette catégorie de menaces que l'on va appeler sextorsion basée principalement sur des emails d'amsonnage contenant ou pas d'ailleurs des vrais photos mais d'une manière générale, cette menace-là est en très grand nombre d'augmentation.
Et puis c'est malheureusement aussi lié au fuite de données qui elles sont aussi en constante augmentation et donc on l'a vu, si le FBI met en garde les utilisateurs contre des fuites de données notamment dans des cabinets de radiologie, c'est qu'il y a un réel danger que celui-ci est concret.

Et malheureusement Benoît, on ne voit pas beaucoup de manière de se prémunir contre ça à titre individuel, qu'est-ce qu'on peut faire ? Pas grand-chose.
Alors il y a deux cas de figure encore une fois, le premier cas de figure c'est si ce n'est pas le cas et ou même si c'est le cas, en cas de chantage, ne pas céder, porter plainte et à partir de là, la police, la justice va faire son travail.
Et aller sur la plateforme Faroze, c'est ça ?
S'il y a plusieurs points d'entrée on va dire pour toucher les autorités et c'est vrai que Sybère Malveillance à ce côté fédérateur et en fonction du problème que vous allez décrire, vous serez renvoyé par la suite sur la bonne plateforme et Faroze en est une je pense à point de contact aussi qui est une association qui permet d'aller signaler du contenu illégal ou illégitime.
Donc ça c'est le premier cas de figure, à partir du moment où on a un chantage notamment quand il arrive par email, porter plainte et puis ne pas céder à la panique même si c'est une situation qui est bien souvent très stressante et puis ensuite il y a le deuxième cas où il y a véritablement le mal qui a été fait notamment si vous voyez une vidéo de vous qui circule avec votre visage sur un film ou une photo pornographique par exemple.
Là le premier réflexe c'est le même, aller porter plainte, ne pas céder à la panique et puis aussi à avertir parfois ses proches pour éviter que même ne tombe sur ce type de contenu problématique.
Ça peut être très dérangeant et prendre les devants, c'est aussi couper l'herbe sous le pied au cybercriminel, vous pouvez faire ce que vous voulez, d'outre façon j'ai prévenu mes proches, ce n'est pas moi sur cette vidéo, c'est un truc cash, c'est un montage donc je ne paierai pas et j'ai porté plainte donc on essaye de leur couper sous le pied.
C'est pas facile et quant aux vols d'information qui sont les nôtres chez des tiers et encore une fois je repense au cabinet de radiologie dont le FBI faisait référence et là c'est vraiment très compliqué parce qu'on ne va pas à chaque fois qu'on va faire une radio ou que l'on va chez un photographe pour prendre des photos d'identité et bien lui demander s'il est bien sécurisé et soi-même s'assurer qu'il est bien sécurisé.
Donc là on est plus dans une…
Mais on y vient drape-tête ?
Il y a un certain nombre de réglementations qui sont en réflexion, on y vient drape-tête.
Après, moi je dirais qu'on devrait déjà y être quand on achète des objets connectés.
C'est à dire que quand vous achetez un objet connecté, notamment s'il contient toute votre vie au smartphone, montre connecté ou même capteur avec des informations de type de données de santé, je pense qu'il faut se poser la question du sérieux de l'entreprise à laquelle on achète cet objet connecté et ça doit, à mon avis, rentrer dans la grille et dans la balance.
Il faut savoir que la cyber-sécurité n'est pas infaillible et deux coups de chair, en fait, si vous comparez deux objets, à partir du moment où vous rajoutez de la cyber-sécurité, forcément l'objet qui en contient a demandé plus d'attention, plus de personnes, des moyens de rechercher développement, certainement plus conséquents que celui qui n'y prête

pas attention.
Ce n'est pas un gage de 100%, mais en tant que consommateur, je pense qu'aujourd'hui, on doit réfléchir à la question cyber de nos données dans le numérique.
Bien sûr.
La sécurité des objets connectés, alors ça, c'est un autre sujet, on aura l'occasion d'en reparler.
Merci beaucoup, Benoît Grunemval, d'experts cyber-sécurités chez AZ.