Orange is the New Black dévoilé : Netflix, une victime de plus des cyber-extorsions

Les entreprises sont probablement loin d'avoir tout vu en matière de cyber-extorsions. Les ransomwares pourraient bien n'être qu'une déclinaison relativement bénigne de ce qui apparaît comme le nouveau gagne-pain des cybercriminels. Le 29 avril, un hacker ou un groupe de pirates du nom de TheDarkOverlord a décidé de publier 10 épisodes inédits de la série de Netflix '*Orange is The New Black*', apparemment dérobés aux studios Larson, une petite société de post-production qui aurait été hackée en décembre dernier.

TheDarkOverload a d'abord tenté de faire chanter Larson Studio avant de se tourner vers le diffuseur, Netflix. Le refus de ce dernier de payer une rançon a poussé le ou les cybercriminels à dévoiler les épisodes de la saison 5 de la célèbre série. Selon DataBreaches.net, l'histoire est en réalité un peu plus complexe, puisque, dans un premier temps, les studios Larson auraient accepté de payer 50 Bitcoins, avant de se rétracter. Poussant les pirates à se tourner vers Netflix. C'est en tout la version que défend TheDarkOverlord.

D'autres diffuseurs sous pression

Au total, The DarkOverlord aurait dérobé 37 films ou séries en passe d'être officiellement mis sur le marché, soit des centaines de Go. Et a déjà annoncé son intention de faire chanter d'autres diffuseurs, comme Fox, ABC ou National Geographic.

Cette affaire est symptomatique de la tendance de certains groupes cybercriminels à utiliser des données confidentielles dérobées à des entreprises pour extorquer de l'argent. On retrouve ainsi le nom de TheDarkOverlord associé à différents chantages ciblant des institutions médicales, après des vols de données relatives à des patients.

La menace d'un DDoS suffit

Si elle peut prendre appui sur un vol de données confidentielles, la cyber-extorsion peut tout aussi bien reposer sur une menace de DDoS (déni de service distribué), qui va porter atteinte à l'image d'une organisation. En 2016, un autre groupe de pirates, Armada Collective, a ainsi envoyé des lettres de menaces à plus de 100 entreprises, leur demandant de payer une rançon faute de quoi elles seraient ciblées par des DDoS massifs. Selon la société CloudFlare, cette technique a permis aux cybercriminels d'amasser des centaines de milliers de dollars… sans lancer une seule attaque. Akamai, un autre prestataire spécialisé dans la protection contre les DDoS, explique que plusieurs groupes distincts (dont DD4BC, Lizard Squad, XMR Squad) opèrent déjà selon un modus operandi similaire.

Accéder aux demandes de rançon des cybercriminels apparaît tant risqué que contre-productif. Risqué parce que rien ne garantit que la menace est réelle ou que les pirates ne vont effectivement plus utiliser à l'avenir les données dérobées en cas de faille de sécurité. Contre-productif, car le

paiement d’une rançon indique au monde du cybercrime qu’une organisation est encline à céder. Il y a donc fort à parier qu’elle sera à nouveau ciblée.

A lire aussi :

Attaques DDoS : une facture moyenne de 2,5 M$ pour les entreprises

Les attaques DDoS, l’autre machine à cash des cybercriminels

Crédit Photo : Scyther5-Shutterstock