Communications coronavirus (COVID-19)
La cyber-menace : un risque accru ou simplement différent ?

HISCOX
CYBERCLEAR®

L'augmentation des risques de cyber-attaques depuis le début de la pandémie de COVID-19 a fait couler beaucoup d'encre dans la presse récemment. Nous pensons qu'il est important de remettre la menace dans son contexte.

Certains cyber-incidents sont moins probables...

Un scénario très commun de cyber-sinistre est la perte d'un ordinateur portable non chiffré. Il n'y a bien entendu aucun risque dans le contexte actuel qu'une personne se rende dans un bar de centre-ville et y oublie son sac contenant son ordinateur portable. Par ailleurs, de nombreuses sociétés (Google, Microsoft etc.) ont déclaré qu'en raison du manque de main d'œuvre, elles ralentiraient la publication de nouvelles versions et mises à jour ainsi que le nombre de changement informatiques, ce qui pourrait réduire les pannes de système.

Mais il existe de nouvelles menaces…

1. **Le travail à distance augmente les angles d'attaque a** mesure que les entreprises mettent en place des solutions de télétravail, non seulement des appareils moins sécurisés sont connectés au réseau des sociétés, mais le déploiement rapide de solutions d'accès à distance peut se faire au détriment des tests de sécurité rigoureux qui auraient été réalisés dans des temps de plus grande stabilité.
2. **Absence de conversations entre collègues –** énéralement lorsqu'on reçoit un email suspect, on peut se tourner vers un collège et lui demander « *je viens de recevoir cet email, tu l'as reçu aussi ? Tu ne penses pas qu'il est suspect ?* » Ce type de conversion ne peut avoir lieu actuellement, donc il y a des risques que davantage d'emails de phishing touchent leur cible.
3. **Nous sommes tous en quête d'informations –** dans ces temps d'incertitude, nous recherchons tous des réponses, et pour étancher cette soif d'informations, nous avons plus tendance à cliquer sur des liens ou des articles que nous trouvons en ligne ou qui sont partagés sur les réseaux sociaux.

Y a-t-il vraiment plus d'attaques par phishing ?

Un certain nombre de communiqués de presse publiés la semaine dernière nourrissent le débat de quelques statistiques intéressantes :

- Google indique avoir bloqué la semaine dernière 18 millions d'emails de phishing sur le thème du COVID-19, ayant pour cible des utilisateurs Gmail. Cela représenterait environ 2,5% des 100 millions d'emails de phishing que Google déclare avoir bloqué tous les jours en 2019.
- Microsoft surveille des milliers de campagnes d'emails de phishing qui représentent des millions de messages malveillants chaque semaine. L'entreprise a indiqué récemment : « sur les millions de messages ciblés que nous voyons passer chaque jour, environ 60 000 contiennent des pièces jointes ou des URL malveillantes liées au COVID-19. Si ce nombre peut sembler élevé, il est important d'observer qu'il ne constitue même pas 2% du volume total de menaces que nous surveillons activement et contre lesquelles nous protégeons nos utilisateurs chaque jour, ce qui confirme également que le volume total de menaces n'augmente pas. Les pirates modifient toutefois leurs techniques pour miser sur la peur.
- Barracuda – a récemment déclaré « *qu'entre le 1er et le 23 mars, Barracuda Sentinel a détecté 467 825 attaques par email de spear-phishing (phishing très ciblé), et 9 116 de ces détections étaient relatives au COVID-19, ce qui représente environ 2% des attaques.* »

Il est intéressant de constater que les chiffres rapportés par ces trois entreprises convergent sur le fait qu'environ 2% de l'ensemble des emails de phishing sont liés au COVID-19. Cela corrobore notre impression que les campagnes de phishing ont dévié pour utiliser des leurres COVID-19, plutôt que les leurres traditionnels de type remboursement d'impôts, Netflix ou Apple auxquels nous sommes habitués.

Sinistres liés au COVID-19

A ce stade, nous n'avons pas enregistré un nombre significatif de sinistres liés au COVID-19, néanmoins deux cas intéressants et relativement semblables sont décrits ci-dessous.

Exemple 1 : en mars, une PME établie au Royaume-Uni a fait l'expérience d'un vol de données depuis une base de données, qui contenait sans doute aux alentours de 2 000 fichiers personnels. Les données appartiennent à un tiers pour lequel notre assuré développait un site web. Les pirates ont exigé une rançon en bitcoin contre la restitution des données. L'attaque semble avoir utilisé une connexion à une base de données ouverte sur un ordinateur de bureau, qui a été emporté à domicile par un salarié pour télétravailler pendant le confinement lié au COVID-19.

En temps ordinaire, le firewall du réseau interne de l'entreprise aurait empêché cette connexion, mais une fois que la machine s'est trouvée au domicile du salarié, la protection du firewall ne fonctionnait plus. En effet, la sécurité du réseau devient dépendante de la configuration de sécurité du routeur du domicile du salarié.

Enseignement : cette affaire souligne la nécessité d'envisager l'impact sécuritaire lié au déplacement des appareils qui, dans des conditions normales, n'auraient pas quitté les bureaux de l'entreprise, et de considérer l'utilisation de firewalls sur les terminaux et sur le réseau à tout moment.

HISCOX
CYBERCLEAR®

Exemple 2 : en mars, une société américaine a fait l'expérience d'une attaque par ransomware par laquelle tous les serveurs de son réseau ont été chiffrés. Bien que découverte mi-mars, les investigations montrent que l'attaque pourrait s'être propagée depuis un seul PC infecté qui était en sommeil depuis janvier 2020. Le PC infecté a été donné à un salarié (afin qu'il puisse télétravailler pendant le confinement lié au COVID-19). Le salarié l'a connecté au réseau, ce qui a causé la propagation involontaire du ransomware.

Enseignement : il s'agit d'un bon exemple montrant qu'il est important d'inspecter les appareils mis hors service ou en sommeil avant qu'ils ne soient remis en service, même s'ils ont été précédemment nettoyés par l'équipe informatique interne ou par un tiers. Cela est particulièrement important pendant cette période où de nouveaux appareils potentiellement moins sécurisés sont distribués aux salariés pour télétravailler.

Hiscox France
19 rue Louis le Grand
75002 Paris

T +33 (0) 1 53 21 83 12
E hiscox.communication@hiscox.fr
www.hiscox.fr