DSIM - Direction des Systèmes d'Information Mutualisée

Hameçonnage ou le Phishing :

L'un des principaux vecteurs de la cybercriminalité.

Le hameçonnage également appelé phishing, est une forme courante d'escroquerie sur internet.

Cette attaque repose généralement sur une usurpation de l'identité de l'expéditeur, et procède par ingénierie sociale forte afin de lier l'objet du courriel et le corps du message à l'activité de la personne ou de l'organisation ciblée.

Généralement, le courriel usurpe l'identité d'une personne morale (établissement financier, service public, concurrent…) ou d'une personne physique (collègue de travail, famille, ami…) dans le but de duper le destinataire qu'il invite à ouvrir une pièce jointe malveillante ou à suivre un lien vers un site Web malveillant. Une fois cette première machine contaminée, l'attaquant en prend le contrôle pour manœuvrer au sein du système d'information de l'organisation constituant la véritable cible (on parle ici « d'infiltration »).

Une fois sa première victime compromise, l'attaquant cherchera à obtenir des droits « d'administrateur » (on parle alors « d'escalade de privilèges ») pour pouvoir rebondir et s'implanter sur les postes de travail et les serveurs de l'organisation où sont stockées les informations convoitées.

Une fois ses cibles atteintes, il recherchera les informations qu'il s'efforcera de capter le plus discrètement possible (on parle alors ici « d'exfiltration ») soit en une seule fois, en profitant d'une période de moindre surveillance du système (la nuit, durant les vacances scolaires, lors d'un pont…), soit de manière progressive plus insidieuse.

Il prend généralement soin de toujours effacer derrière lui toute trace de son activité malveillante.

Le phishing ne se limite pas à la sphère professionnelle :

Dans la sphère privée, Les conséquences de l'hameçonnage peuvent être graves et incluent la perte financière, la violation de la vie privée et le vol d'identité.

Source image : istockphoto.com

Les grandes tendances de la menace en 2022 :

Au total, la plateforme **Cybermalveillance.gouv.fr identifie et traite désormais plus de 51 menaces**.
Sur l'ensemble de ces cybermalveillances traitées par l'outil de diagnostic en ligne,

• l'hameçonnage, **constitue la menace n°1 tous publics confondus, avec +54 % de recherches d'information et d'assistance vs 2021, soit 1,9 million de recherches d'assistance et consultations d'articles dédiés à ce danger,**

• le **piratage de compte** est toujours en forte croissance avec + 97,5 % vs 2021,

• les **rançongiciels** sont dans le top 3 des menaces pour les professionnels (entreprises et collectivités) et restent à un niveau très élevé même s'ils sont légèrement en baisse cette année pour cette cible (-16%).

Quelles sont les differentes formes de « hameçonnage » ?

Savoir les identifier :

Par e-mail : Une attaque qui consiste à envoyer un message malhonnête en se faisant passer pour une entreprise de confiance pour voler des éléments sensibles telles que les mots de passe, les numéros de carte de crédit, etc.

Par SMS : Une attaque qui consiste à envoyer un SMS frauduleux en se faisant passer pour une entreprise de confiance pour inciter les victimes à fournir des renseignements sensibles.

Sur les réseaux sociaux : Une attaque qui consiste à créer un faux compte sur un réseau social pour inciter les victimes à fournir des éléments sensibles.

Dans les annonces sur le net : Une attaque qui consiste à utiliser des annonces frauduleuses pour inciter les victimes à fournir des renseignements sensibles.

Dans les jeux en ligne : Une attaque qui consiste à utiliser des jeux frauduleux pour inciter les victimes à fournir des détails confidentiels.

Source image : Ivanti.com