La coupe du monde au Qatar attire les acteurs malveillants
Info
PostÃ© par : JPilo
PubliÃ©e le : 25/11/2022 14:00:00

Cette fin dâ□□annÃ©e 2022 est marquÃ©e par lâ□□Ã©vÃ©nement sportif le plus attendu dans le football : la coupe du monde au Qatar. Depuis le 20 novembre, les supporters sont nombreux Ã regarder lâ□□Ã©vÃ©nement et les FranÃ§ais Ã©taient dâ□□ailleurs au rendez-vous hier soir pour supporter lâ□□Ã©quipe de France et assister Ã leur premiÃ¨re victoire.

Mais, les fans et les sportifs ne sont pas les seuls intÃ©ressÃ©s par cet Ã©vÃ¨nement... Les acteurs malveillants ne sont pas en reste et ont dÃ©jÃ lancÃ© de nouvelles cyberattaques.

Dans la nouvelle recherche du Advanced Research Center de Trellix, les chercheurs reviennent sur les tactiques utilisÃ©es par les cyberattaquantes Ã lâ□□occasion de la coupe du monde au Qatar.

Parmi les premiÃ¨res conclusions :

â□¢ Les attaquants utilisent la FIFA et les campagnes liÃ©es au football pour cibler les organisations des pays arabes. Il est courant pour les attaquants d'utiliser les Ã©vÃ©nements populaires pour diffuser des tactiques d'ingÃ©nierie sociale et cibler en particulier les organisations qui sont liÃ©es Ã l'Ã©vÃ©nement.

â□¢ Le volume d'e-mails malveillants dans les pays arabes a augmentÃ© de 100 % au mois d'octobre. Si les organisations affiliÃ©es se sont prÃ©parÃ©es Ã cet Ã©vÃ©nement, les risques d'erreur humaine sont plus nombreux.Â

Les hackers en profitent alors pour collecter des informations confidentielles, exfiltrer des donnÃ©es personnelles et financiÃ¨res ou essayer dâ□□atteindre Ã la rÃ©putation du pays.

Plusieurs types dâ□□emails malveillantes ont Ã©tÃ© interceptÃ© par lâ□□Ã©quipe de chercheurs Trellix, voici quelques exemples :

1. La personne qui lance lâ□□attaque prÃ©tend provenir du service d'assistance de FIFA TMS, et le corps de l'e-mail affiche une fausse notification d'alerte concernant la dÃ©sactivation de l'authentification Ã deux facteurs et contient un lien hypertexte qui redirige l'utilisateur vers une page de phishing.

2. Lâ□□hacker usurpe l'identitÃ© de la billetterie de la FIFA et transmet un problÃ¨me de paiement Ã la victime pour qu'il le rÃ©solve de toute urgence. Il contient Ã©galement une piÃ¨ce jointe html qui redirige l'utilisateur vers une page de phishing personnalisÃ©e.

3. Snoonu, le partenaire officiel de livraison de nourriture de la Coupe du monde, est usurpÃ©, offrant de faux billets gratuits Ã ceux qui s'inscrivent. Il contient une piÃ¨ce jointe xlsm malveillante. L'utilisation de ces noms d'organisations de confiance et de leurs modÃ¨les fait que l'utilisateur tombe facilement dans de telles attaques.

Comme si les emails ne suffisaient pas, les chercheurs Trellix ont Ã©galement fait la dÃ©couverte de plusieurs URL malveillants sur le thÃ¨me de la coupe du monde, et de plusieurs familles de logiciels malveillants utilisÃ©s pour cibler les pays arabes tels que : Qakbot, Emotet, Formbook, Remcos, QuadAgent, qui ont pour but dâ□□espionner les appareils Ã©lectroniques, voler des

donnÃ©es, contrÃ´ler les ordinateurs etc.

Pour plus dâ□□informations, veuillez consulter ***le blog Trellix.Â***