

Cybercriminelles visant l'OTAN et le peuple Ukrainien

Internet

Posté par : JulieM

Publié le : 4/3/2022 15:00:00

Les chercheurs en cybersécurité de Proofpoint viennent de publier de nouveaux renseignements montrant une activité cyber importante, soutenue par l'État Biélorusse, qui vise des membres de gouvernements Européens impliqués dans la gestion des flux de réfugiés fuyant les zones de conflits Russo-Ukrainien.

☞ Cette campagne de phishing ciblée, qui infecte les systèmes d'exploitation par le biais d'un logiciel malveillant appelé «SunSeed», provient de la compromission du compte email d'un membre des forces armées Ukrainiennes.

☞ Proofpoint suppose que l'activité provient du groupe TA445 (Ghostwriter / UNC1151) qui semble opérer depuis la Biélorussie, et a longtemps été impliquée dans de larges campagnes de désinformation visant à manipuler le sentiment Européen face aux mouvements de réfugiés au sein de l'OTAN.

☞ Ces attaques par email ont visé les individus impliqués dans la logistique du transport, l'allocation budgétaire et financière, l'administration, et les mouvements de population à travers l'Europe, avec l'intention de collecter des renseignements quant aux mouvements de fonds monétaires, d'équipement, d'aide alimentaire, et de population à travers les pays membres de l'OTAN.

Dans ce contexte de guerre Russo-Ukrainienne, il faut s'attendre à ce que les menaces d'acteurs comme TA445, indirectement soutenus par certains États, continuent de proliférer et de s'attaquer aux gouvernements européens pour tenter d'obtenir des renseignements sur les mouvements de réfugiés en Ukraine ainsi que sur d'autres éléments du conflit qui auraient de l'importance pour la Russie.

Cette activité démontre que les migrants et réfugiés de guerre peuvent devenir des armes de destruction massive dans un conflit hybride où l'information et les attaques cybernetiques font partie du panel de tactiques martiales auxquelles les gouvernements peuvent désormais faire appel.

Les chercheurs Proofpoint commentent : « cette campagne représente un effort déterminé de s'attaquer particulièrement aux entités de l'OTAN, par le biais du compte email corrompu de membres des forces armées Ukrainiennes, en plein cœur d'un conflit armé entre la Russie, ses sympathisants, et l'Ukraine.

Bien que les tactiques utilisées dans cette campagne ne soient pas totalement nouvelles en elles-mêmes, elles peuvent s'avérer dévastatrices lorsqu'elles sont utilisées ensembles, et pendant un conflit de cette envergure. Il faut s'attendre à de nouvelles attaques similaires visant les entités de l'OTAN.

Par ailleurs, l'exploitation des renseignements autour des mouvements de réfugiés en Europe, à des fins de propagande et de campagnes de désinformation, sont des techniques bien connues de la part des services Russes et Biélorusses. Être conscient de cette menace, et en parler ouvertement sont d'une importance capitale pour une meilleure connaissance et appréhension de ces menaces. »

Vous pourrez trouver de plus amples [informations](#) sur ces activités :