CybercriminalitÃ© : Des cibles au Moyen-Orient
Internet
PostÃ© par : JerryG
PubliÃ©e le : 15/11/2023 13:00:00

Proofpoint, lâ□□un des leaders dans les domaines de la cybersÃ©curitÃ© et de la conformitÃ©, dÃ©voile les rÃ©sultats de ses derniÃ¨res recherches sur les activitÃ©s du groupe de cybercriminel Molerats, aussi dÃ©signÃ© TA402 par les chercheurs dÃ©diÃ©s Ã la dÃ©tection des menaces.

Les principales conclusions de cette Ã©tude sont les suivantes :

Les chercheurs de Proofpoint ont suivi TA402 depuis 2020 et estiment que l'acteur est un groupe basÃ© au Moyen-Orient, opÃ©rant en soutien aux objectifs d'espionnage palestinien Ã travers la collection de renseignements.Â

Le groupe cybercriminel utilise une chaÃ®ne d'infection complexe pour cibler les gouvernements du Moyen-Orient avec un nouveau tÃ©lÃ©chargeur d'accÃ¨s initial que Proofpoint a baptisÃ© IronWind.

De juillet Ã octobre 2023, TA402 a changÃ© de mÃ©thode dâ□□infection, en dÃ©veloppant des techniques beaucoup plus complexes qui se dÃ©clinent en trois variantes â□□ liens Dropbox, piÃ¨ces jointes de fichiers XLL et piÃ¨ces jointes de fichiers RAR â□□ chaque variante conduisant systÃ©matiquement au tÃ©lÃ©chargement d'une DLL (Dynamic Link Library) contenant le logiciel malveillant multifonctionnel.

A la fin du mois d'octobre 2023, les chercheurs de Proofpoint n'avaient observÃ© aucun changement dans le ciblage de TA402, un groupe qui a historiquement opÃ©rÃ© dans l'intÃ©rÃªt des territoires Palestiniens, et n'avaient identifiÃ© aucune indication d'un mandat modifiÃ© malgrÃ© le conflit actuel dans la rÃ©gion.Â

Il reste possible que cet acteur de la menace rÃ©oriente ses ressources en fonction de l'Ã©volution des Ã©vÃ¨nements.

Pour Joshua Miller, chercheur en cybersÃ©curitÃ© chez ***Proofpoint,*** Â« Lorsqu'il s'agit d'acteurs de la menace alignÃ©s sur des Ã□tats, la CorÃ©e du Nord, la Russie, la Chine et l'Iran se taillent gÃ©nÃ©ralement la part du lion.

Mais TA402, un groupe de menaces persistantes avancÃ©es (APT) du Moyen-Orient qui opÃ¨re historiquement dans l'intÃ©rÃªt des territoires Palestiniens, s'est toujours rÃ©vÃ©lÃ© Ãªtre un acteur intriguant capable d'un cyber-espionnage trÃ¨s sophistiquÃ© axÃ© sur la collecte de renseignements.

Le conflit en cours au Moyen-Orient ne semble pas avoir entravÃ© leurs opÃ©rations, car ils continuent d'innover et d'utiliser de nouvelles mÃ©thodes de diffusion astucieuses pour contourner les efforts de dÃ©tection.

En utilisant des chaÃ®nes d'infection complexes et en crÃ©ant de nouveaux logiciels malveillants pour attaquer ses cibles, TA402 continue de mener des activitÃ©s extrÃªmement ciblÃ©es en se concentrant sur les entitÃ©s gouvernementales basÃ©es au Moyen-Orient et en Afrique du Nord Â».