Des entreprises russes visÃ©es par des cybercriminels compatriotes
Internet
PostÃ© par : JulieM
PubliÃ©e le : 27/4/2022 13:00:00

Les cybercriminels russophones ont habituellement un code de conduite vis-Ã -vis des entreprises compatriotes : ils ne les attaquent tout simplement pas. Cependant, le gang de ransomware OldGremlin constitue un contre-exemple.

Ce groupe cible des organisations en Russie depuis le printemps 2020 et a rÃ©cemment menÃ© des campagnes qui exploitent les sanctions frappant actuellement le pays.

Selon Julien Fournier, VP Southern Europe chez Netskope, ces cyberattaques font suite aux sanctions imposÃ©es aux entreprises russes Ã cause du contexte gÃ©opolitique :

Â« Ces hackers profitent que plusieurs fournisseurs de solutions de sÃ©curitÃ© ont suspendu leurs opÃ©rations en Russie, pour tirer profit de la surface dâ□□attaque des cibles qui sâ□□est trouvÃ©e Ã©largie en consÃ©quence.

Ainsi, ils ont perpÃ©trÃ© en mars dernier des campagnes malveillantes, avec un e-mail de phishing comme vecteur d'attaque initial, invitant les victimes Ã remplir un formulaire pour demander une nouvelle carte bancaire du fait de la suspension des opÃ©rations Visa et Mastercard en Russie.

Le formulaire prÃ©sumÃ© est en rÃ©alitÃ© un document Office malveillant hÃ©bergÃ© sur Dropbox qui, une fois exÃ©cutÃ©, charge un modÃ¨le hÃ©bergÃ© de nouveau sur Dropbox. Cette campagne mise sur une porte dÃ©robÃ©e, appelÃ©e TinyFluff, que les attaquants utilisent pour contrÃ´ler lâ□□appareil compromis afin de collecter, voler et tÃ©lÃ©charger des fichiers.

Une fois de plus, les cybercriminels ont donc exploitÃ© un service cloud, Ã priori de confiance, pour diffuser du contenu malveillant. Ils profitent Ã©galement de la situation gÃ©opolitique qui rend les organisations et les individus plus vulnÃ©rables.

Il ne sâ□□agit pas de la seule campagne rÃ©cente qui parvient Ã ses fins via Dropbox. Ainsi, des hackers ont aussi ciblÃ© le secteur bancaire africain via le malware RemcosRAT, propagÃ© Ã lâ□□aide de Dropbox et OneDrive.

Curieusement, dans cette deuxiÃ¨me campagne, la charge utile nâ□□a pas Ã©tÃ© opÃ©rÃ©e par un service cloud, mais livrÃ©e grÃ¢ce Ã GuLoaderdownloader et la technique du HTML smuggling. Â»