***TinyNuke : Le malware bancaire s'attaque Ã  la France.***
**Internet**
PostÃ© par : JPilo
PubliÃ©e le : 13/12/2021 15:00:00

Les chercheurs de Proofpoint ont rÃ©cemment identifiÃ© un retour dâ□□activitÃ© continue du .

DÃ©couvert pour la premiÃ¨re fois en 2017 par les Ã©quipes Proofpoint, TinyNuke est un trojan bancaire ciblant des entreprises franÃ§aises. Il est similaire au cÃ©lÃ¨bre cheval de Troie bancaire Zeus, qui possÃ¨de de nombreuses variantes et des fonctionnalitÃ©s identiques. TinyNuke est utilisÃ© pour dÃ©rober des identifiants et d'autres types dâ□□informations privÃ©es. Il peut Ã©galement Ãªtre utilisÃ© pour la diffusion massive de malware.

Ã□ lâ□□occasion de son grand retour, le malware bancaire ne cible presque exclusivement que des entitÃ©s franÃ§aises et des organisations qui exercent France. La technique retenue par lâ□□acteur malveillant, consiste Ã diffuser par email, des leurres de factures censÃ©es provenir dâ□□entreprises issues de plusieurs secteurs dâ□□activitÃ© comme celui de l'industrie, de la technologie, de la finance et bien dâ□□autres.

Lâ□□identification de cette nouvelle campagne malveillante confirme ainsi la rÃ©surgence du malware qui avait atteint son pic de popularitÃ© en 2018. En effet, si TinyNuke est rÃ©apparu sur le devant du paysage des cybermenaces en France, force est de constater que les chercheurs Proofpoint avaient dÃ©jÃ observÃ© des dizaines de campagnes TinyNuke ciblant des entitÃ©s franÃ§aises en 2018, en 2019 et en 2020.

De retour en janvier 2021 avec une campagne distribuant environ 2 000 emails, le malware poursuit avec des campagnes ultÃ©rieures en faibles volumes en mai, juin et septembre. En novembre, Proofpoint a identifiÃ© plusieurs campagnes TinyNuke distribuant environ 2 500 emails Ã destination de centaines dâ□□entreprises franÃ§aises.

Le mode opÃ©ratoire de TinyNuke reste cohÃ©rent et continue de fonctionner avec l'utilisation d'URL vers des fichiers ZIP. Câ□□est ainsi quâ□□il peut enclencher le vol de donnÃ©es et d'argent, et que les machines compromises peuvent Ãªtre ajoutÃ©es Ã un botnet sous le contrÃ´le de l'acteur malveillant.

Pour en savoir plus sur les campagnes de diffusion TinyNuke, veuillez consulter ***le blog Proofpoint*** :