

TinyNuke : Le malware bancaire s'attaque à la France.

Internet

Posté par : JPilo

Publié le : 13/12/2021 15:00:00

Les chercheurs de Proofpoint ont récemment identifié un retour d'activité continue du .

Découvert pour la première fois en 2017 par les équipes Proofpoint, TinyNuke est un trojan bancaire ciblant des entreprises françaises. Il est similaire au célèbre cheval de Troie bancaire Zeus, qui possède de nombreuses variantes et des fonctionnalités identiques. TinyNuke est utilisé pour voler des identifiants et d'autres types d'informations privées. Il peut également être utilisé pour la diffusion massive de malware.

À l'occasion de son grand retour, le malware bancaire ne cible presque exclusivement que des entités françaises et des organisations qui exercent en France. La technique retenue par l'acteur malveillant, consiste à diffuser par email, des lettres de factures censées provenir d'entreprises issues de plusieurs secteurs d'activité comme celui de l'industrie, de la technologie, de la finance et bien d'autres.

L'identification de cette nouvelle campagne malveillante confirme ainsi la résurgence du malware qui avait atteint son pic de popularité en 2018. En effet, si TinyNuke est réapparu sur le devant du paysage des cybermenaces en France, force est de constater que les chercheurs Proofpoint avaient déjà observé des dizaines de campagnes TinyNuke ciblant des entités françaises 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 ultérieures en faibles volumes en mai, juin et septembre. En novembre, Proofpoint a identifié plusieurs campagnes TinyNuke distribuant environ 2 500 emails à destination de centaines d'entreprises françaises.

Le mode opératoire de TinyNuke reste cohérent et continue de fonctionner avec l'utilisation d'URL vers des fichiers ZIP. C'est ainsi qu'il peut déclencher le vol de données et d'argent, et que les machines compromises peuvent être ajoutées à un botnet sous le contrôle de l'acteur malveillant.

Pour en savoir plus sur les campagnes de diffusion TinyNuke, veuillez consulter [le blog Proofpoint](#) :