Ransomware & supply chain : Les menaces en 2022 ?
Internet
PostÃ© par : JulieM
PubliÃ©e le : 12/1/2022 13:00:00

Selon Nordlocker, la France est le quatriÃ¨me pays le plus touchÃ© dans le monde par les ransomware en 2020 et 2021. Quant aux attaques visant la supply chain, elles sont de plus en plus nombreuses et, selon Kaspersky, coÃ»teraient en moyenne deux millions de dollars pour les grandes entreprises.

Selon Shay Nahari, VP of Red Team chez CyberArk, du fait de la rentabilitÃ© des ransomwares et des campagnes malveillantes qui visent la supply chain, les cybercriminels vont poursuivre leurs efforts initiÃ©s ces derniÃ¨res annÃ©es :

Â« Alors que la cybercriminalitÃ© sâ□□organise davantage et ne cesse dâ□□innover, 2022 devrait en subir les consÃ©quences via des attaques plus sophistiquÃ©es et une meilleure comprÃ©hension des entitÃ©s les plus vulnÃ©rables.

Un ransomware opÃ©rationnalisÃ© entraÃ®nera des attaques en 2022

L'Ã©volution du ransomware en tant que service (RaaS) nâ□□en est quâ□□Ã ses dÃ©buts. En 2022, le dÃ©veloppement des ransomwares continuera d'Ã©voluer, dâ□□un niveau "artisanal" Ã une industrie organisÃ©e par groupe dâ□□experts.Â

Les ransomwares pilotÃ©s par les opÃ©rateurs se dÃ©velopperont, avec une distinction claire entre des outils standardisÃ©s et les mÃ©thodes de livraison des criminels qualifiÃ©s se dÃ©plaÃ§ant Ã travers les rÃ©seaux, et des experts crÃ©ant le code des ranÃ§ongiciels.

La meilleure dÃ©tection des ransomwares poussera les hackers Ã innover

La plupart des familles de ransomwares actuelles partagent plusieurs techniques, tactiques, et procÃ©dures ; par exemple, la faÃ§on dont ils suppriment les fonctions de chiffrement de sauvegarde ou effectuent l'exÃ©cution initiale. Par consÃ©quent, les outils de sÃ©curitÃ© identifient ces dÃ©nominateurs communs afin de les bloquer, ce qui oblige les cybercriminels Ã innover pour Ã©viter ces dÃ©tections.

Le nouveau maillon le plus faible : la supply chain

Au cours des derniÃ¨res annÃ©es, de nombreuses attaques dÃ©vastatrices ont commencÃ© via le phishing.Â

Les attaques contre la supply chain Ã©taient historiquement menÃ©es par des criminels financÃ©s par un Ã□tat, qui cherchait Ã viser des cibles de grande valeur ou avec un retour sur investissement Ã©levÃ© ; la campagne contre Kaseya Ã©tant l'un des nombreux exemples.

Cependant, les contrÃ´les anti-hameÃ§onnage gÃ©nÃ©ralisÃ©s, souvent confiÃ©s aux fournisseurs de cloud eux-mÃªmes, ont augmentÃ© le coÃ»t opÃ©rationnel de telles attaques.Â

En consÃ©quence, les attaques contre la supply chain deviendront les plus rÃ©pandues : ces campagnes seront la premiÃ¨re Ã©tape pour de nombreux cybercriminels, en raison d'un retour sur investissement plus Ã©levÃ©, et car cette cible est devenue le maillon le plus faible de la

chaÃ®ne. Â»