Les cybercriminels s'en prennent aux infrastructures criques
Internet
PostÃ© par : JulieM
PubliÃ©e le : 6/10/2021 15:00:00

Le grand port amÃ©ricain de Houston vient de rÃ©vÃ©ler avoir Ã©tÃ© la cible le mois dernier dâ□□un piratage soupÃ§onnÃ© provenir dâ□□un Ã□tat-nation. Les cybercriminels auraient implantÃ© un logiciel malveillant et tentÃ© de voler des informations dâ□□identifications Microsoft.Â

Cependant, les Ã©quipes de lâ□□autoritÃ© portuaire ont dÃ©clarÃ© sâ□□Ãªtre dÃ©fendues avec succÃ¨s contre cette tentative de piratage confirmant quâ□□aucune donnÃ©e ou systÃ¨me opÃ©rationnel nâ□□a Ã©tÃ© touchÃ©.

Loin dâ□□Ãªtre une premiÃ¨re tentative, le sÃ©nateur Rob Portman, R-Ohio, a dÃ©clarÃ© que ce piratage Ã©tait Â« prÃ©occupant Â» et que les Ã□tats-Unis devaient Â« riposter contre ces acteurs Ã©tatiques qui continuent de sonder et de commettre ces crimes contre nos entitÃ©s des secteurs public et privÃ© Â».

En France, le groupe CMA-CGM, leader mondial du transport et de la logistique avait Ã©tÃ© pris pour cible dâ□□un ransomware en septembre 2020, allongeant la liste des grands logisticiens franÃ§ais et mondiaux victimes de la cybercriminalitÃ©.

Tony Fanni Senior Channel System Engineer chez Cohesity commente :

Â« Les infrastructures critiques sont de plus en plus ciblÃ©es par les cybercriminels. Les transports et la logistique, les services financiers, les soins de santÃ©, les fabricants et les fournisseurs d'Ã©nergie sont tous des services essentiels au bon fonctionnement de notre Ã©conomie et de notre sociÃ©tÃ©, et souvent vitaux.

Leur importance leur confÃ¨re la position de cible numÃ©ro une des cybercriminels, notamment pour le vol de donnÃ©es, le verrouillage de systÃ¨mes, les demandes de ranÃ§on - et plus rÃ©cemment l'exfiltration de donnÃ©es.

Notamment lorsque les attaquants dÃ©cident de voler des donnÃ©es et de poursuivre individuellement des clients ou des patients, pour obtenir des ranÃ§ons avant dâ□□afficher publiquement leurs informations personnelles.Â

Le champ d'action a changÃ© en matiÃ¨re de malware/ransomware. L'exfiltration est la nouvelle menace en 2021 et une raison de plus pour les organisations de sÃ©curiser leurs donnÃ©es de maniÃ¨re proactive et de s'assurer que la restauration est possible.

Les organisations sont invitÃ©es Ã renforcer leur cybersÃ©curitÃ© Ã tous les niveaux pour prÃ©server le bien-Ãªtre de ces services essentiels. Les gouvernements du monde entier proposent des meilleures pratiques aux organisations pour les aider Ã mener la bataille.

Les infrastructures critiques sont de plus en plus la cible de cyberattaques et les responsables informatiques doivent recevoir le soutien et le budget nÃ©cessaires pour rendre leurs rÃ©seaux moins vulnÃ©rables, amÃ©liorer leur posture en matiÃ¨re de cybersÃ©curitÃ© et dÃ©velopper des systÃ¨mes de surveillance solides.

La restauration des donnÃ©es Ã l'aide d'un systÃ¨me de fichiers immuable, de la technologie WORM (Write-Once-Read-Many), du chiffrement de bout en bout et de l'authentification multifactorielle (MFA) ne peut se faire qu'avec des solutions de gestion des donnÃ©es modernes. La plupart des solutions disponibles sur le marchÃ© aujourd'hui ont Ã©tÃ© crÃ©Ã©es avant que les ransomwares ne deviennent un sujet crucial - alors pourquoi leur faire confiance ?

En prenant ces mesures, les infrastructures critiques, et toutes leurs parties prenantes, disposeront de plusieurs couches de dÃ©fense pour se protÃ©ger contre les ransomwares et tout autre type de cyberattaque.

Ils disposeront des capacitÃ©s nÃ©cessaires pour minimiser l'impact des celles-ci lorsqu'elles se produisent inÃ©vitablement. De plus, ils seront en mesure de se remettre rapidement de tels incidents et de bÃ©nÃ©ficier dâ□□un dÃ©veloppement en toute sÃ©curitÃ© de leurs activitÃ©s. Â»