Professionnalisation de la cybercriminalitÃ©
Internet
PostÃ© par : JulieM
PubliÃ©e le : 18/1/2023 13:00:00

Le parquet de Paris a ouvert 600 enquÃªtes en 2022, soit dix fois plus que trois ans auparavant. Les attaques par ransomware reprÃ©sentent plus de la moitiÃ© des campagnes malveillantes, continuant ainsi dâ□□Ãªtre lâ□□arme de choix des cybercriminels.

Pourtant, dâ□□autres cibles et vecteurs dâ□□attaques ont Ã©voluÃ©, et sont devenus plus prÃ©sents au fil des mois.

Selon Dirk Schrader, VP of security research chez Netwrix, deux tendances se sont distinguÃ©es lâ□□annÃ©e passÃ©e et sont donc Ã surveiller en 2023 :

Â« La plupart des violations en 2022 prouvent un changement de tactique des cybercriminels. En effet, il y a eu une accÃ©lÃ©ration des attaques visant la supply chain.

Cette derniÃ¨re fait gÃ©nÃ©ralement rÃ©fÃ©rence Ã une entreprise tierce fournissant des biens ou des services Ã une organisation plus grande, une cible plus lucrative pour les hackers mais qui est dÃ©sormais bien cyber-protÃ©gÃ©e. La stratÃ©gie des cybercriminels est alors de compromettre une infrastructure informatique plus vulnÃ©rable et de l'utiliser comme point d'entrÃ©e, notamment dans les entreprises ou les agences gouvernementales.

En outre, les campagnes malveillantes contre la supply chain logicielle sont en forte croissance, câ□□est-Ã -dire lorsque la compromission arrive dÃ¨s le dÃ©veloppement dâ□□un produit via une faille technique. L'exploitation de ces vulnÃ©rabilitÃ©s pourrait mÃªme Ãªtre dÃ©vastatrice.

En utilisant simultanÃ©ment les deux vecteurs de la supply chain, un cybercriminel cible en effet les trois couches de la surface d'attaque d'une entreprise - donnÃ©es, identitÃ©s et infrastructure - avec une multitude de chemins d'attaque Ã sa disposition.

Un autre changement de stratÃ©gie rÃ©side dans la poursuite de la professionnalisation de l'industrie des malwares. Des groupes et des outils qui semblaient Ã©teints ont ainsi refait surface avec un impact fÃ©roce.

Lockbit et Emotet sont les principaux exemples pour illustrer cette expansion de la cybercriminalitÃ© via le ransomware-as-a-service. Et la violation d'Entrust, revendiquÃ©e par Lockbit, documente l'amÃ©lioration des opÃ©rations du groupe.

La cybercriminalitÃ© est aujourdâ□□hui un commerce comme un autre et vise par consÃ©quent Ã gagner de l'argent. Le cÃ´tÃ© positif pour les Ã©quipes IT de cette recherche vÃ©nale et de productivitÃ© est que, plus il est difficile de compromettre un environnement informatique dâ□□une organisation, plus les hackers sont susceptibles d'abandonner rapidement et de passer Ã une autre victime plus vulnÃ©rable.

Les entreprises doivent donc Ã©tendre leurs capacitÃ©s Ã mieux contrÃ´ler les accÃ¨s aux donnÃ©es. Lâ□□authentification et le privilÃ¨ge "juste Ã temps" sont les principales dÃ©fenses Ã mettre en place pour amÃ©liorer la sÃ©curitÃ© contre des tactiques malveillantes de plus en plus sophistiquÃ©es. Â»