Des cybercriminels en difficultÃ© ou mieux armÃ©s en 2022
Internet
PostÃ© par : JulieM
PubliÃ©e le : 10/12/2021 13:00:00

Selon le philosophe grec HÃ©raclite Â« rien nâ□□est permanent, sauf le changement Â». Cette citation est toujours pertinente des milliers d'annÃ©es plus tard, en particulier pour Ã©laborer un bilan de 2021 ; une nouvelle annÃ©e marquÃ©e par des changements continus qui ont poussÃ© les entreprises Ã adopter de nouvelles cyber-stratÃ©gies pour renforcer leur rÃ©silience.Â
De mÃªme, les cybercriminels ont poursuivi leurs efforts pour affiner leurs mÃ©thodes, travailler plus intelligemment, se dÃ©placer plus rapidement et ainsi Ã©tendre les attaques, ou encore sâ□□immiscer plus profondÃ©ment dans les supply chain pour causer des dommages plus importants.
Lavi Lazarovitz, Head of Security Research au CyberArk Labs, observe l'Ã©volution des techniques des hackers et les potentielles consÃ©quences significatives pour lâ□□annÃ©e 2022 :
Â« Il existe principalement deux Ã©volutions qui impacteront grandement les mois Ã venir. Les entreprises criminelles se feront prendre Ã leurs propres jeux, forÃ§ant une refonte de leur sÃ©curitÃ©.

La technologie DevOps change la maniÃ¨re dont les activitÃ©s sont menÃ©es, et les entreprises criminelles ne font pas exception. Tout comme les fournisseurs de logiciels lÃ©gitimes, les cybercriminels utilisent des pipelines CI/CD, une infrastructure cloud et d'autres technologies numÃ©riques pour dÃ©velopper et vendre de nouvelles offres de malwares en tant que service (MaaS).
La nÃ©cessitÃ© de lancer rapidement de nouvelles fonctionnalitÃ©s sur le marchÃ© est motivÃ©e par la demande croissante d'outils, tels que les logiciels malveillants de vol d'identifiants, qui peuvent Ãªtre configurÃ©s pour collecter les identifiants et informations sensibles Ã lâ□□insu des utilisateurs.Â De tels malwares sont non seulement puissants, mais Ã©galement simples Ã utiliser, encourageant les attaquants novices Ã passer Ã lâ□□acte et renforÃ§ant les Ã□tats-nations sophistiquÃ©s qui les vendent.
Pourtant, Ã mesure que ces groupes criminels agissent de plus en plus comme de "vraies" entreprises, constituÃ©s de profils divers, ils s'exposeront Ã©galement Ã de nouveaux risques. Comme toute autre organisation, ils seront en effet confrontÃ©s Ã de nouveaux dÃ©fis de sÃ©curitÃ©, en termes de gestion des applications SaaS multi-tenant ou encore de la sÃ©curisation de l'accÃ¨s Ã distance Ã leurs systÃ¨mes et donnÃ©es sensibles.Â
Tout en Ã©tant obligÃ©s de renforcer leurs propres protections, les hackers malveillants seront donc de plus en plus mis Ã mal par ceux qui sont bienveillants et qui utiliseront leurs tactiques offensives contre eux.
Les innovations technologiques aideront les cybercriminels Ã rester indÃ©tectÃ©sÂ

La cybersÃ©curitÃ© deviendra encore plus compliquÃ©e Ã cause de nouvelles "cachettes" introduites par les technologies du cloud, de la virtualisation et des conteneurs.Â
Ainsi, alors que la micro-virtualisation se dÃ©mocratise, les cybercriminels peuvent isoler les malwares dans ces systÃ¨mes virtuels tout en les gardant cachÃ©s des contrÃ´les de sÃ©curitÃ© de lâ□□entreprise.Â
Bien que ces nouvelles techniques d'attaque n'aient pas encore Ã©tÃ© beaucoup observÃ©es, des hackers motivÃ©s par lâ□□appÃ¢t du gain, ainsi que des Ã□tats-nations, ont Ã©tÃ© repÃ©rÃ©s en train de tester notamment le sous-systÃ¨me Windows pour Linux (WSL) - un sous-systÃ¨me qui sÃ©curise les informations d'identification et processus d'authentification - alors qu'ils recherchaient de nouvelles faÃ§ons de compromettre les appareils.Â En exÃ©cutant un ransomware au sein d'une infrastructure Linux, par exemple, les outils dÃ©diÃ©s aux points dâ□□accÃ¨s ne peuvent gÃ©nÃ©ralement pas identifier l'activitÃ© malveillante, ce qui permet aux acteurs malveillants de chiffrer ou d'exfiltrer facilement les donnÃ©es, tout en restant cachÃ©s de tous.

Si cette premiÃ¨re prÃ©diction est de bon augure pour la lutte contre la cybercriminalitÃ©, la seconde va rendre encore plus difficile lâ□□identification de campagnes malveillantes.Â
Les organisations devront donc sâ□□assurer que leurs stratÃ©gies de cybersÃ©curitÃ© prennent bien en compte lâ□□Ã©volution des cybermenaces et des vulnÃ©rabilitÃ©s associÃ©es Ã lâ□□adoption de nouvelles technologies.Â
Alors seulement, elles pourront protÃ©ger efficacement leurs donnÃ©es sensibles et assurer la pÃ©rennitÃ© des activitÃ©s. Â»