Cyberguerre en 2018 selon Venafi
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 23/1/2018 14:30:00

En matiÃ¨re de cyber criminalitÃ©, 2017 a Ã©tÃ© une annÃ©e record : davantage de sonnÃ©es ont Ã©tÃ© dÃ©robÃ©es sur les six premiÃ¨re mois de lâannÃ©e que par rapport Ã lâensemble de lâannÃ©e 2016. Dâaprã¨s lâindice des niveaux de violation de sÃ©curitÃ© de Gemalto, plus de 900 violations de donnÃ©e ont Ã©tÃ© perpÃ©trÃ©es au premier trimestre 2017, soit plus de 1,9 million de documents compromis.

Selon Jing Xie, chercheur senior en sÃ©curitÃ© numÃ©rique pour le leader du marchÃ© de la cybersÃ©curitÃ© Venafi, cette explosion du nombre dâexfiltrations de donnÃ©es va se poursuivre en 2018.

Autre tendance plus inquiÃ©tante, le nombre de cyberattaques sophistiquÃ©es commanditÃ©es par des Ãtats a lui aussi trÃ¨s nettement augmentÃ© lâan dernier.Â

Â« En 2017, les cyber criminels travaillant pour des Ãtats-nations ont visÃ© lâefficacitÃ© et le retour sur investissement, et ont largement atteint leurs objectifs Â», poursuit J. Xie.Â

Â« Par voie de consÃ©quence, nous devrions assister cette annÃ©e Ã une escalade et Ã des variantes de vecteurs dâattaque similairesÂ».

J. Xie sâest livrÃ© Ã une Ã©tude de lâÃ©tat gÃ©nÃ©ral de la guerre de lâinformation

stratÃ©gique commanditÃ©e par des Ã□tats-nations et tire les conclusions suivantes pour 2018 :

â□¢ Les Ã□tats-nations qui se livrent Ã des cyberattaques vont continuer Ã viser les clÃ©s et les certificats.

Le bras de fer permanent qui oppose les super puissances va changer de nature, pour passer des programmes clandestins essentiellement menÃ©s Ã lâ□□abri des regards Ã des attaques publiques visant des infrastructures et des services stratÃ©giques.Â

Les systÃ¨mes de sÃ©curitÃ© fondamentaux contrÃ´lant la communication entre les machines, beaucoup de cyberattaques viseront les clÃ©s et les certificats compromis ou faux. Un Ã□tat-nation qui possÃ¨de ce pouvoir pourra en effet bombarder des infrastructures stratÃ©giques de toute une sÃ©rie dâ□□attaques de plus en plus sophistiquÃ©es, en sabotant des services de base via des attaques articulÃ©es autour de Stuxnet et Duqu.

â□¢ Les autoritÃ©s de certification pourront constituer une cible en tant que cyber armes.

Les cyber criminels engagÃ©s par les Ã□tats-nations pourront trouver des moyens dâ□□exploiter les modÃ¨les de confiance utilisÃ©s pour contrÃ´ler la communication entre les machines. La faÃ§on la plus simple dâ□□y parvenir serait dâ□□attaquer ou de manipuler les autoritÃ©s de certification et les clÃ©s et les certificats quâ□□elles dÃ©livrent.Â

En cas de rÃ©ussite, ce vecteur dâ□□exploitation permettrait aux cyber criminels dâ□□Ã©couter un large spectre de communications confidentielles, dâ□□intercepter et de rÃ©orienter le trafic cryptÃ© et de viser les chiens de garde de lâ□□Ã□tat et les dÃ©fenseurs des droits de lâ□□homme.

â□¢ Les Ã©lections vont faire lâ□□objet de plus en plus dâ□□attaques et de menaces.

On a pu assister lors de lâ□□Ã©lection prÃ©sidentielle amÃ©ricaine de 2016 Ã de nombreuses campagnes orchestrÃ©es par des Ã□tats sur les mÃ©dias sociaux, qui visaient Ã faire naÃ®tre le doute et la crainte, dans lâ□□opinion publique. La rÃ©ussite de ces campagnes laisse prÃ©sager de nouvelles attaques contre des Ã©lections locales et nationales.Â

Certaines attaques pourront mÃªme utiliser de fausses identitÃ©s, de personnes ou de machines, pour voler puis faire fuiter des donnÃ©es sensibles de certains Ã□tats-nations. Il est dÃ©sespÃ©rant, Ã cet Ã©gard, de constater que des attaques de ce type se produisent bel et bien lors dâ□□Ã©lections organisÃ©es Ã travers le monde.

Â« Les principaux Ã□tats-nations investissent de plus en plus dans la cyberguerre, tant offensive que dÃ©fensive. Les fournisseurs dâ□□infrastructures et de systÃ¨mes de communication publics et privÃ©s devraient, en toute logique, se retrouver au centre de cette cyberguerre.Â

Enfin, si lâ□□on considÃ¨re lâ□□impact cumulÃ© de ces dÃ©penses massives et de la multiplication des attaques, il faut aussi sâ□□attendre cette annÃ©e Ã ce quâ□□au moins un acte de cyberguerre commanditÃ© par un Ã□tat-nation affecte directement les citoyens Â», ajoute J. Xie.

Pour en savoir davantage.