Etude Gigamon : Ã©tat et progression des ransomwares en France
Internet
PostÃ© par : JPilo
PubliÃ©e le : 30/9/2022 14:00:00

Ce nâ□□est plus un secret mais ces derniÃ¨res annÃ©es, les entreprises se sont retrouvÃ©es assaillies de toute part face Ã lâ□□augmentation significative des attaques par ransomwares.

En effet, les ransomwares ont pris une telle place dans le paysage cyber que les Ã©quipes de sÃ©curitÃ© du monde entier doivent constamment redoubler dâ□□effort afin dâ□□adapter leurs pratiques et leurs processus face Ã cet environnement cyber en constante Ã©volution.

Pour comprendre lâ□□ampleur de ce phÃ©nomÃ¨ne, Gigamon, lâ□□expert de l'observabilitÃ© avancÃ©e, a menÃ© une Ã©tude mondiale sur lâ□□Ã©tat et la progression des ransomwares et du paysage des menaces.

Il en ressort notamment que 95% des DSSI/RSSI dÃ©clarent avoir subi des attaques par ransomware au cours de lâ□□annÃ©e Ã©coulÃ©e.

Un paysage hostile

La pandÃ©mie mondiale a bouleversÃ© les entreprises du secteur de lâ□□IT qui ont dÃ» opÃ©rer une vÃ©ritable mÃ©tamorphose dans un laps de temps trÃ¨s court pour sâ□□adapter au nouveau contexte et rester rÃ©silientes.

Cela a ainsi donnÃ© naissance Ã de nombreux projets de transformation numÃ©rique accÃ©lÃ©rÃ©s pour accompagner le passage au cloud. Une situation dont les cybercriminels ont su tirer profit pour multiplier leurs attaques par ransomwares et dÃ©rober des donnÃ©es clÃ©s aux entreprises.

Aujourdâ□□hui, Ã mesure que nous entrons dans une Ã¨re post-pandÃ©mie, la situation ne semble guÃ¨re sâ□□amÃ©liorer pour autant. En effet, 56% des DSI/RSSI franÃ§ais reconnaissent que la crise des ransomwares sâ□□est aggravÃ©e au cours des trois derniers mois.

Fort heureusement, les conseils dâ□□administrations des entreprises franÃ§aises sont conscients de lâ□□ampleur du risque ransomware et considÃ¨rent cette menace comme une prÃ©occupation prioritaire (86%).

Sur la question des mÃ©thodes dâ□□attaque par ransomware observÃ©es en France au cours de lâ□□annÃ©e Ã©coulÃ©e, les personnes interrogÃ©es citent en premier lieu le phishing (56%) et les virus informatiques comme les logiciels malveillants (56%). Dans un second temps viennent, le smishing (phishing par SMS) (31%), les menaces internes accidentelles (30%) et les applications cloud (28%).

Une recrudescence dâ□□attaques ransomwares aux causes multiples

Lâ□□enquÃªte a Ã©galement interrogÃ© les professionnels de la sÃ©curitÃ© franÃ§ais sur ce quâ□□ils considÃ¨rent Ãªtre comme les principaux facteurs et causes de lâ□□augmentation de la frÃ©quence des attaques par ransomware. Pour 63% dâ□□entre eux, lâ□□aggravation de la crise est principalement due Ã la sophistication croissante des cybercriminels. Parmi les autres causes, les professionnels citent :

â¢ La complexitÃ© croissante des environnements hybrides et multicloud qui crÃ©e de nouvelles vulnÃ©rabilitÃ©s que les solutions traditionnelles ne peuvent pas dÃ©tecter (40 %)
â¢ La pÃ©nurie de compÃ©tences IT (40 %)
â¢ La menace interne (29%)

Pour lutter contre cette menace qui ne laisse aucun rÃ©pit aux Ã©quipes de sÃ©curitÃ©, le besoin dâune plus grande visibilitÃ© pour identifier les endroits oÃ¹ les ransomwares peuvent se cacher est dÃ©sormais indispensable.

Lâobservabilitâ© comme moyen de dÃ©fense

Dans un contexte de ressources moindres, de plus grande complexitÃ© liÃ©e aux environnements hybrides et dâune mauvaise configuration du cloud, la visibilitÃ© est un des leviers principaux de lâattÃ©nuation du risque de ransomware. En effet, sans une vision plus globale et prÃ©cise, il devient compliquÃ© pour les entreprises dâanticiper et gÃ©rer les attaques les plus sophistiquÃ©es.

Pour les prochains mois, les entreprises franÃ§aises envisagent de concentrer leurs efforts sur :

â¢ la sensibilisation et formation Ã la sÃ©curitÃ© pour tous les collaborateurs compte tenu du nouveau modÃ¨le de travail hybride : 89%
â¢ Lâadoption d'une architecture de Zero Trust pour encourager une culture de la sÃ©curitÃ© axÃ©e sur la vÃ©rification et la confiance implicite : 57%
â¢ Permettre lâobservabilitÃ© avancÃ©e, une visibilitÃ© holistique, sur lâensemble de lâinfrastructure IT 50%

Si lâinvestissement dans un plus grand nombre dâoutils est en gÃ©nÃ©ral une des premiÃ¨res solutions identifiÃ©es, les entreprises ont pris conscience quâelles ne peuvent plus continuer Ã les empiler pour rÃ©soudre leurs problÃ¨mes de sÃ©curitÃ©.

Dâaprâ¨s lâÃ©tude Gigamon, 57 % des professionnels interrogÃ©s reconnaissent que les outils de sÃ©curitÃ© quâils utilisent actuellement ne sont pas si efficaces sans une visibilitÃ© complÃ¨te. Raison pour laquelle, il est indispensable dâopter pour une optimisation de la visibilitÃ©.

Lâobservabilitâ© avancÃ©e est de plus en plus synonyme de protection contre les ransomwares, en particulier dans le cloud. LâenquÃªte rÃ©vÃ¨le notamment que 85% des responsables franÃ§ais de la sÃ©curitÃ© interrogÃ©s affirment que lâobservabilitâ© avancÃ©e est un Ã©lÃ©ment important de la sÃ©curitÃ© du cloud.

MÃ©thodologie :

Gigamon a analysÃ© les tÃ©moignages de 1020 dÃ©cideurs IT et sÃ©curitÃ© sur six marchÃ©s mondiaux clÃ©s : les Ãtats-Unis, le Royaume-Uni, la France (200), lâAllemagne, lâAustralie et Singapour.