Se protÃ©ger face aux nouvelles formes de ransomwares
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 30/6/2021 13:00:00

Selon lâ□□ANSSI, les ransomwares ont reprÃ©sentÃ© la plus grande menace pour les infrastructures IT en 2020. Les signalements liÃ©s Ã ce type dâ□□attaques ont en effet Ã©tÃ© multipliÃ©s par quatre par rapport Ã 2019. Des secteurs dâ□□activitÃ© critiques, tels que la santÃ© ou les collectivitÃ©s territoriales, sont particuliÃ¨rement ciblÃ©s.

Lors de ces campagnes, les cybercriminels soumettent les organisations Ã une forte pression pour les inciter Ã payer une ranÃ§on en Ã©change du dÃ©chiffrement de donnÃ©es critiques. En outre, les ransomwares sont de plus en plus sophistiquÃ©s pour permettre aux cybercriminels de cibler davantage leurs victimes.

Pour Jean-Christophe Vitu, VP Solutions Engineers chez CyberArk, lâ□□Ã©mergence de nouvelles formes de ransomwares met en avant lâ□□urgence dâ□□une protection efficace et adaptÃ©e des entreprises pour protÃ©ger leurs donnÃ©es les plus critiques :

Â« Des attaques par ransomware ciblÃ©es ont rÃ©cemment vu le jour dans le but dâ□□obtenir des gains plus importants. DÃ©sormais, les cybercriminels visent des organisations spÃ©cifiques, en fonction de leur capacitÃ© (ou de leur besoin) Ã payer des ranÃ§ons Ã©levÃ©es, en utilisant des techniques, tactiques et procÃ©dures (TTP) personnalisÃ©es.

Les centres hospitaliers par exemple, sont plus enclins Ã sâ□□acquitter de la compensation demandÃ©e pour pouvoir reprendre leurs activitÃ©s et prendre en charge les patients.

Les attaquants effectuent des recherches approfondies en amont de lâ□□attaque pour bien comprendre la "pile technologique" de leur cible, soit les spÃ©cificitÃ©s de son infrastructure IT.

Ces campagnes sont ainsi orchestrÃ©es grÃ¢ce Ã lâ□□identification prÃ©cise des vulnÃ©rabilitÃ©s des organisations, telles que les donnÃ©es les plus prÃ©cieuses Ã chiffrer et Ã retenir contre une ranÃ§on.

Les hackers parviennent Ã©galement Ã cibler les dispositifs de sauvegardes de donnÃ©es afin que les organisations ne puissent pas restaurer les fichiers aprÃ¨s leur chiffrement par le ransomware. Ils sont de plus capables de construire des "portes dÃ©robÃ©es" dans les rÃ©seaux, afin de pouvoir sâ□□y rÃ©introduire quand ils le souhaitent. Les organisations peuvent donc se retrouver face Ã des menaces constantes.

A titre dâ□□exemple, des campagnes malveillantes du ransomware Hades ont rÃ©cemment ciblÃ© plusieurs multinationales des secteurs du transport et du commerce de dÃ©tail en suivant un processus bien prÃ©cis.

La compromission dâ□□identifiants liÃ©s Ã des accÃ¨s Ã privilÃ¨ges ont permis aux cybercriminels dâ□□infiltrer les systÃ¨mes de lâ□□entreprise via les rÃ©seaux privÃ©s virtuels (VPN), ou les protocoles permettant dâ□□utiliser les appareils Ã distance (RDP). Ils peuvent ensuite mettre en place des attaques par double extorsion, qui consistent Ã exfiltrer des donnÃ©es sensibles, puis Ã demander une ranÃ§on sous peine de publier ces informations.

Les attaques de ransomware prennent donc gÃ©nÃ©ralement leur source au niveau dâ□□un point

dâ□□entrÃ©e. Lors dâ□□une tentative de connexion, une mauvaise configuration des accÃ¨s Ã privilÃ¨ges constitue une opportunitÃ© pour les cybercriminels de voler et de chiffrer des donnÃ©es. Par consÃ©quent, une simple solution de sÃ©curitÃ© des accÃ¨s, quâ□□il sâ□□agisse dâ□□un dispositif de dÃ©tection ou encore dâ□□un antivirus, ne suffit pas Ã se protÃ©ger de ce type dâ□□attaque.

Il est alors nÃ©cessaire de mettre en place dâ□□une approche globale de sÃ©curisation des terminaux, basÃ©e sur la gestion des accÃ¨s Ã privilÃ¨ges. Cette derniÃ¨re permet de rÃ©duire la vulnÃ©rabilitÃ© des systÃ¨mes informatiques, grÃ¢ce Ã une dÃ©tection efficace des intrusions malveillantes favorisant une intervention rapide des Ã©quipes IT.

Les mises Ã jour rÃ©guliÃ¨res des applications et des systÃ¨mes dâ□□exploitation sont Ã©galement des moyens de protection Ã prendre en compte, puisque celles-ci contiennent gÃ©nÃ©ralement des correctifs de sÃ©curitÃ© permettant de limiter les risques dâ□□attaques liÃ©s Ã lâ□□obsolescence des infrastructures. Enfin, la mise en place de lâ□□approche du moindre privilÃ¨ge est efficace, afin dâ□□accorder aux utilisateurs le niveau dâ□□accÃ¨s minimum requis pour accomplir leur travail ; limitant donc les dÃ©placements latÃ©raux en cas de compromission.

Lâ□□adoption de ces stratÃ©gies permet aux entreprises de rÃ©pondre Ã lâ□□impÃ©ratif dâ□□une protection accrue, imposÃ©e par le perfectionnement des ransomwares. GrÃ¢ce Ã des mesures de sÃ©curitÃ© adÃ©quates et adaptÃ©es Ã ces nouvelles formes dâ□□attaque, les organisations peuvent poursuivre leurs activitÃ©s sereinement, tout en prÃ©servant leurs ressources les plus prÃ©cieuses. Â»Â