Faire face aux ransomware de type Â« Living Off the Land Â»
Internet
PostÃ© par : JulieM
PubliÃ©e le : 18/8/2021 13:00:00

Les cyberattaques de type Â« living off the land Â» (ou LotL) constituent dÃ©sormais lâ□□une des menaces les plus redoutables pour les entreprises. La rÃ©cente campagne de ransomware contre Kaseya nâ□□est ainsi que le dernier exemple en date, dans lequel les cybercriminels ont utilisÃ© les ressources technologiques de lâ□□organisation contre elle. Ces types dâ□□attaques procurent en effet aux cybercriminels deux leviers clÃ©s : lâ□□accÃ¨s et le temps.

Selon Ketty Cassamajor, Responsable Avant-Vente Europe du Sud chez CyberArk, si les attaques LotL ne se concluent pas toujours par un ransomware, les deux vont de plus en plus souvent de pair et sont aussi difficiles Ã Ã©valuer quâ□□Ã prÃ©venir. Une stratÃ©gie de protection efficace commence donc par une solide comprÃ©hension de ce qui constitue une attaque par ransomware LotL et des dommages quâ□□elle peut causer.

Â« DÃ¨s 2017, les attaques de malwares sans fichier ont commencÃ© Ã attirer lâ□□attention du grand public aprÃ¨s la divulgation de rapports faisant Ã©tat dâ□□infections de systÃ¨mes IT de plusieurs grandes organisations. Or, ces malwares sans fichier ont rendu possibles les attaques LotL.

En Ã©liminant la nÃ©cessitÃ© de stocker la charge utile malveillante dans un fichier, ou de lâ□□installer directement sur une machine, les cybercriminels peuvent alors Ã©chapper aux antivirus, et aux autres outils traditionnels de sÃ©curitÃ© des terminaux. Ils se dÃ©placent ensuite latÃ©ralement dans lâ□□environnement, en escaladant les privilÃ¨ges et en dÃ©voilant de nouveaux niveaux dâ□□accÃ¨s, jusquâ□□Ã ce quâ□□ils atteignent le but ultime : les systÃ¨mes, les applications et les bases de donnÃ©es contenant des actifs commerciaux essentiels, tels que les donnÃ©es clients et la propriÃ©tÃ© intellectuelle.

Pour se maintenir dans les systÃ¨mes sans Ãªtre dÃ©tectÃ©s, ces malwares sans fichier se font souvent passer pour un outil de confiance dotÃ© de privilÃ¨ges et dâ□□accÃ¨s Ã©levÃ©s. Cela permet aux attaquants de surveiller lâ□□environnement, de rÃ©cupÃ©rer des identifiants, en prenant tout le temps nÃ©cessaire.

Il est extrÃªmement difficile dâ□□identifier, et encore plus dâ□□arrÃªter, ces attaques, surtout sâ□□il sâ□□agit dâ□□un ransomware sophistiquÃ© qui cible spÃ©cifiquement lâ□□organisation. Pour y faire, il nâ□□y a pas dâ□□autre choix que de penser comme des attaquants, tout en gardant Ã lâ□□esprit quâ□□une campagne nâ□□est pas nÃ©cessairement identique Ã une autre.

Le cheminement des attaques LotL nâ□□est en effet pas linÃ©aire. Lâ□□objectif est donc de dÃ©chiffrer lâ□□environnement et de dÃ©velopper une approche fondÃ©e sur ce qui sâ□□y trouve.

La plupart des attaques LotL suivent ainsi un schÃ©ma similaire : usurper des identitÃ©s pour sâ□□infiltrer dans un rÃ©seau dâ□□entreprise, compromettre des systÃ¨mes, Ã©lever des privilÃ¨ges et se dÃ©placer latÃ©ralement jusquâ□□Ã obtenir lâ□□accÃ¨s aux systÃ¨mes sensibles nÃ©cessaires Ã lâ□□exÃ©cution de lâ□□attaque ou Ã la propagation du ransomware.

Mais Ã chaque Ã©tape, il existe des possibilitÃ©s divergentes qui rendent le suivi et lâ□□anticipation de ces attaques trÃ¨s complexes. Les Ã©quipes IT doivent donc bÃ©nÃ©ficier des

outils nÃ©cessaires pour dÃ©composer les comportements et les indicateurs dâ□□alerte Ã surveiller, lors des Ã©tapes critiques dâ□□une attaque par ransomware LotL, et ce, afin dâ□□accÃ©lÃ©rer la dÃ©tection et de rÃ©duire lâ□□exposition et les dommages.

Cependant, compte tenu du nombre de techniques Ã©prouvÃ©es dont disposent les cybercriminels, il peut se rÃ©vÃ©ler difficile de savoir comment traiter les points de vulnÃ©rabilitÃ© ou par oÃ¹ commencer. Lâ□□Ã©laboration dâ□□une stratÃ©gie de protection efficace contre les ransomwares exige des organisations quâ□□elles Ã©tudient les maillons de la chaÃ®ne dâ□□attaque qui prÃ©sentent les niveaux de risque les plus Ã©levÃ©s et quâ□□elles les classent par ordre de prioritÃ©.

Ainsi, une sÃ©curisation des terminaux Ã plusieurs niveaux - combinant la dÃ©fense par le moindre privilÃ¨ge, lâ□□authentification forte des identitÃ©s, la protection contre le vol dâ□□informations dâ□□identification, le contrÃ´le des applications et le blocage des ransomwares - compliquera considÃ©rablement la tÃ¢che des hackers qui voudront sâ□□introduire et maintenir leur prÃ©sence.

Car une fois quâ□□ils ont un pied dans le rÃ©seau informatique, il leur est facile de brouiller les pistes et dâ□□intensifier leur action. Â»Â