Cryptojacking, la nouvelle ruée vers l'or

Ces derniers mois, une nouvelle tendance de cybercriminalitÃ© est apparue. Certains pirates informatiques ne cherchent plus Ã extorquer de l'argent aux entreprises par le biais dâ€™attaques par logiciel de ranÃ§on. Au lieu de cela, ils utilisent les ordinateurs de leurs victimes Ã leur insu pour gagner de lâ€™argent.

On parle de cryptojacking lorsquâ€™un hacker exploite la puissance dâ€™ordinateurs qui ne lui appartiennent pas pour miner, autrement dit crÃ©er de la monnaie virtuelle. Pertes de productivitÃ©, coÃ»ts d'exploitation Ã©levÃ©s et mÃªme dÃ©tÃ©rioration de l'infrastructure informatique : les dommages causÃ©s par le cryptojacking affectent sensiblement les entreprises.

Le cryptojacking est en plein essor

MalgrÃ© la chute des cours, les cryptomonnaies ont les reins solides et valent encore la peine dâ€™Ãªtre minÃ©es. Cela nÃ©cessite une Ã©norme puissance de calcul. Pour lâ€™atteindre, un cybercriminel peut introduire un malware dans le rÃ©seau d'une entreprise afin dâ€™exploiter et de combiner Ã son insu la puissance de ses ordinateurs.

La technique est de plus en plus prisÃ©e des hackers. Le nombre de nouveaux malware de ce type a augmentÃ© de 4 000% entre 2017 et 2018. Plusieurs raisons Ã cet engouement : la mÃ©thode est simple Ã mettre en Å“uvre, est rarement identifiÃ©e comme une menace directe par les entreprises et promet de bons rÃ©sultats. On estime en effet que le seul script Coinhive, conÃ§u pour miner la cryptomonnaie Minero, gÃ©nÃ¨re chaque mois environ 150 000 dollars.

Avec la puissance combinÃ©e de plusieurs milliers d'ordinateurs, lâ€™efficacitÃ© est dÃ©multipliÃ©e. Câ€™est pourquoi les hackers crÃ©ent des rÃ©seaux entiers de robots dÃ©diÃ©s au cryptominage. Lâ€™un dâ€™entre eux, Smominru, serait ainsi composÃ©, selon les sources, de 500 000 Ã 1 million de machines Windows dans le monde, principalement des serveurs dâ€™entreprises et de gouvernements.

Pertes de productivitÃ©, dommages informatiques et coÃ»ts cachÃ©s

Les attaques de cryptojacking ralentissent considÃ©rablement les opÃ©rations informatiques de lâ€™entreprise, impactent donc sa productivitÃ©, et augmentent Ã©galement les coÃ»ts dâ€™exploitation.

Fin 2018, le minage de Bitcoin consommait Ã lui seul 73 tÃ©rawattheures par an, soit la consommation Ã©lectrique annuelle de l'Autriche. Une proportion croissante des coÃ»ts Ã©nergÃ©tiques liÃ©s au minage de cryptomonnaie est imputable Ã des activitÃ©s illÃ©gales, et en partie incluse dans les coÃ»ts d'exploitation des entreprises.

Des coÃ»ts cachÃ©s, tels qu'une durÃ©e de vie plus courte de l'infrastructure informatique, doivent Ãªtre pris en compte. La dÃ©gradation de lâ€™image dâ€™une entreprise, ainsi que tous les problÃ¨mes liÃ©s Ã la non conformitÃ© aux obligations de notification en cas dâ€™attaque, entrent Ã©galement dans lâ€™Ã©quation.

Comment contrer le cryptojacking ?

La connaissance de lâ€™Ã©tat actuel de lâ€™infrastructure constitue la base de toute stratÃ©gie de dÃ©fense. Les entreprises doivent rÃ©guliÃ¨rement surveiller et auditer l'ensemble de leur architecture informatique, du site Web Ã chaque serveur et client. Elles doivent Ã©galement disposer dâ€™une vue dâ€™ensemble de tous les Ã©lÃ©ments connectÃ©s Ã leur rÃ©seau, y compris les terminaux personnels utilisÃ©s par les salariÃ©s.

Des signaux faibles peuvent vous mettre la puce Ã lâ€™oreille - par exemple, un utilisateur qui se plaint du bruit que fait le ventilateur de son ordinateur. Les tÃ¢ches non identifiÃ©es qui gÃ©nÃ¨rent cette surcharge de travail pour lâ€™ordinateur doivent immÃ©diatement Ãªtre considÃ©rÃ©es comme suspectes et examinÃ©es avec attention. Il vaudra Ã©galement la peine de vÃ©rifier les logiciels tiers qui renvoient Ã du code source autre que celui de lâ€™entreprise.

Lâ€™Ã©tape suivante consiste Ã rÃ©duire la surface d'attaque grÃ¢ce Ã des technologies et des bonnes pratiques. Celles-ci doivent couvrir les trois phases de la cyberdÃ©fense : dÃ©tecter les tentatives d'intrusion, prendre des mesures Ã temps et protÃ©ger les points vulnÃ©rables. La dÃ©fense contre le cryptojacking ne peut par ailleurs pas Ãªtre fondÃ©e sur des mesures isolÃ©es. Seule une approche unifiÃ©e et Ã plusieurs niveaux peut Ãªtre efficace.

Le dÃ©ploiement rÃ©gulier et systÃ©matique des correctifs de sÃ©curitÃ© est aussi indispensable. Les pirates informatiques accÃ¨dent en effet au matÃ©riel principalement par le biais d'applications et de systÃ¨mes d'exploitation obsolÃ¨tes. Smominru exploite par exemple des vulnÃ©rabilitÃ©s connues, pour lesquelles un correctif existe, pour prendre le contrÃ´le des machines Windows.

La sÃ©curitÃ© informatique ne pourra jamais Ãªtre assurÃ©e Ã 100%, mais les attaques peuvent Ãªtre rendues plus difficiles. Les bonnes pratiques telles que le dÃ©ploiement des correctifs et la mise Ã jour des antivirus, ainsi que les technologies de dÃ©couverte, de contrÃ´le des applications et des pÃ©riphÃ©riques ou encore de gestion des droits et des privilÃ¨ges, permettent en effet de maÃ®triser environ 95% des risques informatiques au niveau du poste client.