

Cryptojacking, la nouvelle ruée vers l'or

Ces derniers mois, une nouvelle tendance de cybercriminalité est apparue. Certains pirates informatiques ne cherchent plus à extorquer de l'argent aux entreprises par le biais d'attaques par logiciel de rançon. Au lieu de cela, ils utilisent les ordinateurs de leurs victimes à leur insu pour gagner de l'argent.

On parle de cryptojacking lorsqu'un hacker exploite la puissance d'ordinateurs qui ne lui appartiennent pas pour miner, autrement dit créer de la monnaie virtuelle. Pertes de productivité, coûts d'exploitation élevés et même détérioration de l'infrastructure informatique : les dommages causés par le cryptojacking affectent sensiblement les entreprises.

Le cryptojacking est en plein essor

Malgré la chute des cours, les cryptomonnaies ont les reins solides et valent encore la peine d'être minées. Cela nécessite une énorme puissance de calcul. Pour l'atteindre, un cybercriminel peut introduire un malware dans le réseau d'une entreprise afin d'exploiter et de combiner à son insu la puissance de ses ordinateurs.

La technique est de plus en plus prisée des hackers. Le nombre de nouveaux malwares de ce type a augmenté de 4 000% entre 2017 et 2018. Plusieurs raisons à cet engouement : la méthode est simple à mettre en oeuvre, est rarement identifiée comme une menace directe par les entreprises et promet de bons résultats. On estime en effet que le seul script Coinhive, conçu pour miner la cryptomonnaie Minero, génère chaque mois environ 150 000 dollars.

Avec la puissance combinée de plusieurs milliers d'ordinateurs, l'efficacité est démultipliée. C'est pourquoi les hackers créent des réseaux entiers de robots dédiés au cryptominage. L'un d'entre eux, Smominru, serait ainsi composé, selon les sources, de 500 000 à 1 million de machines Windows dans le monde, principalement des serveurs d'entreprises et de gouvernements.

Pertes de productivité, dommages informatiques et coûts cachés

Les attaques de cryptojacking ralentissent considérablement les opérations informatiques de l'entreprise, impactent donc sa productivité, et augmentent également les coûts d'exploitation.

Fin 2018, le minage de Bitcoin consommait à lui seul 73 térawattheures par an, soit la consommation électrique annuelle de l'Autriche. Une proportion croissante des coûts énergétiques liés au minage de cryptomonnaie est imputable à des activités illégales, et en partie incluse dans les coûts d'exploitation des entreprises.

Des coûts cachés, tels qu'une durée de vie plus courte de l'infrastructure informatique, doivent être pris en compte. La dégradation de l'image d'une entreprise, ainsi que tous les problèmes liés à la non conformité aux obligations de notification en cas d'attaque, entrent également dans l'équation.

Comment contrer le cryptojacking ?

La connaissance de l'état actuel de l'infrastructure constitue la base de toute stratégie de défense. Les entreprises doivent régulièrement surveiller et auditer l'ensemble de leur architecture informatique, du site Web à chaque serveur et client. Elles doivent également disposer d'une vue d'ensemble de tous les éléments connectés à leur réseau, y compris les terminaux personnels utilisés par les salariés.

Des signaux faibles peuvent vous mettre la puce à l'oreille - par exemple, un utilisateur qui se plaint du bruit que fait le ventilateur de son ordinateur. Les tâches non identifiées qui génèrent cette surcharge de travail pour l'ordinateur doivent immédiatement être considérées comme suspectes et examinées avec attention. Il vaudra également la peine de vérifier les logiciels tiers qui renvoient à du code source autre que celui de l'entreprise.

L'étape suivante consiste à réduire la surface d'attaque grâce à des technologies et des bonnes pratiques. Celles-ci doivent couvrir les trois phases de la cyberdéfense : détecter les tentatives d'intrusion, prendre des mesures à temps et protéger les points vulnérables. La défense contre le cryptojacking ne peut par ailleurs pas être fondée sur des mesures isolées. Seule une approche unifiée et à plusieurs niveaux peut être efficace.

Le déploiement régulier et systématique des correctifs de sécurité est aussi indispensable. Les pirates informatiques accèdent en effet au matériel principalement par le biais d'applications et de systèmes d'exploitation obsolètes. Smominru exploite par exemple des vulnérabilités connues, pour lesquelles un correctif existe, pour prendre le contrôle des machines Windows.

La sécurité informatique ne pourra jamais être assurée à 100%, mais les attaques peuvent être rendues plus difficiles. Les bonnes pratiques telles que le déploiement des correctifs et la mise à jour des antivirus, ainsi que les technologies de découverte, de contrôle des applications et des périphériques ou encore de gestion des droits et des privilèges, permettent en effet de maîtriser environ 95% des risques informatiques au niveau du poste client.