Protection contre les malwares de cryptominage

L'un des principaux types de cyberattaques ayant fait son apparition dernièrement repose sur le cryptominage.

Tandis que le cryptominage en tant que tel sert une bonne cause lorsqu'il est pratiqué consciencieusement, il permet également à des acteurs malveillants de gagner rapidement beaucoup d'argent et face au grand nombre de cryptomonnaies disponibles, il devient un moyen très prisé des auteurs d'attaques.

Cette technique consiste essentiellement, pour un pirate, à exploiter la puissance de l'ordinateur d'une tierce personne afin de produire de la cryptomonnaie. Une fois la machine infectée, le malware peut utiliser en intégralité ou en partie la puissance de calcul du processeur, empêchant ce dernier d'exécuter d'autres tâches, privant ainsi l'utilisateur de l'accès à sa machine et à son application.

Le minage de cryptomonnaie nécessite une puissance de calcul considérable. Les auteurs d'attaques de cryptominage recourent donc à des « pools », permettant à un grand nombre de « mineurs » de travailler ensemble et d'augmenter le capital engrangé. Comment les entreprises peuvent-elles protéger leurs systèmes contre une attaque de cette nature ?

Toucher la cible

Les pirates tentent d'exploiter toute interface accessible au public et pouvant leur permettre de mener leur attaque. Il peut s'agir de services cloud mal configurés : bases de données, cache, outils de gestion tels que Kubernetes, etc. Par exemple, une récente étude révèle que 75 % des serveurs Redis sont infectés par un malware de cryptominage. Cela dit, les serveurs web demeurent la principale cible des pirates, puisqu'ils ont vocation à être publics. De fait, le cryptominage est désormais si répandu que dans les derniers mois de 2017, le nombre d'attaques est monté en flèche, les chercheurs observant dans 88 % des cas d'exécution de code à distance (RCE) l'envoi de requêtes vers des sources externes pour tenter de télécharger un malware de cryptominage sur les machines cibles.

Pour lancer des attaques de cryptominage, les pirates commencent par rechercher une faille de type RCE, leur permettant d'exécuter du code arbitraire sur le serveur vulnérable. Par exemple, une récente vulnérabilité RCE exploitée pour le minage de cryptomonnaie était due à un défaut de sécurité dans la désérialisation. En l'occurrence, les assaillants ont manipulé des objets sérialisés qui ont été envoyés à l'application web. Ensuite, une fois l'objet désérialisé, du code malveillant était exécuté sur le serveur vulnérable, produisant de la cryptomonnaie pour l'auteur de l'attaque.

Les attaques de cryptominage emploient des techniques similaires aux autres en termes d'infection, de contournement et de persistance. Cependant, dans certains cas, nous observons des échantillons de malware tentant de maximiser l'attaque et ses profits, soit en se propageant dans le réseau à travers des équipements vulnérables, soit en injectant du code sur le serveur afin de toucher les utilisateurs finaux.

En outre, les attaques de cryptominage peuvent être le prélude d'autres types d'activité malveillante. Si un serveur est infecté, cela signifie généralement qu'il est vulnérable à une forme ou à une autre d'injection de code. La même faille ayant servi à infecter le serveur avec un malware de cryptominage peut être exploitée à nouveau pour une infection par un autre malware ou pour le lancement d'autres attaques par le même pirate. Un poste infecté offre à ce dernier une porte d'entrée dans votre réseau interne et peut lui permettre de propager l'attaque à d'autres machines dans l'entreprise.

Bien qu'il s'agisse sans doute de l'une des cryptomonnaies les plus connues et les plus répandues, les attaques de minage ne portent pas sur le bitcoin, non seulement car du matériel spécial est nécessaire pour en produire, mais aussi parce que les transactions en bitcoin ne sont pas privées. Cela signifie qu'il est possible de remonter à l'origine de chaque bitcoin le long de la chaîne de transaction, par conséquent les auteurs d'attaques ont plus de risques de se faire prendre. C'est pourquoi les attaques sont de plus en plus destinées au minage de cryptomonnaies plus récentes telles que Monero, Ethereum, Electroneum, Karbo... Celles-ci permettent en effet aux assaillants d'engager des transactions sans avoir à craindre leur traçabilité, car le solde de leur compte est invisible et les détails d'une transaction (expéditeur, destinataire ou montant des fonds transférés) sont confidentiels.

Protection contre les attaques de cryptominage

Pour se protéger contre les attaques de cryptominage, une entreprise doit s'efforcer de réduire sa surface d'attaque au minimum, en limitant autant que possible l'accès public à ses ressources et en mettant en place un processus d'authentification complexe. Un malware de cryptominage a généralement besoin d'une puissance de calcul considérable, de sorte qu'un moyen simple de le détecter consiste à surveiller une consommation élevée du processeur. Cependant, certaines attaques de ce type sont programmées pour passer inaperçues. Elles sont spécialement configurées de façon à ne pas surcharger le processeur, ce qui les rend plus difficilement détectables.

Afin d'assurer leur protection, les entreprises doivent tout d'abord veiller à ce que leurs systèmes soient totalement à jour avec tous les correctifs applicables. Pour que le cryptominage fonctionne, les auteurs d'attaques doivent commencer par exploiter une vulnérabilité. Or, si une entreprise est à jour de tous ses correctifs de sécurité, cette porte d'entrée est verrouillée. Etant donné que les pirates ciblent des vulnérabilités RCE pour lancer leur malware, les correctifs revêtent une importance cruciale. La sensibilisation des équipes informatiques et la mise à jour des systèmes avec les plus récents correctifs provenant de leur fournisseur permettent de colmater les failles de ce type.

Une autre solution consiste à appliquer des correctifs virtuels pour protéger activement les applications web contre les attaques. Cette solution permet de réduire la fenêtre de risque ainsi que le coût des correctifs d'urgence et des cycles de correction. Un firewall applicatif web procédant à des correctifs virtuels n'interfère pas avec le workflow normal des applications et assure la protection du site tout en laissant à ses exploitants la possibilité de contrôler la chronologie des correctifs.

Protégez vos systèmes dès à présent

Le cryptominage illicite est un moyen facile pour les acteurs malveillants de gagner de l'argent car il passe inaperçu de ses victimes mais n'en est pas moins lucratif. L'attaque elle-même est simple à

monter et ce vecteur supplante rapidement le ransomware. Bien que certains ne voient dans ce type d'attaque qu'une simple nuisance, le cryptominage peut causer des pannes gigantesques, en cas d'effondrement des infrastructures informatiques, sous l'effet de la production parasite de cryptomonnaies sur des systèmes infectés par des criminels. Les entreprises doivent donc agir pour protéger leurs systèmes contre ces acteurs malveillants espérant réaliser des profits rapides sans se faire repérer.