Protégez votre réseau contre le cryptomining

Comment protéger votre réseau contre le cryptomining illicite? Bloquez les menaces liées au cryptomining dans les e-mails, sur le réseau et dans le trafic web.

Introduction

Les hackers se tournent de plus en plus vers le cryptomining illicite pour augmenter leurs revenus de manière très simple. Le cryptomining se définit comme la production d'une monnaie virtuelle, également connue sous le nom de cryptomonnaie, comme le Bitcoin et le Monero. Il nuit aux performances du système et augmente sa consommation électrique. C'est pourquoi les hackers infiltrent les réseaux de leurs victimes pour exploiter leurs ressources de traitement. Dans ce livre blanc, apprenez à protéger votre entreprise contre le cryptomining illicite avec les solutions de sécurité Cisco®.

Vue d'ensemble

Notre équipe de chercheurs en cybersécurité Cisco Talos surveille l'évolution du cryptomining. Dans une étude récente, elle révèle que la cryptomonnaie Monero a vu sa valeur augmenter d'environ 3 000 % entre mars 2017 et mars 2018. Les analyses des chercheurs Cisco Talos démontrent que le cryptomining est plus rentable que les ransomwares pour les hackers, les rançons n'étant versées qu'une fois sur trois par les victimes. Le cryptomining illicite devrait donc gagner en popularité.

À ce jour, le cryptomining représente encore une part infime des menaces les plus répandues.
Notons qu'il existe des spécificités sectorielles :

- Pour les entreprises du secteur financier, le cryptomining opéré par les collaborateurs, de manière intentionnelle ou pas, peut causer des problèmes de conformité aux réglementations liées à la sécurité.
- Pour le secteur industriel, le cryptomining signifie une exploitation intense des ressources processeur des infrastructures critiques, pouvant dégrader la qualité ou interrompre les services.
- Pour toutes les entreprises, les data centers et les serveurs publics sont des environnements qui comptent de nombreux CPU et processeurs graphiques et qui sont donc très convoités par les cryptomineurs. En cas d'intrusion, les performances sont réduites, affectant l'expérience de l'utilisateur, en particulier sur des sites web publics, ce qui risque aussi de nuire à l'image de marque de l'entreprise.
- Pour toutes les entreprises, un logiciel de cryptomining peut être exploité par un tiers pour lancer une attaque. (Reportez-vous à l'encadré sur les attaques de la chaîne logistique.)

À moins que le cryptomining ne fasse partie des activités de votre entreprise, il est conseillé de bloquer tout le trafic de cryptomining et de supprimer toutes les applications de cryptomining de votre réseau.

Comment les hackers parviennent-ils à infecter les systèmes de leurs victimes ? Ils peuvent user de tous les moyens. Par exemple, un fournisseur d'accès à Internet a envoyé subrepticement des scripts de cryptomining à ses clients. L'appât facile du gain pousse les hackers à développer de nouvelles techniques et méthodes d'infection, plus précisément :

- Attaques de phishing par e-mail
- E-mails contenant des pièces jointes malveillantes
- Les sites web compromis qui injectent du code en exploitant les vulnérabilités des plug-ins du navigateur
- Processus système compromis exécutant du code modifié
- Les applications de cryptomining qui utilisent des communications chiffrées

En raison de la diversité des cibles et des méthodes d'infection, il n'existe pas de solution capable de vous protéger contre toutes les attaques. Une approche basée sur l'architecture est la plus adaptée en matière de couverture et d'évolutivité.

Notre gamme de solutions de sécurité détecte et bloque les menaces présentes dans les e-mails, sur le réseau et dans le trafic web, même si elles se cachent dans le trafic chiffré, les fichiers malveillants, les applications cloud ou les terminaux itinérants. Nous intégrons directement dans nos produits les résultats de nos recherches continues sur les menaces. Nos réponses sont automatisées pour vous protéger contre des menaces en perpétuelle évolution.

Ce livre blanc fournit des informations supplémentaires sur des sujets liés au cryptomining et sur la manière dont notre gamme de solutions de sécurité vous protège contre ces menaces.

Les attaques de la chaîne logistique

Les attaques de la chaîne logistique sont des attaques qui compromettent le processus de développement (la chaîne logistique) des services système et des applications. Étant donné qu'il s'agit de services et d'applications de confiance, les solutions de sécurité comme les antivirus ne les analysent pas. Les hackers exploitent cette confiance et utilisent ensuite le service ou l'application infecté comme point d'entrée permanent sur les réseaux de leurs victimes pour atteindre leur objectif, quel qu'il soit : surveillance, vol de données, attaques malveillantes, cryptomining, etc.

Nyetya et CCleaner en 2017 sont des exemples parfaits d'attaques de la chaîne logistique. Dans ces deux cas, les environnements de développement de fournisseurs d'applications légitimes ont été compromis par des hackers qui ont infecté des versions spécifiques du logiciel de leurs victimes, un logiciel auquel leurs clients se fiaient. L'attaque Nyetya a permis de lancer une attaque destructrice contre les clients du fournisseur de l'application dans le monde entier. Lors de l'attaque CCleaner, les hackers ont ciblé spécifiquement quelques entreprises, mais la version infectée de l'utilitaire CCleaner a été détectée très tôt par les logiciels de sécurité Cisco.

Une attaque de la chaîne logistique est particulièrement préoccupante dans le cas du cryptomining, car le logiciel n'est pas nécessairement un malware et utilise souvent des communications chiffrées. Avec l'adoption massive du cryptomining, les développeurs d'applications sont davantage axés sur la convivialité et la rapidité de déploiement que sur la sécurité. Un tiers malveillant pourrait vraisemblablement exploiter l'environnement du développeur de l'application, puis utiliser l'application compromise à ses propres fins. Par conséquent, nous recommandons aux entreprises de bloquer toutes les applications de cryptomining, sauf si elles les utilisent régulièrement.

Introduction : cryptomining, cryptojacking et cryptomonnaies

La cryptomonnaie est aujourd'hui un sujet de toutes les discussions, en particulier après l'augmentation de sa valeur fin 2017. Durant cette période, certains spéculateurs ont gagné des millions de dollars, ce qui rend le cryptomining illicite très attractif. Nous allons tout d'abord analyser les cryptomonnaies ainsi que les activités qui y sont associées, à savoir le cryptomining et le cryptojacking.

Les cryptomonnaies

Les cryptomonnaies sont des devises virtuelles distribuées qui ne relèvent d'aucune banque centrale ni d'aucun gouvernement. Elles utilisent la technologie Blockchain pour créer un grand livre de comptes distribué et sont donc quasiment infalsifiables. Le bitcoin est la cryptomonnaie la plus connue, mais elle est loin d'être la seule. Les devises virtuelles sont également intéressantes, car elles permettent aux utilisateurs de rester anonymes lors des transactions financières.

Le minage de la cryptomonnaie

Une cryptomonnaie acquiert de la valeur, en partie, en limitant le nombre d'unités de monnaie qui peuvent être créées. Ce processus de création s'appelle le minage ou cryptomining. Lors de la production de cryptomonnaie, l'ordinateur du cryptomineur doit résoudre un problème mathématique si complexe qu'il nuit aux ressources informatiques. Cet effort en matière de traitement se traduit par d'importants coûts énergétiques pour le cryptomineur. La logique voudrait que ces frais limitent le nombre de cryptomineurs et ralentissent ainsi la création d'unités de monnaie sur le long cours. Toutefois, cette approche présente une faille inattendue.

Aux débuts de la cryptomonnaie, un cryptomineur pouvait laisser le logiciel de cryptomining s'exécuter en arrière-plan sur un ordinateur portable sans impact notable sur les performances. Mais ce n'est plus le cas. En raison de la popularité croissante des cryptomonnaies et de la concurrence entre les cryptomineurs, le coût du cryptomining de ces devises ne peut pas être supporté par un utilisateur moyen. Le cryptomining est donc désormais l'apanage de ceux qui ont les moyens d'investir dans une puissance de traitement massive à laquelle la plupart des cryptomineurs potentiels n'ont pas accès.

Cette évolution ne dissuade pas pour autant les acteurs de plus petite envergure. Les cryptomineurs sans scrupules ont dû innover et se tourner vers le cryptojacking.

Le cryptojacking

Le cryptojacking consiste à installer un logiciel de cryptomining sur l'ordinateur ou le terminal mobile d'une victime au profit du hacker. Pour ce faire, ce dernier peut utiliser de nombreux canaux : pièces jointes d'e-mails, plug-ins de navigateurs compromis, sites web infectés ou tout autre moyen à sa disposition pour contourner les systèmes de défense. Les cryptomineurs illicites exploitent des milliers d'appareils dans le monde entier qui se chargent du cryptomining pour leur compte. Ils n'ont pas besoin d'investir dans des data centers ou des superordinateurs parce que leurs victimes peu méfiantes font le travail à leur place.

Qui en bénéficie ?

Les bénéficiaires du cryptomining illicite sont très divers : il peut s'agir de collaborateurs curieux qui vont utiliser leurs terminaux professionnels pour exécuter des logiciels de cryptomining, d'organisations criminelles qui veulent gagner rapidement de l'argent, voire même d'États-nations qui contournent des restrictions financières. Quelles que soient les motivations du hacker, le cryptomining indésirable rend les victimes vulnérables.

Malware, logiciel légitime ou un peu des deux ?

Lorsqu'une entreprise part à la chasse au cryptomining non autorisé, elle doit déterminer si un logiciel de cryptomining est utilisé à des fins légitimes ou illégitimes. Les logiciels de cryptomining ne rentrent pas précisément dans la catégorie des malwares. Au contraire, ils sont considérés comme des applications potentiellement indésirables (PUA pour Potential Unwanted Application). Nous conseillons donc aux entreprises et aux organismes publics qui ne procèdent pas intentionnellement au cryptomining des cryptomonnaies de bloquer ce type de trafic.

Qui paie ?

Les victimes, bien évidemment. Le cryptomining illicite entraîne une augmentation de la consommation électrique et une dégradation des performances des systèmes compromis. Le cryptomining s'apparente davantage à un désagrément si on le compare aux attaques destructrices de malwares, mais il est important de prendre en compte son impact potentiel. Les appareils de contrôle industriels submergés peuvent tomber en panne et nuire à la prestation de services ; les entreprises de services financiers peuvent rencontrer des problèmes de conformité aux réglementations, par exemple.

Il faut voir le cryptomining illicite comme un parasite qui retire des bénéfices tant que l'intégrité de son hôte est préservée et que celui-ci ne le détecte pas. Les cryptomineurs tirent profit de la bonne santé des réseaux de leurs victimes et cherchent à exploiter autant d'appareils que possible aussi longtemps que possible. Il n'est pas dans leur intérêt d'endommager le réseau ou les terminaux qui y sont exécutés. Les victimes ne subiront pas de symptômes évidents, comme une panne du système ou une perte de données comme dans le cas d'une attaque par ransomware. Elles feront plutôt face à une hausse de leurs coûts énergétiques ou à une dégradation des performances, si les cryptomineurs s'infiltrent dans leurs appareils.

Aucune attaque de malware n'a été lancée depuis un logiciel de cryptomining au moment de la rédaction de ce livre blanc. Mais il est concevable qu'un logiciel de cryptomining puisse subir une attaque de la chaîne logistique initiée par un hacker malveillant tiers. Par conséquent, il est recommandé de supprimer totalement les applications de cryptomining non autorisées.

Comment Cisco protège vos ressources

DNS et web

Composant incontournable d'Internet, le système de noms de domaine (DNS) mappe les noms de domaine à des adresses IP. Lorsque vous cliquez sur un lien ou que vous saisissez une URL, une requête DNS se charge de vous connecter à la destination.

Nous sommes un des plus grands fournisseurs de services DNS récursifs et nous résolvons 125 milliards de requêtes chaque jour provenant de 90 millions d'utilisateurs dans le monde entier. Nous analysons ces gigantesques volumes de données télémétriques très diverses afin de détecter un grand nombre de types de menaces et d'anomalies. Nos clients peuvent bloquer le trafic sortant en fonction des classifications de cryptomining des domaines, des adresses IP, des URL et des fichiers. En bloquant l'accès à l'infrastructure de cryptomining au niveau de la couche DNS, il n'est pas nécessaire de savoir si le logiciel de cryptomining est exécuté depuis un navigateur, une application hors ligne ou un utilitaire système compromis. Il est de toute façon bloqué. Il en va de même pour les terminaux mobiles sur le terrain et les appareils connectés à l'IoT sur un réseau.

La puissance de notre gamme

Les cybercriminels motivés mettront à profit tous les moyens à leur disposition. Vos systèmes de défense doivent disposer d'une visibilité étendue sur les menaces et pas simplement multiplier des informations sur des produits isolés. Imaginez le scénario suivant : le hacker commence par un e-mail de phishing, bascule vers un exploit web pour finir par une attaque centrée sur un site web fréquenté habituellement par un utilisateur (dit Watering hole attack). Il peut aussi implémenter ces trois opérations simultanément.

Nous détectons une menace une seule fois et nous assurons une protection globale. Il ne suffit pas de bloquer l'attaque. Tout ce que nous apprenons sur une menace (les fichiers, les URL, les techniques, les modèles de trafic, etc.) se propage au sein de nos solutions pour vous offrir un système de défense renforcé.

En outre, la visibilité en temps réel vous permet d'identifier les appareils et les utilisateurs qui exécutent un logiciel de cryptomining dans votre environnement. Cette capacité, en particulier l'identification des instances inconnues de cryptomining sur votre réseau, vous aide grandement à résoudre les problèmes.

Le point positif pour les acteurs de la protection, c'est que les hackers ont tendance à mettre en place des actions prévisibles lorsqu'ils lancent une campagne de phishing pour le cryptomining. Ils commencent généralement par créer et tester leur infrastructure de contrôle-commande. Chez Cisco, nous détectons cette activité. Ces domaines sont classés dans la catégorie des « nouveaux domaines » pendant que nous déterminons leur état sur le long cours. Nos clients peuvent choisir de bloquer le trafic vers ces domaines avant d'en savoir plus, protégeant ainsi leur réseau avant le lancement de la campagne.

Les terminaux

Toutes les attaques de cryptomining finissent par atteindre les terminaux où se situent les ressources les plus précieuses : les ressources de traitement informatique. Nos solutions de sécurité des terminaux surveillent et analysent en permanence l'activité des fichiers et des lignes de commande au niveau des terminaux. Nous mettons en corrélation des événements sans lien apparent et nous envoyons des alertes en cas de cryptomining. Nous déclenchons, par exemple, des alertes en présence d'un comportement signalant une propagation, comme lorsqu'un hacker tente de se déplacer sur le réseau, met en place une persistance et établit des connexions sortantes vers l'infrastructure du cryptomineur.

Les informations de veille collective basées dans le cloud sont diffusées dans toute votre architecture de sécurité pour contenir la prolifération du cryptomining. Nous propageons rapidement le système de protection contre les fichiers malveillants dès que nous détectons une activité de cryptomining.

Détecter le cryptomining dans le trafic chiffré

Il existe un moyen très efficace de protéger vos données et vos communications contre les concurrents, les criminels ou les utilisateurs indiscrets : le chiffrement. Mais les bénéfices sont à double tranchant. Les hackers peuvent tirer parti des mêmes concepts pour extraire des données sans se faire repérer. Les cryptomineurs utilisent le chiffrement pour masquer le trafic émanant de terminaux infectés en direction de leurs serveurs.

Jusqu'à récemment, le trafic chiffré devait être déchiffré pour pouvoir détecter des communications malveillantes. Vous deviez posséder une ou plusieurs clés de chiffrement privées des entités engagées dans la communication, ce qui n'est pas aussi facile qu'il y paraît. Or, ce n'est plus nécessaire. Nous avons développé des modèles de données étendus pour détecter les comportements signalant la présence de malwares, notamment pour le cryptomining, dans le trafic chiffré sans avoir à le déchiffrer au préalable.

Même s'il est reconnu que les hackers peuvent contrer les acteurs de la protection en une seule fois, notre approche suit la logique inverse. Il suffit que les hackers fassent une seule erreur pour que nous les détections et neutralisions leurs opérations actuelles et futures. Quand nous découvrons une nouvelle menace, nous ne nous contentons pas de mettre à jour nos fonctionnalités de détection. Nous étudions de manière approfondie les caractéristiques de la menace, ses méthodes de communication, son infrastructure de contrôle-commande et ainsi de suite. Nous nous renseignons au maximum sur la menace et nous transmettons ces données à nos clients.

Des services de prospection proactive sur les menaces

Si vous ne savez pas par où commencer ou si vous suspectez des activités de cryptomining sur votre réseau, il est préférable de faire appel à des professionnels. Notre équipe de spécialistes de la gestion des incidents vous propose des services de prospection proactive sur les menaces. Ils tirent parti de la Threat Intelligence de Talos, des bonnes pratiques et d'un large éventail d'outils pour identifier les activités indésirables de cryptomining dans votre entreprise.

Nous travaillerons à vos côtés pour concevoir un plan de prospection personnalisé qui définit l'étendue de notre engagement pour :

- Identifier le niveau de couverture et les problèmes de visibilité
- Déployer la technologie Cisco propriétaire nécessaire pour bénéficier d'une visibilité totale
- Évaluer l'environnement à l'aide de nos informations les plus récentes
- Analyser les résultats
- Fournir un rapport final sur les conclusions et les recommandations prioritaires

Nous pouvons également prendre en main la réponse à déployer au vu des résultats ou vous épauler tout au long de l'évaluation du cryptomining.

Les e-mails

Les e-mails restent toujours un moyen de communication populaire et efficace, et à ce titre, ils représentent un outil fiable pour les cybercriminels. Leur objectif : tromper les destinataires des e-mails en les invitant à visiter un site web malveillant, à ouvrir une pièce jointe malveillante ou à divulguer des informations.

Nous bloquons les attaques basées sur les e-mails en détectant les pièces jointes malveillantes et en supprimant les liens malveillants des messages avant qu'ils atteignent l'utilisateur. Notre moteur d'analyse détecte les techniques de contournement avancées, ce qui complique énormément la tâche aux hackers qui essaient de s'infiltrer dans votre réseau. De plus, notre analyse des menaces est basée dans le cloud, ce qui permet de transformer immédiatement la découverte d'une nouvelle menace en protection pour tous nos clients. Il nous suffit de détecter une menace une seule fois, dans notre laboratoire ou dans le monde réel, pour protéger nos clients dans le monde entier.

Le réseau

« Le réseau » est un terme large, qui regroupe les applications, les protocoles, les technologies, les utilisateurs, les robots, etc. Les hackers peuvent atteindre leurs objectifs par bien des manières. Par conséquent, il est impératif d'utiliser diverses techniques et d'analyser les comportements sur le réseau sous de nombreux angles.

Notre gamme de solutions de sécurité propose l'inspection avancée des paquets, le sandboxing, l'analyse des fichiers, la détection des anomalies et l'analyse NetFlow. Nous analysons le trafic en temps réel et en permanence pour détecter des menaces inconnues, que nous pouvons ensuite éliminer rétroactivement. Encore une fois, nous mettons constamment à jour nos informations sur la sécurité, nos clients sont donc automatiquement informés si nous détectons des menaces et si nous développons de nouvelles protections à leur encontre.

Le bénéfice de la Threat Intelligence

C'est un fait : les méthodes des hackers ne cessent d'évoluer, tout comme celles des acteurs de la protection en réponse aux nouvelles menaces. Mais les acteurs de la protection peuvent-ils évoluer rapidement et efficacement ? Cette question ne dépend pas des capacités des acteurs de la protection, mais plutôt des ressources à leur disposition, principalement en matière de temps et de compétences. Premièrement, les professionnels de la sécurité ne sont tout simplement pas assez nombreux pour répondre à la demande. Nous prévoyons une pénurie d'environ 2 millions de professionnels de la sécurité dans le monde entier en quelques années seulement.

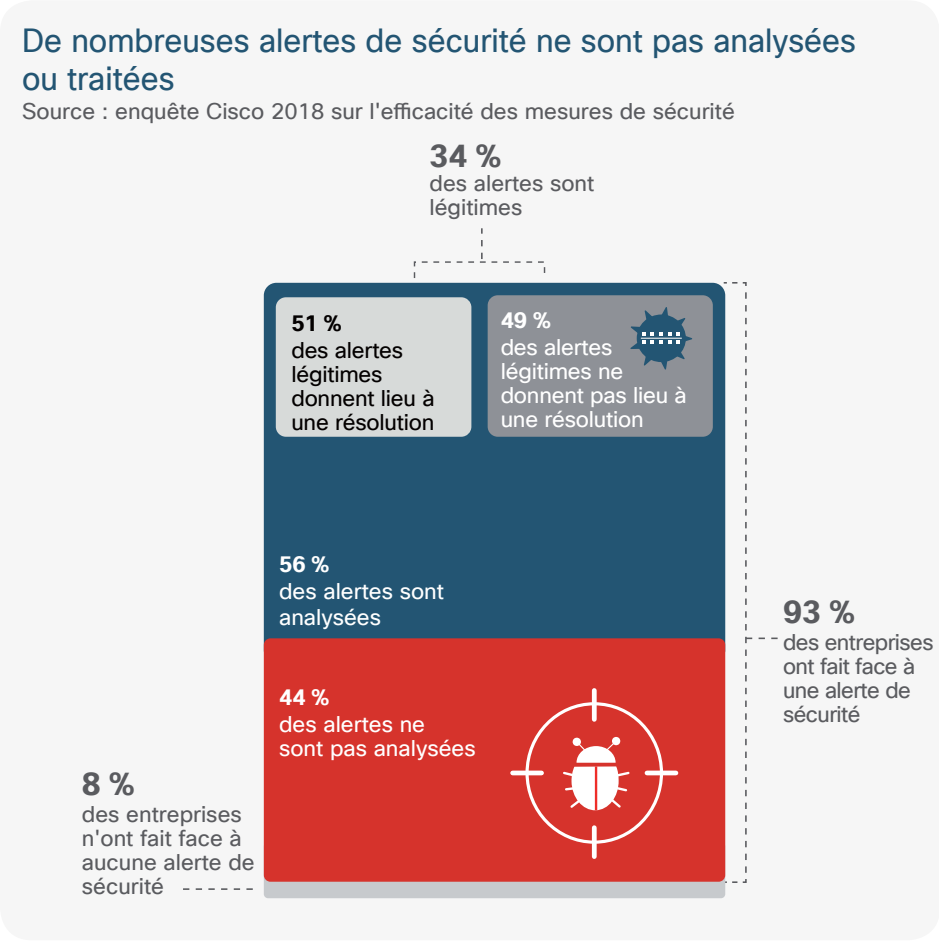
Deuxièmement, les acteurs de la protection doivent faire face à un déluge d'informations, provenant en particulier de très nombreux produits isolés. Ainsi, 44 % des alertes de sécurité en moyenne ne sont pas analysées (voir Figure 1). Cela signifie également que les acteurs de la protection manquent de temps pour se consacrer à des tâches à plus grande valeur ajoutée pour leur entreprise.

La solution ?

Inscrivez-vous pour essayer gratuitement la solution de sécurité DNS Cisco Umbrella à l'adresse https://signup.umbrella.com/.

Vous pouvez aussi nous appeler ou nous envoyer un e-mail pour en discuter plus en détail, découvrir nos fonctionnalités et savoir comment nous pouvons vous aider. Protéger votre entreprise contre les menaces, telles que le cryptomining, fait partie intégrante de la gestion de votre entreprise et nous serions heureux de vous aider. Rendez-vous sur notre site : https://engage2demand.cisco.com/LP=591.

Figure 1. Alertes de sécurité ignorées et non corrigées



Nous analysons et mettons en corrélation les données télémétriques des domaines DNS et des URL, des réseaux et des informations sur les flux, des fichiers, des e-mails, et des applications cloud à l'aide d'une analyse humaine automatisée et de l'apprentissage automatique, de l'ingénierie inverse et de la recherche sur les vulnérabilités. Nous intégrons des chercheurs dans nos équipes de gestion des incidents, ce qui nous permet d'analyser et d'étudier certains incidents de grande envergure dans le monde entier. Les résultats de ces recherches se tiennent à votre disposition dans notre gamme de solutions. Nous les mettons à jour et nous les actualisons continuellement.

Les mises à jour automatiques et les réponses aux menaces en fonction de la Threat Intelligence la plus récente signifient que vous êtes protégé contre des menaces que vous ne connaissiez même pas encore. Pour faire simple : nous détectons un plus grand nombre de menaces pour mieux vous protéger.

C11-740602-00 04/18