PRISMA CLOUD | UNIT 42 BY PALO ALTO NETWORKS

RAPPORT SUR LES MENACES DANS LE CLOUD S1 2021

COVID-19 : conséquences et opportunités pour la sécurité du cloud

Sommaire

Avant-propos 3

Note de synthèse 4

01

Constatations factuelles 5

- Principaux incidents de sécurité cloud liés à la COVID-19 5
- Impact par région 6
- Impact par secteur d'activité 8
- COVID-19 et données de sécurité 10

02

Cloud, COVID-19 et cryptomonnaies 11

- Tendances du minage et évènements du marché 11
- Impact de la pandémie sur le cryptominage 12
- Ralentissement du cryptojacking 13

03

Conclusion et recommandations 14

- Sécurité du cloud : les points de concentration stratégiques 14
- Prêt à identifier les menaces qui pèsent sur votre cloud ? 15

Méthodologie 15

À propos 15

- Prisma Cloud 15
- Unit 42 15
- Auteurs 15

Avant-propos

La crise sanitaire a entraîné une explosion des services cloud dès les premières mesures de confinement des populations. En quelques mois, la part de salariés en télétravail est passée de seulement 20 % à 71 %[1]. Dans le même temps, face à l'urgence de la situation, les entreprises ont dû revoir leurs dépenses cloud à la hausse entre juillet et septembre 2020, avec une progression de 28 % par rapport à l'année précédente[2]. Cette chronologie des évènements est importante, quand on sait que l'Organisation mondiale de la santé (OMS) a déclaré l'état de pandémie planétaire en mars 2020. En clair, la généralisation du travail en distanciel a accéléré le mouvement migratoire des ressources vers le cloud, avec notamment un pic massif au troisième trimestre 2020 par rapport à la même période de l'année précédente.

En décortiquant les données issues de nos capteurs placés aux quatre coins du globe, notre équipe de chercheurs a pu établir une **corrélation entre les incidents de sécurité et la hausse des dépenses cloud imputable à la pandémie**[3]. Concrètement, le nombre de workloads cloud a augmenté de plus de 20 % (entre décembre 2019 et juin 2020) à l'échelle mondiale, engendrant par la même occasion une explosion des incidents de sécurité. Les résultats de notre enquête montrent également que les programmes de sécurité cloud des entreprises n'en sont qu'à leurs balbutiements, notamment en ce qui concerne l'automatisation des contrôles de sécurité selon des approches DevSecOps et « shift left ». Notre constat est le suivant : **à défaut d'une automatisation et d'une intégration complète des contrôles de sécurité au pipeline de développement, la complexité et la croissance rapide des environnements cloud forment un cocktail explosif pour la cybersécurité**. À titre d'exemple, nous montrons dans une précédente étude que 65 % des incidents cloud rendus publics sont le fruit d'erreurs de configuration côté client. On peut donc en déduire qu'en faisant l'impasse sur l'automatisation de la sécurité, les entreprises qui exploitent des environnements cloud d'envergure exposent leurs ressources à des risques inutiles.

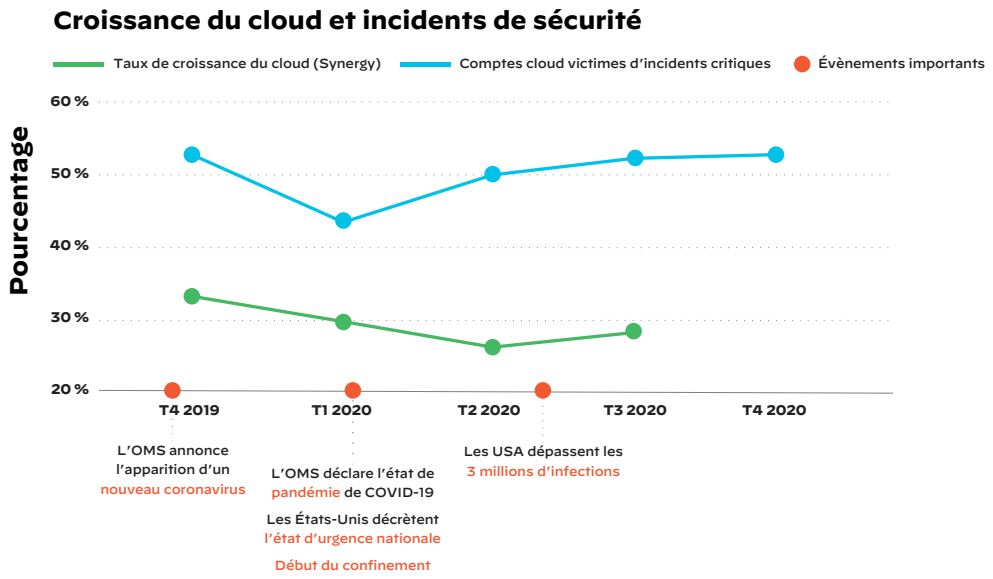

Figure 1 : Croissance du cloud et incidents de sécurité

Dans ce rapport, nous dressons un constat de l'impact des dernières menaces cloud sur votre entreprise. Vous y découvrirez en outre comment l'adoption d'une plateforme et de standards de cybersécurité communs constituent un passage obligé vers le développement d'un programme de sécurité plus mature.

Matthew Chiodi
CSO, cloud public, Palo Alto Networks

1. « How the Coronavirus Outbreak Has – and Hasn't – Changed the Way Americans Work », Pew Research Center, 9 décembre 2020, https://www.pewresearch.org/social-trends/2020/12/09/how-the-coronavirus-outbreak-has-and-hasnt-changed-the-way-americans-work.
2. « COVID-19 Boosts Cloud Service Spending by $1.5 Billion in the Third Quarter », Synergy Research Group, 5 décembre 2020, https://www.srgresearch.com/articles/covid-19-boosts-cloud-service-spending-15-billion-third-quarter.
3. Dans le présent rapport, les incidents de sécurité sont entendus comme des évènements ayant conduit à une violation des politiques de sécurité ainsi qu'à la compromission de données sensibles.

Note de synthèse

Afin de mieux cerner l'impact mondial de la COVID-19 sur la cybersécurité, Unit 42, notre équipe de Threat Intelligence interne, a épluché les données de centaines de comptes cloud dans le monde entre octobre 2019 et février 2021 – soit avant et après l'apparition de la pandémie. Il en ressort que **les incidents de sécurité cloud ont bondi de 188 % entre avril et juin 2020. En effet, malgré la migration rapide des workloads vers le cloud, les entreprises peinent encore à automatiser leur cybersécurité afin de répondre efficacement aux menaces propres à cet environnement.** Enfin, bien que l'IaC (Infrastructure as Code) offre la possibilité d'appliquer les politiques de sécurité de façon systématique, force est de constater que cette fonctionnalité reste largement inexploitée par les équipes DevOps et SecOps.

Dans ce rapport, nous prenons la mesure des effets de la crise sanitaire sur les menaces de sécurité associées au cloud. Nous présentons également les principaux types de risques rencontrés par région et secteur d'activité. Pour finir, nous proposons des mesures concrètes à engager pour réduire la surface de risque du cloud.

Les secteurs d'importance vitale observent une hausse majeure des incidents de sécurité

Dès le début de la pandémie, les entreprises se sont engagées dans une migration tambour battant de leurs ressources vers le cloud. Mais en parallèle, cette évolution a donné lieu à une recrudescence des incidents de sécurité. Notons que **les secteurs les plus touchés sont la grande distribution (402 %), l'industrie (230 %) et les pouvoirs publics (205 %).** Rien de vraiment surprenant quand on sait que ces entreprises ont été en première ligne pour répondre à la crise – qu'il s'agisse des produits de première nécessité pour les acteurs de la distribution ou bien du matériel et des fournitures médicales dans les secteurs de l'industrie et des pouvoirs publics.

La difficulté qu'éprouvent ces secteurs d'importance vitale à sécuriser leur environnement cloud met en évidence les dangers d'un sous-investissement dans la cybersécurité. Ces pics d'incidents montrent bien que si les entreprises ont su monter rapidement en capacités dans le cloud – notamment pour répondre aux besoins du télétravail – elles accusent un net retard sur le terrain de l'automatisation de la sécurité du DevOps et des pipelines d'intégration et de déploiement continus (CI/CD).

Les attaques de cryptojacking sont en recul

Au plus fort de la crise sanitaire, les cryptomonnaies comme le Bitcoin (BTC), l'Ethereum (ETH) et le Monero (XMR) ont connu un engouement qui a vu leur valeur repartir nettement à la hausse. Pourtant, on observe un ralentissement des opérations de cryptojacking : de décembre 2020 à février 2021, seules 17 % des entreprises dotées d'une infrastructure cloud ont montré des signes symptomatiques de ce type d'activité, contre 23 % de juillet à septembre 2020. **C'est le premier recul que nous enregistrons depuis 2018, année de notre premier baromètre des tendances du cryptominage.** Les entreprises semblent donc avoir pris les devants pour mieux protéger l'environnement d'exécution des workloads et ainsi réduire le champ d'action des cryptomineurs malveillants.

Les données sensibles continuent d'être exposées publiquement

Propriété intellectuelle, informations d'identification personnelle ou encore données médicales et financières : 30 % des entreprises exposent du contenu sensible à Internet. Pour accéder à ces données, il suffit donc de connaître ou de deviner les URL en question. Cette négligence engendre un risque significatif pouvant conduire à des accès non autorisés et à de graves entorses réglementaires. Un tel degré d'exposition laisse à penser que les entreprises éprouvent encore des difficultés à appliquer les contrôles d'accès adaptés aux centaines de compartiments de stockage qu'elles opèrent dans le cloud, surtout lorsque ces derniers sont répartis entre plusieurs comptes et fournisseurs.

01

Constatations factuelles

Principaux incidents de sécurité cloud liés à la COVID-19

L'étude d'Unit 42 révèle une augmentation significative des risques de cybersécurité à l'heure de la pandémie : données non chiffrées, exposition publique des ressources ou ports non sécurisés… les dangers dans le cloud sont multiples et variés. La figure 2 ci-dessous fait état d'une quinzaine de catégories d'incidents dont la fréquence a sensiblement augmenté.

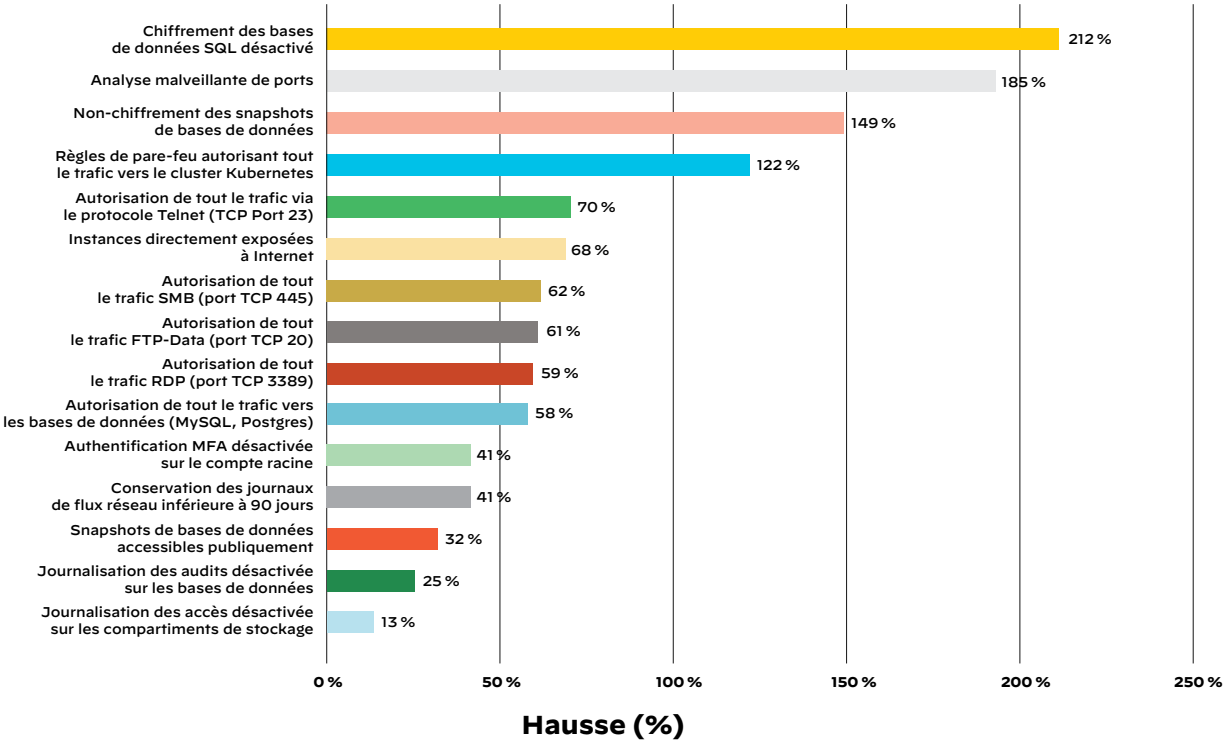

Figure 2 : Incidents de sécurité enregistrant la plus forte hausse durant la pandémie

Pris dans leur ensemble, **ces évènements soulignent une défaillance de bon nombre d'entreprises, chez qui la gouvernance et l'automatisation de la sécurité ne suivent pas la cadence imposée par la migration rapide des workloads dans le cloud**. Pourtant, l'implémentation de modèles IaC (Infrastructure as Code) permettrait d'éviter en grande partie les erreurs de configuration décrites ci-dessus. Comme nous l'évoquions dans de précédents rapports, dès lors qu'ils font l'objet d'analyses d'identification des failles les plus courantes, ces modèles contribuent à sécuriser l'infrastructure cloud – du développement jusqu'à la production.

Parmi les incidents de sécurité en nette progression, prenons l'exemple du non-chiffrement des bases de données relationnelles et SQL (comme Microsoft Azure® SQL Database) : il s'agit d'une négligence qui pourrait être facilement identifiée et corrigée en automatisant les contrôles de sécurité des environnements cloud. Dans la même veine, bien que le scan de ports ne soit pas une technique nouvelle, son regain d'activité depuis l'apparition de la pandémie nous indique que les cybercriminels continuent de rechercher activement la moindre faille créée par une gouvernance lacunaire du cloud.

Les problèmes de gouvernance et d'automatisation ne sont pas nouveaux. Alors que le nombre d'alertes de sécurité cloud a augmenté au cours de la dernière année, nos données montrent que les types d'incidents les plus fréquents restent sensiblement similaires par rapport à nos précédentes observations.

Malgré la migration massive des workloads vers le cloud, on peut donc en conclure que les entreprises continuent de faire les mêmes erreurs stratégiques en matière de sécurité. Le déploiement efficace de modèles IaC est une bonne solution pour éliminer ce type de négligences, mais ces derniers restent largement sous-exploités. La plupart de ces modèles sont créés en trois temps : conception, codage et déploiement. La grande absente de cette approche, c'est l'automatisation de la sécurité. À l'instar du code applicatif, les modèles IaC devraient en effet faire systématiquement l'objet d'une analyse de sécurité lors de leur création et de leurs mises à jour successives.

Notre étude indique pourtant qu'au plus fort de la pandémie, les modèles IaC étaient soit inutilisés, soit déployés sans aucune analyse préalable des failles de sécurité les plus courantes. Ces lacunes laissent donc le champ libre à certaines erreurs comme le non-chiffrement des données sensibles ou l'absence de journalisation, cette dernière jouant pourtant un rôle indispensable pour la surveillance et le contrôle de la sécurité dans le cloud.

Impact par région

La pandémie a produit un effet de levier certain sur la croissance du cloud à l'échelle mondiale. Mais comme le montre la figure 3 ci-dessous, certaines régions enregistrent une progression plus forte que d'autres.

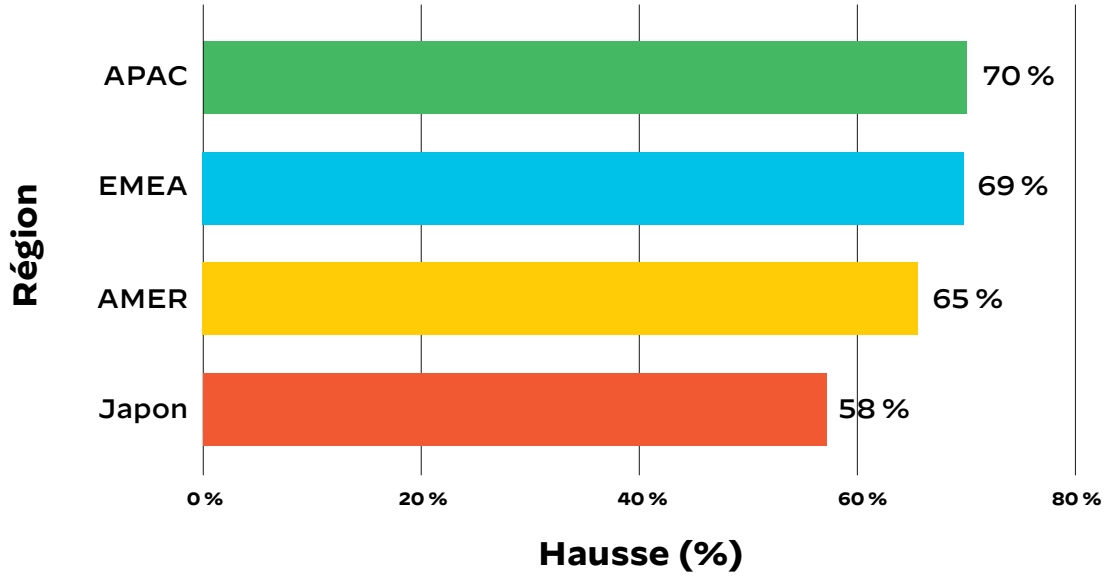

Figure 3 : Augmentation des workloads cloud par région

Le Japon observe globalement un taux d'adoption cloud plus lent depuis le début de la crise. En conséquence, les entreprises nippones présentent moins de configurations non sécurisées : seules 32 % autorisent tout le trafic TCP/UDP vers au moins une machine virtuelle (VM) hébergée dans le cloud, tandis que 39 % exposent le port 22 (SSH) d'un de leurs services SSH hébergé dans le cloud.

En comparaison, 60 % des entreprises dans le monde autorisent l'ensemble du trafic réseau vers leurs plateformes cloud, et 58 % exposent le port 22 à Internet.

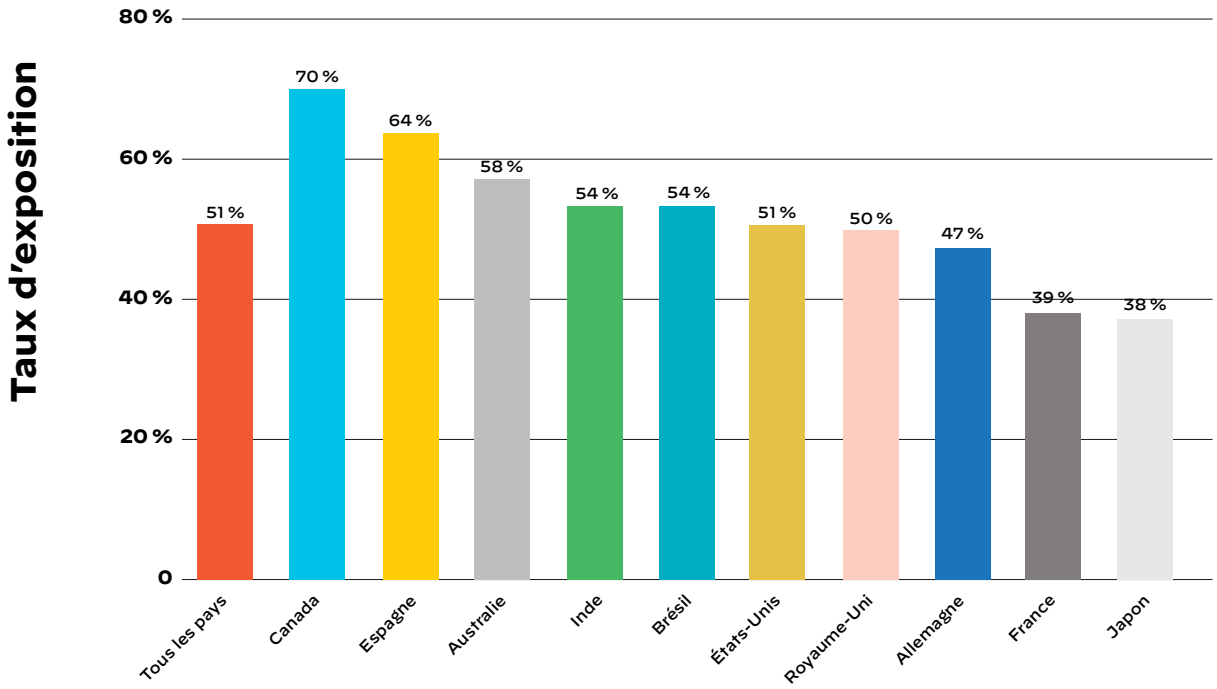

Figure 4 : Pourcentage d'entreprises exposant leur port RDP par pays

L'exposition du protocole Windows RDP (port 3389) varie elle aussi de façon significative entre les régions (voir figure 4). Il s'agit pourtant de l'un des principaux vecteurs d'attaque, puisque l'ouverture des ports RDP permet aux cybercriminels de s'introduire sur les réseaux d'entreprise afin d'en perturber les opérations ou de dérober des données sensibles. Le Canada, dont 70 % des entreprises exposent leur port RDP, est le territoire qui éprouve le plus de difficultés à cet égard.

En comparant la croissance des workloads par région à l'exposition des services RDP par pays, les chercheurs d'Unit 42 ont établi un lien direct avec la hausse des incidents de sécurité autour de la pandémie. Sur l'ensemble des principaux fournisseurs cloud, l'exposition moyenne du port RDP augmente de 27 %.

La non-protection de ces ports critiques constitue là encore une erreur majeure susceptible d'entraîner de lourdes conséquences. Toutefois, cet écueil peut lui aussi être évité en associant une infrastructure IaC sécurisée à l'application continue des politiques par le biais d'une plateforme de sécurité commune.

Impact par secteur d'activité

Le volume de workloads cloud a augmenté dans la quasi-totalité des secteurs, à l'exception de l'énergie : cela peut s'expliquer par la faible demande et donc la production réduite de pétrole et de gaz pendant la pandémie. Notons aussi que l'industrie chimique, les pouvoirs publics, la pharmaceutique et les sciences de la vie ont observé la plus forte progression – une tendance due vraisemblablement à leur rôle de première ligne sur le front de la pandémie.

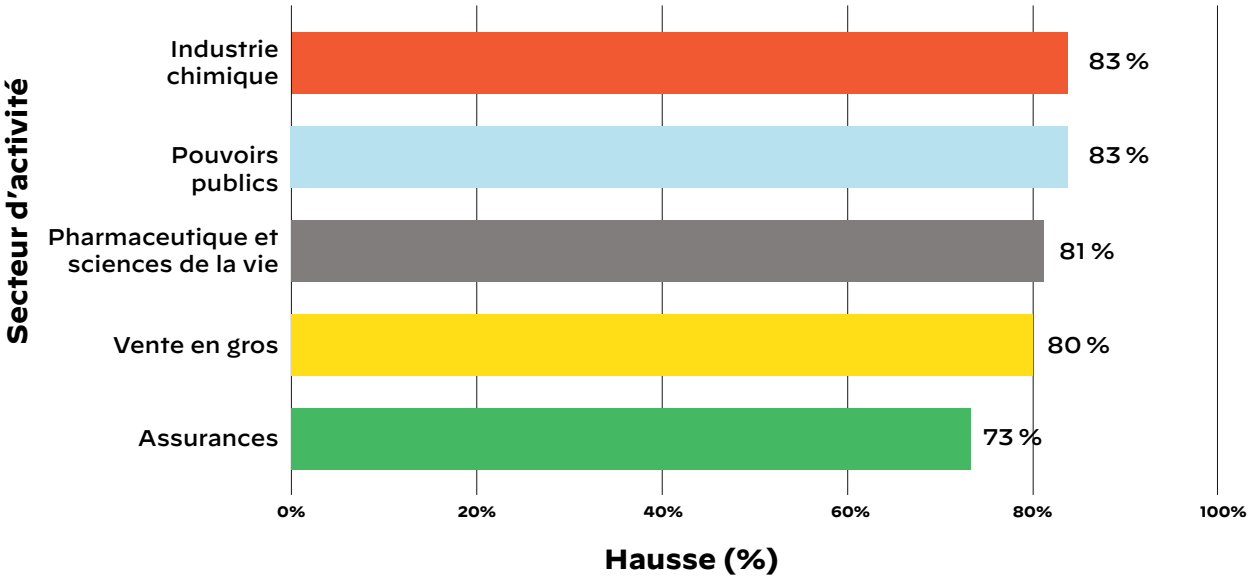

Figure 5 : Pourcentage d'entreprises ayant augmenté leurs workloads cloud, par secteur

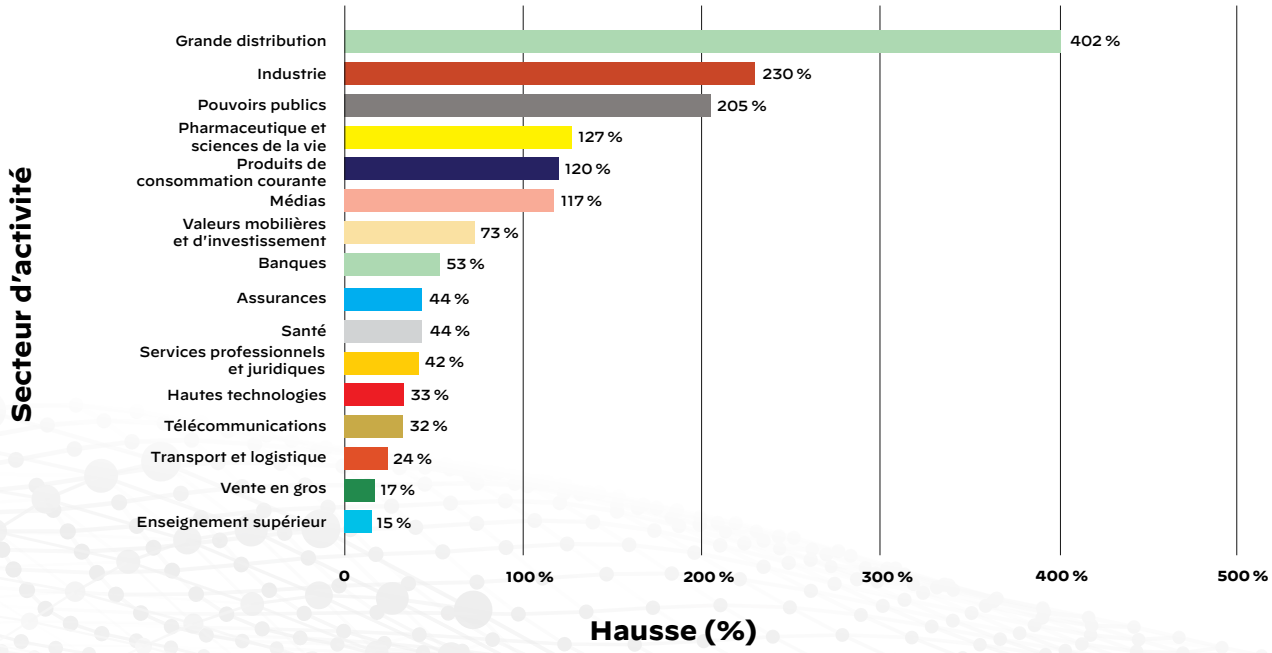

Figure 6 : Pourcentage d'augmentation des incidents de sécurité par secteur

Remarque : certains secteurs dont les données sont insuffisantes ne sont pas inclus dans ces chiffres.

Notre étude montre que la hausse des incidents de sécurité est proportionnelle à l'augmentation des workloads dans le cloud, à tel point que les équipes DevOps et SecOps se retrouvent souvent dépassées par la situation. Parmi les secteurs d'activité les plus touchés, on retrouve la grande distribution (402 %), l'industrie (230 %) et les pouvoirs publics (205 %). Cette tendance n'a rien de vraiment surprenant quand on sait que ces entreprises ont été parmi les plus sollicitées pour répondre à la crise sanitaire – qu'il s'agisse des produits de première nécessité pour les acteurs de la distribution ou bien du matériel et des fournitures médicales dans les secteurs de l'industrie et des pouvoirs publics. Ces incidents ont élargi la surface d'attaque des environnements cloud, ce qui complique la conduite d'audits de sécurité et d'analyses forensiques.

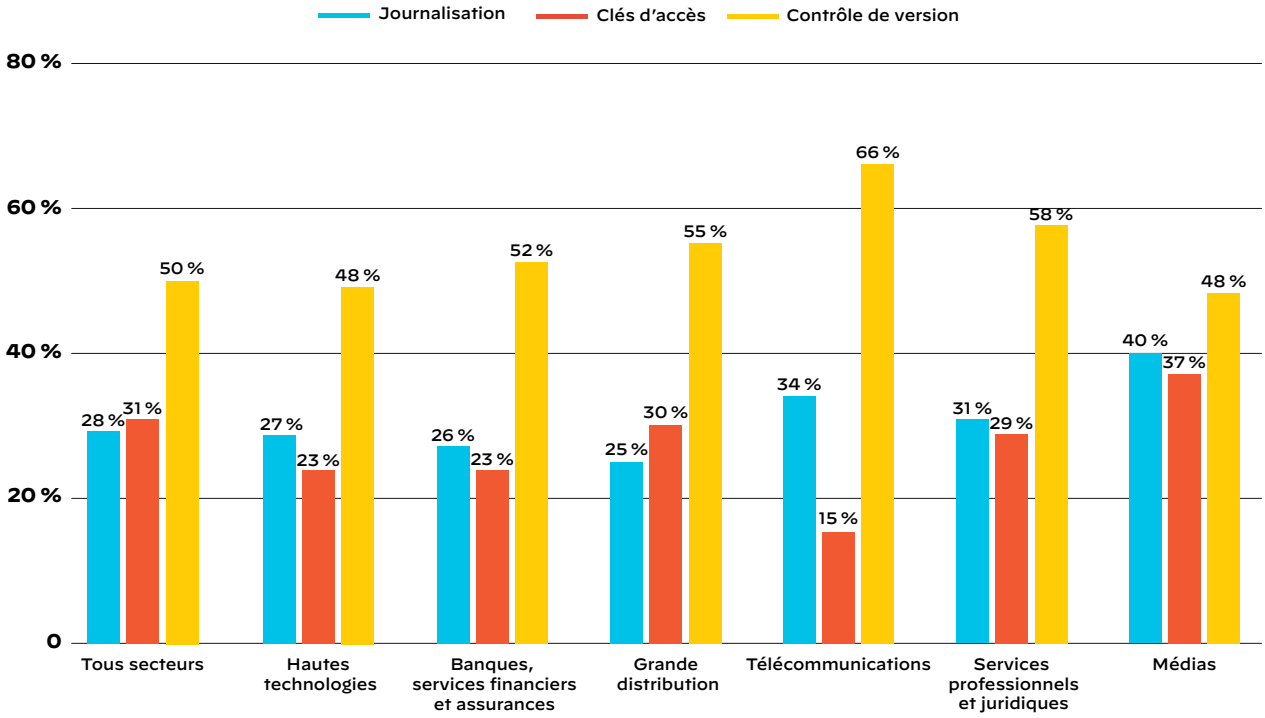

Figure 7 : Pourcentage d'entreprises appliquant des contrôles de sécurité critiques, par secteur

Néanmoins, soulignons que certains secteurs s'en sortent mieux que d'autres en matière de cybersécurité (voir figure 7). Dans les médias, par exemple, 40 % des entreprises activent la journalisation des accès sur l'ensemble de leurs containers de stockage dans le cloud, contre seulement 25 % des acteurs de la grande distribution. Bien que les raisons de cet écart ne soient pas clairement établies, les chercheurs d'Unit 42 pensent qu'il pourrait venir d'une plus grande vigilance des acteurs des médias sur les questions d'accès au contenu, notamment depuis le piratage de Sony Pictures en 2014.

Les médias arrivent également en tête dans le domaine de la rotation des clés d'accès : 37 % utilisent des clés datant de moins de 90 jours, contre seulement 15 % dans le secteur des télécommunications. Nous expliquons là aussi ce phénomène par un meilleur contrôle de l'accès au contenu. Le secteur des télécommunications, qui arrive bon dernier dans cette catégorie, privilégie quant à lui les deux autres formes de contrôle, dont la journalisation : un domaine dans lequel il obtient le deuxième meilleur score.

La mise en œuvre du contrôle de version au sein des containers de stockage cloud est une mesure de sécurité essentielle, dans la mesure où elle détermine la capacité d'une entreprise à se remettre d'une compromission, voire d'une simple corruption de fichiers. Dans le secteur des télécommunications, 66 % appliquent le contrôle de version à l'ensemble des containers cloud, contre seulement 48 % dans les médias et les hautes technologies, au bas du classement. Il est intéressant de noter que les secteurs des médias et des télécommunications présentent des modèles diamétralement opposés sur deux points. Tous deux semblent accorder de l'importance à la journalisation mais, là où les médias favorisent le contrôle des accès, les télécoms privilégient quant à eux le contrôle des versions. En d'autres termes, les médias affichent tout autant de volonté à contrôler l'accès au contenu que le secteur des télécommunications à garantir la non-compromission des données.

COVID-19 et sécurité des données

Le stockage dans le cloud séduit les entreprises en raison de sa fiabilité, sa disponibilité et son évolutivité. D'après notre étude, 64 % des données dans le cloud contiennent des informations sensibles (données à caractère personnel, propriété intellectuelle ou encore données médicales et financières). Parmi celles-ci, les informations d'identification personnelle comptent pour 69 % et les données de propriété intellectuelle pour 34 % (voir figure 8).

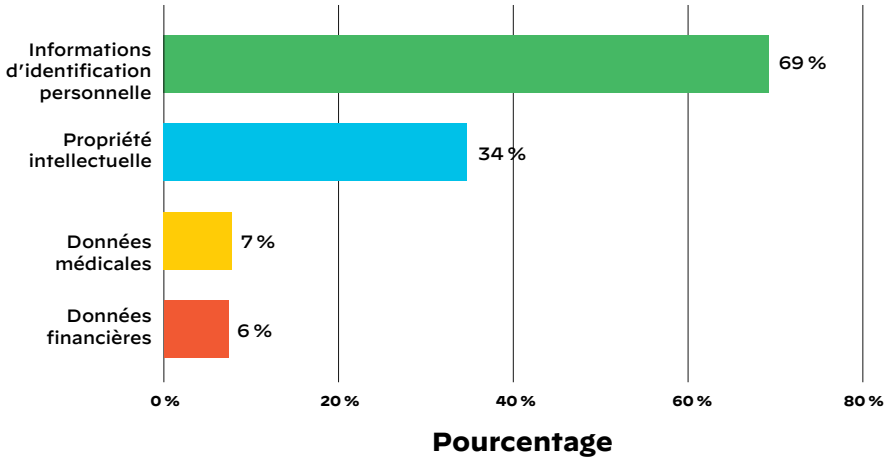

Figure 8 : Types de données sensibles dans le cloud

Malgré la hausse du volume de données stockées dans le cloud, bon nombre d'entreprises n'ont pas su adapter leurs contrôles de sécurité afin d'en garantir la protection. Ainsi, selon notre enquête, 35 % des entreprises dans le monde possèdent des ressources de stockage cloud accessibles publiquement sur Internet. Bien que cette configuration puisse être justifiée dans certains cas particuliers, ce phénomène résulte bien souvent d'un oubli non-détecté, faute de surveillance et d'audit de la sécurité.

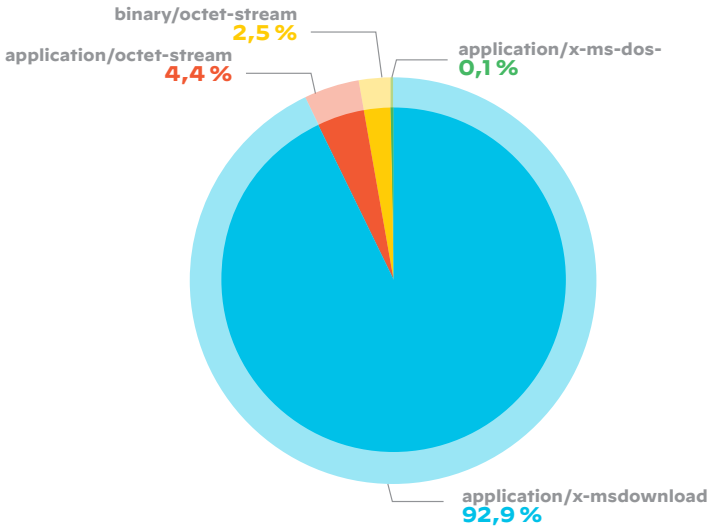

Figure 9 : Types de malwares stockés dans le cloud

Le risque encouru est pourtant majeur, puisque 30 % de ces mêmes entreprises semblent stocker des informations sensibles. **Ce chiffre est d'autant plus alarmant qu'il suffit de connaître les URL en question pour accéder aux données, sans aucun mot de passe ni autre forme d'authentification**. C'est ainsi que les cas d'exposition de données sensibles se sont multipliés ces dernières années. Par exemple, les chercheurs de vpnMentor ont découvert dans le cloud les données à caractère personnel de plus de 30 000 individus, tandis que The Register a trouvé plus de 500 000 fichiers confidentiels appartenant à des milliers de clients.

Mais le cloud n'abrite pas que des données sensibles : les équipes Unit 42 indiquent que 92,9 % des malwares contenus dans ces environnements y sont stockés sous la forme d'exécutables et de bibliothèques de liens dynamiques (fichiers .exe et .dll). Ce chiffre confirme les conclusions d'un rapport de VirusTotal, selon lequel la plupart des malwares ciblent les systèmes Windows et que les fichiers exécutables en sont le principal vecteur d'infection.

La bonne nouvelle, c'est que ces malwares représentent moins de 0,01 % des données stockées dans le cloud. Toutefois, ce faible pourcentage ne doit pas nous détourner du besoin crucial d'étudier comment un malware a pu s'infiltrer et qui a pu y accéder.

02

Cloud, COVID-19 et cryptomonnaies

Bien que la pandémie de COVID-19 ne puisse être l'unique facteur de fluctuation des cryptomarchés et des problèmes de sécurité associés, notre étude révèle des liens intéressants entre les cryptomonnaies, le cloud et l'impact de la crise sanitaire.

Les chercheurs d'Unit 42 se sont penchés sur le cas du Monero (XMR) : une cryptomonnaie très prisée des hackers du fait de sa protection de l'anonymat et de sa simplicité de minage dans le cloud. Les données récoltées couvrent la période de décembre 2020 à février 2021.

Tendances du minage et évènements du marché

Les chiffres indiquent une **hausse de 65 % des connexions aux pools de cryptominage XMR connus**, avec une activité en dents de scie tout au long de la période observée.

À trois reprises, alors que le cours du XMR était au plus haut, nous avons constaté des chutes de connexion importantes (voir figure 10). Ce phénomène semble indiquer que les cryptomineurs opèrent essentiellement lorsque la tendance est baissière, puis stoppent leur activité pour prendre leurs bénéfices lorsque les prix repartent à la hausse. On remarque une autre baisse de connexion entre le 24 décembre 2020 et le 3 janvier 2021 : dans le milieu du cryptojacking aussi, on profite des fêtes de fin d'année.

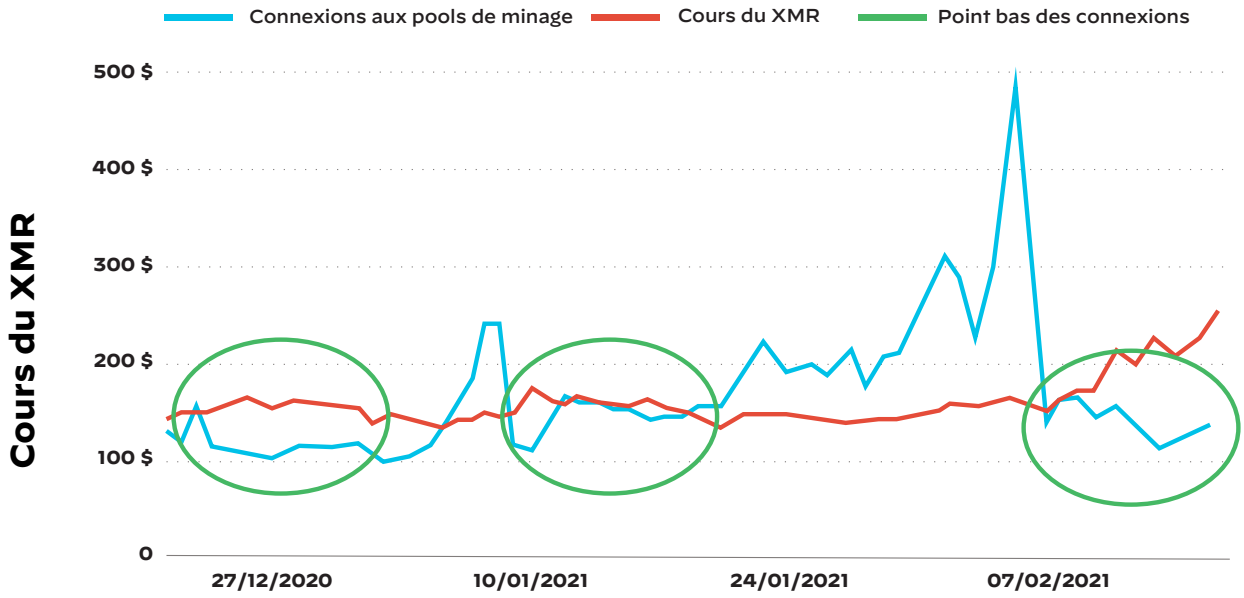

Figure 10 : Comparaison entre les connexions aux pools de minage et le cours du XMR

Impact de la pandémie sur les opérations de minage

Les chercheurs d'Unit 42 ont établi une corrélation évidente entre les activités de minage de Monero et les évènements liés à la pandémie. Afin d'en rendre compte, la figure 11 présente l'évolution de la fréquence de connexion aux pools de minage en parallèle à quelques dates repères de la crise sanitaire.

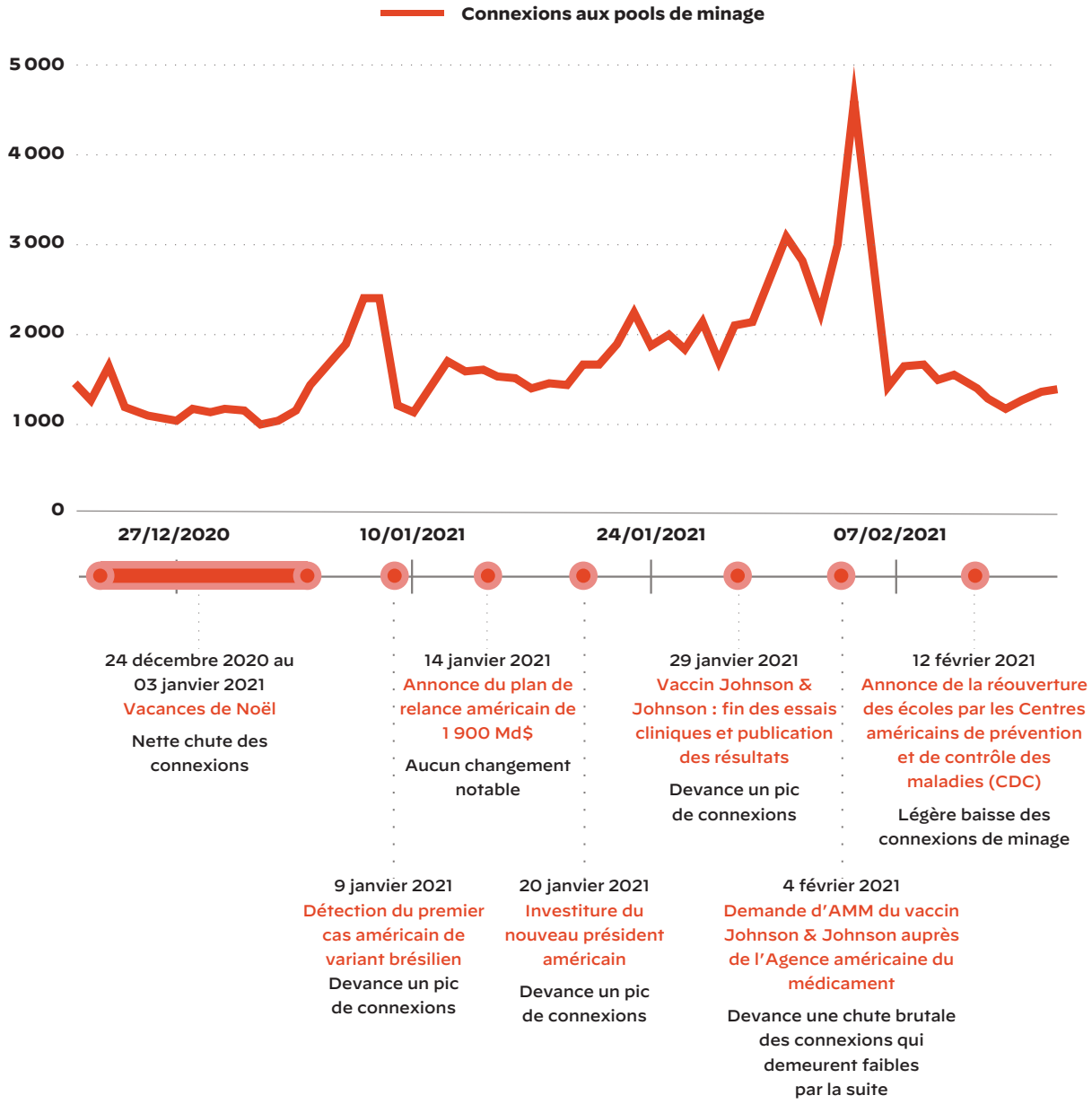

Figure 11 : Connexions aux pools de minage et dates repères

Bien que le volume de données disponible ne nous permette pas de tirer des conclusions définitives, il semble que les évènements politico-sanitaires ont un réel impact sur les opérations de cryptojacking, tout du moins en ce qui concerne le XMR.

Ralentissement du cryptojacking

Malgré l'intensification des activités de minage, le cryptojacking (qui implique le détournement illégal d'une infrastructure) accuse un léger recul à l'heure du COVID-19. D'après nos chiffres, à l'échelle mondiale, 23 % des entreprises gérant des workloads dans le cloud ont été victimes de cryptojacking entre juillet et septembre 2020, contre seulement 17 % de décembre 2020 à février 2021. **C'est le premier recul enregistré depuis la mise en place de ce baromètre en 2018**.

Bien que le XMR se taille la part du lion en ce qui concerne les opérations de minage dans le cloud, d'autres cryptomonnaies sont plus prisées en termes de parts de marché. Les chercheurs d'Unit 42 ont étudié les connexions réseau liées à l'Ethereum (ETH), au Bitcoin (BTC), au Litecoin (LTC) et au Dash. Dans chaque cas, le minage de XMR a systématiquement surclassé les autres cryptodevises, dont les activités cumulées totalisent en moyenne 1 % des connexions attribuées au Monero (voir figure 12).

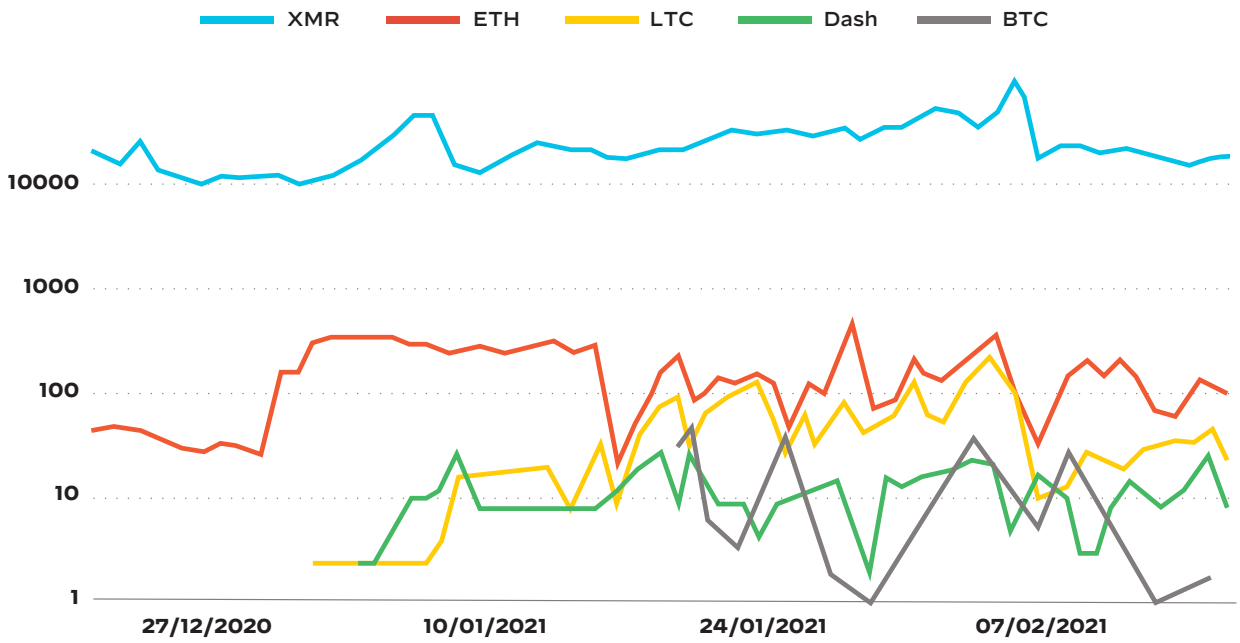

Figure 12 : Connexions aux pools de minage par cryptomonnaie

L'ETH, qui est l'une des cryptomonnaies les plus en vogue, présente le plus grand nombre de connexions à des pools de minage spécifiques, en dehors du XMR. Rien de surprenant, puisque l'ETH est l'une des cryptomonnaies les plus fonctionnelles du marché. Bien que les ressources CPU ne se prêtent pas particulièrement au minage d'ETH, tous les fournisseurs de services cloud proposent des instances de VM basées sur des processeurs graphiques (GPU), qui eux sont bien plus rentables pour miner l'ETH.

Étonnamment, le BTC, le LTC et le Dash ont tous enregistré des connexions réseau à leurs propres pools. Pourtant, le minage et la preuve de travail de ces blockchains sont des opérations bien plus gourmandes en mémoire qui, pour être rentables, requièrent une architecture basée sur les circuits intégrés ASIC. Dans ce cas précis, étant donné l'inefficacité des méthodes classiques (minage CPU/GPU), ainsi que leur mauvais rapport coût-bénéfice, toute connexion à des pools BTC, LTC ou Dash établie à partir d'une infrastructure cloud doit éveiller les soupçons.

03

Conclusion et recommandations

Le verdict de notre rapport est sans appel : **les entreprises n'ont pas suffisamment investi dans les solutions de gouvernance et d'automatisation nécessaires pour garantir la sécurité des workloads dans le cloud**. Ce sous-investissement engendre aujourd'hui de nouveaux risques, à commencer par l'exposition de données sensibles et non chiffrées à Internet, ou encore l'ouverture de ports non sécurisés à la merci des attaquants. Nos précédents rapports constataient déjà des problèmes similaires en 2020, mais les multiples effets de la pandémie de COVID-19 n'ont fait qu'aggraver la situation.

Face à cette menace, les entreprises doivent rééquilibrer leur programme de sécurité cloud sur l'ensemble des étapes du cycle de développement logiciel. Elles pourront ainsi s'imposer sur le marché tout en mettant en place une sécurité cloud évolutive et capable d'affronter les prochains chocs, quel qu'ils soient.

Mesures stratégiques

Les chercheurs d'Unit 42 conseillent aux entreprises d'accorder une attention toute particulière aux aspects suivants de la sécurité du cloud.

Élargir et approfondir votre visibilité sur le cloud

Avant toute chose, vous devez bien comprendre comment vos développeurs et vos équipes métiers utilisent le cloud aujourd'hui. Ce bilan initial est le premier pas vers une gestion simplifiée de la conformité et de la sécurité du cloud. Il vous permettra d'obtenir une lecture beaucoup plus précise et granulaire de votre environnement cloud, jusqu'au niveau des API et des workloads.

Placer des garde-fous

Commencez par répondre à la question suivante : quelles sont les configurations à bannir à tout prix ? Prenons un cas d'école : une base de données ne devrait jamais être directement accessible depuis Internet. Cela tombe sous le sens, et pourtant, nos recherches montrent que cette erreur de configuration se vérifie dans 28 % des environnements cloud. Vos garde-fous doivent être en mesure de corriger ce type de mégarde de façon automatique. Pour garantir leur application, nous vous conseillons d'utiliser des modèles IaC pour sous-tendre votre transition vers une approche shift left. Gardez à l'esprit que ces modèles doivent être régulièrement passés au crible afin de rechercher les erreurs de configuration les plus courantes.

Adopter et appliquer des standards

N'oubliez pas que toute automatisation passe d'abord par un travail de standardisation en amont. On ne compte plus les équipes de sécurité qui parlent d'automatisation avant même d'avoir établi des standards de sécurité. Ne partez pas d'une feuille blanche : le CIS (Center for Internet Security) propose des benchmarks pour l'ensemble des principales plateformes cloud. Automatisez et codifiez ces standards en exploitant l'IaC.

Former et recruter des ingénieurs sécurité sachant coder

Contrairement à la plupart des data centers traditionnels, les clouds publics reposent sur des API. Bien gérer les risques liés au cloud, c'est donc s'appuyer sur ces API afin d'assurer la sécurité des workloads à grande échelle. Or, les API sont difficiles à utiliser sans la présence d'ingénieurs capables de coder et d'automatiser les processus de sécurité dans le cadre du pipeline CI/CD.

Intégrer la sécurité au DevOps

Qui, quoi, quand, comment et où ? Telles sont les questions essentielles à vous poser pour assurer la traçabilité du code déployé dans le cloud. Localisez ensuite les points d'entrée les moins perturbateurs pour vos processus et outils de sécurité dans votre pipeline CI/CD. Mettez toutes les chances de votre côté en obtenant d'emblée l'adhésion des équipes DevOps. Ensuite, efforcez-vous de réduire progressivement l'interaction humaine en automatisant le plus d'opérations possible.

Prêt à identifier les menaces qui pèsent sur votre cloud ?

Prisma Cloud analyse plus de 10 milliards d'incidents par mois. Le verdict est sans appel : les mauvaises configurations, les comportements permissifs et l'absence de politiques créent de nombreuses failles dans lesquelles les attaques et menaces inconnues peuvent s'engouffrer. C'est pourquoi Prisma Cloud détecte proactivement les erreurs de configuration néfastes à la sécurité et la conformité de votre entreprise, puis lance des actions correctives automatiques. Vous répondez ainsi aux exigences de sécurité et de performance de vos workloads cloud dynamiques.

Méthodologie

Ce rapport s'appuie sur les données collectées entre octobre 2019 et février 2021. Nous avons concentré nos recherches sur les entreprises et les secteurs du monde entier, y compris les Amériques (du Nord et du Sud), la région EMEA (Europe, Moyen-Orient et Afrique) et la zone JAPAC (Japon et Asie-Pacifique).

Palo Alto Networks Prisma Cloud

Les données de Prisma® Cloud s'appuient sur différentes sources de Threat Intelligence. Les chercheurs d'Unit 42 ont utilisé des sources de données propriétaires pour recueillir les informations nécessaires sur les alertes et évènements d'entreprise. Ces données ont été anonymisées, analysées puis comparées aux résultats des précédents rapports sur les menaces cloud afin de déterminer les dernières tendances.

Palo Alto Networks WildFire

Le service cloud anti-malware WildFire® s'appuie sur une approche multi-technique unique pour détecter et neutraliser les menaces les plus furtives. Il agit pour cela sur plusieurs tableaux : analyses dynamiques et statiques, techniques de machine learning innovantes et environnement d'analyse bare-metal révolutionnaire.

Palo Alto Networks AutoFocus

Information, analyse et contextualisation : le service de Threat Intelligence AutoFocus™ vous livre tous les éléments nécessaires pour identifier les attaques exigeant une réponse immédiate. Il permet en outre d'exploiter les indicateurs disponibles afin de faciliter la prévention des futures menaces.

À propos

Prisma Cloud

Prisma® Cloud de Palo Alto Networks est la plateforme de sécurité cloud-native la plus complète du marché. Sa mission : assurer la protection et la mise en conformité de vos applications, données et technologies cloud-native tout au long du cycle de développement sur vos environnements cloud hybrides et multicloud.

Unit 42

Unit 42 est l'équipe de Threat Intelligence internationale de Palo Alto Networks. Nos analystes travaillent sans relâche pour traquer les menaces et collecter les données sur les tactiques et les techniques associées. Leur expertise leur permet en outre de décortiquer les malwares pour mieux en révéler la mécanique. Unit 42 assure le lien essentiel entre la Threat Intelligence et les produits de Palo Alto Networks, afin de garantir la protection des clients sur l'ensemble de notre suite de sécurité.

Auteurs

Jay Chen, chercheur senior, sécurité du cloud public, Palo Alto Networks

Nathaniel « Q » Quist, chercheur senior, sécurité du cloud public, Palo Alto Networks

Matthew Chiodi, CSO, cloud public, Palo Alto Networks

UNIT 42
BY PALO ALTO NETWORKS

Oval Tower, De Entrée 99 – 197
1101HE Amsterdam, Pays-Bas

Téléphone : +31 20 888 1883

www.paloaltonetworks.fr

unit42_cloud-threat-report-1h-2021_040121-fr