

Remarque : Ce rapport d'enquête est susceptible d’évoluer jusqu'au 31 juillet 2018 et certains chiffres clés, comme le nombre total de ransomwares collectés, peuvent changer. Nous vous tiendrons informé de tout changement, et n’hésitez pas à nous contacter en cas de questions ou, si nécessaire, pour vérifier certains faits.

Les entretiens avec les chercheurs des SophosLabs et les experts en cybermenaces, ainsi que les graphiques tirés du rapport et émanant des réseaux sociaux, sont disponibles sur demande.

Les commentaires de Sophos, avec des liens vers le document final, seront disponibles en ligne sur les sites suivants :

SophosLabs Uncut : <http://news.sophos.com/en-us/samsam-guide-to-coverage>

Sécurité Naked : <https://nakedsecurity.sophos.com/samsam>

# # #

**SamSam: Le ransomware qui vaut (presque) 6 millions de dollars**

*Synthèse des notes de briefing/presse et highlights de notre enquête sur cette campagne de ransomware*

**Résumé**

Sophos a mené une enquête sur le long terme concernant la campagne de ransomware SamSam, peu de temps après son apparition fin 2015. Ce rapport résume nos conclusions sur les outils, les techniques et les protocoles utilisés par les cybercriminels, dans le but de comprendre plus globalement la nature de cette menace singulière.

La méthode utilisée dans cette attaque reste singulière en raison de son approche manuelle, et tient plus du cambriolage méthodique que du vol à l’arraché improvisé. En effet, le cybercriminel utilise des techniques alternatives (si nécessaire), et est étonnamment habile dans le contournement de nombreux outils de sécurité. Si le processus de chiffrement des données est interrompu, alors le malware supprime complètement et immédiatement toute trace de son passage, afin d’entraver toute investigation.

SamSam est un outil de chiffrement particulièrement complet, rendant inutilisables non seulement les fichiers de données professionnelles, mais aussi tout programme qui n'est pas essentiel au fonctionnement d'un ordinateur Windows, dont la plupart ne sont pas systématiquement sauvegardés. La récupération peut nécessiter la reconfiguration et/ou la réinstallation des logiciels ainsi que la restauration des sauvegardes. Le cybercriminel est très doué pour dissimuler toute trace de son passage et semble devenir de plus en plus paranoïaque (ou expérimenté) au fil du temps, en ajoutant progressivement de plus en plus de fonctionnalités de sécurité dans ses outils et sites web.

**Les principales conclusions**

**Les fondamentaux**

* Le ransomware SamSam a fait son apparition en décembre 2015.
* Certaines victimes ont fait état d’incidents provoqués par un ransomware très répandu, qui a eu un impact significatif sur le fonctionnement opérationnel de certaines grandes entreprises, y compris des hôpitaux, des écoles et des villes.
* Les détails concernant cette attaque ont pris du temps à être récupérés car le ou les cybercriminels(s) impliqué(s) avai(en)t pris soin d’obfusquer leurs méthodes et de supprimer toute preuve pouvant le ou les confondre.
* De nombreuses victimes ont constaté qu'elles ne pouvaient pas suffisamment se rétablir, ou du moins pas assez rapidement, pour assurer la continuité des activités de l’entreprise de manière autonome et, à contrecœur, ont dû payer la rançon.

**Les statistiques**

* En suivant les adresses Bitcoin fournies dans les demandes de rançon et les fichiers échantillon, et en travaillant avec la société Neutrino, Sophos a calculé que SamSam avait rapporté plus de 5,9 millions de dollars (environ 5 millions d’euros) à ses créateurs depuis fin 2015.
* Sophos a déterminé que 74% des victimes connues étaient basées aux États-Unis. D'autres régions connues pour avoir subi des attaques comprennent le Canada, le Royaume-Uni et le Moyen-Orient.
* Les cybercriminels SamSam ont reçu des paiements de rançon allant jusqu'à 64 000 $ (environ 55 000€), sur la base de l'analyse des opérations effectuées vers les portefeuilles Bitcoin qui ont été suivis.
* Contrairement à la plupart des autres ransomwares, SamSam chiffre non seulement les fichiers document, les images et d’autres données personnelles ou professionnelles, mais également les fichiers de configuration et de données nécessaires pour exécuter des applications (par exemple, Microsoft Office). Les victimes, dont la stratégie de sauvegarde ne protège que les documents et les fichiers utilisateur, ne pourront pas récupérer une machine sans la reconfigurer au préalable.
* Chaque nouvelle attaque a montré une évolution dans la sophistication ainsi qu’une compréhension en nette progression des méthodes pour échapper aux techniques de sécurité opérationnelle mises en place.
* Les coûts, subis par les victimes, ont augmenté de façon spectaculaire, et le rythme des attaques ne montre aucun signe de ralentissement.

**Le profil des victimes**

* Un certain nombre d’organisations, grandes et moyennes, du secteur public de la santé, de l'éducation et gouvernementales ont publié des divulgations de violation concernant SamSam.
* 100% des victimes d'organisations gouvernementales connues ont rendu public l'attaque subie. 79% des entreprises de l'industrie de la santé ont fait une divulgation publique, tout comme 38% des victimes d’établissements d'enseignement.
* Les entreprises, qui ont divulgué publiquement une attaque, ne représentent que 37% des victimes de SamSam identifiées par Sophos. Nous pensons qu'il peut y avoir des centaines de victimes de plus qui n'ont fait aucune divulgation publique, mais nous ne pouvons pas les identifier.
* À ce jour, aucun autre secteur industriel ou privé n'a fait de déclaration publique confirmant une attaque de SamSam (que nous avons pu localiser). Plus de la moitié du nombre total de victimes est restée inhabituellement silencieuse au sujet de ces attaques.

**L'attaque en détail**

* Sophos suspecte fortement que de nombreuses attaques ont commencé par la compromission d’un Bureau Distant, au sein d'une machine à l'intérieur d’un réseau. Le cybercriminel est également connu pour déployer des exploits sur des machines vulnérables afin d'exécuter du code à distance.
* Le cybercriminel est particulièrement attentif à la cible sélectionnée et la préparation de l'attaque est méticuleuse.
* Le cybercriminel maintient une présence sur la machine compromise pendant l'analyse du réseau interne.
* Le cybercriminel utilise des outils classiques open-source et commerciaux normalement utilisés pour l'administration de systèmes ou les tests de pénétration pour voler des mots de passe, déplacer des programmes d'installation de ransomwares sur des machines d’Administration de Domaine et acheminer le ransomware vers des stations de travail connectées.
* Contrairement à de nombreuses attaques de ransomware, celles-ci ne proviennent pas d'un spam malveillant classique ou d'une attaque de type drive-by download. Chaque attaque constitue une sorte de pénétration manuelle au sein d'un réseau ciblé.
* Le cybercriminel résiste activement aux tentatives de blocage du programme d'installation de SamSam et utilise régulièrement des techniques qui contournent certains types de protection endpoint au niveau des systèmes ciblés, les rendant ainsi vulnérables vis-à-vis des ransomwares.
* Une fois que le malware a pu analyser le réseau interne et compiler une liste de victimes potentielles, les cybercriminels SamSam attendent le milieu de la nuit, dans le fuseau horaire de la victime, avant de lancer l'attaque à proprement parlé : à savoir une commande pour répandre le malware et commencer le chiffrement des machines infectées. Ce parfait timing, quand la plupart des utilisateurs et des administrateurs sont endormis, augmente un peu plus les chances de succès d’une telle attaque.

**Le bilan**

* Sophos estime que le cybercriminel SamSam a gagné en moyenne un peu moins de 300 000 dollars (environ 256 000 euros) par mois en 2018\*.
* À partir du suivi des paiements Bitcoin vers des adresses de portefeuille connues et détenues par le cybercriminel, Sophos a calculé que le ransomware SamSam avait dépassé les 5,9 millions de dollars de gain (à peu près 5 millions d’euros)\*.
* La plus importante rançon reçue par le cybercriminel SamSam a été évaluée à 64 478$\* (soit environ 55 000€ au moment du paiement).
* Le paiement est effectué par les victimes en Bitcoin via un "site de paiement" personnalisé sur le DarkNet, qui est lié une adresse unique pour chaque entreprise ciblée.
* Le site de paiement permet au cybercriminel SamSam d'interagir directement avec les victimes, via une interface de type tableau d’affichage des messages, afin de pouvoir communiquer.
* Le montant de la rançon varie considérablement selon les entreprises, mais a augmenté régulièrement au fur et à mesure de l'utilisation active du ransomware.
* Une fois le paiement intégral reçu, le cybercriminel SamSam déplace la cryptomonnaie dans un système de type « tumbler/mixer», qui tentent de blanchir la source du Bitcoin grâce à une myriade de micro-transactions.

\* Note : Afin d'estimer avec précision les coûts, en raison des taux de change extrêmement fluctuants, nous avons calculé la valeur d'une quantité donnée de Bitcoin le jour où ils ont été acquis par le cybercriminel SamSam, si ce dernier les avait immédiatement encaissés.

**Curiosités comportementales et autres caractéristiques singulières**

* Les demandes de rançon récentes ont utilisé un ton apologétique, presque contrit, avec un fichier de demande de rançon nommé **SORRY-FOR-FILES.html** et une extension de fichier **.weapologize** sur chaque fichier chiffré.
* Les deux premières versions du malware SamSam ont ajouté plus de 50 extensions de fichiers différentes à des fichiers utilisateur chiffrés avec seulement une variante par attaque, en changeant ces extensions pour chacune d’entre elles. Mais depuis la version 3, il s’est contenté de l'extension ".weapologize".
* SamSam contient dans le code du programme une liste hardcodée des extensions de fichier à cibler en premier pour le chiffrement. Il chiffrera ceux de cette liste avant tous les autres.
* Le ransomware ne chiffre pas seulement les fichiers présents sur la liste des extensions hardcodées. Après avoir terminé le chiffrement des fichiers de cette liste, il chiffre tous les autres fichiers qui ne sont pas nécessaire pour que Windows, le navigateur IE ou Edge fonctionnent. La plupart des méthodes de sauvegarde n’ont pas l’habitude d’effectuer des sauvegardes des répertoires de programmes ou des fichiers de configuration.
* Pendant toute la durée des attaques SamSam, certaines tics comportementaux, sous la forme de fautes d'orthographe ou d’erreurs de ponctuation mineures, ont été répétés. Ces derniers peuvent aider à déterminer la région à partir de laquelle le cybercriminel a agi.
* Les charges virales de SamSam contenaient, par le passé, des séquences qui affichaient les chemins de génération de l'ordinateur utilisé pour compiler les malwares exécutables. Ces chemins de génération peuvent constituer des preuves pour indiquer l'utilisation d'une machine spécifique dans la construction du malware en question.
* L'heure de compilation des malwares SamSam indique que la grande majorité des échantillons a été générée durant une fenêtre temporelle allant de 20h à 23h, correspondant à l'heure locale du lieu où se trouve le cybercriminel.
* Le cybercriminel compile de nouvelles copies des charges virales des malwares exécutables durant toute la semaine, mais en construit moins le lundi, et davantage le mardi. Ainsi, même les cybercriminels n'aiment pas les lundis.
* Si le processus de chiffrement est interrompu à mi-course, un processus interne qui s'exécute depuis le malware SamSam le détecte, et lance un utilitaire de suppression sécurisé qui efface le code SamSam et entrave la récupération forensique.

**Mesures de sécurité recommandées**

Il n'existe pas de solution miracle en matière de sécurité : un modèle de protection actif et construit par couches reste la meilleure option.

* Si vous étudiez la méthodologie, il existe plusieurs points au niveau desquels des mesures de sécurité basiques peuvent contribuer à stopper le cybercriminel SamSam.
* Sophos recommande de mettre en œuvre ces quatre mesures de sécurité de base:
1. Accès restreint au port 3389 (RDP) en autorisant uniquement le personnel utilisant un VPN à accéder à distance aux systèmes. Utiliser l'authentification multi-facteurs pour l'accès VPN.
2. Des analyses régulières de vulnérabilité et des tests de pénétration complets sur l'ensemble du réseau. Si vous n’avez pas pris en compte les récents rapports de tests de pénétration, faites-le maintenant.
3. L’authentification multi-facteurs pour les systèmes internes sensibles, même pour les employés utilisant le LAN ou le VPN.
4. Des sauvegardes hors ligne et hors site comprenant une stratégie de récupération après sinistre qui couvrira la restauration des données et des systèmes complets.
* Les mesures de sécurité supplémentaires optimales recommandées par Sophos :
* Une sécurité, mise en œuvre par couches, qui bloque les cybercriminels vis-à-vis de tous les points d'entrée et interdit les accès une fois à l'intérieur du réseau.
* L’installation des correctifs effectuée de manière rigoureuse et appliquée.
* Une sécurité spécifique dédiée au serveur avec des fonctionnalités de verrouillage et une protection anti-exploit, en particulier pour les systèmes non patchés.
* Une sécurité qui synchronise et partage l'intelligence afin d’activer les processus de verrouillage.
* Une sécurité des systèmes endpoint et des serveurs avec une protection contre le vol d’identifiants.
* Des mots de passe d'administration uniques, difficiles à cracker, avec une authentification multi-facteurs.
* Une amélioration des politiques en matière de mot de passe : Encourager les employés à utiliser des gestionnaires de mots de passe sécurisés, des mots de passe plus longs et la non-réutilisation de ces derniers sur plusieurs comptes : Comment choisir un mot de passe sécurisé.
* Des évaluations périodiques, en utilisant des outils tiers tels que Censys ou Shodan, pour identifier les services et les ports accessibles publiquement au sein de votre espace d'adressage IP public, et les fermer immédiatement.
* Une amélioration des contrôles d'accès aux comptes : adopter des politiques réfléchies pour sécuriser les comptes inactifs, verrouiller automatiquement les comptes et alerter les équipes informatiques après un certain nombre de tentatives de connexion infructueuses.
* L’exécution régulière de tests de phishing et de formations de sensibilisation du personnel sur les dangers associés.

# # #