Rapport du test comparatif de Remediation

Ce test comparatif a été réalisé par AV-TEST GmbH sur demande de la société Enigma Software Group.
Rapport du : 10 mai 2017, actualisé le 24 mai 2017

Résumé

Lors d'un test comparatif réalisé en mars 2017, l'institut AV-TEST a contrôlé les fonctions et capacités réparatrices de SpyHunter, un programme d'Enigma Software Group. Ce test a été réalisé sur un système Windows 7 (SP1, 64 bits) non infecté. La même image disque a ensuite été utilisée sur plusieurs ordinateurs de même type.

21 programmes malveillants différents ont été employés lors de ce test de Remediation et la procédure de test était divisée en deux phases. Durant la première phase du test, il s'agissait d'infecter l'image disque avec un échantillon de logiciel malveillant puis, dans un second temps, d'essayer d'installer le produit de sécurité, d'analyser le système et d'éliminer la menace identifiée. Afin de pouvoir infecter le système, la solution antivirus a été désactivée au début de cette seconde phase de test. Les testeurs ont ensuite réactivé la solution antivirus puis redémarré l'ordinateur afin de vérifier que tous les composants de la solution de sécurité fonctionnaient correctement. La dernière étape correspondait au nettoyage du système et à une analyse supplémentaire du système.

Lors de la première phase du test, SpyHunter a obtenu un résultat presque parfait de 98 % et a réussi à éliminer tous les composants actifs du programme malveillant. Dans un seul cas, l'application créée par le logiciel malveillant est restée dans le système. Les trois produits testés suivants, à savoir Emsisoft Anti-Malware, Malwarebytes Free et Malwarebytes Premium, se sont également acquitté avec succès de cette catégorie du test puisqu'ils ont atteint des taux de 92-93 % tandis que Spybot Search & Destroy et IObit Malware Fighter se sont largement laissé distancer comme le prouve leur taux respectif de 40 % et 10 %.

L'analyse de la seconde phase de test révèle une situation très similaire à la première partie du test en ce qui concerne le classement des produits : avec un taux de 97 %, SpyHunter a de nouveau réalisé une très bonne performance en neutralisant tous les composants actifs du programme malveillant et en ne laissant qu'une entrée de boot dans le registre ainsi que les applications créées dans le système. Emsisoft Anti-Malware, Malwarebytes Free et Malwarebytes Premium ont également obtenu de bons taux situés entre 92 et 93 %. Le rôle de lanterne rouge est à nouveau assumé par Spybot Search & Destroy et IObit dont les résultats ne sont que de l'ordre de 40 et 10 %.

Aperçu

Puisque le nombre de menaces créées et diffusées aujourd'hui sur Internet ne cesse d'augmenter, cela entraine ipso facto une augmentation du risque d'infection des systèmes. Tandis qu'il y a encore quelques années, de nouvelles menaces n'étaient découvertes que tous les deux ou trois jours, un scénario de menace actuel dénombre plutôt plusieurs milliers de nouveaux programmes malveillants par heure.

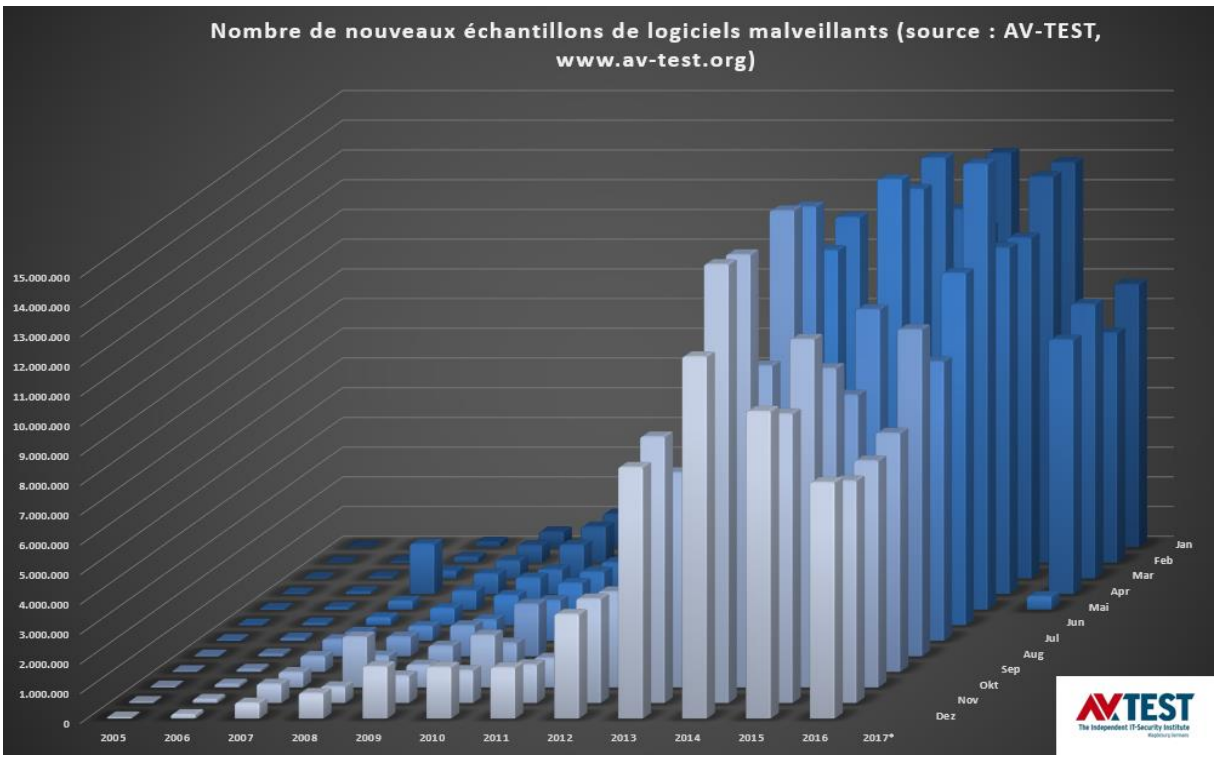

Illustration 1 : Nouveaux échantillons de logiciels malveillants par an

Alors qu'AV-TEST avait comptabilisé plus de 170 000 nouveaux échantillons de programmes malveillants en l'an 2000, ce nombre avait déjà dépassé les 80 millions jusqu'en 2013. Un simple coup d'œil sur l'illustration 1 permet de constater que cette croissance s'est poursuivie en 2016. À l'heure actuelle, plus de 630 millions d'échantillons de logiciels malveillants sont répertoriés dans la base de données d'AV-TEST.

Les fabricants de logiciels de sécurité doivent faire face à une immense quantité de nouveaux malwares pour protéger leurs clients. Cette abondance de programmes peut poser problème, parce qu'il n'est pas toujours possible de protéger un ordinateur des menaces à temps. Même en cas d'installation d'un antivirus actualisé sur l'ordinateur, ce dernier peut malgré tout être infecté s'il s'écoule plusieurs heures entre la découverte d'un nouveau programme malveillant et la mise à disposition de signatures correspondantes. Dans certains cas, il est alors déjà trop tard. Les attaques peuvent résulter en des pertes financières pour les utilisateurs, notamment si des données confidentielles sont volées ou si l'utilisation du système est limitée jusqu'à ce que le logiciel malveillant soit complètement supprimé de l'ordinateur.

Dans ces conditions, les techniques de Remediation prennent une importance croissante dès lors qu'un ordinateur infecté doit vite redevenir opérationnel. Il est cependant indispensable que le

nettoyage par le biais de cette technique soit effectué de manière fiable quant aux deux points suivants :

1. Le programme malveillant ainsi que tous les constituants du malware doivent être supprimés et les systèmes infectés doivent être restaurés.
2. Les programmes inoffensifs de même que le système ne doivent pas être endommagés lors de l'opération de nettoyage.

Produit testé

Le test a été réalisé en mars 2017 et AV-TEST a utilisé la version la plus récente du logiciel qui était disponible au moment du test :

- SpyHunter d'Enigma Software Group

Méthode de test et évaluation

Plateforme

La totalité des essais a été effectuée sur des ordinateurs identiques présentant la configuration matérielle suivante :

- Intel Xeon Quad-Core X3360 CPU
- 4 Go de mémoire vive
- Disque dur de 500 Go (Western Digital)
- Carte réseau Intel Pro/1000 PL (Gigabit Ethernet)

Windows 7 (SP1, 64 bits) a été utilisé comme système d'exploitation avec tous les correctifs de type hotfix installés dans cette version et tous les patchs disponibles jusqu'au 3 janvier 2017.

Méthode de test

Le test de Remediation était composé de dix étapes qui ont été réalisées en suivant la méthode suivante :

1. **Système propre pour chaque programme malveillant**. Avant d'être infectés par un seul échantillon de logiciel malveillant, les ordinateurs d'essai ont tous été nettoyés et restaurés.
2. **Ordinateurs réels.** Seuls de véritables ordinateurs ont été utilisés lors du test tandis qu'aucun environnement virtuel n'a été employé.
3. **Accès à Internet**. Durant le test, les ordinateurs pouvaient toujours se connecter à Internet afin de consulter leur cloud s'ils en avaient besoin.
4. **Configuration des produits**. Le laboratoire s'est servi des paramètres standards de la configuration d'origine pour tous les produits et outils de Remediation correspondants ou encore pour tous les outils de récupération amorçables.
5. **Infection des ordinateurs d'essai.** Un système natif a été infecté par un programme malveillant puis il a été redémarré. L'objectif de cette opération était de vérifier le bon fonctionnement du malware.

6. **Familles de programmes malveillants et maliciels (payloads).** En sélectionnant les échantillons pour le test, les testeurs ont pris soin de choisir des malwares n'appartenant pas à la même famille de programmes malveillants et ne faisant pas appel au même maliciel.
7. **Remediation utilisant toutes les fonctions du produit disponibles**.
    a. Le produit de sécurité devait être installé avec les paramètres standards. Il fallait respecter toutes les indications du produit pour éliminer le programme malveillant.
    b. Si a. était impossible, alors les testeurs devaient essayer un ***outil de réparation autonome ou un outil de récupération*** (si disponible).
    c. Si b. était impossible, alors les testeurs devaient tenter d'éliminer la menace avec une ***solution de démarrage*** autonome (si disponible).
8. **Vérification de la suppression du logiciel malveillant.** L'ordinateur a ensuite été contrôlé manuellement pour vérifier la suppression complète du malware ou constater la présence de fragments de fichiers.
9. **Évaluation de la performance lors de la suppression du logiciel malveillant.** Pour analyser la performance de l'outil et de la solution de sécurité complète, les testeurs se sont appuyés sur un système de points défini.
10. **Conséquences excessives de la Remediation.** Le laboratoire a aussi testé si la solution de sécurité utilisait des méthodes agressives pour nettoyer l'ordinateur. Ainsi, certains produits suppriment des fichiers hosts complets voire des répertoires entiers, quand bien même cela n'est pas requis pour terminer la Remediation avec succès. L'application de méthodes de ce type s'est traduite par un retrait de points lors de l'évaluation.

Évaluation de l'efficacité

Des points ont été attribués pour chaque échantillon de malware testé, et ce, conformément au système suivant :

a. Programme malveillant entièrement éliminé (3 points)
b. Programme malveillant identifié et éliminé, il ne reste que des fragments de fichiers inactifs (2 points)
c. Programme malveillant partiellement identifié et éliminé mais il reste cependant des fichiers du maliciel qui sont encore actifs (1 point)
d. Programme malveillant non identifié et donc non éliminé (0 point)

Lors de l'attribution des points, AV-TEST n'a pas pris en compte laquelle des techniques disponibles a été utilisée pour éliminer le programme malveillant. Cependant, chaque technique devrait avoir été utilisée. Si une solution supprime les entrées dans le fichier hosts pour cette même solution, mais qu'elle laisse derrière elle un système sûr et que le bon fonctionnement de même que la mise à jour du produit restent assurés, alors cette solution mérite la meilleure note pour sa performance de Remediation même si les entrées d'autres fournisseurs de logiciels de sécurité restent dans le fichier hosts.

Échantillons

Le kit de test était composé de 21 programmes malveillants permettant d'attaquer le système Windows 7 (SP1, 64 bits).

Résultats de test

Grâce à sa note finale de 123/126, SpyHunter a obtenu le meilleur résultat lors de ce test comparatif et il est suivi par les deux produits de Malwarebytes qui occupent la deuxième place en raison de leur bonne note de 118/126. Emsisoft Anti-Malware a également fait preuve d'une bonne performance et les talonne de près avec son 116/126. Avec seulement 50 points au total, Spybot Search & Destroy n'est parvenu qu'à un résultat médiocre, tandis qu'IObit Malware enregistre un piètre score de 12/126.

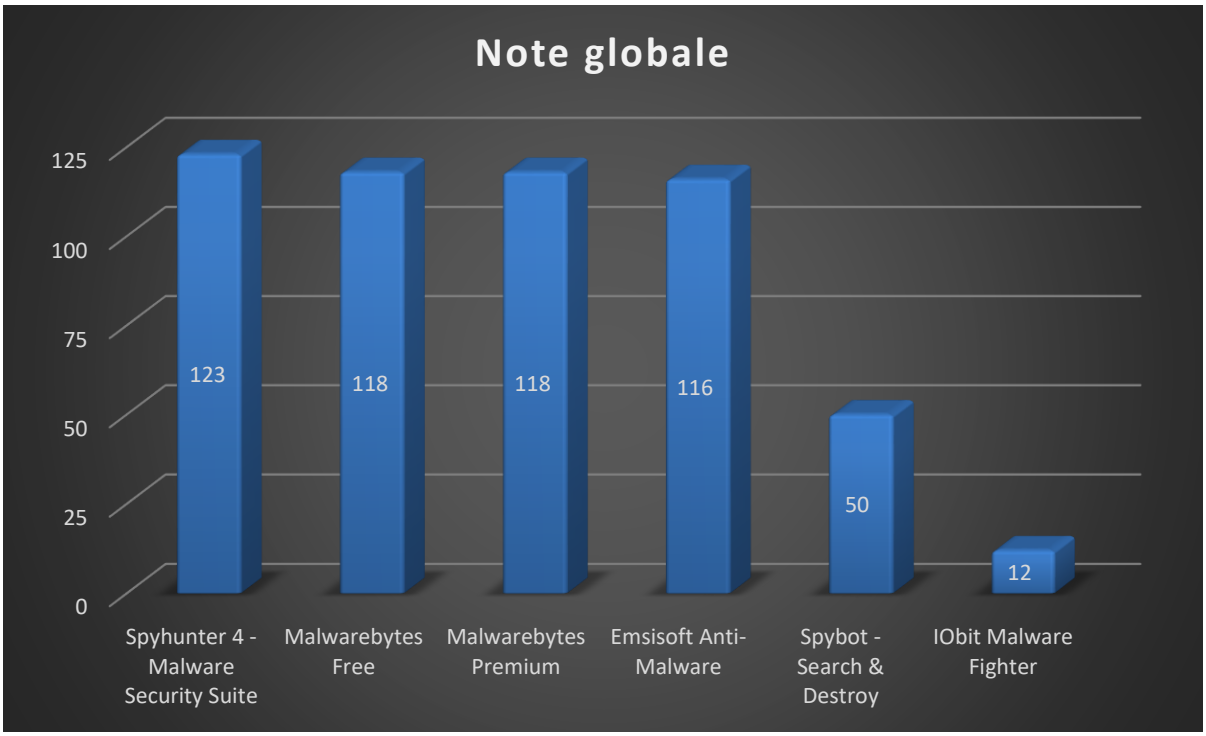

Illustration 2 : Résultat global de la Remediation – phases de test 1.1 et 1.2

Il suffit de jeter un œil sur les illustrations 3 et 4 pour voir que les résultats des phases de test 1 et 2 sont presque identiques. La note maximale à atteindre était de 63/63 pour chaque phase du test.

SpyHunter a obtenu un 62/63 lors de la première partie du test et un 61/63 lors de la seconde. Ce produit a donc fait preuve d'une excellente performance. Le programme n'a laissé qu'une application dans le système lors de ces deux tests et une entrée est restée dans le registre durant la phase de test 2.

Grâce à leur note de 59/63 pour chacun des tests, les deux versions de Malwarebytes ont atteint un bon résultat global, et ce, bien que dans un cas, elles n'aient pas réussi à supprimer le programme malveillant et aient laissé des composants actifs du malware dans le système. Emsisoft Anti-Malware occupe la troisième place du classement grâce aux deux 58/63 obtenus en supprimant tous les composants actifs des 21 échantillons de test et en ne laissant qu'une application ainsi que des entrées de registre dans le système.

Spybot Search & Destroy n'a même pas réussi à éliminer la moitié des échantillons de programmes malveillants testés et n'a donc mérité que 25 points lors des phases de test 1 et 2.

N’ayant atteint qu’une note de 6/63 dans chacun des tests, IObit enregistre le pire résultat : 18 des 21 échantillons de malwares ont eu raison de ce programme.

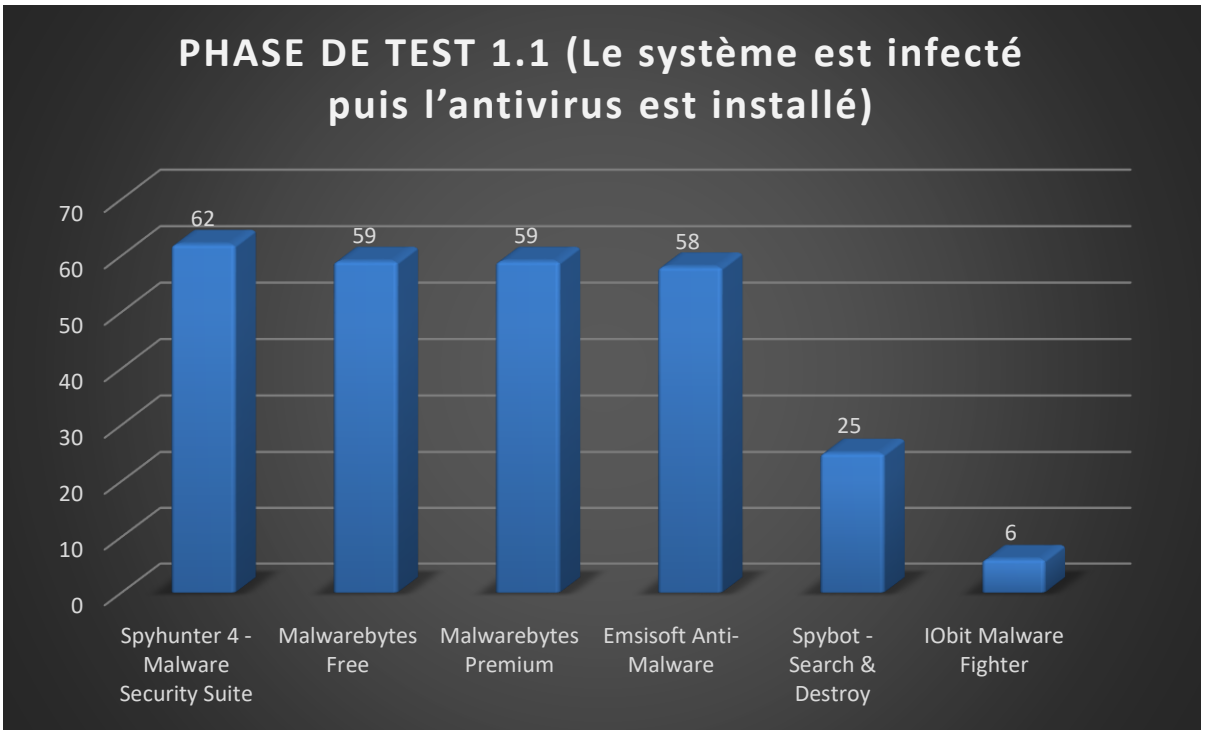

Illustration 3 : Résultat de la Remediation – phases de test 1.1 et 1.2

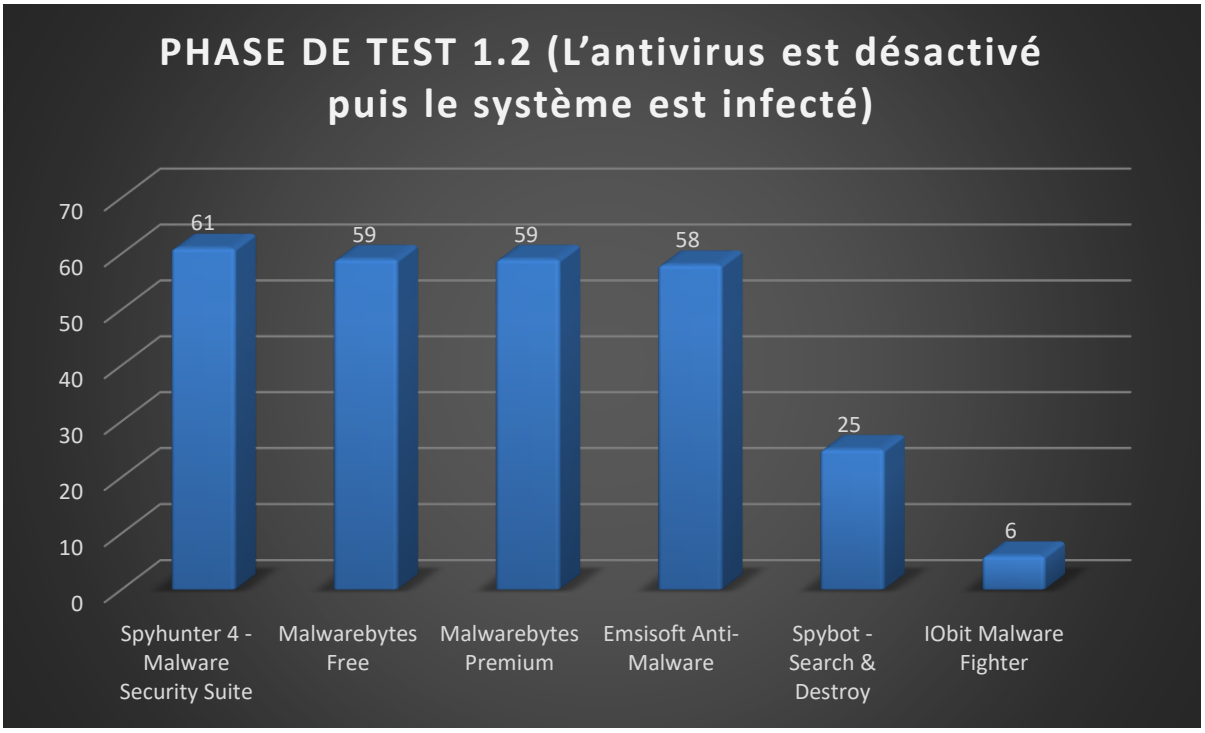

Illustration 4 : Résultat de la Remediation – phases de test 1.2 et 1.2

Annexe

Informations sur la version testée du logiciel

Développeur, fabricant	Nom du produit	Version du programme	Moteur / Version de signature
Emsisoft	Anti-Malware	2017.2.1.7260	4.0.1.856/20170324
Enigma Software Group	SpyHunter 4	4.24.3.4750	2017.01.17v01
IObit	Malware Fighter	4.5.0.3457	1634
Malwarebytes	Malwarebytes Free	3.0.6.1469	nd
Malwarebytes	Malwarebytes Premium	3.0.6.1469	nd
Safer Networking	Spybot Search & Destroy	1.6.2.46	nd

Liste des échantillons de logiciels malveillants utilisés lors du test de Remediation

(SHA256)
* 0x0101d4a72a3685aaf8a7baa4408223914ba7f1c8d193628fabbe98cd377536cd
* 0x01168762ca9a57ffe5b69371b85d7d60339a3a95091554e87750715fc146313d
* 0x0bf7ab1fd378c78ea8206c84dfa780c472d84c5357238d78df369881f762ad99
* 0x246082bd340133a0b634ef874a20f9823336fc3e65baddaddc57c3af5588a35a
* 0x369fab397bbc2ca10601c3ca89f77b24eecf485b080f07d820daf8a6487554a2
* 0x3b56fcb59462dac54bee27b85bc8e29af286d0349909aa9a313868e8be5c96bd
* 0x453442bc8fd9e0fec64febb1c7c81cc1daecc151faa0aa30041b25296b906423
* 0x454ecf8d9846abae025fa57f097fa6bc11b3ac7bd68b9a1c2eb55bc6861b3d4c
* 0x4b91c4e2f69697a888b56147f69d4c96ca13095a2aaf640a48e68994c7228565
* 0x4da0d3e569ceeced62b7128ed35c55cfb48236be628ba64411f066a9a38a5aff
* 0x4e59b6263b5b3a5ce4ea5054dc48cca37945ca930ad1a5aa300029539d8042a3
* 0x6a9936983ee1bc49d5fff7e2ae6435462667c7f62547a710297b8f9c86a36873
* 0x7021df3d38a24a1de948ef5c820b60d8e61c95ed3409c255680eba79e4221123
* 0x7a1e9db7fe1bc6341b1e1a002c19ca6f32224aa0c4eb6582d984d66bb44f339e
* 0x8f995f37b1aee61018742c35ab410820b02982fe2ac0b9a2554d02909f2590a2
* 0x9643447291f6e468611c8acb6e58f8e3b3c40a3394e4f7d5c20489a9af0e0750
* 0xc0d110efbd58448c8fed7e249a3e5503185cd3f2fc4a13339874646256877f9e
* 0xda3458870afb6487c435129bd1ac4c8b994c2133d3790ca505949cc2644293bf
* 0xee7e9a572dd14739aaf6cc16f1d52e66b62347f1902a2c93a9145ab9c0f29d83
* 0xf6c186da15892176e8f8cd31e9dd637024a4e4e08510315011d6d735a32f2c93