Rapport du test de réparation

Le test a été effectué pour le compte de la société EnigmaSoft Limited par AV-TEST GmbH

Date du rapport : le 03 septembre 2018, dernière actualisation le 04 septembre 2018

Version succincte

En août 2018, AV-TEST a effectué un test concernant le service de réparation de SpyHunter de la société EnigmaSoft Limited. Le test a été mis en pratique sur un système propre équipé de Windows 10 (RS3, 64 bits) et la même image disque a été utilisée sur plusieurs ordinateurs identiques.

Le corpus de test des logiciels malveillants pour le test de réparation comprenait 12 modèles et était divisé en deux sections. Section 1 du test : pour commencer, l'image a été infectée avec l'un des modèles de logiciels malveillants. L'étape suivante consistait à installer le programme de protection, à scanner l'ordinateur et à supprimer toutes les menaces détectées. Section 2 du test : dans ce cas, le logiciel AV a tout d'abord été désactivé pour pouvoir infecter le système. Le logiciel AV a ensuite été réactivé et redémarré afin de garantir le fonctionnement correct de tous les composants du logiciel AV. Ces préparatifs ont été suivis de la tentative de réparer le système et d'effectuer un scan supplémentaire du système.

SpyHunter a obtenu un résultat parfait de 100 % dans les deux sections de test. Le logiciel d'Enigma a nettoyé tous les composants actifs et supprimé tous les artefacts malveillants du système.

Vue d’ensemble

Le nombre croissant de menaces publiées et diffusées aujourd'hui sur Internet accroît également le risque d'infection des systèmes. Il y a quelques années, de nouveaux virus apparaissaient uniquement tous les quelques jours. Aujourd'hui, il faut s’attendre à plusieurs milliers de nouvelles menaces chaque heure.

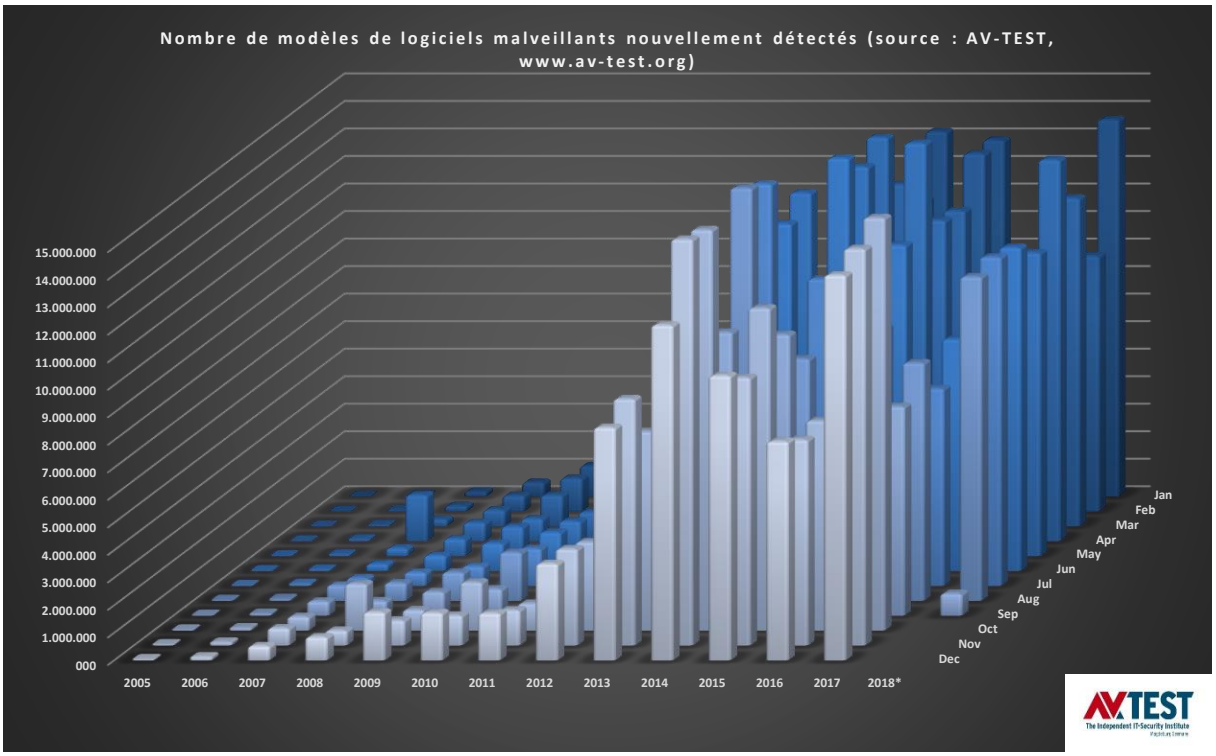


Figure 1 : Nouveaux modèles par an

En 2000, AV-TEST a reçu plus de 170 000 nouveaux modèles ; en 2013, le nombre de nouveaux modèles était passé à plus de 80 000 000. Au cours des années suivantes, ce nombre a continué d'augmenter, comme le montre le graphique de la figure 1. La base de données d’AV-TEST contient actuellement plus de 800 millions de modèles de logiciels malveillants. Au cours du premier semestre 2018, les systèmes de collecte d'AV-TEST ont enregistré environ 10 millions de nouveaux modèles chaque mois.

Les fournisseurs de logiciels anti-malware doivent traiter un grand nombre de nouveaux modèles pour assurer la protection de leurs clients contre d’éventuelles attaques problématiques. Il n'est cependant pas toujours possible de protéger un ordinateur à temps. Une infection peut se produire même si l’ordinateur dispose d’un logiciel anti-malware actuel, étant donné que les signatures ne sont fournies que toutes les quelques heures, ce qui peut parfois être trop tard pour le sauver. Les infections causent des pertes financières dues à l’exploitation frauduleuse de données confidentielles ou entravent une utilisation rentable de l’ordinateur jusqu’à ce que le logiciel malveillant ait été complètement éliminé du système.

Les techniques de réparation sont donc devenues de plus en plus importantes pour qu'un ordinateur infecté puisse être réutilisé correctement. L'utilisation de ces techniques suppose que le processus de nettoyage soit fiable à deux égards :

1. Le logiciel malveillant et tous ses composants doivent être supprimés et toutes les modifications du système effectuées par le logiciel malveillant doivent être annulées.
2. Le processus de nettoyage ne doit pas endommager les applications non infectées ou le système en soi.

Produit testé

Le test a été effectué en août 2018. Pour ce faire, AV-TEST a utilisé la version disponible la plus récente du logiciel suivant au moment du test :

- SpyHunter de la société EnigmaSoft Limited

Méthodologie et cotation

Plate-forme

Tous les tests sont effectués sur des ordinateurs identiques équipés du matériel informatique suivant :

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

Le test a été effectué en août 2018. AV-TEST a utilisé la version disponible la plus récente du logiciel suivant au moment du test.

Méthode de test

L'essai de réparation a été divisé en dix étapes selon la méthode décrite ci-dessous :

1. **Système propre pour chaque modèle**. Les systèmes utilisés pour les tests ont été mis dans un état propre avant d'être exposés à un modèle de logiciel malveillant.
2. **Ordinateur physique**. Les systèmes utilisés pour les tests étaient de véritables ordinateurs physiques. Aucune machine virtuelle n'a été utilisée.
3. **Accès Internet**. Les ordinateurs avaient accès à Internet en tout temps afin de pouvoir utiliser et répondre aux consultations dans le nuage si nécessaire.
4. **Configuration du produit**. Tous les produits et les outils de réparation s'y rapportant ou les outils de restauration démarrables ont utilisé les paramètres préconfigurés par défaut.
5. **Infection des ordinateurs de test**. Un terminal en code natif a été infecté par une menace, puis redémarré. Il fallait s'assurer que la menace courait à plein régime.
6. **Familles de modèles et charges utiles**. Les modèles testés ne provenaient pas de la même famille et n'avaient pas les mêmes charges utiles.
7. **Réparation en utilisant toutes les capacités de produit disponibles**.

a. Tenter d'installer le produit de sécurité avec les paramètres par défaut. S'assurer que toutes les instructions spécifiques à la suppression du produit ont été respectées.
b. Si a. ne fonctionne pas, il faut tenter de résoudre le problème avec l'***outil de réparation autonome / outil de sauvetage*** (si disponible).
c. Si b. ne fonctionne pas, il faut tenter de résoudre le problème avec la ***solution de redémarrage*** autonome (si disponible) et de l'utiliser pour la réparation.

8. **Validation de la distance**. L'ordinateur a été inspecté manuellement pour valider la suppression correcte et la présence d'artefacts.
9. **Évaluation de la portée**. L'efficacité de l'outil et de la solution de sécurité dans son ensemble a été évalué à l'aide du système d'évaluation fourni.
10. **Réparation trop agressive**. Le test a également permis de déterminer l'agressivité d'un produit lors d'une réparation. Certains produits suppriment par exemple complètement le fichier host ou un tout un répertoire, même si cela n'est pas nécessaire pour une réparation réussie. Ce comportement va à l'encontre du produit.

Score d'efficacité

Des points sont attribués à chaque modèle testé selon le système suivant :

a. Suppression complète des logiciels malveillants (3)
b. Détection et suppression de logiciels malveillants en ne laissant que des traces inactives (2)
c. Détection d'une menace et suppression partielle, bien que les traces des logiciels malveillants soient toujours actives (1)
d. Pas de détection ni de suppression d'un logiciel (0)

Le score ne devait pas tenir compte des techniques effectivement utilisées pour supprimer le logiciel malveillant. Cependant, l'utilisation de toutes les techniques possibles était préconisée. Si un produit supprime les entrées se rapportant à un produit dans le fichier host et supprime également les infections de l'ordinateur, bien que le produit demeure fonctionnel et modifiable, il faut lui attribuer le maximum de points pour la réparation, même si les entrées d'autres fournisseurs de sécurité ne sont pas éliminées dans le fichier host.

Modèle

L'ensemble contenait 12 fichiers malveillants capables d'infecter Windows 10 (RS3, 64 bits).

Résultats des tests

La société EnigmaSoft Limited a parfaitement performé avec 100 % dans les deux sections de test. Les résultats des deux sections de test sont présentés à la figure 2.

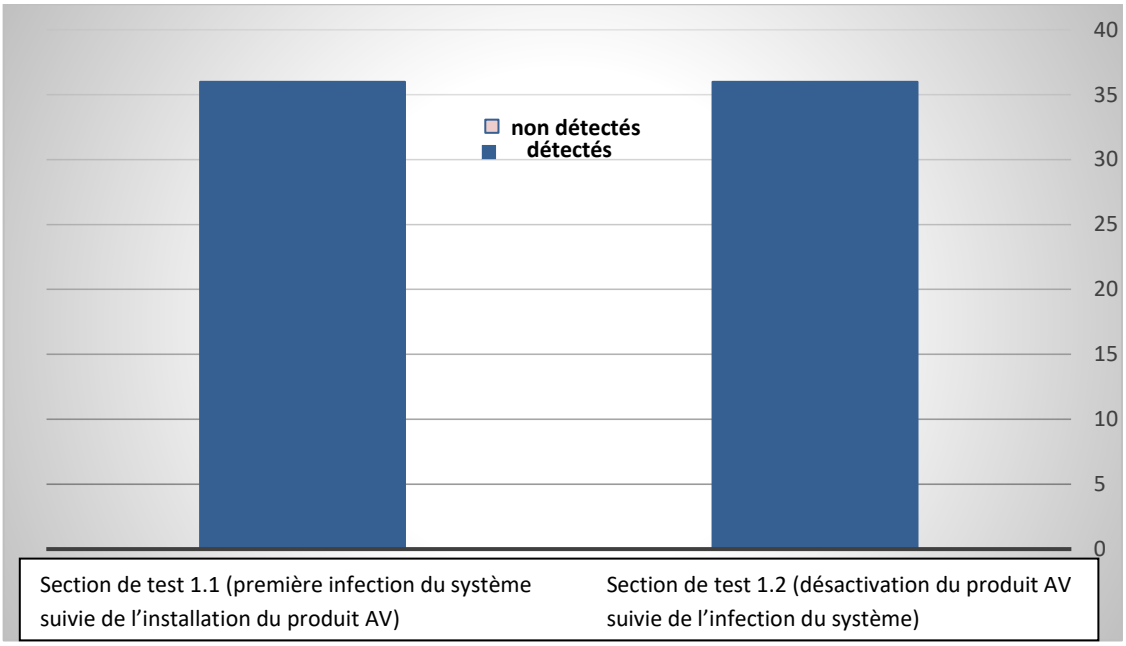
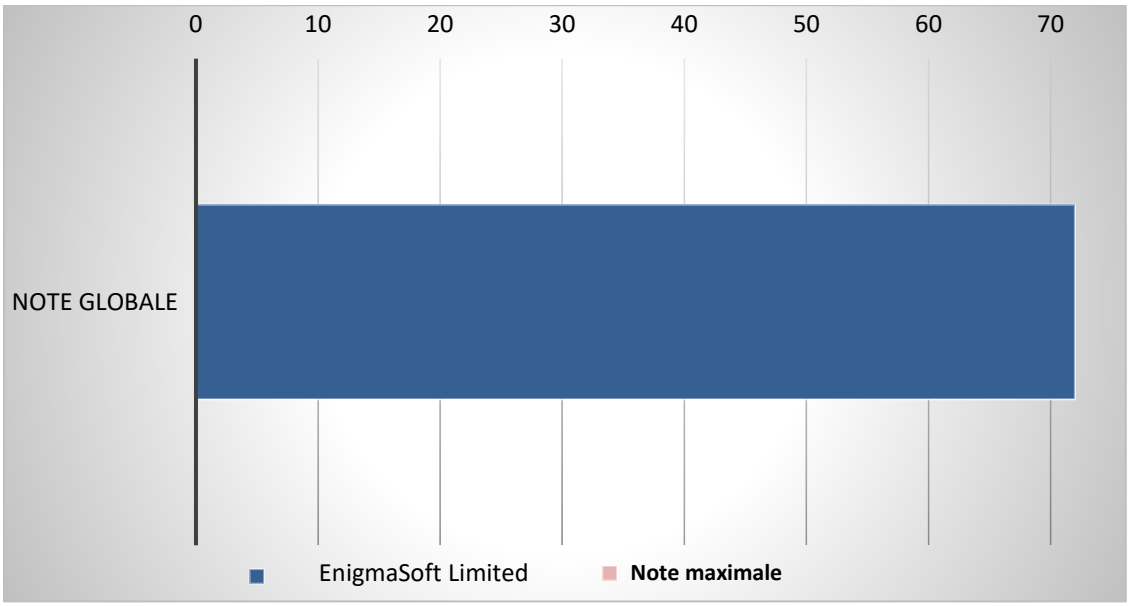


Figure 2 : Résultat de la réparation – sections d'essai 1.1 + 1.2

En termes de performance de suppression, SpyHunter a réussi à supprimer les 12 modèles testés. De plus, tous les artefacts et toutes les entrées du registre ont été parfaitement nettoyés.

Le score maximal pouvant être obtenu était de 72 points. Comme le montre la figure 3, la société EnigmaSoft Limited a obtenu le score exceptionnel de 72 points.



Annexe

Version du logiciel testé

Développeur, Distributeur	Nom du produit	Version du programme
EnigmaSoft Limited	SpyHunter 5	5.0.30.51

Liste des modèles utilisés pour le test de réparation

(SHA256)
0x0bf737607d46bfa4434a8d62b2376b9fdd4b013bb1614bd5f089fa332feef0b2
0x179cb0ba8030ee09e2e7d5be3a9d0f1b20663a5e1f49e8d1d876b3f76e088476
0x3c5fc8acd9a0ef88795d2592fee6a20be800a3874a40f672700bf23707ca9f82
0x4ff747afb05bc711742f3617d92735a8435eb16c8954dbfe1e558cb7b5de7c3d
0x5400e496f79ad8d09b6be069ca680af2e359f81625993e15fa52a09b1444f78b
0x6287b31e3681973ecfc969ce082cc195badd8f571ce057695a021c9227ee63d4
0x6abef4b7e1d91fc80c7f83cfebffa1ac129333c4acb8e7779bd646a1e66129c3
0x7e8a7fd6bb805f8bd42d30c17490b9bd0a9602485efcb708abfca3e1d5b16c01
0xa058357700d6bbec06232492c40a88487f57e343f7a7c6180582b4d83714f1bd
0xc3519c9fc77812b3ad088174729fc3f712de69505659f73e4d277af6b4ba31ab
0xe67ddfdfdca394eb8a4ebf7fe64c7dc7459df1b3b050e680ce94ab51a2e54c0c
0xf4e496f3a1d094eddf13a93e92e22dbc6a224aa8e8e8664fdf7fdbb4b456485c