# Rapport du test de Remediation

Ce test a été réalisé par AV-TEST GmbH sur demande de la société Enigma Software Group.
Rapport du : 19 mai 2016, actualisé le 24 mai 2016

## Résumé

En avril et mai 2016, AV-TEST a testé la performance des fonctions de *Remediation* (terme technique anglais concernant la détection, l'élimination et le nettoyage) de SpyHunter, un produit fabriqué par Enigma Software Group. Ce test a été exécuté sur un système Windows 7 (SP1, 64 bits) sûr et la même image disque a été utilisée sur plusieurs ordinateurs identiques.

Le corpus de programmes malveillants utilisé pour ce test de Remediation incluait 20 programmes malveillants et la procédure de test était composée de deux phases. Phase de test 1 : dans un premier temps, l'image disque a été infectée par un échantillon de programme malveillant. Dans un second temps, les testeurs ont essayé d'installer le produit de sécurité, d'analyser l'ordinateur et d'éliminer la menace identifiée. Phase de test 2 : la solution antivirus a été désactivée au début de cette phase de test consistant à infecter le système. Les testeurs ont ensuite réactivé l'antivirus et redémarré le système afin de garantir que tous les composants de la solution de sécurité ont bien été installés et activés. La dernière étape consistait à essayer de nettoyer le système et à effectuer une analyse supplémentaire du système.

Durant la première phase du test, SpyHunter a réussi à supprimer entièrement 19 des 20 programmes malveillants ce qui constitue un très bon résultat. Lors de la seconde phase du test, 16 des 20 programmes malveillants ont été éliminés ce qui peut encore être considéré comme une bonne prestation.

SpyHunter a su neutraliser les composants actifs des logiciels malveillants situés sur l'ordinateur. La plupart des fichiers restants sont des fichiers exécutables du maliciel qui ont été enregistrés sur le système sous « C:\Users\vtc\AppData\Roaming\ ». Dans un seul cas, SpyHunter n'a pas réussi à traiter les composants actifs du programme malveillant ce qui veut dire que le système est resté infecté.

## Aperçu

Étant donné que le nombre de menaces développées et répandues via Internet est en constante augmentation, le risque d'infection s'accroît en conséquence. Il y a encore quelques années, de nouvelles menaces étaient publiées tous les deux ou trois jours. Cela a radicalement changé et aujourd'hui, il faut compter plusieurs milliers de nouveaux programmes malveillants par heure.

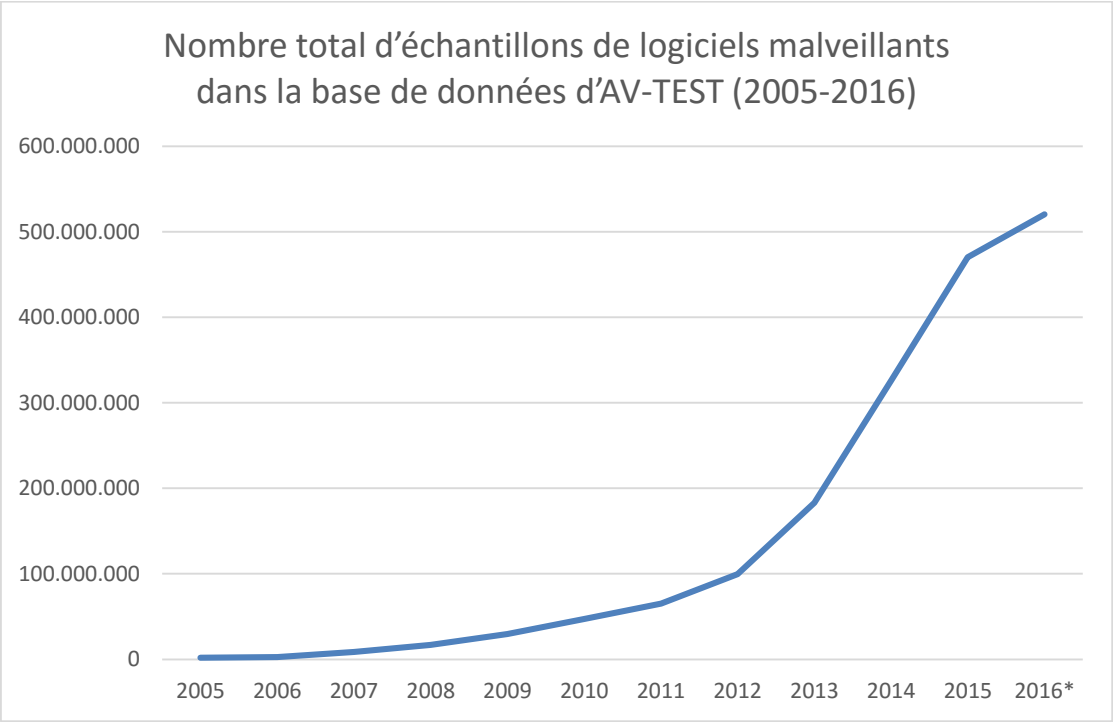



**Illustration 1 : Nouveaux échantillons de logiciels malveillants par an**

Tandis qu'AV-TEST avait collecté environ 170 000 nouveaux échantillons de programmes malveillants en 2000, le nombre de maliciels est passé à plus de 80 millions jusqu'en 2013 et ce chiffre continue d'augmenter en 2016 Cette progression est représentée par l'illustration 1. La base de données d'AV-TEST compte actuellement plus de 500 millions d'échantillons de programmes malveillants.

En tenant compte de cette évolution, on peut supposer que la simple gestion d'une telle quantité de nouveaux programmes malveillants peut déjà poser problème. Or les fabricants de logiciels de sécurité doivent y arriver pour protéger leurs clients. Il n'est pas pourtant toujours possible de protéger un ordinateur à temps contre les menaces. Même lorsqu'un logiciel antivirus actualisé est installé sur l'ordinateur, ce dernier peut tout de même être infecté si plusieurs heures s'écoulent entre la découverte d'un nouveau maliciel et la mise à disposition de signatures adaptées. Il peut alors déjà être trop tard dans certains cas. Les infections peuvent conduire à des dommages financiers pour les utilisateurs, par exemple si des données confidentielles sont volées ou si l'ordinateur ne peut plus être utilisé efficacement, jusqu'à ce que le programme malveillant soit entièrement éliminé du système.

Voilà pourquoi l'opération de nettoyage devient de plus en plus importante lorsqu'un ordinateur infecté doit rapidement redevenir opérationnel. Lors de la suppression du logiciel malveillant, il est essentiel que la procédure de nettoyage se déroule de manière fiable en ce qui concerne deux points :

1. Le programme malveillant et tous les composants du maliciel doivent être éliminés tandis que les systèmes infectés doivent être restaurés.
2. Les programmes sûrs ainsi que le système lui-même ne doivent pas être endommagés par le processus de nettoyage.

## Produit testé

Lors du test réalisé en avril/mai 2016 par AV-TEST, les testeurs ont respectivement utilisé la version la plus récente du logiciel suivant :

- SpyHunter d'Enigma Software Group

## Méthode de test et évaluation

### Plateforme

Tous les tests ont été effectués 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)

En tant que système d'exploitation, les testeurs ont utilisé Windows 7 (SP1, 64 bits) avec tous les patchs et correctifs de type hotfix disponibles jusqu'au 1er mai.

### Méthode de test

**Le test de Remediation a été effectué en dix étapes en respectant la méthode suivante :**

1. **Système propre pour chaque programme malveillant**. Les systèmes d'essai ont respectivement été nettoyés et restaurés avant d'être infectés avec un seul échantillon de logiciel malveillant.
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**. Les ordinateurs avaient à tout moment un accès complet à Internet pour pouvoir consulter leur cloud en cas de besoin pendant le test.
4. **Configuration des produits**. Pour tous les produits et les outils de Remediation correspondants ou les outils de récupération amorçables, les testeurs ont utilisé les paramètres standards, conformément à la configuration d'origine.
5. **Infection des ordinateurs d'essai.** Un système natif a été infecté par un programme malveillant puis il a été redémarré. Cela avait pour but de garantir que le maliciel était complètement fonctionnel.

6. **Familles de programmes malveillants et maliciels (payloads).** Lors du choix des échantillons de test, les testeurs ont veillé à ce qu'ils n'appartiennent pas à la même famille de programmes malveillants et n'utilisent pas le même maliciel.
7. **Remediation.** Durant la procédure de Remediation, toutes les fonctions du produit disponibles devaient être utilisées.
    a. Les testeurs devaient essayer d'installer le produit de sécurité avec les paramètres standards. Les indications du produit devaient entièrement être respectées 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.** La vérification de l'ordinateur a ensuite été réalisée manuellement en contrôlant l'élimination complète ou la présence de fragments de fichiers.
9. **Évaluation de la performance lors de la suppression du logiciel malveillant.** La performance de l'outil et de la solution de sécurité complète a été évaluée en utilisant un système de points défini.
10. **Conséquences excessives de la Remediation.** Les testeurs ont également vérifié dans quelle mesure les solutions de sécurité utilisaient des méthodes agressives pour nettoyer un système. Il existe par exemple des produits qui suppriment complément des fichiers hosts voire des répertoires entiers, alors que ces étapes drastiques ne sont pas nécessaires pour que les mesures de Remediation atteignent leur but. L'utilisation de telles méthodes a donné lieu à une déduction de points lors de l'évaluation.

## Évaluation de l'efficacité

Pour chaque échantillon de programme malveillant testé, des points ont été attribués en suivant la grille suivante :

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 un produit supprime les entrées dans le fichier hosts correspondant à ce même produit, mais qu'il laisse derrière lui un ordinateur propre et que la fonctionnalité ainsi que la mise à jour du produit restent assurées, alors ce produit devrait obtenir la note maximale 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 incluait 20 programmes malveillants avec lesquels il était possible d'infecter le système Windows 7 (SP1, 64 bits).

## Résultats de test

Durant la première phase du test, le produit d'Enigma Software Group a obtenu un très bon résultat et n'a laissé des fragments de fichiers sur le système que dans un seul cas.  SpyHunter a atteint la note de 55/60 lors de la deuxième phase de test. Les deux résultats de test sont représentés dans l'illustration 2.

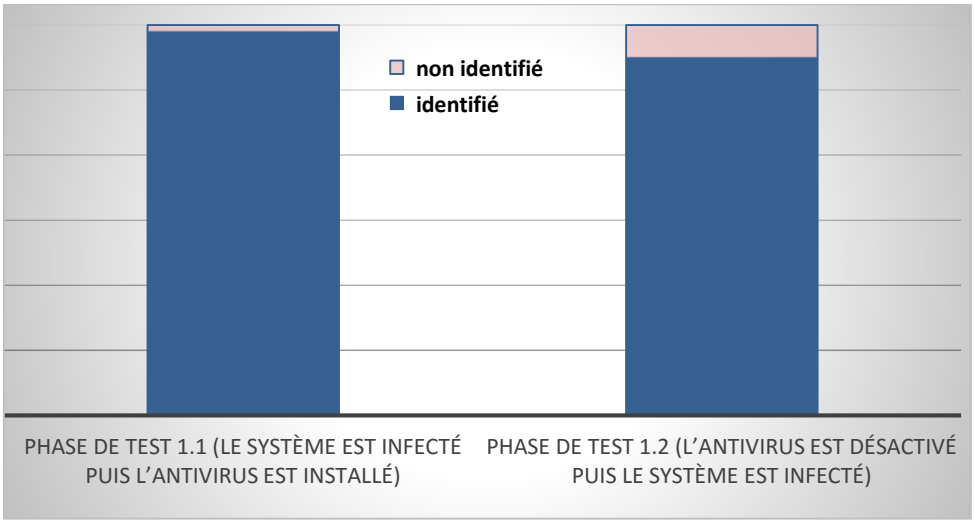
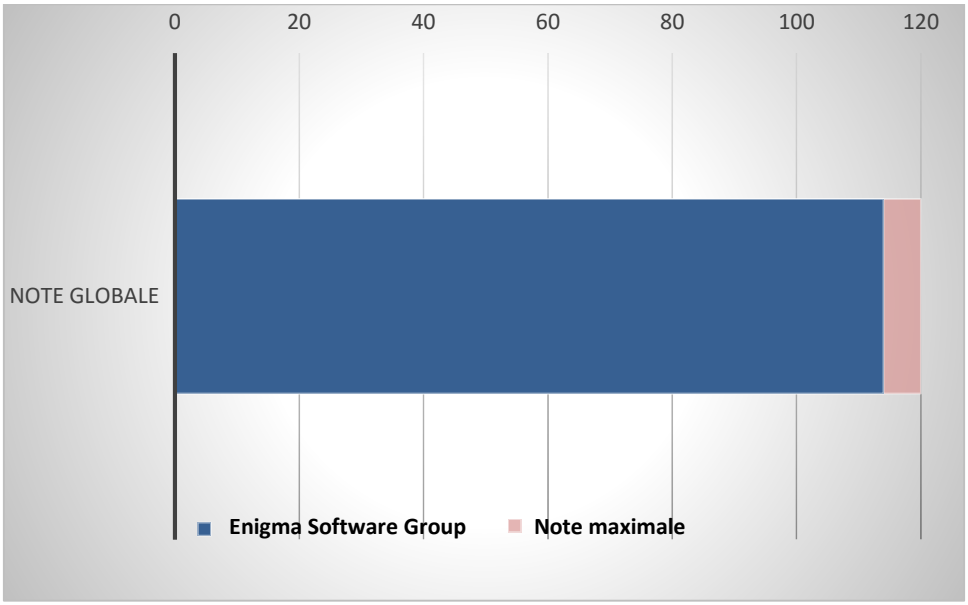



Illustration 2 : Résultat de la Remediation – phases de test 1.1 et 1.2

La note maximale à atteindre durant ce test était de 120/120. La note globale obtenue par Enigma Software Group était de 114/120, voir l'illustration 3. Concernant la performance réalisée lors de l'opération de nettoyage, la deuxième phase du test a démontré que certaines infections ne peuvent pas entièrement être éliminées. SpyHunter a supprimé les composants actifs du programme malveillant sur l'ordinateur. La plupart des fichiers restants étaient des fichiers exécutables du maliciel qui ont été enregistrés sur le système dans le dossier « C:\Users\vtc\AppData\Roaming\ ». Dans un seul cas, SpyHunter n'a pas réussi à traiter les composants actifs du programme malveillant et le système est donc resté infecté.

Durant la phase 1.1, le produit a cependant atteint un très bon résultat en ne réalisant qu'une seule erreur.




# Annexe

## Informations sur la version testée du logiciel

| Développeur, fabricant | Nom du produit | Version du programme | Moteur / Version de signature |
|---|---|---|---|
| **Enigma Software Group** | SpyHunter | 4.22.4.4657 | 2016.04.26v1 |

## Liste des échantillons de logiciels malveillants utilisés (test de Remediation)

| (SHA256) |
|---|
| 0x026bb4f1db988785351ab7d3889c3b322b69398042ae7d52e8e4740e9618eec1 |
| 0x02c6d5aeb2ab78f781d72ba60d6f7ff7f5928d47a26ca8dcc4a5c1398850e62a |
| 0x1e3a054ed8051c06a78dc37922c2297a5c3da51a84beb99bc2a487381851ede4 |
| 0x1eaef8613ab91e13484646dcb61f5721858066850124a7de5ffce2767bad2ff0 |
| 0x2164f112693ab13ef45f159a0444ea64b94942518e829aa55b7d277722b87179 |
| 0x2656834a0380bc4c830daef09cfafd038fd5e7727303b09170a8fe37c35a1e34 |
| 0x32f0a426e80fb26d098a22bf624d3fb21342372a2135337e9f06ffc4af442846 |
| 0x3436da965e7fdbde9a9836acc712ff437d5e7c49a821366451308e11555924f1 |
| 0x406ada699acb288bfa2755a9ebe807aa86b90f475b332799f925d85b0d195c61 |
| 0x443660d22f3c4bfdb2c2ff4d3e25dafd01f7002bcde53ad7bac8b777e700123a |
| 0x56e24a3dc8b07ea6e08e3d4e4ba96e1e9101aca932523c34350fafbcff02ac85 |
| 0x5c596c8afd4656946f0a9741f2be4bb088dda26f1ddcf41eb8c427fbb6d1c3ec |
| 0x60eeb661ad33aa50d9ce1355f9e70afde317411f81e7d0890f38ae28ea79b1b4 |
| 0x659896ed065fd59fb843022022a7796ec76620000c7c29a009c7f399898845cb |
| 0x70b64248b23182827c8f52be598a4a10bf0784dc1d97e8721a528ec9cec3acc9 |
| 0x76c9c0758ea91e38f8cf47fcc01d597a213eed5f2001ff5f8f7763df236e6baf |

| |
|---|
| 0x882ac415de83252554349e3221c7bb5028da1db36b55f196f3cf0a9861ef4597 |
| 0x95a1d1207cc0a75eaaeef1a985b8c8bbe15a314c43f2b4d593033cf426bb9212 |
| 0x9a679f8745896abd8fbe1586eabc3690858f6d966f4a9c5eb52b6f3b64cd35dd |
| 0xa3efd281adaf729075ee466793fe2a2a6972b746d15e9578355957fc7e7daee2 |


Tél. +49 391 6075460, fax +49 391 6075469, Internet http://www.av-test.org