Rapport du test de Remediation

Ce test a été réalisé par AV-TEST GmbH sur demande de la société Enigma Software Group.
Rapport du : 15 février 2017, actualisé le 15 février 2017

Résumé

Au mois de février 2017, l'institut AV-TEST a testé la performance des fonctions de Remediation (terme technique anglais concernant la détection, l'élimination et le nettoyage) 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.

20 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.

Que ce soit durant la phase de test 1 ou 2, SpyHunter a réussi à éliminer avec succès l'intégralité des 20 programmes malveillants et a donc fait preuve d'une excellente performance dans les deux cas.

Ce logiciel est parvenu à neutraliser tous les composants actifs des malwares ainsi qu'à supprimer tous les fragments de fichiers restés au sein du système.

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.

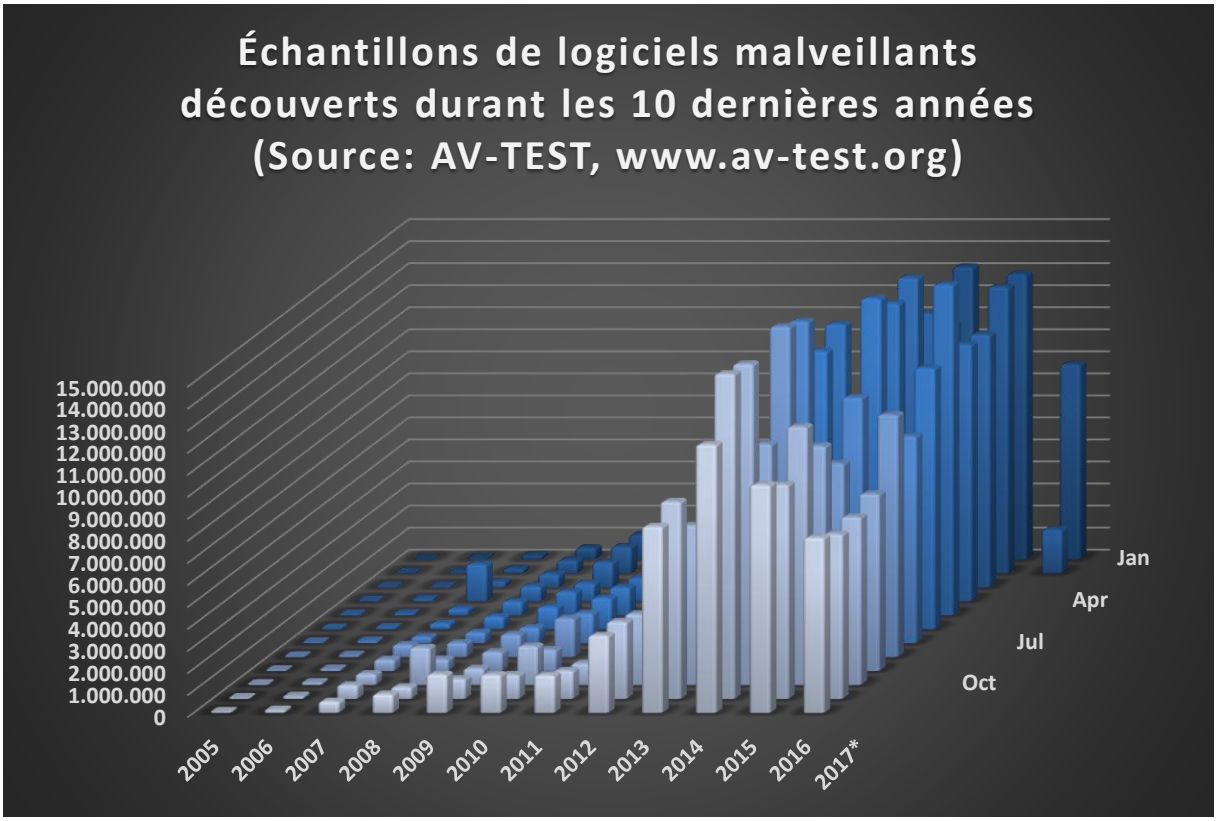


Illustration 1 : Nouveaux échantillons de logiciels malveillants par an

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 600 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 janvier 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 20 programmes malveillants permettant d'attaquer le système Windows 7 (SP1, 64 bits).

Résultats de test

Que ce soit lors de la première ou de la deuxième phase du test, le produit d'Enigma Software Group a atteint la meilleure note possible grâce à un taux de 100 %. Les résultats des deux phases du test sont représentés sur l'illustration 2.

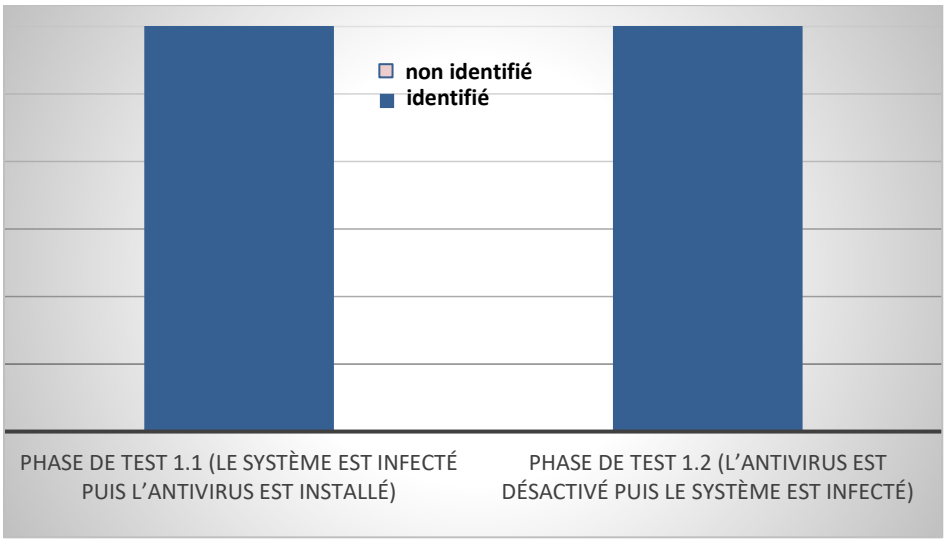
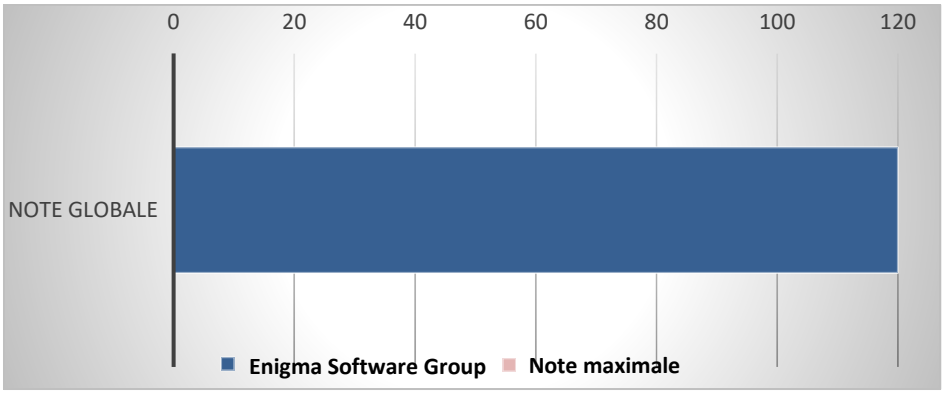


Illustration 2 : Résultat de la Remediation – phases de test 1.1 et 1.2

La note maximale pouvant être attribuée par les testeurs était de 120/120. Comme le montre l'illustration 3, le produit d'Enigma Software Group a obtenu une note globale de 120/120. Le contrôle de la performance de nettoyage dans la phase de test 1.2 a démontré que SpyHunter a réussi à nettoyer le système dans son intégralité.

Ce logiciel a également obtenu un résultat parfait lors de la phase de test 1.1 puisqu'il a atteint un taux de nettoyage du système infecté de 100 %.



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	4.24.3.4750	2017.01.17v01

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

(SHA256)
0x0248aef55dd424770217a568e6d6e621b08f010faecc3bdc889e815bdba562b7
0x2e9b4aa0d8f1fe0c8f75faaad8fea213cc982678925e883199d4e73316830e27
0x379d26795c02cd028f5fc33210b598228a8f23f9926bac365668e1044c30f496
0x3963f5795ab1c34ffe7ae23424b82631d24908c3c25bb5b703fba8403f63e7a8
0x496badd81af03f9a74f3fc321225d8376dc6aff613e2d2e4328fabf33fbe3853
0x4e5212dc24b5d6b3b6281db2ed33bc8b271151c11a1a7b6fc16d5a843aef7bc4
0x4f5bff64160044d9a769ab277ff85ba954e2a2e182c6da4d0672790cf1d48309
0x534ceed806ec84ae75fdd2e3f1c837cb1e263f52e03a73366a199f45456acfc2
0x5847e0b50f7279000e7335af0b0925b413718810cf5591d8ea253ae55893a197
0x6bf17b1dc8eb3b0ae6412bd2d71fe73832e9b4c7ba259d9d13e46427401c4145
0x73e7b43fed5fe22d58ba0c36080eb70f00640ea9e615d8e5ce1785d76d1f2a76
0x814d8c756520ebc86fcf8f544a352d17bb7636333a206c27bc0710320fabd279
0x90c1e0eb0eb37300e2177b465b9289daa910f2df2a6b5e63f3504958f7a71bc8
0x931339d73c08813699f40ff613083fc393e17fe99c1bdbdb2ea8038816b1c289
0xb3cf3567fab18b8a39277b33d0a89b2f0f79a7f2a3583ad663fd5d80f6c49546
0xd32ee2cf13429517274cda35c341861ab9d947533163da3154b74ca40b8161f6
0xd861451d5ee19419ac829bdba0622ce9e1edcc6ef9f1a6f5257ee0744771ae76
0xece08e1c4d119df6217853b7ef22bff31e0c58f9d204878b2e28e6ff9e1ba782
0xefbd13ee753e4b879616a020bdb77212abdf637e6c288ab48672276bb69d24d2
0xf93c7b95df816eed946a5028f44f3e9185baf63ccbcf66047331cfb3b5a2654a