Rapport du test de Remediation

Ce test comparatif a été réalisé par AV-TEST GmbH sur demande de la société Enigma Software Group.
Rapport du : 20 août 2018, actualisé le 20 août 2018

Résumé

Au mois de juillet 2018, 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 10 (RS3, 64 bits) non infecté. La même image disque a ensuite été utilisée sur plusieurs ordinateurs de même type.

12 programmes malveillants différents ont été employés lors de ce test de Remediation et la procédure de test était divisée en deux phases. Phase de test 1 : Durant la première phase, 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. Phase de test 2 : Afin de pouvoir infecter le système, la solution antivirus a été désactivée au début de cette phase. 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 supprimer entièrement 10 des 12 programmes malveillants ce qui constitue un très bon résultat. Le logiciel d'Enigma est également 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.

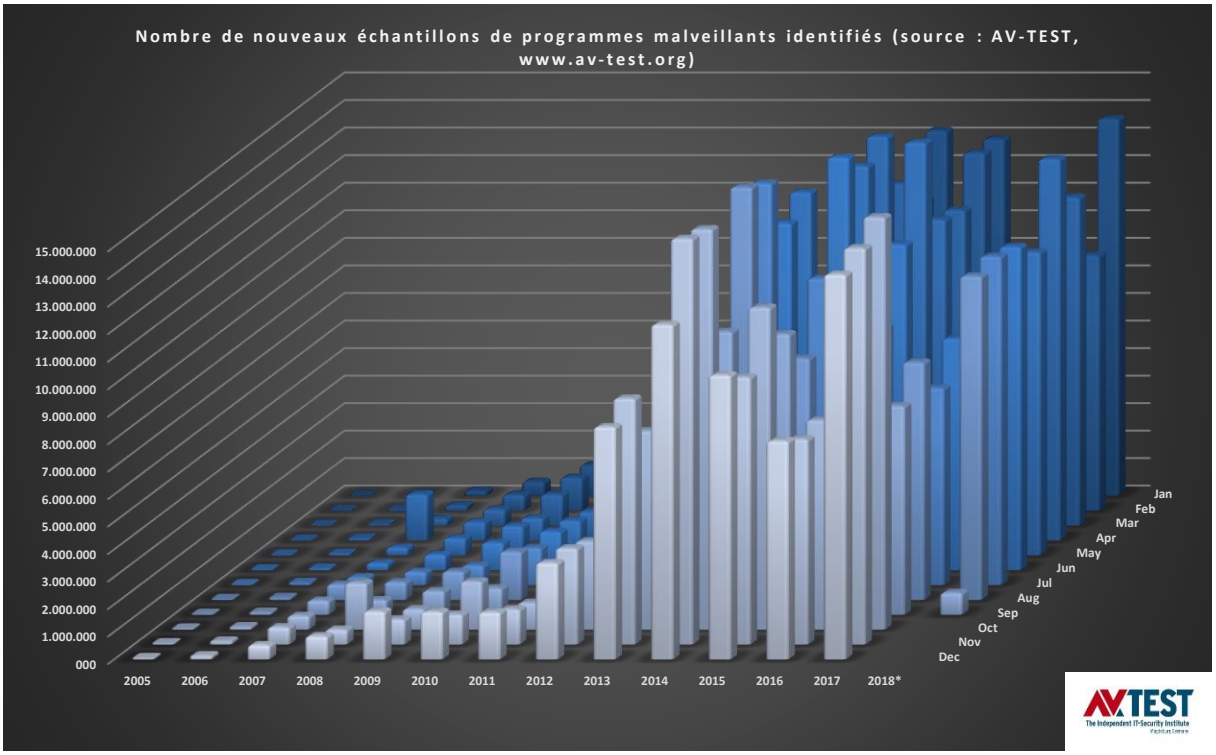


Illustration 1 : Nouveaux échantillons de logiciels malveillants par an

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 dans les années suivantes. À l'heure actuelle, plus de 800 millions d'échantillons de logiciels malveillants sont répertoriés dans la base de données d'AV-TEST, et au cours du premier semestre de cette année les systèmes de détection d'AV-TEST ont registré près de 10 millions de nouveaux programmes malveillants par mois

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 2018 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 10 (RS3, 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 4 juin 2018.

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 12 programmes malveillants permettant d'attaquer le système Windows 10 (RS3, 64 bits).

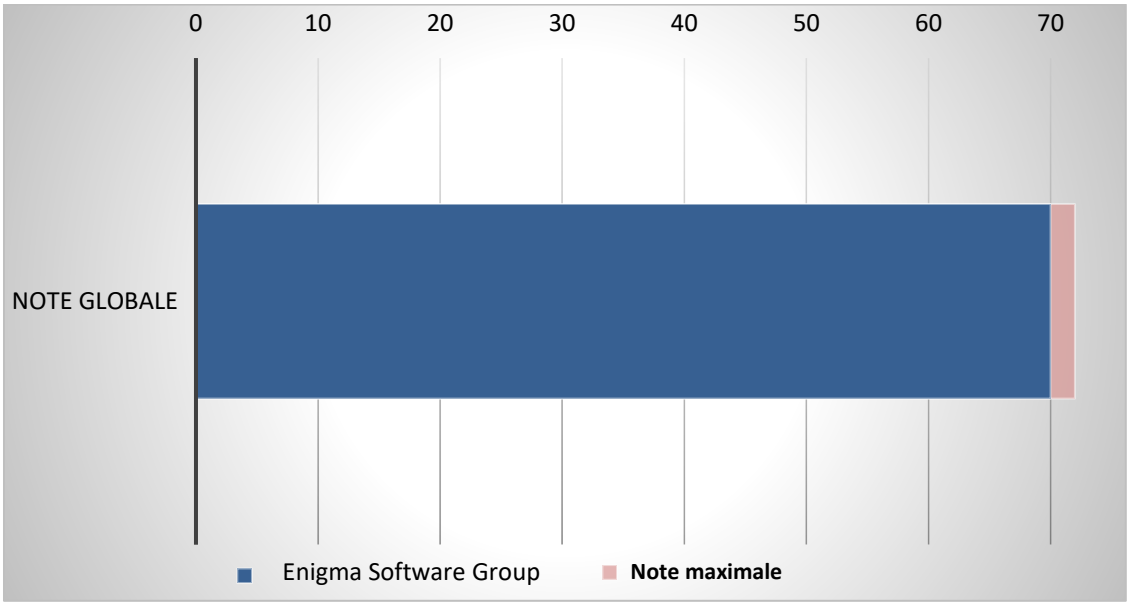
Résultats de test

Que ce soit lors de la première ou de la deuxième phase du test, le produit d'Enigma Software Group a atteint un très bon résultat grâce à un taux de 97,2 pour cent.
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

Le contrôle de la performance de nettoyage a démontré que SpyHunter a réussi à nettoyer le système dans son intégralité dans 10 cas sur 12. Le programme n'a laissé qu'une entrée du malware dans le registre lors de chaque phase du test, ce qui lui a valu une légère déduction de points.

La note maximale pouvant être attribuée par les testeurs était de 72. Comme le montre l'illustration 3, le produit d'Enigma Software Group a obtenu une note globale de 70.



Annexe

Informations sur la version testée du logiciel

Développeur, fabricant	Nom du produit	Version du programme
Enigma Software Group	SpyHunter 5	5.0.30.51

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

(SHA256)
0x10864dff8bcea96f842f6642bca59199b677e28e6e174c3e4d7b65391b0698b0
0x2942841f850c59c1f7bedd1922aca54c886bad1eb51b90b32af7d6b6b6e5cab4
0x5ba58146b785d5e72993430d95960486cbf9bf9429e5e3bf4fa2fe2e88f4e250
0x69bb101c4c53fe2a87ed2200dd46b7d82d92c86943e47a31ce7922455b92d345
0x70179938e6c056df16b1403615cc553a10a90297601446f95d6ad004ca1e29eb
0x86958f2f177eed14d6164d48a18cb15c12516bdb59f1125471d966f3e212b989
0x980f254b3954b3d7ded9772cad328d6872491fbd645ac3dae3d277620cfb88b7
0xac186a20bbec078f08788cc8a4a746de0139a061a6d2588787d217f019c2eb90
0xb3548b485e919e043b935b071ad54f37e1c996046fcfbefae51d76a437ee6a93
0xd8a3f066a3b961b4c8623e0d30e3e867fd7a1c9187aa396de8457df70b602efe
0xe275e10bea80834252aea1b5dba9a817b278b5c4a6d0594b01b1605de0b66f79
0xf92dd910c0c00e5924a27bbffcdb303e5f724b3caf540e844c3f82a291cc7a30