CHECK POINT SANDBLAST ZERO-DAY PROTECTION : LA MEILLEURE PROTECTION À TOUS LES NIVEAUX

« LE NOMBRE DE TÉLÉCHARGEMENTS DE LOGICIELS MALVEILLANTS INCONNUS A BONDI DE 2,2 PAR HEURE EN 2013 À 106 PAR HEURE EN 2014 »

LA MONTÉE DES LOGICIELS MALVEILLANTS CONNUS ET INCONNUS

Logiciels malveillants. C'est un terme qui suscite beaucoup d'attention aujourd'hui de la part des journalistes, des chefs d'entreprise et des experts informatiques. Dans le monde de la sécurité réseau, les logiciels malveillants se répartissent en différentes catégories : logiciels publicitaires, logiciels espions, virus, vers, chevaux de Troie, rootkits, portes dérobées, enregistreurs de frappes au clavier, logiciels rançonneurs et logiciels de détournement de navigateur. Même si ces différents types de logiciels malveillants affectent les systèmes différemment,[1] ils partagent souvent des objectifs communs : dérober des données confidentielles, accéder à des applications ou des privilèges non autorisés, et/ou perturber les activités.

Au début de l'année 2014, les agences de presse du monde entier ont qualifié 2013 « d'année des failles ». Ce fut jusqu'à ce que 2014 se termine. Selon un rapport d'AV-Test de janvier 2015,[2] un institut indépendant de recherche en sécurité informatique, les incidents dus aux logiciels malveillants ont augmenté de 72 % entre 2013 et 2014. Une plus grande quantité de logiciels malveillants a été découverte durant les deux dernières années que durant les 10 années précédentes combinées.[3]

La complexité des logiciels malveillants augmente à mesure que les cybercriminels perfectionnent leurs techniques d'intrusion et de masquage de leur signature, et font appel à différentes méthodes d'attaque. Ce que nous appelons les attaques zero-day, qui exploitent des vulnérabilités jusqu'à présent inconnues, et les nouvelles variantes jusqu'à présent inconnues de logiciels malveillants existants, sont les plus difficiles à stopper. Ces logiciels malveillants sont souvent même capables de contourner les systèmes de prévention d'intrusions et les antivirus les plus à jour, ces derniers ne pouvant généralement ni reconnaître ni bloquer les nouveaux logiciels malveillants inconnus. Selon le Rapport Sécurité 2015 de Check Point, le taux de téléchargement de logiciels malveillants inconnus est passé de 2,2 par heure en 2013 à 106 par heure en 2014.[4]

APPROCHES DE SÉCURITÉ CONTRE LES ATTAQUES ZERO-DAY

Selon le site Internet Live Stats, plus de 2,4 millions d'emails sont envoyés chaque seconde.[5] Au cours des 3 premiers mois de l'année 2015, environ 59,2 % de ces emails étaient du spam.[6] Comme les pièces jointes sont la méthode préférée pour transférer des fichiers, et comme de nombreux utilisateurs estiment qu'ils peuvent ouvrir les pièces jointes provenant d'expéditeurs connus en toute sécurité, la boîte de réception est devenue une cible de choix pour les attaques. La protection de la messagerie pouvait se résumer à ces quelques conseils : installer un bon programme antivirus, le garder à jour, et éviter les fichiers et les sites suspects. Malheureusement, ces sages conseils sont ***nécessaires mais pas suffisants*** pour se protéger contre les logiciels malveillants modernes.

Des logiciels malveillants peuvent se cacher dans des exécutables, des documents courants et des pages web. Les dangers des attaques intégrées à des exécutables sont bien connus depuis de nombreuses années. Grâce à cette prise de conscience, la plupart des utilisateurs suppriment les emails contenant des pièces jointes exécutables. De nombreuses entreprises ont également mis en place des politiques de sécurité réseau qui retirent les pièces jointes exécutables des emails. Les attaques récentes se font à travers des documents apparemment sans danger, contenant des éléments actifs tels que des macros, des scripts et des objets dynamiques, ce qui les rend beaucoup plus susceptibles d'être ouverts. Donc, **les documents constituent aujourd'hui l'un des plus grands risques** pour les entreprises.

« LES DOCUMENTS REPRÉSENTENT DÉSORMAIS LE RISQUE LE PLUS IMPORTANT POUR LES ENTREPRISES »

En 2014, 86 % des entreprises ont accédé à un site web malveillant et 63 % des entreprises ont téléchargé un fichier malveillant.[7] Dans tous les services, des ressources humaines aux ventes et aux achats, les employés doivent régulièrement ouvrir les documents de candidats à l'embauche, de clients et de fournisseurs, et prendre le risque d'exposer leur entreprise à des logiciels malveillants intégrés aux documents.

Le bac à sable est une méthode couramment utilisée pour bloquer ces types de logiciels malveillants les plus récents. Il analyse les fichiers avant qu'ils n'entrent dans votre réseau en émulant un système d'exploitation standard dans un environnement restreint et isolé de votre réseau de production. Les fichiers sont manipulés de différentes manières, comme si un utilisateur réel les ouvrait. Le système est alors attentif à tout comportement au-delà de ce qui est normalement attendu. En combinant un antivirus à jour avec l'analyse comportementale et l'analyse statique, le bac à sable fournit une protection robuste contre les exécutables potentiellement malveillants. Le bac à sable traditionnel effectue l'analyse comportementale pendant l'exécution tandis que l'analyse statique étudie le code de l'exécutable en profondeur.

Les facteurs clés à considérer dans le choix d'une bonne solution de bac à sable comprennent :

- Détection et blocage des attaques
- Résistance aux techniques d'évasion
- Détection rapide et efficace
- Prise en charge des types de fichiers courants
- Prise en charge des objets web tels que Flash

L'analyse d'un large éventail de types de fichiers (.doc, .xls, .ppt, .pdf, .exe, .zip, .rar, etc.), y compris les fichiers d'archivage, améliore le taux de blocage des contenus malveillants d'une couche de sécurité. Si votre solution de bac à sable actuelle ne traite qu'un nombre limité de types de fichiers, vous êtes potentiellement exposé, car les cybercriminels intègrent des logiciels malveillants dans tous les types possibles de fichiers courants. Lorsqu'il est complété par un agent de transfert de message (MTA), le processus de prévention des menaces retient, et même modifie, les emails jusqu'à ce que l'analyse en bac à sable soit terminée. Ainsi, il empêche les logiciels malveillants de franchir la frontière du réseau et d'atteindre les utilisateurs finaux.

L'inspection des fichiers et leur nettoyage avant qu'ils n'entrent dans un réseau devrait faire partie des meilleures pratiques. En réalité, elle est relativement récente. Leur facilité de mise en œuvre et leur impact minimal sur l'expérience utilisateur ont rendu les technologies de bac à sable populaires auprès de nombreuses entreprises. De plus en plus d'entreprises comptent même les ajouter à leurs futures stratégies de sécurité. Malgré le déploiement de solutions de bac à sable, les cybercriminels continuent de développer des techniques de contournement, parfois simples et parfois complexes, pour empêcher la détection des logiciels malveillants. Aujourd'hui, certaines des techniques de contournement de bac à sable les plus fréquentes sont :[8]

- **Le retardement de l'exécution** via une minuterie qui repousse l'exécution du code malveillant de plusieurs minutes/heures après l'ouverture initiale du fichier
- **La recherche d'indicateurs de machines virtuelles** pour identification du bac à sable, tels que des variables dans la base de registre, des processus en cours d'exécution ou la capacité du disque, et déploiement sur des appareils physiques uniquement
- **La recherche d'activités humaines** telles que le défilement des pages, les clics et les mouvements de la souris, qui sont difficiles à reproduire dans un environnement virtuel

Les fournisseurs de technologies de bac à sable créent constamment de nouvelles manières de détecter les techniques récentes de contournement et d'empêcher les logiciels malveillants de pénétrer dans les réseaux. Cependant, les protections contre les techniques de contournement sont encore souvent elles-mêmes détectées par les logiciels malveillants et la lutte pour rester en avance sur les pirates se poursuit. Une fois que les cybercriminels savent qu'ils sont surveillés, peu importe la qualité de la technologie de bac à sable traditionnelle ; des cybercriminels intelligents travaillent à l'éluder. Par conséquent, une défense encore plus avancée est nécessaire.

EST-CE QUE VOTRE BAC À SABLE :

- ✓ *Détecte et bloque les logiciels malveillants ?*
- ✓ *Dispose de fonctionnalités avancées de protection contre les méthodes de contournement ?*
- ✓ *Détecte rapidement et efficacement ?*
- ✓ *Prend en charge un large éventail de types de fichiers, y compris les fichiers d'archivage ?*
- ✓ *Prend en charge les objets web tels que Flash ?*

ANATOMIE D'UNE ATTAQUE DE LOGICIEL MALVEILLANT NON-EXÉCUTABLE

Les attaques de logiciels malveillants non-exécutables sont un des vecteurs d'attaque les plus efficaces car de nombreuses entreprises limitent le téléchargement de fichiers exécutables. Toutefois, des documents tels que Microsoft Word, PowerPoint ou Adobe PDF, entrent et sortent constamment des entreprises. Ces formats prennent en charge des contenus dynamiques tels que des macros et des scripts, qui peuvent être mis à profit pour exploiter des vulnérabilités connues. De nombreuses attaques ciblées et avancées commencent par une attaque de phishing pour conduire leurs victimes à ouvrir des documents d'apparence légitime, conçus pour exploiter une certaine vulnérabilité et infecter leur système voire le réseau tout entier. Par conséquence, il est essentiel de se protéger contre les attaques qui peuvent être introduites par des fichiers non-exécutables.

Il existe des milliers de vulnérabilités dans les logiciels. La plupart sont adressées par des correctifs, qui ne sont cependant pas toujours appliqués à tous les systèmes. Et il existe des millions de variantes de logiciels malveillants qui sont activées en résultat de l'exploitation de ces vulnérabilités. L'armée de l'air américaine définit les vulnérabilités dans son analyse Les trois principes de la cybersécurité comme étant « la combinaison de trois éléments : une susceptibilité ou une faille du système, l'accès des agresseurs à la faille, et la capacité de l'agresseur de l'exploiter. »[9] Avec cette définition à l'esprit, une attaque de logiciel malveillant typique comporte quatre étapes :

- **Découverte d'une vulnérabilité :** Chaque attaque commence par la découverte d'une ou plusieurs vulnérabilités, soit dans le système d'exploitation soit dans une application populaire telle qu'un navigateur ou un lecteur de PDF. L'exploitation de ces vulnérabilités permet aux cybercriminels de déclencher une attaque.
- **Utilisation d'une méthode d'exploitation :** L'exploitation des vulnérabilités permet aux agresseurs d'utiliser le programme qu'ils injectent pour manipuler le système cible et exécuter du code malveillant. Cela nécessite de surmonter les contrôles de sécurité mis en place par le système d'exploitation et le CPU, tels que la *prévention de l'exécution des données* (DEP) et la *distribution aléatoire de l'espace d'adressage* (ASLR). Seule une poignée de méthodes d'exploitation existe, et de nouvelles méthodes voient très rarement le jour.
- **Utilisation d'un code shell :** Un code shell est un petit programme généralement intégré à la page web ou le fichier qui a initié l'attaque. Il est chargé de récupérer le logiciel malveillant et le déposer ensuite dans le système infecté.
- **Exécution du logiciel malveillant :** L'infection se produit suite à l'exécution du logiciel malveillant. C'est à cette étape que les techniques de contournement sont utilisées pour empêcher le déploiement du logiciel malveillant dans le bac à sable.

Un bac à sable avancé disposant de fonctionnalités d'analyse au niveau du CPU détecte ces méthodes en examinant attentivement l'activité du CPU et le flux d'instructions exécutées. Cette analyse est effectuée au niveau du code d'assemblage où l'exploitation se produit. Il est alors pratiquement impossible pour les pirates d'échapper à la détection par l'emploi de tactiques de contournement. La vitesse et l'efficacité des analyses au niveau du CPU intégrées au bac à sable en font la meilleure technologie de détection des menaces inconnues, y compris les attaques zero-day.

CHECK POINT SANDBLAST ZERO-DAY PROTECTION

Les entreprises exigent non seulement une solution de pointe contre les menaces, mais ont également besoin d'une méthode de protection simple, rapide et à toute épreuve. Les logiciels malveillants doivent être éliminés avant même qu'ils n'aient la possibilité d'atteindre les employés. Check Point SandBlast Zero-Day Protection élimine les menaces à l'aide de deux technologies innovantes :

- Un bac à sable avancé avec analyse approfondie au niveau du CPU et inspection au niveau du système d'exploitation pour empêcher les pirates d'échapper à toute détection, et proposer le taux de blocage le plus élevé de logiciels malveillants
- L'extraction des menaces livre rapidement des contenus sains en fournissant une version reconstruite des documents entrants

Le bac à sable avec analyse approfondie au niveau du CPU détecte les infections dans les fichiers de données lors de la phase d'exploitation de vulnérabilité, tandis que l'inspection au niveau du système d'exploitation détecte les attaques dans les fichiers exécutables et les fichiers de données. Ces deux technologies offrent le taux de blocage des menaces le plus élevé. Les fonctionnalités d'extraction des menaces intégrées au bac à sable fournissent une protection immédiate contre les attaques zero-day, en livrant rapidement des versions reconstituées et saines des documents entrants pendant que l'analyse en bac à sable est effectuée en arrière-plan.

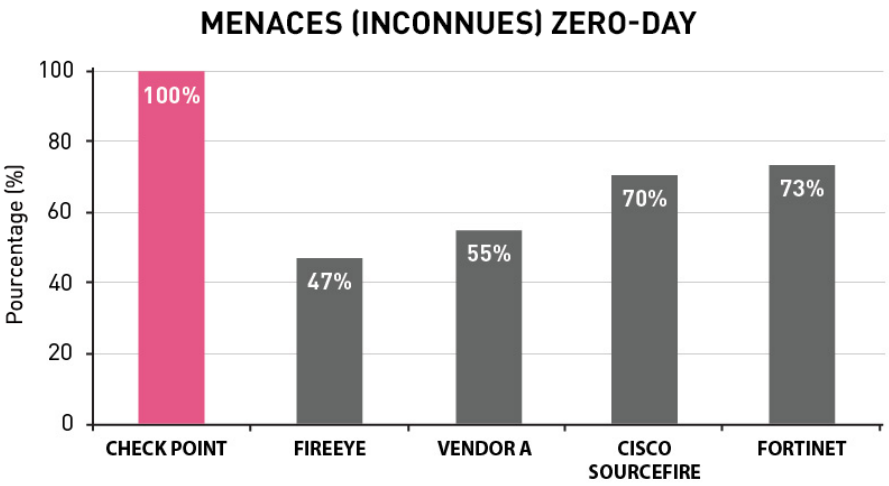
LES TESTS DE MIERCOM MONTRENT QUE L'ÉMULATION DES MENACES AU NIVEAU DU SYSTÈME D'EXPLOITATION DE CHECK POINT EST CAPABLE D'IDENTIFIER DES LOGICIELS MALVEILLANTS ET DE METTRE À JOUR DES SIGNATURES EN 3 MINUTES

TAUX DE BLOCAGE LE PLUS ÉLEVÉ

Check Point SandBlast Zero-Day Protection propose le taux de blocage de logiciels malveillants le plus élevé. Pour évaluer l'efficacité et la vitesse, Check Point a procédé à deux séries de comparatifs : le test zéro seconde[10] et le test des 300 malwares inconnus.[11] Ces tests ont comparés les fonctionnalités d'émulation des menace au niveau du système d'exploitation de Check Point SandBlast Zero-Day Protection avec des bacs à sable d'autres fournisseurs, afin de déterminer (a) le pourcentage de logiciels malveillants inconnus détectés et (b) la durée nécessaire pour la détection. Les résultats :

- L'émulation des menaces au niveau du système d'exploitation de Check Point SandBlast ne prend que quatre minutes pour offrir le meilleur taux de blocage des logiciels malveillants inconnus
- Les autres fournisseurs prenaient de huit à dix-neuf minutes pour compléter la détection. Leur taux de blocage variait de 27 à 70 % des échantillons de logiciels malveillants inconnus.

Une étude menée par Miercom sur les menaces persistantes avancées en 2014 a fourni des conclusions similaires.[12]

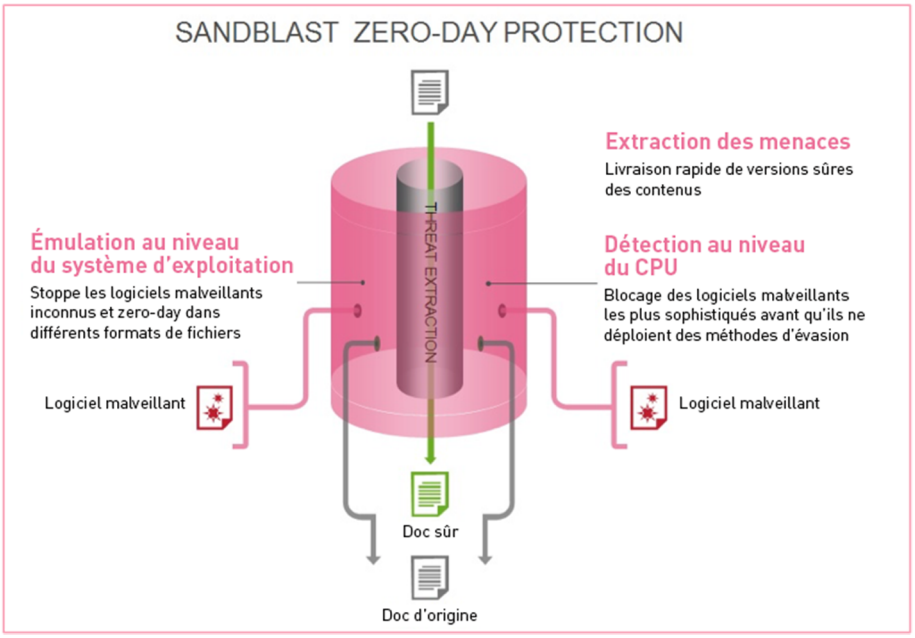


Source : Étude Miercom sur les menaces persistantes avancées en 2014

Même si les tests ont montré que le bac à sable traditionnel de Check Point au niveau du système d'exploitation est le meilleur, la cybersécurité reste un vaste jeu du chat et de la souris. Peu importe la qualité de la technologie de bac à sable traditionnel, un cybercriminel intelligent peut trouver un moyen innovant de le contourner. Pour contrer ces attaques, Check Point SandBlast Zero-Day Protection intègre également une technologie de détection au niveau du CPU pour maximiser la résistance aux techniques de contournement.

RÉSUMÉ : LA MEILLEURE PROTECTION À TOUS LES NIVEAUX

Une protection totale exige bien plus que des pare-feux et des antivirus de nouvelle génération. Les cybercriminels conçoivent de nouvelles façons d'attaquer vos systèmes et vos réseaux. Vous avez besoin d'une solution capable d'identifier les menaces connues, inconnues et zero-day, et de livrer rapidement des documents sains à vos employés.



Pionnier de la sécurité sur Internet, Check Point innove à nouveau avec SandBlast Zero-Day Protection, en introduisant la technologie de détection au niveau du CPU capable de résister aux techniques de contournement et le meilleur bac à sable du marché au niveau du système d'exploitation, en les combinant avec Threat Extraction dans une solution intégrée.

Les fonctionnalités de SandBlast comprennent :

- Threat Extraction convertit les fichiers entrants en fichiers PDF pour améliorer la protection, ou conserve le format d'origine en supprimant les contenus actifs tels que macros et scripts
- L'inspection approfondie des logiciels malveillants au niveau du CPU les identifie là où ils ne peuvent masquer leurs actions
- Des technologies de bac à sable supplémentaires protègent un ensemble complet de documents et de types de fichiers
- L'intégration dans l'infrastructure existante ne nécessite pas de nouveaux équipements
- Prévention des menaces et gestion intégrée de la sécurité pour une visibilité complète sur les menaces
- Partage automatique de nouvelles informations sur les attaques avec Check Point ThreatCloud pour bloquer d'autres occurrences similaires au niveau des passerelles

Il est temps de faire évoluer les défenses contre les menaces et protéger votre entreprise contre les attaques, grâce à la solution la plus rapide offrant le taux de blocage de logiciels malveillants le plus élevé du marché. Avec notre solution SandBlast Zero-Day Protection, votre entreprise bénéficie rapidement d'une protection maximale sans perturbation de la productivité.

POUR PLUS D'INFORMATIONS SUR CHECK POINT SANDBLAST, VEUILLEZ CLIQUER ICI

RÉFÉRENCES :

1 *La vérité sur les logiciels malveillants. http://www.malwaretruth.com/the-list-of-malware-types/*

2 *AV-Test. https://www.av-test.org/en/statistics/malware/*

3 *AV-Test. https://www.av-test.org/en/statistics/malware/*

4 *Check Point Software Technologies. Rapport Sécurité 2015 de Check Point. http://www.checkpoint.com/resources/2015securityreport/*

5 *Internet Live Stats. http://www.internetlivestats.com/one-second/#email-band*

6 *Ilyin, Yuri. « Spam et phishing au 1er trimestre 2015 : les banques et les chevaux de Troie bancaires », Kaspersky Lab Business, 24 juin 2015. https://business.kaspersky.com/spam-and-phishing-in-q1-2015-banks-and-banking-trojans/4113/*

7 *Check Point Software Technologies. Rapport Sécurité 2015 de Check Point http://www.checkpoint.com/resources/2015securityreport/*

8 *Calhoun, Pat. « Un aperçu des techniques récentes de contournement des bacs à sable », Security Week, 15 janvier 2015. http://www.securityweek.com/glimpse-latest-sandbox-evasion-techniques*

9 *Les trois principes de la cybersécurité. http://www.spi.dod.mil/tenets.htm*

10 *Check Point Software Technologies. « Test zéro seconde », 2014. http://www.checkpoint.com/campaigns/zerosecond/zero_second_white_paper.pdf*

11 *Check Point Software Technologies. « Les 300 malwares inconnus », 2014. http://www.checkpoint.com/resources/300/*

12 *Miercom. « Prévention des menaces avancée grâce à l'analyse en bac à sable », octobre 2014. http://www.checkpoint.com/resources/miercom-report/full-miercom-report.pdf*