LIVRE BLANC

FireEye

DÉPASSER L'APPROCHE SANDBOX :

Pourquoi les outils d'analyse automatisés ne se valent pas tous

LA SÉCURITÉ RÉINVENTÉE

SOMMAIRE

Résumé

Admettant à mots couverts que les outils de sécurité conventionnels ne fonctionnent plus, les éditeurs de solutions de sécurité se démènent pour ajouter des outils d'analyse dynamique, aussi appelés « sandbox », à leur offre. Même les fournisseurs bien établis, qui ont longtemps défendu leurs outils vieillissants, adoptent désormais le concept. Au lieu de s'appuyer sur des signatures, les systèmes d'analyse dynamique automatiques observent le comportement des logiciels malveillants à l'aide de machines virtuelles. Ces environnements isolés émulant des systèmes informatiques permettent d'exécuter des fichiers sans provoquer de réels dommages.

En observant les fichiers dans ces environnements restreints, ou « sandbox », les systèmes d'analyse automatisés sont chargés de repérer des comportements révélateurs, par exemple des modifications apportées au système d'exploitation ou des appels transmis aux serveurs de commande et de contrôle des cybercriminels.

Toutefois, face à la multitude d'outils dynamiques proposés sur le marché et à des arguments de marketing qui peinent à se différencier, faire le bon choix peut se révéler un véritable casse-tête.

De nombreux environnements sandbox laissent les ressources informatiques aussi exposées qu'elles l'étaient avant leur déploiement. La plupart d'entre eux présentent certaines lacunes, dont les suivantes :

- Analyse des fichiers de manière isolée et non comme un tout coordonné
- Focalisation sur un seul vecteur de menace
- Incapacité à émuler des systèmes complets
- Émulation d'une image de référence unique
- Mesure des états de départ et d'arrivée des systèmes virtuels, négligeant tout ce qui se passe entre les deux
- Incapacité à s'adapter aux nouvelles technologies de contournement qui visent ces types d'environnements en particulier

Ce livre blanc décrit le fonctionnement des environnements sandbox, expose les raisons de l'échec de la plupart des approches fondées sur ces derniers et souligne les éléments auxquels être attentif dans le choix d'une technologie d'analyse basée sur les machines virtuelles.

Introduction

Et tu, Symantec ?

Dans une entrevue accordée récemment au *Wall Street Journal*, un dirigeant de Symantec porte un coup au marché des logiciels antivirus, pourtant créé par le géant de la sécurité il y a plusieurs dizaines d'années. Déclarant la catégorie de produits comme « morte », il a confié que seulement 45 % des cyberattaques seraient contrées par la technologie antivirus et que celle-ci ne représentait plus un marché porteur[1].

Aussi choquantes que ces déclarations puissent paraître, surtout de la part d'une entreprise qui réalise 40 % de son chiffre d'affaires sur ce marché[2], elles reflètent ce que les experts en sécurité informatique savent depuis des années : les systèmes de protection basés sur les signatures sont impuissants contre les attaques avancées.

Les attaques actuelles contournent sans problème les outils de sécurité classiques. Les logiciels antivirus, les pare-feux traditionnels et de nouvelle génération, les systèmes de prévention des intrusions (IPS) et autres outils similaires ne sont plus d'aucune utilité contre celles-ci.

Comme le signalait Gartner en 2012 : « Il est généralement admis que les attaques avancées contournent nos contrôles de sécurité traditionnels basés sur les signatures et continuent à sévir sur nos systèmes sans être détectées pendant de longues périodes. La menace est bien réelle. Vos systèmes sont déjà compromis ; c'est juste que vous n'en êtes pas conscient[3]. »

Une nouvelle approche

Face à ce constat, de nombreux éditeurs de solutions de sécurité se tournent vers les outils d'analyse automatisés, aussi appelés « sandbox ». Même les fournisseurs bien établis, qui ont longtemps défendu leurs outils vieillissants, adoptent désormais le concept.

Au lieu de s'appuyer sur des signatures, des systèmes d'analyse dynamique automatiques observent le comportement des logiciels malveillants à l'aide de machines virtuelles. Ces environnements isolés émulant des systèmes informatiques permettent d'exécuter des fichiers sans provoquer de réels dommages.

En observant les fichiers dans ces environnements virtuels restreints, les systèmes d'analyse automatisés sont chargés de repérer des comportements révélateurs, par exemple des modifications apportées au système d'exploitation ou des appels transmis aux serveurs de commande et de contrôle des cybercriminels.

Toutes les technologies sandbox ne se valent pas

Au vu de la multitude d'outils dynamiques proposés sur le marché et de messages de marketing qui sèment la confusion par leur similitude, faire le bon choix peut se révéler un véritable casse-tête.

Que les entreprises ne s'y trompent pas : l'analyse dynamique n'est pas la panacée. En soi, les machines virtuelles peuvent uniquement exercer une surveillance et générer des rapports sur les activités des fichiers — analyser celles-ci de façon efficace est une tâche plus difficile, bien qu'absolument indispensable.

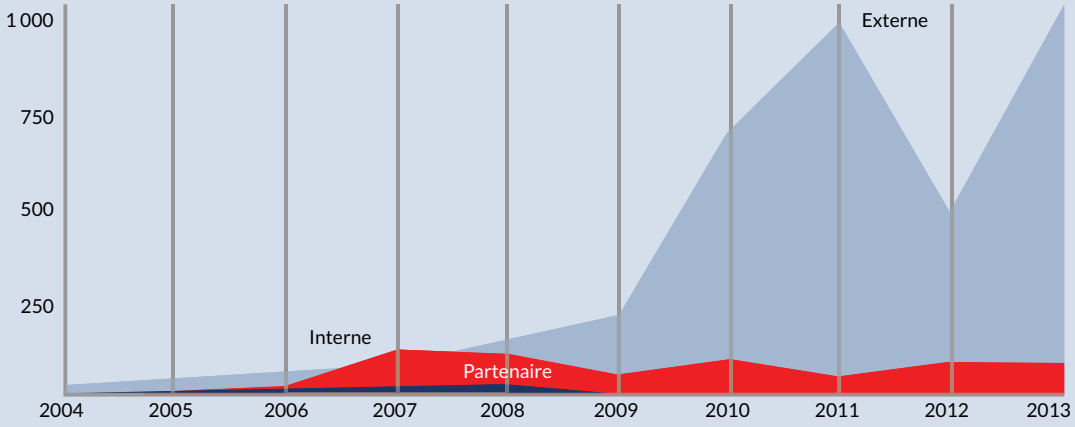
[1] Danny Yadron (The Wall Street Journal), *Symantec Develops New Attack on Cyberhacking*, mai 2014.
[2] Ibid.
[3] Gartner, *Best Practices for Mitigating Advanced Persistent Threats*, janvier 2012.

Des attaques plus fréquentes, plus efficaces et plus coûteuses

Pour la première fois en 2013, le nombre de fuites de données confirmées dont fait état le rapport d'enquête annuel sur les compromissions de données de Verizon (*Data Breach Investigations Report*) a passé la barre de 1 000 unités, soit très exactement 1 367[4]. C'est plus du double des 621 cas recensés l'année précédente[5]. Au cours de la même période, le nombre total d'incidents a augmenté d'environ un tiers, atteignant un volume de 63 437[6].

Selon le Ponemon Institute, le coût moyen d'une compromission de données s'élevait à 3,5 millions de dollars en 2013, soit 15 % de plus qu'en 2012[7]. En d'autres termes, le coût lié à la perte ou au vol d'un fichier est passé de 136 dollars en 2012 à 145 dollars l'année suivante[8].

Nombre de compromissions par catégorie d'auteurs de menaces dans le temps



Source : Ponemon Institute

Coût moyen lié à la détection et à l'escalade des incidents (États-Unis) :
417 700 USD

Coûts moyens de notification (États-Unis) :
509 237 USD

Coûts consécutifs aux compromissions (États-Unis) :
1 599 996 USD

[4] Verizon, *2014 Data Breach Investigations Report*, mai 2014.
[5] Verizon, *2013 Data Breach Investigations Report*, mai 2013.
[6] Calculé à partir des volumes totaux cités dans les éditions 2013 et 2014 du *Data Breach Investigations Report*.
[7] Ponemon Institute, *2014 Cost of Data Breach Study - United States, Global Analysis*, mai 2014.
[8] Ibid.

Pourquoi les moyens de défense traditionnels ne suffisent plus

Les professionnels de la sécurité s'accordent généralement sur le fait que les outils de sécurité basés sur les signatures sont impuissants face aux attaques sophistiquées actuelles[9]. Pour les contourner, les pirates informatiques utilisent un large éventail de techniques, notamment des fichiers binaires en constante mutation, des attaques multiphases et des exploits zero-day.

Les signatures à la traîne des fichiers binaires malveillants

Les auteurs d'attaques ont à leur disposition de nombreuses méthodes leur permettant d'échapper à la détection. Citons les suivantes :

- Empaquetage de fichiers binaires
- Compression
- Chiffrement
- Altération de compilateurs
- Polymorphisme

Ces techniques permettent aux auteurs d'attaques de générer un volume important d'échantillons de fichiers binaires uniques provenant de la même famille de logiciels malveillants, chacun de ces fichiers ayant une valeur de hachage unique.

La mise en correspondance des signatures étant limitée à des échantillons de hachage spécifiques, le temps nécessaire à la détection s'allonge à mesure que le nombre de nouveaux échantillons uniques soumis augmente.

Attaques multiphases

Les attaques avancées se déroulent en plusieurs phases distinctes et coordonnées, et s'appuient souvent sur de nombreux vecteurs de menace : sites Web, messagerie électronique, partages de fichiers ou encore terminaux mobiles. De plus, il n'est pas rare que les campagnes de logiciels malveillants combinent plusieurs de ces vecteurs. Ainsi, une attaque transmise par la messagerie peut contenir des URL malveillantes.

Bon nombre d'attaques avancées sont également multiflux. Plutôt que d'envoyer un seul fichier malveillant sur un système ciblé, où il pourrait déclencher une alerte, les auteurs d'attaques distribuent plusieurs fichiers ou objets qui semblent inoffensifs. Ce n'est qu'une fois combinés que ces fichiers et objets révèlent leur véritable nature.

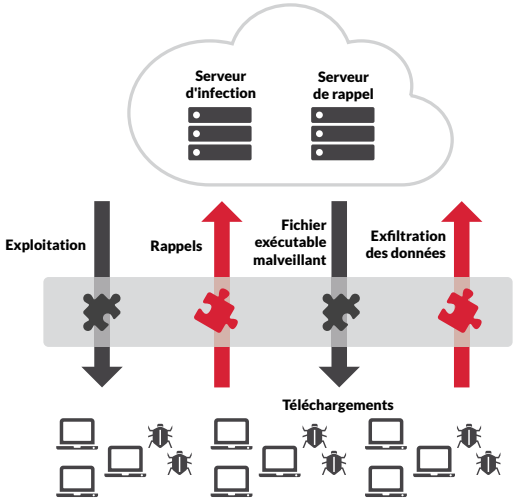


Figure 1 — Les attaques multiphases, multiflux et multivectorielles d'aujourd'hui

[9] Gartner, *Best Practices for Mitigating Advanced Persistent Threats*, janvier 2012.

Ainsi, de nombreuses attaques Web se composent de plusieurs fichiers ou objets téléchargés. Ces objets proviennent souvent de plusieurs requêtes et réponses HTTP, dont des redirections, et de plusieurs sessions TCP.

Un objet peut être utilisé pour mener une attaque via la mémoire (heap spray). Un autre inclure un dépassement de mémoire ou des données non nettoyées à exploiter. Un troisième mettre en échec les défenses du système d'exploitation, comme avec la distribution aléatoire de l'espace d'adressage (ASLR, *Address Space Layout Randomization*) et la prévention de l'exécution des données (DEP, *Data Execution Prevention*). Enfin, un autre fichier binaire téléchargé peut être une image contenant du code malveillant dissimulé, qui ne s'exécute que lorsqu'il est associé à un autre fichier a priori sans danger.

Exploits zero-day

Les vulnérabilités zero-day sont des failles logicielles qui exposent les utilisateurs à des cyberattaques jusqu'à ce qu'une solution temporaire soit mise en place ou un correctif distribué. Parfois, la vulnérabilité est inconnue de tous — à l'exception d'un cybercriminel (ou d'un éditeur prêt à vendre les découvertes de ce type sur le marché noir). Parfois encore, l'éditeur du logiciel concerné l'a identifiée, mais n'a encore distribué aucun correctif permettant d'y remédier.

Par définition, un outil basé sur les signatures ne protège que contre les menaces qui ont été identifiées et répertoriées.

Même si les équipes chargées de la sécurité connaissent les vulnérabilités et disposent d'un correctif, l'application de ce dernier peut prendre du temps, voire poser des problèmes de compatibilité ou détériorer une application personnalisée.

Utilisation de l'analyse dynamique automatisée avec d'autres outils

Les outils de sécurité conventionnels préviennent certaines attaques côté client, mais ils n'offrent pas de solution miracle.

Prenons le cas des listes blanches d'applications. Les listes blanches empêchent un système d'exécuter du code arbitraire envoyé au cours de la phase d'injection d'une attaque avancée ou dans le cadre d'une attaque d'ingénierie sociale. Toutefois, la plupart des attaques avancées débutent bien avant l'arrivée de fichiers binaires sur le système ciblé.

Pendant la première phase de l'attaque, le code d'exploit libère un code shell qui s'exécute au sein du processus exploité, par exemple Internet Explorer, Java ou Adobe Reader. Or les listes blanches ne restreignent pas tous les types de code exécutable. Plusieurs langages interprétés s'exécutent selon un processus d'ajout des hôtes sur liste blanche. En voici quelques-uns :

- VBScript
- JScript
- Fichiers de commandes
- Applications Java
- PowerShell
- Python
- Macros Visual Basic pour Applications et Office

Bien qu'à ce stade, aucun code binaire ne soit écrit sur le disque, l'auteur de l'attaque exécute déjà du code sur le système compromis.

Certaines attaques côté client peuvent également être contrées par la distribution rapide de correctifs au niveau des systèmes d'exploitation et des applications, à condition toutefois qu'il ne s'agisse pas de vulnérabilités zero-day, dont les pirates sont friands.

C'est là que l'analyse dynamique entre en jeu. La technologie sandbox est conçue pour combler les lacunes des autres moyens de défense.

Pourquoi la plupart des environnements sandbox ne rencontrent pas les attentes

De nombreux environnements sandbox, parce qu'ils présentent des défauts fondamentaux, laissent les ressources informatiques aussi vulnérables qu'elles ne l'étaient auparavant. Beaucoup sont faciles à détecter et à contourner. Certains analysent les fichiers de manière isolée et non comme un tout coordonné. D'autres se focalisent sur un seul vecteur de menace. D'autres encore ne parviennent pas à émuler des systèmes complets ou émulent seulement une image de référence unique. Enfin, certains ne mesurent que les états de départ et d'arrivée des systèmes virtuels, négligeant tout ce qui se passe entre les deux.

Détection et contournement aisés

Conscients que le code malveillant risque d'être exécuté dans un environnement sandbox avant d'atteindre la cible, les auteurs de logiciels malveillants écrivent désormais du code capable de détecter les machines virtuelles. Celui-ci se garde de tout comportement révélateur jusqu'à ce qu'il atteigne sa proie dans l'environnement « réel ». Comme aucune action suspecte n'est détectée dans l'environnement sandbox, l'analyse de sécurité considère le code comme étant inoffensif.

Voici quelques exemples de techniques de contournement des environnements sandbox[10] :

- **Interactions humaines.** Certains logiciels malveillants s'exécutent après plusieurs clics de souris ou suite à des actions de l'utilisateur par le biais de boîtes de dialogue. Dans la mesure où ils sont incapables de reproduire les interventions de l'utilisateur, les environnements sandbox risquent de ne pas identifier des logiciels malveillants dont l'exécution est soumise à ce type d'interaction.
- **Appels de mise en veille et déclencheurs temporels.** La plupart des environnements sandbox exécutent les fichiers pendant une durée limitée. Partant, les logiciels malveillants capables de détecter un sandbox peuvent rester inactifs pendant un temps déterminé ou jusqu'à ce qu'un déclencheur prédéfini soit atteint en dehors des délais d'exécution.
- **Dissimulation de processus.** Les logiciels malveillants peuvent exploiter des pointeurs internes non documentés de la fonction *PsCreateProcessNotifyRoutine* de Windows pour annuler les rappels enregistrés et, ainsi, empêcher les environnements sandbox de détecter tout processus malveillant.
- **Contrôles propres à VMware.** Certains outils de sécurité faisant appel à la technologie sandbox utilisent des machines virtuelles vendues dans le commerce, notamment VMware. Les images système VMware présentent des caractéristiques particulières qu'un logiciel malveillant avancé peut facilement détecter et contourner.

Analyse des fichiers de manière isolée

La plupart des environnements sandbox analysent un par un les fichiers et objets suspects. En revanche, comme expliqué précédemment, les attaques avancées actuelles s'appuient sur une combinaison d'éléments multiples.

Le cycle d'une attaque classique se déroule comme suit :

1. Exploitation
2. Rappel
3. Téléchargement du logiciel malveillant
4. Exfiltration des données

Chacune de ces phases peut sembler inoffensive si elle n'est pas examinée dans un contexte général, si bien que la plupart des environnements sandbox ne constatent rien d'anormal. Pourtant, l'effet combiné de ces éléments peut être dévastateur une fois le système ciblé atteint.

Il est d'autant plus important de détecter l'exploitation initiale que les phases ultérieures de l'attaque recourent souvent à des techniques de chiffrement ou de dissimulation. Récemment, des attaques ont utilisé des outils d'accès à distance pour envoyer des données dérobées via des canaux de commande et de contrôle chiffrés en vue d'échapper à la détection.

[10] FireEye, *Simple comme bonjour : le contournement des environnements sandbox d'exécution de fichiers*, août 2013.

Focalisation sur un seul vecteur de menace

La plupart des environnements sandbox se concentrent sur un seul vecteur de menace, tel que la messagerie électronique ou le Web, alors que bon nombre d'attaques avancées sont multivectorielles. Ainsi, les campagnes de messages de harponnage (spear-phishing) débutent souvent par l'envoi d'une pièce jointe malveillante contenant l'exploit et se poursuivent avec le téléchargement d'une charge malveillante sur le Web, par exemple.

S'il n'est pas en mesure de corréler les activités sur plusieurs vecteurs de menace, l'environnement sandbox ne peut pas révéler la véritable nature de chaque élément isolé.

Incapacité à émuler des systèmes complets

De nombreux environnements sandbox sont conçus pour analyser les fichiers exécutables uniquement. Si le rôle joué par de tels fichiers est indéniable, les attaques avancées actuelles n'en « phagocytent » pas moins des documents et d'autres fichiers de contenu. Ces fichiers « piégés », altérés à des fins malveillantes, exploitent les vulnérabilités présentes dans les logiciels clients, notamment Adobe Reader, Microsoft Office et Java Runtime Environment.

Ainsi, les attaques par harponnage ciblées emploient fréquemment des fichiers PDF ou des documents Office piégés. Quant aux attaques de type téléchargement à l'insu de l'utilisateur (drive-by) et aux attaques de point d'eau (watering hole), elles dissimulent leurs exploits parmi le contenu de pages Web.

Pour que l'environnement sandbox puisse analyser les exploits et le contenu de documents, il doit être associé à une application côté client qui permette l'ouverture de tels fichiers.

Émulation d'une image de référence unique

Parmi les environnements sandbox qui parviennent à émuler des systèmes complets, beaucoup utilisent une image unique, correspondant souvent à l'installation de référence dans l'entreprise. Ce n'est pas la bonne approche.

Il est fréquent que les attaques avancées ciblent des combinaisons spécifiques de système d'exploitation et de logiciel client. Si ces associations ne sont pas prises en considération dans le sandbox, le logiciel malveillant reste inactif et échappe à la détection, puis s'exécute dès qu'il atteint un système sur lequel la combinaison ciblée est présente.

Il faut également tenir compte du fait que les systèmes des utilisateurs finaux sont rarement identiques, quand bien même les paramètres de configuration sont soumis à une gestion rigoureuse. Certains utilisateurs choisissent de mettre à jour leur navigateur Web, d'autres oublient d'appliquer un correctif Adobe Reader. Et si l'image de référence de l'environnement sandbox varie, même légèrement, de celles des utilisateurs finaux, l'attaque risque de passer inaperçue.

La seule façon de détecter les attaques avancées consiste à recourir à une analyse dynamique capable d'examiner les objets et fichiers suspects dans diverses configurations.

Analyse du delta plutôt que de l'exécution

Veiller à ce que l'environnement sandbox comprenne les applications et le contenu adéquats n'est pas tout. En effet, sa capacité à détecter les attaques avancées dépend de la façon dont il surveille le contenu et réagit tout au long de son exécution.

En règle générale, deux approches sont possibles :

- Analyse du delta — Comparaison de l'image du sandbox avant et après l'exécution
- Analyse de l'exécution — Intégration d'instruments de mesure pour observer les fichiers en cours d'exécution

De nombreux environnements sandbox recourent à l'analyse du delta, c.-à-d. que seules les modifications révélées au terme de l'exécution sont enregistrées, sans tenir compte des événements qui se produisent entre les états de départ et d'arrivée.

Ainsi, l'analyse du delta ne surveille pas les opérations qui s'exécutent dans la mémoire, pas plus qu'elle ne détecte les fichiers écrits puis supprimés en cours d'exécution. C'est pourquoi elle ne permet ni de détecter les logiciels malveillants furtifs qui effacent les traces de leur passage, ni de réagir face aux techniques de contournement des environnements sandbox décrites précédemment. (Voir « Détection et contournement aisés ».)

Ce qui différencie FireEye

Spécialement conçu pour combattre les tactiques les plus récentes créées par les cybercriminels aguerris, le moteur FireEye Multi-Vector Virtual Execution™ (MVX) transcende les environnements sandbox, qu'ils soient orientés objet ou fichier. Il capture et confirme les menaces ciblées et zero-day.

Le moteur MVX confine les pièces jointes, objets Web et fichiers suspects au sein de plusieurs environnements virtuels instrumentés pour provoquer le déclenchement de leur charge active. Plutôt que d'analyser un sous-ensemble de fichiers de manière isolée, il met en corrélation les activités enregistrées sur plusieurs vecteurs de menace et lors de phases d'attaque diverses.

Bref, il établit les liens qui permettent d'analyser une attaque dans son contexte global.

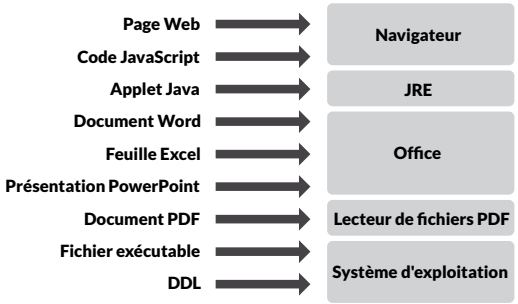


Figure 2 — Combinaison de fichiers et d'objets multiples au sein d'une même attaque

Hyperviseur propriétaire à la sécurité renforcée

Contrairement à certaines technologies sandbox, le moteur MVX n'est pas une machine virtuelle vendue en grande distribution, détectable et contournable en un tournemain. Il inclut un hyperviseur à la sécurité renforcée conçu dans un seul but : analyser les logiciels malveillants. Cette technologie brevetée permet l'exécution de plusieurs machines virtuelles sur une appliance unique, tout en exploitant des microtâches parallèles au sein de chaque machine virtuelle afin d'accélérer l'exécution.

Le moteur MVX gère les flux de trafic ultrarapides en conditions réelles. De plus, il intègre des contre-mesures en évolution constante destinées à neutraliser les logiciels malveillants.

Analyse en contexte

L'analyse dynamique est essentielle tout au long du cycle de vie de l'attaque, de l'exploitation initiale à l'exfiltration des données. C'est pourquoi les produits isolés qui ciblent des objets uniques, tels que les fichiers exécutables malveillants, les bibliothèques de liaisons dynamiques (DLL) ou les fichiers PDF, ne parviennent pas à détecter la grande majorité des attaques. Ils n'ont aucune visibilité sur ce cycle de vie complet.

Le moteur MVX prend en charge toute une série d'environnements d'exécution parallèle. Il peut ainsi analyser les attaques selon les circonstances dans lesquelles elles se produisent véritablement : sur de nombreux flux, en de multiples phases et via plusieurs vecteurs de menace.

Une multitude d'environnements et de conditions

Les machines virtuelles du moteur MVX exécutent les fichiers et objets suspects au sein d'un large éventail de systèmes d'exploitation, de Service Packs et d'applications. Cette diversité permet au moteur MVX de détecter des logiciels malveillants très ciblés, capables de contourner les environnements sandbox se bornant à émuler le système d'exploitation ou une image système unique.

Figure 3 — Modèle de détection virtuelle de FireEye

Conclusions et recommandations

Les environnements sandbox ne constituent pas une arme absolue contre les attaques avancées : leur efficacité est directement proportionnelle à celle de l'analyse qu'ils réalisent.

Pour véritablement protéger les actifs informatiques, les analyses basées sur des machines virtuelles doivent contrer les techniques de contournement des environnements sandbox employées par les logiciels malveillants sophistiqués. Et lorsque de nouvelles techniques de contournement émergent, les éditeurs doivent rapidement mettre leurs outils à jour.

En d'autres termes, une analyse dynamique doit analyser les fichiers et les objets en contexte, et sur plusieurs vecteurs de menace. Par ailleurs, elle doit permettre de détecter les logiciels malveillants visés dans une large gamme de configurations.

Les analyses reposant sur des machines virtuelles sont encore plus efficaces lorsqu'elles sont renforcées par des renseignements dynamiques, en temps réel, sur les menaces et par une palette complète de services. Si elles disposent d'une vue d'ensemble des attaques au sein d'une entreprise, d'une région ou d'un secteur, les équipes de sécurité peuvent mieux prévenir, détecter et contrer les attaques sophistiquées.

Que rechercher dans un outil d'analyse dynamique automatisé

Les entreprises à la recherche d'un système d'analyse dynamique automatisé doivent privilégier une solution qui présente les caractéristiques suivantes.

Une multitude d'environnements et d'applications

- Prise en charge du plus large éventail possible de versions de systèmes d'exploitation et de correctifs.
- Prise en charge d'un grand choix de navigateurs Web et de plug-in — Cette sélection doit comprendre plusieurs versions d'Internet Explorer, de Firefox et de Chrome, ainsi que des plug-in tels que Java, Flash, Shockwave et Silverlight.
- Prise en charge d'applications de bureau telles qu'Adobe Reader et Microsoft Office — L'outil doit être en mesure d'analyser des fichiers et objets inconnus dans toutes les versions des applications utilisées sur le réseau, et non pas uniquement dans la version la plus courante.
- Mise en correspondance automatique et dynamique entre, d'une part, la version et le type de navigateur ainsi que les versions de plug-in utilisés dans l'analyse reposant sur des machines virtuelles et, d'autre part, ceux installés sur les postes de travail clients réels.

Une visibilité complète sur le comportement des objets et des fichiers

- Capture et mise en corrélation du cycle de vie complet de l'attaque.
- Identification et blocage des canaux de rappel observés lors de l'exécution du logiciel malveillant dans la machine virtuelle.
- Détection et blocage de la phase d'injection du code binaire observée lors de l'exécution du code shell de l'exploit dans la machine virtuelle.
- Détection des attaques multiphases et multivectorielles — Celles-ci incluent des exploits ciblant les navigateurs qui se composent de plusieurs fichiers et dépendances dans de nombreuses applications côté client.
- Détection et classification des logiciels malveillants polymorphes par l'observation de traits déterministes.
- Détection des vulnérabilités logicielles encore inconnues et des exploits zero-day — Pour ce faire, l'outil doit être capable de mettre au jour des techniques telles que les attaques via la mémoire, l'injection de code, l'utilisation non conforme des API Windows, l'accrochage des processus d'API et la modification des routines du noyau.
- Investigation numérique complète révélant le comportement des logiciels malveillants, notamment les appels d'API Windows réalisés, les dépassements et les corruptions de la mémoire, les lectures ou modifications des emplacements de fichier et de Registre, les mutex connus, et bien d'autres indicateurs d'activités malveillantes.
- Analyse de l'exécution « en temps réel » plutôt qu'une simple analyse du delta.

Un hyperviseur axé sur la sécurité

- Environnement d'exécution dynamique conçu spécifiquement pour l'analyse des logiciels malveillants.
- Hyperviseur propriétaire capable de contrer les techniques de détection et de contournement des environnements sandbox.
- Mises à jour proposées régulièrement par l'éditeur pour contrer les techniques de contournement les plus récentes.

Une analyse dynamique adaptée aux besoins de votre entreprise

- Taux très bas de faux positifs et absence de faux négatifs.
- Analyse des fichiers et des objets sur site et dans le cloud.
- Analyse des messages électroniques avant remise pour éviter que les utilisateurs soient exposés à du contenu malveillant.
- Limitation rapide des dommages si du contenu Web venait à atteindre les utilisateurs avant d'avoir pu être identifié comme malveillant — Les mesures à prendre peuvent inclure la mise en quarantaine ou le blocage de l'accès au réseau des ordinateurs infectés.

Pour savoir comment la plate-forme FireEye peut vous aider à prévenir, à détecter et à neutraliser les menaces actuelles, consultez le site FireEye.com.

À propos de FireEye, Inc.

FireEye protège les actifs les plus précieux des déploiements à travers le monde contre la convoitise des cybercriminels. Grâce à notre combinaison unique de technologies, de renseignements et de compétences, renforcée par une présence agressive sur le terrain, nous vous aidons à éviter de subir les conséquences d'une compromission de sécurité. Par une vigilance constante, à chaque phase d'une attaque, nous démasquons les pirates et bloquons leur progression. Avec FireEye, vous détecterez les attaques à mesure qu'elles surviennent, vous comprendrez le danger que celles-ci font peser sur vos actifs les plus importants, et vous disposerez des ressources nécessaires pour répondre aux incidents de sécurité et les neutraliser.
La communauté de défense mondiale de FireEye compte plus de 2 700 clients dans 67 pays, dont plus de 150 figurent au classement Fortune 500.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 | france@FireEye.com | **www.FireEye.com**

FireEye