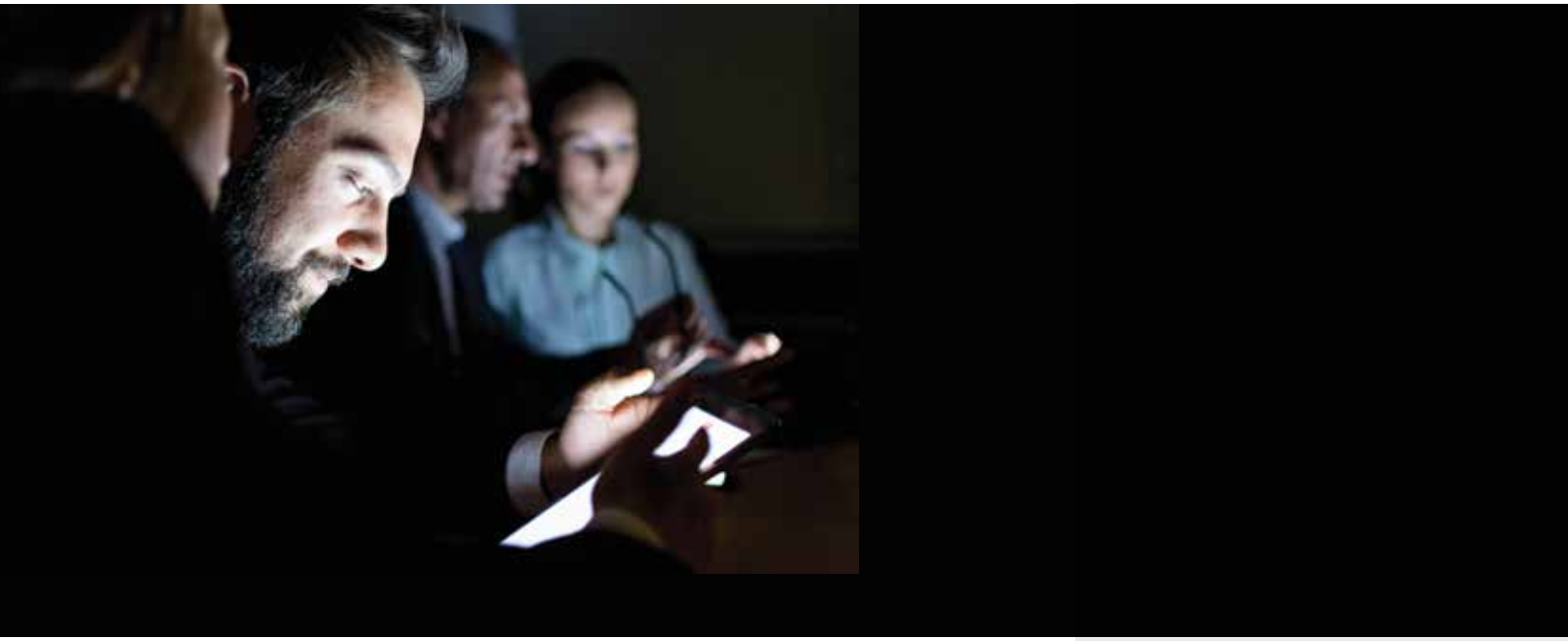
FORTINET

LIVRE BLANC

Au cœur de la technologie Sandbox

Découverte de la technologie Sandbox et de son application pratique face aux menaces actuelles



Introduction

Au cœur de la technologie Sandbox

Dans le domaine informatique, le terme Sandbox a longtemps été utilisé pour désigner un environnement sécurisé et isolé dans lequel exécuter un code malveillant en vue d'une analyse par des experts. Ce même concept est désormais appliqué par les appliances de sécurité réseau pour exécuter et inspecter le trafic réseau, et découvrir ainsi les codes malveillants qui étaient auparavant susceptibles d'échapper aux mesures de sécurité classiques.

Capable d'émuler virtuellement des systèmes d'exploitation entiers, une solution de Sandbox exécute en toute sécurité le code malveillant de manière à observer son activité. Les activités malveillantes, notamment les opérations sur fichier/disque, les connexions réseau, les changements de configuration du registre/système, etc., sont démasquées, ce qui permet de neutraliser les menaces.

Utilisés jusqu'à présent pour les fichiers exécutables, les systèmes de Sandbox sont désormais aussi employés pour exécuter des données applicatives susceptibles de dissimuler un code malveillant, comme Adobe Flash et JavaScript entre autres. Certaines applications telles qu'Adobe Reader X intègrent leur propre Sandbox avec la même finalité. Par exemple, si Reader X tombe sur un code malveillant à l'ouverture d'un fichier PDF, le code est confiné dans un environnement Sandbox et ne peut donc pas infecter le système d'exploitation.

Pourquoi recourir aujourd'hui à la technologie Sandbox ?

Dans le domaine informatique, le terme Sandbox a longtemps été utilisé pour désigner un environnement sécurisé et isolé dans lequel exécuter un code malveillant en vue d'une analyse par des experts. Ce même concept est désormais appliqué par les appliances de sécurité réseau pour exécuter et inspecter le trafic réseau, et découvrir ainsi les codes malveillants qui étaient auparavant susceptibles d'échapper aux mesures de sécurité classiques. Capable d'émuler virtuellement des systèmes d'exploitation entiers, une solution de Sandbox exécute en toute sécurité le code malveillant de manière à observer son activité. Les activités malveillantes, notamment les opérations sur fichier/disque, les connexions réseau, les changements de configuration du registre/système, etc., sont démasquées, ce qui permet de neutraliser les menaces.

Utilisés jusqu'à présent pour les fichiers exécutables, les systèmes de Sandbox sont désormais aussi employés pour exécuter des données applicatives susceptibles de dissimuler un code malveillant, comme Adobe Flash et JavaScript entre autres. Certaines applications telles qu'Adobe Reader X intègrent leur propre Sandbox avec la même finalité. Par exemple, si Reader X tombe sur un code malveillant à l'ouverture d'un fichier PDF, le code est confiné dans un environnement Sandbox et ne peut donc pas infecter le système d'exploitation.
Pourquoi recourir aujourd'hui à la technologie Sandbox ?

Si la technologie Sandbox est si ancienne, pourquoi prend-elle tout à coup une telle importance ? Les cybercriminels arrivent à mieux comprendre les méthodes de détection courantes et ont donc tendance à renforcer leurs efforts de recherche et développement afin de déjouer les solutions de sécurité. La technologie Sandbox permet aujourd'hui de déceler les nouvelles menaces dissimulées ou les anciennes menaces qui prennent une nouvelle apparence trompeuse.

Sandbox et détection proactive des signatures

La technologie Sandbox est cependant très gourmande en ressources. Le code doit être intégralement exécuté dans l'environnement Sandbox avant de pouvoir être analysé. Et l'exploration de tous les chemins d'exécution du code malveillant, avec les éventuels modules supplémentaires qu'il tente de télécharger, prend du temps. Fortinet combine la technologie Sandbox avec la détection proactive des signatures afin de filtrer le trafic avant son arrivée dans l'environnement Sandbox. Ce procédé est en effet plus rapide que la technologie Sandbox seule.

Le processus classique de détection des signatures est réactif, car les signatures sont simplement les empreintes des menaces qui ont été repérées « dans la nature ». Le langage breveté Compact Pattern Recognition Language (CPRL) de Fortinet est une technologie de détection proactive des signatures à inspection approfondie, développée après plusieurs années de recherche par FortiGuard Labs. Une seule signature CPRL peut intercepter plus de 50 000 camouflages employés par un logiciel malveillant. Associée à la technologie Sandbox, la détection proactive des signatures CPRL permet d'élargir le champ de recherche aux attaques et méthodes utilisées par les menaces persistantes avancées (APT) et les techniques avancées de contournement (AET).

> « ... Les cybercriminels arrivent à mieux comprendre les méthodes de détection courantes et ont donc tendance à renforcer leurs efforts de recherche et développement afin de déjouer les solutions de sécurité. »

Menaces persistantes avancées

Les menaces persistantes avancées sont des attaques ciblées élaborées sur mesure. Elles peuvent échapper à la détection directe grâce à des logiciels malveillants inconnus jusqu'à présent (ou « zero-day ») et exploiter les vulnérabilités existantes (failles de sécurité non corrigées). Elles peuvent provenir d'URL et d'adresses IP hôtes totalement nouvelles ou inoffensives en apparence. Leur objectif est d'infecter le système cible au moyen de techniques avancées de codage qui tentent de contourner les barrières de sécurité et de rester inaperçues aussi longtemps que possible.

Techniques avancées de contournement

Les menaces peuvent contourner les barrières de sécurité de multiples façons. Voici quelques-unes des techniques de contournement de Sandbox les plus courantes.

Bombes logiques

Les bombes logiques les plus répandues sont les bombes à retardement, qui ont été utilisées dans des attaques très médiatisées. Dans une bombe à retardement, la partie malveillante du code reste cachée pendant un laps de temps donné. Le pirate peut dissimuler des logiciels malveillants sur plusieurs systèmes. Ils passent inaperçus jusqu'au moment fixé pour l'explosion de toutes les bombes. D'autres bombes logiques se déclenchent au moment d'une interaction humaine (clic sur la souris, redémarrage du système, etc.), ce qui indique que la bombe se trouve dans l'ordinateur de l'utilisateur, et non dans une appliance d'inspection Sandbox. Les bombes logiques sont difficiles à détecter, car il est peu probable que les conditions logiques puissent être réunies dans l'environnement Sandbox. Le code ne suit donc pas le chemin d'exécution malveillant durant l'inspection. Fortinet élabore l'environnement approprié pour démasquer les bombes logiques grâce à la technologie CPRL et à une analyse par émulation de code avant l'exécution proprement dite du code. La technologie CPRL effectue une analyse en temps réel des véritables instructions d'exploitation, de manière à pouvoir observer les conditions logiques qui déclencheront la bombe.

Rootkits et bootkits

Les logiciels malveillants avancés contiennent souvent un composant rootkit qui corrompt le système d'exploitation en implantant un code au niveau du noyau de manière à prendre le contrôle total du système. Les systèmes de Sandbox sont potentiellement vulnérables à cette technique de contournement, car les dispositifs de surveillance comportementale peuvent également être corrompus. Par ailleurs, les bootkits infectent le système en introduisant un logiciel malveillant au moment de l'amorçage. C'est un procédé qui ne peut généralement pas être observé par une solution de Sandbox. Fortinet résout à nouveau ce problème grâce à la détection CPRL qui permet de détecter les routines de rootkit/bootkit avancées avant leur exécution.

Détection de Sandbox

Une autre technique avancée de contournement est la reconnaissance de l'environnement. Le code APT peut contenir des routines qui tentent de déterminer s'il s'exécute dans un environnement virtuel, signe qu'il se trouve peut-être dans un environnement Sandbox. Il peut aussi rechercher les empreintes des environnements Sandbox spécifiques des fournisseurs. Si le code détecte un environnement Sandbox, il ne suit pas son chemin d'exécution malveillant. La technologie CPRL est capable d'inspecter en profondeur, de détecter et de capturer tout code enquêtant sur un environnement Sandbox.

Fenêtre de commande et de contrôle botnet

L'activité de commande et de contrôle botnet commence généralement par l'introduction d'un injecteur. L'injecteur est un code parfaitement anodin différent d'une routine, qui se connecte à une URL/adresse IP afin de télécharger un fichier sur commande. La commande peut être émise par un pirate plusieurs heures, jours ou semaines après l'exécution initiale. Si le serveur auquel l'injecteur se connecte est inactif durant la fenêtre d'opportunité, pendant laquelle le système de Sandbox exécute le code, aucune activité malveillante n'est observée. La technologie CPRL permet d'intercepter les techniques de codage inhabituelles associées aux logiciels malveillants sans avoir à atteindre cette fenêtre d'opportunité. Le réseau mondial de veille FortiGuard inclut par ailleurs une surveillance des botnets qui révèle toute activité de botnet sur le terrain dès apparition.

Réseau Fast Flux

Les logiciels malveillants avancés peuvent utiliser des techniques Fast Flux ou des algorithmes de génération de domaine pour modifier l'URL/adresse IP à laquelle l'élément infecté va se connecter. Durant l'observation dans l'environnement Sandbox, l'élément infecté recherche une adresse donnée, mais au fil du temps le code dans la machine de l'utilisateur va emprunter un autre chemin vers une seconde adresse pour faire passer le trafic malveillant. FortiGuard suit les réseaux Fast Flux et renvoie les informations de sécurité recueillies au système de Sandbox en vue d'une utilisation durant les analyses préliminaires. Fortinet examine le niveau DNS, et pas uniquement les listes noires d'adresses IP comme les autres fournisseurs se contentent de faire.

Archives chiffrées

Une bonne vieille astuce utilisée par les pirates est de chiffrer simplement les logiciels malveillants dans des archives. Puis, avec une pointe d'ingénierie sociale, ils incitent l'utilisateur à ouvrir l'élément infecté en saisissant le mot de passe. Comme le système de Sandbox ne peut pas entrer automatiquement le mot de passe, le logiciel malveillant ne s'exécute pas pendant le processus d'observation. La technologie Fortinet brevetée d'inspection des en-têtes d'archives compressées permet de détecter les signatures de logiciels malveillants camouflées par le chiffrement.

Packers binaires

Les packers binaires dissimulent les logiciels malveillants en les chiffrant sous forme de portions tronquées que les antivirus classiques ont du mal à analyser. Le code est décompressé lors de son exécution et infecte alors l'hôte. Des techniques similaires sont employées pour intégrer un code malveillant dans des langages tels que JavaScript et ActionScript pour Adobe Flash. À l'origine, cette technologie était utilisée pour compresser un code exécutable en cas d'espace mémoire limité. Aujourd'hui, la capacité mémoire n'est plus un problème, mais les packers binaires sont fréquemment employés pour déjouer l'inspection antivirus. Dans le cas de JavaScript et ActionScript, cette méthodologie

peut être utilisée en toute légalité pour la protection contre la copie. Le moteur antivirus FortiGate permet de démasquer et de détecter de nombreux packers binaires. Il décompresse les logiciels malveillants dans leur format natif en vue d'une analyse approfondie basée sur CPRL, ce qui permet une détection en temps réel et une neutralisation ou une exécution ultérieure dans l'environnement Sandbox.

Logiciels malveillants polymorphes

Les logiciels malveillants polymorphes changent d'apparence à chaque exécution et ajoutent ainsi des portions de code altéré afin de déjouer les technologies d'inspection basées sur les modèles et les sommes de contrôle. Le code malveillant s'exécute lors de la décompression par un système d'exploitation. Le code polymorphe constitue un véritable défi pour les technologies classiques d'inspection réactive. Mais Fortinet relève ce défi avec brio par une association entre son moteur antivirus d'inspection proactive, sa technologie CPRL et le système de Sandbox. Le moteur peut décompresser les logiciels malveillants dans leur format natif afin de filtrer le plus de trafic possible avec un nombre réduit de ressources de traitement, avant d'exécuter les éléments restants dans l'environnement Sandbox pour une inspection approfondie.

Reproduction dans l'environnement Sandbox

L'objectif de la technologie Sandbox est de reproduire intégralement le comportement d'un code malveillant. Dans l'idéal, le résultat dans l'environnement Sandbox devrait être identique au résultat observé si le code était exécuté dans l'environnement d'un utilisateur. En pratique, il est difficile d'obtenir des résultats identiques en raison du nombre de variables en jeu. C'est comme essayer de faire pousser deux plantes identiques à partir de graines : les moindres variations au niveau de la quantité d'eau, de la lumière, de la température et de la composition du sol produisent des résultats différents.

Exploits et applications

Les menaces avancées peuvent se dissimuler dans des documents qui incitent l'application associée (telle que Word, Excel ou Adobe Reader) à exécuter un code malveillant. Pour reproduire fidèlement ce comportement, la technologie Sandbox doit passer par toute une série de systèmes d'exploitation, chacun exécutant plusieurs versions des applications. Ce processus de tâtonnement est à la fois long et coûteux. De nombreuses solutions de Sandbox tentent de résoudre ce problème par l'ajout de ressources, c'est-à-dire des CPU plus puissants, un nombre plus élevé de machines virtuelles ou une mémoire RAM plus importante. Mais cela s'avère inefficace et pas du tout rentable. La méthode optimale consiste à mettre en balance les systèmes d'exploitation et les applications en fonction de leur fréquence d'utilisation et à choisir l'environnement le plus propice pour déclencher le comportement malveillant.

32 bits ou 64 bits, Windows XP ou Windows 7/8

Le code 32 bits peut s'exécuter dans les environnements 32 bits et 64 bits. C'est pourquoi les créateurs de logiciels malveillants privilégient le code 32 bits pour maximiser les infections. La plupart des logiciels malveillants d'aujourd'hui se dissimulent encore dans des fichiers exécutables, notamment dans le format Portable Executable 32 bits (PE32). Les fichiers PE32 s'exécutent dans les environnements Windows XP et 7/8. La plupart des comportements malveillants peuvent donc être observés sous Windows XP (qui ne prend pas en charge le code 64 bits) sans tests ultérieurs sous Windows 7/8. Mais le moteur antivirus de Fortinet fonctionnant sur FortiSandbox avec CPRL prend totalement en charge les codes 32 bits et 64 bits ainsi que de nombreuses plateformes : Windows, Mac, Linux, Android, Windows Mobile, iOS, Blackberry et Symbian.

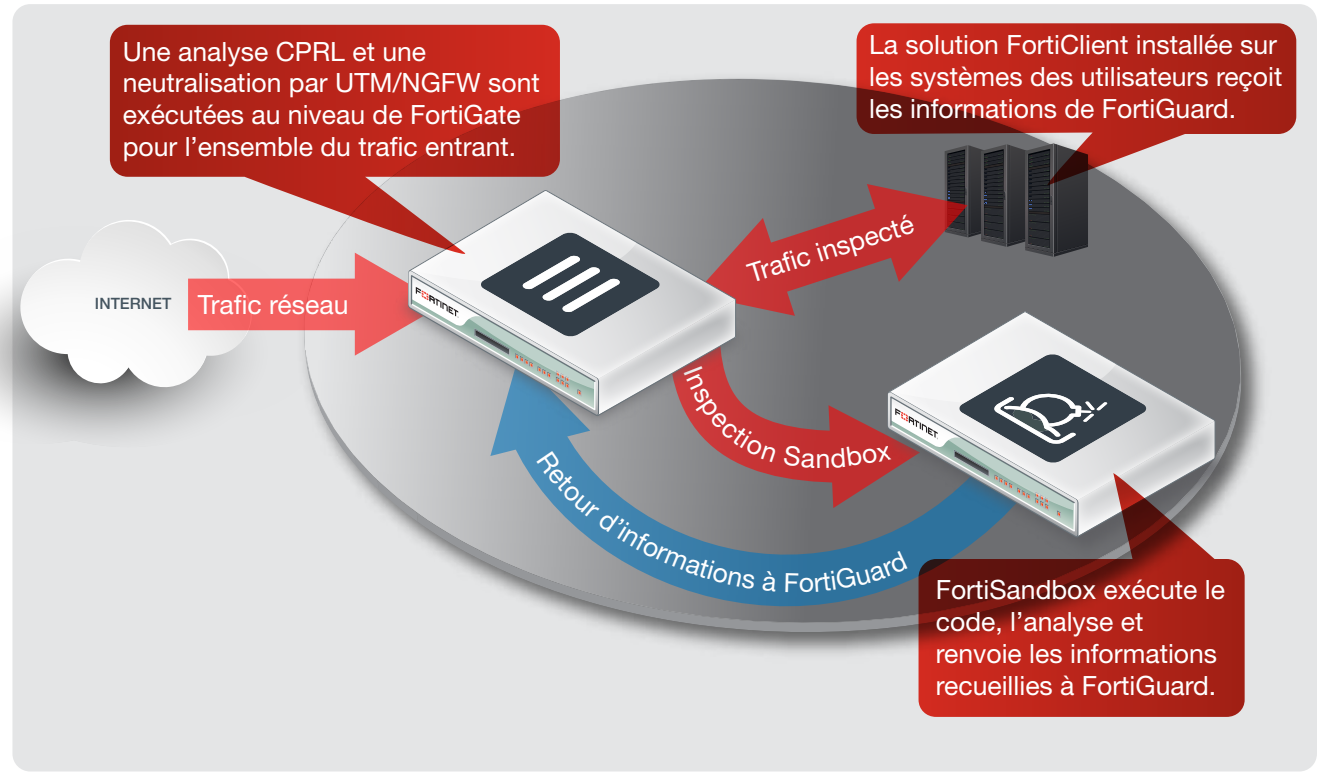
> « ... Les cybercriminels arrivent à mieux comprendre les méthodes de détection courantes et ont donc tendance à renforcer leurs efforts de recherche et développement afin de déjouer les solutions de sécurité. »

Mécanismes de sécurité Windows 7/8

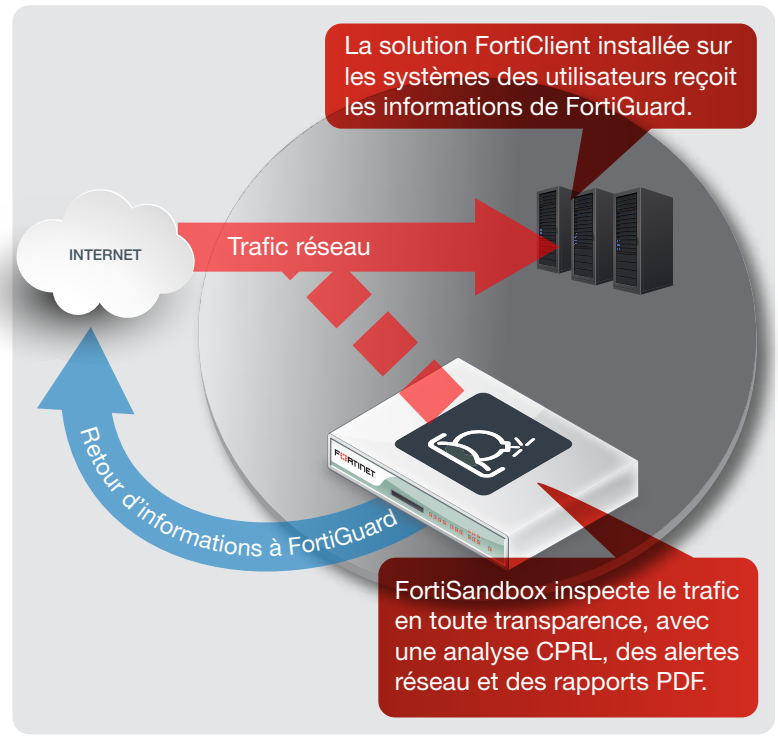
Windows a introduit une technologie de sécurité dans Windows 7/8 pour empêcher l'exécution des codes malveillants et des exploits de documents. Windows XP ne disposant pas de la même technologie, l'exécution du code sous XP dans l'environnement Sandbox améliore la détection, même si la menace est conçue spécialement pour Windows 7/8.

Fin de vie de Windows XP

Windows XP est un terrain fertile pour les infections, et le meilleur système d'exploitation pour une reproduction fidèle des menaces en vue de l'inspection Sandbox. Mais à compter du 8 avril 2014, Windows XP ne sera plus pris en charge par Microsoft et plus aucun correctif de sécurité ne sera alors publié. Des failles de sécurité toujours plus nombreuses devraient donc apparaître dans les environnements XP. Ces derniers seront encore plus propices aux infections. La bonne nouvelle, c'est qu'un nombre encore plus élevé de logiciels malveillants se déclencheront correctement sous XP dans l'environnement Sandbox. La mauvaise nouvelle, c'est que les pirates vont trouver là une cible particulièrement intéressante. Il y a fort à parier que des logiciels malveillants vont être développés afin de tirer parti au maximum de la nonchalance des utilisateurs qui ne sont pas encore passés à Windows 7/8. Au vu des tendances passées, la migration ne va pas se faire du jour au lendemain.



Solution FortiSandbox déployée avec FortiGate



Déploiement autonome de FortiSandbox

Le paysage des menaces en bref

La plupart des menaces observées par FortiGuard Labs utilisent le code 32 bits et sont conçues pour s'exécuter dans les environnements Windows XP. Windows XP reste un marché actif ainsi qu'une cible facile. Tant que les pirates peuvent développer des logiciels malveillants 32 bits qui fonctionnent sous XP aujourd'hui et restent actifs sous Windows 7/8 lorsque les utilisateurs procèdent à une migration, rien ne les pousse à concevoir des logiciels malveillants personnalisés pour Windows 7/8. Bien que FortiGuard Labs ne prévoit pas un afflux immédiat de menaces 64 bits, Fortinet est déjà en position de capturer les deux codes grâce au trio CPRL, moteur antivirus et FortiSandbox.

Systèmes d'exploitation pris en charge par FortiSandbox

Pour intercepter les menaces avec succès et efficacité, FortiSandbox alloue des ressources aux environnements virtuels Windows XP et Windows 7/8 en fonction du paysage actuel des menaces. Les environnements pris en charge évoluent ainsi au même rythme que ce paysage. Les avancées en matière de détection des nouvelles technologies de contournement et des plateformes ciblées sont intégrées dans FortiGate et FortiSandbox au fur et à mesure de leur apparition. FortiSandbox assure également une détection indépendante du système d'exploitation avec l'émulation de code et le préfiltrage par moteur antivirus.

Neutralisation proactive et protection des terminaux

La technologie Sandbox peut détecter les menaces, mais leur blocage efficace repose plutôt sur une gestion renforcée des menaces réseau ou sur des appliances de Firewall. Si une activité malveillante est découverte, les appliances de gestion unifiée des menaces (UTM) et le système de protection avancée contre les menaces (ATP) basé sur les Firewalls de Nouvelle Génération (NGFW) sont capables de la bloquer.

FortiGate et les autres produits Fortinet sont conçus pour neutraliser les menaces avancées dans le cadre d'une première ligne de défense au niveau du périmètre et du cœur. La technologie proactive utilisée permet de détecter les attaques en temps réel et de les contrecarrer avant qu'elles ne deviennent nuisibles. FortiSandbox est une extension de la solution UTM/NGFW de référence proposée par Fortinet, qui renvoie à FortiGate et/ou FortiGuard les informations de sécurité qu'elle recueille. Les nouvelles attaques perpétrées par des menaces découvertes par FortiSandbox peuvent être bloquées dans le cadre de la première ligne de défense alors que le cycle de vie se poursuit.

Conclusion

Toutes les formes de technologies de sécurité sont en réalité connues des créateurs de logiciels malveillants. Certains d'entre eux conçoivent donc des camouflages et utilisent des techniques avancées de contournement. La détection se résume à inspecter le plus grand nombre de couches possibles par tous les angles potentiels d'attaque. La meilleure approche consiste alors à combiner une inspection basée sur la passerelle et le système de Sandbox.

Le système de Sandbox fournit un niveau de défense supplémentaire utile dans le paysage actuel des menaces. Utilisé correctement, c'est un formidable outil d'apprentissage. Et lorsqu'il est associé au dispositif de sécurité de la passerelle, il permet d'identifier rapidement toute nouvelle activité malveillante sur le réseau et de réagir plus facilement aux incidents. La capacité d'intégration entre ces appliances est essentielle. FortiGuard Labs détecte fréquemment des techniques de contournement émergentes et les surveille, ce qui permet d'envoyer rapidement aux solutions Fortinet des informations et des mises à jour pour les contrecarrer. Fortinet prend actuellement en charge l'intégration de FortiSandbox avec les appliances de sécurité FortiGate, FortiManager et FortiMail.

www.fortinet.com ou
www.fortinet.fr

France
TOUR ATLANTIQUE
11ème étage, 1 place de la Pyramide
92911 Paris La Défense Cedex
France
Ventes: +33-1-8003-1655

SIÈGE SOCIAL MONDIAL
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
États-Unis
Tél. : +1 408 235 7700
www.fortinet.com/sales

SUCCURSALE EMEA
120, rue Albert Caquot
06560, Sophia Antipolis,
France
Tél. : +33 (0)4 89 87 05 10

SUCCURSALE APAC
300 Beach Road 20-01
The Concourse
Singapore 199555
Tél. : +65 6513 3730

SUCCURSALE AMÉRIQUE LATINE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tél. : 011 52 (55) 5524 8480