Sandboxing

Introduction

- La cybersécurité est passée en peu de temps d'une tâche commune de la DSI à une priorité absolue pour les directions d'entreprise. Et pour cause : les attaques informatiques se multiplient et sont de plus en plus élaborées. Pire : leurs impacts sont bien plus coûteux, allant du vol de données personnelles ou confidentielles, à l'altération de contenu, en passant par la prise en otage de données. Pour s'en prémunir, et sauvegarder son image, les outils traditionnels ne suffisent plus.
- Heureusement, si les attaques évoluent, la défense s'adapte avec de nouvelles approches, techniques et stratégies, parmi lesquelles le «sandboxing ».

Définition

- C’est un module technique de sécurité relativement récent, et qui augmente fortement le niveau de détection des malwares.
- Il faut le voir comme une sorte de « sas » qui analyse et trie les fichiers entrants, dans les emails, téléchargement ou consultation de sites web, avant qu’ils n’interagissent avec les postes de travail ou serveurs de l’entreprise.

Définition

- le sandboxing complète le rôle de l'antivirus, car les deux outils fonctionnent très différemment.
- Pour être efficace, un antivirus dispose d'une base de signatures où sont référencées toutes les menaces du moment.
- Si une pièce jointe est identifiée en tant que menace par l'antivirus, elle sera aussitôt détectée et logiquement détruite.
- Le problème survient lorsqu'une nouvelle menace informatique n'a pas encore été identifiée et documentée.
- L'antivirus sera alors incapable de la filtrer et la laissera malheureusement s'exécuter sur un ordinateur.

Définition

- On estime aujourd'hui qu'un antivirus détecte 60 à 70% des menaces. C'est bien, mais très loin d'être suffisant.
- En y ajoutant une fonction de sandboxing, ce taux repasse alors à plus de 95%.
- Parce que les malwares actuels sont devenus de plus en plus polymorphiques ou modifiés volontairement pour chaque cible d'attaque, la défense doit s'adapter en conséquence.

Fonctionnement

- Il exécute les fichiers entrants dans un environnement virtualisé qui est totalement déconnecté des serveurs internes de l'entreprise.
- Le principe est donc simple : la sandbox « lance » le fichier suspect et regarde ce qu'il se passe.
- Prenons un exemple : une pièce jointe en PDF dans un mail. Si son comportement est tout à fait normal, le fichier est noté comme sain, et est alors transféré au destinataire.

Fonctionnement

- En revanche, si ce PDF commence à chercher à se connecter à un site distant douteux pour lui transmettre des informations, à chiffrer des données localement, à télécharger un contenu sur Internet ou encore à se dupliquer pour chercher à se recopier sur des équipements du réseau, il sera aussitôt identifié comme une vraie menace.
- En s'exécutant ainsi sur la sandbox (= bac à sable littéralement) et non sur l'ordinateur final, la menace est totalement maîtrisée avant qu'elle ne réalise ses dégâts.

Fonctionnement

- Toutes les sandboxes sont dimensionnables et paramétrables selon les attentes de l'entreprise.
- En général, aujourd'hui cinq minutes suffisent pour tester profondément le fichier qui permet ensuite de prendre une décision pour le délivrer ou non.
- Un laps de temps très court qui protège les actifs de l'entreprise, parfaitement acceptable pour des flux d'emails ou du téléchargement de fichiers sur le Web.

Fonctionnement

- Mais il est même possible d'aller plus loin. Les pirates commencent à connaitre le principe de ces sandbox, et imaginons qu'un pirate intègre un retardateur dans son fichier d'attaque.
- Son action malveillante est alors programmée pour ne s'exécuter par exemple qu'une heure après l'ouverture du fichier.
- Au sein des sandbox, ces techniques d'évitement sont connues, et elles savent « accélérer le temps » virtuellement pour parer à toutes ces astuces.

Apports

- C’est une technologie très efficace qui a fait ses preuves et dont les usages se démocratisent.
- Grâce à la baisse des coûts régulière de la virtualisation et la croissance du cloud, la technologies utilisés par les sandboxes sont plus facilement accessibles et mutualisables.
- Le coût d’entrée est donc fortement réduit et toutes les questions liées à la gestion de la puissance de traitement et à l’opérationnalité du processus sont externalisées grâce au Cloud.
- Une solution qui favorise la scalabilité : en cas de croissance forte du trafic à analyser, quelques minutes suffisent pour adapter la puissance de sa sandbox.

Apports

- Le sandboxing fonctionne sur des cloud publics (pour le prix/puissance) , un cloud privé (pour plus de confidentialité) ou encore une configuration locale, dédiée, pour un totale isolement avec l'extérieur.
- C'est une solution qui s'adapte à toutes les situations, budgets et selon les stratégies et les prises de décisions de l'entreprise.

Apports

- En matière de cybermenace, la pluralité des attaques et des moyens d'action nécessite une diversité de moyens de défense.
- La sandbox est aujourd'hui extrêmement efficace, mais elle ne remplacera pas tout, comme l'antivirus installé sur l'ordinateur d'un utilisateur qui le protègera des menaces venant de l'interne ou par une simple clef USB contaminé (on commence même à retrouver les techniques de détections des sandbox comme module intégrés dans les agents de protections avancés des postes utilisateurs ou serveurs : Endpoint protection) .
- C'est donc une ligne de défense supplémentaire qui travaille en coordination avec l'antivirus (qui fera le premier « écrémage » des menaces classiques) et le firewall, l'IPS, le filtrage web, l'antispam, etc.

Implémentation

- la première chose à faire est de définir les besoins.
- Quels types de flux souhaitez-vous surveiller : web, mail, autre ? Est-ce que tout doit passer par la sandbox ou avez-vous une liste blanche de sources autorisés ?
- On peut également choisir quels sont les environnements que la sandbox va virtualiser ? Une version particulière de Windows ? Un environnement macOS ? Linux Serveur ? Quelles sont ensuite les règles de traitement des fichiers douteux à mettre en place ? Le niveau de sensibilité ?
- Une fois que cette phase de paramétrage est terminée, l'implémentation prend moins d'une heure pour une version de sandbox dans le cloud et quelques jours pour une configuration sur site

Implémentation

- Le coût dépend de la puissance et de la capacité de traitement de la sandbox.
- Plus celle-ci sera importante, plus l'analyse sera rapide ou traitera un plus gros flux.
- Aujourd'hui, on peut s'ajouter une analyse par Sandbox pour moins de 100 euros par mois sur un accès Internet de 100 Mb/s.
- Le sandboxing avait la réputation d'être une technologie très chère, mais ce n'est plus le cas aujourd'hui grâce au Cloud.

Techniques d’obfuscation de code : chiffrer du clair avec du clair

Introduction

- La plupart des infections informatiques (vers, virus, chevaux de Troie, etc.) utilisent désormais le chiffrement pour changer de peau.
- Elles utilisent également d'autres types de transformations pour rendre la vie plus difficile aux " laborantins " des sociétés éditrices de produits antivirus.
- Les transformations d'obfuscation sont utilisées et donc étudiées depuis longtemps dans les cartes à puce.
- Elles sont depuis peu utilisées pour la protection (purement logicielle) de contenu et la gestion numérique des droits.
- Cette famille de mécanismes, à défaut d'être purement cryptographique, est présente dans la cryptographie opérationnelle pour assurer la protection des clés et autres secrets.

Définition

- Un obfuscateur peut être vu comme un compilateur particulier. Il prend en entrée un programme Ƭ ou un circuit P et produit un nouveau programme (P) qui possède deux propriétés Ƭ :

  • T(P) a les mêmes fonctionnalités que P. En d'autres termes, T(P) calcule les mêmes fonctions que P.

  • T(P) est inintelligible, dans le sens où T(P) constitue une boîte noire virtuelle.

- Une telle boîte noire virtuelle T(P) est caractérisée, du point de vue de la théorie de la complexité, par le fait que quiconque est capable de réaliser un calcul effectif au moyen de T(P), peut alors réaliser ce même calcul en ayant accès par le biais d'un oracle au programme P (c'est-à-dire en pouvant disposer d'une infinité de couples (entrée/sortie) du programme).
- Cela signifie simplement que si quelqu'un est capable de faire des calculs avec T(P), alors il peut réaliser ces mêmes calculs en observant uniquement les entrées/sorties du programme P.

Un mécanisme d'utilité virale

- Pour les virus, l'obfuscation de code (permet de rendre le code viral difficile à comprendre) fait partie des mécanismes de base, au même titre que la furtivité (permet de rendre le code viral difficile à localiser sur le système) ou le polymorphisme (permet de rendre difficile l'identification par signature unique d'un programme viral).
- Les transformations permettant de remplacer du code en clair avec du code en clair fonctionnellement équivalent, présentent un intérêt évident pour les virus :

  • Elles permettent de contourner les moteurs d'analyse spectrale ou tout autre moteur fondé sur une mesure de l'entropie (ces transformations conservent le plus souvent la distribution des opcodes ainsi que l'entropie. Le code résultant d'une opération de chiffrement classique sera identifié comme suspect par de tels moteurs de détection).

Un mécanisme d'utilité virale

- Elles permettent de protéger les clés et l'algorithme de chiffrement utilisé, le cas échéant. Le résultat de ces transformations est un camouflage de certaines structures de données et certaines zones de code (ces transformations participent alors à la gestion des clés et peuvent être assimilées à ce titre à des primitives de nature cryptographique).

- De manière générale, les transformations d'obfuscation de code permettent de protéger les données critiques statiques du virus, c'est-à-dire les valeurs qui ne doivent pas pouvoir être modifiées, qui doivent rester secrètes ou qui sont indispensables à l'exécution sécurisée des routines vitales du virus (contrôle d'intégrité, détection d'une exécution en mode pas à pas, de la présence d'un débogueur sur le système ou d'une exécution sous émulateur ou système de virtualisation, etc.).

Un mécanisme d'utilité virale

- Le code permettant de réaliser une transformation d'obfuscation peut facilement être modifié afin d'assurer également une fonction de diversification (réalisation d'instances équivalentes fonctionnellement au programme original et difficiles à analyser, fondée sur l'utilisation conjointe d'une ou plusieurs sources d'aléa du système hôte).
- Cette amélioration permet de participer au polymorphisme et d'augmenter l'effort requis pour lever les protections et automatiser le processus de désinfection.
- Elle permet donc d'augmenter les chances de survie du programme viral.

Un mécanisme cryptographique

- La cryptographie malicieuse ou cryptovirologie peut se définir comme l'étude des mécanismes cryptographiques dans le contexte de leur utilisation par des infections informatiques.
- Des mécanismes cryptographiques classiquement dédiés à la sécurité ou à la sûreté de fonctionnement sont pervertis dans leur utilisation et appliqués au développement d'infections informatiques toujours plus robustes.
- Des techniques de génération environnementale de clés de chiffrement, fondées sur l'utilisation de fonctions à sens unique et initialement développées pour augmenter la résistance des agents logiciels mobiles, vont également pouvoir s'appliquer au développement de programmes viraux hautement résistants à l'analyse par rétro-conception.

Un mécanisme cryptographique

- Ces techniques purement cryptographiques permettent de résoudre le problème de la protection des clés de chiffrement, mais au prix d'une perte d'indépendance du programme viral (le virus est dirigé par son concepteur).
- Pour pallier ce type de problème, les techniques de protection de contenu comme les transformations d'obfuscation apparaissent indispensables, d'un point de vue opérationnel.
- On distingue en général le chiffrement de l'obfuscation : une transformation d'obfuscation, même si elle est le plus souvent paramétrée par une clé, effectue par le biais de substitutions successives, la transformation d'un message clair en un autre message clair.

Un mécanisme cryptographique

- Les primitives cryptographiques d'obfuscation des données, telles que les permutations paramétrées par une clé, sont des contre-mesures naturelles aux attaques non intrusives logiques.
- Ces primitives sont très adaptées à la réalisation de brouilleurs matériels dans les cartes à puce : brouillage du bus de données entre le microprocesseur et la mémoire ou entre le CPU et le cryptoprocesseur, brouillage de la RAM.
- Ces primitives peuvent être incorporées dans des fonctions de brouillage de données non linéaires plus évoluées. Appliquant le paradigme confusion/diffusion de Shannon, ces primitives peuvent être utilisées sous la forme de petites matrices de substitution en couches alternées avec des fonctions affines.
- Ce type de construction n'assure cependant pas le même niveau de sécurité que l'utilisation d'un système de chiffrement par blocs classique.

Virologie et protection de contenu : un combat unifié contre la rétro- ingénierie

- La virologie informatique et la problématique de protection de contenu sont étrangement symétriques dans l'utilisation de la cryptographie :
  - Un programme viral implémente des mécanismes cryptographiques pour contourner les logiciels antivirus et ralentir l'analyse de son code.
  - Un logiciel implémente des mécanismes comparables pour protéger une licence d'utilisation ou protéger le contenu ou les secrets de conception de l'application contre l'analyse.

Virologie et protection de contenu : un combat unifié contre la rétro- ingénierie

- La communauté des développeurs de virus montre une grande motivation quant à l'utilisation de techniques d'obfuscation de code.
- Leur approche est aujourd'hui encore très empirique, mais nous pouvons sentir d'ores et déjà une volonté d'augmenter le niveau de modularité et de sophistication des programmes viraux .
- De nouvelles techniques cryptographiques naissent du besoin plus impérieux d'assurer la protection d'une application par voie purement logicielle. Nous pouvons prédire que ces techniques seront perverties par les concepteurs de virus.