Sécurité : Comment piéger les logiciels malveillants.
Sécurité
Posté par : JulieM
Publiée le : 17/12/2013 13:30:00

L'émulation des menaces est une nouvelle technique clé pour stopper les attaques, « zero-day » et ciblées. **Thierry Karsenti**, Directeur Technique Europe de Check Point, explique comment cette méthode offre une protection inégalée contre les menaces connues et inconnues.

« Connaître son ennemi aussi bien que soi-même » est une maxime souvent citée dans le milieu de la sécurité informatique. Mais avec le nombre et la complexité des cyberattaques, apprendre à connaître son ennemi est une tâche énorme. Les agresseurs se bousculent chaque jour aux portes des entreprises. Ils déploient un nombre impressionnant de logiciels malveillants pour tenter de perturber l'activité des entreprises et siphonner furtivement des données confidentielles. Les entreprises continuent d'être vulnérables aux attaques « zero-day », si l'on en veut

pour preuve le volume de nouveaux logiciels malveillants capables de se cacher dans des fichiers inoffensifs. Bien que nous ne puissions pas tout savoir de nos ennemis, les nouvelles technologies de sécurité peuvent fournir des renseignements vitaux pour identifier et neutraliser les nouveaux risques qui voient le jour quotidiennement.

La cybercriminalité est devenue une grande entreprise, et comme dans n'importe quel autre secteur d'activité, les criminels cherchent à augmenter leurs revenus et accroître leurs parts de marché.

Ils ciblent des centaines voire des milliers d'entreprises, pour augmenter leurs chances de succès. Rien qu'en 2012, de 70 000 à 100 000 nouveaux échantillons de logiciels malveillants ont été créés et diffusés chaque jour, soit plus de 10 fois plus par jour qu'en 2011 et plus de 100 fois plus qu'en 2006.

Le Rapport Sécurité 2013 de Check Point a constaté que 63% des entreprise sont infectées par des bots, et plus de la moitié sont infectées par de nouveaux logiciels malveillants au moins une fois par jour. Il s'avère impossible pour les approches antimalwares traditionnelles de suivre le rythme de cette croissance effrénée.

Cachés aux yeux de tous

Les logiciels malveillants furtifs sont la technique d'attaque la plus couramment utilisée. Ils sont conçus pour être difficiles à détecter par les équipes informatiques. Le code de la majorité de ces nouveaux logiciels malveillants est caché dans des types de fichiers courants que nous utilisons tous pour nos activités : emails et leurs pièces jointes, documents Word, PDF, Excel et ainsi de suite.

Des boîtes à outils de piratage permettent d'obscurcir ces scripts exécutables pour dissimuler leurs actions malveillants, par exemple la modification de la base de registre sur l'ordinateur d'un utilisateur, ou le téléchargement d'un fichier exécutable capable d'infecter un réseau.

Et même si les défenses multicouches de détection et de prévention des intrusions peuvent aider à bloquer certaines actions des logiciels malveillants, elles ne peuvent pas toujours stopper les infections atteignant le réseau et s'y propageant.

Ces menaces exploitent de nouvelles failles ou encore des variantes de failles connues pour lesquelles il n'existe pas de signatures et donc de défenses conventionnelles pour les détecter. Tandis que les antivirus, les antispywares et autres solutions de protection similaires sont utiles pour « nettoyer » après une attaque, ils sont inefficaces comme moyen de défense contre ces nouveaux types d'attaques.

Tout comme les contrôles frontaliers d'un pays font appel à différentes techniques pour observer les individus qui entrent et identifier ceux qui représentent une menace, de nouvelles techniques de sécurité permettent de scruter les emails, les fichiers et les données qui entrent dans un réseau en temps réel. Les fichiers malveillants peuvent être isolés sur la passerelle à la périphérie du réseau ou dans le Cloud, selon le choix de l'entreprise, de manière à empêcher les infections. Cette couche externe protège contre les attaques sans impacter l'activité de l'entreprise.

À la recherche des logiciels malveillants

Ce processus d'isolation et d'évaluation est effectué à l'aide d'une technique appelée « émulation des menaces ». À la manière des scanners à rayons X installés aux frontières, cette technique permet de regarder à l'intérieur des fichiers suspects qui arrivent dans la passerelle, qu'il s'agisse de pièces jointes d'emails ou de fichiers téléchargés depuis le web, et d'inspecter leur contenu dans une zone de quarantaine virtualisée appelée « bac à sable ». Cette version virtualisée et isolée d'un environnement informatique agit comme une zone de sécurité permettant l'exécution des différentes applications à risque ou destructives.

Les fichiers y sont ouverts et surveillés pour détecter tout comportement inhabituel en temps réel, tel que les tentatives de changements anormaux de la base de registre ou les connexions réseau non autorisées. Lorsqu'un comportement est jugé suspect ou malveillant, le fichier est bloqué et mis en quarantaine, empêchant ainsi toute infection d'atteindre le réseau et entraîner des dommages. À ce stade, d'autres actions peuvent être effectuées pour identifier et classifier la nouvelle menace afin de faciliter toute identification ultérieure.

Regardons maintenant de plus près comment l'émulation des menaces identifie de nouveaux types d'attaques et de logiciels malveillants pour lesquels il n'existe pas de signatures, et comment elle met fin à ces nouvelles attaques furtives.

Construction du bac à sable

Le moteur d'émulation des menaces et le bac à sable sont gérés par un hyperviseur, qui exécute simultanément plusieurs environnements : Windows XP, 7 et 8 ; Office 2003, 2007 et 2010 ; et Adobe 9, ainsi que des instances virtualisées des applications de bureautique les plus couramment utilisées, telles que Word, Excel, PowerPoint et autres. Comme l'écrasante majorité des logiciels malveillants modernes utilise des méthodes d'ingénierie sociale pour inciter les utilisateurs à cliquer sur des pièces jointes ou télécharger des fichiers semblant légitimes, l'inspection des fichiers utilisant ces environnements et applications courantes est le meilleur moyen d'empêcher les infections.

La sélection des fichiers jugés suspects et devant être inspectés à savoir, le cheminement vers le bac à sable se déroule soit au niveau des passerelles de sécurité de l'entreprise soit dans le Cloud, à l'aide d'un agent fonctionnant en parallèle du serveur de messagerie de l'entreprise. Cette sélection peut même se faire dans le trafic chiffré des tunnels SSL et TLS qui contournent habituellement de nombreuses implémentations de sécurité.

Le processus de sélection se fait à l'aide d'une combinaison de méthodes heuristiques et d'autres méthodes d'analyse. Par exemple, lorsque plusieurs instances d'un même fichier ont déjà été mises en cache dans la passerelle ou par l'agent de messagerie, le système peut considérer que le fichier fait partie d'une tentative de phishing visant plusieurs employés. Cette approche optimise et

accélère l'analyse en ne choisissant que les fichiers suspects pour une inspection plus approfondie. Lorsque des fichiers sont sélectionnés, ils sont ensuite envoyés au bac à sable contenant le moteur d'émulation, qui fonctionne soit sur la passerelle de sécurité soit dans le Cloud.

Détection des menaces

Les fichiers envoyés au moteur d'émulation des menaces sont copiés et lancés dans plusieurs systèmes d'exploitation et environnements applicatifs virtuels. Ils sont ensuite soumis à un processus d'inspection en cinq étapes :

1. Tout fichier entraînant le mal fonctionnement de l'instance virtualisée du programme, ou tentant de décompresser et substituer un autre document, est signalé comme étant malveillant. De plus, toute tentative d'appel d'un fichier .dll ou .exe signale un comportement potentiellement anormal et malveillant.

2. La base de registre virtuelle est analysée pour détecter toute tentative de modification, qui est une caractéristique des logiciels malveillants et une action qu'un document courant ne devrait jamais tenter.

3. Le système de fichiers et les processus sont également analysés à la recherche de toute tentative de modification apportée. Comme indiqué ci-dessus, un document ordinaire ne devrait pas tenter de faire des changements.

4. Le moteur vérifie toute tentative de communication avec le web, par exemple, pour communiquer avec un centre de commande et de contrôle ou télécharger du code malveillant.

5. Enfin, le moteur consigne et génère un rapport de toutes les activités effectuées par le fichier, avec des captures d'écran des environnements virtuels, et crée une « empreinte numérique » du fichier qui peut être rapidement utilisée lors de détections ultérieures.

Les fichiers malveillants détectés par le moteur sont placés en quarantaine afin qu'ils n'atteignent pas l'utilisateur final et n'infectent pas le réseau. Même le code malveillant prévu pour détecter son exécution dans un environnement virtualisé n'est pas à l'abri du bac à sable. Ce type de code malveillant tente de camoufler ses actions ou d'agir de manière inoffensive dans l'environnement afin de contourner la détection. Toutefois, cette activité de camouflage contribue effectivement à identifier une intention malveillante. Cette tentative de déguisement est reconnue par le moteur d'émulation et consignée en tant qu'activité suspecte.

La totalité de ce processus se déroule de manière transparente pour la majorité des fichiers, ce qui signifie que, même dans les rares cas où un fichier est inspecté et marqué comme étant « sain », le destinataire du fichier ne remarque aucun impact dans son service de messagerie. Les informations relatives aux activités des fichiers sont mises à disposition de l'équipe informatique dans un rapport détaillé des menaces.

Partage d'informations sur les menaces au niveau mondial

Et si après la détection et le blocage d'un fichier par ce moyen, les entreprises étaient en mesure de partager les informations sur cette nouvelle menace pour aider d'autres entreprises à stopper également l'infection ? Après tout, la nouvelle menace a été identifiée et son empreinte numérique a été créée, ce qui signifie que les infections résultantes peuvent être évitées.

C'est le principe du service Check Point ThreatCloud, qui permet de diffuser les connaissances acquises au sujet d'un nouvel ennemi. De la même façon que les organismes de santé collaborent à l'échelle mondiale pour lutter contre les infections émergentes, développer des vaccins et autres traitements, l'approche collaborative de ThreatCloud réduit les délais entre la découverte d'une

nouvelle attaque et la possibilité de s'en protéger. Dès qu'une nouvelle menace est identifiée, les détails la concernant (y compris les descripteurs clés tels que son adresse IP, son URL ou son DNS) sont communiqués à ThreatCloud et automatiquement partagés avec les abonnés du service à travers le monde.

Lorsqu'une nouvelle menace est par exemple utilisée comme attaque ciblée sur une banque à Hong Kong et est identifiée par l'émulation des menaces, la nouvelle signature peut être appliquée en quelques minutes à des passerelles disséminées dans le monde entier. En vaccinant les entreprises contre les attaques avant que les infections ne se propagent, l'émulation des menaces empêche ces infections de se transformer en épidémies et améliore la sécurité pour tous.

Donc même si les cybercriminels ciblent des centaines ou des milliers d'entreprises, l'émulation des menaces peut jouer un rôle clé dans la protection des entreprises contre de nouvelles souches de logiciels malveillants et d'attaques « zero-day ». L'utilisation de l'émulation des menaces pour « connaître son ennemi » pourrait devenir l'une des méthodes les plus robustes pour sécuriser les réseaux des entreprises, en créant une nouvelle première ligne de défense contre les logiciels malveillants.