SÃ©curitÃ© : Comment piÃ©ger les logiciels malveillants.
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 17/12/2013 13:30:00

L'Ã©mulation des menaces est une nouvelle technique clÃ© pour stopper les attaques, Â« zero-day Â» et ciblÃ©es. **Thierry Karsenti**, Directeur Technique Europe de Check Point, explique comment cette mÃ©thode offre une protection inÃ©galÃ©e contre les menaces connues et inconnues.

Â« ConnaÃ®tre son ennemi aussi bien que soi-mÃªme Â» est une maxime souvent citÃ©e dans le milieu de la sÃ©curitÃ© informatique. Mais avec le nombre et la complexitÃ© des cyberattaques, apprendre Ã connaÃ®tre son ennemi est une tÃ¢che Ã©norme. Les agresseurs se bousculent chaque jour aux portes des entreprises. Ils dÃ©ploient un nombre impressionnant de logiciels malveillants pour tenter de perturber l'activitÃ© des entreprises et siphonner furtivement des donnÃ©es confidentielles. Les entreprises continuent d'Ãªtre vulnÃ©rables aux attaques Â« zero-day Â», 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 sÃ©curitÃ© peuvent fournir des renseignements vitaux pour identifier et neutraliser les nouveaux risques qui voient le jour quotidiennement.

La cybercriminalitÃ© est devenue une grande entreprise, et comme dans n'importe quel autre secteur d'activitÃ©, les criminels cherchent Ã augmenter leurs revenus et accroÃ®tre leurs parts de marchÃ©.

Ils ciblent des centaines voire des milliers d'entreprises, pour augmenter leurs chances de succÃ¨s. Rien qu'en 2012, de 70 000 Ã 100 000 nouveaux Ã©chantillons de logiciels malveillants ont Ã©tÃ© crÃ©Ã©s et diffusÃ©s chaque jour, soit plus de 10 fois plus par jour qu'en 2011 et plus de 100 fois plus qu'en 2006.

Le Rapport SÃ©curitÃ© 2013 de Check Point a constatÃ© que 63% des entreprise sont infectÃ©es par des bots, et plus de la moitiÃ© sont infectÃ©es par de nouveaux logiciels malveillants au moins une fois par jour. Il s'avÃ¨re impossible pour les approches antimalwares traditionnelles de suivre le rythme de cette croissance effrÃ©nÃ©e.

CachÃ©s aux yeux de tous

Les logiciels malveillants furtifs sont la technique d'attaque la plus couramment utilisÃ©e. Ils sont conÃ§us pour Ãªtre difficiles Ã dÃ©tecter par les Ã©quipes informatiques. Le code de la majoritÃ© de ces nouveaux logiciels malveillants est cachÃ© dans des types de fichiers courants que nous utilisons tous pour nos activitÃ©s : emails et leurs piÃ¨ces jointes, documents Word, PDF, Excel et ainsi de suite.

Des boÃ®tes Ã outils de piratage permettent d'obscurcir ces scripts exÃ©cutables pour dissimuler leurs actions malveillants, par exemple la modification de la base de registre sur l'ordinateur d'un utilisateur, ou le tÃ©lÃ©chargement d'un fichier exÃ©cutable capable d'infecter un rÃ©seau.

Et mÃªme si les dÃ©fenses multicouches de dÃ©tection et de prÃ©vention des intrusions peuvent aider Ã bloquer certaines actions des logiciels malveillants, elles ne peuvent pas toujours stopper les infections atteignant le rÃ©seau 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 dÃ©fenses conventionnelles pour les dÃ©tecter. Tandis que les antivirus, les antispywares et autres solutions de protection similaires sont utiles pour Â« nettoyer Â» aprÃ¨s une attaque, ils sont inefficaces comme moyen de dÃ©fense contre ces nouveaux types d'attaques.

Tout comme les contrÃ´les frontaliers d'un pays font appel Ã diffÃ©rentes techniques pour observer les individus qui entrent et identifier ceux qui reprÃ©sentent une menace, de nouvelles techniques de sÃ©curitÃ© permettent de scruter les emails, les fichiers et les donnÃ©es qui entrent dans un rÃ©seau en temps rÃ©el. Les fichiers malveillants peuvent Ãªtre isolÃ©s sur la passerelle Ã la pÃ©riphÃ©rie du rÃ©seau ou dans le Cloud, selon le choix de l'entreprise, de maniÃ¨re Ã empÃªcher les infections. Cette couche externe protÃ¨ge contre les attaques sans impacter l'activitÃ© de l'entreprise.

Ã la recherche des logiciels malveillants

Ce processus d'isolation et d'Ã©valuation est effectuÃ© Ã l'aide d'une technique appelÃ©e Â« Ã©mulation des menaces Â». Ã la maniÃ¨re des scanners Ã rayons X installÃ©s aux frontiÃ¨res, cette technique permet de regarder Ã l'intÃ©rieur des fichiers suspects qui arrivent dans la passerelle, qu'il s'agisse de piÃ¨ces jointes d'emails ou de fichiers tÃ©lÃ©chargÃ©s depuis le web, et d'inspecter leur contenu dans une zone de quarantaine virtualisÃ©e appelÃ©e Â« bac Ã sable Â». Cette version virtualisÃ©e et isolÃ©e d'un environnement informatique agit comme une zone de sÃ©curitÃ© permettant l'exÃ©cution des diffÃ©rentes applications Ã risque ou destructives.

Les fichiers y sont ouverts et surveillÃ©s pour dÃ©tecter tout comportement inhabituel en temps rÃ©el, tel que les tentatives de changements anormaux de la base de registre ou les connexions rÃ©seau non autorisÃ©es. Lorsqu'un comportement est jugÃ© suspect ou malveillant, le fichier est bloquÃ© et mis en quarantaine, empÃªchant ainsi toute infection d'atteindre le rÃ©seau et entraÃ®ner des dommages. Ã ce stade, d'autres actions peuvent Ãªtre effectuÃ©es pour identifier et classifier la nouvelle menace afin de faciliter toute identification ultÃ©rieure.

Regardons maintenant de plus prÃ¨s comment l'Ã©mulation 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 Ã ces nouvelles attaques furtives.

Construction du bac Ã sable

Le moteur d'Ã©mulation des menaces et le bac Ã sable sont gÃ©rÃ©s par un hyperviseur, qui exÃ©cute simultanÃ©ment plusieurs environnements : Windows XP, 7 et 8 ; Office 2003, 2007 et 2010 ; et Adobe 9, ainsi que des instances virtualisÃ©es des applications de bureautique les plus couramment utilisÃ©es, telles que Word, Excel, PowerPoint et autres. Comme l'Ã©crasante majoritÃ© des logiciels malveillants modernes utilise des mÃ©thodes d'ingÃ©nierie sociale pour inciter les utilisateurs Ã cliquer sur des piÃ¨ces jointes ou tÃ©lÃ©charger des fichiers semblant lÃ©gitimes, l'inspection des fichiers utilisant ces environnements et applications courantes est le meilleur moyen d'empÃªcher les infections.

La sÃ©lection des fichiers jugÃ©s suspects et devant Ãªtre inspectÃ©s â Ã savoir, le cheminement vers le bac Ã sable â se dÃ©roule soit au niveau des passerelles de sÃ©curitÃ© de l'entreprise soit dans le Cloud, Ã l'aide d'un agent fonctionnant en parallÃ¨le du serveur de messagerie de l'entreprise. Cette sÃ©lection peut mÃªme se faire dans le trafic chiffrÃ© des tunnels SSL et TLS qui contournent habituellement de nombreuses implÃ©mentations de sÃ©curitÃ©.

Le processus de sÃ©lection se fait Ã l'aide d'une combinaison de mÃ©thodes heuristiques et d'autres mÃ©thodes d'analyse. Par exemple, lorsque plusieurs instances d'un mÃªme fichier ont

dÃ©jÃ Ã©tÃ© mises en cache dans la passerelle ou par l'agent de messagerie, le systÃ¨me peut considÃ©rer que le fichier fait partie d'une tentative de phishing visant plusieurs employÃ©s. Cette approche optimise et accÃ©lÃ¨re l'analyse en ne choisissant que les fichiers suspects pour une inspection plus approfondie. Lorsque des fichiers sont sÃ©lectionnÃ©s, ils sont ensuite envoyÃ©s au bac Ã sable contenant le moteur d'Ã©mulation, qui fonctionne soit sur la passerelle de sÃ©curitÃ© soit dans le Cloud.

DÃ©tection des menaces

Les fichiers envoyÃ©s au moteur d'Ã©mulation des menaces sont copiÃ©s et lancÃ©s dans plusieurs systÃ¨mes d'exploitation et environnements applicatifs virtuels. Ils sont ensuite soumis Ã un processus d'inspection en cinq Ã©tapes :

1. Tout fichier entraÃ®nant le mal fonctionnement de l'instance virtualisÃ©e du programme, ou tentant de dÃ©compresser et substituer un autre document, est signalÃ© comme Ã©tant 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 analysÃ©e pour dÃ©tecter toute tentative de modification, qui est une caractÃ©ristique des logiciels malveillants et une action qu'un document courant ne devrait jamais tenter.

3. Le systÃ¨me de fichiers et les processus sont Ã©galement analysÃ©s Ã la recherche de toute tentative de modification apportÃ©e. Comme indiquÃ© ci-dessus, un document ordinaire ne devrait pas tenter de faire des changements.

4. Le moteur vÃ©rifie toute tentative de communication avec le web, par exemple, pour communiquer avec un centre de commande et de contrÃ´le ou tÃ©lÃ©charger du code malveillant.

5. Enfin, le moteur consigne et gÃ©nÃ¨re un rapport de toutes les activitÃ©s effectuÃ©es par le fichier, avec des captures d'Ã©cran des environnements virtuels, et crÃ©e une Â« empreinte numÃ©rique Â» du fichier qui peut Ãªtre rapidement utilisÃ©e lors de dÃ©tections ultÃ©rieures.

Les fichiers malveillants dÃ©tectÃ©s par le moteur sont placÃ©s en quarantaine afin qu'ils n'atteignent pas l'utilisateur final et n'infectent pas le rÃ©seau. MÃªme le code malveillant prÃ©vu pour dÃ©tecter son exÃ©cution dans un environnement virtualisÃ© n'est pas Ã l'abri du bac Ã sable. Ce type de code malveillant tente de camoufler ses actions ou d'agir de maniÃ¨re inoffensive dans l'environnement afin de contourner la dÃ©tection. Toutefois, cette activitÃ© de camouflage contribue effectivement Ã identifier une intention malveillante. Cette tentative de dÃ©guisement est reconnue par le moteur d'Ã©mulation et consignÃ©e en tant qu'activitÃ© suspecte.

La totalitÃ© de ce processus se dÃ©roule de maniÃ¨re transparente pour la majoritÃ© des fichiers, ce qui signifie que, mÃªme dans les rares cas oÃ¹ un fichier est inspectÃ© et marquÃ© comme Ã©tant Â« sain Â», le destinataire du fichier ne remarque aucun impact dans son service de messagerie. Les informations relatives aux activitÃ©s des fichiers sont mises Ã disposition de l'Ã©quipe informatique dans un rapport dÃ©taillÃ© des menaces.

Partage d'informations sur les menaces au niveau mondial

Et si aprÃ¨s la dÃ©tection et le blocage d'un fichier par ce moyen, les entreprises Ã©taient en mesure de partager les informations sur cette nouvelle menace pour aider d'autres entreprises Ã stopper Ã©galement l'infection ? AprÃ¨s tout, la nouvelle menace a Ã©tÃ© identifiÃ©e et son empreinte numÃ©rique a Ã©tÃ© crÃ©Ã©e, ce qui signifie que les infections rÃ©sultantes peuvent Ãªtre Ã©vitÃ©es.

C'est le principe du service Check Point ThreatCloud, qui permet de diffuser les connaissances acquises au sujet d'un nouvel ennemi. De la mÃªme faÃ§on que les organismes de santÃ© collaborent Ã l'Ã©chelle mondiale pour lutter contre les infections Ã©mergentes, dÃ©velopper des vaccins et autres traitements, l'approche collaborative de ThreatCloud rÃ©duit les dÃ©lais entre la dÃ©couverte d'une nouvelle attaque et la possibilitÃ© de s'en protÃ©ger. DÃ¨s qu'une nouvelle menace est identifiÃ©e, les dÃ©tails la concernant (y compris les descripteurs clÃ©s tels que son adresse IP, son URL ou son DNS) sont communiquÃ©s Ã ThreatCloud et automatiquement partagÃ©s avec les abonnÃ©s du service Ã travers le monde.

Lorsqu'une nouvelle menace est par exemple utilisÃ©e comme attaque ciblÃ©e sur une banque Ã Hong Kong et est identifiÃ©e par l'Ã©mulation des menaces, la nouvelle signature peut Ãªtre appliquÃ©e en quelques minutes Ã des passerelles dissÃ©minÃ©es dans le monde entier. En vaccinant les entreprises contre les attaques avant que les infections ne se propagent, l'Ã©mulation des menaces empÃªche ces infections de se transformer en Ã©pidÃ©mies et amÃ©liore la sÃ©curitÃ© pour tous.

Donc mÃªme si les cybercriminels ciblent des centaines ou des milliers d'entreprises, l'Ã©mulation des menaces peut jouer un rÃ´le clÃ© dans la protection des entreprises contre de nouvelles souches de logiciels malveillants et d'attaques Â« zero-day Â». L'utilisation de l'Ã©mulation des menaces pour Â« connaÃ®tre son ennemi Â» pourrait devenir l'une des mÃ©thodes les plus robustes pour sÃ©curiser les rÃ©seaux des entreprises, en crÃ©ant une nouvelle premiÃ¨re ligne de dÃ©fense contre les logiciels malveillants.