Les 5 techniques que les cybercriminels utilisent pour pénétrer les réseaux | Le Net Expert Informatique

Il existe au moins 5 techniques de nature « discrète et graduelle » que les cybercriminels utilisent désormais pour pénétrer les réseaux et accomplir leur mission, et que les professionnels de la sécurité doivent comprendre et repérer afin de défendre plus efficacement leur entreprise :

1. Les kits d'exploits : les concepteurs de kits d'exploits connus comme Blackhole ont été repérés par les autorités et stoppés dans leurs actions. Les hackers ont ainsi réalisés que les attaques de grande ampleur ne sont pas toujours les plus efficaces – que ce soit de par la taille des infrastructures ou des moyens malveillants mis en œuvre. Ainsi les hackers préfèrent disposer du 4ème ou 5ème kit d'exploits le plus connu et utilisé, pour ne pas trop attirer l'attention.

2. Le spam « Snowshoe » : avec cette technique, le hacker diffuse beaucoup de messages sur une grande surface d'attaque pour échapper aux outils de détection traditionnels. Le spammeur Snowshoe envoie un email non sollicité en utilisant un grand nombre d'adresses IP mais à un faible volume de messages par adresse IP, avec pour objectif de contourner les technologies de réputation anti-spam basées sur l'adresse IP. Il change rapidement le corps du texte, les liens, les adresses IP utilisées pour la diffusion et ne répète jamais la même combinaison.

3. Le spear phishing sophistiqué : les hackers continuent d'affiner leurs messages, bien souvent en utilisant des techniques d'ingénierie sociale, de sorte que même les internautes expérimentés ont du mal à repérer les faux messages. Les récentes attaques de spear phishing semblent provenir de fournisseurs ou d'opérateurs connus, desquels les utilisateurs reçoivent régulièrement des messages – par exemple, les prestataires de services, les sites de vente en ligne et les fournisseurs de contenus musicaux et de loisirs. Ces emails peuvent contenir un nom de confiance, un logo connu et inviter le destinataire à réaliser une action familière, comme donner son avis à propos d'une commande récente, ou donner un numéro pour le suivi de sa livraison. Cette mécanique bien huilée et discrète donne aux utilisateurs un faux sentiment de sécurité, les incitant à cliquer sur des liens malveillants contenus dans l'e-mail.

4. Le partage d'exploits entre deux fichiers différents : les malwares Flash peuvent désormais interagir avec JavaScript pour cacher des activités malveillantes en partageant un exploit entre deux fichiers et formats différents : un fichier Flash, un fichier JavaScript. Cela dissimule l'activité malveillante et rend l'identification, le blocage ainsi que l'analyse de l'exploit beaucoup plus difficile. Cette approche permet également aux hackers d'être plus efficaces dans leurs attaques. Par exemple, si la première étape d'une attaque est entièrement en JavaScript, la seconde étape, le transfert du code malicieux, ne se produirait qu'après l'exécution avec succès du code JavaScript. De cette façon, seuls les utilisateurs qui peuvent exécuter le fichier malveillant reçoivent celui-ci.

5. Le malvertising : les créateurs de malwares ont mis au point un nouveau business modèle perfectionné qui utilise les modules publicitaires des navigateurs Web pour diffuser des logiciels malveillants et des applications indésirables. Les utilisateurs achètent, téléchargent et installent des outils tels que Adobe ou des logiciels vidéo depuis des sources qu'ils estiment légitimes. En réalité, ces applications sont livrées avec un logiciel malveillant. Cette nouvelle approche de diffusion de malwares est un succès pour les hackers car de nombreux utilisateurs font naturellement confiance aux publicités ou les considèrent comme bénignes. Les hackers gagnent de l'argent à partir d'un grand nombre utilisateurs, par petites touches, en infectant de manière persistante leur navigateur et en se cachant sur leur machine.

Les professionnels de la sécurité et les cybercriminels sont dans une course permanente pour tenter de déjouer l'autre. Les hackers sont de plus en plus professionnels, non seulement dans leurs approches pour lancer des attaques, mais aussi pour échapper aux outils de détection, par des moyens que nous n'avions pas vus jusqu'à présent. Mais en continuant à innover et à apprendre sur la base de ce qu'ils observent, les professionnels de la sécurité peuvent identifier et contrer ces nouvelles techniques d'attaques.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.informatiquenews.fr/quelles-reponses-aux-nouvelles-cyberattaques-christophe-jolly-cisco-31360
Par Christophe Jolly, Directeur Sécurité de Cisco France

La NSA et sa consœur britannique surveillent aussi les cartes SIM

Crédit : Fotolia

La NSA et sa consœur britannique surveillent aussi les cartes SIM

Aucun vecteur informatique ne semble échapper aux radars de l'agence de sécurité américaine. Cette fois, la NSA (et la GCHQ) s'est offert un accès aux clients de 450 opérateurs, via les cartes SIM.

Une nouvelle révélation sur la NSA démontre, si ce n'était pas déjà suffisant, l'étendue de la portée de l'agence de sécurité américaine. Selon le site The Intercept, l'organisation accompagnée par son homologue britannique, le GCHQ, ont toutes deux pénétré dans les réseaux informatiques du premier fabricant de cartes SIM dans le monde, le franco-néerlandais Gemalto, qui produit plus de deux milliards de cartes par an.

A ce stade, la société ciblée ne peut pas « confirmer ces informations » et souligne qu'elle n'avait « aucune connaissance préalable que ces agences gouvernementales conduisaient cette opération », rejetant donc une quelconque complicité. Gemalto indique prendre cet article « très au sérieux » et met en œuvre « tous les moyens nécessaires pour investiguer et comprendre l'étendue de ces techniques sophistiquées ».
Selon The Intercept, qui se base sur des documents fournis par le lanceur d'alertes Edward Snowden, la NSA et le GCHQ ont mis la main sur des clés de chiffrement après avoir installé un malware sur des ordinateurs de Gemalto. Pour cela, l'agence américaine aurait fait appel à son programme de surveillance XKeyscore, qui lui donne accès aux e-mails, conversations Facebook et historiques Internet, lui aussi mis au jour, en août 2013.
Ces clés, utilisées pour protéger la confidentialité des communications téléphoniques, permettent aux deux organisations d'intercepter les échanges vocaux, les SMS et les données Internet des clients mobiles.

Les clients de 450 opérateurs écoutés
En visant Gemalto, les deux consœurs ont pu toucher les clients de 450 opérateurs de téléphonie mobile dans 85 pays. « En possédant ces clés de chiffrement, les agences de renseignement peuvent surveiller les communications mobiles sans demander l'autorisation des opérateurs télécoms ni des gouvernements étrangers », écrit l'auteur de ces révélations. Il ajoute que « c'est aussi un moyen de se passer de mandat, tout en ne laissant aucune trace sur le réseau qui révéleraient que des personnes ont été mises sur écoute ».
La révélation de ce nouvel avatar de la surveillance américaine intervient alors que que le ministre de l'Intérieur, Bernard Cazeneuve, est en déplacement aux États-Unis, où il tente de mobiliser les grands acteurs comme Google et Facebook dans la lutte anti-terroriste sur Internet. S'il leur est demandé une collaboration plus étroite avec le gouvernement sur les enquêtes en cours, et une meilleure réactivité sur la suppression du contenu appelant au terrorisme, rien ne semble empêcher le travail en tâche de fond de la tentaculaire NSA.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://pro.clubic.com/it-business/securite-et-donnees/actualite-755133-sim-gemalto.html
Par Thomas Pontiroli

Alerte informatique, vague de rançongiciel, adoptez les bonnes pratiques | Le Net Expert Informatique

	Alerte informatique, vague de rançongiciel, adoptez les bonnes pratiques