Comment fonctionnent les Kits d’exploitation ?

Comment fonctionnent les Kits d’exploitation ?

Ces dernières années, nous avons observé une augmentation massive de l'utilisation des kits d'exploitation de vulnérabilités. Aucun site web n'est de taille face à la puissance d'un grand nombre de ces kits, à l'image de celui d'un célèbre quotidien britannique, notoirement victime d'une campagne de publicité malveillante exposant des millions de lecteurs au ransomware CryptoWall.

Les Exploit kits, des boites à outils faciles à utiliser

Cependant, l'aspect peut-être le plus préoccupant des kits d'exploitation tient à leur facilité d'utilisation. Ces « boîtes à outils à louer » ont principalement pour but de réduire les compétences techniques nécessaires au lancement de campagnes de malware, afin qu'un assaillant n'ait pas besoin de créer ou implanter le code malveillant lui-même. De fait, de nombreux kits s'accompagnent même désormais d'une interface ergonomique, permettant aux malfaiteurs de gérer et de surveiller leur malware tout au long d'une campagne.

La charge malveillante des kits d'exploitation se présentait jusque-là sous la forme de différentes sortes de malwares, qu'il s'agisse de fraude au clic publicitaire, de malware bancaire ou de ransomware, la nature de ces attaques variant selon le profil de l'utilisateur. Compte tenu de la facilité de personnalisation d'une attaque et de l'ergonomie des kits, il n'est guère surprenant que ceux-ci soient devenus l'arme de prédilection d'un grand nombre de cybercriminels, moins compétents sur le plan technique.

De quoi sont-ils faits ?

En règle générale, l'infrastructure d'un kit d'exploitation comprend trois composants :

- le « back-end », qui contient le tableau de commande et les charges malveillantes ;
- la couche intermédiaire, qui héberge le code malveillant et crée un tunnel dans le serveur back-end ;
- la couche proxy, qui transmet le malware directement à la victime.

La chaîne d'infection/exploitation demeure en outre largement similaire pour les différents kits :

- La victime se rend sur le site web, entièrement ou partiellement contrôlé par l'assaillant ;
- Elle est ensuite redirigée à travers de nombreux serveurs intermédiaires ;
- À son insu, elle aboutit sur le serveur hébergeant le kit d'exploitation ;
- Le kit tente alors de s'installer en exploitant une vulnérabilité logicielle sur le serveur cible ;

En cas d'installation réussie, la charge malveillante est alors activée.

La différence marquante entre les kits réside dans les types de vulnérabilités exploitées pour infecter les visiteurs et les diverses astuces employées pour échapper aux antivirus.

Vers la multiplication des cibles mobiles

Alors que les kits d'exploitation avaient traditionnellement tendance à cibler principalement les ordinateurs, les appareils mobiles sont de plus en plus visés en raison du grand nombre d'utilisateurs qui s'en servent pour surfer sur le Web, échanger des e-mails, consulter les réseaux sociaux et même pour effectuer des opérations bancaires. La plupart de ces utilisateurs n'étant pas au fait des meilleures pratiques pour sécuriser correctement leur mobile, ils offrent par essence une cible bien plus facile.

Il faut donc s'attendre à ce que les auteurs des attaques s'orientent progressivement vers la diffusion de malware mobile via des pages web sur un navigateur mobile, c'est-à-dire essentiellement le même mode d'infection que dans la plupart des cas sur les ordinateurs.

Dès lors que le virus réussit à s'implanter sur un ordinateur ou un mobile, il peut opérer derrière les firewalls d'une entreprise ou d'un particulier. Le malware se propage ainsi à d'autres équipements et se connecte au serveur de commande et de contrôle (C&C) via Internet, ce qui lui permet ensuite d'exfiltrer des données ou de télécharger d'autres logiciels malveillants. Cette communication entre le serveur C&C et la machine infectée passe souvent par le serveur de noms de domaines (DNS) de la cible.

Connaître son ennemi

Même si tous les kits d'exploitation ne sont pas identiques, il est important d'en identifier deux principaux.

Le baromètre Infoblox des menaces DNS observées au 4ème trimestre 2015 révèle que le kit Angler a représenté 56 % des nouvelles activités de ce type, et le kit RIG 20 %. En quoi consistent ces kits et leurs activités ?

Le kit d'exploitation Angler est l'un des plus élaborés actuellement utilisé par les cybercriminels. Notoirement connu pour avoir inauguré la technique du « masquage de domaine », Angler peut ainsi contrer les stratégies de blocage sur la base de la réputation et infiltrer des URL malveillantes dans des réseaux publicitaires légitimes. Il redirige ensuite les visiteurs du site web qui cliquent sur les liens publicitaires infectés vers d'autres sites qui implantent à leur tour un malware. Ces kits tendent à être actualisés avec les dernières failles « zero day » découvertes dans des logiciels répandus, tels que Apache Flash ou WordPress. Si l'on y ajoute l'utilisation de techniques complexes de dissimulation, cela rend Angler particulièrement difficile à détecter pour les solutions antivirus classiques.

Face à cette évolution constante, les entreprises doivent investir dans des technologies de protection qui non seulement bloquent un composant du kit Angler mais sont aussi capables d'identifier et d'interrompre l'activité malveillante sur l'ensemble de la chaîne d'infection.

Bien que de conception plus ancienne, le kit d'exploitation RIG a récemment fait son retour. Cela montre que les menaces passées peuvent réapparaître sous une nouvelle forme à mesure que les kits sont mis à jour. L'analyse par Infoblox de l'activité de RIG en 2015 révèle que celui-ci a commencé à utiliser des techniques de masquage de domaine similaires à celles employées par Angler.

Même si RIG est souvent déployé dans le cadre de campagnes de publicité malveillante, Heimdal Security a récemment découvert qu'il sert également pour la pollution de référencement Google, consistant à détourner les tactiques d'optimisation du moteur de recherche pour faire la promotion de sites web malveillants.

Avec leurs différentes déclinaisons et techniques, les kits d'exploitation offrent aux malfaiteurs dépourvus de compétences techniques l'opportunité de tirer profit du monde de la cybercriminalité. Pour se protéger contre cette menace sans cesse croissante, les entreprises doivent faire appel à une source fiable de veille des menaces et s'appuyer sur ces informations pour interrompre les communications des malwares passant par des protocoles au sein de leur propre infrastructure, notamment le DNS… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, arnaques Internet...) et judiciaires (contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Suivez-nous sur

Réagissez à cet article

Source : *Comment fonctionnent les Kits d’exploitation ? – Global Security Mag Online*