Rapport de synthèse

L'opération Troy sous la loupe : cyberespionnage en Corée du Sud

Ryan Sherstobitoff et Itai Liba, McAfee® Labs, et
James Walter, bureau du Directeur des Technologies (CTO) de McAfee

Lorsque l'attaque DarkSeoul lancée contre des entreprises sud-coréennes des secteurs des médias et des services financiers a commencé à faire parler d'elle au lendemain de l'offensive du 20 mars 2013, le principal sujet de discussion était la fonctionnalité d'effacement du secteur de démarrage principal. De fait, toutes les données présentes sur les disques durs des ordinateurs infectés avaient été effacées. McAfee Labs a toutefois découvert que, outre la fonctionnalité prenant pour cible le secteur de démarrage principal, l'attaque DarkSeoul fait appel à un large éventail de technologies et de tactiques.

Les données d'analyse « post-mortem » révèlent que l'attaque DarkSeoul n'est que le dernier-né d'un projet de développement de logiciels malveillants (*malware*), baptisé « Operation Troy » en raison de la présence récurrente du terme *Troy* (nom anglais de l'ancienne cité de Troie) dans les chaînes de chemin de compilation du logiciel malveillant. Premier sur le banc des suspects : le gang New Romanic Cyber Army Team, dont le code regorge de termes liés à la Rome antique. L'enquête menée par McAfee Labs sur l'incident DarkSeoul a cependant mis au jour une opération d'espionnage intérieur de longue haleine visant des cibles militaires en Corée du Sud et s'appuyant sur du code qui avait fait son apparition en 2009.

Qu'ils agissent à des fins légitimes ou criminelles, les développeurs de logiciels laissent en général des empreintes numériques et parfois même des empreintes d'impact dans leur code. Les experts en investigations numériques peuvent exploiter ces traces pour identifier à quel endroit et à quel moment le code a été créé. Bien qu'un chercheur parvienne rarement à remonter jusqu'aux développeurs individuels (à moins que ceux-ci ne fassent preuve de négligence, ce qui est inhabituel), de tels artefacts peuvent souvent servir à déterminer la source originelle d'un nouveau « produit » et à reconstituer sa généalogie de développement. Parfois, ces empreintes constituent de véritables signatures apposées à dessein par les développeurs pour revendiquer la « propriété » d'une nouvelle menace informatique, une pratique à laquelle ont recours New Romanic Cyber Army Team ou encore Poetry Group. McAfee Labs emploie des techniques sophistiquées d'analyse du code et d'analyse « post-mortem » pour identifier les sources des nouvelles menaces, car ces méthodes apportent fréquemment un éclairage sur la meilleure manière d'endiguer une attaque ou permettent de prévoir l'évolution future probable de la menace.

Historique de Troy

L'histoire d'Operation Troy débute en 2010, avec l'apparition du cheval de Troie NSTAR. Depuis lors, sept variantes connues ont été identifiées (voir le diagramme ci-dessous). Malgré un cycle de distribution plutôt rapide, les fonctionnalités de base d'Operation Troy n'ont pas beaucoup évolué. En réalité, les principales différences entre NSTAR, Chang/Eagle et HTTP Troy étaient davantage liées à la technique de programmation qu'aux fonctionnalités.

Les premières véritables améliorations sur le plan fonctionnel sont apparues avec la version Concealment Troy, au début de l'année 2013. Concealment Troy a introduit une refonte de l'architecture de contrôle et a progressé dans l'art de camoufler sa présence pour échapper aux techniques de sécurité standard.

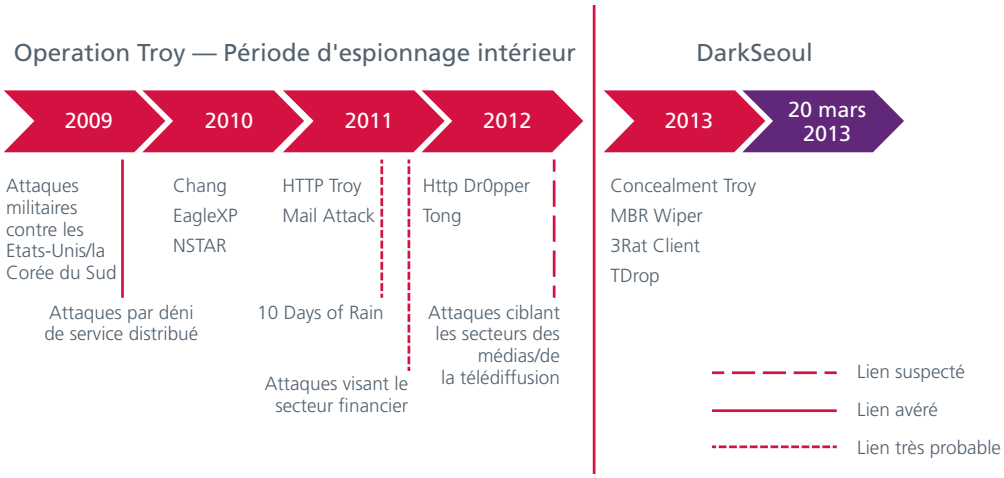

Figure 1. L'attaque DarkSeoul a été précédée de plusieurs années de cyberespionnage.

Empreintes numériques

S'il est certes intéressant de se pencher sur le passé d'Operation Troy, les empreintes numériques et d'impact qui permettent à McAfee Labs de retracer les générations antérieures de l'attaque sont encore plus révélatrices. Dans la catégorie « empreintes numériques » figure ce que les développeurs appellent le « chemin de compilation », qui n'est autre que le chemin de répertoire menant à l'emplacement où réside le code source sur l'ordinateur du développeur.

Une des premières variantes de Troy de 2010, liée à NSTAR et à HTTP Troy au travers de composants recyclés, utilisait le chemin de compilation suivant :

```
D:\VMware\eaglexp(Backup)\eaglexp\vmshare\Work\BsDll-up\Release\BsDll.pdb
```

Une deuxième variante datant de 2010, compilée le 27 mai, contenait un chemin de compilation très similaire. Nous avons pu obtenir un certain trafic avec le serveur de contrôle.

```
D:\\Chang\\vmshare\\Work\\BsDll-up\\Release\\BsDll.pdb
```

McAfee Labs a systématiquement constaté la présence du répertoire Work, de même que dans l'ensemble des logiciels malveillants apparus après 2010 utilisés dans le cadre de cette campagne. En analysant des attributs tels que le chemin de compilation, les chercheurs de McAfee Labs ont réussi à établir des liens entre les variantes de Troy et à documenter les modifications apportées à leur code à la fois sur le plan fonctionnel et de la conception.

Les variantes Chang et EagleXP sont toutes deux basées sur le code qui a servi à créer NSTAR et les variantes ultérieures de Troy. L'utilisation du même code prouve également que les cybercriminels s'en sont pris à des cibles sud-coréennes pendant plus de trois ans.

Empreintes d'impact

L'examen de la catégorie « empreintes d'impact » a permis à McAfee Labs d'attribuer la modification fonctionnelle la plus notable à la version 2013 de Concealment Troy. Auparavant, le processus de contrôle d'Operation Troy impliquait des commandes d'exploitation de routage exécutées via des serveurs IRC (Internet Relay Chat) sous camouflage.

Du point de vue de l'auteur de l'attaque, cette approche pose deux problèmes. Premièrement, si les propriétaires d'un serveur infecté découvrent les processus IRC malveillants, ils les suppriment, de sorte que l'auteur de l'attaque perd le contrôle des clients infectés par Troy. Deuxièmement, les développeurs de Troy ont en fait codé en dur le nom du serveur IRC dans chaque variante de Troy. Cela signifie qu'ils ont dû au préalable trouver un serveur vulnérable, installer un serveur IRC, puis recompiler la source de Troy dans une nouvelle variante contrôlée par ce serveur spécifique. C'est pour cette raison que pratiquement toutes les variantes de Troy devaient être contrôlées par un serveur de commande distinct.

Conclusion

Cette enquête sur les cyberattaques du 20 mars 2013 a révélé une chasse au renseignement clandestine persistante. D'après les conclusions de McAfee Labs, celles-ci ne constituaient pas un événement isolé strictement lié à la destruction de systèmes, mais plutôt la dernière attaque en date d'une vague amorcée en 2010. Pendant des années, ces opérations sont restées dissimulées sans être détectées par les mécanismes de défense technologiques en place au sein des organisations ciblées.

Un exemplaire du rapport complet est disponible à l'adresse suivante : http://www.mcafee.com/fr/resources/literature/white-papers/wp-dissecting-operation-troy.pdf.

McAfee
An Intel Company

McAfee S.A.S.
Tour Franklin, La Défense 8
92042 Paris La Défense Cedex
France
+33 1 47 62 56 00 (standard)
www.mcafee.com/fr

60360exs_operation-troy_0613_ETMG