Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 08 décembre 2014
N° CERTFR-2014-ACT-049

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-049

1 - Publication d'un rapport sur la campagne d'espionnage DarkHotel

En novembre, Kaspersky Lab a publié un rapport concernant une campagne d'espionnage nommée DarkHotel. Resté dans l'ombre pendant au moins sept ans, le groupe d'attaquants à l'origine de cette campagne a mené des attaques précises contre des clients ciblés d'hôtels de luxe en Asie mais également en diffusant des infections via des attaques d'hameçonnage ciblées (spear-phishing) et sur des réseaux pair à pair.

La campagne DarkHotel présente des caractéristiques singulières. En effet, il apparaît que les attaquants ciblent des dirigeants de grands groupes industriels en employant un mode opératoire particulier. En maintenant une compromission sur le réseau Wi-Fi d'un hôtel, les attaquants attendent que la victime se connecte sur le réseau puis vérifient son identité en utilisant le numéro de la chambre et l'identifiant de l'utilisateur. La victime est ensuite invitée à télécharger puis à installer une porte dérobée prétendant être une mise à jour d'un logiciel légitime tel que Google Toolbar, Adobe Flash ou Windows Messenger. Une fois le système de la victime infecté, des outils permettant de subtiliser des données vont être installés. Ces logiciels malveillants sont signés par des certificats compromis. Une attention particulière est portée par les attaquants afin de ne pas être détectés. En effet, après la collecte d'information, l'ensemble des outils est soigneusement désinstallé.

L'arsenal des attaquants est composé de plusieurs outils tels que des codes d'exploitations ciblant des vulnérabilités non corrigées (Zero Day) et utilisés dans des campagnes d'hameçonnage ciblées ou bien un enregistreur de frappe positionné dans le noyau Windows. Ces outils sont détectés par Kaspersky sous les noms Tapaoux, Pioneer, Karba et Nemin.

Les secteurs ciblés par la campagne sont variés, on peut citer :

- le secteur de l'énergie ;
- les sociétés d'investissement ;
- le milieu pharmaceutique ;
- les fabricants de produits cosmétique ;
- les constructeurs automobile ;
- le secteur de la défense ;
- les organisations non gouvernementales.

Devant la multiplicité de ce type de menace, il est important de prendre en compte un certain nombre de considérations avant de partir en voyage. L'ANSSI propose un guide permettant de centraliser ces recommandations.

De plus, il est primordial de considérer tous les réseaux des hôtels comme potentiellement dangereux. Il faut donc veiller à :

- télécharger des mises à jour directement sur le site de l'éditeur et non à partir de la page d'accueil de l'accès Wi-Fi de l'hôtel puis vérifier si elles sont correctement signées par ce même éditeur ;
- utiliser un VPN afin de chiffrer ses communications ;
- vérifier que l'ensemble du système d'exploitation et des logiciels utilisés sur le poste de travail sont à jour.

Documentation

– http://www.ssi.gouv.fr/passeport-de-conseils-aux-voyageurs

2 - Publication de rapports sur le code malveillant Regin

De nombreux acteurs de la sécurité informatique ont récemment publié des rapports sur un logiciel malveillant baptisé « Regin ». Le mode opératoire associé à ce code est intéressant sur plusieurs points.

En premier lieu, la méthode utilisée pour dissimuler le flux de contrôle-commande est peu courante. Dans un des exemples cités, toutes les communications malveillantes étaient chiffrées et ont transité via deux entités connues de la victime, entre lesquelles des communications SSL étaient non seulement légitimes, mais aussi coutumières. Ce constat appelle à plus de vigilance lorsque sont qualifiées de « légitimes » des communications chiffrées vers une entité réputée de confiance. L'inspection périmétrique des flux ne permet pas seule de détecter un canal ainsi conçu et doit prendre en considération la durée moyenne des sessions, la plage horaire ou encore les volumes échangés.

Le code de persistance du logiciel malveillant est très différent des techniques habituelles des RATs. Il s'agit d'une copie d'un code légitime existant (différent pour chaque victime), auquel sont adjointes quelques routines de déchiffrement et de chargement de code, et lancé au démarrage par une clef classique et évidente de la base de registre. Cette technique a plusieurs avantages pour l'attaquant. Premièrement, une analyse rapide du code (chaînes de caractères, imports, etc.) indiquera un code globalement légitime. En effet, il n'y a pas à ce stade de technique d'obscurcissement suspecte (comme une compression ou un empaquetage du binaire). De plus, les techniques de condensats partiels ou de calcul de distance entre binaires indiqueront peu de similitudes entre les versions placées sur des victimes distinctes. Celles-ci, bien qu'ayant toujours la même charge utile, seront en effet très peu semblables entre elles. Des outils trop dépendants de ces techniques risquent d'être mis en défaut.

Enfin, le niveau d'investissement de l'attaquant dans la conception d'un module qui cible les opérateurs de téléphonie témoigne du niveau de menace à prendre en compte dans les analyses de risque. Ce type de code malveillant a une excellente adaptation aux techniques de détection généralement utilisées, et appelle à remettre en question et à faire évoluer les habitudes et réflexes du traitement d'incident de sécurité.

3 - Rappel des avis émis

Dans la période du 01 au 07 décembre 2014, le CERT-FR a émis les publications suivantes :

– CERTFR-2014-AVI-503 : Multiples vulnérabilités dans les produits Mozilla
– CERTFR-2014-AVI-504 : Multiples vulnérabilités dans Citrix XenServer
– CERTFR-2014-AVI-505 : Multiples vulnérabilités dans Apple Safari
– CERTFR-2014-AVI-506 : Multiples vulnérabilités dans phpMyAdmin

Gestion détaillée du document

08 décembre 2014 version initiale.