Des cybercriminels dérobent 25M$ à des banques russes

	Des cybercriminels dérobent 25M$ à des banques russes

Un groupe de cybercriminels baptisé Anunak a réussi à infiltrer les réseaux informatiques et à détourner les distributeurs automatiques d'institutions bancaires en Russie et dans des pays voisins. Il a également ciblé des terminaux point de vente de revendeurs américains et européens.

Un groupe de cybercriminels très aguerris a volé plus de 25 millions de dollars en piratant l'infrastructure de plusieurs institutions financières russes et de pays de l'ancien bloc soviétique, et en détournant des systèmes de points de vente appartenant à des revendeurs américains et européens. Des chercheurs de l'entreprise russe spécialisée dans la cybercriminalité Group-IB, et de l'entreprise de sécurité néerlandaise Fox-IT, ont baptisé le groupe Anunak, d'après le malware qui a servi de base au set d'outils utilisé par les pirates.
En général, les cybercriminels ciblent les clients des institutions financières, mais le groupe Anunak s'est attaqué directement aux institutions elles-mêmes, s'infiltrant dans leurs réseaux informatiques, jusqu'aux postes de travail et aux serveurs. Grâce à cet accès, le groupe a pu transférer des fonds sur des comptes dont ils avaient le contrôle, réussissant même dans certains cas, à détourner des distributeurs de billets automatiques sur lesquels ils ont pu ensuite retirer frauduleusement de l'argent. « Depuis 2013, ce groupe est parvenu à infiltrer les réseaux de plus de 50 banques russes et de 5 systèmes de paiement, et deux de ces institutions ont été privées de leur licence bancaire », a déclaré l'entreprise de sécurité russe Group-IB dans un rapport publié lundi. « À ce jour, le montant total du vol dépasse le milliard de roubles (environ 25 millions de dollars), la plus grande partie ayant été volée au cours du second semestre de 2014 ».

Un arsenal d'outils au service du piratage
Tout commence par l'infection des ordinateurs des salariés avec des logiciels malveillants, lesquels servent ensuite de point d'accès au réseau interne, aux serveurs et aux comptes de domaine actifs. Et le groupe Anunak ne lésine pas sur les outils : scanners de réseau, keyloggers, logiciels pour cracker les mots de passe, backdoors SSH, programmes de contrôle à distance, avec en plus, la plupart du temps, le framework Metasploit pour tester les failles et réaliser des exploits. Mais, leur principal outil est un cheval de Troie nommé Anunak. Celui-ci est basé sur le malware Carberp, conçu pour dérober des informations d'identification sur les sites de banque en ligne et dont le code source a été rendu public en juin 2013. Les chercheurs de Group-IB pensent que le groupe Anunak comprend sûrement des membres de l'ancien gang Carberp, éclaté en 2013 après des conflits internes.
Les attaquants utilisent plusieurs méthodes pour infecter les ordinateurs avec le Trojan Anunak. Par exemple, le téléchargement de logiciels malveillant quand les ordinateurs se connectent à certains sites (autrement appelé drive-by downloads) via des kits d'exploits (les chercheurs pensent que le groupe a injecté du code malveillant sur le site php.net en 2013 pour attaquer les visiteurs) ; des faux e-mails avec des pièces jointes malveillantes à en-tête de la Banque centrale de la Fédération de Russie ; l'installation d'autres programmes malveillants en utilisant les services de botnets. « Les cybercriminels sont de mèche avec plusieurs propriétaires de botnets pour diffuser massivement leurs programmes malveillants », ont expliqué les chercheurs de Group-IB. « Ils achètent aux propriétaires de botnets des informations sur les adresses IP des ordinateurs sur lesquels il y a déjà des logiciels malveillants contrôlés par le botnet et ils vérifient si les adresses IP appartiennent à des institutions financières ou gouvernementales. Si le malware du botnet se trouve dans les plages d'adresses que le groupe veut cibler, ils paient le propriétaire du réseau de zombies pour qu'il diffuse leur logiciel malveillant ».

Le vol de données de cartes de crédit confirmé
Depuis le début du second trimestre 2014, le groupe Anunak a également ciblé des revendeurs aux États-Unis, en Australie et en Europe, l'objectif étant d'infecter les terminaux points de vente avec leurs logiciels malveillants et de voler des données de cartes de paiement au moment des transactions. « Plus d'une quinzaine de violations potentielles ont été identifiées, dont une douzaine aux États-Unis, et le vol de données de cartes de crédit a été confirmé dans trois de ces cas », ont déclaré les chercheurs dans leur rapport. Le groupe a également compromis les ordinateurs de trois entreprises du secteur des relations publiques et des médias basées aux États-Unis. « Ils cherchaient peut-être des informations qu'ils pouvaient exploiter sur le marché boursier », ont déclaré les chercheurs. « Nous n'avons aucune preuve du piratage de banques en Europe occidentale ou aux États-Unis, mais les attaquants peuvent très bien utiliser les mêmes méthodes pour cibler des banques hors de Russie », ont mis en garde les chercheurs.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-des-cybercriminels-derobent-25m$-a-des-banques-russes-59699.html
Par Jean Elyan