CeBIT 2013 : Kaspersky revient sur Octobre Rouge

Après avoir révélé en janvier une vaste campagne de cyberespionnage basée sur un malware nommé Rocra, diminutif d'Octobre Rouge, l'éditeur **Kaspersky** a détaillé l'ampleur du phénomène la semaine dernière lors du CeBIT de Hanovre.

Octobre Rouge, en bref

Le réseau Octobre Rouge aurait fonctionné pendant au moins cinq ans, depuis 2007, attaquant les systèmes et réseaux fixes et mobiles d'ambassades et laboratoires de recherche dans une quarantaine de pays.

Des pays d'Europe de l'Est, ex-Union soviétique, Asie Centrale, Europe de l'Ouest et Amérique du Nord auraient été touchés, comme l'a signalé Kaspersky début 2013.

Au total, plusieurs centaines de systèmes et réseaux auraient été visés et chaque attaque, par le biais d'une porte dérobée et d'extensions de logiciels comme Adobe Reader et Microsoft Word, avait pour objectif le vol d'informations sensibles spécifiques.

Pour contrôler les machines infectées, aurait été constituée une infrastructure de contrôle (C&C) basée sur plus de 60 domaines et de serveurs hébergés essentiellement en Allemagne et en Russie, ajoute le spécialiste russe de la sécurité Internet.

Les systèmes de chiffrement de l'UE attaqués ?

L'opération pourrait avoir des répercussions plus importantes que celles communiquées en début d'année, observe *TechWeek Europe*.

Selon **Costin Raiu**, directeur de recherche chez Kaspersky Lab, les auteurs des attaques auraient eu accès aux systèmes de chiffrement utilisés par le gouvernement allemand, l'Union européenne et l'OTAN (Organisation du traité de l'Atlantique nord).

Ainsi, les hackers semblaient posséder les clés leur permettant de décoder les échanges utilisant le programme allemand de chiffrement Chiasmus, ainsi que l'Acid Cryptofiler utilisé par de nombreuses institutions, dont l'UE, a déclaré Costin Raiu.

Le logiciel malveillant qui sous-tend ces attaques aurait largement réutilisé du code d'origine chinoise déjà connu. Quant à l'infrastructure C&C mise en place, elle aurait été démantelée quelques heures après avoir été mise à jour.

Octobre Rouge s'inscrit dans la droite ligne des campagnes de cyberespionnage qui mettent à l'épreuve les services de renseignement des grandes puissances, États-Unis et Chine en tête.

Voir aussi

L’édito de la semaine : focus sur le CeBIT 2013