

Un gang de pirates informatiques Russes spécialisés dans le pillage de banques démantelé

✖ Un gang de pirates informatiques Russes spécialisés dans le pillage de banques démantelé

Adepte du malware Lurk, un réseau de cybercriminels vient d'être démantelé en Russie. Il est responsable du vol de plus de 22 millions de euros à des banques. ✖

Une cinquantaine d'interpellations en Russie ont abouti au démantèlement d'un réseau de cybercriminels surnommé Lurk. Un nom qui découle de l'emploi d'un cheval de Troie identifié en 2012.

À l'époque, Kaspersky Lab avait évoqué le cas de Lurk dans des attaques drive-by. Conçu pour voler des données sensibles d'utilisateurs afin d'obtenir un accès à des services de banques en ligne russes, le malware n'était pas téléchargé sur le disque dur et opérait uniquement dans la mémoire RAM.

Threatpost (Kaspersky Lab) écrit que Lurk a commencé à attaquer des banques il y a un an et demi, et a rapatrié divers malwares de serveurs de commande et contrôle. Les attaquants ont utilisé un VPN compromis afin de rendre leur campagne plus difficile à détecter.

Grâce à Lurk, les cybercriminels ont dérobé plus de 1,7 milliard de roubles (près de 22 millions d'euros) à des comptes d'institutions financières russes, a indiqué le FSB (l'ancien KGB) à l'agence de presse russe TASS.

Article original de Jérôme GARAY

✖

Réagissez à cet article

Original de l'article mis en page : Piratage de banques : un gang russe démantelé