Seules 100 personnes sont responsables de la cybercriminalité dans le monde

Seules 100 personnes sont responsables de la cybercriminalité dans le monde

Selon le Centre de lutte contre la Cybercriminalité d'Europol, il n'y aurait qu'une centaine de personnes responsables de la cybercriminalité dans le monde.

Ce chiffre reflète effectivement la réalité de l'industrialisation de la cybercriminalité d'aujourd'hui, à laquelle sont confronté les entreprises, les Etats et les individus. Ainsi, seul un tout petit nombre de programmes permettant d'exploiter des failles logicielles connues (exploits) et d'outils en matière de cybercriminalité sont très largement exploités par les réseaux cybercriminels professionnels dans le monde entier.
Le dernier rapport semestriel sur la sécurité de Cisco a d'ailleurs mis en évidence le fait que le nombre de kits d'exploits a chuté de 87% depuis que le créateur présumé de Blackhole a été arrêté en 2013. Cela montre à quel point ce kit a largement été utilisé par la communauté cybercriminelle.

Nous savons également que les réseaux de cybercriminels sont si bien organisés qu'ils achètent désormais « clef en main » les kits d'exploits et logiciels qu'ils utilisent pour mener à bien leurs activités. La plupart du temps, ces logiciels sont même fournis avec des manuels d'utilisation et un support technique 24/7. Ensuite, les cybercriminels utilisent Internet pour mettre en place un « réseau de distribution » dans le monde entier et diffuser leurs attaques, que ce soit physiquement ou en ligne, via des réseaux de botnets.
Selon Europol, ces kits et ces malwares sont si sophistiqués qu'avec très peu d'effort ils peuvent être réutilisés maintes fois et adaptés aux cibles des cybercriminels.
Mais si ces outils sont si fréquemment et si largement répandus, pourquoi les entreprises ne parviennent-elles pas à prévenir les attaques de leurs réseaux et leurs PC?
Ceci est en partie dû au fait que les cybercriminels ont une longueur d'avance sur les responsables de la sécurité en trouvant de nouvelles variantes à leurs kits d'exploit alors que les experts en sécurité cherchent le moyen de les bloquer. Cette « course à l'armement » ne cessera jamais et nous savons même que de nombreux réseaux de cybercriminels vont jusqu'à acheter les solutions de sécurité pour tester leurs exploits afin de voir si ces dernières parviennent à les arrêter. Et, si tel est le cas, ils développent une nouvelle version de l'exploit pour la communauté cybercriminelle.
Ce que les professionnels de la cybersécurité ont bien compris depuis longtemps, c'est que les hackers sont très motivés, bien équipés et très qualifiés pour s'enrichir grâce à leurs activités illégales.
Les entreprises doivent ainsi s'assurer que leur sécurité est à jour et dispose des toutes dernières signatures, protections et solutions disponibles. Car, tandis que de nombreuses attaques sont destinées à une entreprise en particulier (attaque ciblée) , nous savons que beaucoup d'entre elles sont moins ciblées mais réussissent grâce à un manque de patching ou de mise à jour des signatures, des protections ou des solutions dont sont équipées les entreprises.
Aussi, les entreprises doivent s'assurer que leurs solutions de sécurité ne prennent pas seulement en compte uniquement la défense des postes de travail, mais qu'elles soient également capables de détecter les activités malicieuses potentielles sur l'ensemble de leur réseau – où les menaces peuvent apparaître. Il est fort probable que votre entreprise soit attaquée un jour, mais plus vite vous le saurez et vous agirez, plus vite vous pourrez déterminer l'ampleur des dommages sur votre business et sur la réputation de votre entreprise.

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

Source : http://www.huffingtonpost.fr/christophe-jolly/seules-100-personnes-responsable-cybercriminalite-mondiale_b_6248606.html