

Les marchés noirs de la cybercriminalité révélés : le numérique, une économie mature
Internet

Posté par : JerryG

Publié le : 14/4/2014 15:00:00

Juniper Networks, leader de l'innovation réseau, constate que les marchés noirs de la cybercriminalité ont donné naissance à une économie mature, qui n'est pas loin de ressembler à une métropole en plein essor.

Dans un nouveau rapport international sponsorisé par Juniper Networks et réalisé par RAND Corporation, plusieurs indicateurs prouvent que ces marchés ont atteint un niveau de maturité et de croissance sans précédent.

Si des recherches poussées ont permis de mesurer les différentes activités des marchés noirs de la cybercriminalité, le rapport de RAND intitulé « Markets for cybercrime Tools and Stolen Data: Hackers' Bazaar » (Marchés des outils de la cybercriminalité et des données volées : le bazar du pirate) examine pour la première fois ces marchés dans leur intégralité et propose des analyses économiques afin de mieux comprendre comment ils s'organisent.

RAND révèle que les produits, canaux de distribution et les ventes sur les marchés noirs ont atteint des niveaux spectaculaires de sophistication, de fiabilité, d'accessibilité et de discrétion.

La solide expérience de Juniper dans le domaine de la sécurité réseau vient confirmer le rapport de RAND, qui indique que les marchés noirs de la cybercriminalité possèdent plusieurs milliards de dollars et s'appuient sur une infrastructure et une organisation sociale très solides. RAND souligne que cette économie numérique, elle aussi, par les forces du marché telles que l'offre et la demande ne cesse d'évoluer.

Principales caractéristiques :



Juniper compare les marchés noirs de la cybercriminalité à une métropole en plein essor, dans laquelle interagissent divers secteurs et communautés :

• Boutiques en ligne : Nombre d'enregistrements de données, de kits d'exploitation et autres produits sont achetés et vendus dans des boutiques en ligne sophistiquées offrant des fonctions de dialogue en direct ou encore des forums. RAND révèle que certaines organisations comptent entre 70 et 80 000 personnes dans le monde, qui rapportent plusieurs centaines de millions de dollars.

• Économie de services : RAND constate que la cybercriminalité touche les produits,

mais aussi les services. Les outils vendus comme des logiciels classiques ou proposés à la location sur le marché noir peuvent aider les pirates les moins expérimentés à lancer des attaques complexes et évolutives. RAND cite notamment l'exemple des « botnets » qui, pour la modique somme de 50 dollars, permettent de lancer une attaque par déni de service (DDoS, Distributed Denial of Service) valable 24 heures.

ii. Modèles hiérarchiques ■ RAND souligne qu'à l'instar d'une activité légitime, la cybercriminalité exige des contacts et des relations. Ceux qui sont au sommet de la pyramide s'appuient sur des contacts personnels, tout en se taillant la part du lion.

iii. État de droit ■ Les pirates respectent, eux aussi, un code d'honneur. RAND a constaté que nombre d'activités cybercriminelles sont parfaitement structurées et régies par un ensemble de règles. D'ailleurs, ceux qui tentent d'escroquer les autres sont régulièrement bannis du marché.

iv. Éducation et formation ■ RAND a identifié sur les marchés noirs de nombreux outils et ressources permettant de s'initier au piratage : instructions sur les kits d'exploitation, références pour l'achat de cartes de crédit, etc. Cet accès à des formations a favorisé le développement d'attaques sophistiquées et la diversification des rôles, tout en facilitant l'accès à l'économie souterraine.

v. Devises ■ Dans l'univers de la cybercriminalité, les transactions sont souvent réalisées dans des devises numériques telles que Bitcoin, Pecunix, AlertPay, PPcoin, Litecoin, Feathercoin et les extensions Bitcoin comme Zerocoin. RAND révèle que les sites malhonnêtes sont de plus en plus nombreux à n'accepter que les crypto-devises numériques, gages d'anonymat et de sécurité.

vi. Diversité ■ Si c'est en Chine, en Amérique latine et en Europe de l'Est que les cybercriminels sont les plus actifs pour les attaques malicieuses, les pirates russes, eux, se distinguent plutôt sur le plan de la qualité. RAND révèle en outre que les domaines d'expertise et champs d'action varient d'un pays à l'autre. Par exemple, de nombreux groupes de cybercriminels vietnamiens sont spécialisés dans le piratage du commerce électronique. Les attaquants russes, roumains, lituaniens et ukrainiens ciblent, pour leur part, les établissements financiers. Les cybercriminels chinois s'attaquent à la propriété intellectuelle. Enfin, les groupes de pirates basés aux États-Unis ciblent essentiellement les systèmes financiers américains. Outre la diversité des rôles, RAND constate une pollinisation croisée toujours plus forte au sein de ces groupes.

vii. Criminels ■ On retrouve également sur le marché noir de la cybercriminalité des « rippers », à savoir des personnes malhonnêtes qui proposent des produits ou services fictifs.

Pour son rapport « Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar » (Marchés des outils de la cybercriminalité et des données volées : le bazar du pirate), RAND a mené entre octobre et décembre 2013 des entretiens approfondis avec des spécialistes mondiaux travaillant ou ayant travaillé sur le marché noir, notamment des professeurs, des spécialistes de la sécurité, des journalistes, des éditeurs de logiciels de sécurité et des agents des services de police.

À

Ce rapport est le premier d'une série d'étude de RAND Corporation sponsorisée par Juniper Networks.