Les bénéfices illégaux de la cybercriminalité qui échappent à l'impôt alimentent des dépenses ménagères, la cupidité et des investissements

Les travaux de recherche de Bromium sur le
Web of Profit
, le Web des profits révèlent les différences socio-économiques et de dépenses entre les cybercriminels

CUPERTINO, Californie, le 11 avril 2018 (GLOBE NEWSWIRE) — Bromium®, Inc., pionnier et leader dans l'isolation d'applications utilisant la sécurité basée sur la virtualisation, a annoncé aujourd'hui les résultats d'une étude universitaire indépendante sur les montants empochés par les cybercriminels et sur la manière dont ils dépenses cet argent. Ces conclusions font partie d'une étude de plus grande ampleur effectuée sur onze mois intitulée
Into the Web of Profit
,

parrainée par Bromium
.

Ces travaux révèlent comment les revenus et dépenses sont des quasi clichés. Alors que les cybercriminels n'ont pas d'impôts à payer sur leurs revenus, leur niveau de revenu annuel pourrait les pousser dans les tranches d'imposition les plus élevées.

- Ceux qui gagnent des revenus importants empochent jusqu'à
  2 millions d'USD/1,4 million de GBP
  – presqu'autant qu'un

  PDG d'une entreprise du FTSE250

- Les criminels de niveau intermédiaire empochent jusqu'à
  900 000 USD/639 000 GBP
  – soit plus du double du

  salaire du président des États-Unis

- Les pirates au bas de l'échelle gagnent
  42 000 USD/30 000

GBP
– soit nettement plus qu'un
diplômé britannique
moyen

« Chaque fois qu'une personne verse une rançon, elle participe au Web of Profit », déclare Gregory Webb, PDG de Bromium. « La cybercriminalité est une activité lucrative dont les risques sont relativement faibles par rapport à d'autres formes de criminalité. Les cybercriminels se font rarement prendre et sont rarement condamnés car ils sont virtuellement invisibles. À mesure que les criminels monétisent toujours plus leur activité en permettant à tout un chacun de se procurer des logiciels malveillants prêts à l'emploi ou de recruter des pirates informatiques à la demande, il devient encore plus difficile d'attraper les cerveaux. Le secteur de la cybersécurité, les entreprises et les organismes chargés de la répression des fraudes doivent unir leurs forces pour perturber l'activité des pirates informatiques et interrompre leurs sources de revenus. En se concentrant sur de nouvelles techniques de cybersécurité qui visent la protection plutôt que la détection, nous sommes convaincus de pouvoir amplement compliquer la tâche des cybercriminels ».

Les données compilées dans le cadre d'entretiens en tête à tête menés avec une centaine de cybercriminels condamnés ou actuellement en activité, conjuguées à des investigations conduites sur le Dark Web (la face obscure de l'Internet), révèlent les éléments suivants :

- 15 % des cybercriminels consacrent la majeure partie de leurs bénéfices illégaux à des besoins immédiats – comme l'achat de
  couches pour bébés
  et le
  règlement des factures
- 20 % des cybercriminels consacrent leurs dépenses à de mauvaises habitudes – comme l'
  achat de drogues
  ou la
  rémunération de prostituées
- 15 % des cybercriminels dépensent leur argent pour s'acheter un statut, ou impressionner leur partenaire et d'autres criminels – par exemple, l'
  achat de bijoux onéreux
- 30 % des cybercriminels convertissent une partie de leurs revenus en placements – tels que les
  biens immobiliers
  ou

  les
  instruments financiers
  , et d'autres articles de valeur tels que les
  oeuvres d'art
  ou les
  grands crus
- 20 % des cybercriminels réinvestissent au moins une partie de leurs revenus dans d'autres activités criminelles – par exemple, l'

achat de matériel informatique

En effet, le rapport fait état d'un marché croissant destiné aux cybercriminels en leur permettant de régler leurs achats en monnaie virtuelle. Des sites tels que
White Company
,
Bitcoin Real Estate
et
de Louvois
proposent des produits de luxe facturés en Bitcoin, ce qui
devient une source de préoccupation
pour les analystes financiers.

« L'éventail des habitudes de dépenses chez les cybercriminels est fascinante », indique le Dr. Mike McGuire, chercheur. « Nombreux sont les cybercriminels qui dépensent leur argent pour améliorer leur statut social, que ce soit auprès de leurs pairs ou auprès de leurs conquêtes. Au Royaume-Uni, une personne qui empochait 1,2 million de GBP par an, a dépensé des sommes colossales pour un voyage à Las Vegas, où elle a prétendu avoir dépensé 40 000 USD dans les casinos et 6 000 USD en location de voitures de sports afin de pouvoir faire une « arrivée remarquée » dans les casinos et hôtels de la ville. Un autre cybercriminel britannique a dépensé ses gains dans de l'or, de la drogue, des montres de luxe et dépensé 2 000 GBP par semaine en prostituées. Le constat est alarmant : les cybercriminels n'ont aucun mal à dépenser leurs bénéfices illégaux. Il existe bien un marché en croissance constante qui est quasiment fait sur mesure pour que les cybercriminels puissent réaliser leurs achats ostentatoires, ledit marché n'étant soumis à aucune règlementation ni surveillance, voire très peu ».

D'autres résultats seront publiés lors de la Conférence RSA de San Francisco. Le Dr. McGuire présentera les résultats complets au cours de son
intervention qui aura lieu le 20 avril
, de 9h00 à 9h45 sur le suivi des mashups en matière de sécurité – code MASH-F01.

Méthodologie

Into the Web of Profit
(
Dans la toile des profits
) est une étude universitaire de neuf mois menée par le Dr. Mike McGuire, maître de conférence en criminologie à l'Université de Surrey. Elle s'appuie sur des entretiens en tête à tête avec des cybercriminels condamnés, des données provenant d'organismes internationaux chargés de la répression des fraudes, des institutions financières et des observations secrètes effectuées à travers le Dark Web (Toile secrète). Pour obtenir le rapport gratuitement :
https://learn.bromium.com/rprt-web-of-profit.html.

À propos de Bromium, Inc.

Bromium protège votre marque, vos données et vos collaborateurs grâce à la sécurité basée sur la virtualisation. Nous convertissons la plus grande source de vulnérabilité d'une entreprise, à savoir

ses terminaux, pour en faire sa meilleure défense. En combinant notre conteneurisation matérielle brevetée permettant l'isolation et le contrôle des applications à un réseau de capteurs distribués permettant une protection vis-à-vis des principaux vecteurs de menaces et types d'attaques, nous arrêtons les logiciels malveillants dans leur progression. Contrairement aux technologies de sécurité traditionnelles, Bromium isole automatiquement les menaces et s'adapte aux nouvelles attaques en utilisant l'analyse comportementale et partage instantanément les informations sur les menaces pour éliminer l'impact des logiciels malveillants. Bromium offre une sécurité de qualité militaire et compte parmi ses clients un nombre croissant de sociétés classée au Fortune 500 et d'agences gouvernementales.

Consulter le site Web de Bromium :

https://www.bromium.com

Lire le blog de Bromium :

https://blogs.bromium.com/

Suivre Bromium sur Twitter :

Tweets by bromium

Suivre Bromium sur LinkedIn :
https://www.linkedin.com/company/bromium

À propos du Dr. Mike McGuire

Le Dr. Michael McGuire a rejoint le département en tant que maître de conférences en criminologie en septembre 2012. Le Dr. McGuire a étudié la méthode philosophique et scientifique à la London School of Economics, où il a brillamment obtenu un Master en Économie et a terminé son doctorat au Kings College à Londres. Il a ensuite développé un profil international dans l'étude de la technologie et du système judiciaire, et a publié de nombreux écrits dans ces domaines. Contact : m.mcguire@surrey.ac.uk

CONTACTS PRESSE :

Royaume-Uni

Spark Communications

bromium@sparkcomms.co.uk

+44 20 7436 0420

États-Unis – Commercial

Mullikin Communications

rich@mullikincommunications.com

+1 925-354-7444

États-Unis – Secteur public

Sage Communications

Jon-Michael Basile

FedBromium@aboutsage.com

+1 925.246.3433
