www.animasoft.com
Pays : France
Dynamisme : 39

Visualiser l'article

Le casse du XXIe siècle sera informatique, Par Luc d'Urso, PDG de Wooxo

Le volume de données numériques ne cesse aujourd'hui d'augmenter, et avec lui le volume des données menacées. Si l'année 2016 constitue une année charnière en matière de cybercriminalité, quel avenir envisager à une époque où n'importe qui peut devenir un pirate informatique ?
68 % des entreprises reconnaissent avoir été victimes d'une fraude au cours des 24 derniers mois 1 (liée à une attaque cybercriminelle dans plus d'un cas sur deux). Un constat inquiétant qu'il convient de rapprocher à la progression rapide et constante de la cybercriminalité, elle-même directement liée à la croissance exponentielle du nombre de programmes malveillants (passé de 22 000 en 2005 à 430 millions en 2015 2).
Les premiers mois de l'année 2016 confirment cette tendance : pour le seul mois de février, le nombre d'attaques recensées égale celui des cinq mois précédents cumulés 3.
Et pour cause, les 3.2 milliards d'internautes dans le monde (46% de la population mondiale, 81,3% des ménages dans les pays développés) 4 et les 20.8 milliards d'objets qui seront connectés à l'horizon 2020 5, sont autant de cibles pour les cybercriminels et autant de portes d'accès pour commettre leurs forfaits. Puisque le casse du XXIe siècle sera informatique, l'année 2016 marque-t-elle le début de l'ère du Far-West numérique ?

Les données : une mine d'or au filon inépuisable

A la différence des mines d'or de l'Ouest américain, les filons actuels d'informations représentent un gisement inépuisable et en perpétuelle expansion. La croissance du volume des données s'est faite par étapes : d'abord avec la dématérialisation des documents avec le passage à l'an 2000, puis avec l'échange d'information par textes, images et vidéos grâce aux applications et réseaux sociaux des années 2010. Désormais, on prévoit qu'à l'horizon 2020, le stock d'informations au format numérique atteindra 44 Zettabytes 6, avec une contribution entre 10 et 21% réservée aux objets connectés.
Pourtant, il convient de souligner que plus de 50% des informations concernées par un enjeu de sécurité (données personnelles, médicales, financières…) ne sont toujours pas protégées.

Le piratage informatique : une rentabilité exceptionnelle

En effet, si les activités cybercriminelles ont longtemps été l'apanage d'une « élite » informatique malintentionnée, ce n'est plus le cas aujourd'hui. Avec un marché aussi prometteur, il n'est pas étonnant que les services de piratage à la demande (plus connus sous le nom de « Haas - Hacking as a service ou Caas - Crimeware-as-a-Service ») se soient rapidement développés dans les milieux autorisés. Fichiers d'adresses de messagerie vendus sur le marché « gris », codes malveillants prêts à l'emploi, infrastructures de déploiement… L'arsenal du parfait cybercriminel est désormais accessible sur Internet à tout titulaire d'une carte bleue.
A la lumière des gains engrangés par les pirates exploitant le rançongiciel Cryptolockers depuis 2014 (soit 100 millions de dollars par période de 100 jours 7), et un retour sur investissement de l'activité estimé à près de 1500% 8, on comprend que la rentabilité affichée du cybercrime aiguise les appétits des milieux interlopes.

La cybercriminalité : une activité peu risquée

Si plusieurs organes de répression spécialisés – tels que l'OCLCTIC, le département informatique de l'IRCGN ou encore le STRJD 9 – ont été créés pour lutter contre ce fléau, les poursuites à l'encontre des contrevenants s'avèrent cependant très complexes. Elles se heurtent d'une part à la sophistication souvent poussée de l'ingénierie employée pour les attaques (utilisation de proxys, routeurs TOR, foreign IPs, ordinateurs relais compromis et utilisés à des fins criminelles ou botnets 10) et d'autre part aux difficultés inhérentes à toute investigation à l'échelle internationale. Les procédures doivent composer avec les lois en vigueur dans chaque état virtuellement associé afin de protéger les droits des individus et des citoyens et garantir la souveraineté desdits États sur leur territoire.

Visualiser l'article

Pour simplifier ces procédures, une quarantaine d'États ont signé la Convention sur la cybercriminalité 11 mais l'on peut légitimement s'interroger sur l'efficacité de cette collaboration lorsqu'on sait que les Etats eux-mêmes utilisent ces techniques. Les affaires d'espionnage des communications à très grande échelle impliquant des services de renseignements officiels 12 qui ont récemment fait la Une des médias ne laissent aucun doute sur le sujet.

Au vu des complexités et lenteurs inhérentes aux procédures, on comprend que les cybercriminels aient la conviction de sévir en toute impunité. Il est même probable que l'on assiste au cours des prochaines années à un transfert des ressources investies dans les activités criminelles traditionnelles au profit de la cybercriminalité.

Des évolutions technologiques propices au développement de l'activité cybercriminelle

L'exercice de la cybercriminalité est facilité par plusieurs facteurs :

- Le datacenter : l'avènement du Cloud a entrainé la création de banques de données colossales stockées sur un même lieu physique : le centre d'hébergement. La forte concentration de valeur en un lieu unique a toujours attisé les convoitises, le butin potentiel étant bien supérieur à celui de rapines de données éparses.
- Un abaissement du niveau de protection des données : nous avons privilégié le confort d'utilisation sur la sécurité en exigeant que l'information soit disponible depuis tout équipement connecté, en tout lieu, à tout moment, et avec le minimum de contrainte. Difficile en effet d'assurer la sécurité des données stockées ou transportées si le contrôle des utilisateurs est rendu impossible ou délégué. C'est un peu comme vouloir faire du transfert de fonds sans camions blindés. La virtualisation ajoute à la complexité en matière de sécurité, puisque les applications et données de plusieurs clients sont hébergées sur une même machine et que le niveau de sécurité de l'ensemble est étalonné sur le maillon le plus faible. Il faudrait connaître le pédigrée et la politique de sécurité de ses colocataires à tout instant.
- Les réseaux télécoms : Ils complètent le paysage en permettant d'opérer à distance dans l'anonymat, d'interagir directement avec les victimes sans aucun risque physique, de disposer d'un arsenal accessible en ligne pour commettre ses méfaits et de profiter d'une place de marché mondiale pour revendre le fruit de ses exactions.

Le jeu du chat et de la souris le plus sophistiqué

Les moyens dont disposent les organisations cybercriminelles leur permettent de challenger sérieusement les acteurs de la sécurité informatique. Ainsi, seuls 5 antivirus parmi 57 répertoriés ont détecté le cryptolocker Locky lors de la première vague d'attaques.

Certaines évolutions sont prévisibles :

- La mutation des Menaces Persistantes Avancées 13 en Menaces Temporaires Avancées, des intrusions éclair destinées à collecter de l'information sans laisser à la victime le temps de détecter l'attaque ;
- Des rançongiciels proposés en multiplateformes pour les stations de travail, Mac ne faisant plus exception à la règle, comme pour les terminaux mobiles ;
- L'arrivée de nouveaux outils permettant aux cybercriminels de compromettre l'hyperviseur à partir d'une instance virtuelle leur permettra de passer d'une machine virtuelle à l'autre au sein d'un datacenter et ainsi de propager les programmes malveillants ;
- La contamination des objets connectés, victimes d'une forte pression sur les prix les privant de système de sécurité adapté. Il en sera de même (si ce n'est déjà le cas) de la plupart des applications vendues en mode SaaS ou des sites web marchands à trafic moyen ou faible, les sites à fort trafic étant déjà régulièrement ciblés.
- Des programmes malveillants seront dédiés à biaiser ou orienter le machine learning et les programmes d'intelligence artificielle. D'autres feront de l'injection, ou de la substitution massive de données pour compromettre les analyses du Big Data.
- Le crime ayant une fâcheuse tendance à s'organiser dans un souci d'efficacité, une forme de cybercriminalité collaborative devrait rapidement voir le jour.

Mais néanmoins de bonnes raisons de rester optimiste

www.animasoft.com
Pays : France
Dynamisme : 39

Visualiser l'article

Il faut bien envisager que l'année 2016 constitue une année charnière en matière de cybercriminalité, et plus encore en considérant une cybercriminalité en phase d'industrialisation ; et si cet état de fait désole les observateurs pessimistes, d'autres y voient un nouveau défi à relever.
Le concept de Blockchain 14 se dresse comme un nouveau rempart face à la cybercriminalité en permettant de désintermédier la plupart des « tiers de confiance » centralisés (hébergeurs, métiers de banques, assurances, notaires, santé…) par des systèmes informatiques distribués. Son champ d'application est immense et reste à exploiter, et porter une attaque contre ce réseau est une aventure coûteuse. Il faudrait disposer d'une puissance de calcul équivalente à la puissance totale du projet bitcoin, soit approximativement 1.400.000 Téra HASH au mois de juin 2016, plus un petit delta (Attaque dite 51%). La mobilisation de telles ressources aurait un coût approximatif de 5,6 milliards de dollars 15. On ne voit pas bien quelle organisation aurait intérêt à investir dans un tel projet.
1 - PWC - Global economic crime survey 2016
2 - Symantec - Internet Security Threat - April 2016
3 - Wooxo - Les entreprises françaises face à la cybercriminalité
4 - Le rapport de référence annuel de l'UIT du 30 novembre 2015 – UIT est l'institution spécialisée des Nations Unies pour les technologies de l'information et de la communication (TIC).
5 - Gartner – Novembre 2015
6 - Etude IDC – Digital Universe 2014
7 - Estimation Kaspersky Lab. Cryptolocker est un logiciel malveillant découvert en 2013. Ce rançongiciel se diffuse principalement via des mails infectés et s'active à l'ouverture d'une pièce jointe attachée. Une fois activé, il chiffre les données présentes sur le poste et demande une rançon à l'utilisateur au travers d'une boîte de dialogue.
8 - Trustwave : Rapport Global Security 2015
9 - OCLCTIC : L'Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication a été créé le 15 mai 2000
IRCGN : Département informatique et électronique de l'Institut de Recherche Criminelle de la Gendarmerie nationale
SRRJD : Département cybercriminalité du service technique de recherches judiciaires et de documentation de la Gendarmerie Nationale
10 - Botnets : Réseau de robots, de machines zombies manipulées à distance par des pirates informatiques
11 - Bureau des Traités du Conseil de l'Europe : STCE N°185 – Budapest 23/11/2001 entré en vigueur le 01/07/2004
12 - En juin 2013, Edward Snowden révélait les agissements abusifs de l'Agence Nationale de Sécurité (NSA), les États-Unis procédant à une surveillance de masse des communications et partageant ces informations avec l'Australie, le Canada, la Nouvelle-Zélande et le Royaume-Uni au sein de l'alliance dite des « Cinq yeux ».
13 - (APT – Advanced Persistant Threat)
14 - Une blockchain est une base de données distribuée qui gère une liste d'enregistrements protégés contre 15 - Coût d'1 Téra Hash est estimé à 4.000 $.