Les groupes de hackers dans la cyber-malveillance

Plusieurs organisations dominent le marché des groupes de hackers malveillant. Certaines d'entre elles seront commentées dans ce document. Nous ne faisons en aucun cas l'apologie, ou la propagande de leur exaction, ce document est dans un but totalement éducatif.

ATP31 : Les hackers chinois soutenus par le Gouvernement

ATP31 (affilié à Pékin) comme son nom l'indique c'est sous cette nomenclature que le spécialiste de la cybersécurité FireEye a classé un groupe de hackers qui est régulièrement identifié en raison de son mode opératoire.

APT **pour Advanced Persistent Threat**, en français, menaces persistantes avancées signifie qu'il s'agit de groupes généralement très bien organisés, capables de manœuvres sophistiquées s'étendant parfois sur plusieurs mois ou plusieurs années.

Unité 180, Unité 121, Lazarus Group : Les différents teams de hackers Nord-coréen

Actuellement au nombre de 8 500 membres, ces pirates sont des surdoués en mathématiques et informatique, remarqués dès le collège et envoyés dans des universités pour être spécialement formés au codage. Ils complètent ensuite leur formation, le plus souvent en Chine.

Dès qu'une cyberattaque de grande portée frappe une entreprise ou une institution, la Corée du Nord compte parmi les premiers suspects. La propagation du ransomware WannaCry, qui a touché plus de 200 000 ordinateurs dans 150 pays, n'a pas échappé à la règle : une partie du code retrouvée dans une première version du logiciel était en effet semblable à celle d'un backdoor utilisé par les hackers nord-coréens du Lazarus Group en 2015.

L'Unité 180 : « [Cette cellule] *est dédiée au piratage d'établissements financiers par l'intrusion et le retrait d'argent sur des comptes bancaires*. *Les hackers se rendent à l'étranger pour trouver des lieux dotés d'une meilleure connectivité à Internet qu'en Corée du Nord et pour ne pas laisser de trace* ».

Comme l'explique Kim Heung-kwang, ancien professeur d'informatique, qui a gagné la Corée du Sud en 2004

D'après un article de Reuters, la section 121, également connu sous le nom de gang DarkSeoul est composé des experts informatiques les plus talentueux de Corée du Nord. Le bureau compte environ **1 800 spécialistes.**

De nombreux hackers du bureau sont des diplômés triés sur le volet de **l'Université de l'automatisation, Pyongyang**. Alors que ces spécialistes sont dispersés à travers le monde, leurs familles bénéficient d'un traitement privilégié en Corée du Nord

Cette section spécialise ses attaques directement sur les entreprises de la Corée du Sud ainsi que leur institution gouvernementale.

Gang76, Shelby familly, Iznaye : Les groupes de Hackers Français

Le Gang 76 aussi connue comme faisant partie du 18-25 de jeuxvideo.com est une organisation organisé dans le racket d'influence. Cette organisation qui compte 70 membres principalement black hat, harcèle et intimide des personnalités publiques sur le net.

Proposant un service de sécurité sur de prestation de lutte contre le harcèlement s'élevant entre quelques centaines d'euros, à plusieurs milliers pour certains streamers de la plateforme de twitch.

Agissant principalement en solo ils ne sont jamais accusés de violence en bande organisé car aucune preuve n'est jamais recevable pour justifier de la communication en interne.

Ils sont donc condamnés à de faibles peine de prison et comme un gang se soutiennent entre eux quand l'un doit faire un court séjour en prison. Ils font sans nul doute parti de la cyber-malveillance qui va poser de nombreuse problématique dans cette décennie.

La shelby familly plus discret que les ombres noirs (groupe de hacker indien), est connue pour être les distributeurs des teams black hat française. Assistant l'ensemble des organisations par un symbole méconnu ₩ *(lettre de l'alphabet latin).* Comme son nom l'indique elle sert de clin d'œil à la série Peaky Blinders et est apparu en même temps que la sortie de la série.

Dans le commerce BE to BE ce sont les rois, logiciel de spoofings, clés USB hacker, conseil juridique, base de données piratés, code d'accès, développement de virus. Tous ce que vous voulez il vous le trouve tant que vous pouvez mettre le prix.

On ne sait pas grand-chose à leur sujet mais séjourne principalement sur des serveurs discord ou les liens d'invitations sont extrêment difficile à trouver.

La plupart du temps la réception de lien d'invitation se fait par le bouche à oreille de hacker à hacker ne cherchant pas à être connue il désactive régulièrement leur compte et serveurs pour éviter d'être espionner par les autorités.

Leur niveau de compétence est-elle que ils ont des « employés ou aspirant » qui se salice les mains pour administré la communication et la réception des moyens de paiement. Cette méthode leur permet de toujours être certains qu'en cas de descente de ne pouvoir être condamné par les autorités.

la Iznaye team black hat française connue pour le piratage de burger king et Citroenne il exploite des techniques rudimentaires comme des injections de SQL, attaques de brute force, ou encore Ransonware.

Ne se cachant pas pour faire leur exaction il publie régulièrement des messages sur leur compte Twitter ou sur les sites victimes de leur piratage. Recherché par les autorités ils sont aux nombres de 12. Une petite PME qui fait de gros dégât. (En relation avec la Shelby familly)

La muslim hacker team : sous les ordres d'ISIS

Cette unité de hacker malveillante est le faire de lance des piratages informatique menée par l'organisation état islamique, ciblant régulièrement des états, ou site de ne respectant pas le prophète Mahomet. Ils sont d'avantage un but de propagande qu'un réel but de financer l'organisation.