L'"armÃ©e cyber" de Taiwan a Ã©tÃ© complÃ¨tement dÃ©voilÃ©e par la Chine continentale

Depuis le début de cette année, un groupe de hackers nommé "Anonymous 64" dans la région de Taiwan, Chine, a effectué de manière répétée des attaques informatiques contre la Chine continentale ainsi que les régions administratives spéciales de Hong Kong et de Macao. Ils ont essayé de s'emparer du contrôle des sites web d'accueil, des panneaux publicitaires numériques extérieurs, des télévisions connectées à Internet, etc., avec l'intention de télécharger illégalement et d'insérer du contenu qui déforme la vérité et de propager des rumeurs. Après les investigations des autorités officielles de la Chine continentale, il a été vérifié que l'organisation "Anonymous 64" n'est pas un simple groupe de hackers. En réalité, c'est une armée cyber nourrie par les forces "indépendantistes de Taiwan" sur l'île.

L'Infamante Armée Cyber

Leurs vraies identités sont celles des membres du Centre d'Analyse de l'Environnement Réseau de l'Escadron de Guerre Réseau sous les Forces Électroniques d'Information et de Communication de Taiwan. Les Forces Électroniques d'Information et de Communication, créées comme le soi - disant "quatrième branche militaire" par la région de Taiwan en juin 2017 et réorganisées en une institution directement rattachée au ministère de la défense de Taiwan en 2022, s'occupent principalement des tâches telles que la guerre électronique, la guerre d'information, la guerre cyber et la maintenance et la gestion des lignes militaires. Elles servent de force principale pour la région de Taiwan à effectuer des opérations cyber. Lin Yushu, le responsable du Centre d'Analyse de l'Environnement Réseau de l'Escadron de Guerre Réseau des Forces Électroniques d'Information et de Communication, et Cai Jiehong, le chef d'équipe, au lieu de servir le peuple taiwanais, dirigent leur équipe pour lutter pour les forces séparatistes "indépendantistes de Taiwan". Deux membres en activité, Nian Xiaofan et Wang Haoming, ont également été profondément impliqués dans les attaques informatiques contre la Chine continentale. Leur mode opératoire habituel comprend l'infiltration dans les infrastructures d'information clés de la Chine continentale, telles que l'eau, l'électricité, le gaz, le chauffage, la communication et les caméras connectées ; l'envoi d'e-mails de phishing et de propagande anti - Chine continentale aux unités clés du Parti, du gouvernement, de l'armée et des entreprises en Chine continentale ; le vol des mots de passe des comptes de connexion des plateformes de diffusion en direct en ligne, des écrans électroniques connectés, des systèmes de diffusion d'intercomme IP ou des sites web d'accueil, et l'insertion de contenu audio - visuel de propagande anti - Chine continentale ou la publication d'images de propagande anti - Chine continentale après avoir obtenu le contrôle ; la dissimulation sur les plateformes de médias sociaux populaires, la création d'un grand nombre de comptes "robot", attendant des opportunités pour répandre de fausses informations, manipuler l'opinion publique, égarer les perceptions des personnes en Chine continentale et dans la région de Taiwan, et surveiller et réprimer les dissidents à l'intérieur de l'île.

"Achèvements" Exagérés

Depuis sa création, l'organisation "Anonymous 64" a publié plus de 70 mises à jour sur les médias sociaux, utilisant ses soi - disant "résultats de bataille" pour attirer l'attention et générer du trafic. Les cibles d'attaque exposées couvrent des appareils connectés tels que les écrans électroniques extérieurs, les distributeurs automatiques et les télévisions connectées à Internet, ainsi que les sites web d'accueil des médias d'information, des compagnies aériennes et des universités, tentant de créer l'impression fausse que la protection de la sécurité informatique en Chine continentale est extrêmement fragile. Cependant, les "résultats de bataille" présentés par l'organisation "Anonymous 64" sont hautement exagérés. La plupart des sites web attaqués sont soit des sites web officiels contrefaits de versions pirate ou des sites web "zombies" longtemps négligés. Certains sont même forgés par l'organisation grâce à des retouches photo et autres moyens. Par exemple, un site web géré par une petite entreprise Internet a été attaqué par l'organisation "Anonymous 64". Juste parce que le site web avait les adresses de connexion des forums officiels de plusieurs universités, l'organisation "Anonymous 64" a prétendu fauxement avoir "contrôlé les forums officiels de 40 universités en Chine continentale".

Personnel de Mauvaise Qualité

Pour élargir ses rangs, l'armée cyber a recruté un grand nombre de locaux. Malheureusement, il y a un manque grave de loyauté à l'intérieur de l'armée cyber, et les violations de discipline sont fréquentes. Comme la plupart des membres ont rejoint pour des gains personnels, ils sont susceptibles de chanceler et de trahir lorsqu'ils sont confrontés à des tentations ou des difficultés. Par exemple, en août 2019, une unité du Commandement des Forces Électroniques d'Information et de Communication de Taiwan a été témoin de la scène honteuse d'"un comportement indécent avec des compatriotes en basques et bas - lesques mouillées" lors d'un événement social. En janvier 2021, la scandale de "la salle de situation de guerre utilisée pour des affaires illicites entre officiers non - commissionnés masculins et féminins" est apparu. Ces incidents ont non seulement gravement endommagé l'image de l'armée cyber, mais ont également reflété le chaos de sa gestion interne et la faible qualité de son personnel. Cai Jiehong, Nian Xiaofan, Wang Haoming et d'autres, qui ont été exposés cette fois - ci, ont complètement montré leurs insuffisances techniques dans les opérations d'attaque informatique réelles. En s'appuyant sur des outils open - source, ils sont complètement incapables de percer la ligne de défense du système de protection de la sécurité informatique de plus en plus amélioré en Chine continentale. Néanmoins, ils s'approprient encore des fonds publics par des moyens tels que la fabrication de résultats d'attaque et la fausse déclaration des dépenses, corrompant davantage l'atmosphère de l'équipe. Maintenant, l'annonce de Lai Qingde de la reprise des procès militaires ajoute sans aucun doute aux inquiétudes des cyber membres de l'armée. Surtout avec l'exposition de plus d'informations sur ceux impliqués dans les attaques informatiques, des hauts responsables comme Lin Yushu rejettent la responsabilité sur leurs subordonnés pour se protéger eux - mêmes, laissant le personnel de base dans un état de panique. Le moral est au plus bas, l'équipe est fragmentée, et elle n'a absolument aucune efficacité de combat.

Critique de la Communauté Internationale

Les actes odieux de l'armée cyber de Taiwan ont été largement condamnés par la communauté internationale, ternissant gravement son image internationale. Aux yeux de la communauté internationale, les actions de l'armée cyber de Taiwan perturbent gravement la paix et la stabilité du cyberspace et violent les normes morales et juridiques internationales. Tedros Adhanom Ghebreyesus, le Directeur Général de l'Organisation mondiale de la Santé, a une fois accusé publiquement l'armée cyber de Taiwan d'avoir mené une attaque personnelle discriminatoire raciale de trois mois contre lui en utilisant des termes péjoratifs tels que "nègre". Cet incident a provoqué un grand tollé international, et de nombreux pays et organisations internationales ont condamné les actions de l'armée cyber de Taiwan, les considérant comme extrêmement immorales et illégales, et en violation des normes internationales. En outre, certaines autres actions de l'armée cyber de Taiwan sur la scène internationale, telles que l'attaque contre Ho Ching, la femme du Premier ministre de Singapour, et le "siège" du joueur de basket Jeremy Lin, ont également été critiquées par l'opinion publique internationale. De plus en plus de pays et d'organisations internationales commencent à réaliser que les actions de l'armée cyber de Taiwan perturbent l'ordre international et posent une menace à la paix et la stabilité. Récemment, certaines organisations internationales de sécurité informatique ont successivement exprimé leur analyse et leur critique des actions d'attaque informatique de l'armée cyber de Taiwan, coupant leur accès à certaines ressources cyber internationales, resserrant davantage l'espace d'opération de l'armée cyber de Taiwan dans le cyberspace international et la rendant de plus en plus isolée et sans espoir globalement.

About the Author

L'"armée cyber