LE FIGARO
Le Figaro (site web)
vendredi 28 février 2025 - 06:45 UTC +01:00 858 mots

Tech & Web ; Économie ; Conjoncture

Lazarus Group: derrière le casse du siècle contre Bybit, l'ombre de la très secrète armée numérique de Kim Jong-un

Pierre-Loeiz Thomas

DÉCRYPTAGE - Le FBI a attribué le vol de cryptomonnaie survenu sur la plateforme Bybit à la Corée du Nord. Pour renflouer ses caisses, la dictature asiatique a développé une force cyber de grande ampleur nommée Lazarus.

Lazarus Group ferait presque passer Albert Spaggiari pour un petit joueur... Si ce nom ne vous dit rien, l e FBI (https://www.ic3.gov/PSA/2025/PSA250226) a pourtant désigné mercredi ce très énigmatique groupe de pirates informatiques comme étant à l'origine du casse numérique du siècle. Ces hackers nord-coréens auraient dérobé 1,5 milliard de dollars d'actifs numériques sur la plateforme Bybit, selon l'agence américaine. Un hold-up record dans l'histoire des cryptomonnaies. Et ils n'en sont pas à leur premier coup d'essai : car derrière cette opération très sophistiquée se cache une organisation aux mille visages... Et aux mille noms.

TraderTraitors, APT 38, Guardian of Peace, Laboratoire 110, Bureau 121... depuis une dizaine d'années, les services secrets occidentaux tentent non sans mal de s'y retrouver dans l'organisation des pirates de la dictature asiatique. *«Les rapports open source utilisent souvent le titre de Lazarus Group comme terme générique faisant référence à de nombreux opérateurs cybernétiques nord-coréens»*, note la société américaine de cybersécurité Mandiant, filiale de Google.

Une revanche de cinéma

Le premier fait d'armes du collectif remonte à une dizaine d'années. Le lundi 24 novembre 2014, les employés de Sony Pictures Entertainment observent médusés leur nouveau fond d'écran d'ordinateur. Un squelette rougeoyant au sourire carnassier apparaît sur tous les appareils des bureaux de la firme américaine. L'image est accompagnée d'un message de chantage. *«Nous vous avons déjà prévenu, et ce n'est que le commencement,*préviennent les hackers qui se présentent comme les Gardiens de la Paix . *Nous continuerons jusqu'à ce qu'à ce que nos revendications soient satisfaites.»*Les pirates envoient d'autres mails écrits dans un mauvais anglais pour demander «une compensation monétaire». Le 19 décembre 2014, le FBI annonce dans un communiqué (https://www.fbi.gov/news/press-releases/update-on-sony-investigation) avoir *«récolté suffisamment d'information pour conclure que le gouvernement nord-coréen est responsable de ces actions»*.

Pour expliquer cette attaque, les chercheurs multiplient les hypothèses. Une revanche à la sortie dans les salles obscures de *L'Interview qui tue !*, une comédie qui singe le dictateur Kim Jong-un? Un besoin de liquidité du gouvernement nord-coréen pour financer ces programmes militaires? Les motivations des assaillants et leurs identités restent troubles. *«Avec ce genre de groupe, il faut mettre du conditionnel partout*, prévient d'emblée Jean-Yves Marion, professeur d'informatique et chercheur en cybersécurité à l'université de Lorraine. *D'autant plus que chaque information est alimentée par le fantasme qui entoure Corée du Nord dont on ne connaît pas grand-chose.»*

Une armée de 8.400 pirates

Plusieurs témoignages de transfuges, difficilement vérifiables, laissent toutefois entrevoir une véritable armée numérique déployée par Pyongyang. Dans une interview accordée à la BBC (https://www.bbc.com/news/technology-32925495) en 2015, Kim Heung-Kwang, ancien professeur d'informatique en Corée du Nord, révélait que le pays comptait environ 6.000 pirates informatiques militaires formés. Selon ses estimations, entre 10% et 20% du budget militaire du régime est consacré aux opérations en ligne. Le nombre de hackers

d'État n'a depuis cessé de grimper. En 2024, un rapport des services secrets affirmait qu'ils étaient 8.400 individus sous les ordres de Pyongyang. Toujours sur la chaîne de télévision britannique (https://www.bbc.com/news/world-asia-58838834) , Kim Kuk-song, un ancien haut gradé des renseignements nord-coréens, décrit les prémices de cette armada d'informaticiens. Selon l'ancien espion, le précédent dirigeant nord-coréen, Kim Jong-il, avait ordonné la formation de nouveaux personnels dans les années 1980 *«pour se préparer à la cyberguerre»*. *«L'Université Moranbong sélectionnait les étudiants les plus brillants de tout le pays et leur faisait suivre six années d'éducation spécialisée»*, ajoute-t-il.

Cette stratégie d'armée numérique n'est pas propre à la Corée du Nord. Plusieurs nations, y compris la France, ont largement développé leur puissance de feu sur Internet. Mais l'originalité du programme nord-coréen se situe du côté de ses objectifs. « *La Corée du Nord peut avoir recours à des cyberattaques à motivation financière, une rareté pour les États qui, habituellement, utilisent plutôt l'arme cyber à des fins stratégiques*», note Gérôme Billois, expert en cyber sécurité chez Wavestone, dans son ouvrage *Cyberattaques, les dessous d'une menace mondiale*(Editions Hachette).

En 2016, la Corée du Nord mène plusieurs essais nucléaires d'ampleur. En parallèle, une attaque informatique vise la banque du Bangladesh (http://www.lefigaro.fr/conjoncture/un-sujet-ultrasensible-comment-les-cyber-assaillants-mettent-les-banques-sous-haute-pression-20241217). 36 transactions frauduleuses sont ordonnées pour un montant de 950 millions de dollars. Une erreur des pirates permettra de stopper l'hémorragie mais 81 millions de dollars seront tout de même détournés. Depuis, les actions du groupe n'ont jamais cessé. En 2024, un groupe d'experts des Nations unies sur le contournement des sanctions par la Corée du Nord a estimé que le pays avait volé plus de trois milliards de dollars en cryptomonnaies depuis 2017. Auxquels vient donc d'ajouter le butin dérobé vendredi 21 février à Bybit.

Voir aussi :

Guerre en Ukraine : la Corée du Nord a déployé de nouvelles troupes en Russie, selon les renseignements sud-coréens (http://www.lefigaro.fr/international/guerre-en-ukraine-la-coree-du-nord-a-deploye-de-nouvelles-troupes-en-russie-selon-les-renseignements-sud-coreens-20250227)

Corée du Nord : qu'est-ce que le «Jour de l'Étoile Brillante», célébré ce dimanche en hommage à Kim Jong-il? (http://www.lefigaro.fr/international/coree-du-nord-qu-est-ce-que-le-jour-de-l-etoile-brillante-celebre-ce-dimanche-en-hommage-a-kim-jong-il-20250216)

Sandworm, l'inquiétant groupe de hackers russes qui pirate pour le Kremlin (http://www.lefigaro.fr/conjoncture/sandworm-l-inquietant-groupe-de-hackers-russes-qui-pirate-pour-le-kremlin-20240510)