Méthodes numériques pour contourner les sanctions de l'ONU
Étude de cas de la Cyber Force de la République populaire démocratique de Corée

Par Ashley Taylor

Introduction

La cybersphère est une nouvelle ligne de front dans la mise en œuvre et le contournement des sanctions de l'ONU. Parce que l'Internet fournit un espace virtuel pour la communication et les transactions instantanées, il ouvre par nature des voies moins coûteuses et non réglementées permettant aux acteurs malhonnêtes de violer les normes internationales. Les utilisations illicites des technologies numériques dépassent les progrès des technologues licites, qui ne privilégient généralement pas la sécurité internationale dans leurs activités.

La République populaire démocratique de Corée (RPDC), en particulier, est de plus en plus apte à utiliser des outils numériques pour contourner les sanctions. Ils ont mis au point des techniques numériques pour générer des revenus afin de financer leurs efforts de prolifération illégale, acquérir du renseignement et du savoir-faire technique et nuire aux affaires et à la réputation de leurs adversaires étrangers, y compris pour perturber ceux qui surveillent l'application du régime de sanctions de la RPDC adopté avec l'ONU résolution 1718 en octobre 2006. Kim Jong-Un s'est récemment vanté de ce que « la guerre cybernétique, ainsi que des armes nucléaires et des missiles, est une » épée polyvalente « garantissant la capacité de notre armée à frapper sans relâche ». Un transfuge militaire nord-coréen a déclaré que la cyberforce était considérée l'arme la plus puissante de la « guerre secrète » et ses membres sont considérés comme faisant partie de l'élite et constituent l'un des rares postes bien rémunérés.

Où iront-ils d'ici? Les preuves suggèrent que les acteurs étatiques nord-coréens et les mandataires non étatiques recourent de plus en plus à de nouvelles technologies d'anonymisation tels que les cryptodevises, le Web sombre, le cryptage et les cyberattaques évoluées difficiles à détecter. Le rapport du Groupe d'experts de l'ONU sur la RPDC a estimé que le seul vol de cryptomonnaies lui avait rapporté 571 millions de dollars.

Cette étude de cas se concentrera d'abord sur les origines de la cyberforce nord-coréenne en examinant les attaques documentées menées à l'aide de méthodes de piratage traditionnelles,

en décrivant les tactiques observées lors d'intrusions et d'attaques antérieures et en examinant les rapports sur les adaptations de la Corée du Nord à des technologies plus avancées. Cet article se terminera par des recommandations sur les mesures de cybersécurité et les directives réglementaires à adopter.

Cybersphère et sanctions de l'ONU : le contexte réglementaire

Les entrepreneurs en technologie exploitant le potentiel de transformation et de perturbation richement gratifiant des technologies numériques ont toujours été encouragés par des normes réglementaires souples. Cependant, la reconnaissance de l'impact potentiellement néfaste de ces nouvelles technologies sur les questions politiques, sociales et de sécurité incite maintenant les régulateurs européens et américains à intervenir et à discipliner les entreprises technologiques qui enfreignent les normes nationales et internationales.

Bien que des cadres nationaux de cyberréglementation aient été adoptés par 138 pays, la plupart mettent l'accent sur la prévention de la criminalité au niveau national tout en restant parfaitement détachés des conséquences pour la sécurité internationale d'une cybersphère armée. Le Conseil de sécurité des Nations Unies n'a abordé les cybermenaces que de manière inégale et incohérente, malgré 20 années de rapports et de preuves sur la manière dont la technologie numérique a provoqué des conflits et profité à des acteurs sanctionnés. À ce jour, seul le Groupe d'action financière (GAFI) modifie progressivement ses 40 recommandations relatives à la prévention et à la protection contre les variations numériques de la lutte contre le blanchiment d'argent, le financement de la lutte contre le terrorisme et le financement de la non-prolifération.

Certaines mesures unilatérales ont été prises dans le sens des cybersanctions. Par exemple, les États-Unis ont approuvé deux comptes de cryptomonnaie appartenant à des Iraniens, et l'UE a publié des directives, notamment une boîte à outils pour la cyberdiplomatie. Pourtant, ces étapes sont loin de l'approche globale nécessaire.

Comme indiqué dans les sections suivantes, l'utilisation diversifiée des technologies numériques par la Corée du Nord illustre le défi multiforme de l'application des sanctions dans le cyberespace. La capacité démontrée de la RPDC à mener des cyberattaques monastiques, mais à peine perceptibles et peu coûteuses, sur des données ou des avoirs financiers appartenant à des gouvernements, à des entreprises et à des particuliers incite énormément à adopter des outils offensifs de guerre numérique et informatique. Les chefs de file de l'industrie et les décideurs doivent également se pencher sur le rôle que jouent des applications civiles apparemment inoffensives telles que les cryptomonnaies ou les boucliers d'identité en ligne.

Au niveau international, les sanctions existantes contre la Corée du Nord ne qualifient pas les atteintes à la cyberinfrastructure internationale des actes sanctionnables. Compte tenu de la nature nébuleuse de la lutte contre les cybermenaces liées à la Corée du Nord, les leaders du gouvernement et de l'industrie, passifs, courent le risque de :
(1) Les Nord-Coréens attaquant ou se préparant à attaquer leurs systèmes informatiques, entraînant une perte de revenus, de données critiques et de capacités opérationnelles;
(2) les manquements à la conformité et la perte de réputation dus à des actions nord-coréennes permettant des violations des sanctions et
(3) être laissé pour compte dans les efforts et les initiatives visant à réglementer le secteur des technologies, avec des implications potentiellement considérables pour leur économie et leur sécurité nationale
En outre, dans les régions où le secteur de la cybersécurité et le contrôle gouvernemental ne disposent pas de voies bien établies pour le partage des connaissances et la collaboration, le potentiel de réaction efficace et/ou responsable face aux cyberattaques est moindre.

Réseaux Internet de la RPDC

On estime que la RPDC compte jusqu'à 6 000 cyberguerriers, organisés en différents groupes appelés Lazarus, Bureau 121, Hidden Cobra, Bluenoroff, Apt 38, TEMP.Hermit et Andariel. Un des principaux contributeurs au cyber arsenal nord-coréen est la canalisation du système éducatif nord-coréen, depuis son plus jeune âge, des meilleurs esprits techniques en sciences et en mathématiques vers des cours d'informatique et d'ingénierie, et finalement vers l'université de science et technologie de Pyongyang (PUST), la seule université financée par l'étranger dans le pays. PUST a été ouvert en 2010 avec un contrat entre le gouvernement de la Corée du Nord et la Fondation pour l'éducation et la culture de l'Asie du Nord-Est (NAFEC). Certains volontaires étrangers travaillent à l'université, tandis que d'autres viennent quelques semaines pour enseigner un cours.

En 2015, le défenseur nord-coréen Jang Se-yul, qui affirme faire partie du commandement de la cyberguerre à Pyongyang, a déclaré que les formations de PUST préparaient les étudiants au piratage. PUST rejette ces allégations en invoquant des preuves insuffisantes. Quoi qu'il en soit, il est vrai qu'un sous-produit de l'apprentissage de l'ingénierie informatique et de la sécurité est en train de jeter les bases du piratage informatique. Les bases informatiques, telles que la rédaction de programmes informatiques, la création d'algorithmes (procédures d'analyse de données) et l'interface avec un système d'exploitation, font également partie intégrante du piratage. Tout étudiant légitime en cybersécurité finira par mener des expériences de piratage « au chapeau blanc », dans le cadre desquelles il tentera de pénétrer dans les réseaux d'information de manière à révéler ses vulnérabilités.

Une fois bien formés, certains étudiants rejoignent la cyberforce située en Corée du Nord, tandis que d'autres se joignent à des équipes à l'étranger pour lutter contre le piratage

informatique ou à l'étranger pour créer des sociétés-écrans afin de contourner les sanctions.[1] Private security firms have analyzed the internet activities of DRPK-based users to understand the network of supporters abroad, and found evidence of supporters physically located or living in Bangladesh, China, India, Indonesia, Kenya, Mozambique, Nepal and Thailand.[2]

L'utilisation des technologies les plus avancées, telles que les techniques d'anonymisation permettant des attaques anonymes, et les cryptomonnaies, qui permettent de nouvelles méthodes de génération de fonds et de transfert secret des gains piratés constitue une arme majeure pour ce réservoir de talents. Démontrant sa capacité à adopter les dernières tendances en matière de cyber, la RPDC a organisé une conférence sur la chaîne de blocs et les cryptodevises à PUST en avril 2019, organisée avec l'aide d'un entrepreneur britannique.[3]

Les principales technologies d'anonymisation utilisées par la Corée du Nord, ainsi que les technologies auxiliaires, sont expliquées dans le tableau suivant.

Technologies pour les attaques anonymes et les sanctions

technologies	Description et utilisation par la RPDC
Intranet	Un réseau fermé non connecté au Web libre et ouvert; une collection interne de serveurs et d'ordinateurs en réseau permettant uniquement l'accès à certaines pages et à certains fichiers (l'infrastructure Internet de la RPDC est un intranet appelé Kwangmyong qui n'est accessible que de l'intérieur des frontières de la Corée du Nord)
Web sombre	La partie de l'Internet qui n'est pas indexée par les moteurs de recherche populaires tels que Google ou Yahoo, ce qui signifie que les pages ne sont pas faciles à découvrir, à moins que l'utilisateur ne sache où regarder ; où des activités illégitimes peuvent se produire sans être détectées, telles que des forums et des marchés pour l'acquisition d'armes, le vol de propriété intellectuelle, etc.
Tor	Un navigateur qui permet d'accéder au Web sombre. Il peut être téléchargé gratuitement par toute personne ayant accès à Internet.

[1] https://www.reuters.com/article/us-sony-cybersecurity-northkorea/in-north-korea-hackers-are-a-handpicked-pampered-elite-idUSKCN0JJ08B20141205

[2] https://www.recordedfuture.com/north-korea-internet-usage/

[3] https://www.independent.co.uk/life-style/gadgets-and-tech/news/north-korea-cryptocurrency-blockchain-conference-pyongyang-a8643391.html

technologies	Description et utilisation par la RPDC
cryptage	Il s'agit de coder des données avec des codes secrets que ne possèdent que les participants prévus. Il est utilisé pour la messagerie cryptée, afin que les informations puissent transiter par les protocoles Internet sans être détectées. Il est également utilisé comme élément de conception fondamental pour la création de cryptodevises. Les Nord-Coréens ont utilisé l'application de messagerie cryptée chinoise WeChat pour coordonner les transferts de navire à navire.
cryptomonnaies	Un type de monnaie numérique, où chaque version a des règles spécifiques sur la manière dont les pièces naissent et sur leur utilisation. Il utilise le cryptage pour rendre les pièces difficiles à contrefaire et fournir l'anonymat aux utilisateurs, ce qui signifie que l'identité du monde réel n'est pas nécessaire pour les acquérir ou les échanger. Chaque cryptomonnaie, qui compte des milliers, a ses propres règles et demandes du marché pour obtenir des pièces. Les transactions sont enregistrées sur un grand livre partagé, appelé chaîne de blocs.
chaîne de blocs	Une base de données composée du grand livre des transactions d'une cryptomonnaie spécifique. Une fois saisie, leur modification est très difficile/coûteuse. C'est donc un moyen utile de suivre les données « de confiance » au fil du temps. Chaque transaction est visible à jamais pour l'ensemble du réseau. La devise native de chaque chaîne de blocs est généralement nécessaire pour interagir sur le réseau. Ces réseaux chaîne de blocs et leurs devises peuvent être publics, telles que Bitcoin, ou privés, uniquement utilisables par un groupe sélectionné.
virtual private network (VPN)	Un service qui permet à un utilisateur de créer un portail privé pour accéder anonymement à l'Internet public, de sorte que leurs données, leurs informations et leur accès au Web ne puissent être suivis et/ou que leur contenu ne puisse être ni observé ni censuré
virtual private server (VPS)	Un service d'hébergement d'applications Web ne nécessitant pas l'utilisation d'un serveur tiers, tel que Google, Microsoft ou Amazon
transport layer security (TLS)	Un niveau supplémentaire de cryptage ajouté aux réseaux d'information pour garantir que toutes les données transférées sur le réseau sont difficiles à obtenir/à observer

technologies	Description et utilisation par la RPDC
Réseaux sociaux	Ce sont les quartiers en ligne, ou les lieux de la sphère numérique où les gens interagissent. Dans le cas de la RPDC, les médias sociaux sont utiles pour promouvoir leur propagande auprès de leurs partisans à l'étranger, ainsi que pour créer des comptes frauduleux afin de promouvoir des entreprises de façade et d'accomplir d'autres tactiques de piratage sans révéler leur véritable identité.

À partir d'avril 2018, les chercheurs en sécurité ont constaté une augmentation de 1 200 % de l'utilisation de ces services Internet privés, ce qui aide les Nord-Coréens dans leurs recherches et leurs attaques. Ces outils, combinés au Kwangmyong Intranet, hautement censuré, de la RPDC, limitent la capacité des agences étrangères de cyberrenseignement et de sécurité à comprendre pleinement la cyberforce nord-coréenne.[4]

Les Nord-Coréens utilisent toujours le Web public, en particulier les médias sociaux, pour coordonner le contournement des sanctions. Depuis fin 2017, ils s'éloignent des réseaux sociaux et des médias occidentaux au profit des versions chinoises, où ils s'assimilent plus facilement sans être identifiés. Une exception notable est l'utilisation continue de LinkedIn, qui reste probablement utile pour créer de fausses personnalités (c'est-à-dire sans affiliation nord-coréenne) afin de promouvoir des sociétés-écrans, de créer des relations avec des victimes potentielles de cyberattaques et de comprendre comment les pirater au mieux et promouvoir les opportunités commerciales telles que les nouvelles monnaies numériques. Ces incidences sont décrites plus en détail dans les sections suivantes.

Techniques utilisées par la RPDC pour contourner les sanctions

Le tableau suivant décrit les techniques utilisées par les Nord-Coréens dans diverses attaques.

Techniques	Description
maliciel	Les pirates informatiques installent un programme informatique nuisible sur l'ordinateur de la victime, qui peut permettre d'atteindre un certain nombre de buts, tels que l'accès du pirate informatique à l'ordinateur

[4] https://krebsonsecurity.com/2014/12/the-case-for-n-koreas-role-in-sony-hack/#more-29249
internet usage report

Techniques	Description
botnet	Lorsque les pirates informatiques s'emparent de nombreux ordinateurs et créent une infrastructure de coordination des attaques nécessitant une puissance de traitement importante, telle que DDOS (next)
distributed denial of service (DDOS)	Utiliser de nombreux ordinateurs (souvent des réseaux de zombies) pour tenter d'accéder à une page Web donnée, de sorte qu'elle soit surchargée et cesse de fonctionner. L'attaque vise souvent à nuire à l'entreprise (par exemple, l'incapacité du commerce normal de fonctionner)
phishing	Envoi de fausses communications, telles qu'un faux courrier électronique, qui poussent les utilisateurs à entrer leurs mots de passe sur une page Web appartenant aux pirates informatiques et/ou à télécharger un faux fichier contenant des logiciels malveillants
harponnage	Similaire aux hameçonnages, sauf que les victimes sont plus ciblées, après une enquête de base menée par les assaillants, afin de déterminer ce à quoi la victime sera le plus susceptible, par exemple en créant un faux compte et en se liant d'amitié avec les médias sociaux
exploit de vulnérabilité système	Trouver des failles dans les systèmes d'infrastructure/d'exploitation telle que Microsoft Windows qui donnera aux pirates l'accès à l'ordinateur. Ces failles sont utiles aux pirates pour coordonner des attaques généralisées visant de nombreuses victimes qui utilisent toutes le même logiciel avec cette vulnérabilité.
virus	Un programme informatique conçu pour infecter les ordinateurs et provoquer un résultat spécifique (par exemple, détruire des fichiers, voler des informations) qui se propage automatiquement, ce qui signifie qu'il trouve le moyen d'infecter autant d'autres ordinateurs que possible via l'ordinateur infecté, causant ainsi des dommages importants peu de temps
échange/échange de cryptomonnaie	Une industrie florissante de services qui permettent aux utilisateurs de transférer des cryptodevises dans d'autres cryptodevises et fiat (monnaies garanties par l'État). En ce qui concerne les Nord-Coréens, ces transferts peuvent transformer des pièces volées en argent liquide et/ou masquer facilement une piste de propriété de pièces volées en passant d'une cryptomonnaie à une autre. Il existe de nombreux échanges de cryptomonnaie qui permettent la négociation sans aucune réglementation.
extraction de cryptomonnaie	Chaque cryptomonnaie a des règles spécifiées sur la manière dont de nouvelles pièces peuvent être gagnées, ce qui nécessite souvent l'utilisation d'ordinateurs spécialisés dotés de puissants GPU pour traiter les données en permanence tout au long de la compétition pour gagner de nouvelles

Techniques	Description
	pièces libérées sur une période de temps spécifiée
Initial Coin Offering (ICO)	La création d'une nouvelle cryptomonnaie avec une levée de fonds réalisée pour prévendre une partie des pièces, avec des promesses quant à la manière dont les utilisateurs pourront utiliser les pièces, souvent avec le sous-texte d'un retour financier
watering hole attack	L'attaquant compromet un site Web présentant un intérêt pour la ou les cibles visées et ajoute du code pour inciter un utilisateur à accéder à une nouvelle page Web qui l'incitera à installer un logiciel malveillant
ransomware (type de virus)	Un logiciel malveillant qui crypte le disque dur de la victime et demande une rançon dans un délai limité s'ils souhaitent que leurs données soient restituées et non détruites

Méthodes spécifiques utilisées pour contourner les sanctions

Bien que les techniques décrites ci-dessus puissent être des composants autonomes d'une attaque ou d'une acquisition, elles sont souvent combinées dans les méthodes suivantes et répétées au cours de multiples incidents.

Méthodes pour nuire aux adversaires, voler des informations et parfois demander une rançon

Les Nord-Coréens ont perpétré des cyberattaques pour nuire à leurs adversaires. Ils ont été en mesure de causer des dommages considérables, comme dans le cas de l'attaque de Sony Pictures. En réponse à la sortie prochaine d'un film décrivant l'assassinat de Kim Jong-un, des pirates informatiques de la RPDC ont détruit des fichiers, divulgué des informations sensibles, telles que des informations sur les salaires des employés ayant entraîné une crise de l'égalité des sexes pour l'entreprise, et causé environ 100 millions de dollars dans cyber dommages liés à l'entreprise.

Comme le montre le tableau ci-dessous, les attaques de la RPDC évoluent dans le sens d'une intégration des moyens de générer des revenus en plus de causer des dommages. En 2017, le virus Wannacry s'est répandu dans le monde entier, infectant les ordinateurs et cryptant toutes leurs données. Wannacry a alors activé une demande urgente de paiement d'une rançon en bitcoin, si les utilisateurs voulaient récupérer leurs données. Comme les bitcoins sont difficiles à associer à leurs propriétaires réels, il est très difficile de savoir combien les Nord-Coréens ont réellement généré de cette attaque. Au moins 140 000 USD ont été détectés, bien que le nombre réel soit probablement beaucoup plus élevé. Cependant, les dommages causés aux

entreprises infectées se chiffraient à des millions et ont souvent des conséquences catastrophiques, telles que l'arrêt des ordinateurs critiques dans les hôpitaux britanniques.

Incidences (ordre du temps)	Techniques utilisées	Dommages connus
DDOS (2009)	botnet, ddos	31 millions USD à 46 millions USD de préjudice
DDOS (20 011)	botnet, ddos	40 sites Web, 820 disques durs affectés
320 Dark Seoul (2013)	harponnage, maliciel	données détruites, 75 millions USD de réparations
Sony Pictures (2014)	harponnage, maliciel	tentative infructueuse de rançon d'informations sensibles volées, puis fuite des informations portant atteinte à la réputation et coût de réparation des systèmes informatiques : environ 100 millions de dollars
Korea Hydro & Nuclear Power Attack (2014)	harponnage, maliciel	A attaqué 3 571 employés de Korea Hydro et tenté de détruire leurs disques. Les pirates ont obtenu et publié des plans pour six centrales nucléaires à six reprises sur Twitter et ont réclamé 10 milliards de dollars américains.
Interpark (2016)	maliciel	fuite d'informations privées de 10,3 millions d'utilisateurs. tentative de rançon en Bitcoin de 2,7 millions USD
Entreprises non divulguées dans l'industrie de la défense (2016)	exploit de vulnérabilité système	A obtenu et divulgué des données classifiées, telles que les plans d'avions
Autorité de surveillance financière polonaise (2017), entre autres objectifs	attaque au point d'eau, maliciel	les banques visitant le site Web vers une autre page où les victimes étaient invitées à télécharger des logiciels malveillants. Peut-être a été utilisé dans les attaques rapides (section suivante)
Virus Wannacry (2017)	exploit de vulnérabilité système pour insérer un ransomware qui chiffrait les fichiers des ordinateurs cibles et exigeait une rançon bitcoin pour les fichiers	Au moins 140 000 USD gagnés en cryptomonnaies, dommages critiques causés aux entreprises et aux institutions telles que les hôpitaux britanniques

Incidences (ordre du temps)	Techniques utilisées	Dommages connus
Groupe d'experts des Nations Unies sur la RPDC	inconnu	A saboté le comité en retardant la publication de son rapport sur la RPDC

Méthodes purement génératrices de revenus

Ces dernières années, les Nord-Coréens ont manifesté leur préférence pour la génération de fonds grâce à leur cyberexpertise. En février 2016, des pirates informatiques nord-coréens ont harponné des employés de la Banque centrale du Bangladesh et ont installé des logiciels malveillants pour obtenir leurs informations d'identification légitimes pour le système de messagerie interbancaire mondial SWIFT. Ils ont ensuite compromis le compte du Bangladesh auprès de la Réserve fédérale américaine et tenté de transférer 951 millions USD des fonds de la banque à des comptes du monde entier, tout en ne réussissant à acquérir que 81 millions USD. L'argent a été transféré sur un compte aux Philippines et a été blanchi au moyen de plusieurs comptes bancaires, d'une entreprise d'envoi de fonds et de casinos.[5] Cette même attaque a été tentée à maintes reprises dans des banques du monde entier, d'autres hacks ayant gagné entre 10 et 15 millions de dollars chacun.

Après ces attaques, les pirates nord-coréens ont commencé à concentrer leurs efforts sur les échanges de cryptomonnaie, les services qui servent de banques en ligne pour échanger la multitude de cryptodevises. Les auteurs ciblent les portefeuilles numériques où les échanges de cryptomonnaie stockent les fonds détenus entre les transactions pour les clients. Ces portefeuilles sont des cibles très lucratives, car ils contiennent d'énormes quantités de fonds de clients. Le vol des signatures numériques (mots de passe) qui contrôlent ces portefeuilles et la réappropriation des fonds génèrent des gains très importants.

La RPDC était responsable de 75 % des piratages d'échange de cryptomonnaie rapportés dans le monde (environ 882 millions USD) de la fin de 2016 à l'automne 2018. Ce revenu numérique est difficile à localiser et peut donc être utilisé pour contourner ou geler le gel des avoirs et autres les sanctions.

[5] https://www.thecipherbrief.com/kim-digs-cybercrime-coin-sanctions-cant-snatch

Incidences notables (ordre du temps)	Techniques utilisées	Dommages causés/impacts estimés
Cybercrise du Bangladesh Bank (2016)	harponnage, maliciel, virement bancaire Swift frauduleux	a volé 81 millions USD
Casinos en ligne piratés (2016, 2017)	maliciel, inséré une astuce dans le jeu	inconnu
Banque internationale d'Extrême-Orient (2017)	harponnage, maliciel, virement bancaire Swift frauduleux	60 millions USD transférés, mais la plupart récupérés
Standard Chartered Plc – Bancomext (2018)	harponnage, maliciel, virement bancaire Swift frauduleux	tentative infructueuse de piratage de 110 millions USD, bien que 15 millions USD aient été volés d'autres attaques contre des banques mexicaines
Banco de Chile (2018)	harponnage, maliciel, virement bancaire Swift frauduleux	10 millions de dollars US acquis et transférés vers des comptes à Hong Kong
Open Bazaar store pour les produits nord-coréens — (depuis 2016)	a créé un magasin pour vendre des articles spécialisés nord-coréens tels que des cigarettes, de l'argent et des timbres	inconnus
Échange de cryptomonnaie Yazipon (2017)	harponnage pour obtenir le mot de passe du compte Exchange, échange cryptomonnaie	5,3 millions USD volés
Andariel maliciel (2017)	maliciel installé qui extrait la cryptomonnaie sur l'ordinateur cible	70 pièces onero, $ 26 000 USD gagnés
Échange de cryptomonnaie Coinis (2017)	harponnage pour obtenir le mot de passe du compte Exchange, échange cryptomonnaie	7 millions de dollars US volés
Échange de cryptomonnaie Yobit (2017)	harponnage pour obtenir le mot de passe du compte Exchange, échange cryptomonnaie	5,6 millions USD volés

Incidences notables (ordre du temps)	Techniques utilisées	Dommages causés/impacts estimés
Échange de cryptomonnaie Coincheck (2018)	harponnage pour obtenir le mot de passe du compte Exchange détenant un nouveau cryptomonnaie NEM Coin, échange de cryptomonnaie	534 millions USD volés
Échange de cryptomonnaie Bithumb (2018)	harponnage pour obtenir le mot de passe du compte Exchange, échange cryptomonnaie	32 millions USD volés
Interstellaire, Stellaire, HOLD ou HUZU (2018)	une offre initiale de pièces (ICO) pour une nouvelle cryptomonnaie; le nom a été changé plusieurs fois pour essayer de brouiller les origines	inconnu
MarineChain (2018)	un ICO pour une nouvelle cryptomonnaie qui prétendait frauduleusement vendre la propriété de gros navires.	fonds inconnus gagnés lorsque le projet s'est dissipé lorsqu'il a été exposé. Cependant, il évoque un nouveau moyen d'éviter les sanctions sur la navigation en créant un nouveau moyen de dissimuler la propriété d'un navire.
Extraction/échange de cryptomonnaies (2015 - présent)	utiliser des ordinateurs en Corée du Nord pour extraire diverses cryptomonnaies, puis les convertir en monnaie utilisable ou les échanger contre d'autres biens	estimation de 150 000 USD/200 000 USD par an

Il est clair qu'avec le temps, les pirates nord-coréens se lancent dans des attaques génératrices de revenus, en particulier celles qui tirent parti des normes réglementaires peu strictes en matière de cryptomonnaie. Les Nord-Coréens montrent clairement qu'ils sont prêts à tirer parti des tendances technologiques. Leurs hacks d'échange de cryptomonnaie et ICO coïncident parfaitement avec un engouement spéculatif de la fin de 2017 — début de 2018, lorsque la valeur marchande des devises numériques a atteint son plus haut niveau. Le marché total de ces pièces en 2018 a oscillé entre 128,9 milliards de dollars et 818,1 milliards de dollars.[6]

[6] https://coinmarketcap.com/charts/

Mesures de recommandation de cybersécurité

Pour faire face à ces menaces, des mesures de cybersécurité peuvent être adoptées et, le cas échéant, requises par la réglementation. Les deux domaines les plus importants à traiter pour prévenir les cyberattaques sont les suivants :

(1) Formation des employés sur la manière de reconnaître les tentatives de piratage, telles que le harponnage et les pièces jointes suspectes

Quel que soit le niveau de sécurité d'une nouvelle technologie telle que la chaîne de blocs, les techniques telles que le harponnage prévaudront comme méthode de compromission des systèmes. L'authentification à deux facteurs peut réduire l'impact d'une violation, mais elle ne remplace pas le besoin d'éducation.[7] Quel que soit le niveau de sécurité d'une nouvelle technologie telle que la chaîne de blocs, les techniques telles que le harponnage prévaudront comme méthode de compromission des systèmes. L'authentification à deux facteurs peut réduire l'impact d'une violation, mais elle ne remplace pas le besoin d'éducation.

(2) Maintenir les protocoles des systèmes informatiques au diapason des normes de l'industrie en matière de cybersécurité, notamment rester informé des cyberattaques récentes.

Comme indiqué dans le présent rapport, de nombreuses attaques nord-coréennes se concentrent sur les vulnérabilités des protocoles de système d'exploitation. Les équipes informatiques/de sécurité doivent rester à jour en :

- Créant de mots de passe forts et mise en place d'un système nécessitant la modification régulière des mots de passe et, si possible, l'utilisation d'un système de gestion de mots de passe;
- Restant au courant de toutes les versions de correctifs et les appliquer rapidement;
- Remplaçant les anciens systèmes d'exploitation par les dernières versions;
- Maintenant un logiciel antivirus à jour, le cas échéant, et analyser tous les logiciels téléchargés sur Internet avant de les exécuter.
- Limitant les possibilités (autorisations) des utilisateurs d'installer et d'exécuter des applications logicielles non désirées et d'appliquer le principe des privilèges minimaux à tous les systèmes et services;

[7] Une authentification à deux facteurs est une procédure de sécurité qui demande à l'utilisateur de vérifier son identité en plus de saisir un mot de passe en entrant un code reçu sur son appareil mobile. Il est préférable d'utiliser une application pour l'authentification plutôt qu'un numéro de téléphone mobile, car les numéros de téléphone mobiles peuvent être plus facilement basculés vers le contrôle des pirates.

- Recherchant et supprimer les pièces jointes suspectes. Les entreprises et les organisations peuvent bloquer les messages électroniques provenant de sources suspectes contenant des pièces jointes. et
- Activant un pare-feu personnel sur les postes de travail de l'organisation et le configurer pour refuser les demandes de connexion non sollicitées.

S'adresser au Ransomware

- Sauvegardez régulièrement les systèmes et conservez une copie chiffrée des sauvegardes récentes hors site et hors ligne.
- Il existe des logiciels qui prétendent arrêter les biens en rançon en bloquant le cryptage non autorisé de fichiers. Demandez au personnel de sécurité d'évaluer ces outils.

Réglementation et juridiction

En matière de cybersécurité, de guerre de l'information et d'élaboration de politiques connexes, la meilleure stratégie consiste à devancer la menace. Pour les pays et les chefs de file de l'industrie qui attendent des informations sur la composante cybernétique des sanctions, il est sage de prendre des mesures pour que les sociétés de technologie numérique veillent à ce que les violations des sanctions ne soient pas commises dans le cyberespace, ouvrant ainsi à l'industrie un moyen de progresser, conformément aux normes de paix et de sécurité humaines déjà définies. Il est également nécessaire que les entreprises technologiques communiquent les mesures qu'elles prennent pour se conformer aux sanctions imposées par l'ONU.

La priorité absolue est de traiter les meilleures pratiques en matière de cyberactivités comme leur équivalent dans le monde réel. En fin de compte, il n'y a pas de différence entre le blanchiment d'argent avec des actifs classiques ou cybernétiques. L'anonymat et la nouveauté de ces technologies renforcent le potentiel de pratiques trompeuses et d'actions risquées des entités déjà sanctionnées et des nouveaux acteurs menaçants. En raison des risques accrus, les pratiques de diligence raisonnable doivent être plus résolues. Les acteurs qui préfèrent opérer au sein de réseaux d'information à base de chaînes de blocs ou hautement cryptés s'écartent des pratiques en vigueur dans l'industrie et des obligations de rapport existantes. Par conséquent, une vigilance accrue est requise pour toute entité engagée dans des transactions relatives aux armes ou aux finances, dans les transports maritimes ou aériens, ainsi que dans les interactions avec les travailleurs ou les diplomates nord-coréens, pour lesquels l'utilisation de plates-formes technologiquement avancées est suggérée.

Les mesures recommandées comprennent :

- Insister sur la divulgation complète de l'identification vérifiable, de l'objet des transactions proposées et de toute autre information pertinente qui serait prise en compte dans une transaction réelle;
- Clarifier la raison d'être de l'activité proposée pour faire en sorte que toutes les étapes économiques servent des objectifs raisonnables, logiques et légitimes;
- Vérifier toutes les parties impliquées lors de la création de nouvelles cyberentreprises, assurez-vous que le financement et les capitaux, versés sous forme de monnaie numérique ou non, ne sont pas liés à une violation des sanctions ni à des actifs qui doivent être bloqués;
- Imposer des exigences de divulgation à toute entreprise ou entreprise basée sur la technologie de la chaîne de blocs pour authentifier la légitimité des actifs, du contenu des portefeuilles numériques ou des objectifs des contrats intelligents;
- Partager des informations sur les attaques contre la communauté de la cybersécurité et renforcer la coopération avec la recherche et la réglementation;
- Insister sur les protections professionnelles du réseau pour les institutions financières et les entreprises, y compris les émetteurs de cryptomonnaie ou les échanges, en commençant par la formation aux logiciels malveillants/phishing/mots de passe et la politique visant à mieux protéger le système financier national contre les intrusions non autorisées;
- S'assurer que les sociétés d'hébergement Web vérifient que la nature du trafic des sites qu'elles hébergent ne contribue pas aux violations des sanctions;
- Veiller à ce que les entreprises de médias numériques/sociaux surveillent les publicités pour s'assurer qu'elles ne contribuent pas aux violations des sanctions; et
- Imposer des obligations d'intégrité aux exploitants d'installations d'informatique en nuage pour maximiser la protection et s'assurer qu'ils n'hébergent pas d'activités passibles de sanctions, par exemple, logiciels malveillants.

Lorsque vous traitez avec des individus, des entreprises ou des entités déjà sous sanctions de l'ONU :

- Bloquer tout commerce de produits, composants ou technologies soumis à un embargo;
- Bloquer les comptes financiers et les portefeuilles numériques, et signalez les rapports de transaction suspecte, le cas échéant; et
- Interdire toutes les activités numériques ou l'accès aux comptes sur les plates-formes technologiques numériques, y compris les médias sociaux, les marchés, les applications, l'informatique en nuage et la messagerie électronique, s'il existe des indications selon lesquelles des activités pourraient contribuer à sanctionner des violations.

Conclusion

Reconnaître l'expertise de la cyberforce nord-coréenne est particulièrement important alors que la communauté internationale continue de rechercher un accord de non-prolifération nucléaire avec la RPDC. Il faudra s'intéresser aux futures négociations pour comprendre comment la Corée du Nord acquiert des technologies et collecte secrètement des fonds. Pour décrypter les prochains mouvements des Nord-Coréens, il sera important de prêter attention à la direction prise par le secteur de l'anonymisation des technologies, en particulier les industries de la cryptomonnaie et des technologies cryptées, et d'extrapoler le type d'avantages qu'un acteur malhonnête aurait à gagner avec peu de réglementation ces champs. Plus d'idées liées à la manière dont elles vont progresser seront laissées à une étude ultérieure.

À propos de Ashley Taylor

Praticienne, entrepreneure et chercheuse, Ashley Taylor est profondément plongée dans l'intersection des technologies numériques et de la sécurité internationale. En tant que membre de la première génération d'entrepreneurs chaîne de blocs, Taylor a été très tôt attiré par les ramifications potentielles des communications cryptées et des technologies de grand livre distribué sur l'intégrité du commerce et le développement social. Travaillant avec des organisations technologiques et financières, elle développe actuellement un cadre humaniste impliquant de nouvelles technologies et des critères de mise en œuvre qui soutiennent le maintien de la paix et de la sécurité internationales.