16 mai 2022

INSTRUCTIONS CONCERNANT LES INFORMATICIENS DE LA RÉPUBLIQUE POPULAIRE DÉMOCRATIQUE DE CORÉE

Le Département d'État américain, le Département du Trésor américain et le Federal Bureau of Investigation (FBI) émettent cette alerte de sécurité à l'intention de la communauté internationale, du secteur privé et du public afin de les mettre en garde contre les tentatives de travailleurs du secteur des technologies de l'information (TI) de la République populaire démocratique de Corée (RPDC ou la Corée du Nord) pour obtenir un emploi en se faisant passer pour des ressortissants non nord-coréens. Il existe des risques de réputation et des conséquences juridiques potentielles, y compris la désignation de sanctions en vertu des autorités des États-Unis et des Nations Unies (ONU), pour les personnes et les entités qui participent ou soutiennent les activités des travailleurs nord-coréens du secteur des technologies de l'information et qui traitent les transactions financières connexes.

La RPDC envoie des milliers d'informaticiens hautement qualifiés dans le monde entier pour générer des revenus qui contribuent à ses programmes d'armes de destruction massive (ADM) et de missiles balistiques qui vont à l'encontre des sanctions des États-Unis et de l'ONU. Ces informaticiens profitent de la demande existante de compétences informatiques spécifiques, telles que le développement de logiciels et d'applications mobiles, pour obtenir des contrats de travail en freelance auprès de clients du monde entier, notamment en Asie de l'Est, en Europe et Amérique du Nord. Dans la plupart des cas, ils se présentent comme des télétravailleurs basés aux États-Unis et/ou non nord-coréens. Ils peuvent également dissimuler leur identité et/ou leur localisation en sous-traitant des travaux à des personnes qui ne sont pas nord-coréennes. Bien que ces informaticiens de la RPDC effectuent normalement des travaux informatiques différents des activités cybernétiques malveillantes, ils ont utilisé l'accès privilégié obtenu en tant que prestataires pour autoriser les intrusions informatiques malveillantes de la Corée du Nord. De plus, il existe probablement des cas où les travailleurs sont soumis au travail forcé.

Ce document fournit des informations détaillées sur le mode opératoire des informaticiens nord-coréens, des signes avant-coureurs permettant aux entreprises qui embauchent des développeurs indépendants et aux plateformes de paiement et de travail en freelance d'identifier les informaticiens de la RPDC, ainsi que des mesures d'atténuation générales permettant aux entreprises de mieux se protéger contre l'embauche ou la facilitation des opérations de ces travailleurs. Une annexe fournit des

informations supplémentaires sur les informaticiens nord-coréens, tirées des rapports du Groupe d'experts du Comité 1718. Le FBI encourage les entreprises américaines à signaler aux bureaux locaux toute activité suspecte, y compris celles des informaticiens nord-coréens.

INFORMATICIENS DE LA RPDC : CONTEXTE

Ils constituent un flux de revenus essentiel qui contribue à financer les plus grandes priorités économiques et sécuritaires du régime de la RPDC, comme son programme de développement d'armes. Kim Jong Un, le dirigeant de la RPDC reconnaît l'importance des informaticiens comme une importante source de devises et de revenus et soutient leurs activités.

Des milliers d'informaticiens sont à la fois envoyés à l'étranger et basés en Corée du Nord, générant des revenus qui sont reversés à leur gouvernement. Ils se trouvent principalement en République populaire de Chine (RPC) et en Russie, et un nombre plus restreint en Afrique et en Asie du Sud-Est. Ils comptent généralement sur leurs contacts à l'étranger pour obtenir des emplois en freelance et établir des contacts plus directs avec les clients.

Tous les informaticiens de la RPDC gagnent de l'argent pour soutenir le régime du dirigeant nord-coréen Kim Jong Un. La grande majorité d'entre eux sont subordonnés et travaillent pour le compte des entités qui sont directement impliquées dans les programmes d'armes de destruction massive et de missiles balistiques de la RPDC, interdits par l'ONU, ainsi que dans les secteurs du développement et du commerce des armes conventionnelles avancées. Il en résulte que les revenus générés par ces travailleurs sont utilisés par la RPDC pour développer ses programmes d'armes de destruction massive et de missiles balistiques de la RPDC qui vont à l'encontre des sanctions des États-Unis et de l'ONU. Nombre de ces entités ont été désignées pour faire l'objet de sanctions par l'ONU et les États-Unis. Les entités nord-coréennes qui envoient des informaticiens sont :

- **Le 313 General Bureau of the Munitions Industry Department (MID),** qui contrôle la recherche, le développement et la production d'armes de la Corée du Nord, y compris les armes nucléaires et les missiles balistiques, et d'autres équipements militaires. Le MID est subordonné au Comité central du Parti du travail de Corée et, par l'intermédiaire du 313 General Bureau, déploie à l'étranger la majorité de la main-d'œuvre informatique de la RPDC. Tous les biens et intérêts fonciers du Parti du travail de Corée sont bloqués conformément au décret 13722.

- **Le ministère de l'Industrie de l'énergie atomique**—un acteur essentiel dans le développement des armes nucléaires de la RPDC et responsable des opérations quotidiennes du programme d'armes nucléaires. Le ministère de l'Industrie de l'énergie atomique est désigné conformément au décret 13382.

- Des entités militaires subordonnées au **Ministère de la Défense et à l'Armée populaire de Corée**. L'Armée populaire de Corée est désignée sur la liste des ressortissants spécialement désignés et des biens bloqués.

- Des entités moins connues, telles que le **Bureau du commerce extérieur de la Commission de l'éducation de la RPDC** et le **Bureau des technologies de l'information de Pyongyang du Département des sciences et de l'éducation du Comité central.** Tous les biens et intérêts fonciers du Parti du travail de Corée sont bloqués conformément au décret 13722.

Un informaticien nord-coréen à l'étranger gagne au moins dix fois plus qu'un ouvrier nord-coréen classique qui travaille dans une usine ou sur un projet de construction à l'étranger. Dans certains cas, ils peuvent gagner individuellement plus de 300 000 USD par an, et des équipes d'informaticiens peuvent gagner collectivement plus de 3 millions USD par an. Un pourcentage important de leurs revenus bruts soutient les priorités du régime de la RPDC, notamment son programme d'armes de destruction massive.

Les entreprises informatiques de la RPDC et leurs employés s'engagent normalement dans un large éventail de travaux de développement de complexité et de difficulté variables, tels que :

- des applications mobiles et des applications basées sur le Web,

- la création de plateformes d'échange de devises virtuelles et de monnaie numériques,
- l'assistance informatique générale,
- l'animation graphique,
- les logiciels de pari en ligne,
- les jeux mobiles,
- les applications de rencontre,
- les applications liées à l'intelligence artificielle,
- le développement de matériel et de micrologiciels,
- la programmation de réalité virtuelle et de réalité augmentée,
- les logiciels de reconnaissance faciale et biométrique, et
- le développement et la gestion de bases de données.

Les logiciels et les applications développés par les informaticiens nord-coréens couvrent plusieurs secteurs et domaines, notamment les affaires, la santé et le fitness, les réseaux sociaux, le sport, le divertissement et le mode de vie. Ils travaillent généralement sur des projets qui impliquent des devises virtuelles. Certains d'entre eux ont conçu des plateformes de vente et d'achat de monnaies virtuelles ou créé des outils d'analyse et des applications pour les commerçants en devises virtuelles et ont commercialisé eux-mêmes leurs produits.

Depuis des décennies, la RPDC souligne l'importance de l'enseignement des mathématiques et des sciences pour ses citoyens. L'accent qui est mis sur l'avancement de la science et de la technologie a toujours été une priorité pour le régime Kim et cela se reflète dans l'investissement de ressources et de personnel dans les domaines de recherche connexes. L'enseignement de la cybernétique et des technologies de l'information en RPDC a été fondé sur cette volonté de progrès et a donné lieu à un programme intégré coordonné avec le Parti des travailleurs, les centres de recherche et l'armée.

- Ces dernières années, sous la direction de Kim Jong Un, le régime a mis davantage l'accent sur l'éducation et la formation dans les domaines liés aux technologies de l'information et a mis en place des programmes de diplômes en technologies de l'information dans plusieurs établissements d'enseignement prestigieux de la RPDC, notamment l'Université de science et de technologie de Pyongyang, l'Université de technologie Kim Chaek et l'Université Kim Il Sung. Environ 30 000 apprenants étudient des sujets liés aux technologies de l'information et de la communication seulement dans ces meilleures universités.

- En 2019, 37 universités auraient mis en place 85 programmes qui donnent des cours dans des matières scientifiques, technologiques, d'ingénierie et de mathématiques (STIM) avancées, y compris la sécurité de l'information, et chaque province a créé au moins une nouvelle école secondaire pour favoriser les étudiants prometteurs.

- Le système éducatif nord-coréen est très compétitif et seuls les meilleurs étudiants sont acceptés dans les programmes scientifiques et technologiques d'élite. Les apprenants sont recrutés à un jeune âge dans des écoles secondaires comme la Kumsong Academy et la Kumsong Middle School Number 1.

- Les informaticiens nord-coréens suivent une formation supplémentaire à l'étranger et dans leurs propres organisations, souvent par le biais de centres de recherche régionaux afin de développer davantage leurs compétences. Autrefois, ils ont suivi une formation en Afrique de l'Est, en Asie du Sud-Est et en Asie du Sud et bénéficient considérablement de leur formation à l'étranger.

LE MODE OPÉRATOIRE DES INFORMATICIENS DE LA RPC

Ils recherchent des contrats en freelance auprès d'employeurs situés dans des pays riches, notamment en Asie de l'Est, en Europe et en Amérique du Nord. Dans de nombreux cas, ils se présentent comme des télétravailleurs sud-coréens, chinois, japonais ou d'Europe de l'Est qui sont basés aux États-Unis.

Dans certains cas, ces informaticiens dissimulent davantage leur identité en concluant des accords avec des sous-traitants tiers. Ces derniers sont des informaticiens indépendants non nord-coréens qui remplissent des contrats pour des informaticiens de la RPDC. Les responsables informatiques de la RPDC ont également engagé leurs propres équipes d’informaticiens qui ne sont pas nord-coréens et qui ignorent généralement la véritable identité de leur employeur nord-coréen ou le fait qu’il est une

entreprise de la RPDC. Ces responsables utilisent leurs employés sous-traités pour acheter des logiciels et interagir avec les clients dans des situations qui pourraient autrement exposer un informaticien nord-coréen.

Bien que ces informaticiens de la RPDC effectuent normalement des travaux informatiques non malveillants, ils ont utilisé l'accès privilégié obtenu en tant que prestataires pour autoriser les intrusions informatiques malveillantes de la Corée du Nord. Certains informaticiens nord-coréens basés à l'étranger ont fourni une assistance logistique à des pirates qui sont en RPDC, même s'il est peu probable que ces informaticiens soient eux-mêmes impliqués dans des activités cybernétiques malveillantes. Ils ont la possibilité de partager l'accès à l'infrastructure virtuelle, de faciliter la vente de données volées par les cyberacteurs de la RPDC ou de participer au blanchiment d'argent et aux transferts de monnaie virtuelle du pays.

Ils ont également aidé les responsables de leur pays à se procurer des articles liés aux armes de destruction massive et aux missiles balistiques pour les programmes d'armement interdits de la RPDC.

Dans certains cas, les travailleurs sont soumis au trafic d'êtres humains et aussi au travail forcé. Des rapports crédibles montrent que de nombreux travailleurs nord-coréens qui se trouvent à l'étranger sont soumis à des horaires de travail excessifs, à une surveillance constante et étroite par des agents de sécurité du gouvernement nord-coréen, à des conditions de vie dangereuses et insalubres et à une faible liberté de mouvement. Le gouvernement nord-coréen retient jusqu'à 90 % des salaires de ses citoyens qui travaillent à l'étranger, ce qui génère un revenu annuel de plusieurs centaines de millions de dollars pour le gouvernement.

Informaticiens de la RPDC : compétences et plateformes

Le plus souvent, les équipes informatiques de la RPDC qui se trouvent à l'étranger obtiennent des emplois en freelance par le biais de diverses plateformes en ligne. Les entreprises utilisent ces plateformes pour publier des offres de projets auxquelles les développeurs informatiques indépendants peuvent postuler. Plus rarement, les équipes informatiques de la RPDC trouvent des ressortissants locaux, non originaires de la RPDC, et les placent à la tête d'entreprises qui sont en réalité contrôlées par des Nord-Coréens. Il est également arrivé que ces équipes semblent, sur le papier, travailler pour une entreprise locale légitime, mais poursuivent leur propre activité de manière indépendante - et en échange de la dissimulation de leurs origines nord-coréennes, l'équipe informatique de la RPDC verse des honoraires à l'entreprise étrangère. Généralement, les membres de ces équipes maîtrisent une langue étrangère, comme le chinois ou l'anglais.

Les informaticiens de la RPDC s'inscrivent sur plusieurs sites de travail en freelance, d'outils et des plateformes de développement de logiciels, d'applications de messagerie et des sites de réseautage et de réseaux sociaux afin d'obtenir des contrats de développement pour des entreprises du monde entier, ainsi que sur un certain nombre de plateformes et de sites de paiement en ligne pour être payés pour leur travail. Ils utilisent également des plateformes de trading et des sites d'achat et de vente de

monnaies virtuelles pour gérer les paiements en ligne qu'ils reçoivent en échange de contrats, ainsi que pour blanchir et déplacer les fonds qu'ils reçoivent.

Informaticiens de la RPDC : cacher leur identité

Ils dissimulent délibérément leur identité, leur localisation et leur nationalité en ligne, en utilisant souvent des noms non coréens comme pseudonymes. Ils utilisent également des réseaux privés virtuels (VPN), des serveurs privés virtuels (VPS) ou des adresses IP de pays tiers pour donner l'impression qu'ils se connectent à Internet à partir d'endroits discrets et réduire la probabilité d'une recherche approfondie de leur localisation ou de leurs relations avec la RPDC. Les informaticiens de la RPDC comptent généralement sur l'anonymat des accords de télétravail, utilisent des proxies pour la création et la maintenance des comptes, et privilégient l'utilisation d'intermédiaires et les communications par écrit plutôt que par appels vidéo.

Ils font également usage des comptes proxy pour soumissionner, gagner, travailler et être payés pour des projets sur des sites de développeurs de logiciels indépendants. Ces comptes appartiennent à des personnes tierces, dont certaines vendent leurs informations d'identification et de compte aux informaticiens de la RPDC. Dans certains cas, ils paient ces personnes afin d'utiliser leurs comptes officiels sur la plateforme. Les informaticiens de la RPDC peuvent remplir les profils des plateformes de freelance avec les affiliations et l'expérience professionnelle réelles du mandataire.

Parfois, ils contactent d'autres travailleurs indépendants non nord-coréens via les plateformes pour leur proposer une collaboration sur des projets de développement. Un informaticien de la RPDC profite de ces relations d'affaires pour obtenir de nouveaux contrats et comptes de monnaie virtuelle utilisés pour effectuer le travail informatique sur une infrastructure virtuelle américaine ou européenne, en contournant les mesures de sécurité destinées à empêcher toute utilisation frauduleuse. En créant des comptes avec l'aide d'autres travailleurs indépendants, les informaticiens de la RPDC peuvent prétendre être des ressortissants de pays tiers qui ont besoin de documents d'identité américains ou occidentaux et de comptes sur des plateformes indépendantes pour gagner plus d'argent.

Le fait de masquer leur véritable localisation leur permet de violer les conditions d'utilisation des plateformes et services en ligne qu'ils utilisent pour leurs activités. Dans le cadre de leurs activités, les informaticiens de la RPDC peuvent également utiliser des appareils uniques et dédiés pour chacun de leurs comptes, notamment pour les services bancaires, afin d'éviter d'être détectés par les mesures de prévention de la fraude, de respect des sanctions et de lutte contre le blanchiment d'argent.

Les informaticiens de la RPDC utilisent régulièrement des documents contrefaits, altérés ou falsifiés, y compris des documents d'identité et des signatures contrefaites, qu'ils ont eux-mêmes créés à l'aide de logiciels tels que Photoshop ou qu'ils ont payé une entreprise de falsification de documents pour qu'elle les modifie, en combinant la photo du travailleur ou une photo fournie avec les informations d'identification d'une personne réelle. Habituellement, ils se procurent de faux documents tels que :

- des permis de conduire,
- des cartes de sécurité sociale,
- des passeports,
- des cartes d'identité nationales,
- des cartes de résident étranger,
- des diplômes d'études secondaires et universitaires,
- des visas de travail, et
- des relevés de cartes de crédit, de comptes bancaires et de services publics.

Dans certains cas, ces pièces d'identité sont volées, tandis que dans d'autres, les informaticiens ont demandé à un ressortissant non nord-coréen d'ouvrir un compte en utilisant ses propres informations personnelles ou des informations auxquelles il a accès, après quoi le contrôle du compte est transféré aux informaticiens de la RPDC contre une forte rémunération. Cela permet à l'informaticien de dissimuler son identité lorsqu'il soumissionne et réalise des projets indépendants pour des clients en ligne, en utilisant l'infrastructure du véritable titulaire du compte via un accès à distance à l'ordinateur. Chaque informaticien utilise souvent plusieurs identités et comptes, qui peuvent également être partagés entre les informaticiens d'une même équipe. Ces comptes et identités sont censés provenir de pays du monde entier.

Les informaticiens de la RPDC peuvent voler les informations de comptes clients des banques américaines ou internationales pour vérifier leur identité auprès des plateformes de freelance, des fournisseurs de paiement et des entreprises qui emploient les informaticiens nord-coréens. Dans au moins un cas, ces informaticiens ont falsifié des chèques en utilisant des informations de compte bancaire volées. Les comptes et les CV associés aux identités de substitution des informaticiens de la RPDC contiennent souvent des informations falsifiées, mais réalistes et détaillées, sur les études et l'emploi, y compris de fausses coordonnées d'établissements d'enseignement et d'employeurs précédents.

Ils peuvent également remplir les sections d'emploi de leurs profils de développeurs en ligne avec des noms de petites ou moyennes entreprises occidentales pour paraître comme des Européens ou des Américains de bonne réputation lorsqu'ils postulent pour des projets. Ils ont la possibilité d'utiliser les noms de réels employés et des adresses électroniques qui semblent similaires au domaine légitime de l'entreprise occidentale.

Les informaticiens de la RPDC falsifient également des contrats de travail, des factures, des documents de communication avec les clients et d'autres documents destinés à être utilisés sur des plateformes de freelancing, probablement pour répondre aux exigences des mesures de connaissance du client et de lutte contre le blanchiment d'argent (KYC/AML) ou des procédures similaires mises en place par les

plateformes pour garantir la légitimité de l'activité des utilisateurs. Ces documents falsifiés peuvent comporter un minimum de coordonnées de contact afin d'éviter toute vérification.

Les informaticiens de la RPDC peuvent également tenter de masquer leur nationalité en se présentant comme des citoyens sud-coréens ou simplement « coréens ».

Ceux qui obtiennent des postes en freelance auprès d'une entreprise non avertie sont également connus pour recommander à l'entreprise d'employer d'autres informaticiens de la RPDC qui travaillent en freelance.

Curriculum vitae d'un informaticien nord-coréen

Les informaticiens de la RPDC affichent des compétences en matière de développement de systèmes et de logiciels, de systèmes de gestion de bases de données et d'utilisation d'une grande variété de langages, de cadres, d'outils et de ressources sur un cloud. Il s'agit souvent de compétences solides dans un certain nombre de langages de codage et de balisage. La plupart d'eux exercent dans le domaine du développement d'applications mobiles et web. Ils utilisent également des plateformes collaboratives et des services d'hébergement pour gérer les flux de travail et les données. Ces travailleurs déclarent souvent avoir de l'expérience avec plusieurs bases de données et sont familiers avec le cloud et les produits et services d'analyse des principaux fournisseurs. Ils mentionnent également sur leur CV des compétences de développement de plateformes de paiement numérique et de vente en ligne.

Les informaticiens de la RPDC créent des sites « portfolio », dont la conception est généralement simple, afin d'accroître la crédibilité de leur personnage de développeur indépendant. Ces portfolios virtuels représentent le travail des informaticiens de la RPDC et sont souvent liés à leur compte de développeur indépendant en ligne. Les informations qui figurent sur ces sites Internet, notamment les coordonnées et la localisation, ainsi que l'historique de travail et la formation, sont probablement fausses.

LES INDICATEURS D'ALERTE

Les entreprises de travail indépendant et les plateformes de paiement doivent être conscientes de ces activités qui peuvent être des indices ou des comportements d'informaticiens nord-coréens qui pourraient utiliser leurs plateformes.

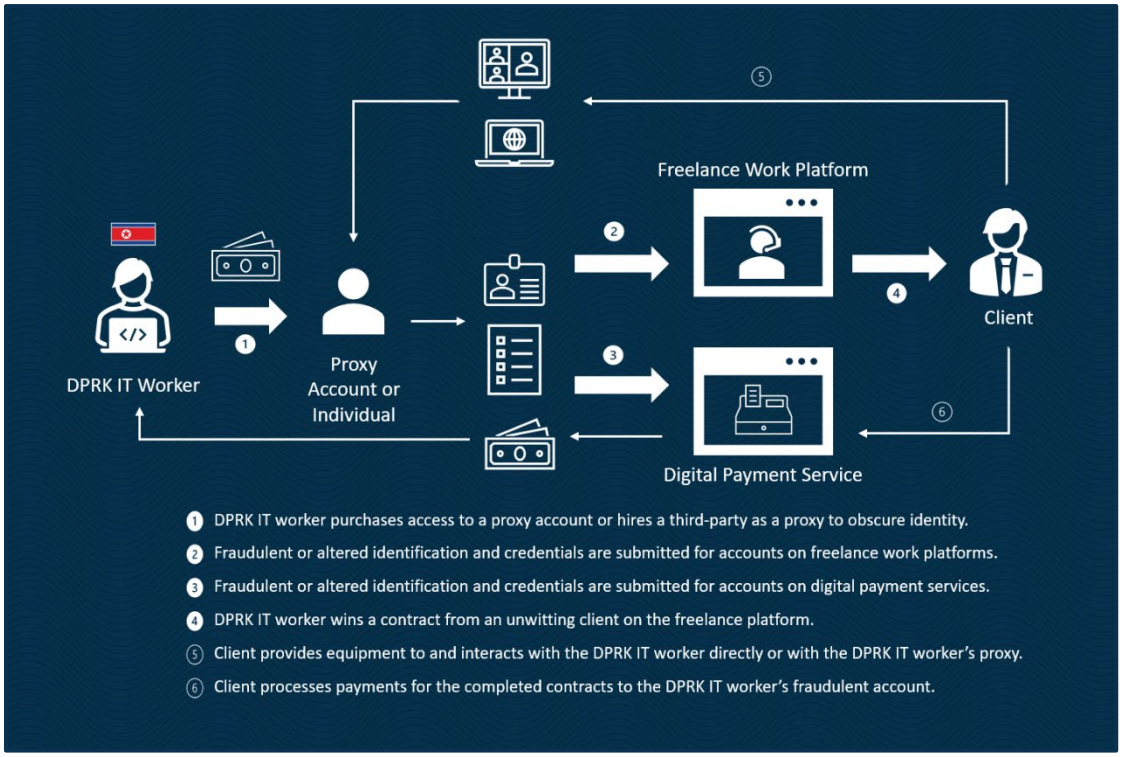
- Plusieurs connexions à un compte à partir de diverses adresses IP dans un laps de temps relativement court, surtout si les adresses IP sont associées à différents pays ;
- Les développeurs se connectent à plusieurs comptes sur la même plateforme à partir d'une seule adresse IP ;
- Ils se connectent à leurs comptes de manière continue pendant un ou plusieurs jours ;
- Port du routeur ou autres configurations techniques associées à l'utilisation d'un logiciel de partage à distance, comme le port 3389 du routeur utilisé pour accéder au compte, en particulier si l'utilisation d'un logiciel de partage à distance n'est pas une pratique standard de l'entreprise ;
- Les développeurs utilisent un compte client frauduleux pour augmenter la note du compte de développeur, mais les comptes client et développeur utilisent tous deux le même compte PayPal pour les transferts et les retraits d'argent (se payant avec leur propre argent) ;
- Utilisation fréquente de modèles de documents pour des éléments tels que les documents d'appel d'offres et les méthodes de communication du projet, notamment les mêmes modèles utilisés sur différents comptes de développeurs ;
- Plusieurs comptes de développeurs recevant des notes élevées de la part d'un compte client sur une courte période, avec une documentation similaire ou identique utilisée pour créer les comptes de développeurs et/ou le compte client ;
- Des appels d'offres intensifs pour des projets et un faible nombre d'offres acceptées par rapport au nombre de projets pour lesquels un développeur a postulé ; et
- Des transferts d'argent fréquents par le biais de plateformes de paiement, en particulier vers des comptes bancaires basés en Chine, et parfois acheminés par une ou plusieurs sociétés afin de dissimuler la destination finale des fonds.

Les entreprises qui emploient des développeurs indépendants doivent être conscientes de ces activités qui peuvent être des indices ou des modes opératoires d'informaticiens nord-coréens.

- Fermeture d'un site de développement de logiciels freelance ou d'un compte sur une plateforme de paiement ou si le travailleur contacte l'employeur pour demander l'utilisation d'un autre compte, surtout s'il est enregistré sous un autre nom ;

- Utilisation de services de paiement en ligne, surtout des services liés à la Chine ;
- Des incohérences dans l'orthographe du nom, la nationalité, le lieu de travail déclaré, les coordonnées, le niveau d'études, les expériences professionnelles et d'autres détails sur les profils d'un développeur sur une plateforme de travail en freelance, sur les réseaux sociaux, les sites Internet de portefeuille externes, les plateformes de paiement et les lieux et heures d'évaluation ;
- Des sites web de portfolio, des profils sur les réseaux sociaux ou des profils de développeurs d'une simplicité surprenante ;
- Des messages directs ou des démarchages téléphoniques de la part de personnes prétendant être des cadres de niveau C de sociétés de développement de logiciels pour solliciter des services ou faire de la publicité pour des compétences ;
- Des demandes de communication avec des clients et des clients potentiels sur un site autre que la plateforme de freelance d'origine sur laquelle le client a trouvé l'informaticien ;
- Un employeur propose d'envoyer des documents ou des équipements liés au travail, comme un ordinateur portable, à un développeur, et ce dernier demande que les articles soient envoyés à une adresse qui ne figure pas sur ses documents d'identification. Méfiez-vous surtout si un développeur dit qu'il ne peut pas recevoir d'articles à l'adresse qui figure sur ses documents d'identification ;
- Demander un paiement en monnaie virtuelle dans le but d'échapper aux mesures KYC/AML et à l'utilisation du système financier formel ;
- Demander le paiement de contrats sans respecter les critères de production ou les réunions de contrôle ;
- Incapacité à mener des activités pendant les heures de travail requises ;
- Des coordonnées incorrectes ou modifiées, notamment les numéros de téléphone et les adresses électroniques ;
- Des informations biographiques qui ne semblent pas correspondre au candidat ;
- L'incapacité d'accomplir les tâches en temps voulu ou de répondre aux tâches ;
- L'impossibilité de les joindre en temps voulu, notamment par des méthodes de communication « instantanée » ; et
- Demander à des collègues de travail d'emprunter certaines de leurs informations personnelles pour obtenir d'autres contrats.

Aperçu des activités des informaticiens nord-coréens



LES POTENTIELLES MESURES D'ATTÉNUATION

Pour les plateformes de travail en freelance et de paiement

- Vérifiez les documents soumis dans le cadre de l'examen des propositions et des procédures de diligence raisonnable en matière de contrats, par exemple en vérifiant de manière indépendante les factures et les contrats de travail en contactant les clients répertoriés à l'aide des coordonnées indiquées dans les bases de données des entreprises et non des coordonnées fournies dans les documents soumis ;

- Passez au crible les documents de vérification de l'identité soumis pour voir s'ils sont falsifiés, en sollicitant éventuellement l'aide des forces de l'ordre locales. Rejetez les images de mauvaise qualité envoyées dans le cadre de la vérification de l'identité ;

- Vérifiez l'existence de tous les sites Internet fournis pour créer les comptes ; renforcez le contrôle de tous les comptes qui ont utilisé des sites web révolus pour créer les comptes.

- Dans le cadre des processus contractuels initiaux de diligence raisonnable et des politiques de rafraîchissement, exigez la soumission d'une vidéo de vérification de l'identité ou passer un entretien vidéo pour vérifier l'identité ;

- Utilisez régulièrement les fonctions de vérification des ports pour voir si quelqu'un a accédé à la plateforme à distance via un logiciel de partage ou un VPN ou VPS, surtout si l'utilisation d'un logiciel de partage à distance ou de services VPN pour accéder aux comptes n'est pas une pratique courante ;

- Signalez automatiquement pour une évaluation supplémentaire les comptes de clients et de développeurs qui utilisent la même documentation ou une documentation similaire pour créer des comptes ou qui utilisent les mêmes comptes de services de paiement numérique ;

- Signalez automatiquement, en vue d'un examen supplémentaire, l'utilisation de modèles de documents identiques ou similaires pour la communication des appels d'offres et des projets sur différents comptes de développeurs ;

- Signalez automatiquement, en vue d'un examen supplémentaire, les comptes de développeurs multiples recevant des notes élevées d'un seul compte client sur une courte période, en particulier si une documentation similaire ou identique a été utilisée pour créer les comptes ;

- Signalez automatiquement pour examen supplémentaire les comptes de développeurs ayant des taux de soumission élevés ainsi que les comptes ayant un faible nombre d'offres de projets acceptées par rapport au nombre d'offres de projets. Signalez également les comptes qui ont un nombre élevé d'offres de projets par rapport au nombre de connexions au compte ;

- N'autorisez aucune activité sur les comptes nouvellement créés avant la vérification complète du compte ;

- Accordez une attention particulière aux comptes nouvellement créés ; et

Pour les entreprises qui recrutent des programmeurs et des développeurs sur des plateformes de freelance

- Passez un entretien vidéo pour vérifier l'identité d'un potentiel travailleur indépendant ;

- Procédez à une vérification des antécédents avant l'embauche, à un test de dépistage de drogues et à une connexion par empreinte digitale/biométrique pour vérifier l'identité et le lieu déclaré. Évitez les paiements en monnaie virtuelle et exigez la vérification des informations bancaires correspondant à d'autres documents d'identification ;

- Soyez très prudent lorsque vous interagissez avec des développeurs indépendants par le biais d'applications de collaboration à distance, telles que les applications de bureau à distance. Pensez à désactiver les applications de collaboration à distance sur tout ordinateur fourni à un développeur indépendant ;

- Vérifiez les antécédents d'emploi et d'études supérieures directement auprès des entreprises et des établissements d'enseignement répertoriés, en utilisant les coordonnées identifiées via un moteur de recherche ou une autre base de données commerciale, et non obtenues directement de l'employé potentiel ou de son profil ;

- Vérifiez que l'orthographe du nom, la nationalité, l'emplacement déclaré, les coordonnées, le cursus scolaire, les expériences professionnelles et d'autres détails d'une embauche potentielle sont cohérents entre les profils du développeur sur la plateforme de freelance, sur les réseaux sociaux, les sites Internet de portefeuille externes, la plateforme de paiement et avec le lieu ainsi que les heures de travail évalués. Faites preuve d'une grande prudence à l'égard des sites portfolio, des profils sur les réseaux sociaux ou des profils de développeurs simples ;

- Méfiez-vous d'un développeur qui demande à communiquer sur une autre plateforme en dehors du site de freelance d'origine où l'entreprise a initialement trouvé l'informaticien ;

- Si vous envoyez à un développeur des documents ou des équipements liés au travail, tels qu'un ordinateur portable, envoyez-les uniquement à l'adresse qui figure sur les documents d'identification du développeur et demandez des documents supplémentaires si le développeur demande que l'ordinateur portable ou d'autres articles soient envoyés à une adresse inconnue. Méfiez-vous si un développeur est incapable de recevoir des articles à l'adresse qui figure sur ses documents d'identification.

- Faites preuve de vigilance quant aux petites transactions non autorisées qui peuvent être effectuées frauduleusement par des informaticiens sous contrat. À une occasion, des informaticiens nord-coréens, employés comme développeurs par une société américaine, ont frauduleusement débité le compte de l'entreprise et ont volé plus de 50 000 USD en 30 petits versements sur quelques mois. L'entreprise ne savait pas que les développeurs étaient nord-coréens ni de l'activité de vol en cours en raison des faibles montants.

CONSÉQUENCES DE L'ADOPTION D'UN COMPORTEMENT INTERDIT OU PASSIBLE DE SANCTIONS

Les entités et les personnes qui soutiennent ou prennent part à des activités liées aux informaticiens de la RPDC, y compris le traitement des transactions financières connexes, doivent prendre connaissance des potentielles conséquences juridiques d'un comportement interdit ou répréhensibles.

Les résolutions 2321, 2371 et 2397 du Conseil de sécurité des Nations Unies soulignent que les revenus générés par les travailleurs étrangers de la RPDC contribuent aux programmes d'armes nucléaires et de missiles balistiques de la Corée du Nord. La résolution 2375 du Conseil de sécurité des Nations Unies interdit à ses États membres de fournir de nouvelles autorisations de travail, ou de renouveler des autorisations expirées, pour les ressortissants de la RPDC qui se trouvent dans leur pays dans le cadre de l'entrée sur leur territoire, à moins d'une approbation préalable du Comité 1718 du

Conseil de sécurité de l'ONU. La résolution 2397 du Conseil de sécurité de l'ONU exige que tous les États membres rapatrient, d'ici le 22 décembre 2019, les ressortissants nord-coréens qui gagnent un revenu dans leur juridiction, peu importe le moment où les autorisations de travail ont été délivrées pour ces ressortissants en question.

L'Office of Foreign Assets Control (OFAC) du département du Trésor a le pouvoir d'imposer des sanctions financières à toute personne déterminée qui, entre autres :

- s’est engagée dans des activités importantes au nom du gouvernement nord-coréen ou du Parti des travailleurs de Corée qui nuisent à la cybersécurité ;
- opère pour le compte de la RPDC dans le secteur des technologies de l'information ;
- s'est engagée dans certaines autres activités malveillantes liées à la cybernétique ;
- s'est engagée dans au moins une importation ou exportation importante de biens, de services ou de technologies en provenance ou à destination de la RPDC ;
- a vendu, fourni, transféré ou acheté, directement ou indirectement, à la Corée du Nord ou à toute personne agissant pour ou au nom du gouvernement de la RPDC ou du Parti du travail de Corée, des logiciels, pourvu que les biens reçus ou les revenus puissent bénéficier le gouvernement ou le Parti ; ou
- a apporté une aide matérielle, un parrainage ou un soutien financier, matériel ou technologique au gouvernement de la RPDC ou au Parti des travailleurs de Corée, ou qui a fourni des biens ou des services à ces derniers ou en leur faveur.

Par exemple, en 2018, les États-Unis ont inscrit la société technologique Yanbian Silverstar Network Technology Co, Ltd, basée en Chine sur la liste des entités visées par des sanctions. En principe, cette société était une entreprise informatique chinoise, mais en réalité elle était gérée et contrôlée par des Nord-Coréens. Elle a également créé une société écran basée en Russie, Volasys Silver Star, afin de contourner les exigences d'identification sur les plateformes d'emploi en freelance.

Par ailleurs, si le secrétaire au Trésor, en consultation avec le secrétaire d'État, détermine qu'une institution financière étrangère a sciemment mené ou facilité un commerce important avec la RPDC, ou a sciemment mené ou facilité une transaction importante au nom d'une personne désignée en vertu d'un décret relatif à la RPDC, ou en vertu du décret 13382 pour une activité liée à la Corée du Nord, cette institution peut, entre autres restrictions potentielles, perdre la possibilité d’avoir un compte de correspondants ou un compte de passage aux États-Unis.

L'OFAC enquête sur les violations apparentes de ses règlements sur les sanctions et exerce son autorité de mise en application, comme indiqué dans les Economic Sanctions Enforcement Guidelines, 31 C.F.R. part 501, Annexe A. Ceux qui enfreignent les règles sur les sanctions à l'encontre de la Corée du

Nord, 31 C.F.R. part 510, peuvent se voir infliger des sanctions pécuniaires civiles pouvant aller jusqu'au plus élevé des montants prévus par la loi ou deux fois la valeur de la transaction sous-jacente.

Par ailleurs, la section 321(b) (article 9241a du 22 U.S.C.) du Countering America's Adversaries Through Sanctions Act (CAATSA ; Public Law 115-44), qui a modifié le North Korea Sanctions and Policy Enhancement Act de 2016 (article 9241 et seq. du 22 U.S.C.), a créé une présomption réfutable selon laquelle les biens, les marchandises et les articles importants extraits, produits ou fabriqués en totalité ou en partie par des ressortissants nord-coréens ou des citoyens nord-coréens partout dans le monde sont des marchandises de travail forcé interdites à l'importation en vertu de la loi de 1930 sur les droits de douane à l'importation (article 1301 du 19 U.S.C). Cela signifie que ces marchandises n'ont pas le droit d'entrer dans un quelconque port des États-Unis et qu'elles peuvent faire l'objet d'une détention, d'une saisie et d'une confiscation. Les violations peuvent entraîner des sanctions civiles, ainsi que des poursuites pénales. Toutefois, en vertu de la CAATSA, ces marchandises peuvent être importées aux États-Unis si le commissaire du service des douanes et de la protection des frontières des États-Unis estime, sur la base de preuves claires et convaincantes, qu'elles n'ont pas été produites par du travail de détenus, du travail forcé ou du travail sous contrat. L'interdiction d'importer des marchandises produites par des détenus, du travail forcé ou du travail sous contrat dans le cadre de sanctions pénales (y compris le travail forcé ou sous contrat des enfants) a été créée par la loi Hawley-Smoot et est donc en vigueur depuis près de 90 ans.

Le ministère de la Justice est responsable des enquêtes et des poursuites relatives aux lois fédérales applicables, notamment l'International Emergency Economic Powers Act ("IEEPA"), articles 1701 et seq. du 50 U.S.C., et la Bank Secrecy Act (BSA), articles 518 et 5322 du 31 U.S.C. En vertu de l'IEEPA, c'est un crime de violer délibérément, de tenter de violer, de conspirer pour violer ou de provoquer la violation de toute licence, ordre, règlement ou interdiction émis conformément l'IEEPA, y compris tout décret lié à la RPDC (par exemple, les décrets 13722 et 13810), le décret 13382 et les règlements sur les sanctions contre la Corée du Nord, 31 C.F.R. partie 510. Les personnes qui violent délibérément l'IEEPA risquent jusqu'à 20 ans d'emprisonnement, des amendes allant jusqu'à 1 million de dollars ou totalisant deux fois le gain brut, selon le montant le plus élevé, et la confiscation potentielle de tous les fonds impliqués dans ces transactions. La BSA exige que les institutions financières, entre autres, mettent en place des programmes efficaces de lutte contre le blanchiment d'argent et déposent certains rapports auprès du Financial Crimes Enforcement Network. Ceux qui enfreignent la BSA sont passibles d'une peine d'emprisonnement pouvant aller jusqu'à 5 ans, d'une amende pouvant atteindre 250 000 dollars et d’une confiscation potentielle des biens impliqués dans ces infractions. Les sociétés et autres entités qui violent l'IEEPA, la BSA et d'autres lois fédérales applicables peuvent également faire l'objet de poursuites pénales. Le ministère de la Justice travaille également avec des partenaires étrangers pour partager des preuves pour soutenir les enquêtes et les poursuites pénales aux États-Unis et à l'étranger.

En vertu de l'article 5318(k) du 31 U.S.C., le secrétaire au Trésor ou le procureur Général peut convoquer et amener une institution financière étrangère qui tient un compte de correspondant bancaire aux États-Unis à fournir des documents conservés à l'étranger. Lorsque le Secrétaire au Trésor

ou le procureur Général notifie par écrit à une institution financière américaine qu'une institution financière étrangère ne s'est pas conformée à une telle assignation, l'institution financière américaine doit mettre fin à la relation de correspondant bancaire dans les dix jours ouvrables. Le non-respect à cette obligation peut exposer les institutions financières américaines à des pénalités civiles quotidiennes.

LE PROGRAMME « REWARDS FOR JUSTICE » EN FAVEUR DE LA RPDC

Si vous disposez d'informations sur les activités illicites de la RPDC dans le cyberespace, y compris les opérations antérieures ou en cours, vous pourriez être éligible pour recevoir une récompense allant jusqu'à 5 millions de dollars en fournissant ces informations par le biais du programme Rewards for Justice du Département d'État. Pour plus de détails, veuillez consulter le site https://rewardsforjustice.net/index/?north-korea=north-korea.

ANNEXE

Rapport du groupe d'experts des Nations Unies sur les informaticiens nord-coréens

Le Comité des sanctions 1718 du Conseil de sécurité des Nations Unies contre la RPDC est soutenu par un groupe d'experts qui recueille, examine et analyse les informations fournies par les États membres de l'ONU, les organes compétents de l'ONU et d'autres parties sur la mise en œuvre des mesures décrites dans les résolutions du Conseil de sécurité des Nations Unies concernant la Corée du Nord. Le groupe fait également des recommandations sur la manière d'améliorer la mise en œuvre des sanctions en fournissant un rapport à mi-mandat et un rapport final au Comité 1718. Ces rapports peuvent être consultés à l'adresse suivante :
https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports

Le groupe a enquêté sur de multiples cas d'informaticiens nord-coréens, tels que ceux subordonnés au Munitions Industry Department (MID) désigné par l'ONU, et a présenté des informations sur ces enquêtes dans ses rapports semestriels, notamment les suivants :

Le groupe d'experts a d'abord fait état des informaticiens de la RPDC dans son rapport à mi-mandat de 2019, tout en mentionnant que le MID, qui avait été désigné pour son rôle de supervision dans le développement des programmes nucléaires et de missiles balistiques de la RPDC, utilisait ses sociétés commerciales subordonnées pour déployer à l'étranger des travailleurs nord-coréens, tels que des programmeurs et des développeurs de logiciels, afin de gagner des devises étrangères. À l'époque, ces informaticiens qui se trouvent en Europe, en Asie, en Afrique et au Moyen-Orient utilisaient des sites Internet étrangers pour obtenir des emplois en freelance tout en dissimulant leur identité. Parallèlement aux travaux informatiques non malveillants, ils effectuaient des travaux illicites impliquant le vol d'actifs tels que des monnaies virtuelles pour aider les cyberacteurs de la RPDC à contourner les sanctions financières.

Le groupe a poursuivi son enquête sur les informaticiens nord-coréens dans son rapport final de 2020, et a constaté que la plupart d'eux qui sont à l'étranger sont employés par des sociétés soumises au MID. En 2019, le MID était soupçonné d'avoir envoyé au moins 1 000 informaticiens à l'étranger dans le but de générer des revenus, par le biais d'entités subordonnées ou de sociétés écrans. Cependant, en raison de leurs techniques d'obscurcissement, le nombre réel d'informaticiens qui se trouvent à l'étranger et en RPDC n'est pas connu. Le groupe d'experts a constaté que les informaticiens nord-coréens utilisent plusieurs méthodes pour obtenir du travail en freelance sans révéler leur identité, notamment en créant des comptes sur des plateformes de développeurs indépendants avec des clients involontaires dans le monde entier, surtout aux États-Unis, au Canada, en Serbie, en Ukraine, en Russie et en Chine. Le groupe a également enquêté sur plusieurs cas spécifiques d'équipes d'informaticiens de la RPDC et de sociétés associées au Vietnam, au Népal et en Chine.

Il a également enquêté sur un certain nombre d'équipes d'informaticiens nord-coréens en Russie et en Chine, et a présenté les détails de ses enquêtes dans son rapport de mi-mandat de 2020. Le groupe

d'experts a constaté que des centaines d'informaticiens de la RPDC subordonnés au MID opéraient en Chine en 2019 et 2020, en accédant de façon illicite à des comptes de plateformes de freelance au nom de personnes physiques vivant des les pays tiers. Le groupe a également remarqué que plusieurs groupes d'informaticiens de la RPDC subordonnés au MID opéraient en Russie en 2019 et 2020, en utilisant de fausses identités étrangères pour accéder à des plateformes de freelance qui proposent des travaux en TIC, à des sites de monnaie virtuelle et de paiement.

Selon le rapport final de 2021 du groupe d'experts, les travailleurs en TIC de la RPDC peuvent échapper aux mesures de diligence raisonnable des employeurs et aux protocoles KYC/AML en utilisant des méthodes d'obscurcissement similaires à celles utilisées par la Corée du Nord pour accéder au système financier international, notamment en fournissant de fausses identités, en utilisant des VPN et en créant des sociétés écrans. Le groupe a également constaté que la plupart des comptes liés à la RPDC opèrent depuis des sites en Chine. Pour éviter un examen minutieux, ces comptes se désactivent après que ces travailleurs ont établi le contact avec des clients potentiels qui cherchent à louer des services informatiques. Les utilisateurs liés à la RPDC ciblent également les plateformes de freelance en TIC dont le niveau de sécurité est faible ou dont les procédures de vigilance sont moins rigoureuses. Le groupe d'experts a spécifiquement souligné les dangers auxquels sont confrontées les plateformes informatiques indépendantes dans l'exécution des obligations de conformité et la facilitation involontaire de l'accès de la RPDC aux systèmes de paiement internationaux, recommandant aux États membres de l'ONU de travailler avec les entreprises informatiques indépendantes afin de promouvoir et d'améliorer la capacité de mise en œuvre du respect des sanctions.