FICHE D'INFORMATIONS :

INSTRUCTIONS CONCERNANT LES INFORMATICIENS DE LA RÉPUBLIQUE POPULAIRE DÉMOCRATIQUE DE CORÉE

16 mai 2022

Le gouvernement américain publie ces **instructions** en tant que ressource complète pour la communauté internationale, le secteur privé et le public afin de mieux comprendre et de se prémunir contre le recrutement, l'embauche et la facilitation par inadvertance de travailleurs du domaine des technologies de l'information (TI) de la République populaire démocratique de Corée (RPDC également connu sous le nom de Corée du Nord). Ce document fournit des informations détaillées sur le mode de fonctionnement des informaticiens de la RPDC et identifie les indices ainsi que les mesures de vigilance appropriées pour aider les entreprises à ne pas embaucher des développeurs indépendants de la RPDC et pour aider les indépendants et les plateformes de paiement numérique à identifier les informaticiens nord coréens qui abusent de leurs services. Le fait de les embaucher ou de soutenir leurs activités présente de nombreux risques, allant du vol de propriété intellectuelle, de données et de fonds à l'atteinte à la réputation et aux conséquences juridiques, y compris les sanctions imposées par les autorités des États-Unis et des Nations unies (ONU).

La RPDC a envoyé des milliers d'informaticiens hautement qualifiés dans le monde entier, ce qui lui procure des revenus qui contribuent à ses programmes d'armement qui violent les sanctions des États-Unis et de l'ONU. Ces travailleurs :

- utilisent de façon malveillante les plateformes de travail en freelance pour obtenir subrepticement des contrats de développement informatique auprès d'entreprises clientes du monde entier - et font une mauvaise utilisation de plusieurs réseaux sociaux - pour communiquer avec les clients et les plateformes de paiement afin de recevoir le paiement de leur travail ;
- développent des applications et des logiciels qui couvrent plusieurs secteurs, y compris, mais sans s'y limiter, les affaires, les crypto-monnaies, la santé et le fitness, les réseaux sociaux, les sports, le divertissement et le style de vie ;
- se présentent dans la plupart des cas sous une fausse identité comme des télétravailleurs étrangers (non nord-coréens) ou basés aux États-Unis, en utilisant surtout des réseaux privés virtuels (VPN), des serveurs privés virtuels (VPS), des adresses IP achetées dans des pays tiers, des comptes proxy et des documents d'identification falsifiés ou volés ; et
- utilisent l'accès privilégié obtenu en tant que prestataire à des fins illicites pour permettre des cyberintrusions malveillantes par d'autres acteurs de la RPDC.

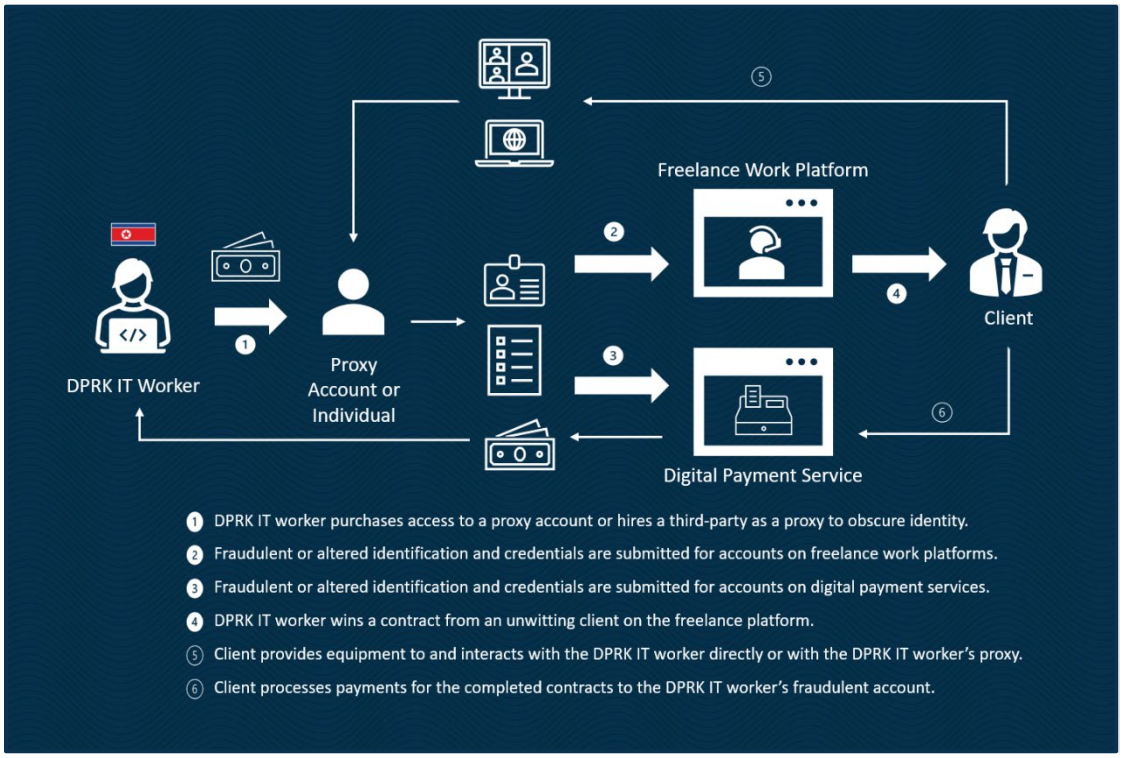
Voici quelques indicateurs d'alerte d'une activité potentielle d'un informaticien de la RPDC :

- 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 ;
- des transferts fréquents d'argent par le biais de plateformes de paiement, notamment vers des comptes bancaires basés en République populaire de Chine (RPC), ou des demandes de paiement en crypto-monnaie ;
- 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 ; et
- l'impossibilité de mener des activités pendant les heures de travail requises et l'impossibilité de joindre le travailleur en temps voulu, notamment par des méthodes de communication « instantanée ».

Les mesures de vigilance appropriées que le secteur privé peut envisager pour empêcher l'embauche involontaire ou par inadvertance d'informaticiens nord-coréens sont :

- vérifier les documents envoyés dans le cadre de l'évaluation des propositions ou des demandes d'emploi directement auprès des entreprises et des établissements d'enseignement répertoriés (sans utiliser les coordonnées fournies dans les documents soumis) ;
- passer soigneusement au crible les documents de vérification de l'identité soumis pour vérifier s'ils sont faux ;
- passer un entretien vidéo pour vérifier l'identité d'un potentiel travailleur indépendant ;
- effectuer une vérification des antécédents avant l'embauche et/ou une connexion par empreinte digitale ou biométrique pour vérifier l'identité et le lieu de travail déclaré ;
- éviter les paiements en crypto-monnaie et exiger la vérification des informations bancaires correspondant à d'autres documents d'identification ;
- vérifier 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, les profils sur les réseaux sociaux, les sites Internet de portefeuille externes, les comptes sur la plateforme de paiement et le lieu ainsi que les heures de travail évalués ; et
- se méfier si un développeur est incapable de recevoir des articles à l'adresse indiquée sur ses documents d'identification.

Aperçu des activités des informaticiens nord-coréens



Pour plus d'informations, consultez le ***DPRK Cyber Advisory****, visitez le* ***Treasury resource center****, et/ou contactez le* ***bureau du FBI de votre localité****. 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.*