FOLHA INFORMATIVA:

DOCUMENTO INFORMATIVO DA REPÚBLICA POPULAR DEMOCRÁTICA DA COREIA SOBRE OS TRABALHADORES DE TECNOLOGIA DA INFORMAÇÃO

16 de maio de 2022

O Governo dos EUA emite este **documento informativo** como um recurso pormenorizado para a comunidade internacional, setores privado e público, para que haja melhor entendimento e vigilância contra o recrutamento, contratação e facilitação inadvertidos dos trabalhadores da área de Tecnologia da Informação (TI) da República Popular Democrática da Coreia (RPDC, mais comummente designada Coreia do Norte). Este documento informativo apresenta informações detalhadas sobre como os trabalhadores da RPDC operam e identificam indicadores de alerta e medidas de devida diligência para ajudar as empresas a evitar a contratação de programadores freelancers da RPDC e para ajudar plataformas de pagamento de freelancers e profissionais da área digital a identificar trabalhadores de TI da RPDC que abusem dos seus serviços. Contratar ou apoiar as atividades dos trabalhadores da RPDC representa muitos riscos, desde o roubo de propriedade intelectual, dados e fundos, a danos à reputação e consequências legais, incluindo sanções tanto sob as autoridades dos EUA quanto das Nações Unidas (ONU).

A RPDC enviou milhares de trabalhadores de TI altamente qualificados para todo o mundo, recebendo rendimentos para a RPDC que contribuem para os seus programas de armas em violação das sanções dos EUA e da ONU. Esses trabalhadores:

- Abusam de todo o ecossistema de plataformas de trabalho freelance para obter sub-repticiamente contratos de desenvolvimento de TI de empresas clientes em todo o mundo - bem como abusar de muitas plataformas de comunicação social - para comunicar com clientes e plataformas de pagamento para receber pagamento pelo seu trabalho;
- Desenvolver aplicações e software que abrangem uma diversidade de setores, incluindo, mas sem se limitar, as áreas de negócios, criptomoedas, saúde e fitness, redes sociais, desportos, entretenimento e estilo de vida;
- Em muitos casos, apresentando-se indevidamente como estrangeiros (e não norte-coreanos), ou como teletrabalhadores americanos, através da utilização de redes privadas virtuais (VPN), servidores privados virtuais (VPS), endereços de IP adquiridos de países terceiros, contas proxy, e documentos de identificação falsificados ou roubados; e
- Utilizam acesso privilegiado adquirido como funcionários contratados para fins ilícitos, que incluem facilitar intrusões cibernéticas maliciosas por parte de outros atores da RPDC.

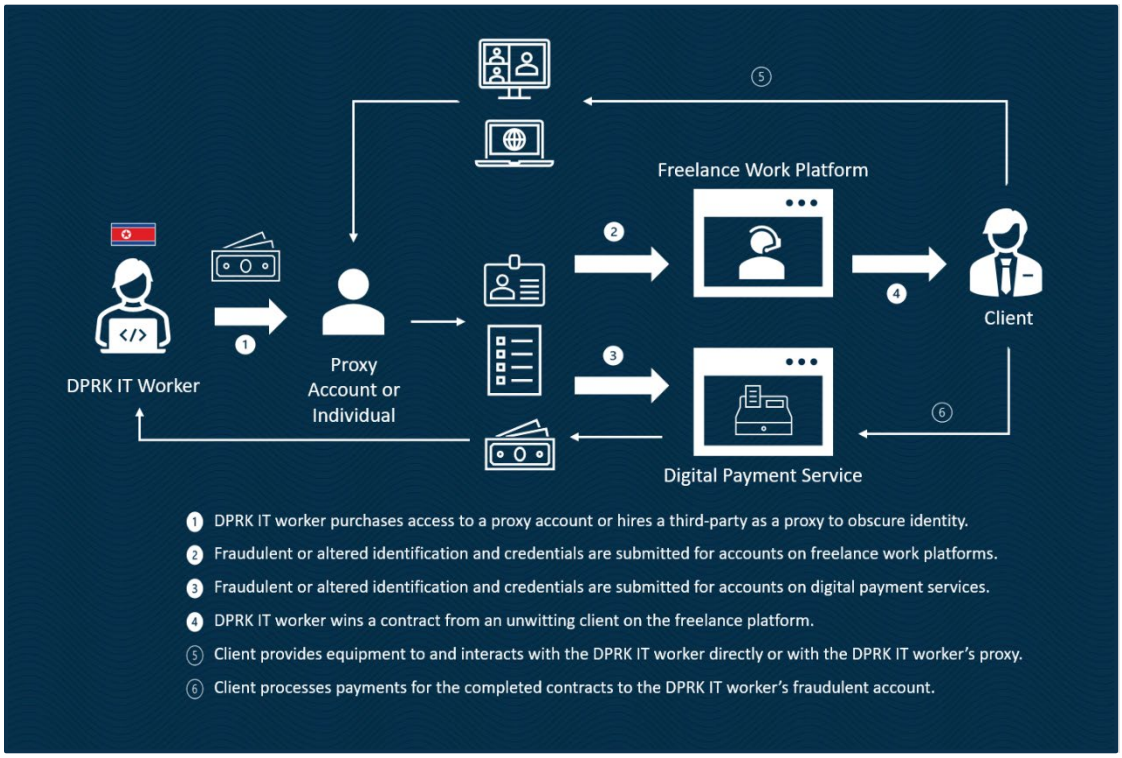
Alguns indicadores de sinais de alerta de atividade por parte de potenciais funcionários de TI da RPDC incluem:

- Logins múltiplos a uma conta a partir de diversos endereços de IP num espaço de tempo relativamente curto, especialmente se os endereços de IP estiverem associados a países diferentes.
- Transferências de dinheiro frequentes através de plataformas de pagamento, especialmente contas de banco com base na República Popular da China (RPC), ou pedidos de pagamento em criptomoedas;
- Incoerências relativamente à ortografia de nomes, nacionalidade, local de trabalho declarado, informações de contato, histórico escolar, histórico profissional e outros dados nos perfis de programadores nas plataformas de freelancers, perfis de redes sociais, páginas web de plataformas de portfolios, e a locais e horas estimados; e
- Inabilidade de conduzir os negócios durante as horas de trabalho exigidas, inabilidade de contactar o trabalhador atempadamente, especialmente através de meios de comunicação "instantâneos".

Medidas de diligência devida que o setor privado pode considerar para prevenir a contratação inadvertida ou involuntária de trabalhadores da RPDC incluem:

- Verificar os documentos enviados como parte de propostas para análise ou candidaturas a empregos diretamente com as empresas listadas e instituições de ensino (e não utilizando as informações de contato fornecidas na documentação enviada);
- Analisar minuciosamente documentos de comprovação de identidade enviados para averiguar se há falsificação;
- Realizar uma entrevista por vídeo para verificar a identidade do trabalhador freelancer em potencial;
- Realizar uma investigação contextual pré-contratação e/ou login por impressão digital/biométrico para comprovar a identidade e o local declarado;
- Evitar pagamentos em criptomoedas e exigir a comprovação de dados bancários que correspondam a outros documentos identificados;
- Verificar se a ortografia de nomes, nacionalidade, local de trabalho declarado, informações de contato, histórico escolar, histórico profissional e outros dados de um potencial funcionário coincidem com os perfis do programador nas plataformas de freelancers, perfis de redes sociais, páginas web de plataformas de portfolios, e locais e horas estimados; e
- Suspeitar se um programador não puder receber encomendas na morada contida na sua documentação de identificação.

Visão Geral das Operações dos Trabalhadores de TI da RPDC



Para mais informações, consulte o ***Documento Informativo sobre o Ambiente Virtual da RPDC****, visite o* ***Centro de Recursos da Administração Fiscal****, e/ou contate o seu* ***escritório local do FBI****. Caso tenha informações sobre atividades ilícitas da RPDC no espaço virtual, incluindo operações passadas ou em curso, poderá ser elegível para receber uma recompensa de até US$ 5 milhões por fornecer tais informações através do programa* ***Recompensas por Justiça*** *do Departamento de Estado.*