SCHEDA DATI:

GUIDA RELATIVA AI LAVORATORI DELLA REPUBBLICA POPOLARE DEMOCRATICA DI COREA NEL SETTORE DELLA TECNOLOGIA DELL'INFORMAZIONE

16 maggio 2022

Il Governo degli Stati Uniti pubblica il presente **avviso** come risorsa completa per la comunità internazionale, il settore privato e il pubblico al fine di meglio comprendere e prevenire il reclutamento, l'assunzione e la facilitazione involontaria di lavoratori o sviluppatori informatici (IT) della Repubblica Popolare Democratica di Corea (RPDC, cioè la Corea del Nord). L'avviso presenta informazioni dettagliate su come operano i suddetti lavoratori identificando i segnali di allarme e le necessarie misure di controllo (due diligence) utili alle aziende per evitare l'assunzione dei suddetti sviluppatori freelance della Corea del Nord e per aiutare le piattaforme per freelancer e di pagamento digitale a identificare tali lavoratori che abusano dei servizi offerti da tali piattaforme. Assumere lavoratori informatici della Corea del Nord o favorire le loro attività comporta molti rischi, che vanno dal furto di proprietà intellettuale, di dati e di denaro, al danno alla reputazione con relative conseguenze legali, comprese le sanzioni previste dalle autorità sia degli Stati Uniti, sia delle Nazioni Unite (ONU).

La Repubblica Popolare Democratica di Corea ha distaccato migliaia di abilissimi lavoratori informatici in tutto il mondo che generano redditi per il proprio Paese contribuendo ai suoi programmi di armamento, in violazione delle sanzioni degli Stati Uniti e delle Nazioni Unite. Questi lavoratori:

- Abusano dell'intero ecosistema di piattaforme di lavoro freelance per ottenere in modo surrettizio contratti di sviluppo informatico da aziende clienti in tutto il mondo; inoltre abusano di molte piattaforme di social media per comunicare con i loro clienti e delle piattaforme di pagamento per ricevere il compenso per il proprio lavoro;
- Sviluppano applicazioni e software in una vasta gamma di settori, tra cui, a titolo meramente esemplificativo, il commercio, le criptovalute, la salute e fitness, i social network, lo sport, l'intrattenimento e lo stile di vita;
- In molti casi fingono di essere telelavoratori stranieri (non nordcoreani) o statunitensi, anche attraverso l'uso di reti private virtuali (VPN), server privati virtuali (VPS), indirizzi IP di Paesi terzi, conti proxy e documenti di identità contraffatti o rubati; inoltre,
- In qualità di lavoratori a contratto si servono del loro accesso privilegiato per scopi illeciti, compresa l'abilitazione di intrusioni cibernetiche dolose da parte di altri agenti nordcoreani.

Alcuni segnali di allarme di potenziali attività di lavoratori informatici della Corea del Nord:

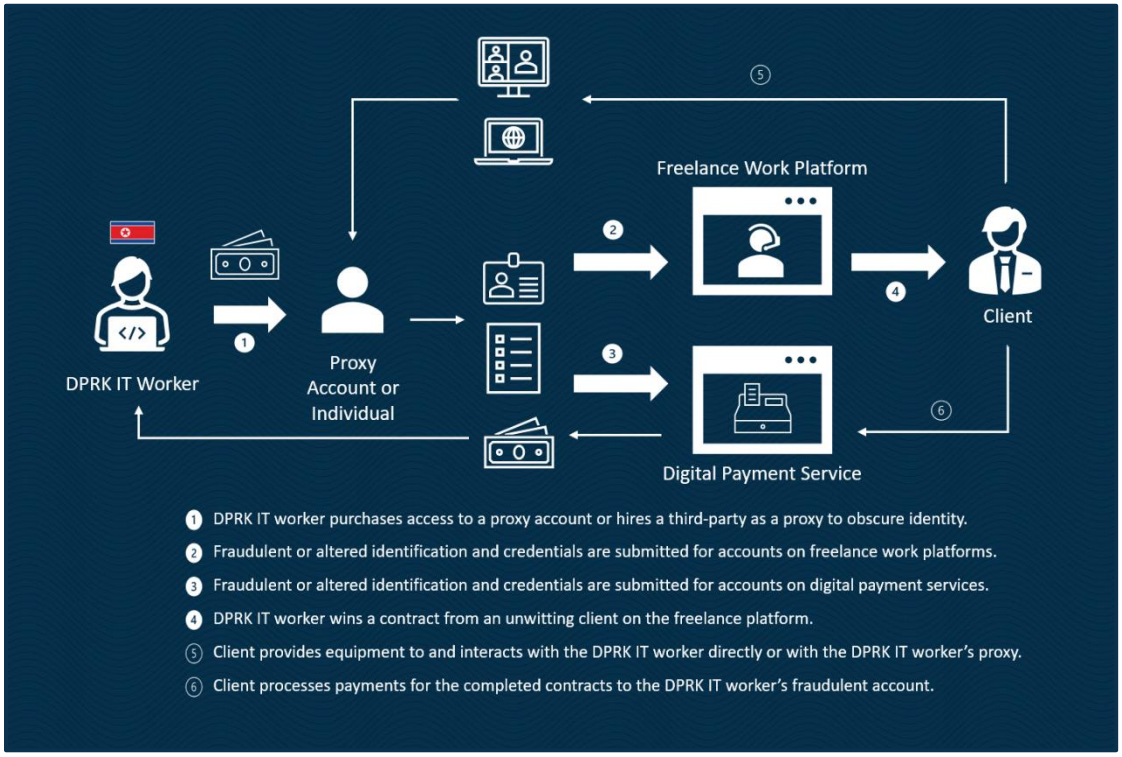
- Accessi multipli a un conto da diversi indirizzi IP in un periodo di tempo relativamente breve, soprattutto se gli indirizzi IP sono associati a Paesi diversi;

- Trasferimenti frequenti di denaro su piattaforme di pagamento, soprattutto verso conti bancari nella Repubblica Popolare Cinese (RPC), o richieste di pagamento in criptovaluta;
- Mancanza di uniformità nell'ortografia del nome del lavoratore, nella sua nazionalità, località di lavoro dichiarata, informazioni di contatto, curriculum di studi, esperienza lavorativa e altri dettagli, tra il profilo che egli pubblica sulle piattaforme per freelancer e quello sui social media, sui siti web di portfolio esterni, sulle piattaforme di pagamento e sul luogo e gli orari di lavoro dichiarati; inoltre,
- L'impossibilità di svolgere la propria attività durante gli orari di lavoro richiesti e di essere raggiunto in modo tempestivo, soprattutto con mezzi di comunicazione "istantanei".

Le misure di due diligence che il settore privato può eventualmente adottare per evitare l'assunzione involontaria o inconsapevole di lavoratori informatici della Corea del Nord includono:

- Verifica di documenti in appoggio alla valutazione di proposte o di domande di lavoro presentati direttamente ad aziende o istituti scolastici (che non usano le informazioni di contatto indicate nella documentazione);
- Un attento esame dei documenti presentati per verificare l'identità e individuare eventuali contraffazioni;
- Condurre colloqui video per accertare l'identità dei potenziali lavoratori freelance;
- Controllo pre-assunzione dei precedenti anche attraverso impronte digitali o dati biometrici per verificare l'identità e la località dichiarata;
- Evitare i pagamenti in criptovaluta e verificare che le informazioni bancarie corrispondano agli altri documenti di identità;
- Verificare che l'ortografia del nome, la nazionalità, la località dichiarata, le informazioni di contatto, il curriculum studi, l'esperienza lavorativa e gli altri dati di un potenziale lavoratore corrispondano ai dati sulle piattaforme per freelancer, sui social media, sui siti web di portfolio esterni, sui conti delle piattaforme di pagamento e sui luoghi e orari di lavoro dichiarati; infine,
- Diffidare di un lavoratore che non può ricevere posta all'indirizzo indicato nei suoi documenti di identità.

Panoramica delle operazioni dei lavoratori informatici della RPDC



*Per maggiori informazioni, vedere l'**Avviso riguardo alle attività cibernetiche della RPDC**, visitare il **Centro risorse del Dipartimento del Tesoro**, o rivolgersi all'**ufficio locale dell'FBI**. Se disponete di informazioni sulle attività illecite della RPDC nello spazio cibernetico, sia trascorse che attualmente in corso, potreste avere diritto a ricevere un premio di fino a 5 milioni di dollari se fornite le informazioni attraverso il programma **Rewards for Justice** del Dipartimento di Stato.*