16 maggio 2022

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

Il Dipartimento di Stato degli Stati Uniti, quello del Tesoro e il Federal Bureau of Investigation (FBI) rilasciano il presente avviso per la comunità internazionale, il settore privato e il pubblico al fine di avvertire riguardo ai tentativi di lavoratori informatici della Repubblica Popolare Democratica di Corea (RPDC, cioè la Corea del Nord) di ottenere lavoro facendosi passare per cittadini di altri Paesi. Esistono rischi legati al buon nome della persona o dell'azienda, oltre a possibili conseguenze legali, fra cui le sanzioni imposte dalle autorità statunitensi e dalle Nazioni Unite (ONU) contro persone fisiche e/o giuridiche impegnate nelle attività di lavoratori informatici della Corea del Nord o che le appoggiano o ne elaborano le relative operazioni finanziarie.

La Corea del Nord distacca migliaia di abilissimi lavoratori tecnici IT in tutto il mondo, al fine di generare per il loro Paese redditi che contribuiscono ai programmi di armi di distruzione di massa e di missili balistici, in violazione delle sanzioni imposte alla Corea del Nord dagli Stati Uniti e dalle Nazioni Unite. Questi lavoratori approfittano della domanda esistente di competenze informatiche specifiche, come ad esempio lo sviluppo di software e di applicazioni mobili, per aggiudicarsi contratti come collaboratori autonomi (freelance) da clienti di tutto il mondo, tra cui l'America settentrionale, l'Europa e l'Asia orientale. In molti casi, si spacciano per telelavoratori con sede negli Stati Uniti o comunque non nordcoreani. Essi possono inoltre occultare la loro identità o sede subappaltando il lavoro a terzi che non sono di nazionalità nordcoreana. Sebbene non siano normalmente impegnati in attività dolose, essi hanno però abusato in passato del loro accesso privilegiato in qualità di collaboratori a contratto per permettere intrusioni cibernetiche illecite da parte della Corea del Nord. Inoltre, è probabile che alcuni di loro siano costretti al lavoro forzato.

Questo avviso fornisce informazioni dettagliate su come operano i lavoratori IT della Corea del Nord, importanti segnali di allarme per le aziende che assumono sviluppatori con contratti di lavoro autonomo (freelance) e per le piattaforme per lavoratori freelance e di pagamento, che possono aiutare le aziende a identificare tali lavoratori. Offre anche misure generali di mitigazione per le aziende per una migliore protezione contro l'assunzione involontaria o l'agevolazione delle operazioni dei suddetti

tecnici IT nordcoreani. Un allegato al presente offre ulteriori informazioni su di essi, desunte dalle relazioni pubblicate dal Gruppo di esperti sulla Corea del Nord del Comitato sanzioni ONU 1718. L'FBI incoraggia le aziende statunitensi a segnalare agli uffici locali dell'FBI qualsiasi attività sospetta, comprese quelle di lavoratori informatici che si sospetta siano di nazionalità nordcoreana.

LAVORATORI INFORMATICI DELLA COREA DEL NORD: CONTESTO

I lavoratori informatici forniscono alla Corea del Nord un'importante fonte di reddito che aiuta a finanziare i programmi economici e di sicurezza più importanti del regime, come ad esempio il programma di sviluppo di armamenti. Kim Jong Un, il leader del Paese, riconosce l'importanza di questi tecnici come fonte importante di valuta estera e di reddito e ne supporta le attività.

Migliaia di tecnici IT nordcoreani, sia distaccati all'estero sia ubicati nel loro territorio, generano introiti che vengono rimessi al loro governo. Essi si trovano principalmente nella Repubblica Popolare Cinese (RPC) e in Russia, con un numero minore in Africa e nel Sud-est asiatico e fanno spesso affidamento sui loro contatti all'estero per ottenere lavori freelance e per relazionarsi più direttamente con i clienti.

Scopo di questi lavoratori è sostenere con i loro proventi il regime del loro leader Kim Jong Un. Infatti la stragrande maggioranza di loro dipende e lavora per conto di entità coinvolte direttamente nei programmi nordcoreani di armi di distruzione di massa e di missili balistici, vietati dalle Nazioni Unite, nonché nei settori dello sviluppo e del commercio di armi convenzionali avanzate. In poche parole, i loro introiti servono alla Corea del Nord per sviluppare i suoi programmi di armi di distruzione di massa e balistici, in violazione delle sanzioni imposte dagli Stati Uniti e dalle Nazioni Unite. Molte di queste entità sono oggetto di sanzioni da parte dell'ONU e degli Stati Uniti. Le entità che inviano lavoratori informatici all'estero includono:

- **L'Ufficio generale 313 del Dipartimento dell'industria delle munizioni (MID, *Munitions Industry Department*)** che sopravvede alla ricerca, sviluppo e produzione di armi della Corea del Nord, tra cui armi nucleari e missili balistici, e altre attrezzature militari. Il MID dipende dal Comitato centrale del Partito dei lavoratori della Corea e, attraverso l'Ufficio generale 313, dispiega la maggior parte della forza lavoro informatica nordcoreana all'estero. Tutti i beni e gli interessi in beni di proprietà del Partito dei lavoratori della Corea sono bloccati in base all'ordine esecutivo (E.O., *Executive Order*) 13722.

- **Il Ministero dell'industria dell'energia atomica,** un protagonista centrale nello sviluppo delle armi nucleari nordcoreane, responsabile delle operazioni quotidiane del programma di armi nucleari. Il Ministero dell'industria dell'energia atomica è bloccato ai sensi dell'ordine esecutivo 13382.

- Enti militari subordinati al **Ministero della difesa e all'Esercito popolare della Corea**. L'Esercito popolare della Corea è stato incluso nella Lista specifica di cittadini identificati e di beni bloccati.

- Entità meno conosciute, come ad esempio l'**Ufficio commercio estero della Commissione per l'istruzione della Corea del Nord** e l'**Ufficio per l'informatica di Pyongyang del Dipartimento scienza e istruzione del Comitato centrale.** Tutti i beni e gli interessi in beni di proprietà del governo nordcoreano sono bloccati ai sensi dell'ordine esecutivo 13722.

I lavoratori informatici nordcoreani distaccati all'estero guadagnano almeno dieci volte di più di rispetto a un normale operaio di fabbrica o dell'edilizia nordcoreano che lavora all'estero. In alcuni casi, guadagnano più di 300.000 dollari all'anno; i team IT possono guadagnare collettivamente più di 3 milioni di dollari all'anno. Una percentuale importante dei loro introiti lordi sostiene le priorità del regime del loro Paese, fra cui il programma di armi di distruzione di massa.

Le aziende informatiche nordocoreane e i loro tecnici si dedicano normalmente a un'ampia gamma di attività nello sviluppo informatico di varia complessità e difficoltà, come ad esempio:

- applicazioni mobili e web,
- costruzione di piattaforme virtuali cambiavalute e di moneta digitale,
- supporto informatico in genere,
- animazione grafica,
- programmi di gioco d'azzardo online,
- giochi per cellulari,
- applicazioni per appuntamenti,
- applicazioni legate all'intelligenza artificiale,
- sviluppo di hardware e firmware,
- programmazione di realtà virtuale e realtà aumentata,
- software di riconoscimento facciale e biometrico, e
- sviluppo e gestione di banche di dati.

Le applicazioni e i programmi software sviluppati dai tecnici IT nordcoreani spaziano su diversi campi e settori, tra cui affari, salute e fitness, social network, sport, intrattenimento e stile di vita. Spesso si occupano di progetti riguardanti le valute virtuali. Alcuni di loro hanno messo a punto dei programmi per il cambio virtuale di valute o creato strumenti analitici e applicazioni per chi commercia in valute virtuali, e hanno commercializzato essi stessi i propri prodotti.

Per decenni, la Corea del Nord ha sottolineato l'importanza per i suoi cittadini dell'istruzione in matematica e nelle scienze. L'enfasi sul progresso della scienza e della tecnologia, storicamente una priorità per il regime Kim, si riflette nell'investimento di risorse e di personale in campi di ricerca correlati. L'odierna istruzione informatica e cibernetica nella Corea del Nord prende le basi da questa

spinta al progresso ed è sfociata in un curriculum integrato coordinato con il Partito dei lavoratori, con centri di ricerca e con le forze armate.

- Negli ultimi anni, sotto Kim Jong Un, il regime ha dedicato un'attenzione sempre maggiore all'istruzione e alla formazione nelle materie legate all'informatica sviluppando solidi programmi universitari presso diversi istituti nazionali di primo piano, in particolare l'Università Kim Il Sung, l'Università di tecnologia Kim Chaek e l'Università di scienza e tecnologia di Pyongyang. Solo in queste università di alto livello circa 30.000 studenti studiano materie legate alle tecnologie dell'informazione e della comunicazione.

- Secondo quanto riferito, al 2019, 37 università avevano istituito 85 programmi di corsi avanzati in materie scientifiche, tecnologiche, ingegneristiche e matematiche (STEM, *science, technology, engineering, and math*), tra cui la sicurezza informatica, e ogni provincia del Paese aveva fondato almeno una nuova scuola secondaria per coltivare gli studenti più promettenti.

- Il sistema educativo della Corea del Nord è altamente competitivo e solo i migliori studenti vengono accettati nei programmi scientifici e tecnologici d'élite. Gli studenti vengono reclutati in giovane età da scuole secondarie come l'Accademia di Kumsong e la scuola media numero 1 di Kumsong.

- Per affinare ulteriormente le proprie competenze, i lavoratori informatici nordcoreani ricevono formazione supplementare all'estero e presso le loro stesse organizzazioni, spesso attraverso centri di ricerca informatica regionali. In passato, hanno ricevuto corsi di formazione in Africa orientale, nel Sud-est asiatico e nell'Asia meridionale ottenendo notevoli benefici dalla loro formazione all'estero.

COME OPERANO I LAVORATORI INFORMATICI DELLA COREA DEL NORD

I lavoratori informatici nordcoreani mirano a contratti freelance da datori di lavoro con sede in Paesi più ricchi, tra cui quelli dell'America settentrionale, dell'Europa e dell'Asia orientale. In molti casi, si presentano come telelavoratori sudcoreani, cinesi, giapponesi, dell'Europa orientale o degli Stati Uniti.

In alcuni casi, questi tecnici IT occultano ulteriormente la loro identità tramite accordi con subappaltatori terzi. Questi subappaltatori a loro volta sono lavoratori autonomi (freelance) non nordcoreani che lavorano sui contratti dei tecnici nordcoreani. A volte, i manager di aziende IT nordcoreane assumono team di tecnici IT non nordcoreani i quali di solito non si rendono conto della vera identità del loro datore di lavoro o del fatto si tratti di un'azienda nordcoreana. I manager di aziende IT nordcoreane si servono di dipendenti che lavorano per loro in outsourcing per l'acquisto di software o per interagire con clienti in situazioni che altrimenti potrebbero rivelare l'identità nordcoreana dell'azienda o dei loro tecnici.

Sebbene i tecnici IT nordcoreani siano normalmente impegnati in attività non dannose, ad esempio lo sviluppo di programmi per il cambio virtuale di valuta o di siti web, hanno però utilizzato il loro accesso privilegiato in qualità di operatori a contratto per consentire intrusioni cibernetiche dolose da parte della Corea del Nord. Alcuni di questi tecnici distaccati all'estero (sebbene non coinvolti di prima persona in tali dolose attività cibernetiche) hanno però fornito supporto logistico ad agenti nordcoreani malintenzionati. In effetti, i tecnici IT nordcoreani sono in grado di condividere il loro accesso all'infrastruttura virtuale, facilitare la vendita di dati trafugati da agenti cibernetici nordcoreani, o assistere la loro Nazione nel riciclaggio di denaro e nel trasferimento di valuta virtuale.

I tecnici IT nordcoreani hanno anche assistito i funzionari della loro Nazione nell'approvvigionamento di pezzi utili alle armi di distruzione di massa e ai missili balistici per i programmi di armamenti vietati.

In alcuni casi, questi lavoratori sono vittime della tratta di esseri umani, compreso il lavoro forzato. Resoconti attendibili indicano che molti di questi lavoratori dislocati all'estero sono sottoposti a orari di lavoro eccessivi, a una sorveglianza stretta e costante da parte degli agenti di sicurezza del governo nordcoreano, a condizioni di vita insicure e insalubri, e con una ristretta libertà di movimento. Il governo nordcoreano trattiene fino al 90% dei loro salari, il che genera centinaia di milioni di dollari in introiti annuali per il governo.

I lavoratori informatici della Corea del Nord: competenze e piattaforme

I team IT dislocati all'estero di solito ottengono lavoro autonomo attraverso varie piattaforme online per lavoro freelance dove le aziende inseriscono annunci per contratti di lavoro e i tecnici IT presentano le loro offerte per i vari progetti. Meno frequentemente, i team trovano cittadini locali, non di nazionalità nordcoreana, che accettano di fungere da responsabili di aziende che sono controllate a tutti gli effetti da cittadini nordcoreani. In alcuni casi, questi team nordcoreani sembrano lavorare ufficialmente per un'azienda locale legittima, ma svolgono invece attività autonome, pagando un compenso all'azienda straniera in cambio dell'occultazione delle loro origini nordcoreane. Questi team IT nordcoreani spesso includono degli esperti in una lingua straniera, come l'inglese o il cinese.

Questi lavoratori si servono di un'ampia varietà di piattaforme di appalto freelance tradizionali e specifiche del settore IT, strumenti e piattaforme di sviluppo software, applicazioni di messaggistica e siti web di social media e networking per ottenere contratti di sviluppo da aziende di tutto il mondo, oltre a utilizzare piattaforme di pagamento digitale o siti web per ricevere i compensi per il proprio lavoro. Utilizzano anche scambi di valuta virtuale e piattaforme di trading per gestire i pagamenti digitali ricevuti nonché per riciclare e trasferire tali fondi.

I lavoratori informatici della Corea del Nord: occultazione della loro identità

I lavoratori informatici nordcoreani oscurano deliberatamente online la loro identità, la località in cui si trovano e la loro nazionalità, spesso usando come pseudonimi nomi non coreani. Si servono anche di reti private virtuali (VPN), server privati virtuali (VPS) o indirizzi IP di Paesi terzi per far credere che si collegano a Internet da località che non danno nell'occhio, riducendo così la probabilità di un controllo accurato o dei loro legami con la Corea del Nord. Di solito fanno affidamento sull'anonimato degli accordi di telelavoro, delegando terzi per aprire e mantenere i loro account e preferiscono l'uso di intermediari e di comunicazioni tramite chat di testo anziché videochiamate.

I lavoratori informatici nordcoreani utilizzano account fittizi per presentare offerte, ottenere progetti, lavorare e farsi pagare sui siti web di sviluppatori freelance di software. Questi account fittizi appartengono a persone terze, alcune delle quali vendono i propri dati identificativi e le informazioni relative ai propri account ai tecnici IT nordcoreani. In alcuni casi, quest'ultimi pagano delle commissioni per poter utilizzare questi account legittimi. In certi casi compilano anche i propri profili sulle piattaforme per lavoratori freelance con le affiliazioni reali e l'esperienza lavorativa dell'individuo che impersonano.

A volte, i tecnici IT nordcoreani assumono lavoratori freelance non nordcoreani presenti sulle piattaforme proponendo loro di collaborare a progetti di sviluppo. Un tecnico IT nordcoreano approfitterà di questi rapporti commerciali per ottenere l'accesso a nuovi contratti e a conti in valuta virtuale utilizzati per svolgere il lavoro informatico su infrastrutture virtuali statunitensi od europee, aggirando così le misure di sicurezza mirate a prevenire usi fraudolenti. Nel creare account con l'aiuto di altri lavoratori autonomi, i nordcoreani possono farsi passare per cittadini di Paesi terzi che hanno bisogno di documenti di identità statunitensi o di altri Paesi occidentali e di account su piattaforme di freelance al fine di guadagnare di più.

Il non svelare la propria posizione geografica reale consente ai tecnici IT nordcoreani di violare i termini degli accordi di prestazioni per le piattaforme e i servizi online che utilizzano per le loro attività. Come parte del loro modus operandi, utilizzano anche dispositivi singoli e dedicati per ciascuno dei loro conti, soprattutto per i servizi bancari, onde eludere il rilevamento mediante le misure di prevenzione delle frodi, dell'osservanza delle sanzioni e delle misure antiriciclaggio.

Essi di norma si servono di documenti falsi, alterati o contraffatti, compresi documenti di identità e firme contraffatte, che hanno realizzato da soli con software tipo Photoshop, o che hanno ottenuto a pagamento da società di falsari, combinando con i dati di una persona reale la propria foto o un'altra foto. Si procurano solitamente documenti falsi come i seguenti:

- patenti di guida,
- tessere della previdenza sociale,
- passaporti,
- carte d'identità nazionali,
- carte di identità per residenti esteri,

- diplomi scolastici o universitari,
- visti per lavoro,
- estratti conto di carte di credito o di banca e bollette di servizi pubblici.

In alcuni casi, queste identità vengono rubate; in altri, i lavoratori informatici nordcoreani chiedono a cittadini non nordcoreani di creare dei conti utilizzando i loro dati personali o i dati cui hanno accesso, dopodiché il controllo del conto viene trasferito dietro pagamento ai nordcoreani . Questo permette loro di occultare la loro vera identità quando presentano delle offerte o completano online dei progetti freelance per clienti, utilizzando l'infrastruttura del titolare reale del conto tramite accesso al desktop remoto. Ciascuno di questi tecnici spesso utilizza più identità e conti, che possono anche essere condivisi tra i lavoratori dello stesso team. Questi conti e queste identità pretendono di provenire da Paesi di ogni parte del mondo.

I lavoratori informatici nordcoreani si impossessano dei dati di conti cliente di banche statunitensi o internazionali allo scopo di convalidare la loro propria identità su piattaforme per lavoratori freelance o di pagamento e ad aziende che li impiegano . In almeno un caso, alcuni di loro hanno falsificato assegni con informazioni rubate da un conto bancario. Gli account e i curriculum associati alle identità fittizie dei lavoratori IT nordcoreani spesso includono informazioni falsificate, ma realistiche e dettagliate, sul curriculum professionale e di studi, comprese false informazioni di contatto degli istituti educativi e dei precedenti datori di lavoro.

I lavoratori IT nordcoreani compilano anche le sezioni online relative alla loro esperienza professionale di sviluppatore con i nomi di aziende occidentali di piccole o medie dimensioni, in modo che, quando presentano offerte per i progetti, appaiono come americani o europei rispettabili. A volte usano i nomi di dipendenti reali e indirizzi e-mail che rassomigliano al dominio legittimo di aziende occidentali.

Inoltre, falsificano contratti di lavoro, fatture, documentazione di comunicazioni con il cliente e altri documenti da usare sulle piattaforme di freelance, che possono soddisfare le misure di verifica dei clienti e di antiriciclaggio (cosiddette KYC/AML, *know-your-customer and anti-money laundering*) o procedure simili che le piattaforme utilizzano per garantire la legittimità dell'attività degli utenti. Le informazioni di contatto riportate in questi documenti falsificati sono a volte minime, proprio per scoraggiare verifiche.

Questi lavoratori tentano anche di mascherare la propria nazionalità dichiarandosi cittadini sudcoreani o semplicemente "coreani".

In certi casi, ottengono posti di collaboratore autonomo presso un'azienda inconsapevole, e in seguito raccomandano all'azienda l'assunzione di altri lavoratori IT nordcoreani freelance.

Curriculum di un lavoratore informatico della Corea del Nord

I lavoratori informatici nordcoreani pubblicizzano le proprie competenze in materia di sviluppo di sistemi e di programmi, sistemi di gestione di database, e conoscenza di un'ampia varietà di linguaggi, framework, strumenti e risorse cloud comuni. Spesso, queste competenze includono una solida conoscenza di diversi linguaggi di programmazione e di markup. La maggior parte dei progetti realizzati questi tecnici riguarda lo sviluppo di applicazioni mobili e web. Essi usano anche piattaforme di collaborazione e servizi di hosting per la gestione dei dati e dei flussi di lavoro. Spesso dichiarano di avere esperienza con una varietà di database e di conoscere i prodotti e i servizi cloud e di analisi dei principali fornitori. Inoltre, includono nel proprio lavoro piattaforme di pagamento digitale e di e-commerce.

Questi lavoratori realizzano siti web che mostrano il loro lavoro, generalmente semplici nel design, nel tentativo di aumentare la propria credibilità di sviluppatori autonomi. Questi curriculum virtuali rappresentano in realtà l'esperienza di lavoro di profili contraffatti e sono spesso collegati agli account online di sviluppatori freelance dei tecnici IT nordcoreani. Le informazioni pubblicate su tali questi siti, comprese le informazioni di contatto e la sede, nonché il curriculum lavorativo e il percorso formativo, sono probabilmente false.

SEGNALI DI ALLARME

Le società che offrono lavoro di collaboratore autonomo e le piattaforme di pagamento devono essere consapevoli delle seguenti attività e comportamenti, possibili indizi che dei lavoratori informatici nordcoreani potrebbero avvalersi delle loro piattaforme.

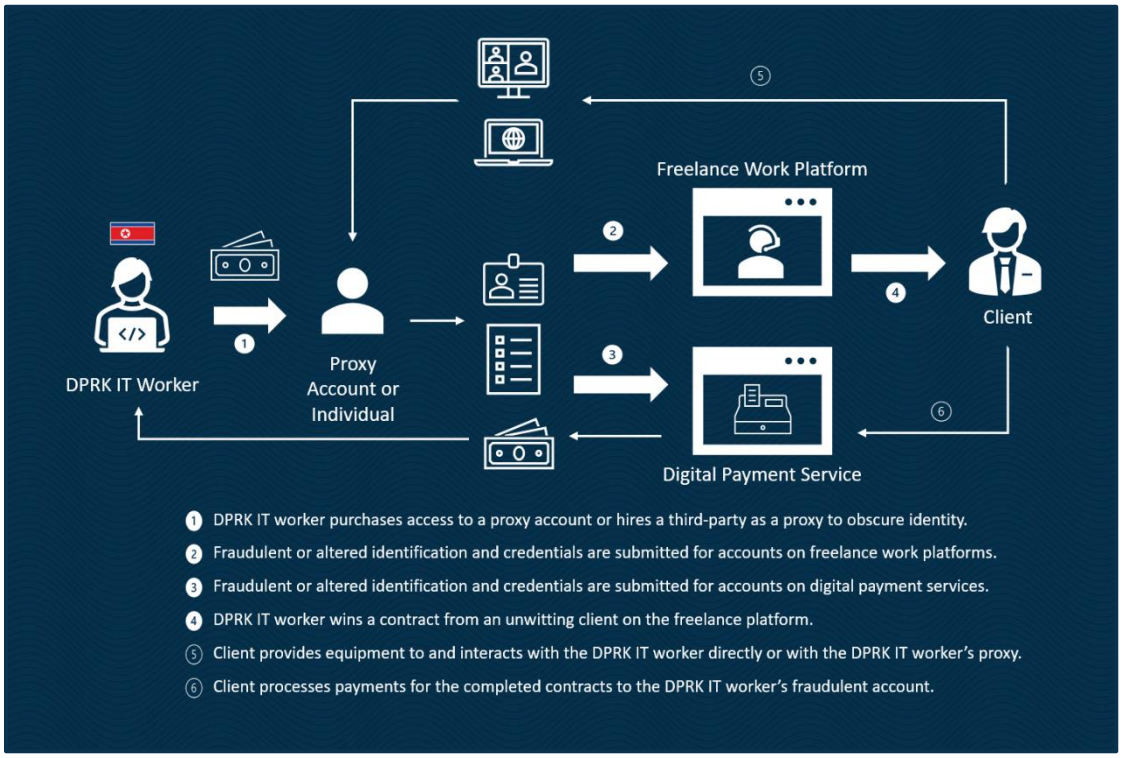
- Accessi multipli a un account da diversi indirizzi IP in un periodo di tempo relativamente breve, soprattutto se gli indirizzi IP sono associati a Paesi diversi;
- Sviluppatori che accedono a più account sulla stessa piattaforma da un unico indirizzo IP;
- Sviluppatori che accedono ai loro account in modo continuativo per uno o più giorni alla volta;
- Porta del router o altre configurazioni tecniche associate all'uso di un software di condivisione di desktop remoto, come ad esempio, la porta 3389 del router utilizzato per accedere all'account, in particolare se l'uso del software di condivisione del desktop remoto non costituisce una prassi aziendale standard;
- Gli account degli sviluppatori utilizzano un conto cliente fraudolento per ottenere migliori valutazioni, ma sia l'account del cliente sia quello dello sviluppatore utilizzano lo stesso conto PayPal per trasferire/prelevare denaro (pagando se stessi con il proprio denaro);
- L'uso frequente di identici modelli di documenti per i documenti di offerta e i metodi di comunicazione del progetto; in particolare l'uso degli stessi modelli da account di sviluppatori diversi;
- Più account di sviluppatori che ricevono valutazioni elevate da un unico conto cliente in un breve periodo, con documentazione simile o identica per creare gli account degli sviluppatori e/o del cliente;
- Frequente partecipazione alle gare d'appalto per progetti ma un basso numero di contratti ottenuti rispetto al numero delle gare in cui lo sviluppatore ha partecipato con un'offerta.
- Trasferimenti frequenti di denaro attraverso piattaforme di pagamento, soprattutto verso conti bancari basati nella Repubblica Popolare Cinese, e talvolta convogliati attraverso una o più società per mascherare la destinazione finale dei fondi.

Le società che impiegano sviluppatori autonomi a contratto devono essere consapevoli delle seguenti attività e comportamenti, possibili indizi che si tratta di lavoratori informatici nordcoreani.

- Se un sito web di sviluppo software freelance o un conto su una piattaforma di pagamento è stato chiuso o il lavoratore contatta il datore di lavoro chiedendo di utilizzare un account diverso, soprattutto se registrato sotto un nome diverso;
- L'uso di servizi di pagamento digitali, in particolare quelli legati alla Repubblica Popolare Cinese;
- Mancanza di uniformità nell'ortografia del nome, nella nazionalità, nella sede di lavoro dichiarata, nelle informazioni di contatto, nel curriculum di studi, nell'esperienza lavorativa e in altri dettagli tra i profili del lavoratore presente sulle piattaforme di freelance, sui social media, sui siti web esterni che hanno il loro curriculum lavorativo sulle piattaforme di pagamento, e la sede e gli orari verificati di uno sviluppatore;
- Siti web con il curriculum di lavoro, profili sui social media o profili di sviluppatore sorprendentemente semplici;
- Messaggi diretti o chiamate inaspettate da parte di persone che si dichiarano dirigenti di alto livello di aziende di sviluppo software per offrire servizi o informare sulle proprie competenze;
- Richieste di comunicare con clienti effettivi o potenziali su una piattaforma separata rispetto al sito web della piattaforma originale per freelance, dove il cliente ha trovato il lavoratore informatico;
- Un datore di lavoro propone di inviare dei documenti o delle attrezzature di lavoro, ad esempio un computer portatile, a uno sviluppatore, e quest'ultimo chiede che vengano spediti a un indirizzo non riportato nei suoi documenti di identità. Il fatto che egli dichiari di non poter ricevere posta all'indirizzo indicato nei suoi documenti è da considerarsi particolarmente sospetto;
- Richieste di pagamento in una valuta virtuale nel tentativo di eludere le misure KYC/AM e l'uso del sistema finanziario tradizionale;
- Richieste di pagamento anche se non sono stati rispettati i requisiti di produzione o la partecipazione a riunioni di verifica;
- L'impossibilità di condurre l'attività durante gli orari di lavoro richiesti;
- Informazioni di contatto errate o modificate, in particolare numeri di telefono e indirizzi di posta elettronica;
- Dati biografici che non sembrano corrispondere al candidato;
- Mancato completamento degli incarichi in modo tempestivo o mancata risposta agli incarichi;

- L’impossibilità di contattare il lavoratore in modo tempestivo, soprattutto attraverso metodi di comunicazione “istantanei”; infine,
- Chiedere ai colleghi di prendere a prestito alcuni dei loro dati personali per ottenere altri contratti.

Panoramica delle operazioni dei lavoratori informatici della Corea del Nord



MISURE DI POSSIBILE MITIGAZIONE

Per le aziende che offrono lavoro ai lavoratori freelance e per le piattaforme di pagamento

- Controllare i documenti presentati in appoggio alla valutazione di proposte ed effettuare le procedure di verifica (*due-diligence*) dei contratti, ad esempio verificando in modo autonomo fatture e accordi di lavoro contattando i clienti elencati ma utilizzando le informazioni di contatto riportate nelle banche dati aziendali e non quelle indicate nella documentazione presentata;

- Esaminare attentamente i documenti presentati a comprova dell'identità per accertare che non siano falsi, rivolgendosi eventualmente alle forze dell'ordine locali per assistenza. Respingere i documenti inviati a comprova dell'identità quando sono immagini di bassa qualità;

- Verificare l'esistenza di qualsiasi sito web indicato all'atto della creazione di un account; in particolar modo, controllare attentamente qualsiasi account che abbia utilizzato siti web defunti per creare l'account.

- Nell'ambito dei processi di verifica iniziale per i contratti e delle politiche di aggiornamento, chiedere un video di verifica dell'identità o un colloquio video per verificare l'identità;

- Utilizzare regolarmente le funzionalità di controllo delle porte per determinare se l'accesso alla piattaforma avviene da remoto tramite un software di condivisione desktop, una VPN o un VPS, in particolare se l'utilizzo di software di condivisione desktop remoto o di servizi VPN per accedere agli account non è una prassi normale;

- Contrassegnare automaticamente per ulteriore revisione gli account di clienti e sviluppatori che utilizzano documentazione identica o simile per creare account o che utilizzano gli stessi account per i servizi di pagamento digitale;

- Contrassegnare automaticamente per ulteriore revisione l'uso di modelli di documenti identici o simili per la presentazione delle offerte e per comunicazioni relative a progetti in account per sviluppatori differenti;

- Contrassegnare automaticamente per ulteriore revisione gli account di molteplici sviluppatori che ricevono valutazioni elevate da un singolo conto cliente in un breve periodo di tempo, soprattutto se è stata impiegata documentazione simile o identica per creare gli account;

- Contrassegnare automaticamente per ulteriore revisione gli account di sviluppatori con un alto numero di offerte d'appalto presentate ma un basso numero di offerte accettate rispetto a quelle offerte. Inoltre, contrassegnare gli account con un alto numero di offerte d'appalto presentate rispetto al numero di login per l'account;

- Non permettere alcuna attività in conti di recente creazione prima che sia stata effettuata una verifica completa;

- Effettuare un controllo supplementare per i conti di recente creazione; e

Per le aziende che assumono programmatori e sviluppatori su piattaforme per freelance

- Condurre colloqui video per accertare l'identità dei potenziali lavoratori freelance;

- Effettuare un controllo dei precedenti, controllo sull'uso di stupefacenti e delle impronte digitali o dei dati biometrici per verificare l'identità e la sede dichiarata; Evitare i pagamenti in valute virtuali e richiedere la verifica delle informazioni bancarie corrispondenti agli altri documenti di identità;

- Usare molta cautela nell'interagire con sviluppatori freelance attraverso applicazioni di collaborazione a distanza, come ad esempio le applicazioni di desktop remoto. Prendere in considerazione la possibilità di disabilitare le applicazioni di collaborazione remota su eventuali computer forniti allo sviluppatore freelance;

- Verificare le esperienze lavorative e di studi superiori direttamente con le aziende e gli istituti scolastici, utilizzando però informazioni di contatto prese da un motore di ricerca o altro database aziendale, e non ottenute direttamente dal candidato o dal suo profilo;

- Verificare che l'ortografia del nome, la nazionalità, la sede dichiarata, le informazioni di contatto, il curriculum di studi e di lavoro e altri dettagli di un candidato si conformino con quelli presenti sui profili delle piattaforme di freelance, dei social media, dei siti web esterni presentati come esperienze lavorative e dei conti sulle piattaforme di pagamento, oltre alla sede e agli orari di lavoro verificati dello sviluppatore. Sospettare particolarmente di siti web di esperienze lavorative, di profili sui social media e di profili di sviluppatore insolitamente semplici;

- Sospettare di sviluppatori che chiedono di comunicare su una piattaforma diversa rispetto al sito web della piattaforma originale per freelance dove l'azienda ha trovato inizialmente il lavoratore IT;

- Quando si inviano a uno sviluppatore documenti o attrezzature di lavoro come un computer portatile, farlo solo all'indirizzo riportato sui suoi documenti di identità ed esigere documentazione supplementare nel caso egli ne chieda la spedizione a un indirizzo sconosciuto. Diffidare se uno sviluppatore non può ricevere posta all'indirizzo indicato nei suoi documenti di identità; inoltre,

- Fare attenzione ad operazioni non autorizzate, di piccola entità, che potrebbero essere eseguite a scopo fraudolento da lavoratori IT a contratto. In un caso segnalato, alcuni di questi tecnici IT nordcoreani assunti come sviluppatori da un'azienda statunitense, hanno caricato addebiti falsi al conto di pagamento dell'azienda americana, appropriandosi di oltre 50.000 dollari in 30 piccole operazioni nell'arco di alcuni mesi. Data l'esiguità degli importi, l'azienda statunitense non si era accorta che gli sviluppatori erano nordcoreani né dei furti eseguiti a più riprese.

CONSEGUENZE DEI COMPORTAMENTI VIETATI O SANZIONABILI

Le persone e le entità impegnate in attività legate ai lavoratori informatici della Corea del Nord o che le supportano, compresa l'elaborazione delle relative operazioni finanziarie, devono essere consapevoli delle possibili conseguenze legali derivanti da comportamenti vietati o sanzionabili.

Le risoluzioni 2321, 2371 e 2397 del Consiglio di Sicurezza delle Nazioni Unite sottolineano che gli introiti generati dai lavoratori nordcoreani all'estero contribuiscono ai programmi di armi nucleari e di missili balistici della Corea del Nord. La risoluzione 2375 del Consiglio di Sicurezza delle Nazioni Unite proibisce agli Stati membri dell'ONU nelle rispettive giurisdizioni di fornire nuovi permessi di lavoro a cittadini della Corea del Nord o di rinnovare quelli scaduti che permettano loro l'ammissione nel territorio di tali Stati membri, a meno che tali autorizzazioni non siano state preventivamente approvate dal Comitato 1718 del Consiglio di Sicurezza ONU. La risoluzione 2397 del Consiglio di

Sicurezza delle Nazioni Unite impone a tutti gli Stati membri di rimpatriare, entro il 22 dicembre 2019, i cittadini della Corea del Nord che percepiscono un reddito nella loro giurisdizione, indipendentemente da quando o se siano stati rilasciati permessi di lavoro per loro.

L'Ufficio per il controllo dei beni esteri del Dipartimento del Tesoro (OFAC, *Office of Foreign Assets Control*) ha l'autorità di imporre sanzioni finanziarie a qualsiasi persona che risulti, tra le altre cose:

- Essere impegnata in attività significative che minano la sicurezza informatica per conto del governo della Corea del Nord o del Partito dei lavoratori della Corea;
- Operare nel settore informatico per conto della Corea del Nord;
- Essere impegnata in certe altre attività dolose rese possibili dalla tecnologia cibernetica;
- Essere impegnata in almeno un'importante operazione di importazione da o esportazione verso la Corea del Nord di beni, servizi o tecnologie;
- Aver venduto, fornito, trasferito o acquistato software, direttamente o indirettamente, da o verso la Corea del Nord o verso qualsiasi persona che agisce per conto del governo della Corea del Nord o del Partito dei lavoratori della Corea, laddove qualsiasi ricavo o merce ricevuta possa andare a vantaggio del governo della Corea del Nord o del Partito dei lavoratori della Corea; oppure
- Aver assistito materialmente, sponsorizzato o fornito sostegno finanziario, materiale o tecnologico, oppure beni o servizi, al governo della Corea del Nord o al Partito dei lavoratori della Corea.

Ad esempio, nel 2018, gli Stati Uniti hanno designato come passibile di sanzioni la Yanbian Silverstar Network Technology Co., Ltd., un'azienda tecnologica con sede in Cina. Quest'azienda era nominalmente un'azienda informatica cinese, ma in realtà era gestita e controllata da nordcoreani. L'azienda aveva anche creato una società di comodo con sede in Russia, la Volasys Silver Star, per aggirare i requisiti di identificazione sui forum di lavoro freelance.

Inoltre, se il Segretario del Tesoro, in consultazione con il Segretario di Stato, determina che un'istituzione finanziaria estera ha consapevolmente condotto o facilitato attività commerciali importanti con la Corea del Nord, o ha consapevolmente condotto o facilitato un'operazione importante per conto di una persona designata ai sensi di un ordine esecutivo legato alla Corea del Nord, o ai sensi dell'ordine esecutivo 13382 (Proliferatori di armi di distruzione di massa e loro sostenitori) per attività legate alla Corea del Nord, tale istituzione potrebbe, tra le altre potenziali restrizioni, perdere l'autorizzazione a mantenere un conto corrispondente o un conto per pagamento (PTA, *payable-through account*) negli Stati Uniti.

L'OFAC indaga su apparenti violazioni dei suoi regolamenti sulle sanzioni ed esercita l'autorità esecutiva, così come delineato nelle Linee guida per l'applicazione delle sanzioni economiche, 31 C.F.R. parte 501, appendice A. Coloro che violano i regolamenti sulle sanzioni alla Corea del Nord, 31 C.F.R. parte 510, possono essere soggetti a sanzioni pecuniarie civili fino al maggiore tra la sanzione massima prevista dalla legge e il doppio del valore dell'operazione sottostante.

Inoltre, la legge mirata a contrastare gli avversari degli Stati Uniti tramite l'applicazione di sanzioni (il *Countering America's Adversaries Through Sanctions Act* o CAATSA; Legge Pubblica 115-44) Sezione 321(b) (22 U.S.C. § 9241a) che ha emendato la legge sulle sanzioni contro la Corea del Nord del 2016 (il *North Korea Sanctions and Policy Enhancement Act*) (22 U.S.C. § 9241 e segg.), ha istituito una "*rebuttable presumption*" (*praesumptio iuris tantum*, ovvero presunzione giuridica che ammette una prova contraria) che i beni, i prodotti, le merci e gli articoli importanti estratti, prodotti o fabbricati in tutto o in parte da cittadini nordcoreani in qualsiasi parte del mondo siano beni provenienti dal lavoro forzato di cui è vietata l'importazione ai sensi della legge sulle tariffe del 1930 (*Tariff Act*, 19 U.S.C. § 1307). Ciò significa che tali merci non hanno diritto all'ingresso in nessun porto degli Stati Uniti e possono essere soggette al trattenimento, al sequestro e alla confisca. Le violazioni possono comportare sanzioni civili e penali. Tuttavia, ai sensi della CAATSA, tali beni possono essere importati negli Stati Uniti ove il Commissario alle dogane e alla protezione delle frontiere degli Stati Uniti (CBP, *Customs and Border Protection*) stabilisca, in base a prove chiare e convincenti, che i beni non sono stati prodotti con il lavoro di detenuti o con lavoro forzato o coatto. Il divieto di importazione di beni prodotti con manodopera di detenuti o manodopera forzata o coatta che ricade sotto sanzioni penali (compreso il lavoro minorile forzato o coatto) è stato creato con la Legge sulle tariffe del 1930 e, come tale, è in vigore da quasi 90 anni.

Il Dipartimento della Giustizia è responsabile delle indagini e delle azioni giudiziarie relative alle leggi federali in vigore, tra cui la legge sui poteri economici di emergenza internazionali (IEEPA, *International Emergency Economic Powers Act*), 50 U.S.C. §§ 1701 e segg., e la legge sul segreto bancario (BSA, *Bank Secrecy Act*), 31 U.S.C. §§ 5318 e 5322. Ai sensi dell'IEEPA, è reato violare, tentare di violare, congiurare per violare o causare la violazione di qualsiasi licenza, ordine, regolamento o divieto emesso ai sensi dell'IEEPA, incluso qualsiasi ordine esecutivo che interessi la Corea del Nord (ad esempio, gli ordini esecutivi 13722 e 13810), l'ordine esecutivo 13382 e i regolamenti sulle sanzioni contro la Corea del Nord, 31 C.F.R. parte 510. Chiunque risulti aver deliberatamente violato l'IEEPA rischia fino a 20 anni di reclusione, multe fino a 1 milione di dollari o il doppio del proprio guadagno lordo, qualunque sia la cifra maggiore, e la potenziale confisca di tutti i fondi legati a tali operazioni. La BSA impone alle istituzioni finanziarie, tra le altre cose, di mantenere programmi efficaci contro il riciclaggio di denaro e di inoltrare determinate relazioni al FinCEN. Le persone che violano la BSA rischiano fino a 5 anni di reclusione, multe fino a 250.000 dollari e la confisca dei beni legati a tali violazioni. Le aziende e le altre entità che violano l'IEEPA, la BSA e altre leggi federali pertinenti possono anche essere perseguite penalmente. Il Dipartimento della Giustizia collabora anche con partner stranieri alla condivisione di prove a supporto di indagini e procedimenti penali negli Stati Uniti e all'estero.

Ai sensi del 31 U.S.C. § 5318(k), il Segretario del Tesoro o il Procuratore Generale Federale possono spiccare mandati di comparizione contro istituzioni finanziarie straniere che mantengano un conto bancario corrispondente negli Stati Uniti forzando tale istituzione a consegnare documenti conservati all'estero. Nel caso in cui il Segretario del Tesoro o il Procuratore Generale Federale comunichino per iscritto a un'istituzione finanziaria statunitense che un'istituzione finanziaria estera non ha ottemperato a una tale citazione, l'istituzione finanziaria statunitense è tenuta ad interrompere il rapporto bancario di corrispondenza entro dieci giorni lavorativi. In caso contrario, le istituzioni finanziarie statunitensi potrebbero essere soggette a penali quotidiane di tipo civile.

Rewards for Justice per la Corea del Nord

Se disponete di informazioni su attività illecite della Corea del Nord nel ciberspazio, sia trascorse che attualmente in corso, fornire tali informazioni attraverso il programma *Rewards for Justice* del Dipartimento di Stato potrebbe darvi diritto a ricevere un premio di fino a 5 milioni di dollari. Per maggiori informazioni, visitare https://rewardsforjustice.net/index/?north-korea=north-korea.

ALLEGATO

Relazione del Gruppo di esperti delle Nazioni Unite sui lavoratori informatici della Repubblica Popolare Democratica di Corea

Il Comitato sanzioni 1718 del Consiglio di Sicurezza dell'ONU sulla Repubblica Popolare Democratica di Corea (la Corea del Nord) si avvale di un gruppo di esperti (il Gruppo) che raccoglie, esamina e analizza le informazioni provenienti dagli Stati membri dell'ONU, dagli organismi ONU competenti e da altre parti sull'attuazione delle misure delineate nelle risoluzioni del Consiglio di Sicurezza dell'ONU relative alla Corea del Nord. Il Gruppo formula anche raccomandazioni su come rendere più efficace l'esecuzione delle sanzioni, fornendo una relazione intermedia ed una finale al Comitato 1718. Questi rapporti sono reperibili al seguente indirizzo: https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports

Il Gruppo ha indagato su molteplici casi di lavoratori informatici della Corea del Nord, come ad esempio quelli dipendenti dal Dipartimento dell'industria delle munizioni (MID, *Munitions Industry Department*), designato dalle Nazioni Unite, e ha presentato informazioni su queste indagini nelle relazioni semestrali del Gruppo, compreso quanto segue:

Il Gruppo ha riferito per la prima volta sui lavoratori informatici nordcoreani nel Rapporto intermedio del 2019, facendo notare che il MID, che era stato designato per il suo ruolo di supervisione nello sviluppo dei programmi nucleari e di missili balistici nordcoreani, utilizzava le sue società commerciali subordinate per dislocare all'estero lavoratori informatici nordcoreani in qualità di programmatori e sviluppatori di software, al fine di generare introiti in valuta estera. All'epoca, i lavoratori informatici nordcoreani dislocati in Europa, Asia, Africa e Medio Oriente utilizzavano siti web stranieri per ottenere lavori freelance dissimulando la propria identità. Oltre al lavoro informatico legittimo, essi svolgevano attività dolose fra cui il furto di beni come ad esempio le valute virtuali, a sostegno di agenti cibernetici nordcoreani tesi ad evadere le sanzioni finanziarie.

Il Gruppo ha proseguito le indagini sui lavoratori informatici nordcoreani nella Relazione finale 2020, riscontrando che la maggior parte di quelli dislocati all'estero sono impiegati da aziende che dipendono dal MID. Si sospetta che, al 2019, il MID abbia inviato almeno mille di questi tecnici all'estero allo scopo di generare introiti, spesso servendosi di entità subordinate o società di comodo. Tuttavia, a causa delle loro tecniche di occultamento, non era chiaro il numero reale di questi tecnici dislocati all'estero o impiegati nel loro Paese. Il Gruppo ha fatto notare che i tecnici IT nordcoreani si servono di vari metodi per ottenere contratti di lavoro freelance senza rivelare la propria identità, tra cui la creazione di account su piattaforme per sviluppatori freelance con clienti inconsapevoli in tutto il mondo, soprattutto in Cina, Russia, Ucraina, Serbia, Canada e Stati Uniti. Il Gruppo ha inoltre analizzato diversi casi specifici di team di tecnici IT nordcoreani e di aziende associate in Cina, Nepal e Vietnam.

Il Gruppo ha indagato su un certo numero di questi team in Cina e in Russia, descrivendo in dettaglio le indagini nella Relazione intermedia 2020. Il Gruppo ha rilevato che centinaia di questi lavoratori subordinati al MID operavano in Cina nel 2019 e nel 2020 e accedevano illecitamente ad account sulle piattaforme per freelance a nome di persone di Paesi terzi. Il Gruppo di esperti ha inoltre notato che diversi gruppi di questi tecnici subordinati al MID operavano in Russia nel 2019 e nel 2020 con false identità straniere che permettevano loro di accedere a piattaforme per freelance IT, siti web di valuta virtuale e siti web per i pagamenti.

Secondo la Relazione finale 2021 del Gruppo di esperti, questi lavoratori sono in grado di eludere gli sforzi di dovuta verifica dei datori di lavoro e i protocolli KYC/AML impiegando metodi di depistaggio simili a quelli utilizzati dalla Corea del Nord per accedere al sistema finanziario internazionale, tra cui la presentazione di identificativi falsi, l'uso di servizi VPN e la creazione di società di comodo. Il Gruppo ha inoltre notato che la maggior parte degli account collegati alla Corea del Nord operano da sedi ubicate in Cina. Per evitare i controlli, questi account vanno "fuori sede" dopo aver stabilito un contatto con i potenziali clienti di servizi informatici. Gli utenti legati alla Corea del Nord si avvalgono anche di piattaforme per lavoro freelance IT con livelli di sicurezza inferiori o procedure di dovuta verifica meno rigorose. Il Gruppo ha evidenziato in modo specifico i pericoli che corrono queste piattaforme nell'adempimento degli obblighi di conformità e nel facilitare involontariamente l'accesso della Corea del Nord ai sistemi di pagamento internazionali, raccomandando agli Stati membri dell'ONU di collaborare con le aziende informatiche per freelance al fine di promuovere e migliorare la capacità e le competenze in materia di osservanza delle sanzioni.