MERIDIAN GROUP

# **Weekly** *Report*

27/01/2025

**TLP: WHITE**

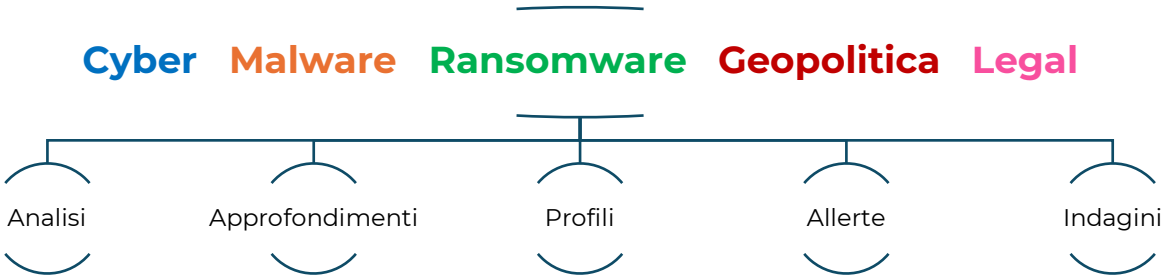
**MERIDIAN S.R.L**

Viale Erminio Spalla, 9-00142 Roma (RM) | +39 06 99 70 66 80 | P.IVA/CF 13693001003 | meridiangroup@legalmail.it | info@meridian-group.eu | www.meridian-group.eu | 

# Sommario

# Metodologie e Risorse

Il team di *Cyber Intelligence* (CI) utilizza i seguenti metodi e risorse per l'analisi delle notizie e per l'acquisizione di informazioni utili al contenimento degli attacchi informatici.




Il Team di CI, attraverso questo report settimanale, mira a fornire analisi tempestive e accurate riguardo alle aree, di cui sopra, consentendo ai lettori di essere a conoscenza delle ultime notizie riguardanti nuove vulnerabilità, potenziali minacce e cambiamenti nello scenario geopolitico.

L'analisi giornaliera delle notizie sulla piattaforma Kitsune è essenziale per gli analisti di CI al fine di monitorare e comprendere i rischi emergenti nelle diverse categorie, sopra esposte, consentendo così di prevenire o mitigare le potenziali minacce alla sicurezza dei clienti.

CYBER

# Il nome del Ministero della Salute utilizzato per frodi informatiche

È stata individuata una **campagna di phishing**, attualmente in corso, la quale sfrutta il logo e il nome del **Ministero della Salu**te con l'intento di indurre le vittime a fornire illecitamente dati personali e finanziari.

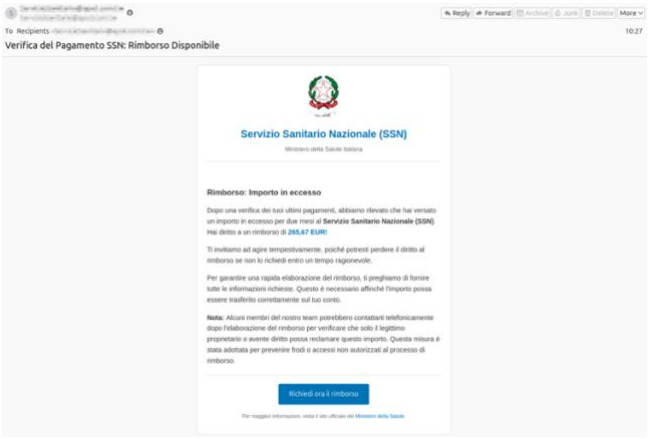



*Figura 1 - Email utilizzata per la campagna di phishing*

Attraverso l'invio di email gli utenti sono invitati a cliccare su un collegamento che li reindirizza a una pagina web contraffatta. In tale pagina, è richiesto di **inserire dati personali e i dettagli della carta di credito** al fine di ottenere un **presunto rimborso** pari a €265,67 da parte del Servizio Sanitario Nazionale.

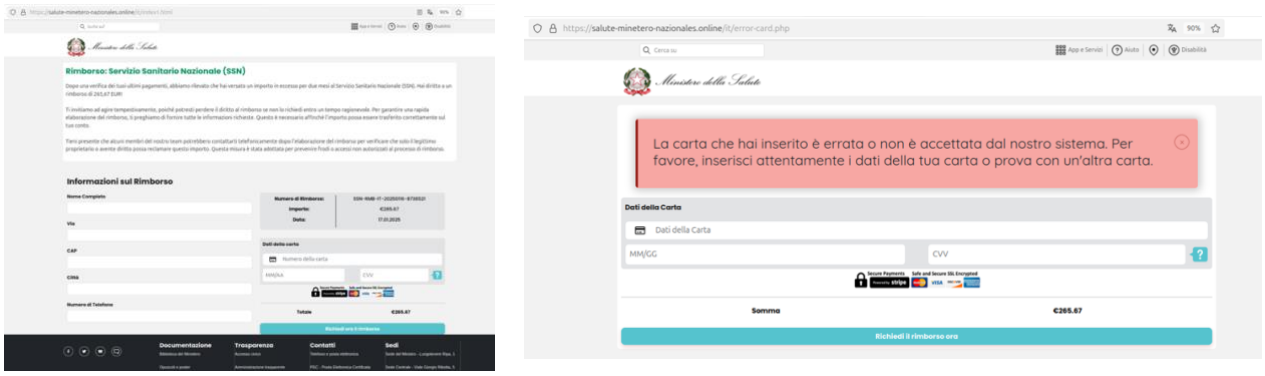



*Figura 2 - Pagina di richiesta inserimento dati personali*

Una volta compilati i campi richiesti, la vittima è ulteriormente indirizzata a una seconda pagina, in cui le viene fraudolentemente richiesto di inserire nuovamente i dati della carta di credito. Tale strategia, orchestrata dai cybercriminali, mira sia a ridurre il rischio di errori di digitazione sia a ottenere, qualora possibile, i dati di una seconda carta di credito.

GEOPOLITICA

# Elon Musk, polemica sui gesti durante l'insediamento di Trump: "gesto nazista o simbolo di entusiasmo?"

Durante i festeggiamenti per **l'insediamento del presidente Donald Trump**, avvenuti lunedì 20 gennaio, Elon Musk ha compiuto un gesto con la mano che ha suscitato un acceso dibattito online. Alcuni utenti lo hanno **paragonato al saluto nazista**, ma **l'Anti-Defamation League**, che monitora l'antisemitismo, ha respinto l'accusa, descrivendolo come un **gesto entusiasta e imbarazzante**, non collegato a simbologie estremiste. Musk ha liquidato le critiche definendole "un attacco stanco" e privo di fondamento.

Sul palco della Capital One Arena di Washington, accolto da applausi fragorosi, Musk ha esordito ringraziando il pubblico per il supporto e sottolineando l'importanza del momento: "Questa non è stata una vittoria ordinaria. È stato un bivio sulla strada della civiltà umana". Nel corso del discorso, si è battuto la mano sul cuore con le dita aperte, poi ha teso il braccio destro verso l'alto con il palmo rivolto verso il basso, un gesto ripetuto verso la folla dietro di lui, accompagnato dalla frase: "**Il mio cuore è con voi. È grazie a voi che il futuro della civiltà è assicurato**".

Il gesto ha subito attirato l'attenzione, con il *Jerusalem Post* che ha domandato ironicamente se Musk avesse fatto il "Sieg Heil" durante l'evento. La **presidente della comunità ebraica** di Monaco e dell'Alta Baviera, Charlotte Knobloch, ha definito il **gesto "altamente irritante"**, ma ha evidenziato che le sue **preoccupazioni principali riguardano le posizioni politiche di Musk.** Musk, infatti, ha espresso il suo s**ostegno all'estrema destra tedesca di Alternative für Deutschland (AfD)**, un partito anti-immigrazione e antislamico classificato come estremista di destra dai servizi di sicurezza tedeschi. Musk ha persino ospitato una trasmissione con il leader del partito sulla sua piattaforma di social media X.

In risposta alle critiche, Musk ha ribattuto ironicamente: "Francamente, hanno bisogno di trucchi sporchi migliori. L'attacco 'tutti sono Hitler' è passato". Dopo il suo intervento, ha condiviso su X un video del discorso, definendo il futuro "eccitante". Alcuni utenti della piattaforma si sono schierati in sua difesa, sostenendo che il gesto rappresentava un sincero "il mio cuore è con te", e criticando chi lo ha interpretato diversamente.

GEOPOLITICA

# Trump tra isolazionismo e polemiche: ritiro da OMS e accordo di Parigi e tensioni con la Cina

Nel suo primo giorno di ritorno alla Casa Bianca, Donald Trump ha intrapreso una serie di **azioni esecutive** che hanno avuto un impatto immediato sia a livello interno sia internazionale. Sul fronte interno, ha firmato provvedimenti per **limitare l'immigrazione**, **revocare normative ambientali** e **ridurre iniziative sulla diversità razziale e di genere**, oltre a **concedere la grazia a circa 1.500 suoi sostenitori coinvolti nell'attacco al Campidoglio** del 2021.

A livello internazionale, Trump ha annunciato il **ritiro degli Stati Uniti dall'Organizzazione Mondiale della Sanità (OMS)**, accusando l'agenzia di una cattiva gestione della pandemia di COVID-19 e di essere influenzata dalla Cina. Pechino ha criticato questa decisione, sottolineando l'importanza di rafforzare la governance sanitaria globale.

Inoltre, Trump ha firmato un ordine esecutivo che **ritira gli Stati Uniti nuovamente dall'Accordo di Parigi sul clima**, collocando così gli USA tra i pochi paesi che non aderiscono al patto globale per limitare il riscaldamento globale. Tale gesto ha suscitato preoccupazione a livello internazionale, con la presidente della Commissione Europea, Ursula Von Der Leyen, che ha ribadito l'impegno dell'Europa nel contrasto al cambiamento climatico: *"L'Accordo di Parigi rappresenta la migliore speranza per l'umanità."*

Anche la Cina ha espresso preoccupazione per il ritiro di Trump dagli accordi sul clima. Il portavoce del ministero degli Esteri cinese, Guo Jiakun, ha sottolineato che la Cina è fortemente impegnata nella risposta alla crisi climatica e continuerà a promuovere la transizione energetica a livello globale. Inoltre, Guo ha aggiunto che il ruolo dell'Organizzazione Mondiale della Sanità (OMS) "dovrebbe essere solo rafforzato, non indebolito", esprimendo il sostegno della Cina all'agenzia sanitaria globale, nonostante l'ordine esecutivo che prevede il ritiro degli Stati Uniti dall'OMS.

Sul piano commerciale, Trump ha dichiarato l'intenzione di **intensificare la politica dei dazi**, minacciando **tariffe del 25% su Canada e Messico**, mentre ha lasciato intendere che nuove misure contro la Cina potrebbero essere introdotte. Le tensioni con Pechino restano elevate, alimentate dalle dispute commerciali e dal controllo su aziende come TikTok.
Il ritorno di Trump alla presidenza sottolinea una politica estera caratterizzata da isolazionismo e scetticismo verso la cooperazione internazionale, con un impatto significativo sugli equilibri globali e sulle relazioni con i principali partner economici e politici.

CYBER LEGAL

# Star Blizzard sfrutta WhatsApp per raccogliere dati sensibili: la risposta giuridica internazionale

Il **gruppo di hacker russi Star Blizzard** ha recentemente preso di mira gli **account WhatsApp di alti funzionari governativi e diplomatici** in vari paesi, utilizzando una tecnica di phishing sofisticata. Le vittime ricevevano email apparentemente inviate da funzionari statunitensi, con un invito a unirsi a **gruppi WhatsApp per supportare iniziative umanitarie in Ucraina**. L'email conteneva un codice QR che, se scansionato, permetteva agli hacker di collegarsi agli account WhatsApp delle vittime e accedere ai loro messaggi, raccogliendo informazioni sensibili.


Suddetto attacco è un esempio di come i gruppi di **hacker sponsorizzati dallo stato possano evolversi**, passando da tecniche di spear phishing più tradizionali a metodi più sofisticati, mirati a piattaforme di comunicazione sicure come WhatsApp, spesso utilizzate per scambi riservati da diplomatici e funzionari governativi. Sebbene WhatsApp utilizzi la crittografia end-to-end, l'attacco ha evidenziato la **vulnerabilità degli account** quando gli utenti interagiscono con link o codici malevoli.

Tale attacco solleva **importanti questioni giuridiche**, in particolare riguardo alla **protezione dei dati e alla sicurezza delle comunicazioni**. Per le vittime risiedenti nell'Unione Europea, l'incidente potrebbe configurarsi come una **violazione del GDPR**, che impone rigorosi obblighi sulla protezione dei dati personali. Inoltre, l'intrusione nelle comunicazioni ufficiali dei funzionari può essere interpretata come una violazione della sovranità digitale degli Stati. Quando gli attacchi sono sponsorizzati da Stati, la situazione giuridica diventa ancora più complessa, poiché il **diritto internazionale non sempre fornisce risposte chiare per l'attribuzione di responsabilità**. Le possibili reazioni giuridiche includono sanzioni internazionali, ma attribuire la responsabilità a uno Stato specifico resta una questione difficile sia sul piano legale che politico.

GEOPOLITICA 

# Huawei sfida Nvidia: espansione nel mercato cinese dei chip per l'intelligenza artificiale

**Huawei punta a espandere la propria presenza nel mercato cinese dei chip per l'intelligenza artificiale, attualmente dominato da Nvidia**, incoraggiando le aziende locali a utilizzare i suoi processori Ascend per le attività di "inferenza". Le principali aziende cinesi nel campo dell'IA si affidano tradizionalmente alle GPU di Nvidia per l'addestramento di modelli linguistici di grandi dimensioni, considerandole essenziali per lo sviluppo tecnologico.

Tuttavia, anziché competere con Nvidia nell'addestramento, Huawei sta promuovendo i suoi processori Ascend come la **soluzione ideale per l'inferenza**, ovvero i calcoli utilizzati dai modelli linguistici per generare risposte. L'azienda ritiene che l'inferenza diventerà una componente fondamentale della domanda futura, soprattutto se il ritmo dell'addestramento rallenterà e le applicazioni di IA, come le chatbot, diventeranno sempre più diffuse. Huawei sta seguendo una strategia meno complessa dal punto di vista tecnico ma potenzialmente redditizia, lavorando per rendere **compatibili i modelli di IA addestrati con GPU Nvidia con i suoi chip Ascend**. Poiché i due processori utilizzano software differenti, Huawei ha sviluppato strumenti che garantiscono la compatibilità tra i sistemi, semplificando la transizione per le aziende.

**L'iniziativa è sostenuta anche dal governo cinese**, che ha invitato i giganti tecnologici locali ad acquistare i chip Huawei, riducendo la dipendenza da Nvidia. Secondo fonti vicine a Nvidia in Cina, Huawei è considerata il concorrente più serio nel mercato interno, grazie alle sue avanzate capacità di progettazione. Le **restrizioni all'esportazione degli Stati Uniti limitano l'accesso delle aziende cinesi alle GPU più potenti**. Sebbene **Nvidia fornisca in Cina i suoi chip H20, meno avanzati per conformarsi alle normative**, questi sono ancora molto richiesti, superando le alternative locali in termini di prestazioni.

Nonostante ciò, i chip Ascend di Huawei non sono ancora pronti per competere nell'addestramento di modelli di grandi dimensioni. Problemi tecnici, come la connessione tra chip in cluster più ampi, rappresentano un ostacolo significativo. "I chip Ascend funzionano bene singolarmente, ma ci sono limiti nella connettività tra di essi" ha spiegato Lin Qingyuan, analista di semiconduttori presso Bernstein. Un'altra sfida è convincere gli sviluppatori a migrare dal software Cuda di Nvidia, considerato uno standard per l'efficienza e la semplicità d'uso. Tuttavia, Huawei prevede di superare questo ostacolo con l'imminente lancio del **chip Ascend 910C**, che dovrebbe includere aggiornamenti significativi sia hardware che software.

Oltre a Huawei e Nvidia, anche altre aziende cinesi, come **Baidu** e **Cambricon**, stanno investendo nello sviluppo di chip per l'IA. Nel frattempo, negli Stati Uniti, colossi come Amazon e Microsoft cercano di guadagnare terreno nei chip per l'inferenza. Secondo SemiAnalysis, Nvidia ha registrato un fatturato di 12 miliardi di dollari in Cina nel 2023, vendendo un milione di chip H20, il doppio rispetto ai chip Ascend 910B di Huawei. Tuttavia, Huawei sta colmando il divario aumentando rapidamente la capacità produttiva. "Il vantaggio di Nvidia si sta riducendo, ma Huawei deve ancora affrontare problemi di offerta limitata" ha aggiunto Dylan Patel, analista capo di SemiAnalysis.

**Le restrizioni statunitensi hanno spinto le aziende cinesi a concentrarsi sull'inferenza**, un settore dove è possibile ottenere grandi miglioramenti in termini di efficienza anche utilizzando chip meno potenti. Ad esempio, la start-up cinese DeepSeek ha recentemente presentato il modello V3, che si distingue per costi di addestramento e inferenza più bassi, e inoltre ha collaborato con Huawei per adattare il proprio modello ai chip Ascend, fornendo supporto tecnico agli sviluppatori.

Nonostante le difficoltà, Huawei continua a investire nell'espansione del mercato dei chip per l'inferenza, puntando a soddisfare una domanda crescente di soluzioni più economiche ed efficienti. Tale strategia potrebbe ridefinire il panorama tecnologico in Cina, rafforzando ulteriormente la sua indipendenza dai colossi occidentali.

RANSOMWARE

# Attacchi ransomware: i cybercriminali russi sfruttano Microsoft teams con nuove tecniche di frode

I criminali informatici russi stanno adottando un nuovo schema fraudolento che prevede di **spacciarsi per operatori del supporto tecnico su Microsoft Teams**. Con questa tecnica, convincono le vittime di avere un problema informatico, per poi indurle a consentire l'installazione di ransomware sulle reti informatiche delle loro aziende.

La società britannica di cybersicurezza Sophos ha identificato oltre 15 episodi in cui due gruppi distinti hanno sfruttato le **impostazioni predefinite dei servizi Microsoft Office 365 per introdursi nei sistemi delle vittime attraverso tecniche di ingegneria sociale**. Uno di suddetti gruppi presenta connessioni con il gruppo noto come **Storm-1811**, già identificato da Microsoft per operazioni simili a quella in corso. L'altro gruppo, che sembra emulare le tattiche di Storm-1811, potrebbe essere legato al gruppo criminale **FIN7**.

Le nuove campagne sono state scoperte durante le indagini su alcuni casi di **malware BeaverTail**, legati ad attacchi di attori nordcoreani, che fingendosi da reclutatori su piattaforme di ricerca lavoro, inducendo le vittime a scaricare malware per sottrarre criptovalute dai dispositivi, ma gli attacchi russi presentano caratteristiche completamente diverse dal modus operandi nordcoreano, sia per il tipo di malware impiegato sia per la tipologia delle vittime.

Un episodio emblematico è avvenuto durante il giorno delle elezioni negli Stati Uniti. Due dipendenti di un'azienda hanno ricevuto un'enorme quantità di e-mail in breve tempo. Uno di loro, lavorando da remoto, è stato poi contattato tramite una **chiamata Teams da un presunto responsabile del supporto tecnico**, che ha avviato l'attacco.

I due gruppi criminali sfruttavano i propri tenant di Microsoft Office 365 per attuare gli attacchi, approfittando di una **configurazione predefinita di Microsoft Teams che consente agli utenti di domini esterni di avviare chat o riunioni con utenti interni**. In alcuni casi, i criminali hanno effettuato chiamate vocali o video tramite Teams; in altri, hanno inviato messaggi di testo contenenti link che conducevano a strumenti per ottenere il controllo remoto del dispositivo della vittima. Per questa fase, gli attaccanti hanno utilizzato strumenti Microsoft come **QuickAssist** o la funzione di condivisione dello schermo di Teams.

Un altro attacco significativo si è verificato quando il falso operatore di supporto ha convinto un dipendente a consentire **una sessione di controllo remoto**. L'attaccante ha così aperto un terminale di comando, caricato file e avviato malware, tra cui un archivio Java (JAR) e un file .zip contenente codice Python. Suddetti metodi, pur sofisticati, si basano su codice liberamente disponibile online, e che strumenti utilizzati da gruppi come FIN7 sono stati venduti ad altri criminali informatici.

GEOPOLITICA

# Terrorismo, arrestato a Napoli 30enne affiliato all'ISIS: progetti violenti contro la comunità ebraica

Mercoledì 20 gennaio a Napoli, un cittadino di origini marocchine di 30 anni è stato **arrestato con l'accusa di associazione a scopo di terrorismo internazionale** e di eversione dell'ordine democratico. L'operazione è stata il risultato di complesse indagini coordinate dal gruppo antiterrorismo della procura partenopea, che hanno consentito di identificare l'uomo e di ricostruire il suo **legame con l'ISIS**. Durante l'inchiesta, che ha incluso accertamenti anche sul web, sono stati effettuati sequestri e perquisizioni nei confronti di altri individui ritenuti collegati all'arrestato.

Secondo quanto emerso, il giovane aveva aderito all'ideologia dell'Isis, impegnandosi nella **diffusione e nell'apologia di materiale propagandistico** e multimediale riconducibile al contesto terroristico, incluso materiale utilizzato per addestramento. Gli investigatori hanno inoltre accertato che il trentenne aveva manifestato **intenzioni violente, in particolare contro la comunità ebraica di Napoli**, e aveva espresso la volontà di procurarsi un coltello per realizzare i suoi progetti terroristici.

Il provvedimento cautelare è stato emesso dal giudice per le indagini preliminari di Napoli, su richiesta dell'ufficio della procura guidato dal procuratore Nicola Gratteri. L'arresto rappresenta un'importante operazione nell'ambito del contrasto al terrorismo internazionale e alla radicalizzazione violenta.

CYBER GEOPOLITICA

# Iran e Russia rafforzano la cooperazione nel cyberspazio con un nuovo accordo strategico

Iran e Russia hanno siglato un **accordo** volto a **rafforzare i legami tra i due Paesi nei settori militare e delle tecnologie**. L'accordo, tra le nazioni più sanzionate al mondo, mira ad elevare le relazioni bilaterali a un livello superiore, come sottolineato dal Cremlino. In particolare, alcune clausole si concentrano sulla **cooperazione in cybersicurezza** e **sulla regolamentazione di internet**.

Nel corso degli anni, la Russia ha firmato trattati simili con altri Paesi, come Cina e Corea del Nord, per condividere esperienze nel campo delle tecnologie dell'informazione e dello sviluppo digitale. L'accordo firmato a Mosca dai presidenti Vladimir Putin e Masoud Pezeshkian prevede **l'espansione della cooperazione nel contrasto all'uso illecito delle tecnologie dell'informazione e della comunicazione**. Inoltre, i due Paesi hanno concordato uno **scambio di competenze nella gestione delle rispettive reti nazionali** e hanno preso l'impegno di promuovere una **regolamentazione più severa del cyberspazio**, con l'obiettivo di creare norme per le aziende tecnologiche internazionali.

Sia in Russia sia in Iran, **internet** è considerato **"non libero"**, a causa di una **forte censura**, **campagne di disinformazione**, **sorveglianza e pene per le opinioni espresse online**. La Russia ha infatti tentato a lungo di limitare l'accesso alla rete globale per ottenere un controllo maggiore su internet, recenti sforzi che hanno incluso il **blocco di app e siti web** e il **test del cosiddetto "internet sovrano"**. Anche l'Iran ha adottato politiche simili, rendendo l'accesso a internet internazionale più difficile e costoso, orientando gli utenti verso una versione nazionale della rete, dove le autorità possono monitorare e controllare i contenuti con maggiore efficacia.

L'accordo tra Russia e Iran non impone obblighi vincolanti, ma formalizza i legami già esistenti tra i due Paesi, con disposizioni in materia di sicurezza simili a quelle contenute in un trattato precedente del 2021. Quest'ultimo, entrato in vigore nel 2022, si concentrava sulla cooperazione in cybersicurezza, nella prevenzione del crimine informatico e nell'impegno reciproco a non attaccarsi nel cyberspazio. Nel 2023, il ministero digitale russo, insieme a importanti aziende tecnologiche locali come Rostelecom-Solar e Positive Technologies, ha incontrato il ministero delle comunicazioni e della tecnologia iraniano per discutere di esportazione di tecnologia russa e di collaborazioni in cybersicurezza. Inoltre, il portavoce della Commissione per la Sicurezza Nazionale dell'Iran ha confermato che la Russia sta contribuendo attivamente alla cybersicurezza dell'Iran, un segno tangibile della crescente collaborazione tra i due Paesi in questo settore.

GEOPOLITICA CYBER

# Trump firma un ordine esecutivo sulle criptovalute: nuove regolamentazioni, riserva nazionale digitale e divieto delle CBDC

Il 23 gennaio, il Presidente degli Stati Uniti Donald Trump ha firmato un **ordine esecutivo** per istituire un **gruppo di lavoro dedicato alle criptovalute** che avrà il compito di **elaborare nuove regolamentazioni per gli asset digitali** e di **valutare la possibilità di creare una riserva nazionale di criptovalute**. L'iniziativa rappresenta un primo passo concreto verso la riforma della politica statunitense sulle criptovalute, come promesso da Trump durante la sua campagna elettorale.

L'ordine esecutivo include anche misure per garantire **l'accesso ai servizi bancari da parte delle aziende del settore**, rispondendo alle denunce secondo cui i regolatori statunitensi avrebbero spinto le banche a interrompere i rapporti con queste società, accuse che le autorità negano. Inoltre, è stato imposto il **divieto di creare valute digitali delle banche centrali (CBDC) negli Stati Uniti**, per evitare che possano competere con le criptovalute già esistenti.

Un altro importante passo a favore dell'industria delle criptovalute è arrivato dalla **Securities and Exchange Commission (SEC)**, che ha revocato alcune direttive contabili considerate troppo onerose per le aziende quotate incaricate di custodire criptovalute per conto di terzi. Secondo i rappresentanti del settore, queste norme avevano ostacolato la diffusione degli asset digitali.

Trump, che durante la campagna elettorale si era definito **"il Presidente delle criptovalute**", ha adottato un approccio diametralmente opposto rispetto all'amministrazione Biden. Quest'ultima aveva intrapreso azioni legali contro diverse piattaforme, tra cui Coinbase e Binance, per presunte violazioni delle leggi statunitensi, accuse sempre respinte dalle aziende coinvolte.

L'ordine esecutivo di Trump è stato accolto con entusiasmo dal settore, che da tempo chiedeva un segnale chiaro di sostegno. *"Questo ordine segna un cambiamento epocale nella politica statunitense sugli asset digitali"* ha dichiarato Nathan McCauley, CEO e co-fondatore di Anchorage Digital. *"L'approccio globale e coordinato adottato dall'amministrazione rappresenta un passo significativo verso l'introduzione di regole chiare e coerenti per il settore".*

Gli esperti di regolamentazione ritengono che, se pienamente implementato, il provvedimento possa spingere le criptovalute verso una maggiore accettazione mainstream. L'iniziativa segue l'annuncio della SEC di una task force dedicata alla revisione della normativa sulle criptovalute.

L'entusiasmo per **l'amministrazione pro-cripto** si è riflesso anche sui mercati: **lunedì il Bitcoin ha raggiunto un nuovo record di 109.071 dollari, chiudendo giovedì a circa 103.000 dollari**. *"Con pochi giorni dall'inizio del suo mandato, il*

*Presidente Trump sta mantenendo le sue promesse, assicurando che gli Stati Uniti restino leader nell'innovazione digitale",* ha dichiarato Tim Scott, senatore repubblicano e presidente della Commissione Bancaria del Senato.

Da anni, il settore chiede una revisione delle normative, giudicate inadeguate per gli asset digitali. Secondo l'ordine esecutivo, il gruppo di lavoro, che includerà il **Segretario al Tesoro**, i **vertici della SEC e della Commodity Futures Trading Commission**, nonché altri rappresentanti di alto livello, sarà incaricato di definire un **quadro normativo chiaro per le criptovalute**, incluse le stablecoin, generalmente ancorate al valore del dollaro.

Tra i compiti del gruppo rientra anche la valutazione della **creazione di una riserva nazionale di asset digitali**, **composta da criptovalute confiscate legalmente dal governo federale**. Tuttavia, non sono stati forniti ulteriori dettagli sulle modalità di costituzione di questa riserva. Gli analisti sono divisi sulla necessità di un intervento del Congresso, sebbene alcuni ritengano che la riserva possa essere istituita tramite il Fondo di Stabilizzazione del Cambio del Tesoro, già utilizzato per acquistare e vendere valute estere e, potenzialmente, per detenere Bitcoin.