di Roberto Russo*

IL SEQUESTRO DI CRIPTOVALUTE NEL CORSO DELL'ESECUZIONE DI PROVVEDIMENTI CAUTELARI REALI: la modalità operativa

Le criptovalute, o cryptocurrency, sono dei valori sequestrabili nel corso di provvedimenti ablativi, al pari di immobili, denaro e altre disponibilità. Ma mentre sappiamo benissimo cosa fare quando si parla di immobili, preziosi o disponibilità liquide, se si è di fronte alle criptovalute resta il dubbio di come operare il sequestro e come cautelare la riservatezza delle operazioni. Ovviamente per brevità espositiva non si potranno spiegare le nozioni fondamentali dell'universo crypto, rimandando il lettore/operatore per gli approfondimenti nozionistici alle numerosissime guide disponibili in rete. Verrà trattata la parte pratica relativa al sequestro, ipotizzando un caso generico nel quale si individui un wallet.

COSA CERCARE IN UNA PERQUISIZIONE

Le monete virtuali sono normalmente custodite in wallet[1] (letteralmente portafogli digitali), suddivisi principalmente in *hard e soft wallet*. I wallet sono soluzioni per l'amministrazione di più indirizzi che permettono d'inviare e ricevere transazioni indipendentemente dagli indirizzi in essi contenuti. Gli indirizzi sono invece le singole unità di accumulo e di trasferimento dei bitcoin. In altre parole, un indirizzo può essere visto come un codice IBAN bancario, che può ricevere somme da terzi e trasferirne verso terzi. Un wallet è un insieme di codici IBAN gestiti tutti dalla stessa piattaforma, che permette di abbinare più codici IBAN per generare transazioni complesse e con cifre che superano, ad esempio la disponibilità di un singolo conto bancario.
Ogni transazione ha almeno un indirizzo di destinazione, non riservato, consistente in una stringa alfanumerica di lunghezza compresa tra i 25 e i 34 caratteri, utilizzabile per ricevere *criptovalute* e dal quale le stesse possono essere inviate, il cui primo carattere è l'1 o il 3 o bc1. Per poter eseguire le transazioni è necessario disporre della chiave privata associata all'indirizzo (come fosse una password) ed è l'unico modo per gestirlo. La chiave privata si presenta

come un numero a 256 bit (256 caratteri che possono essere 0 e 1), e può essere espressa in vari formati, come quello esadecimale, con 64 cifre da 4 bit ciascuna. La chiave privata può essere trasformata in un insieme di 12 o 24 parole (SEED), scelte da un vocabolario di 2048 parole in lingua inglese[2] in cui ognuna occupa un posto determinato. Il numero di possibili combinazioni è pertanto 2048 elevato alla 12esima o alla 24esima. Se quindi nella perquisizione troviamo un elenco di 12 o 24 parole….. occhio perché avremo in mano il sacro graal.

Per *hard* (come hardware) *wallet* si intendono contenitori rigidi dove archiviare le chiavi private. Questi dispositivi sono resistenti agli attacchi informatici poiché le chiavi private non sono mai esposte direttamente alla rete internet. Possono anche essere analogici, ovvero custodie rigide che non necessitano di essere connesse. All'interno, specie di quelli rigidi, sarà conservato il seed o la chiave privata sotto forma di numero. Lo svantaggio è che una volta trovate da terzi danno libero accesso, al contrario di quelle digitali su supporto che possono essere protette con un codice[3]. Si possono citare i paper wallet, semplici fogli di carta su cui sono stampati la chiave privata e il corrispondente indirizzo pubblico o supporti durevoli come quello in foto, in materiali resistenti come acciaio o metalli vari per resistere anche a incolumità. Esistono poi anche pendrive usb che conservano le chiavi private degli indirizzi gestiti. Normalmente sono abbinati a client software che consentono all'utente di gestire le proprie monete. Quando si dovesse avere bisogno di inviare una transazione, questa sarà generata dal client, inviata al dispositivo che la firmerà senza rivelare o condividere la chiave privata né con il computer a cui è collegato né con l'utente e la restituirà al client che potrà occuparsi di propagarla nella rete delle criptovalute.

Esempi di hard wallet

Per *soft* (come software) *wallet* si intende un tipo di wallet crittografico archiviato localmente all'interno del desktop o del disco rigido del computer. Un *wallet software* (mobile, desktop, online) è un programma che può essere scaricato da Internet per archiviare le chiavi. Questi wallets sono generalmente molto economici rispetto ai wallets hardware e, in alcuni casi, possono essere gratuiti. Sebbene siano molto economici, sono suscettibili agli hacker online poiché questi wallets sono collegati con un PC o uno smartphone collegato a sua volta alla rete Internet.

COME PROCEDERE AL SEQUESTRO

Il primo passo è *predisporre un paper wallet* per una criptomoneta da scegliere e i token derivati, da utilizzare per depositarvi le disponibilità di monete virtuali rinvenute nell'ambito dell'attività di P.G: eseguita nei confronti della parte. I passi potrebbero essere, a titolo esemplificativo, sul pc dell'operatore:

• **Avvio di una distribuzione Linux Tsurugi in modalità live**. Tale distribuzione di cui all'indirizzo https://tsurugi-linux.org è stata appositamente ideata per attività di Digital Forensic and Incident Respons (DFIR), le attività di perizia informatica svolte dai consulenti e dagli esperti informatici forensi delle forze di polizia. Nella distribuzione, ideata da due italiani, si possono trovare già installati interessanti tools tra cui bitaddress.otg, mediante il quale è possibile generare un paper wallet. Il fine di una distribuzione forense, come si legge nella presentazione della stessa, è : "*fornire un ambiente di lavoro predisposto per attività operative di acquisizione forense e di analisi, con gli strumenti testati, aggiornati e pre-configurati in modo tale da non richiedere procedure di installazione e, se possibile, con le proprietà di write-blocking atte a non impattare su eventuali dispositivi esistenti sul Pc su cui si opera o connessi successivamente*". L'avvio in modalità live permette l'esecuzione del sistema operativo senza richiederne l'istallazione, caricando le informazioni necessarie nella memoria RAM così da non permettere al s.o. di tenere traccia delle operazioni eseguite dopo lo spegnimento.

• **Connessione alla rete internet del dispositivo per permettere il download e l'istallazione del componente aggiuntivo** dedicato per le criptovalute sulle quali si opera. Ad esempio, in caso di Ethereum il client deputato ad operare alla gestione dei token operativi su tale blockchain è "Metamask";
• **Disattivazione delle connessioni del dispositivo**, al fine di evitare la comunicazione di dati sensibili, anche inconsapevolmente. E' importante in questa fase escludere sia collegamenti fisici, come cavi Lan, che Wireless (bt, wi-fi). Ove l'ambiente di lavoro fosse compromesso non vi sarebbe comunque perdita di dati;
• **Creazione di un nuovo wallet**, casuale, univoco e non replicabile, ottenendo un seed di 12 parole (o 24) e un indirizzo pubblico;
• **Annotazione dell'indirizzo pubblico su un documento di testo**;
• **Trascrizione del paper wallet**, contenente il seed generato e non replicabile, subito riposto all'interno di una busta non trasparente opportunamente cautelata per evitare che si possa vedere all'interno;
• **Cautela della busta secondo le ordinarie prassi** (sigilli, carta vergatina, fili piombati) apponendo timbro del reparto e firma dei verbalizzanti;
• **Spegnimento del dispositivo e riavvio con altro sistema operativo**;

Successivamente **si accede al wallet della parte**, ipotizziamo che la parte abbia un'app sul telefonino (quindi un soft wallet, ed esattamente un device software wallet), per verificare il saldo al cambio attuale. Non viene richiesto il cambio in moneta fiat[4] perché si tratta di un provvedimento cautelare, quindi non si può entrare nella scelta di investimento ma si vuole solo impedirne l'accesso alla parte finchè l'A.G. non valuterà il da farsi. Trattandosi di un telefonino il primo passo sarà stato disattivare la modalità aereo (precedentemente attività in sede di rinvenimento dell'apparato). Successivamente si va ad **operare sullo smartphone della parte**, dopo aver disattivato la modalità aereo (il primo passo in caso di perquisizione è sempre l'attivazione della modalità aereo) ove vi era l'app della piattaforma di gestione del wallet. In caso di Ethereum ad esempio Monolith. **Da lì si dispone il trasferimento di tutte le cripto**, al netto delle commissioni, **verso il paper wallet appena creato**.
Ad operazione conclusa, si riepiloga tutto quanto svolto in un verbale di sequestro che dovrà dare atto che non sono state create ulteriori copie del paper wallet e che la procedura svolta non consente di tenere traccia dell'attività. La busta col paper wallet andrà poi trasmessa all'A.G. Sarà poi cura dell'amministratore nominato valutare se trasformare le criptovalute in moneta fiat o se mantenerle nella loro forma originaria, rischiando ovviamente le fluttuazioni di valore.

**** Ten.Col. della Guardia di Finanza***

1 - Il portafoglio che raccoglie i diversi indirizzi/address bitcoin, più facile da gestire rispetto a lavorare direttamente con gli indirizzi. In genere protetto da password. Può essere gerarchico deterministico.
2 - https://github.com/spesmilo/electrum/blob/master/electrum/wordlist/english.txt
3 - Un wallet hardware è il tipo di wallet più sicuro e protetto poiché è tenuto su un dispositivo fisico che non è connesso a Internet, il che lo rende totalmente resistente agli hacker di Internet. Su un wallet rigido, un investitore può essere certo che i suoi beni sono al sicuro. Un wallet hardware, tuttavia, potrebbe essere erroneamente smarrito dal proprietario, nel qual caso il proprietario perderebbe tutti i suoi beni.
4 - Per moneta fiat si intende una valuta nazionale non ancorata al prezzo di una materia prima come oro o argento. Il valore di una moneta fiat è legato in larga parte alla fiducia nei confronti dell'autorità che la emette, di norma uno Stato o una banca centrale. In questo caso si intende nel significato di "valuta corrente".