Poliziamoderna

Truffe a colpi di bit

Dimenticatevi l'immagine "romantica" di Totò che tenta di vendere la Fontana di Trevi al commendator Decio Cavallo, l'italoamericano tornato in patria dopo aver fatto fortuna negli States, in "Totòtruffa '62". Quell'immagine tipica e a suo modo romantica del truffatore che, per sbarcare il lunario, escogita gli stratagemmi più disparati ai danni dei ricchi malcapitati, mettendoci anche del genio nell'ideare truffe ogni volta più sbalorditive, oggi non esiste più. O meglio, il "genio" oggi ha una tastiera, un mouse e un computer dal quale, a volte chiuso nella sua cameretta, altre invece come tassello di vere e proprie holding del crimine informatico, agisce facendo cadere nella sua rete malcapitati più o meno consapevoli di essere vittime di una truffa o, peggio, complici di quest'ultima.

Il detto "Paese che vai, usanze che trovi", al giorno d'oggi potrebbe essere trasformato in "periodo storico che attraversi, truffa che trovi", perché truffe e truffatori si sono aggiornati e oggi agiscono su Internet, sulle piattaforme di messaggistica istantanea o nel Dark Web, avendo così a disposizione una sterminata platea di possibili clienti e vittime.

Due sono i fenomeni che, principalmente in questo momento storico, complice anche la pandemia, stanno andando per la maggiore: il traffico di falsi Green pass e le finte offerte di lavoro.

Falsi e "finti-veri" Green pass Basta guardare il telegiornale o aprire un quotidiano e, quasi ogni giorno, uno dei servizi è dedicato ai modi più disparati per ottenere l'agognato certificato verde che, chi contrario al vaccino, escogita per evitare di farsi inoculare quello che per lui è considerato quasi come un veleno o un mezzo di controllo da parte dei "poteri forti". Si va dall'infermiere connivente che svuota la siringa e finge di inoculare il vaccino, a chi, complice la Rete e la grande accelerazione informatica compiuta dal sistema sanitario italiano a causa della pandemia, riesce a rimediare a pagamento un QR code che gli permetterà di girare indisturbato senza incorrere nelle sanzioni previste e nelle restrizioni sancite nello stato di emergenza attuale.

Proprio su quest'ultimo caso l'attenzione del Servizio polizia postale e delle comunicazioni non ha momenti di sosta e, soprattutto negli ultimi tempi, è diventata sempre più capillare e specializzata: «L'attenzione sul Green pass – ci ha detto Ivano Gabrielli, direttore della 3^ divisione del Servizio polizia postale e delle comunicazioni – per noi è fondamentale. Svolgiamo un'attività a protezione di quelle che possono essere attività malevole rispetto al complesso sistema informatico che permette la gestione dei Green pass». La pandemia ha accelerato molto l'informatizzazione della pubblica amministrazione e fino a qualche anno fa era impensabile quello che, soprattutto in ambito sanitario, riusciamo a fare oggi: due esempi su tutti, la ricetta "dematerializzata" e il fascicolo medico elettronico, che consente ai medici e agli utenti di accedere a vere e proprie cartelle cliniche on line. Così come anche il rilascio del Green pass che, come ben sappiamo, avviene totalmente per vie informatiche, scaricandolo da app dedicate o andando sul sito del ministero della Salute con un codice che ci arriva via sms: «È un sistema informatico che ha valenza europea – prosegue Gabrielli – e si basa sostanzialmente su due eventi, la vaccinazione o l'esito di un tampone negativo, che poi consentono agli operatori di inserire all'interno del sistema il dato, poi riscontrato in un certificato che viene consegnato all'utente, cartaceo o dematerializzato. Quest'ultimo è il prodotto di un sistema che deve essere reso protetto e ovviamente è un prodotto che ha con sé una tecnologia semplice, ma allo stesso tempo sicura: il QR code, una sorta di codice a barre bidimensionale che non solo porta con sé alcune informazioni che riguardano il soggetto che lo esibisce, ma anche che è stato rilasciato dai sistemi informatici che gestiscono il Green pass».

Vien da sé che un attacco informatico che potrebbe minare la funzionalità di questa struttura sarebbe destabilizzante non soltanto dal punto di vista sanitario, ma anche per la gestione dell'ordine e sicurezza pubblica: «Pensiamo se saltasse il sistema – continua il dirigente – da subito non si avrebbe più la certezza sui soggetti titolati ad accedere a tutti quei servizi o luoghi per i quali la certificazione verde è necessaria ai fini del contenimento della pandemia in atto, con tutte le ripercussioni che ciò comporterebbe».

Detenere e conservare questo sistema è un'attività impegnativa e presuppone anche una sorta di

“trust” tra i vari Stati, perché il nostro Green pass vale in Europa e quello europeo vale in Italia. Quindi vengono conservate gelosamente soprattutto le chiavi che permettono di emettere Green pass, nonché tutti i dati personali. Pensiamo solo a quanto questi ultimi possano fare gola a soggetti terzi che in qualche modo possono avviare attività di studio e analisi su quello che è l’andamento della pandemia o a chi in qualche modo cerca di destabilizzare il sistema del Green pass, nonché a chi se ne vuole impossessare eventualmente per produrre a sua volta certificazioni che passino gli strumenti di validazione. Questa è la prima nostra missione: cercare di proteggere quelle infrastrutture critiche e lo facciamo attraverso il Centro nazionale anticrimine informatico per la protezione infrastrutture critiche (Cnaipic)».

Ci sono stati diversi allarmi nel tempo, soprattutto quando iniziarono ad uscire fuori Green pass intestati a Topolino o ad Adolf Hitler e che avevano destato preoccupazione, temendo la fuoriuscita della chiave elettronica che avrebbe permesso la replicazione dei certificati.

«Quel che ha destato il nostro interesse – prosegue Gabrielli – è stato il proliferare di soggetti che si sono affacciati soprattutto sulle piattaforme di messaggistica istantanea (principalmente Telegram) offrendo la possibilità di emettere Green pass falsi a prezzi che variavano tra i 100 e i 200euro, proponendo anche “sconti famiglia”. Nella quasi totalità dei casi eravamo davanti però a soggetti che stavano truffando coloro che chiedevano il pass, perché a fronte del pagamento e della richiesta di documentazione personale (tra l’altro inutile perché per emettere un Green pass basta sapere nome, cognome, data di nascita e al limite il codice fiscale) venivano chiesti documenti d’identità e carte di credito. La gente, pur di ottenere il pass, non solo ha fornito i propri documenti ma ha anche pagato non rendendosi conto di dare in mano a dei soggetti dati utili per aprire conti all’estero o fare movimentazioni bancarie abusive».

Quindi, c’è stato un fenomeno per i cui concorrenti nel reato si sono trovati ad essere loro stesse vittime di reato. «Purtroppo a questo fenomeno se n’è affiancato – conclude il dirigente – un altro ben più serio, a danno dei farmacisti, escogitato da truffatori con grandi capacità informatiche, in grado di replicare siti istituzionali e numeri di telefono “credibili”, per carpire ai farmacisti stessi credenziali di accesso ai sistemi informatici.

Da qui la possibilità non più quindi di emettere un Green pass falso o di rivendere un certificato intestato a Tizio o Caio, ma di creare da zero gran pass “reali”».

False offerte di lavoro Altra faccia della medaglia delle truffe più in voga in questo ultimo periodo è quella delle false offerte di lavoro nelle quali, più o meno consapevolmente, cadono malcapitati dal profilo sociale totalmente eterogeneo, ma con un tratto in comune: le difficoltà economiche che, acuitesi durante la pandemia, sono state causate dalla perdita del posto di lavoro per molte persone. Non è una truffa bancaria volta a svuotare il conto e non è di tipo “sentimentale” che mira a “spillare” dei soldi facendo leva su situazioni di infelicità sentimentale, ma che sempre più spesso vede coinvolte importanti ed articolate organizzazioni criminali che hanno la necessità di “ripulire” i propri proventi o di far viaggiare merci senza il pericolo del tracciamento che potrebbe portare a scovare il mittente.

«Un’organizzazione criminale che a monte mette in campo delle truffe informatiche di tipo “massivo” – spiega Riccardo Croce, vice questore aggiunto in servizio alla 3^ divisione della Postale ed esperto dell’argomento – a valle è responsabile di migliaia di truffe “semplici”, di minore importo, che assume però un valore maggiore nell’aggregato. Un’organizzazione interessata a fare questo deve dotarsi di diverse componenti: internamente esiste una sorta di divisione del lavoro, così come in una grande azienda, dove c’è chi si occupa del lato informatico (sviluppo malware, frodi legate al phishing, siti internet cloni), chi di quello finanziario (riciclare, ripulire e far arrivare di nuovo alla base il profitto illecito) e chi, come i reclutatori, agisce sul campo per trovare i “muli”».

Uno dei modi preferiti dalle organizzazioni criminali per convincere qualcuno a diventare un “mulo di denaro”, è attraverso la falsa offerta di lavoro, in cui più o meno inconsapevolmente o incautamente la persona, aderendo a quella che sembra un’offerta di lavoro, si presta a fare altro: «Principalmente – prosegue il funzionario – ad aprire conti correnti intestati a suo nome su cui accetta, come se fosse un lavoro, che qualcuno faccia arrivare dei soldi per poi, stando alle istruzioni, re-inviarli ulteriormente da quel conto ad altri conti correnti; l’altra tipologia è il “mulo non di denaro”, quindi la falsa offerta di lavoro viene fatta nel campo della “logistica e spedizioni”, ossia l’inoltro di pacchi; per cui l’offerta che viene fatta è “lavora per me, riceverai dei pacchi a casa che tu talvolta dovrai aprire per verificarne il contenuto, altre solamente da inviare di nuovo ad un altro destinatario con i tuoi riferimenti come mittente”. Esattamente come per riciclare il denaro, la logica è la stessa: disperdere le tracce affinché

risulti complicato risalire all'origine».

E, purtroppo, qui alla Postale sono tante le storie sull'argomento tali da diventare quasi indagini quotidiane per i nostri investigatori informatici: «Lo scenario è spesso complicato dal carattere internazionale del conto corrente su cui viene fatto transitare il denaro, il più delle volte piccole somme per non destare sospetti ma che poi nell'aggregato possono portare a scoprire truffe da milioni di euro – continua Riccardo Croce – Non c'è necessariamente bisogno del paradiso fiscale che non collaborerà mai con le autorità straniere, ma di facilità nell'operatività, ad esempio nell'aprire un conto corrente a cui si lega l'internazionalità del pagamento; ovviamente come polizia non ci possiamo muovere all'estero con gli stessi poteri con cui agiamo sul nostro territorio, se non percorrendo le vie consentite dall'ordinamento, che in molti casi possono essere lunghe. Nel caso invece dei muli di pacchi, registriamo principalmente casi nei quali l'autore, che è allo stesso tempo vittima, quando gli viene chiesta una spiegazione dagli investigatori, è facile che venga colto alla sprovvista. Questo è il caso del "mulo inconsapevole" che spesso e volentieri guadagna poco o nulla, ma molte volte la figura del mulo risulta anch'essa coinvolta attivamente nella truffa, fino a lasciare la posizione di mulo per "salire di grado" e diventare "reclutatore"».

Sono tutte transazioni che, comunque, prevedono l'uso di denaro, anche se ultimamente si stanno affacciando in questo campo le criptovalute, il cui inquadramento legislativo non è ancora ben definito, poiché la norma è in ritardo rispetto al fenomeno che invece è già operativo da molti anni: «Il problema dell'assenza di una legge che ne regolamenti precisamente l'uso – conclude Riccardo Croce – non vuol dire che le criptovalute come il Bitcoin consentano transazioni anonime, anzi sono metodi di pagamento che basano la propria credibilità sulla assoluta tracciabilità delle transazioni; il sistema regge ed è affidabile di fronte ai suoi consumatori perché è matematicamente certo il tracciamento delle transazioni ed è sicuro. A differenza delle transazioni in denaro, come il bonifico bancario, il tracciamento delle criptovalute riguarda però una transazione che è avvenuta da un nodo informatico ad un altro; quindi quello che si va percorrere in senso inverso è il tracciamento di quel che è accaduto tra due nodi che, non sempre direttamente riconducibili a una identità fisica. Il buon esito delle indagini dipende dalle capacità dell'investigatore, dagli strumenti a disposizione e anche dalla collaborazione internazionale fornita da chi gestisce gli *exchanger* di criptovalute».

09/02/2022