AML / CFT NEWS

NEWSLETTER AIF

Notizie relative al contrasto del riciclaggio e del finanziamento del terrorismo pubblicate sui principali siti nazionali ed internazionali.

AGENZIA DI INFORMAZIONE FINANZIARIA
FINANCIAL INTELLIGENCE AGENCY

Via del Voltone n.122
Rep. San Marino

Tel. 0549-888180

Fax. 0549-888181

05 Dicembre 2021

INDICE

PREFAZIONE

Nell'ottica di accrescere la conoscenza dei Soggetti Designati sulle minacce, vulnerabilità e rischi collegati al riciclaggio, al terrorismo, alla proliferazione delle armi di distruzione di massa e al loro finanziamento l'Agenzia continua la sua attività di informazione attraverso la pubblicazione periodica di Newsletter.

Le informazioni selezionate hanno il precipuo scopo di evidenziare le ultime tendenze relative ai settori economici maggiormente coinvolti nelle indagini condotte a livello italiano ed europeo.

Nell'ultimo trimestre del 2021, l'attenzione degli organismi internazionali preposti al contrasto del riciclaggio e del finanziamento al terrorismo, nonché quella degli organi di polizia, si è concentrata sugli ***attacchi informatici (c.d. "cyber attack") perpetrati durante la pandemia*** che ***sono risultati in aumento***. Tali attacchi vengono condotti in particolar modo nei confronti di istituzioni e soggetti che operano nel settore della sanità, ma non sono avulsi da tale rischio anche gli intermediari finanziari, le banche ed i loro clienti.

Come più volte rimarcato, la comprensione ed il monitoraggio di questi aspetti sono indispensabili per interpretare eventuali segnali di anomalia utili anche al fine di ottemperare in maniera più compiuta e consapevole agli obblighi di adeguata verifica della clientela e a quelli obblighi di segnalazione.

EUROPOL

Ad ottobre è stato siglato un accordo (c.d. "*Working Arrangement*") tra il Comandante del Corpo della Gendarmeria di San Marino, Maurizio Faraone e il Direttore Esecutivo di EUROPOL, Catherine De Bolle, ai fini di collaborare nella prevenzione e nella lotta alla criminalità e al terrorismo. Più in particolare, tale collaborazione riguarda la prevenzione e la repressione di numerose ipotesi delittuose tra le quali il terrorismo, il crimine organizzato, i reati finanziari, la falsificazione del denaro e di mezzi di pagamento[1].

Le operazioni condotte da EUROPOL nell'ultimo trimestre del 2021 riguardano principalmente i seguenti reati:

- ***traffico di sostanze stupefacenti;***
- ***traffico di essere umani***;
- ***contraffazione*** di materiali farmaceutici e sostanze dopanti, di abbigliamento e scarpe, di manufatti d'arte;
- ***crimini informatici*** (in particolare *ransomeware attack* e truffe).

Si segnala un'operazione che ha coinvolto il territorio italiano riguardante le ***energie rinnovabili***. Tra il 2016 e il 2020, una rete criminale ha ottenuto illegalmente certificazioni per l'efficienza energetica (c.d. certificati "bianchi"), al fine di ricevere sussidi attraverso progetti fittizi. I fondi così ottenuti sono stati trasferiti in Germania, Svizzera ed altri paesi europei.

Inoltre Europol ha concentrato la propria attenzione sul contrasto alla crescente attività di riciclaggio basata sugli ***asset virtuali*** e sul contrasto di altre attività illecite sempre collegate agli asset virtuali.

INTERNET ORGANISED CRIME THREAT ASSESSMENT

Il tema principale affrontato nello IOCTA[2], pubblicato lo scorso ottobre, è il *cybercrime*; che risulta essere in costante evoluzione avvantaggiato anche dalle condizioni socio-economiche determinate dal dilagare della pandemia di COVID-19. I punti focali della pubblicazione riguardano:

[1] https://www.sanmarinortv.sm/news/attualita-c4/collaborazione-piu-stretta-tra-le-autorita-di-contrasto-di-san-marino-ed-europol-per-la-prevenzione-e-lotta-alla-criminalita-e-al-terrorismo-a213426

[2] Europol (2021), Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg: https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

- gli ***attacchi ransomware***, che prevendono il pagamento di un riscatto per ripristinare o non divulgare a terzi i dati che vengono resi (momentaneamente) inaccessibili dai virus. Tali virus infettano non solo i sistemi operativi di aziende pubbliche e private, ma anche quelli dei singoli utenti;

- lo ***sfruttamento online di materiale pedopornografico***, compreso quello "auto-generato" dall'adescamento di minori che, a seguito delle restrizioni sociali adottate per contenere la pandemia, utilizzano sempre più frequentemente internet;

- le ***frodi on-line,*** tra le quali si annoverano

    - le *investment fraud* legate agli investimenti finanziari;
    - le *card-not-present fraud* legate alle truffe sulle carte di credito on-line;
    - il *phishing* attraverso il quale si cercano di estorcere informazioni personali, anche finanziarie, agli utenti;

- il ***DARK WEB***, la cui infrastruttura non ha subito forti cambiamenti, ma viene utilizzato per l'acquisto di asset virtuali anonimi come Monero e la commercializzazione di beni illegali.

INTERPOL

Sulla scorta di quanto riscontrato da EUROPOL, anche durante la 48^{esima} Conferenza Regionale Europea dell'ICPO-INTERPOL è stato rimarcato come la pandemia abbia comportato un aumento esponenziale dei crimini informatici soprattutto nel DARK WEB. Tali crimini riguardano in particolare:

- la ***contraffazione*** di green pass;

- lo ***sfruttamento dei minori*** con lo scambio di immagini pedopornografiche;

- le ***truffe online***.

Nel periodo di riferimento sono stati perpetrati numerosi attacchi informatici, in particolare tramite *ransomware*, alle strutture ospedaliere e alle case farmaceutiche dove si producono i vaccini o beni legati al contrasto della diffusione della pandemia. Le ricerche esperite hanno evidenziato come i criminali abbiano guadagnato 350 milioni di dollari in ***asset virtuali***, in particolare ***criptovalute*** (con un incremento del 311% nel 2020 rispetto all'anno precedente). Non sono esenti dalla minaccia di attacchi informatici, sotto forma di *ransomware*, anche le infrastrutture pubbliche o quelle considerate "critiche".

Sul versante del contrasto al ***terrorismo*** e al suo finanziamento si segnala l'operazione "Neptune III" volta a contrastare una minaccia legata al possibile ingresso in Europa di sospetti terroristi provenienti dall'Africa attraverso il bacino del Mediterraneo.

GUARDIA DI FINANZA

Le operazioni condotte della GUARDIA DI FINANZA nell'ultimo trimestre del 2021 riguardano i seguenti reati:

- la ***contraffazione*** di beni riguardanti diversi settori economici (***giocattoli, abbigliamento, gadget sportivi e materiale elettrico***);
- la ***truffa*** con particolare riferimento alle ***energie rinnovabili***;
- il ***traffico illecito di rifiuti, di sostanze stupefacenti, di tabacco e petroli***;
- il riciclaggio di proventi illeciti derivanti dai seguenti reati presupposto: ***reati tributari, bancarotta fraudolenta, ricettazione e truffa***.

Inoltre si segnalano le seguenti operazioni, meglio descritte nell'accluso schema riepilogativo:

- "Operazione Dark Huntor" – concernente il sequestro di un BLACK MARKET in cui venivano forniti, tra gli altri, i ***servizi di "Bank Drops"***, che riguardano la possibilità di richiedere ad un intermediario di effettuare una transazione verso un conto corrente di un soggetto terzo indicato dal cliente, dietro pagamento di una commissione;
- "Operazione Piccadilly" - riguardante il coinvolgimento di ***professionisti*** esperti di consulenza finanziaria e fiscale nell'ideazione di uno schema di riciclaggio internazionale riguardante il settore del ***commercio all'ingrosso di calzature e abbigliamento***;
- riguardante il ***riciclaggio*** di capitali illeciti e ***favoreggiamento dell'immigrazione clandestina***. Le indagini hanno avuto luogo in diverse province italiane, tra le quali si annovera anche la limitrofa ***Ravenna***.

Inoltre la GUARDIA DI FINANZA ha effettuato diversi controlli sui cosiddetti ***compro-oro*** al fine di verificare le attività di compravendita e ingrosso di oggetti preziosi.

GLOSSARIO ed ACRONIMI

AML
Acronimo di *Anti Money Laundering* ovvero Antiriciclaggio.

Black Market
Il Black Market o Mercato Darknet è un sito web commerciale del dark web. La sua funzione primaria è quella del mercato nero, permettendo la compravendita di varie tipologie di beni e servizi illeciti quali droghe, armi cibernetiche, contraffazione di denaro, carte di credito rubate, creazione di documenti falsi, farmaci senza licenza, steroidi anabolici; tuttavia vengono commercializzati anche beni leciti.

CTF
Acronimo di *Counter Terrorist Financing* ovvero Contrasto al finanziamento del terrorismo.

Dark web
Il Dark Web (in italiano: web oscuro o rete oscura) è la terminologia che si usa per definire i contenuti del World Wide Web nelle darknet (reti oscure) che si raggiungono via Internet attraverso specifici software, configurazioni e accessi autorizzativi.
Il Dark Web è un gruppo di siti Internet nascosti e accessibili solo attraverso un browser apposito. Il suo scopo è quello di mantenere l'attività online anonima e privata al fine di condurre attività illegali, ma non solo.

Europol
L'ufficio europeo di polizia (anche Europol, contrazione da *European Police Office*) è un'agenzia dell'Unione Europea finalizzata alla lotta al crimine nel territorio degli Stati membri dell'Unione europea, divenuta operativa il 1º luglio 1999. Europol persegue l'obiettivo di rendere l'Europa più sicura coopera con molti stati partner non membri dell'Unione Europea e con Organizzazioni Internazionali, in particolare opera in collaborazione con le forze dell'ordine, i dipartimenti governativi e il settore privato.
Per ulteriori informazioni si rimanda al sito di riferimento: www.europol.europa.eu.

Guardia di Finanza (GdF)
I compiti di istituto della Guardia di Finanza sono la prevenzione, la ricerca e la denuncia delle evasioni e violazioni delle leggi finanziarie; la repressione del contrabbando; la vigilanza in mare per fini di polizia finanziaria e di concorso ai servizi di polizia marittima e di assistenza; il concorso al mantenimento dell'ordine e della sicurezza pubblica. I compiti militari comprendono il concorso alla difesa delle frontiere dello Stato e, in tempo di guerra, la partecipazione alle operazioni militari. Alla Guardia di Finanza competono funzioni di polizia giudiziaria e tributaria.
Per ulteriori informazioni si rimanda al sito di riferimento: www.gdf.gov.it.

Interpol (The International Criminal Police Organization - ICPO-INTERPOL)
L'Organizzazione internazionale della polizia criminale - Interpol è dedita alla cooperazione tra forze di polizia e al contrasto del crimine internazionale. San Marino ha aderito a tale Organizzazione nel 2006. In conformità con lo statuto dell'Organizzazione, San Marino si è dotato di un proprio Ufficio Centrale Nazionale, preposto alla cooperazione internazionale di polizia nel rispetto degli accordi vigenti.
Per ulteriori informazioni si rimanda ai siti di riferimento: https://www.interpol.int/Who-we-are/What-is-INTERPOL; http://www.esteri.sm/on-line/home/link/interpol.html.