DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

# Ransomware e antiriciclaggio: evoluzione e trends negli Stati Uniti

**19 Dicembre 2022**

**Antonio Martino**, Of Counsel, DLA Piper
**Ernesto Carile**, Security Manager, Leonardo Helicopters Division

**Antonio Martino**, Of Counsel, DLA Piper

**Ernesto Carile**, Security Manager, Leonardo Helicopters Division

**Antonio Martino**

Antonio Martino è esperto di diritto penale dell'economia con particolare riferimento ai reati fiscali, finanziari, fallimentari e contro la P.A. nonché delle tematiche concernenti la prevenzione dell' utilizzo del sistema finanziario a scopo di riciclaggio. Quale Ufficiale superiore della Guardia di Finanza, per oltre dieci anni (1999-2010), è stato a capo della Sezione di Polizia Giudiziaria della Procura della Repubblica di Milano coordinando alcune delle più rilevanti indagini a livello nazionale su casi di corruzione, bancarotta fraudolenta, truffa ai danni dello Stato, reati fiscali e finanziari e riciclaggio.

**Ernesto Carile**

Ernesto Carile è Security Manager presso Leonardo Helicopters Division. Già Tenente Colonnello della Guardia di finanza.

Siti istituzionali statali, reti informatiche infrastrutturali strategiche, aziende private e singoli cittadini, nessuno ormai può considerarsi esente da attacchi *cyber*. La contaminazione patologica degli ecosistemi informatici da parte del *cybercrime* sta inesorabilmente dimostrando la gravità della situazione al livello globale e quanto sia complesso disinnescare il problema nonostante le continue azioni di mitigazione dei rischi che tutti gli attori coinvolti cerchino di attuare.

Una delle modalità di aggressione più pervasiva è costituita dal *ransomware* che semplicisticamente potrebbe essere accostato al classico sequestro a scopo di estorsione, non di persone ma di dati informatici. Questo si sostanzia in un *software* dannoso ("*malware*") progettato per bloccare l'accesso ad un sistema informatico, spesso crittografando i dati o i programmi in esso contenuti, finalizzato ad estorcere alle vittime un riscatto in cambio della decrittografia delle informazioni e del ripristino dell'accesso. L'attaccante tiene i dati in ostaggio fino a quando viene pagato un riscatto, il più delle volte in Bitcoin. Nel corso degli anni si è assistito ad un cambio di metodologia di attacco che è passata da un approccio "massivo" con alti volumi di obbiettivi, ad una maggiore selettività nella scelta delle vittime, prendendo di mira imprese o istituzioni più grandi per richiedere riscatti maggiori così massimizzando il "ritorno sugli investimenti". Inoltre si osserva l'introduzione di un vero e proprio "modello di business" che offre di sul *dark web* servizi *ransomware user friendly* in cambio di una percentuale di riscatto (*ransomware-as-a-service - RaaS*), creando ulteriori difficoltà nell'individuazione dei potenziali attacchi dovute all'estensione della superficie soggettiva delle minacce.

In alcuni casi, inoltre, gli autori dell'attacco, replicando le tattiche estorsive già utilizzate con i sequestri di persona, minacciano di pubblicare file sensibili appartenenti alle vittime se la richiesta di riscatto non viene pagata.

La natura di questo strumento, oltre alle questioni intrinsecamente tecniche, ha anche una fase prettamente "venale" che consta nel pagamento del riscatto, che per sua natura è un provento illecito che quindi va occultato/trasferito, il più delle volte con l'utilizzo di criptovalute. Sulla base di tale evidenza le Autorità antiriciclaggio internazionali[1] e nazionali hanno emanato nel corso degli ultimi anni specifi-

1 Fatf Report Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing – 14 settembre 2020 - http://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf.

**vedi l'articolo online**

che indicazioni operative per i soggetti obbligati per sensibilizzali a porre maggiore attenzione al fenomeno, anche con l'individuazione di indicatori di anomalia appositamente plasmati rispetto al rischio. Va detto poi che, nel particolare contesto geopolitico attuale, gli attacchi *cyber* tramite il *ransomware* costituiscono un mezzo di "guerra asimmetrica" utilizzata dalla Russia, che ne ha incrementato l'uso in maniera esponenziale.

Gli Stati Uniti sono tra i paesi che maggiormente considerano strategica la lotta al fenomeno e attribuiscono al sistema di contrasto al riciclaggio e al finanziamento del terrorismo un ruolo centrale ineludibile, proprio nella fase dell'occultamento e trasferimento dei proventi dei riscatti. Infatti il Financial Crimes Enforcement Network (FinCEN)[2], Autorità AML negli USA, aveva inserito nell'"*Anti-Money Laundering and Countering the Financing of Terrorism National Priorities*"[3] per il quadriennio 2021-2024, la criminalità cibernetica tra i maggiori rischi per la sicurezza nazionale ponendo massima attenzione proprio al *ransomware*, cui aveva inoltre dedicato l'emissione di apposite istruzioni operative per i soggetti obbligati[4] individuando specifici indicatori per la redazioni di segnalazioni di operazioni sospette ("*Suspicious Activity Report – SAR*").

In tale contesto il FinCEN ha pubblicato una dettagliata anali sulle tendenze del fenomeno del *ransomware* derivato dai dati relativi al 2021, da cui emerge un inesorabile aumento degli attacchi e delle relative segnalazioni (con un forte incremento connesso ad "attori collegati alla Russia"), nonché dei relativi valori interessati[5]. Il Rapporto, pubblicato ai sensi della normativa antiriciclaggio americana[6], rappresenta una fotografia di quanto il fenomeno si stia incrementando soprattutto a causa di aggressioni riconducibili alla Russia (circa il 75% degli attacchi relativi al secondo semestre 2021) e comunque evidenzia differenze anno su anno che lasciano pochi margini interpretativi. Tra il 2020 e il 2021 si passa da un numero di 602 segnalazioni per un valore stimato di 527 milioni di dollari, a 1.251 per un importo totale di 886 milioni; ma stupisce l'incremento nel solo secondo semestre 2021 che ha visto 793 attacchi, contro i 458 del primo. Inoltre i valori totali fanno addirittura rilevare un incremento dei casi del 188% sul 2020, per un importo di circa 1,2 miliardi di dollari. I dati delle segnalazioni e dei relativi importi sorprendono ancor di più se si osserva il loro incremento rispetto all'ultimo decennio durante il quale

2 Il Financial Crimes Enforcement Network è stato istituito con il Treasury Order nr. 105-08 del Segretario del Tesoro degli Stati Uniti il 25 aprile 1990 e, attualmente, è integrato nel Dipartimento del Tesoro degli Stati Uniti. La missione istituzionale di FinCEN è proteggere da attività illecite il sistema finanziario e combattere il riciclaggio di denaro sporco e promuovere la sicurezza nazionale attraverso la raccolta, l'analisi e la diffusione di informazioni finanziarie e l'uso strategico delle autorità finanziarie. FinCEN svolge la sua missione ricevendo e conservando i dati delle transazioni finanziarie; inoltre analizza e diffonde tali dati a fini di contrasto e coopera a livello globale con le organizzazioni omologhe degli altri Stati (FIU) e con gli organismi internazionali (GAFI, Gruppo Egmont). FinCEN esercita funzioni regolatorie principalmente ai sensi del Currency and Transaction Reporting Act del 1970 (il cui quadro legislativo viene comunemente definito "Bank Secrecy Act" - "BSA"), modificato dal Titolo III del Patriot Act del 2001, nonché da diverse norme che ne hanno esteso ed integrato i poteri e le competenze. Il BSA è il primo e più completo statuto federale che detta le linee di contrasto al riciclaggio di denaro e al finanziamento del terrorismo. Il BSA autorizza il Segretario del Tesoro a emanare regolamenti che impongono alle banche e ad altri istituti finanziari di adottare una serie di precauzioni contro i reati finanziari, tra cui l'istituzione di programmi AML e l'archiviazione di rapporti connessi con indagini e procedimenti penali, fiscali e regolamentari, anche in materia di intelligence e antiterrorismo. Il Segretario del Tesoro delega il Direttore di FinCEN ad attuare, amministrare e far rispettare il Bank Secrecy Act e le altre normative di settore. Il Congresso degli Stati Uniti ha assegnato a FinCEN specifici poteri diretti alla raccolta, l'analisi e la diffusione a livello centrale delle informazioni connesse al monitoraggio del sistema finanziario a supporto delle Autorità pubbliche e dell'industria finanziaria a livello federale, statale, locale e internazionale. Nel 2021, con l'approvazione del National Defense Authorization Act (NDAA) che include l'Anti-Money Laundering Act (AML Act) ed il Corporate Transparency Act (CTA), è stata introdotta una imponente riforma alla normativa AML/CFT. In particolare, l'AML Act mira a rafforzare, modernizzare e semplificare il regime statunitense promuovendo l'innovazione, la riforma normativa e l'impegno di tutte le Autorità competenti e dei soggetti obbligati per identificare i rischi e le priorità AML; inoltre, con il CTA vengono stabiliti requisiti uniformi di segnalazione della titolarità effettiva per le società, le società a responsabilità limitata e gli altri enti che svolgono attività commerciali negli Stati Uniti, autorizzando il FinCEN a raccogliere informazioni e condividerle con le autorità governative e le istituzioni finanziarie.

3 Anti-Money Laundering and Countering the Financing of Terrorism National Priorities - 30 giugno 2021 - https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf. In merito alle priorità AML/CFT e anticorruzione degli Stati Uniti per il 2021/2024: Diritto Bancario – Antiriciclaggio: gli Stati Uniti dettano le priorità strategiche dei prossimi 4 anni - Antonio Martino e Ernesto Carile – 09/07/2021 - https://www.dirittobancario.it/art/antiriciclaggio-gli-stati-uniti-dettano-le-priorita-strategiche-dei-prossimi-4-anni/.

4 Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments – 1 ottobre 2020 - https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf. Per approfondimenti: I pericoli del ransomware e le indicazioni dell'Autorità antiriciclaggio U.S.A. (FinCEN) – Diritto Bancario – 4 dicembre 2020 - Antonio Martino ed Ernesto Carile - https://www.dirittobancario.it/news/antiriciclaggio/i-pericoli-del-ransomware-e-le-indicazioni-dell-autorita-antiriciclaggio-usa-fincen .

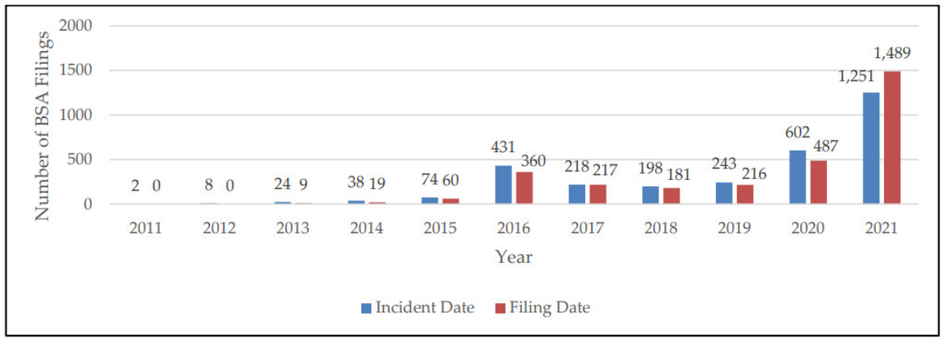
5 FinCEN Analysis Reveals Ransomware Reporting in BSA Filings Increased Significantly During the Second Half of 2021 – 1 novembre 2022 - https://www.fincen.gov/sites/default/files/2022-11/Financial%20Trend%20Analysis_Ransomware%20FTA%202_508%20FINAL.pdf .

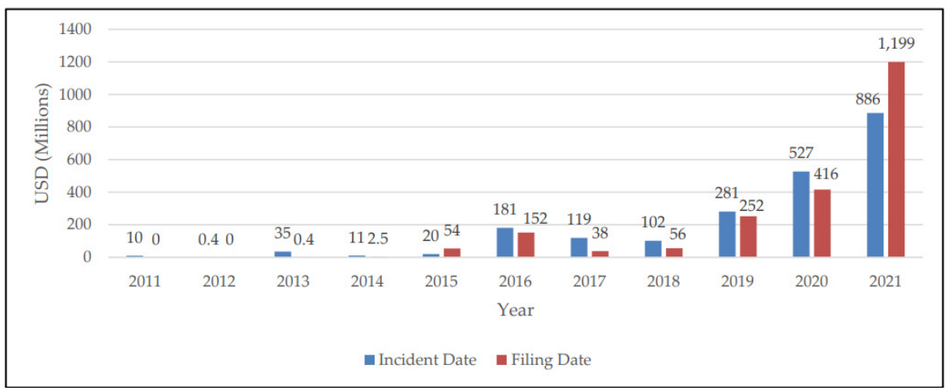
6 Sezione nr. 6206 dell'Anti-Money Laundering Act (AML Act), emanato come Division F, §§ 6001-6511, del William M. (Mac) Thornberry National Defense Authorization Act per l'Anno Fiscale 2021, Pub. L.116-283 (2021).



vedi l'articolo online

le segnalazioni totali sono state 3.193 valorizzate per circa 2,31 miliardi di dollari (vedi dati del Rapporto sul *ransomware* pubblicato dal FinCEN periodo 2011-2021 sul numero degli "incidenti"/segnalazioni e importo)[7].




7 Pagine 4 e 5 del documento.



Va sottolineato che la crescita delle *SARs* potrebbe derivare anche dalla maggiore attenzione che i soggetti obbligati hanno posto al fenomeno *ransomware* a seguito delle specifiche indicazioni emanate sia dal FinCEN che dal Dipartimento del Tesoro, tramite l'Office of Foreign Assets Control (OFAC)[8].

Il Rapporto dedica una particolare attenzione alle segnalazioni collegate a gruppi cyber russi soprattutto nel secondo semestre del 2021 (75% del totale). Tali indiscutibili evidenze, che derivano dalla riconducibilità dei *malware* e dei codici in lingua russa e portano il valore degli attacchi del secondo semestre 2021 a 337 milioni di dollari su un totale di 500 (69%), fanno prospettare ulteriori aumenti nel corso dei prossimi anni dovuti alla situazione di crisi in Ucraina[9].

I dati emersi rendono evidente come i soggetti obbligati, ed in particolare le istituzioni finanziarie, rivestiranno un ruolo sempre più importante nel contrasto al trasferimento dei proventi derivanti dal *ransomware* mediante una costante attività di *customer due diligence* AML che dovrà scaturire nella immediata trasmissione di segnalazioni di operazioni sospette. Infine, FinCEN richiama l'applicazione degli indicatori di anomalia (*red flag indicators*) emanati nel corso degli anni che prevedono di arricchire le *SAR* con ogni informazione tecnica per l'approfondimento della segnalazione come indirizzi e-mail e IP, nominativi dei file, riferimento al portafoglio di valuta virtuale utilizzata per il pagamento del riscatto.

8 L'Office of Foreign Assets Control (OFAC) è inquadrato all'interno del Dipartimento del Tesoro degli Stati Uniti è svolge la funzione di amministrazione e applicane delle sanzioni economiche e commerciali basate sulla politica estera degli Stati Uniti e sugli obiettivi di sicurezza nazionale contro paesi e regimi stranieri, terroristi, narcotrafficanti internazionali, soggetti coinvolti in attività legate alla proliferazione di armi di distruzione di massa e altre minacce alla sicurezza nazionale, alla politica estera o all'economia degli Stati Uniti.

9 *FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts, FIN-2022-Alert001* – 7 marzo 2022 - https://www.fincen.gov/sites/default/files/2022-03/FinCEN%20Alert%20Russian%20Sanctions%20Evasion%20FINAL%20508.pdf. Per approfondimenti sulle indicazioni del FinCEN collegate alle Russia: Sanzioni alla Russia: gli Stati Uniti arruolano l'antiriciclaggio – Diritto Bancario – 10 marzo 2022 - https://www.dirittobancario.it/art/sanzioni-alla-russia-gli-stati-uniti-arruolano-lantiriciclaggio/ .

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

**dirittobancario.it**