DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

ATTUALITÀ

Cyber-crime e riciclaggio: minacce, schemi operativi e SOS

18 Settembre 2024

Alessio Castronuovo, AML Governance, FinecoBank

Alessio Castronuovo, AML Governance, FinecoBank *

** Le opinioni espresse non impegnano l'Istituto di appartenenza*

Premessa

"Io cerco nuovi adepti nelle migliori università mondiali tu vai ancora alla ricerca di quattro scemi in mezzo alla strada che vanno a fare così: bam, bam! Io cerco quelli che fanno così, invece: pin, pin! Che cliccano! Quelli cliccano e movimentano. È tutta una questione di indice, capito?"[1]

Con il passare del tempo, combattere il riciclaggio di denaro è diventato sempre più difficile. Meno dell'1% dei flussi finanziari illeciti finisce nella rete degli inquirenti.[2] Anche in conseguenza del contesto geopolitico attuale, tra le minacce più attive preliminari al riciclaggio - dopo il narcotraffico - crescono le frodi informatiche e le estorsioni digitali[3].

Nel mondo, in Europa, come anche in Italia, il maggiore threat actor è la criminalità informatica organizzata. Organizzazioni, cioè, che offrono servizi di "crime-as-a-service" che consentono agli affiliati di: lanciare attacchi informatici senza avere conoscenze o competenze tecniche; rendere indisponibili i dati alle vittime; minacciarne la pubblicazione e chiederne il riscatto, solitamente in bitcoin.[4] Divisioni specializzate dell'ecosistema cyber-crime si occupano poi di riciclare i proventi ottenuti.

Risulta quindi necessario disegnare nuovi presìdi di prevenzione e rafforzare le misure di contrasto dei reati informatici. Sul piano repressivo, in Italia, con l'approvazione finale del DDL cybersicurezza è stato introdotto il delitto di estorsione mediante reati informatici ed esteso il perimetro nonché le sanzioni previste per le truffe informatiche. Riguardo le misure di prevenzione, ancora una volta, il sistema anti-riciclaggio deve evolversi per arginare l'avanguardia criminale del cyber-laundering, la nuova frontiera

1 N. Gratteri e A. Nicaso "*Il grifone. Come la tecnologia sta cambiando il volto della 'ndrangheta*", Mondadori, 2023, cit.

2 United Nations Office on Drugs and Crime, Research report "*Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes*", Ottobre 2011.

3 Europol, report "*Decoding the Eu's most threatening criminal networks*" del 5 aprile 2024 e "*Cyber-attacks: the apex of crime-as-a-service*" del 13 settembre 2023.

4 OFAC "*United States Sanctions Senior Leader of the LockBit Ransomware Group*" del 7 maggio 2024, "*United States Sanctions Affiliates of Russia-Based LockBit Ransomware Group*" e Europol "*Law enforcement disrupt world's biggest ransomware operation*" del 20 febbraio 2024. Per l'Italia, la relazione annuale al Parlamento sulle attività svolte dall'Agenzia per la cybersicurezza nazionale (ACN) diffusa il 24 aprile 2024.

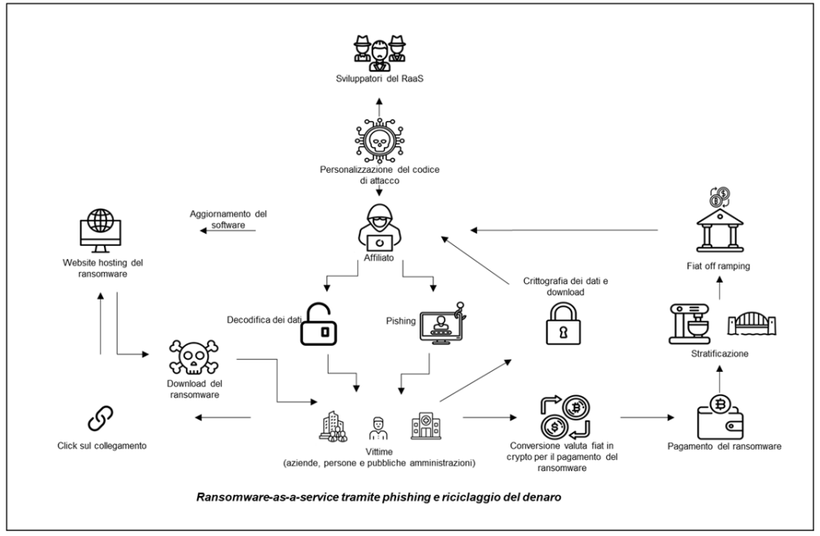
vedi l'articolo online

del riciclaggio del denaro.

Le minacce del cyber-crime. Tassonomia, schemi operativi e riciclaggio

Nel 2023 il FATF-GAFI, l'Organismo intergovernativo che ha lo scopo di elaborare e sviluppare strategie di lotta al riciclaggio dei capitali di origine illecita, ha rilasciato due report tematici sul contrasto al finanziamento delle estorsioni digitali (meglio note come "ransomware") e sui flussi finanziari derivanti da frodi informatiche con l'obiettivo di migliorare la comprensione globale alle nuove minacce digitali e definire alcune best practice sui presìdi normativi e di prevenzione da considerare per fronteggiare il cyber-riciclaggio, tra cui un elenco di indicatori di anomalia e misure di coordinamento tra controlli antifrode e antiriciclaggio.[5]

Sulla base della tassonomia definita dal watchdog sul riciclaggio le minacce digitali per quanto multiformi possono distinguersi - per semplificare - in due categorie: frodi informatiche e ransomware[6]. Le prime, o presuppongono l'inganno delle vittime (come nel caso del phishing, delle frodi romantiche o sugli investimenti e del pig butchering scam[7]) oppure sono offensive digitali volte a compromettere la disponibilità di un sistema (tra cui, il malware e i DDoS[8]). Nel ransomware, invece, l'obiettivo del criminale cibernetico è ottenere il pagamento di un riscatto per rendere nuovamente disponibili i dati cifrati tramite un'estorsione che può diventare doppia o tripla. Doppia, nella misura in cui la minaccia oltre che riguardare l'impossibilità di accedere al sistema riferisce anche alla pubblicazione dei dati. Tripla, laddove l'intimidazione sia indirizzata anche ai terzi interessati dalla divulgazione dei dati in ostaggio. Il ransomware è diventato un business scalabile con l'intuizione del ransomware-as-a-service (RaaS).



Ransomware-as-a-service tramite phishing e riciclaggio del denaro

Nella figura rappresentata la vittima, dopo aver ricevuto la richiesta di riscatto per riottenere la disponibilità dei dati oggetto di frode informatica (nell'esempio, il phishing), si attiva per acquistare tipo e quantità di asset richiesti dall'estorsore digitale. In pratica, deve convertire valuta fiat in crypto e per far questo trasmette fondi con bonifico o carta di credito a un fornitore di servizi crypto e riceve in cambio il suo corrispettivo in valuta virtuale, per poi trasferirlo nel portafoglio digitale del gruppo ransomware. Attraverso servizi di mixer o cross-chain bridge[9] c'è la c.d. stratificazione che rende complicata la

5 FATF report "*Countering Ransomware Financing*" del 14 marzo 2023 e "*Illicit Financial Flows from Cyber-enabled Fraud*" del 9 novembre 2023.

6 Fattispecie, quest'ultima, che può naturalmente essere ricondotta a una frode informatica. La distinzione è puramente funzionale al testo in ragione dell'atteso pagamento del riscatto.

7 In particolare, il phishing è un attacco informatico avente l'obiettivo di carpire informazioni sensibili (user ID, password, numeri di carte di credito, PIN) con l'invio di false e-mail generiche a un gran numero di indirizzi allo scopo di convincere i destinatari ad aprire un allegato o ad accedere a siti web fake. Le truffe romantiche o sugli investimenti, anch'essi assolutamente eterogenei, inducono la vittima a investire su piattaforme inesistenti o inviare denaro o crypto in ragione del sentimento nel frattempo creato con il truffatore. Il pig buthcering scam è la combinazione tra una truffa romantica e una frode sugli investimenti per cui, consolidato il rapporto, i criminali convincono la vittima a investire i propri risparmi in piattaforme trading o crypto-trading fasulle.

8 Mentre gli eventi DDoS (Distributed Denial of Service) mirano a compromettere la disponibilità di un sistema mediante esaurimento delle sue risorse di rete, elaborazione o memoria, il malware è un programma inserito in un sistema informatico con l'intenzione di compromettere la riservatezza, l'integrità o la disponibilità dei dati, delle applicazioni o dei sistemi operativi dell'obiettivo.

9 In parole semplici, i mixer sono dei servizi offerti da piattaforme che mischiano i fondi di molteplici utenti, creando un pool di criptovalute. Le crypto così mischiate vengono, poi, inviate a nuovi indirizzi forniti dagli utenti, ma in quantità diverse dagli importi originali. Con il che, diventa difficile - se non impossibile - tracciare il percorso originale dei fondi. I cross chain bridge sono dei protocolli che consentono attraverso smart contract il trasferimento

vedi l'articolo online

ricostruzione dei flussi in ingresso che saranno convertiti da un ulteriore fornitore di servizi crypto in valuta fiat per atterrare nel comparto della finanza tradizionale. Da ultimo, il pagamento ricevuto dalle vittime è ripartito tra gli sviluppatori del RaaS e l'affiliato e risulta determinato dalla percentuale di successo degli attacchi lanciati nonché dei profitti generati: da circa il 20-40% del riscatto di base, fino all'80% dei profitti in ragione dell'affidabilità criminale conseguita dall'affiliato. Per avere una stima del fenomeno a livello globale, nel 2023 i pagamenti estorti alle vittime di ransomware - quasi sempre in bitcoin - sono stati maggiori di 1 miliardo di dollari[10]. La minaccia delle estorsioni digitali cresce rispetto alle ulteriori fattispecie del cyber-crime sia perché i target preferiti sono le aziende di alto profilo o le pubbliche amministrazioni per cui diventa più redditizia l'estorsione tripla, sia perché il ransomware è diventato ormai uno strumento di hacktivismo politico.[11]

In questa prospettiva, in particolare, è determinante il rafforzamento della collaborazione attiva da parte dei fornitori di servizi crypto. Molte delle omesse segnalazioni di operazioni sospette loro contestate riguardano proprio l'aver consentito operatività con marketplace del darkweb, entità o individui oggetto di sanzioni finanziarie piuttosto che aver permesso il fiat off ramping presso intermediari designati.[12]

Nelle frodi informatiche, invece, per riciclare i proventi della truffa al lavoro degli hacker spesso si affianca quello dei "pastori" che hanno il compito di selezionare "muli di denaro" consapevoli o inconsapevoli. Ad esempio, quando inconsapevole, dopo aver ricevuto un sms di allerta relativo a richieste di pagamento sospette, a cui segue una telefonata da un presunto operatore della Banca di riferimento o un falso agente di polizia, la vittima fornisce ai truffatori i suoi dati bancari.[13] Quando consapevole, il mulo di denaro fornisce la disponibilità del proprio conto corrente per il versamento delle somme provenienti dalle frodi informatiche. Ostacola quindi l'identificazione della provenienza delittuosa del denaro, da altri precedentemente ricavato quale profitto conseguito del reato di frode informatica, consentendone il trasferimento tramite bonifici bancari: riciclaggio.[14]

In definitiva, entrambi i rapporti FATF-GAFI condividono che le due principali fonti di informazioni per individuare e indagare sul riciclaggio di denaro connesso al cyber-crime sono: la denuncia delle vittime e le segnalazioni di operazioni sospette. In entrambi i casi, per nulla scontate.

Prospettive d'intervento per fronteggiare il cyber-crime. Sistemi di segnalazione e collaborazione attiva

Tra i settori prioritari di intervento raccomandati alle singole giurisdizioni dall'Organismo intergovernativo sulle strategie antiriciclaggio per fronteggiare il cyber-crime ci sono: il consolidamento della collaborazione multilaterale tra Paesi e aziende coinvolte; l'adozione di iniziative per aumentare la segnalazione delle vittime; il rafforzamento dei sistemi di monitoraggio delle operazioni sospette.

In particolare, la collaborazione tra Paesi e aziende così come una maggiore accessibilità ai sistemi di segnalazione in favore delle vittime può aversi con lo sviluppo di piattaforme dedicate che, da un lato, fungono da database per centralizzare le informazioni relative alle frodi informatiche trasmesse da aziende e magari anche dagli intermediari interessati, dall'altro, consentono di segnalare scam o richieste di riscatto digitale senza ritardo. Un sistema di comunicazione così articolato garantirebbe infatti una rapida ed efficace circolazione delle informazioni a vantaggio di tutti gli attori coinvolti (vittime, aziende o istituti bancari interessati, forze di polizia locali ed estere) indipendentemente dal suo input o canale di segnalazione.

Proprio perché le denunce delle vittime risultano sottostimate rispetto all'ampiezza del fenomeno, le segnalazioni di operazioni sospette trasmesse dagli intermediari ai fini antiriciclaggio rappresentano una fonte indipendente e necessaria di rilevamento dei flussi finanziari legati al cyber-crime. In

di asset e dati tra diverse blockchain garantendo l'interoperabilità tra le varie catene di blocco, permettendo così agli utenti di muovere crypto senza dover passare da un fornitore di servizi crypto. Definizioni tratte da "*Cripto, riciclaggio a 7 miliardi di dollari. Ma gli illeciti valgono solo lo 0,34% del totale*" di Vittorio Carlini, Sole24Ore del 12 luglio 2024.

10 Fonte: Chainalysis "*The 2024 Crypto Crime Report - the latest trends in ransomware, scams, hacking and more*", Febbraio 2024.

11 Cfr. Nota 3 e 4.

12 Cfr. FinCEN Consent Order 2023-04.

13 Sul tema, la "Nuova campagna di phishing rivolta ai titolari di conti correnti bancari" della Polizia Postale del 29 maggio 2024 e Banca d'Italia nella campagna "Occhio alle truffe" lanciata il 14 maggio 2024 in collaborazione con le associazioni dei consumatori sulla tipologia di truffe più diffuse e relative misure di difesa.

14 Cass. Pen., Sez. II, 6 luglio 2023, n. 29346.

vedi l'articolo online

quest'ottica il FATF-GAFI intanto propone di sfruttare le sinergie tra i controlli antifrode e quelli antiriciclaggio. Nel concreto, l'attivazione di servizi di "verifica del beneficiario", rafforzare le informazioni raccolte in onboarding specie se digitale (es. indirizzi IP e coordinate GPS[15]), così come l'implementazione di sistemi di monitoraggio delle transazioni real time facilitano l'individuazione di potenziali segnali di allerta in ottica frodi o estorsioni digitali. Anzi, tra questi, ne sono riportati alcuni esemplificativi di condotte proxy ai crimini digitali.

Ad esempio, sono red flag: un'operatività caratterizzata da ricezione fondi e successivi o multipli prelievi di contanti o bonifici in uscita al fine di svuotare il conto o, se in crypto, acquisto di asset virtuali e trasmissione dell'intero saldo in favore di un unico indirizzo che ha sempre come conseguenza lo svuotamento del conto-crypto; bonifici in uscita in favore di società specializzate nel recupero dei fondi in caso di truffa online o sulla gestione di incidenti informatici; bonifici in entrata ricevuti da compagnie assicurative specializzate nei rischi informatici.

Sul tema red flag collegati alle frodi informatiche a livello italiano sono in corso riflessioni affinché siano assicurate adeguate attività di prevenzione[16] e, in prospettiva, chissà che la nuova Autorità Europea dedicata all'antiriciclaggio fornisca un contributo decisivo per la rilevazione e la segnalazione delle operazioni sospette connesse al cyber-crime.

In conclusione, l'incremento del cyber-crime e del riciclaggio dei riflessi proventi illeciti richiede di stabilire un solido quadro globale che favorisca la collaborazione nella prevenzione, investigazione e perseguimento della criminalità informatica organizzata.[17] La sensibilizzazione dell'opinione pubblica sulle minacce associate al cyber-crime e alle connessioni con le mafie è altrettanto necessaria.

Nel frattempo, la qualità della collaborazione attiva degli intermediari bancari e dei provider di servizi crypto è di importanza cruciale per il suo impatto sull'efficacia e sull'efficienza del sistema antiriciclaggio nel suo complesso.[18] Invero, come vaticinava Giovanni Falcone nel lontano 1991: "*Si è discusso a lungo e si continua a discutere sulla opportunità di una banca dati per tutto il sistema bancario che possa consentire la individuazione delle operazioni sospette; ma si dovrebbe pure cominciare a discutere delle strutture necessarie per la elaborazione di questa enorme massa di dati e per il compimento delle necessarie, conseguenti, indagini; altrimenti, mentre continueremo a discutere sul modo migliore di combattere il riciclaggio, correremo il rischio di apparire come coloro che vogliono gattopardianamente modificare tutto perché tutto resti come prima.*"

15 Cfr. Rapporto Annuale 2023 - Unità di Informazione Finanziaria per l'Italia.

16 Non a caso con il Provvedimento in tema di indicatori di anomalia dell'UIF del 12 maggio 2023, in vigore dal 1° gennaio 2024, non è disposta la non applicabilità, tra gli altri, della Comunicazione UIF del 5 febbraio 2010 - Schemi rappresentativi di comportamenti anomali: frodi informatiche.

17 Rapporto "*Cyber Organized Crime – Le mafie nel cyberspace. Analisi e strumenti di policy*" a cura di A. Nicaso e W. Rauti per Fondazione Magna Grecia rilasciato il 14 giugno 2024.

18 Così, il Direttore della FIU italiana Enzo Serata in audizione alla Commissione Parlamentare di Inchiesta sul fenomeno delle mafie in tema "*le segnalazioni di operazioni sospette e il ruolo della UIF*" il 4 aprile 2024.

vedi l'articolo online

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it