FiscoOggi
RIVISTA ONLINE DELL'AGENZIA DELLE ENTRATE

Articolo pubblicato su FiscoOggi (http://fiscooggi.it)

Dal mondo

Usa, in 1 anno sequestrati dal Fisco 1,8 miliardi di milioni di byte

1 Febbraio 2019

E’ la lotta al cyber-crime la nuova frontiera per le Amministrazioni finanziarie di tutto il mondo

Nel 2018, le Entrate statunitensi hanno creato una speciale unità per i crimini informatici. I risultati sono sorprendenti: più di 500 perquisizioni, rdi di byte, 1.900 pc e 1.800 dispositivi *mobile*.

In realtà, l’Irs, l’equivalente dell’Agenzia delle Entrate italiana, aveva iniziato a sviluppare un programma sperimentale sui crimini informatici per affrontare la crescita esponenziale della criminalità informatica che ha impatto sui sistemi fiscali, finanziari ed economici, già dal 2015. E’ però dal 2018 che nasce una effettiva ed autonoma Cyber Crime Unit (CCU) con sedi a Los Angeles e Washington D.C.

Cos’è la Cyber Crime Unit

La CCU è composta da due gruppi operativi di agenti speciali, personale professionale, ingegneri informatici e agenti speciali di vigilanza (SSA). I rispettivi SSA effettuano le segnalazioni attraverso gli agenti speciali che operano a Los Angeles e Washington, L’Irs ha anche iniziato a collocare agenti speciali della CCU in altri uffici sul campo per facilitare il trasferimento di esperienza investigativa cibernetica. In particolare, le indagini della CCU riguardano Internet e tecnologie basate sul web che consentono ai criminali di svolgere attività illecite con anonimato e senza una presenza fisica definita. L'unità concentra i propri sforzi su indagini che interessano più giurisdizioni, e questo perché casi con ramificazioni più estese pongono generalmente le minacce più significative ai sistemi fiscali, finanziari ed economici, non soltanto degli Stati Uniti. Naturalmente, come per tutti i tipi di crimini all'interno dell'area di responsabilità dell’Irs, gli agenti

speciali che lavorano su indagini sui crimini informatici usano la stessa strategia "*segui il denaro*" che ha reso il coinvolgimento di CI in indagini complesse un punto fermo sin dalla creazione dell'agenzia. Gli sforzi dell'IC sono stati cruciali, ad esempio, in vari casi con al centro il mercato del web, tra cui Silk Road, Mt. Gox, Alphabay, BTC e Backpage.com.

I risultati

Nel 2018, il personale della Cyber Unit dell'Irs ha partecipato a 327 mandati di perquisizione, effettuati in 553 sedi; ha sequestrato 1,76 petabyte di dati da 1.918 computer / laptop / dispositivi esterni e 1.845 dispositivi mobili; e testimoniato in 16 prove. In totale, un volume di 2miliardi di dollari recuperati o osti sotto controllo delle autorità.

Il nuovo diritto informatico di rilevanza fiscale

In sostanza, nei 3 anni passati il fisco Usa ha esteso il suo campo d'intervento in termini di diritto e controllo sulle seguenti tipologie di indagine: • Intrusione di dati, compromissione di e-mail aziendali, schemi di *phishing*, acquisizioni di conti bancari e perdita di dati • Vendita, acquisto e compromissione di informazioni personali tramite Internet • Schemi basati sull'impiego di valute virtuali e riciclaggio di denaro • Proprietari, amministratori e grandi venditori connessi alle aree del "*Dark web*"• Finanziamento del terrorismo che include l'uso di moneta virtuale, reti di rete e altri mezzi online per raccogliere fondi, riciclare i proventi illegali e incanalare denaro per le organizzazioni terroristiche

Criminalità Informatica, non più solo evasione ed elusione

Il fisco Usa continuerà a concentrarsi su reati fiscali e finanziari, espandendo al contempo la propria presenza nell'ambiente cibernetico. La definizione del concetto di criminalità informatica si materializza ogniqualvolta si utilizzi Internet come mezzo essenziale per commettere un crimine, rimanere anonimi, eludere le forze dell'ordine e nascondere transazioni finanziarie, proprietà di beni o altra prova.

Il perché della svolta cyber

Negli ultimi anni, l'Irs ha visto una crescita significativa del numero di criminali che utilizzano l'ambiente cibernetico per facilitare differenti schemi di frodi di rimborso, falsificazione di identità, transazioni finaziarie. Durante lo stesso periodo, gli incidenti di perdita di dati segnalati all'IRS sono aumentati drasticamente. Queste criticità includono intrusioni nei dati personali, compromissione della posta elettronica aziendale, schemi di *phishing* e acquisizioni di conti bancari che hanno colpito le entità del settore privato, cittadini non soltanto aziende, coinvolte nell'ecosistema fiscale e nell'IRS stessa. Questi furti mirano a dati finanziari dettagliati, dichiarazioni dei redditi dell'anno precedente e dati sui salari che i criminali utilizzano per generare

dichiarazioni che rispecchiano la dichiarazione dei redditi effettiva di una vittima. Almeno 10mila i casi rilevati dal 2015 ad oggi. Per questo l’Irs ha deciso di creare una unità innovativa come la Cyber Crime.

Una nuova tipologia investigativa

Le indagini condotte riguardano prove digitali e multimediali che generalmente provengono da molte fonti, come testimoni, citazioni, personal computer, dispositivi mobili (telefoni, tablet, ecc.), Computer / server aziendali di piccole e grandi dimensioni, server farm, cloud storage o persino dalla rete Dark. La corretta raccolta e revisione delle prove digitali richiede che competenze specialistiche siano ammissibili in procedimenti giudiziari.

La funzione primaria di IRS-CI Electronic Crimes è infatti l'acquisizione, l'analisi e la testimonianza forense delle prove digitali e multimediali relative a indagini penali.

di

Stefano Latini

URL: https://www.fiscooggi.it/rubrica/dal-mondo/articolo/usa-1-anno-sequestrati-dal-fisco-18-miliardi-milioni-byte