Con gli atti hackerati a legali e consulenti business milionario

Ivan Cimmarusti


Professionisti

Si dimezzano gli alert antiriciclaggio

Segnalazioni sospette dagli studi in calo del 43,5% con la fine della voluntary disclosure

Con gli atti hackerati a legali e consulenti business milionario

5.052

2,6

Richieste di chiarimenti sul rientro dei capitali

Il prossimo passo è la denuncia di operazioni a rischio-elusione

DÜRER E IL RINASCIMENTO

Furto di dati, rischio di depenalizzazione

Crimini online. Il vice questore Gabrielli spiega le difese Un computer sicuro è un computer scollegato dalla rete. Ma è anche una macchina inutile. «Investimenti nella cyber security e rispetto di canoni di prudenza, magari codificate in best practice aziendali, sono le risposte giuste per la prevenzione agli attacchi hacker», assicura il vice questore Ivano Gabrielli, capo del Cnaipic (Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche) della polizia Postale. In ballo c' è un business milionario basato sul traffico illecito di dati sensibili, spesso sottratti con virus informatici e utilizzati per danneggiare i legittimi titolari, attraverso frodi informatiche ed estorsioni. Non è esclusa la rivendita all' interno dei black market allocati nel dark web, quella parte di internet che rende difficoltosi controlli, perché coperta da un sistema di anonimizzazione. Nel mirino ci sono soprattutto avvocati e commercialisti, ma anche quelle imprese che si rivolgono a questi professionisti per operazioni finanziarie che dovrebbero rimanere segrete ma che rischiano di finire in mano a organizzazioni criminali informatiche che possono rivenderle, favorendo anche forme di insider trading. Dati sensibili e privacy Tutto ruota attorno alla sfera della privacy e al traffico dei dati sensibili, la cui vendita online promette massimi guadagni ma rischi contenuti (si veda l' intervista in basso). Si tratta di materiale riservato che può riguardare «la struttura finanziaria di uno studio professionale o di una azienda - spiega Gabrielli - ma anche dati che attengono alla sfera personale dei soggetti, che così potrebbero finire vittima anche di ricatti». Gli investigatori hanno spesso a che fare con due tipologie di reati informatici, in cui incorrono anche gli studi professionali. Il più critico è il "ransomware": un sistema che può essere paragonato a un «"worm", verme - spiega Gabrielli - che una volta entrato attraverso una email, comincia a muoversi da computer a computer cifrando il contenuto dei file con una

chiave d' accesso impossibile da decifrare. In pochi minuti lo studio professionale si trova privato di tutti i suoi dati. Per riottenerli deve pagare attraverso criptovalute che rendono difficoltosa anche l' indagine di tipo finanziario». Dark web Cosa diversa sono le frodi "Ceo" e "Bec": la prima prende il nome dal chief executive officer - ossia l' amministratore delegato di una società - mentre la seconda da business email compromise. Attraverso queste due forme di frodi gli studi professionali possono vedersi sottrarre dati sensibili riservati che potrebbero essere utilizzati per vari fini, oltre che per truffe. Gli investigatori non escludono che dietro questi attacchi possano nascondersi hacker appositamente ingaggiati sul dark web per entrare nei sistemi informatici di studi professionali e aziende, così da sottrarre documenti sensibili relativi a operazioni finanziarie delicate. Protocolli e cyber security La tutela deve seguire due binari paralleli: da una parte l' investimento in termini di cyber security, un costo relativo a migliorare la sicurezza dell' infrastruttura informatica, dall' altra a pianificare un vero e proprio protocollo cui fare riferimento per arginare al massimo il rischio che i computer siano infettati. «Emanare precise policy aziendali di sicurezza informatica può essere un importante fattore di governo del rischio» conclude Gabrielli.