decripto
.org

Cybersicurezza e Blockchain

Giorgio Scura

Mi chiamo Giorgio Scura, sono un giornalista professionista e fondatore di Decripto, società specializzata nell'analisi delle blockchain a fini forensi e in contrasto alle truffe informatiche. Ringrazio dell'opportunità offertami.

Il Sottosegretario Mantovano ha dato numeri allarmanti e pochissimi attacchi sono stati ricondotti a un responsabile. Inoltre, soprattutto in ambito privato, la percentuale di denunce è bassissima. Crediamo che i numeri, per quanto allarmanti, siano sottostimati.

La verità è che da un punto di vista di sicurezza delle reti informatiche siamo molto vulnerabili. E vi cito una frase che abbiamo intercettato in un gruppo Telegram di hacker russi: "Attaccare l'Italia è come pescare in una vasca da bagno".

Ogni volta che vediamo un profilo social di una carica istituzionale hackerata o l'home page di un sito web di un ministero sostituita con un qualsiasi messaggio, sappiate che è un segnale. Questi gruppi ci vogliono far sapere: "Guardate, siamo dentro, possiamo fare quello che vogliamo".

Non conosciamo il livello di permeabilità delle nostre infrastrutture informatiche. Gli hacker di alto livello, quelli dediti allo spionaggio internazionale, infatti, restano silenti e invisibili. Penetrano e controllano. Leggono, scaricano, informano. Rubano segreti, marchi e brevetti. Monitorano in attesa di un ordine di attacco che potrebbe arrivare in qualsiasi momento.

Allo stato attuale forse non saremmo nemmeno in grado di capire la provenienza dell'attacco. E non sono escluse conseguenze drammatiche come hanno raccontato gli Obama con il loro film "Il Mondo dietro di te". Petroliere che si schiantano sulle coste, comunicazioni internet interrotte, traffico aereo e ferroviario nel caos, strada bloccate, morte, feriti, disperazione….. certo lo scenario peggiore di tutti.

Le cronache degli ultimi tempi, nazionali e internazionali, riportano numerosi attacchi a strutture pubbliche: Albania, Irlanda, ma anche Lazio. La lista è infinita e crescerà ancora perché strumenti come l'intelligenza artificiale aumenteranno la scalabilità di questi attacchi e anche la loro efficacia: cresceranno di quantità e di qualità.

Lo ha detto chiaramente anche il ministro Crosetto, il web è uno scenario militare come aria, terra e acqua e come tale va presidiato.

Dalla nostra esperienza, dopo aver letto il testo, salta all'occhio la mancanza di riferimenti a concetti come criptovalute, blockchain, analisi dei flussi economici (o follow the money), raccolta dati, creazione database o monitoraggio delle reti sociali. Strumenti che riteniamo indispensabili per una risposta immediata a questa emergenza.

Dobbiamo studiare la blockchain e raccogliere dati su di essa, partendo dalla blockchain di Bitcoin.

Il crimine, infatti, ha fatto un salto di qualità nelle attività on-line da quando sono arrivate le criptovalute che hanno permesso di poter inviare e gestire enormi somme di denaro con costi e tempi irrisori e in un regime di semi-anonimato.

Decripto da alcuni anni studia e raccoglie dati sui movimenti di denaro in criptovaluta proveniente da attività illecite a danno di cittadini italiani. Truffe, frodi, riciclaggi da miliardi che poi vanno a finanziare attacchi di ogni genere, come ha detto a questa commissione il Questore Gabrielli.

E vi confermo che da questo punto di vista si può fare molto. Innanzitutto si deve creare un database nazionale in cui censire tutti questi dati relativi ai flussi economici: da dove entrano i soldi nella blockchain, da dove escono, come e chi li riscuote.

Avere queste informazioni è assolutamente necessario ed è il primo passo in chiave di prevenzione e resilienza verso questo tipo di attacchi: dobbiamo avere le informazioni, tonnellate di dati, quelli che Decripto ha già raccolto e quelli che raccoglieremo.

Se vogliamo essere efficaci in questa lotta così importante dobbiamo seguire i soldi, come ci ha insegnato Giovanni Falcone. Queste organizzazioni devono fare molti pagamenti, raccogliere montagne di milioni e poi capire come riciclarli e riuscire a spenderli. E lì possono diventare attaccabili perché spesso usano exchange centralizzati, dove si cambiano euro e dollari per cripto, direttamente come mezzo di pagamento e riciclaggio. Oppure si rendono riconoscibili in altro modo, magari sono stati già segnalati in rete o hanno partecipato ad altre azioni note.

Dobbiamo raccogliere i wallet, gli address e le transazioni.

Acquisire le banche dati esistenti, usare software e intelligenza artificiale per organizzare la difesa, la prevenzione ma anche la previsione di attacchi, perché studiando i modelli su blockchain si possono anche prevedere scenari futuri.

Si consiglia un approccio pratico e snello e l'Agenzia Nazionale della Cybersicurezza deve avere più poteri e deve poter mettere in campo uomini ed attrezzature di primissimo livello.

Deve poter fare indagini operative, avere un ruolo concreto, non solo teorico. E per quanto riguarda le risorse umane, si badi che stiamo parlando di un settore altamente specializzato con stipendi ben più alti della norma. In questo senso si consiglia la possibilità di arruolare anche giovani o giovanissimi in via di formazione, ma con grandi capacità operative.

L’istituzione del Nucleo speciale sarà sicuramente utile, come può esserlo anche uno sportello telematico pubblico per raccogliere queste segnalazioni e i relativi dati anche in forma anonima. Partire dai dati ci aiuterà a capire da dove cominciare: chi è il nemico? Cosa sappiamo di lui? In quali attività criminali è specializzato? E come ricicla i proventi?

In questa occasione, poi, si potrebbe anche fare una riflessione su quali possano essere le tecnologie migliori da mettere in campo in ottica di difesa e di resilienza.

La tecnologia blockchain va presa in considerazione anche sotto questo aspetto, perché offre formidabili soluzioni. Sia per la sicurezza della gestione dei dati, sia per la trasmissione degli stessi, oltre che per il monitoraggio degli accessi alle banche dati e per la protezione delle informazioni sensibili e classificate.

In conclusione possiamo dire che il Ddl è un buon primo passo perché finalmente il problema cybersicurezza in Italia è stato preso in mano, ma di certo non basta. Il nostro consiglio è quello di concentrarsi sui flussi di denaro in rete attraverso le criptovalute, seguendolo.

Giorgio Scura
Mail: info@decripto.org
E-mail: 340 2918970
Decripto.org
Decriptoworld.com