Ransomware, un libro per capire e arginare il fenomeno



Cybercrime: una delle minacce più inquietanti dei nostri tempi. Quante volte abbiamo sentito parlare di crimini informatici, hacker, furto di dati e conseguenti violazioni della privacy? I criminali informatici sono riusciti spesso a invadere spazi protetti della pubblica amministrazione, delle grandi aziende, con il rischio di sottrarre dati importanti, e utilizzarli per scopi illeciti.

Il libro "**Il ransomware nell'economia del cybercrime: analisi d'intelligence sul gruppo Conti**", porta il lettore dentro questi argomenti, fornendo le basi per leggere il fenomeno.

Gli autori, **Giuseppe Brando**, **Marco Di Costanzo** e **Camilla Salini**, spiegando com'è nato il testo, parlano di una "scintilla", ovvero, all'inizio del conflitto russo-ucraino e nel pieno delle prime azioni cinetiche, il collettivo Conti comunica il suo pieno sostegno alla Federazione russa. Evento senza precedenti nel mondo cyber, non si è mai visto un gruppo di criminali, oltretutto di stampo informatico, schierarsi politicamente con il governo di una nazione.

Tre giorni dopo, un'entità non meglio specificata, dopo essere riuscita a entrare in possesso di materiale speciale del gruppo, inizia a riversarlo su Twitter. Il profilo ContiLeaks inizia quindi a rendere pubblici dati riservati e un archivio contenente anni di chat interne tra i membri di uno dei gruppi cibernetici più temuti al mondo: Conti.

Una storia affascinante che, per usare le parole degli stessi autori, apre "una breccia nella cortina di fumo che avvolge la criminalità informatica di lingua russa, dimostrando che la banda operava come una start-up con stipendi, bonus e premi di

riconoscimento per i dipendenti”.

Nell’analisi del fenomeno e nella scrittura gli autori si soffermano sulle operazioni, le dinamiche interne del gruppo e ne analizzano i profili criminologici. Per spiegare qualcosa in più possiamo dire che si tratta di un collettivo russofono di cybercriminali, tra i più attivi nel settore ransomware, che ha preso di mira ospedali, entità governative, istituzioni finanziarie e aziende di tutto il mondo, arrivando a incassare dai riscatti – secondo le stime dell’FBI – più di 200 miliardi di dollari. Per aumentare gli introiti avevano addirittura creato un programma di affiliazione, concedendo l’accesso e l’uso dei loro malware e dei loro servizi ad altri criminali informatici, in cambio di una quota dei riscatti ricevuti.

Una vera e propria spy-story

Prima di portarci all’interno della vicenda che ha come protagonista questo gruppo di criminali, gli autori del libro non trascurano nel dettagliato racconto le origini del fenomeno, nozioni fondamentali non solo per chi si approccia alla materia per la prima volta. Un testo capace di rendere un argomento tecnico alla portata di tutti, che con un linguaggio chiaro e comprensibile fa appassionare curiosi e addetti ai lavori. Chi leggerà il libro troverà molto utili gli schemi, le rappresentazioni grafiche e gli spezzoni di chat, idonei a supportare il lettore nella galassia del cybercrime.

I diritti d’autore saranno interamente devoluti all’associazione di promozione sociale (APS) Informatici senza frontiere.

L’acquisto è disponibile sul sito di Hoeply.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/ransomware-un-libro-per-capire-e-arginare-il-fenomeno/