Ransomware, un libro per capire e arginare il fenomeno

Cybercrime: una delle minacce più inquietanti dei nostri tempi, un problema attualissimo.

Quante volte abbiamo sentito parlare di crimini informatici, hacker, furto di dati, violazioni della privacy?

I criminali informatici riescono sempre più spesso a invadere gli spazi protetti delle aziende, anche delle più grandi, della pubblica amministrazione, degli stessi cittadini, riuscendo a sottrarre dati importanti che poi utilizzano per scopi illeciti.

Una questione affrontata dal libro "Il ransomware nell'economia delle cybercrime: analisi d'intelligence sul gruppo Conti" appena pubblicato da **edizioni Themis** nella collana dedicata alle scienze sociali, tecnologie e sicurezza.

Gli autori **Giuseppe Brando**, **Marco Di Costanzo** e **Camilla Salini**, esperti di analisi delle minacce cyber, affrontano il tema con chiarezza e rigore.

"Il libro – raccontano – nasce da una scintilla, risalente all'inizio del conflitto russo-ucraino, quando il Collettivo Conti comunica il suo pieno sostegno alla Federazione Russa: un evento senza precedenti nel mondo cyber, perché non si era mai visto un gruppo di criminali, oltretutto di stampo informatico, schierarsi politicamente con il governo di una Nazione".

"Tre giorni dopo – proseguono – un'entità non meglio specificata, dopo essere riuscita a entrare in possesso di materiale secretato del gruppo, inizia a riversarlo su Twitter: il profilo ContiLeaks inizia 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".

Una vicenda che sa di spy-story, tanto affascinante quanto inquietante, che secondo gli autori ha aperto "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".

Ma che cos'è il Collettivo Conti?

"Sono cybercriminali, tra i più attivi nel ransomware – spiegano i nostri – che hanno preso di mira ospedali, enti governativi, 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".

Il ransomware è un software dannoso (c.d. malware) che blocca l'accesso di un utente ai propri documenti e dispositivi informatici ed è inviato da soggetti che in cambio chiedono un riscatto sostanzioso per ripristinarne l'accesso da parte del legittimo proprietario.

Nel libro vengono tracciate le origini del fenomeno, analizzati i casi più eclatanti, forniti consigli per mettere in atto misure di sicurezza adeguate.

I diritti d'autore saranno devoluti a Informatici Senza Frontiere (ISF), associazione di promozione sociale che si batte per la "democrazia digitale" e contro il "digital divide".

Ufficio stampa Themis

Giuseppe De Paoli