La criminalità informatica dilaga, così come i gruppi specializzati in operazioni cibernetiche illegali altamente sofisticate. Il conflitto russo-ucraino ha fornito esempi tangibili di come gruppi dediti al cybercrime possano interferire e divertarne parte attiva, schierandosi politicamente e utilizzando le loro capacità per alterare gli equilibri geopolitici.

Questo lavoro di ricerca trae ispirazione da un caso concreto: la presa di posizione di Conti, collettivo criminale russofono attivo dal 2017 e specializzato in attacchi ransomware, a favore dell'operazione militare avviata dalla Russia. Nel testo sono analizzati gli eventi, il modus operandi, le conversazioni via chat dei membri del gruppo.

Attraverso un approccio multidisciplinare, gli autori ci portano all'interno del mondo della cyber-criminalità organizzata e del suo modello di business basato su ransomware e virus informatici. Con l'obiettivo di accrescere la consapevolezza del cybercrime e dei pericoli ad esso legati, verranno analizzate le origini, gli sviluppi e le attività del gruppo Conti, con un focus specifico sui profili criminologici.

Un libro adatto a tutti coloro che vogliono approfondire la conoscenza dell'ecosistema ransomware: manager d'azienda, appassionati, curiosi ma anche a chi vuole avvicinarsi al settore della cyber intelligence.

Collana interdisciplinare
di scienze sociali, tecnologiche e della sicurezza

ISBN 978-88-96069-53-0

€ 20,00

Giuseppe Brando – Marco Di Costanzo – Camilla Salini

Il ransomware nell'economia del cybercrime

EDIZIONI THEMIS

Giuseppe Brando
Marco Di Costanzo
Camilla Salini

Il ransomware nell'economia del cybercrime

Analisi d'intelligence sul gruppo Conti

EDIZIONI THEMIS