

SOMMARIO

PREFAZIONE	7
INTRODUZIONE	11
1. CYBERCRIME: EVOLUZIONE STORICA E PANORAMA UNDERGROUND	13
1.1 Introduzione al Cybercrime	13
1.2 Un po' di storia sugli hacker	16
1.3 Un modello di business organizzato	22
2. LA MINACCIA RANSOMWARE	35
2.1 Nascita ed evoluzione	35
2.2 L'economia dei ransomware	45
3. ANALISI DEL GRUPPO CONTI	53
3.1 Le origini	53
3.2 L'inizio del conflitto Russia-Ucraina	60
3.3 Struttura e gerarchie	64
3.4 Affiliati, colloqui e lavoro	71
3.5 Modalità operative e connessioni	79
3.6 Progetto Blockchain	100
4. PROFILI CRIMINOLOGICI	105
5. LA CYBER THREAT INTELLIGENCE	119
5.1 Definizione dei termini	119
5.2 Modelli di attribuzione	125

6. CONSIDERAZIONI CONCLUSIVE: VERSO UN APPROCCIO PROATTIVO	135
GLOSSARIO	143
BIBLIOGRAFIA	151
FONTI FIGURE	181
GLI AUTORI	183
RINGRAZIAMENTI	185

INTRODUZIONE

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 i gruppi cybercrime possono esserne parte attiva, schierandosi politicamente a favore dell'una o dell'altra parte, utilizzando le loro capacità e strategie per interferire negli equilibri geopolitici e pertanto nei conflitti tra Stati. Questo libro è il frutto di anni di studi dedicati a quel mondo.

Per comprendere lo stato dell'arte, illustriamo prima la storia del cybercrime passando per l'evoluzione del ransomware (un virus informatico capace di bloccare i dispositivi digitali e per il cui sblocco viene richiesto un riscatto) come modello di business illecito, per poi concentrarci sulle operazioni e sulle dinamiche di Conti. Questo collettivo russofono di cybercriminali è annoverato tra i più attivi di sempre nel settore dei ransomware, noto per aver preso di mira ospedali, entità governative, istituzioni finanziarie e aziende di tutto il mondo. Per aumentare gli introiti ha creato un programma di affiliazione, concedendo l'accesso e l'uso dei suoi malware ad altri criminali informatici in cambio di una quota dei riscatti ricevuti.

Il *Federal Bureau of Investigation* (FBI) ha definito Conti come «il ransomware più costoso mai documentato». Si stima che ci

siano state più di 1.000 vittime e che i pagamenti e gli introiti totali dei riscatti abbiano superato i 150 milioni di dollari.¹

Il 24 febbraio 2022 Conti ha offerto il suo pieno sostegno alla Federazione russa, che aveva appena invaso l'Ucraina. Dopo solo tre giorni, compare online l'account Twitter @ContiLeaks; qualcuno, dopo essere riuscito a entrare nel server del gruppo scovando i dati riservati e le chat segrete dei membri, ha cominciato a divulgare queste informazioni.

Grazie alle prove tangibili individuate, per i ricercatori di cybersecurity, le forze dell'ordine e le agenzie d'intelligence, è stato possibile studiare le dinamiche di Conti, gli strumenti e le infrastrutture usate per gli attacchi informatici, le modalità operative dell'organizzazione, fino all'identificazione di probabili legami con le agenzie di intelligence del governo russo. Questo ha permesso di aprire 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.

Inoltre, la profilazione delle caratteristiche comportamentali di questi criminali informatici permetterà al lettore di fare un viaggio nella loro mente, di comprendere chi sono, cosa fanno nella vita e le motivazioni che li spingono a eseguire azioni di questo genere.

Insomma, sembra davvero la trama di un film, invece è la realtà.

¹ <https://www.state.gov/reward-offers-for-information-to-bring-conti-ransomware-variant-co-conspirators-to-justice/>