**A colpi di cyber: il profilo dei moderni pirati del web**

Pubblicato da [**Anna Popa**](https://www.scienzeforensi.org/blog/?author=Anna_Popa) in [Digital Forensics & Cyber Security](https://www.scienzeforensi.org/blog/?category=Digital_Forensics_%26_Cyber_Security) · 29 Aprile 2022

Nelle ultime settimane, la stampa mondiale si mostra quasi ridondante nell’inserire termini quali *Cyber War, cyber attacchi, guerra cibernetica* vicino ai titoli inerenti alla recente guerra in Ucraina. Nonostante l’attuale conflitto non sia né il primo né l'unico dove vengono utilizzate azioni cibernetiche, l’interesse mediatico è decisamente più significativo rispetto ad altri scontri.

Prima di addentrarsi nella comprensione di questi vocaboli, è necessario fare un passo indietro cercando di capire le generalità e le caratteristiche di coloro che sono alla base di tali azioni: gli **hacker**, o come si dice in gergo, *i pirati del web.*

**Hacking e le sue tipologie**

Con il termine “hacking” - *dall’inglese to hack, attaccare*- si intende l'insieme dei metodi, delle tecniche e delle operazioni volte a conoscere, accedere e modificare un sistema informatico hardware (parte tangibile del computer, come, ad esempio il monitor, la tastiera o il mouse) o software (parte intangibile, traducibile come il supporto logico del computer). Quindi, tali attività sono volte alla compromissione di dispositivi digitali e di intere reti, intaccando tutto ciò che è protetto senza averne l’autorizzazione. Colui che pratica l’hacking viene identificato come hacker.

Gli hacker vengono in genere classificati in tre tipologie: **black, white e grey hat**.

Il colore nero è associato ai black hat, meglio conosciuti come **“crackers”**; essi hanno un’intenzione criminale, volta alla violazione di dati sensibili utilizzandoli a proprio vantaggio. Nel gergo comune, essi sono detti *cybercriminali.*

Il bianco viene associato ai white hat (in italiano **hacker etici**), i quali lottano continuamente contro gli attacchi della controparte *black*; solitamente, essi lavorano per il Governo o per conto di associazioni, con l’intento di rafforzare la sicurezza di un sistema informatico, proteggendolo da un’eventuale azione offensiva.

Infine, il colore grigio è collegato agli hackers che non si schierano né da una parte, né dall'altra. Le loro intenzioni sono considerate sia buone, in quanto una volta entrati in un sistema informatico, le informazioni ottenute non vengono utilizzate per un vantaggio personale, tanto quanto cattive, in quanto essi, essendo hackers a tutti gli effetti, invadono tutto ciò per cui occorre avere un’autorizzazione, naturalmente senza averla.

**Il caso Anonymous**

Un’organizzazione collocata fra i *grey hat* potrebbe essere **Anonymous**. Nella cronaca recente, in particolare in riferimento al conflitto fra Russia e Ucraina, il nome di Anonymous è salito alla ribalta per la decisione di hackerare la televisione russa trasmettendo su tutti i canali, in diretta nazionale, immagini inerenti al conflitto che proseguiva in Ucraina.

L’ideologia che li accomuna sembra essere basata principi di stampo etico e morale quali la libertà di parola e di espressione, l’uguaglianza e la difesa dei più deboli e degli oppressi. **Attacchi informatici: tra interessi e danni economici.**

Un hacker che si macchia di crimini informatici, ad esempio vendendo informazioni di vulnerabilità di un’azienda a terzi, può raggiungere introiti che superano il milione. **L’Italia nel 2021 è stato il quarto Paese al mondo e il primo in Europa più colpito dai malware**, con 62.371.693 attacchi (nel 2020 erano stati 22.640.386).

Le aziende lotteranno ininterrottamente per tutelarsi e difendersi dai numerosi attacchi offensivi e infine persone comuni, continueranno a sentirsi vittime. La soluzione? La **cybersecurity** è sicuramente una.

Énoncé : *Veuillez effectuer un résumé en langue française d’environ 180 -190 mots.*