

La sicurezza cibernetica in Italia

Le operazioni cibernetiche condotte a danno del nostro Paese da attori statuali, organizzazioni criminali e hacktivisti hanno coinvolto soggetti pubblici e privati. Sono state impiegate diverse tecniche di attacco e, tra le finalità perseguite, ha assunto maggiore rilevanza il tentativo di acquisire vantaggi economici e strategici. Le seguenti elaborazioni statistiche si riferiscono alle attività cibernetiche ostili osservate nel 2024 in danno di assetti informatici rilevanti per la sicurezza nazionale.

DEFINIZIONI

Tipologie di attori

Cyber espionage

Comprende tutte le azioni di spionaggio poste in essere in genere da attori di natura statale o state sponsored, condotte con l'uso di sistemi informatici o telematici.

Criminalità

Sono incluse tutte le azioni di matrice criminale, perpetrate attraverso l'utilizzo abusivo di un sistema informatico o telematico.

Hacktivismo

Azioni riconducibili all'attivismo digitale, condotte mediante l'uso sovversivo di computer o computer network al fine di promuovere un'agenda politica o principi di connotazione sociale.

Tecniche

Defacement

Attacco condotto contro un sito web e consistente nel modificare i contenuti dello stesso limitatamente alla home page ovvero includendo anche le sottopagine del sito.

DDoS (Distributed Denial of Service)

Attacco DoS lanciato da un elevato numero di sistemi compromessi e infetti (botnet), volto a rendere un sistema informatico o una risorsa non disponibile ai legittimi utenti attraverso la saturazione delle risorse e il sovraccarico delle connessioni di rete dei sistemi server.

SQL Injection

Offensive volte ad attaccare – tramite lo sfruttamento di specifiche vulnerabilità – applicazioni che gestiscono dati, al fine di accedere alle funzioni di amministrazione del sistema, oltre che sottrarre o alterare dati stessi.

Bug hunting

Azioni che prevedono lo studio e l'analisi del target attraverso la ricerca di vulnerabilità (bug) sfruttabili in un'eventuale successiva azione ostile.

Registrazione domini malevoli

Attività relative alla registrazione di domini web

Finalità

Discredito

Condotte finalizzate a influenzare negativamente le opinioni dell'utenza o della collettività verso un determinato target.

Vantaggio economico/strategico

Azioni poste in essere al fine di trarre vantaggio economico o acquisire un vantaggio strategico a discapito del target.

Spionaggio

Azioni condotte con finalità spionistica, nel cui ambito l'attore ostile accede a dati sensibili o confidenziali per scopi strategici o economici.

Esiti

Esfiltrazione dati

Offensive che hanno avuto come esito la copia, il trasferimento o la sottrazione illecita di dati da un sistema informativo.

Attività prodromiche

Include tutte le attività preliminari utili a raccogliere informazioni per identificare e selezionare l'obiettivo di future operazioni cibernetiche, a partire da caratteristiche e vulnerabilità dei sistemi.

Minaccia avanzata e persistente (APT)

Operazioni particolarmente mirate e persistenti, solitamente portate avanti da attori di matrice statale o state sponsored, in genere condotte mediante l'impiego di malware all'interno delle reti bersaglio al fine di mantenere attivi i canali impiegati per l'esfiltrazione di informazioni sensibili o confidenziali dalle infrastrutture IT del target.

Condizionamento opinione pubblica

Azioni ostili in grado di influenzare l'opinione pubblica, polarizzandola verso gli obiettivi strategici dell'attore ostile che le pone in essere.

Furto d'identità/credenziali

Offensive che si concretizzano nell'esfiltrazione di credenziali/identità dai sistemi del target, successivamente impiegate per condurre azioni ostili o messe in vendita su portali e forum dedicati del dark & deep web.

Negazione del servizio

Azioni digitali ostili che provocano l'esaurimento delle risorse di un sistema che eroga pubblicamente un servizio (ad esempio un sito web su un web server), fino a renderlo non più in grado di rispondere alle richieste degli utenti.

