# Ogni mese ti proteggiamo dalle nuove minacce del Web

Fondamentale è adottare una protezione adeguata dei propri dati, soprattutto contro Malware e Phishing. PC, Tablet, smartphone e in generale tutti i device che si connettono alla rete sono i punti più deboli da proteggere. Scarica la Guida Navigazione Sicura e leggi i Termini e Condizioni del Servizio


## Cosa sono i Botnet?

Una botnet, o rete di bot è una rete composta da un gran numero di computer controllati clandestinamente da un aggressore informatico (hacker). Assumendo il controllo di centinaia o perfino migliaia di computer, le botnet vengono generalmente utilizzate per inviare spam o virus, rubare i dati personali o lanciare attacchi DDoS. Sono considerate una delle principali minacce online odierne.

Un attacco DDoS (Distributed Denial of Service) è un tentativo ostile di bloccare il normale traffico di un server, servizio o rete sopraffacendo la vittima o l'infrastruttura circostante inondandola di traffico Internet. Gli attacchi DDoS raggiungono l'efficacia sfruttando come fonti di attacco più sistemi informatici compromessi.

È possibile riconoscere un computer infetto da una botnet nello stesso modo in cui si identifica un computer infetto da altri tipi di malware. I segnali includono un rallentamento del computer, un funzionamento insolito dello stesso, la comparsa di messaggi di errore o l'avvio improvviso della ventola con il computer non utilizzato. Questi sono tutti possibili sintomi del controllo in remoto del computer all'interno di una rete di bot.

## Cos'è il Malware?

Acronimo di malicious software (software dannoso) è in generale un software che attacca e danneggia altri software alterandone il comportamento atteso. Il malware va inteso anche come un programma che può rubare di nascosto informazioni di vario tipo, da commerciali a private (es. credenziali di accesso, numero carte di credito, etc..), senza essere rilevato dall'utente anche per lunghi periodi di tempo. Oltre a carpire informazioni di nascosto, un malware può essere creato con l'intento di arrecare danni ad un sistema informatico, spesso tramite sabotaggio oppure può criptare i dati del computer della vittima, estorcendo denaro per la decriptazione.

Tra i principali tipi di malware si possono elencare trojan, ransomware (molto noto "WannaCry" che ha colpito tra i 200 e i 300 mila computer in oltre 150 paesi), spyware, hijacker, miner, rootkit, adware, malvertising, keylogger.

## Cos'è il Phishing?

Il phishing è un tipo di truffa effettuata su Internet attraverso la quale un malintenzionato cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso, fingendosi un ente affidabile in una comunicazione digitale. Si tratta di un'attività illegale ove il malintenzionato effettua un invio massivo di messaggi che imitano, nell'aspetto e nel contenuto, messaggi legittimi di fornitori di servizi; tali messaggi fraudolenti richiedono di fornire informazioni riservate come, ad esempio, il numero della carta di credito o la password per accedere ad un determinato servizio. Per la maggior parte è una truffa perpetrata usando messaggi di posta elettronica, ma non mancano casi simili che sfruttano altri mezzi, quali i messaggi SMS, i post su social media quali twitter/facebook, etc..

Aggiornato al 30/06/2024