Threat Intelligence

Il malware include virus, worm, cavalli di Troia e spyware. Dopo una diminuizione globale del malware durante la pandemia (2020-2021), il suo utilizzo è aumentato notevolmente entro la fine del 2021, quando le persone hanno iniziato a tornare in ufficio.

Il malware o “software malevolo” è un termine generico che descrive un programma o un codice dannoso che mette a rischio un sistema.

I malware cercano di invadere, danneggiare o disattivare compute, sistemi, rete e dispositivi mobili, spesso assumendo il controllo parziale delle operazioni del dispositivo.

Lo scopo del malware è quello di lucrare illecitamente a spese degli utenti.

Nel 2022, gli attacchi ransomware sono state una delle minacce informatiche principali.

I ransomware sono malware che impediscono all’utente di accedere al proprio dispositivo, e, in molti casi criptando i file, obbligando a pagare un riscatto per riottenerli. I ransomware son stati definiti “l’arma scelta” dei criminali perché richiedono un pagamento rapido e ingente in criptovalute difficili da rintracciare. Il codice dei ransomware è semplice da ottenere su marketplace criminali e difendersi da essi è qausi imossibile.

Un Trojan o “Cavallo di Troia” è uno dei malware più pericolosi. Di solito si presenta come qualcosa di utile, per ingannare l’utente. Una volta ottenuto l’accesso, i criminali ottengono l’accesso non autorizzato del computer della vittima. Da qui i Trojan possono essere utilizzati per per rubare dati finanziari o installare altre minacce, come virus o ransomware.