PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 27 - numero 5851 di Lunedì 19 maggio 2025

Il rapporto annuale Mandiant sulla evoluzione dei crimini informatici

Il crimine a base economica è il più diffuso, in particolare, il ransomware assume una posizione dominante. Ecco una breve panoramica del contenuto del volume, che i lettori potranno scaricare con il link riportato in fondo al testo.

La pubblicazione annuale, curata da Mandiant, offre una panoramica aggiornata delle varie tipologie di crimine informatico, registrate nel 2024. Ancora una volta il ransomware rappresenta il 55% degli attacchi, in crescita rispetto al 2022 ed al 2023. Evidentemente, il crimine informatico è redditizio, per i malviventi, e quindi non deve stupire il costante aumento di questa specifica tipologia; merita però attenzione il fatto che i criminali informatici diventano sempre più abili e utilizzano strumenti di attacco sempre più efficaci.

Il documento evidenza come queste tipologie di attacco si articolino in vari modi, sia mediante il blocco dell'accesso ai dati del soggetto attaccato, sia mediante furto dei dati, sia mediante alterazione dei dati stessi.

Si evolvono anche le modalità con cui i malviventi chiedono il pagamento del riscatto, utilizzando ad esempio cripto valute.

Gli studiosi hanno anche rilevato come gli attacchi possano diventare più sofisticati grazie ad applicativi di intelligenza artificiale ed a tecnologie automatizzate, che permettono ad esempio di rendere sempre più agevole la perpetrazione di attacchi per DDoS (Distributed Denial of service).

Le tecniche più diffuse di attacco ai sistemi informativi delle vittime si basano sulla penetrazione, consentita da vulnerabilità note (33% dei casi). La seconda tipologia di attacco prevede invece l'uso di credenziali di accesso, ottenute in vari modi, come ad esempio con phishing di posta elettronica, compromissioni del Web ed altre tecniche ormai abbastanza conosciute.

Di particolare interesse è il tempo richiesto per portare a termine l'attacco, dopo che i malviventi sono penetrati del sistema attaccato. Mediamente sono necessari 11 giorni per l'introduzione nel sistema, il predisporre le tecniche specifiche di attacco e alla fine per impartire il colpo di grazia. Questo intervallo di tempo si è ridotto, rispetto agli anni precedenti, quando questo intervallo si aggirava sui 16 giorni. Gli esperti ritengono che l'utilizzo di applicativi di intelligenza artificiale possa aver dato un significativo contributo alla riduzione di questo tempo di perpetrazione dell'attacco.

I compilatori del manuale hanno prestato particolare attenzione alle attività criminose informatiche, sviluppate da malviventi riconducibili a specifiche nazioni. Anche se i mezzi di comunicazione di massa danno ampio rilievo a queste categorie di attaccanti, nella realtà si tratta di numeri relativamente modesti, rispetto a quelli legati alle attività di criminali comuni. Ciò non toglie che i gruppi, sostenuti da paesi sovrani, hanno spesso portato a termine attacchi particolarmente dannosi, come ad esempio gli attacchi perpetrati nel 2024 sulla infrastruttura informatica ucraina, a supporto dell'invasione russa. Questi gruppi vengono adesso classificati con una sigla APT (APT ? advanced persistent threat), seguita da un numero. Ad esempio, il gruppo APT 45 è riconducibile senza esitazione al regime nordcoreano ed è descritto in questo manuale come un operatore alquanto sofisticato, presente sul campo sin dal lontano 2009.

Se è vera l'affermazione che il primo compito di un esperto, per difendersi da un attaccante, è di conoscere le sue modalità operative, non v'è dubbio che questo manuale rappresenti un prezioso strumento di aggiornamento delle tecniche di attacco, a disposizione dei responsabili della sicurezza informatica.

MANDIANT - M-TRENDS ? 2025 REPORT

Adalberto Biasiotti