REPORT ANALISI WEB APP

Dal report fornito, ci sono alcuni punti che potrebbero essere considerati significativi, ma non necessariamente indicano attività sospette o malevole:

considerazioni:

Autorun delle web app: dal report fornito si evince come le applicazioni web si siano lanciate da sole, questo può essere dovuto ad un'impostazione che prevede la loro apertura all'avvio del sistema.

Richieste di indirizzi IP non trovati: Ripetute richieste per risolvere nomi di dominio in indirizzi IP risultano in "IP Addresses not found". Questo potrebbe indicare problemi di risoluzione DNS. Questo non è in sé un segnale di attività malevola, ma potrebbe suggerire che il sistema ha difficoltà a connettersi a determinati servizi.

Tempi di risposta elevati: I tempi di risposta per molte richieste sono eccessivamente lunghi. Un ritardo così lungo nel caricamento delle risorse potrebbe essere indicativo di congestione della rete o di problematiche con il server di destinazione, piuttosto che un attacco malevolo.

Conclusioni:

Per trarre conclusioni più sicure, sarebbe utile avere ulteriori informazioni, come la frequenza delle richieste, e se queste avvengano a seguito dell'accensione della macchina, o successivamente ad altri eventi.

Alcuni attacchi prevedono un sovraccarico e successivo rallentamento del sistema tramite richieste di collegamento, allo scopo di rendere più occultato l'ingresso di file malevoli o l'utilizzo di funzioni sospette, rendendo difficile il loro rilevamento, ma non sembra essere questo il caso.

Altri attacchi prevendono la condivisione di pagine web "apparentemente" legittime, che sono in realtà fasulle e aventi come scopo, quello di inviare i dati delle credenziali inserite in fase di accesso, ad una terza parte.

In caso di sistemi connessi alla rete aziendale, si sconsiglia comunque l'utilizzo di queste Web App.

Si pensa quindi che il report presenti solo un autorun delle Web App, con successivi problemi di connessione.

Suggeriamo comunque di mantenerci aggiornati su eventuali altri eventi sospetti, e di lanciare scansioni con software antivirus per avere maggiori certezze.