RELAZIONE ANALISI ACCESSO AI SOCIAL NETWORK TRAMITE ANY.RUN

Introduzione

Il presente documento riporta l'esito di un'analisi eseguita con la piattaforma **ANY.RUN**, riguardante un'attività sospetta rilevata all'interno di un ambiente aziendale.
L'analisi, effettuata in data **25 agosto 2024 alle ore 16:48:49**, ha avuto come oggetto il processo **chrome.exe**, avviato su un sistema operativo **Windows 10 Pro**.

Lo scopo dell'analisi è stato verificare l'eventuale presenza di **minacce informatiche** durante un accesso non autorizzato o improprio a **siti di social network** (nello specifico **Instagram** e **Facebook**) da parte di un utente interno all'infrastruttura aziendale.

Link ANY.RUN:
https://app.any.run/tasks/f1f20828-2222-46fb-a886-09f77581e67b

Link report any.run:
https://any.run/report/6df8ab4acfc5c751f09f2c8632464c8c5e6da9d04539a69edb0fc53cb561dfbc/f1f20828-2222-46fb-a886-09f77581e67b

Svolgimento

1. Dati tecnici del file analizzato

- **Nome file**: `chrome.exe`
- **Tipo di malware**: **Nessuna minaccia rilevata**
- **Hash identificativi**:
    - **MD5**: `4C091A5A8C03EBC2EA267980D0DA9F8D`
    - **SHA1**: `F52CB78B7F23559FFCE5D1125EFD7B399165DFFC`
    - **SHA256**: `6DF8AB4ACFC5C751F09F2C8632464C8C5E6DA9D04539A69EDB0FC53CB561DFBC`

2. Risultati dell’analisi

- **Processi totali rilevati**: 139
- **Processi monitorati attivamente da ANY.RUN**: 10
- **Processi sospetti o malevoli**: **0**

L’analisi ha evidenziato che non vi sono comportamenti anomali, indicatori di compromissione (IoC) o attività dannose associate al processo `chrome.exe`.
Tuttavia, è stato rilevato che l’utente ha **tentato l’accesso a pagine social** tramite Google Chrome, in particolare su **Instagram e Facebook**, attività che **non è correlata a operazioni lavorative legittime** e può rappresentare un rischio dal punto di vista della sicurezza informatica.

Conclusione

L’analisi eseguita su `chrome.exe` ha **escluso la presenza di malware**, confermando l’integrità del sistema durante la sessione registrata.
Tuttavia, l’utilizzo di dispositivi aziendali per accedere a social network può:

- Esporre il sistema a **minacce esterne** come **phishing, malware drive-by e truffe online**.
- Rappresentare un **rischio per la produttività e la sicurezza operativa**, soprattutto in contesti ad alta riservatezza.

Raccomandazioni per l’ambiente aziendale

- **Bloccare l’accesso ai social network** tramite policy firewall/DNS nei dispositivi aziendali.
- **Monitorare regolarmente il traffico web** per identificare attività non conformi.
- **Fornire formazione sulla sicurezza informatica** per sensibilizzare i dipendenti sui rischi legati alla navigazione inappropriata.
- Applicare **criteri di utilizzo accettabile** (AUP – Acceptable Use Policy) chiaramente definiti e condivisi.