Report di Analisi Malware - Nessuna Minaccia Rilevata

Nome File: chrome.exe

Verdetto: Nessuna minaccia rilevata

Data Analisi: 25 Agosto 2024 alle 22:44:49

Sistema Operativo: Windows 10 Professional (64 bit)

Indicatori di Compromissione (IoCs)

- **MD5:** 4C091A5A8C03EBC2EA267980D0DA9F8D
- **SHA1:** F52CB78B7F23559FFCE5D1125EFD7B399165DFFC
- **SHA256:** 6DF8AB4ACFC5C751F09F2C8632464C8C5E6DA9D04539A69EDB0FC53CB561DFBC

Opzioni di Analisi

- **Durata:** 300 secondi
- **Rete:** Attiva
- **Privacy:** Pubblica
- **MITM Proxy:** Disattivato
- **Route via Tor:** No

Software Presenti nel Sistema

- Google Chrome (122.0.6261.70)
- Microsoft Edge (122.0.2365.59)
- Mozilla Firefox (123.0)
- Microsoft Office Professional 2019 (varie lingue)
- Adobe Acrobat (23.001.20093)
- Java 8 Update 271 (64-bit)
- FileZilla 3.65.0

Indicatori di Attività

- **Nessuna minaccia identificata**
- **Nessuna attività sospetta**
- **Nessuna esecuzione di processi dannosi**

L'analisi del file "Malware analysis 2" non ha rilevato alcuna minaccia o attività sospetta. Il file non mostra segni di comportamento dannoso o compromissione del sistema.

Possibile Tentativo di Phishing

Anche se il file analizzato non presenta rischi, è sempre opportuno prestare attenzione a possibili tentativi di phishing. Il phishing è una tecnica utilizzata da cybercriminali per ingannare gli utenti e indurli a inserire le proprie credenziali in siti malevoli che imitano quelli legittimi (ad esempio, home banking, portali aziendali o social network).

Come Comportarsi in Caso di Phishing:

1. **Verificare l'URL** prima di inserire credenziali o informazioni sensibili.
2. **Non cliccare su link sospetti** ricevuti via email o messaggi.
3. **Non scaricare allegati non richiesti**, specialmente se provenienti da mittenti sconosciuti.
4. **Segnalare immediatamente** qualsiasi email o messaggio sospetto al reparto IT.
5. **Utilizzare password uniche e complesse** e attivare l'autenticazione a due fattori (2FA) quando possibile.

Accesso ai Social Network sul Posto di Lavoro

L'accesso ai social media sul posto di lavoro può rappresentare un rischio per la sicurezza aziendale, in quanto:

- Aumenta l'esposizione a tentativi di phishing.
- Può essere veicolo di malware o link dannosi.
- Riduce la produttività e incrementa il rischio di divulgazione accidentale di informazioni aziendali.

Per questi motivi, si raccomanda di evitare l'accesso ai social network dai dispositivi aziendali e di attenersi alle policy di sicurezza interne.

Conclusioni

L'analisi condotta sul file "Malware analysis 2" non ha evidenziato alcun comportamento malevolo. Tuttavia, è sempre fondamentale adottare misure preventive per proteggere il sistema da eventuali minacce informatiche, come il phishing e l'uso improprio di risorse aziendali. La sicurezza informatica è una responsabilità condivisa e ogni utente deve essere consapevole dei rischi e delle buone pratiche da adottare per garantire un ambiente di lavoro sicuro.

Analisi completa disponibile su:

Link all'analisi