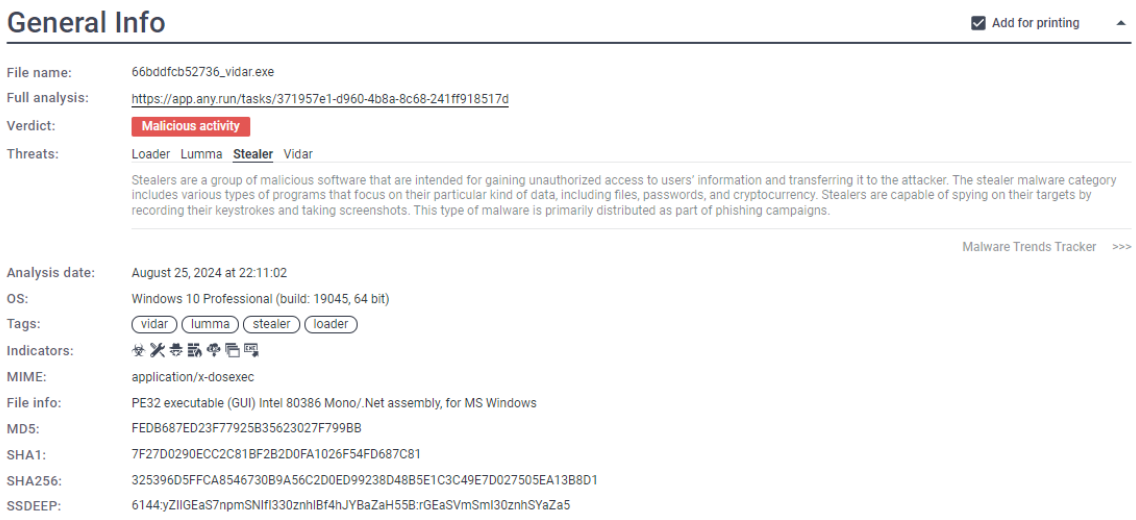
Esercizio 2 – Anyrun I – vidar.exe

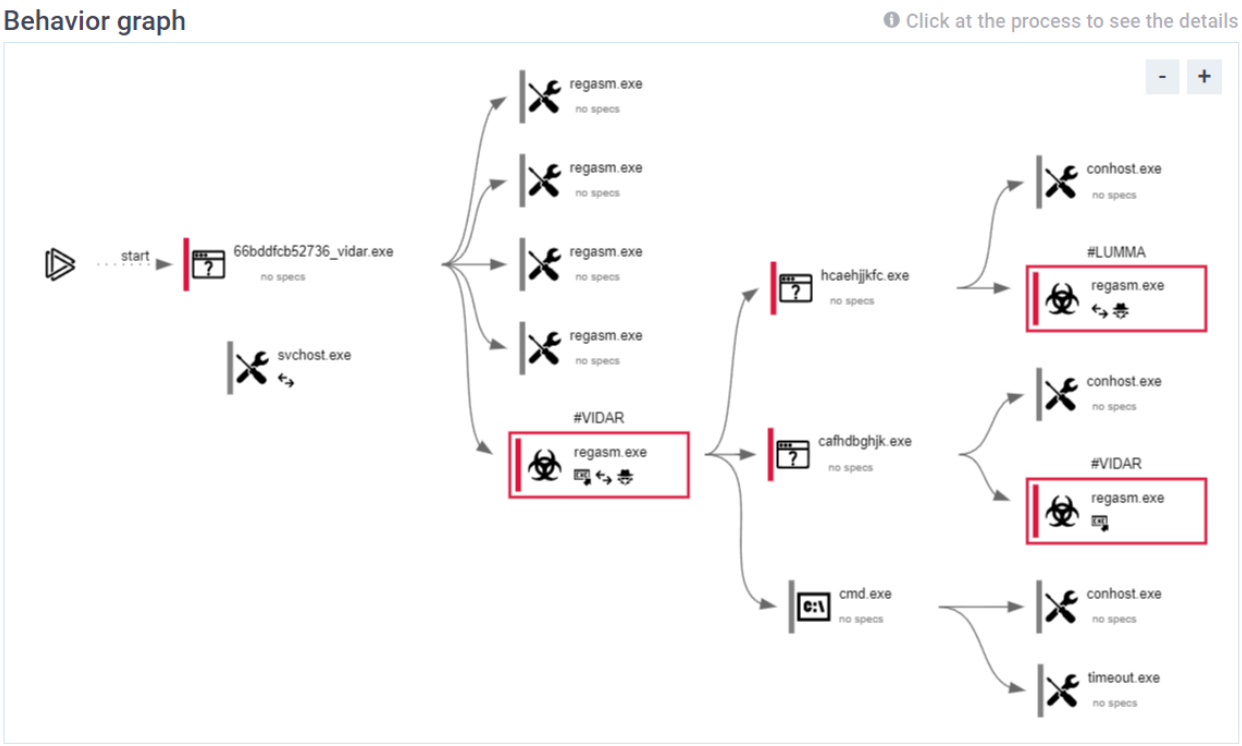
File Analizzato: 66bddfcb52736_vidar.exe

Verdetto: Attività dannosa rilevata.

Descrizione delle Minacce, I

1. **Vidar (Stealer)**: Questo malware ruba informazioni personali e criptovalute, colpendo credenziali di accesso, dati del browser, e wallet digitali. È particolarmente pericoloso per la sua capacità di evolversi, implementando regolari aggiornamenti.
2. **Lumma (Stealer)**: Malware sviluppato per sottrarre dati di accesso e informazioni sensibili. Target primario sono account finanziari e portafogli digitali, con modalità avanzate di evasione che rendono complesso il rilevamento.
3. **Loader**: Un software nocivo che ha il compito di infiltrarsi nei dispositivi per installare e diffondere altri malware (come trojan o stealer). I loader vengono comunemente veicolati tramite email di phishing o link ingannevoli, sfruttando la manipolazione psicologica per indurre l'utente a scaricare e aprire file infetti.





Azioni Rilevate

- **Download e Installazione di File Eseguibili**: Sono stati osservati tentativi di scaricare ulteriori eseguibili potenzialmente dannosi.
- **Accesso a Credenziali Browser e Wallet**: L'infezione tenta di sottrarre dati da browser (come cronologia, credenziali e dati di pagamento).
- **Evasione dei Controlli di Sicurezza**: Il malware verifica impostazioni di sicurezza del sistema e modifica impostazioni di sistema per garantire la persistenza.

Raccomandazioni di Remediation

1. **Messa in Quarantena del File**: Il file dovrebbe essere immediatamente messo in quarantena per evitare ulteriori propagazioni all'interno della rete aziendale.
2. **Eliminazione dei File Infetti**: Dopo l'analisi e una volta confermata la dannosità, si raccomanda di eliminare tutti i file correlati al malware rilevati nel sistema, garantendo la rimozione completa.
3. **Blacklist dei Domini e IP Correlati**: Gli indirizzi IP e i domini utilizzati dal malware per le comunicazioni dovrebbero essere bloccati per prevenire future connessioni e attività sospette.
4. **Consultazione del Vendor Antivirus**: Vista la natura avanzata dei malware Vidar e Lumma, si consiglia di consultare il fornitore di software antivirus per verificare se esistano aggiornamenti o patch che possano migliorare la rilevazione e la protezione contro queste minacce.
5. **Monitoraggio e Analisi Post-Infezione**: Per identificare eventuali compromissioni residue, è fondamentale attivare un monitoraggio approfondito della rete e dei sistemi colpiti, verificando log di accesso e attività sospette.

Considerazioni Finali

Questi malware rappresentano minacce concrete per la sicurezza dei dati aziendali. Implementare le misure di remediation suggerite e adottare strategie preventive (come formazione sulla sicurezza informatica per evitare il phishing) ridurranno notevolmente il rischio di infezioni future.

Panoramica della minaccia – Anyrun II

1. **Verifica del malware**: Non sono state rilevate minacce note, indicatori dannosi o comportamenti sospetti. Gli elementi analizzati (file eseguibili, connessioni di rete e richieste DNS) non mostrano attività anomale.
2. **Attività del sistema**: I processi monitorati (principalmente legati a Google Chrome) hanno eseguito normali operazioni di sistema come lettura/scrittura di chiavi di registro e creazione di file temporanei, senza evidenze di infezioni.

Dalla verifica risulta un *falso positivo*, dove il file è stato segnalato per errore come possibile minaccia. Questo significa che non sono necessarie azioni correttive invasive come l'eliminazione o la quarantena.

Scelte di remediation consigliate

- **Falso positivo**: Nessun intervento distruttivo. È possibile **aggiungere il file in una whitelist** o segnalarlo come sicuro, evitando future segnalazioni inutili.
- **Richiesta al vendor**: In alcuni casi, è consigliabile contattare il fornitore del software per verificare che il comportamento sia normale, soprattutto se aggiornamenti del software possono prevenire falsi positivi futuri.

Questa gestione consente di evitare interruzioni non necessarie delle attività e ridurre i falsi allarmi, garantendo al contempo che il sistema continui a funzionare senza rischi di infezioni reali.