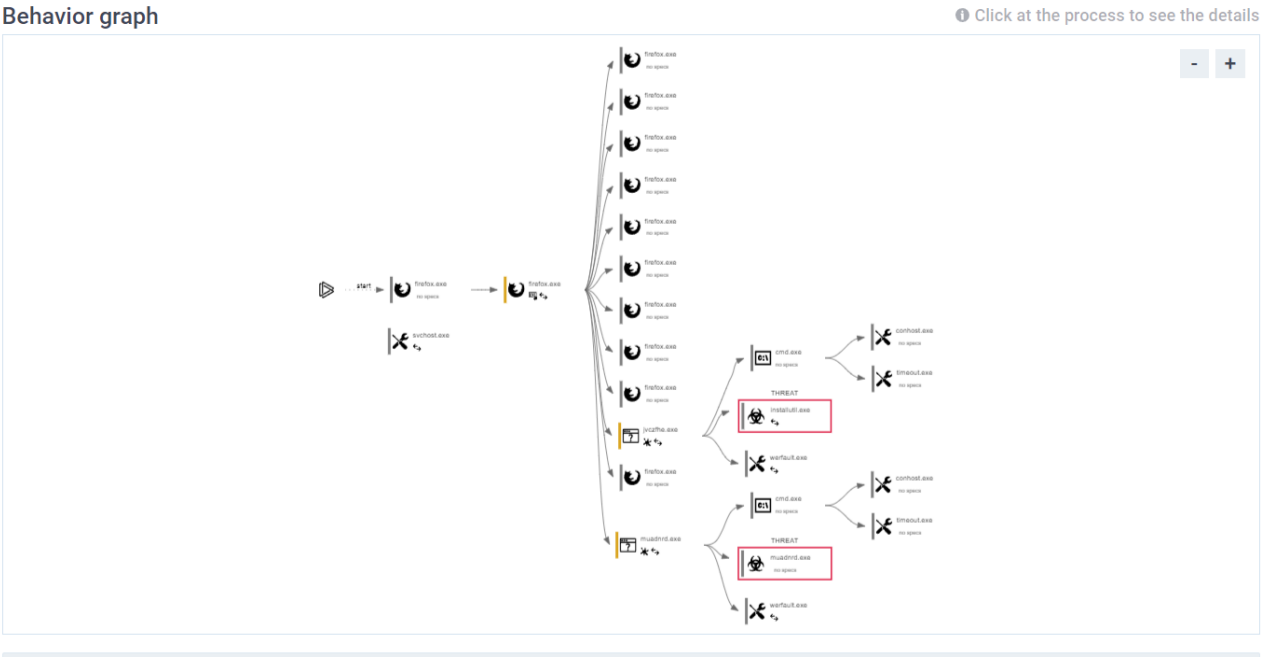
Bonus 1 – Anyrun

1. **Verdetto**: l'attività è stata classificata come malevola.
2. **Sistema operativo**: Windows 10 Professional, 64-bit.
3. **Indicatori di compromissione**:
    - **Hash** del file per identificazione:
        - MD5: `00B5E91B42712471CDFBDB37B715670C`
        - SHA1: `D9550361E5205DB1D2DF9D02CC7E30503B8EC3A2`
        - SHA256: `0307EE805DF8B94733598D5C3D62B28678EAEADBF1CA3689FA678A3780DD3DF0`



Attività sospette rilevate

- **Esecuzione di comandi tramite CMD.EXE**: `Jvczfhe.exe` ha avviato comandi tramite la console.
- **Modifica delle impostazioni di sicurezza di Internet Explorer** e lettura delle chiavi di registro di Microsoft Office, suggerendo tentativi di evasione delle difese del sistema e possibili esfiltrazioni.
- **Timeout per ritardare l'esecuzione** tramite il comando `TIMEOUT.EXE`, un comportamento comune nei malware per eludere l'analisi.
- **Connessioni a porte insolite** e tentativi di accesso ai settaggi di proxy.

Analisi dei processi e delle modifiche di registro

- Il file ha interagito con diversi processi, inclusi `InstallUtil.exe` e `cmd.exe`, per eseguire operazioni sulla configurazione di sistema e applicare modifiche ai registri.
- Ha disabilitato i log di traccia, suggerendo un tentativo di evitare rilevazioni.

File e directory modificate

- Sono stati creati e modificati file all'interno della directory dell'utente, comprese impostazioni di sicurezza e configurazioni di browser.

Conclusioni

L'analisi rileva che `Jvczfhe.exe` mostra comportamenti dannosi, con azioni che modificano impostazioni di sicurezza e utilizzano processi di sistema per nascondere la propria presenza. Per mitigare, è consigliabile un'ulteriore analisi del file e un ripristino del sistema compromesso.